

1.0 USE AND APPLICATION

1.1 Definitions

-----NOTE-----

The defined terms of this section appear in capitalized type and are applicable throughout these Technical Specifications and Bases.

<u>Term</u>	<u>Definition</u>
ACTIONS	ACTIONS shall be that part of a Specification that prescribes Required Actions to be taken under designated Conditions within specified Completion Times.
ACTUATION LOGIC TEST	An ACTUATION LOGIC TEST —Analog (the application of —Analog (application of test for <u>the test for which is applied to</u> analog equipment) shall be the application of analog equipment) various simulated or actual input combinations in conjunction with each possible interlock logic state required for OPERABILITY of a logic circuit and the verification of the required logic output, <u>including Time Delays</u> . The ACTUATION LOGIC TEST —Analog, as a minimum, shall include a continuity check of output devices.
ACTUATION LOGIC TEST (application of test for digital equipment, PSMS)	An ACTUATION LOGIC TEST is a check of the PSMS software memory integrity to ensure there is no change to the internal PSMS software that would impact its functional operation or the continuous self-test function.
	The PSMS is self-tested on a continuous basis from the digital side of all input modules to the digital side of all output modules. Self-testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. For the PSMS the self-testing is described in Topical Report, "Safety I&C System Description and Design Process," MUAP-07004 Section 4.3 and Topical Report, "Safety System Digital Platform—MELTAC," MUAP-07005 Section 4.1.5. The software memory integrity test is described in Topical Report, "Safety I&C System Description and Design Process," MUAP-07004 Section 4.4.1 and Topical Report, "Safety System Digital Platform—MELTAC," MUAP-07005 Section 4.1.4.1.c.
AXIAL FLUX DIFFERENCE (AFD)	AFD shall be the difference in normalized flux signals between the top and bottom halves of a two section excor neutron detector.

1.1 Definitions

CHANNEL CALIBRATION

A CHANNEL CALIBRATION shall be the adjustment, as necessary, of ~~the channel~~ output measurement devices such that ~~it the channel~~ responds within the necessary range and accuracy to known values of the parameter that the channel monitors.

The CHANNEL CALIBRATION shall encompass all devices in the channel required for channel OPERABILITY. This shall include the processing of the signal within the digital controller to which the channel measurement device is directly interfaced (i.e., RPS, ESFAS or SLS).

CHANNEL CALIBRATION encompasses devices that are subject to drift between surveillance intervals and all input devices that are not tested through continuous automated automatic self-testing. Refer to TADOT for output devices that are not tested through continuous ~~automated~~ automatic self-testing.

The performance of a CHANNEL CALIBRATION shall be consistent with ~~specification~~ Specification 5.5.21 "Setpoint Control Program" (SCP).

~~For analog measurements on each Technical Specification required automatic protection instrumentation function implemented with a digital bistable function,~~ CHANNEL CALIBRATION confirms the accuracy of the channel from sensor to digital Visual Display Unit (VDU) readout, ~~as described in Topical Report, "Safety I&C System Description and Design Process," MUAP-07004 Section 4.4.2. The digital value read on the VDU originates in the controller that processes the trip, actuation, interlock or safety-related display Functions, and is the same digital value processed for those Functions. The CHANNEL CALIBRATION overlaps with other surveillance requirements to adequately test the PSMS safety Functions.~~

~~For analog measurements,~~ CHANNEL CALIBRATION confirms the analog measurement channel accuracy at five calibration settings corresponding to 0%, 25%, 50%, 75% and 100% of the instrument range. ~~During the calibration of the instrument, the analog signal generated by the instrument is confirmed via the calibration settings on any VDU (e.g., Operational VDU or Safety VDU).~~

~~For analog measurements on each Technical Specification required automatic protection instrumentation function implemented with an analog bistable function, the CHANNEL CALIBRATION confirms the accuracy of the channel from~~

~~sensor to output device. For these channels, CHANNEL CALIBRATION confirms the analog measurement accuracy at the Nominal Trip Setpoint (NTSP).~~

For binary measurements, the CHANNEL CALIBRATION confirms the accuracy of the channel's state change, ~~as described in Topical Report, "Safety I&C System Description and Design Process," MUAP-07004 Section 4.4.1~~ at the required setpoint.

Calibration of instrument channels with resistance temperature detector (RTD) or thermocouple sensors may consist of an in-place qualitative assessment of sensor behavior and normal calibration of the remaining ~~adjustable~~ devices in the channel.

The CHANNEL CALIBRATION may be performed by means of any series of sequential, overlapping, or total channel steps.

CHANNEL CHECK

A CHANNEL CHECK shall be the qualitative assessment, by observation, of channel behavior during operation. This determination shall include, where possible, comparison of the channel indication and status to other indications or status derived from independent instrument channels measuring the same parameter. A CHANNEL CHECK may be conducted manually or automatically. Either method may be used to satisfy the surveillance frequency requirement. Where the CHANNEL CHECK is conducted automatically, an alarm shall be generated when the agreement criteria are not met. If the automated CHANNEL CHECK function is unavailable, a manual CHANNEL CHECK shall be conducted at the minimum surveillance frequency.

1.1 Definitions

<p>CHANNEL OPERATIONAL TEST (COT) <u>TEST (COT)</u> -Analog (application of test for analog equipment)</p>	<p>A COT -Analog shall be the injection of a simulated or actual signal into the channel as <u>close to at a point that overlaps with the sensor as practicable signal checked during CHANNEL CALIBRATION</u> to verify OPERABILITY of all <u>remaining</u> devices in the channel required for channel OPERABILITY. - The COT -Analog shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for channel OPERABILITY such that the setpoints are within the necessary range and accuracy. - The COT -Analog may be performed by means of any series of sequential, overlapping, or total channel steps.</p>
<p>CHANNEL OPERATIONAL TEST (COT) (application of test for digital equipment, PSMS)</p>	<p>A COT is a check of the PSMS software memory integrity to ensure there is no change to the internal PSMS software that would impact its functional operation or the continuous self test function.</p> <p>The PSMS is self-tested on a continuous basis from the digital side of all input modules to the digital side of all output modules. Self testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. For the PSMS the self-testing is described in Topical Report, "Safety I&C System Description and Design Process," MUAP-07004 Section 4.3 and Topical Report, "Safety System Digital Platform-MELTAC," MUAP-07005 Section 4.1.5. The software memory integrity test is described in Topical Report, "Safety I&C System Description and Design Process," MUAP-07004 Section 4.4.1 and Topical Report, "Safety System Digital Platform-MELTAC," MUAP-07005 Section 4.1.4.1.c.</p>
<p>CORE ALTERATION</p>	<p>CORE ALTERATION shall be the movement of any fuel, sources, or reactivity control components, within the reactor vessel with the vessel head removed and fuel in the vessel. Suspension of CORE ALTERATIONS shall not preclude completion of movement of a component to a safe position.</p>
<p>CORE OPERATING LIMITS REPORT (COLR)</p>	<p>The COLR is the unit-specific document that provides cycle-specific parameter limits. These cycle-specific parameter limits shall be determined for each cycle in accordance with Specification 5.6.3. Plant operation within these limits is addressed in individual Specifications.</p>

1.1 Definitions

DOSE EQUIVALENT I-131	DOSE EQUIVALENT I-131 shall be that concentration of I-131 (microcuries/gram) that alone would produce the same committed effective dose equivalent as the quantity and isotopic mixture of I-131, I-132, I-133, I-134, and I-135 actually present. The dose conversion factors used for this calculation shall be those listed in Table 2.1 of EPA Federal Guidance Report No. 11, "Limiting Values of Radionuclide Intake and Air Concentration and Dose Conversion Factors for Inhalation, Submersion, and Ingestion," EPA-520/1-88-020, September 1988.
DOSE EQUIVALENT XE-133	DOSE EQUIVALENT XE-133 shall be that concentration of Xe-133 (microcuries per gram) that alone would produce the same effective dose equivalent as the quantity and isotopic mixture of noble gases (Kr-85m, Kr-85, Kr-87, Kr-88, Xe-133, and Xe-135) actually present. The dose conversion factors used for this calculation shall be those listed in Table III.1 of EPA Federal Guidance Report No. 12, "External Exposure to Radionuclides in Air, Water, and Soil," EPA 402-R-93-081, September 1993.
ENGINEERED SAFETY <u>FEATURES</u> FEATURE (ESF) RESPONSE TIME (ESF) <u>RESPONSE TIME</u>	The ESF RESPONSE TIME shall be that time interval from _when the monitored parameter exceeds its actuation setpoint at the channel sensor until the ESF equipment is -capable of performing its safety function (i.e., the valves travel to their required positions, pump discharge pressures reach their required values, etc.). Times shall include Class 1E GTG starting and sequence loading delays, where applicable. The response time may be measured by means of any series of sequential, overlapping, or total steps so that the entire response time is measured. In lieu of measurement, response time may be verified for selected components provided that the components and methodology for verification have been previously reviewed and approved by the NRC. <u>The ESF RESPONSE TIME includes post-test maintenance as necessary, based on manufacturer's recommendation, to maintain device reliability.</u>

1.1 Definitions

LEAKAGE

LEAKAGE shall be:

a. Identified LEAKAGE

1. LEAKAGE, such as that from pump seals or valve packing (except reactor coolant pump (RCP) seal water injection or leakoff), that is captured and conducted to collection systems or a sump or collecting tank,
2. LEAKAGE into the containment atmosphere from sources that are both specifically located and known either not to interfere with the operation of leakage detection systems or not to be pressure boundary LEAKAGE, or
3. Reactor Coolant System (RCS) LEAKAGE through a steam generator to the Secondary System (primary to secondary LEAKAGE);

b. Unidentified LEAKAGE

All LEAKAGE (except RCP seal water injection or leakoff) that is not identified LEAKAGE, and

c. Pressure Boundary LEAKAGE

LEAKAGE (except primary to secondary LEAKAGE) through a nonisolable fault in an RCS component body, pipe wall, or vessel wall.

MEMORY INTEGRITY CHECK (MIC)

A MEMORY INTEGRITY CHECK (MIC) is a check of the PSMS software memory integrity to ensure there is no change to the internal PSMS software that would impact its functional operation, including digital Nominal Trip Setpoint values, Time Constants, Time Delays or the continuous automatic self-test function. The MIC overlaps with other surveillance requirements to adequately test the PSMS safety functions.

The PSMS is automatically self-tested on a continuous basis from the digital side of all input modules to the digital side of all output modules. Continuous automatic self-testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. For the PSMS the continuous automatic self-testing is described in "Safety I&C System Description and Design Process," MUAP-07004 Section 4.3 and "Safety System

Digital Platform -MELTAC-, "MUAP-07005 Section 4.1.5. The software memory integrity test is described in "Safety I&C System Description and Design Process, "MUAP-07004 Section 4.4.1 and "Safety System Digital Platform -MELTAC-, "MUAP-07005 Section 4.1.4.1.c.

MODE

A MODE shall correspond to any one inclusive combination of core reactivity condition, power level, average reactor coolant temperature, and reactor vessel head closure bolt tensioning specified in Table 1.1-1 with fuel in the reactor vessel.

1.1 Definitions

OPERABLE – OPERABILITY	A system, subsystem, train, component, or device shall be OPERABLE or have OPERABILITY when it is capable of performing its specified safety function(s) and when all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication, and other auxiliary equipment that are required for the system, subsystem, train, component, or device to perform its specified safety function(s) are also capable of performing their related support function(s).
PHYSICS TESTS	<p>PHYSICS TESTS shall be those tests performed to measure the fundamental nuclear characteristics of the reactor core and related instrumentation. These tests are:</p> <ol style="list-style-type: none"> a. Described in Chapter 14, Initial Test Program, b. Authorized under the provisions of 10 CFR 50.59, or c. Otherwise approved by the Nuclear Regulatory Commission.
PRESSURE AND TEMPERATURE LIMITS REPORT (PTLR)	The PTLR is the unit specific document that provides the reactor vessel pressure and temperature limits, including heatup and cooldown rates and the low temperature overpressure protection arming temperature, for the current reactor vessel fluence period. These pressure and temperature limits shall be determined for each fluence period in accordance with Specification 5.6.4.
QUADRANT POWER TILT RATIO (QPTR)	QPTR shall be the ratio of the maximum upper excore detector calibrated output to the average of the upper excore detector calibrated outputs, or the ratio of the maximum lower excore detector calibrated output to the average of the lower excore detector calibrated outputs, whichever is greater.
RATED THERMAL POWER (RTP)	RTP shall be a total reactor core heat transfer rate to the reactor coolant of 4451 MWt.

1.1 Definitions

REACTOR TRIP SYSTEM (RTS) RESPONSE TIME	The RTS RESPONSE TIME shall be that time interval from when the monitored parameter exceeds its RTS trip setpoint at the channel sensor until loss of stationary gripper coil voltage. The response time may be measured by means of any series of sequential, overlapping, or total steps so that the entire response time is measured. In lieu of measurement, response time may be verified for selected components provided that the components and methodology for verification have been previously reviewed and approved by the NRC. <u>The RTS RESPONSE TIME includes post-test maintenance as necessary, based on manufacturer's recommendation, to maintain device reliability.</u>
<u>SAFETY VDU TEST</u>	<u>A SAFETY VDU TEST is a check of the touch response and display OPERABILITY of the Safety VDU (S-VDU). Safety VDU touch screens are tested by manually touching screen targets and confirming correct safety VDU response. The SAFETY VDU TEST overlaps with the MIC for the Safety VDU processor, to ensure the S-VDU is OPERABLE. The SAFETY VDU TEST is explained in "Safety I&C System Description and Design Process," MUAP-07004 Section 4.4.1.</u>
SHUTDOWN MARGIN (SDM)	SDM shall be the instantaneous amount of reactivity by which the reactor is subcritical or would be subcritical from its present condition assuming: <ul style="list-style-type: none"> <li data-bbox="633 1197 1442 1501">a. All rod cluster control assemblies (RCCAs) are fully inserted except for the single RCCA of highest reactivity worth, which is assumed to be fully withdrawn. However, with all RCCAs verified fully inserted by two independent means, it is not necessary to account for a stuck RCCA in the SDM calculation. With any RCCA not capable of being fully inserted, the reactivity worth of the RCCA must be accounted for in the determination of SDM, and <li data-bbox="633 1533 1442 1638">b. In MODES 1 and 2, the fuel and moderator temperatures are changed to the nominal zero power design level.
STAGGERED TEST BASIS	A STAGGERED TEST BASIS shall consist of the testing of one of the systems, subsystems, channels, or other designated components during the interval specified by the Surveillance Frequency, so that all systems, subsystems, channels, or other designated components are tested during n Surveillance Frequency intervals, where n is the total

number of systems, subsystems, channels, or other designated components in the associated function.

THERMAL POWER

THERMAL POWER shall be the total reactor core heat transfer rate to the reactor coolant.

1.1 Definitions

**TRIP ACTUATING DEVICE
OPERATIONAL TEST
(TADOT)**

A TADOT shall consist of operating the trip actuating device and verifying the OPERABILITY of all devices in the channel required for trip actuating device OPERABILITY. ~~The TADOT shall include adjustment, as necessary, of the trip actuating device so that it actuates at the required setpoint within the necessary accuracy.~~ The TADOT may be performed by means of any series of sequential, overlapping, or total channel steps.

There are two types of binary devices - those that have no drift potential, such as Manual Initiation switches and Actuation Outputs, and those that have drift potential, such as undervoltage (UV) relays, valve position limit switches and RTB trip devices. The ~~operability~~ OPERABILITY of binary devices that have drift potential is confirmed through CHANNEL CALIBRATION and/or RESPONSE TIME testing. For some binary devices subject to drift potential, a TADOT may be specified in addition to these surveillance requirements. The ~~operability~~ OPERABILITY of binary devices that have no drift potential is confirmed only through TADOT. ~~The~~

For devices with drift potential, the CHANNEL CALIBRATION confirms the accuracy of the device's binary state change with regard to its trip setpoint requirement (i.e., the Allowable Value). The RESPONSE TIME test confirms the accuracy of the devices state change with regard to its trip timing requirement. The TADOT confirms only the state change ~~operability~~ OPERABILITY (i.e., there is no setpoint or timing accuracy confirmation needed). The TADOT also includes ~~adjustments~~ maintenance as necessary, based on manufacturer's recommendation, to maintain device reliability.

For some binary devices with drift potential, a TADOT is specified in addition to the CHANNEL CALIBRATION and/or RESPONSE TIME test. The TADOT is specified on a more frequent basis than the CHANNEL CALIBRATION or RESPONSE TIME test, to confirm the state change ~~operability~~ OPERABILITY of the devices, without checking its state change setpoint or timing accuracy. Checking the setpoint or timing accuracy more frequently than the CHANNEL CALIBRATION or RESPONSE TIME test interval is unnecessary, because the total channel uncertainty, including setpoint and/or timing drift between test intervals, is included in determination of the Nominal Setpoint, the Allowable Value and the response time requirement.

Table 1.1-1 (page 1 of 1)
MODES

MODE	TITLE	REACTIVITY CONDITION (k_{eff})	% RATED THERMAL POWER ^(a)	AVERAGE REACTOR COOLANT TEMPERATURE (°F)
1	Power Operation	≥ 0.99	> 5	NA
2	Startup	≥ 0.99	≤ 5	NA
3	Hot Standby	< 0.99	NA	≥ 350
4	Hot Shutdown ^(b)	< 0.99	NA	$350 > T_{avg} > 200$
5	Cold Shutdown ^(b)	< 0.99	NA	≤ 200
6	Refueling ^(c)	NA	NA	NA

(a) Excluding decay heat.

(b) All reactor vessel head closure bolts fully tensioned.

(c) One or more reactor vessel head closure bolts less than fully tensioned.

3.1 REACTIVITY CONTROL SYSTEMS

3.1.9 PHYSICS TESTS Exceptions – MODE 2

LCO 3.1.9 During the performance of PHYSICS TESTS, the requirements of:

LCO 3.1.3, "Moderator Temperature Coefficient,"
LCO 3.1.4, "Rod Group Alignment Limits,"
LCO 3.1.5, "Shutdown Bank Insertion Limits,"
LCO 3.1.6, "Control Bank Insertion Limits," and
LCO 3.4.2, "RCS Minimum Temperature for Criticality"

may be suspended and the number of required channels for LCO 3.3.1, "RTS Instrumentation," Functions 2, 3 and 15.c, may be reduced to 3 required channels, provided:

- a. RCS lowest loop average temperature is $\geq 541^{\circ}\text{F}$,
- b. SDM is within the limits specified in the COLR, and
- c. THERMAL POWER is $\leq 5\%$ RTP.

APPLICABILITY: During PHYSICS TESTS initiated in MODE 2.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. SDM not within limit.	A.1 Initiate boration to restore SDM to within limit.	15 minutes
	<u>AND</u> A.2 Suspend PHYSICS TESTS exceptions.	1 hour
B. THERMAL POWER not within limit.	B.1 Open reactor trip breakers.	Immediately
C. RCS lowest loop average temperature not within limit.	C.1 Restore RCS lowest loop average temperature to within limit.	15 minutes

ACTIONS (continued)

CONDITION	REQUIRED ACTION	COMPLETION TIME
D. Required Action and associated Completion Time of Condition C not met.	D.1 Be in MODE 3.	15 minutes

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.1.9.1	Perform a -CHANNEL CALIBRATION on power range and intermediate range channels <u>per SR 3.3.1.109</u> , consistent with SR 3.3.1.10 , and Specification 5.5.21, Setpoint Control Program (SCP).	Prior to initiation of PHYSICS TESTS
SR 3.1.9.2	Verify the RCS lowest loop average temperature is $\geq 541^{\circ}\text{F}$.	[30 minutes OR In accordance with the Surveillance Frequency Control Program]
SR 3.1.9.3	Verify THERMAL POWER is $\leq 5\%$ RTP.	[30 minutes OR In accordance with the Surveillance Frequency Control Program]
SR 3.1.9.4	Verify SDM is within the limits specified in the COLR.	[24 hours OR In accordance with the Surveillance Frequency Control Program]

3.3 INSTRUMENTATION

3.3.1 Reactor Trip System (RTS) Instrumentation

LCO 3.3.1 The RTS instrumentation for each Function in Table 3.3.1-1 shall be OPERABLE.

APPLICABILITY: According to Table 3.3.1-1.

ACTIONS

-----NOTE-----
Separate Condition entry is allowed for each Function.

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more Functions with one or more required channels or trains inoperable.	A.1 Enter the Condition referenced in Table 3.3.1-1 for the channel(s) or train(s).	Immediately
B. One required Manual Reactor Trip train Function inoperable.	B.1 Restore three trains train to OPERABLE status.	72 hours
	<u>OR</u> B.2 Be in MODE 3.	78 hours
C. One required Manual Reactor Trip train Function inoperable.	C.1 Restore train to OPERABLE status.	72 hours
	<u>OR</u> C.2.1 Initiate action to fully insert all rods.	72 hours
	<u>AND</u> C.2.2 Place the Rod Control System in a condition incapable of rod withdrawal.	73 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
D. One required train inoperable.	D.1 Restore train to OPERABLE status.	48 hours
	<u>OR</u>	
	D.2.1 Initiate action to fully insert all rods. <u>AND</u> D.2.2 Place the Rod Control System in a condition incapable of rod withdrawal.	48 hours 49 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
E. One High Power Range Neutron Flux (high setpoint <u>High Setpoint</u>) channel inoperable.	<p>-----NOTE----- One channel may be bypassed for up to 12 hours for surveillance testing and<u>or</u> setpoint adjustment, <u>provided the other channels are OPERABLE or placed in the trip condition.</u> -----</p>	
	E.1.1 Place channel in trip.	72 hours
	<u>AND</u>	
	E.1.2 Reduce THERMAL POWER to $\leq 75\%$ RTP.	78 hours
	<u>OR</u>	
	E.2.1 Place channel in trip.	72 hours
	<u>AND</u>	
	E.2.2 -----NOTE----- Only required to be performed when the Power Range Neutron Flux input to QPTR is inoperable. -----	
	Perform SR 3.2.4.2.	Once per 12 hours
<u>OR</u>		
E.3 Be in MODE 3.		78 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
F. One required channel inoperable.	<p>-----NOTE----- For High Power Range Neutron Flux channels only, one <u>One</u> channel may be bypassed for up to 12 hours for surveillance testing →, <u>provided the other channels are OPERABLE or placed in the trip condition.</u></p> <p>-----</p> <p>F.1 Place channel in trip.</p> <p><u>OR</u></p> <p>F.2 Be in MODE 3.</p>	<p>72 hours</p> <p>78 hours</p>
G. One High Intermediate Range Neutron Flux channel inoperable.	<p>G.1 Reduce THERMAL POWER to < P-6.</p> <p><u>OR</u></p> <p>G.2 Increase THERMAL POWER to > P-10.</p>	<p>24 hours</p> <p>24 hours</p>
H. Two High Intermediate Range Neutron Flux channels inoperable.	<p>H.1 -----NOTE----- Limited plant cooldown or boron dilution is allowed provided the change is accounted for in the calculated SDM.</p> <p>-----</p> <p>Suspend operations involving positive reactivity additions.</p> <p><u>AND</u></p> <p>H.2 Reduce THERMAL POWER to < P-6.</p>	<p>Immediately</p> <p>2 hours</p>

CONDITION	REQUIRED ACTION	COMPLETION TIME
I. One High Source Range Neutron Flux channel inoperable.	<p>-----NOTE----- Limited plant cooldown or boron dilution is allowed provided the change is accounted for in the calculated SDM. -----</p> <p>I.1 Suspend operations involving positive reactivity additions.</p>	Immediately
J. Two High Source Range Neutron Flux channels inoperable.	J.1 Open reactor trip breakers (RTBs).	Immediately
K. One High Source Range Neutron Flux channel inoperable.	<p>K.1 Restore channel to OPERABLE status.</p> <p><u>OR</u></p> <p>K.2.1 Initiate action to fully insert all rods.</p> <p><u>AND</u></p> <p>K.2.2. Place the Rod Control System in a condition incapable of rod withdrawal.</p>	<p>48 hours</p> <p>48 hours</p> <p>49 hours</p>

CONDITION	REQUIRED ACTION	COMPLETION TIME
L. One required channel inoperable.	<p>-----NOTE----- Except for Pressurizer Pressure, Pressurizer Level, and SG Water Level, one <u>One required</u> channel may be bypassed for up to 12 hours for surveillance testing, <u>provided the other required channels are OPERABLE or placed in the trip condition.</u></p> <p>-----</p> <p>L.1 Place channel in trip.</p> <p><u>OR</u></p> <p>L.2 Reduce THERMAL POWER to < P-7.</p>	<p>72 hours</p> <p>78 hours</p>
M. One required train inoperable.	<p>-----NOTE----- One inoperable <u>required</u> train may be bypassed for up to 4 hours for surveillance testing, provided the other two <u>required</u> trains are OPERABLE.</p> <p>-----</p> <p>M.1 Restore train to OPERABLE status.</p> <p><u>OR</u></p> <p>M.2 Be in MODE 3.</p>	<p>24 hours</p> <p>30 hours</p>
N. One required RTB train inoperable.	<p>N.1 Restore train to OPERABLE status.</p> <p><u>OR</u></p> <p>N.2 Apply the requirements of 5.5.18.</p>	<p>24 hours</p> <p>24 hours]</p>

CONDITION	REQUIRED ACTION	COMPLETION TIME
O. One or more channels inoperable.	O.1 Verify interlock is in required state for existing unit conditions. <u>OR</u> O.2 Be in MODE 3.	1 hour 7 hours
P. One or more <u>trains inoperable or one or more required</u> channels inoperable.	P.1 Verify interlock is in required state for existing unit conditions. <u>OR</u> P.2 Be in MODE 2.	1 hour 7 hours
Q. One trip mechanism inoperable for <u>one required</u> RTB.	Q.1 Restore inoperable trip mechanism to OPERABLE status. <u>OR</u> Q.2 Apply the requirements of Specification 5.5.18.	48 hours 48 hours]
R. One required train inoperable.	-----NOTE----- One <u>inoperable required</u> train may be bypassed for up to 4 hours for surveillance testing, provided the other <u>two required</u> trains are OPERABLE. ----- R.1 Restore train to OPERABLE status. <u>OR</u> R.2 Apply the requirements of Specification 5.5.18.	 24 hours 24 hours]

CONDITION	REQUIRED ACTION	COMPLETION TIME
S. Required Action and associated Completion Time for Condition N, Q, or R not met.	S.1 Be in MODE 3.	6 hours
え	<p>-----NOTE----- One channel may be bypassed for up to 12 hours for surveillance testing. -----</p> <p>T.1 Place channel in trip.</p> <p><u>OR</u></p> <p>T.2 Reduce thermal power <u>THERMAL POWER</u> to <-P-7</p>	<p>12 hours</p> <p>18 hours</p>
<u>U. One required channel inoperable.</u>	<p><u>U.1 Place channel in trip.</u></p> <p><u>AND</u></p> <p><u>U.2 Restore channel to OPERABLE status.</u></p>	<p><u>1 hour</u></p> <p><u>72 hours</u></p>
<u>V. Required Action and associated Completion Time of Condition U not met.</u>	<u>V.1 Be in MODE 3.</u>	<u>6 hours</u>
<u>W. One required channel inoperable.</u>	<p><u>W.1 Place channel in trip.</u></p> <p><u>AND</u></p> <p><u>W.2 Restore channel to OPERABLE status.</u></p>	<p><u>1 hour</u></p> <p><u>72 hours</u></p>
<u>X. Required Action and associated Completion Time of Condition W not met.</u>	<u>X.1 Reduce THERMAL POWER to < P-7.</u>	<u>6 hours</u>

--	--	--

SURVEILLANCE REQUIREMENTS

-----NOTE-----
Refer to Table 3.3.1-1 to determine which SRs apply for each RTS Function.

SURVEILLANCE	FREQUENCY
SR 3.3.1.1 Perform CHANNEL CHECK.	[12 hours OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.1.2 -----NOTE----- 1. Not required to be performed until 12 hours after THERMAL POWER is \geq 15% RTP. ----- Compare results of calorimetric heat balance calculation to power range channel output. Adjust power range channel output if calorimetric heat balance calculations results exceed power range channel output by more than +2% RTP.	[24 hours OR In accordance with the Surveillance Frequency Control Program]

SURVEILLANCE	FREQUENCY
<p>SR 3.3.1.3</p> <p>-----NOTE----- Not required to be performed until 24 hours after THERMAL POWER is \geq 15% RTP. -----</p> <p>Compare results of the incore detector measurements to Nuclear Instrumentation System (NIS) AFD. Adjust NIS channel if absolute difference is \geq 3%.</p>	<p>[31 effective full power days (EFPD)]</p> <p>OR</p> <p>In accordance with the Surveillance Frequency Control Program]</p>
<p>SR 3.3.1.4 Perform TADOT.</p>	<p>[62 days on a STAGGERED TEST BASIS]</p> <p>OR</p> <p>In accordance with the Surveillance Frequency Control Program]</p>
<p>SR 3.3.1.5 Perform ACTUATION LOGIC TEST.</p>	<p>[24 months]</p> <p>OR</p> <p>In accordance with the Surveillance Frequency Control Program]</p>

SURVEILLANCE	FREQUENCY
<p>SR 3.3.1.65</p> <p>-----NOTE----- Not required to be performed until 24 hours after THERMAL POWER is $\geq 50\%$ RTP. -----</p> <p>Calibrate excore channels to agree with incore detector measurements.</p>	<p>[92 EFPD OR In accordance with the Surveillance Frequency Control Program]</p>
<p>SR 3.3.1.7</p> <p>-----NOTE----- Not required to be performed for source range instrumentation prior to entering MODE 3 from MODE 2 until 4 hours after entry into MODE 3. -----</p> <p><u>6</u> Perform COTMIC consistent with Specification 5.5.21, Setpoint Control Program (SCP).</p>	<p>[24 months OR In accordance with the Surveillance Frequency Control Program]</p>

SURVEILLANCE	FREQUENCY
SR 3.3.1. 8 <u>7</u> Perform CHANNEL CHECK.	Within 4 hours after reducing power below P-6 <u>AND</u> [Every 12 hours thereafter OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.1.9 NOTE This Surveillance shall include verification that the time constants are adjusted to the prescribed values. <u>8</u> Perform a-CHANNEL CALIBRATION on each required channel consistent with Specification 5.5.21, Setpoint Control Program (SCP).	[24 months OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.1. 10 <u>9</u> -----NOTE----- Neutron detectors are excluded from CHANNEL CALIBRATION. ----- Perform a-CHANNEL CALIBRATION on each required channel consistent with Specification 5.5.21, Setpoint Control Program (SCP).	[24 months OR In accordance with the Surveillance Frequency Control Program]

SURVEILLANCE	FREQUENCY
<p>SR 3.3.1.11<u>10</u> Perform a-CHANNEL CALIBRATION on each required channel consistent with Specification 5.5.21, Setpoint Control Program (SCP).</p>	<p>[24 months OR In accordance with the Surveillance Frequency Control Program]</p>
<p>SR 3.3.1.12 NOTE Verification of setpoint is not required.</p> <p><u>11</u> Perform TADOT.</p>	<p>Prior to exceeding the P-7 interlock whenever the unit has been in MODE 3, if not performed within the previous 31 days</p>
<p>SR 3.3.1.13<u>12</u> -----NOTE----- Neutron detectors are excluded from response time testing. ----- Verify RTS RESPONSE TIME is within limits.</p>	<p>[24 months on a STAGGERED TEST BASIS OR In accordance with the Surveillance Frequency Control Program]</p>

Table 3.3.1-1 (page 1 of 96)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
1. Manual Reactor Trip Initiation	1,2	3 trains	B	SR 3.3.1.4
	3 ^(a) , 4 ^(a) , 5 ^(a)	3 trains	C	SR 3.3.1.4
2. High Power Range Neutron Flux				
a. high setpoint <u>High Setpoint</u>	1,2	4	E	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1. 76 SR 3.3.1. 409 SR 3.3.1. 4312
b. low setpoint <u>Low Setpoint</u>	1 ^(b) , 2	4	F	SR 3.3.1.1 SR 3.3.1. 76 SR 3.3.1. 409 SR 3.3.1. 4312
3. High Power Range Neutron Flux Rate				
a. Positive Rate	1,2	4	F	SR 3.3.1.1 SR 3.3.1. 76 SR 3.3.1. 409 SR 3.3.1. 4312
b. Negative Rate	1,2	4	F	SR 3.3.1.1 SR 3.3.1. 76 SR 3.3.1. 409 SR 3.3.1. 4312
4. High Intermediate Range Neutron Flux	1 ^(b) , 2 ^(c)	2	G,H	SR 3.3.1.1 SR 3.3.1. 76 SR 3.3.1. 409 SR 3.3.1. 4312

- (a) With Rod Control System capable of rod withdrawal or one or more rods not fully inserted.
- (b) Below the P-10 (Power Range Neutron Flux) interlocks.
- (c) Above the P-6 (Intermediate Range Neutron Flux) interlocks.

Table 3.3.1-1 (page 2 of 96)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
5. High Source Range Neutron Flux	2 ^(d)	2	I,J	<u>SR 3.3.1.6</u> SR 3.3.1.7 SR 3.3.1.89 SR 3.3.1.40 SR 3.3.1.13 <u>12</u>
	3 ^(a) , 4 ^(a) , 5 ^(a)	2	J,K	SR 3.3.1.1 SR 3.3.1.76 SR 3.3.1.409 SR 3.3.1.4312
6. Overtemperature ΔT^{\oplus}	1,2	3	<u>F,U,V</u>	SR 3.3.1.1 SR 3.3.1.3 <u>SR 3.3.1.5</u> SR 3.3.1.6 SR 3.3.1.710 SR 3.3.1.4412 SR 3.3.1.13

(a) With Rod Control System capable of rod withdrawal or one or more rods not fully inserted.

(d) Below the P-6 (Intermediate Range Neutron Flux) interlocks.

~~(j) Refer to Note 1 after this table.~~

Table 3.3.1-1 (page 3 of 96)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
7. Overpower $\Delta T^{(k)}$	1,2	3	FU,V	SR 3.3.1.1 SR 3.3.1.3 SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.7 SR 3.3.1.10 SR 3.3.1.11 SR 3.3.1.13 12
8. Pressurizer Pressure				
a. Low Pressurizer Pressure	1 ^(e)	3	LW,X	SR 3.3.1.1 SR 3.3.1.7 SR 3.3.1.9 SR 3.3.1.13 12
b. High Pressurizer Pressure	1,2	3	FU,V	SR 3.3.1.1 SR 3.3.1.7 SR 3.3.1.9 SR 3.3.1.13 12
9. High Pressurizer Water Level	1 ^(e)	3	LW,X	SR 3.3.1.1 SR 3.3.1.7 SR 3.3.1.9 SR 3.3.1.13 12
10. Low Reactor Coolant Flow	1 ^(e)	3 per loop	L	SR 3.3.1.1 SR 3.3.1.7 SR 3.3.1.9 SR 3.3.1.13 12
11. Low Reactor Coolant Pump (RCP) Speed	1 ^(e)	3	L	SR 3.3.1.1 SR 3.3.1.7 SR 3.3.1.9 SR 3.3.1.13 12

(e) Above the P-7 (Low Power Reactor Trips Block) interlock.

~~(k) Refer to Note 2 after this table.~~

Table 3.3.1-1 (page 4 of 96)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
12. Steam Generator (SG) Water Level				
a. Low	1,2	3 per SG	F <u>U,V</u>	SR 3.3.1.1 SR 3.3.1. 76 <u>76</u> SR 3.3.1. 98 <u>98</u> SR 3.3.1. 1312 <u>1312</u>
b. High-High	1 ^(e)	3 per SG	L <u>W,X</u>	SR 3.3.1.1 SR 3.3.1. 76 <u>76</u> SR 3.3.1. 98 <u>98</u> SR 3.3.1. 1312 <u>1312</u>
13. Turbine Trip				
a. Turbine Emergency Trip Oil Pressure	1 ^(e)	3	L	SR 3.3.1. 18 <u>18</u> SR 3.3.1. 7 <u>7</u> SR 3.3.1.9 SR 3.3.1.1211
b. Main Turbine Stop Valve Position	1 ^(e)	1 per valve	T	SR 3.3.1. 98 <u>98</u> SR 3.3.1. 1211 <u>1211</u>

(e) Above the P-7 (Low Power Reactor Trips Block) interlock.

Table 3.3.1-1 (page 5 of 96)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
14. ECCS Actuation	1,2	3 trains	M	SR 3.3.1.56
15. Reactor Trip System Interlocks				
a. Intermediate Range Neutron Flux, P-6	2 ^(d)	2	O	SR 3.3.1.76 SR 3.3.1.409
b. Low Power Reactor Trips Block, P-7	1	1 per train	P	SR 3.3.1.56
c. Power Range Neutron Flux, P-10	1,2	4	O	SR 3.3.1.76 SR 3.3.1.409
d. Turbine Inlet Pressure, P-13	1	3	P	SR 3.3.1.1 SR 3.3.1.76 SR 3.3.1.98
16. Reactor Trip Breakers (RTBs)	1,2	3 trains ^(f)	N,S	SR 3.3.1.4 SR 3.3.1.4312
	3 ^(ba) , 4 ^(ba) , 5 ^(ba)	3 trains ^(f)	D	SR 3.3.1.4 SR 3.3.1.4312

(ba) With Rod Control System capable of rod withdrawal or one or more rods not fully inserted.

(d) Below the P-6 (Intermediate Range Neutron Flux) interlocks.

(f) Two reactor trip breakers per train.

Table 3.3.1-1 (page 6 of 96)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES		REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
	OR OTHER SPECIFIED CONDITIONS				
17. Reactor Trip Breaker Undervoltage and Shunt Trip Mechanisms	1,2		3 trains 1 each per RTB	Q,S	SR 3.3.1.4 SR 3.3.1. 43 <u>12</u>
	3 ^(ba) , 4 ^(ba) , 5 ^(ba)		3 trains 1 each per RTB	D	SR 3.3.1.4 SR 3.3.1. 43 <u>12</u>
18. Automatic Trip Logic	1,2		3 trains	R,S	SR 3.3.1. 56 <u>6</u>
	3 ^(ba) , 4 ^(ba) , 5 ^(ba)		3 trains	D	SR 3.3.1. 56 <u>6</u>

(ba) With Rod Control System capable of rod withdrawal or one or more rods not fully inserted.

Table 3.3.1-1 (page 7 of 9)

Reactor Trip System Instrumentation

Note 1: Overtemperature ΔT

The Overtemperature ΔT Function is initiated based on setpoints derived for DNB protection or core exit boiling conditions.

$$\Delta T_{SP} = \text{Lowselect}(\Delta T_{SP1}, \Delta T_{SP2})$$

$$\Delta T \frac{(1 + T_7 s) \left(\frac{1}{(1 + T_8 s)(1 + T_9 s)} \right)}{(1 + T_8 s)(1 + T_9 s)} \geq \Delta T_{SP}$$

Where: $T_7 = [^*] \text{sec}$ $T_8 = [^*] \text{sec}$ $T_9 = [^*] \text{sec}$

1. DNB Protection

$$\Delta T_{SP1} = \Delta T_0 \left(K_1 + K_2 \frac{(1 + T_2 s)}{(1 + T_3 s)} (T_{avg} - T_{avg0}) + K_3 (P - P_0) f_1(\Delta I) \right)$$

Where: ΔT is measured RCS ΔT , °F.

ΔT_0 is indicated RCS ΔT at RTP, °F

s is the Laplace transform operator, sec^{-1} .

T_{avg} is the measured RCS average temperature, °F.

T_{avg0} is the nominal T_{avg} at RTP, $\leq [^*] \text{°F}$.

P is the measured pressurizer pressure, psig

P_0 is the nominal RCS operating pressure, $\geq [^*] \text{psig}$

$K_1 \leq [^*]$ $K_2 \geq [^*] / \text{F}$ $K_3 \geq [^*] / \text{psig}$

$T_2 \geq [^*] \text{sec}$ $T_3 \leq [^*] \text{sec}$

$f_1(\Delta I) = [^*] \{ [^*] - (q_t - q_b) \}$ when $q_t - q_b \leq [^*] \% \text{ RTP}$

0% of RTP when $[^*] \% \text{ RTP} < q_t - q_b \leq [^*] \% \text{ RTP}$

$[^*] \{ (q_t - q_b) - [^*] \}$ when $q_t - q_b > [^*] \% \text{ RTP}$

Where q_t and q_b are percent RTP in the upper and lower halves of the core, respectively, and $q_t + q_b$ is the total THERMAL POWER in percent RTP.

These values denoted with $[^]$ are specified in the COLR.

Table 3.3.1-1 (page 8 of 9)
Reactor Trip System Instrumentation

Note 1: Overtemperature ΔT (continued)

2. Core Exit Boiling Limit

$$\Delta T_{SP2} = \Delta T_0 \left(K_4 - K_5 \frac{(1 + T_4 s)}{(1 + T_5 s)} (T_{avg} - T_{avg0}) + K_6 (P - P_0) \right)$$

Where: ΔT is measured RCS ΔT , °F.

ΔT_0 is indicated RCS ΔT at RTP, °F

s is the Laplace transform operator, sec^{-1} .

T_{avg} is the measured RCS average temperature, °F.

T_{avg0} is the nominal T_{avg} at RTP, \leq [*] °F.

P is the measured pressurizer pressure, psig

P_0 is the nominal RCS operating pressure, \geq [*] psig

$K_4 \leq$ [*] $K_5 \geq$ [*]/°F $K_6 \geq$ [*]/psig

$T_4 \geq$ [*] sec $T_5 \leq$ [*] sec

These values denoted with [] are specified in the COLR.

~~Table 3.3.1-1 (page 9 of 9)
Reactor Trip System Instrumentation~~

~~Note 2: Overpower ΔT~~

$$\Delta T \frac{(1+T_{13}s)}{(1+T_{14}s)} \left(\frac{1}{1+T_{15}s} \right) \geq \Delta T_0 \left(K_7 K_8 \frac{T_6 s}{1+T_6 s} T_{avg} K_9 (T_{avg} - T_{avg0}) f_2(\Delta T) \right)$$

~~Where: ΔT is measured RCS ΔT , °F.~~

~~ΔT_0 is indicated RCS ΔT at RTP, °F.~~

~~s is the Laplace transform operator, sec^{-1} .~~

~~T_{avg} is the measured RCS average temperature, °F.~~

~~T_{avg0} is the nominal T_{avg} at RTP, \leq [*]°F.~~

~~$K_7 \leq$ [*] $K_8 \geq$ [*]/°F for increasing T_{avg} $K_9 \geq$ [*]/°F when $T_{avg} > T_{avg0}$
[*]/°F for decreasing T_{avg} [*]/°F when $T_{avg} \leq T_{avg0}$~~

~~$T_6 \geq$ [*] sec $T_{13} \geq$ [*] sec $T_{14} \leq$ [*] sec~~

~~$T_{15} \leq$ [*] sec~~

~~$f_2(\Delta T) =$ [*]~~

~~*These values denoted with [*] are specified in the COLR.~~

3.3 INSTRUMENTATION

3.3.2 Engineered Safety Feature Actuation System (ESFAS) Instrumentation

LCO 3.3.2 The ESFAS instrumentation for each Function in Table 3.3.2-1 shall be OPERABLE.

APPLICABILITY: According to Table 3.3.2-1.

ACTIONS

-----NOTE-----
Separate Condition entry is allowed for each Function.

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more Functions with one or more required channels or trains inoperable.	A.1 Enter the Condition referenced in Table 3.3.2-1 for the channel(s) or train(s).	Immediately
B. One required train inoperable.	B.1 Restore train to OPERABLE status.	72 hours
	<u>OR</u> B.2.1 Be in MODE 3.	78 hours
	<u>AND</u> B.2.2 Be in MODE 5.	108 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
C. One required train inoperable.	<p>-----NOTE----- One required train may be bypassed for up to 4 hours for surveillance testing, provided the other required train(s) <u>is</u><u>are</u> OPERABLE. -----</p> <p>C.1 Restore train to OPERABLE status.</p> <p><u>OR</u></p> <p>C.2.1 Be in MODE 3.</p> <p><u>AND</u></p> <p>C.2.2 Be in MODE 5.</p>	<p>24 hours</p> <p>30 hours</p> <p>60 hours</p>
D. One required channel inoperable.	<p>-----NOTE----- One <u>required</u> channel may be bypassed for up to 12 hours for surveillance testing, <u>provided the other required channels are OPERABLE or placed in the trip condition.</u> -----</p> <p>D.1 Place channel in trip.</p> <p><u>OR</u></p> <p>D.2.1 Be in MODE 3.</p> <p><u>AND</u></p> <p>D.2.2 Be in MODE 4.</p>	<p>72 hours</p> <p>78 hours</p> <p>84 hours</p>

CONDITION	REQUIRED ACTION	COMPLETION TIME
E. One required Containment Pressure channel inoperable.	<p>E.1 Restore required number of OPERABLE channels.</p> <p><u>-----NOTE-----</u></p> <p><u>One required channel may be bypassed for up to 12 hours for surveillance testing, provided the other required channels are OPERABLE.</u></p> <p><u>E.1 Restore channel to OPERABLE status.</u></p> <p><u>OR</u></p> <p>E.2.1 Be in MODE 3.</p> <p><u>AND</u></p> <p>E.2.2 Be in MODE 4.</p>	<p>72 hours</p> <p>78 hours</p> <p>84 hours</p>
F. One required channel or <u>required</u> train inoperable.	<p><u>-----NOTE-----</u></p> <p><u>One Loss of Offsite Power channel may be bypassed for up to 4 hours for surveillance testing, provided the other channels are OPERABLE or placed in the trip condition.</u></p> <p>F.1 Restore channel or train to OPERABLE status.</p> <p><u>OR</u></p> <p>F.2.1 Be in MODE 3.</p> <p><u>AND</u></p> <p>F.2.2 Be in MODE 4.</p>	<p>72 hours</p> <p>78 hours</p> <p>84 hours</p>
G. One required train inoperable.	<p><u>-----NOTE-----</u></p> <p>One inoperable train may be bypassed for up to 4 hours for surveillance testing, provided the</p>	

	<p>other train(s) is(are) OPERABLE.</p> <p>-----</p> <p>G.1 Restore train to OPERABLE status.</p> <p><u>OR</u></p> <p>G.2.1 Be in MODE 3.</p> <p><u>AND</u></p> <p>G.2.2 Be in MODE 4.</p>	<p>24 hours</p> <p>30 hours</p> <p>36 hours</p>
--	--	---

CONDITION	REQUIRED ACTION	COMPLETION TIME
H. One channel for trip of all <u>required</u> Main Feedwater Pumps <u>trips channel</u> inoperable.	H.1 Restore channel to OPERABLE status. <u>OR</u> H.2 Be in MODE 3.	48 hours 54 hours
I. One or more <u>required Pressurizer Pressure, P-11</u> channels inoperable.	I.1 Verify interlock is in required state for existing unit condition. <u>OR</u> I.2.1 Be in MODE 3. <u>AND</u> I.2.2 Be in MODE 4.	1 hour 7 hours 13 hours
J. One required <u>Emergency Feedwater Actuation</u> train inoperable.	-----NOTE----- One inoperable <u>required</u> train may be bypassed for up to 4 hours for surveillance testing, provided the other train(s) is (<u>required trains are</u>) OPERABLE. ----- J.1 Restore train to OPERABLE status. <u>OR</u> J.2 Apply the requirements of Specification 5.5.18.	72 hours 72 hours]

CONDITION	REQUIRED ACTION	COMPLETION TIME
<p>K. One required Containment High <u>Range</u> Area Radiation monitoring-channel inoperable.</p>	<p>K.1 Restore channel to OPERABLE status.</p> <p>OR</p> <p>K.2.1 — Be in MODE 3.</p> <p>— AND</p> <p>K.2.2 — Be in MODE 5.</p>	<p>72 hours</p> <p>78 hours</p> <p>108 hours</p>
<p>L. One or more Actuation Logic and Actuation Output <u>Containment Purge Isolation</u> trains inoperable.</p> <p>OR</p> <p>Two or more <u>required</u> Containment High Range Area Radiation Monitoring-channels inoperable.</p> <p>OR</p> <p>Required Action and associated Completion Time of Condition K not met.</p>	<p>L.1 Enter applicable Conditions and Required Actions of LCO 3.6.3, "Containment Isolation Valves," for containment purge and exhaust isolation valves made inoperable by isolation instrumentation.</p>	<p>Immediately</p>
<p>M. One or more Functions with one <u>required</u> channel or train inoperable.</p>	<p>M.1 — Place one train of the affected subsystem(s) in the emergency mode, depending on the inoperable train. <u>M.1 Place channel in trip.</u></p> <p>————— Note</p> <p>Inoperable train A or D affects both subsystem MCREFS and subsystem MCRATCS, while inoperable train B or C affects only subsystem MCRATCS.</p>	<p>7 days <u>1 hour</u></p> <p>72 hours</p>

	<hr/> <p><u>AND</u></p> <p><u>M.2 Restore channel to</u> <u>OPERABLE status.</u></p>	
--	--	--

<p>CONDITION<u>N.</u> <u>Required Action and associated Completion Time of Condition M not met.</u></p>	<p>REQUIRED ACTION<u>N.1</u> <u>AND</u> <u>N.2 Be in MODE 4.</u></p>	<p>COMPLETION TIME<u>6 hours</u> <u>12 hours</u></p>
<p>N. One or more Functions with two channels or two trains inoperable.<u>O. One S-VDU train inoperable.</u></p>	<p>N.1.1 Place the affected subsystem(s) in the emergency mode. -----NOTE-----</p> <p>AND</p> <p>N.1.2 Enter applicable Conditions and Required Actions for the affected subsystem(s) made inoperable by inoperable actuation instrumentation, depending on inoperable trains.</p> <p>OR</p> <p>N.2 Place all trains of the affected subsystem(s) in emergency mode.</p> <p>-----Note----- Inoperable train A or D affects both subsystem MCREFS and subsystem MCRATGS, while inoperable train B or C affects only subsystem MCRATGS. <u>One train may be bypassed for up to 4 hours for surveillance testing, provided the other trains are OPERABLE.</u> -----</p> <p><u>O.1 Restore train to OPERABLE status.</u></p> <p>OR</p> <p><u>O.2 Enter applicable Conditions and Required Actions for the ESF components made inoperable by the inoperable S-VDU train.</u></p>	<p>Immediately</p> <p>Immediately</p> <p><u>72 hours</u></p> <p><u>72 hours</u></p> <p>Immediately</p>

<p>O. Required Action and associated Completion Time for Condition M or N not met in MODE 1, 2, 3, or 4. P. One COM-2 train inoperable.</p>	<p>O.1 Be in MODE 3.----- ---NOTE--------</p> <p>AND</p> <p>O.2 Be in MODE 5. <u>One train may be bypassed for up to 4 hours for surveillance testing, provided the other trains are OPERABLE.</u></p> <p>-----</p> <p><u>P.1 Restore train to OPERABLE status.</u></p> <p><u>OR</u></p> <p><u>P.2 Enter applicable Conditions and Required Actions for the ESF components made inoperable by the inoperable COM-2 train.</u></p>	<p>6</p> <p><u>12</u> hours</p> <p>36 <u>12</u> hours</p>
--	---	---

<p>P. Required Action and associated Completion Time for Condition M or N not met during movement of irradiated fuel assemblies. <u>CONDITION</u></p>	<p>P.1 Suspend movement of irradiated fuel assemblies. <u>REQUIRED ACTION</u></p>	<p>Immediately <u>COMPLETION TIME</u></p>
--	--	--

--	--	--

<p>S. One required train inoperable. <u>CONDITION</u></p>	<p>NOTE One inoperable train may be bypassed for up to 4 hours for surveillance testing provided the other train(s) is(are) OPERABLE.</p> <hr/> <p>S.1 Restore train to OPERABLE status.</p> <p><u>OR</u></p> <p>S.2 Apply the requirements of Specification 5.5.18. <u>REQUIRED ACTION</u></p>	<p><u>COMPLETION TIME</u></p> <p>24 hours</p> <p>24 hours]</p>
--	--	--

<p>CONDITIONS. <u>One train inoperable.</u></p>	<p>REQUIRED ACTION----- <u>NOTE</u>----- <u>One train may be bypassed for up to 4 hours for surveillance testing, provided the other train is OPERABLE.</u> ----- <u>S.1 Restore train to OPERABLE status.</u> <u>[OR</u> <u>S.2 Apply the requirements of Specification 5.5.18.</u></p>	<p>COMPLETION TIME</p> <p><u>24 hours</u></p> <p><u>24 hours]</u></p>
<p>T. Required Action and associated Completion Time for Condition J or S not met.</p>	<p>T.1 Be in MODE 3. <u>AND</u> T.2 Be in MODE 4.</p>	<p>6 hours</p> <p>12 hours</p>
<p><u>U. One or more MCR Outside Air Intake Radiation Functions with one channel inoperable.</u></p>	<p><u>U.1 Place one MCREFS train and two MCRATCS trains in the emergency mode.</u></p>	<p><u>7 days</u></p>

<u>CONDITION</u>	<u>REQUIRED ACTION</u>	<u>COMPLETION TIME</u>
<u>V. One or more MCR Outside Air Intake Radiation Functions with two channels inoperable.</u>	<u>V.1 Place one MCREFS train and two MCRATCS trains in the emergency mode.</u> <u>AND</u> <u>V. 2.1 Restore one channel to OPERABLE status.</u> <u>OR</u> <u>V. 2.2 Place two MCREFS trains and three MCRATCS trains in the emergency mode.</u>	<u>Immediately</u> <u>7 days</u> <u>7 days</u>
<u>W. One or more Functions with one train, A or D, inoperable.</u>	<u>-----NOTE-----</u> <u>This condition is only applicable to Train A or D. For inoperable Train B or C there is no action required.</u> <u>-----</u> <u>W.1 Place the affected train of MCREFS in the emergency mode.</u>	 <u>7 days</u>
<u>X. One or more Functions with two trains, A and D, inoperable.</u>	<u>-----NOTE-----</u> <u>This condition is only applicable to Trains A and D. Other inoperable two-train combinations are addressed in Condition Y.</u> <u>-----</u> <u>X.1 Place one MCREFS train in the emergency mode.</u> <u>AND</u> <u>X.2.1 Restore one MCREFS train to OPERABLE status (i.e.,</u>	 <u>Immediately</u> <u>7 days</u>

	<p><u>one train in the emergency mode and one train OPERABLE).</u></p> <p><u>OR</u></p> <p><u>X.2.2 Place two MCREFS trains in the emergency mode.</u></p> <p><u>AND</u></p> <p><u>X.3.1 Restore one affected MCRATCS train to OPERABLE status (i.e., three trains OPERABLE).</u></p> <p><u>OR</u></p> <p><u>X.3.2 Place one affected MCRATCS train in the emergency mode (i.e., one train in the emergency mode and two trains OPERABLE).</u></p>	<p><u>7 days</u></p> <p><u>7 days</u></p> <p><u>7 days</u></p>
<p><u>Y. One or more Functions with two trains, except A and D, inoperable.</u></p>	<p><u>-----NOTE-----</u></p> <p><u>==</u></p> <p><u>Inoperable Train A or D affects MCREFS and MCRATCS.</u></p> <p><u>Inoperable Train B or C affects MCRATCS.</u></p> <p><u>-----</u></p> <p><u>Y.1 Restore one affected train to OPERABLE status for the affected subsystem(s).</u></p> <p><u>OR</u></p> <p><u>Y.2 Place one affected train in the emergency mode for the affected subsystem(s).</u></p>	<p><u>7 days</u></p> <p><u>7 days</u></p>
<p><u>Z. Required Action and associated Completion Time for Condition U, V, W, X or Y not met in MODE 1, 2, 3, or 4.</u></p>	<p><u>Z.1 Be in MODE 3.</u></p> <p><u>AND</u></p> <p><u>Z.2 Be in MODE 5.</u></p>	<p><u>6 hours</u></p> <p><u>36 hours</u></p>

<u>AA. Required Action and associated Completion Time for Condition U, V, W, X or Y not met during movement of irradiated fuel assemblies.</u>	<u>AA.1 Suspend movement of irradiated fuel assemblies.</u>	<u>Immediately</u>
<u>BB. One required Reactor Trip, P-4 train inoperable.</u>	<u>BB.1 Restore train to OPERABLE status.</u> <u>OR</u> <u>BB.2.1 Be in MODE 3.</u> <u>AND</u> <u>BB.2.2 Be in MODE 4.</u>	<u>48 hours</u> <u>54 hours</u> <u>60 hours</u>

SURVEILLANCE REQUIREMENTS

-----NOTE-----

Refer to Table 3.3.2-1 to determine which SRs apply for each ESFAS Function.

SURVEILLANCE	FREQUENCY
SR 3.3.2.1 Perform CHANNEL CHECK.	[12 hours OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.2.2 Perform ACTUATION LOGIC TEST <u>MIC consistent with Specification 5.5.21, Setpoint Control Program (SCP).</u>	[24 months OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.2.3 Perform GOT.	[24 months OR In accordance with the Surveillance Frequency Control Program]

SURVEILLANCE	FREQUENCY
SR 3.3.2.4 ³ Perform TADOT for actuation outputs <u>Actuation Outputs</u> .	[24 months OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.2.5 NOTE Verification of relay setpoints not required. ⁴ Perform TADOT.	[92 days OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.2.6 NOTE Verification of setpoint not required for manual initiation functions. ⁵ Perform TADOT.	[24 months OR In accordance with the Surveillance Frequency Control Program]

SURVEILLANCE	FREQUENCY
<p>SR 3.3.2.7 NOTE This Surveillance shall include verification that the time constants are adjusted to the prescribed values.</p> <p><u>6</u> Perform CHANNEL CALIBRATION on each required channel consistent with Specification 5.5.21, Setpoint Control Program (SCP).</p>	<p>[24 months OR In accordance with the Surveillance Frequency Control Program]</p>
<p>SR 3.3.2.<u>8</u><u>7</u> -----NOTE----- Not required to be performed for the turbine driven EFW pumps until 24 hours after SG pressure is ≥ 1000 psig. ----- Verify ESFAS RESPONSE TIMES are <u>TIME is</u> within limit.</p>	<p>[24 months on a STAGGERED TEST BASIS OR In accordance with the Surveillance Frequency Control Program]</p>
<p>SR 3.3.2.9 NOTE Verification of setpoint not required.</p> <p><u>8</u> Perform TADOT.</p>	<p>Once per reactor trip breaker cycle</p>
<p><u>SR 3.3.2.9</u> Perform SAFETY VDU TEST.</p>	<p><u>[24 months</u> <u>OR</u></p>

	<p><u>In accordance with the Surveillance Frequency Control Program]</u></p>
--	--

Table 3.3.2-1 (page 1 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
1. ECCS Actuation				
a. Manual Initiation	1,2,3,4	3 trains	B	SR 3.3.2.65
b. Actuation Logic and Actuation Outputs	1,2,3,4	3 trains	Q,R	SR 3.3.2.2 SR 3.3.2.43
c. High Containment Pressure	1,2,3	3	D	SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8
d. Low Pressurizer Pressure	1,2,3 ^(a)	3	D M,N	SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8
e. Low Main Steam Line Pressure	1,2,3 ^(a)	3 per steam line	D M,N	SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8

(a) Above the P-11 (Pressurizer Pressure) interlock.

Table 3.3.2-1 (page 2 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
2. Containment Spray				
a. Manual Initiation	1,2,3,4	2 switches per train for 3 <u>4</u> trains	B	SR 3.3.2. 6 <u>5</u>
b. Actuation Logic and Actuation Outputs	1,2,3,4	3 trains	Q,R	SR 3.3.2.2 SR 3.3.2. 4 <u>3</u>
c. High-3 Containment Pressure	1,2,3	3	E	SR 3.3.2.1 SR 3.3.2. 3 <u>2</u> <u>SR 3.3.2.6</u> SR 3.3.2.7 SR 3.3.2.8

Table 3.3.2-1 (page 3 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
3. Containment Isolation				
a. Phase A Isolation				
(1) Manual Initiation	1,2,3,4	Trains A and D	B	SR 3.3.2.65
(2) Actuation Logic and Actuation Outputs	1,2,3,4	Trains A and D	C	SR 3.3.2.2 SR 3.3.2.43
(3) ECCS Actuation	Refer to Function 1 (ECCS Actuation) for all initiation functions and requirements.			
b. Phase B Isolation				
(1) Containment Spray - Manual Initiation	Refer to Function 2.a (Containment Spray - <u>Manual Initiation</u>) for all initiation functions and requirements.			
(2) Actuation Logic and Actuation Outputs	1,2,3,4	4 trains	C	SR 3.3.2.2 SR 3.3.2.43
(3) High-3 Containment Pressure	Refer to Function 2.c (Containment Spray) for all - High-3 Containment Pressure) <u>for all</u> requirements.			

Table 3.3.2-1 (page 4 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
4. Main Steam Line Isolation				
a. Manual Initiation	1, 2- ^(h) , 3- ^(h)	Trains A and D	F	SR 3.3.2.65
b. Actuation Logic and Actuation Outputs	1, 2- ^(h) , 3- ^(h)	Trains A and D	S, T	SR 3.3.2.2 SR 3.3.2.43
c. High-High Containment Pressure	1, 2- ^(h) , 3 ^(h)	3	D	SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8
d. Main Steam Line Pressure				
(1) Low Main Steam Line Pressure	1, 2- ^(h) , 3 ^{(a)-(h)}	3 per steam line	D M,N	SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8
(2) High Main Steam Line Pressure Negative Rate	3 ^{(f)-(h)g)}	3 per steam line	D M,N	SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8

(a) Above the P-11 (Pressurizer Pressure) interlock.

(b)
(f) Below the P-11 (Pressurizer Pressure) interlock.

(g) _____

(h) Except when all MSIVs are closed.

Table 3.3.2-1 (page 5 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
5. Main Feedwater Isolation				
5A. Main Feedwater Regulation valve Closure				
a. Manual Initiation	1,2,3	Trains A and D	F	SR 3.3.2.5
a. Low T_{avg} Actuation Logic and Actuation Outputs	1,2^(f),3^(f)	3 Trains A and D	DS,I	SR 3.3.2.12 SR 3.3.2.3 SR 3.3.2.7 SR 3.3.2.8
— Coincident with Reactor Trip, P-4	Refer to Function 11.a for all P-4 requirements.			
5B. Main Feedwater Isolation				
c. High-High SG Water Level	1,2,3^(c)	3 per SG	M,N	SR 3.3.2.1 SR 3.3.2.2 SR 3.3.2.6 SR 3.3.2.7
d. ECCS Actuation	Refer to Function 1 (ECCS Actuation) for all requirements.			
a. Manual Initiation	1,2^(f),3^(f)	Trains A and D3	FM,N	SR 3.3.2.1 SR 3.3.2.2 SR 3.3.2.6 SR 3.3.2.7
e. Low T_{avg}^(d)				
b. Actuation Logic and Actuation Outputs	1,2^(f),3^(f)	Trains A and D	S,I	SR 3.3.2.2 SR 3.3.2.4
c. High High SG Water Level	1,2^(f),3^{(a)(f)}	3 per SG	D	SR 3.3.2.1 SR 3.3.2.3 SR 3.3.2.7 SR 3.3.2.8
d. ECCS Actuation	Refer to Function 1 (ECCS Actuation) for all initiation functions and requirements.			

(a) — Above the P-11 (Pressurizer Pressure) interlock.

(i) — Except when all MFIVs, MFRVs, MFBRVs, and SGWFCVs are closed.

(j) — Except when all MFRVs are closed.

~~Table 3.3.2-1 (page 6 of 11)~~

Coincident with
Reactor Trip, P-4

Refer to Function 11.a (ESFAS Interlocks - Reactor Trip, P-4) for all requirements.

-
- (c) The sub-function for trip of all MFW pumps, and closure of the MFIVs and SGWFCVs may be manually bypassed in MODE 3 below the P-11 (Pressurizer Pressure) interlock.
- (d) Low T_{avg} coincident with Reactor Trip, P-4 only closes MFW Regulation valves.

Table 3.3.2-1 (page 6 of 11)

Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES		REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
	OR OTHER SPECIFIED CONDITIONS				
6. Emergency Feedwater Actuation					
a. Manual Initiation	1,2,3		3 trains	F	SR 3.3.2.65
b. Actuation Logic and Actuation Outputs	1,2,3		3 trains	J,T	SR 3.3.2.2 SR 3.3.2.43
c. Low SG Water Level	1,2,3		3 per SG	D M,N	SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8
d. ECCS Actuation	Refer to Function 1 (ECCS Actuation) for all initiation functions and requirements.				
e. LOOP Signal	1,2,3		3 per bus for each EFW train	F	SR 3.3.2.54 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8
f. Trip of all Main Feedwater Pumps	1,2		1 per pump	H	SR 3.3.2.65 SR 3.3.2.87

(f) ~~Nominal Trip Setpoint~~

Table 3.3.2-1 (page 7 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
7. Emergency Feedwater Isolation				
a. Manual Initiation	1,2,3	2 trains per SG	F	SR 3.3.2. 6 <u>5</u>
b. Actuation Logic and Actuation Outputs	1,2,3	2 trains per SG	G	SR 3.3.2.2 SR 3.3.2. 4 <u>3</u>
c. High SG Water Level	1,2,3 ^(a)	3 per SG	D <u>M,N</u>	SR 3.3.2.1 SR 3.3.2. 3 <u>2</u> <u>SR 3.3.2.6</u> SR 3.3.2.7 SR 3.3.2.8
Coincident with Reactor Trip, P-4	Refer to Function 11.a (ESFAS Interlocks - Reactor Trip, P-4) for all P-4 requirements.			
and				
No Low Main Steam Line Pressure	Refer to Function- 7.d (Emergency Feedwater Isolation - Low Main Steam Line Pressure) for all initiation functions and requirements.			
d. Low Main Steam Line Pressure	1,2,3 ^(a)	3 per SG	D <u>M,N</u>	SR 3.3.2.1 SR 3.3.2. 3 <u>2</u> <u>SR 3.3.2.6</u> SR 3.3.2.7 SR 3.3.2.8
8. CVCS Isolation				
a. Manual Initiation	1,2,3	Trains A and D	F	SR 3.3.2. 6 <u>5</u>
b. Actuation Logic and Actuation Outputs	1,2,3	Trains A and D	G	SR 3.3.2.2 SR 3.3.2. 4 <u>3</u>
c. High Pressurizer Water Level	1,2,3 ^(a)	3	D <u>M,N</u>	SR 3.3.2.1 SR 3.3.2. 3 <u>2</u> <u>SR 3.3.2.6</u> SR 3.3.2.7 SR 3.3.2.8

(a) Above the P-11 (Pressurizer Pressure) interlock.

Table 3.3.2-1 (page 8 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
9. Turbine Trip				
a. Actuation Logic and Actuation Outputs	1,2,3	4 trains <u>Trains A and D</u>	G	SR 3.3.2.2 SR 3.3.2. 4 <u>3</u>
b. Reactor Trip, P-4	Refer to Function 11.a (<u>ESFAS Interlocks - Reactor Trip, P-4</u>) for all P-4 requirements.			
c. High-High SG Water Level	1,2- ⁽ⁱ⁾ ,3- ⁽ⁱ⁾	3 per SG	D <u>M,N</u>	SR 3.3.2.1 SR 3.3.2. 3 <u>2</u> <u>SR 3.3.2.6</u> SR 3.3.2.7 SR 3.3.2.8
10. Reactor Coolant Pump Trip				
a. ECCS Actuation Coincident with Reactor Trip, P-4	Refer to Function 1 (ECCS Actuation) for all initiation functions and requirements.			
	Refer to Function 11.a (<u>ESFAS Interlocks - Reactor Trip, P-4</u>) for all P-4 requirements.			
11. ESFAS Interlocks				
a. Reactor Trip, P-4	1,2,3	3 trains	F <u>B</u> B	SR 3.3.2. 9 <u>8</u>
b. Pressurizer Pressure, P-11	1,2,3	3	I	SR 3.3.2.1 SR 3.3.2. 3 <u>2</u> SR 3.3.2. 7 <u>6</u>

(i) ~~Except when all MFIVs, MFRVs, MFBRVs, and SGWFECVs are closed.~~

Table 3.3.2-1 (page 9 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES		SURVEILLANCE REQUIREMENTS
	OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	
12. Containment Purge Isolation			
a. Containment Isolation Phase A - Manual Initiation			Refer to Function 3.a.(1) (Containment Isolation - Phase A <u>Isolation</u> - Manual Initiation) for all initiation functions and requirements.
b. Containment Spray - Manual Initiation			Refer to Function 2.a- (Containment Spray - Manual Initiation) for all initiation functions and requirements.
c. Actuation Logic and Actuation Outputs	1,2,3,4	Trains A and D	L SR 3.3.2.2 SR 3.3.2.43
d. ECCS Actuation			Refer to Function 1 (ECCS Actuation) for all initiation functions and requirements.
e. Containment High Range Area Radiation	1,2,3,4	3	K, L SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8

Table 3.3.2-1 (page 10 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
13. Main Control Room (MCR) Isolation				
a. Manual Initiation	1,2,3,4,(^k e)	3 trains including A and D(^m f)	M, N, O, <u>P, W, X, Y, Z,</u> <u>AA,</u>	SR 3.3.2.65
b. Actuation Logic and Actuation Outputs	1,2,3,4,(^k e)	3 trains including A and D(^m f)	M, N, O, P, W, <u>X, Y, Z, AA</u>	SR 3.3.2.2 SR <u>SR 3.3.2.43</u>
c. MCR Outside Air Intake Radiation				
(1) MCR Outside Air Intake Gas Radiation	1,2,3,4,(^k e)	2	M, N, O, <u>P, U, V, Z,</u> <u>AA</u>	SR 3.3.2.1 SR 3.3.2.32 <u>SR 3.3.2.6</u> SR 3.3.2.7 SR 3.3.2.8
(2) MCR Outside Air Intake Particulate Radiation	1,2,3,4,(^k e)	2	M, N, O, <u>P, U, V, Z,</u> <u>AA</u>	SR 3.3.2.1 SR 3.3.2.32 <u>SR 3.3.2.6</u> SR 3.3.2.7 SR 3.3.2.8
(3) MCR Outside Air Intake Iodine Radiation	1,2,3,4,(^k e)	2	M, N, O, <u>P, U, V, Z,</u> <u>AA</u>	SR 3.3.2.1 SR 3.3.2.32 <u>SR 3.3.2.6</u> SR 3.3.2.7 SR 3.3.2.8
d. ECCS Actuation	Refer to LCO 3.3.2, "ESFAS Instrumentation," Function 1, (<u>ECCS Actuation</u>) for all initiation functions and requirements.			

(^ke) During movement of irradiated fuel assemblies.

(^mf) Two trains of MCREFS are required to be operable (trains A and D); three trains of MCRATS are required to be operable (three out of four trains A, B, C, D).

Table 3.3.2-1 (page 11 of 11)
Engineered Safety Feature Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
14. Block Turbine Bypass and Cooldown Valves				
a. Manual Initiation	1,2 ^(H) ,3 ^(H)	Trains A and D	F	SR 3.3.2.65
b. Actuation Logic and Actuation Outputs	1,2 ^(H) ,3 ^(H)	Trains A and D	S,T	SR 3.3.2.2 SR 3.3.2.43
c. Low-Low T _{avg} Signal	1,2 ^(H) ,3 ^(H)	3	D M,N	SR 3.3.2.1 SR 3.3.2.32 SR 3.3.2.6 SR 3.3.2.7 SR 3.3.2.8
(j) — Except when all MSIVs are closed.				
15. Manual Control of ESF Components				
a. Safety VDU	1, 2, 3, 4, 5, 6	4 trains	O	SR 3.3.2.2 SR 3.3.2.9
b. COM-2	1, 2, 3, 4, 5, 6	4 trains	P	SR 3.3.2.2
c. Actuation Logic and Actuation Outputs	Refer to LCO 3.4 through 3.7 for all requirements applicable to the controlled ESF components.			SR 3.3.2.2 SR 3.3.2.3

3.3 INSTRUMENTATION

3.3.3 Post Accident Monitoring (PAM) Instrumentation

LCO 3.3.3 The PAM ~~instrumentation for each~~ Instrumentation Function in Table 3.3.3-1, and for all four trains of the PAM Display Function, shall be OPERABLE.

APPLICABILITY: MODES 1, 2, and 3.

ACTIONS

-----NOTE-----

1. Separate Condition entry is allowed for each Function.
-

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more <u>PAM Instrumentation</u> Functions with one required channel inoperable. <u>OR</u> <u>One train of the PAM Display Function inoperable.</u>	A.1 Restore required channel <u>or train</u> to OPERABLE status.	30 days

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. Required Action and associated Completion Time of Condition A not met.	<p>B.1</p> <p>-----NOTE-----</p> <p>1. For RCS Hot and Cold Leg Temperatures, this Condition is applicable only if at least one channel (Hot or Cold) is operable in each loop. Otherwise, go to Condition C.</p> <p>2. For SG Water Level and EFW flow, this condition is applicable only if at least one channel (Level or flow) is operable in each loop. Otherwise, go to Condition C.</p> <p>-----</p> <p>Initiate action in accordance with Specification 5.6.5.</p>	Immediately

CONDITION	REQUIRED ACTION	COMPLETION TIME
D. Required Action and associated Completion Time of Condition <u>Condition C</u> not met.	D.1 Enter the Condition referenced <u>Be in Table</u> MODE 3.3.3-1 for the channel. <u>AND</u> <u>D.2 Be in MODE 4.</u>	Immediately <u>6 hours</u> <u>12 hours</u>
E. As by Required Action D.1 and referenced in Table 3.3.3-1.	E.1 Be in MODE 3. AND E.2 Be in MODE 4.	6 hours 12 hours
F. As by Required Action D.1 and referenced in Table 3.3.3-1.	F.1 Initiate action in accordance with Specification 5.6.5.	Immediately

SURVEILLANCE REQUIREMENTS

-----NOTE-----

SR 3.3.3.1 and SR 3.3.3.2 apply to each PAM ~~instrumentation~~ Instrumentation Function in Table 3.3.3-1.

SURVEILLANCE	FREQUENCY
SR 3.3.3.1 Perform CHANNEL CHECK for each required instrumentation channel that is normally energized.	[31 days OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.3.2 -----NOTE----- Neutron detectors are excluded from CHANNEL CALIBRATION. ----- Perform CHANNEL CALIBRATION.	[24 months OR In accordance with the Surveillance Frequency Control Program]
<u>SR 3.3.3.3 Perform MIC for the PAM Instrumentation.</u>	<u>[24 months</u> <u>OR</u> <u>In accordance with the Surveillance Frequency Control Program]</u>

<u>SURVEILLANCE</u>	<u>FREQUENCY</u>
<u>SR 3.3.3.4</u> <u>Perform SAFETY VDU TEST for all four trains of the PAM Display Function.</u>	<u>[24 months</u> <u>OR</u> <u>In accordance</u> <u>with the</u> <u>Surveillance</u> <u>Frequency</u> <u>Control Program]</u>

Table 3.3.3-1 (page 1 of 1)
Post Accident Monitoring Instrumentation

FUNCTION	REQUIRED CHANNELS	CONDITION REFERENCED FROM REQUIRED ACTION D.1
1. Wide Range Neutron Flux	2	E
2. Reactor Coolant System (RCS) Hot Leg Temperature (Wide Range)	1 per loop ^(d) 3	E
3. RCS Cold Leg Temperature (Wide Range)	1 per loop ^(d) 3	E
4. RCS Pressure (Wide Range)	2	E
5. Reactor Vessel Water Level	2 ^(d)	F
6. Containment Pressure	2	E
7. Containment Isolation Valve Position	2 per penetration flow path ^{(a)(b)}	E
8. Containment High Range Area Radiation	2	F
9. Pressurizer Water Level	2	E
10. Steam Generator Water Level (Wide Range)	1 per steam generator ^(d) SG	E
11. Steam Generator Water Level (Narrow Range)	2 per steam generator SG	E
12. Core Exit Temperature - Quadrant 1	2 ^(c)	E
13. Core Exit Temperature - Quadrant 2	2 ^(c)	E
14. Core Exit Temperature - Quadrant 3	2 ^(c)	E
15. Core Exit Temperature - Quadrant 4	2 ^(c)	E
16. Emergency Feedwater Flow	1 per SG ^(d)	E
17. Degrees of Subcooling	2	E
18. Main Steam Line Pressure	2 per steam generator SG	E
19. Emergency Feedwater Pit Level	2	E
20. Refueling Water Storage Pit Level (Wide Range)	2	E
21. Refueling Water Storage Pit Level (Narrow Range)	2	E

(a) Not required for isolation valves whose associated penetration is isolated by at least one closed and deactivated automatic valve, closed manual valve, blind flange, or check valve with flow through the valve secured.

(b) Only one position indication channel is required for penetration flow paths with only one installed control room indication channel.

~~(c) A channel consists of two core exit thermocouples.~~

~~(d) A RCS hot leg temperature wide range and RCS cold leg temperature wide range of the same loop are pair PAM functions. Similarly, SG water level wide range and an emergency feedwater flow of the same steam generator~~

~~are pair PAM functions. Either parameter forming a pair can fulfill all PAM requirements. Therefore, only 1 per loop/SG of either parameter of the pair is required.~~(c) Two thermocouple channels are required from each of two trains. For each train, one thermocouple channel is required near the center of the core and one thermocouple channel is required near the core perimeter.

(d) A channel consists of three sections with two sensors per section. A channel is OPERABLE if at least one sensor is OPERABLE in all three sections.

3.3 INSTRUMENTATION

3.3.4 Remote Shutdown Console (RSC)

LCO 3.3.4 The RSC shall be OPERABLE.

APPLICABILITY: MODES 1, 2 and 3.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
<p>A. RSC <u>One required channel or train inoperable for the Display and Control Function</u></p> <p><u>OR</u></p> <p><u>One train inoperable for the Transfer of Control Function.</u></p>	<p>A.1 Restore <u>channel or train</u> to OPERABLE status.</p>	30 days
<p>B. Required Action and associated Completion Time <u>of Condition A</u> not met.</p>	<p>B.1 Be in MODE 3.</p> <p><u>AND</u></p> <p>B.2 Be in MODE 4.</p>	<p>6 hours</p> <p>12 hours</p>

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.3.4.1	Perform TADOT for each -Transfer Switch <u>es</u> .	[24 months OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.4.2	Perform ACTUATION LOGIC <u>SAFETY VDU TEST</u> for each PSMS train <u>all four trains of the RSC Display Function</u> .	[24 months OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.4.3	Perform Safety VDU Test <u>CHANNEL CHECK</u> for each train of the PSMS <u>RSC Instrumentation Function</u> .	[24 months] <u>[31 days]</u> OR In accordance with the Surveillance Frequency Control Program]

<p><u>SR 3.3.4.4</u> -----NOTE----- <u>Neutron detectors are excluded from CHANNEL CALIBRATION.</u> <u>Perform CHANNEL CALIBRATION for each RSC Instrumentation Function.</u></p>	<p><u>[24 months</u> <u>OR</u> <u>In accordance with the Surveillance Frequency Control Program]</u></p>
<p><u>SR 3.3.4.5</u> <u>Perform MIC for the RSC.</u></p>	<p><u>[24 months</u> <u>OR</u> <u>In accordance with the Surveillance Frequency Control Program]</u></p>
<p><u>SR 3.3.4.6</u> <u>Perform TADOT for Actuation Outputs of each RSC Control Function.</u></p>	<p><u>[24 months</u> <u>OR</u> <u>In accordance with the Surveillance Frequency Control Program]</u></p>

3.3 INSTRUMENTATION

3.3.5 Loss of Power (LOP) Class 1E Gas Turbine Generator (GTG) Start Instrumentation

LCO 3.3.5 The following Loss of Power (LOP) Class 1E Gas Turbine Generator (GTG) Start Instrumentation shall be OPERABLE.

- a. Three channels per required bus of the loss of voltage Function and three channels per required bus of the degraded voltage Function ~~shall be OPERABLE, and~~
- b. One train per required bus of the LOP Actuation Function.

APPLICABILITY: MODES 1, 2, 3, and 4,
When associated Class 1E GTG is required to be OPERABLE by LCO 3.8.2, "AC Sources - Shutdown."

ACTIONS

-----NOTE-----
Separate Condition entry is allowed for each Function.

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more Functions with one or more channels <u>channel</u> per required bus inoperable.	A.1 -----NOTE----- The inoperable <u>One</u> channel may be bypassed for up to 4 hours for surveillance testing of, provided the other channels on the same bus are operable or placed in the trip condition. ----- Place channel in trip.	6 hours
B. One or more Functions with two or more channels per required bus inoperable.	B.1 Restore all but one channel per <u>required</u> bus to OPERABLE status.	1 hour
C. <u>One train of the LOP Actuation Function per</u>	C.1 Enter applicable Condition(s) and Required	Immediately

CONDITION	REQUIRED ACTION	COMPLETION TIME
<u>required bus inoperable.</u> <u>OR</u> Required Action and associated Completion Time <u>of Conditions A or B</u> not met.	Action(s) for the associated Class 1E GTG made inoperable by LOP Class 1E GTG start instrumentation. <u>Start Instrumentation.</u>	

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.3.5.1	Perform CHANNEL CHECK <u>TADOT</u> for LOP <u>undervoltage relays</u> .	[12 hours] <u>[31 days]</u> OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.5.2	Perform TADOT <u>CHANNEL CALIBRATION</u> for the following LOP undervoltage relays <u>consistent with Specification 5.5.21, Setpoint Control Program (SCP)</u> . <u>a. Loss of voltage</u> <u>b. Degraded voltage</u>	[31 days] <u>[24 months]</u> OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.5.3	Perform CHANNEL CALIBRATION <u>MIC</u> for LOP undervoltage relays with Specification 5.5.21, Setpoint Control Program (SCP), with the following time delays <u>Class 1E GTG Start Instrumentation</u> . a. Loss of voltage V with a time delay of \leq [0.8] second b. Degraded voltage with a time delay of \leq [20] seconds.	[24 months] OR In accordance with the Surveillance Frequency Control Program]

<p>SURVEILLANCE <u>SR 3.3.5.4 Perform TADOT for GTG control outputs.</u></p>	<p>FREQUENCY <u>[24 months</u> <u>OR</u> <u>In accordance with</u> <u>the Surveillance</u> <u>Frequency Control</u> <u>Program]</u></p>
<p>SR 3.3.5.4 Perform ACTUATION LOGIC TEST.</p>	<p>[24 months OR In accordance with the Surveillance Frequency Control Program]</p>
<p>SR 3.3.5.5 Perform TADOT for Class 1E GTG start Actuation Outputs.</p>	<p>[24 months OR In accordance with the Surveillance Frequency Control Program]</p>

3.3 INSTRUMENTATION

3.3.6 Diverse Actuation System (DAS) Instrumentation

LCO 3.3.6 DAS for each function in Table 3.3.6-1 shall be OPERABLE.

APPLICABILITY: According to Table 3.3.6-1.

ACTION

-----NOTE-----
Separate Condition entry is allowed for each Function.

CONDITION	REQUIRED ACTION	COMPLETION TIME
<p>A. One or more <u>Functions, with one or more subsystems or required DAS Functions channels</u> inoperable-.</p>	<p>-----NOTES-----</p> <ol style="list-style-type: none"> 1. <u>The Actuation Logic of one subsystem, or one required channel may be bypassed for up to 4 hours for surveillance testing, provided the Actuation Logic in the other subsystems or the other required channels are OPERABLE.</u> 2. <u>The Actuation Outputs of two subsystems may be bypassed for up to 4 hours for surveillance testing of the Actuation Outputs from the other subsystems, or surveillance testing of the Rod Drive Motor-Generator Set Trip Devices.</u> <hr/> <p>A.1 Restore required Function subsystem or channel to OPERABLE status.</p> <p>OR</p> <p>A.2.1 Be in MODE 3.</p> <p>AND</p>	<p>30 days</p> <p>Within the following 6 hours</p> <p>Within the following</p>

CONDITION	REQUIRED ACTION	COMPLETION TIME
	A.2.2 Be in MODE 4.	12 hours
<u>B. Required Action and associated Completion Time of Condition A not met.</u>	<u>B.1 Be in MODE 3.</u> <u>AND</u> <u>B.2 Be in MODE 4.</u>	<u>6 hours</u> <u>12 hours</u>

SURVEILLANCE REQUIREMENTS

-----NOTE-----

Refer to Table 3.3.6-1 to determine which SRs apply for each DAS Function.

SURVEILLANCE		FREQUENCY
SR 3.3.6.1	Perform CHANNEL CHECK for each required channel.	[31 days OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.6.2	Perform COT analog <u>consistent with Specification 5.5.21, Setpoint Control Program (SCP).</u>	[24 months OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.6.3	<p>-----NOTE----- <u>The CHANNEL CALIBRATION conducted for the PSMS in LCO 3.3.1 or 3.3.2 may be credited for DAS.</u></p> <p>Perform a CHANNEL CALIBRATION on each required channel consistent with Specification 5.5.21, Setpoint Control Program (SCP).</p>	[24 months OR In accordance with the Surveillance Frequency Control Program]
SR 3.3.6.4	Perform ACTUATION LOGIC TEST.	[24 months]

SURVEILLANCE	FREQUENCY
	OR In accordance with the Surveillance Frequency Control Program]

Table 3.3.6-1 (page 1 of 2)
Diverse Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
1.Reactor Trip/ Turbine Trip/ MFW Isolation				
a. Manual Initiation	1,2,3 ^(a)	1 ^(b)	A,B	SR 3.3.6.5 SR 3.3.6.6
b. Automatic -Actuation Logic and Actuation Outputs	1,2,3 ^(a)	2-4 subsystems	A,B	SR 3.3.6.4 SR 3.3.6.5
c. Low Pressurizer Pressure	1,2,3 ^(a)	2 3 ^(c)	A,B	SR 3.3.6.1 SR 3.3.6.2 SR 3.3.6.3
d. High Pressurizer Pressure	1,2,3 ^(a)	2 3 ^(c)	A,B	SR 3.3.6.1 SR 3.3.6.2 SR 3.3.6.3
e. Low Steam Generator Water Level	1,2,3 ^(a)	1 ^(a) per SG for any 2-3 SGs	A,B	SR 3.3.6.1 SR 3.3.6.2 SR 3.3.6.3
f. Rod Drive Motor-Generator Set <u>Trip Device</u>	1,2,3 ^(a)	<u>2 subsystems</u> (1 for each MG-Set)	A,B	SR 3.3.6.6
2. EFWS Actuation				
a. Manual Initiation	1,2,3 ^(a)	1 ^(b)	A,B	SR 3.3.6.5
b. Automatic -Actuation Logic and Actuation Outputs	1,2,3 ^(a)	2-4 subsystems	A,B	SR 3.3.6.5
c. Low Steam Generator Water Level	Refer to Function 1.e (<u>Reactor Trip/ Turbine Trip/ MFW Isolation - Low Steam Generator Water Level</u>) for all Low Steam Generator Water Level requirements.			

(a) With the Pressurizer Pressure > P-11

(b) Manual ~~initiation~~-Initiation and Manual Control ~~functions~~-Functions require operation of 2 switches on the DHP: (1) the Permissive Switch for DAS HSI, which is common to all Manual Initiation and Manual Control Functions, and (2) the manual initiation/Manual Initiation or Manual Control switch on the DHP, which is unique for each Function. Therefore, a channel consists of both switches and their respective interfaces to two of the four DAAC subsystems.

(c) Required channels for each of the four DAAC subsystems must be OPERABLE.

Table 3.3.6-1 (page 2 of 2)
Diverse Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS
3. <u>ECCS Actuation</u>				
a. Manual Initiation	1,2,3 ^(a)	1 ^(b)	A,B	SR 3.3.6.5
b. <u>Actuation Logic and Actuation Outputs</u>	1,2,3 ^(a)	4 subsystems	A,B	SR 3.3.6.4 SR 3.3.6.5
c. <u>Low-Low Pressurizer Pressure</u>	1,2,3 ^(a)	3 ^(c)	A,B	SR 3.3.6.1 SR 3.3.6.2 SR 3.3.6.3
4. <u>Containment Isolation</u>				
a. Manual Initiation	1,2,3 ^(a)	1 ^(b)	A,B	SR 3.3.6.5
5. EFW Isolation Valves				
a. Manual Control	1,2,3 ^(a)	1 ^(b) for each SG	A,B	SR 3.3.6.5
6. Pressurizer Safety Depressurization Valves				
a. Manual Control	1,2,3 ^(a)	1 ^(b)	A,B	SR 3.3.6.5
b. <u>Actuation Logic and Actuation Outputs</u>	1,2,3 ^(a)	4 subsystems	A,B	SR 3.3.6.4 SR 3.3.6.5
7. Main Steam Depressurization Valves				
a. Manual Control	1,2,3 ^(a)	1 ^(b) for each SG	A,B	SR 3.3.6.5
b. <u>Actuation Logic and Actuation Outputs</u>	1,2,3 ^(a)	4 subsystems	A,B	SR 3.3.6.4 SR 3.3.6.5
8. <u>Main Steam Line Isolation</u>				
a. <u>Manual Initiation</u>	1,2,3 ^(a)	1 ^(b)	A,B	SR 3.3.6.5
b. <u>Actuation Logic and Actuation Outputs</u>	1,2,3 ^(a)	4 subsystems	A,B	SR 3.3.6.4 SR 3.3.6.5

(a) With the Pressurizer Pressure > P-11

(b) ~~One channel is~~ Manual Initiation and Manual Control Functions require operation of 2 switches on the DHP: (1) ~~the~~ The Permissive Switch for DAS HSI₁ which is common to all Manual Initiation and Manual Control functions, and (2) the Manual Initiation or Manual Control switch, which is unique for each Function. Therefore, a channel consists of both switches and their respective interfaces to two of the four DAAC subsystems.

(c) Required channels for each of the four DAAC subsystems must be OPERABLE.

5.5 Programs and Manuals

5.5.20 Control Room Envelope Habitability Program (continued)

- e. The quantitative limits on unfiltered air leakage into the CRE. These limits shall be stated in a manner to allow direct comparison to the unfiltered air leakage measured by the testing described in paragraph c. The unfiltered air leakage limit for radiological challenges is the leakage flow rate assumed in the licensing basis analyses of DBA consequences. Unfiltered air leakage limits for hazardous chemicals must ensure that exposure of CRE occupants to these hazards will be within the assumptions in the licensing basis.
- f. The provisions of SR 3.0.2 are applicable to the Frequencies for assessing CRE habitability, determining CRE unfiltered leakage, and measuring CRE pressure and assessing the CRE boundary as required by paragraphs c and d, respectively.

5.5.21 Setpoint Control Program (SCP)

- a. The Setpoint Control Program (SCP) implements the regulatory requirement of 10 CFR 50.36 (c)(1)(ii) (A) that technical specifications will include items in the category of limiting safety system settings (LSSS), which are settings for automatic protective devices related to those variables having significant safety functions.
- b. The Nominal Trip Setpoint (NTSP), Allowable Value (AV), Performance Test Acceptance Criteria (PTAC), and Calibration Tolerance (CT) for each Technical Specification required automatic protection instrumentation function (i.e., reactor trip, ESFAS actuation and permissive interlocks) shall be calculated in conformance with the instrumentation setpoint methodology previously reviewed and approved by the NRC in [Title, Revision No., dated Month dd, yyyy, (MLxxxxxxx)] and the conditions stated in the associated NRC safety evaluation, [Letter to MHI from NRC, Title, dated Month, dd, yyyy, (MLxxxxxxx)].
- c. For each Technical Specification required automatic protection instrumentation function implemented with a ~~digital bistable function~~ conventional analog bistable, performance of a ~~CHANNEL CALIBRATION~~ COT surveillance shall include the following:
 1. ~~If all as found calibration setting values are inside the two-sided limits of (calibration setting \pm pre-defined test acceptance criteria band (PTAC)), then the channel is fully operable. The as-found value of the instrument channel trip setting shall be compared with the previous as-left value or the specified NTSP.~~
 - i. ~~2. If any as found calibration setting value is outside the two-sided limits of (calibration setting \pm PTAC), but inside the limits of \pm AV, then the channel is operable but degraded, and corrective action is~~

~~required to restore the channel to within specifications. If the as-found value of the instrument channel trip setting differs from the previous as-left value or the specified NTSP by more than the PTAC, but less than the specified AV, then the instrument channel shall be evaluated to verify that it is functioning in accordance with its design basis before declaring the surveillance requirement met and returning the instrument channel to service. This condition shall be dispositioned by the plant's corrective action program.~~

- ~~3.— If any the as-found calibration setting value is outside the two-sided limits of $\pm AV$, then the channel is inoperable, and corrective action is required, including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.~~

~~The Calibration Tolerance (CT) limits are applied to the calibration setting. The instrument channel calibration settings shall be set or confirmed to be within the specified CT around the five calibration settings (0, 25, 50, 75 and 100 percent) at the completion of each CHANNEL CALIBRATION surveillance. CT is a two-sided limit controlled by plant procedures, and is typically Sensor Calibration Accuracy (SCA), Rack Calibration Accuracy (RCA), or a combination of both.~~

- ~~d.— For each Technical Specification required automatic protection instrumentation function implemented with a binary sensor connected to a digital channel or an analog bistable function, performance of a CHANNEL CALIBRATION surveillance (binary sensors connected to digital channels) or a COT-analog surveillance (analog bistables) shall include the following:~~
- ~~1.— If the as found trip setting differs from the specified NTSP by less than the PTAC, then the channel is fully operable.~~
 - ~~2.— If the as found trip setting differs from the specified NTSP by more than the PTAC, but less than the specified AV, then the channel is operable but degraded, and corrective action is required to restore the channel to within specifications.~~
 - ~~ii. 3.— If the as found trip setting is differs from the specified NTSP by more than the specified AV, then the channel is inoperable, and corrective action is required, including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.~~

~~The CT limits are applied to NTSP.~~

surveillance requirement is not met and the instrument channel shall be immediately declared inoperable.

2. The instrument channel trip setting shall be set or confirmed to be within the specified CT around the NTSP at the completion of each COT-~~analog~~ surveillance; otherwise, the ~~surveillance. CT is a two-sided limit~~

~~controlled by plant procedures, and is typically a function of SCA, RCA or a combination of both.~~ requirement is not met and the instrument channel shall be immediately declared inoperable.

- ~~d.~~ e.—For each Technical Specification required automatic protection instrumentation function implemented with ~~an~~ a conventional analog bistable ~~function~~, the difference between the instrument channel trip setting as-found value and either the previous as-left ~~trip setting~~ value or the specified NTSP shall be trended and evaluated to verify that the instrument channel is functioning in accordance with its design basis.
- e. For each Technical Specification required automatic protection instrumentation function implemented with a binary sensor (e.g., pressure switches, UV relays), performance of a CHANNEL CALIBRATION surveillance shall include the following:
1. The as-found value of the instrument channel state change shall be compared with the previous as-left value or the specified NTSP.
 - i. If the as-found value of the instrument channel state change differs from the previous as-left value or the specified NTSP by more than the PTAC, but less than the specified AV, then the instrument channel shall be evaluated to verify that it is functioning in accordance with its design basis before declaring the surveillance requirement met and returning the instrument channel to service. This condition shall be dispositioned by the plant's corrective action program.
 - ii. If the as-found value of the instrument channel state change differs from the specified NTSP by more than the specified AV, then the surveillance requirement is not met and the instrument channel shall be immediately declared inoperable.
 2. The instrument channel state change shall be set or confirmed to be within the specified CT around the NTSP at the completion of each CHANNEL CALIBRATION surveillance; otherwise, the surveillance requirement is not met and the instrument channel shall be immediately declared inoperable.
- f. For each Technical Specification required automatic protection instrumentation function implemented with a binary sensor, the difference between the instrument channel ~~trip setting~~ state change as-found value and either the previous as-left ~~trip setting~~ value or the specified NTSP shall be trended and evaluated to verify that the instrument channel is functioning in accordance with its design basis.
- g. For each Technical Specification required automatic protection instrumentation function implemented with ~~a digital bistable function~~ an analog sensor (e.g.,

pressure transmitter), performance of a CHANNEL CALIBRATION surveillance shall include the following:

1. The as-found value of the instrument channel calibration setting shall be compared with the previous as-left value or the specified calibration setting at five calibration settings corresponding to 0%, 25%, 50%, 75% and 100% of the instrument range.
 - i. If any as-found calibration setting value is outside the two-sided limits of “previous as-left value \pm PTAC” or “calibration setting \pm PTAC,” but inside the specified limits of \pm AV, then the instrument channel shall be evaluated to verify that it is functioning in accordance with its design basis before declaring the surveillance requirement met and returning the instrument channel to service. This condition shall be dispositioned by the plant’s corrective action program.
 - ii. If any as-found calibration setting value is outside of the two-sided limits of \pm AV, then the surveillance requirement is not met and the instrument channel shall be immediately declared inoperable.
 2. The instrument channel calibration settings shall be set or confirmed to be within the specified CT around the five calibration settings (0%, 25%, 50%, 75%, and 100%) at the completion of each CHANNEL CALIBRATION surveillance; otherwise, the surveillance requirement is not met and the instrument channel shall be immediately declared inoperable.
- h. For each Technical Specification required automatic protection instrumentation function implemented with an analog sensor, the difference between the instrument channel calibration setting (0%, 25%, 50%, 75%, and 100 percent%) as-found value and either the previous as-left values-value or the specified calibration setting shall be trended and evaluated to verify that the instrument channel is functioning in accordance with its design basis.
- i. ~~f.~~—The SCP shall establish a document containing the current values of the specified NTSP, AV, PTAC, and CT for each Technical Specification required automatic protection instrumentation function, and references to the calculation documentation. Changes to this document shall be governed by the regulatory requirements of 10 CFR 50.59. In addition, changes to the specified NTSP, AV, PTAC, and CT values shall be governed by the approved setpoint methodology. This document, including any midcycle revisions or supplements, shall be provided upon issuance for each reload cycle to the NRC.
- j. For each Technical Specification required automatic protection instrumentation function implemented with a digital bistable, the Nominal Trip Setpoint value shall be confirmed during the software MEMORY INTEGRITY CHECK (MIC).

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

The referenced NRC approved setpoint methodology shall meet the following guidance, and shall be applicable to Technical Specification required automatic protection instrumentation function surveillances that require verification that ~~setpoints (or channel outputs)~~ channel trip settings, state change values, and calibration settings are within the necessary range and accuracy (e.g., COT, CHANNEL CALIBRATIONS):

1. ~~1.~~—The methodology allows little variation in the values calculated by different analysts using identical input values (such as uncertainties and channel calibration drift).
2. ~~2.~~ ~~For each Technical Specification required automatic protection instrumentation function implemented with an analog bistable function, the as-left value of the instrument channel trip setting~~ The as-left value of the instrument channel (applicable to trip settings, state change values, and calibration settings) shall be the value at which the channel was set or left at the completion of the surveillance with no additional adjustment of the instrument channel.

~~For each Technical Specification required automatic protection instrumentation function implemented with a digital bistable function, the as-left value of the instrument channel calibration of the surveillance with no additional adjustment of the instrument channel.~~

3. ~~3.~~ ~~For each Technical Specification required automatic protection instrumentation function implemented with an analog bistable function, the~~ The as-found value of the instrument channel (applicable to trip settings, state change values, and calibration settings) shall be the ~~trip setting~~ value measured during the subsequent performance of the surveillance before making any adjustment to the instrument channel that could change the ~~trip setting~~ value.

~~4.~~

4. If the requirements of 5.5.21.c.1 or 5.5.21.d include an allowance for e.1 are satisfied by comparing the as-found value to be compared with the specified calibration setting or NTSP, then the following conditions shall be applied:

- a. ~~a.~~—The setting tolerance band (i.e., the specified CT) must be less than or equal to the square root of the sum of the squares of reference accuracy, measurement and test equipment errors, and readability uncertainties;
- b. ~~b.~~—The setting tolerance band (i.e., the specified CT) must be included in the total loop uncertainty; and
- c. ~~c.~~—The pre-defined test acceptance criteria band (i.e., the specified PTAC) for the as-found value must include either the setting tolerance

band (the specified CT) or the uncertainties associated with the setting tolerance band (the specified CT), but not both of these.

5. If the requirements of 5.5.21.g.1 are satisfied by comparing the as-found value to the specified calibration setting, then the following conditions shall be applied:
 - a. The setting tolerance band (i.e., the specified CT) must be less than or equal to the square root of the sum of the squares of reference accuracy, measurement and test equipment errors, and readability uncertainties;
 - b. The setting tolerance band (i.e., the specified CT) must be included in the total loop uncertainty; and
 - c. The pre-defined test acceptance criteria band (i.e., the specified PTAC) for the as-found value must include either the setting tolerance band (the specified CT) or the uncertainties associated with the setting tolerance band (the specified CT), but not both of these.
-
-

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.9 PHYSICS TESTS Exceptions - MODE 2

BASES

BACKGROUND

The primary purpose of the MODE 2 PHYSICS TESTS exceptions is to permit relaxations of existing LCOs to allow certain PHYSICS TESTS to be performed.

Section XI of 10 CFR 50, Appendix B (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that the specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. This testing is an integral part of the design, construction, and operation of the plant. Requirements for notification of the NRC, for the purpose of conducting tests and experiments, are specified in 10 CFR 50.59 (Ref. 2).

The key objectives of a test program are to (Ref. 3):

- a. Ensure that the facility has been adequately designed,
- b. Validate the analytical models used in the design and analysis,
- c. Verify the assumptions used to predict unit response,
- d. Ensure that installation of equipment in the facility has been accomplished in accordance with the design, and
- e. Verify that the operating and emergency procedures are adequate.

To accomplish these objectives, testing is performed prior to initial criticality, during startup, during low power operations, during power ascension, at high power, and after each refueling. The PHYSICS TESTS requirements for reload fuel cycles ensure that the operating characteristics of the core are consistent with the design predictions and that the core can be operated as designed (Ref. 4).

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of the testing required to ensure that the design intent is met. PHYSICS TESTS are performed in accordance with these procedures and test results are approved prior to continued power escalation and long term power operation.

BASES

BACKGROUND (continued)

The PHYSICS TESTS required for reload fuel cycles (Ref. 4) in MODE 2 are listed below:

- a. Critical Boron Concentration - Control Rods Withdrawn,
- b. Control Rod Worth, and
- c. Isothermal Temperature Coefficient (ITC)

These tests are performed in MODE 2. These and other supplementary tests may be required to diagnose operational problems. These tests may cause the operating controls and process variables to deviate from their LCO requirements during their performance.

- a. The Critical Boron Concentration - Control Rods Withdrawn Test measures the critical boron concentration at hot zero power (HZP). With all rods out, the lead control bank is at or near its fully withdrawn position. HZP is where the core is critical ($k_{\text{eff}} = 1.0$), and the Reactor Coolant System (RCS) is at design temperature and pressure for zero power. Performance of this test should not violate any of the referenced LCOs.

BASES

BACKGROUND (continued)

- b. The Control Rod Worth Test is used to measure the reactivity worth of selected control banks. This test is performed at HZP and has three alternative methods of performance. The first method, the Boron Exchange Method, varies the reactor coolant boron concentration and moves the selected control bank in response to the changing boron concentration. The reactivity changes are measured with a reactivity computer. This sequence is repeated for the remaining control banks. The second method, the Rod Swap Method, measures the worth of a predetermined reference bank using the Boron Exchange Method above. The reference bank is then nearly fully inserted into the core. The selected bank is then inserted into the core as the reference bank is withdrawn. The HZP critical conditions are then determined with the selected bank fully inserted into the core. The worth of the selected bank is inferred, based on the position of the reference bank with respect to the selected bank. This sequence is repeated as necessary for the remaining control banks. The third method, the Boron Endpoint Method, moves the selected control bank over its entire length of travel and then varies the reactor coolant boron concentration to achieve HZP criticality again. The difference in boron concentration is the worth of the selected control bank. This sequence is repeated for the remaining control banks. Performance of this test could violate LCO 3.1.4, LCO 3.1.5, or LCO 3.1.6.
- c. The ITC Test measures the ITC of the reactor. This test is performed at HZP and has two methods of performance. The first method, the Slope Method, varies RCS temperature in a slow and continuous manner. The reactivity change is measured with a reactivity computer as a function of the temperature change. The ITC is the slope of the reactivity versus the temperature plot. The test is repeated by reversing the direction of the temperature change, and the final ITC is the average of the two calculated ITCs. The second method, the Endpoint Method, changes the RCS temperature and measures the reactivity at the beginning and end of the

BASES

BACKGROUND (continued)

temperature change. The ITC is the total reactivity change divided by the total temperature change. The test is repeated by reversing the direction of the temperature change, and the final ITC is the average of the two calculated ITCs. Performance of this test could violate LCO 3.4.2, "RCS Minimum Temperature for Criticality."

 APPLICABLE
SAFETY
ANALYSES

The fuel is protected by LCOs that preserve the initial conditions of the core assumed during the safety analyses. The methods for development of the LCOs that are excepted by this LCO are described in Ref. 5. The above mentioned PHYSICS TESTS, and other tests that may be required to calibrate nuclear instrumentation or to diagnose operational problems, may require the operating control or process variables to deviate from their LCO limitations.

Section 14.2 (Ref.6) defines requirements for initial testing of the facility, including PHYSICS TESTS. The zero, low power, and power tests are summarized in this section. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS-19.6.1-2005 (Ref. 4). Although these PHYSICS TESTS are generally accomplished within the limits for all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TESTS possible or practical. This is acceptable as long as the fuel design criteria are not violated. When one or more of the requirements specified in LCO 3.1.3, "Moderator Temperature Coefficient (MTC)," LCO 3.1.4, LCO 3.1.5, LCO 3.1.6, and LCO 3.4.2 are suspended for PHYSICS TESTS, the fuel design criteria are preserved as long as the power level is limited to $\leq 5\%$ RTP the reactor coolant temperature is kept $\geq 541^\circ\text{F}$, and SDM is within the limits provided in the COLR.

The PHYSICS TESTS include measurement of core nuclear parameters or the exercise of control components that affect process variables. Among the process variables involved are AFD and QPTR, which represent initial conditions of the unit safety analyses. Also involved are the movable control components (control and shutdown rods), which are required to shut down the reactor. The limits for these variables are specified for each fuel cycle in the COLR.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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

LCO

This LCO allows the reactor parameters of MTC and minimum temperature for criticality to be outside their specified limits. In addition, it allows selected control and shutdown rods to be positioned outside of their specified alignment and insertion limits. One power range neutron flux channel may be bypassed, reducing the number of required channels from 4 to 3. Operation beyond specified limits is permitted for the purpose of performing PHYSICS TESTS and poses no threat to fuel integrity, provided the SRs are met.

The requirements of LCO 3.1.3, LCO 3.1.4, LCO 3.1.5, LCO 3.1.6, and LCO 3.4.2 may be suspended and the number of required channels for LCO 3.3.1, "RTS Instrumentation," Functions 2, 3 and 15.c may be reduced to 3 required channels during the performance of PHYSICS TESTS provided:

- a. RCS lowest loop average temperature is $\geq 541^{\circ}\text{F}$,
- b. SDM is within the limits provided in the COLR, and
- c. THERMAL POWER is $\leq 5\%$ RTP.

APPLICABILITY

This LCO is applicable when performing low power PHYSICS TESTS. The Applicability is stated as "during PHYSICS TESTS initiated in MODE 2" to ensure that the 5% RTP maximum power level is not exceeded. Should the THERMAL POWER exceed 5% RTP, and consequently the unit enter MODE 1, this Applicability statement prevents exiting this Specification and its Required Actions.

BASES

ACTIONS

A.1 and A.2

If the SDM requirement is not met, boration must be initiated promptly. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. The operator should begin boration with the best source available for the plant conditions. Boration will be continued until SDM is within limit.

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

B.1

When THERMAL POWER is > 5% RTP, the only acceptable action is to open the reactor trip breakers (RTBs) to prevent operation of the reactor beyond its design limits. Immediately opening the RTBs will shut down the reactor and prevent operation of the reactor outside of its design limits.

C.1

When the RCS lowest T_{avg} is < 541°F, the appropriate action is to restore T_{avg} to within its specified limit. The allowed Completion Time of 15 minutes provides time for restoring T_{avg} to within limits without allowing the plant to remain in an unacceptable condition for an extended period of time. Operation with the reactor critical and with temperature below 541°F could violate the assumptions for accidents analyzed in the safety analyses.

D.1

If the Required Actions cannot be completed within the associated Completion Time, the plant must be brought to a MODE in which the requirement does not apply. To achieve this status, the plant must be brought to at least MODE 3 within an additional 15 minutes. The Completion Time of 15 additional minutes is reasonable, based on operating experience, for reaching MODE 3 in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE
REQUIREMENTSSR 3.1.9.1

The power range and intermediate range neutron detectors must be verified to be OPERABLE in MODE 2 by LCO 3.3.1, "Reactor Trip System (RTS) Instrumentation." A CHANNEL CALIBRATION is performed on each power range and intermediate range channel per SR 3.3.1.9, consistent with Specification 5.5.21, Setpoint Control Program (SCP), prior to initiation of the PHYSICS TESTS. This will ensure that the RTS is properly aligned to provide the required degree of core protection during the performance of the PHYSICS TESTS.

SR 3.1.9.2

Verification that the RCS lowest loop T_{avg} is $\geq 541^{\circ}\text{F}$ will ensure that the unit is not operating in a condition that could invalidate the safety analyses. [Verification of the RCS temperature at a Frequency of 30 minutes during the performance of the PHYSICS TESTS will ensure that the initial conditions of the safety analyses are not violated. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.1.9.3

Verification that the THERMAL POWER is $\leq 5\%$ RTP will ensure that the plant is not operating in a condition that could invalidate the safety analyses. [Verification of the THERMAL POWER at a Frequency of 30 minutes during the performance of the PHYSICS TESTS will ensure that the initial conditions of the safety analyses are not violated. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.1.9.4

The SDM is verified by performing a reactivity balance calculation, considering the following reactivity effects:

- a. RCS boron concentration,
- b. Control bank position,
- c. RCS average temperature,

BASES

SURVEILLANCE REQUIREMENTS (continued)

- d. Fuel burnup based on gross thermal energy generation,
- e. Xenon concentration,
- f. Samarium concentration,
- g. Isothermal temperature coefficient (ITC), when below the zero power testing range,
- h. Moderate defect, when above the zero power testing range, and
- i. Doppler defect, when above the zero power testing range.

Using the ITC accounts for Doppler reactivity in this calculation when the reactor is subcritical or critical but below the zero power testing range, and the fuel temperature will be changing at the same rate as the RCS.

[The Frequency of 24 hours is based on the generally slow change in required boron concentration and on the low probability of an accident occurring without the required SDM. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

REFERENCES

- 1. 10 CFR 50, Appendix B, Section XI.
 - 2. 10 CFR 50.59.
 - 3. Regulatory Guide 1.68, Revision 3, March, 2007.
 - 4. ANSI/ANS-19.6.1-2005, November 29, 2005.
 - 5. MUAP-07026-P, "Mitsubishi Reload Evaluation Methodology", December, 2007
 - 6. Section 14.2.
-
-

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Trip System (RTS) Instrumentation

BASES

BACKGROUND

The RTS initiates a unit shutdown, based on the values of selected unit parameters, to protect against violating the core fuel design limits and Reactor Coolant System (RCS) pressure boundary during anticipated operational occurrences (AOOs) and to assist the Engineered Safety Features (ESF) Systems in mitigating accidents.

The protection and monitoring systems have been designed to assure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RTS, as well as specifying LCOs on other reactor system parameters and equipment performance.

Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices...so chosen that automatic protective action will correct the abnormal situation before a Safety Limit (SL) is exceeded." The ~~Analytic~~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 a SL is not exceeded. Any automatic protection action that occurs on reaching the ~~Analytic~~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 ~~Analytic~~Analytical Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The Nominal Trip Setpoint, recorded and maintained in a document established by the Setpoint Control Program (SCP), is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the ~~Analytic~~Analytical Limit and thus ensuring that the SL would not be exceeded. As such, the Nominal Trip Setpoint accounts for uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., repeatability), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors which may influence its actual performance (e.g., harsh accident environments). In this manner, the Nominal Trip Setpoint plays an important role in ensuring that SLs are not exceeded. As such, the Nominal Trip Setpoint meets the definition of an LSSS (Ref. 1) and is used to meet the requirement that they be contained in the Technical Specifications. This is an acceptable approach for digital systems because the digital setpoints do not drift as in analog systems. -The Nominal Trip Setpoint is applicable to automatic

protection instrumentation functions for Reactor Trip, ESF Actuation System (ESFAS) actuation and permissive interlocks.

Technical Specifications contain ~~measured accuracy values~~ Allowable Values related to the OPERABILITY of equipment required for safe operation of the facility. - The ~~measured accuracy value~~ Allowable Value accommodates expected drift in the analog components of the channel that would have been specifically accounted for in the setpoint methodology for calculating the Nominal Trip Setpoint and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as-found" settings 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 recalibrate the device 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. This value needs to be specified in the Technical Specifications in order to define OPERABILITY of the devices and is designated as the Allowable Value. ~~The Allowable Value is another important component of the LSSS~~

- The Allowable Value, recorded and maintained in a document established by the Setpoint Control Program (SCP) ~~demonstrates~~, is considered a limiting value such that a channel is OPERABLE if the ~~measured accuracy is as-found~~ value does not to exceed the Allowable Value during CHANNEL CALIBRATION ~~(protection functions implemented with digital bistable functions) or GOT (protection functions implemented with~~ -The Allowable Value, is applicable to automatic protection instrumentation functions for Reactor Trip, ESFAS actuation and permissive interlocks.

For analog ~~bistable functions).~~ The measurements, the CHANNEL CALIBRATION verifies the instrument channel accuracy at five calibration settings corresponding to 0%, 25%, 50%, 75% and 100% of the instrument range. For binary measurements, the CHANNEL CALIBRATION verifies the accuracy of the channel's state change at the required setpoint. As such, the Allowable Value accounts for the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will still meet the LSSS definition and ensure that a SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval.

Note that, although the channel is "OPERABLE" under these circumstances, the channel ~~should~~ shall be left adjusted to a value within the established channel ~~calibration tolerance~~ Calibration Tolerance (CT) band, in accordance with uncertainty assumptions stated in the referenced setpoint methodology (as-left criteria), and confirmed to be operating within the statistical allowances of the uncertainty terms

assigned. -The Calibration Tolerance, recorded and maintained in a document established by the SCP, is applicable to automatic protection instrumentation functions for Reactor Trip, ESFAS actuation and permissive interlocks.

If the ~~actual accuracy~~ as-found value of the device is found to have exceeded the Allowable Value, or the as-left value of the device cannot be adjusted to a value within the Calibration Tolerance, the device would be considered inoperable from a technical specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

In the Protection and Safety Monitoring System (PSMS), setpoints associated with analog measurements are stored as digital values that have no potential for variation due to time, environmental drift or component aging. For analog measurements, the only factors that can result in variation in the ~~trip function~~ trip Functions reside in the uncertainties that are pertinent to the analog portion of the system. Therefore, for analog measurements in the PSMS, it is appropriate for the Allowable Value to be expressed in terms of values that are measured during periodic testing of the analog portion of the system (i.e., CHANNEL CALIBRATION).

For PSMS analog measurements, the as-found and as-left values are measured from sensor to digital Visual Display Unit (VDU) readout during CHANNEL CALIBRATION. The US-APWR enhances human performance by establishing a standard CHANNEL CALIBRATION method for all analog measurements, whereby the as-found and as-left values read at the VDU are measured at the same five calibration settings, regardless of the PSMS trip setpoint(s).

Since the PSMS trip logic and setpoints for analog measurements are stored as digital values with no drift potential, and those digital values are confirmed through the MEMORY INTEGRITY CHECK (MIC), the only untested area required to confirm channel operability pertains to the accuracy of the analog input signal. - When the analog input accuracy is confirmed, by reading the digital values of the five point CHANNEL CALIBRATION settings on any VDU driven by the same digital value used in the controller that executes the ~~trip function~~ trip Functions, the operability of the complete channel is confirmed, including the accuracy of all trip setpoints associated with that channel.

In the PSMS, setpoints associated with binary measurements are stored within the binary device itself. These setpoints have potential for variation due to time, environmental drift or component aging. However, these sensors are interfaced to the digital portion of the PSMS, which has no potential for variation due to time, environmental drift or component aging. For binary measurements, the only factors that can result in variation in the ~~trip function~~ trip Functions reside in the uncertainties that are pertinent

to the binary sensor itself. Therefore, for binary measurements in the PSMS, it is appropriate for the Allowable Value to be expressed in terms of values that are measured during periodic testing of the binary device (i.e., CHANNEL CALIBRATION).

For PSMS binary measurements, the as-found and as-left state change values are measured from sensor to VDU readout during CHANNEL CALIBRATION. The US-APWR enhances human performance by establishing a standard CHANNEL CALIBRATION method for all binary measurements, whereby the as-found and as-left values read at the VDU are measured at the channel's required state change.

Since the PSMS trip logic for binary sensors is stored as digital values with no drift potential, and those digital values are confirmed through the MIC, the only untested area required to confirm channel operability pertains to the accuracy of the binary input signal.- When the binary input accuracy is confirmed, by reading the channel's state change on any VDU driven by the same digital value used in the controller that executes the ~~trip function~~ trip Functions, the operability of the complete channel is confirmed, including the accuracy of the trip setpoint associated with that channel.

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

1. The Departure from Nucleate Boiling Ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling (DNB),
2. Fuel centerline melt shall not occur, and
3. The RCS pressure SL of 2733.5 psig shall not be exceeded.

Operation within the SLs of Specification 2.0, "Safety Limits (SLs)," also maintains the above values and assures that offsite dose will be within the 10 CFR 50 and 10 CFR 100 criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the unit life. The acceptable limit during accidents is that offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 limits. Different accident categories are allowed a different fraction of these limits, based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

The RTS instrumentation is segmented into four distinct but interconnected modules as illustrated in Chapter 7 (Ref. 2), and as identified below:

1. Field transmitters, process sensors or field contacts: provide a measurable electronic signal based upon the physical characteristics of the parameter being measured,
2. The RPS, including Nuclear Instrumentation System (NIS): provides signal conditioning, analog to digital conversion, ~~bistable~~digital bistables for setpoint comparison, process algorithm actuation, compatible electrical signal output to the ~~reactor trip breakers~~Reactor Trip Breakers (RTBs), and digital output to control board/control room/miscellaneous VDUs, and
3. Reactor trip -breakers (RTBs): provide the means to interrupt power to the control rod drive mechanisms (CRDMs) and allows the rod cluster control assemblies (RCCAs), or "rods," to fall into the core and shut down the reactor.
- ~~4.~~ 4. Manual Reactor Trip switches: provide the ~~manual reactor trip initiation~~Manual Reactor Trip Initiation in the control room.
- 4.

Field Transmitters or Sensors

To meet the design demands for redundancy and reliability, more than one, and often as many as four, field transmitters or sensors are used to measure unit parameters. To account for the calibration tolerances and instrument drift, which are assumed to occur between calibrations, statistical allowances are provided in the Nominal Trip Setpoint and Allowable Values. The OPERABILITY of each transmitter or sensor is determined by ~~either~~ "as-found" calibration data evaluated during the CHANNEL CALIBRATION ~~or~~and by qualitative assessment of field transmitter or sensor as related to the channel behavior observed during performance of the CHANNEL CHECK.

Protection and Safety Monitoring System

Generally, four channels of process control equipment are used for the signal processing of unit parameters measured by the field instruments. Four channels provides the capability for unlimited bypass of one channel while maintaining single failure criteria, therefore generally allowing a requirement for only three channels to be OPERABLE. The process control equipment provides signal conditioning, analog to digital conversion, comparable digital output signals for VDUs located on the main control board, and comparison of measured input signals with setpoints established by safety analyses. ~~These setpoints are defined in Chapter 7 (Ref. 2).~~ If the measured value of a unit parameter exceeds the predetermined setpoint, ~~an~~ a digital output from a digital bistable is processed for decision evaluation. Channel separation is maintained throughout the PSMS. Some unit parameters provide input only to the PSMS, while others are ~~use~~used by the PSMS and are retransmitted to

the Plant Control and Monitoring System (PCMS) for use in one or more control systems.

Generally, if a parameter is used only for input to the protection circuits, three channels with a two-out-of-three logic are sufficient to provide the required reliability and redundancy. If one channel fails in a direction that would not result in a partial Function trip, the Function is still OPERABLE with a two-out-of-two logic. If one channel fails, such that a partial Function trip occurs, a trip will not occur and the Function is still OPERABLE with a one-out-of-two logic.

Generally, if a parameter is used for input to the protection circuits and a control function, three channels with a two-out-of-three logic are also sufficient to provide the required reliability and redundancy. ~~The~~ When three or more channels are OPERABLE, the Signal Selection Algorithm (SSA) within the PCMS ensures the control systems can withstand an input failure to the control system without causing erroneous control system operation, which would otherwise require the protection function actuation. Since the input failure does not cause an erroneous control system action that challenges the protection function, the input failure is considered a single failure in the RTS and the RTS remains capable of providing its protective function with the remaining two ~~operable~~ OPERABLE channels. Again, a single failure will neither cause nor prevent the protection function actuation. These requirements are described in IEEE-603-1991 (Ref. 4). The actual number of channels required for each unit parameter is specified in Reference 2. When there are less than three OPERABLE channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for shared channels, when there are only three required channels.

The RTB trains are arranged in a two-out-of-four configuration. Therefore, three logic trains are required to ensure no single random failure of a logic train will disable the RTS. The logic trains are designed such that testing required while the reactor is at power may be accomplished without causing trip. Provisions allow removing logic trains from service during maintenance.

Allowable Values and RTS Setpoints

The Nominal Trip Setpoints used in the digital bistables or binary sensors are based on the Analytical Limits defined in the accident analysis and the channel uncertainty. The selection of these Nominal Trip Setpoints is such that adequate protection is provided when all sensor and processing ~~time delays~~ Time Delays are taken into account.

To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors for those RTS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 5), the Nominal Trip Setpoints ~~recorded~~ and ~~maintained in a~~

~~document established by the SCP in the accompanying LCO-Allowable Values~~ are conservative ~~with respect to~~ protect the Analytical Limits. The methodology identified in the SCP, used to calculate the Allowable Values and Nominal Trip Setpoints, incorporates all of the known uncertainties applicable to each channel (Ref. 12). The magnitudes of these uncertainties are factored into the determination of each Nominal Trip Setpoint and ~~corresponding~~ Allowable Value.

The Nominal Trip Setpoint entered into the digital bistable ~~or binary sensor~~ is more conservative than that specified by the ~~Analytical~~~~Analytical~~~~Analytical~~ Limit (~~LSSS~~) ~~to account~~. The Nominal Trip Setpoint -accounts for measurement errors detectable by the CHANNEL CALIBRATION ~~- and other unmeasurable errors (such as the effects of anticipated environmental conditions), which are both considered in the Allowable Value for CHANNEL CALIBRATION.~~ The Allowable Value serves as the Technical Specification OPERABILITY limit for the purpose of the CHANNEL CALIBRATION. One example of such a change in measurement error is drift during the surveillance interval. If the ~~measured accuracy as found value~~ does not exceed the Allowable Value, the channel is considered OPERABLE.

The Nominal Trip Setpoint (i.e., LSSS) is the value at which the digital bistable ~~or binary sensor~~ is set. The Nominal Trip Setpoint value ensures the ~~LSSS and the~~ safety analysis limits are met for the surveillance interval selected when a channel is adjusted based on the stated channel uncertainties. Any channel is considered to be properly adjusted when the "as-left" value is within the established Calibration Tolerance (CT) band, in accordance with the methods and assumptions ~~in of~~ the SCP. The Nominal Trip Setpoint value (i.e., expressed as a value without inequalities) ~~is used~~ for digital bistables, is confirmed during the purposes of COTMIC. The Nominal Trip Setpoint value (i.e., expressed as a value with inequalities) for binary sensors is confirmed during the CHANNEL CALIBRATION.

Nominal Trip Setpoints and Allowable Values, consistent with the requirements of the ~~Allowable Value~~ SCP, ensure that SLs are not violated during AOOs ~~(and that the consequences of Postulated Accidents (PAs) will be acceptable, providing provided~~ the unit is operated from within the LCOs at the onset of the AOO or PA and the equipment functions as designed).

~~Digital~~ Within the PSMS controllers, Nominal Trip Setpoints and Time Constants are digital settings maintained in non-volatile software memory within each Reactor Protection System (RPS) train. Digital settings have no potential for variation due to time, environmental drift or component aging; therefore, these digital settings have no surveillance tolerance. Each ~~train of the process control equipment is~~ PSMS controller has continuous automatic self-tested continuously on-line to verify testing, which verifies that the digital Nominal Trip Setpoint and Time Constant settings are correct. ~~-~~ Nominal Trip Setpoints and Time Constants are

also verified periodically through ~~a diverse software memory integrity test, which may~~ the MIC which must be conducted with the ~~RTS train~~ affected PSMS controller out of service. A designated instrument channel is taken out of service for periodic ~~calibration~~ CHANNEL CALIBRATION. SRs for the channels and trains are specified in the SRs section.

NOTE: The Allowable Value ~~recorded and maintained in a document established by the SCP~~ is the maximum deviation ~~at the calibration setpoints~~ that can be measured during CHANNEL CALIBRATION, whereby the channel is considered OPERABLE. This value ~~is~~ includes the deviations that are included in the calculations that determined the ~~TRIP SETPOINT recorded and maintained in a document established by the SCP~~ Nominal Trip Setpoint. The "expected as-found value" shall be as specified in the plant-specific setpoint analysis. The expected as-found value reflects the expected normal drift of actual plant equipment, so that a degraded device can be identified before the Allowable Value limit is reached. The expected as-found value is also referred to as the Performance Test Acceptance Criteria (PTAC). The PTAC, recorded and maintained in a document established by the SCP, is applicable to automatic protection instrumentation functions for Reactor Trip, ESFAS actuation and permissive interlocks.

Reactor Trip Breakers

The RTBs are in the electrical power supply line from the control rod drive motor generator set power supply to the CRDMs. Opening of the RTBs interrupts power to the CRDMs, which allows the shutdown rods and control rods to fall into the core by gravity. There are eight RTBs, two from each of four RTB trains, arranged in a ~~two-out-of-four~~ two-out-of-four configuration.

During normal operation the output from the RPS is a voltage signal that energizes the undervoltage coils in the RTBs. When protective action is required, the RPS output voltage signal is removed, the undervoltage coils are de-energized, the breaker trip lever is actuated by the de-

energized undervoltage coil, and the RTBs are tripped open. This allows the shutdown rods and control rods to fall into the core. In addition to the de-energization of the undervoltage coils, each breaker is also equipped with a shunt trip device that is energized to trip the breaker open upon receipt of a ~~reactor trip~~ Reactor Trip signal from the RPS. Either the undervoltage coil or the shunt trip mechanism is sufficient by itself, thus providing a diverse trip mechanism.

The decision logic matrix Functions are described in the functional diagrams included in Reference 2. In addition to the ~~reactor trip~~ Reactor Trip or ESF, these diagrams also describe the various "permissive interlocks" that are associated with unit conditions. Each train has built in continuous automatic self-testing that automatically tests the decision logic Functions while the unit is at power. When any one or two trains are

taken out of service for testing, the other two trains are capable of providing unit monitoring and protection until the testing has been completed.

APPLICABLE
SAFETY
ANALYSES, LCO,
and APPLICABILITY

The RTS ~~functions~~Functions to maintain the SLs during all AOOs and mitigates the consequences of PAs in all MODES in which the Rod Control System is capable of rod withdrawal or one or more rods are not fully inserted.

Each of the analyzed accidents and transients can be detected by one or more RTS Functions. The accident analysis described in Reference 3 and 9 takes credit for most RTS ~~trip~~-Functions. RTS ~~trip~~ Functions not specifically credited in the accident analysis are qualitatively credited in the safety analysis and the NRC staff approved licensing basis for the unit. These RTS ~~trip~~ Functions may provide protection for conditions that do not require dynamic transient analysis to demonstrate Function performance. They may also serve as backups to RTS ~~trip~~ Functions that were credited in the accident analysis.

The LCO requires all instrumentation performing an RTS Function, listed in Table 3.3.1-1 in the accompanying LCO, to be OPERABLE. A channel is OPERABLE provided the "as-found" value, measured during surveillance testing, does not exceed its associated Allowable Value. ~~For digital functions and provided the "as-left" value is within the specified calibration tolerance at the completion of each CHANNEL CALIBRATION. For analog measurements,~~ Allowable Values are defined in terms pertinent to the five channel calibration settings. ~~For analog functions~~ 0%, 25%, 50%, 75% and 100%. ~~For binary measurements there is one~~ Allowable Values ~~are~~ defined in terms pertinent to the state change at the Nominal Trip Setpoint. A Nominal Trip Setpoint ~~may be~~ set more conservative than the Limiting Trip Setpoint as necessary in response Allowable Value to plant conditions. ~~account for channel uncertainties.~~ Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

The LCO generally requires OPERABILITY of three or two channels in each instrumentation Function, three trains of Manual Reactor Trip ~~in each logic Function~~Initiation, and three trains in each Automatic Trip Logic Function. Three OPERABLE instrumentation channels in a two-out-of-three configuration are required when one RTS channel is also used as a control system input. ~~The~~ When there are three or more OPERABLE channels, the SSA within the control system prevents the possibility of ~~the a~~ shared channel failing in such a manner that it creates a transient that requires RTS action. The input failure is considered a single failure in the RTS and RTS remains capable of providing its protective function with the remaining two ~~operable~~OPERABLE channels. The SSA ensures there is no potential for control system and protection system interaction that could simultaneously create a need for RTS trip and disable one RTS channel. When there are less than three OPERABLE channels, the SSA cannot prevent erroneous control system

operation due to an input failure. This is reflected in the LCO Completion Times for shared channels, when there are only three required channels.

The two-out-of-three configuration allows one channel to be tripped during maintenance or testing without causing a ~~reactor trip~~ Reactor Trip. Specific exceptions to the above general philosophy exist and are discussed below.

~~In all cases where the LCO states "Restore channel or train to OPERABLE status", this means restore the required number of channels or trains to OPERABLE status. Therefore, restoration of an alternate channel or train, other than the failed channel or train, is also acceptable~~ Due to redundant components within the PSMS, such as controllers, communication links and power supplies, an inoperable component may or may not result in an inoperable channel/train. Where an inoperable component results in an inoperable required channel/train, LCOs are entered. For inoperable components that do not result in inoperable channels/trains, LCOs are not entered.

Reactor Trip System Functions

The safety analyses and OPERABILITY requirements applicable to each RTS Function are discussed below:

1. Manual Reactor Trip iInitiation

The Manual Reactor Trip iInitiation ensures that the control room operator can initiate a ~~reactor trip~~ Reactor Trip at any time by using any ~~two-out-of-four~~ two-out-of-four hardwired reactor trip switches in the control room. A Manual Reactor Trip iInitiation accomplishes the same results as any one of the automatic trip Functions. It is used by the reactor operator to shut down the reactor whenever any parameter is rapidly trending toward its Nominal Trip Setpoint.

The LCO requires three Manual Reactor Trip ~~train~~ Functions to be OPERABLE. Each train is controlled by a manual reactor trip switch. Each train activates two ~~reactor trip breakers~~ Reactor Trip Breakers in its respective train. Three independent trains are required to be OPERABLE so that no single random failure will disable the Manual Reactor Trip iInitiation Function.

In MODE 1 or 2, ~~manual initiation~~ Manual Initiation of a ~~reactor trip~~ Reactor Trip must be OPERABLE. These are the MODES in which the shutdown rods and/or control rods are partially or fully withdrawn from the core. In MODE 3, 4, or 5, the ~~manual initiation~~ Manual Initiation Function must also be OPERABLE if one or more shutdown rods or control rods are withdrawn or the Rod Control System is capable of withdrawing the shutdown rods or the control rods. In this condition, inadvertent control rod withdrawal is possible. In MODE 3, 4, or 5, ~~manual initiation~~ Manual Initiation of a ~~reactor~~

~~trip~~ Reactor Trip does not have to be OPERABLE if the Rod Control System is not capable of withdrawing the shutdown rods or control rods and if all rods are fully inserted. If the rods cannot be withdrawn from the core, or all of the rods are inserted, there is no need to be able to trip the reactor. In MODE 6, neither the shutdown rods nor the control rods are permitted to be withdrawn and the CRDMs are disconnected from the control rods and shutdown rods. Therefore, the ~~manual initiation~~ Manual Initiation Function is not required.

2. High Power Range Neutron Flux

The NIS power range detectors are located external to the reactor vessel and measure neutrons leaking from the core. Four channels are required because each channel measures neutron flux in one quadrant of the core. Anomalies occurring in one core quadrant can be seen by the neutron flux detector in that quadrant and by the neutron detectors in the two adjacent quadrants, but may not be detected by the detector in the opposite quadrant. Therefore, to ensure event detection and accommodate a single failure, neutron flux detectors must be OPERABLE in all four quadrants.

The NIS power range detectors also provide input control inputs to the Rod Control System and the Steam Generator (SG) Water Level Control System. The interface from the safety channels in the PSMS to the PCMS is through the Signal ~~Selector~~ Selection Algorithm (SSA). ~~The~~ When there are three or more OPERABLE NIS power range channels, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, four ~~When there are less than three OPERABLE NIS power range channels are sufficient, an additional channel is not required.~~ Therefore, the actuation logic must be able to withstand SSA cannot prevent erroneous control system operation due to an input failure to the control system, which may then require the protection function actuation, and a single failure in the other channels providing the protection function actuation. This is reflected in the LCO Completion Times for shared NIS power range channels.

Note that this Function also provides a signal to prevent automatic and manual rod withdrawal prior to initiating a ~~reactor trip~~. Reactor Trip. Limiting further rod withdrawal may terminate the transient and eliminate the need to trip the reactor.

a. ~~high setpoint~~ High Setpoint

The High Power Range Neutron Flux (~~high setpoint~~ High Setpoint) trip Function ensures that protection is provided, from all power levels, against a positive reactivity excursion leading to DNB during power operations. These can be caused by rod withdrawal or reductions in RCS temperature.

The LCO requires all four of the High Power Range Neutron Flux (~~high setpoint~~High Setpoint) channels to be OPERABLE.

In MODE 1 or 2, when a positive reactivity excursion could occur, the High Power Range Neutron Flux (~~high setpoint~~High Setpoint) trip must be OPERABLE. This Function will terminate the reactivity excursion and shut down the reactor prior to reaching a power level that could damage the fuel. In MODE 3, 4, 5, or 6, the NIS power range detectors cannot detect neutron levels in this range. In these MODES, the High Power Range Neutron Flux (~~high setpoint~~High Setpoint) does not have to be OPERABLE because the reactor is shut down and reactivity excursions into the power range are extremely unlikely. Other RTS Functions and administrative controls provide protection against reactivity additions when in MODE 3, 4, 5, or 6.

b. ~~low setpoint~~Low Setpoint

The LCO requirement for the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) trip Function ensures that protection is provided against a positive reactivity excursion from low power or subcritical conditions.

The LCO requires all four of the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) channels to be OPERABLE.

In MODE 1, below the Power Range Neutron Flux (P-10 setpoint), and in MODE 2, the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) trip must be OPERABLE. This Function may be manually blocked by the operator when ~~two-out of four~~two-out-of-four power range channels are greater than approximately 10% RTP (P-10 setpoint). This Function is automatically unblocked when three out of four power range channels are below the P-10 setpoint. Above the P-10 setpoint, positive reactivity additions are mitigated by the High Power Range Neutron Flux (~~high setpoint~~High Setpoint) trip Function.

In MODE 3, 4, 5, or 6, the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) trip Function does not have to be OPERABLE because the reactor is shut down and the NIS power range detectors cannot detect neutron levels in this range. Other RTS ~~trip~~ Functions and administrative controls provide protection against positive reactivity additions or power excursions in MODE 3, 4, 5, or 6.

3. High Power Range Neutron Flux Rate

The High Power Range Neutron Flux Rate trips use the same channels as discussed for Function 2 above. Four channels are

required because each channel measures neutron flux in one quadrant of the core. Anomalies occurring in one core quadrant can be seen by the neutron flux detector in that quadrant and by the neutron detectors in the two adjacent quadrants, but not by the detector in the opposite quadrant. Therefore, to ensure event detection and accommodate a single failure, neutron flux detectors must be OPERABLE in all four quadrants.

a. Positive Rate

The High Power Range Neutron Flux Positive Rate trip Function ensures that protection is provided against rapid increases in neutron flux that are characteristic of an RCCA drive rod housing rupture and the accompanying ejection of the RCCA. This Function compliments the High Power Range Neutron Flux (~~high~~High and ~~low setpoint~~Low Setpoint) trip Functions to ensure that the criteria are met for a rod ejection from the power range.

The LCO requires all four of the High Power Range Neutron Flux Positive Rate channels to be OPERABLE.

In MODE 1 or 2, when there is a potential to add a large amount of positive reactivity from a rod ejection accident (REA), the High Power Range Neutron Flux Positive Rate trip must be OPERABLE. In MODE 3, 4, 5, or 6, the High Power Range Neutron Flux Positive Rate trip Function does not have to be OPERABLE because other RTS ~~trip~~ Functions and administrative controls will provide protection against positive reactivity additions. Also, since only the shutdown banks may be withdrawn in MODE 3, 4, or 5, the remaining complement of control bank worth ensures a sufficient degree of SDM in the event of an REA. In MODE 6, no rods are withdrawn and the SDM is increased during refueling operations. The reactor vessel head is also removed or the closure bolts are detensioned preventing any pressure buildup. In addition, the NIS power range detectors cannot detect neutron levels present in this ~~mode~~MODE.

This Function has a dynamic transfer function. The Time Constants for this Function are recorded and maintained in a document established by the Setpoint Control Program (SCP).

b. Negative Rate

The High Power Range Neutron Flux Negative Rate trip Function ensures that protection is provided for multiple rod drop accidents. At high power levels, a multiple rod drop accident could cause local flux peaking that would result in an unconservative local DNBR. DNBR is defined as the ratio of the

heat flux required to cause a DNB at a particular location in the core to the local heat flux. The DNBR is indicative of the margin to DNB. No credit is taken for the operation of this Function for those rod drop accidents in which the local DNBRs will be greater than the limit.

The LCO requires all four High Power Range Neutron Flux Negative Rate channels to be OPERABLE.

In MODE 1 or 2, when there is potential for a multiple rod drop accident to occur, the High Power Range Neutron Flux Rate trip must be OPERABLE. In MODE 3, 4, 5, or 6, the High Power Range Neutron Flux Negative Rate trip Function does not have to be OPERABLE because the core is not critical and DNB is not a concern. Also, since only the shutdown banks may be withdrawn in MODE 3, 4, or 5, the remaining complement of control bank worth ensures a sufficient degree of SDM in the event of an REA. In MODE 6, no rods are withdrawn and the required SDM is increased during refueling operations. In addition, the NIS power range detectors cannot detect neutron levels present in this MODE.

This Function has a dynamic transfer function. The Time Constants for this Function are recorded and maintained in a document established by the Setpoint Control Program (SCP).

4. High Intermediate Range Neutron Flux

The High Intermediate Range Neutron Flux trip Function ensures that protection is provided against an uncontrolled RCCA bank rod withdrawal accident from a subcritical condition during startup. This trip Function provides redundant protection to the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) trip Function. The NIS intermediate range detectors are located external to the reactor vessel and measure neutrons leaking from the core. The NIS intermediate range detectors do not provide any input to control systems. Note that this Function also provides a signal to prevent automatic and manual rod withdrawal prior to initiating a ~~reactor trip~~Reactor Trip. Limiting further rod withdrawal may terminate the transient and eliminate the need to trip the reactor.

The LCO requires two channels of High Intermediate Range Neutron Flux to be OPERABLE. Two OPERABLE channels are sufficient to ensure no single random failure will disable this trip Function.

Because this trip Function is important only during startup, there is generally no need to disable channels for testing while the Function is required to be OPERABLE. Therefore, a third channel is unnecessary.

In MODE 1 below the P-10 setpoint, and in MODE 2 above the P-6 setpoint, when there is a potential for an uncontrolled RCCA bank rod withdrawal accident during reactor startup, the Intermediate Range Neutron Flux trip must be OPERABLE. Above the P-10 setpoint, the High Power Range Neutron Flux (~~high setpoint~~High Setpoint) trip and the High Power Range Neutron Flux Positive Rate trip provide core protection for a rod withdrawal accident. In MODE 2 below the P-6 setpoint, the High Source Range Neutron Flux trip provides the core protection for reactivity accidents. In MODE 3, 4, or 5, the High Intermediate Range Neutron Flux trip does not have to be OPERABLE because the control rods must be fully inserted and only the shutdown rods may be withdrawn. The reactor cannot be started up in this condition. The core also has the required SDM to mitigate the consequences of a positive reactivity addition accident. In MODE 6, all rods are fully inserted and the core has a required increased SDM. Also, the NIS intermediate range detectors cannot detect neutron levels present in this MODE.

5. High Source Range Neutron Flux

The LCO requirement for the High Source Range Neutron Flux trip Function ensures that protection is provided against an uncontrolled RCCA bank rod withdrawal accident from a subcritical condition during startup. This trip Function provides redundant protection to the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) trip Function. In MODES 3, 4, and 5, administrative controls also prevent the uncontrolled withdrawal of rods. The NIS source range detectors are located external to the reactor vessel and measure neutrons leaking from the core. The NIS source range detectors do not provide any inputs to control systems. The source range trip is the only RTS automatic protection function required in MODES 3, 4, and 5 when rods are capable of withdrawal or one or more rods are not fully inserted. Therefore, the functional capability at the specified Nominal Trip Setpoint is assumed to be available.

The High Source Range Neutron Flux Function provides protection for control rod withdrawal from subcritical, boron dilution and control rod ejection events.

In MODE 2 when below the P-6 setpoint and in MODES 3, 4, and 5 when there is a potential for an uncontrolled RCCA bank rod withdrawal accident, the High Source Range Neutron Flux trip must be OPERABLE. Two OPERABLE channels are sufficient to ensure no single random failure will disable this trip Function. Above the P-6 setpoint, the High Intermediate Range Neutron Flux trip and the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) trip will provide core protection for reactivity accidents. Above the P-6 setpoint, the High Source Range Neutron Flux trip may be manually bypassed which will also de-energize the NIS source range detectors.

Above the P-10 setpoint, the High Source Range Neutron Flux trip is automatically bypassed and the NIS source range detectors are automatically de-energized.

In MODES 3, 4, and 5 with all rods fully inserted and the Rod Control System not capable of rod withdrawal, and in MODE 6, the outputs of the Function to RTS logic are not required OPERABLE.

6. Overtemperature ΔT

The Overtemperature ΔT trip Function is initiated based on setpoints derived for DNB protection or core exit conditions. This trip Function also limits the range over which the Overpower ΔT trip Function must provide protection. The inputs to the Overtemperature ΔT trip include all pressure, coolant temperature, axial power distribution, and reactor power as indicated by loop ΔT assuming full reactor coolant flow. Protection from violating the DNBR limit or core exit boiling is assured for those transients that are slow with respect to delays from the core to the measurement system. The Function monitors both variation in power and flow since a decrease in flow has the same effect on ΔT as a power increase. The ~~reactor trip~~ Reactor Trip occurs if ~~indicated~~ measured loop ΔT exceeds the lower setpoint of the DNB protection limit setpoint and the core exit boiling limit setpoint. The Overtemperature ΔT trip Function uses each loop's ΔT as a measure of reactor power and is compared with a setpoint that is automatically varied with the following parameters:

- reactor coolant average temperature - the Nominal Trip Setpoint is varied to correct for changes in coolant density and specific heat capacity with changes in coolant temperature,
- ~~pressurizer pressure~~ Pressurizer Pressure - the Nominal Trip Setpoint is varied to correct for changes in system pressure, and
- axial power distribution - $f(\Delta I)$, the Nominal Trip Setpoint is varied to account for imbalances in the axial power distribution as detected by the NIS upper and lower power range detectors. If axial peaks are greater than the design limit, as indicated by the difference between the upper and lower NIS power range detectors, the Nominal Trip Setpoint is reduced in accordance with ~~Note FSAR Section 7.2.1-of Table 3.4.3.1-1~~ (Ref. 2).

Dynamic compensation is included for system piping delays from the core to the temperature measurement system.

The Overtemperature ΔT trip Function is calculated for each loop as described in ~~Note FSAR Section 7.2.1-of Table 3.4.3.1-1~~ (Ref. 2). Trip occurs if Overtemperature ΔT is indicated in two loops. The pressure and temperature signals are used for other control functions. The interface from the safety channels in the PSMS to the PCMS is

through the SSA. ~~The~~ When three or more temperature and pressure channels are OPERABLE, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore the protection function requires only two additional channels to provide the protection function actuation (i.e., ~~three~~ three channels total). When there are less than three OPERABLE temperature and pressure channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for temperature and pressure channels, since there are only three required channels.

Note that this Function also provides a signal to generate a turbine runback prior to reaching the Nominal Trip Setpoint. A turbine runback will reduce turbine power and reactor power. A reduction in power will normally alleviate the Overtemperature ΔT condition and may prevent a ~~reactor trip~~ Reactor Trip.

The LCO requires three channels of the Overtemperature ΔT trip Function to be OPERABLE. Note that the Overtemperature ΔT Function receives input from channels shared with other RTS Functions. Failures that affect multiple Functions require entry into the Conditions applicable to all affected Functions.

In MODE 1 or 2, the Overtemperature ΔT trip must be OPERABLE to prevent DNB. In MODE 3, 4, 5, or 6, this trip Function does not have to be OPERABLE because the reactor is not operating and there is insufficient heat production to be concerned about DNB.

The cycle dependent variables for this Function are specified in the COLR.

7. Overpower ΔT

The Overpower ΔT trip Function ensures that protection is provided to ensure the integrity of the fuel (i.e., no fuel pellet melting and less than 1% cladding strain) under all possible overpower conditions. This trip Function also limits the required range of the Overtemperature ΔT trip Function and provides a backup to the High Power Range Neutron Flux (~~high setpoint~~ High Setpoint) trip. The Overpower ΔT trip Function ensures that the allowable heat generation rate (kW/ft) of the fuel is not exceeded. It uses the ΔT of each loop as a measure of reactor power with a setpoint that is automatically varied with the following parameters:

- reactor coolant average temperature - the Nominal Trip Setpoint is varied to correct for changes in coolant density and specific heat capacity with changes in coolant temperature, and

- rate of change of reactor coolant average temperature - including dynamic compensation for the delays between the core and the temperature measurement system.

The Overpower ΔT trip Function is calculated for each loop as per ~~Note FSAR Section 7.2 of Table 1.4.3.3.1-1.2 (Ref. 2)~~. Trip occurs if Overpower ΔT is indicated in two loops. The temperature signals are also used for other control functions. The interface from the safety channels in the PSMS to the PCMS is through the SSA. ~~The~~ When three or more temperature channels are OPERABLE, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). When there are less than three OPERABLE temperature channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for temperature channels, since there are only three required channels.

Note that this Function also provides a signal to generate a turbine runback prior to reaching the Allowable Value. A turbine runback will reduce turbine power and reactor power. A reduction in power will normally alleviate the Overpower ΔT condition and may prevent a ~~reactor trip~~ Reactor Trip.

The LCO requires three channels of the Overpower ΔT trip Function to be OPERABLE. Note that the Overpower ΔT trip Function receives input from channels shared with other RTS Functions. Failures that affect multiple Functions require entry into the Conditions applicable to all affected Functions.

In MODE 1 or 2, the Overpower ΔT trip Function must be OPERABLE. These are the only times that enough heat is generated in the fuel to be concerned about the heat generation rates and overheating of the fuel. In MODE 3, 4, 5, or 6, this trip Function does not have to be OPERABLE because the reactor is not operating and there is insufficient heat production to be concerned about fuel overheating and fuel damage.

The cycle dependent variables for this Function are specified in the COLR.

8. Pressurizer Pressure

The same sensors provide ~~input~~ inputs to the High and Low Pressurizer Pressure trips and the Overtemperature ΔT trip. The Pressurizer Pressure channels are also used to provide ~~input-control~~ inputs to the Pressurizer Pressure Control System. The interface from the safety channels in the PSMS to the PCMS is through the

SSA. ~~The~~ When three or more Pressurizer Pressure channels are OPERABLE, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). When there are less than three OPERABLE pressure channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times Pressurizer Pressure channels, since there are only three required channels.

a. Low Pressurizer Pressure

The Low Pressurizer Pressure trip Function ensures that protection is provided against violating the DNBR limit due to low pressure.

The LCO requires three channels of Low Pressurizer Pressure to be OPERABLE.

In MODE 1, when DNB is a major concern, the Low Pressurizer Pressure trip must be OPERABLE. This trip Function is automatically enabled on increasing power by the P-7 interlock (NIS power range P-10 or ~~turbine inlet pressure~~ Turbine Inlet Pressure greater than approximately 10% of full power equivalent (P-13)). On decreasing power, this trip Function is automatically blocked below P-7. Below the P-7 setpoint, no conceivable power distributions can occur that would cause DNB concerns.

This Function has a dynamic transfer function. The Time Constants for this Function are recorded and maintained in a document established by the Setpoint Control Program (SCP).

b. High Pressurizer Pressure

The High Pressurizer Pressure trip Function ensures that protection is provided against ~~overover~~ pressurizing the RCS. This trip Function operates in conjunction with the pressurizer relief and safety valves to prevent RCS overpressure conditions.

The LCO requires three channels of the High Pressurizer Pressure to be OPERABLE.

The High Pressurizer Pressure LSSS is selected to be below the pressurizer safety valve actuation pressure setting. This setting minimizes challenges to safety valves.

In MODE 1 or 2, the High Pressurizer Pressure trip must be OPERABLE to help prevent RCS overpressurization and minimize challenges to the safety valves. In MODE 3, 4, 5, or 6, the High Pressurizer Pressure trip Function does not have to be OPERABLE because transients that could cause an overpressure condition will be slow to occur. Therefore, the operator will have sufficient time to evaluate unit conditions and take corrective actions. Additionally, low temperature overpressure protection systems provide overpressure protection when below MODE 4.

9. High Pressurizer Water Level

The High Pressurizer Water Level trip Function provides a backup signal for the High Pressurizer Pressure trip and also provides protection against water relief through the pressurizer safety valves. These valves are designed to pass steam in order to achieve their design energy removal rate. A ~~reactor trip~~ Reactor Trip is actuated prior to the pressurizer becoming water solid. The LCO requires three channels of High Pressurizer Water Level to be OPERABLE. The pressurizer level channels are used as input to the Pressurizer Level Control System. The interface from the safety channels in the PSMS to the PCMS is through the SSA. ~~The~~ When three or more High Pressurizer Water Level channels are OPERABLE, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). When there are less than three OPERABLE High Pressurizer Water Level channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for High Pressurizer Water Level channels, since there are only three required channels

In MODE 1, when there is a potential for overfilling the pressurizer, the High Pressurizer Water Level trip must be OPERABLE. This trip Function is automatically enabled on increasing power by the P-7 interlock. On decreasing power, this trip Function is automatically blocked below P-7. Below the P-7 setpoint, transients that could raise the ~~pressurizer water level~~ Pressurizer Water Level will be slow and the operator will have sufficient time to evaluate unit conditions and take corrective actions.

10. Low Reactor Coolant Flow

The Low Reactor Coolant Flow trip Function ensures that protection is provided against violating the DNBR limit due to low flow in one or more RCS loops, while avoiding ~~reactor trip~~ Reactor Trips due to normal variations in loop flow. Above the P-7 setpoint, the ~~reactor trip~~ Reactor Trip on low flow in any one RCS loop is automatically

enabled. Each RCS loop has four flow detectors to monitor flow. The flow signals are not used for any control system input.

The LCO requires three Low Reactor Coolant Flow channels per loop to be OPERABLE in MODE 1 above P-7.

In MODE 1 above the P-7 setpoint, a loss of flow in one RCS loop could result in DNB conditions in the core. Below the P-7 setpoint, all ~~reactor-trip~~ Reactor Trips on low flow are automatically blocked since there is insufficient heat production to generate DNB conditions.

11. Low Reactor Coolant Pump (RCP) Speed

The Low RCP Speed trip Function ensures that protection is provided against violating the DNBR limit due to a loss of flow in two or more RCS loops. The speed of each RCP is monitored. Above the P-7 setpoint a low speed detected on two or more RCPs will initiate a ~~reactor-trip~~ Reactor Trip. The Nominal Trip Setpoint reflects only steady state instrument uncertainties as the detectors do not provide primary protection for any event that results in a harsh environment.

The LCO requires three Low RCP Speed channels (one channel per loop) to be OPERABLE in MODE 1 above P-7. One channel per loop is sufficient for this trip Function because the Low RCS Flow trip alone provides sufficient protection of unit SLs for loss of flow events. The Low RCP Speed trip serves only to anticipate the low flow trip, minimizing the thermal transient associated with loss of a pump. Below the P-7 setpoint, all ~~reactor-trip~~ Reactor Trips on loss of flow are automatically blocked since no power distributions are expected to occur that would cause a DNB concern at this low power level. Above the P-7 setpoint, the ~~reactor-trip~~ Reactor Trip on loss of flow in two or more loops is automatically enabled.

12. Steam Generator Water Level

The same sensors provide ~~input~~ inputs to the Low SG Water Level trip and the High-High SG Water Level trip. Additionally, the level transmitters provide ~~input-control~~ inputs to the SG Level Control System. The interface from the safety channels in the PSMS to the PCMS is through the SSA. ~~The~~ When three or more High-High SG Water Level channels are OPERABLE for each Steam Generator, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). When there are less than three OPERABLE High-High SG Water Level channels for each Steam Generator, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO

Completion Times for High-High SG Water Level channels, since there are only three required channels for each Steam Generator.

a. Low SG Water Level

The Low SG Water Level trip Function ensures that protection is provided against a loss of heat sink and actuates the Emergency Feedwater (EFW) System prior to uncovering the SG tubes. The SGs are the heat sink for the reactor. In order to act as a heat sink, the SGs must contain a minimum amount of water. A narrow range low level in any SG is indicative of a loss of heat sink for the reactor. This Function also performs the ESFAS function of starting the EFW pumps on low SG level.

The LCO requires three channels of Low SG Water Level per SG to be OPERABLE.

In MODE 1 or 2, when the reactor requires a heat sink, the Low SG Water Level trip must be OPERABLE. The normal source of water for the SGs is the Main Feedwater (MFW) System (not safety related). The MFW System is only in operation in MODE 1 or 2. The EFW System is the safety related backup source of water to ensure that the SGs remain the heat sink for the reactor. During normal startups and shutdowns, the EFW System provides feedwater to maintain SG level. In MODE 3, 4, 5, or 6, the Low SG Water Level Function does not have to be OPERABLE because the MFW System is not in operation and the reactor is not operating or even critical. Decay heat removal is accomplished by the EFW System in MODE 3 and by the Residual Heat Removal (RHR) System in MODE 4, 5, or 6.

b. High-High SG Water Level

The High-High SG Water Level trip Function ensures that protection is provided against an excessive cooldown due to increase in feedwater flow. An increase in the feedwater flow rate will cause an increase in SG ~~water level~~Water Level and reduction in the reactor coolant temperature. Reduction in the coolant temperature adds reactivity as a result of the positive moderator density coefficient, thereby increasing the reactor power.

This Function also performs the ESFAS functions of generating a ~~turbine trip~~Turbine Trip and initiating ~~main feedwater isolation~~Main Feedwater Isolation.

The LCO requires three channels of the High-High SG Water Level trip Function to be OPERABLE in MODE 1 above P-7. The trip Function is automatically enabled on increasing power by the P-7 interlock and automatically blocked on decreasing power

once the P-7 interlock is cleared. Although the High-High SG Water Level trip is blocked below the P-7 setpoint, the ESFAS functions to trip the turbine and isolate Main Feedwater are OPERABLE above and below the P-7 setpoint. These ESFAS functions allow the operator sufficient time to evaluate plant conditions and take corrective actions.

13. Turbine Trip

a. Turbine Emergency Trip Oil Pressure

The Turbine Emergency Trip Oil Pressure trip Function anticipates the loss of heat removal capabilities of the secondary system following a ~~turbine trip~~ Turbine Trip. This trip Function acts to minimize the pressure/temperature transient on the reactor. Any ~~turbine trip~~ Turbine Trip from a power level below the P-7 setpoint, approximately 10% power, will not actuate a ~~reactor trip~~ Reactor Trip. Four pressure switches monitor the control oil pressure in the Turbine Electrohydraulic Control System. A low pressure condition sensed by two-out-of-four pressure switches will actuate a ~~reactor trip~~ Reactor Trip. These pressure switches do not provide any input to the control system. The unit is designed to withstand a complete loss of load and not sustain core damage or challenge the RCS pressure limitations. Core protection is provided by the High Pressurizer Pressure trip Function and RCS integrity is ensured by the pressurizer safety valves.

The LCO requires three channels of Turbine Emergency Trip Oil Pressure to be OPERABLE in MODE 1 above P-7.

Below the P-7 setpoint, a ~~turbine trip~~ Turbine Trip does not actuate a ~~reactor trip~~ Reactor Trip. In MODE 2, 3, 4, 5, or 6, there is no potential for a ~~turbine trip~~ Turbine Trip, and the Turbine Emergency Trip Oil Pressure trip Function does not need to be OPERABLE.

b. Turbine Trip - Main Turbine Stop Valve Position

The Main Turbine Stop Valve Position trip Function anticipates the loss of heat removal capabilities of the secondary system following a ~~turbine trip~~ Turbine Trip from a power level Above the P-7 setpoint. This action will actuate a ~~reactor trip~~ Reactor Trip. The trip Function anticipates the loss of secondary heat removal capability that occurs when the stop valves close. Tripping the reactor in anticipation of loss of secondary heat removal acts to minimize the pressure and temperature transient on the reactor. This trip Function will normally operate in the presence of a single failure due to redundant limit switches on each valve.

However this trip Function is not required to operate in the presence of a single channel failure. The unit is designed to withstand a complete loss of load and not sustain core damage or challenge the RCS pressure limitations. Core protection is provided by the High Pressurizer Pressure trip Function, and RCS integrity is ensured by the pressurizer safety valves. This trip Function is diverse to the Turbine Emergency Trip Oil Pressure ~~turbine-trip~~ Turbine Trip Function. Each main turbine stop valve is equipped with two limit switches that input to the RTS. If the limit switches indicate that all four stop valves are closed, a ~~reactor-trip~~ Reactor Trip is initiated.

The LSSS for this Function is set to assure channel trip occurs when the associated stop valve is completely closed.

The LCO requires four Main Turbine Stop Valve Position channels, one per valve, to be OPERABLE in MODE 1 above P-7. One channel on each valve must trip to cause ~~reactor~~ trip Reactor Trip.

Below the P-7 setpoint, a load rejection can be accommodated by the Turbine Bypass System. In MODE 2, 3, 4, 5, or 6, there is no potential for a load rejection, and the Turbine Trip - Main Turbine Stop Valve Position trip Function does not need to be OPERABLE.

14. ~~ECCS actuation~~ Actuation

The ECCS ~~actuation reactor-trip~~ Actuation Reactor Trip function ensures that if a ~~reactor-trip~~ Reactor Trip has not already been generated by the RTS, the ESFAS ~~automatic-actuation logic~~ Automatic Actuation Logic will initiate a ~~reactor-trip~~ Reactor Trip upon any signal that initiates ECCS ~~a~~ Actuation. This is a condition of acceptability for the loss of coolant accident (LOCA). However, other transients and accidents take credit for varying levels of ESF performance and rely upon rod insertion, except for the most reactive rod that is assumed to be fully withdrawn, to ensure reactor shutdown. Therefore, a ~~reactor-trip~~ Reactor Trip is initiated every time an ~~S~~ ECCS Actuation signal is present.

Nominal Trip Setpoint and Allowable Values are not applicable to this Function. The ECCS ~~a~~ Actuation signals are provided within the RPS. Therefore, there is no measurement signal with which to associate an LSSS.

The LCO requires three trains of ECCS ~~a~~ Actuation to be OPERABLE in MODE 1 or 2.

~~A reactor-trip~~ A Reactor Trip is initiated every time an ECCS ~~a~~ Actuation signal is present. Therefore, this trip Function must be

OPERABLE in MODE 1 or 2, when the reactor is critical, and must be shut down in the event of an accident. In MODE 3, 4, 5, or 6, the reactor is not critical, and this trip Function does not need to be OPERABLE.

15. Reactor Trip System Interlocks

Reactor protection interlocks are provided to ensure ~~reactor trip~~ Reactor Trip are in the correct configuration for the current unit status. They back up operator actions to ensure protection system Functions are not bypassed during unit conditions under which the safety analysis assumes the Functions are not bypassed. Therefore, the interlock Functions do not need to be OPERABLE when the associated ~~reactor trip~~ Reactor Trip functions are outside the applicable MODES. These are:

a. Intermediate Range Neutron Flux, P-6

The Intermediate Range Neutron Flux, P-6 interlock is actuated when any NIS intermediate range channel goes approximately one decade above the minimum channel reading. If both channels drop below the setpoint, the permissive will automatically be defeated. The LCO requirement for the P-6 interlock ensures that the following Functions are performed:

- on increasing power, the P-6 interlock allows the manual block of the NIS Source Range, Neutron Flux ~~reactor trip~~ Reactor Trip. This prevents a premature block of the source range trip and allows the operator to ensure that the intermediate range is OPERABLE prior to leaving the source range. When the source range trip is blocked, the high voltage to the detectors is also removed,
- on decreasing power, the P-6 interlock automatically energizes the NIS source range detectors and enables the NIS Source Range Neutron Flux ~~reactor trip~~ Reactor Trip, and
- on increasing power, the P-6 interlock provides a backup block signal to the source range flux doubling circuit. Normally, this Function is manually blocked by the control room operator during the reactor startup.

The LCO requires two channels of Intermediate Range Neutron Flux, P-6 interlock to be OPERABLE in MODE 2 when below the P-6 interlock setpoint.

Above the P-6 interlock setpoint, the NIS Source Range Neutron Flux ~~reactor trip~~ Reactor Trip will be blocked, and this Function will no longer be necessary.

In MODE 3, 4, 5, or 6, the P-6 interlock does not have to be OPERABLE because the NIS Source Range is providing core protection.

b. Low Power Reactor Trips Block, P-7

The Low Power Reactor Trips Block, P-7 interlock is actuated by input from either the Power Range Neutron Flux, P-10, or the Turbine Inlet Pressure, P-13 interlock. The LCO requirement for the P-7 interlock ensures that the following Functions are performed:

(1) on increasing power, the P-7 interlock automatically enables ~~reactor trip~~ Reactor Trips on the following Functions:

- Low Pressurizer Pressure,
- High Pressurizer Water Level,
- Low Reactor Coolant Flow,
- Low RCP Speed,
- High Steam Generator (SG) Water Level,
- Turbine Trip - Turbine Emergency Trip Oil Pressure, and
- Turbine Trip - Main Turbine Stop Valve Position.

These ~~reactor trip~~ Reactor Trips are only required when operating above the P-7 setpoint (approximately 10% power). The ~~reactor trip~~ Reactor Trips provide protection against violating the DNBR limit. Below the P-7 setpoint, the RCS is capable of providing sufficient natural circulation without any RCP running.

(2) on decreasing power, the P-7 interlock automatically blocks ~~reactor trip~~ Reactor Trips on the following Functions:

- Low Pressurizer Pressure,
- High Pressurizer Water Level,
- Low Reactor Coolant Flow,
- Low RCP Speed,
- High Steam Generator (SG) Water Level,

- Turbine Trip - Turbine Emergency Trip Oil Pressure, and
- Turbine Trip - Main Turbine Stop Valve Position.

Nominal Trip Setpoint and Allowable Value are not applicable to the P-7 interlock because it is a logic Function and thus has no parameter with which to associate an LSSS.

The P-7 interlock is a logic Function with train and not channel identity. Therefore, the LCO requires the Low Power Reactor Trips Block, P-7 interlock to be OPERABLE in each OPERABLE RTS train in MODE 1.

The low power trips are blocked below the P-7 setpoint and unblocked above the P-7 setpoint. In MODE 2, 3, 4, 5, or 6, this Function does not have to be OPERABLE because the interlock performs its Function when power level drops below 10% power, which is in MODE 1.

c. Power Range Neutron Flux, P-10

The Power Range Neutron Flux, P-10 interlock is actuated at approximately 10% power, as determined by two-out-of-four NIS power range detectors. If power level falls below 10% RTP on 3 of 4 channels, the nuclear instrument trips will be automatically unblocked. The LCO requirement for the P-10 interlock ensures that the following Functions are performed:

- on increasing power, the P-10 interlock allows the operator to manually block the Intermediate Range Neutron Flux ~~reactor trip~~ Reactor Trip. Note that blocking the ~~reactor trip~~ Reactor Trip also blocks the signal to prevent automatic and manual rod withdrawal,
- on increasing power, the P-10 interlock allows the operator to manually block the High Power Range Neutron Flux (~~low setpoint~~) ~~reactor trip~~ Low Setpoint Reactor Trip,
- on increasing power, the P-10 interlock automatically provides a backup signal to block the Source Range Neutron Flux ~~reactor trip~~ Reactor Trip, and also to de-energize the NIS source range detectors,
- the P-10 interlock provides one of the two inputs to the P-7 interlock, and
- on decreasing power, the P-10 interlock automatically enables the High Power Range Neutron Flux (~~low setpoint~~)

~~reactor trip~~Low Setpoint) Reactor Trip and the Intermediate Range Neutron Flux ~~reactor trip~~Reactor Trip (and rod stop).

The LCO requires four channels of Power Range Neutron Flux, P-10 interlock to be OPERABLE in MODE 1 or 2.

OPERABILITY in MODE 1 ensures the Function is available to perform its decreasing power Functions in the event of a reactor shutdown. This Function must be OPERABLE in MODE 2 to ensure that core protection is provided during a startup or shutdown by the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) and High Intermediate Range Neutron Flux ~~reactor trips~~Reactor Trips. In MODE 3, 4, 5, or 6, this Function does not have to be OPERABLE because the reactor is not at power and the Source Range Neutron Flux ~~reactor trip~~Reactor Trip provides core protection.

d. Turbine Inlet Pressure, P-13

The Turbine Inlet Pressure, P-13 interlock is actuated when the pressure in the first stage of the high pressure turbine is greater than approximately 10% of the ~~turbine rated full~~ power ~~pressure~~. This is determined by two-out-of-four pressure detectors. The LCO requirement for this Function ensures that three of the inputs to the P-7 interlock are available.

The LCO requires three channels of Turbine Inlet Pressure, P-13 interlock to be OPERABLE in MODE 1.

The Turbine Inlet Chamber Pressure, P-13 interlock must be OPERABLE when the turbine generator is operating. The interlock Function is not required OPERABLE in MODE 2, 3, 4, 5, or 6 because the turbine generator is not operating.

16. Reactor Trip Breakers

This trip Function applies to the RTBs exclusive of individual trip mechanisms. The LCO requires three OPERABLE trains of trip breakers. A trip breaker train consists of all trip breakers associated with a single RTS logic train that are racked in, closed, and capable of supplying power to the Rod Control System. Thus, the train consists of two main breakers. Three OPERABLE trains ensure no single random failure can disable the RTS trip capability.

These trip Functions must be OPERABLE in MODE 1 or 2 when the reactor is critical. In MODE 3, 4, or 5, these RTS ~~trip~~ Functions must be OPERABLE when the Rod Control System is capable of rod withdrawal or one or more rods are not fully inserted.

17. Reactor Trip Breaker Undervoltage and Shunt Trip Mechanisms

The LCO requires both the Undervoltage and Shunt Trip Mechanisms to be OPERABLE for each RTB that is in service. The trip mechanisms are not required to be OPERABLE for trip breakers that are open, racked out, incapable of supplying power to the Rod Control System, or declared inoperable under Function 19 above. OPERABILITY of both trip mechanisms on each breaker ensures that no single trip mechanism failure will prevent opening any breaker on a valid signal.

These trip Functions must be OPERABLE in MODE 1 or 2 when the reactor is critical. In MODE 3, 4, or 5, these RTS ~~trip~~ Functions must be OPERABLE when the Rod Control System is capable of rod withdrawal or one or more rods are not fully inserted.

18. Automatic Trip Logic

The LCO requirement for the RTBs (Functions 16 and 17) and Automatic Trip Logic (Function 18) ensures that means are provided to interrupt the power to allow the rods to fall into the reactor core. Each RTB is equipped with an undervoltage coil and a shunt trip coil to trip the breaker open when needed. The ~~reactor trip~~ Reactor Trip signals generated by the RTS Automatic Trip Logic cause the RTBs to open and shut down the reactor.

The LCO requires three trains of RTS Automatic Trip Logic to be OPERABLE. Having three OPERABLE trains ensures that random failure of a single logic train will not prevent ~~reactor trip~~ Reactor Trip.

These trip Functions must be OPERABLE in MODE 1 or 2 when the reactor is critical. In MODE 3, 4, or 5, these RTS ~~trip~~ Functions must be OPERABLE when the Rod Control System is capable of rod withdrawal or one or more rods are not fully inserted.

The RTS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii) (Ref. 8).

BASES

ACTIONS

A Note has been added to the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function listed in Table 3.3.1-1.

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

When the number of inoperable channels in a trip Function exceeds those specified in one or other related Conditions associated with a trip Function, then the unit is outside the safety analysis. Therefore, LCO 3.0.3 must be immediately entered if applicable in the current MODE of operation.

In all cases where the LCO states “Restore channel or train to OPERABLE status”, this means restore the required number of channels or trains to OPERABLE status. Therefore, restoration of an alternate channel or train, other than the failed channel or train, is also acceptable.

A.1

Condition A applies to all RTS protection Functions.

Condition A addresses the situation where one or more required channels or trains for one or more Functions are inoperable at the same time. The Required Action is to refer to Table 3.3.1-1 and to take the Required Actions for the protection functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

B.1 and B.2

Condition B applies to the Manual Reactor Trip in MODE 1 or 2. This action addresses the train orientation for this Function. With one required train inoperable, the inoperable train must be restored to OPERABLE status within 72 hours. In this Condition, the remaining two OPERABLE trains are adequate to perform the safety function.

~~The Completion Time of 72 hours is reasonable considering that there are three automatic actuation trains and two other Manual Reactor Trip trains OPERABLE, and the low probability of an event occurring during this interval. The completion time also considers that the manual reactor trip function, for the inoperable Manual Reactor Trip train, can also be actuated from the Safety VDU for that train. Therefore, the ability to initiate a manual reactor trip through safety related equipment remains functional in all three required trains.~~

If the Manual Reactor Trip Function cannot be restored to OPERABLE status within the allowed 72 hour Completion Time, the unit must be brought to a MODE in which the requirement does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 6 additional hours (78 hours total time). The 6 additional hours to reach MODE 3 is reasonable, based on operating experience, to reach MODE 3 from full power operation in an orderly manner and without challenging unit systems.

With the unit in MODE 3, ACTION C would apply to any inoperable Manual Reactor Trip Function if the Rod Control System is capable of rod withdrawal or one or more rods are not fully inserted.

The ~~initial completion time~~ Completion Time of 72 hours is justified ~~in because two trains are adequate to perform the PSMS reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6A.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19. The manual reactor trips safety function remains fully operable from the Safety VDUs, even when one, and there are three automatic actuation trains and two other Manual Reactor Trip channel is~~ trains OPERABLE. In addition, the Completion Time considers that the Mmanual Reactor Trip Ffunction, for the inoperable Manual Reactor Trip trainFunction, can be actuated from the Safety VDU for that train. Therefore, the ability to initiate a manual Reactor Trip through safety related equipment remains functional in all three trains.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

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

Condition C applies to the Manual ~~reactor trip~~ Reactor Trip Function in MODE 3, 4, or 5 with the Rod Control System capable of rod withdrawal or one or more rods not fully inserted.

● ~~Manual Reactor Trip~~

This action addresses the train orientation for ~~one~~ this Function. With one required train inoperable, the inoperable train must be restored to OPERABLE status within 72 hours. If the affected Function cannot be restored to OPERABLE status within the allowed 72 hour Completion Time, the unit must be placed in a MODE in which the requirement does not apply. To achieve this status, action must be initiated within the same 72 hours to ensure that all rods are fully inserted, and the Rod Control System must be placed in a condition incapable of rod withdrawal within the next hour. The additional hour provides sufficient time to accomplish the action in an orderly manner. With rods fully inserted and the Rod Control System incapable of rod withdrawal, this Function is no longer required.

The Completion Time of ~~72 hours is reasonable considering that 72 hours is justified because two trains are adequate to perform the safety function, and there are three automatic actuation trains and two other Manual Reactor Trip trainFunctions OPERABLE, and the low probability of an event occurring during this interval. The completion time also.~~ In addition, the Completion Time considers that the Mmanual reactor trip-Reactor Trip Ffunction, for the inoperable Manual Reactor Trip train, can also be

actuated from the Safety VDU for that train. Therefore, the ability to initiate a manual ~~reactor trip~~ Reactor Trip through safety related equipment remains functional in all three ~~required~~ trains.

~~The initial completion time~~ The Completion Time of 72 hours is also justified in the PSMS-US-APWR reliability analysis. ~~For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6A.12. The and risk analyses, the summary and result of the PSMS reliability analysis is evaluated and confirmed which are documented in the US-APWR PRA FSAR Chapter 19. The manual reactor trip function remains fully operable from the Safety VDUs, even when one Manual Reactor Trip channel is inoperable (Ref. 10).~~

D.1, D.2.1, and D.2.2

Condition D applies to the following ~~reactor trip~~ Reactor Trip Functions in MODE 3, 4, or 5 with the Rod Control System capable of rod withdrawal or one or more rods not fully inserted:

- RTBs,
- RTB Undervoltage and Shunt Trip Mechanisms, and
- Automatic Trip Logic.

This action addresses the train orientation for these Functions. With one required train inoperable, the inoperable train must be restored to OPERABLE status within 48 hours. If the affected Function(s) cannot be restored to OPERABLE status within the allowed 48 hour Completion Time, the unit must be placed in a MODE in which the requirement does not apply. To achieve this status, action must be initiated within the same 48 hours to ensure that all rods are fully inserted, and the Rod Control System must be placed in a condition incapable of rod withdrawal within the next hour. The additional hour provides sufficient time to accomplish the action in an orderly manner. With rods fully inserted and the Rod Control System incapable of rod withdrawal, these Functions are no longer required.

The Completion Time of 48 hours is ~~reasonable considering that in this Condition, justified because~~ the two remaining OPERABLE trains are adequate to perform the safety function, ~~and given~~. In addition, the ~~low probability of an event occurring during this interval. The~~ Completion Time ~~also~~ considers that the two remaining OPERABLE trains each have continuous automatic self-testing ~~and redundant RTBs for the Automatic Trip Logic~~.

The Completion Time of 48 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

E.1.1, E.1.2, E.2.1, E.2.2, and E.3

Condition E applies to the Power Range Neutron Flux (~~high setpoint~~High Setpoint) Function.

~~The NIS power range detectors provide input to the Rod Control System and the SG Water Level Control System and, therefore, have a two-out-of-four trip logic. A known~~

With one channel inoperable, the inoperable channel must be placed in the ~~tripped trip~~ condition within 72 hours. This results in a partial trip condition requiring only one-out-of-three logic for actuation. ~~of the two-out-of-four trips.~~

The ~~72-Completion Time of 72 hours~~ allowed to place the inoperable channel in the tripped condition is justified because the three remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the three remaining OPERABLE channels have continuous automatic self-testing (as described for COT), and continuous automatic CHANNEL CHECKS. In addition, with the remaining three OPERABLE channels, the SSA within the PCMS ensures the control systems can withstand an input failure to the control system without causing erroneous control system operation, which would otherwise require the protection function actuation.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

In addition to placing the inoperable channel in the ~~tripped trip~~ condition, THERMAL POWER must be reduced to $\leq 75\%$ RTP within 78 hours. Reducing the power level prevents operation of the core with radial power distributions beyond the design limits. With one of the NIS power range detectors inoperable, 1/4 of the radial power distribution monitoring capability is lost.

As an alternative to the above ~~actions~~Required Actions, the inoperable channel can be placed in the ~~tripped trip~~ condition within 72 hours and the QPTR monitored once every 12 hours as per SR 3.2.4.2, QPTR verification. Calculating QPTR every 12 hours compensates for the lost monitoring capability due to the inoperable NIS power range channel and allows continued unit operation at power levels $< 75\%$ RTP. The 12 hour Surveillance Frequency is consistent with LCO 3.2.4, "QUADRANT POWER TILT RATIO (QPTR)."

As an alternative to the above Required Actions, the plant must be placed in a MODE where this Function is no longer required OPERABLE. Seventy-eight hours are allowed to place the plant in MODE 3. The 78 hour Completion Time includes 72 hours for channel corrective maintenance, and an additional 6 hours for the MODE reduction as

required by Required Action E.3. This is a reasonable time, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems. If Required Actions cannot be completed within their allowed Completion Times, LCO 3.0.3 must be entered.

~~One~~ The Required Actions are modified by a Note that allows placing one channel ~~may be bypassed~~ in bypass for up to ~~12~~ 12 hours ~~for while performing surveillance testing and~~, or setpoint adjustments when a setpoint adjustment. The 12 hours bypass limit is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to the US-APWR reduction is required by other Technical Report MUAP-07030 PRA, Attachment 6A.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19. Specifications, provided the other channels are OPERABLE, or two channels are OPERABLE and one is placed in the trip condition. With one channel bypassed, the system can detect all anomalies, but it cannot also sustain a single failure.

The Bypass Time of 12 hours is justified because the remaining OPERABLE channels are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

The Bypass Time of 12 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

~~The Required Actions have been modified by a Note that allows placing the inoperable channel in the bypass condition for up to 12 hours while performing routine surveillance testing of other channels. The Note also allows placing the inoperable channel in the bypass condition to allow setpoint adjustments of other channels when required to reduce the setpoint in accordance with other Technical Specifications. The 12 hour time limit is justified based on operating experience.~~

Required Action E.2.2 has been modified by a Note which only requires SR 3.2.4.2 to be performed if the Power Range Neutron Flux input to QPTR becomes inoperable. Failure of a component in the Power Range Neutron Flux Channel which renders the High Flux Trip Function inoperable may not affect the capability to monitor QPTR. As such, determining QPTR using the movable incore detectors once per 12 hours may not be necessary.

~~The initial completion time of 72 hours is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6A.12. The result of the~~

~~PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~

F.1 and F.2

Condition F applies to the following Reactor Trip~~reactor trip~~ Functions:

- High Power Range Neutron Flux (~~low setpoint~~Low Setpoint),
- ~~• Overtemperature ΔT ,~~
- ~~• Overpower ΔT ,~~
- High Power Range Neutron Flux Rate (Positive Rate~~), and~~
- High Power Range Neutron Flux Rate (Negative Rate~~),~~
- ~~• High Pressurizer Pressure, and~~
- ~~• Low SG Water Level~~

~~A known~~With one ~~required channel~~ inoperable, the inoperable channel must be placed in the tripped condition within 72 hours. Placing the channel in the tripped condition results in a partial trip condition requiring only one-out-of-two logic ~~(for the trip functions where the required number of operable channels is three) or one-out-of three logic (for the trip functions where the required number of operable channels is four)~~ for actuation of the two-out-of-N~~four~~ trips, ~~where N is three or four (depending on the required number of operable channels).~~

The Completion Time of 72 hours to place the inoperable channel in the tripped condition is justified because the three remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the three remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

In addition, with the remaining three OPERABLE channels, the SSA within the PCMS ensures the control systems can withstand an input failure to the control system without causing erroneous control system operation, which would otherwise require the protection function actuation.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).~~The 72 hours allowed to place the inoperable channel in the tripped condition is justified because the~~

~~remaining two operable channels (for the trip functions where the required number of operable channels is three) or the remaining three operable channels (for the trip functions where the required number of operable channels is four) have automatic self-testing (as described for COT, and automatic CHANNEL CHECKS.~~

If the inoperable channel cannot be placed in the trip condition within the specified Completion Time, the unit must be placed in a MODE where these Functions are not required OPERABLE. An additional 6 hours ~~is~~ are allowed to place the unit in MODE 3. Six hours is a reasonable time, based on operating experience, to place the unit in MODE 3 from full power in an orderly manner and without challenging unit systems.

~~The number of Required Channels for the High Power Range Neutron Flux Rate is four. Four channels are required because each channel measures neutron flux in one quadrant of the core. Anomalies occurring in one core quadrant can be seen by the neutron flux detector in that quadrant and by the neutron detectors in the two adjacent quadrants, but not by the detector in the opposite quadrant. So to ensure event detection and accommodate a single failure, neutron flux detectors must be operable in all four quadrants.~~

The Required Actions ~~have been~~ are modified by a Note, that allows placing ~~the inoperable one~~ channel in ~~the bypassed condition~~ bypass for up to 12 hours while performing ~~routine~~ surveillance testing, ~~of provided~~ the other channels ~~are OPERABLE, or two channels are OPERABLE and one is placed in the trip condition. With one channel bypassed, the system can detect all anomalies, but it cannot also sustain a single failure.~~

The Bypass Time of 12 hours is justified because the remaining OPERABLE channels are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

The Bypass Time of 12 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10). ~~The 12 hour time limit is based on operating experience.~~

~~The initial completion time of 72 hours is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6A.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~

~~One channel may be bypassed for up to 12 hours for surveillance testing and setpoint adjustment. The 12 hours bypass limit is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self testing. For detail information, refer to the~~

~~US-APWR Technical Report MUAP-07030 PRA, Attachment 6A.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~

G.1 and G.2

Condition G applies to the Intermediate Range Neutron Flux trip when THERMAL POWER is above the P-6 setpoint and below the P-10 setpoint, and one channel is inoperable. Above the P-6 setpoint and below the P-10 setpoint, the NIS intermediate range detector performs the monitoring Functions. If THERMAL POWER is greater than the P-6 setpoint but less than the P-10 setpoint, 24 hours is allowed to reduce THERMAL POWER below the P-6 setpoint or increase to THERMAL POWER above the P-10 setpoint.

The NIS Intermediate Range Neutron Flux channels must be OPERABLE when the power level is above the capability of the source range, P-6, and below the capability of the power range, P-10. If THERMAL POWER is greater than the P-10 setpoint, the NIS power range detectors perform the monitoring and protection functions and the intermediate range is not required.

The Completion Times allow for a slow and controlled power adjustment above P-10 or below P-6 and take into account the redundant capability afforded by the redundant OPERABLE channel, ~~and the low probability of its failure during this period.~~

This action does not require the inoperable channel to be tripped because the Function uses one-out-of-two logic. Tripping one channel would trip the reactor. Thus, the Required Actions specified in this Condition are only applicable when channel failure does not result in Reactor Trip reactor trip.

H.1 and H.2

Condition H applies to two inoperable Intermediate Range Neutron Flux trip channels in MODE 2 when THERMAL POWER is above the P-6 setpoint and below the P-10 setpoint. Required Actions specified in this Condition are only applicable when channel failures do not result in Reactor Trip reactor trip. Above the P-6 setpoint and below the P-10 setpoint, the NIS intermediate range detector performs the monitoring Functions.

With no intermediate range channels OPERABLE, the Required Actions are to suspend operations involving positive reactivity additions immediately. This will preclude any power level increase since there are no OPERABLE Intermediate Range Neutron Flux channels. The operator must also reduce THERMAL POWER below the P-6 setpoint within two hours. Below P-6, the Source Range Neutron Flux channels will be able to monitor the core power level. The Completion Time of 2 hours will

allow a slow and controlled power reduction to less than the P-6 setpoint ~~and takes into account the low probability of occurrence of an event during this period that may require the protection afforded by the NIS Intermediate Range Neutron Flux trip.~~

Required Action H.1 is modified by a Note to indicate that normal plant control operations that individually add limited positive reactivity (e.g., temperature or boron fluctuations associated with RCS inventory management or temperature control) are not precluded by this Action, provided they are accounted for in the calculated SDM.

I.1

Condition I applies to one inoperable Source Range Neutron Flux trip channel when in MODE 2, below the P-6 setpoint, and performing a reactor startup. With the unit in this Condition, below P-6, the NIS source range performs the monitoring and protection functions. With one of the two channels inoperable, operations involving positive reactivity additions shall be suspended immediately.

This will preclude any power escalation. With only one source range channel OPERABLE, core protection is severely reduced and any actions that add positive reactivity to the core must be suspended immediately.

Required Action I.1 is modified by a Note to indicate that normal plant control operations that individually add limited positive reactivity (e.g., temperature or boron fluctuations associated with RCS inventory management or temperature control) are not precluded by this Action, provided they are accounted for in the calculated SDM.

J.1

Condition J applies to two inoperable Source Range Neutron Flux trip channels when in MODE 2, below the P-6 setpoint, and in MODE 3, 4, or 5 with the Rod Control System capable of rod withdrawal or one or more rods not fully inserted. With the unit in this Condition, below P-6, the NIS source range performs the monitoring and protection functions. With both source range channels inoperable, the RTBs must be opened immediately. With the RTBs open, the core is in a more stable condition.

K.1, K.2.1, and K.2.2

Condition K applies to one inoperable source range channel in MODE 3, 4, or 5 with the Rod Control System capable of rod withdrawal or one or more rods not fully inserted. With the unit in this Condition, below P-6, the NIS source range performs the monitoring and protection functions. With one of the source range channels inoperable, 48 hours is allowed to restore it to an OPERABLE status. If the channel cannot be returned to an OPERABLE status, action must be initiated within the same 48 hours to ensure that all rods are fully inserted, and the Rod Control System

must be placed in a condition incapable of rod withdrawal within the next hour.

L.1 and L.2

Condition L applies to the following ~~reactor trip~~Reactor Trip Functions:

- ~~• Low Pressurizer Pressure,~~
- ~~• High Pressurizer Water Level,~~
- Low Reactor Coolant Flow,
- Low Reactor Coolant Pump Speed, and
- ~~• High-High SG Water Level, and~~
- Turbine Trip – Turbine Emergency Trip Oil Pressure.

With one required channel inoperable, the inoperable channel must be placed in the ~~tripped~~ condition within 72 hours. Failure of one channel places the Function in a two-out-of-two configuration, when the failed channel does not result in a trip channel. This configuration provides adequate plant protection, but does not meet the single failure criteria. Therefore, within 72 hours the inoperable channel must be tripped to place the Function in a one-out-of-two configuration that satisfies the single failure criteria. Placing the channel in the ~~tripped-trip~~ condition when above the P-7 setpoint, results in a partial trip condition requiring only one additional channel to initiate a ~~reactor trip~~Reactor Trip.

These Functions do not have to be OPERABLE below the P-7 setpoint because there is insufficient heat production to generate DNB conditions below the P-7 setpoint. ~~The 72 hours allowed to place the channel in the tripped condition is justified because the remaining two operable channels have automatic self testing (as described for COT), and automatic CHANNEL CHECKS. An additional 6 hours is allowed to reduce THERMAL POWER to below P-7 if the inoperable channel cannot be restored to OPERABLE status or placed in trip within the specified Completion Time.~~

~~Allowance of this time interval takes into consideration the redundant capability provided by the remaining redundant OPERABLE channels, and the low probability of occurrence of an event during this period that may require the protection afforded by the Functions associated with Condition L.~~ The Completion Time of 72 hours to place the inoperable channel in the trip condition is justified because the two remaining OPERABLE channels are adequate to perform the safety function. The Completion Time also considers that the two remaining OPERABLE channels have continuous automatic self-testing.

In addition, the two remaining OPERABLE channels have continuous automatic CHANNEL CHECKS, except for Turbine Trip – Turbine Emergency Trip Oil Pressure. This additional justification is not needed for Turbine Trip – Turbine Emergency Trip Oil Pressure, because this is an anticipatory function that is not credited in the safety analysis.

~~Expect for Pressurizer~~For all functions (except Turbine Trip – Turbine Emergency Trip Oil Pressure, ~~Pressurizer Level, and SG Water Level, one channel may be bypassed for up to 12 hours for surveillance testing. The 12 hours bypass limit is-~~), the Completion Time of 72 hours is also justified in the PSMS-US-APWR reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to and risk analyses, the US-APWR Technical Report MUAP-07030 PRA, Attachment 6A.12. The summary and result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA which are documented in FSAR Chapter 19. This bypass is not allowed for Pressurizer Pressure, Pressurizer Level, and SG Water Level because these channels are also used for control. If a failure were to occur in one of the two remaining control channels, a plant transient could occur that would require a plant trip, but a plant trip would not occur with only one remaining operable channel.
(Ref. 10).

~~The initial completion time of 72 hours is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6A.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~The Required Actions are modified by a Note that allows placing one required channel in bypass for up to 12 hours while performing surveillance testing, provided the other required channels are OPERABLE, or one required channel is OPERABLE and the other required channel is placed in the trip condition. With one required channel bypassed, the system can detect all anomalies, but it cannot also sustain a single failure.

The Bypass Time of 12 hours is justified because the remaining OPERABLE channels are adequate to perform the safety function. The Bypass Time also considers that the remaining OPERABLE channels have continuous automatic self-testing.

In addition the remaining OPERABLE channels have continuous automatic CHANNEL CHECKS, except for Turbine Trip – Turbine Emergency Trip Oil Pressure. This additional justification is not needed for Turbine Trip – Turbine Emergency Trip Oil Pressure, because this is an anticipated function that is not credited in the safety analysis.

The Bypass Time of 12 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

M.1 and M.2

Condition M applies to the ECCS ~~a~~Actuation input in MODES 1 and 2. These actions address the train orientation of the RTS for these Functions. With one required train inoperable, 24 hours are allowed to restore the train to OPERABLE status or the unit must be placed in MODE 3 within the next 6 hours.

The Completion Time of ~~24-24~~ hours is ~~reasonable considering that in this Condition, justified because~~ the two remaining OPERABLE trains are adequate to perform the safety function ~~and given. In addition, the low probability of an event during this interval. The 24 hours allowed to restore the train to OPERABLE status also~~ Completion Time considers that the two remaining OPERABLE trains each have continuous automatic self-testing ~~as described for ACTUATION LOGIC TEST.~~

The Completion Time of 24 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging unit systems.

The Required Actions have been modified by a Note that allows bypassing ~~placing~~ one ~~inoperable~~ required train in bypass for up to ~~4~~ 4 hours ~~for~~ while performing surveillance testing, provided the other ~~two~~ required trains are OPERABLE.

The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE trains have continuous automatic self-testing.

The Bypass Time of 4 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

N.1 [and N.2]

Condition N applies to the RTBs in MODES 1 and 2. These actions address the train orientation of the RTS for the RTBs. With one required train inoperable, 24 hours ~~is~~ are allowed for train corrective maintenance to restore the train to OPERABLE status.

The ~~24 hour~~ Completion Time ~~is reasonable considering that in this Condition, of 24 hours is justified because~~ the two remaining OPERABLE trains are adequate to perform the safety function ~~and given the low probability of an event during this interval.~~ In addition, the Completion

Time considers that the two remaining OPERABLE trains each have continuous automatic self-testing.

The Completion Time of 24 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

[Required Action N.2 allows the option to apply the requirements of Specification 5.5.18 to determine a Risk Informed Completion Time.]

~~The initial completion time of 24 hours is justified in the PSMS reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6A.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~

O.1 and O.2

Condition O applies to the P-6 and P-10 interlocks. With one or more ~~required~~ channels inoperable ~~for one out of two or two out of four coincidence logic~~, the associated interlock must be verified to be in its required state for the existing unit condition within 1 hour or the unit must be placed in MODE 3 within the next 6 hours. Verifying the interlock status manually accomplishes the interlock's Function.

The Completion Time of 1 hour is based on operating experience and the minimum amount of time allowed for manual operator actions.

The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging unit systems.

The 1 hour and 6 hour Completion Times are equal to the time allowed by LCO 3.0.3 for shutdown actions in the event of a complete loss of RTS Function.

P.1 and P.2

Condition P applies to the P-7 and P-13 interlocks in MODE 1. With one or more required channels ~~inoperable (P-13), or one or more~~ trains inoperable ~~for two out of four coincidence logic (P-7)~~, the associated interlock must be verified to be in its required state for the existing unit condition within 1 hour or the unit must be placed in MODE 2 within the next 6 hours. These actions are conservative for the case where power level is being raised. Verifying the interlock status manually accomplishes the interlock's Function.

The Completion Time of 1 hour is based on operating experience and the minimum amount of time allowed for manual operator actions.

The Completion Time of 1 hour is required because the P-13 interlock is generated using the Turbine Inlet Pressure instrumentation channels, which are shared with the PCMS. The SSA within the PCMS prevents erroneous control system actions due to a single failed shared instrument channel, which would otherwise require the protection function actuation. When there are less than three OPERABLE required Turbine Inlet Pressure instrumentation channels, the SSA cannot prevent erroneous control system operation due to an input failure.

The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power in an orderly manner and without challenging unit systems.

Q.1 [and Q.2]

Condition Q applies to the RTB Undervoltage and Shunt Trip Mechanisms, i.e., diverse trip features, in MODES 1 and 2. For ~~one RTB~~either of the two RTBs in a required train, with one of the diverse trip features inoperable, it must be restored to an OPERABLE status within 48 hours.

The Completion Time of 48 hours for Required Action Q.1 is reasonable considering that in this Condition there is one remaining diverse feature for the affected RTB, one OPERABLE RTB in the affected RTB train and two OPERABLE RTB trains capable of performing the safety function ~~and given the low probability of an event occurring during this interval.~~

The Completion Time of 48 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

[Required Action Q.2 allows the option to apply the requirements of Specification 5.5.18 to determine a Risk Informed Completion Time.]

R.1 [and R.2]

Condition R applies to the RTS Automatic Trip Logic in MODES 1 and 2. These actions address the train orientation of the RTS for these Functions. With one required train inoperable, 24 hours are allowed to restore the train to OPERABLE status.

The Completion Time of ~~24~~24 hours is ~~reasonable considering that in this Condition, justified because~~ the two remaining OPERABLE required trains are adequate to perform the safety function ~~and given~~. In addition, the ~~low probability of an event during this interval. The 24 hours allowed to restore the train to OPERABLE status also~~ Completion Time considers that the two remaining OPERABLE required trains each have continuous automatic self-testing ~~as described for ACTUATION LOGIC TEST.~~

The Completion Time of 24 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

[Required Action R.2 allows the option to apply the requirements of Specification 5.5.18 to determine a Risk Informed Completion Time.]

The Required Actions have been modified by a Note that allows ~~bypassing~~ placing one ~~inoperable~~ required train in bypass for up to 4 hours ~~for~~ while performing surveillance testing, provided the other ~~two~~ required trains are OPERABLE.

The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE trains have continuous automatic self-testing.

The Bypass Time of 4 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

S.1

Condition S applies when the Required Action and associated Completion Time for Condition N, Q, or R have not been met. If the train cannot be returned to OPERABLE status, the unit must be placed in a MODE where the requirement does not apply. This is accomplished by placing the unit in MODE 3 within 6 hours. The Completion Time of 6 hours is a reasonable time, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging unit systems.

Placing the unit in MODE 3 ~~from Condition N,~~ with any of the applicable Functions inoperable, results in Condition D entry ~~while an RTB is inoperable.~~

~~(From Condition Q) With the unit in MODE 3, Condition D would apply to any inoperable RTB trip mechanism.~~

T.1 and T.2

Condition T applies to Main Turbine Stop Valve Closure. With one channel inoperable, the inoperable channel must be placed in the trip condition within 12 hours. If placed in the tripped condition, this results in a partial trip condition requiring three additional channels to initiate a ~~reactor trip.~~ Reactor Trip. If the channel can not be restored to OPERABLE status or placed in the trip condition, then power must be reduced below the P-7 setpoint within the next 6 hours. The 6 hours allowed for reducing power ~~is~~ are consistent with other power reduction action ~~completion times~~ Completion Times.

The Required Actions are modified by a Note that allows placing one channel in bypass for up to 12 hours while performing ~~routine~~ surveillance testing. ~~These times~~

The Completion Time and Bypass Time are justified because this is an anticipatory trip that is not credited in the safety analysis, and a diverse ~~turbine trip~~ Turbine Trip is also initiated from the Turbine Emergency Oil Pressure.

U.1 and U.2

Condition U applies to the following Reactor Trip Functions:

- Overtemperature ΔT .
- Overpower ΔT .
- High Pressurizer Pressure, and
- Low SG Water Level.

With one required channel inoperable, the inoperable channel must be placed in the trip condition within 1 hour and restored to OPERABLE status in 72 hours.

This Condition applies to functions that operate on two-out-of-three logic and have channels that are shared with the control systems. Normally the SSA can prevent erroneous control system operations. However, when there are less than three OPERABLE required channels, the SSA cannot prevent erroneous control system operation due to an input failure. With two OPERABLE required channels and one required channel in the trip condition, if a channel failure occurs in an OPERABLE required channel and results in erroneous control system operation, the remaining OPERABLE required channel can provide a plant trip. However, the channel that causes the erroneous control system operation cannot be credited as the single failure; therefore, this configuration does not satisfy the single failure criteria. To satisfy the single failure criteria, three required channels must be restored to OPERABLE status within 72 hours.

The Completion Time of 1 hour to place the failed channel in the trip condition is based on operating experience and the minimum amount of time allowed for manual operator actions.

The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the two remaining OPERABLE channels have continuous automatic self-testing and continuous automatic channel checks.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref.10).

Bypass of a required channel is not allowed because there are only three required channels and these channels are also used for control. If a failure were to occur in one of the two remaining required control channels, a plant transient could occur that would require a plant trip, but a plant trip would not occur with only one remaining OPERABLE required channel.

V.1

If the Required Action and associated Completion Time of Condition U is not met, the unit must be placed in a MODE where these Functions are not required OPERABLE. An additional 6 hours ~~is~~ are allowed to place the unit in MODE 3. Six hours is a reasonable time, based on operating experience, to place the unit in MODE 3 from full power in an orderly manner and without challenging unit systems.

W.1 and W.2

Condition W applies to the following Reactor Trip Functions:

- Low Pressurizer Pressure.
- High Pressurizer Water Level, and
- High-High SG Water Level.

With one required channel inoperable, the inoperable channel must be placed in the trip condition within 1 hour and restored to OPERABLE status in 72 hours.

This Condition applies to functions that operate on two-out-of-three logic and have channels that are shared with the control systems. Normally the SSA can prevent erroneous control system operations. However, when there are less than three OPERABLE required channels, the SSA cannot prevent erroneous control system operation due to an input failure. With two OPERABLE required channels and one required channel in the trip condition, if a channel failure occurs in an OPERABLE required channel and results in erroneous control system operation, the remaining OPERABLE required channel can provide a plant trip. However, the channel that causes the erroneous control system operation cannot be credited as the single failure; therefore, this configuration does not satisfy the single failure criteria. When above the P-7 setpoint, to satisfy the single failure criteria, three channels must be restored to OPERABLE status within 72 hours.

These Functions do not have to be OPERABLE below the P-7 setpoint because there is insufficient heat production to generate DNB conditions below the P-7 setpoint.

The Completion Time of 1 hour to place the failed channel in the trip condition is based on operating experience and the minimum amount of time allowed for manual operator actions.

The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the two remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref.10).

Bypass of a required channel is not allowed because there are only three required channels and these channels are also used for control. If a failure were to occur in one of the two remaining required control channels, a plant transient could occur that would require a plant trip, but a plant trip would not occur with only one remaining OPERABLE required channel.

X.1

If the Required Action and associated Completion Time of Condition W is not met, the unit must be placed in which THERMAL POWER is below P-7. Six hours ~~is~~ are allowed to reduce THERMAL POWER to below P-7 if the inoperable channel cannot be restored to OPERABLE status or placed in trip within the specified Completion Time.

The Completion Time of 6 hours is reasonable, based on operating experience, to reduce THERMAL POWER to below P-7 from full power in an orderly manner and without challenging unit systems.

BASES

SURVEILLANCE REQUIREMENTS

The SRs for each RTS Function are identified by the SRs column of Table 3.3.1-1 for that Function.

A Note has been added to the SR Table stating that Table 3.3.1-1 determines which SRs apply to which RTS Functions.

Note that each channel of process protection supplies all trains of the RTS. However, when testing a Channel, it is only necessary to manually verify that the channel is OPERABLE in its respective train. This is because the interface to other trains is continuously verified through continuous automatic self-testing. ~~Self~~Continuous automatic self-testing

is confirmed through periodic ~~GOT and ACTUATION LOGIC TEST~~. MIC. The CHANNEL CALIBRATION is performed in a manner that is consistent with the ~~method~~ methods and assumptions of ~~Section~~ Specification 5.5.21, Setpoint Control Program (SCP).

SR 3.3.1.1

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

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

[The Surveillance Frequency of 12 hours is based on operating experience that demonstrates channel failure is rare. The CHANNEL CHECK supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the LCO required channels.

~~OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

A CHANNEL CHECK may be conducted manually or automatically. For the US-APWR an automated CHANNEL CHECK is normally conducted continuously, which satisfies the 12 hour Ssurveillance Ffrequency requirement. Where the CHANNEL CHECK is conducted automatically, an alarm shall be generated when the agreement criteria is not met. If the automated CHANNEL CHECK function is unavailable, a manual CHANNEL CHECK shall be conducted at the minimum 12 hour Ssurveillance Ffrequency.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

~~The equipment that performs the automated CHANNEL CHECK, and continuous self testing described for GOT and ACTUATION LOGIC TEST, shall be confirmed OPERABLE every 12 hours. This shall include the capability to generate fault alarms.~~

SR 3.3.1.2

SR 3.3.1.2 compares the calorimetric heat balance calculation to the power range channel output. If the calorimetric heat balance calculation results exceed the power range channel output by more than 2% RTP, the power range channel is not declared inoperable, but must be adjusted. The power range channel output shall be adjusted consistent with the calorimetric heat balance calculation results if the calorimetric calculation exceed the power range channel output by more than + 2% RTP. If the power range channel output cannot be properly adjusted, the channel is declared inoperable.

If the calorimetric is performed at part power (<70% RTP), adjusting the power range channel indication in the increasing power direction will assure a ~~reactor trip~~ Reactor Trip below the safety analysis limit (<118% RTP). Making no adjustment to the power range channel in the decreasing power direction due to a part power calorimetric assures a ~~reactor trip~~ Reactor Trip consistent with the safety analyses.

This allowance does not preclude making indicated power adjustments, if desired, when the calorimetric heat balance calculation is less than the power range channel output. To provide close agreement between indicated power and to preserve operating margin, the power range channels are normally adjusted when operating at or near full power during steady-state conditions. However, discretion must be exercised if the power range channel output is adjusted in the decreasing power direction due to a part power calorimetric (< 70% RTP). This action may introduce a non-conservative bias at higher power levels which may result in an NIS ~~reactor trip~~ Reactor Trip above the safety analysis limit (> 118% RTP). The cause of the potential non-conservative bias is the decreased accuracy of the calorimetric at reduced power conditions. The primary error contributor to the instrument uncertainty for a secondary side power calorimetric measurement is the feedwater flow measurement, which is typically a ΔP measurement across a feedwater venturi. While the measurement uncertainty remains constant in ΔP as power decreases, when translated into flow, the uncertainty increases as a square term.

Thus a 1% flow error at 100% power can approach a 10% flow error at 30% RTP even though the ΔP error has not changed. An evaluation of extended operation at part power conditions would conclude that it is prudent to administratively adjust the digital setpoint of the High Power Range Neutron Flux (~~high setpoint~~ High Setpoint) digital bistables to $\leq 85\%$ RTP when: 1) the power range channel output is adjusted in the decreasing power direction due to a part power calorimetric below 70% RTP; or 2) for a post refueling startup. The evaluation of extended

operation at part power conditions would also conclude that the potential need to adjust the indication of the High Power Range Neutron Flux in the decreasing power direction is quite small, primarily to address operation in the intermediate range about P-10 (nominally 10% RTP) to allow enabling of the High Power Range Neutron Flux (~~low setpoint~~Low Setpoint) and the Intermediate Range Neutron Flux ~~reactor trips~~Reactor Trips. Before the High Power Range Neutron Flux (~~high setpoint~~High Setpoint) digital bistables are reset to $\leq 109\%$ RTP, the power range channel adjustment must be confirmed based on a calorimetric performed at $\geq 70\%$ RTP.

The Note clarifies that this SurveillanceSR is required only if reactor power is $\geq 15\%$ RTP and that 12 hours are allowed for performing the first SurveillanceSR after reaching 15% RTP. A power level of 15% RTP is chosen based on plant stability, i.e., automatic rod control capability and turbine generator synchronized to the grid.

[The Surveillance Frequency of every 24 hours is adequate. It is based on unit operating experience, considering instrument reliability and operating history data for instrument drift. Together these factors demonstrate that a difference between the calorimetric heat balance calculation and the power range channel output of more than +2% RTP is not expected in any 24 hour period.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.] In addition, control room operators periodically monitor redundant indications and alarms to detect deviations in channel outputs.

SR 3.3.1.3

SR 3.3.1.3 compares the incore system to the NIS channel output. If the absolute difference is $\geq 3\%$, the NIS channel is still OPERABLE, but must be readjusted. The excore NIS channel shall be adjusted if the absolute difference between the incore and excore AFD is $\geq 3\%$.

If the NIS channel cannot be properly readjusted, the channel is declared inoperable. This SurveillanceSR is performed to verify the $f(\Delta I)$ input to the Overtemperature ΔT Function and Overpower ΔT Function.

A Note clarifies that the SurveillanceSR is required only if reactor power is $\geq 15\%$ RTP and that 24 hours ~~is~~are allowed for performing the first SurveillanceSR after reaching 15% RTP.

[The Surveillance Frequency of every 31 effective full power days (EFPD) is adequate. It is based on unit operating experience, considering instrument reliability and operating history data for instrument drift. Also, the slow changes in neutron flux during the fuel cycle can be detected during this interval.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.1.4

SR 3.3.1.4 is the performance of a TADOT. This test shall verify RTB train OPERABILITY by actuation of the two RTBs for each train to their ~~tripped trip~~ state. Each RTB may be actuated together or individually.

The RTB train test shall include three separate but overlapping tests: (1) The Undervoltage ~~Test~~ for verification of RTB operability using only the ~~undervoltage trip mechanism~~. Undervoltage Trip Mechanism, (2) The Shunt Trip test for verification of RTB operability using only the ~~shunt trip mechanisms~~. Shunt Trip Mechanisms, and (3) The Manual Reactor Trip ~~Test~~ for verification of RTB operability using the hardwired switches. The Undervoltage ~~Test~~ shall bypass the ~~shunt trip mechanism~~ Shunt Trip Mechanism, so each RTB actuates using only the ~~undervoltage mechanism~~. Undervoltage Trip Mechanism. The Shunt Trip ~~Test~~ shall bypass the ~~undervoltage mechanism~~ Undervoltage Trip Mechanism, so each RTB actuates using only the ~~shunt trip mechanism~~. Shunt Trip Mechanism. The Manual Reactor Trip ~~Test~~ shall actuate the RTB with both mechanisms. Figure 4.4-1 of ~~Topical Report~~ MUAP-07004 (Ref. 6) describes an acceptable overlapping method for conducting these three separate tests that confirms OPERABLE status.

[The Surveillance Frequency of every 62 days on a STAGGERED TEST BASIS applies to all four RTB trains. This ~~Surveillance test F~~ frequency is justified based on industry experience. The ~~Surveillance test F~~ frequency also considers the added reliability of the US-APWR RTB configuration, which includes redundant RTBs within each train and the overall two-out-of-four train configuration. Since each test actuates each RTB to its required ~~tripped trip~~ state, the STAGGERED TEST BASIS results in each RTB being tested every 248 days, and each tripping method being tested every 744 days. ~~OR~~

~~The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.~~

~~The TADOT STAGGERED TEST BASIS~~ ES Surveillance F frequency of 62 days, with each RTB tested every 248 days, and each trip methodology ultimately tested every 744 days, is also justified in the ~~PSMS reliability analysis~~. ~~For detailed information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6A.12. The reliability and risk analyses, the summary and result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA which are documented in FSAR Chapter 19.] (Ref. 10).~~

SR 3.3.1.5

~~SR 3.3.1.5 is the performance of an ACTUATION LOGIC TEST. The PSMS is self tested on a continuous basis from the digital side of all input modules to the digital side of all output modules. Self testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. The self testing is described in Reference 6 and 7. The ACTUATION LOGIC TEST is a check of the RTS software memory integrity to ensure there is no change to the internal RTS software that would impact its functional operation or the continuous self test function. The software memory integrity test is described in Reference 6 and 7. [The Frequency of every 24 months is justified based on the reliability of the PSMS. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

~~The complete continuity check from the input device to the output device is performed by the combination of the continuous CHANNEL CHECK, the 24 month CHANNEL CALIBRATION for the non-digital side of the input module, the continuous self-testing for the digital side, the 24 month COT, the 24 month ACTUATION LOGIC TEST and the STAGGERED 62 days TADOT for the non-digital side of the output module. The Channel CALIBRATION, COT, ACTUATION LOGIC TEST and TADOT, which are manual tests, overlap with the CHANNEL CHECK and self-testing and confirm the functioning of the self-testing.~~

~~The ACTUATION LOGIC TEST interval of 24 months with the self test capability is justified in the PSMS reliability analysis. For detailed information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6A.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.]~~

SR 3.3.1.65

SR 3.3.1.65 is a calibration of the excore channels to the incore channels. If the measurements do not agree, the excore channels are not declared inoperable but must be calibrated to agree with the incore detector measurements. If the excore channels cannot be adjusted, the channels are declared inoperable. This **SurveillanceSR** is performed to verify the f(Δ I) input to the Overtemperature Δ T Function and Overpower Δ T Function.

A Note modifies SR 3.3.1.6-5. The Note states that this **SurveillanceSR** is required only if reactor power is > 50% RTP and that 24 hours **is-are** allowed for performing the first **surveillanceSR** after reaching 50% RTP.

[The Surveillance Frequency of 92 EFPD is adequate. It is based on industry operating experience, considering instrument reliability and operating history data for instrument drift.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.1.76

SR 3.3.1.76 is the performance of a COT MIC for the RTS Instrumentation. This includes the RPS.

The PSMS is self-tested automatically on a continuous basis from the digital side of all input modules to the digital side of all output modules. Self Continuous automatic self-testing encompasses all digital PSMS safety-related functions including digital Nominal Trip Setpoints, Time Constants and trip actuation logic functions.- The continuous automatic self-testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. The continuous automatic self-testing is described in Reference 6 and 7. The COT Reference 6 and Reference 7.

The MIC is a diverse check of the RTS-PSMS software memory integrity, consistent with the Setpoint Control Program (SCP), to ensure there is no change to the internal RTSPSMS software that would impact its functional operation, including digital Nominal Trip Setpoint values Setpoints, Time Constants, actuation logic functions or the continuous self test function. automatic self-testing. The software memory integrity test MIC is described in Reference 6 and 7.

A COT ensures the entire channel will perform the intended Function. A COT also ensures that the logic processing for interlocks (i.e., P-6 and P-10) is operating correctly. The combination of the COT, CHANNEL CALIBRATION, continuous self testing and continuous CHANNEL CHECK ensures the complete P-Reference 6 and P-10 interlocks are operating correctly. Reference 7.

[The Frequency of 24 months is justified based on the reliability of the PSMS. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program. The capability to generate continuous automatic self-testing fault alarms shall be confirmed OPERABLE during the MIC.

The complete continuity OPERABILITY check from the measurement channel input device to the output device Reactor Trip Breaker is performed by the combination of the continuous automatic self-testing for the digital devices (the RPS and data communication interfaces), the continuous automatic CHANNEL CHECK (SR 3.3.1.1 and SR 3.3.1.7),

the ~~24-month~~ CHANNEL CALIBRATION (SR 3.3.1.8, SR 3.3.1.9 and SR 3.3.1.10), the MIC (SR 3.3.1.6) and the TADOT (SR 3.3.1.4 and SR 3.3.1.11). The CHANNEL CALIBRATION ~~for the non-digital side of the input module, the continuous self-testing for the digital side, the 24 month COT, 24 months Actuation Logic Test~~ MIC and the ~~STAGGERED 62 days TADOT for the non-digital side of the output module. The CHANNEL CALIBRATION, COT and TADOT, which are manual tests, overlap with the CHANNEL CHECK and~~ continuous automatic self-testing and confirm the functioning of the continuous automatic self-testing.

~~The COT interval of 24 months with the self test capability is justified in the PSMS reliability analysis. For detailed information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6A.12. The~~ The Surveillance Frequency of 24 months is justified because the software memory integrity is checked by the continuous automatic self-testing.

The Surveillance Frequency of 24 months is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 10).

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

~~result of the PSMS reliability analysis is evaluated and confirmed in the US-APWT PRA Chapter 19.]~~

~~The Note allows a normal shutdown to proceed without a delay for testing in MODE 2 and for a short time in MODE 3 until the RTBs are open and SR~~

~~SR 3.3.1.7 is no longer required to be performed. If the unit is to be in MODE 3 with the RTB closed for 4 hours this Surveillance must be performed prior to 4 hours after entry into MODE 3.~~

SR 3.3.1.8

Performance of the CHANNEL CHECK within 4 hours after reducing power below P-6 and [once every 12 hours thereafter OR in accordance with the Surveillance Frequency Control Program] ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between ~~the two~~ instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined based on a combination of the channel instrument uncertainties. 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.

The Surveillance Frequency of 4 hours is based on the need to verify OPERABILITY of the SR instruments within a reasonable time after being re-energized.

[The 12 hour Surveillance Ffrequency thereafter is based on operating experience that demonstrates channel failure is rare. The CHANNEL CHECK supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the LCO required channels. ~~OR The Surveillance Frequency thereafter is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.~~]

A CHANNEL CHECK may be conducted manually or automatically. For the US-APWR an automated CHANNEL CHECK is normally conducted continuously, which satisfies the 12 hour Ssurveillance Ffrequency requirement. Where the CHANNEL CHECK is conducted automatically, an alarm shall be generated when the agreement criteria is not met. If the automated CHANNEL CHECK function is unavailable, a manual CHANNEL CHECK shall be conducted at the minimum 12 hour Ssurveillance Ffrequency.

~~The equipment that performs the automated CHANNEL CHECK, and continuous self-testing described for GOT and ACTUATION LOGIC TEST, shall be confirmed OPERABLE including the capability to generate fault alarms.~~OR The Surveillance Frequency thereafter is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

SR 3.3.1.98

SR 3.3.1.8 is the performance of a CHANNEL CALIBRATION.

CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test ~~verifies~~must be performed consistent with the methods and assumptions of Specification 5.5.21, SCP, to verify that the channel responds to a measured parameter within the necessary range and accuracy ~~as defined by the Allowable Value.~~

The CHANNEL CALIBRATION confirms the accuracy of the channel from sensor to digital VDU readout as described in Reference 6.

For analog measurements, the CHANNEL CALIBRATION confirms the ~~accuracy of the channel from sensor to digital VDU read out (Ref. 6).~~ The

~~CHANNEL CALIBRATION confirms the analog measurement accuracy conforms to calibration settings are within~~ the Allowable Value at multiple points over the entire measurement channel span, encompassing all ~~reactor trip~~ Reactor Trip and interlock Nominal Trip Setpoint values. Digital ~~reactor trip~~ Reactor Trip and interlock Nominal Trip Setpoint values are confirmed through a ~~GOT~~ MIC.

For binary measurements, the CHANNEL CALIBRATION confirms the accuracy of the channel's state change, ~~as described in Reference 6.~~ The state change must occur within the Allowable Value of the Nominal Trip Setpoint.

~~CHANNEL CALIBRATIONS must be performed consistent with the methods and assumptions in Section 5.5.21 SCP~~ The equipment that performs the automated CHANNEL CHECK shall be confirmed OPERABLE, including the capability to generate fault alarms during the CHANNEL CALIBRATION.

[The Surveillance Frequency of 24 months is based on the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in accordance with ~~Section~~ Specification 5.5.21, Setpoint Control Program (SCP).

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

~~SR 3.3.1.9 is modified by a Note stating that this test shall include verification that the time constants are adjusted to the prescribed values where applicable.~~

SR 3.3.1. ~~109~~ is the performance of a CHANNEL CALIBRATION, as described in ~~SR~~ SR 3.3.1.9-8, for the neutron flux channels. This SR is modified by a Note stating that the neutron detectors are excluded from the CHANNEL CALIBRATION. ~~The CHANNEL CALIBRATION~~

~~For this surveillance requirement~~ SR the calibration for the power range neutron detectors consists of a normalization of the detectors based on a power calorimetric and flux map performed above 15% RTP. ~~The CHANNEL CALIBRATION~~ For this surveillance requirement SR the calibration for the source range and intermediate range neutron detectors consists of obtaining the detector plateau or discriminator curves, evaluating those curves, and comparing the curves to the manufacturer's data. This Surveillance ~~SR~~ is not required for the NIS power range detectors for entry into MODE 2 or 1, and is not required for the NIS intermediate range detectors for entry into MODE 2, because the unit must be in at least MODE 2 to perform the test for the intermediate range detectors and MODE 1 for the power range detectors.

[The 24 month Surveillance Frequency is based on the need to perform this SurveillanceSR under the conditions that apply during a plant outage and the potential for an unplanned transient if the SurveillanceSR were performed with the reactor at power. Operating experience has shown these components usually pass the SurveillanceSR when performed on the 24 month Surveillance Frequency.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.1.4110

SR 3.3.1.4110 is the performance of a CHANNEL CALIBRATION, as described in ~~SR SR 3.3.1.9. Whenever a sensing element is replaced, the next required~~ CHANNEL CALIBRATION ~~of the resistance temperature detectors (RTD) sensors~~ is accomplished by an in-place a cross calibration that compares the other sensing elements with the recently signals from the installed sensing element channels to a channel with a reference RTD, in accordance with FSAR Section 7.1.3.14 (Ref. 13).

~~This test will verify the~~ The rate lag compensation for flow from the core to the RTDs is implemented in the RPS through digital functions; this rate lag function is confirmed through the MIC, SR 3.3.1.6.

[The Surveillance Frequency is justified by the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in accordance with ~~Section Specification~~ 5.5.21, Setpoint Control Program (SCP).

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.1.4211

SR 3.3.1.4211 is the performance of a TADOT of Turbine Trip Functions. This TADOT is performed prior to exceeding the P-7 interlock whenever the unit has been in MODE 3. This SurveillanceSR is not required if it has been performed within the previous 31 days. Verification of the Nominal Trip Setpoint ~~does is not have to be~~ performed for this during the TADOT SurveillanceSR; the Nominal Trip Setpoint is verified during CHANNEL CALIBRATION. Performance of this test will ensure that the ~~turbine trip~~ Turbine Trip Function is OPERABLE prior to exceeding the P-7 interlock.

SR 3.3.1.4312

SR 3.3.1.13~~12~~ verifies that the ~~response times for all~~ RTS functions ~~are~~ RESPONSE TIME is less than or equal to the maximum values assumed in the accident analysis. Accident analysis response time values are ~~defined~~ specified in Reference 2. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the ~~Trip Setpoint value at the~~ sensor Analytical Limit to the point at which the equipment reaches the required functional state (i.e., control and shutdown rods fully inserted in the reactor core).

~~The PSMS dynamic transfer functions employ time constants that are installed as digital values and processed through digital algorithms. Therefore, the time response of the dynamic transfer functions has no potential for variation due to time or environmental drift or component aging. The COT confirms the integrity of the time constants and algorithms through the periodic software memory integrity check. The complete PSMS response time is determined one time by analysis and confirmed one time in the factory test. The response times of analog instruments that provide input to the dynamic transfer functions are periodically checked in Surveillance 3.3.1.13, because they do have the potential for response time variation. RTBs and RTDs are known to have aging or wear-out mechanisms that can impact response time and require response time measurement. Response time for other components can be affected by random failures or calibration discrepancies, which can be detected by other testing and calibration methods required by other surveillances.~~

Response time may be verified by actual response time tests in any series of sequential, overlapping or total channel measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the channel.

Allocations for sensors, signal ~~conditioning,~~ processing and actuation logic response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. ~~MUAP-09021-P "Response Time of safety I&G System"~~

The PSMS MELTAC controllers employ dynamic transfer functions with Time Constants that are installed as digital values and processed through digital algorithms. Therefore, the time response of all digital PSMS functions has no potential for variation due to time, environmental drift or component aging.

PSMS Time Constants are set at the nominal values assumed in the safety analysis. The combination of continuous automatic self-testing and MIC confirms the integrity of the dynamic transfer functions, Time Constants and actuation logic functions.

The response time for the digital portion of the PSMS is determined one time by analysis and confirmed one time in the factory test. Therefore, for PSMS digital functions, including Functions with Time Constants, response time tests are not required; instead, a response time allocation may be applied.

Response time for PSMS MELTAC input signal conditioning, can be affected by random failures or degradation, which can be detected by CHANNEL CALIBRATION. Section 4.6 of MUAP-07005, "Safety System Digital Platform -MELTAC-" (Ref. 7) describes the basis for crediting CHANNEL CALIBRATION for detecting PSMS signal conditioning response time degradation. Therefore, for PSMS input signal conditioning, response time tests are not required; instead, a response time allocation may be applied.

MUAP-09021-P, "Response Time of Safety I&C System" (Ref. 11), provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the report. Response time verification for other sensor types must be demonstrated by test. MUAP-09021-P also provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the protection system channel response time. ~~Section 4.4 of MUAP-07005, "Safety System Digital Platform -MELTAC-" describes how response times of each individual MELTAC module are combined to determine the total digital system response time.~~

In addition, MUAP-09021-P identifies the acceptance criteria for RTS components that require response time measurement (such as RTBs and RTDs which are known to have aging or wear-out mechanisms that can impact response time), taking into consideration the total RTS RESPONSE TIME requirement and the allocations for other components that do not require testing.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.

[As appropriate, each channel's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices (i.e., RTBs) is included in the testing. Response times cannot be determined during unit operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillanceSR when performed at the 24 months Surveillance Frequency. Therefore, the Surveillance Frequency was concluded to be acceptable from a reliability standpoint.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.1.1312 is modified by a Note stating that neutron detectors are excluded from RTS RESPONSE TIME testing. This Note is necessary because of the difficulty in generating an appropriate detector input signal. Excluding the detectors is acceptable because the principles of detector operation ensure a virtually instantaneous response.

REFERENCES

1. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety Related Instrumentation."
2. FSAR Section 7.2.
3. FSAR Chapter 15.
4. IEEE-603-1991.
5. 10 CFR 50.49.
6. MUAP-07004-P (~~Proprietary~~) and MUAP-07004-NP (~~Non-Proprietary~~), Revision 7, "Safety I&C System Description and Design Process."
7. MUAP-07005-P (~~Proprietary~~) and MUAP-07005-NP (~~Non-Proprietary~~), Revision 8, "Safety System Digital Platform – MELTAC."
8. 10 CFR 50.36.
9. FSAR Section 6.2.1.
10. FSAR Chapter 19.
11. MUAP-09021-P, Revision 2, "Response Time of Safety I&C System."
12. MUAP-09022-P, Revision 2, "US-APWR Instrument Setpoint Methodology."

13. FSAR Section 7.1.

B 3.3 INSTRUMENTATION

B 3.3.2 Engineered Safety ~~Feature~~Features 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 the Reactor Coolant System (RCS) pressure boundary, and to mitigate accidents.

The ESFAS instrumentation is segmented into ~~three~~four distinct but interconnected modules as identified below:

- Field transmitters or process sensors and instrumentation: provide a measurable electronic signal based on the physical characteristics of the parameter being measured,
- The Reactor Protection System (RPS) provides signal conditioning, analog to digital conversion, ~~bistable-digital bistables for~~ setpoint comparison, process algorithm actuation, ~~compatible electrical signal~~digital output to ~~plant process components~~the ESFAS, and digital output to control board/~~main control room~~Main Control Room (MCR)/miscellaneous VDUs, ~~and~~
- The ESFAS and Safety Logic System (SLS) provides Actuation Logic, and Actuation Outputs to initiate the proper unit shutdown or ~~engineered safety feature~~Engineered Safety Features (ESF) actuation in accordance with the defined logic ~~and~~ based on the partial actuation inputs from the RPS, ~~and~~
- The Safety VDUs (S-VDU) and Communication Subsystems (COM) provide Manual Control of ESF Components and backup manual initiation of Reactor Trip and ESFAS Functions.

The Nominal Trip Setpoint, recorded and maintained in a document established by the Setpoint Control Program (SCP), 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 Nominal Trip Setpoint accounts for uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., repeatability), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors which may influence its actual performance (e.g., harsh accident environments). In this manner, the Nominal Trip Setpoint plays an important role in ensuring that SLs are not exceeded. As such, the Nominal Trip Setpoint meets the definition of an LSSS (Ref. 13) and is used to meet the requirement that they be contained in the Technical Specifications. This is an acceptable approach for digital systems because the digital setpoints do not drift as

in analog systems. The Nominal Trip Setpoint is applicable to automatic protection instrumentation functions for Reactor Trip, ESFAS actuation and permissive interlocks.

Technical Specifications contain Allowable Values related to the OPERABILITY of equipment required for safe operation of the facility. The Allowable Value accommodates expected drift in the analog components of the channel that would have been specifically accounted for in the setpoint methodology for calculating the Nominal Trip Setpoint and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as-found" setting of the protective device. Therefore, the device would still be OPERABLE since it would have performed its safety function and the only corrective action required would be to recalibrate the device 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. This value needs to be specified in the Technical Specifications in order to define OPERABILITY of the devices and is designated as the Allowable Value.

The Allowable Value, in conjunction with the Nominal Trip Setpoint and LCO₂ establishes the threshold for ESFAS action to prevent exceeding acceptable limits such that the consequences of Postulated Accidents (PAs) will be acceptable. The Allowable Value, recorded and maintained in a document established by the Setpoint Control Program (SCP), is considered a limiting value such that a channel is OPERABLE if the ~~measured accuracy is as-found~~ value does not ~~to~~ exceed the Allowable Value during ~~the~~ CHANNEL CALIBRATION. ~~The Allowable Value is applicable to automatic protection instrumentation functions for Reactor Trip, ESFAS actuation and permissive interlocks.~~

For analog measurements, the CHANNEL CALIBRATION verifies the ~~instrument channel accuracy~~ at five calibration ~~setpoints~~ settings corresponding to 0%, 25%, 50%, 75% and 100% of the instrument range. For binary measurements, the CHANNEL CALIBRATION verifies the accuracy of the channel's state change at the required setpoint. As such, the Allowable Value accounts for the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will still meet the LSSS definition and ensure that a SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval.

Note that, although ~~a~~ the channel is "OPERABLE" under these circumstances, the channel ~~must~~ shall be left adjusted to a value within the established channel ~~calibration tolerance~~ Calibration Tolerance (CT) band in accordance with the 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. The Calibration Tolerance, recorded and maintained in a document established by the SCP, is applicable to automatic protection instrumentation functions for Reactor Trip, ESFAS actuation and permissive interlocks.

If the as-found value of the device is found to have exceeded the Allowable Value, or the as-left value of the device cannot be adjusted to a value within the Calibration Tolerance, the device would be considered inoperable from a technical specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

In the Protection and Safety Monitoring System (PSMS), setpoints associated with analog measurements are stored as digital values that have no potential for variation due to time, environmental drift or component aging. For analog measurements, the only factors that can result in variation in the trip functions reside in the uncertainties that are pertinent to the analog portion of the system. Therefore, for analog measurements in the PSMS, it is appropriate for the Allowable Value to be expressed in terms of values that are measured during periodic testing of the analog portion of the system (i.e., CHANNEL CALIBRATION).

For PSMS analog measurements, the as-found and as-left values are measured from sensor to digital Visual Display Unit (VDU) readout during CHANNEL CALIBRATION. The US-APWR enhances human performance by establishing a standard CHANNEL CALIBRATION method for all analog measurements, whereby the as-found and as-left values read at the VDU are measured at the same five calibration settings, regardless of the PSMS trip setpoint(s).

Since the PSMS trip logic and setpoints for analog measurements are stored as digital values with no drift potential, and those digital values are confirmed through the MEMORY INTEGRITY CHECK (MIC), the only untested area required to confirm channel operability pertains to the accuracy of the analog input signal. When the analog input accuracy is confirmed, by reading the digital values of the five point CHANNEL CALIBRATION settings on any VDU driven by the same digital value used in the controller that executes the trip functions, the operability of the complete channel is confirmed, including the accuracy of all trip setpoints associated with that channel.

In the PSMS, setpoints associated with binary measurements are stored within the binary device itself. These setpoints have potential for variation due to time, environmental drift or component aging. However, these sensors are interfaced to the digital portion of the PSMS, which has no potential for variation due to time, environmental drift or component aging. For binary measurements, the only factors that can result in variation in the trip functions reside in the uncertainties that are pertinent to the binary sensor itself. Therefore, for binary measurements in the PSMS, it is appropriate for the Allowable Value to be expressed in terms of values

that are measured during periodic testing of the binary device (i.e., CHANNEL CALIBRATION).

For PSMS binary measurements, the as-found and as-left state change values are measured from sensor to VDU readout during CHANNEL CALIBRATION. The US-APWR enhances human performance by establishing a standard CHANNEL CALIBRATION method for all binary measurements, whereby the as-found and as-left values read at the VDU are measured at the channel's required state change.

Since the PSMS trip logic for binary sensors is stored as digital values with no drift potential, and those digital values are confirmed through the MIC, the only untested area required to confirm channel operability pertains to the accuracy of the binary input signal. When the binary input accuracy is confirmed, by reading the channel's state change on any VDU driven by the same digital value used in the controller that executes the trip functions, the operability of the complete channel is confirmed, including the accuracy of the trip setpoint associated with that channel.

Field Transmitters or Sensors

To meet the design demands for redundancy and reliability, more than one, and often as many as four, field transmitters or sensors are used to measure unit parameters. In many cases, field transmitters or sensors that input to the ESFAS are shared with the Reactor Trip System (RTS). In some cases, the same channels also provide control system inputs. To account for calibration tolerances and instrument drift, which are assumed to occur between calibrations, statistical allowances are provided in the Nominal Trip Setpoint and Allowable Values. The OPERABILITY of each transmitter or sensor is determined by ~~either~~ "as-found" calibration data evaluated during the CHANNEL CALIBRATION ~~or~~ and by qualitative assessment of field transmitter or sensor, as related to the channel behavior observed during performance of the CHANNEL CHECK.

~~Signal Processing Equipment~~ Protection and Safety Monitoring System

Generally, four channels of process control equipment are used for the signal processing of unit parameters measured by the field instruments. The process control equipment provides signal conditioning, analog to digital conversion, comparable digital output signals for VDUs located on the main control board, and comparison of measured input signals with setpoints established by safety analyses. These setpoints are ~~defined~~ recorded and maintained in ~~Chapter 7 (Ref. 2) and Chapter 8 (Ref. 8) a~~ document established by the Setpoint Control Program (SCP). If the measured value of a unit parameter exceeds the predetermined setpoint, a digital output from a digital ~~bistable output~~ is forwarded to the ESFAS for decision evaluation. Channel separation is maintained throughout the PSMS. Some unit parameters provide input only to the PSMS, while others are ~~used~~ use used by the PSMS and are retransmitted to the Plant Control and Monitoring System (PCMS) for use in one or more control systems.

Generally, if a parameter is used only for input to the protection circuits, three channels with a two-out-of-three logic are sufficient to provide the required reliability and redundancy. If one channel fails in a direction that would not result in a partial Function trip, the Function is still OPERABLE with a two-out-of-two logic. If one channel fails such that a partial Function trip occurs, a trip will not occur and the Function is still OPERABLE with a one-out-of-two logic.

Generally, if a parameter is used for input to the protection circuits and a control function, three channels with a two-out-of-three logic are also sufficient to provide the required reliability and redundancy. ~~The~~ When three or more channels are OPERABLE, the Signal Selection Algorithm (SSA) within the PCMS ensures the control systems can withstand an input failure to the control system without causing erroneous control system operation, which would otherwise require the protection function actuation. Since the input failure does not cause an erroneous control system action that challenges the protection function, the input failure is considered a single failure in the ESFAS and the ESFAS remains capable of providing its protective function with the remaining two ~~operable~~ OPERABLE channels. Again, a single failure will neither cause nor prevent the protection function actuation. When there are less than three OPERABLE channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for shared channels, when there are only three required channels.

These requirements are described in IEEE-603-1991 (Ref. 4). The actual number of channels required for each unit parameter is specified in Reference 2.

Allowable Values and ESFAS Setpoints

The Nominal Trip Setpoints used in the digital bistables or binary sensors are based on the Analytical Limits defined in the accident analysis and the channel uncertainty. The selection of these Nominal Trip Setpoints is such that adequate protection is provided when all sensor and processing ~~time delays~~ Time Delays are taken into account.

To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors for those ESFAS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 5), the Allowable Values and Nominal Trip Setpoints ~~recorded and maintained in a document established by the SCP in the accompanying LCO~~ are conservative ~~with respect to~~ protect the Analytical Limits. The ~~SCP~~ methodology identified in the SCP, used to calculate the Allowable Values and ~~ESFAS~~ Nominal Trip setpoints, incorporates all of the known uncertainties applicable to each channel (Ref. 7.12). The magnitudes of these uncertainties are factored into the determination of each ~~ESFAS~~ Nominal Trip Setpoint and ~~corresponding~~ Allowable Value.

The ~~ESFAS~~Nominal Trip Setpoint entered into the bistable or binary sensor is more conservative than that specified by the Analytical Limit ~~to account~~. The Nominal Trip Setpoint accounts for measurement errors detectable by the CHANNEL CALIBRATION and other unmeasurable errors (such as the effects of anticipated environmental conditions), which are both considered in the Allowable Value for CHANNEL CALIBRATION. The Allowable Value serves as the Technical Specification OPERABILITY limit for the purpose of the CHANNEL CALIBRATION. One example of such a change in measurement error is drift during the surveillance interval. If the ~~measured accuracy as found value~~ does not exceed the Allowable Value, the channel is considered OPERABLE.

The ~~ESFAS~~-Nominal Trip ~~Setpoints are~~Setpoint (i.e., LSSS) is the values at which the ~~bistables are~~digital bistable or binary sensor is set. The ~~ESFAS~~Nominal Trip Setpoint value ensures the safety analysis limits are met for the surveillance interval selected when a channel is adjusted based on stated channel uncertainties. Any channel is considered to be properly adjusted when the "as-left" value is within the established Calibration Tolerance (CT) band in accordance with the methods and assumptions ~~in of~~ the SCP. ~~The~~ ~~ESFAS~~Nominal Trip Setpoint value (i.e., expressed as a value without inequalities) ~~is used for digital bistables, is confirmed during the purposes of the COT~~MIC. The Nominal Trip Setpoint value (i.e., expressed as a value with inequalities) for binary sensors is confirmed during the CHANNEL CALIBRATION.

~~ESFAS~~-Nominal Trip ~~Setpoints~~Setpoints and Allowable Values, consistent with the requirements of the ~~Allowable Value~~-SCP, ensure that SLs are not violated during AOOs and that the consequences of ~~Postulated Accidents (PAs)~~ will be acceptable, ~~providing provided~~ the unit is operated from within the LCOs at the onset of the PA and the equipment functions as designed.

~~Digital~~Within the PSMS controllers, Nominal Trip Setpoints, Time Constants and Time Delays are digital settings maintained in non-volatile software memory within each RPS train. ~~Digital settings have no potential for variation due to time, environmental drift or component aging; therefore, these digital settings have no surveillance tolerance.~~ Each ~~train is~~PSMS controller has continuous automatic self-tested continuously on line to verify testing, which verifies that the digital Nominal Trip Setpoint and Time Constant settings are correct. ~~ESFAS Trip Setpoints~~Nominal Trip Setpoints and Time Constants are also verified periodically through ~~a diverse software memory integrity test, which is the MIC which must be conducted with the RPS train affected PSMS controller out of service.~~ A designated instrument channel is taken out of service for periodic ~~calibration~~-CHANNEL CALIBRATION. SRs for the channels and trains are specified in the SR section.

The Allowable Value is the maximum deviation that can be measured during CHANNEL CALIBRATION, whereby the channel is considered OPERABLE. This value includes the deviations that are included in the

calculations that determined the Nominal Trip Setpoint. The “expected as-found value” shall be as specified in the plant-specific setpoint analysis. The expected as-found value reflects the expected normal drift of actual plant equipment, so that a degraded device can be identified before the Allowable Value limit is reached. The expected as-found value is also referred to as the Performance Test Acceptance Criteria (PTAC). The PTAC, recorded and maintained in a document established by the SCP, is applicable to automatic protection instrumentation functions for Reactor Trip, ESFAS actuation and permissive interlocks.

ESFAS and SLS

The ESFAS and SLS equipment ~~is~~are used for the decision logic processing of outputs from the RPS. ~~The SLS is also used for manual control of ESF components for accident mitigation and to achieve safe shutdown. To meet the redundancy requirements~~single failure criteria and accommodate on-line maintenance for four train ESF systems, four trains of ESFAS-SLS, each performing the same functions, are provided. If one train is taken out of service for maintenance or test purposes, the remaining trains will provide ESF actuation for the unit. Two train ESF systems are actuated by Trains A and D, or B and C of the ESFAS-SLS.

Each train is packaged in its own cabinet for physical and electrical separation to satisfy separation and independence requirements. ~~In addition, each train provides qualified features, such as separate function processors and communication processors, to ensure communications independence.~~

The ESFAS ~~and~~ SLS performs the decision logic for most ESF equipment actuation; generates the electrical output signals that initiate the required actuation; and provides the status, permissive, and annunciator output signals to the ~~main control room~~MCR of the unit.

The ~~bistable outputs~~digital output signals from all trains of the RPS are sensed by each ESFAS train and combined into logic that represent combinations indicative of various transients. If a required logic combination is completed, the ESFAS train will send actuation signals via the Safety Bus to its respective SLS train. The SLS actuates those components whose aggregate Function best serves to alleviate the condition and restore the unit to a safe condition. Examples are given in the Applicable Safety Analyses, LCO, and Applicability sections of ~~this~~these Bases. The SLS also actuates ESF components based on manual control signals received from non-safety Operational VDUs, and based on signals from Safety VDUs for the Manual Control of ESF Components Function.

The ESFAS and SLS ~~are continuously automatically~~have continuous automatic self-~~tested while the unit is at power.~~testing. When any one train is taken out of service for manual testing, the remaining trains are

capable of providing unit monitoring and protection until the testing has been completed.

~~The~~The automatic or manual actuation of ESF components is accomplished through solid state Actuation Outputs. The SLS energizes the Actuation Outputs appropriate for the condition of the unit. Each Actuation Output energizes one plant component. Actuation Outputs are tested in conjunction with their respective plant components. This test overlaps with the continuous automatic self-testing.

S-VDU and COM

The Safety VDUs (S-VDU) and Communication Subsystems (COM) provide backup controls for manual initiation of Reactor Trip and ESFAS Functions, and credited controls and indications for the Manual Control of ESF Components.

The S-VDU in each train consists of a VDU and S-VDU processor. There are two COM Subsystems in each train, COM-1 and COM-2.

The S-VDU provides backup controls for Manual Initiation of Reactor Trip (LCO 3.3.1) and ESFAS functions. Manual initiation signals are interfaced from the S-VDU to the RPS and ESFAS through COM-2, where they are combined with corresponding signals from non-safety Operational VDUs (O-VDU), through logic that prioritizes the S-VDU signal. The combined and prioritized S-VDU and O-VDU signals are then interfaced to the RPS or ESFAS where it is combined with the Manual Initiation pushbuttons, which are required by this LCO. These backup S-VDU controls are not credited in determining when the Manual Initiation Function is OPERABLE or in determining the number of required trains. However, these backup controls are considered in the Manual Initiation Function Completion Times for the Required Actions.

The S-VDU provides credited safety related displays and controls for the Manual Control of ESF Components Function. This Function supports the ESFAS and is used to achieve and maintain safe shutdown (e.g., LCO 3.5.2 for Safety Injection). Component control signals are interfaced from the S-VDU to the SLS through COM-2, where they are combined with corresponding signals from non-safety Operational VDUs (O-VDU), through logic that prioritizes the S-VDU signal. The combined and prioritized S-VDU and O-VDU signals are then interfaced to the SLS. Component position feedback signals for status displays are interfaced from the SLS to the S-VDU.

To meet the single failure criteria and accommodate on-line maintenance, for four train ESF systems, four trains of S-VDU and COM-2 are provided, each performing the same functions. If one train is taken out of service for maintenance or test purposes, the remaining trains will provide displays and manual controls for the unit. The S-VDU and COM-2 for Trains A and D, or Trains B and C support ESF systems with only two trains.

The S-VDU and COM-2 for each train are packaged in their own cabinet for physical and electrical separation to satisfy separation and independence requirements.

The S-VDU and COM-2 have continuous automatic self-testing while in service. When any one train is taken out of service for manual testing, the remaining trains are capable of providing unit monitoring and protection until the testing has been completed.

COM-1 provides signal interfaces from the ESFAS and SLS to the PCMS for non-safety functions only, such as the display of ESF component position on non-safety Operational VDUs (O-VDU). Therefore, there are no operability requirements for COM-1.

APPLICABLE
SAFETY
ANALYSES, LCO,
and APPLICABILITY

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. For example, Low Pressurizer Pressure is a primary actuation signal for small loss of coolant accidents (LOCAs) and a backup actuation signal for steam line breaks (SLBs) outside containment. Functions such as ~~manual initiation~~ Manual Initiation, not specifically credited in the accident safety analysis, are qualitatively credited in the safety analysis and the NRC staff approved licensing basis for the unit. These Functions may provide protection for conditions that do not require dynamic transient analysis to demonstrate Function performance. These Functions may also serve as backups to Functions that were credited in the accident analysis (Ref. 3).

The LCO requires all instrumentation performing an ESFAS Function, listed in Table 3.3.2-1 in the accompanying LCO, to be OPERABLE. A channel is OPERABLE provided the "as-found" value measured during surveillance testing, does not exceed its associated Allowable Value. ~~A trip setpoint may be set more conservative than the Trip Setpoint as necessary in response to plant conditions.~~ and provided the "as-left" value is within the specified calibration tolerance at the completion of each CHANNEL CALIBRATION. For analog measurements, Allowable Values are defined in terms pertinent to the five channel calibration settings 0%, 25%, 50%, 75% and 100%. For binary measurements there is one Allowable Value defined in terms pertinent to the state change at the Nominal Trip Setpoint. A Nominal Trip Setpoint is set more conservative than the Allowable Value to account for channel uncertainties. Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

The LCO generally requires OPERABILITY of two or three channels in each instrumentation ~~function~~ Function, two or three trains of Manual Initiation, and two or three trains in each logic ~~and manual initiation~~

~~function. The two-out-of-three and the two-out-of-four configurations allow~~Function. Three OPERABLE instrumentation channels in a two-out-of-three configuration are required when one ESFAS channel is also used as a control system input. When there are three or more OPERABLE channels, the SSA within the control system prevents the possibility of a shared channel failing in such a manner that it creates a transient that requires ESFAS action. The input failure is considered a single failure in the ESFAS and ESFAS remains capable of providing its protective function with the remaining two OPERABLE channels. The SSA ensures there is no potential for control system and protection system interaction that could simultaneously create a need for ESFAS initiation and disable one ESFAS channel. When there are less than three OPERABLE channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for shared channels, when there are only three required channels.

The two-out-of-three configuration allows one channel to be tripped during maintenance or testing without causing an ESFAS initiation. Two or three ~~trains of logic or manual initiation channels are required and~~ Manual Initiation functions are required to ensure no single random failure disables the ESFAS. The required channels of ESFAS instrumentation provide unit protection in the event of any of the analyzed accidents.

Due to redundant components within the PSMS, such as controllers, communication links and power supplies, an inoperable component may or may not result in an inoperable channel or train. Where an inoperable component results in an inoperable required channel or train, LCOs are entered. For inoperable components that do not result in inoperable channels or trains, LCOs are not entered.

ESFAS protection functions are as follows:

1. ECCS Actuation

ECCS Actuation (ECCS) provides two primary functions:

1. Primary side water addition to ensure maintenance or recovery of ~~reactor vessel water level~~Reactor Vessel Water Level (coverage of the active fuel for heat removal, clad integrity, and for limiting peak clad temperature to < 2200°F), and
2. Boration to ensure recovery and maintenance of SDM ($k_{\text{eff}} < 1.0$).

These functions are necessary to mitigate the effects of high energy line breaks (HELBs) both inside and outside of containment. The ECCS signal is also used to initiate other Functions such as:

- Phase A Isolation,
- Containment Purge Isolation,

- Reactor Trip,
- Feedwater Isolation,
- Start of Emergency Feedwater (EFW) pumps,
- ~~Main Control Room~~MCR Isolation, and
- Reactor Coolant Pump Trip.

These other functions ensure:

- Isolation of nonessential systems through containment penetrations,
- Trip of the reactor to limit power generation,
- Isolation of main feedwater (MFW) to limit secondary side mass losses,
- Start of EFW to ensure secondary side cooling capability,
- Isolation of the ~~main control room~~MCR to ensure habitability, and
- Trip of the Reactor Coolant Pump to prevent the unexpected Reactor Coolant Pump Trip after a small break LOCA.

a. ECCS Actuation - Manual Initiation

The LCO requires three trains to be OPERABLE. The operator can initiate ECCS at any time by using any two out of four ECCS - Manual Initiation switches in the ~~main control room~~MCR. This action will cause actuation of all components in the same manner as any of the automatic actuation signals.

The LCO for the Manual Initiation Function ensures the proper amount of redundancy is maintained in the manual ESFAS actuation circuitry to ensure the operator has manual ESFAS initiation capability.

Each train consists of one push button and the interconnecting wiring to the actuation logic cabinet. Each push button actuates its own train directly. A signal from each pushbutton is also interfaced to all other trains via internal PSMS communication links. In addition to direct actuation by its own train pushbutton, each train is also actuated by two out of three Manual Initiation signals received from the other trains. The signals from the other trains are not credited in determining when the Manual Initiation Function is OPERABLE or in determining the number of required trains. However, these additional signals are considered in the Completion Times for the Required Actions.

b. ECCS Actuation - Actuation Logic and Actuation Outputs

This LCO requires three trains to be OPERABLE. Actuation logic consists of all circuitry housed within the actuation subsystems, including the actuation output devices responsible for actuating the ESF equipment.

Manual and automatic initiation of ECCS must be OPERABLE in MODES 1, 2, and 3. In these MODES, there is sufficient energy in the primary and secondary systems to warrant automatic initiation of ESF systems. Manual Initiation is also required in MODE 4 even though automatic actuation is not required. In this MODE, adequate time is available to manually actuate required components in the event of a PA, but because of the large number of components actuated on ~~a~~an ECCS, actuation is simplified by the use of the manual actuation push buttons. Actuation Logic and ~~actuation outputs~~Actuation Outputs must be OPERABLE in MODE 4 to support system level ~~manual initiation~~Manual Initiation.

These Functions are not required to be OPERABLE in MODES 5 and 6 because 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. Unit pressure and temperature are very low and many ESF components are administratively locked out or otherwise prevented from actuating to prevent inadvertent over-pressurization of unit systems.

c. ECCS Actuation - High Containment Pressure

This signal provides protection against the following accidents:

- SLB inside containment,
- LOCA, and
- Feed line break inside containment.

High Containment Pressure provides no input to any control functions. There are four High Containment Pressure channels in a two-out-of-four logic configuration. Three OPERABLE channels are sufficient to satisfy protective requirements with a two-out-of-three logic. The transmitters (d/p cells) and electronics are located outside of containment with the sensing line (high pressure side of the transmitter) located inside containment.

Thus, the high pressure Function will not experience any adverse environmental conditions and the Nominal Trip Setpoint reflects only steady state instrument uncertainties.

High Containment Pressure must be OPERABLE in MODES 1, 2, and 3 ~~when~~. In these MODES, there is sufficient energy in the primary and secondary systems to pressurize the containment following a pipe break. In MODES 4, 5, and 6, there is insufficient energy in the primary or secondary systems to pressurize the containment.

d. ECCS Actuation - Low Pressurizer Pressure

This signal provides protection against the following accidents:

- Inadvertent opening of a steam generator (SG) relief or safety valve,
- SLB,
- A spectrum of rod cluster control assembly ejection accidents (rod ejection),
- Inadvertent opening of a pressurizer relief or safety valve,
- LOCAs, and
- SG Tube Rupture.

There are four Low Pressurizer Pressure channels in a two-out-of-four logic configuration. Pressurizer Pressure provides both control and protection functions: input to the Pressurizer Pressure Control System, ~~reactor-trip~~ Reactor Trip, and ECCS. The interface from the safety channels in the PSMS to the PCMS is through the Signal ~~Selector~~ Selection Algorithm (SSA). The When three or more Low Pressurizer Pressure channels are OPERABLE, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three channels total must be OPERABLE. When there are less than three OPERABLE Low Pressurizer Pressure channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for shared Low Pressurizer Pressure channels.

The transmitters are located inside containment, with the taps in the vapor space region of the pressurizer, and thus possibly experiencing adverse environmental conditions (LOCA, SLB

inside containment, rod ejection). Therefore, the Nominal Trip Setpoint reflects the inclusion of both steady state and adverse environmental instrument uncertainties.

This Function must be OPERABLE in MODES 1, and 2, and in MODE 3 (above the P-11) setpoint to mitigate the consequences of an HELB inside containment. This signal may be manually ~~blocked~~ bypassed by the operator in MODE 3 below the P-11 setpoint. Automatic ECCS ~~actuation~~ Actuation below this pressure setpoint is then performed by the High Containment Pressure signal.

This Function is not required to be OPERABLE in MODE 3 below the P-11 setpoint. —, because the plant is in hot standby in preparation for a startup or shutdown process. Under hot standby conditions, reactor power is limited to decay heat so LOCA is not a critical condition in this situation. For SLB, the RCS boron concentration is higher (larger shutdown margin) and the moderator density coefficient is smaller due to the higher boron concentration compared to the FSAR Chapter 15 analysis. Thus, there is no need for automatic ECCS Actuation under these less limiting conditions. Therefore, when shutting down, the Low Pressurizer Pressure ECCS signal can be bypassed in MODE 3 below the P-11 setpoint. There is sufficient time margin for manual ECCS Actuation, if necessary. When starting up, the Low Pressurizer Pressure ECCS signal is automatically enabled above the P-11 setpoint.

Other ESF functions are used to detect accident conditions and actuate the ESF systems in this MODE. In MODES 4, 5, and 6, this Function is not needed for accident detection and mitigation.

e. ECCS Actuation - Low Main Steam Line Pressure

Low Main Steam Line Pressure provides protection against the following accidents:

- SLB,
- Feed line break, and
- Inadvertent opening of an SG relief or an SG safety valve.

~~Low Main Steam Line Pressure provides no input to any control functions.~~—There are four Low Main Steam Line Pressure channels on each steam line in a two-out-of-four logic configuration. Main Steam Line Pressure provides control inputs to the Steam Generator Pressure Control System, and protection inputs to ECCS and Main Steam Line Isolation protective functions. The interface from the safety channels in the PSMS to the PCMS is through the Signal Selection Algorithm (SSA).

When three or more Main Steam Line Pressure channels are OPERABLE, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three OPERABLE channels on each steam line are sufficient to satisfy the protective requirements with a two-out-of-three logic on each steam line. When there are less than three OPERABLE Main Steam Line Pressure channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for shared Main Steam Line Pressure channels.

~~This Function is anticipatory and has a typical lead/lag ratio of 50/5~~ dynamic transfer function. The Time Constants for this Function are recorded and maintained in a document established by the Setpoint Control Program (SCP).

Low Main Steam Line Pressure must be OPERABLE in ~~MODES MODES 1, and 2, and and MODE 3~~ (above the P-11) ~~when setpoint. In these MODES,~~ a secondary side break or stuck open valve could result in the rapid depressurization of the steam lines. This signal may be ~~manually blocked~~ bypassed by the operator in MODE 3 below the P-11 setpoint. ~~Below P-11, feed line break is not a concern. Inside containment SLB will be terminated by automatic ECCS actuation via High Containment Pressure, and outside containment SLB will be terminated by the High Main Steam Line Pressure Negative Rate signal for main steam line isolation.~~

This Function is not required to be OPERABLE in MODE 3 below the P-11 setpoint because the plant is in hot standby in preparation for a startup or shutdown process. Under hot standby conditions, the RCS boron concentration is higher (larger shutdown margin) and the moderate density coefficient is smaller due to the higher boron concentration compared to the FSAR Chapter 15 analysis. Thus, there is no need for automatic ECCS Actuation under these less limiting conditions. Therefore, when shutting down, the Low Main Steam Line Pressure ECCS signal can be bypassed in MODE 3 below the P-11 setpoint. There is sufficient time margin for manual ECCS Actuation, if necessary. However, considering the potential impact to containment integrity due to pressure increase from a SLB, the High Main Steam Line Pressure Negative Rate signal is required to be OPERABLE in MODE 3 below the P-11 setpoint to provide automatic Main Steam Line Isolation. The High Main Steam Line Pressure Negative Rate signal is automatically enabled when the Low Main Steam Line Pressure ECCS signal is bypassed. When starting up, the Low Main Steam Line Pressure ECCS signal is

automatically enabled above the P-11 setpoint, and the High Main Steam Line Pressure Negative Rate signal is automatically disabled.

This Function is not required to be OPERABLE in MODE 4, 5, or 6 because there is insufficient energy in the secondary side of the unit to cause an accident.

2. Containment Spray

Containment Spray provides two primary functions:

1. Lowers containment pressure and temperature after an HELB in containment, and
2. Reduces the amount of radioactive iodine in the containment atmosphere.

These functions are necessary to:

- Ensure the pressure boundary integrity of the containment structure,
- Limit the release of radioactive iodine to the environment in the event of a failure of the containment structure, and
- Minimize corrosion of the components and systems inside containment following a LOCA.

The ~~containment spray~~ Containment Spray actuation signal starts the containment spray pumps and aligns the discharge of the pumps to the containment spray nozzle headers in the upper levels of containment. Containment spray is actuated manually or by High 3 Containment Pressure.

a. Containment Spray - Manual Initiation

The operator can initiate ~~containment spray~~ Containment Spray at any time from the ~~main control room~~ MCR by simultaneously actuating two ~~containment spray~~ Containment Spray actuation switches per train for any two out of four trains. Because an inadvertent actuation of ~~containment spray~~ Containment Spray could have such serious consequences, two switches must be actuated simultaneously concurrently to initiate ~~containment spray~~ Containment Spray for each train. There are four sets of two switches each in the ~~main control room~~ MCR. Simultaneously Concurrently actuating the two switches will actuate ~~containment spray~~ Containment Spray in each train in the same manner as the automatic actuation signal. ~~Two~~ Therefore, two Manual Initiation switches in ~~each of three trains~~ a train are required to be OPERABLE for a train to ~~ensure no single failure~~

~~disables the Manual Initiation Function.~~ be OPERABLE. Note that Manual Initiation of ~~containment spray~~ Containment Spray also actuates Phase B ~~containment isolation~~ Containment Isolation.

Each train consists of two push buttons and the interconnecting wiring to the actuation logic cabinet. Each push button actuates its own train directly through two out of two logic. A signal from the output of this two out of two logic is also interfaced to all other trains via internal PSMS communication links. In addition to direct actuation by its own train pushbuttons, each train is also actuated by two out of three Manual Initiation signals received from the other trains. The signals from the other trains are not credited in the determining when the Manual Initiation Function is OPERABLE or in determining the number of required trains. However, these additional signals are considered in the Completion Times for the Required Actions.

For Containment Spray only two 50% trains are needed to achieve 100% capacity; therefore, only three of four trains of manual initiation are needed to meet the single failure criteria. However, for Phase B Containment Isolation, although only two trains are needed to meet the single failure criteria for any single containment penetration, the containment penetrations are distributed to all four trains. Therefore, since Containment Spray - Manual Initiation this is a combined Function for Containment Spray and Phase B Containment Isolation, two switches in each of all four trains are required to be OPERABLE.

b. Containment Spray - Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b.

Manual and automatic initiation of ~~containment spray~~ Containment Spray must be OPERABLE in MODES 1, 2, and 3 ~~when.~~ In these MODES, there is a potential for an accident to occur, and sufficient energy in the primary or secondary systems to pose a threat to containment integrity due to overpressure conditions. Manual initiation is also required in MODE 4, even though automatic actuation is not required. In this MODE, adequate time is available to manually actuate required components in the event of a PA. However, because of the large number of components actuated on a ~~containment spray~~ Containment Spray, actuation is simplified by the use of the manual actuation push buttons. Actuation Logic and Actuation Outputs must be OPERABLE in MODE 4 to support system level ~~manual initiation.~~ Manual Initiation. In MODES 5 and 6, there is insufficient energy in the primary and secondary systems to result in containment overpressure. In MODES 5 and 6, there is

also adequate time for the operators to evaluate unit conditions and respond, to mitigate the consequences of abnormal conditions by manually starting individual components.

c. Containment Spray - High-3 Containment Pressure

This signal provides protection against a LOCA or an SLB inside containment. The transmitters (d/p cells) are located outside of containment with the sensing line (high pressure side of the transmitter) located inside containment. The transmitters and electronics are located outside of containment. Thus, they will not experience any adverse environmental conditions and the Nominal Trip Setpoint reflects only steady state instrument uncertainties.

High-3 Containment Pressure has four channels in a two-out-of-four logic configuration. Three OPERABLE channels are sufficient to satisfy protective requirements with two-out-of-three logic.

High-3 Containment Pressure must be OPERABLE in MODES 1, 2, and 3 ~~when~~. In these MODES, there is sufficient energy in the primary and secondary sides to pressurize the containment following a pipe break. In MODES 4, 5, and 6, there is insufficient energy in the primary and secondary sides to pressurize the containment and reach the High-3 Containment Pressure setpoint.

3. Containment Isolation

Containment Isolation provides isolation of the containment atmosphere, and all process systems that penetrate containment, from the environment. This Function is necessary to prevent or limit the release of radioactivity to the environment in the event of a large break LOCA.

For any single containment penetration, isolation can be accomplished by either of two redundant trains. However, all ~~containment isolation~~ Containment Isolation functions are distributed among all four ESFAS trains.

There are two separate Containment Isolation signals, Phase A and Phase B. Phase A ~~isolation~~ isolation isolates all automatically isolable process lines, except component cooling water (CCW), at a relatively low containment pressure indicative of primary or secondary system leaks. For these types of events, forced circulation cooling using the reactor coolant pumps (RCPs) and SGs is the preferred (but not required) method of decay heat removal. Since CCW is required to support RCP operation, not isolating CCW on the low pressure Phase A signal enhances unit safety by allowing

operators to use forced RCS circulation to cool the unit. Isolating CCW on the low pressure signal may force the use of feed and bleed cooling, which could prove more difficult to control.

Phase A ~~containment isolation~~ Containment Isolation is actuated automatically by ECCS Actuation, or manually via the Actuation Logic. All process lines penetrating containment, with the exception of CCW, are isolated.

CCW is not isolated at this time to permit continued operation of the RCPs with cooling water flow to the thermal barrier heat exchangers and air or oil coolers. All process lines not equipped with remote operated isolation valves are manually closed, or otherwise isolated, prior to reaching MODE 4.

Manual Phase A Containment Isolation is accomplished by two switches in the ~~main control room~~ MCR. Each push button actuates its own train directly. ~~A signal from each pushbutton is also interfaced to all other trains via internal PSMS communication links. In addition to direct actuation by its own train pushbutton, each train is also actuated by two out of three Manual Initiation signals received from the other trains.~~

Note that manual actuation of Phase A Containment Isolation also actuates Containment Purge Isolation.

The Phase B signal isolates CCW. This occurs at a relatively high containment pressure that is indicative of a large break LOCA or an SLB. For these events, forced circulation using the RCPs is no longer desirable. Isolating the CCW at the higher pressure does not pose a challenge to the containment boundary because the CCW System is a closed loop inside containment. Although some system components do not meet all of the ASME Code requirements applied to the containment itself, the system is continuously pressurized to a pressure greater than the Phase B setpoint. Thus, routine operation demonstrates the integrity of the system pressure boundary for pressures exceeding the Phase B setpoint. Furthermore, because system pressure exceeds the Phase B setpoint, any system leakage prior to initiation of Phase B ~~isolation~~ Isolation would be into containment. Therefore, the combination of CCW System design and Phase B ~~isolation~~ Isolation ensures the CCW System is not a potential path for radioactive release from containment.

Phase B ~~containment isolation~~ Containment Isolation is actuated by the same signals that actuate Containment Spray including High-3 Containment Pressure, or Containment Spray - Manual Initiation, via the Actuation Logic. For containment pressure to reach a value high enough to actuate High-3 Containment Pressure, a large break LOCA or SLB must have occurred, and ~~containment spray~~ Containment Spray must have been actuated. RCP operation will no longer be required and CCW to the RCPs is, therefore, no

longer necessary. The RCPs can be operated with seal injection flow alone and without CCW flow to the thermal barrier heat exchanger.

Manual Phase B Containment Isolation is accomplished by the same switches that actuate Containment Spray. When the two switches per train for two out of four trains -are actuated ~~simultaneously~~concurrently, Phase B Containment Isolation and Containment Spray will be actuated in all trains.

a. Containment Isolation - Phase A Isolation

(1) Phase A Isolation - Manual Initiation

Manual Phase A Containment Isolation is actuated by two switches in the ~~main control room~~MCR. Each push button actuates its own train directly.

Note that ~~manual initiation~~Manual Initiation of Phase A Containment Isolation also actuates Containment Purge Isolation.

(2) Phase A Isolation - Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. Phase A Isolation valves are distributed to Trains A and D. Both trains must be OPERABLE.

Manual and automatic initiation of Phase A Containment Isolation must be OPERABLE in MODES 1, 2, and 3, ~~when~~ In these MODES, there is a potential for an accident to occur. Manual ~~initiation~~Initiation is also required in MODE 4 even though automatic actuation is not required. In this MODE, adequate time is available to manually actuate required components in the event of a PA, but because of the large number of components actuated on a Phase A Containment Isolation, actuation is simplified by the use of the manual actuation push buttons. Actuation Logic and ~~actuation outputs~~Actuation Outputs must be OPERABLE in MODE 4 to support system level ~~manual initiation~~Manual Initiation. In MODES 5 and 6, there is insufficient energy in the primary or secondary systems to pressurize the containment to require Phase A Containment Isolation. There also is adequate time for the operator to evaluate unit conditions and manually actuate individual isolation valves in response to abnormal or accident conditions.

(3) Phase A Isolation - ECCS Actuation

Phase A Containment Isolation is also initiated by all Functions that initiate ECCS Actuation. The Phase A Containment Isolation requirements for these Functions are the same as the requirements for their ECCS Actuation function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 1, ECCS Actuation, is referenced for all initiating Functions and requirements. Note that all four Containment Isolation trains are actuated when any two out of four ECCS Actuation - Automatic or Manual Initiation signals are actuated.

b. Containment Isolation - Phase B Isolation

Phase B Containment Isolation is accomplished by Manual Initiation, Actuation Logic and Actuation Outputs, and by Containment Pressure channels (the same channels that actuate Containment Spray, Function 2).

(1) Phase B Isolation - Manual Initiation

Phase B Containment Isolation is manually initiated by Containment Spray – Manual Initiation. The Phase B Containment Isolation requirements for these Functions are the same as the requirements for their Containment Spray function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 2, Containment Spray, is referenced for all initiating Functions and requirements.

Note that all four Phase B Containment Isolation trains are actuated when any two out of four Containment Spray – Manual Initiation signals are actuated.

(2) Phase B Isolation - Actuation Logic and Actuation Outputs

Manual and automatic initiation of Phase B ~~containment isolation~~ Containment Isolation must be OPERABLE in MODES 1, 2, and 3, ~~when~~ In these MODES, there is a potential for an accident to occur. Manual ~~initiation~~ Initiation is also required in MODE 4 even though automatic actuation is not required. In this MODE, adequate time is available to manually actuate required components in the event of a PA. However, because of the large number of components actuated on a Phase B ~~containment isolation~~ Containment Isolation, actuation is simplified by the use of the manual actuation push buttons. Actuation Logic and ~~actuation outputs must be~~ Actuation Outputs must be OPERABLE in MODE 4 to support system level ~~manual initiation~~ Manual Initiation. In MODES 5 and 6, there is insufficient energy in the primary or secondary systems to pressurize the containment to require Phase B ~~containment isolation~~ Containment Isolation. There also is adequate time

for the operator to evaluate unit conditions and manually actuate individual isolation valves in response to abnormal or accident conditions.

Four trains of Phase B Containment Isolation - Actuation Logic and Actuation Outputs must be ~~operable~~OPERABLE due to the distribution of ~~containment isolation valves~~Containment Isolation Valves to all four trains.

4. Main Steam Line Isolation

Isolation of the main steam lines provides protection in the event of an SLB inside or outside containment. Rapid isolation of the main steam lines will limit the steam break accident to the blowdown from one SG, at most. For an SLB upstream of the main steam isolation valves (MSIVs), inside or outside of containment, closure of the MSIVs limits the accident to the blowdown from only the affected SG. For an SLB downstream of the MSIVs, closure of the MSIVs terminates the accident as soon as the main steam lines depressurize. Main Steam Line Isolation also mitigates the effects of a feed line break and ensures a source of steam for the turbine driven EFW pump during a feed line break.

Main Steam Line Isolation components are distributed to Trains A and D.

a. Main Steam Line Isolation - Manual Initiation

Manual ~~initiation~~Initiation of Main Steam Line Isolation can be accomplished from the ~~main control room~~MCR. There are two switches in the ~~main control room~~MCR, one for each train. ~~Either~~Each MSIV is actuated from both trains. Therefore, either switch can initiate action to immediately close all MSIVs. The LCO requires two trains to be OPERABLE.

b. Main Steam Line Isolation - Actuation Logic and Actuation Outputs

Actuation Logic and ~~actuation outputs~~Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. Main Steam Line Isolation valves are distributed to Trains A and D. Both trains must be OPERABLE.

Manual Initiation and ~~automatic initiation~~Actuation Logic and Actuation Outputs of Main Steam Line Isolation must be OPERABLE in MODES 1, 2, and 3 ~~when~~. In these MODES, there is sufficient energy in the RCS and SGs to have an SLB or other accident. This could result in the release of significant quantities of energy and cause a cooldown of the primary system. ~~The Main Steam Line Isolation Function is required in MODES 2 and 3 unless all MSIVs~~

~~are closed.~~ In MODES 4, 5, and 6, there is insufficient energy in the RCS and SGs to experience an SLB or other accident releasing significant quantities of energy.

c. Main Steam Line Isolation - High-High Containment Pressure

This Function actuates closure of the MSIVs in the event of a LOCA or an SLB inside containment to maintain at least one unfaulted SG as a heat sink for the reactor, and to limit the mass and energy release to containment. The transmitters (d/p cells) are located outside containment with the sensing line (high pressure side of the transmitter) located inside containment. High-High Containment Pressure provides no input to any control functions. There are four High-High Containment Pressure channels in a two-out-of-four logic configuration. Three OPERABLE channels are sufficient to satisfy protective requirements with two-out-of-three logic. The transmitters and electronics are located outside of containment. ~~Thus~~ Therefore, they will not experience any adverse environmental conditions; ~~and the~~. The Nominal Trip Setpoint reflects only steady state instrument uncertainties.

High-High Containment Pressure must be OPERABLE in MODES 1, 2, and 3, ~~when~~. In these MODES, there is sufficient energy in the primary and secondary side to pressurize the containment following a pipe break. This would cause a significant increase in the containment pressure, thus allowing detection and closure of the MSIVs. ~~The Main Steam Line Isolation Function remains OPERABLE in MODES 2 and 3 unless all MSIVs are closed.~~ In MODES 4, 5, and 6, there is not enough energy in the primary and secondary sides to pressurize the containment to the High-High Containment Pressure setpoint.

d. Main Steam Line Isolation - Main Steam Line Pressure

(1) Low Main Steam Line Pressure

Low Main Steam Line Pressure provides closure of the MSIVs in the event of an SLB to maintain at least ~~one~~ two unfaulted ~~SG~~ SGs as a heat sink for the reactor, and to limit the mass and energy release to containment. This Function provides closure of the MSIVs in the event of a feed line break to ensure a supply of steam for the turbine driven EFW pump. Low Main Steam Line Pressure was discussed previously under ECCS Function 1.e.

Low Main Steam Line Pressure Function must be OPERABLE in MODES 1 and 2, and MODE 3 above the P-11 setpoint, in these MODES, a secondary side break, spuriously opened valve, or stuck open valve could result in the rapid depressurization of the steam lines. This signal

may be manually bypassed by the operator in MODE 3 below the P-11 setpoint. In MODE 3 below the P-11 setpoint, an SLB inside containment will be terminated by automatic actuation via the High-High Containment Pressure signal. Stuck valve transients and SLBs outside containment will be terminated by the High Main Steam Line Pressure Negative Rate signal for Main Steam Line Isolation in MODE 3 below the P-11 setpoint when ECCS has been manually bypassed.

This Function is not required to be OPERABLE in MODES 4, 5, and 6 because there is insufficient energy in the secondary side of the unit to have an accident.

This Function has a dynamic transfer function. The Time Constants for this Function are recorded and maintained in a document established by the Setpoint Control Program (SCP).

(2) High Main Steam Line Pressure Negative Rate

High Main Steam Line Pressure Negative Rate provides closure of the all MSIVs for an SLB in MODE 3 below the P-11 setpoint, to maintain at least two unfaulted SGs as a heat sink for the reactor, and to limit the mass and energy release to containment. When the operator manually bypasses the Low Main Steam Line Pressure Main Steam Line Isolation signal in MODE 3 below the P-11 setpoint, the High Main Steam Line Pressure Negative Rate signal is automatically enabled. Main Steam Line Pressure provides both control and protection functions, as described previously under ECCS Function 1.e. There are four High Main Steam Line Pressure Negative Rate signals in a two-out-of-four logic configuration. Three OPERABLE channels are sufficient to satisfy requirements with a two-out-of-three logic on each steam line.

~~Low~~High Main Steam Line Pressure ~~Function~~Negative Rate must be OPERABLE in MODES ~~1, 2, and 3~~ (above/below the P-11), ~~with any main steam valve open, when setpoint. In this MODE,~~ a secondary side break or stuck open valve could result in the rapid depressurization of the main steam line(s). ~~This signal may be manually blocked by the operator below). Above the P-11 setpoint. Below P-11, an inside containment SLB will be terminated by automatic actuation via High-High Containment Pressure. Stuck valve transients, this signal is automatically disabled and outside containment SLBs will be terminated by the High/Low Main Steam Line Pressure Negative Rate signal for Steam Line Isolation below P-11 when ECCS has been manually blocked. is automatically enabled.~~ The Main Steam Line Isolation

Function is required ~~in MODES 2 and 3 unless all MSIVs are closed. This Function is not required~~ to be OPERABLE in MODES 1, 2 and 3. In MODES 4, 5, and 6 because, there is insufficient energy in the primary and secondary side of the unitsides to have an SLB or other accident.

~~(2) High Main Steam Line Pressure Negative Rate~~

~~High Main Steam Line Pressure Negative Rate provides closure of the MSIVs for an SLB when less than the P-11 setpoint, to maintain at least one unfaulted SG as that would result in a heat sink for the reactor, and to limit the mass and energy release to containment. When the operator manually blocks the Low Main Steam Line Pressure main steam isolation signal when less than the P-11 setpoint, the High Main Steam Line Pressure Negative Rate signal is automatically enabled. High Main Steam Line Pressure Negative Rate provides no input to any control functions. There are four High Main Steam Line Pressure Negative Rate signals in a two-out-of-four logic configuration. Three OPERABLE channels are sufficient to satisfy requirements with a two-out-of-three logic on each steam line of significant enough quantities of energy to cause a cooldown of the RCS.~~

While the transmitters may experience elevated ambient temperatures due to an SLB, the trip function is based on rate of change, not the absolute accuracy of the indicated steam pressure. Therefore, the Nominal Trip Setpoint reflects only steady state instrument uncertainties.

This Function has a dynamic transfer function. The Time Constants for this Function are recorded and maintained in a document established by the Setpoint Control Program (SCP).

All Main Steam Isolation Functions are applicable in MODES 1, 2 and 3 as stated above, regardless of valve position, because the Functions are credited to mitigate spurious valve opening from Operational VDUs. In MODES 4, 5, and 6, these Functions are not required to be OPERABLE, as stated above.

5. Main Feedwater Isolation

~~High Main Steam Line Pressure Negative Rate must be OPERABLE in MODE 3 when less than the P-11 setpoint, when a secondary side break or stuck open valve could result in the rapid depressurization of the main steam line(s). In MODES 1 and 2, and in MODE 3, when above the P-11 setpoint, this signal is automatically disabled and the Low Main Steam Line Pressure signal is automatically enabled. The Main Steam Line Isolation Function is required to be~~

~~OPERABLE in MODES 2 and 3 unless all MSIVs are closed. In MODES 4, 5, and 6, there is insufficient energy in the primary and secondary sides to have an SLB or other accident that would result in a release of significant enough quantities of energy to cause a cooldown of the RCS.~~

~~While the transmitters may experience elevated ambient temperatures due to an SLB, the trip function is based on rate of change, not the absolute accuracy of the indicated steam pressure. Therefore, the Trip Setpoint reflects only steady state instrument uncertainties.~~

~~5. Main Feedwater Isolation~~

~~5A. Main Feedwater Regulation Valve Closure~~

~~The primary function of the Main Feedwater Regulation Valve Closure is to stop the excessive flow of feedwater into the SGs. This Function is necessary to mitigate the effects of a high water level in the SGs, which could result in excessive cooldown of the primary system.~~

~~This Function is actuated when T_{avg} is less than the low setpoint coincident with reactor trip, and closes all the main Feedwater Regulation valves.~~

~~a. Main Feedwater Isolation – Low T_{avg}~~

~~There are four Low T_{avg} channels per loop in a two-out-of-four configuration. Three channels of T_{avg} per loop are required to be OPERABLE. The T_{avg} channels are combined in a logic such that two-out-of-three channels tripped cause a trip for the parameter. The accidents that this Function protects against cause reduction of T_{avg} in the entire primary system. Therefore, the provision of two OPERABLE channels in a two-out-of-four configuration ensures no single random failure disables the Low T_{avg} Function. The T_{avg} channels provide control inputs interfaced from the PSMS to the PCMS through an SSA. But the control function cannot initiate events that the Function acts to mitigate. Therefore, the SSA is not required to address control protection interaction issues.~~

~~With the T_{avg} resistance temperature detectors (RTDs) located inside the containment, it is possible for them to experience adverse environmental conditions during an SLB event. Therefore, the Trip Setpoint reflects both steady state and adverse environmental instrumental uncertainties.~~

~~The Main Feedwater Isolation – Low T_{avg} signal is enabled by the Main Feedwater Isolation – Reactor Trip, P-4 interlock, described below.~~

~~Coincident with Reactor Trip, P-4~~

~~The Main Feedwater Isolation – Low T_{avg} signal is enabled when the reactor is tripped as indicated by the P-4 interlock. Therefore, the requirements for the P-4 interlock are not repeated in Table 3.3.2-1. Instead, Function 11, Reactor Trip P-4, is referenced for the initiating Function and requirements. Note that all four Turbine Trip actuation trains are actuated when any two out of four RTB trains are actuated.~~

~~5B. Main Feedwater Isolation~~

The primary function of the Main Feedwater Isolation is to stop the excessive flow of feedwater into the SGs. This Function is necessary to mitigate the effects of a high water level in the SGs, which could result in excessive cooldown of the primary system. The High SG Water Level is due to excessive feedwater flows.

The Function on High-High SG Water Level is actuated when the level in any SG exceeds the high-high setpoint, ~~and.~~

The Main Feedwater Isolation Function performs the following functions:

- Trips the MFW pumps,
- ~~Initiates feedwater isolation, and~~
- Shuts the MFW ~~regulating~~isolation valves, ~~the MFW bypass feedwater regulating valves and the SG water filling control valves.~~
- Shuts the MFW Regulation Valves, the MFW Bypass Regulation Valves, and the SG Water Filling Control Valves.

This Function is actuated by High-High SG Water Level ~~or by~~, an ECCS Actuation signal ~~or manually~~, or Manual Initiation.

The ECCS Actuation signal was discussed previously.

The Function on Low Tavg coincident with Reactor Trip closes all the Main Feedwater Regulation valves.

Main Feedwater Isolation ~~components~~Valves, MFW Regulation Valves, MFW Bypass Regulation Valves, and SG Water Filling Control Valves are distributed to Trains A and D.

a. Main Feedwater Isolation - Manual Initiation

Manual ~~initiation~~Initiation of Main Feedwater Isolation can be accomplished from the ~~main control room~~MCR. There are two switches in the ~~main control room~~MCR, one for each train. ~~Either~~Each of the valves is actuated from both trains. Therefore, either switch can initiate action to immediately ~~close~~actuate all ~~feedwater isolation valves.~~Main Feedwater Isolation Components. The LCO requires two trains to be OPERABLE.

b. Main Feedwater Isolation - Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. All Main Feedwater ~~isolation valves~~isolation Components are distributed to Trains A and D. Both trains must be OPERABLE.

c. Main Feedwater Isolation - High-High Steam Generator Water Level

This signal provides protection against excessive feedwater flow. There are four High-High Steam Generator Water Level channels in a two-out-of-four logic configuration for each Steam Generator. The ESFAS SG ~~water level~~Water Level instruments provide input to the SG Water Level Control System. The

interface from the safety channels in the PSMS to the PCMS is through the Signal ~~Selector~~ Selection Algorithm (SSA). The When there are three or more OPERABLE High-High Steam Generator Water Level channels for each Steam Generator, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three channels total must be OPERABLE. When there are less than three OPERABLE High-High Steam Generator Water Level channels for each Steam Generator, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for High-High Steam Generator Water Level channels, since there are only three required channels for each Steam Generator.

The transmitters (d/p cells) are located inside containment. However, the events that this Function protects against cannot cause a severe environment in containment. Therefore, the Nominal Trip Setpoint reflects only steady state instrument uncertainties.

d. Main Feedwater Isolation - ECCS Actuation

Main Feedwater Isolation is also initiated by all Functions that initiate ECCS Actuation. The Feedwater Isolation Function requirements for these Functions are the same as the requirements for their ECCS Actuation function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead Function 1, ECCS Actuation, is referenced for all initiating functions and requirements. Note that both Main Feedwater Isolation trains are actuated when any two out of four ECCS Actuation - Automatic or Manual Initiation signals are actuated.

e. Main Feedwater Isolation - Low T_{avg}

This Function is actuated when T_{avg} is less than the low setpoint coincident with Reactor Trip. It closes only the Main Feedwater Regulation valves.

There are four Low T_{avg} channels (one per loop) in a two out of four configuration. Three channels of T_{avg} are required to be OPERABLE. The T_{avg} channels are combined in a logic such that two out of three channels cause a trip for the Function. The accidents that this Function protects against cause reduction of T_{avg} in the entire primary system. Therefore, the provision of three OPERABLE channels in a two-out-of-four configuration ensures no single random failure disables the Low T_{avg} Function.

T_{avg} channels provide inputs to both control and protection functions. T_{avg} channels provide control inputs to the Rod Control System, Pressurizer Water Level Control System, and Turbine Bypass Control System. The interface from the safety channels in the PSMS to the PCMS is through the Signal Selection Algorithm (SSA). When three or more T_{avg} channels are OPERABLE, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three channels total must be OPERABLE. When there are less than three OPERABLE T_{avg} channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for shared T_{avg} channels.

With the T_{avg} resistance temperature detectors (RTDs) located inside the containment, it is possible for them to experience adverse environmental conditions during an SLB event. Therefore, the Nominal Trip Setpoint reflects both steady state and adverse environmental instrument uncertainties.

The Main Feedwater Isolation - Low T_{avg} signal is enabled by the Main Feedwater Isolation - Reactor Trip, P-4 interlock, described below.

Coincident with Reactor Trip, P-4

The Main Feedwater Isolation - Low T_{avg} signal is enabled when the reactor is tripped as indicated by the P-4 interlock. Therefore, the requirements for the P-4 interlock are not repeated in Table 3.3.2-1. Instead, Function 11.a, Reactor Trip, P-4, is referenced for the initiating Function and requirements. Note that both Turbine Trip actuation trains, Trains A and D, are actuated when any two-out-of-four RTB trains are actuated.

All Main Feedwater Isolation Functions, except for the sub-function of High-High Steam Generator Water Level, ~~must be OPERABLE in MODES 1 and 2 and 3 except when all,~~ which trips the MFW pumps and closes the MFIVs, MFRVs, MFBRVs and SGWFCVs ~~are closed when the MFW System is in operation,~~ must be OPERABLE in MODE 1, 2 and 3. In MODES 4, 5, and 6, the MFW System is not in service and ~~this Function is~~ the Isolation Functions are not required to be OPERABLE.

The sub-function of the MFW Isolation on High-High Steam Generator Water Level, which trips the MFW pumps and closes the MFIVs and SGWFCVs, must be OPERABLE in MODES 1 and 2, and in MODE 3 (above the P-11) ~~except when all MFIVs, MFRVs, MFBRVs and~~

~~SGWFCVs are closed when the MFW System is in operation. This signal setpoint.~~

~~The sub-function may be manually blocked~~bypassed by the operator ~~below the P-11 setpoint. This function is not required to be OPERABLE~~ in MODE 3 below the P-11 setpoint. This manual bypass is needed to allow control of steam generator water level using the SGWFCVs under these conditions. The MFIVs and SGWFCVs are configured in series such that the feedwater flow rate is limited by the SGWFCV capacity which is a very small fraction of the nominal feedwater flow. The manual bypass is acceptable because expected feedwater flow due to open SGWFCVs is not a critical concern under these conditions. Sufficient time margin exists for manual SGWFCV closure, if necessary. Therefore, manual bypass of the automatic trip of MFW pumps and automatic closure of MFIVs and SGWFCVs on High-High SG Water Level in MODE 3 below the P-11 setpoint is acceptable and necessary to maintain the Steam Generators filled with water in preparation for shutdown conditions (wet layup operation). When starting up, the automatic trip of MFW pumps and automatic closure of MFIVs and SGWFCVs on High-High SG Water Level is automatically enabled above the P-11 setpoint.

These Functions are applicable in MODES 1, 2 and 3 as stated above, regardless of valve position, because the Functions are credited to mitigate spurious valve opening from Operational VDUs. In MODES 4, 5, and 6, the MFW System is not in service and this Function is not required to be OPERABLE.

6. Emergency Feedwater Actuation

The EFW Actuation System is designed to provide a secondary side heat sink for the reactor in the event that the MFW System is not available. The system has four trains, with two motor driven pumps and two turbine driven pumps, making it available during normal unit operation, during a loss of AC power, a loss of MFW, and during a Feedwater System pipe break. The LCO requires three OPERABLE EFW trains. The normal source of water for the EFW System is the Emergency Feedwater pit (EFW pit). This pit has a sufficient capacity to lead the plant safe shutdown. If the water level of EFW pit reached low-low level, operators are given alarm in ~~main control room~~MCR. Then the EFW pumps will be stopped or the water source will be switched to Demineralized Water Storage Tank manually to keep the sufficient EFW if necessary.

a. Emergency Feedwater Actuation - Manual Initiation

Manual ~~initiation~~Initiation of Emergency Feedwater Actuation can be accomplished from the ~~main control room~~MCR. There are four switches in the ~~main control room~~MCR, one for each train. Each switch actuates its own train directly. A signal from

each switch is also interfaced to all other trains via internal PSMS communication links. In addition to direct actuation by its own train switch, each train is also actuated by two out of three Manual Initiation signals received from the other trains. The signals from the other trains are not credited in determining when the Manual Initiation Function is OPERABLE or in determining the number of required trains. However, these additional signals are considered in the Completion Times for the Required Actions. The LCO requires three trains to be OPERABLE.

b. Emergency Feedwater Actuation - Actuation Logic and Actuation Outputs

Actuation Logic and ~~actuation-outputs~~ Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. Three trains must be OPERABLE.

c. Emergency Feedwater Actuation - Low Steam Generator Water Level

Low SG Water Level provides protection against a loss of heat sink. A feed line break, inside or outside of containment, or a loss of MFW, would result in a loss of SG water level. There are four Low SG Water Level channels in a two-out-of-four logic configuration. Low SG Water Level provides input to the SG Level Control System. The interface from the safety channels in the PSMS to the PCMS is through the Signal ~~Selector~~ Selection Algorithm (SSA). The-When three or more Low SG Water Level channels are OPERABLE for each Steam Generator, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three channels total must be OPERABLE. When there are less than three OPERABLE Low SG Water Level channels for each Steam Generator, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for Low SG Water Level channels, since there are only three required channels for each Steam Generator.

With the transmitters (d/p cells) located inside containment and thus possibly experiencing adverse environmental conditions (feed line break), the Nominal Trip Setpoint reflects the inclusion of both steady state and adverse environmental instrument uncertainties.

d. Emergency Feedwater Actuation - ECCS Actuation

An ECCS Actuation signals all four EFW trains. The EFW initiation functions are the same as the requirements for their

ECCS Actuation function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 1, ECCS Actuation, is referenced for all initiating functions and requirements.

e. Emergency Feedwater Actuation - Loss of Offsite Power

A loss of offsite power will be accompanied by a loss of reactor coolant pumping power and the subsequent need for some method of decay heat removal. The loss of offsite power is detected by a voltage drop on each Class 1E bus (4 trains). The voltage drop is detected by three undervoltage devices on each bus, in a two out of three configuration. Loss of ~~power~~Power to a Class 1E bus will actuate its respective EFW train (with either its motor or turbine driven pump). This ensures that, for a sitewide loss of offsite power, at least two SGs contain enough water to serve as the heat sink for reactor decay heat and sensible heat removal following the ~~reactor trip~~Reactor Trip.

The LCO requires three OPERABLE undervoltage devices on each Class 1E bus corresponding to each OPERABLE EFW train.

This Function has Time Delays. The Time Delays for this Function are recorded and maintained in a document established by the Setpoint Control Program (SCP).

Functions 6.a through 6.e must be OPERABLE in MODES 1, 2, and 3 to ensure that the SGs remain the heat sink for the reactor. Low SG Water Level in any operating SG will cause the EFW trains to actuate. The system is aligned so that upon a start of the EFW pump, water immediately begins to flow to the SGs. These Functions do not have to be OPERABLE in MODES 5 and 6 because there is not enough heat being generated in the reactor to require the SGs as a heat sink. In MODE 4, EFW actuation does not need to be OPERABLE because either EFW or residual heat removal (RHR) will already be in operation to remove decay heat or sufficient time is available to manually place either system in operation.

f. Emergency Feedwater Actuation - Trip of All Main Feedwater Pumps

A Trip of all MFW pumps is an indication of a loss of MFW and the subsequent need for some method of decay heat and sensible heat removal to bring the reactor back to no load temperature and pressure. Each motor driven MFW pump is equipped with ~~aredundant~~breaker position sensing devices. An open supply breaker indicates that the pump is not running. Emergency Feedwater Actuation on ~~trip~~Trip of ~~all-main-feedwater pumps~~All Main Feedwater Pumps is an anticipatory function that is not credited in the safety analysis. Therefore, this function does not need to meet the single failure criterion; the LCO

requires one OPERABLE channel per pump (i.e., one of the redundant breaker position sensing devices on each pump). A trip of all MFW pumps actuates all EFW trains to ensure that at least two SGs are available with water to act as the heat sink for the reactor.

This function must be OPERABLE in MODES 1 and 2. This ensures that at least two ~~SG is~~ SGs are provided with water to serve as the heat sink to remove reactor decay heat and sensible heat in the event of an accident. In MODES 3, 4, and 5, the MFW pumps may be normally shut down, and thus ~~neither~~ MFW pump trip is is not indicative of a condition requiring automatic EFW initiation.

7. Emergency Feedwater Isolation

One of the objectives of EFW Isolation is to prevent SG overfill in the event of SGTR. The Other objective of EFW Isolation is to stop the flow of EFW into the affected SG in the event of MSLB. For both objectives, the EFW ~~isolation~~ Isolation Functions are automatically actuated by High SG Water Level signal, or by Low Main Steam Line Pressure signal. The Function may also be actuated manually. ~~EFW Isolation is distributed to Trains A and D~~ The EFW Isolation Function is actuated separately for each SG, either manually or automatically. EFW Isolation valves are distributed to all four trains, with two trains of valves for each SG.

a. Emergency Feedwater Isolation - Manual Initiation

This LCO requires 2 ~~Manual~~ EFW Isolation ~~Actuation~~ Manual Initiation trains for each SG. ~~This Function closes the EFW Isolation Valve for the SG associated with the switches~~ Each Manual Initiation train closes the EFW isolation valve for one train on one SG. Two Manual Initiation trains must be OPERABLE for each SG to ensure each SG can be isolated with a single failure.

b. Emergency Feedwater Isolation - Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. ~~Emergency Feedwater isolation valves are distributed to Trains A and D. Trains A~~ Each Actuation Logic and Actuation Outputs train closes the EFW isolation valve for one train on one SG. Two Actuation Logic and ~~D~~ Actuation Outputs trains for each SG must be OPERABLE to ensure each SG can be isolated with a single failure.

Manual and automatic initiation of EFW Isolation Functions must be OPERABLE in MODES 1, 2 and 3 ~~when~~. In these MODES,

the SGs are in operation. In MODES 4, 5, and 6, SGs are not in service and this Function is not required to be OPERABLE.

c. Emergency Feedwater Isolation - High Steam Generator Water Level Coincident with P-4 signal and No Low Main Steam Line Pressure

This signal provides protection against damaged SG overflow. There are four High Steam Generator Water Level channels in a two-out-of-four logic configuration for each Steam Generator. The ESFAS SG ~~water level~~ Water Level instruments provide input to the SG Water Level Control System. The interface from the safety channels in the PSMS to the PCMS is through the Signal ~~Selector~~ Selection Algorithm (SSA). ~~The~~ When three or more High SG Water Level channels are OPERABLE for each Steam Generator, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three channels total must be OPERABLE. When there are less than three OPERABLE High SG Water Level channels for each Steam Generator, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for High SG Water Level channels, since there are only three required channels for each Steam Generator.

The transmitters (d/p cells) are located inside containment. However, the events that this Function protects against cannot cause a severe environment in containment. Therefore, the Nominal Trip Setpoint reflects only steady state instrument uncertainties.

High Steam Generator Water Level must be OPERABLE in MODES ~~1, 2~~ and 2, and MODE 3 ~~(above the P-11)~~ when setpoint. In these MODES, the SGs are in operation. This signal may be manually ~~blocked~~ bypassed by the operator in MODE 3 below the P-11 setpoint. This function is not required to be OPERABLE in MODE 3 below the P-11 setpoint. —, because the plant may be transitioning from using the SGs as a heat sink to using the RHR system. This function is bypassed in MODE 3 below the P-11 setpoint to allow the operator to control EFW during the transition to RHR cooling and to maintain the Steam Generators filled with water in preparation for shutdown conditions (wet layup operation). When starting up, the High Steam Generator Water Level signal is automatically enabled above the P-11 setpoint.

In MODES 4, 5, and 6, SGs are not in service and this Function is not required to be OPERABLE.

d. Emergency Feedwater Isolation - Low Main Steam Line Pressure

This signal provides protection against excessive cooling from damaged SG. A steam line break or a feed line ~~brake~~break inside of containment, would result in a low steam line pressure.

~~Low Main~~ Steam Line Pressure provides ~~no input to any both~~ control ~~and protection~~ functions, ~~as described previously under ECCS Function 1.e.~~ There are four Low Main Steam Line Pressure channels on each steam line in a two-out-of-four logic configuration. Three OPERABLE channels on each main steam line are sufficient to satisfy the protective requirements with a two-out-of-three logic on each steam line.

Low Main Steam Line Pressure must be OPERABLE in MODES 1, ~~and 2,~~ and MODE 3 (above the P-11) when setpoint. In these MODES, the SGs are in operation. This signal may be manually ~~blocked~~bypassed by the operator in MODE 3 below the P-11 setpoint. This function is not required to be OPERABLE in MODE 3 below the P-11 setpoint, because a secondary break is not limiting under these conditions, as described previously. There is sufficient time margin for manual Emergency Feedwater Isolation, if necessary. When starting up, the Low Main Steam Line Pressure signal is automatically enabled above the P-11 setpoint.

In MODES 4, 5, and 6, SGs are not in service and this Function is not required to be OPERABLE.

8. CVCS Isolation

The objective of CVCS Isolation is to prevent Pressurizer overfill in the event of a CVCS malfunction. For this objective, the CVCS Isolation is automatically actuated by High Pressurizer Water Level signal. The Function may also be actuated manually.

CVCS Isolation valves are distributed to Trains A and D. Both trains must be OPERABLE.

a. CVCS Isolation – Manual Initiation

Manual ~~initiation~~Initiation of CVCS Isolation can be accomplished from the ~~main control room~~MCR. There are two switches in the ~~main control room~~MCR, one for each train. Each CVCS Isolation Valve is actuated from both trains. Therefore, either switch can initiate action to immediately close all CVCS Isolation Valves. This LCO requires 2 Manual CVCS Isolation Actuation switches. ~~Operation of either switch will actuate this Function.~~

b. CVCS Isolation – Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. CVCS Isolation valves are distributed to Trains A and D. Both trains must be OPERABLE.

Manual and automatic initiation of CVCS Isolation Functions must be OPERABLE in MODES 1, 2 and 3. In MODES 4, 5, and 6, the Pressurizer may be filled with water and this Function is not required to be OPERABLE.

c. CVCS Isolation - High Pressurizer Water Level

This signal provides protection against that the Pressurizer overfill in the event of CVCS malfunction.

There are four High Pressurizer Water Level channels in a two-out-of-four logic configuration. Pressurizer Water Level provides input to the Pressurizer Level Control System. The interface from the safety channels in the PSMS to the PCMS is through the Signal ~~Selector~~ Selection Algorithm (SSA).- When three or more High Pressurizer Water Level channels are OPERABLE, The SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three channels total must be OPERABLE. When there are less than three OPERABLE High Pressurizer Water Level channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for High Pressurizer Water Level channels, since there are only three required channels.

The transmitters (d/p cells) are located inside containment. However, the events that this Function protects against cannot cause a severe environment in containment. Therefore, the Nominal Trip Setpoint reflects only steady state instrument uncertainties.

High Pressurizer Water Level must be OPERABLE in MODES 1, ~~2~~ and 2, and MODE 3 (above the P-11); ~~setpoint~~. This signal may be manually ~~blocked~~ bypassed by the operator in MODE 3 below the P-11 setpoint. This function is not required to be OPERABLE in MODE 3 below the P-11 setpoint, ~~because the~~ Pressurizer Water Level is much lower than in higher MODES providing a larger time margin to the pressurizer becoming full. Therefore, the automatic CVCS Isolation on High Pressurizer Water Level function is not required under these conditions. When starting up, the High Pressurizer Water Level signal is automatically enabled above the P-11 setpoint

In MODES 4, 5, and 6, the Pressurizer may be filled with water and this Function is not required to be OPERABLE.

9. Turbine Trip

The primary functions of the Turbine Trip are to prevent damage to the turbine due to water in the steam lines, and to stop the excessive cooldown of the primary system.

The Turbine Trip Function is actuated by High-High Steam Generator Water Level or on Reactor Trip (~~P-4~~).

a. Turbine Trip - Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. ~~Four Turbine trip Trip~~ solenoid valves are arranged in a ~~selective one two out of two twice~~ configuration, ~~taken separately for Train A turbine trip will occur from Turbine Trip actuation from Trains A or C, and Trains B or D. A Turbine Trip will be generated by Train A or Train D. Therefore a single train failure will not prevent a valid Turbine Trip.~~ The LCO requires ~~all four two~~ trains, Trains A and D, to be OPERABLE.

b. Turbine Trip - Reactor Trip, P-4

The turbine is tripped on a ~~reactor trip~~ Reactor Trip. Turbine trip on ~~reactor trip~~ Reactor Trip is an un-credited non-safety function in the safety analysis. However, ~~turbine trip~~ Turbine Trip on ~~reactor trip~~ Reactor Trip is assumed in the safety analysis in order to prevent unnecessary ECCS Actuation and to shift to the safe shutdown state by appropriate actions after AOO and PA conditions.

Turbine Trip is initiated when the reactor trips as indicated by the P-4 interlock. Therefore, the requirements for the P-4 interlock are not repeated in Table 3.3.2-1. Instead, Function 11, Reactor Trip P-4, is referenced for the initiating Function and requirements. Note that ~~all four both~~ Turbine Trip actuation trains, Trains A and D, are actuated when any two ~~out of four~~ RTB trains are actuated.

c. High-High Steam Generator Water Level

The High-High Steam Generator Water Level signal prevents water in the steam lines that could lead to turbine generator damage. Turbine trip on High-High Steam Generator Water Level is an un-credited non-safety function in the safety analysis.

There are four High-High Steam Generator Water Level channels in a two-out-of-four logic configuration for each Steam Generator. Note that both Turbine Trip actuation trains, Trains A and D, are actuated when any two-out-of-four High-High Steam Generator Water Level channels are actuated.

The PSMS SG ~~water level~~Water Level instruments provide input to the SG Water Level Control System. The interface from the safety channels in the PSMS to the PCMS is through the Signal ~~Selector~~Selection Algorithm (SSA). ~~The~~When three or more High-High SG Water Level channels are OPERABLE for each Steam Generator, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three channels total must be OPERABLE. When there are less than three OPERABLE High-High SG Water Level channels for each Steam Generator, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for High-High SG Water Level channels, since there are only three required channels for each Steam Generator.

10. Reactor Coolant Pump Trip

TMI Action Plan Item II.K.3.5 (Ref. 1) requires automatic trip of reactor coolant pumps (RCPs) following a loss-of-coolant accident (LOCA). The requirement is based on the consideration that a delayed-trip or continuous operation of the RCPs during a small break LOCA would lead to more severe consequences than if the RCPs are tripped early following a postulated break. Tripping all the RCPs early during a small break LOCA precludes the occurrence of excessive fuel cladding temperature.

a. Reactor Coolant Pump Trip – ECCS Actuation coincident with P-4 signal

The consequence of continuous RCP operation is the extensive liquid discharge from the break beyond the time that the system would drained down to allow steam discharge from the break had the pumps been immediately tripped. Therefore pump trip following a ~~reactor trip~~Reactor Trip and indication of ECCS ~~actuation~~Actuation would be effective.

For the small break LOCA analysis, the loss of offsite power triggered by ~~reactor trip~~Reactor Trip signal is conservatively assumed, which would cause the earliest RCP trip. In case that the automatic RCP trip is enabled, an earlier RCP trip results in earlier flow coastdown leading to more severe consequences.

11. Engineered Safety ~~Feature~~Features Actuation System Interlocks

To allow some flexibility in unit operations, several interlocks are included as part of the ESFAS. These interlocks permit the operator to ~~block~~bypass some signals, automatically enable other signals, prevent some actions from occurring, and cause other actions to occur. The interlock Functions back up manual actions to ensure bypassable functions are in operation under the conditions assumed in the safety analyses.

a. Engineered Safety ~~Feature~~Features Actuation System Interlocks - Reactor Trip, P-4

The P-4 ~~interlock~~Interlock is enabled when RTBs have opened in two out of four RTB trains. RTB position signals from each RTB are interfaced to all PSMS trains via internal PSMS data links so that the P-4 interlock is generated independently within each train. Therefore this LCO requires three trains to be OPERABLE.

This Function allows operators to take manual control of ECCS systems after the initial phase of ECCS Actuation is complete. Once ECCS is overridden, automatic actuation of ECCS cannot occur again until the RTBs have been manually closed. The functions of the P-4 interlock are:

- Trip the main turbine,
- ~~Isolate~~Close MFW ~~with~~ Regulation Valves coincident ~~low~~with Low T_{avg} ,
- Enable a manual override of ECCS Actuation and prevent ECCS reactivation,
- EFW Isolation ~~with~~ coincident with High SG Water Level and No Low Main Steam Line Pressure, and
- Trip the Reactor Coolant Pump ~~with~~ coincident with ECCS Actuation.

Each of the above Functions except Reactor Coolant Pump Trip is interlocked with P-4 to avert or reduce the continued cooldown of the RCS following a Reactor Trip. An excessive cooldown of the RCS following a Reactor Trip could cause an insertion of positive reactivity with a subsequent increase in generated power. Reactor Coolant Pump Trip function is interlocked with P-4 to prevent the unexpected Reactor Coolant Pump Trip after a small break LOCA. The unexpected Reactor Coolant Pump Trip after a small break LOCA could cause the increasing of the Peak Clad Temperature (PCT). To avoid such these situations, the noted Functions have been interlocked with P-4 as part of the design of the unit control and protection system.

The RTB position switches that provide input to the P-4 interlock only function to energize or de-energize or open or close contacts. Therefore, this Function has no adjustable trip setpoint.

This Function must be OPERABLE in MODES 1, 2, and 3. In these MODES, the reactor may be critical or approaching criticality. This Function does not have to be OPERABLE in MODE 4, 5, or 6 because the main turbine, the MFW System, and the Turbine Bypass System are not in operation.

~~Each of the above Functions except Reactor Coolant Pump Trip is interlocked with P-4 to avert or reduce the continued cooldown of the RCS following a reactor trip. An excessive cooldown of the RCS following a reactor trip could cause an insertion of positive reactivity with a subsequent increase in generated power. Reactor Coolant Pump Trip function is interlocked with P-4 to prevent the unexpected Reactor Coolant Pump Trip after a small break LOCA. The unexpected Reactor Coolant Pump Trip after a small break LOCA could cause the increasing of the Peak Clad Temperature (PCT). To avoid such these situations, the noted Functions have been interlocked with P-4 as part of the design of the unit control and protection system.~~

~~The RTB position switches that provide input to the P-4 interlock only function to energize or de-energize or open or close contacts. Therefore, this Function has no adjustable trip setpoint. This Function must be OPERABLE in MODES 1, 2, and 3 when the reactor may be critical or approaching criticality. This Function does not have to be OPERABLE in MODE 4, 5, or 6 because the main turbine, the MFW System, and the Turbine Bypass System are not in operation.~~

b. Engineered Safety ~~Feature~~Features Actuation System Interlocks - Pressurizer Pressure, P-11

The P-11 interlock permits a normal unit cooldown and depressurization without actuation of ECCS, Main Steam Line Isolation, CVCS Isolation, EFW Isolation or Main Feedwater Isolation on High-High SG Water Level.

With two-out-of-four ~~pressurizer pressure~~ Pressurizer Pressure channels (discussed previously) less than the P-11 setpoint, the operator can manually ~~block~~ bypass the Low Pressurizer Pressure and Low Main Steam Line Pressure ECCS Actuation signals, the Low Main Steam Line Pressure ~~main steam line isolation~~ Main Steam Line Isolation signal, the CVCS Isolation signal, the EFW Isolation signals, and the High-High SG Water Level Main Feedwater Isolation signal (previously discussed). When the Low Main Steam Line Pressure ~~main steam line isolation~~ Main Steam Line Isolation signal is manually ~~blocked, a main steam isolation signal bypassed, a Main Steam Line Isolation signal~~ on High Main Steam Line Pressure Negative Rate is enabled. This provides protection for an SLB by closure of the MSIVs.

With two-out-of-three ~~pressurizer pressure~~ Pressurizer Pressure channels above the P-11 setpoint, the Low Pressurizer Pressure and Low Main Steam Line Pressure ECCS Actuation signals, the Low Main Steam Line Pressure ~~main steam line isolation~~ Main Steam Line Isolation signal, the CVCS Isolation signal, the EFW Isolation signals, and the High-High SG Water Level Main Feedwater Isolation signal are automatically enabled. The operator can also enable these trips by use of the respective manual reset buttons. When the Low Main Steam Line Pressure ~~main steam line isolation~~ Main Steam Line Isolation signal is enabled, the ~~main steam isolation~~ Main Steam Line Isolation on High Main Steam Line Pressure Negative Rate is disabled.

~~The~~ The Nominal Trip Setpoint reflects only steady state instrument uncertainties.

This Function must be OPERABLE in MODES 1, 2, and 3 to allow an orderly cooldown and depressurization of the unit without the actuation of ECCS, ~~main steam line isolation~~ Main Steam Line Isolation, CVCS Isolation, EFW Isolation or Main Feedwater Isolation on High-High SG Water Level. This Function does not have to be OPERABLE in MODE 4, 5, or 6 because system pressure must already be below the P-11 setpoint for the requirements of the heatup and cooldown curves to be met.

12. Containment Purge Isolation

Containment Purge Isolation initiates on Containment High Range Area Radiation, an ~~automatic~~ ECCS Actuation signal, by ~~manual initiation~~ Manual Initiation of Containment Isolation Phase A, or by ~~manual initiation~~ Manual Initiation of Containment Spray.

Containment Purge Isolation components are distributed to PSMS Trains A and D. Two trains are sufficient to provide the safety function. Both are required to be OPERABLE to provide the safety function with a concurrent single failure.

a. Containment Isolation Phase A - Manual Initiation

Containment Purge Isolation is manually initiated by Containment Isolation Phase A - Manual Initiation. The Containment Purge Isolation requirements for this Function are the same as the requirements for the Containment Isolation Phase A Function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 3.a, Containment Isolation Phase A- Manual Initiation, is referenced for all initiating Functions and requirements.

b. Containment Spray - Manual Initiation

Containment Purge Isolation is manually initiated by Containment Spray - Manual Initiation. The Containment Purge Isolation requirements for this Function are the same as the requirements for the Containment Spray Function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 2.a, Containment Spray – Manual Initiation, is referenced for all initiating Functions and requirements.

Note that ~~all two~~ both Containment Purge Isolation trains are actuated when any two-out-of-four Containment Spray - Manual Initiation signals are actuated.

c. Containment Purge Isolation - Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. Containment Purge Isolation valves are distributed to Trains A and D. Both trains must be OPERABLE.

d. Containment Purge Isolation - ECCS Actuation

Containment Purge Isolation is also initiated by all Functions that initiate ECCS. The Containment Purge Isolation requirements for these Functions are the same as the requirements for the ECCS function. Therefore, the requirements are not repeated in

Table 3.3.2-1. Instead, Function 1, ECCS, is referenced for all initiating Functions and requirements.

Note that ~~all two~~both Containment Purge Isolation trains are actuated when any two out of four ECCS - Automatic or Manual Initiation signals are actuated.

e. Containment Purge Isolation - Containment High Range Area Radiation

Containment High Range Area Radiation has four channels in a two-out-of-four logic configuration. Three OPERABLE channels are sufficient to satisfy protective requirements with two-out-of-three logic.

The Containment Purge Isolation Functions are required OPERABLE in MODES 1, 2, 3, and 4. Under these conditions, the potential exists for an accident that could release significant fission product radioactivity into containment. Therefore, the Containment Purge Isolation instrumentation must be OPERABLE in these MODES.

While in MODES 5 and 6, including fuel handling in progress, the Containment Purge Isolation instrumentation ~~need is not required to~~ be OPERABLE ~~since the potential for radioactive releases is minimized and operator action is sufficient to ensure post accident offsite doses are maintained within acceptable limits. This is because the doses at the exclusion area boundary, at the low population zone outer boundary, and in the main control room MCR are maintained within acceptable limits for the case where a fuel handling accident occurs without the containment being isolated, as described in FSAR Section 15.7.4 (Ref. 10).~~

13. Main Control Room Isolation

The ~~Main Control Room~~MCR Isolation function provides an enclosed ~~main control room~~MCR environment from which the unit can be operated following an uncontrolled release of radioactivity. MCR Isolation controls the ~~main control room~~Main Control Room HVAC System (MCRVS) which includes two subsystems: Main Control Room Emergency Filtration System (MCREFS) and Main Control Room Air Temperature Control System (MCRATCS), described in the ~~DCD~~FSAR Chapter 16 Section 3.7.10.

There are four ~~Main Control Room~~MCR Isolation trains. ~~Train~~Trains A and D of MCR Isolation control two 100% capacity trains of subsystem MCREFS, and all four trains of MCR Isolation control four 50% capacity trains of subsystem MCRATCS. Two trains of MCR Isolation, including A or D, must actuate to properly provide the safety function (i.e., isolate and supply filtered air to the ~~main control room~~MCR), and three trains, including A and D, must be OPERABLE to provide the safety function with a concurrent single failure.

The MCR Isolation actuation instrumentation consists of redundant radiation monitors. A high radiation signal will initiate all four MCR Isolation trains. The ~~main control room~~MCR operator can also initiate MCR Isolation trains by manual switches in the ~~main control room~~MCR. MCR Isolation is also actuated by an ECCS Actuation signal.

The ~~main control room~~MCR must be kept habitable for the operators stationed there during accident recovery and post accident operations. The MCR Isolation function acts to terminate the supply of unfiltered outside air to the ~~main control room~~MCR, initiate filtration, and allows pressurization of the ~~main control room~~MCR. These actions are necessary to ensure the ~~main control room~~MCR is kept habitable for the operators stationed there during accident recovery and post accident operations by minimizing the radiation exposure of the ~~main control room~~MCR personnel.

In MODES 1, 2, 3, and 4, the radiation monitor actuation of MCR Isolation is a backup for the ECCS Actuation. This ensures initiation of the MCR Isolation during a loss of coolant accident or steam generator tube rupture.

The radiation monitor actuation of MCR Isolation during movement of irradiated fuel assemblies are the primary means to ensure ~~main control room~~MCR habitability in the event of a fuel handling accident.

~~a. Manual Initiation~~

~~The LCO requires four trains OPERABLE. The MCREFS and MCRATCS components (e.g., fans, dampers) can be manually controlled by the Safety VDUs (S-VDUs) of the corresponding train, and by the non-safety operational VDUs (O-VDUs). MCR Isolation signals, (either automatically or manually initiated) have priority over all manual component control signals, and therefore will block any signals from the O-VDUs, including spurious signals.~~

The automatic initiation of MCR Isolation is credited to ensure any spurious signals from the non-safety O-VDUs cannot prevent the MCR Isolation safety function. To accommodate various inoperable conditions, MCREFS and/or MCRATCS components are manually placed in the position they would be automatically actuated to by the MCR Isolation signal. For conditions where the automatic initiation function is inoperable, the MCRVS O-VDU Disconnect function is manually activated from the S-VDU for the affected MCREFS and/or MCRATCS train(s). The MCRVS O-VDU Disconnect function blocks signals from the O-VDUs, including spurious signals, in the same manner as the credited automatic initiation signal.

a. Main Control Room Isolation - Manual Initiation

The operator can initiate MCR Isolation for all four MCR Isolation trains at any time by using four Manual Initiation switches in the ~~main control room~~ MCR. Each push-button actuates its own train directly. A signal from each pushbutton is also interfaced to all other trains via internal PSMS communication links. In addition to direct actuation by its own train pushbutton, each train is also actuated by two-out-of-three Manual Initiation signals received from the other trains. The signals from the other trains are not credited in determining when the Manual Initiation Function is OPERABLE or in determining the number of required trains. However, these additional signals are considered in the Completion Times for the Required Actions. This action will cause actuation of all components in the same manner as any of the automatic actuation signals.

~~The LCO for Manual Initiation ensures the proper amount of redundancy is maintained in the manual actuation circuitry to ensure the operator has manual initiation capability.~~
The LCO requires three trains, including A and D, to be OPERABLE due to the two train configuration of MCREFS and four train configuration of MCRATCS, as described above.

Each ~~channel~~ train consists of one push button and the interconnecting wiring to the ESFAS cabinet.

b. Main Control Room Isolation - Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b., ECCS Actuation. However, for MCR Isolation ~~4~~ three trains, including A and D, must be ~~operable~~ OPERABLE due to the ~~distribution~~ two train configuration of ~~main control room isolation dampers to all~~ MCREFS and ~~four trains-~~ train configuration of MCRATCS, as described above.

c. Main Control Room Isolation - Main Control Room Radiation

There are three kinds of Main Control Room Radiation monitor functions (gas monitor, iodine monitor, and particulate monitor). ~~One monitor~~ Each monitoring function includes two detectors of Train A and D. RPS trains A and D provide separate digital bistable setpoint comparison functions for each monitor. These digital bistable output signals are distributed from RPS trains A and D to each of the four ESFAS trains. Within each of the four ESFAS trains the MCR Isolation signal is actuated on a signal from either the A or D train detectors using 1-out-of-2 logic for each type of monitor.

The LCO specifies two required Main Control Room Radiation monitors for each function to ensure that the radiation monitoring

instrumentation necessary to initiate the MCR Isolation remains OPERABLE.

For sampling systems, channel OPERABILITY involves more than OPERABILITY of channel electronics. OPERABILITY may also require correct valve lineups, sample pump operation, and filter motor operation, as well as detector OPERABILITY, if these supporting features are necessary for trip to occur under the conditions assumed by the safety analyses.

d. Main Control Room Isolation - ECCS ACTUATION

~~Main Control Room~~MCR Isolation is also initiated by all Functions that initiate ECCS Actuation. The MCR Isolation requirements for these Functions are the same as the requirements for their ECCS Actuation function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 1, ECCS Actuation, is referenced for all initiating Functions and requirements. Note that all four MCR Isolation trains are actuated when any two out of four ECCS Actuation - Automatic or Manual Initiation signals are actuated.

The MCR Isolation Functions must be OPERABLE in MODES 1, 2, 3, and 4, and during movement of irradiated fuel assemblies.

14. Block Turbine Bypass and Cooldown Valves

The Block Turbine Bypass and Cooldown Valves function prevents the ~~overcooldown~~overcooling of the reactor coolant system when T_{avg} is decreased abnormally.

Block turbine bypass and cooldown valves are distributed to Trains A and D. Both trains must be OPERABLE in MODE 1, 2 and 3. In MODES 4, 5, and 6, the average coolant temperature is below the Low-Low T_{avg} Signal setpoint and this function is not required to be OPERABLE.

a. Block Turbine Bypass and Cooldown Valves – Manual Initiation

Manual ~~initiation~~Initiation of Block Turbine Bypass and Cooldown Valves can be accomplished from the ~~main control room~~MCR. There are two switches in the ~~main control room~~MCR, one for each train. Each Turbine Bypass and Cooldown Valve is blocked from both trains. Therefore, either switch can be initiated to immediately block the opening of all Turbine Bypass and Cooldown Valves. This LCO requires 2 Manual Block Turbine Bypass and Cooldown Valves Actuation switches. ~~Operation of either switch will actuate this Function.~~ to be OPERABLE.

b. Block Turbine Bypass and Cooldown Valves - Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for ESFAS Function 1.b. Block ~~turbine bypass~~ Turbine Bypass and ~~cooldown valves~~ Cooldown Valves are distributed to Trains A and D. Both trains must be OPERABLE.

c. Block Turbine Bypass and Cooldown Valves - Low-Low T_{avg} Signal

~~This function must be OPERABLE in MODES 1, 2 and 3. In MODES 4, 5, and 6, the average coolant temperature is below the low-low T_{avg} signal setpoint and this function is not~~ There are four Low T_{avg} channels (one per loop) in a two out of four configuration. Three channels of T_{avg} are required to be OPERABLE. The T_{avg} channels are combined in a logic such that two out of three channels cause a trip for the Function. The accidents that this Function protects against cause reduction of T_{avg} in the entire primary system. Therefore, the provision of three OPERABLE channels in a two-out-of-four configuration ensures no single random failure disables the Low T_{avg} Function.

T_{avg} channels provide inputs to both control and protection functions. T_{avg} channels provide control inputs to the Rod Control System, Pressurizer Water Level Control System, and Turbine Bypass Control System. The interface from the safety channels in the PSMS to the PCMS is through the Signal Selection Algorithm (SSA).

When three or more T_{avg} channels are OPERABLE, the SSA ensures an input failure to the control system does not result in erroneous control system action that would require the protection function actuation. Therefore, the protection function requires only two additional channels to provide the protection function actuation (i.e., three channels total). Three channels total must be OPERABLE. When there are less than three OPERABLE T_{avg} channels, the SSA cannot prevent erroneous control system operation due to an input failure. This is reflected in the LCO Completion Times for shared T_{avg} channels.

With the T_{avg} resistance temperature detectors (RTDs) located inside the containment, it is possible for them to experience adverse environmental conditions during an SLB event. Therefore, the Nominal Trip Setpoint reflects both steady state and adverse environmental instrumental uncertainties.

Low-Low T_{avg} Signal - Low-Low T_{avg} Signal is enabled by the Block Turbine Bypass and Cooldown Valves.

15. Manual Control of ESF Components

The Manual Control of ESF Components Function provides credited manual controls for accidents and safe shutdown, as defined for the plant components in LCO 3.4 through 3.7.

a. Manual Control of ESF Components – S-VDU

An S-VDU train consists of a VDU and S-VDU processor. An S-VDU train must be OPERABLE for the same trains and MODES as required for the controlled ESF components. For ESF components with four trains (three required trains), three S-VDU trains must be OPERABLE for the same three trains as the required OPERABLE ESF components. For ESF components with only two required trains, an S-VDU train must be OPERABLE for the same two trains as the required OPERABLE ESF components. However, for Phase B Containment Isolation, there are two-train components assigned to Trains A and D, and two-train components assigned to Trains B and C. Therefore, because all four trains are required for Phase B Containment Isolation, all four trains of S-VDU are required. Since Manual Control of ESF Components is required for some ESF systems in all MODES, S-VDU must be OPERABLE to support ESF components in MODES 1, 2, 3, 4, 5 and 6.

b. Manual Control of ESF Components - COM-2

COM-2 combines the manual control signals from non-safety Operational VDUs with the manual control signals from S-VDUs. The combined signal is interfaced to the Actuation Logic in the SLS for manual control of ESF components. Since COM-2 controls ESF components assigned to all four trains as explained above for the S-VDU, some of which are required in all MODES, four COM-2 trains are required in MODES 1, 2, 3, 4, 5 and 6.

c. Manual Control of ESF Components - Actuation Logic and Actuation Outputs

The Actuation Logic and Actuation Outputs for the Manual Control of ESF Components Function is implemented in the SLS. For ESFAS components, the SLS combines the automatic actuation signals from the ESFAS with the manual control signals from COM-2. For all ESF components the SLS generates Actuation Outputs, based on automatic and/or manual control signals, which control the state of the ESF components. For the Manual Control of ESF Components Function, the Actuation Logic and Actuation Outputs within any SLS controller must be OPERABLE in the same MODES and for the same trains as for the required ESF components. LCO 3.4 through 3.7 provide MODE and train requirements applicable to ESF components.

The ESFAS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii) (Ref. 9).

ACTIONS

A Note has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function listed on Table 3.3.2-1.

In the event a channel's accuracy is found non-conservative with respect to the Allowable Value, or the transmitter, instrument ~~Loop~~loop, signal processing electronics, or digital bistable is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the LCO Condition(s) entered for the protection Function(s) affected. When the Required Channels in Table 3.3.2-1 are specified (e.g., on a per steam line, per loop, per SG, etc., basis), then the Condition may be entered separately for each steam line, loop, SG, etc., as appropriate.

When the number of channels inoperable ~~channels~~ in a trip function exceeds those specified in one or other related Conditions associated with a trip function, then the unit is outside the safety analysis. Therefore, LCO 3.0.3 should be immediately entered if applicable in the current MODE of operation.

In all cases where the LCO states "Restore channel or train to OPERABLE status", this means restore the required number of channels or trains to OPERABLE status. Therefore, restoration of an alternate channel or train, other than the failed channel or train, is also acceptable.

A.1

Condition A applies to all ESFAS protection functions.

Condition A addresses the situation where one or more required channels or trains for one or more Functions are inoperable at the same time. The Required Action is to refer to Table 3.3.2-1 and to take the Required Actions for the protection functions affected. The Completion Times are those from the referenced Conditions and Required Actions.

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

Condition B applies to ~~manual initiation~~ Manual Initiation of:

- ECCS Actuation,
- Containment Spray, and
- Containment Phase A Isolation.

This action addresses the train orientation of the PSMS for the functions listed above. If ~~a channel or one~~ required train is inoperable, 72 hours ~~is~~ are allowed to return it to an OPERABLE status. Note that for

~~containment spray~~Containment Spray and Phase B ~~isolation~~isolation, failure of one or both channels in one train renders the train inoperable. Condition B, therefore, encompasses both situations.

The ~~specified~~Completion Time is reasonable considering that the remaining OPERABLE of 72 hours is justified because (1) for ECCS two trains provide protection for each Function, and the low probability of an event occurring during this interval. The completion time also considers that are adequate to perform the safety function and there are three required automatic actuation trains and two other required Manual Initiation for all functions can also be actuated from the Safety VDU for each train. Therefore all safety related trains OPERABLE, (2) for Containment Spray three trains are adequate to perform the safety function and there are four automatic actuation trains and three other Manual Initiation functions remain operable. In addition, the trains OPERABLE, or (3) for Containment Phase A Isolation one train is adequate to perform the safety function and there are two automatic actuation trains and one other Manual Initiation function for train OPERABLE. The Completion Time also considers that all trains is actuated of ECCS can be initiated by the Manual Initiation pushbuttons for Function from the two remaining trains, and Containment Spray can be initiated by the Manual Initiation Function from any two out of the remaining three trains.

In addition, the Completion Time considers that each train of all Functions can be manually initiated from the Safety VDU for that train. Therefore, manual initiation through safety related equipment remains functional in all required trains.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

If the train cannot be restored to OPERABLE status, the unit must be placed in a MODE in which the LCO does not apply. This is done by placing the unit in at least MODE 3 within an additional 6 hours (78 hours total time) and in MODE 5 within an additional 30 hours (108 hours total time). The allowable 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.

~~The initial completion time of 72 hours is justified in the PSMS reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6B.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19. The PSMS reliability analysis credits the continued compliance to the single failure criteria, since the ESFAS manual initiation function remains fully operable from the Safety VDUs, even when one ESFAS manual initiation function is inoperable.~~

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

Condition C applies to the Actuation Logic and Actuation Outputs for the following ~~functions~~Functions:

- Containment Phase A Isolation, and
- Containment Phase B Isolation.

This action addresses the train orientation of the PSMS. If one train is inoperable, 24 hours are allowed to restore the train to OPERABLE status. ~~The 24 hours allowed for restoring the inoperable train to OPERABLE status is reasonable considering that there are sufficient trains OPERABLE to ensure the capability of the required Function, and the low probability of an event occurring during this interval.~~

The Completion Time ~~also of 24 hours is justified because the remaining OPERABLE train(s) are adequate to perform the safety function. In addition, the Completion Time~~ considers that the remaining OPERABLE train(s) each have continuous automatic self-testing.

The Completion Time of 24 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

If the train cannot be restored to OPERABLE status, the unit must be placed in a MODE in which the LCO does not apply. This is done by placing the unit in at least MODE 3 within an additional 6 hours (30 hours total time) and in MODE 5 within an additional 30 hours (60 hours total time). The 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.

The Required Actions are modified by a Note that allows placing one train ~~to be bypassed~~in bypass for up to 4 hours ~~for while performing~~ surveillance testing, provided the other train(s) ~~is~~are OPERABLE. This ~~allowance is~~4 hour bypass time is reasonable based on ~~the reliability analysis assumption~~operating experience that 4 hours is the average time required to perform a train surveillance.

~~The bypassed condition for up to 4 hours and the initial completion time of 24 hours are~~The Bypass Time of 4 hours is justified because the remaining OPERABLE train(s) are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE train(s) have continuous automatic self-testing.

The Bypass Time of 4 hours is also justified in the PSMS-US-APWR reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6B.12. The and risk analyses, the summary and result of the PSMS-reliability analysis is evaluated and confirmed which are documented in the US-APWR PRA FSAR Chapter 19. (Ref. 11).

D.1, D.2.1, and D.2.2

Condition D applies to:

- High ~~Containment Pressure,~~ and
- ~~Low Pressurizer Pressure,~~
- ~~Low Main Steam Line Pressure,~~
- ~~Low T_{avg} ,~~
- ~~High Pressurizer Water Level,~~
- High-High Containment Pressure, and
~~High Main Steam Line Pressure Negative Rate, High SG Water Level,~~

~~Low SG Water Level,~~

~~High-High SG Water Level, and~~

~~Low-low T_{avg} .~~

If one required channel is inoperable, 72 hours are allowed to restore the channel to OPERABLE status or to place it in the tripped condition. ~~Generally this Condition applies to functions that operate on two-out-of-three logic. Therefore, failure~~ Failure of one channel places the Function in a two-out-of-two configuration. One, when the failed channel does not result in a trip channel. This configuration provides adequate plant protection, but does not meet the single failure criteria. Therefore, within 72 hours the inoperable channel must be tripped to place the Function in a one-out-of-three ~~two~~ configuration that satisfies redundancy requirements. ~~The 72 hours allowed to restore the channel to OPERABLE status or to place it in the tripped condition is justified because the remaining two~~ the single failure criteria.

The Completion Time of 72 hours is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the two remaining OPERABLE channels have continuous automatic self-testing (as described for COT), and continuous automatic CHANNEL CHECKS.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

Failure to restore the channel inoperable ~~channel~~ to OPERABLE status or place it in the tripped condition within 72 hours requires the unit be placed in MODE 3 within the following 6 hours and MODE 4 within the next 6 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. In MODE 4, these Functions are no longer required OPERABLE.

~~The initial completion time of 72 hours is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6B.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~

~~One channel may be bypassed. Required Actions are modified by a Note that allows placing one required channel in bypass for up to 12 hours for while performing surveillance testing. The 12 hours bypass limit is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6B.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19. This bypass is not allowed for, provided the other functions because these required channels are also used for control. If a failure were to occur in one of the two remaining control channels, a plant transient could occur that would require a plant trip, but a plant trip would not occur with only OPERABLE, or one remaining operable required channel is OPERABLE and the other required channel is placed in the trip condition.~~

The Bypass Time of 12 hours is justified because the remaining OPERABLE required channels are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE required channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

The Bypass Time of 12 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

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

Condition E applies to:

- Containment Spray - High-3 Containment Pressure, and
- Containment Phase B Isolation - High-3 Containment Pressure.

~~This LCO requires three operable channels. None of these signals has input to a control function. Two out of three logic is necessary to meet acceptable protective requirements. However, a two-out-of-three design would require tripping a failed channel. This~~
if one required channel is inoperable, 72 hours are allowed to restore the channel to OPERABLE status. Failure of one channel places the Function in a two-out-of-two configuration, when the failed channel does not result in a tripped channel.

This configuration provides adequate plant protection, but does not meet the single failure criteria. Therefore, within 72 hours the inoperable channel must be restored to OPERABLE status.

Tripping a channel, as in Condition D, is undesirable because a single failure would then cause spurious containment spray initiation. Spurious spray actuation is undesirable because of the cleanup problems presented.

~~Restoring the channel to OPERABLE status within 72 hours is sufficient because of the low probability of an event occurring during this interval because the remaining two-~~ The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the two remaining OPERABLE channels have continuous automatic self-testing (as described for COT), and continuous automatic CHANNEL CHECKS.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

Failure to restore the required number of channels to OPERABLE status within 72 hours, requires the unit be placed in MODE 3 within the following 6 hours and MODE 4 within the next 6 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. In MODE 4, these Functions are no longer required OPERABLE.

~~The initial completion time of 72 hours is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6B.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~

The Required Actions are modified by a Note that allows placing one required channel in bypass for up to 12 hours while performing surveillance testing, provided the other required channels are OPERABLE. Bypassing with another channel in trip, as in Condition D, is undesirable because a single failure during surveillance testing would then cause spurious Containment Spray initiation. Spurious spray actuation is undesirable because of the cleanup problems presented.

Bypass Time of 12 hour is justified because the remaining OPERABLE channels are adequate to perform the safety function. In addition, the remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

The Bypass Time of 12 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

F.1, F.2.1, and F.2.2

Condition F applies to:

Loss of Offsite Power, ~~and~~

~~• P-4 Interlock.~~

Condition F also applies to the ~~manual initiation~~ Manual Initiation for:

- Main Steam Line Isolation,
- Main Feedwater Isolation,
- Emergency Feedwater Actuation,
- Emergency Feedwater Isolation,
- CVCS Isolation, and
- Block Turbine Bypass and Cooldown Valves.

For all Functions, this action addresses the train orientation of the PSMS. For the Loss of Offsite Power Function, this action also recognizes the lack of manual trip provision for a failed channel.

If ~~a train or one~~ channel or required train is inoperable, 72 hours ~~is are~~ allowed to return it to OPERABLE status. ~~The specified Completion Time is reasonable considering the nature of these Functions, the available redundancy, and the low probability of an event occurring during this interval.~~

For the Loss of Offsite Power Function, the Completion Time of 72 hours is justified because the two remaining OPERABLE undervoltage devices for each train of the Emergency Feedwater Actuation Function are adequate to perform the safety function. Since the undervoltage devices are dedicated for each of the four Class 1E busses, and two undervoltage devices are adequate to perform the safety function of each bus, the Emergency Feedwater Actuation on Loss of Offsite Power continues to meet the single failure criterion (i.e., three trains of the Emergency Feedwater Actuation Function will still actuate if there is an additional undervoltage device failure on one bus).

For Manual Initiation Functions, the Completion Time of 72 hours is justified because (1) for Emergency Feedwater Actuation the remaining two trains are adequate to perform the safety function and there are three automatic actuation trains and two other Manual Initiation trains

OPERABLE, or (2) for Main Steam Line Isolation, Main Feedwater Isolation, Emergency Feedwater Isolation, CVCS Isolation, and Block Turbine Bypass and Cooldown Valves the remaining train is adequate to perform the safety function and there are two automatic actuation trains and one other Manual Initiation train OPERABLE. The Completion Time also considers that Emergency Feedwater Actuation for all trains can be initiated by the Manual Initiation Function from the two remaining trains.

In addition, the Completion Time for the Manual Initiation Function considers that each train can be manually initiated from the Safety VDU for that train. Therefore, manual initiation through safety related equipment remains functional in all trains.

For all Functions, the Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

If the Function cannot be returned to OPERABLE status, the unit must be placed in MODE 3 within the next 6 hours and MODE 4 within the following 6 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power in an orderly manner and without challenging unit systems. In MODE 4, the unit does not have any analyzed transients or conditions that require the explicit use of the protection functions noted above.

~~The initial completion time of 72 hours is justified in the PSMS reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6B.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19. For the manual initiation functions, the PSMS reliability analysis credits the continued compliance to the single failure criteria, since the ESFAS manual initiation function remains fully operable from the Safety VDUs, even when one ESFAS manual initiation function is inoperable.~~

For the Loss of Offsite Power Function a Note is added to allow placing one channel in bypass for up to 4 hours while performing surveillance testing, provided the other channels on the same bus are OPERABLE, or one channel is OPERABLE and the other is placed in the trip condition.

The Bypass Time of 4 hours is justified because the Function remains fully OPERABLE on every bus. In addition, the Bypass Time considers that each OPERABLE train has continuous automatic self-testing.

The 4 hour bypass time is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 5).

G.1, G.2.1, and G.2.2

Condition G applies to the Actuation Logic and Actuation Outputs for the;

- Emergency Feedwater Isolation,

- CVCS Isolation, and
- Turbine Trip Functions.

The action addresses the train orientation of the PSMS for these ~~functions.~~Functions. If one train is inoperable, 24 hours are allowed to restore the train to OPERABLE status. ~~The 24 hours allowed for restoring the inoperable train to OPERABLE status is reasonable considering that the safety function can be performed by the remaining OPERABLE trains, and the low probability of an event occurring during this interval. The Completion Time also~~

The Completion Time of 24 hours is justified because the remaining OPERABLE train is adequate to perform the safety function. In addition, the Completion Time considers that the remaining OPERABLE trains each have~~train has~~ continuous automatic self-testing.

The Completion Time of 24 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

If the train cannot be returned to OPERABLE status, the unit must be brought to MODE 3 within the next 6 hours and MODE 4 within the following 6 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. Placing the unit in MODE 4 removes all requirements for OPERABILITY of the protection channels and actuation functions. In this MODE, the unit does not have analyzed transients or conditions that require the explicit use of the protection functions noted above.

The Required Actions are modified by a Note that allows placing one train ~~to be bypassed~~in bypass for up to 4 hours ~~for~~while performing surveillance testing, provided the other ~~trains are~~train is OPERABLE. ~~This allowance is based on the assumption that 4 hours is the average time required to perform channel surveillance.~~

~~The bypassed condition for up to 4 hours and the initial completion time of 24 hours are~~The Bypass Time of 4 hours is justified because the remaining OPERABLE train is adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE train has continuous automatic self-testing.

The Bypass Time of 4 hours is also justified in the ~~PSMS US-APWR~~ reliability ~~analysis.~~analysis. ~~For detail information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6B.12. The~~ and risk analyses, the summary and result of the PSMS reliability analysis is evaluated and confirmed ~~which are documented in the US-APWR PRA~~FSAR Chapter 19 (Ref. 11).

H.1 and H.2

Condition H applies to the ~~EFW pump start~~ Emergency Feedwater Actuation on ~~trip~~ Trip of ~~all~~ All MFW ~~pumps~~ Pumps.

This action addresses the train orientation of the PSMS for the auto start function of the EFW System on loss of all MFW pumps. The OPERABILITY of the EFW System must be assured by allowing automatic start of the EFW System pumps.

If a required channel is inoperable, 48 hours are allowed to return it to an OPERABLE status.

The allowance of 48 hours to return the train to an OPERABLE status is justified because Trip of All Main Feedwater Pumps is an anticipatory function that is not credited in the safety analysis.

If the function cannot be returned to an OPERABLE status, 6 hours are allowed to place the unit in MODE 3.

The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging unit systems. In MODE 3, the unit does not have any analyzed transients or conditions that require the explicit use of the protection function noted above. ~~The allowance of 48 hours to return the train to an OPERABLE status is justified because trip of all main feedwater pumps is an anticipatory function that is not credited in the safety analysis.~~

I.1, I.2.1, and I.2.2

Condition I applies to the P-11 interlock.

With one or more required channels inoperable, the operator must verify that the interlock is in the required state for the existing unit condition. This action manually accomplishes the function of the interlock. Determination must be made within 1 hour. The 1 hour Completion Time is equal to the time allowed by LCO 3.0.3 to initiate shutdown actions in the event of a complete loss of ESFAS function.

If the interlock is not in the required state (or placed in the required state) for the existing unit condition, the unit must be placed in MODE 3 within the next 6 hours and MODE 4 within the following 6 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. Placing the unit in MODE 4 removes all requirements for OPERABILITY of this interlocks.

J.1 [and J.2]

Condition J applies to the Actuation Logic and Actuation Outputs for the Emergency Feedwater Actuation.

The action addresses the train orientation of the PSMS for ~~these functions.~~ this Function.

If one required train is inoperable, 72 hours are allowed to restore the train to OPERABLE status. ~~The 72 hours allowed for restoring the inoperable train to OPERABLE status is reasonable considering that the safety function can be performed by the remaining OPERABLE trains, and the low probability of an event occurring during this interval. The Completion Time also~~

The Completion Time of 72 hours is justified because the two remaining OPERABLE trains are adequate to perform the safety function. In addition, the Completion Time considers that the two remaining OPERABLE trains each have continuous automatic self-testing.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

[Required Action J.2 allows the option to apply the requirements of Specification 5.5.18 to determine a Risk Informed Completion Time.]

The Required Actions are modified by a Note that allows placing one train to be bypassed required train in bypass for up to 4 hours ~~for while performing~~ surveillance testing, provided the other required trains are OPERABLE. ~~This allowance is based on the assumption that 4 hours is the average time required to perform channel surveillance.~~

~~The bypassed condition for up to 4 hours and the initial completion time of 72 hours are~~ The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE trains have continuous automatic self-testing.

~~The Bypass Time of 4 hours is also justified in the PSMS-US-APWR reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6B.12. The and risk analyses, the summary and result of the PSMS reliability analysis is evaluated and confirmed which are documented in the US-APWR PRA/FSAR Chapter 19 (Ref. 11).~~

K.1

Condition K applies to the failure of one Containment High Range Area Radiation ~~monitor~~ channel. Since the three Containment High Range Area Radiation ~~monitors~~ channels measure the same parameters, failure

of a single channel does not result in loss of the radiation monitoring Function for any events.

If one required channel is inoperable, 72 hours are allowed to restore the channel to OPERABLE status ~~or to place it in the tripped condition.~~ ~~Generally this Condition applies to functions that operate on two-out-of-three logic. Therefore, failure.~~ Failure of one channel places the Function in a two-out-of-two configuration. ~~One channel must be tripped to place the Function in a one-out-of-three configuration that satisfies redundancy requirements.~~

The ~~72-Completion Time of 72~~ hours ~~allowed~~ to restore the inoperable channel ~~to OPERABLE status or to place it in the tripped condition~~ is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the two remaining OPERABLE channels have continuous automatic self-testing (as described for COT), and continuous automatic CHANNEL CHECKS.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19. (Ref. 11).

~~Failure to restore the inoperable channel to OPERABLE status or place it in the tripped condition within 72 hours requires the unit be placed in MODE 3 within the following 6 hours and MODE 5 within the next 30 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. In MODE 5, these Functions are no longer required OPERABLE.~~

~~The initial completion time of 72 hours is justified in the PSMS reliability analysis, considering that the remaining operable channels have continuous self-testing. For detail information, refer to the US-APWR Technical Report MUAP-07030-PRA, Attachment 6B.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~

L.1

Condition L applies to the Containment Purge Isolation - Actuation Logic and Actuation ~~Output~~Outputs Function and addresses the train orientation of the Engineered Safety Features Actuation System (ESFAS). #Condition L also addresses the failure of multiple Containment Purge Isolation - Containment High Range Area Radiation ~~Monitoring~~ channels, or the ~~inability to restore a single failed channel to OPERABLE status in the time allowed for Required Action K.4~~Required Action and associated Completion Time of Condition K not met.

If ~~an a train of~~ Actuation Logic and Actuation ~~Output train~~ Outputs is inoperable, multiple required channels of Containment High Range Area Radiation ~~Monitoring channels~~ are inoperable, or the Required Action and associated Completion Time of Condition K are not met, operation may continue as long as the Required Action for the applicable Conditions of LCO 3.6.3 is met for each valve made inoperable by failure of isolation instrumentation.

M.1 and M.2

Condition M applies to ~~the Actuation Logic and Actuation Outputs Function of the MCR Isolation, the Main Control Air monitor Functions, and the Manual Initiation Functions.;~~

~~If one Actuation Logic and Actuation Outputs train is inoperable, one Main Control Room Radiation channel is inoperable in one or more Functions, or one Manual Initiation train is inoperable, 7 days are permitted to restore it to OPERABLE status. The 7 day Completion Time is the same as is allowed if one train of the mechanical portion of the system is inoperable. The basis for this Completion Time is the same as provided in LCO 3.7.10. If the channel/train cannot be restored to OPERABLE status, one train of the affected subsystem(s) must be placed in the emergency mode of operation. This accomplishes the actuation instrumentation Function and places the unit in a conservative mode of operation.~~

- Low Pressurizer Pressure.
- ~~Affected subsystems depend on inoperable train, as follows.~~ Low Main Steam Line Pressure.
- ~~If train A or D is inoperable, MCREFS doesn't satisfy the single failure criterion. Therefore, one train MCREFS is placed on emergency mode. MCRATCS is unaffected, since three required trains remain operable.~~
- ~~If train B or C is inoperable, MCREFS is unaffected and three required trains of MCRATCS remain operable. Therefore, no action is required.~~
- Low T_{avg} .
- Low-Low T_{avg} .
- High Pressurizer Water Level.
- High Main Steam Line Pressure Negative Rate.
- High SG Water Level.
- Low SG Water Level, and
- High-High SG Water Level.

N.1.1, N.1.2, and N.2

~~Condition N applies to the failure of two MCR Isolation Actuation Logic and Actuation Outputs trains, two Main Control Room Radiation channels, or two Manual Initiation trains for one or more Functions. The first Required Action is to place the affected subsystem(s) in the emergency mode of operation immediately. For MCREFS this requires one train, since each is 100% capacity. Two trains of MCRATCS are required since each is 50% capacity. This accomplishes the actuation instrumentation Function that may have been lost and places the unit in a conservative mode of operation. The applicable Conditions and Required Actions of LCO 3.7.10 must also be entered for the MCRVS train made inoperable by the inoperable actuation instrumentation. This ensures appropriate limits are placed upon train inoperability as discussed in the Bases for LCO 3.7.10.~~

~~Alternatively, all trains of the affected subsystem(s) may be placed in the emergency mode. This ensures the MCR Isolation function is performed even in the presence of a single failure.~~

~~Affected subsystems depend on inoperable train, as follows.~~

- ~~• If trains A and D are inoperable, MCREFS is completely inoperable. Therefore, one train of MCREFS is placed on emergency mode and the required action of MCRVS is applied (to restore in 7 days). Or two trains of MCREFS are placed on emergency mode. And one train of MCRATCS is placed on emergency mode, since MCRATCS does not satisfy the single failure criterion.~~
- ~~• If trains A and B, or A and C, or B and D, or C and D are inoperable, one train of MCREFS and one train of MCRATCS is placed on emergency mode since both subsystems don't satisfy the single failure criterion.~~
- ~~• If trains B and C are inoperable, MCREFS is unaffected. One train of MCRATCS is placed on emergency mode since MCRATCS does not satisfy the single failure criterion.~~

With one required channel inoperable the inoperable channel must be placed in the trip condition within 1 hour and restored to OPERABLE status in 72 hours.

This Condition applies to functions that operate on two-out-of-three logic and have channels that are shared with the control systems. Failure of one channel places the Function in a two-out-of-two configuration, when the failed channel does not result in a trip channel. Normally the SSA can prevent erroneous control system operations. However, when there are less than three OPERABLE channels, the SSA cannot prevent erroneous control system operation due to an input failure. With two OPERABLE channels and one channel in the trip condition, if a channel failure occurs in an OPERABLE channel and results in erroneous control system operation, the remaining OPERABLE channel can provide a plant trip. However, the channel that causes the erroneous control system operation

cannot be credited as the single failure; therefore, this configuration does not satisfy the single failure criteria. To satisfy the single failure criteria, three channels must be restored to OPERABLE status within 72 hours.

The Completion Time of 1 hour to place the failed channel in the trip condition is based on operating experience and the minimum amount of time allowed for manual operator actions.

The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the two remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

The Completion Time of 72 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19. (Ref.11).

Bypass of a required channel is not allowed because there are only three required channels and these channels are also used for control. If a failure were to occur in one of the two remaining control channels, a plant transient could occur that would require a plant trip, but a plant transient would not occur with only one remaining OPERABLE channel.

N.1 and N.2

If the Required Action and associated Completion Time of Condition M are not met, the unit must be brought to MODE 3 within the next 6 hours and MODE 4 within the following 6 hours. Placing the unit in MODE 4 removes all requirements for OPERABILITY of the protection channels and actuation functions. In this MODE, the unit does not have analyzed transients or conditions that require the explicit use of the protection functions noted above.

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.

O.1 and O.2

~~Condition O applies when the Required Action and associated Completion Time for Condition M or N have not been met and the unit is in MODE 1, 2, 3, or 4. The unit must be brought to a MODE in which the LCO requirements are not applicable. To achieve this status, the unit must be brought to MODE 3 within 6 hours and 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.~~
Condition O applies to the S-VDU trains for the Manual Control of ESF Components Function.

If one train is inoperable, 72 hours are allowed to restore the train to OPERABLE status. If the inoperable S-VDU train cannot be restored to OPERABLE status, the applicable Conditions and Required Actions must be entered for ESF components made inoperable by the inoperable S-VDU train. This ensures appropriate limits are placed upon train inoperability. LCO 3.4 through 3.7 provide MODE and train requirements applicable to ESF components.

P.1

~~Condition P applies when the Required Action and associated Completion Time for Condition M or N have not been met when irradiated fuel assemblies are being moved. Movement of irradiated fuel assemblies must be suspended immediately to reduce the risk of accidents that would require MCR Isolation actuation.~~

The Required Actions are modified by a Note that allows placing one train in bypass for up to 4 hours while performing surveillance testing, provided the other trains are OPERABLE. This 4 hour Bypass Time is reasonable based on operating experience that 4 hours is the average time required to perform a train surveillance.

The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition the Bypass Time considers that the remaining OPERABLE trains have continuous automatic self-testing.

P.1, P.2

Condition P applies to the COM-2 trains for the Manual Control of ESF Components Function.

If one train is inoperable, 12 hours are allowed to restore the train to OPERABLE status. If the inoperable COM-2 train cannot be restored to OPERABLE status, the applicable Conditions and Required Actions must be entered for the affected train of all ESF components made inoperable by the inoperable COM-2 train. This ensures appropriate limits are placed upon train inoperability. LCO 3.4 through 3.7 provide MODE and train requirements applicable to ESF components.

The Required Actions are modified by a Note that allows placing one train in bypass for up to 4 hours while performing surveillance testing, provided the other trains are OPERABLE. This 4 hour Bypass Time is reasonable based on operating experience that 4 hours is the average time required to perform a train surveillance.

The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE trains have continuous automatic self-testing.

Q.1 [and Q.2]

Condition Q applies to the Actuation Logic and Actuation Outputs for the following functions:

- ECCS Actuation, and
- Containment Spray.

This action addresses the train orientation of the PSMS.

If one required train is inoperable, 24 hours are allowed to restore the train to OPERABLE status. ~~The 24 hours allowed for restoring the inoperable train to OPERABLE status is reasonable considering that there are sufficient trains OPERABLE to ensure the capability of the required Function, and the low probability of an event occurring during this interval.~~

The Completion Time ~~also of 24 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Completion Time~~ considers that the remaining OPERABLE trains each have continuous automatic self-testing.

The Completion Time of 24 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

[Required Action Q.2 allows the option to apply the requirements of Specification 5.5.18 to determine a Risk Informed Completion Time. This Required Action is not applicable in MODE 4, because Risk Informed Completion Times are only applicable to MODES 1, 2 and 3.]

The Required Actions are modified by a Note that allows placing one train to be bypassed required train in bypass for up to 4 hours ~~for while~~ performing surveillance testing, provided the other ~~train(s) is required~~ trains are OPERABLE. This ~~allowance is 4 hour Bypass Time is reasonable~~ based on ~~the reliability analysis assumption operating experience~~ that 4 hours is the average time required to perform a train surveillance.

~~The bypassed condition for up to 4 hours and the initial completion time of 24 hours are~~ The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE trains have continuous automatic self-testing.

The Bypass Time of 4 hours is also justified in the PSMS-US-APWR reliability analysis. ~~For detail information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6B.12. The and risk analyses, the summary and result of the PSMS reliability analysis is evaluated and confirmed which are documented in the US-APWR PRA FSAR Chapter 19 (Ref. 11).~~

R.1 and R.2

Condition R applies to the Actuation Logic and Actuation Outputs for the following functions:

- ECCS Actuation, and
- Containment Spray,

If the ~~train cannot be restored to OPERABLE status~~ Required Action and associated Completion Time of Condition Q are not met, the unit must be placed in a MODE in which the LCO does not apply. This is done by placing the unit in at least MODE 3 within 6 hours and in MODE 5 within an additional 30 hours (36 hours total time).

The 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.

S.1 [and S.2]

Condition S applies to the Actuation Logic and Actuation Outputs for the;

- Main Steam Line Isolation,
- Main Feedwater Isolation, and
- Block Turbine Bypass and Cooldown Valves.

The action addresses the train orientation of the PSMS for these ~~functions.~~ Functions.

If one train is inoperable, 24 hours are allowed to restore the train to OPERABLE status. ~~The 24 hours allowed for restoring the inoperable train to OPERABLE status is reasonable considering that the safety function can be performed by the remaining OPERABLE trains, and the low probability of an event occurring during this interval. The Completion Time also~~

The Completion Time of 24 hours is justified because the remaining OPERABLE train is adequate to perform the safety function. In addition, the Completion Time considers that the remaining OPERABLE trains each have ~~train has~~ continuous automatic self-testing.

The Completion Time of 24 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

[Required Action S.2 allows the option to apply the requirements of Specification 5.5.18 to determine a Risk Informed Completion Time.]

The Required Actions are modified by a Note that allows placing one train ~~to be bypassed~~in bypass for up to 4 hours ~~for~~while performing surveillance testing, provided the other ~~trains are~~train is OPERABLE. ~~This allowance is based on the assumption that 4 hours is the average time required to perform channel surveillance.~~

~~The bypassed condition for up to 4 hours and the initial completion time of 24 hours are~~The Bypass Time of 4 hours is justified because the remaining OPERABLE train is adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE train has continuous automatic self-testing.

~~The Bypass Time of 4 hours is also justified in the PSMS-US-APWR reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6B.12. The and risk analyses, the summary and result of the PSMS reliability analysis is evaluated and confirmed which are documented in the US-APWR PRAFSAR Chapter 19 (Ref. 11).~~

T.1 and T.2

Condition T applies to the Actuation Logic and Actuation Outputs for the following functions:

- Main Steam Line Isolation,
- Main Feedwater Isolation,
- Emergency Feedwater Actuation, and
- Block Turbine Bypass and Cooldown Valves.

Condition T applies when the Required Action and associated Completion Time for Condition J or S have not been met.

If the train cannot be returned to OPERABLE status, the unit must be brought to MODE 3 within the next 6 hours and MODE 4 within the following 6 hours (12 hours total time). ~~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.~~ Placing the unit in MODE 4 removes all requirements for OPERABILITY of the protection channels and actuation functions. In this MODE, the unit does not have analyzed transients or conditions that require the explicit use of the protection functions.

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.

U.1

Condition U applies when one MCR Outside Air Intake Radiation monitoring channel is inoperable in one or more Functions. There are two 100% capacity MCREFS Trains A and D, with two trains required, and four 50% capacity MCRATCS Trains A, B, C and D, with three trains required. There are two channels, A and D, for each of three MCR Outside Air Intake Radiation monitoring Functions, with two channels required for each function. An inoperable MCR Outside Air Intake Radiation monitoring channel affects all MCREFS and MCRATCS trains.

If one channel for any of the MCR Outside Air Intake Radiation monitoring Functions is inoperable, the instrumentation Function of MCREFS and MCRATCS can provide 100% capacity but doesn't satisfy the single failure criterion. Therefore, within 7 days one MCREFS train and two MCRATCS trains are placed in the emergency mode. With these trains in the emergency mode, 100% capacity is provided for MCR Outside Air Intake Radiation monitoring Functions. In addition, with one OPERABLE MCR Outside Air Intake Radiation monitoring channel remaining for all Functions, an additional MCREFS train and MCRATCS train are capable of automatic initiation, therefore all MCR Outside Air Intake Radiation monitoring Functions meet the single failure criterion.

The 7 day Completion Time is the same as is allowed if one train of the mechanical portion of the system is inoperable. The basis for this Completion Time is the same as provided in LCO 3.7.10 for the mechanical systems.

The emergency mode of operation requires components of the specified trains to be manually placed in the position that they would be automatically actuated to by the MCR Isolation signal. In addition, the controlled components must be configured to prevent erroneous component repositioning from spurious signals from Operational VDUs by manually activating the MCRVS O-VDU Disconnect function. This action is needed because the automatic initiation signals are credited to override any spurious Operational VDU signals, but those signals are affected in this Condition. These two actions accomplish the actuation instrumentation Function and place the unit in a conservative mode of operation.

The "emergency mode" for this Condition, is defined as the pressurization mode specified in LCO 3.7.10. Automatic transfer to the isolation mode for protection against smoke ingress [or toxic gas] is not affected by this condition.

V.1, V. 2.1, and V. 2.2

Condition V applies when two MCR Outside Air Intake Radiation monitoring channels are inoperable in one or more Functions. There are two 100% capacity MCREFS trains, A and D, with two trains required.

and four 50% capacity MCRATCS trains, A, B, C and D, with three trains required. There are two channels, A and D, for each of three MCR Outside Air Intake Radiation monitoring Functions, with two channels required for each function. Two inoperable MCR Outside Air Intake Radiation monitoring channels affect all MCREFS and MCRATCS trains.

If two MCR Outside Air Intake Radiation monitoring channels for the same Function are inoperable in one or more Functions, the MCREFS and MCRATCS instrumentation Functions are completely inoperable. Therefore, one MCREFS train and two MCRATCS trains are immediately placed in the emergency mode. With these trains in the emergency mode, 100% capacity is provided for all MCR Outside Air Intake Radiation monitoring Functions, but the system does not meet the single failure criterion.

Action must be taken within 7 days to restore compliance to the single failure criteria by either restoring one channel of each MCR Outside Air Intake Radiation monitoring Function to OPERABLE status (V.2.1), or placing two trains of MCREFS and three trains of MCRATCS in the emergency mode (V.2.2).

For V.2.1, with one MCREFS train and two MCRATCS trains in the emergency mode, and one additional train of each Function capable of automatic initiation, the system provides 100% capacity and satisfies the single failure criterion.

For V.2.2, with two trains of MCREFS and three trains of MCRATCS in the emergency mode, the system provides 100% capacity and satisfies the single failure criterion.

The 7 day Completion Time is the same as is allowed if one train of the mechanical portion of the system is inoperable. The basis for this Completion Time is the same as provided in LCO 3.7.10 for the mechanical systems.

The emergency mode of operation requires components of the specified trains to be manually placed in the position that they would be automatically actuated to by the MCR Isolation signal. In addition, the controlled components must be configured to prevent erroneous component repositioning from spurious signals from Operational VDUs by manually activating the MCRVS O-VDU Disconnect function. This action is needed because the automatic initiation signals are credited to override any spurious Operational VDU signals, but those signals are affected in this Condition. These two actions accomplish the actuation instrumentation Function and place the unit in a conservative mode of operation.

The “emergency mode” for this Condition, is defined as the pressurization mode specified in LCO 3.7.10. Automatic transfer to the isolation mode

for protection against smoke ingress [or toxic gas] is not affected by this condition.

W.1

Condition W applies when one train, A or D, of the MCR Isolation Actuation Logic and Actuation Outputs Function is inoperable, or one train, A or D, of the MCR Isolation Manual Initiation Function is inoperable. There are two 100% capacity MCREFS trains, A and D, with two trains required, and four 50% capacity MCRATCS trains, A, B, C and D, with three trains required. There are four Manual Initiation trains, with three trains required, including Trains A and D.

If Train A or D of the MCR Isolation Actuation Logic and Actuation Outputs Function or the MCR Isolation Manual Initiation Function is inoperable, the instrumentation of MCREFS provides 100% capacity but doesn't satisfy the single failure criterion. Therefore, within 7 days the affected train of MCREFS is placed in the emergency mode. With one train in the emergency mode the system provides 100% capacity, and with the remaining OPERABLE MCREFS train capable of automatic actuation, the system satisfies the single failure criterion for automatic actuation. In addition, with the remaining OPERABLE MCREFS train capable of Manual Initiation, the system satisfies the single failure criterion for Manual Initiation.

The 7 day Completion Time is the same as is allowed if one train of the mechanical portion of the system is inoperable. The basis for this Completion Time is the same as provided in LCO 3.7.10 for the mechanical systems.

Although one instrumentation train of MCRATCS is inoperable due to inoperable Train A or D, there is no Required Action to place any train of MCRATCS in the emergency mode, since three required instrumentation trains of MCRATCS are unaffected and remain OPERABLE.

If Train B or C is inoperable, the instrumentation of MCREFS is unaffected. Although one instrumentation train of MCRATCS is inoperable, there is no Required Action to place any train of MCRATCS in the emergency mode, since three required instrumentation trains of MCRATCS are unaffected and remain OPERABLE.

The emergency mode of operation requires components of the specified train to be manually placed in the position that they would be automatically actuated to by the MCR Isolation signal. In addition, when the ESFAS is inoperable (which affects automatic actuation and manual initiation), but the SLS remains OPERABLE, the controlled components must be configured to prevent erroneous component repositioning from spurious signals from Operational VDUs by manually activating the MCRVS O-VDU Disconnect function. This action is needed because the automatic actuation signals are credited to override any spurious Operational VDU signals, but those signals are affected in this Condition.

These two actions accomplish the actuation instrumentation Function and place the unit in a conservative mode of operation.

[The “emergency mode” for this Condition, is defined as the pressurization mode specified in LCO 3.7.10. While operating in the pressurization mode, smoke ingress must be manually monitored and may require prompt manual transfer to the emergency isolation mode. This is because when the MCR Isolation Actuation Logic and Actuation Outputs Function is inoperable, manual transfer from the MCR to the isolation mode for smoke protection and automatic transfer to the isolation mode for smoke protection, are affected.]

OR The “emergency mode” for this Condition, is defined as the isolation mode specified in LCO 3.7.10, to accommodate toxic gas protection.]

X.1, X.2.1, X.2.2, X.3.1 and X.3.2

Condition X applies when Trains A and D of the MCR Isolation Actuation Logic and Actuation Outputs Function are inoperable, or Trains A and D of the MCR Isolation Manual Initiation Function are inoperable. There are two 100% capacity MCREFS trains, A and D, with two trains required, and four 50% capacity MCRATCS trains, A, B, C and D, with three trains required. There are four Manual Initiation trains, with three trains required, including Trains A and D. Other inoperable two-train combinations are addressed in Condition Y.

Inoperable Trains A and D affect MCREFS and MCRATCS. The effects and required actions are as follows:

MCREFS

If two Actuation Logic and Actuation Outputs trains (A and D) are inoperable, or two MCR Isolation Manual Initiation trains (A and D) are inoperable, the MCREFS Function is completely inoperable. Therefore, one train of MCREFS is immediately placed in the emergency mode. With one train in the emergency mode MCREFS provides 100% capacity, but does not meet the single failure criterion.

Action must be taken within 7 days to restore compliance to the single failure criteria by either restoring one train of MCREFS instrumentation to OPERABLE status with the other train in the emergency mode (X.2.1), or placing two trains of MCREFS in the emergency mode (X.2.2).

For X.2.1, with one train of MCREFS in the emergency mode and one train capable of automatic actuation and manual initiation, MCREFS provides 100% capacity and satisfies the single failure criterion for automatic actuation and manual initiation.

For X.2.2, with two trains of MCREFS in the emergency mode, the MCREFS provides 100% capacity and satisfies the single failure criterion.

MCRATCS

If two Actuation Logic and Actuation Outputs trains (A and D) are inoperable, or if two MCR Isolation Manual Initiation trains (A and D) are inoperable, the two remaining OPERABLE instrumentation trains (B and C) of MCRATCS provide 100% capacity, but do not meet the single failure criterion.

Action must be taken within 7 days to restore compliance to the single failure criteria by either restoring one affected train of MCRATCS to OPERABLE status (X.3.1), or placing one affected train of MCRATCS in the emergency mode (X.3.2).

For X.3.1, with three trains of MCRATCS capable of automatic actuation and manual initiation, MCRATCS provides 100% capacity and satisfies the single failure criterion for automatic actuation and manual initiation.

For X.3.2 with one train in the emergency mode and two trains capable of automatic actuation and manual initiation, MCRATCS provides 100% capacity and satisfies the single failure criterion for automatic actuation and manual initiation.

The 7 day Completion Time is the same as is allowed if one train of the mechanical portion of the system is inoperable. The basis for this Completion Time is the same as provided in LCO 3.7.10 for the mechanical systems.

The emergency mode of operation requires components of the specified train(s) to be manually placed in the position that they would be automatically actuated to by the MCR Isolation signal. In addition, when the ESFAS is inoperable (which affects automatic and manual initiation), but the SLS remains OPERABLE, the controlled components must be configured to prevent erroneous component repositioning from spurious signals from Operational VDUs by manually activating the MCRVS O-VDU Disconnect function. This action is needed because the automatic actuation signals are credited to override any spurious Operational VDU signals, but those signals are affected in this Condition. These two actions accomplish the actuation instrumentation Function and place the unit in a conservative mode of operation.

[The “emergency mode” for this Condition, is defined as the pressurization mode specified in LCO 3.7.10. While operating in the pressurization mode, smoke ingress must be manually monitored and may require prompt manual transfer to the emergency isolation mode. This is because when the MCR Isolation Actuation Logic and Actuation Outputs Function is inoperable, manual transfer from the MCR to the

isolation mode for smoke protection and automatic transfer to the isolation mode for smoke protection, are affected.

OR the “emergency mode” for this Condition, is defined as the isolation mode specified in LCO 3.7.10, to accommodate toxic gas protection.]

Y.1 and Y.2

Condition Y applies when two MCR Isolation Actuation Logic and Actuation Outputs trains or two MCR Isolation Manual Initiation trains are inoperable, except for inoperable Trains A and D, which are addressed in Condition X. There are two 100% capacity MCREFS trains, A and D, with two trains required, and four 50% capacity MCRATCS trains, A, B, C and D, with three trains required. There are four Manual Initiation trains, with three trains required, including Trains A and D.

The affected Functions and Required Actions depend on the inoperable trains, as follows:

- If Trains A and B, or A and C, or B and D, or C and D are inoperable, the one remaining OPERABLE instrumentation train of MCREFS and the two remaining OPERABLE instrumentation trains of MCRATCS provide 100% capacity, but they don't meet the single failure criterion. Action must be taken within 7 days to restore compliance to the single failure criteria by either restoring the affected instrumentation train of MCREFS and one affected instrumentation train of MCRATCS to OPERABLE status (Y.1), or placing the affected train of MCREFS and one affected train of MCRATCS in the emergency mode (Y.2).

For Y.1, with two trains of MCREFS and three trains of MCRATCS capable of automatic actuation and manual initiation, MCREFS and MCRATCS provide 100% capacity and satisfy the single failure criterion for automatic actuation and manual initiation.

For Y.2, with one train of MCREFS in the emergency mode and one train capable of automatic actuation and manual initiation, MCREFS provides 100% capacity and satisfies the single failure criterion for automatic actuation and manual initiation. With one train of MCRATCS in the emergency mode and two trains capable of automatic actuation and manual initiation, MCRATCS provides 100% capacity and satisfies the single failure criterion for automatic actuation and manual initiation.

- If trains B and C are inoperable, the instrumentation of MCREFS is unaffected. The two remaining OPERABLE instrumentation trains of MCRATCS provide 100% capacity, but do not meet the single failure criterion.

Action must be taken within 7 days to restore compliance to the single failure criteria by either restoring one affected instrumentation train of

MCRATCS to OPERABLE status (Y.1) or placing one affected train of MCRATCS in the emergency mode (Y.2).

For Y.1, with three trains of MCRATCS capable of automatic actuation or manual initiation, MCRATCS provides 100% capacity and satisfies the single failure criterion for automatic actuation and manual initiation.

For Y.2, with one train of MCRATCS in the emergency mode and two trains capable of automatic actuation and manual initiation, MCRATCS provides 100% capacity and satisfies the single failure criterion for automatic actuation and manual initiation.

The 7 day Completion Time is the same as is allowed if one train of the mechanical portion of the system is inoperable. The basis for this Completion Time is the same as provided in LCO 3.7.10 for the mechanical systems.

The emergency mode of operation requires components of the specified train(s) to be manually placed in the position that they would be automatically actuated to by the MCR Isolation signal. In addition, when the ESFAS is inoperable (which affects automatic actuation and manual initiation), but the SLS remains OPERABLE, the controlled components must be configured to prevent erroneous component repositioning from spurious signals from Operational VDUs by manually activating the MCRVS O-VDU Disconnect function. This action is needed because the automatic actuation signals are credited to override any spurious Operational VDU signals, but those signals are affected in this Condition. These two actions accomplish the actuation instrumentation Function and place the unit in a conservative mode of operation.

[The “emergency mode” for this Condition, is defined as the pressurization mode specified in LCO 3.7.10. While operating in the pressurization mode, smoke ingress must be manually monitored and may require prompt manual transfer to the emergency isolation mode. This is because when the MCR Isolation Actuation Logic and Actuation Outputs Function is inoperable, manual transfer from the MCR to the isolation mode for smoke protection and automatic transfer to the isolation mode for smoke protection, are affected.

OR the “emergency mode” for this Condition, is defined as the isolation mode specified in LCO 3.7.10, to accommodate toxic gas protection.]

Z.1 and Z.2

Condition Z applies when the Required Action and associated Completion Time for Condition U, V, W, X or Y have not been met and the unit is in MODE 1, 2, 3, or 4. The unit must be brought to a MODE in which the LCO requirements are not applicable. To achieve this status, the unit must be brought to MODE 3 within 6 hours and 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.

AA.1

Condition AA applies when the Required Action and associated Completion Time for Condition U, V, W, X or Y have not been met when irradiated fuel assemblies are being moved. Movement of irradiated fuel assemblies must be suspended immediately to reduce the risk of accidents that would require MCR Isolation actuation.

BB.1, BB.2.1 and BB.2.2

Condition BB applies to the P-4 Interlock.

This action addresses the train orientation of the PSMS.

If a required train is inoperable, 48 hours are allowed to restore the train to OPERABLE status.

The Completion Time of 48 hours is justified because the two remaining OPERABLE trains are adequate to perform the safety function. In addition, the Completion Time considers that the two remaining OPERABLE trains each have continuous automatic self-testing.

The Completion Time of 48 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 11).

If the train cannot be restored to OPERABLE status, the unit must be placed in MODE 3 within the next 6 hours and MODE 4 within the following 6 hours. In MODE 4, the unit does not have any analyzed transients or conditions that require the explicit use of the interlock function noted above.

The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power in an orderly manner and without challenging unit systems.

BASES

SURVEILLANCE REQUIREMENTS

The SRs for each ESFAS Function are identified by the SRs column of Table 3.3.2-1.

A Note has been added to the SR Table to clarify that Table 3.3.2-1 determines which SRs apply to which ESFAS Functions.

Note that each channel of process protection supplies all trains of the ESFAS. However, when testing a channel, it is only necessary to manually verify that the channel is OPERABLE in its respective division.

This is because the interface to other divisions is automatically verified through continuous automatic self-testing. ~~Self~~Continuous automatic self-testing is confirmed through periodic ~~GOT and ACTUATION LOGIC TEST.MIC~~. The CHANNEL CALIBRATION is performed in a manner that is consistent with the methods and assumptions of ~~Section~~Specification 5.5.21, Setpoint Control Program (SCP).

SR 3.3.2.1

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

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

[The Surveillance Frequency of 12 hours is based on operating experience that demonstrates channel failure is rare. The CHANNEL CHECK supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the LCO required channels. ~~OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

A CHANNEL CHECK may be conducted manually or automatically. For the US-APWR an automated CHANNEL CHECK is normally conducted continuously, which satisfies the 12 hour Surveillance Frequency requirement. Where the CHANNEL CHECK is conducted automatically, an alarm shall be generated when the agreement criteria is not met. If the automated CHANNEL CHECK function is unavailable, a manual CHANNEL CHECK shall be conducted at the minimum 12 hour Surveillance Frequency.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

~~The equipment that performs the automated CHANNEL CHECK, and automatic self-testing described for GOT and ACTUATION LOGIC TEST,~~

~~shall be confirmed OPERABLE including the capability to generate fault alarms.~~

SR 3.3.2.2

~~SR~~ SR 3.3.2.2 is the performance of an ACTUATION LOGIC TEST. a MIC for the ESFAS Instrumentation. This includes the Safety VDU processors, the RPS, the ESFAS, the SLS, and the COM-2.

The PSMS is self-tested automatically on a continuous basis from the digital side of all input modules to the digital side of all output modules. Self-Continuous automatic self-testing encompasses all PSMS safety-related functions including digital Nominal Trip Setpoints, Time Constants, Time Delays and actuation logic functions. The continuous automatic self-testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS.- The continuous automatic self-testing is described in Reference 6 and Reference 7.

~~-The ACTUATION LOGIC TEST MIC is a diverse check of the ESFAS PSMS software memory integrity, consistent with the Setpoint Control Program (SCP), to ensure there is no change to the internal ESFAS PSMS software that would impact its functional operation, including digital Nominal Trip Setpoints, Time Constants, Time Delays, actuation logic functions or the continuous self-test function. automatic self-testing. The software memory integrity test MIC is described in Reference 6 and Reference 7. [The Frequency of every 24 months is justified based on the reliability of the PSMS. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

The capability to generate continuous automatic self-testing fault alarms shall be confirmed OPERABLE during the MIC.

The complete ~~continuity~~ OPERABILITY check from the measurement channel input device to the SLS output device is performed by the combination of the continuous ~~CHANNEL CHECK, and the 24-month CHANNEL CALIBRATION~~ automatic self-testing for the ~~non-digital side of devices~~ (the input module RPS, ESFAS, SLS, and data communication interfaces), the continuous ~~self-testing for~~ automatic CHANNEL CHECK (SR 3.3.2.1), the digital side CHANNEL CALIBRATION (SR 3.3.2.6), the 24-month COT, the 24-month ACTUATION LOGIC TEST MIC (SR 3.3.2.2), and the 24-month ESFAS and SLS TADOT for the non-digital side of the output module. (SR 3.3.2.3, SR 3.3.2.4, SR 3.3.2.5 and SR 3.3.2.8). The ~~Channel~~ CHANNEL CALIBRATION, COT, ACTUATION LOGIC TEST ~~the MIC, and the~~ TADOT, which are manual tests, overlap with the ~~CHANNEL CHECK and~~ continuous automatic self-testing and confirm the functioning of the continuous automatic self-testing.

~~The ACTUATION LOGIC TEST interval~~ The complete OPERABILITY check from the Safety VDU (S-VDU) input device to the SLS output device is performed by the combination of the continuous automatic self-testing for the digital devices (Safety VDU processors, COM-2, SLS and data communication interfaces), the SAFETY VDU TEST (SR 3.3.2.9), MIC for the Safety VDU processors, COM-2 and SLS (SR 3.3.2.2) and TADOT for SLS outputs (SR 3.3.2.3). The SAFETY VDU TEST, MIC, and TADOT, which are manual tests, overlap with the automatic self-testing and confirm the functioning of the automatic tests.

[The Surveillance Frequency of 24 months is justified because the software memory integrity is checked by the continuous automatic self-testing.

The Surveillance Frequency of 24 months ~~with the self test capability is also justified in the PSMS reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6B.12. The reliability and risk analyses, the summary and result of the PSMS reliability analysis is evaluated and confirmed which are documented in the US-APWR PRAFSAR Chapter 19 (Ref. 11).~~

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.2.3

SR 3.3.2.3 is the performance of a ~~COT~~TADOT for the Actuation Outputs of all ESFAS Functions, and the Actuation Outputs of the Manual Control of ESF Components Function. This surveillance test actuates the outputs of the SLS.

~~The PSMS is self-tested on an automatic basis from the digital side of all input modules to the digital side of all output modules. Self testing encompasses all Trip Setpoints and trip functions. The self testing is described in Reference 6 and Reference 7. ESFAS setpoint and bistable functions are implemented within the RPS. Therefore, the COT is a check of the RPS software memory integrity to ensure there is no change to the internal RPS software that would impact its functional operation, including digital Trip Setpoint values or the continuous self test function. The software memory integrity test is described in Reference 6 and Reference 7. Therefore, this test is typically conducted in conjunction with testing the plant process components. Since this test is conducted in conjunction with testing for plant process components, this test may be conducted more frequently, as may be required for the plant process components.~~

~~A COT ensures the entire channel will perform the intended Function.~~ [The Surveillance Frequency of 24 months is adequate, based on industry

operating experience, considering instrument reliability and operating history data of solid state Actuation Output devices.

~~[The Frequency of 24 months is justified based on the reliability of the PSMS. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

~~The complete continuity check from the input device to the output device is performed by the combination of the continuous CHANNEL CHECK, the 24 month CHANNEL CALIBRATION for the non-digital side of the input module, the continuous self-testing for the digital side, the 24 month COT and the 24 month TADOT for the non-digital side of the output module. The Channel CALIBRATION, COT and TADOT, which are manual tests, overlap with the CHANNEL CHECK and self testing and confirm the functioning of the self testing.~~

~~The COT interval of 24 months with the self test capability is justified in the PSMS reliability analysis. For detail information, refer to the US-APWR Technical Report MUAP-07030 PRA, Attachment 6B.12. The result of the PSMS reliability analysis is evaluated and confirmed in the US-APWR PRA Chapter 19.~~

SR 3.3.2.4

SR 3.3.2.4 is the performance of a TADOT for the Loss of Offsite Power Function. The LOP inputs to the ESFAS are tested up to, and including, the signal status readout on a VDU.

Verification of the undervoltage relay Nominal Trip Setpoint is not performed during the TADOT; the undervoltage relay Nominal Trip Setpoint is verified during CHANNEL CALIBRATION.

[The Surveillance Frequency of 92 days is adequate. It is based on industry operating experience, considering instrument reliability and operating history data.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.2.5

SR 3.3.2.5 is the performance of a TADOT for all Manual Initiation Functions and for the EFW Actuation - Trip of all MFW Pumps Function. Each Function is tested up to, and including, the signal status readout on a VDU. These Functions have no associated setpoints.

[The Surveillance Frequency of 24 months is adequate, based on industry operating experience and is consistent with the typical refueling cycle.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.2.4

~~SR 3.3.2.4 is the performance of a TADOT for the Actuation Outputs of all ESFAS functions. This function actuates the outputs of the SLS.~~

~~Therefore, this test is typically conducted in conjunction with testing the plant process components. [The Frequency of 24 months is adequate, based on industry operating experience, considering instrument reliability and operating history data. The Actuation Outputs are solid state devices. Since this test is conducted in conjunction with testing for plant process components, this test may be conducted more frequently, as may be required for the plant process components. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

SR 3.3.2.5

~~SR 3.3.2.5 is the performance of a TADOT for the Loss of Offsite Power, Function. The LOP inputs to the ESFAS are tested up to, and including, the signal status readout on a digital display.~~

~~The SR is modified by a Note that excludes verification of setpoints for relays. Relay setpoints require elaborate bench calibration and are verified during CHANNEL CALIBRATION. [The Frequency of 92 days is adequate. It is based on industry operating experience, considering instrument reliability and operating history data. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

SR 3.3.2.6

~~SR 3.3.2.6 is the performance of a TADOT for all Manual Initiation Functions and EFW pump start on trip of all MFW pumps. Each Manual Initiation Function is tested up to, and including, the signal status readout on a digital display. [The Frequency of 24 months is adequate, based on industry operating experience and is consistent with the typical refueling cycle. CHANNEL CALIBRATION.]~~

CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test must be performed consistent with the methods and assumptions of Specification 5.5.21, SCP, to verify that the

channel responds to a measured parameter within the necessary range and accuracy.

The CHANNEL CALIBRATION confirms the accuracy of the channel from sensor to digital VDU readout, as described in Reference 6.

For analog measurements, the CHANNEL CALIBRATION confirms the calibration settings are within the Allowable Value at multiple points over the entire measurement channel span, encompassing all ESF actuation and interlock Nominal Trip Setpoint values. Digital ESF actuation and interlock Nominal Trip Setpoint values are confirmed through MIC.

For binary measurements, the CHANNEL CALIBRATION confirms the accuracy of the channel's state change. The state change must occur within the Allowable Value of the Nominal Trip Setpoint.

The equipment that performs the automated CHANNEL CHECK shall be confirmed OPERABLE, including the capability to generate fault alarms during the CHANNEL CALIBRATION.

[The Surveillance Frequency of 24 months is based on the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in accordance with Specification 5.5.21, Setpoint Control Program (SCP).

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.] ~~The SR is modified by a Note that excludes verification of setpoints during the TADOT for manual initiation Functions. The manual initiation Functions have no associated setpoints.~~

SR 3.3.2.7

~~SR 3.3.2.7 is the performance of a CHANNEL CALIBRATION.~~

~~CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test verifies that the channel responds to measured parameter within the necessary range and accuracy, as described in Section 5.5.21, SCP.~~

~~For analog measurements, the CHANNEL CALIBRATION confirms the accuracy of the channel from sensor to VDU as described in Reference 6. CHANNEL CALIBRATION confirms the analog measurement accuracy conforms to the Allowable Value at multiple points over the entire measurement channel span, encompassing all reactor trip and interlock Trip Setpoint values. Digital reactor trip and interlock Trip Setpoint values are confirmed through COT.~~

~~For binary measurements, the CHANNEL CALIBRATION confirms the accuracy of the channel's state change, as described in Reference 6. The state change must occur within the Allowable Value of the Trip Setpoint.~~

~~CHANNEL CALIBRATIONS must be performed consistent with the methods and assumptions in Section 5.5.21, SCP. [The Frequency of 24 months is based on the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in accordance with Section 5.5.21, Setpoint Control Program (SCP). OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

~~This SR is modified by a Note stating that this test should include verification that the time constants are adjusted to the prescribed values where applicable.~~

SR-3.3.2.8

This SR ensures the ~~response times for all ESFAS functions are~~ ESF RESPONSE TIME is less than or equal to the maximum ~~values value~~ assumed in the accident analysis. Accident analysis response time values are ~~defined specified~~ in Reference 2. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the ~~Trip Setpoint value at the sensor, Analytical Limit~~ to the point at which the equipment in ~~all trains the minimum credited train(s)~~ reaches the required functional state (e.g., pumps at rated discharge pressure, valves in full open or closed position).

~~The PSMS dynamic transfer functions employ time constants that are installed as digital values and processed through digital algorithms. Therefore, the time response of the dynamic transfer functions has no potential for variation due to time or environmental drift or component aging. The COT confirms the integrity of the time constants and algorithms through the periodic software memory integrity check. The complete PSMS response time is determined one time by analysis and confirmed one time in the factory test. The response times of analog instruments that provide input to the dynamic transfer functions are periodically checked in Surveillance 3.3.2.8, because they do have the potential for response time variation. Electro-mechanical components in the ESFAS have aging or wear-out mechanisms that can impact response time. Response time for other components may be affected by random failures or calibration discrepancies, which are detectable by other testing and calibration methods required by other surveillances.~~

Response time may be verified by actual response time tests in any series of sequential, overlapping or total channel measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the channel.

Allocations for sensors, signal conditioning and actuation logic response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications.

The PSMS MELTAC controllers employ dynamic transfer functions with Time Constants and actuation logic functions with Time Delays that are installed as digital values and processed through digital algorithms. Therefore, the time response of all digital PSMS functions has no

potential for variation due to time, environmental drift or component aging. PSMS Time Constants and Time Delays are set at the nominal values assumed in the safety analysis. The combination of continuous automatic self-testing and MIC confirms the integrity of the dynamic transfer functions, Time Constants, Time Delays and actuation logic functions.

The response time for the digital portion of the PSMS is determined one time by analysis and confirmed one time in the factory test. Therefore, for PSMS digital functions, including Functions with Time Constants and Time Delays, response time tests are not required; instead, a response time allocation may be applied.

Response time for PSMS MELTAC input signal conditioning, can be affected by random failures or degradation, which can be detected by CHANNEL CALIBRATION. Section 4.6 of MUAP-07005, "Safety System Digital Platform -MELTAC-" (Ref. 7) describes the basis for crediting CHANNEL CALIBRATION for detecting PSMS signal conditioning response time degradation. Therefore, for PSMS input signal conditioning, response time tests are not required; instead, a response time allocation may be applied.

MUAP-09021-P-"Response Time of Safety I&C System" (Ref. 8), 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 report. Response time verification for other sensor types must be demonstrated by test. MUAP-09021-P also provides the basis and methodology for using allocated signal processing and actuation logic response times in the overall verification of the protection system channel response time. Section 4.4 of MUAP-07005, "Safety System Digital Platform -MELTAC-" describes how response times of each individual MELTAC module are combined to determine the total digital system response time. In addition, MUAP-09021-P identifies the acceptance criteria for ESFAS components that require response time measurement (such as LOOP undervoltage relays which are known to have aging or wear-out mechanisms that can impact response time), taking into consideration the total ESF RESPONSE TIME requirement and the allocations for other components that do not require testing.

The allocations for sensor, signal conditioning, and actuation logic response times must be verified prior to placing the component in operational service and re-verified following maintenance that may adversely affect response time. In general, electrical repair work does not impact response time provided the parts used for repair are of the same type and value. One example where response time could be affected is replacing the sensing assembly of a transmitter.

[ESF RESPONSE TIME tests are conducted on a 24 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. The final actuation device in one train is tested with each~~

~~channel. Therefore, staggered testing results in response time verification of these devices every 24 months.~~ The 24 month Surveillance Frequency is consistent with the typical refueling cycle and 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.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

This SR is modified by a Note that clarifies that the tests for the turbine driven EFW pumps are conducted within 24 hours after reaching 1000 psig in the SGs.

SR 3.3.2.98

SR 3.3.2.98 is the performance of a TADOT for the P-4 ~~Reactor Trip Interlock, and the~~ The Surveillance Frequency is once per RTB cycle, ~~as required by SR 3.3.1.4.~~ Each RTB status contact is tested up to, and including, the signal status readout on a digital ~~display.~~ VDU. This Surveillance Frequency is based on operating experience demonstrating that undetected failure of the P-4 interlock sometimes occurs when the RTB is cycled.

~~The SR is modified by a Note that excludes verification of setpoints during the TADOT.~~ The ~~Function tested~~ P-4 Interlock has no associated setpoint.

SR 3.3.2.9

SR 3.3.2.9 is the performance of a SAFETY VDU TEST for the Safety VDUs in the MCR. The SAFETY VDU TEST is explained in Reference 6.

This SR confirms the Safety VDU is capable of providing all display and control functions for the MCR. This SR overlaps with the MIC (SR 3.3.2.2), to ensure the S-VDU is OPERABLE.

[The Surveillance Frequency of 24 months is adequate, based on industry operating experience, considering instrument reliability and operating history data. In addition, the Surveillance Frequency considers that all indications and controls for each safety train and channel are available in the MCR on non-safety Operational VDUs.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

BASES

-
- REFERENCES
1. NUREG-0737, "Clarification of TMI Action Plan Requirements."
 2. FSAR Section 7.3.1-
 3. FSAR Chapter 15.
 4. IEEE-603-1991.
 5. 10 CFR 50.49.
 6. MUAP-07004-P (~~Proprietary~~) and MUAP-07004-NP (~~Non-Proprietary~~), Revision 7, "Safety I&C System Description and Design Process."
 7. MUAP-07005-P (~~Proprietary~~) and MUAP-07005-NP (~~Non-Proprietary~~), Revision 8, "Safety System Digital Platform – ~~MELTAC~~."
 8. ~~FSAR Section 8.3.1.8.~~ MUAP-09021-P, Revision 2, "Response Time of Safety I&C System."
 9. 10 CFR 50.36.
 10. FSAR Section 15.7.4.
 11. FSAR Chapter 19.
 12. MUAP-09022-P, Revision 2, "US-APWR Instrument Setpoint Methodology."
 13. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety Related Instrumentation."
 14. FSAR Chapter 9.4.1.2.2.
-

B 3.3 INSTRUMENTATION

B 3.3.3 Post Accident Monitoring (PAM) Instrumentation

BASES

BACKGROUND

The purpose of displaying PAM parameters is to assist [Main Control Room \(MCR\)](#) personnel in evaluating the safety status of the plant. PAM parameters are direct measurements or derived variables representative of the safety status of the plant. The primary function of the PAM parameters is to aid the operator in the rapid detection of abnormal operating conditions. As an operator aid, the PAM variables represent a minimum set of plant parameters from which the plant safety status can be assessed.

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

The availability of accident monitoring instrumentation is important so that responses to corrective actions can be observed and the need for, and magnitude of, further actions can be determined. These essential instruments are identified by ~~Chapter~~ [FSAR Section 7.5](#) (Ref. 4) addressing the recommendations of Regulatory Guide 1.97 (Ref. 1) as required by Supplement 1 to NUREG-0737 (Ref. 2).

The instrument channels required to be OPERABLE by this LCO include parameters based on IEEE 497-2002 (Ref. 5), which is endorsed by Regulatory Guide 1.97 (Ref. 1), identified as Type A, B and C variables.

[FSAR Section 7.5 \(Ref. 4\) describes the PAM Instrumentation, and in particular, the process that was used for determining the bounding list of PAM variables in Table 3.3.3-1.](#)

Type A, B, and C variables are the key variables deemed risk significant because they are needed to:

Type A

Take planned manually controlled actions for accomplishment of safety-related functions for which there is no automatic control.

Type B

Assess the process of accomplishing or maintaining plant critical safety functions.

Type C

Indicate potential for a breach of fission product barriers.
Indicate an actual breach of fission product barriers.



The specific instrument Functions listed in Table 3.3.3-1 are discussed in the LCO section.

APPLICABLE
A, B and C
SAFETY
ANALYSES

The PAM ~~instrumentation~~Instrumentation ensures the operability of Type variables so that the control room operating staff can:

- Perform the diagnosis specified in the emergency operating procedures (these variables are restricted to preplanned actions for the primary success path of ~~PAs~~Postulated Accidents), e.g., loss of coolant accident (LOCA),
- Take the specified, pre-planned, manually controlled actions, for which no automatic control is provided, and that are required for safety systems to accomplish their safety function,
- Determine whether systems important to safety are performing their intended functions,
- Determine the likelihood of a gross breach of the barriers to radioactivity release,
- Determine if a gross breach of a barrier has occurred, and
- Initiate action necessary to protect the public and to estimate the magnitude of any impending threat.

The PAM Instrumentation is interfaced to the Protection and Safety Monitoring System (PSMS) through the Reactor Protection System (RPS), with the exception of Containment Isolation Valve (CIV) position, which is interfaced via the Safety Logic System (SLS). The RPS, including Nuclear Instrumentation System (NIS), and SLS provide signal conditioning, analog to digital conversion, and digital signals for display of the PAM Instrumentation measurements on MCR VDUs.

The PAM Instrumentation is displayed in the MCR via Safety VDUs and non-safety Operational VDUs. Only the Safety VDUs are credited for the PAM Display Function. The S-VDU in each train consists of a VDU and S-VDU processor.

To meet the single failure criteria and accommodate on-line maintenance, four trains of S-VDU, RPS and SLS are provided, each performing the same functions. If one train is taken out of service for maintenance or test purposes, the remaining trains will provide PAM displays for the unit.

The S-VDU, RPS and SLS for each train are packaged in their own cabinet for physical and electrical separation to satisfy separation and independence requirements.

The S-VDU, RPS and SLS have continuous automatic self-testing while in service. When any one train is taken out of service for manual testing, the remaining trains are capable of providing unit monitoring and protection until the testing has been completed.

LCO

The LCO requires all instrumentation performing the PAM Instrumentation Function, listed in Table 3.3.3-1 in the accompanying LCO, to be OPERABLE. A channel is OPERABLE provided the "as-found" value, measured during surveillance testing, does not ~~The PAM instrumentation~~ exceed its associated Allowable Value, and provided the "as-left" value is within the specified calibration tolerance at the completion of each CHANNEL CALIBRATION.

The PAM Instrumentation LCO provides OPERABILITY requirements for Type A variables, which provide information required by the control room operators to perform certain manual actions specified in the unit Emergency Operating Procedures. These manual actions ensure that a system can accomplish its safety function, and are credited in the safety analyses. Additionally, this LCO addresses instruments that have been designated Type B and C.

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

~~LCO 3.3.3 requires two OPERABLE~~The number of channels available for most PAM Instrumentation Functions—Two is shown in FSAR Chapter 7 Table 7.5-3. For PAM Instrumentation Functions with two channels, the channels are assigned to Trains A and D; both channels are required. For PAM Instrumentation Functions with four channels, the channels are assigned to Trains A, B, C and D; the required number of which is two, three, or four depending on the variable.

LCO 3.3.3 requires two, three or four OPERABLE channels. The specified number of OPERABLE channels ensures no single failure prevents operators from getting the information necessary for them to determine the safety status of the unit, and to bring the unit to and maintain it in a safe condition following an accident.

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

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

Due to redundant components within the PSMS, such as controllers, communication links and power supplies, an inoperable component may or may not result in an inoperable channel. Where an inoperable component results in an inoperable required channel, LCOs are entered. For inoperable components that do not result in inoperable channels, LCOs are not entered.

Table 3.3.3-1 provides a list of the PAM variables.

Type A, B, ~~C~~ and ~~D-C~~ variables are required to meet requirements defined in IEEE 497-2002 (Ref. 5) for seismic and environmental qualification, and testability. Type A, B and C variables must also meet requirements for single failure criterion, separation and independence, quality, utilization of emergency standby power, information ambiguity and recording of display. In addition, Type A and B variables require continuously visible displays. These design features are described in Chapter 7 (Ref. 4).

Listed below are discussions of the specified instrument Functions listed in Table 3.3.3-1. ~~These discussions are intended as examples of what should be provided for each Function when the unit specific list is prepared.~~

1. Wide Range Neutron Flux

Wide Range Neutron Flux indication is provided to verify reactor shutdown. ~~The~~ A single wide range instrument for each channel covers the full range of flux that may occur post accident.

Neutron flux is used for accident diagnosis, verification of subcriticality, and diagnosis of positive reactivity insertion.

2,3. Reactor Coolant System (RCS) Hot and Cold Leg Temperatures (Wide Range)

~~RCS Hot and Cold Leg Temperatures are provided for verification of core cooling and long term surveillance.~~ Verification of core cooling can be determined by RCS Hot or Cold Leg Temperature in any one RCS loop. The Emergency Operating Procedure (EOP) operator action threshold points, for events such as steam generator tube rupture, can only be determined by RCS Hot Leg Temperature in any one RCS loop.

In addition, RCS cold leg temperature is used in conjunction with RCS hot leg temperature to verify the unit conditions necessary to establish natural circulation in the RCS.

The PAM function

There is one channel each of RCS Hot Leg and Cold Leg Temperature (Wide Range) to monitor the core cooling condition. There will be little temperature deviation between the Hot Leg and Cold Leg after an accident and reactor shutdown. Thus, Hot Leg and Cold Leg Temperatures can be defined as equivalent parameters to monitor the trend of core cooling. Thus, Hot Leg and RCS Cold Leg Temperature of the same (Wide Range) per loop are pair PAM functions credited for compliance with the single failure criteria. Therefore, only one of each channel of Hot Leg Temperature and Cold Leg Temperature and a minimum of any three loops are required in for each loop, since with a failure of either channel adequate core cooling can still be monitored parameter. Therefore, in any one loop both instruments may be OPERABLE (i.e., RCS Hot Leg and Cold Leg Temperature) or only one instrument may be OPERABLE (i.e., RCS Hot Leg or Cold Leg Temperature).

Only three channels are required for each parameter because if the break is in one of the instrumented loops, the instrumentation in either remaining instrumented loop (i.e., RCS Hot Leg Temperature or RCS Cold Leg Temperature) provides sufficient indication of core cooling, and the EOP operator action threshold points can be confirmed by the RCS Hot Leg Temperature instrumentation in either remaining instrumented loop. Therefore, with only 3 required channels for each parameter (each monitoring any three loops), a single failure affecting one or both instruments (i.e., RCS Hot leg Temperature/RCS Cold Leg Temperature) in any intact loop can be accommodated.

4. Reactor Coolant System Pressure (Wide Range)

RCS ~~wide range pressure~~ Pressure (Wide Range) is provided for verification of core cooling and RCS integrity long term surveillance.

5. Reactor Vessel Water Level

Reactor Vessel Water Level is provided for verification and long term surveillance of core cooling. It is also used for accident diagnosis and to determine reactor coolant inventory adequacy. There are two channels and two channels are required. A channel consists of three sections with two sensors per section. A channel is OPERABLE if at least one sensor is OPERABLE in all three sections.

6. Containment Pressure

Containment Pressure is provided for verification of RCS and containment OPERABILITY and is used to verify closure of main steam isolation valves (MSIVs), and ~~containment spray~~ Phase B ~~isolation~~ Containment Isolation when High-3 ~~containment pressure is~~ Containment Pressure is reached. Additionally, Containment Pressure is provided for indication of maintaining RCS integrity and containment integrity.

7. Containment Isolation Valve Position

Penetration Flow Path CIV Position is provided for verification of Containment OPERABILITY, and Phase A and Phase B ~~isolation~~ isolation.

When used to verify Phase A and Phase B ~~isolation~~isolation, the important information is the isolation status of the containment penetrations. The LCO requires one channel of valve position indication in the control room to be OPERABLE for each active CIV in a containment penetration flow path, i.e., ~~two~~ two total channels of CIV position indication for a penetration flow path with two active valves.

For containment penetrations with only one active CIV having control room indication, Note (b) in Table 3.3.3-1 requires a single channel of valve position indication to be OPERABLE. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve, as applicable, and prior knowledge of a passive valve, or via system boundary status. If a normally active CIV is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

Note (a) ~~to the Required Channels~~in Table 3.3.3-1 states that the Function is not required for isolation valves whose associated penetration is isolated by at least one closed and deactivated automatic valve, closed manual valve, blind flange, or check valve with flow through the valve secured.

Each penetration is treated separately and each penetration flow path is considered a separate function. Therefore, separate Condition entry is allowed for each inoperable penetration flow path.

8. Containment High Range Area Radiation

Containment Area Radiation is provided to monitor for the potential of significant radiation releases and to provide release assessment for use by operators in determining the need to invoke site emergency plans. Containment radiation level is used to determine if a high energy line break (HELB) has occurred, and whether the event is inside or outside of containment.

9. Pressurizer Water Level

Pressurizer Water Level is used to determine whether to terminate ~~S~~ECCS Actuation, if still in progress, or to reinitiate ~~S~~ECCS Actuation if it has been stopped. ~~Knowledge of pressurizer water level~~Pressurizer Water Level is also used to verify the unit conditions necessary to establish natural circulation in the RCS and to verify that the unit is maintained in a safe shutdown condition.

10,11. Steam Generator Water Level (Wide Range and Narrow Range)

SG Water Level is provided to monitor operation of decay heat removal via the SGs. ~~The indication of SG level is the extended startup range level instrumentation. The extended startup range level covers a span above the lower tubesheet.~~

SG Water Level (~~Wide~~Narrow Range) is used to:

- identify the faulted SG following a tube rupture,
- verify that the intact SGs are an adequate heat sink for decay heat removal from the reactor,
- determine the nature of the accident in progress (e.g., verify an SGTR), and
- verify unit conditions for termination of ~~SI~~ECCS Actuation during secondary unit HELBs outside containment.

Operator action is based on the control room indication of SG level. The RCS response during a design basis small break LOCA depends on the break size. For a certain range of break sizes, ~~the boiler condenser mode of heat transfer is~~ SGs are necessary to remove decay heat. ~~Extended startup range level is a Type A variable because the operator must manually raise and control SG level to establish boiler condenser heat transfer. Operator action is initiated on a loss of subcooled margin. Feedwater flow is increased until the indicated extended startup range level reaches the boiler condenser setpoint. This function is an alternate mean with EFW Flow.~~ SG Water Level (Narrow Range) can be used to manually control SG level to remove decay heat via the SGs.

~~The PAM function of Steam Generator Water Level Wide Range and Emergency Feedwater Flow is to monitor heat removal capability of the Steam Generators. Since during accident or shutdown conditions, SG water level is directly attributed to emergency feedwater flow, either provides an indication of SG heat removal capability. Thus the SG Water Level Wide Range and EFW Flow can be defined as equivalent parameters to monitor the heat removal capability of the secondary. Thus, the~~ SG Water Level (Wide Range), which covers the span above the lower tubesheet, is used to verify that the intact SGs are an adequate heat sink for decay heat removal from the reactor.

~~There is one SG Water Level and EFW Flow of same loop are pair PAM functions credited for compliance with the single failure criteria. Therefore, only one of each (Wide Range) channel of SG Water Level and EFW Flow are required in each loop, since with a failure of either channel adequate heat removal capability can still be monitored per loop. All four loops are required because if the break is in one of the instrumented SGs and there is a single failure affecting the instrumentation in another SG, the instrumentation in the remaining two SGs provide sufficient indication of heat sink availability; two SGs are required for sensible heat removal.~~

12, 13, 14, 15. Core Exit Temperature

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

~~Twenty~~For Post Accident Monitoring, ~~twenty~~ six core exit ~~thermocouples~~thermocouple channels are provided for measuring core cooling ~~as the post accident monitors. These thermocouples.~~The thermocouple channels are arranged in two safety trains, A and D, with each train ~~consists~~consisting of thirteen ~~thermocouples.~~ These thermocouples in each train are distributed at the exit of the core nearly uniformly and a minimum of 2 thermocouples are provided for each core quadrant. ~~These distributed thermocouples provide adequate information of temperature distribution of core exit fluid.~~thermocouple channels. A minimum of 2 thermocouple channels from each of two trains (4 total) are required for each core quadrant. For each train and each core quadrant, one thermocouple channel is required near the center of the core and one thermocouple channel is required near the core perimeter. The two thermocouple channels indicate the radial temperature gradient across their core quadrant. The uniform ~~distributions of two train thermocouples ensure the~~distribution of thermocouple channels from both trains ensures adequate information of radial temperature distribution ~~in even with~~ a single train failure condition.

16. Emergency Feedwater Flow

Emergency Feedwater (EFW) Flow is provided to monitor operation of decay heat removal via the SGs.

EFW flow is used three ways:

- to verify delivery of EFW flow to the SGs,
- ~~to determine whether to terminate SI ECCS Actuation if still in progress, in conjunction with SG water level (narrow range), and~~
- ~~to regulate EFW flow so that the SG tubes remain covered.~~
- ~~This function is an alternate mean with SG Water Level: (Narrow Range), and~~
- to verify that the intact SGs are an adequate heat sink for decay heat removal from the reactor.

There is one channel of EFW Flow per loop. All four loops are required, because if the break is in one of the instrumented SGs and there is a single failure affecting the instrumentation in another SG, the instrumentation in the remaining two SGs provide sufficient indication of heat sink availability; two SGs are required for sensible heat removal.

17. Degrees of Subcooling

~~The~~ Degrees of Subcooling is provided for verification of core cooling. Degrees of Subcooling utilizes sensors for RCS ~~cold~~ Cold and ~~hot leg temperatures, core exit temperature~~ Hot Leg Temperatures, Core Exit Temperature and RCS ~~pressure~~ Pressure. The saturation temperature is calculated from ~~the minimum temperature~~ pressure input. The temperature subcooled ~~or superheated~~ margin is the difference between the calculated saturation temperature and the sensor temperature input. Two ~~temperatures temperature~~ subcooled ~~or superheated~~ margin ~~presentation~~ presentations are available as follows:

- RCS saturation margin – ~~the~~ The temperature saturation margin is based on the difference between the saturation temperature and the maximum temperature from the RTDs in the hot and cold legs.
- Upper head saturation margin – The temperature saturation margin is based on the difference between the saturation temperature and the ~~core exit temperature~~ Core Exit Temperature.

18. Main Steam Line Pressure

Steam Generator Pressure is provided to monitor ~~operation of~~ decay heat removal via the SGs.

19. Emergency Feedwater Pit Level

EFW Pit Level is provided to ensure water supply for ~~emergency feedwater~~Emergency Feedwater (EFW). The EFW Pits provide the ensured safety grade water supply for the EFW System. There are two identical EFW Pits, each of which supplies one motor driven and one turbine driven EFW pump. Redundant level indication for each EFW Pit is displayed in the ~~main control room~~MCR.

~~The PAs that required EFW are the loss of electric power, steam line break (SLB), and small break LOCA.~~

20, 21. Refueling Water Storage Pit (RWSP) Level (Wide Range, Narrow Range)

RWSP Level is provided for verification and long term surveillance of RCS integrity and is used to determine:

- RWSP level accident diagnosis, and
- Whether to terminate ~~S~~ECCS Actuation, if still in progress.

PAM Display Function

The PAM Display Function is provided by four trains of Safety VDUs (S-VDU). A Safety VDU train consists of a VDU and S-VDU processor. An S-VDU train must be OPERABLE for the corresponding channels of the required PAM Instrumentation Functions, and in the same MODES. For PAM Instrumentation Functions with four channels (two or three required channels), two or three corresponding S-VDU trains must be OPERABLE. For PAM Instrumentation Functions with only two required channels, two corresponding S-VDU trains must be OPERABLE. For CIV position, there are two-train components assigned to Trains A and D, and two-train components assigned to Trains B and C. Therefore, because all four trains are required for CIV position, all four trains of S-VDU are required to be OPERABLE.

APPLICABILITY	The PAM instrumentation <u>Instrumentation</u> LCO is applicable in MODES 1, 2, and 3. These variables are related to the diagnosis and pre-planned actions required to mitigate PAs. The applicable PAs are assumed to occur in MODES 1, 2, and 3. In MODES 4, 5, and 6, unit conditions are such that the likelihood of an event that would require PAM instrumentation <u>Instrumentation</u> is low; therefore, the PAM instrumentation <u>Instrumentation</u> is not required to be OPERABLE in these MODES.
---------------	--

ACTIONS

The ACTIONS Table has been modified by ~~two Notes~~.

~~The first a Note excludes the MODE change restriction of LCO 3.0.4. This exception allows entry into an applicable MODE while relying on the ACTIONS even though the ACTIONS may eventually require a plant shutdown. This exception is acceptable due to the passive function of the instruments, the operator's ability to respond to an accident using alternate instruments and methods, and low probability of an event requiring these instruments.~~

~~—The second note has been added in the ACTIONS~~ to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function listed on Table 3.3.3-1 and the PAM Display Function. The Completion Time(s) of the inoperable channel(s) of a Function will be tracked separately for each Function starting from the time the Condition was entered for that Function.

In all cases where the LCO states “Restore channel or train to OPERABLE status”, this means restore the required number of channels or trains to OPERABLE status. Therefore, restoration of an alternate channel or train, other than the failed channel or train, is also acceptable.

A.1

Condition A applies when one or more PAM Instrumentation Functions have one required channel ~~that inoperable, or one train of the PAM Display Function~~ is inoperable.

Required Action A.1 requires restoring the inoperable channel or train to OPERABLE status within 30 days. The 30 day Completion Time is based on operating experience and takes into account the remaining OPERABLE channel(s) or trains (or in the case of a Function that has only one required channel, other non-Regulatory Guide 1.97 instrument channels to monitor the Function), the passive nature of the instrument (operability for automatic actions that may occur from these instruments is covered by LCOs in other sections), and the low probability of an event requiring PAM ~~instrumentation~~ instrumentation during this interval.

B.1

Condition B applies when the Required Action and associated Completion Time for Condition A are not met. This Required Action specifies initiation of actions in Specification 5.6.5, which requires a written report to be submitted to the NRC immediately. This report discusses the results of the root cause evaluation of the inoperability and identifies proposed restorative actions. This action is appropriate in lieu of a shutdown requirement since alternative actions are identified before loss of functional capability, and given the likelihood of unit conditions that would require information provided by this instrumentation.

C.1 [and C.2]

Condition C applies when one or more PAM Instrumentation Functions have two ~~inoperable~~ required channels ~~(i.e. inoperable, or two channels~~ trains of the PAM Display Function are inoperable ~~in the same Function).~~

Required Action C.1 requires restoring one channel in the Function(s) to OPERABLE status within 7 days. The Completion Time of 7 days is based on the relatively low probability of an event requiring PAM instrument operation and the availability of alternate means to obtain the required information. Continuous operation with two trains or two required channels inoperable in a Function is not acceptable because the alternate indications may not fully meet all performance qualification requirements applied to the PAM ~~instrumentation~~ instrumentation. Therefore, requiring restoration of one inoperable channel or train of the Function limits the risk that the PAM Function will be in a degraded condition should an accident occur.

[Required Action C.2 allows the option to apply the requirements of Specification 5.5.18 to determine a Risk Informed Completion Time.

Required Action C.2 is modified by a Note that indicates C.2 ~~is~~may only ~~required to~~ be performed when the Emergency Feedwater Pit Level is inoperable.]

D.1

~~Condition and D applies when the Required Action and associated Completion Time of Condition C is not met. Required Action D.1 requires entering the appropriate Condition referenced in Table 3.3.3-1 for the channel immediately. The applicable Condition referenced in the Table is Function dependent. Each time an inoperable channel has not met the Required Action of Condition C, and the associated Completion Time has expired, Condition D is entered for that channel and provides for transfer to the appropriate subsequent Condition.~~

E.1 and E.2

If the Required Action and associated Completion Time of Condition C ~~is~~are not met ~~and Table 3.3.3-1 directs entry into Condition E~~, the unit must be brought to a MODE where the requirements of this LCO do not apply. To achieve this status, the unit must be brought to at least MODE 3 within 6 hours and MODE 4 within 12 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.

E.1

~~At this unit, alternate means of monitoring Reactor Vessel Water Level and Containment High Area Radiation have been developed and tested. These alternate means may be temporarily installed if the normal PAM channel cannot be restored to OPERABLE status within the allotted time. If these alternate means are used, the Required Action is not to shut down the unit but rather to follow the directions of Specification 5.6.5, in the Administrative Control section of the TS. The report provided to the NRC should discuss the alternate means used, describe the degree to which the alternate means are equivalent to the installed PAM channels,~~

~~justify the areas in which they are not equivalent, and provide a schedule for restoring the normal PAM channels.~~

SURVEILLANCE
REQUIREMENTS
Table 3.3.3-1.

A Note has been added to the SR Table to clarify that SR 3.3.3.1 and SR 3.3.3.2 apply to each PAM ~~instrumentation~~ Instrumentation Function in

SR 3.3.3.1

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

Agreement criteria are determined based on a combination of the channel instrument uncertainties. 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.

~~As specified in the SR, a CHANNEL CHECK is only required for those channels that are normally energized.~~

[The Surveillance Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the LCO required channels. ~~OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.~~]

A CHANNEL CHECK may be conducted manually or automatically. For the US-APWR an automated CHANNEL CHECK is normally conducted continuously, which satisfies the 31 day Surveillance Frequency requirement. Where the CHANNEL CHECK is conducted automatically, an alarm shall be generated when the agreement criteria is not met. If the automated CHANNEL CHECK function is unavailable, a manual CHANNEL CHECK shall be conducted at the minimum 31 day Surveillance Frequency.

~~The equipment that performs the automated CHANNEL CHECK shall be confirmed OPERABLE including the capability to generate fault alarms.~~ OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

SR 3.3.3.2

CHANNEL CALIBRATION is a complete check of the instrument loop, ~~from sensor to VDU as described in Reference 3. The test verifies~~ including the sensor. The test must be performed consistent with the methods and assumptions of MUAP-09022, "US-APWR Instrument Setpoint Methodology" (Ref. 6), to verify that the channel responds to a measured parameter with the necessary range and accuracy.

The CHANNEL CALIBRATION confirms the accuracy of the channel from sensor to digital VDU read out as described in Reference 3.

For analog measurements, except Core Exit Temperature Channels, CHANNEL CALIBRATION confirms the channel accuracy at five

calibration settings corresponding to 0%, 25%, 50%, 75% and 100% of the instrument range.

For binary measurements, the CHANNEL CALIBRATION confirms the accuracy of the channel's state change at the required setpoint.

This SR includes the RCS Hot Leg and Cold Leg Temperature channels. The CHANNEL CALIBRATION of the RCS Hot Leg and Cold Leg Temperature channels is accomplished by a cross calibration that compares the signals from the installed channels to a channel with a reference RTD, in accordance with FSAR Section 7.1.3.14 (Ref. 8).

This SR includes the Core Exit Temperature channels. The CHANNEL CALIBRATION of the Core Exit Temperature channels is accomplished by a cross calibration that compares the signals from the installed channels to the signals from the RCS Hot Leg and Cold Leg Temperature channels, after they have been calibrated as described above.

This SR is modified by a Note that excludes the neutron detectors from the CHANNEL CALIBRATION for the Wide Range Neutron Flux channels; the remaining channel devices are included. The calibration method for neutron detectors is specified in the Bases for SR 3.3.1.9 of LCO 3.3.1, "Reactor Trip System (RTS) Instrumentation."

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

The equipment that performs the automated CHANNEL CHECK shall be confirmed OPERABLE, including the capability to generate fault alarms during the CHANNEL CALIBRATION.

The Surveillance Frequency of 24 months is based on operating experience ~~and consistency~~, and on the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in accordance with MUAP-09022, "US-APWR Instrument Setpoint Methodology", and is consistent with the typical industry refueling cycle.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

|

SR 3.3.3.3

SR 3.3.3.3 is the performance of a MEMORY INTEGRITY CHECK (MIC) for the PAM Instrumentation. This includes the Safety VDU processors, RPS and SLS.

The PSMS is self-tested automatically on a continuous basis from the digital side of all input modules to the digital side of all visual display units. Continuous automatic self-testing encompasses all PSMS safety-related functions. The continuous automatic self-testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. The continuous automatic self-testing is described in Reference 3 and Reference 7.

The MIC is a diverse check of the PSMS software memory integrity to ensure there is no change to the internal PSMS software that would impact its functional operation, including the continuous automatic self-testing. The MIC is described in Reference 3 and Reference 7.

The capability to generate continuous automatic self-testing fault alarms shall be confirmed OPERABLE during the MIC.

The complete operability check from the measurement channel input device to the Safety VDU is performed by the combination of the continuous automatic self-testing for the digital devices (the Safety VDU processors, RPS, SLS, COM-2 and data communication interfaces), the continuous automatic CHANNEL CHECK (SR 3.3.3.1), the CHANNEL CALIBRATION (SR 3.3.3.2) and the MIC (SR 3.3.3.3). The CHANNEL CALIBRATION, the MIC, and the TADOT, which are manual tests, overlap with the continuous automatic self-testing and confirm the functioning of the continuous automatic self-testing.

[The Surveillance Frequency of 24 months is justified because the software memory integrity is checked by the continuous automatic self-testing.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.3.4

SR 3.3.3.4 is the performance of a SAFETY VDU TEST for the Safety VDUs in the MCR. The SAFETY VDU TEST is explained in Reference 3.

This **Surveillance** SR confirms the Safety VDU is capable of providing all display functions for the MCR. This test overlaps with the MIC (SR 3.3.3.3), to ensure the S-VDU is OPERABLE.

[The Surveillance Frequency of 24 months is adequate, based on industry operating experience, considering instrument reliability and operating history data.

In addition, the Surveillance Frequency considers that all indications and controls for each safety train and channel are available in the MCR on six other non-safety Operational VDUs.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

BASES

REFERENCES

1. Regulatory Guide 1.97, Rev. 4.
 2. NUREG-0737, "Clarification of TMI Action Plan Requirements."
 3. ~~MUAP-07004-P (Proprietary) and MUAP-07004-NP (Non-Proprietary)~~, Revision 7, "Safety I&C System Description and Design Process."
 4. FSAR Section 7.5.
 5. IEEE 497-2002.
 6. MUAP-09022-P, Revision 2, "US-APWR Instrument Setpoint Methodology."
 7. MUAP-07005-P, Revision 8, "Safety System Digital Platform -MELTAC-."
 8. FSAR Section 7.1.3.14.
-
-

B 3.3 INSTRUMENTATION

B 3.3.4 Remote Shutdown Console (RSC)

BASES

BACKGROUND The RSC provides sufficient displays and controls for the ~~control room~~ Main Control Room (MCR) operator to place and maintain the unit in a ~~safe shutdown~~ hot standby condition (MODE 3), to place and maintain the unit in a hot shutdown condition (MODE 4), and to place and maintain the unit in a cold shutdown condition (MODE 5), from a location outside the ~~Main Control Room-MCR~~ MCR if the ~~control room~~ MCR becomes inaccessible. In accordance with Section 7.4 (Ref. 4), MODES 3, 4 or 5 are referred to as safe shutdown.

With the unit in MODE 3, the Emergency Feedwater (EFW) System and the steam generator (SG) safety valves or the main steam depressurization valves (MSDVs) can be used to remove core decay heat and meet all safety requirements. The long term supply of water for the EFW System and the ability to borate the Reactor Coolant System (RCS) from outside the ~~control room~~ MCR allows extended operation in MODE 3. If the ~~control room~~ MCR becomes inaccessible, the operators can establish control at the RSC, and place and maintain the unit in MODE 3 for an extended period of time. The RSC also provides the capability to transition and maintain the unit in MODE 5, using the Residual Heat Removal System.

APPLICABLE The RSC is located outside the ~~control room~~ MCR with ~~at~~ the capability to promptly shutdown, cooldown and maintain the unit in a safe condition in MODE 3 ~~ANALYSES~~ and the capability to transition and maintain the unit in a safe condition in MODE 4 or 5, in accordance with the design described in FSAR Section 7.4 (Ref. 4).

The criteria governing the design and specific system requirements for remote shutdown are located in 10 CFR 50, Appendix A, GDC 19 (Ref. 1). These criteria are applied to the RSC of the US-APWR.

The RSC satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii) (Ref. 2).

The RSC LCO provides the OPERABILITY requirements for the RSC, which includes the displays and controls necessary to place and maintain the unit in MODE 3, with the capability to transition to MODES 4 or 5 and the ability to transfer control from the MCR to the RSC.

LCO Due to redundant components within the PSMS, such as controllers, communication links and power supplies, an inoperable component may or may not result in an inoperable channel or train. Where an inoperable component results in an inoperable required channel or train, LCOs are

entered. For inoperable components that do not result in inoperable channels or trains, LCOs are not entered. The instrumentation required are listed in Table B 3.3.4-1.

Display and Control Function

~~————~~ The displays and controls at the RSC are functionally the same as the displays and controls used by the operator to achieve and maintain MODE 3, 4 or 5 from the ~~main control room, MCR~~. These displays and controls are provided by four trains of Safety VDUs, and non-safety Operational VDUs. MODE 3, 4 or 5 can be achieved and maintained using only safety related plant equipment which is controlled and monitored from Safety VDUs or Operational VDUs.

The Display and Control Function of the RSC encompasses the measurement channels and component controls required for safe shutdown, and the subsystems of the PSMS that support that equipment. The measurement channels and component controls available to achieve normal and safe shutdown are identified in Table 7.4-1 and Table 7.4-2 of FSAR Section 7.4 (Ref. 4).

The measurement channels for safe shutdown, that are required to be OPERABLE for this LCO, are listed in Table B 3.3.4-1, including the required number of channels. These measurement channels are interfaced to the Reactor Protection System (RPS) and then provided to the RSC. Each item listed in Table B 3.3.4-1 is referred to as an RSC Instrumentation Function.

The component controls for safe shutdown, that are required to be OPERABLE for this LCO, are listed in Table B 3.3.4-2, including the required number of trains. The Safety Logic System (SLS) provides the Actuation Logic and Actuation Outputs for these components. Safe shutdown can be achieved by only one train of plant equipment for two train ESF systems and by two trains of plant equipment for four train ESF systems. One additional train is required to meet the single failure criteria. Each item listed in Table B 3.3.4-2 is referred to as an RSC Control Function.

The Display and Control Function also encompasses the Safety VDUs (S-VDU) and Communication Subsystem (COM-2). The S-VDU is required for the display of safe shutdown measurement channels. The S-VDU and COM-2 are required for manual control of safe shutdown components. Since for all required safe shutdown systems, the required OPERABLE safety plant components may be distributed to all four trains, all four trains of Safety VDUs and COM-2 are required. The Safety VDU in each train consists of a VDU and Safety VDU processor.

~~————~~ ~~Non~~All plant equipment, including non-safety plant equipment is controlled and monitored from the Operational VDUs at the RSC. This

equipment is provided for convenience and is not necessary to achieve or maintain MODE 3, 4 or 5. Therefore the Operational VDUs are not covered by this LCO.

Transfer of Control

~~The controls in the MCR are normally enabled, while the controls at the RSC are normally disabled. Actuation of Transfer Switches disables the controls in the MCR and enables the controls at the RSC. There are two Transfer Switches for each safety train of the PSMS and two transfer switches for the PCMS. Activating both transfer switches for a train, transfers the controls for that train.~~

The RSC equipment covered by this LCO does not need to be continuously energized to be considered OPERABLE. However, it is necessary to energize this equipment for surveillance testing.

Transfer of Control Function

The controls in the MCR are normally enabled, while the controls at the RSC are normally disabled. Actuation of Transfer Switches disables the controls in the MCR and enables the controls at the RSC. There are two Transfer Switches for each safety train of the Protection and Safety Monitoring System (PSMS) (8 switches) and two Transfer Switches for the Plant Control and Monitoring System (PCMS) (which has only one train). Activating both Transfer Switches for a train, transfers the controls for that train. Transferring control also blocks signals from the disabled location that could otherwise interfere with safe shutdown operations. Since all trains must be capable of control transfer and signal blocking, both Transfer Switches for all four PSMS trains and the PCMS are required to be OPERABLE.

The Transfer of Control Function also encompasses the COM-2. The COM-2 is required for transfer of control from the MCR to the RSC. Since for all required safe shutdown systems, the required OPERABLE safety plant components may be distributed to all four trains, all four trains of COM-2 are required.

APPLICABILITY

The RSC LCO is applicable in MODES 1, 2 and 3. This applicability recognizes the need for being able to place and maintain the unit in a safe shutdown condition (MODE 3, with the capability to transition to MODES 4 or 5) from a location outside the ~~main control room~~ MCR if the MCR becomes inaccessible while the RCS contains a large amount of energy.

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

necessary instrument control functions if ~~control room~~MCR instruments or controls become unavailable.

ACTIONS

In all cases where the LCO states “Restore channel or train to OPERABLE status”, this means restore the required number of channels or trains to OPERABLE status. Therefore, restoration of an alternate channel or train, other than the failed channel or train, is also acceptable.

A.1

Condition A addresses the situation where ~~the Remote Shutdown Console is inoperable. This includes one required channel or train for the Display and Control Function and is inoperable, or one train for the Transfer of Control Function.~~

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

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

B.1 and B.2

Condition B applies when the Required Action and associated Completion Time of Condition A are not met. In this condition, 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 to MODE 4 within 12 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

SR 3.3.4.1

SR 3.3.4.1 is the performance of a TADOT for the ~~-Transfer of Control Function from the main control room~~MCR to the RSC, which verifies the RSC Transfer Switches perform their required functions for each PSMS

train and the PCMS. Each Transfer Switch is tested up to, and including, the signal status readout on a digital display.

This SurveillanceSR verifies that the controls and interfaces for the Transfer of Control Function are OPERABLE.

[The 24 month Surveillance Frequency is adequate, based on industry operating experience, considering instrument reliability and operating history data. Allowing this test during unit outage conditions is reasonable given the robustness of the transfer switchesTransfer Switches and the potential for unplanned transients if performed at power.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.4.2

SR 3.3.4.2 is the performance of an ACTUATION LOGICa SAFETY VDU TEST for all Safety VDUs on the RSC. The ~~PSMS are self tested on a continuous basis from the digital side of all input modules to the digital side of all output modules. Self testing also encompasses all data communications within a PSMS train, between PSMS trains. The self testing is described~~SAFETY VDU TEST is explained in Reference 3 and 5. ~~The ACTUATION LOGIC TEST is a check of the PSMS software memory integrity to ensure there is no change to the internal software that would impact its functional operation or the continuous self test function. The software memory integrity test is described in Reference 3 and 5.~~

~~This Surveillance verifies that all logic and communications with the PSMS for the Transfer of Control Function is OPERABLE. It also verifies that all logic functions within the PSMS associated with controls and indications at the RSC are OPERABLE.~~

This Surveillance SR confirms the Safety VDU is capable of providing all Display and Control Functions for the RSC. This test overlaps with the MEMORY INTEGRITY CHECK (MIC) for the Safety VDU processor (SR 3.3.4.5), to ensure the Display and Control Function is OPERABLE.

~~[The Surveillance Frequency of every 24-24 months is justified adequate, based on the industry operating experience, considering instrument reliability of and operating history data. In addition, the PSMS. The 24 month Surveillance Frequency supports conduct of this test during outage conditions. considers that all indications and controls for each safety train and channel are available on two other non-safety Operational VDUs.~~

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.4.3

~~SR SR 3.3.4.3 is the performance of a Safety VDU test for all Safety VDUs on the RSC. The Safety VDU Test is explained in Reference 3.~~

~~This Surveillance confirms the Safety VDU is capable of providing all display and control functions for the RSC. This test overlaps with the Actuation Logic Test of SR 3.3.4.2 to ensure the Display and Control CHANNEL CHECK for each RSC Instrumentation Function is OPERABLE in Table 3.3.4-1.~~

~~[The Frequency of 24 months is adequate, based on industry operating experience, considering instrument reliability and operating history data. In addition, the frequency considers that all indications and controls for each safety train and channel are available on two other non-safety Operational VDUs.~~

Performance of the CHANNEL CHECK ensures that a gross instrumentation failure 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. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

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

The Surveillance Frequency of 31 days is based on operating experience that demonstrates that channel failure is rare. The CHANNEL CHECK supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the LCO required channels.

A CHANNEL CHECK may be conducted manually or automatically. For the US-APWR an automated CHANNEL CHECK is normally conducted continuously, which satisfies the 31 day Surveillance Frequency requirement. Where the CHANNEL CHECK is conducted automatically, an alarm shall be generated when the agreement criteria is not met. If the automated CHANNEL CHECK function is unavailable, a manual CHANNEL CHECK shall be conducted at the minimum 31 day Surveillance Frequency.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.4.4

SR 3.3.4.4 is the performance of a CHANNEL CALIBRATION for each RSC Instrumentation Function in Table B 3.3.4-1.

The CHANNEL CALIBRATION confirms the accuracy of the channel from sensor to digital VDU readout, as described in Reference 3.

CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test must be performed consistent with the methods and assumptions of MUAP-09022, "US-APWR Instrument Setpoint Methodology" (Ref. 6), to verify that the channel responds to a measured parameter with the necessary range and accuracy.

For analog measurements, CHANNEL CALIBRATION confirms the channel accuracy at five calibration settings corresponding to 0%, 25%, 50%, 75% and 100% of the instrument range. For binary measurements, the CHANNEL CALIBRATION confirms the accuracy of the channel's state change at the required setpoint.

This SR is applicable to all channels, including the Wide Range Neutron Flux channels. However, this SR is modified by a Note that excludes neutron detectors. The calibration method for neutron detectors is

specified in the Bases for SR 3.3.1.9 of LCO 3.3.1, "Reactor Trip System (RTS) Instrumentation."

This SR includes the RCS Hot Leg and Cold Leg Temperature channels. The calibration of the channels is accomplished by a cross calibration that compares the signals from the installed channels to a channel with a reference RTD, in accordance with FSAR Section 7.1.3.14 (Ref. 7).

The equipment that performs the automated CHANNEL CHECK shall be confirmed OPERABLE, including the capability to generate fault alarms during the CHANNEL CALIBRATION.

[The Surveillance Frequency of 24 months is based on operating experience, and on the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in accordance with MUAP-09022, "US-APWR Instrument Setpoint Methodology", and is consistent with the typical industry refueling cycle.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.4.5

SR 3.3.4.5 is the performance of a MIC for the RSC. This includes the Safety VDU processors, RPS, SLS and COM-2.

The PSMS is self-tested automatically on a continuous basis from the digital side of all input modules to the digital side of all output modules. Continuous automatic self-testing encompasses all PSMS safety-related functions including actuation logic functions. The continuous automatic self-testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. The continuous automatic self-testing is described in Reference 3 and Reference 5.

The MIC is a diverse check of the PSMS software memory integrity to ensure there is no change to the internal PSMS software that would impact its functional operation, including actuation logic functions or the continuous automatic self-testing. The MIC is described in Reference 3 and Reference 5.

The capability to generate continuous automatic self-testing fault alarms shall be confirmed OPERABLE during the MIC.

The complete operability check from the Safety VDUs (S-VDU) input device to the Safety Logic System (SLS) output device is performed by the combination of the continuous automatic self-testing for the digital devices (Safety VDU processors, COM-2, SLS and digital communication interfaces), the SAFETY VDU TEST (SR 3.3.4.2), MIC for the Safety VDU

processors, COM-2 and SLS (SR 3.3.4.5) and TADOT for SLS outputs (SR 3.3.4.6). The SAFETY VDU TEST, MIC, and TADOT, which are manual tests, overlap with the continuous automatic self-testing and confirm the functioning of the continuous automatic self-testing.

The complete operability check from the measurement channel sensing device to the S-VDU is performed by the combination of the continuous automatic self-testing for the digital devices (Safety VDU processors and RPS, and digital communication interfaces), the SAFETY VDU TEST (SR 3.3.4.2), MIC for the Safety VDU processors and RPS (SR 3.3.4.5), the continuous automatic CHANNEL CHECK (SR 3.3.4.3) and the CHANNEL CALIBRATION (SR 3.3.4.4). The CHANNEL CALIBRATION, MIC and Safety VDU TEST, which are manual tests, overlap with the continuous automatic self-testing and confirm the functioning of the continuous automatic self-testing.

[The Surveillance Frequency of 24 months is justified because the software memory integrity is checked by the continuous automatic self-testing.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.4.6

SR 3.3.4.6 is the performance of a TADOT for the Actuation Outputs of each required train for each RSC Control Function. This test actuates the outputs of the SLS for all components required to achieve and maintain safe shutdown. Therefore, this test is typically conducted in conjunction with testing the plant process components. Since this test is conducted in conjunction with testing for plant process components, this test may be conducted more frequently, as may be required for the plant process components.

[The Surveillance Frequency of 24 months is adequate, based on industry operating experience, considering instrument reliability and operating history data of solid state Actuation Output devices.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

REFERENCES

1. 10 CFR 50, Appendix A, GDC 19.
2. 10 CFR 50.36.
3. MUAP-07004-P-~~(Proprietary)~~ and MUAP-07004-NP-~~(Non-Proprietary)~~, Revision 7, "Safety I&C System Description and Design Process."

4. FSAR Section 7.4.4.
 5. MUAP-07005-P (~~Proprietary~~) and MUAP-07005-NP (~~Non-Proprietary~~), Revision 8, “Safety System Digital Platform –
MELTAC.”
 6. MUAP-09022-P, Revision 2, “US-APWR Instrument Setpoint
Methodology.”
 7. FSAR Section 7.1.3.14.
-
-

Table B 3.3.4-1 (page 1 of 1)
Remote Shutdown Console Instrumentation

<u>FUNCTION</u>	<u>REQUIRED NUMBER OF CHANNELS</u>
<u>1. Reactor Coolant System</u>	
<u> a. Pressurizer Water Level</u>	<u>2</u>
<u> b. Pressurizer Pressure</u>	<u>2</u>
<u> c. Reactor Coolant Hot Leg Temperature (Wide Range)</u>	<u>3</u>
<u> d. Reactor Coolant Cold Leg Temperature (Wide Range)</u>	<u>3</u>
<u> e. Reactor Coolant Pressure</u>	<u>2</u>
<u>2. Safety Injection System</u>	
<u> a. Safety Injection Pump Discharge Flow</u>	<u>1 per Required Pump</u>
<u> b. Safety Injection Pump Minimum Flow</u>	<u>1 per Required Pump</u>
<u> c. Safety Injection Pump Discharge Pressure</u>	<u>1 per Required Pump</u>
<u> d. Safety Injection Pump Suction Pressure</u>	<u>1 per Required Pump</u>
<u> e. Accumulator Pressure</u>	<u>1 per Tank</u>
<u>3. Residual Heat Removal System</u>	
<u> a. CS/RHR Hx Outlet Temperature</u>	<u>1 per Required Pump</u>
<u> b. CS/RHR Pump Discharge Flow</u>	<u>1 per Required Pump</u>
<u> c. CS/RHR Pump Minimum Flow</u>	<u>1 per Required Pump</u>
<u> d. CS/RHR Pump Discharge Pressure</u>	<u>1 per Required Pump</u>
<u> e. CS/RHR Pump Suction Pressure</u>	<u>1 per Required Pump</u>
<u>4. Emergency Feedwater System</u>	
<u> a. EFW Pit Water Level</u>	<u>2 per Pit</u>
<u> b. EFW Flow</u>	<u>1 per SG</u>
<u> c. EFW Pump Discharge Pressure</u>	<u>1 per Required Pump</u>
<u>5. Condensate and Feedwater System</u>	
<u> SG Water Level (Wide Range)</u>	<u>1 per SG</u>
<u>6. Main Steam Supply System</u>	
<u> a. Main Steam Line Pressure</u>	<u>2 per Line</u>
<u>7. Component Cooling Water System</u>	
<u> a. CCW Surge Tank Water Level</u>	<u>1 per Required Tank Compartment</u>
<u> b. CCW Header Pressure</u>	<u>1 per Required Pump</u>
<u> c. CCW Header Flow</u>	<u>1 per Required Pump</u>
<u> d. CCW Supply Temperature</u>	<u>1 per Required Pump</u>

Table B 3.3.4-1 (page 2 of 2)
Remote Shutdown Console Instrumentation

<u>FUNCTION</u>	<u>REQUIRED NUMBER OF CHANNELS</u>
<u>8. Essential Service Water System</u>	
<u> a. CCW Hx ESW Flow</u>	<u>1 per Required Pump</u>
<u> b. ESW Header Pressure</u>	<u>1 per Required Pump</u>
<u>9. Refueling Water Storage System</u>	
<u> a. RWSP Water Level (Wide Range)</u>	<u>2</u>
<u>10. Nuclear Instrumentation System</u>	
<u> a. Source Range Neutron Flux</u>	<u>2</u>
<u>[11. UHS Instrumentation.</u>	<u>1 per Required Pump]</u>

Table B 3.3.4-2 (page 1 of 2)
Remote Shutdown Console Controls

<u>FUNCTION</u>	<u>REQUIRED NUMBER OF TRAINS</u>
<u>1. Reactor Trip System</u>	
<u> a. Reactor Trip Breaker</u>	<u>3 (2 Breakers per Train)</u>
<u>2. Reactor Coolant System</u>	
<u> a. Safety Depressurization Valve</u>	<u>2</u>
<u> b. Safety Depressurization Valve Block Valve</u>	<u>2</u>
<u> c. Pressurizer Heater Backup Group</u>	<u>3</u>
<u> d. Reactor Vessel (RV) Vent Valve</u>	<u>2 per Line</u>
<u>3. Chemical Volume Control System</u>	
<u> a. Seal Water Return Line Isolation Valve</u>	<u>2 per Line</u>
<u>4. Safety Injection System</u>	
<u> a. Safety Injection Pump (SIP)</u>	<u>3</u>
<u> b. SIPs Suction Isolation Valve</u>	<u>1 per Required Pump</u>
<u> c. SIPs Discharge Containment Isolation Valve</u>	<u>1 per Required Pump</u>
<u> d. Direct Vessel Safety Injection Line Valve</u>	<u>1 per Required Pump</u>
<u> e. Emergency Letdown Line Isolation Valve</u>	<u>2 per Line</u>
<u> f. Accumulator Discharge Valve</u>	<u>1 per Tank</u>
<u> g. ACC Nitrogen Supply Line Isolation Valve</u>	<u>1 per Tank</u>
<u> h. ACC Nitrogen Discharge Valve</u>	<u>2 per Tank</u>
<u>5. Residual Heat Removal System</u>	
<u> a. CS/RHR Pump</u>	<u>3</u>
<u> b. CS/RHR Pump Hot Leg Isolation Valve</u>	<u>1 per Required Pump (2 Valves per Train)</u>
<u> c. CS/RHR Pumps RWSP Suction Isolation Valve</u>	<u>1 per Required Pump</u>
<u> d. RHR Discharge Line Containment Isolation Valve</u>	<u>1 per Required Pump</u>
<u> e. RHR Flow Control Valve</u>	<u>1 per Required Pump</u>
<u> f. CS/RHR Pump Full-Flow Test Line Stop Valve</u>	<u>1 per Required Pump</u>
<u>6. Emergency Feedwater System</u>	
<u> a. EFW Pump (Motor-Driven or Turbine Driven)</u>	<u>3</u>
<u> b. EFW Control Valve</u>	<u>1 per SG</u>
<u> c. EFW Isolation Valve</u>	<u>1 per SG</u>
<u> d. T/D-EFW Pump MS Line Steam Isolation Valve</u>	<u>1 per Required Pump</u>
<u> e. T/D-EFW Pump Actuation Valve</u>	<u>1 per Required Pump</u>

Table B 3.3.4-2 (page 2 of 2)
Remote Shutdown Console Controls

<u>FUNCTION</u>	<u>REQUIRED NUMBER OF TRAINS</u>
<u>7. Main Steam Supply System</u>	
<u> a. Main Steam Depressurization Valve</u>	<u>1 per SG</u>
<u> b. Main Steam Relief Valve Block Valve</u>	<u>1 per SG</u>
<u> c. Main Steam Isolation Valve</u>	<u>1 per SG</u>
<u> d. Main Steam Bypass Isolation Valve</u>	<u>1 per SG</u>
<u>8. Component Cooling Water System</u>	
<u> a. CCW Pump</u>	<u>3</u>
<u> b. CS/RHR Hx CCW Outlet Valve</u>	<u>1 per Required Pump</u>
<u>9. Essential Service Water System</u>	
<u> a. ESW Pump</u>	<u>3</u>
<u> b. ESW Pump Discharge Valve</u>	<u>1 per Required Pump</u>
<u>10. Steam Generator Blowdown System</u>	
<u> a. SGBD Line Containment Isolation Valve</u>	<u>1 per SG</u>
<u> b. SGBD Line Isolation Valve</u>	<u>1 per SG</u>
<u> c. SGBD Sampling Line Containment Isolation Valve</u>	<u>1 per SG</u>
<u>11. Heating, Ventilation, and Air Conditioning</u>	
<u> a. MCR Air Handling Unit & Damper</u>	<u>3</u>
<u> b. Class 1E Electrical Room Air Handling Unit & Damper</u>	<u>3</u>
<u> c. Class 1E Electrical Room Return Air Fan</u>	<u>3</u>
<u> d. Class 1E Battery Room Exhaust Fan & Damper</u>	<u>3</u>
<u> e. Class 1E Electrical Room In-duct heater</u>	<u>3</u>
<u> f. CCW Pump Area Air Handling Unit</u>	<u>3</u>
<u> g. Essential Chiller Unit Area Air Handling Unit</u>	<u>3</u>
<u> h. EFW Pump Area Air Handling Unit</u>	<u>3</u>
<u> i. Essential Chiller Unit</u>	<u>3</u>
<u> j. Essential Chilled Water Pump & Valves</u>	<u>3</u>
<u>[12. UHS Components</u>	<u>3]</u>

B 3.3 INSTRUMENTATION

B 3.3.5 Loss of Power (LOP) Class 1E Gas Turbine Generator (GTG) Start Instrumentation

BASES

BACKGROUND

The Class 1E ~~GTG~~-GTGs provide a source of emergency power when offsite power is either unavailable or is insufficiently stable to allow safe unit operation. Undervoltage protection will generate an LOP start if a loss of voltage or degraded voltage condition occurs in the switchyard. There are four LOP start signals, one for each 6.9 kV Class 1E bus.

Field Sensors

Three undervoltage relays with inverse time characteristics are provided on each 6.9 kV Class 1E bus for detecting a sustained degraded voltage condition or a loss of bus voltage. ~~The~~Signals from the undervoltage relays are interfaced to the ESFAS.

ESFAS and SLS

Signals from the undervoltage relays are combined in a two-out-of-three actuation logic within the ESFAS to generate an LOP signal when the voltage is dropped before reaching the loss of voltage limit for a short time or before reaching the degraded voltage limit for a long time. The LOP signal is interfaced from the ESFAS via internal digital data communication to the SLS controllers of the PSMS, which provide the GTG actuation logic, GTG control system and GTG control output. The GTG actuation logic combines manual and automatic start demands, with other GTG control interlocks; the GTG control system provides continuous closed loop control of the GTG via the GTG control output. The LOP start actuation is described in Reference 1.

~~The Allowable Value in conjunction with the Trip Setpoint and LCO establishes the threshold for Engineered Safety Features Actuation System (ESFAS) action to prevent exceeding acceptable limits such that the consequences of Postulated Accidents (PAs) will be acceptable. The Allowable Value is considered a limiting value such that a channel is OPERABLE if the setpoint is found not to exceed the Allowable Value during the CHANNEL CALIBRATION. Note that although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to within the established calibration tolerance band of the setpoint in accordance with Section 5.5.21, SCP.~~

Allowable Values and LOP Class 1E GTG Start Instrumentation Setpoints

The Nominal Trip Setpoint and Allowable Value are recorded and maintained in a document established by the Setpoint Control Program (SCP).

The Allowable Value in conjunction with the Nominal Trip Setpoint and LCO establishes the threshold for Engineered Safety Features Actuation System (ESFAS) action to prevent exceeding acceptable limits such that the consequences of Postulated Accidents (PAs) will be acceptable. The Allowable Value is considered a limiting value such that a channel is OPERABLE if the setpoint is found not to exceed the Allowable Value during the CHANNEL CALIBRATION (Ref. 7). Note that although a channel is OPERABLE under these circumstances, the setpoint shall be left adjusted to within the established Calibration Tolerance band of the setpoint 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. The Calibration Tolerance is recorded and maintained in the document established by the SCP.

If the as-found value of the device is found to have exceeded the Allowable Value, or the as-left value of the device cannot be adjusted to the value within the Calibration Tolerance, the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

Setpoints adjusted consistent with the requirements of Section Specification 5.5.21, SCP ensure that the consequences of accidents will be acceptable, providing provided the unit is operated from within the LCOs at the onset of the accident and that the equipment functions as designed. The time delay of required to start the Class 1E GTG starting, which is initiated by LOOP the LOP signal, is considered as mitigation system time delay in the analysis presented in FSAR Chapter 15 (Ref. 6).

~~The trip setpoints are selected to ensure that the setpoint measured by the surveillance procedure does not exceed the Allowable Value if the relay is performing as required.~~ The Nominal Trip Setpoint entered into the LOP binary sensor is more conservative than that specified by the Analytical Limit. The Nominal Trip Setpoint accounts for measurement errors detectable by the CHANNEL CALIBRATION and other unmeasurable errors (such as the effects of anticipated environmental conditions), which are both considered in the Allowable Value for the LOP Nominal Trip Setpoint, which is checked during CHANNEL CALIBRATION. If the ~~measured~~ as-found value of the LOP setpoint does not exceed the Allowable Value, the ~~relay~~ channel is considered OPERABLE. Operation with a trip setpoint less conservative than the ~~nominal~~ Nominal Trip Setpoint, but within the Allowable Value, is acceptable provided that operation and testing is consistent with the assumptions of the unit specific setpoint calculation.

Within the Protection and Safety Monitoring System (PSMS), LOP Time Delays are digital settings maintained in non-volatile software memory within each ESFAS train. Digital settings have no potential for variation due to time, environmental drift or component aging; therefore, these digital settings have no surveillance tolerance. Each train of the process control equipment has continuous automatic self-testing, which verifies that the digital Time Delay settings are correct. Time Delays are also verified periodically through a diverse software MEMORY INTEGRITY CHECK (MIC).

BASES

APPLICABLE
SAFETY
ANALYSES

The LOP Class 1E GTG start instrumentation is required for the Engineered Safety Features (ESF) Systems to function in any accident with a loss of offsite power. Its design basis is that of the ESF Actuation System (ESFAS). Accident analyses credit the loading of the Class 1E GTG based on the loss of offsite power during a loss of coolant accident (LOCA). The actual Class 1E GTG start has historically been associated with the ESFAS actuation. The Class 1E GTG loading has been included in the delay time associated with each safety system component requiring Class 1E GTG supplied power following a loss of offsite power. The analyses assume a non-mechanistic Class 1E GTG loading, which does not explicitly account for each individual component of loss of power detection and subsequent actions.

The required channels of LOP Class 1E GTG start instrumentation, in conjunction with the ESF systems powered from the Class 1E GTGs, provide unit protection in the event of any of the analyzed accidents discussed in Chapter 15, in which a loss of offsite power is assumed.

The delay times assumed in the safety analysis for the ESF equipment include the ~~100 second~~ Class 1E GTG start delay, and the appropriate sequencing delay, if applicable. The response times for ESFAS actuated equipment in LCO 3.3.2, "Engineered Safety ~~Feature~~Features Actuation System (ESFAS) Instrumentation," include the appropriate Class 1E GTG loading and sequencing delay.

The LOP Class 1E GTG start instrumentation channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii) (Ref. 4).

LCO

The Loss of Power (LOP) Class 1E Gas Turbine Generator (GTG) Start Instrumentation shall be OPERABLE for each bus that is required to be OPERABLE.

The LCO for LOP Class 1E GTG start instrumentation requires ~~that~~ three OPERABLE channels per required bus of both the loss of voltage and degraded voltage Functions ~~shall be OPERABLE~~ in MODES 1, 2, 3, and 4, ~~as well as whenever the associated GTG is required to be OPERABLE by LCO 3.8.2, "AC Sources - Shutdown." A Class 1E GTG is not required to be OPERABLE if its associated Class 1E 6.9 kV bus is not powering any required ESF loads. Therefore the associated Class 1E 6.9 kV bus is not required.~~

For MODES 5 and 6, three channels per required bus of both the loss of voltage and degraded voltage Functions shall be OPERABLE whenever the associated GTG is required to be OPERABLE by LCO 3.8.2, "AC Sources - Shutdown" to ensure that the automatic start of the GTG is available when needed.

In addition, for each required bus, the LCO for LOP Class 1E GTG Start Instrumentation requires the ESFAS actuation logic, GTG actuation logic, GTG control system and GTG control output in the associated train of the ESFAS and SLS to be OPERABLE. These logic, control and output functions are collectively referred to as the LOP Actuation Function. There are four trains for the LOP Actuation Function, one train for each bus and its associated GTG.

Loss of the LOP Class 1E GTG Start Instrumentation Function could result in the delay of safety systems initiation when required. This could lead to unacceptable consequences during accidents. During the loss of offsite power the Class 1E GTG powers the motor driven Emergency Feedwater Pumps. Failure of these pumps to start would leave two turbine driven pumps, as well as an increased potential for a loss of decay heat removal through the secondary system.

BASES

~~APPLICABILITY — The LOP Class 1E GTG Start Instrumentation Functions are required in MODES 1, 2, 3, and 4, as well as whenever the associated Class 1E GTG is required to be OPERABLE by LCO 3.8.2, "AC Sources — Shutdown." A Class 1E GTG is not required to be OPERABLE if its associated Class 1E 6.9 kV bus is not powering any required ESF loads. Therefore the associated Class 1E 6.9 kV bus is not required.~~ Due to redundant components within the PSMS, such as controllers, communication links and power supplies, an inoperable component may or may not result in an inoperable channel or train. Where an inoperable component results in an inoperable required channel or train, LCOs are entered. For inoperable components that do not result in inoperable channels or trains, LCOs are not entered.

APPLICABILITY The LOP GTG Start Instrumentation Functions are required in MODES 1, 2, 3, and 4 because ESF Functions are designed to provide protection in these MODES. This Function is also required in MODE 5 or 6 whenever the required GTG must be OPERABLE so that it can perform its function on an LOP or degraded power to its associated bus.

ACTIONS In the event a channel Nominal Trip Setpoint is found non-conservative with
 _____ respect to the Allowable Value, or the channel or train is found
 _____ inoperable, then
 _____ the function that channel or train provides must be declared inoperable and the LCO Condition entered for the particular protection function affected.

Because the required channels are specified on a per bus basis, the Condition may be entered separately for each bus as appropriate.

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

In all cases where the LCO states “Restore channel or train to OPERABLE status”, this means restore the required number of channels or trains to OPERABLE status. Therefore, restoration of an alternate channel or train, other than the failed channel or train, is also acceptable.

A.1

Condition A applies to the LOP Class 1E GTG ~~start~~ Start Instrumentation Functions with one loss of voltage or one degraded voltage channel per required Class 1E 6.9 kV bus inoperable.

If one channel is inoperable, Required Action A.1 requires that channel to be placed in trip within 6 hours. With a channel in trip, the LOP Class 1E GTG start instrumentation channels are configured to provide a one-out-of-two logic to initiate a trip of the incoming offsite power.

~~A Note is added to allow bypassing an inoperable channel for up to 4 hours for surveillance testing of other channels. This allowance is made where bypassing the channel does not cause an actuation and where at least two other channels are monitoring that parameter.~~

~~The specified Completion Time and time allowed for bypassing one channel are reasonable considering the Function remains fully OPERABLE on every bus and the low probability of an event occurring during these intervals.~~

The Completion Time of 6 hours is justified because the two remaining OPERABLE undervoltage devices for each bus are adequate to perform the safety function. Since the undervoltage devices are dedicated for each of the four Class 1E busses, and two undervoltage devices are adequate to perform the safety function of each bus, the LOP Class 1E GTG Start Instrumentation Function continues to meet the single failure criterion (i.e., three GTGs will still actuate if there is an additional undervoltage device failure on one bus).

The Completion Time of 6 hours is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 5).

A Note is added to allow placing one channel in bypass for up to 4 hours while performing surveillance testing, provided the other channels on the same bus are OPERABLE, or one channel is OPERABLE and the other is placed in the trip condition.

The Bypass Time of 4 hours is justified because the remaining OPERABLE channels are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE channels have continuous automatic self-testing.

The 4 hour Bypass Time is also justified in the US-APWR reliability and risk analyses, the summary and result of which are documented in FSAR Chapter 19 (Ref. 5).

B.1

Condition B applies when two or more loss of voltage or two or more degraded voltage ~~channel~~channels per required Class 1E 6.9 kV bus are inoperable.

Required Action B.1 requires restoring all but one channel per required Class 1E 6.9 kV bus to OPERABLE status. The 1 hour Completion Time should allow ample time to repair most failures and takes into account the low probability of an event requiring an LOP start occurring during this interval.

C.1

Condition C applies ~~to each~~when one train of the LOP ~~Class 1E GTG start Functions~~Actuation Function is inoperable for a required bus, or when the Required Action and associated Completion Time for Condition A or B are not met.

In these circumstances the Condition(s) specified in LCO 3.8.1, "AC Sources - Operating," or LCO 3.8.2, "AC Sources - Shutdown," for the Class 1E GTG made inoperable by failure of the LOP Class 1E GTG ~~start instrumentation~~Start Instrumentation are required to be entered immediately. The actions of those LCOs provide for adequate compensatory actions to assure unit safety.

BASES

SURVEILLANCE
REQUIREMENTSSR 3.3.5.1~~REQUIREMENTS~~

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

~~Agreement criteria are determined based on a combination of the channel instrument uncertainties. 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.~~

~~A CHANNEL CHECK may be conducted manually or automatically. For the US-APWR an automated CHANNEL CHECK is normally conducted continuously. Where the CHANNEL CHECK is conducted automatically, an alarm shall be generated when the agreement criteria is not met.~~

~~[The equipment that performs the automated CHANNEL CHECK shall be confirmed OPERABLE every 12 hours. This shall include the capability to generate fault alarm~~SR 3.3.5.1 is the performance of a TADOT for the LOP undervoltage relays and their interface to the ESFAS. For these tests, the undervoltage relays are confirmed to actuate with reasonable proximity to the Nominal Trip Setpoints. Undervoltage trip setpoint Allowable Values are verified during CHANNEL CALIBRATION (SR 3.3.5.2). Undervoltage Time Delays, which are implemented in the ESFAS, are verified during MIC (SR 3.3.5.3) for the ESFAS.

~~[The Surveillance Frequency of 31 days is based on the known reliability of the relays and binary input devices for the PSMS, and the multi-channel redundancy available, and has been shown to be acceptable through operating experience.~~

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.5.2

~~SR 3.3.5.2 is the performance of a TADOT for the LOP undervoltage relays and their interface to the PSMS. For these tests, the undervoltage relay is confirmed to actuate with reasonable proximity to the Nominal Trip Setpoints. Undervoltage trip setpoints Allowable Values and time delays are verified during CHANNEL CALIBRATION, SR 3.3.5.3.~~

~~[The Frequency of 31 days is based on the known reliability of the relays and binary input devices for the PSMS, and the multi-channel redundancy available, and has been shown to be acceptable through operating experience. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

~~SR 3.3.5.3~~

~~SR 3.3.5.3 is the performance of a~~ CHANNEL CALIBRATION.

~~The setpoints, as well as the response to a loss of voltage and a degraded voltage test, shall include a single point verification that the trip occurs within the required time delay.~~

~~CHANNEL CALIBRATION~~ for a binary ~~process~~ measurement is a complete check of the instrument loop, including the sensor and interface to the PSMS, as described in Reference 2. The test verifies that the channel responds to measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION confirms the accuracy of the channel from sensor to digital Visual Display Unit (VDU) readout, as described in Reference 2. The CHANNEL CALIBRATION confirms the accuracy of the channel's state change at the required setpoint.

CHANNEL CALIBRATIONS must be performed consistent with the methods and assumptions in Section Specification 5.5.21, SCP. For binary measurements, the CHANNEL CALIBRATION confirms the accuracy of the channel's state change. The state change must occur within the Allowable Value of the Nominal Trip Setpoint. Time Delays associated with Loss of Voltage and Degraded Voltage are recorded and maintained in a document established by the Setpoint Control Program (SCP) and confirmed through MIC.

[The Surveillance Frequency of 24 months is based on operating experience and consistency is consistent with the typical industry refueling cycle ~~and~~. The Surveillance Frequency of 24 months is justified by the assumption of a 24 month calibration interval in the determination of the magnitude of equipment drift in Section accordance with Specification 5.5.21, SCP.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

The equipment that performs the automated CHANNEL CHECK shall be confirmed OPERABLE, including the capability to generate fault alarms during the CHANNEL CALIBRATION.

SR 3.3.5.3

SR 3.3.5.3 is the performance of a MIC for the LOP Class 1E GTG Start Instrumentation. This includes the ESFAS and the SLS.

The PSMS is self-tested automatically on a continuous basis from the digital side of all input modules to the digital side of all output modules. Continuous automatic self-testing encompasses all PSMS safety-related functions including Time Delays, actuation logic functions and continuous control functions. The continuous automatic self-testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. The continuous automatic self-testing is described in Reference 2 and Reference 3.

The MIC is a diverse check of the PSMS software memory integrity, consistent with the Setpoint Control Program (SCP), to ensure there is no change to the internal PSMS software that would impact its functional operation, including digital Time Delays, actuation logic functions, continuous control functions or the continuous automatic self-testing. The MIC is described in Reference 2 and Reference 3.

The capability to generate continuous automatic self-testing fault alarms shall be confirmed OPERABLE during the MIC.

The complete OPERABILITY check from the measurement channel input device to the Safety Logic System (SLS) output device is performed by the combination of the continuous automatic self-testing for the digital devices (the ESFAS, SLS and data communication interfaces), the TADOT (SR 3.3.5.1) and CHANNEL CALIBRATION (SR 3.3.5.2) for the LOP undervoltage relays, the MIC (SR 3.3.5.3) and the TADOT for the GTG control output of the SLS (SR 3.3.5.4). The CHANNEL CALIBRATION, MIC, and TADOTs, which are manual tests, overlap with the continuous automatic self-testing and confirm the functioning of the automatic tests. The MIC is described in Reference 2 and Reference 3.

[The Surveillance Frequency of 24 months is justified because the software memory integrity is checked by the continuous automatic self-testing.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.5.4

SR 3.3.5.4 is the performance of ~~an ACTUATION LOGIC TEST. The Class 1E GTG start logic within the PSMS is self tested on a continuous basis from the digital side of all input modules to the digital side of all output modules. Self testing also encompasses all data communications within a PSMS train, between PSMS trains and between the PSMS and PCMS. The self testing is described in Reference 2 and 3. The ACTUATION LOGIC TEST is a check of the PSMS software memory integrity to ensure there is no change to the internal PSMS software that would impact its functional operation or the continuous self test function. The software memory integrity test is described in Reference 2 and 3. [The Frequency of every 24 months is justified based on the reliability of the PSMS. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]~~

~~The complete continuity check from the input device to the output device is performed by the combination of the continuous CHANNEL CHECK, the 24 month CHANNEL CALIBRATION for the non digital sided of the input module, the continuous self testing for the digital side, the 24 month ACTUATION LOGIC TEST, and the 24 month ESFAS and SLS TADOT for the non digital side of the output module. The CHANNEL CALIBRATION, ACTUATION LOGIC TEST and TADOT, which are manual tests, overlap with the CHANNEL CHECK and self testing and confirm the functioning of the self testing.~~

~~The ACTUATION LOGIC TEST interval of 24 months with the self test capability is justified in the PSMS reliability analysis. For detail information, refer to the US APWR Technical Report MUAP-07030 PRA, Attachment 6A.12. The result of the PSMS reliability analysis is~~

~~evaluated and confirmed in the US APWR PRA Chapter 19.~~

SR 3.3.5.5

~~SR 3.3.5.5 is the performance of a TADOT for the Actuation Outputs to start the Class 1E GTGs. This function actuates the GTG control outputs of the SLS. Therefore~~

~~The scope of this TADOT is limited to the GTG control outputs of the SLS, including the interface of those outputs to the GTG. However, this test is typically conducted in conjunction with testing the Class 1E complete GTG. [The Frequency of 24 months is adequate, based on industry operating experience, considering instrument reliability, including the fuel system and operating history data. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is~~

~~controlled under the Surveillance Frequency Control Program.] The Actuation Outputs are solid state devices, other GTG engine components, in accordance with LCO 3.8.1. Since this test is conducted in conjunction with testing for the Class 1E GTG components, this test may be conducted more frequently, as may be required for the Class 1E GTG components.~~

[The Surveillance Frequency of 24 months is adequate, based on industry operating experience, considering instrument reliability and operating history data of solid state control output devices.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

BASES

REFERENCES

1. FSAR Section 8.3.1.
2. MUAP-07004-P-~~(Proprietary)~~ and MUAP-07004-NP-~~(Non-Proprietary)~~, Revision 7, "Safety I&C System Description and Design Process."
3. MUAP-07005-P-~~(Proprietary)~~ and MUAP-07005-NP-~~(Non-Proprietary)~~, Revision 8, "Safety System Digital Platform—~~MELTAC~~."
4. 10 CFR 50.36.
5. FSAR Chapter 19.
6. FSAR Chapter 15.
7. MUAP-09022-P, Revision 2, "US-APWR Instrument Setpoint Methodology."

B 3.3 INSTRUMENTATION

B 3.3.6 Diverse Actuation System (DAS) Instrumentation

BASES

BACKGROUND

The Diverse Actuation System (DAS) provides non-Class 1E backup controls in case of beyond design basis common-cause failure (CCF) of the digital I&C ~~system~~ systems. CCF is a condition that concurrently affects all safety and non-safety systems that contain the same digital software. CCF is considered for the Protection and Safety Monitoring System (PSMS) and the Plant Control and Monitoring System (PCMS). The DAS is not credited for mitigating accidents in the FSAR Chapter 15 (Ref. 6) analyses.

To initiate ~~reactor trip~~ Reactor Trip, the DAS uses equipment that is diverse from the PSMS equipment (hardware and software) that is used to initiate a ~~reactor trip~~ Reactor Trip. This diversity does not include the analog input sensors or analog signal distribution devices.

To initiate ESF functions including ~~turbine trip~~ Turbine Trip, the DAS uses equipment that is diverse from the PSMS software. This diversity does not include the analog input sensors or analog signal distribution devices, or the final solid state Actuation Outputs in the PSMS, which are referred to as Power Interface (PIF) modules.

The DAS includes manual and automatic initiation capability.

~~Chapter 7~~ Defense-in-Depth and Diversity (Ref. 1) and FSAR Section 7.8 (Ref. 3) provides a description of the DAS.

The DAS ~~instrumentation~~ Instrumentation is segmented into ~~three~~ four distinct but interconnected modules as described in ~~Chapter~~ the Defense-in-Depth and Diversity report (Ref. 1) and FSAR Section 7.8 (Ref. 3), and as identified below:

1. Field transmitters or process sensors: provide a measurable electronic signal based upon the physical characteristics of the parameter being measured. The DAS shares field transmitters and process sensors, and signal distribution devices with the PSMS.
2. The Diverse Automatic Actuation Cabinet (DAAC): provides signal conditioning, analog ~~bistable~~ bistables for setpoint comparison, process algorithm actuation, compatible electrical signal output to actuation devices, and control room indications. DAAC outputs provide the means to actuate the Rod Drive Motor-Generator Set Trip Devices which interrupt power ~~to~~ from the Rod Drive Motor-Generator sets for ~~reactor trip and~~ Reactor Trip. DAAC outputs also provide the means to actuate ~~turbine trip~~ Turbine Trip and other ESF functions,

through the Power Interface modules of the PSMS. There are four DAACs. Each is referred to as a DAAC subsystem.

3. Diverse Human System Interface Panel (DHP): provides indications, alarms and Manual Initiation controls for DAS.

4. The Rod Drive Motor-Generator Set Trip Devices are actuated by output signals from the DAACs to interrupt power from the Rod Drive Motor-Generator Sets for Reactor Trip.

Field Transmitters or Sensors

To meet the design demands for redundancy and reliability, four field transmitters or sensors are used to measure each unit parameter. To account for the calibration tolerances and instrument drift, which are assumed to occur between calibrations, statistical allowances are provided in the ~~trip setpoint~~ Nominal Trip Setpoint and Allowable Values. The OPERABILITY of each channel from the transmitter or sensor through the signal distribution device is determined by ~~either~~ "as-found" and "as-left" calibration data evaluated during the CHANNEL CALIBRATION ~~or, and~~ by ~~qualitative assessment of field transmitter or sensor as related to~~ the channel behavior observed during performance of the CHANNEL CHECK. Since all DAS measurement channels are shared with the PSMS, the PSMS CHANNEL CALIBRATION and CHANNEL CHECK also confirm OPERABILITY of the DAS instrumentation from the transmitter or sensor through the signal distribution device.

DAAC ~~Signal Processing~~ Process Control Equipment

For each DAS automatic actuation function, ~~generally~~, four channels of process control equipment are used in each ~~DAS-DAAC~~ subsystem for the signal processing of unit parameters measured by the field instruments. The process control equipment provides signal conditioning, ~~comparable~~ output signals for instruments located on the DHP, and analog comparison of measured input signals with setpoints established by the D3 Coping Analysis (Ref. 2). These analog setpoints are recorded and maintained in a document established by the Setpoint Control Program (SCP). If the measured value of a unit parameter exceeds the predetermined setpoint, ~~an a~~ binary output from a DAAC analog bistable is forwarded to the DAAC voting logic for decision evaluation. Channels are isolated in the PSMS prior to their interface to the DAAC subsystems.

In each DAAC subsystem ~~Three~~our channels with ~~a two-out-of-three~~four logic are ~~sufficient to provide the required reliability and redundancy provided for each parameter.~~ If one channel fails in a direction that would not result in a partial Function trip, the Function is still OPERABLE with a two-out-of-~~two~~three logic. If one channel fails, such that a partial Function trip occurs, a spurious trip will not occur and the Function is still OPERABLE with a one-out-of-~~two~~three logic. Two

channels are necessary to generate a trip or ESF actuation, and since the DAS needs to function with a concurrent fire or flood in any PSMS I&C equipment room, which is where these signals originate, three channels are required. A channel of process control equipment consists of the signal path from field transmitter or sensor through the analog bistable in each DAAC.

The DAAC includes provisions to bypass a failed channel to prevent spurious trip/or actuation conditions.

~~Two measurement channels are required to ensure no single random failure of a DAAC measurement channel will result in spurious reactor trip, turbine trip or ESF actuation.~~ The measurement channels are designed such that testing may be accomplished while the reactor is at power and without causing trip/or actuation. ~~Three~~Four measurement channels are provided for each function ~~to allow~~, which allows one channel to be taken out of service with no operational restrictions.

The OPERABILITY of the DAAC process control equipment is determined by a CHANNEL OPERATIONAL TEST (COT) and by an ACTUATION LOGIC TEST. The COT overlaps with the CHANNEL CALIBRATION and the ACTUATION LOGIC TEST Overlaps with the COT. OPERABILITY of the interface from each DAAC to the PSMS PIF modules and to the Rod Drive Motor-Generator Set Trip Devices is determined by a TRIP ACTUATING DEVICE OPERATIONAL TEST (TADOT), which overlaps with the ACTUATION LOGIC TEST.

Allowable Values and DAS Setpoints

The CHANNEL CALIBRATION verifies the accuracy of the measurement channels at five calibration settings corresponding to 0%, 25%, 50%, 75% and 100% of the instrument range. If the as-found value of the device is found to have exceeded the Allowable Value, or the as-left value of the device cannot be adjusted to a value within the Calibration Tolerance, the device would be considered inoperable from a technical specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required. Since DAS measurement channels are shared with the PSMS, the PSMS Reactor Trip or ESFAS Functions establish the accuracy requirements for the channel, including the Allowable Value and Calibration Tolerance for CHANNEL CALIBRATION.

Regulatory guidance (Ref. 8) allows best estimate methods for analysis that demonstrate adequate coping for Anticipated Operational Occurrences (AOOs) and Postulated Accidents (PA) with concurrent CCF. Therefore, ~~The trip setpoints~~ he Nominal Trip Setpoints used in the DAAC analog bistables are ~~based on~~ the analytical limits ~~stated~~ specified in the D3 Coping Analysis. ~~These setpoints~~ (Ref. 2), with no channel uncertainty and no safety margin, in accordance with the setpoint methodology (Ref.7). This results in analog setpoints that are generally

less conservative than the corresponding digital setpoints in the PSMS to allow ensure the PSMS to actuate actuates first. If the PSMS actuates, DAS actuation is blocked. For plant operators, DAS actuation is indicative of an accident with a concurrent CCF in the PSMS, which prompts the use of special emergency procedures for beyond design basis plant conditions. Therefore, avoiding unnecessary DAS actuation is an important design basis consideration.

The selection of ~~these~~ the DAS analytical limits and corresponding trip setpoints is such that adequate protection is provided when ~~all~~ sensor and processing time delays are taken into account. ~~To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors for those DAS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 4), the Allowable Values recorded and maintained in a document established by the SCP in the accompanying LCO are conservative with respect to the analytical limits. A detailed description of the methodology used to calculate the Allowable Values and trip setpoints, incorporates the known uncertainties applicable to each channel. The magnitudes of these uncertainties are factored into the determination of each trip setpoint and corresponding Allowable Value. The trip setpoint entered into the bistable is more conservative than that specified by the Allowable Value to account for measurement errors detectable by the COT analog. The Allowable Value for the Nominal Trip Setpoint serves as the Technical Specification OPERABILITY limit for the purpose of the COT analog. Since the Nominal Trip Setpoints for DAS are set at the analytical limits in the D3 Coping Analysis (Ref. 2), the Allowable Value is established only to identify unexpected measurement error. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint as found value does not exceed the Allowable Value, the analog bistable is considered OPERABLE.~~

The ~~trip setpoint~~ Nominal Trip Setpoint is the value at which the analog bistable is set and is the expected value to be achieved during ~~calibration. COT.~~ The ~~trip setpoint~~ Nominal Trip Setpoint value ensures the D3 Coping Analysis (Ref. 2) limits are met ~~for surveillance interval selected when a channel is adjusted based on stated channel uncertainties. Any bistable is considered to be properly adjusted when the "as left" setpoint value is within the band for CHANNEL CALIBRATION uncertainty allowance (i.e., \pm rack calibration + comparator setting uncertainties). The trip setpoint value is therefore considered a "nominal" value (i.e., expressed as a value without inequalities) for the purposes of COT analog and CHANNEL CALIBRATION. A DAS analog bistable is considered to be properly adjusted when the "as left" value is within the specified calibration tolerance around the Nominal Trip Setpoint.~~

OPERABLE channels, with calibration settings and Nominal Trip setpoints Setpoints consistent with the requirements of the Allowable Value ensure that the consequences of AOOs and PAs will be acceptable,

~~providing~~provided the unit is operated from within the LCOs at the onset of the AOO or PA and the equipment functions as designed. The calibration setting Allowable Values, and the Nominal Trip Setpoints and corresponding Allowable Values, are recorded and maintained in a document established by the SCP. The setpoint methodology identified in the SCP (Ref. 7), is used to calculate the Allowable Values and Nominal Trip Setpoints.

BASESThe “expected as-found value” shall be as specified in the plant-specific setpoint analysis. The expected as-found value reflects the expected normal drift of actual plant equipment, so that a degraded device can be identified before the Allowable Value limit is reached. The expected as-found value is also referred to as the Performance Test Acceptance Criteria (PTAC). The PTAC, recorded and maintained in a document established by the SCP, is applicable to DAS automatic trip and actuation Functions.

Each channel of the process control equipment can be tested ~~on-line~~while in service to verify that the measurement channel signal or analog bistable setpoint accuracy is within the specified allowance requirements. Once a designated channel is taken out of service for testing, the field transmitter or sensor is stimulated or 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. SRs for the channels are specified in the SRs section.

DAAC Actuation Logic and Actuation Outputs

There are four DAAC subsystems. Each DAAC subsystem processes each of the four measurement channels from the PSMS through separate analog bistables. ~~The DAAC provides the decision logic processing of outputs from the signal processing equipment bistables.~~ The DAAC Actuation Logic processes the outputs from the DAAC analog bistables through two-out-of-four voting logic. The outputs from the voting logic for one or more parameters are combined to generate the DAAC outputs for Reactor Trip, Turbine Trip and ESF actuation.

The DAAC subsystems also process the signals and generate the Actuation Outputs for the Manual Initiation and Manual Control Functions. For Functions that have both automatic and manual signals, the signals are combined in each DAAC subsystem to generate a common Actuation Output.

To prevent spurious actuation, ~~two~~ and loss of the functions due to one DAAC subsystem failure, the output signals from four DAAC subsystems ~~of DAAC~~, each performing the same functions, are ~~provided~~combined in a ~~two-out-of-two~~ voting logic after taking one-out-of-two voting logic twice. If the same Function outputs are generated from a selective two DAAC subsystems (i.e., DAAC1 or DAAC3, concurrent with DAAC2 or DAAC4), a Reactor Trip, Turbine Trip and/or ESF actuation will result.

The DAS needs to function with a concurrent fire or flood in any PSMS I&C equipment room, which is where these subsystems are located. All four DAAC subsystems are required because the outputs of the DAAC subsystems are configured in a selective two-out-of-four configuration, not a full two-out-of-four configuration.

The subsystems are designed such that testing may be accomplished while the reactor is at power and without causing ~~trip~~Reactor Trip, Turbine Trip or ESF actuation. If one subsystem is actuated for maintenance or test purposes, ~~there will be no reactor trip, turbine trip or ESF actuation~~DAS Functions for Reactor Trip, Turbine Trip or ESF actuation are maintained for the unit. ~~If both subsystems are actuated, a reactor trip, turbine trip and/or ESF actuation will result.~~ Each DAAC subsystem is packaged in its own cabinet ~~for~~to satisfy physical ~~and electrical separation to satisfy separation and independence~~ requirements. The system has been designed to not trip ~~or~~ actuate in the event of a loss of power, to prevent spurious actuation.

The DAAC performs the decision logic for actuating a ~~reactor trip, turbine trip~~Reactor Trip, Turbine Trip or ESF actuation, generates the electrical output signal that will initiate the required trip or actuation, and provides the status, permissive, and annunciator output signals to the ~~main control room~~Main Control Room (MCR) of the unit.

~~Within each DAAC subsystem, the bistable outputs from the signal processing equipment are combined into logic matrices that represent combinations indicative of various unit upset and accident transients. If a required logic matrix combination is completed, the system will send actuation signals, to those components whose aggregate Function best serves to alleviate the condition and restore the unit to a safe condition, via PSMS Power Interface modules, if necessary. Examples are given in the Applicable Safety Analyses, LCO, and Applicability sections of this Bases. Output signals from each DAAC Subsystem are combined in a two-out-of-two logic within Rod Drive Motor Generator set trip devices or the Power Interface module for each plant component. When each DAAC subsystem is tested, the interface to the Power Interface is tested. When plant components~~

The OPERABILITY of the DAAC Actuation Logic Function is determined by an ACTUATION LOGIC TEST. The ACTUATION LOGIC TEST overlaps with the COT.

The OPERABILITY of DAAC Actuation Outputs for ESF functions and Turbine Trip, which interface from each DAAC to the PIF modules in the PSMS, is determined by a TADOT (SR 3.3.6.5) which overlaps with the ACTUATION LOGIC TEST. When PIF modules are actuated ~~from the PSMS~~, either during the ESFAS Instrumentation TADOT (SR 3.3.2.3) or for testing or control of ESF plant components, the ~~PSMS~~Safety Logic System (SLS) output signals overlap with the DAAC output signals within

~~the Power Interface. This overlap completes the DAS Function testing. Testing of PSMS components is per LCO 3.3.2. PIF modules.~~

BASES The OPERABILITY of DAAC Actuation Outputs for Reactor Trip, which interface from each DAAC to the Rod Drive Motor-Generator Set Trip Devices, and the OPERABILITY of the Rod Drive Motor-Generator Set Trip Devices themselves, is determined by a TADOT (SR 3.3.6.6) which overlaps with the ACTUATION LOGIC TEST.

Rod Drive Motor-Generator ~~sets~~Set Trip Devices

The Rod Drive Motor-Generator sets are the electrical power supply for the control rod drive mechanisms (CRDMs—Tripping). Actuating the Rod Drive Motor-Generator ~~sets trip devices~~Set Trip Devices interrupts power to the CRDMs, which allows the control rod shutdown banks and control banks to fall into the core by gravity. There are two Rod Drive Motor-Generator ~~sets~~Sets operating in parallel—to power all rods. Each has its own Rod Drive Motor-Generator Set Trip Device. The DAS trips both Rod Drive Motor-Generator ~~sets trip devices~~Set Trip Devices.

The DAS ~~interface~~interfaces to the Rod Drive Motor-Generator ~~sets is~~Set Trip Devices are via hardwired circuit.~~This interface may be tested, with no reactor trip, as described in subsection 7.8.2.4. Actual tripping of the Rod Drive Motor-Generator set may be tested from the DAS. Rod Drive Motor-Generator sets may be tripped one at a time for testing-s. Actual tripping of each Motor-Generator Set and the associated DAS interface may be tested one at a time, with no Reactor Trip. Actual tripping of each Rod Drive Motor-Generator Set may be tested from the DAS.~~

Diverse Human System Interface Panel (DHP)

The DHP provides Manual Initiation switches for all DAS automatic actuation functions and for additional functions that are required, per the D3 Coping Analysis (Ref. 2), to control all critical safety functions. Manual Initiation and Control switches are not redundant. To prevent spurious actuation due to a failure of any of the above switches, a separate manual actuation ~~permissive switch~~Permissive Switch is provided. This is referred to as the “Permissive Switch for DAS HSI.”

The Manual Initiation and Manual Control switches interface to DAAC subsystems 1 and 3, and the Permissive Switch for DAS HSI interface to DAAC subsystems 2 and 4. Manual Initiation/Control signals and Permissive signals are combined with automatic actuation signals to generate the same DAS outputs. Therefore, as for automatic signals, if the same Manual Initiation/Control Function outputs are generated from a selective two DAAC subsystems (i.e., DAAC1 or DAAC3, concurrent with DAAC2 or DAAC4), a Reactor Trip, Turbine Trip and/or ESF actuation will result.

The OPERABILITY of the DHP Manual Initiation/Control and Permissive switches, including the interface to the DAAC subsystems and the interface from the DAAC subsystems to the PSMS PIF modules, is determined by a TADOT (SR 3.3.6.5). The OPERABILITY of the DHP Manual Initiation/Control and Permissive switches, including the interface to the DAAC subsystems and the interface from the DAAC subsystems to the Rod Drive Motor-Generator set trip devices, is determined by a TADOT (SR 3.3.6.6). These TADOTs overlap with the ACTUATION LOGIC TEST.

The DHP also provides indications, ~~per~~ and alarms to support the manual actions credited in the D3 Coping Analysis, (Ref. 2), and to monitor all ~~and control~~ critical safety functions.

~~The DHP also provides indications, per the D3 Coping Analysis, to monitor RCS Leakage.~~

APPLICABLE
SAFETY
ANALYSES, LCO,
and APPLICABILITY

The DAS is required to provide a diverse capability to trip the reactor and actuate the specified safety-related equipment. The DAS is not credited for mitigating accidents in the Chapter 15 safety analyses. The DAS satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii) (Ref. 5).

The DAS LCO provides the requirements for the OPERABILITY of the DAS necessary to place the reactor in a shutdown condition and to remove decay heat in the event that required PSMS components do not function due to CCF.

A DAS measurement channel consists of the measurement device, its interface to each of the four DAAC subsystems, and the associated bistable within each of the four DAAC subsystems. A DAS measurement channel is OPERABLE provided the "as-found" values of the calibration settings checked during CHANNEL CALIBRATION do not exceed their associated Allowable Values, and the "as-found" value of the analog bistable trip setpoint checked during COT does not exceed its associated Allowable Value. ~~A Nominal Trip Setpoint may be set more conservative than the Limiting Trip Setpoint as necessary in response to plant conditions.~~ Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

Due to redundant components within the DAS, such as analog bistables, voting logic, time delays and power supplies, an inoperable component may or may not result in an inoperable channel/subsystem. Where an inoperable component results in an inoperable required channel/subsystem, LCOs are entered. For inoperable components that do not result in inoperable channels/subsystems, LCOs are not entered.

The DAS is required to be OPERABLE in the MODES specified in Table 3.3.6-1. All functions of the DAS are required to be OPERABLE in MODES 1, 2 and 3 with the ~~pressurizer pressure~~ Pressurizer Pressure

> P-11.

DAS functions are as follows:

1. Reactor Trip, Turbine Trip and Main Feedwater Isolation

a. Manual Initiation

The LCO requires ~~4~~one channel to be OPERABLE. ~~This~~The channel consists of the Reactor Trip, Turbine Trip and Main Feedwater Isolation - Manual Initiation switch. ~~This function requires operation of~~ and its interface to DAAC 1 and 3, and the Permissive Switch for DAS HSI and its interface to DAAC 2 and 4. The Permissive Switch for DAS HSI is common for all DAS Manual Initiation/Control Functions. The operator can initiate ~~this function a~~ specific DAS Function at any time by operation of both of these switches in the control room. This action will cause actuation of all components in the same manner as any of the automatic actuation signals.

b. ~~Automatic~~ Actuation Logic and Actuation Outputs

This LCO requires ~~two channels~~four DAAC subsystems to be OPERABLE. Actuation ~~logic~~Logic and Actuation Outputs consists of all circuitry housed within the DAAC, up to the Rod Drive Motor-Generator set trip devices or the Power Interface modules ~~responsible for actuating~~ the ESF equipment.

c. Low Pressurizer Pressure

There are four Low Pressurizer Pressure channels ~~in~~with two-out-of-four voting logic in each DAAC subsystem. This automatic function is automatically blocked when status signals (P-4) are received indicating that the minimum combination of the RTBs have actuated for the RT function. The LCO requires ~~2~~3 Low Pressurizer Pressure channels for each DAAC subsystem to be OPERABLE.

d. High Pressurizer Pressure

There are four High Pressurizer Pressure channels ~~in~~with two-out-of-four voting logic in each DAAC subsystem. This automatic function is automatically blocked when status signals (P-4) are received indicating that the minimum combination (2-out-of-4) of the RTBs have actuated for the RT function. The LCO requires ~~2~~3 High Pressurizer Pressure channels for each DAAC subsystem to be OPERABLE.

e. Low Steam Generator Water Level

There is one Low SG Water Level channel for each SG (four total). The LCO requires 1 Low SG Water Level channel for each DAAC subsystem to be OPERABLE on any 23 Steam Generators. These signals from each SG are processed throughwith two-out-of-four voting logic in each DAAC subsystem. The D3 Coping Analysis (Ref. 2) demonstrates that the two-out-of-four voting logic is adequate for all secondary events including loss of feedwater and SG rupture. This automatic function is automatically blocked when status signals (P-4) are received indicating that the minimum combination (2-out-of-4) of the RTBs have actuated for the RT function.

f. Rod Drive Motor-Generator Set Trip Device

This LCO requires two Rod Drive Motor-Generator ~~s~~Set

~~This LCO requires two channels~~ Trip Device subsystems, one for each Motor-Generator set, to be OPERABLE. ~~Each channel~~ This is because each subsystem trips one Motor-Generator set. ~~Both and both~~ Motor-Generator sets must be tripped for this Reactor Trip Function. The DAS cannot initiate a Reactor Trip with a failure of a Rod Drive Motor-Generator Set Trip Device.

2. Emergency Feedwater Actuation

a. Manual Initiation

Manual Initiation consists of the same features and operates in the same manner as described for DAS Function 1.a. One channel is required to be OPERABLE.

b. ~~Automatic~~ Actuation Logic and Actuation Outputs

~~Automatic actuation logic~~ Actuation Logic and ~~actuation outputs~~ Actuation Outputs consist of the same features and operate in the same manner as described for DAS Function 1.b. Four subsystems are required to be OPERABLE.

c. Low Steam Generator Water Level

The Low Steam Generator Water Level channels consist of the same features and operate in the same manner as described for DAS Function 1.e. ~~This~~ One Low SG Water Level channel for each DAAC subsystem is required to be OPERABLE on any 3 Steam Generators.

The DAS Emergency Feedwater (EFW) Actuation automatic function is automatically blocked when status signals are received indicating that the PSMS ESFAS EFW function has actuated correctly. Correct actuation is indicated when ~~2-out-of-4~~ status

signals are received from limit switch contacts on the steam inlet valves to the turbine driven EFW pumps **and/or** from auxiliary contacts on the motor starters controlling the motor driven EFW pumps.

3. ECCS Actuation

a. Manual Initiation

Manual Initiation consists of the same features and operates in the same manner as described for DAS Function 1.a. One channel is required to be OPERABLE.

b. Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for DAS Function 1.b. Four subsystems are required to be OPERABLE.

c. ECCS Actuation – Low-Low Pressurizer Pressure

There are four Low-Low Pressurizer Pressure channels with two-out-of-four voting logic in each DAAC subsystem. This automatic function is automatically blocked when status signals are received from auxiliary contacts on the motor starters controlling the Safety Injection (SI) pumps, indicating that 2-out-of-4 pumps have actuated. The LCO requires 3 Low-Low Pressurizer Pressure channels for each DAAC subsystem to be OPERABLE.

4. Containment Isolation

a. Manual Initiation

There are two valves for each containment penetration. Only one of the two valves is controlled by the DAS. Manual Initiation consists of the same features and operates in the same manner as described for DAS Function 1.a. One channel is required to be OPERABLE.

b. Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for DAS Function 1.b. Four subsystems are required to be OPERABLE.

5. EFW Isolation Valves

a. Manual Control

There are separate EFW Isolation Valves Control ~~switches~~channels for each Steam Generator. Manual Initiation consists of the same features and operates in the same manner as described for DAS Function 1.a. The LCO requires ~~4~~one channel to be OPERABLE for each of ~~the~~four Steam Generators. ~~This consists of the EFW Isolation Valves – Manual Control switch, and the Permissive Switch for DAS HSI. The Permissive Switch for DAS HSI is common for all DAS Manual Initiation/Control Functions.~~ The operator can initiate this ~~function~~Function for any single Steam Generator at any time by operation of both of these switches in the control room.

b. Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for DAS Function 1.b. Four subsystems are required to be OPERABLE.

6. Pressurizer Safety Depressurization Valves

a. Manual Control

There are four Pressurizer Safety Depressurization Valves. Only one of the four valves is controlled by the DAS. The LCO requires one channel to be OPERABLE. The channel consists of the Pressurizer Safety Depressurization Valves - Manual Control switch, and the Permissive Switch for DAS HSI. The Permissive Switch for DAS HSI is common for all DAS Manual Initiation ~~consists~~Control Functions. The operator can initiate this function at any time by operation of both of these switches in the control room.

b. Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operates in the same manner as described for DAS Function 1.~~ab.~~ Four subsystems are required to be OPERABLE.

7. Main Steam Depressurization Valves

a. Manual Control

There are separate Main Steam Depressurization Valve ~~switches~~Control channels for each Steam Generator. The LCO requires ~~4~~one channel to be OPERABLE for each ~~of the four~~Steam Generator.~~This s.~~ A channel consists of the Main Steam Depressurization Valves - Manual Control switch, and the Permissive Switch for DAS HSI. The Permissive Switch for DAS HSI is common for all DAS Manual Initiation/Control Functions. The operator can initiate ~~Main Steam Depressurization Valves~~this

Function for any single Steam Generator at any time by operation of both of these switches in the control room.

8. Main Steam Line Isolation

a. Manual Initiation

Manual Initiation consists of the same features and operates in the same manner as described for DAS Function 1.a. One channel is required to be OPERABLE.

b. Actuation Logic and Actuation Outputs

Actuation Logic and Actuation Outputs consist of the same features and operate in the same manner as described for DAS Function 1.b. Four subsystems are required to be OPERABLE.

ACTIONS

In all cases where the LCO states “Restore channel or subsystem to OPERABLE status”, this means restore the required number of channels or subsystems to OPERABLE status. Therefore, restoration of an alternate channel or subsystem, other than the failed channel or subsystem, is also acceptable.

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

Condition A applies when one or more subsystems or required ~~DAS Functions are~~ channels are inoperable.

~~If in~~ in one or more ~~required DAS functions are~~ Functions. With one subsystem or required channel inoperable, 30 days are allowed to restore the ~~Function~~ channel or subsystem to OPERABLE status. ~~30-~~

The Completion Time of 30 days is reasonable justified because the DAS is a separate and diverse non-safety backup system. ~~The 30 days Completion Time allows sufficient time to repair an inoperable DAS and ensures the control is repaired to provide backup protection~~ In addition, the Completion Time considers that the remaining OPERABLE channels and Actuation Logic and Actuation Outputs subsystems are adequate to perform the DAS Function.

~~Failure to restore the inoperable channel to OPERABLE status or place it in the tripped condition within 30 days, requires the unit be placed in MODE 3 within the following 6 hours and MODE 4 within the next 6 hours.~~ The Required Actions are modified by two Notes. Note 1 allows placing the Actuation Logic of one subsystem or one required channel in bypass for up to 4 hours while performing surveillance testing, provided the Actuation Logic in the other subsystems or the other required channels are OPERABLE. This Note does not allow a bypass with one

channel or subsystem in the tripped condition, as for the RTS and ESFAS, to avoid a spurious DAS actuation.

The Bypass Time of 4 hours for Actuation Logic and channels is justified because the remaining OPERABLE channels or subsystems are adequate to perform the safety function.

Note 2 allows placing the Actuation Outputs of two subsystems in bypass for up to 4 hours while performing surveillance testing of the Actuation Outputs from the other subsystems, or surveillance testing of the Rod Drive Motor-Generator Set Trip Devices. This bypass avoids spurious DAS actuation, because the Actuation Outputs and Rod Drive Motor-Generator Set Trip Devices must be actuated for these tests and they do not have bypass test capability.

When the Actuation Outputs of DAAC 1 or DAAC 3 are tested, this Note allows bypassing the Actuation Outputs of DAAC 2 and DAAC 4, to prevent spurious signals that would result in a spurious reactor trip or ESF actuation. When the Actuation Outputs of DAAC 2 or DAAC 4 are tested, this Note allows bypassing the Actuation Outputs of DAAC 1 and DAAC 3, to prevent spurious signals that would result in a spurious reactor trip or ESF actuation.

When Rod Drive Motor-Generator Set Trip Device 1 is tested, this Note allows bypassing the Actuation Outputs of DAAC 2 and DAAC 4, to prevent spurious signals that would trip Rod Drive Motor-Generator Set Trip Device 2 and cause a spurious reactor trip. When Rod Drive Motor-Generator Set Trip Device 2 is tested, this Note allows bypassing the Actuation Outputs of DAAC 1 and DAAC 3, to prevent spurious signals that would trip Rod Drive Motor-Generator Set Trip Device 1 and cause a spurious reactor trip.

The Bypass Time of 4 hours for Actuation Outputs is justified because the DAS is a separate and diverse non-safety backup system.

The 4 hour Bypass Time for all Functions is reasonable, based on operating experience that 4 hours is the average time required to perform a channel, Actuation Logic, Actuation Output or Rod Drive Motor-Generator Set Trip Device surveillance.

B.1 and B.2

Condition B applies when the Required Action and associated Completion Time of Condition A are not met. In this condition, 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 to MODE 4 within 12 hours. The allowed Completion Times ~~for Required Actions A.2 and A.3~~ 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. ~~In MODE 4, these Functions are no longer required OPERABLE.~~

SURVEILLANCE REQUIREMENTS

SR 3.3.6.1

SR 3.3.6.1 is performance of CHANNEL CHECK. Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between ~~the two~~ instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying 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 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.~~

[The Surveillance Frequency of 31 days is justified based on the following: Since sensor signals used by the DAS are distributed from the PSMS, the CHANNEL CHECK of the DAS sensors is included in the PSMS CHANNEL CHECK, which is conducted automatically and continuously. The isolation module of the PSMS and the indicator of the DAS, that cannot be confirmed ~~in~~by the continuous CHANNEL CHECK on the PSMS, are manually confirmed by this SR. These conventional analog devices, which operate only in mild environments, have a long history of proven reliability.

~~The reliability of the isolation module is included in the scope of the PRA, and the adequacy of the test interval of once every 31 days is confirmed in the PRA.~~

OR ~~The~~the Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.6.2

A COT ~~-analog~~ is performed on each required channel to ensure the ~~entire channel~~ DAAC process control equipment (including analog bistable modules) and DHP indications and alarms will perform ~~the~~their intended Function. The COT for DAS is performed by injecting simulated process measurement signals at a point that overlaps with the CHANNEL CALIBRATION. The signal distribution module for sensors shared

between PSMS and DAS shall be checked by either CHANNEL CALIBRATION or COT.

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

~~Setpoints~~ The COT confirms the accuracy of the channel's trip setting (i.e., the channel's analog bistable state change). The state change must occur within the Allowable Value administered of the Nominal Trip Setpoint. The Nominal Trip Setpoints and Allowable Values are recorded and maintained in a document established by the SCP.

The analog setpoint shall be left set consistent with the Calibration Tolerance recorded and maintained in a document established by the SCP ~~the assumptions of the current unit specific setpoint methodology.~~

[The Surveillance Frequency of 24 months is adequate. It is based on industry operating experience ~~with Anticipated Transient Without Scram (ATWS) mitigation systems.~~

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.6.3

CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test ~~verifies~~ must be performed consistent with the methods and assumptions of Specification 5.5.21, SCP, to verify that the channel responds to a measured parameter within the necessary range and accuracy. Since all DAS channels are shared with the PSMS, a Note has been added that allows the CHANNEL CALIBRATION conducted for the PSMS in LCO 3.3.1 or 3.3.2 to be credited for DAS.

~~CHANNEL CALIBRATION must be performed consistent with the methods and assumptions in Section 5.5.21, SCP.~~

[The Surveillance Frequency of 24 months is based on the assumption of 24 months calibration interval in the determination of the magnitude of equipment drift in ~~the setpoint methodology.~~ accordance with Specification 5.5.21, Setpoint Control Program (SCP).

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.6.4

An ACTUATION LOGIC TEST is performed on each of the DAAG (four Diverse Automatic Actuation Cabinet) ~~using the semiautomatic tester. The channel being tested is placed in the bypass condition, thus preventing inadvertent actuation. Through the semiautomatic tester, all~~ subsystems. All possible logic combinations are tested for each protection function. Verification of ~~Bistable module,~~ each Logic module, and Output module is included in this test.

[The Surveillance Frequency of 24 months is adequate. It is based on industry operating experience ~~with Anticipated Transient Without Scram (ATWS) mitigation systems.~~

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.6.5

A TADOT is performed for the Manual Initiation/Control and Actuation Outputs of all DAS functions. This test actuates the outputs to the PSMS Power Interface modules. Through overlap with the ACTUATION LOGIC TEST, the TADOT confirms these outputs can be generated from the Manual Initiation/Control switches and from the ~~Automatic Actuation Logic.~~ automatic actuation logic.

[The Surveillance Frequency of 24 months is adequate, based on industry operating experience with ATWS mitigation systems, considering instrument reliability and operating history data ~~of solid state Actuation Outputs devices.~~

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.] ~~The Actuation Outputs are solid state devices.~~

SR 3.3.6.6

A TADOT for the Rod Drive Motor-Generator set trip devices is performed by actuating the Manual Initiation switch from the control room and by verifying actuation of the Rod Drive Motor-Generator set trip device. Through overlap with the ACTUATION LOGIC TEST, the TADOT confirms the Rod Drive Motor-Generator set trip devices can be actuated from the Manual Initiation/Control switches and from the ~~Automatic Actuation Logic~~ automatic actuation logic.

[The Surveillance Frequency of 24 months is based on known reliability of the Functions, and has been shown to be acceptable through operating experience ~~with ATWS mitigation systems.~~

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

REFERENCES

1. MUAP-07006-P-~~(Proprietary)~~ and MUAP-07006-NP-~~(Non-Proprietary)~~-A, Revision 2, “Defense-in-Depth and Diversity.”
 2. MUAP-07014-P-~~(Proprietary)~~ and MUAP-07014-NP-~~(Non-Proprietary)~~, Revision 4, “Defense-in-Depth and Diversity Coping Analysis.”
 3. FSAR Section 7.8.
 4. 10 CFR 50.49.
 5. 10 CFR 50.36.
 6. FSAR Chapter 15.
 7. MUAP-09022-P, Revision 2, “US-APWR Instrument Setpoint Methodology.”
 8. U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems.”
-

16.2 Combined License Information

COL 16.1(1)	<i>Adoption of RMTS is to be confirmed and the relevant descriptions are to be fixed.</i>	
COL 16.1(2)	<i>Adoption of SFCP is to be confirmed and the relevant descriptions are to be fixed.</i>	
COL 16.1_3.3.1(1)	<i>Deleted.</i>	<i>COL 16.1_3.3.2(2) LCO 3.3.2 and associated Bases for hazardous chemical are to be confirmed by the evaluation with site-specific condition.</i>
COL 16.1_3.3.2(1)	<i>Deleted.</i>	
COL 16.1_3.3.5(1)	<i>The time delay values in SR 3.3.5.3 are to be confirmed based on the plant specific transmission system performance.</i>	<i>Deleted.</i>
COL 16.1_3.3.6(1)	<i>Deleted.</i>	<i>COL 16.1_3.3.4(1) Component controls and instrumentation required for safe shutdown related to the Ultimate Heat Sink in Tables B 3.3.4-1 and B 3.3.4-2 to be specified.</i>
COL 16.1_3.4.17(1)	<i>Deleted.</i>	
COL 16.1_3.7.9(1)	<i>LCO 3.7.9 and associated Bases for the Ultimate Heat Sink based on plant specific design, including required UHS water volume, lowest water level for ESW pumps and maximum water temperature of the UHS, are to be developed.</i>	
COL 16.1_3.7.10(1)	<i>LCO 3.7.10 and associated Bases for hazardous chemical are to be confirmed by the evaluation with site-specific condition.</i>	
COL 16.1_3.8.4(1)	<i>The battery float current values in required action A.2 is to be confirmed after selection of the plant batteries.</i>	
COL 16.1_3.8.5(1)	<i>The battery float current values in required action A.2 is to be confirmed after selection of the plant batteries.</i>	
COL 16.1_3.8.6(1)	<i>The battery float current values in condition B, required action B.2, and SR 3.8.6.1 are to be confirmed after selection of the plant batteries.</i>	
COL 16.1_4.1(1)	<i>The site specific information for site location is to be provided.</i>	
COL 16.1_4.3.1(1)	<i>Deleted.</i>	
COL 16.1_5.1.1(1)	<i>The titles for members of the unit staff are to be specified .</i>	
COL 16.1_5.1.2(1)	<i>The titles for members of the unit staff are to be specified .</i>	
COL 16.1_5.2.1(1)	<i>The titles for members of the unit staff are to be specified.</i>	
COL 16.1_5.2.2(1)	<i>The titles and number for members of the unit staff are to be specified.</i>	
COL 16.1_5.3.1(1)	<i>Minimum qualification for unit staff is to be specified.</i>	

Appendix 19B Summary of PSMS Reliability Analysis in PRA

In the US-APWR Base PRA, the Protection and Safety Monitoring System (PSMS) is modeled in the Fault Tree Analysis (FTA) at the module level (Refer to Attachments 6A.12, 6A.13 and 6A.14.10 of MUAP-07030 "US-APWR Probabilistic Risk Assessment"). With one exception, described below, the unavailability of each module of the reactor trip (RT) and engineered safety features (ESF) actuation functions of the PSMS is calculated based on the bounding longest Completion Time (CT), Bypass Time (BT) and Surveillance Frequency (SF) defined in the US-APWR Technical Specification (TS). Due to the use of digital technology, some of these times are extended from past industry experience, as represented by the Westinghouse Owners Group (WOG) Standard Technical Specifications (STS). For the RT and ESF actuation functions Tables 19B-1 and 19B-2, respectively, show the times for the US-APWR TS, the corresponding times for the WOG STS and the times used in the US-APWR Base PRA.

In the PRA unavailability calculation, a single FTA model is used to represent all RT and ESF functions of the PSMS. As explained above, for this representative model, the longest values of CT, BT and SF are applied for the RPS and ESFAS subsystems of the PSMS in order to bound all RT and ESF actuation functions. For the SLS subsystem of the PSMS, the longest TS values of CT and BT are also applied. However, for the SLS subsystem, the PRA credits a more realistic test frequency value, which is the frequency for in-service testing (IST) of the mechanical components, which are actuated by the SLS. Since the SLS controls these mechanical components, and the SLS is actuated during IST, the IST value is applicable.

With the bounding longest values of CT, BT and SF for most of the PSMS, as defined by the US-APWR TS, and the IST SF values for the SLS portion of the PSMS, the US-APWR Base PRA shows acceptable CDF results. In addition, to supplement the Base PRA results, sensitivity analyses are also performed to show how changes in the PSMS CT, BT and SF affect the resulting CDF (Refer to Attachment 18A.1 of MUAP-07030 "Probabilistic Risk Assessment"). The Base PRA (Case 0) and the additional evaluated cases (Case 1-4) are summarized in Table 19B-3. The evaluated cases reflect (1) comparisons for using shorter WOG STS values for CT, BT and SF, instead of the US-APWR TS values used in the Base PRA, and (2) comparisons for longer US-APWR TS values for the SLS SF, instead of the SLS IST value used in the Base PRA. For each Case, Table 19B-3 shows the changes from the Base PRA (Case 0), the resulting CDF for internal events, and a comparison of that CDF to the CDF for the Base PRA (Case 0). The following summarizes each Case:

Case 0: Base case of US-APWR PRA, using US-APWR TS CT, BT SF value with IST value for SLS SF.

Case 1: This case was performed to assess the impact of using the US-APWR IST value for the SLS SF in the Base PRA (Case 0). The US-APWR IST value used in the Base PRA is more frequent than the US-APWR TS SF value for the SLS. In this case the SLS IST SF value used in Case 0, is replaced with the US-APWR TS SF value. The results show that when the less frequent US-APWR TS SF value is used, the CDF increases 1.9% compared to the Base PRA (Case 0).

Case 2: This case was performed to assess the impact of using the US-APWR TS CT and BT values in the Base PRA (Case 0). Some of the US-APWR TS CT and BT values used in the Base PRA are longer than the WOG STS CT and BT values. In this case the US-APWR TS CT and BT values used in Case 0, are replaced with the WOG STS CT and BT values. The results show that when the more frequent WOG STS CT and BT values are used, the CDF decreases by 0.1% compared to the Base PRA (Case 0).

Case 3: This case was performed to assess the impact of using the US-APWR TS SF values, and the IST SF value for the SLS in the Base PRA (Case 0). Some of the US-APWR TS SF values are less frequent than the WOG STS SF values. In this case the US-APWR TS SF values and the SLS IST SF value used in Case 0, are replaced with the WOG STS SF values. The results show that when the more frequent WOG STS SF values are used, the CDF decreases by 4.2% compared to the Base PRA (Case 0).

Case 4: This case was performed to assess the impact of using the US-APWR TS CT, BT and SF values, and the IST SF value for the SLS in the Base PRA (Case 0). Some of the US-APWR TS CT and BT values are longer than the WOG STS CT and BT values, and some of the US-APWR TS SF values are less frequent than the WOG STS SF values. In this case the US-APWR TS CT, BT and SF values, and the IST SF value for the SLS, are replaced with the WOG STS CT, BT and SF values. The results show that when the more frequent WOG STS CT, BT and SF values are used, the CDF decreases by 4.3% compared to the Base PRA (Case 0).

As shown in Table 19B-3 for Cases 1-4, the changes in CDF from internal events, compared to the Base PRA (Case 0), are less than 5% for all comparison cases. Therefore, the sensitivity analyses shows (1) an insignificant risk impact for the extension of the US-APWR TS values from the WOG STS values and (2) an insignificant risk impact when the actual US-APWR TS values for SLS surveillance frequency are applied, instead of the IST values.

It is noted that there are also differences in the values of CT, BT and SF between the US-APWR TS and WOG STS for Manual Initiation of RT and ESFAS. However, as indicated in the risk important analysis documented in this Chapter, the Manual Initiation functions are considered negligible for CDF reduction (i.e., other failures dominate the failure of RT or ESF actuation). Therefore, no sensitivity analyses were performed for Manual Initiation functions.

Table 19B-1 Comparison of TS requirements for reactor trip system

Function	US-APWR TS *0, *1			WOG STS *1			Value Used in US-APWR Base PRA *2					
	CT	BT	SF	CT	BT	SF	CT	BT	SF			
High Pressurizer Pressure / Low SG Water Level	<u>1h</u>	<u>NA</u>	12h	72h	12h	12h	72h *3	12h	12h	Surveillance Test		
			<u>24M</u>			184d					24M	MEMORY INTEGRITY CHECK*11
			<u>24M</u>			18M					24M	
Automatic Trip Logic (RPS, except output)	24h /48h *5	4h	<u>24M</u>	24h /48h *5	4h	92d STB	72h *6	4h	24M	MEMORY INTEGRITY CHECK*11		
RPS output and Reactor Trip Breaker*7	24h /48h *8	<u>NA</u>	<u>62d</u> STB *9	24h /48h *8	4h	62d STB	48h *10	NA	62d STB	TRIP ACTUATION DEVICE OPERATIONAL TEST		

*0: In the US-APWR TS columns, the values that are different from the WOG STS are underlined.

*1: These columns indicate the Tech Spec values for the specific functions represented in the Function column.

*2: The values in these columns bound the US-APWR TS values for the functions represented in the Function column, and all other RT functions.

*3: 72 hours CT is used in the unavailability calculation since other RT functions have 72 hours CT.

*4: 12 hours BT is used in the unavailability calculation since other RT functions have 12 hours BT.

*5: Automatic Trip Logic in Mode 1 and 2 has 24 hours CT. In other Modes, Automatic Trip Logic has 48 hours CT.

*6: 72 hours CT is used since the same I&C equipment is shared between the channel processing part and logic processing part of RPS, and the longest CT for the channel processing part is 72 hours, as explained in Item 3, above.

*7: Includes the mechanical portion of the reactor trip breakers, and the reactor trip breaker undervoltage mechanisms and shunt trip mechanisms.

*8: Only the mechanical portion of the RTB in Mode 1 and 2 has 24 hours CT. RPS output, mechanical portion of the RTB in other Modes, and reactor trip breaker undervoltage mechanisms and shunt trip mechanisms have 48 hours CT.

*9: This number is underlined because the US-APWR has four trains. Therefore the test frequency for the same component is not the same as for WOG STS.

- *10: 48 hours CT is used in all RTB unavailability calculations for simplicity.
- *11: The CHANNEL OPERATIONAL TEST and the ACTUATION LOGIC TEST, as used in the WOG STS, correspond to the MEMORY INTEGRITY CHECK (SR 3.3.1.6) in the US-APWR TS.

Table 19B-2 Comparison of TS requirements for ESF actuation system

Function	US-APWR TS *0, *1			WOG STS *1			Value Used in US-APWR Base PRA *2			
	CT	BT	SF	CT	BT	SF	CT	BT	SF	
High Containment Pressure / Low Pressurizer Pressure	72h / 1h *3	12h / NA *3	12h	72h	12h	12h	72h *4	12h *5	12h	Surveillance Test CHANNEL CHECK MEMORY INTEGRITY CHECK*9 CHANNEL CALIBRATION
			<u>24M</u>			184d			24M *6	
			<u>24M</u>			18M			24M *6	
Actuation Logic (ESFAS)	24h	4h	<u>24M</u>	24h	4h	92d STB *6	72h *8	4h	92d *7	MEMORY INTEGRITY CHECK*9 and Manual Initiation TADOT*6 In-service Test for Mechanical Components *7
Actuation Logic (SLS)										
Actuation Outputs (SLS)										

*0: In the US-APWR TS columns, the values that are different from WOG STS are underlined.

*1: These columns indicate the Tech Spec values only for ECCS actuation, as a representative function.

*2: These columns bound all ESFAS functions.

*3: In the US-APWR TS, Pressurizer Pressure has 1 hour CT and no bypass capability, while Containment Pressure has 72 hours CT and 12 hours BT.

*4: 72 hours CT is used in the unavailability calculation since other ESF actuation functions have 72 hours CT.

*5: 12 hours BT is used in the unavailability calculation since other ESF actuation functions have 12 hours BT.

*6: The ACTUATION LOGIC TEST (92 days Staggered Test Basis (STB)) and the MASTER RELAY TEST (92 days STB) of the WOG STS, correspond to the MEMORY INTEGRITY CHECK*9 (SR 3.3.2.2) and ESFAS Manual Initiation TRIP ACTUATING DEVICE OPERATIONAL TEST (TADOT) (SR 3.3.2.5) (24 months) in the US-APWR TS.

*7: The SLAVE RELAY TEST (92 days) of the WOG STS corresponds to the test of the Actuation Logic (SR 3.3.2.2) and Actuation Outputs (SR 3.3.2.3) of the US-APWR SLS (24 months). However, the US-APWR In-service Test for Mechanical Components (92 days) also confirms the Actuation Logic and Actuation Outputs of the SLS.

*8: 72 hours CT is used in unavailability calculation since the Emergency Feedwater Actuation Function has 72 hours CT.

*9: The CHANNEL OPERATIONAL TEST and ACTUATION LOGIC TEST, as used in the WOG STS, correspond to the MEMORY INTEGRITY CHECK (SR 3.3.2.2) in the US-APWR TS.

Table 19B-3 Sensitivity analyses cases

Analysis Case	Applied Values for PSMS Unavailability Calculation		Internal events CDF [/RY]	Deviation of CDF Compared to Case 0 [/RY (%)]
	CT and BT	SF		
Case 0	US-APWR TS	US-APWR TS (IST frequency is applied to SLS)	1.03E-6	-
Case 1	US-APWR TS	US-APWR TS (including SF for SLS*)	1.05E-6	2.0E-08 (+1.9%)
Case 2	WOG STS*	US-APWR TS (IST frequency is applied to SLS)	1.03E-6	-1.0E-09 (-0.1%)
Case 3	US-APWR TS	WOG STS*	9.86E-7	-4.3E-08 (-4.2%)
Case 4	WOG STS*	WOG STS*	9.85E-7	-4.4E-08 (-4.3%)

*Changes from Base PRA (Case 0)