



Westinghouse Electric Company
Nuclear Power Plants
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, D.C. 20555

Direct tel: 412-374-6206
Direct fax: 724-940-8505
e-mail: sisk1rb@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP_NRC_002864

May 6, 2010

Subject: AP1000 Response to Request for Additional Information (SRP 16)

Westinghouse is submitting a response to the NRC request for additional information (RAI) on SRP Section 16. This RAI response is submitted in support of the AP1000 Design Certification Amendment Application (Docket No. 52-006). The information included in this response is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification and the AP1000 Design Certification Amendment Application.

Enclosure 1 provides the response for the following RAI(s):

RAI-SRP16.3-CTSB-SCP-1 R1

Questions or requests for additional information related to the content and preparation of this response should be directed to Westinghouse. Please send copies of such questions or requests to the prospective applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Robert Sisk', written over a horizontal line.

Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Strategy

/Enclosure

1. Response to Request for Additional Information on SRP Section 16

DO63
N120

cc:	D. Jaffe	-	U.S. NRC	1E
	E. McKenna	-	U.S. NRC	1E
	S. Mitra	-	U.S. NRC	1E
	T. Spink	-	TVA	1E
	P. Hastings	-	Duke Power	1E
	R. Kitchen	-	Progress Energy	1E
	A. Monroe	-	SCANA	1E
	P. Jacobs	-	Florida Power & Light	1E
	C. Pierce	-	Southern Company	1E
	E. Schmiech	-	Westinghouse	1E
	G. Zinke	-	NuStart/Entergy	1E
	R. Grumbir	-	NuStart	1E
	B. Seelman	-	Westinghouse	1E

ENCLOSURE 1

Response to Request for Additional Information on SRP Section 16

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP16.3-CTSB-SCP-1

Revision: 1

Question:

Please propose by incorporating into the AP1000 DCD technical specifications (TS) a Setpoint Control Program (SCP) in the TS Administrative Controls Section, in accordance with COL/DC-ISG-8, "Technical Specification Information that Combined License Applicants Must Provide in Combined License Application," that specifies use of an NRC-approved methodology for determining instrumentation trip setpoints (i.e., WCAP-16361, APP-PMS-JEP-001, Revision 0, May 2006, "Westinghouse Setpoint Methodology for Protection Systems – AP1000"). This will facilitate combined license (COL) applicants' adoption of the AP1000 DCD TS. The Reference COL plant intends to incorporate an SCP into its plant-specific TS.

Westinghouse Response:

The changes identified herein incorporate a Setpoint Program into the AP1000 DCD technical specifications consistent with COL/DC-ISG-8. These changes include the addition of a new subsection in the administrative controls programs and manuals section of chapter 16; revisions of a number of Surveillance Requirements; and revisions to appendix subsections B3.3.1 and B3.3.2.

Design Control Document (DCD) Revision:

The DCD changes herein are reflected in 5 areas: 1) Addition of section 5.5.14; 2) Markup of the surveillance requirements sections 3.1.8, 3.3.1, and 3.3.2, and markup of the section 3.1.8 surveillance requirements bases; 3) Section B.3.3.1 provided in its entirety containing revisions; 4) Section B.3.3.2 provided in its entirety containing revisions; and 5) markup of sections 7.2 and 7.3.

1) Revise DCD Section 16.1, to add new Administrative Control Technical Specification 5.5.14 to read:

5.5.14 Setpoint Program (SP)

- a. The Setpoint Program (SP) 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.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

- b. The Nominal Trip Setpoint (NTS), As-Found Tolerance (AFT), and As-Left Tolerance (ALT) for each Technical Specification required automatic protection instrumentation function shall be calculated in conformance with WCAP-16361-P, "Westinghouse Setpoint Methodology for Protection Systems – AP1000," May 2006.
- c. For each Technical Specification required automatic protection instrumentation function, performance of a CHANNEL CALIBRATION, CHANNEL OPERATIONAL TEST (COT), or REACTOR TRIP CHANNEL OPERATIONAL TEST (RTCOT) surveillance "in accordance with the Setpoint Program" shall include the following:
 - 1. The as-found value of the instrument channel trip setting shall be compared with the previously recorded as-left value.
 - i. If the as-found value of the instrument channel trip setting differs from the previously recorded as-left value by more than the pre-defined test acceptance criteria band (i.e., the specified AFT), 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. An Instrument Channel is determined to be functioning in accordance with its design basis if it can be set to within the ALT. This as-found condition shall be entered into the plant's corrective action program.
 - ii. If the as-found value of the instrument channel trip setting is less conservative than the specified AFT the surveillance requirement is not met and the instrument channel shall be immediately declared inoperable.
 - 2. The instrument channel trip setting shall be set to a value within the specified ALT around the specified NTS at the completion of the surveillance; otherwise, the surveillance requirement is not met and the instrument channel shall be immediately declared inoperable.
- d. The difference between the instrument channel trip setting as-found value and the previously recorded as-left value for each Technical Specification required automatic protection instrumentation function shall be trended and evaluated to verify that the instrument channel is functioning in accordance with its design basis.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

- e. The SP shall establish a document containing the current value of the specified NTS, AFT, and ALT 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 requirement of 10 CFR 50.59. In addition, changes to the specified NTS, AFT, and ALT values shall be governed by the approved setpoint methodology. This document, including any revisions or supplements, shall be provided upon issuance to the NRC.

2) Revise DCD Section 16.3.1 and 16.3.3 as shown on in Attachment 16.3A-1. The attachment provides a markup of the surveillance requirements sections 3.1.8, 3.3.1, and 3.3.2, and markup of the section 3.1.8 surveillance requirements bases is shown in Attachment 16.3A-2.

3) Chapter 16 Section B.3.3.1 provided in its entirety containing revisions as shown in Attachment 16.3B.

4) Chapter 16 Section B.3.3.2 provided in its entirety containing revisions as shown in Attachment 16.3C.

5) Chapter 7 markup sections 7.2.1.2.2 and 7.3.1.5.2 shown in Attachment 16.3D.

PRA Revision:

None.

Technical Report (TR) Revision:

None

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Attachment 16.3A-1

Markup of Surveillance Requirements for Sections 3.1.8, 3.3.1, and 3.3.2

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

PHYSICS TESTS Exceptions – MODE 2
3.1.8

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 3.1.8.1	Perform a REACTOR TRIP CHANNEL OPERATIONAL TEST on power range and intermediate range channels per SR 3.3.1.78.	Prior to initiation of PHYSICS TESTS
SR 3.1.8.2	Verify the RCS lowest loop average temperature is $\geq 541^{\circ}\text{F}$.	30 minutes
SR 3.1.8.3	Verify THERMAL POWER is $< 5\%$ RTP.	30 minutes
SR 3.1.8.4	Verify SDM is within the limits specified in the COLR.	24 hours

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
3.3.1

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE		FREQUENCY
SR 3.3.1.5	<p>-----</p> <p>- NOTE -</p> <p>Required to be met within 24 hours after reaching 50% RTP.</p> <p>-----</p> <p>Calibrate excore channels to agree with incore detector measurements.</p>	92 EFPD
SR 3.3.1.6	<p>-----</p> <p>- NOTE -</p> <p>This Surveillance must be performed on both reactor trip breakers associated with a single division.</p> <p>-----</p> <p>Perform TADOT.</p>	92 days on a STAGGERED TEST BASIS
SR 3.3.1.7	Perform RTCOT	92 days
SR 3.3.1.78	<p>-----</p> <p>- NOTE -</p> <p>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>-----</p> <p>Perform RTCOT in accordance with Setpoint Program.</p>	92 days

Response to Request For Additional Information (RAI)

RTS Instrumentation

3.3.1

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE	FREQUENCY
<p>SR 3.3.1.89</p> <hr/> <p style="text-align: center;">- NOTE -</p> <p>This Surveillance shall include verification that interlocks P-6 and P-10 are in their required state for existing unit conditions.</p> <hr/> <p>Perform RTCOT in accordance with Setpoint Program.</p>	<hr/> <p style="text-align: center;">- NOTE -</p> <p>Only required when not performed within previous 92 days</p> <hr/> <p>Prior to reactor startup</p> <p><u>AND</u></p> <p>Four hours after reducing power below P-10 for power and intermediate instrumentation</p> <p><u>AND</u></p> <p>Four hours after reducing power below P-6 for source range instrumentation</p> <p><u>AND</u></p> <p>Every 92 days thereafter</p>

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
3.3.1

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE	FREQUENCY
<p>SR 3.3.1.910 -----</p> <p style="text-align: center;">- NOTE -</p> <p>This Surveillance shall include verification that the time constants are adjusted to the prescribed values.</p> <p>-----</p> <p style="color: red;">Perform CHANNEL CALIBRATION in accordance with Setpoint Program.</p>	24 months
<p>SR 3.3.1.4011 -----</p> <p style="text-align: center;">- NOTE -</p> <p>Neutron detectors are excluded from CHANNEL CALIBRATION.</p> <p>-----</p> <p style="color: red;">Perform CHANNEL CALIBRATION in accordance with Setpoint Program.</p>	24 months
<p>SR 3.3.1.4112 -----</p> <p style="text-align: center;">- NOTE -</p> <p>Verification of setpoint is not required.</p> <p>-----</p> <p>Perform TADOT.</p>	24 months
<p>SR 3.3.1.4213 -----</p> <p style="text-align: center;">- NOTE -</p> <p>Neutron detectors are excluded from response time testing.</p> <p>-----</p> <p>Verify RTS RESPONSE TIME is within limits.</p>	24 months on a STAGGERED TEST BASIS

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
3.3.1

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE	FREQUENCY

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
3.3.1

Table 3.3.1-1 (page 1 of 45)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
1. Manual Reactor Trip	1,2 3 ^(a) ,4 ^(a) ,5 ^(a)	2 2	B C	SR 3.3.1.124 SR 3.3.1.124	NA NA	NA NA
2. Power Range Neutron Flux						
a. High Setpoint	1,2	4	D	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1.87 SR 3.3.1.110 SR 3.3.1.132	≤100.06% RTP	100% RTP
b. Low Setpoint	1 ^(b) ,2	4	E	SR 3.3.1.1 SR 3.3.1.98 SR 3.3.1.110 SR 3.3.1.132	≤25.06% RTP	25% RTP
3. Power Range Neutron Flux High Positive Rate	1,2	4	E	SR 3.3.1.87 SR 3.3.1.110 SR 3.3.1.132	≤5.06% RTP with time constant ≥2 sec	5.0% RTP with time constant ≥2 sec
4. Intermediate Range Neutron Flux	1 ^(b) ,2 ^(c)	4	F,G	SR 3.3.1.1 SR 3.3.1.98 SR 3.3.1.110 SR 3.3.1.132	≤25.23% RTP	25% RTP
	2 ^(d)	4	H	SR 3.3.1.1 SR 3.3.1.98 SR 3.3.1.110 SR 3.3.1.132	≤25.23% RTP	25% RTP
5. Source Range Neutron Flux High Setpoint	2 ^(d)	4	I,J	SR 3.3.1.1 SR 3.3.1.98 SR 3.3.1.110 SR 3.3.1.132	≤1.01 E5 cps	1.0 E5 cps
	3 ^(a) ,4 ^(a) ,5 ^(a)	4	J,Q	SR 3.3.1.1 SR 3.3.1.87 SR 3.3.1.110 SR 3.3.1.132	≤1.01 E5 cps	1.0 E5 cps
	3 ^(e) ,4 ^(e) ,5 ^(e)	1	R	SR 3.3.1.1 SR 3.3.1.110	NA	NA

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation 3.3.1

- (a) With Reactor Trip Breakers (RTBs) closed and Plant Control System capable of rod withdrawal.
- (b) Below the P-10 (Power Range Neutron Flux) interlocks.
- (c) Above the P-6 (Intermediate Range Neutron Flux) interlocks.
- (d) Below the P-6 (Intermediate Range Neutron Flux) interlocks.
- (e) With RTBs open. In this condition, Source Range Function does not provide reactor trip but does provide indication.

[Reviewer Note: In all cases, the values specified for trip setpoints and allowable values must be confirmed following completion of the plant specific setpoint study. Upon selection of the plant specific instrumentation, the Trip Setpoints will be calculated in accordance with the setpoint methodology described in WCAP-16361-P. Allowable Values will be calculated in accordance with the setpoint methodology and specified in the Allowable Value column. The plant specific setpoint calculations will reflect the latest licensing analysis/design basis and may incorporate NRC accepted improvements in setpoint methodology.]

Table 3.3.1-1 (page 2 of 45)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
6. Overtemperature ΔT	1,2	4	E	SR 3.3.1.1 SR 3.3.1.3 SR 3.3.1.4 SR 3.3.1.5 SR 3.3.1.87 SR 3.3.1.109 SR 3.3.1.132	Refer to Note 4 Table 3.3.1-1 (Page 5 of 5)	Refer to Note 4 Table 3.3.1-1 (Page 5 of 5)
7. Overpower ΔT	1,2	4	E	SR 3.3.1.1 SR 3.3.1.3 SR 3.3.1.87 SR 3.3.1.109 SR 3.3.1.132	Refer to Note 2 Table 3.3.1-1 (Page 5 of 5)	Refer to Note 2 Table 3.3.1-1 (Page 5 of 5)
8. Pressurizer Pressure						
a. Low Setpoint	1 ^(f)	4	K	SR 3.3.1.1 SR 3.3.1.87 SR 3.3.1.109 SR 3.3.1.132	≥ 1800.9 psig	1810.3 psig
b. High Setpoint	1,2	4	E	SR 3.3.1.1 SR 3.3.1.87 SR 3.3.1.109 SR 3.3.1.132	≤ 2420.7 psig	2420.3 psig
9. Pressurizer Water Level – High 3	1 ^(f)	4	K	SR 3.3.1.1 SR 3.3.1.87 SR 3.3.1.109 SR 3.3.1.132	$\leq 71.05\%$	71%
10. Reactor Coolant Flow – Low	1 ^(f)	4 per hot leg	K	SR 3.3.1.1 SR 3.3.1.87 SR 3.3.1.109 SR 3.3.1.132	$\geq 89.96\%$ ^(h)	90% ^(h)

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

						RTS Instrumentation 3.3.1	
11. Reactor Coolant Pump (RCP) Bearing Water Temperature – High	1,2	4 per RCP	E	SR 3.3.1.1	≤100.4°F	100°F	
				SR 3.3.1.87			
				SR 3.3.1.109			
				SR 3.3.1.132			
12. RCP Speed – Low	1 ^(f)	4	K	SR 3.3.1.1	≥90.9%	91%	
				SR 3.3.1.87			
				SR 3.3.1.109			
				SR 3.3.1.132			

(f) Above the P-10 (Power Range Neutron Flux) interlock.

(i) 90% of loop specific indicated flow.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
3.3.1

Table 3.3.1-1 (page 3 of 45)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
13. Steam Generator (SG) Narrow Range Water Level – Low	1,2	4 per SG	E	SR 3.3.1.1 SR 3.3.1.87 SR 3.3.1.109 SR 3.3.1.132	$\geq 20.05\%$ span	21% span
14. Steam Generator (SG) Narrow Range Water Level – High 2	1,2 ^(k)	4 per SG	E	SR 3.3.1.1 SR 3.3.1.87 SR 3.3.1.109 SR 3.3.1.132	$\leq 82.05\%$ span	82% span
15. Safeguards Actuation Input from Engineered Safety Feature Actuation System						
a. Manual	1,2	2	B	SR 3.3.1.124	NA	NA
b. Automatic	1,2	4	L	SR 3.3.1.7	NA	NA
16. Reactor Trip System Interlocks						
a. Intermediate Range Neutron Flux, P-6	2	4	M	SR 3.3.1.87 SR 3.3.1.110	$\geq 0.01 \pm 6\%$ RTP	1E-5% RTP
b. Power Range Neutron Flux, P-10	1,2	4	M	SR 3.3.1.87 SR 3.3.1.110	$\geq 0.04\%$ RTP $\leq 10.06\%$ RTP	10% RTP
c. Pressurizer Pressure, P-11	1,2	4	M	SR 3.3.1.87 SR 3.3.1.110	≤ 1070.4 psig	1070 psig
17. Reactor Trip Breakers	1,2 3 ^(j) , 4 ^(j) , 5 ^(j)	4 divisions with 2 RTBs per division	N,O	SR 3.3.1.6	NA	NA
18. Reactor Trip Breaker (RTB) Undervoltage and Shunt Trip Mechanisms	1,2 3 ^(j) , 4 ^(j) , 5 ^(j)	1 each per RTB mechanism	N,O	SR 3.3.1.6	NA	NA
19. Automatic Trip Logic	1,2 3 ^(j) , 4 ^(j) , 5 ^(j)	4 divisions 4 divisions	L P	SR 3.3.1.7 SR 3.3.1.7	NA NA	NA NA

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

(j) With Reactor Trip Breakers closed and Plant Control System capable of rod withdrawal.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
3.3.1

Table 3.3.1-1 (page 4 of 54)
Reactor Trip System Instrumentation

FUNCTION	APPLICABLE MODES OR SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
20. ADS Stages 1, 2, and 3 Actuation input from engineered safety feature actuation system						
a. Manual	1,2	2 switch sets	B	SR 3.3.1.124	NA	NA
	3 ^(j) , 4 ^(j) , 5 ^(j)	2 switch sets	B	SR 3.3.1.124	NA	NA
b. Automatic	1,2	4	L	SR 3.3.1.7	NA	NA
	3 ^(j) , 4 ^(j) , 5 ^(j)	4	P	SR 3.3.1.7	NA	NA
21. Core Makeup Tank Actuation input from engineered safety feature actuation system						
a. Manual	1,2	2 switch sets	B	SR 3.3.1.124	NA	NA
	3 ^(j) , 4 ^(j) , 5 ^(j)	2 switch sets	B	SR 3.3.1.124	NA	NA
b. Automatic	1,2	4	L	SR 3.3.1.7	NA	NA
	3 ^(j) , 4 ^(j) , 5 ^(j)	4	P	SR 3.3.1.7	NA	NA

(j) With Reactor Trip Breakers closed and Plant Control System capable of rod withdrawal.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
3.3.1

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

Note 1: Overtemperature ΔT

The ΔT power signal, $q_{\Delta T}$, shall not be less than the measured reactor thermal power by more than 1% of RTP, where the ΔT power signal, $q_{\Delta T}$, is computed as

$$q_{\Delta T} = \rho(T_C, P_{PZR}) [h(T_H, P_{PZR}) - h(T_C, P_{PZR})] / \Delta T^\circ$$

where:

$$T_C = [(1 + T_{1s}) / (1 + T_{2s})] T_{COLD}, \text{ where } T_{COLD} \text{ is the measured cold leg temperature, } ^\circ\text{F, with lead/lag compensation applied to compensate for cold leg to core transit time}$$

$$T_H = [(1 + T_{3s}) / (1 + T_{4s})] T_{HOT}, \text{ where } T_{HOT} \text{ is the measured hot leg temperature, } ^\circ\text{F, with lead/lag compensation applied to compensate for core to hot leg transit time}$$

$$\tau_1 \geq [^*] \text{ sec} \quad \tau_2 \leq [^*] \text{ sec}$$

$$\tau_4 \geq [^*] \text{ sec} \quad \tau_5 \leq [^*] \text{ sec}$$

$$\rho(T_C, P_{PZR}) = \text{density of water at the measured cold leg temperature in the cold leg } (T_C), ^\circ\text{F, and measured pressurizer pressure, } P_{PZR}, \text{ psia}$$

$$h(T, P_{PZR}) = \text{enthalpy of water at the specified measured temperature } (T_H \text{ or } T_C) \text{ and measured pressurizer pressure, } P_{PZR}, \text{ psia}$$

$$\Delta T^\circ = \text{a conversion factor, such that the value of } q_{\Delta T} \text{ is 100 percent at normal rated thermal power}$$

$$s = \text{Laplace transform operator}$$

And the Overtemperature ΔT setpoint shall not exceed the following nominal Trip Setpoint by more than 0.2% of RTP for T_{HOT} ; 0.2% of RTP for T_{COLD} ; 0.06% of RTP for pressure; and 0.14% of RTP for ΔT .

$$\text{OTAT}_{SP} = \text{OTAT}_{SP}^\circ - f_1(\Delta t)$$

where:

$$\text{OTAT}_{SP}^\circ = f(P_{PZR}, T_C), \text{ determined by interpolation from tables } [^*] \text{ of allowable core thermal power as a function of core inlet temperature at various pressures}$$

$$P_{PZR} \text{ and } T_C \text{ pressurizer pressure and cold leg temperature, are as defined above}$$

$$f_1(\Delta t) = \begin{cases} [^*] \{ [^*] + (q_t - q_b) \} & \text{when } q_t - q_b \leq [^*] \% \text{ RTP} \\ 0 \% \text{ of RTP} & \text{when } [^*] \% \text{ RTP} < q_t - q_b \leq [^*] \% \text{ RTP} \\ [^*] \{ (q_t - q_b) - [^*] \} & \text{when } q_t - q_b > [^*] \% \text{ RTP} \end{cases}$$

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.

Note 2: Overpower ΔT

The Overpower ΔT setpoint shall not exceed the following nominal Trip Setpoint by more than 0.2% of RTP for T_{HOT} ; and 0.2% of RTP for T_{COLD} .

$$\text{OPAT}_{SP} = K_4 - f_2(\Delta t)$$

Where:

$$K_4 \leq [^*]$$

$$f_2(\Delta t) = [^*]$$

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

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

SURVEILLANCE REQUIREMENTS

- NOTE -

Refer to Table 3.3.2-1 to determine which SRs apply for each Engineered Safety Features (ESF) Function.

SURVEILLANCE		FREQUENCY
SR 3.3.2.1	Perform CHANNEL CHECK.	12 hours
SR 3.3.2.2	Perform ACTUATION LOGIC TEST.	92 days on a STAGGERED TEST BASIS
SR 3.3.2.3	<p>- NOTE -</p> <p>Verification of setpoint not required for manual initiation functions.</p> <p>Perform TRIP ACTUATING DEVICE OPERATIONAL TEST (TADOT).</p>	24 months
SR 3.3.2.4	<p>- NOTE -</p> <p>This surveillance shall include verification that the time constants are adjusted to the prescribed values.</p> <p>Perform CHANNEL CALIBRATION in accordance with Setpoint Program.</p>	24 months
SR 3.3.2.5	Perform CHANNEL OPERATIONAL TEST (COT) in accordance with Setpoint Program.	92 days
SR 3.3.2.6	Verify ESFAS RESPONSE TIMES are within limit.	24 months on a STAGGERED TEST BASIS
SR 3.3.2.7	<p>- NOTE -</p> <p>This Surveillance is not required to be performed for actuated equipment which is included in the Inservice Test (IST) Program.</p>	

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Perform ACTUATION DEVICE TEST.

24 months

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE		FREQUENCY
SR 3.3.2.8	Perform ACTUATION DEVICE TEST for squib valves.	24 months
SR 3.3.2.9	Perform ACTUATION DEVICE TEST for pressurizer heater circuit breakers.	24 months

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 1 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
1. Safeguards Actuation						
a. Manual Initiation	1,2,3,4	2 switches	E,O	SR 3.3.2.3	NA	NA
	5	2 switches	G,Y	SR 3.3.2.3	NA	NA
b. Containment Pressure – High 2	1,2,3,4	4	B,O	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤6.21 psig	6.2 psig
c. Pressurizer Pressure – Low	1,2,3 ^(a)	4	B,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥1794.9 psig	1795.3 psig
d. Steam Line Pressure – Low	1,2,3 ^(a)	4 per steam line	B,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥559.7 psig ^(b)	560.3 psig ^(b)
e. RCS Cold Leg Temperature (T _{cold}) – Low	1,2,3 ^(a)	4 per loop	B,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥504.8°F ≤505.4°F	505°F

(a) Above the P-11 (Pressurizer Pressure) interlock, when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F.

(b) Time constants used in the lead/lag controller are $\tau_1 \geq 50$ seconds and $\tau_2 \leq 5$ seconds.

[Reviewer Note: In all cases, the values specified for trip setpoints and allowable values must be confirmed following completion of the plant-specific setpoint study. Upon selection of the plant-specific instrumentation, the Trip Setpoints will be calculated in accordance with the setpoint methodology described in WCAP-16361-P. Allowable Values will be calculated in accordance with the setpoint methodology and specified in the Allowable Value column. The plant-specific setpoint calculations will reflect the latest licensing analysis/design basis and may incorporate NRC accepted improvements in setpoint methodology.]

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 2 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
2. Core Makeup Tank (CMT) Actuation						
a. Manual Initiation	1,2,3,4 ^(j)	2 switches	E,N	SR 3.3.2.3	NA	NA
	4 ⁽ⁿ⁾ , 5 ^(l)	2 switches	E,U	SR 3.3.2.3	NA	NA
b. Pressurizer Water Level – Low 2	1,2,3,4 ^(j)	4	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	$\geq 0.95\%$ span $\leq 10.05\%$ span	10% span
	4 ⁽ⁿ⁾ , 5 ^(l)	4	B,V	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	$\geq 0.95\%$ span $\leq 10.05\%$ span	10% span
c. Safeguards Actuation	1,2,3,4,5 ^(l)	Refer to Function 1 (Safeguards Actuation) for initiating functions and requirements.				
d. ADS Stages 1, 2, & 3 Actuation	1,2,3,4,5 ^(l)	Refer to Function 9 (ADS Stages 1, 2 & 3 Actuation) for all initiating functions and requirements.				
3. Containment Isolation						
a. Manual Initiation	1,2,3,4	2 switches	E,O	SR 3.3.2.3	NA	NA
	5 ^(m) , 6 ^(m)	2 switches	G,Y	SR 3.3.2.3	NA	NA
b. Manual Initiation of Passive Containment Cooling	1,2,3,4,5 ^(e,m) , 6 ^(e,m)	Refer to Function 12.a (Passive Containment Cooling Actuation) for initiating functions and requirements.				
c. Safeguards Actuation	1,2,3,4,5 ^(m)	Refer to Function 1 (Safeguards Actuation) for initiating functions and requirements.				

(e) With decay heat > 9.0 MWt.

(l) With the RCS pressure boundary intact.

(j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).

(m) Not applicable for valve isolation Functions whose associated flow path is isolated.

(n) With the RCS being cooled by the RNS.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 3 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
4. Steam Line Isolation						
a. Manual Initiation	1,2 ^(l) ,3 ^(l) ,4 ^(l)	2 switches	E,S	SR 3.3.2.3	NA	NA
b. Containment Pressure – High 2	1,2 ^(l) ,3 ^(l) ,4 ^(l)	4	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤6.21 psig	6.2 psig
c. Steam Line Pressure						
(1) Steam Line Pressure – Low	1,2 ^(l) ,3 ^(a,l)	4 per steam line	B,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥559.7 psig ^(b)	560.3 psig ^(b)
(2) Steam Line Pressure – Negative Rate – High	3 ^(d,l)	4 per steam line	B,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤100.1 psig with time constant ≥50 seconds	100 psig with time constant ≥50 seconds
d. T _{cold} – Low	1,2 ^(l) ,3 ^(a,l)	4 per loop	B,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥504.9°F ≤505.1°F	505°F
5. Turbine Trip						
a. Manual Main Feedwater Isolation	1,2	Refer to Function 6.a (Manual Main Feedwater Control Valve Isolation) for requirements.				
b. SG Narrow Range Water Level – High 2	1,2	4 per SG	B,L	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤82.05% span	82% span
c. Safeguards Actuation	1,2	Refer to Function 1 (Safeguards Actuation) for initiating functions and requirements.				
d. Reactor Trip	1,2	Refer to Function 18.ba (ESFAS Interlocks, Reactor Trip, P-4) for requirements.				

(a) Above the P-11 (Pressurizer Pressure) interlock, when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F.

(b) Time constants used in the lead/lag controller are $\tau_1 \geq 50$ seconds and $\tau_2 \leq 5$ seconds.

(d) Below the P-11 (Pressurizer Pressure) interlock.

(l) Not applicable if all MSIVs are closed.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 4 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER		REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
	SPECIFIED CONDITIONS	OTHER					
6. Main Feedwater Control Valve Isolation							
a. Manual Initiation	1,2,3,4 ^(m)		2 switches	E,S	SR 3.3.2.3	NA	NA
b. SG Narrow Range Water Level – High 2	1,2,3,4 ^(j,m)		4 per SG	B,R	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤82.05% span	82% span
c. Safeguards Actuation	1,2,3,4 ^(m)		Refer to Function 1 (Safeguards Actuation) for all initiating functions and requirements.				
d. Reactor Coolant Average Temperature (T _{avg}) – Low 1	1,2		4	B,L	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥549.9°F	550°F
Coincident with Reactor Trip	1,2		Refer to Function 18.ba (ESFAS Interlocks, Reactor Trip, P-4) for requirements.				
7. Main Feedwater Pump Trip and Valve Isolation							
a. Manual Initiation	Refer to Function 6.a (Manual Main Feedwater Control Valve Isolation) for requirements.						
b. SG Narrow Range Water Level – High 2	1,2,3,4 ^(j,m)		4 per SG	B,R	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤82.05% span	82% span
c. Safeguards Actuation	1,2,3,4 ^(m)		Refer to Function 1 (Safeguards Actuation) for all initiating functions and requirements.				
d. Reactor Coolant Average Temperature T _{avg} – Low 2	1,2		2 per loop	B,L	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥541.9°F	≥542°F
Coincident with Reactor Trip	1,2		Refer to Function 18.ba (ESFAS Interlocks, Reactor Trip, P-4) for requirements.				

(j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).

(m) Not applicable for valve isolation Functions whose associated flow path is isolated.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 5 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
8. Startup Feedwater Isolation						
a. SG Narrow Range Water Level – High 2	1,2,3,4 ^(o)	4 per SG	B,S	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤82.05% span	82% span
b. T _{cold} – Low	1,2,3 ^(a)	4 per loop	B,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥504.0°F ≤506.4°F	505°F
c. Manual Initiation	Refer to Function 6.a (Manual Main Feedwater Control Valve Isolation) for requirements.					
9. ADS Stages 1, 2 & 3 Actuation						
a. Manual Initiation	1,2,3,4	2 switch sets	E,O	SR 3.3.2.3	NA	NA
	5 ^(k) ,6 ^(g,k)	2 switch sets	G,X	SR 3.3.2.3	NA	NA
b. Core Makeup Tank (CMT) Level – Low 1	1,2,3,4	4 per tank	B,O	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥56.0% span	61.0% span
	5 ^(c,k)	4 per OPERABLE tank	B,V	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥56.0% span	61.0% span
Coincident with CMT Actuation	Refer to Function 2 (CMT Actuation) for all initiating functions and requirements.					

(a) Above the P-11 (Pressurizer Pressure) interlock, when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F.

(c) With pressurizer level ≥20%.

(g) With upper internals in place.

(o) Not applicable when the startup feedwater flow paths are isolated.

(k) Not applicable when the required ADS valves are open. See LCO 3.4.12 and LCO 3.4.13 for ADS valve and equivalent relief area requirements.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 6 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
10. ADS Stage 4 Actuation						
a. Manual Initiation Coincident with	1,2,3,4	2 switch sets	E,O	SR 3.3.2.3	NA	NA
	5 ^(k) , 6 ^(g,k)	2 switch sets	G,X	SR 3.3.2.3	NA	NA
RCS Wide Range Pressure – Low, or	1,2,3,4	4	B,O	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥1198 psig	1200 psig
	5 ^(k) , 6 ^(g,k)	4	B,X	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥1198 psig	1200 psig
ADS Stages 1, 2 & 3 Actuation	Refer to Function 9 (Stages 1, 2, & 3 Actuation) for initiating functions and requirements					
b. CMT Level – Low 2	1,2,3,4	4 per tank	B,O	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥56.9% span	61.9% span
	5 ^(c,k)	4 per OPERABLE tank	B,V	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥56.9% span	61.9% span
Coincident with RCS Wide Range Pressure – Low, and	1,2,3,4	4	B,O	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥1198 psig	1200 psig
	5 ^(c,k)	4	B,V	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥1198 psig	1200 psig
Coincident with ADS Stages 1, 2 & 3 Actuation	1,2,3,4,5 ^(c,k)	Refer to Function 9 (ADS Stages 1, 2 & 3 Actuation) for initiating functions and requirements				
c. Coincident RCS Loop 1 and 2 Hot Leg Level – Low 2	4 ⁽ⁿ⁾ , 5 ^(k) , 6 ^(k)	1 per loop	BB,Y	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥2.98 in. above inside surface of the bottom of the hot legs	3 in. above inside surface of the bottom of the hot legs

(c) With pressurizer level ≥20%.

(g) With upper internals in place.

(k) Not applicable when the required ADS valves are open. See LCO 3.4.12 and LCO 3.4.13 for ADS valve and equivalent relief area requirements.

(n) With the RCS being cooled by the RNS.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 7 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
11. Reactor Coolant Pump Trip						
a. ADS Stages 1, 2 & 3 Actuation	Refer to Function 9 (ADS Stages 1, 2 & 3 Actuation) for initiating functions and requirements.					
b. Reactor Coolant Pump Bearing Water Temperature – High	1,2	4 per RCP	B,L	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤190.4°F	190°F
c. Manual CMT Actuation	Refer to Function 2.a (Manual CMT Actuation) for requirements.					
d. Pressurizer Water Level – Low 2	1,2,3,4 ^(j)	4	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥0.95% span ≤10.05% span	10% span
	4 ⁽ⁿ⁾ ,5 ^(c,j)	4	B,V	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥0.95% span ≤10.05% span	10% span
e. Safeguards Actuation	Refer to Function 1 (Safeguards Actuation) for initiating functions and requirements.					
12. Passive Containment Cooling Actuation						
a. Manual Initiation	1,2,3,4	2 switches	E,O	SR 3.3.2.3	NA	NA
	5 ^(e) ,6 ^(e)	2 switches	G,Y	SR 3.3.2.3	NA	NA
b. Containment Pressure – High 2	1,2,3,4	4	B,O	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤6.21 psig	6.2 psig

(c) With pressurizer level ≥20%.

(e) With decay heat > 9.0 MWt.

(j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).

(n) With the RCS being cooled by the RNS.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 8 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
13. Passive Residual Heat Removal Heat Exchanger Actuation						
a. Manual Initiation	1,2,3,4	2 switches	E,O	SR 3.3.2.3	NA	NA
	5 ^(l)	2 switches	E,U	SR 3.3.2.3	NA	NA
b. SG Narrow Range Water Level – Low	1,2,3,4 ^(j)	4 per SG	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥20.95% span	24% span
Coincident with Startup Feedwater Flow – Low	1,2,3,4 ^(j)	2 per feedwater line	H,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥198.8 gpm per SG	200 gpm per SG
c. SG Wide Range Water Level – Low	1,2,3,4 ^(j)	4 per SG	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥53.95% span	54% span
d. ADS Stages 1, 2 & 3 Actuation	1,2,3,4,5 ^(l)	Refer to Function 9 (ADS Stages 1, 2 & 3 Actuation) for initiating functions and requirements.				
e. CMT Actuation	Refer to Function 2 (CMT Actuation) for initiating functions and requirements.					
f. Pressurizer Water Level, High 3	1,2,3,4 ^(j,p)	4	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤71.05% span	74% span
14. SG Blowdown Isolation						
a. Passive Residual Heat Removal Heat Exchanger Actuation	1,2,3,4 ^(j,m)	Refer to Function 13 (Passive Residual Heat Removal Heat Exchanger Actuation) for all initiating functions and requirements.				
b. SG Narrow Range Water Level – Low	1,2,3,4 ^(j,m)	4 per SG	B,R	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥20.95% span	24% span

(l) With the RCS pressure boundary intact.

(j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).

(m) Not applicable for valve isolation Functions whose associated flow path is isolated.

(p) Above the P-19 (RCS Pressure) interlock.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 9 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
15. Boron Dilution Block						
a. Source Range Neutron Flux Doubling	2 ^(f) , 3 ^(f) , 4 ^(m)	4	B,T	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤Source Range Flux X 2.201 in 50 minutes	Source Range Flux X 2.2 in 50 minutes
	5 ^(m)	4	B,P	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤Source Range Flux X 2.201 in 50 minutes	Source Range Flux X 2.2 in 50 minutes
b. Reactor Trip	Refer to Function 18.ab (ESFAS Interlocks, Reactor Trip, P-4) for all requirements.					
16. Chemical Volume and Control System Makeup Isolation						
a. SG Narrow Range Water Level – High 2	1,2,3 ^(m) , 4 ^(j,m)	4 per SG	B,R	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤82.05% span	82% span
b. Pressurizer Water Level – High 1	1,2,3 ^(m)	4	B,Q	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤23.05% span	23% span
	Coincident with Safeguards Actuation	1,2,3 ^(m)	Refer to Function 1 (Safeguards Actuation) for initiating functions and requirements.			
c. Pressurizer Water Level – High 2	1,2,3,4 ^(j,m,p)	4	B,T	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤59.05% span	59% span
d. Containment Radioactivity – High 2	1,2,3 ^(m)	4	B,Q	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤150 R/hr	100 R/hr
e. Manual Initiation	1,2,3 ^(m) , 4 ^(j,m)	2 switches	E,R	SR 3.3.2.3	NA	NA
f. Source Range Neutron Flux Doubling	Refer to Function 15.a (Boron Dilution Block, Source Range Neutron Flux Doubling) for all requirements.					

(f) Not applicable when critical or during intentional approach to criticality.

(j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).

(m) Not applicable for valve isolation Functions whose associated flow path is isolated.

(p) Above the P-19 (RCS Pressure) interlock.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 10 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
17. Normal Residual Heat Removal System Isolation						
a. Containment Radioactivity – High 2	1,2,3 ^(m)	4	B,Q	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤150-R/hr	100-R/hr
b. Safeguards Actuation	1,2,3 ^(m)	Refer to Function 1 (Safeguards Actuation) for all initiating functions and requirements.				
c. Manual Initiation	1,2,3 ^(m)	2 switch sets	E,Q	SR 3.3.2.3	NA	NA
18. ESFAS Interlocks						
a. Reactor Trip Breaker Open, P-3	1,2,3	3 divisions	D,M	SR 3.3.2.3		
ba. Reactor Trip, P-4	1,2,3	3 divisions	D,M	SR 3.3.2.3	NA	NA
c. Intermediate Range Neutron Flux, P-6	2	4	J,L	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5		
db. Pressurizer Pressure, P-11	1,2,3	4	J,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5	≤1970.4-psig	1970-psig
c. Intermediate Range Neutron Flux, P-6	2	4	J,L	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5	≥0.01 E-6% RTP	1E-5% RTP
ed. Pressurizer Level, P-12	1,2,3,4,5,6	4	J,M BB,Y	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5	≤16.05% span	16%-span
fe. RCS Pressure, P-19	1,2,3,4 ^(l)	4	J,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5	≤702-psig	700-psig
f. Reactor Trip Breaker Open, P-3	1,2,3	3 divisions	D,M	SR 3.3.2.3	NA	NA
19. Containment Air Filtration System Isolation						
a. Containment Radioactivity – High 1	1,2,3,4 ^(l)	4	B,Z	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤3-R/hr	2-R/hr
b. Containment Isolation	Refer to Function 3 (Containment Isolation) for initiating functions and requirements.					

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

- (j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).
- (m) Not applicable for valve isolation Functions whose associated flow path is isolated.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 11 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
20. Main Control Room Isolation and Air Supply Initiation						
a. Control Room Air Supply Radiation – High 2	1,2,3,4	2	F,O	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	$\leq 1.5 \times 10^{-6}$ curies/m ³ DOSE EQUIVALENT I-131	1×10^{-6} curies/m ³ DOSE EQUIVALENT I-131
	Note (h)	2	G,K	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	$\leq 1.5 \times 10^{-6}$ curies/m ³ DOSE EQUIVALENT I-131	1×10^{-6} curies/m ³ DOSE EQUIVALENT I-131
b. Pressurizer Pressure – Low	1,2,3 ^(a)	4	B,M	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥ 1794.9 psig	1795.3 psig
21. Auxiliary Spray and Purification Line Isolation						
a. Pressurizer Water Level – Low 1	1,2	4	B,L	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	$\geq 19.95\%$ span	20.0% span
b. Manual Initiation	1,2	Refer to Function 16.e (Manual Chemical Volume Control System (Makeup Isolation) for requirements.				
22. In-Containment Refueling Water Storage Tank (IRWST) Injection Line Valve Actuation						
a. Manual Initiation	1,2,3,4 ^(j)	2 switch sets	E,N	SR 3.3.2.3	NA	NA
	4 ⁽ⁿ⁾ ,5,6	2 switch sets	G,Y	SR 3.3.2.3	NA	NA
b. ADS 4th Stage Actuation	Refer to Function 10 (ADS 4th Stage Actuation) for initiating functions and requirements.					

(a) Above the P-11 (Pressurizer Pressure) interlock, when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F.

(h) During movement of irradiated fuel assemblies.

(j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).

(n) With the RCS being cooled by the RNS.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 12 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
23. IRWST Containment Recirculation Valve Actuation						
a. Manual Initiation	1,2,3,4 ^(j)	2 switch sets	E,N	SR 3.3.2.3	NA	NA
	4 ⁽ⁿ⁾ ,5,6	2 switch sets	G,Y	SR 3.3.2.3	NA	NA
b. ADS Stage 4 Actuation	Refer to Function 10 (ADS Stage 4 Actuation) for all initiating functions and requirements:					
Coincident with IRWST Level – Low 3	1,2,3,4 ^(j)	4	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥Containment Elevation @ 100.99 ft.	Containment Elevation @ 110 ft.
	4 ⁽ⁿ⁾ ,5 ^(k) ,6 ^(k)	4	I,Y	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥Containment Elevation @ 100.99 ft.	Containment Elevation @ 110 ft.
24. Refueling Cavity Isolation						
a. Spent Fuel Pool Level – Low	6	3	H,P	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥39.74 ft.	39.75 ft.
25. ESF Coincidence Logic						
a. Coincidence Logic	1,2,3,4	4 divisions, 1 battery- backed subsystem per division	D,O	SR 3.3.2.2	NA	NA
	5,6	4 divisions, 1 battery- backed subsystem per division	G,W	SR 3.3.2.2	NA	NA

(k) Not applicable when the required ADS valves are open. See LCO 3.4.12 and LCO 3.4.13 for ADS valve and equivalent relief area requirements.

(j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).

(n) With the RCS being cooled by the RNS.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

Table 3.3.2-1 (page 13 of 13)
Engineered Safeguards Actuation System Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS	CONDITIONS	SURVEILLANCE REQUIREMENTS	ALLOWABLE VALUE	TRIP SETPOINT
26. ESF Actuation						
a. ESF Actuation Subsystem	1,2,3,4	4 divisions, 1 battery- backed subsystem per division	D,O	SR 3.3.2.2 SR 3.3.2.7 SR 3.3.2.8	NA	NA
	5,6	4 divisions, 1 battery- backed subsystem per division	G,W	SR 3.3.2.2 SR 3.3.2.7	NA	NA
27. Pressurizer Heater Trip						
a. Core Makeup Tank Actuation	1,2,3,4 ^(i,p)	Refer to Function 2 (Core Makeup Tank Actuation) for all initiating functions and requirements. In addition to the requirements for Function 2, SR 3.3.2.9 also applies.				
b. Pressurizer Water Level, High 3	1,2,3,4 ^(i,p)	4	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≤71.05%	71%
28. Chemical and Volume Control System Letdown Isolation						
a. Hot Leg Level – Low 1	4 ^(n,i) ,5 ^(r) ,6 ^(q,r)	1 per loop	C,AA	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥17.98 in. above inside surface of the bottom of the hot legs	18 in. above inside surface of the bottom of the hot legs
29. SG Power Operated Relief Valve and Block Valve Isolation						
a. Manual Initiation	1,2,3,4 ⁽ⁱ⁾	2 switches	E,N	SR 3.3.2.3	NA	NA
b. Steam Line Pressure – Low	1,2,3,4 ⁽ⁱ⁾	4 per steam line	B,N	SR 3.3.2.1 SR 3.3.2.4 SR 3.3.2.5 SR 3.3.2.6	≥559.7 psig	560.3 psig ^(b)

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
3.3.2

~~(b) Time constants used in the lead/lag controller are $\tau_1 \geq 50$ seconds and $\tau_2 \leq 5$ seconds.~~

- (j) With the RCS not being cooled by the Normal Residual Heat Removal System (RNS).
- (n) With the RCS being cooled by the RNS.
- (p) Above the P-19 (RCS Pressure) interlock.
- (q) With the water level < 23 feet above the top of the reactor vessel flange.
- (r) Below the P-12 (Pressurizer Level) interlock.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Attachment 16.3A-2

Markup of Surveillance Requirements Bases for Section 3.1.8

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

PHYSICS TESTS Exceptions – MODE 2
B 3.1.8

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.8.1

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 **REACTOR TRIP CHANNEL OPERATIONAL TEST** is performed on each power range (**Functions 2.a and 2.b**) and intermediate range (**Function 4**) channel 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 3.1.8.2

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 provide assurance that the initial conditions of the safety analyses are not violated.

SR 3.1.8.3

Verification that the THERMAL POWER is $< 5\%$ 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.

SR 3.1.8.4

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;
- d. Fuel burnup based on gross thermal energy generation;
- e. Xenon concentration;
- f. Samarium concentration; and
- g. Isothermal temperature coefficient (ITC).

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Attachment 16.3B

Markup of Bases for Specification 3.3.1

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Trip System (RTS) Instrumentation

BASES

BACKGROUND

The RTS initiates a unit shutdown, based upon 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 Feature Actuation System (ESFAS) in mitigating accidents.

The Protection and Safety Monitoring System (PMS) has 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 include LSSS for variables that have significant safety functions. LSSS are defined by the regulation as "Where a LSSS is specified for a variable on which a safety limit has been placed, the setting must be chosen so that automatic protective actions will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Safety Analysis Limit (SAL) is the limit of the process variable at which a protective action is initiated, as established by the safety analysis, to assure that a SL is not exceeded. However, in practice, the actual settings for automatic protection channels must be chosen to be more conservative than the Safety Analysis Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The LSSS values are identified and maintained in the Setpoint Control Program (SCP) and are controlled by 10 CFR 50.59.

REVIEWER'S NOTE

For Westinghouse AP1000 plants, the term Nominal Trip Setpoint (NTS) is defined as the "Field setting" and is suggested as the actual setpoint implemented in the plant surveillance procedures. The as-found and as-left tolerances will apply to the NTS implemented in the Surveillance procedures to confirm channel performance.

The NTS is included in the SCPSP.

The Nominal Trip Setpoint (NTS) specified in the SCPSP is a predetermined field setting for a protection channel chosen to initiate automatic actuation prior to the process variable reaching the Safety Analysis Limit and thus assures that the SL

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

is not exceeded. As such, the NTS accounts for uncertainties in setting the channel (e.g., calibration), uncertainties in how the channel might actually perform (e.g., repeatability), changes in the point of action of the channel 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 NTS assures that the SLs are not exceeded. Therefore, the NTS meets the 10 CFR 50.36 definition of an LSSS.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety functions(s)." Relying solely on the NTS to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as-found" value of a protection channel setting during a surveillance. This would result in Technical Specification compliance problems, as well as reports and corrective actions required by the rule which are not necessary to ensure safety. For example, an automatic protection channel with a setting that has been found to be different from the NTS due to some drift of the setting may still be OPERABLE since drift is to be expected. This expected drift would have been specifically accounted for in the setpoint methodology for calculating the NTS and thus the automatic protective action would still have assured that the SL would not be exceeded with the "as-found" setting of the protection channel. Therefore, the channel would still be OPERABLE since it would have performed its safety function. If the as-found condition of the channel is near the as-found tolerance, recalibration is considered appropriate to allow for drift during the next surveillance interval.

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 2750 psia shall not be exceeded.

Operation within the SLs of Specification 2.0, "Safety Limits (SLs)," also maintains the above values and assures that offsite doses are within the acceptance criteria during AOOs.

Design Basis Accidents (DBA) are events that are analyzed even though they are not expected to occur during the unit life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

fraction of the limits. Different accident categories are allowed a different fraction of these limits, based on the probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

The RTS maintains surveillance on key process variables which are directly related to equipment mechanical limitations, such as pressure, and on variables which directly affect the heat transfer capability of the reactor, such as flow and temperature. Some limits, such as Overtemperature ΔT , are calculated in the protection and safety monitoring system cabinets from other parameters when direct measurement of the variable is not possible.

The RTS instrumentation is segmented into four distinct but interconnected modules as identified below:

- Field inputs from process sensors, nuclear instrumentation;
- Protection and Safety Monitoring System Cabinets;
- Voting Logic; and
- Reactor Trip Switchgear Interface.

Field Transmitters and Sensors

Normally, four redundant measurements using four separate sensors are made for each variable used for reactor trip. The use of four channels for protection functions is based on a minimum of two channels being required for a trip or actuation, one channel in test or bypass, and a single failure on the remaining channel. The signal selector algorithm in the Plant Control System (PLS) will function with only three channels. This includes two channels properly functioning and one channel having a single failure. For protection channels providing data to the control system, the fourth channel permits one channel to be in test or bypass. Minimum requirements for protection and control ~~is~~ **are** achieved with only three channels OPERABLE. The fourth channel is provided to increase plant availability, and permits the plant to run for an indefinite time with a single channel out of service. The circuit design is able to withstand both 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. Again, a single failure will neither cause nor prevent the protection Function actuation. These requirements are described in IEEE-603 (Ref. 5). The actual number of channels required for each plant parameter is specified in Reference 2.

Selected analog measurements are converted to digital form by digital converters within the protection and safety monitoring system cabinets. Signal conditioning

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

may be applied to selected inputs following the conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for the given parameter is generated if one channel measurement exceeds its predetermined or calculation limit. Processing on all variables for reactor trip is duplicated in each of the four redundant divisions of the protection system. Each division sends its partial trip status to each of the other three divisions over isolated multiplexed links. Each division is capable of generating a reactor trip signal if two or more of the redundant channels of a single variable are in the partial trip state.

The reactor trip signal from each division is sent to the corresponding reactor trip actuation division. Each of the four reactor trip actuation divisions consists of two reactor trip circuit breakers. The reactor is tripped when two or more actuation divisions receive a reactor trip signal. This automatic trip demand initiates the following two actions:

1. It de-energizes the undervoltage trip attachment on each reactor trip breaker, and
2. It energizes the shunt trip device on each reactor trip breaker.

Either action causes the breakers to trip. Opening of the appropriate trip breakers removes power to the control rod drive mechanism (CRDM) coils, allowing the rods to fall into the core. This rapid negative reactivity insertion shuts down the reactor.

Protection and Safety Monitoring System Cabinets

The protection and safety monitoring system cabinets contain the necessary equipment to:

- Permit acquisition and analysis of the sensor inputs, including plant process sensors and nuclear instrumentation, required for reactor trip and ESF calculations;
- Perform computation or logic operations on variables based on these inputs;
- Provide trip signals to the reactor trip switchgear and ESF actuation data to the ESF coincidence logic as required;
- Permit manual trip or bypass of each individual reactor trip Function and permit manual actuation or bypass of each individual voted ESF Function;

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

- Provide data to other systems in the Instrumentation and Control (I&C) architecture;
- Provide separate input circuitry for control Functions that require input from sensors that are also required for protection Functions.

Each of the four divisions provides signal conditioning, comparable output signals for indications in the main control room, and comparison of measured input signals with established setpoints. The basis of the setpoints are described in References ~~1, 2, and 3~~ and 4. If the measured value of a unit parameter exceeds the predetermined setpoint, an output is generated which is transmitted to the ESF coincidence logic for logic evaluation.

Within the ~~protection and safety monitoring system~~ PMS, redundancy is generally provided for active equipment such as processors and communication hardware. This redundancy is provided to increase plant availability and facilitate surveillance testing. A division or channel is OPERABLE if it is capable of performing its specified safety function(s) and all the required supporting functions or systems are also capable of performing their related support functions. Thus, a division or channel is OPERABLE as long as one set of redundant components within the division or channel is capable of performing its specified safety function(s).

Voting Logic

The voting logic provides a reliable means of opening the reactor trip switchgear in its own division as demanded by the individual protection functions.

Reactor Trip Switchgear Interface

The final stage of the voting logic provides the signal to energize the undervoltage trip attachment on each RTB within the reactor trip switchgear. Loss of the signal de-energizes the undervoltage trip attachments and results in the opening of those reactor trip switchgear. An additional external relay is de-energized with loss of the signal. The normally closed contacts of the relay energize the shunt trip attachments on each switchgear at the same time that the undervoltage trip attachment is de-energized. This diverse trip actuation is performed external to the PMS cabinets. The switchgear interface including the trip attachments and the external relay are within the scope of the PMS. Separate outputs are provided for each switchgear. Testing of the interface allows trip actuation of the breakers by either the undervoltage trip attachment or the shunt trip attachment.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

Nominal Trip Setpoints (NTS) and Allowable Values

The ~~Trip Setpoints~~ NTS is the nominal values at which the trip output is set. Any trip output is considered to be properly adjusted when the "as-left" value is within the band for CHANNEL CALIBRATION, ~~accuracy~~ (i.e., \pm rack calibration accuracy).

The ~~Trip Setpoints~~ used in the trip output are based on the ~~analytical limit~~ Safety Analysis Limits stated in Reference 43. The ~~selection~~ determination of these Nominal 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, instrument drift, and severe environment errors for those RTS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 6), the ~~Trip Setpoint~~ NTSs and Allowable Values specified in Table 3.3.1-4 in the ~~accompanying LCO SCPSP~~ are conservatively adjusted with respect to the ~~analytical limit~~ Safety Analysis Limits. A detailed description of the methodology used to calculate the ~~Trip Setpoints~~ NTSs, including their explicit uncertainties, is provided in the "Westinghouse Setpoint Methodology for Protection Systems" (Refs. 4 and 9). The as-left tolerance and as-found tolerance band methodology is provided in the SCPSP. ~~The actual nominal Trip Setpoint entered into the trip output is more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a COT. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the Allowable Value, the trip output is considered OPERABLE. The as-found OPERABILITY limit for the purpose of the REACTOR TRIP CHANNEL OPERATIONAL TEST (RTCOT) is defined as the as-left limit, i.e., \pm rack calibration accuracy about the NTS (i.e., \pm rack calibration accuracy).~~

~~Setpoints in accordance with the Allowable Value ensure that SLs are not violated during AOOs (and that the consequences of DBAs will be acceptable, providing the unit is operated from within the LCOs at the onset of the AOO or DBA and the equipment functions as designed). Note that in the accompanying LCO 3.3.1, the Trip Setpoints of Table 3.3.1-4 are the LSSS.~~

The Nominal Trip Setpoints and Allowable Values listed in the SCPSP Table 3.3.1-4 are based on the methodology described in Reference 4, which incorporates all of the known uncertainties applicable for each channel. (Reference 4 is an AP600 document that describes a methodology that is applicable to AP1000. AP1000 has some slight differences in instrument spans as a result of the higher power level.) The magnitudes of these uncertainties are factored into the determination of each NTSTrip Setpoint. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes. Transmitter and signal processing equipment calibration tolerances and drift allowances must be specified in plant calibration procedures; and must be consistent with the values

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

used in the setpoint methodology.

The OPERABILITY of each transmitter or sensor can be evaluated when its "as-found" calibration data are compared against the "as-left" data and are shown to be within the setpoint methodology assumptions. The basis of the setpoints is described in References 1, 2, 3, and 4. Trending of ~~transmitter~~ calibration results is required by the program description in Technical Specifications 5.5.14.d. ~~Generic Letter 91-04, "Changes in Technical Specification Surveillance Intervals to Accommodate a 24-Month Fuel Cycle."~~

Note that the as-left and as-found tolerances listed in the SCPSP define the OPERABILITY limits for a channel during a periodic CHANNEL CALIBRATION or RTCOT that requires trip setpoint verification.

The protection and safety monitoring system testing features are designed to allow for complete functional testing by using a combination of system self-checking features, functional testing features, and other testing features. Successful functional testing consists of verifying that the capability of the system to perform the safety function has not failed or degraded. For hardware functions this would involve verifying that the hardware components and connections have not failed or degraded. Since software does not degrade, software functional testing involves verifying that the software code has not changed and that the software code is executing. To the extent possible, protection and safety monitoring system functional testing will be accomplished with continuous system self-checking features and the continuous functional testing features.

The protection and safety monitoring system incorporates continuous system self-checking features wherever practical. Self-checking features include on-line diagnostics for the computer system and the hardware and communications tests. These self-checking tests do not interfere with normal system operation.

In addition to the self-checking features, the system includes functional testing features. Functional testing features include continuous functional testing features and manually initiated functional testing features. To the extent practical, functional testing features are designed not to interfere with normal system operation.

In addition to the system self-checking features and functional testing features, other test features are included for those parts of the system which are not tested with self-checking features or functional testing features. These test features allow for instruments/sensor checks, calibration verification, response time testing, setpoint verification and component testing. The test features again include a combination of continuous testing features and manual testing features.

All of the testing features are designed so that the duration of the testing is as short as possible. Testing features are designed so that the actual logic is not

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

modified. To prevent unwanted actuation, the testing features are designed with either the capability to bypass a Function during testing and/or limit the number of signals allowed to be placed in test at one time.

Reactor Trip (RT) Channel

An RT Channel extends from the sensor to the output of the associated reactor trip subsystem in the protection and safety monitoring system cabinets, and includes the sensor (or sensors), the signal conditioning, any associated datalinks, and the associated reactor trip subsystem. For RT Channels containing nuclear instrumentation, the RT Channel also includes the nuclear instrument signal conditioning and the associated Nuclear Instrumentation Signal Processing and Control (NISPAC) subsystem.

Automatic Trip Logic

The Automatic Trip Logic extends from, but does not include, the outputs of the various RT Channels to, but does not include, the reactor trip breakers. Operator bypass of a reactor trip function is performed within the Automatic Trip Logic.

APPLICABLE SAFETY ANALYSES, LCOs, and APPLICABILITY

The RTS functions to maintain the SLs during all AOOs and mitigates the consequences of DBAs in all MODES in which the RTBs are closed.

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

Permissive and interlock functions are based upon the associated protection function instrumentation. Because they do not have to operate in adverse environmental conditions, the trip settings of the permissive and interlock functions use the normal environment, steady-state instrument uncertainties of the associated protection function instrumentation. This results in OPERABILITY criteria (i.e. as-found tolerance and as-left tolerance) that are the same as the associated protection function sensor and process rack modules. The Nominal Trip Setpoints for permissives and interlocks are based on the associated protection function OPERABILITY requirements, i.e., permissives and interlocks performing enabling functions must be set to occur prior to the specified trip setting of the associated protection function.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

The LCO requires all instrumentation performing an RTS Function, listed in Table 3.3.1-1 in the accompanying LCO, to be OPERABLE. The as-left and as-found tolerances specified in the SCPSP define the OPERABILITY limits for a channel during a CHANNEL CALIBRATION or RTCOT. As such, the as-left and as-found tolerances differ from the NTS by \pm the PMS rack calibration accuracy and envelope the expected calibration accuracy and drift for the digital process racks. In this manner, the actual setting of the channel (NTS) prevents exceeding an SL at any given point of time as long as the channel has not drifted beyond the expected tolerances during the surveillance interval. Note that the as-left and as-found recorded values must be confirmed to be operating within the assumptions of the statistical uncertainty calculations.

If the actual setting of the channel is found outside the as-found tolerance, the channel is considered inoperable. This condition of the channel will be further evaluated during performance of the SR. This evaluation will consist of resetting the channel setpoint to the NTS (within the allowed tolerance), and evaluating the channel's response. If the channel is functioning as required and is expected to pass the next surveillance, then the channel is OPERABLE and can be restored to service at the completion of the surveillance. After the surveillance is completed, the channel as-found condition will be entered into the Corrective Action Program for further evaluation.

A trip setpoint may be set more conservative than the NTS as necessary in response to plant conditions. However, in this case, the operability of this instrument must be verified based on the actual field setting and not the NTS. 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 channels in each instrumentation Function.

Reactor Trip System Functions

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

1. Manual Reactor Trip

The Manual Reactor Trip ensures that the main control room operator can initiate a reactor trip at any time by using either of two reactor trip actuation devices in the main control room. A Manual Reactor Trip accomplishes the same results as any one of the automatic trip Functions. It can be used by the reactor operator to shutdown the reactor whenever any parameter is rapidly trending toward its Trip Setpoint. The safety analyses do not take credit for the Manual Reactor Trip.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

The LCO requires two Manual Reactor Trip actuation devices be OPERABLE in MODES 1 and 2 and in MODES 3, 4, and 5 with RTBs closed and PLS capable of rod withdrawal. Two independent actuation devices are required to be OPERABLE so that no single random failure will disable the Manual Reactor Trip Function.

In MODE 1 or 2, manual initiation of a 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 Function must also be OPERABLE if the shutdown or control rods are withdrawn or the PLS is capable of withdrawing the shutdown or control rods. In MODES 3, 4, and 5, manual initiation of a reactor trip does not have to be OPERABLE if the PLS is not capable of withdrawing the shutdown or control rods. If the rods cannot be withdrawn from the core, there is no need to be able to trip the reactor because all of the rods are inserted. 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 Function does not have to be OPERABLE.

2. Power Range Neutron Flux

The PMS power range detectors are located external to the reactor vessel and measure neutrons leaking from the core. The PMS power range detectors provide input to the PLS. Minimum requirements for protection and control is achieved with three channels OPERABLE. The fourth channel is provided to increase plant availability, and permits the plant to run for an indefinite time with a single channel in trip or bypass. This Function also satisfies the requirements of IEEE 603 (Ref. 5) with 2/4 logic. This Function also provides a signal to prevent automatic and manual rod withdrawal prior to initiating a reactor trip. Limiting further rod withdrawal may terminate the transient and eliminate the need to trip the reactor.

a. Power Range Neutron Flux – High

The Power Range Neutron Flux –High trip Function ensures that protection is provided, from all power levels, against a positive reactivity excursion during power operations. Positive reactivity excursions can be caused by rod withdrawal or reductions in RCS temperature.

The LCO requires four Power Range Neutron Flux – High channels to be OPERABLE in MODES 1 and 2.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

In MODE 1 or 2, when a positive reactivity excursion could occur, the Power Range Neutron Flux – High trip must be OPERABLE. This Function will terminate the reactivity excursion and shutdown the reactor prior to reaching a power level that could damage the fuel. In MODE 3, 4, 5, or 6, the Power Range Neutron Flux – High trip does not have to be OPERABLE because the reactor is shutdown and a reactivity excursion in the power range cannot occur. Other RTS Functions and administrative controls provide protection against reactivity additions when in MODE 3, 4, 5, or 6. In addition, the PMS power range detectors cannot detect neutron levels in this range.

b. Power Range Neutron Flux – Low

The LCO requirement for the Power Range Neutron Flux – Low trip Function ensures that protection is provided against a positive reactivity excursion from low power or subcritical conditions. The Trip Setpoint reflects only steady state instrument uncertainties as this

Function does not provide primary protection for any event that results in a harsh environment.

The LCO requires four of the Power Range Neutron Flux – Low channels to be OPERABLE in MODE 1 below the Power Range Neutron Flux P-10 Setpoint and MODE 2.

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

In MODE 3, 4, 5, or 6, the Power Range Neutron Flux – Low trip Function does not have to be OPERABLE because the reactor is shutdown and the PMS power range detectors cannot detect neutron levels generated in MODES 3, 4, 5, and 6. Other RTS trip Functions and administrative controls provide protection against positive reactivity additions or power excursions in MODE 3, 4, 5, or 6.

3. Power Range Neutron Flux – High Positive Rate

The Power Range Neutron Flux – High Positive Rate trip Function ensures

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

that protection is provided against rapid increases in neutron flux which are characteristic of a rod cluster control assembly (RCCA) drive rod housing rupture and the accompanying ejection of the RCCA. This Function compliments the Power Range Neutron Flux – High and Low trip Functions to ensure that the criteria are met for a rod ejection from the power range. The Power Range Neutron Flux Rate trip uses the same channels as discussed for Function 2 above.

The LCO requires four Power Range Neutron Flux – High 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 Power Range Neutron Flux – High Positive Rate trip must be OPERABLE. In MODE 3, 4, 5, or 6, the Power Range Neutron Flux – High 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 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 PMS power range detectors cannot detect neutron levels present in this MODE.

4. Intermediate Range Neutron Flux

The Intermediate Range Neutron Flux trip Function ensures that protection is provided against an uncontrolled RCCA bank withdrawal accident from a subcritical condition during startup. This trip Function provides redundant protection to the Power Range Neutron Flux – Low Setpoint trip Function. The PMS intermediate range detectors are located external to the reactor vessel and measure neutrons leaking from the core. The safety analyses do not take credit for the Intermediate Range Neutron Flux trip Function. Even though the safety analyses take no credit for the Intermediate Range Neutron Flux trip, the functional capability at the specified Trip Setpoint enhances the overall diversity of the RTS. The Trip Setpoint reflects only steady state instrument uncertainties as the detectors do not provide primary protection for any events that result in a harsh environment. This trip can be manually blocked by the main control room operator when above the P-10 setpoint, which is the respective PMS power range channel greater than 10% power, and is automatically unblocked when below the P-10 setpoint, which is the respective PMS power range channel less than 10% power. This Function also provides a signal to prevent automatic and manual rod withdrawal prior to initiating a reactor trip. Limiting further rod withdrawal may terminate the transient and eliminate the need to trip the reactor.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

The LCO requires four channels of Intermediate Range Neutron Flux to be OPERABLE. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

In MODE 1 below the P-10 setpoint, and in MODE 2, when there is a potential for an uncontrolled rod withdrawal accident during reactor startup, the Intermediate Range Neutron Flux trip must be OPERABLE. Above the P-10 setpoint, the Power Range Neutron Flux – High Setpoint trip and the Power Range Neutron Flux – High Positive Rate trip provide core protection for a rod withdrawal accident. In MODE 3, 4, or 5, the 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 PMS intermediate range detectors cannot detect neutron levels present in this MODE.

5. Source Range Neutron Flux

The LCO requirement for the Source Range Neutron Flux trip Function ensures that protection is provided against an uncontrolled bank rod withdrawal accident from a subcritical condition during startup. This trip Function provides redundant protection to the Power Range Neutron Flux – Low Setpoint and Intermediate Range Neutron Flux trip Functions. In MODES 3, 4, and 5, administrative controls also prevent the uncontrolled withdrawal of rods. The PMS source range detectors are located external to the reactor vessel and measure neutrons leaking from the core. The safety analyses do not take credit for the Source Range Neutron Flux trip Function. Even though the safety analyses take no credit for the Source Range Neutron Flux trip, the functional capability at the specified Trip Setpoint is assumed to be available and the trip is implicitly assumed in the safety analyses.

The Trip Setpoint reflects only steady state instrument uncertainties as the detectors do not provide primary protection for any events that result in a harsh environment. This trip can be manually blocked by the main control room operator when above the P-6 setpoint (Intermediate Range Neutron Flux interlock) and is automatically unblocked when below the P-6 setpoint. The manual block of the trip function also de-energizes the source range detectors. The source range detectors are automatically re-energized when below the P-6 setpoint. The trip is automatically blocked when above the P-10 setpoint (Power Range Neutron Flux interlock). The source range

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

trip is the only RTS automatic protective Function required in MODES 3, 4, and 5. Therefore, the functional capability at the specified Trip Setpoint is assumed to be available.

The LCO requires four channels of Source Range Neutron Flux to be OPERABLE in MODE 2 below P-6 and in MODE 3, 4, or 5 with RTBs closed and Control Rod Drive System capable of rod withdrawal. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. In MODE 3, 4, or 5 with the RTBs open, the LCO does not require the Source Range Neutron Flux channels for reactor trip Functions to be OPERABLE.

In MODE 2 when below the P-6 setpoint during a reactor startup, the Source Range Neutron Flux trip must be OPERABLE. Above the P-6 setpoint, the Intermediate Range Neutron Flux trip and the Power Range Neutron Flux – Low Setpoint trip will provide core protection for reactivity

accidents. Above the P-6 setpoint, the PMS source range detectors are de-energized and inoperable as described above.

In MODE 3, 4, or 5 with the reactor shutdown, the Source Range Neutron Flux trip Function must also be OPERABLE. If the PLS is capable of rod withdrawal, the Source Range Neutron Flux trip must be OPERABLE to provide core protection against a rod withdrawal accident. If the PLS is not capable of rod withdrawal, the source range detectors are required to be OPERABLE to provide monitoring of neutron levels and provide protection for events like an inadvertent boron dilution. These Functions are addressed in LCO 3.3.2, "Engineered Safety Feature Actuation System (ESFAS) Instrumentation." The requirements for the PMS source range detectors in MODE 6 are addressed in LCO 3.9.3, "Nuclear Instrumentation."

6. Overtemperature ΔT

The Overtemperature ΔT trip Function ensures that protection is provided to ensure that the design limit DNBR is met. 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 combinations of pressure, power, coolant temperature, and axial power distribution, assuming full reactor coolant flow. Protection from violating the DNBR limit is assured for those transients that are slow with respect to delays from the core to the measurement system. The Overtemperature ΔT trip Function uses the measured THOT and TCOLD in each loop, together with the measured pressurizer pressure, to compute the reactor core thermal power. Equations to fit the properties of density and enthalpy

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

are programmed in the software, such that the ΔT power signal is presented as a percent of RTP for direct comparison with measured calorimetric power. The overtemperature ΔT setpoint is automatically varied for changes in the parameters that affect DNB as follows:

- reactor core inlet temperature – the Trip Setpoint is varied to correct for changes in core inlet temperature based on measured changes in cold leg temperature with dynamic compensation to account for cold leg-to-core transit time;
- pressurizer pressure – the Trip Setpoint is varied to correct for changes in system pressure; and
- axial power distribution – the Trip Setpoint is varied to account for imbalances in the axial power distribution as detected by the PMS 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 PMS power range detectors, the Trip Setpoint is reduced in accordance with algorithms documented in the SCPSP Note 1 of Table 3.3.1-1.

Dynamic compensation of the ΔT power signal 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 1 of Table 3.3.1-1 the SCPSP. This Function also provides a signal to generate a turbine runback prior to reaching the 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. No credit is taken in the safety analyses for the turbine runback.

The LCO requires four channels of the Overtemperature ΔT trip Function to be OPERABLE in MODES 1 and 2. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. 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.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

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 Power Range Neutron Flux – 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 same ΔT power signal generated for the Overtemperature ΔT . The setpoint is automatically varied with the following parameter:

- Axial power distribution – the Trip Setpoint is varied to account for imbalances in the axial power distribution as detected by the PMS 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 PMS power range detectors, the Trip Setpoint is reduced in accordance with [algorithms documented in the SCPSP Note 2 of Table 3.3.1-1](#).

The Overpower ΔT trip Function is calculated for each loop as [per described in the SCPSP Note 2 of Table 3.3.1-1](#). The Trip Setpoint reflects the inclusion of both steady state and adverse environmental instrument uncertainties as the detectors provide protection for a steam line break and may be in a harsh environment. Note that this Function also provides a signal to generate a turbine runback prior to reaching the Trip Setpoint. A turbine runback reduces turbine power and reactor power. A reduction in power normally alleviates the Overpower ΔT condition and may prevent a reactor trip.

The LCO requires four channels of the Overpower ΔT trip Function to be OPERABLE in MODES 1 and 2. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. The Overpower 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 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.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

8. Pressurizer Pressure

The same sensors provide input to the Pressurizer Pressure – High and – Low trips and the Overtemperature ΔT trip.

a. Pressurizer Pressure – Low

The Pressurizer Pressure – Low trip Function ensures that protection is provided against violating the DNBR limit due to low pressure. The Trip Setpoint reflects both steady state and adverse environmental instrument uncertainties as the detectors provide primary protection for an event that results in a harsh environment.

The LCO requires four channels of Pressurizer Pressure – Low to be OPERABLE in MODE 1 above P-10. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

In MODE 1, when DNB is a major concern, the Pressurizer Pressure – Low trip must be OPERABLE. This trip Function is automatically enabled on increasing power by the P-10 interlock. On decreasing power, this trip Function is automatically blocked below P-10. Below the P-10 setpoint, no conceivable power distributions can occur that would cause DNB concerns.

b. Pressurizer Pressure – High

The Pressurizer Pressure – High trip Function ensures that protection is provided against overpressurizing the RCS. This trip Function operates in conjunction with the safety valves to prevent RCS overpressure conditions. The 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 four channels of the Pressurizer Pressure – High to be OPERABLE in MODES 1 and 2. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

In MODE 1 or 2, the Pressurizer Pressure – High trip must be OPERABLE to help prevent RCS overpressurization and LCOs, and minimizes challenges to the safety valves. In MODE 3, 4, 5, or 6, the Pressurizer Pressure – High trip Function does not have to be OPERABLE because transients which could cause an overpressure condition will be slow to occur. Therefore, the operator will have sufficient time to evaluate plant conditions and take corrective

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

actions. Additionally, low temperature overpressure protection systems provide overpressure protection when below MODE 4.

9. Pressurizer Water Level – High 3

The Pressurizer Water Level – High 3 trip Function provides a backup signal for the Pressurizer Pressure – High 3 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 is actuated prior to the pressurizer becoming water solid. The 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 level channels do not actuate the safety valves.

The LCO requires four channels of Pressurizer Water Level – High 3 to be OPERABLE in MODE 1 above P-10. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

In MODE 1 when there is a potential for overfilling the pressurizer, the Pressurizer Water Level – High 3 trip must be OPERABLE. This trip

Function is automatically enabled on increasing power by the P-10 interlock. On decreasing power, this trip Function is automatically blocked below P-10. Below the P-10 setpoint, transients which could raise the pressurizer water level will be slow and the operator will have sufficient time to evaluate plant conditions and take corrective actions.

10. Reactor Coolant Flow – Low

Reactor Coolant Flow

The Reactor Coolant Flow – Low trip Function ensures that protection is provided against violating the DNBR limit due to low flow in one or more RCS hot legs. Above the P-10 setpoint, a loss of flow in any RCS hot leg will actuate a Reactor trip.

Each RCS hot leg has four flow detectors to monitor flow. The 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 four Reactor Coolant Flow – Low channels per hot leg to be OPERABLE in MODE 1 above P-10. Four OPERABLE channels are provided to permit one channel in trip or bypass indefinitely and still ensure

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

no single random failure will disable this trip Function.

In MODE 1 above the P-10 setpoint, when a loss of flow in one RCS hot leg could result in DNB conditions in the core, the Reactor Coolant Flow – Low trip must be OPERABLE.

11. Reactor Coolant Pump (RCP) Bearing Water Temperature – High

RCP Bearing Water Temperature – High

The RCP Bearing Water Temperature – High reactor trip Function ensures that protection is provided against violating the DNBR limit due to a loss of flow in one RCS cold leg. The 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 four RCP Bearing Water Temperature – High channels per RCP to be OPERABLE in MODE 1 or 2. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

In MODE 1 or 2, when a loss of flow in any RCS cold leg could result in DNB conditions in the core, the RCP Bearing Water Temperature – High trip must be OPERABLE.

12. Reactor Coolant Pump Speed – Low

The RCP Speed – Low trip Function ensures that protection is provided against violating the DNBR limit due to a loss of flow in two or more RCS cold legs. The speed of each RCP is monitored. Above the P-10 setpoint a low speed detected on two or more RCPs will initiate a reactor trip. The 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 four RCP Speed – Low channels to be OPERABLE in MODE 1 above P-10. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

In MODE 1 above the P-10 setpoint, the RCP Speed – Low trip must be OPERABLE. Below the P-10 setpoint, all 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-10

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

setpoint, the reactor trip on loss of flow in two or more RCS cold legs is automatically enabled.

13. Steam Generator Water Level – Low

The SG Water Level – Low trip Function ensures that protection is provided against a loss of heat sink. 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 steam generator is indicative of a loss of heat sink for the reactor. The Trip Setpoint reflects the inclusion of both steady state and adverse environmental instrument uncertainties as the detectors provide primary protection for an event that results in a harsh environment. This Function also contributes to the coincidence logic for the ESFAS Function of opening the Passive Residual Heat Removal (PRHR) discharge valves.

The LCO requires four channels of SG Water Level – Low per SG to be OPERABLE in MODES 1 and 2. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

In MODE 1 or 2, when the reactor requires a heat sink, the SG Water Level – Low trip must be OPERABLE. The normal source of water for the SGs is the Main Feedwater System (non-safety related). The Main Feedwater System is normally in operation in MODES 1 and 2. PRHR is the safety related backup heat sink for the reactor. During normal startups and shutdowns, the Main and Startup Feedwater Systems (non-safety related) can provide feedwater to maintain SG level. In MODE 3, 4, 5, or 6, the SG Water Level – Low Function does not have to be OPERABLE because the reactor is not operating or even critical.

14. Steam Generator Water Level – High 2

The SG Water Level – High 2 trip Function ensures that protection is provided against excessive feedwater flow by closing the main feedwater control valves, tripping the turbine, and tripping the reactor. While the transmitters (d/p cells) are located inside containment, the events which this function protects against cannot cause severe environment in containment. Therefore, the Trip Setpoint reflects only steady state instrument uncertainties.

The LCO requires four channels of SG Water Level – High 2 per SG to be OPERABLE in MODES 1 and 2. Four channels are provided to permit one channel in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

In MODES 1 and 2 above the P-11 interlock, the SG Water Level – High 2 trip must be OPERABLE. The normal source of water for the SGs is the Main Feedwater System (non-safety related). The Main Feedwater System is only in operation in MODES 1 and 2. In MODE 3, 4, 5, or 6, the SG Water Level – High 2 Function does not have to be OPERABLE because the reactor is not operating or even critical. The P-11 interlock is provided on this Function to permit bypass of the trip Function when the pressure is below P-11. This bypass is necessary to permit rod testing when the steam generators are in wet layup.

15. Safeguards Actuation Signal from Engineered Safety Feature Actuation System

The Safeguards Actuation Signal from ESFAS ensures that if a reactor trip has not already been generated by the RTS, the ESFAS automatic actuation logic will initiate a reactor trip upon any signal which initiates the Safeguards Actuation signal. This is a condition of acceptability for the Loss of Coolant Accident (LOCA). However, other transients and accidents take credit for varying levels of ESFAS performance and rely upon rod insertion, except for the most reactive rod which is assumed to be fully withdrawn, to ensure reactor shutdown.

The LCO requires two manual and four automatic divisions of Safeguards Actuation Signal Input from ESFAS to be OPERABLE in MODES 1 and 2. Four automatic divisions are provided to permit one division bypass indefinitely and still ensure no single random failure will disable this trip Function.

A reactor trip is initiated every time a Safeguards Actuation signal is present. Therefore, this trip Function must be OPERABLE in MODES 1 and 2, when the reactor is critical, and must be shutdown in the event of an accident. In MODE 3, 4, 5, or 6, the reactor is not critical.

16. Reactor Trip System Interlocks

Reactor protection interlocks are provided to ensure reactor trips are in the correct configuration for the current plant status. They back up operator actions to ensure protection system Functions are not blocked during plant conditions under which the safety analysis assumes the Functions are OPERABLE. Therefore, the interlock Functions do not need to be OPERABLE when the associated 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

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

when the respective PMS Intermediate Range Neutron Flux channel ~~goes-increases to~~ approximately one decade above the ~~minimum~~ channel ~~readinglower range limit~~. The LCO requirement for the P-6 interlock ensures that the following Functions are performed:

- (1) on increasing power, the P-6 interlock allows the manual block of the respective PMS Source Range, Neutron Flux 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.
- (2) on decreasing power, the P-6 interlock automatically energizes the PMS source range detectors and enables the PMS Source Range Neutron Flux reactor trip.
- (3) on increasing power, the P-6 interlock provides a backup block signal to the source range neutron flux doubling circuit. Normally, this Function is manually blocked by the main control room operator during the reactor startup.

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

In MODE 2, when below the P-6 interlock setpoint, the P-6 interlock must be OPERABLE. Above the P-6 interlock setpoint, the PMS Source Range Neutron Flux reactor trip will be blocked; and this Function will no longer be necessary. In MODES 3, 4, 5, and 6, the P-6 interlock does not have to be OPERABLE because the PMS Source Range is providing core protection.

b. Power Range Neutron Flux, P-10

The Power Range Neutron Flux, P-10 interlock is actuated at approximately 10% power as determined by the respective PMS power-range detector. The LCO requirement for the P-10 interlock ensures that the following functions are performed:

- (1) on increasing power, the P-10 interlock automatically enables reactor trips on the following Functions:
 - Pressurizer Pressure – Low,

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

- Pressurizer Water Level – High 3,
- Reactor Coolant Flow – Low, and
- RCP Speed – Low.

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

- (2) on increasing power, the P-10 interlock allows the operator to manually block the Intermediate Range Neutron Flux reactor trip.
- (3) on increasing power, the P-10 interlock allows the operator to manually block the Power Range Neutron Flux – Low Setpoint reactor trip.
- (4) on increasing power, the P-10 interlock automatically provides a backup block signal to the Source Range Neutron Flux reactor trip and also to de-energize the PMS source range detectors.
- (5) on decreasing power, the P-10 interlock automatically blocks reactor trips on the following Functions:
 - Pressurizer Pressure – Low,
 - Pressurizer Water Level – High 3,
 - Reactor Coolant Flow – Low, and
 - RCP Speed – Low.
- (6) on decreasing power, the P-10 interlock automatically enables the Power Range Neutron Flux – Low reactor trip and the Intermediate Range Neutron Flux 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.

In MODE 1, when the reactor is at power, the Power Range Neutron Flux, P-10 interlock must be OPERABLE. This Function must be

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

OPERABLE in MODE 2 to ensure that core protection is provided during a startup or shutdown by the Power Range Neutron Flux – Low Setpoint and Intermediate Range Neutron Flux 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 provides core protection.

c. Pressurizer Pressure, P-11

With pressurizer pressure channels less than the P-11 setpoint, the operator can manually block the Steam Generator Narrow Range Water Level – High 2 reactor Trip. This allows rod testing with the steam generators in cold wet layup. With pressurizer pressure channels > P-11 setpoint, the Steam Generator Narrow Range Water Level – High 2 reactor Trip is automatically enabled. The operator can also enable these actuations by use of the respective manual reset.

17. Reactor Trip Breakers

This trip Function applies to the RTBs exclusive of individual trip mechanisms. There are eight reactor trip breakers with two breakers in each division. The reactor trip circuit breakers are arranged in a two-out-of-four logic configuration, such that the tripping of the two circuit breakers associated with one division does not cause a reactor trip. This circuit breaker arrangement is illustrated in DCD Figure 7.1-7. The LCO requires four divisions of the Reactor Trip Switchgear to be OPERABLE with two trip breakers associated with each required division. This logic is required to meet the safety function assuming a single failure.

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 RTBs are closed, and the PLS is capable of rod withdrawal.

18. 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 PLS, or declared inoperable under Function 17 above. OPERABILITY of both trip mechanisms on each breaker ensures that no single trip mechanism failure will prevent opening the breakers on a valid signal.

These trip Functions must be OPERABLE in MODES 1 and 2 when the reactor is critical. In MODES 3, 4, and 5,

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

these RTS trip Functions must be OPERABLE when the RTBs are closed, and the PLS is capable of rod withdrawal.

19. Automatic Trip Logic

The LCO requirement for the RTBs (Functions 17 and 18) and Automatic Trip Logic (Function 19) ensures that means are provided to interrupt the power to the CRDMs and 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 automatic trip logic includes the ESF coincidence logic and the voting logic.

The LCO requires four divisions of RTS Automatic Trip Logic to be OPERABLE. Four OPERABLE divisions are provided to ensure that a random failure of a single logic channel will not prevent 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 RTBs are closed and the PLS is capable of rod withdrawal.

20. ADS Stages 1, 2 and 3 Actuation Input from Engineered Safety Feature Actuation System

The LCO requirement for this Function provides a reactor trip for any event that may initiate depressurization of the reactor.

The LCO requires four divisions of RTS Automatic Trip Logic to be OPERABLE. Four OPERABLE divisions are provided to ensure that a random failure of a single logic channel will not prevent 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 RTBs are closed and the PLS is capable of rod withdrawal.

21. Core Makeup Tank (CMT) Actuation Input from Engineered Safety Feature Actuation System

The LCO requirement for this Function provides a reactor trip for any event that may initiate CMT injection.

The LCO requires four divisions of RTS Automatic Trip Logic to be OPERABLE. Four OPERABLE divisions are provided to ensure that

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

random failure of a single logic channel will not prevent reactor trip.

These trip Functions must be OPERABLE in MODES 1 and 2 when the reactor is critical. In MODE 3, 4, and 5 these RTS trip Functions must be OPERABLE when the RTBs are closed and the PLS is capable of rod withdrawal.

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

~~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 3.3.1-1.~~

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 3.3.1-1.~~

In the event a channel's as-found condition is outside the as-found tolerance described in the SCPSP, or the channel is not functioning as required, or the transmitter, instrument loop, signal processing electronics, or trip output 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 exceed those specified in one or other related Conditions associated with a trip Function, then

the plant is outside the safety analysis. Therefore, LCO 3.0.3 must be immediately entered if applicable in the current MODE of operation.

A.1

Condition A applies to all RTS protection Functions. Condition A addresses the situation where one or more required channels 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, B.2.1, and B.2.2

Condition B applies to the Manual Reactor Trip, Manual Safeguards Actuation, Manual ADS Stages 1, 2, and 3 Actuation and Manual Core Makeup Tank Actuation in MODES 1 and 2 and in MODES 3, 4, and 5 with the reactor trip

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

breakers closed and the plant control system capable of rod withdrawal. These Required Actions address inoperability of one manual initiation device of the Manual Reactor Trip Function, Manual Safeguards Actuation Function, Manual ADS Stages 1, 2, and 3 Actuation Function and/or Manual Core Makeup Tank Actuation Function. One device consists of an actuation switch and the associated hardware (such as contacts and wiring) up to but not including the eight Reactor Trip Breakers. With one device inoperable, the inoperable device must be restored to OPERABLE status within 48 hours. In this Condition, the remaining OPERABLE device is adequate to perform the safety function.

If the manual Function(s) cannot be restored to OPERABLE status in the allowed 48 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 (54 hours total time) followed by opening the RTBs within 1 additional hour (55 hours total time). The 6 additional hours to reach MODE 3 and the 1 hour to open the RTBs are reasonable, based on operating experience, to reach MODE 3 and open the RTBs from full power operation in an orderly manner and without challenging unit systems. With the RTBs open and the unit in MODE 3, this trip Function is no longer required to be OPERABLE.

C.1 and C.2

Condition C applies to the Manual Reactor Trip in MODES 3, 4, and 5 with the RTBs closed and the PLS capable of rod withdrawal. These Required Actions address inoperability of one manual initiation device of the Manual Reactor Trip Function. One device consists of an actuation switch and the associated hardware (such as contacts and wiring) up to but not including the eight Reactor Trip Breakers. With one device inoperable, the inoperable device must be

restored to OPERABLE status within 48 hours. In this Condition, the remaining OPERABLE device is adequate to perform the safety function.

If the Manual Reactor Trip Function cannot be restored to OPERABLE status in 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, the RTBs must be opened within the next 1 hour. With the RTBs open, this Function is no longer required.

D.1.1, D.1.2, D.1.3, D.2.1, D.2.2, and D.3

Condition D applies to the Power Range Neutron Flux – High Function in MODES 1 and 2.

With one or two channels inoperable, one affected channel must be placed in a bypass or trip condition within 6 hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is bypassed and one channel is tripped, the logic becomes one-out-of-two, while still meeting the single failure criterion. The 6 hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference 7.

In addition to placing the inoperable channel(s) in the bypassed or tripped condition, THERMAL POWER must be reduced to $\leq 75\%$ RTP within 12 hours. Reducing the power level prevents operation of the core with radial power distributions beyond the design limits. With one or two of the PMS power range detectors inoperable, partial radial power distribution monitoring capability is lost. However, the protective function would still function even with a single failure of one of the two remaining channels.

As an alternative to reducing power, the inoperable channel(s) can be placed in the bypassed or tripped condition within 6 hours and the QPTR monitored every 12 hours as per SR 3.2.4.2, QPTR verification. Calculating QPTR compensates for the lost monitoring capability and allows continued plant operation at power levels $> 75\%$ RTP. The 12 hour Frequency is consistent with LCO 3.2.4, "QUADRANT POWER TILT RATIO (QPTR)."

Required Action D.2.2 has been modified by a Note which only requires SR 3.2.4.2 to be performed if OPDMS and the Power Range Neutron Flux input to QPTR become inoperable. Power distribution limits are normally verified in accordance with LCO 3.2.5, "OPDMS – Monitored Power Distribution Parameters." However, if OPDMS becomes inoperable, then LCO 3.2.4, "QUADRANT POWER TILT RATIO (QPTR)," becomes applicable. 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. If either OPDMS or the channel input to QPTR is OPERABLE, then performance of SR 3.2.4.2 once per 12 hours is not necessary.

As an alternative to the above Actions, the plant must be placed in a MODE where this Function is no longer required OPERABLE. Twelve hours are allowed to place the plant in MODE 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.

E.1.1, E.1.2, and E.2

Condition E applies to the following reactor trip Functions:

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

- Power Range Neutron Flux – Low;
- Overtemperature ΔT ;
- Overpower ΔT ;
- Power Range Neutron Flux – High Positive Rate;
- Pressurizer Pressure – High;
- RCP Bearing Water Temperature – High;
- SG Water Level – Low; and
- SG Water Level – High 2.

With one or two channels inoperable, one affected channel must be placed in a bypass or trip condition within 6 hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is bypassed and one channel is tripped, the logic becomes one-out-of-two, while still meeting the single failure criterion. The 6 hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference 7.

If the Required Actions described above cannot be met within the specified Completion Times, the unit must be placed in a MODE where this Function is no longer required to be OPERABLE. An additional 6 hours is allowed to place the unit in MODE 3. Six hours is a reasonable time, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.

F.1.1, F.1.2, F.2, and F.3

Condition F applies to the Intermediate Range Neutron Flux trip when above the P-6 setpoint and below the P-10 setpoint. Above the P-6 setpoint and below the P-10 setpoint, the PMS intermediate range detector performs the monitoring functions.

With one or two channels inoperable, one affected channel must be placed in a bypass or trip condition within 2 hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is tripped, the logic becomes one-out-of-three, while still meeting the

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is bypassed and one channel is tripped, the logic becomes one-out-of-two, while still meeting the single failure criterion. The 2 hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference 7.

As an alternative to placing the channel(s) in bypass or trip if THERMAL POWER is greater than the P-6 setpoint but less than the P-10 setpoint, 2 hours are allowed to reduce THERMAL POWER below the P-6 setpoint or to increase the THERMAL POWER above the P-10 setpoint. The PMS 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 PMS power range detectors perform the monitoring and protective functions and the intermediate range is not required. The Completion Times allow for a slow and controlled power adjustment below P-6, and takes into account the redundant capability afforded by the two remaining OPERABLE channels and the low probability of their failure during this period.

G.1 and G.2

Condition G applies to three Intermediate Range Neutron Flux trip channels inoperable in MODE 2 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. Above the P-6 setpoint and below the P-10 setpoint, the PMS intermediate range detector performs the monitoring Functions. With only one intermediate range channel OPERABLE, the Required Actions are to suspend operations involving positive reactivity additions immediately. This will preclude any power level increase since there are

insufficient OPERABLE Intermediate Range Neutron Flux channels to adequately monitor the power ~~rise~~escalation. The operator must also reduce THERMAL POWER below the P-6 setpoint within 2 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 PMS Intermediate Range Neutron Flux trip.

H.1

Condition H applies to the Intermediate Range Neutron Flux trip when THERMAL POWER is below the P-6 setpoint and one or two channels ~~is-are~~ inoperable. Below the P-6 setpoint, the PMS source range performs the monitoring and protective functions. At least three of the four PMS intermediate range channels must be returned to OPERABLE status prior to increasing power above the P-6

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

setpoint. With the unit in this Condition, below P-6, the PMS source range performs the monitoring and protection functions.

I.1

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

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

J.1

Condition J applies to three inoperable Source Range Neutron Flux channels when in MODE 2, below the P-6 setpoint, and performing a reactor startup, or in MODE 3, 4, or 5 with the RTBs closed and the CRD System capable of rod withdrawal. With the unit in this Condition, below P-6, the NIS source range performs the monitoring and protection functions. With three source range channels inoperable, the RTBs must be opened immediately. With the RTBs open, the core is in a more stable condition and the unit enters Condition T.

K.1.1, K.1.2, and K.2

Condition K applies to the following reactor trip Functions:

- Pressurizer Pressure – Low;
- Pressurizer Water Level – High 3;
- Reactor Coolant Flow – Low; and
- RCP Speed – Low.

With one or two channels inoperable, one affected channel must be placed in a bypass or trip condition within 6 hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is bypassed and one channel is tripped, the logic becomes one-out-of-two, while still meeting the single failure criterion. The 6 hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference 7.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

If Required Actions described above cannot be met within the specified Completion Times, the unit must be placed in a MODE where this Function is no longer required to be OPERABLE. A Completion Time of an additional 6 hours is allowed to reduce power < P-10. Allowance of this time interval takes into consideration the redundant capability provided by the remaining two 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 K.

L.1 and L.2

Condition L applies to the Safeguards Actuation signal from ESFAS reactor trip, the RTS Automatic Trip Logic, automatic ADS Stages 1, 2, and 3 actuation, and automatic CMT injection in MODES 1 and 2.

With one or two channels or divisions inoperable, the Required Action is to restore three of the four channels/divisions within 6 hours. Restoring all channels/divisions but one to OPERABLE status ensures that a single failure will neither cause nor prevent the protective function. The 6 hour Completion Time is considered reasonable since the protective function will still function.

If Required Actions described above cannot be met within the specified Completion Times, the unit must be placed in a MODE where this Function is no longer required to be OPERABLE. A Completion Time of an additional 6 hours is allowed to place the unit in MODE 3. The Completion Time is a reasonable time, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems. Allowance of this time interval takes into consideration the redundant capability provided by the remaining two

redundant OPERABLE channels/divisions and the low probability of occurrence of an event during this period that may require the protection afforded by this Function.

M.1, M.2.1, M.2.2, and M.3

Condition M applies to the P-6, P-10, and P-11 interlocks. With one or two channels inoperable, the associated interlock must be verified to be in its required state for the existing plant condition within 1 hour, or the Functions associated with inoperable interlocks placed in a bypassed or tripped condition within 7 hours, or the unit must be placed in MODE 3 within 13 hours. Verifying the interlock manually accomplishes the interlock condition.

If one interlock channel is inoperable, the associated Function(s) must be placed in a bypass or trip condition within 7 hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

one channel is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.)

If two interlock channels are inoperable, one channel of the associated Function(s) must be bypassed and one channel of the associated Function(s) must be tripped. In this state, the logic becomes one-out-of-two, while still meeting the single failure criterion. The 7 hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference 7.

If placing the associated Functions in bypass or trip is impractical, for instance as the result of other channels in bypass or trip, the Completion Time of an additional 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.

N.1, N.2.1, and N.2.2

Condition N applies to the RTBs, and RTB undervoltage and shunt trip mechanisms in MODES 1 and 2, and in MODES 3, 4, and 5 with the RTBs closed and the PLS capable of rod withdrawal. This Condition is primarily associated with mechanical damage that can prevent the RTBs from opening.

With one division inoperable, the reactor trip breakers in the inoperable division must be opened within 8 hours. A division is inoperable, if, within that division, one or both of the RTBs and/or one or both of the trip mechanisms is inoperable.

With one division inoperable (with its RTBs open) and with three OPERABLE divisions remaining, the trip logic becomes one-out-of-three. The one-out-of-three trip logic meets the single failure criterion. (A failure in one of the three remaining divisions will not prevent the protective function.) If, coincident with RTBs inoperable in one division, the automatic trip logic is inoperable in another division, the trip logic becomes one-out-of-two, which meets the single failure criterion. If Required Actions described above cannot be met within the specified Completion Times, the unit must be placed in a MODE where this Function is no longer required to be OPERABLE within an additional 6 hours. This is **done performed** by opening all of the RTBs. With the RTBs open, these Functions are no longer required.

O.1, O.2.1, and O.2.2

Condition O applies to the RTBs in MODES 1 and 2, and in MODES 3, 4, and 5 with the RTBs closed and the PLS capable of rod withdrawal. With two divisions of RTBs and/or RTB Undervoltage and Shunt Trip Mechanisms inoperable, 1 hour is allowed to restore the three of the four divisions to OPERABLE status or the unit must be placed in MODE 3, 4 or 5 and the RTBs opened within the next 6 hours. The Completion Time of 6 hours is reasonable, based on operating

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

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. Placing the unit in MODE 3 with the RTBs open removes the requirement for this particular Function.

P.1 and P.2

Condition P applies to automatic ADS Stages 1, 2, and 3 Actuation, automatic CMT Actuation and the RTS Automatic Trip Logic in MODES 3, 4, and 5 with the RTBs closed and the PLS capable of rod withdrawal.

With one or two channels/divisions inoperable, three of the four channels/divisions must be restored to OPERABLE status in 48 hours. Restoring all channels but one to OPERABLE ensures that a single failure will neither cause nor prevent the protective function. The 48 hour Completion Time is considered reasonable since the protective function will still function.

If Required Actions described above cannot be met within the specified Completion Times, the unit must be placed in a MODE where this Function is no longer required to be OPERABLE. A Completion Time of an additional 1 hour is allowed to open the RTBs. With RTBs open, these Functions are no longer required.

Q.1 and Q.2

Condition Q applies to one or two inoperable Source Range Neutron Flux channels in MODE 3, 4, or 5 with the RTBs closed and the PLS capable of rod withdrawal. With the unit in this Condition, below P-6, the NIS source range performs the monitoring and protection functions. With one or two of the source range channels inoperable, 48 hours is allowed to restore three of the four channels to an OPERABLE status. If the channels cannot be returned to an OPERABLE status, 1 additional hour is allowed to open the RTBs. Once the RTBs are open, the core is in a more stable condition and the unit enters Condition R. The allowance of 48 hours to restore the channel to OPERABLE status, and the additional hour to open the RTBs, are justified in Reference 7.

R.1, R.2, and R.3

Condition R applies when the required Source Range Neutron Flux channel is inoperable in MODE 3, 4, or 5 with the RTBs open. With the unit in this Condition, the NIS source range performs the monitoring and protection functions. With the required source range channel inoperable, operations involving positive reactivity additions shall be suspended immediately. This will preclude any power escalation. In addition to suspension of positive reactivity additions, all valves that could add unborated

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

water to the RCS must be closed within 1 hour as specified in LCO 3.9.2. The isolation of unborated water sources will preclude a boron dilution accident.

Also, the SDM must be verified within 1 hour and once every 12 hours thereafter as per SR 3.1.1.1, SDM verification. With no source range channels OPERABLE, core protection is severely reduced. Verifying the SDM within 1 hour allows sufficient time to perform the calculations and determine that the SDM requirements are met. The SDM must also be verified once per 12 hours thereafter to ensure that the core reactivity has not changed. Required Action R.3 precludes any positive reactivity additions; therefore, core reactivity should not be increasing, and a 12 hour Frequency is adequate. The Completion Times of within 1 hour and once per 12 hours are based on operating experience in performing the Required Actions and the knowledge that unit conditions will change slowly.

SURVEILLANCE REQUIREMENTS

The SRs for each RTS Function are identified in 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.

The CHANNEL CALIBRATION and RTCOT are performed in a manner that is consistent with the assumptions used in analytically calculating the required channel accuracies. For channels that include dynamic transfer functions, such as, lag, lead/lag, rate/lag, the response time test may be performed with the transfer function set to one, with the resulting measured response time compared to the appropriate Chapter 7 response time (Ref. 2). Alternately, the response time test can be performed with the time constants set to their nominal value provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

SR 3.3.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of even something more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment have drifted outside ~~its~~ **their corresponding** limits.

The channels to be checked are:

- Power Range Neutron Flux
- Intermediate Range Neutron Flux
- Source Range Neutron Flux (**below P-6**)
- Overtemperature Delta T
- Overpower Delta T
- Pressurizer Pressure
- Pressurizer Water Level
- Reactor Coolant Flow – each hot leg
- RCP Bearing Water Temperature – each RCP
- RCP Speed
- SG Narrow Range Level – each SG

- RCS Loop T-cold – each cold leg
- RCS Loop T-hot – each cold leg

The Frequency is based on operating experience that demonstrates ~~the~~ **that** channel failure is rare. Automated operator aids may be used to facilitate the performance of the CHANNEL CHECK.

SR 3.3.1.2

SR 3.3.1.2 compares the calorimetric heat balance to the nuclear instrumentation channel output every 24 hours. If the calorimetric measurement between 70% and 100% RTP, differs from the nuclear instrument channel output by > 1% RTP, the nuclear instrument channel is not declared inoperable, but must be adjusted. If the nuclear instrument channel output cannot be properly adjusted, the channel is declared inoperable.

Three Notes modify SR 3.3.1.2. The first Note indicates that the nuclear instrument channel output shall be adjusted consistent with the calorimetric results if the absolute difference between the nuclear instrument channel output and the calorimetric measurement between 70% and 100% RTP is > 1% RTP. The second Note clarifies that this Surveillance is required only if reactor power is $\geq 15\%$ RTP and that 12 hours is allowed for performing the first Surveillance after reaching 15% RTP. At lower power levels the calorimetric data **from feedwater flow venturi measurements** are ~~inaccurate~~ **accurate**. The third

Response to Request For Additional Information (RAI)

BASES

The third Note is required because at power levels below 70%, calorimetric uncertainty creates the potential for non-conservative adjustment of the ΔT° conversion factor, in cases where the calculated ΔT power would be reduced to

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

match the calorimetric power. Therefore, if the calorimetric heat measurement is less than 70% RTP, and if the calculated ΔT power is lower than the calorimetric measurement by $> 5\%$, then the ΔT° conversion factor shall be adjusted so that the calculated ΔT power matches the calorimetric measurement. No ΔT° conversion factor adjustment is required if the calculated ΔT power is higher than the calorimetric measurement.

The Frequency of every 24 hours is based on plant operating experience, considering instrument reliability and the limited effects of fuel burnup and rod position changes on the accuracy of the calculated ΔT power.

SR 3.3.1.4

SR 3.3.1.4 compares the AXIAL FLUX DIFFERENCE determined using the incore system to the nuclear instrument channel AXIAL FLUX DIFFERENCE every 31 EFPD.

If the absolute difference is $\geq 3\%$ AFD the nuclear instrument channel is still OPERABLE, but must be readjusted. If the nuclear instrument channel cannot be properly readjusted, the channel is declared inoperable. This surveillance is performed to verify the $f(\Delta I)$ input to the overtemperature ΔT function.

Two Notes modify SR 3.3.1.4. The first Note indicates that the excore nuclear instrument channel shall be adjusted if the absolute difference between the incore and excore AFD is $\geq 3\%$ AFD. Note 2 clarifies that the Surveillance is required only if reactor power is $\geq 20\%$ RTP and that 24 hours is allowed for performing the first Surveillance after reaching 20% RTP. Below 20% RTP, the design of the incore detector system, low core power density, and detector accuracy make use of the incore detectors inadequate for use as a reference standard for comparison to the excore channels.

The Frequency of every 31 EFPD is adequate. ~~It is~~ based on plant 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.

SR 3.3.1.5

SR 3.3.1.5 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-adjusted~~ to agree with the incore detector measurements. If the excore channels cannot be adjusted, the channels are declared inoperable. This Surveillance is performed to verify the $f(\Delta I)$ input to the overtemperature ΔT Function.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

A Note modifies SR 3.3.1.5. The Note states that this Surveillance is required only if reactor power is > 50% RTP and that 24 hours is allowed for performing the first surveillance after reaching 50% RTP.

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

SR 3.3.1.6

SR 3.3.1.6 is the performance of a TADOT every 92 days on a STAGGERED TEST BASIS. This test shall verify OPERABILITY by actuation of the end devices.

The Reactor Trip Breaker (RTB) test shall include separate verification of the undervoltage and shunt trip mechanisms. Each RTB in a division shall be tested separately in order to minimize the possibility of an inadvertent trip.

The Frequency of every 92 days on a STAGGERED TEST BASIS is adequate. ~~It is~~ based on industry operating experience, considering instrument reliability and operating history data. In addition, the AP1000 design provides additional breakers to enhance reliability.

The SR is modified by a Note to clarify that both breakers in a single division are to be tested during each STAGGERED TEST.

SR 3.3.1.7 and SR 3.3.1.8

SR 3.3.1.7 and SR 3.3.1.8 ~~are~~ the performance of a REACTOR TRIP CHANNEL OPERATIONAL TEST (RTCOT) every 92 days. The SR 3.3.1.8 testing is performed in accordance with the SCPSP. If the actual setting of the channel is found to be outside the as-found tolerance, the channel is considered inoperable. This condition of the channel will be further evaluated during performance of the SR. This evaluation will consist of resetting the channel setpoint to the NTS (within the allowed tolerance), and evaluating the channel's response. If the channel is functioning as required and is expected to pass the next surveillance, then the channel is OPERABLE and can be restored to service at the completion of the surveillance. After the surveillance is completed, the channel as-found condition will be entered into the Corrective Action Program for further evaluation.

A RTCOT is performed on each required channel to provide reasonable

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

assurance that the entire channel will perform the intended Function.

A test subsystem is provided with the protection and safety monitoring system to aid the plant staff in performing the RTCOT. The test subsystem is designed to allow for complete functional testing by using a combination of system self checking features, functional testing features, and other testing features. Successful functional testing consists of verifying that the capability of the system to perform the safety function has not failed or degraded.

For hardware functions this would involve verifying that the hardware components and connections have not failed or degraded. Generally this verification includes a comparison of the outputs from two or more redundant subsystems or channels.

Since software does not degrade, software functional testing involves verifying that the software code has not changed and that the software code is executing.

To the extent possible, protection and safety monitoring system functional testing is accomplished with continuous system self-checking features and the continuous functional testing features. The RTCOT shall include a review of the operation of the test subsystem to verify the completeness and adequacy of the results.

If the RTCOT can not be completed using the built-in test subsystem, either because of failures in the test subsystem or failures in redundant channel hardware used for functional testing, the RTCOT can be performed using portable test equipment.

This test frequency of 92 days is justified based on Reference 7 and the use of continuous diagnostic test features, such as deadman timers, cross-check of redundant channels, memory checks, numeric coprocessor checks, and tests of timers, counters and crystal time bases, which will report a failure within the protection and safety monitoring system cabinets to the operator within 10 minutes of a detectable failure.

SR 3.3.1.7-8 is modified by a note that provides a 4 hour delay in the requirement to perform this Surveillance for source range instrumentation when entering MODE 3 from MODE 2. This 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 3.3.1.7-8 is no longer required to be performed. If the unit is to be in MODE 3 with the RTBs closed for a time greater than 4 hours, this Surveillance must be performed prior to 4 hours after entry into MODE 3.

During the RTCOT, the protection and safety monitoring system cabinets in the division under test may be placed in bypass.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

SR 3.3.1.89

SR 3.3.1.8-9 is the performance of a RTCOT as described in SR 3.3.1.7, and SR 3.3.1.8 except it is modified by a Note that this test shall include verification that the P-6 and P-10 interlocks are in their required state for the existing unit condition. The test is performed in accordance with the SCPSP. If the actual setting of the channel is found to be outside the as-found tolerance, the channel is considered inoperable. This condition of the channel will be further evaluated during performance of the SR. This evaluation will consist of resetting the channel setpoint to the NTS (within the allowed tolerance), and evaluating the channel's response. If the channel is functioning as required and is expected to pass the next surveillance, then the channel is OPERABLE and can be restored to service at the completion of the surveillance. After the surveillance is completed, the channel as-found condition will be entered into the Corrective Action Program for further evaluation.

The Frequency is modified by a Note that allows this surveillance to be satisfied if it has been performed within 92 days of the Frequencies prior to reactor startup and four hours after reducing power below P-10 and P-6. The Frequency of "prior to startup" ensures this surveillance is performed prior to critical operations and applies to the source, intermediate and power range low instrument channels. The Frequency of "4 hours after reducing power below P-10" (applicable to intermediate and power range low channels) and "4 hours after reducing power below P-6" (applicable to source range channels) allows a normal shutdown to be completed and the unit removed from the MODE of Applicability for this surveillance without a delay to perform the testing required by this surveillance. The Frequency of every 92 days thereafter applies if the plant remains in the MODE of Applicability after the initial performances of prior to reactor startup and four hours after reducing power below P-10 or P-6. The MODE of Applicability for this surveillance is < P-10 for the power range low and intermediate range channels and < P-6 for the source range channels. Once the unit is in MODE 3, this surveillance is no longer required. If power is to be maintained < P-10 or < P-6 for more than 4 hours, then the testing required by this surveillance must be performed prior to the expiration of the 4 hour limit. Four hours is a reasonable time to complete the required testing or place the unit in a MODE where this surveillance is no longer required. This test ensures that the NIS source, intermediate, and power range low channels are OPERABLE prior to taking the reactor critical and after reducing power into the applicable MODE (< P-10 or < P-6) for periods > 4 hours.

SR 3.3.1.910

A CHANNEL CALIBRATION is performed every 24 months, or approximately at every refueling. CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test verifies that the channel responds to a

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

measured parameter within the necessary range and accuracy.

The test is performed in accordance with the SCPSP. If the actual setting of the channel is found to be outside the as-found tolerance, the channel is considered inoperable. This condition of the channel will be further evaluated during performance of the SR. This evaluation will consist of resetting the channel setpoint to the NTS (within the allowed tolerance), and evaluating the channel response. If the channel is functioning as required and is expected to pass the next surveillance, then the channel is OPERABLE and can be restored to service at the completion of the surveillance. After the surveillance is completed, the channel as-found condition will be entered into the Corrective Action Program for further evaluation. Transmitter calibration must be performed consistent with the assumptions of the setpoint methodology. The differences between the current as-found values and the previous as-left values must be consistent with the transmitter drift allowance used in the setpoint methodology.

The setpoint methodology requires that 30 months drift be used (1.25 times the surveillance calibration interval, 24 months). ~~based on Generic Letter 91-04, "Changes in Technical Specification Surveillance Intervals to Accommodate a 24-month Fuel Cycle."~~

SR 3.3.1.9-10 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 3.3.1.101

SR 3.3.1.101 is the performance of a CHANNEL CALIBRATION every 24 months. This SR is modified by a Note stating that neutron detectors are excluded from the CHANNEL CALIBRATION. ~~The test is performed in accordance with the SCPSP. If the actual setting of the channel is found to be outside the as-found tolerance, the channel is considered inoperable. This condition of the channel will be further evaluated during performance of the SR. This evaluation will consist of resetting the channel setpoint to the NTS (within the allowed tolerance), and evaluating the channel's response. If the channel is functioning as required and is expected to pass the next surveillance, then the channel is OPERABLE and can be restored to service at the completion of the surveillance. After the surveillance is completed, the channel as-found condition will be entered into the Corrective Action Program for further evaluation.~~

-The CHANNEL CALIBRATION for the power range neutron detectors consists of a normalization of the detectors based on a power calorimetric and flux map performed above 20% RTP. Below 20% RTP, the design of the incore detector system, low core power density, and detector accuracy make use of the incore detectors inadequate for use as a reference standard for comparison to the excore channels. The CHANNEL CALIBRATION for the source range and intermediate range neutron detectors consists of obtaining the detector plateau

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

or preamp discriminator curves, evaluating those curves, and comparing the curves to the manufacturer's data. This Surveillance is not required for the power range detectors for entry into MODES 2 and 1, and is not required for the intermediate range detectors for entry into MODE 2, because the plant 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 Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed on the 24 month Frequency.

SR 3.3.1.142

SR 3.3.1.142 is the performance of a TADOT of the Manual Reactor Trip, and the SI, ADS Actuation, and CMT Injection inputs from the ESF logic. This TADOT is performed every 24 months. The test shall independently verify the OPERABILITY of the undervoltage and shunt trip mechanisms for the Manual Reactor Trip Function for the Reactor Trip Breakers.

The Frequency is based on the known reliability of the Functions and the multichannel redundancy available, and has been shown to be acceptable through operating experience.

The SR is modified by a Note that excludes verification of setpoints from the TADOT. The Functions affected have no setpoints associated with them.

SR 3.3.1.123

This SR 3.3.1.123 verifies that the individual channel/division actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response Time testing criteria are included in Reference 2.

For channels that include dynamic transfer Functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer Function set to one, with the resulting measured response time compared to the appropriate **FSAR-DCD Chapter 7** response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

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

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

actual response time tests on the remainder of the channel. Allocations for sensor 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. WCAP-13632-P-A, Revision 2, "Elimination of Pressure Sensor Response Time Testing Requirements" (Ref. 840), 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 WCAP. Response time verification for other sensor types must be demonstrated by test.

Each division response must be verified every 24 months on a STAGGERED TEST BASIS (i.e., all four Protection Channel Sets would be tested after 96 months). Response times cannot be determined during plant operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this surveillance when performed on a refueling frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

The SR 3.3.1.132 is modified by a note exempting neutron detectors from response time testing. A Note to the Surveillance indicates that neutron detectors may be 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. Chapter 6.0, "Engineered Safety Features."
2. Chapter 7.0, "Instrumentation and Controls."
3. Chapter 15.0, "Accident Analysis."
4. WCAP-16361-P, "Westinghouse Setpoint Methodology for Protection Systems – AP1000," May 2006 (proprietary).
5. Institute of Electrical and Electronic Engineers, IEEE-603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," June 27, 1991.
6. 10 CFR 50.49, "Environmental Qualifications of Electric Equipment Important to Safety for Nuclear Power Plants."
7. APP-GW-GSC-020, "Technical Specification Completion Time and

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RTS Instrumentation
B 3.3.1

BASES

Surveillance Frequency Justification."

- 8. ~~NRC Generic Letter No. 83-27, Surveillance Intervals in Standard Technical Specifications.~~
 - 9. ~~ESBU TB 97-01, Westinghouse Technical Bulletin, "Digital Process Rack Operability Determination Criteria," May 1, 1997.~~
 - 8.40. ~~WCAP-13632-P-A (Proprietary) and WCAP-13787-A (Non-Proprietary), Revision 2, "Elimination of Pressure Sensor Response Time Testing Requirements," January 1996.~~
- =====

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Attachment 16.3C

Markup of Bases for Specification 3.3.2

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

B 3.3 INSTRUMENTATION

B 3.3.2 Engineered Safety Feature Actuation System (ESFAS) Instrumentation

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits and the Reactor Coolant System (RCS) pressure boundary, and to mitigate accidents. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the ESFAS, as well as specifying LCOs on other reactor system parameters and equipment performance.

Technical Specifications are required by 10 CFR 50.36 to include LSSS for variables that have significant safety functions. LSSS are defined by the regulation as "Where a LSSS is specified for a variable on which a safety limit has been placed, the setting must be chosen so that automatic protective actions will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Safety Analysis Limit (SAL) is the limit of the process variable at which a protective action is initiated, as established by the safety analysis, to assure that a SL is not exceeded. However, in practice, the actual settings for automatic protection channels must be chosen to be more conservative than the Safety Analysis Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur. The LSSS values are identified and maintained in the Setpoint Program (SP) and are controlled by 10.CFR.50.59.

REVIEWER'S NOTE

For Westinghouse AP1000 plants, the term Nominal Trip Setpoint (NTS) is defined as the "Field setting" and is suggested as the actual setpoint implemented in the plant surveillance procedures. The as-found and as-left tolerances will apply to the NTS implemented in the Surveillance procedures to confirm channel performance.

The NTS is included in the SP.

The Nominal Trip Setpoint (NTS) specified in the SP is a predetermined field setting for a protection channel chosen to initiate automatic actuation prior to the process variable reaching the Safety Analysis Limit and thus assuring that the SL is not exceeded. As such, the NTS accounts for uncertainties in setting the channel (e.g., calibration), uncertainties in how the channel might actually perform (e.g., repeatability), changes in the point of action of the channel 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 NTS assures that the SL is not exceeded. Therefore, the NTS meets

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

the 10 CFR 50.36 definition of an LSSS.

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety functions(s)." Relying solely on the NTS to define OPERABILITY in Technical Specifications would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as-found" value of a protection channel setting during a surveillance. This would result in Technical Specification compliance problems, as well as reports and corrective actions required by the rule which are not necessary to ensure safety. For example, an automatic protection channel with a setting that has been found to be different from the NTS due to some drift of the setting may still be OPERABLE since drift is to be expected. This expected drift would have been specifically accounted for in the setpoint methodology for calculating the NTS and thus the automatic protective action would still have assured that the SL would not be exceeded with the "as-found" setting of the protection channel. Therefore, the channel would still be OPERABLE since it would have performed its safety function. If the as-found condition of the channel is near the as-found tolerance, recalibration is considered appropriate to allow for drift during the next surveillance interval.

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 2750 psia 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 40 CFR 50 and 40 CFR 100 acceptance criteria during AOOs.

Design Basis Accidents (DBA) 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 40 CFR 100 the 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 ESFAS instrumentation is segmented into distinct but interconnected modules.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Field Transmitters and Sensors

Normally, four redundant measurements using four separate sensors, are made for each variable used for actuation of ESF. The use of four channels for protection Functions is based on a minimum of two channels being required for a trip or actuation, one channel in test or bypass, and a single failure on the remaining channel. The signal selector in the Plant Control System will function correctly with only three channels. This includes two channels properly functioning and one channel having a single failure. Minimum requirements for protection and control ~~is-are~~ achieved with **only** three channels OPERABLE. The fourth channel is provided to increase plant availability, and permits the plant to run for an indefinite time with a single channel out of service. The circuit design is able to withstand both 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. Again, a single failure will neither cause nor prevent the protection Function actuation. These requirements are described in IEEE-603 (Ref. 4). The actual number of channels provided for each plant parameter is specified in Reference 2.

Engineered Safety Features (ESF) Channel

An ESF channel extends from the sensor to the output of the associated ESF subsystem and shall include the sensor (or sensors), the signal conditioning, any associated data links, and the associated ESF subsystem. For ESF channels containing nuclear instrumentation, the ESF channel shall also include the nuclear instrument signal conditioning and the associated Nuclear Instrumentation Signal Processing and Control (NISPAC) subsystem. Any manual ESF controls that are associated with a particular ESF channel are also included in that ESF channel.

Plant Protection Subsystem

The Plant Protection contains the necessary equipment to:

- Permit acquisition and analysis of the sensor inputs, including plant process sensors and nuclear instrumentation, required for reactor trip and ESF calculations;
- Perform computation or logic operations on variables based on these inputs;
- Provide trip signals to the reactor trip switchgear and ESF actuation data to the ESF coincidence logic as required;
- Permit manual trip or bypass of each individual reactor trip Function and permit manual actuation or bypass of each individual voted ESF Function;
- Provide data to other systems in the Instrumentation and Control (I&C) architecture; and
- Provide separate input circuitry for control Functions that require input from sensors that are also required for protection Functions.

Each of the four divisions of plant protection provides signal conditioning,

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

comparable output signals for indications in the main control room, and comparison of measured input signals with established setpoints. The basis of the setpoints are described in References ~~1, 2, and 3~~ and 9. If the measured value of a unit parameter exceeds the predetermined setpoint, an output is generated which is transmitted to the ESF coincidence logic for logic evaluation.

Within the ~~p~~Protection and ~~s~~Safety ~~m~~Monitoring ~~s~~System (PMS), redundancy is generally provided for active equipment such as processors and communication hardware. This redundancy is provided to increase plant availability and facilitate surveillance testing. A division or channel is OPERABLE if it is capable of performing its specified safety function(s) and all the required supporting functions or systems are also capable of performing their related support functions. Thus, a division or channel is OPERABLE as long as one set of redundant components within the division or channel are capable of performing its specified safety function(s).

ESF Coincidence Logic

The ESF coincidence logic contains the necessary equipment to:

- Permit reception of the data supplied by the four divisions of plant protection and perform voting on the trip outputs;
- Perform system level logic using the input data from the plant protection subsystems and transmit the output to the ESF actuation subsystems; and
- Provide redundant hardware capable of providing system level commands to the ESF actuation subsystems.

ESF Actuation Subsystems

The ESF actuation subsystems contain the necessary equipment to:

- Receive automatic system level signals supplied by the ESF coincidence logic;
- Receive and transmit data to/from main control room multiplexers;
- Receive and transmit data to/from other PLCs on the same logic bus;
- Receive status data from component position switches (such as limit switches and torque switches); and
- Perform logic computations on received data, generate logic commands for final actuators (such as START, STOP, OPEN, and CLOSE).

ESF Coincidence Logic and ESF Actuation Subsystem OPERABILITY Background

Each ESF coincidence logic and ESF actuation subsystem has two subsystems that communicate by means of redundant halves of the logic bus. This arrangement is provided to facilitate testing. If one subsystem is removed from service, the remaining subsystem continues to function and the ESF division continues to provide full protection. At least one of these redundant halves is connected to the battery backed portion of the power system. This provides full

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

functionality of the ESF division even when all ac power sources are lost. As long as one battery subsystem within an ESF coincidence logic or ESF actuation subsystem continues to operate, the ESF division is unaffected. An ESF division is only affected when all battery backed subsystems within that division's ESF coincidence logic or ESF actuation subsystem are not OPERABLE.

Nominal Trip Setpoints (NTSs) and Allowable Values

The ~~NTS is Trip Setpoints are~~ the nominal values at which the trip output is set. Any trip output is considered to be properly adjusted when the "as-left" value is within the band for CHANNEL CALIBRATION ~~accuracy, i.e., \pm rack calibration accuracy.~~

The ~~Trip S~~etpoints used in the trip output are based on the ~~analytical limit~~Safety Analysis Limits stated in Reference 23. The ~~calculation determination selection~~ of these Nominal 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, 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 ~~Trip Setpoints NTSPNTSs and Allowable Values~~ specified in ~~Table 3.3.2-1 in the SCPSP accompanying LCO are~~ conservatively ~~adjusted~~ with respect to the ~~analytical limit~~Safety Analysis Limits. A detailed description of the methodology used to calculate the ~~NTSPNTSs Trip Setpoints~~, including their explicit uncertainties, is provided in the "Westinghouse Setpoint Methodology for Protection Systems" (Refs. 9 and 10). ~~(Reference 9 is an AP600 document that describes a methodology that is applicable to AP1000. AP1000 has some slight differences in instrument spans as a result of the higher power level.)~~ The as-left tolerance and as-found tolerance band methodology is provided in the SCPSP. ~~The actual NTSP nominal Trip Setpoint entered into the bistable is more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a COT. The Allowable Value serves as the as-found Technical Specification OPERABILITY limit for the purpose of the COT. The as-found OPERABILITY limit for the purpose of the CHANNEL OPERATIONAL TEST (COT) is defined as the as-left limit, i.e., \pm rack calibration accuracy, about the NTS, (i.e., \pm rack calibration accuracy). OT. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the Allowable Value, the trip output is considered OPERABLE.~~

~~Setpoints in accordance with the Allowable Value ensure that the consequences of Design-Basis Accidents (DBAs) will be acceptable, providing the unit is operated from within the LCOs at the onset of the DBA and the equipment functions as designed.~~

The ~~Nominal Trip Setpoints and Allowable Values~~ listed in the ~~SCPSP Table 3.3.2-1~~ are based on the methodology described in Reference 9, which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each ~~NTSPNTS Trip Setpoint~~. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

uncertainty magnitudes. Transmitter and signal processing equipment calibration tolerances and drift allowances must be specified in plant calibration procedures, and must be consistent with the values used in the setpoint methodology.

~~Calibration tolerances and drift allowances must be specified in plant calibration procedures, and must be consistent with the values used in the setpoint methodology.~~

The OPERABILITY of each transmitter or sensor can be evaluated when its "as-found" calibration data are compared against the "as-left" data and are shown to be within the setpoint methodology assumptions. The basis of the setpoints is described in References 1, 2, 3, and 9. Trending of ~~transmitter~~ calibration results is required by the program description in Technical Specification 5.5.14.d. ~~Generic Letter 91-04, "Changes in Technical Specification Surveillance Intervals to Accommodate a 24-Month Fuel Cycle."~~

Note that the as-left and as-found tolerances listed in the SCPSP define the OPERABILITY limits for a channel during a periodic CHANNEL CALIBRATION, CHANNEL OPERATIONAL TESTS, or a TRIP ACTUATING DEVICE OPERATIONAL TEST that requires trip setpoint verification.

The protection and safety monitoring system testing features are designed to allow for complete functional testing by using a combination of system self-checking features, functional testing features, and other testing features. Successful functional testing consists of verifying that the capability of the system to perform the safety function has not failed or degraded. For hardware functions this would involve verifying that the hardware components and connections have not failed or degraded. Since software does not degrade, software functional testing involves verifying that the software code has not changed and that the software code is executing. To the extent possible, protection and safety monitoring system functional testing will be accomplished with continuous system self-checking features and the continuous functional testing features.

The protection and safety monitoring system incorporates continuous system self-checking features wherever practical. Self-checking features include on-line diagnostics for the computer system and the hardware and communications tests. These self-checking tests do not interfere with normal system operation.

In addition to the self-checking features, the system includes functional testing features. Functional testing features include continuous functional testing features and manually initiated functional testing features. To the extent practical, functional testing features are designed not to interfere with normal system operation.

In addition to the system self-checking features and functional testing features, other test features are included for those parts of the system which are not tested with self-checking features or functional testing features. These test features allow for instruments/sensor checks, calibration verification, response time testing, setpoint verification and component testing. The test features again include a combination of continuous testing features and manual testing features.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

All of the testing features are designed so that the duration of the testing is as short as possible. Testing features are designed so that the actual logic is not modified. To prevent unwanted actuation, the testing features are designed with either the capability to bypass a Function during testing and/or limit the number of signals allowed to be placed in test at one time.

APPLICABLE SAFETY ANALYSES, LCOs, 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, Pressurizer Pressure – Low 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 not specifically credited in the accident safety analysis are qualitatively credited in the safety analysis and the NRC staff approved licensing basis for the plant. These Functions may provide protection for conditions which 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).

Permissive and interlock functions are based upon the associated protection function instrumentation. Because they do not have to operate in adverse environmental conditions, the trip settings of the permissive and interlock functions use the normal environment, steady-state instrument uncertainties of the associated protection function instrumentation. This results in OPERABILITY criteria (i.e. as-found tolerance and as-left tolerance) that are the same as the associated protection function sensor and process rack modules. The Nominal Trip Setpoints for permissives and interlocks are based on the associated protection function OPERABILITY requirements, i.e., permissives and interlocks performing enabling functions must be set to occur prior to the specified trip setting of the associated protection function.

The LCO requires all instrumentation performing an ESFAS Function, listed in Table 3.3.2-1 in the accompanying LCO, to be OPERABLE. The as-left and as-found tolerances specified in the SCPSP define the OPERABILITY limits for a channel during the CHANNEL CALIBRATION or CHANNEL OPERATIONAL TEST (COT). As such, the as-left and as-found tolerances differ from the NTS by \pm the PMS rack calibration accuracy and envelope the expected calibration accuracy and drift for these racks. In this manner, the actual setting of the channel (NTS) prevents exceeding an SL at any given point of time as long as the channel has not drifted beyond the expected tolerances during the surveillance interval. Note that the as-left and as-found recorded values must be confirmed to be operating within the assumptions of the statistical uncertainty calculations.

If the actual setting of the channel is found outside the as-found tolerance, the channel is considered inoperable. This condition

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

of the channel will be further evaluated during performance of the SR. This evaluation will consist of resetting the channel setpoint to the NTS (within the allowed tolerance) and evaluating the channel's response. If the channel is functioning as required and expected to pass the next surveillance, then the channel is OPERABLE and can be restored to service at the completion of the surveillance. After the surveillance is completed, the channel as-found condition will be entered into the Corrective Action Program for further evaluation.

A trip setpoint may be set more conservative than the NTS as necessary in response to plant conditions. However, in this case, the operability of this instrument must be verified based on the actual field setting and not the NTS. Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

The LCO generally requires OPERABILITY of four channels in each instrumentation/logic Function and two devices for each manual initiation Function. The two-out-of-four configurations allow one channel to be bypassed during maintenance or testing without causing an ESFAS initiation. Two manual initiation channels are required to ensure no single random failure disables the ESFAS.

The required channels of ESFAS instrumentation provide plant protection in the event of any of the analyzed accidents. ESFAS protective functions are as follows:

1. Safeguards Actuation

The Safeguards Actuation signal actuates the alignment of the Core Makeup Tank (CMT) valves for passive injection to the RCS. The Safeguards Actuation signal provides two primary Functions:

- Primary side water addition to ensure maintenance or recovery of reactor vessel water level (coverage of the active fuel for heat removal and clad integrity, peak clad temperature < 2200°F); and
- Boration to ensure recovery and maintenance of SHUTDOWN MARGIN ($k_{eff} < 1.0$).

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

- Containment Isolation;
- Reactor Trip;
- Turbine Trip;
- Close Main Feedwater Control Valves;
- Trip Main Feedwater Pumps and Closure of Isolation and Crossover Valves; and
- Reactor Coolant Pump Trip.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

These other Functions ensure:

- Isolation of nonessential systems through containment penetrations;
- Trip of the turbine and reactor to limit power generation;
- Isolation of main feedwater to limit secondary side mass losses;
- Trip of the reactor coolant pumps to ensure proper CMT actuation;
- Enabling automatic depressurization of the RCS on CMT Level – Low 1 to ensure continued safeguards actuated injection.

Manual and automatic initiation of Safeguards Actuation must be OPERABLE in MODES 1, 2, 3, and 4. In these MODES there is sufficient energy in the primary and secondary systems to warrant automatic initiation of ESF systems. Automatic actuation in MODE 4 is provided by the high containment pressure signal. Manual initiation is required in MODE 5 to support system level initiation. Automatic initiation is not required to be OPERABLE in MODE 5 because parameters are not available to provide automatic actuation, and manual initiation is sufficient to mitigate the consequences of an accident.

These Safeguards Actuation Functions are not required to be OPERABLE in MODE 6 because there is adequate time for the operator to evaluate plant conditions and respond by manually starting individual systems, pumps, and other equipment to mitigate the consequences of an abnormal condition or accident. Plant pressure and temperature are very low and many ESF components are administratively locked out or otherwise prevented from actuating to prevent inadvertent overpressurization of plant systems.

1.a. Manual Initiation

The LCO requires that two manual initiation devices are OPERABLE. The operator can initiate the Safeguards Actuation signal at any time by using either of two switches in the main control room. This action will cause actuation of all components in the same manner as any of the automatic actuation signals.

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

Each device consists of one switch and the interconnecting wiring to all four divisions. Each manual initiation device actuates all four divisions. This configuration does not allow testing at power.

1.b. Containment Pressure – High 2

This signal provides protection against the following accidents:

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

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

The transmitters (d/p cells) and electronics are located inside of containment. Since the transmitters and electronics are located inside of containment, they will experience adverse environmental conditions and the ~~trip setpoint~~ NTSPNTS reflects both steady state and adverse environmental instrument uncertainties. The Containment Pressure – High 2 setpoint has been specified as low as reasonable, without creating potential for spurious trips during normal operations, consistent with the TMI action item (NUREG-0933, Item II.E.4.2) guidance.

The LCO requires four channels of Containment Pressure – High 2 to be OPERABLE in MODES 1, 2, 3, and 4. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

1.c. Pressurizer Pressure – Low

This signal provides protection against the following accidents:

- Inadvertent opening of a steam generator (SG) safety valve;
- SLB;
- A spectrum of rod cluster control assembly ejection accidents (rod ejection);
- Inadvertent opening of a pressurizer safety valve;
- LOCAs; and
- Steam Generator Tube Rupture (SGTR).

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). Therefore, the ~~Trip Setpoint~~ NTSPNTS reflects the inclusion of both steady state and adverse environmental instrument uncertainties.

The LCO requires four channels of Pressurizer Pressure – Low to be OPERABLE in MODES 1, 2, and 3 (above P-11, when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F), to mitigate the consequences of a high energy line rupture inside containment. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. This signal may be manually blocked by the operator below the P-11 setpoint. Automatic actuation below this pressure is then performed by the Containment Pressure – High 2 signal.

This Function is not required to be OPERABLE in MODE 3 below the P-11 setpoint. Other ESF Functions are used to detect accident conditions and actuate the ESF systems in this MODE. In MODES 4,

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

5, and 6, this Function is not needed for accident detection and mitigation.

1.d. Steam Line Pressure – Low

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

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

It is possible for the transmitters to experience adverse environmental conditions during a secondary side break. Therefore, the ~~Trip Setpoint NTSPNTS~~ reflects both steady state and adverse environmental instrument uncertainties.

This Function is anticipatory in nature and has a typical lead/lag ratio of 50/5.

The LCO requires four channels of Steam Line Pressure – Low to be OPERABLE in MODES 1, 2, and 3 (above P-11, when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F). At these conditions, a secondary side break or stuck open valve could result in the rapid depressurization of the steam lines. Four channels are provided in each steam line to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. This signal may be manually blocked by the operator below the P-11 setpoint. Below P-11, feed line break is not a concern, inside containment SLB will be terminated by automatic actuation via Containment Pressure – High 2, and outside containment SLB will be terminated by the Steam Line Pressure-Negative Rate – High signal for steam line isolation. In MODE 4, 5, or 6, this Function is not needed for accident detection and mitigation because the steam line pressure is below the actuation setpoint. Low steam line pressure in these MODES is not an adequate indication of a feed line or steam line break.

1.e. RCS Cold Leg Temperature (Tcold) – Low

This signal provides protection against the following accidents:

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

The LCO requires four channels of Tcold – Low to be OPERABLE in MODES 1 and 2, and in MODE 3 with any main steam isolation

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

valve open and above P-11 when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F. At these conditions, a secondary side break or stuck open valve could result in the rapid cooldown of the primary side. Four channels are provided in each loop to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. In MODES 4, 5, and 6, this Function is not needed for accident detection and mitigation because the cold leg temperature is reduced below the actuation setpoint.

2. Core Makeup Tank (CMT) Actuation

CMT Actuation provides the passive injection of borated water into the RCS. Injection provides RCS makeup water and boration during transients or accidents when the normal makeup supply from the Chemical and Volume Control System (CVS) is lost or insufficient. Two tanks are available to provide passive injection of borated water. CMT injection mitigates the effects of high energy line breaks by adding primary side water to ensure maintenance or recovery of reactor vessel water level following a LOCA, and by borating to ensure recovery or maintenance of SHUTDOWN MARGIN following a steam line break. CMT Valve Actuation is initiated by the Safeguards Actuation signal, Pressurizer Level – Low 2, ADS Stages 1, 2 and 3 Actuation, or manually.

The LCO requires that manual and automatic CMT Valve Actuation be OPERABLE in MODES 1 through 4. Manual and Automatic actuation of the CMT valves is additionally required in MODE 5 with the RCS pressure boundary intact. Actuation of this Function is not required in MODE 5 with the RCS pressure boundary open, or MODE 6 because the CMTs are not required to be OPERABLE in these MODES.

2.a. Manual Initiation

Manual CMT Valve Actuation is accomplished by either of two switches in the main control room. Either switch activates all four divisions.

2.b. Pressurizer Water Level – Low 2

This Function also initiates CMT Valve Actuation from the coincidence of pressurizer level below the Low 2 Setpoint in any two of the four divisions. This function can be manually blocked when the pressurizer water level is below the P-12 Setpoint. This Function is automatically unblocked when the pressurizer water level is above the P-12 Setpoint. The Setpoint reflects both steady state and adverse environmental instrument uncertainties as the detectors provide protection for an event that results in a harsh environment.

2.c. Safeguards Actuation (Function 1)

CMT Valve Actuation is also initiated by all Functions that initiate the Safeguards Actuation signal. The CMT Valve Actuation Function

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

requirements are the same as the requirements for the Safeguards Actuation Functions, but only apply in MODES 1 through 4, and in MODE 5 with the RCS pressure boundary intact. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 1 is referenced for all initiating Functions and requirements.

2.d. ADS Stages 1, 2, and 3 Actuation (Function 9)

The CMTs are actuated on an ADS Stages 1, 2, and 3 actuation. The CMT Actuation Function requirements are the same as the requirements for the ADS Stages 1, 2, and 3 Actuation Function, but only apply in MODES 1 through 4, and in MODE 5 with the RCS pressure boundary intact. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 9 is referenced for all initiating functions and requirements.

3. Containment Isolation

Containment Isolation provides isolation of the containment atmosphere and selected process systems which 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.

Containment Isolation is actuated by the Safeguards Actuation signal, manual actuation of containment cooling, or manually.

Manual and automatic initiation of Containment Isolation must be OPERABLE in MODES 1, 2, 3, and 4, when containment integrity is required. Manual initiation is required in MODE 5 and MODE 6 for closure of open penetrations providing direct access from the containment atmosphere to the outside atmosphere. Manual initiation of this Function in MODES 5 and 6 is not applicable if the direct access lines penetrating containment are isolated. Initiation of containment isolation by manual initiation of passive containment cooling in MODE 5 or 6 with decay heat ≤ 9.0 MWt is not required because OPERABILITY of the passive containment cooling system is not required when air cooling is sufficient. This provides the capability to manually initiate containment isolation during all MODES. Automatic Safeguards Actuation is required in MODE 5 for closure of open penetrations providing direct access from the containment atmosphere to the outside atmosphere. Automatic Safeguards Actuation is not required in MODE 6 because manual initiation is sufficient to mitigate the consequences of an accident in this MODE.

3.a. Manual Initiation

Manual Containment Isolation is accomplished by either of two switches in the main control room. Either switch actuates all four ESFAC divisions.

3.b. Manual Initiation of Passive Containment Cooling (Function 12.a)

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Containment Isolation is also initiated by Manual Initiation of Passive Containment Cooling. This is accomplished as described for ESFAS Function 12.a, but are not applicable if the direct access flow paths are isolated.

3.c. Safeguards Actuation (Function 1)

Containment Isolation is also initiated by all Functions that initiate the Safeguards Actuation signal. The Containment Isolation Function requirements are the same as the requirements for the Safeguards Actuation Function, but are not applicable if the direct access flow paths are isolated. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 1 is referenced for all initiating functions and requirements.

4. 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 steam lines will limit the steam break accident to the blowdown from one SG at most. For an SLB upstream of the isolation valves, inside or outside of containment, closure of the isolation valves limits the accident to the blowdown from only the affected SG. For a SLB downstream of the isolation valves, closure of the isolation valves terminates the accident as soon as the steam lines depressurize.

Closure of the turbine stop and control valves and the main steam branch isolation valves is initiated by this Function. Closure of these valves limits the accidental depressurization of the main steam system associated with an inadvertent opening of a single steam dump, relief, safety valve, or a rupture of a main steam line. Closure of these valves also supports a steam generator tube rupture event by isolating the faulted steam generator.

4.a. Manual Initiation

Manual initiation of Steam Line Isolation can be accomplished from the main control room. There are two switches in the main control room and either switch can initiate action to immediately close all main steam isolation valves (MSIVs). The LCO requires two OPERABLE channels in MODES 1, 2, 3, and 4 with any main steam valve open, when there is sufficient energy in the RCS and SGs to have an SLB or other accident resulting in the release of significant quantities of energy to cause a cooldown of the primary system. In MODES 5 and 6, this Function is not required to be OPERABLE because there is insufficient energy in the secondary side of the unit to cause an accident.

4.b. Containment Pressure – High 2

This Function actuates closure of the MSIVs in the event a SLB inside containment to limit the mass and energy release to

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

containment and limit blowdown to a single SG.

The transmitters and electronics are located inside containment, thus, they will experience harsh environmental conditions and the **Trip Setpoint NTSPNTS** reflects both steady state and adverse environmental instrument uncertainties.

The Containment Pressure – High 2 setpoint has been specified as low as reasonable, without creating potential for spurious trips during normal operations, consistent with the TMI action item (NUREG-0933, Item II.E.4.2) guidance. The LCO requires four channels of Containment Pressure – High 2 to be OPERABLE in MODES 1, 2, 3, and 4, with any main steam valve open, when there is sufficient energy in the primary and secondary side to pressurize the containment following a pipe break. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. There would be a significant increase in the containment pressure, thus allowing detection and closure of the MSIVs. In MODES 5 and 6, there is not

enough energy in the primary and secondary sides to pressurize the containment to the Containment Pressure – High 2 setpoint.

4.c. Steam Line Pressure

(1) Steam Line Pressure – Low

Steam Line Pressure – Low provides closure of the MSIVs in the event of an SLB to limit the mass and energy release to containment and limit blowdown to a single SG.

The LCO requires four channels of Steam Line Pressure – Low Function to be OPERABLE in MODES 1, 2, and 3 (above P-11, when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F), with any main steam isolation valve open, when a secondary side break or stuck open valve could result in the rapid depressurization of the steam lines. Four channels are provided in each steam line to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. This signal may be manually blocked by the operator below the P-11 setpoint. Below P-11, an inside containment SLB will be terminated by automatic actuation via Containment Pressure – High 2, and stuck open valve transients and outside containment steam line breaks will be terminated by the Steam Line Pressure-Negative Rate – High signal for Steam Line Isolation. In MODES 4, 5, and 6, this Function is not needed for accident detection and mitigation.

(2) Steam Line Pressure-Negative Rate – High

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Steam Line Pressure-Negative Rate – High provides closure of the MSIVs for an SLB, when less than the P-11 setpoint, to maintain at least one unfaulted SG as a heat sink for the reactor and to limit the mass and energy release to containment. When the operator manually blocks the Steam Line Pressure – Low when less than the P-11 setpoint, the Steam Line Pressure-Negative Rate – High signal is automatically enabled.

The LCO requires four channels of Steam Line Pressure-Negative Rate – High to be OPERABLE in MODE 3, with any main steam valve open, when less than the P-11 setpoint, when a secondary side break or stuck open valve could result in the rapid depressurization of the steam line(s). Four channels are provided in each steam line to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. In MODES 1 and 2, and in MODE 3 when above the P-11 setpoint with the RCS boron concentration below that necessary to meet the SDM requirements at an RCS temperature of 200°F, this signal is automatically disabled and the Steam Line Pressure – Low signal is automatically enabled.

In MODES 4, 5, and 6, this Function is not needed for accident detection and mitigation. While the transmitters may experience elevated ambient temperatures due to a steam line break, the Trip Function is on rate of change, not the absolute accuracy of the indicated steam pressure. Therefore, the **Trip Setpoint NTSPNTS** reflects only steady state instrument uncertainties.

4.d. Tcold – Low

This Function provides closure of the MSIVs during a SLB or inadvertent opening of a SG relief or a safety valve to maintain at least one unfaulted SG as a heat sink for the reactor and to limit the mass and energy release to containment.

This Function was discussed as Safeguards Actuation Function 1.e.

The LCO requires four channels of Tcold – Low to be OPERABLE in MODES 1 and 2, and in MODE 3 above P-11 when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F, with any main steam isolation valve open, when a secondary side break or stuck open valve could result in the rapid cooldown of the primary side. Four channels are provided in each loop to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. In MODE 3 below P-11 and in MODES 4, 5, and 6, this Function is not needed for accident detection and mitigation because

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

the cold leg temperature is reduced below the actuation setpoint.

5. Turbine Trip

The primary Function of the Turbine Trip is to prevent damage to the turbine due to water in the steam lines. This Function is necessary in MODES 1 and 2; and 3 above P-11 to mitigate the effects of a large SLB or a large Feedline Break (FLB). Failure to trip the turbine following a SLB or FLB can lead to additional mass and energy being delivered to the steam generators, resulting in excessive cooldown and additional mass and energy release in containment. In MODES 3, 4, 5, and 6, the turbine is not in operation and this function is not required to be OPERABLE.

This Function is actuated by Steam Generator Water Level – High 2, by a Safeguards Actuation signal, or manually. The Reactor Trip Signal also initiates a turbine trip signal whenever a reactor trip (P-4) is generated.

5.a. Manual Main Feedwater Isolation

The Turbine Trip is also initiated by the Manual Main Feedwater Control Valve Isolation Function. The requirements for this Function are the same as the requirements for Manual Main Feedwater Control Valve Isolation (Function 6.a), but only apply in MODES 1 and 2. Therefore, the requirements are not repeated in Table 3.3.2-1, and Function 6.a is referenced for all requirements.

5.b. Steam Generator Narrow Range Water Level – High 2

This signal provides protection against excessive feedwater flow by closing the main feedwater control, isolation and crossover valves, tripping of the main feedwater pumps, and tripping the turbine. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. The transmitters (d/p cells) are located inside containment.

However, the events which this Function protect against cannot cause severe environment in containment. Therefore, the Setpoint reflects only steady state instrument uncertainties.

5.c. Safeguards Actuation (Function 1)

Turbine Trip is also initiated by all Functions that initiate the Safeguards Actuation signal. The Turbine Trip Function requirements are the same as the requirements for the Safeguards Actuation Function, but only apply in MODES 1 and 2. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead Function 1 is referenced for all initiating Functions and requirements. The Safeguards Actuation signal closes all main feedwater control, isolation and crossover valves, trips all main feedwater pumps, and trips the turbine.

5.d. Reactor Trip (Function 18.ba)

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Turbine Trip is also initiated by all functions that initiate Reactor Trip. The turbine trip function requirements are the same as the requirements for the Reactor Trip Function, but only apply in MODES 1 and 2. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead Function 18.ba, P-4 (Reactor Trip), is referenced for all initiating Functions and requirements.

6. Main Feedwater Control Valve Isolation

The primary Function of Main Feedwater Control Valve Isolation is to prevent damage to the turbine due to water in the steam lines and to stop the excessive flow of feedwater into the SGs. This Function is actuated by Steam Generator Narrow Range Water Level – High 2, by a Safeguards Actuation signal, or manually. The Reactor Trip Signal also initiates closure of the main feedwater control valves coincident with a low RCS average temperature (Tavg) signal whenever a reactor trip (P-4) is generated.

Closing the Main Feedwater Control Valves on Manual Main Feedwater Isolation, SG Narrow Range Water Level-High 2, or Safeguards Actuation is necessary in MODES 1, 2, and 3 to mitigate the effects of a large SLB or a large FLB. This Function is also required to be OPERABLE in MODES 1 and 2 on Tavg Low-1 coincident with Reactor Trip (P-4). Failure to close the main feedwater control valves following a SLB or FLB can lead to additional mass and energy being delivered to the steam generators, resulting in excessive cooldown and additional mass and energy release in containment. Manual main feedwater isolation is required to be OPERABLE in MODE 4 when the main feedwater control valves are open. This Function is not applicable in MODE 4 for valve isolation if the main feedwater line is isolated. Automatic actuation on a Steam Generator Narrow Range Water Level – High 2 is required to be OPERABLE in MODE 4 when the RCS is not being cooled by the RNS. In MODES 5 and 6, the energy in the RCS and the steam generators is low and this function is not required to be OPERABLE.

6.a. Manual Main Feedwater Isolation

Manual Main Feedwater Isolation can be accomplished from the main control room. There are two switches in the main control room and either switch can initiate action in both divisions to close all main and startup feedwater control, isolation and crossover valves, trip all main and startup feedwater pumps, and trip the turbine.

6.b. Steam Generator Narrow Range Water Level – High 2

This signal provides protection against excessive feedwater flow by closing the main feedwater control, isolation and crossover valves, tripping of the Main Feedwater Pumps, and tripping the turbine.

Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. The transmitters (d/p cells) are located

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

inside containment. However, the events which this Function protect against cannot cause severe environment in containment. Therefore, the Setpoint reflects only steady state instrument uncertainties.

6.c. Safeguards Actuation (Function 1)

This Function is also initiated by all Functions that initiate the Safeguards Actuation signal. The Main Feedwater Control Valve Isolation Function requirements are the same as the requirements for the Safeguards Actuation Function, but do not apply in MODE 4 with the flow paths isolated. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead Function 1 is referenced for all initiating Functions and requirements. The Safeguards Actuation signal closes all main feedwater control, isolation and crossover valves, trips all main feedwater pumps, and trips the turbine.

6.d. Tavg Low-1 Coincident with Reactor Trip (P-4)

This signal provides protection against excessive feedwater flow by closing the main feedwater control valves. This signal results from a coincidence of two of the four divisions of reactor loop average temperature below the Low 1 setpoint coincident with the P-4 permissive. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure that no single random failure will disable this trip Function.

7. Main Feedwater Pump Trip and Valve Isolation

The primary function of the Main Feedwater Pump Trip and Isolation is to prevent damage to the turbine due to water in the steam lines and to stop the excessive flow of feedwater into the SGs. Valve isolation includes closing the main feedwater isolation and crossover valves. Isolation of main feedwater is necessary to prevent an increase in heat removal from the reactor coolant system in the event of a feedwater system malfunction. Addition of excessive feedwater causes an increase in core power by decreasing reactor coolant temperature. This Function is actuated by Steam Generator Water Level – High 2, by a Safeguards Actuation signal, or manually. The Reactor Trip Signal also initiates a turbine trip signal whenever a reactor trip (P-4) is generated.

This Function is necessary in MODES 1, 2, 3, and 4 to mitigate the effects of a large SLB or a large FLB except Tavg Low 2 coincident with Reactor Trip (P-4) which is required to be OPERABLE in MODES 1 and 2. Failure to trip the turbine or isolate the main feedwater system following a SLB or FLB can lead to additional mass and energy being delivered to the steam generators, resulting in excessive cooldown and additional mass and energy release in containment. Manual main feedwater isolation is required to be OPERABLE in MODE 4 when the main feedwater isolation valves are open. This Function is not applicable in MODE 4 for valve isolation if the main feedwater line is isolated. Automatic actuation on a Steam Generator Narrow Range Water Level – High 2 is required to be OPERABLE in

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

MODE 4 when the RCS is not being cooled by the RNS. In MODES 5 and 6, the energy in the RCS and the steam generators is low and this Function is not required to be OPERABLE.

7.a. Manual Main Feedwater Isolation

The Main Feedwater Pump Trip and Valve Isolation is also initiated by the Manual Main Feedwater Control Valve Isolation Function. The requirements for this Function are the same as the requirements for Manual Main Feedwater Control Valve Isolation (Function 6.a). Therefore, the requirements are not repeated in Table 3.3.2-1, and Function 6.a is referenced for all requirements.

7.b. Steam Generator Narrow Range Water Level – High 2

This signal provides protection against excessive feedwater flow by closing the main feedwater control, isolation and crossover valves, tripping of the main feedwater pumps, and tripping the turbine. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. The transmitters (d/p cells) are located inside containment. However, the events which this Function protect against cannot cause severe environment in containment. Therefore, the Setpoint reflects only steady state instrument uncertainties.

7.c. Safeguards Actuation (Function 1)

This Function is also initiated by all Functions that initiate the Safeguards Actuation signal. The Main Feedwater Pump Trip and Valve Isolation Function requirements are the same as the requirements for their Safeguards Actuation Function, but do not apply in MODE 4 with the flow paths isolated. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead Function 1 is referenced for all initiating Functions and requirements. The Safeguards Actuation signal closes all main feedwater control, isolation and crossover valves, trips all main feedwater pumps, and trips the turbine.

7.d. Tavg Low-2 Coincident with Reactor Trip (P-4)

This signal provides protection against excessive feedwater flow by closing the main feedwater isolation and crossover leg valves, and tripping of the main feedwater pumps. This signal results from a coincidence of two out of four divisions of reactor loop average temperature below the Low 2 setpoint coincident with the P-4 permissive. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure that no single random failure will disable this trip Function. This Function may be manually blocked when the pressurizer pressure is below the P-11 setpoint. The block is automatically removed when the pressurizer pressure is above the P-11 setpoint.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

8. Startup Feedwater Isolation

The primary Function of the Startup Feedwater Isolation is to stop the excessive flow of feedwater into the SGs. This Function is necessary in MODES 1, 2, 3, and 4 to mitigate the effects of a large SLB or a large FLB. Failure to isolate the startup feedwater system following a SLB or FLB can lead to additional mass and energy being delivered to the steam generators, resulting in excessive cooldown and additional mass and energy release in containment.

Startup feedwater isolation must be OPERABLE in MODES 1, 2, 3, and 4 when there is significant mass and energy in the RCS and the steam generators. This Function is not applicable in MODE 4 when the startup feedwater flow paths are isolated. In MODES 5 and 6, the energy in the RCS and the steam generators is low and this Function is not required to be OPERABLE.

8.a. Steam Generator (SG) Narrow Range Water Level – High 2

If steam generator narrow range level reaches the High 2 setpoint in either steam generator, then all startup feedwater control and isolation valves are closed and the startup feedwater pumps are tripped. Four channels are provided in each steam generator to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

8.b. Tcold – Low

This Function closes the startup feedwater control and isolation valves and trips the startup feedwater pumps if reactor coolant system cold leg temperature is below the Tcold setpoint in any loop. Startup feedwater isolation on this condition may be manually blocked when the pressurizer pressure is below the P-11 setpoint. This function is automatically unblocked when the pressurizer pressure is above the P-11 setpoint with the RCS boron concentration below that necessary to meet the SDM requirements at an RCS temperature of 200°F. Four channels are provided in each loop to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

8.c. Manual Main Feedwater Control Valve Isolation (Function 6.a)

The Startup Feedwater Isolation is also initiated by the Manual Main Feedwater Control Valve Isolation Function. The requirements for this Function are the same as the requirements for the Manual Main Feedwater Control Valve Isolation (Function 6.a). Therefore, the requirements are not repeated in Table 3.3.2-1, and Function 6.a is referenced for all requirements.

9. ADS Stages 1, 2, & 3 Actuation

The Automatic Depressurization System (ADS) provides a sequenced

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

depressurization of the reactor coolant system to allow passive injection from the CMTs, accumulators, and the in-containment refueling water storage tank (IRWST) to mitigate the effects of a LOCA. The depressurization is accomplished in four stages, with the first three stages discharging into the IRWST and the last stage discharging into containment. Each of the first three stages consists of two parallel paths with each path containing an isolation valve and a depressurization valve.

The first stage isolation valves open on any ADS Stages 1, 2, and 3 actuation. The first stage depressurization valves are opened following a preset time delay after the actuation of the isolation valves. The second stage isolation valves are opened following a preset time delay after actuation of the first stage depressurization valves open. The second stage depressurization valves are opened following a preset time delay after the second stage isolation valves are actuated, similar to stage one. Similar to the second stage, the third stage isolation valves are opened following a preset time delay after the actuation of the second stage depressurization valves. The third stage depressurization valves are opened following a preset time delay after the third stage isolation valves are actuated.

9.a. Manual Initiation

The first stage depressurization valves open on manual actuation. Any ADS Stages 1, 2, and 3 actuation also actuates PRHR and trips all reactor coolant pumps. The operator can initiate an ADS Stages 1, 2, and 3 actuation from the main control room by simultaneously actuating two ADS actuation devices in the same set. There are two sets of two switches each in the main control room. Simultaneously actuating the two devices in either set will actuate ADS Stages 1, 2, and 3. This Function must be OPERABLE in MODES 1, 2, 3, and 4. This Function must also be OPERABLE in MODES 5 and 6 when the required ADS valves are not open, and in MODE 6 with the upper internals in place. The required ADS valves or equivalent relief area are specified in LCO 3.4.12, ADS - Shutdown, RCS Intact and LCO 3.4.13, ADS - Shutdown, RCS Open.

9.b. CMT Level – Low 1 Coincident with CMT Actuation

This Function ensures continued passive injection or borated water to the RCS following a small break LOCA. ADS Stages 1, 2 and 3 actuation is initiated when the CMT Level reaches its Low 1 Setpoint coincident with any CMT Actuation signal (Function 2). Four channels are provided in each CMT to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

The ADS Stages 1, 2, and 3 Actuation Function requirements are the same as the requirements discussed in Function 2 (CMT Actuation). Therefore, the requirements are not repeated in Table 3.3.2-1. Instead Function 2 is referenced for all initiating functions and requirements. This Function must be

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

OPERABLE in MODES 1, 2, 3, and 4.

This Function must also be OPERABLE in MODE 5 with pressurizer level $\geq 20\%$ and the required ADS valves not open. The required ADS valves or equivalent relief area are specified in LCO 3.4.12, ADS - Shutdown, RCS Intact and LCO 3.4.13, ADS - Shutdown, RCS Open. In MODE 5, only one CMT is required to be OPERABLE in accordance with LCO 3.5.3, CMTs - Shutdown, RCS Intact; therefore, CMT level channels are only required on an OPERABLE CMT.

10. ADS Stage 4 Actuation

The ADS provides a sequenced depressurization of the reactor coolant system to allow passive injection from the CMTs, accumulators, and the IRWST to mitigate the effects of a LOCA. The depressurization is accomplished in four stages, with the first three stages discharging into the IRWST and the fourth stage discharging into containment.

The fourth stage of the ADS consists of four parallel paths. Each of these paths consists of a normally open isolation valve and a depressurization valve. The four paths are divided into two groups with two paths in each group. Within each group, one path is designated to be substage A and the second path is designated to be substage B.

The substage A depressurization valves are opened following a preset time delay after the substage A isolation valve confirmatory open signal. The sequence is continued with substage B. A confirmatory open signal is provided to the substage B isolation valves following a preset time delay after the substage A depressurization valve has been opened. The signal to open the substage B depressurization valve is provided following a preset time delay after the substage B isolation valves confirmatory open signal.

10.a. Manual Initiation Coincident with RCS Wide Range Pressure – Low or ADS Stages 1, 2, and 3 Actuation (Function 9)

The fourth stage depressurization valves open on manual actuation. The operator can initiate Stage 4 of ADS from the main control room. There are two sets of two switches each in the main control room. Actuating the two switches in either set will actuate all 4th stage ADS valves. This manual actuation is interlocked to actuate with either the low RCS pressure signal or with the ADS Stages 1, 2, & 3 actuation (Function 9). These interlocks minimize the potential for inadvertent actuation of this Function. This interlock with Function 9 allows manual actuation of this Function if automatic or manual actuation of the ADS Stages 1, 2, & 3 valves fails to depressurize the RCS due to common-mode failure. This consideration is important in PRA modeling to improve the reliability of reducing the RCS pressure

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

following a small LOCA or transient event. This Function must be OPERABLE in MODES 1, 2, 3, and 4. This Function must also be OPERABLE in MODES 5 and 6 when the required ADS valves are not open, and in MODE 6 with the upper internals in place. The required ADS valves or equivalent relief area are specified in LCO 3.4.12, ADS - Shutdown, RCS Intact and LCO 3.4.13, ADS - Shutdown, RCS Open.

10.b. CMT Level – Low 2 Coincident with RCS Wide Range Pressure – Low

The fourth stage depressurization valves open on CMT Level – Low 2 in two-out-of-four channels in either CMT. Actuation of the fourth stage depressurization valves is interlocked with the third stage depressurization signal such that the fourth stage is not actuated unless the third stage has been previously actuated following a preset time delay. Actuation of the fourth stage ADS valves are further interlocked with a low RCS pressure signal such that the ADS Stage 4 actuation is not actuated unless the RCS pressure is below a predetermined setpoint. Four channels of CMT level are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. This Function must be OPERABLE in MODES 1, 2, 3, and 4. This Function must also be OPERABLE in MODE 5 when the required ADS valves are not open and with the pressurizer level $\geq 20\%$. The required ADS valves or equivalent relief area are specified in LCO 3.4.12, ADS - Shutdown, RCS Intact and LCO 3.4.13, ADS - Shutdown, RCS Open. In MODE 5, only one CMT is required to be OPERABLE in accordance with LCO 3.5.3, CMTs - Shutdown, RCS Intact; therefore, CMT level channels are only required on an OPERABLE CMT.

10.c. Coincident RCS Loop 1 and 2 Hot Leg Level – Low

A signal to automatically open the ADS Stage 4 is also generated when coincident loop 1 and 2 reactor coolant system hot leg level indication decreases below an established setpoint for a duration exceeding an adjustable time delay. This Function is required to be OPERABLE in MODE 4 with the RCS being cooled by the RNS. This Function is also required to be OPERABLE in MODE 5 and in MODE 6 when the required ADS valves are not open. The required ADS valves or equivalent relief area are specified in LCO 3.4.12, ADS - Shutdown, RCS Intact and LCO 3.4.13, ADS - Shutdown, RCS Open.

11. Reactor Coolant Pump Trip

Reactor Coolant Pump (RCP) Trip allows the passive injection of borated water into the RCS. Injection provides RCS makeup water and boration during transients or accidents when the normal makeup supply from the CVS is lost or insufficient. Two tanks

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

provide passive injection of borated water by gravity when the reactor coolant pumps are tripped. CMT injection mitigates the effects of high energy line breaks by adding primary side water to ensure maintenance or recovery of reactor vessel water level following a LOCA, and by borating to ensure recovery or maintenance of SHUTDOWN MARGIN following a steam line break. RCP trip on high bearing water temperature protects the RCP coast down. A high bearing water temperature trip signal will result in the tripping of all the RCPs. RCP trip is actuated by High RCP bearing water temperature, ADS Stages 1, 2, and 3 Actuation (Function 9), Manual CMT Actuation (Function 2.a), Pressurizer Water Level – Low 2, and Safeguards Actuation (Function 1).

11.a. ADS Stage 1, 2, and 3 Actuation (Function 9)

The RCPs are tripped any time ADS Stage 1, 2, and 3 actuation is initiated. The RCP trip Function requirements for the ADS Stage 1, 2, and 3 actuation are the same as the requirements for the ADS Function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead Function 9 is referenced for all initiating functions and requirements.

11.b. Reactor Coolant Pump Bearing Water Temperature – High

The RCPs are tripped if two-out-of-four sensors on any RCP indicate high bearing water temperature. This Function is required to be OPERABLE in MODES 1 and 2. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

11.c. Manual CMT Actuation (Function 2.a)

RCP trip is also initiated by the manual CMT actuation Function. The RCP trip Function requirements are the same as the requirements for the manual CMT actuation Function. Therefore, the requirements are not repeated in Table 3.3.2-1, and Function 2.a is referenced for all requirements.

11.d. Pressurizer Water Level – Low 2

The RCPs are tripped when the pressurizer water level reaches its Low 2 setpoint. This signal results from the coincidence of pressurizer water level below the Low 2 setpoint in any two-of-four divisions. This Function is required to be OPERABLE in MODES 1, 2, 3, and 4. This Function is also required to be OPERABLE in MODE 5 with pressurizer level $\geq 20\%$, when the RCS is not being cooled by the RNS. This Function can be manually blocked when the pressurizer water level is below the P-12 setpoint. This Function is automatically unblocked when the pressurizer water level is above the P-12 setpoint.

11.e. Safeguards Actuation (Function 1)

This Function is also initiated by all Functions that initiated the

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Safeguards Actuation signal. The requirements for the reactor trip Functions are the same as the requirements for the Safeguards Actuation Function. Therefore, the requirements are not repeated in Table 3.3.2.1. Instead, Function 1 is referenced for all initiating Functions and requirements.

12. Passive Containment Cooling Actuation

The Passive Containment Cooling System (PCS) transfers heat from the reactor containment to the environment. This Function is necessary to prevent the containment design pressure and temperature from being exceeded following any postulated DBA (such as LOCA or SLB). Heat removal is initiated automatically in response to a Containment Pressure – High 2 signal or manually.

A Passive Containment Cooling Actuation signal initiates water flow by gravity by opening the isolation valves. The water flows onto the containment dome, wetting the outer surface. The path for natural circulation of air along the outside walls of the containment structure is always open.

The LCO requires this Function to be OPERABLE in MODES 1, 2, 3, and 4 when the potential exists for a DBA that could require the operation of the Passive Containment Cooling System. In MODES 5 and 6, with decay heat more than 9.0 MWt, manual initiation of the PCS provides containment heat removal. Section B 3.6.7, Applicability, provides the basis for the decay heat limit.

12.a. Manual Initiation

The operator can initiate Containment Cooling at any time from the main control room by actuating either of the two containment cooling actuation switches. There are two switches in the main control room, either of which will actuate containment cooling in all divisions. Manual Initiation of containment cooling also actuates containment isolation.

12.b. Containment Pressure – High 2

This signal provides protection against a LOCA or SLB inside containment. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

The transmitters and electronics are located inside containment, thus, they will experience harsh environmental conditions and the ~~trip setpoint NTSPNTS~~ reflects ~~only both~~ steady state and adverse environmental instrument uncertainties ~~associated with the containment environment~~. The Containment Pressure – High 2 setpoint has been specified as low as reasonable, without creating potential for spurious trips during normal operations, consistent with the TMI action item (NUREG-0933, Item II.E.4.2) guidance.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

13. PRHR Heat Exchanger Actuation

The PRHR Heat Exchanger (HX) provides emergency core decay heat removal when the Startup Feedwater System is not available to provide a heat sink. PRHR is actuated when the discharge valves are opened in response to Steam Generator Narrow Range (NR) Level – Low coincident with Startup Feedwater Flow – Low, Steam Generator Wide Range (WR) Level – Low, ADS Stages 1, 2, and 3 Actuation, CMT Actuation, Pressurizer Water Level – High 3, or Manual Initiation.

13.a. Manual Initiation

Manual PRHR actuation is accomplished by either of two switches in the main control room. Either switch actuates all four ESFAC Divisions.

This Function is required to be OPERABLE in MODES 1, 2, 3, and 4, and MODE 5 with the RCS pressure boundary intact. This ensures that PRHR can be actuated in the event of a loss of the normal heat removal systems.

13.b. Steam Generator Narrow Range Level – Low Coincident with Startup Feedwater Flow – Low

PRHR is actuated when the Steam Generator Narrow Range Level reaches its low setpoint coincident with an indication of low Startup Feedwater Flow.

The LCO requires four channels per steam generator to be OPERABLE to satisfy the requirements with a two-out-of-four logic. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. The Setpoint reflects both steady state and adverse environmental instrument uncertainties as the detectors provide protection for an event that results in a harsh environment.

Startup Feedwater Flow – Low uses a one-out-of-two logic on each of the two startup feedwater lines. This Function is required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 when the RCS is not being cooled by the Normal Residual Heat Removal System (RNS). This ensures that PRHR can be actuated in the event of a loss of the normal heat removal systems. In MODE 4 when the RCS is being cooled by the RNS, and in MODES 5 and 6, the SGs are not required to provide the normal RCS heat sink. Therefore, startup feedwater flow is not required, and PRHR actuation on low startup feedwater flow is not required.

13.c. Steam Generator Wide Range Level – Low

PRHR is also actuated when the SG Wide Range Level reaches its Low Setpoint. There are four wide range level channels for each

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

steam generator and a two-out-of-four logic is used. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. This Function is required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 when the RCS is not being cooled by the RNS. This ensures that PRHR can be actuated in the event of a loss of the normal heat removal systems. In MODE 4 when the RCS is being cooled by the RNS, and in MODES 5 and 6, the SGs are not required to provide the normal RCS heat sink. Therefore, SG Wide Range Level is not required, and PRHR actuation on low wide range SG level is not required.

13.d. ADS Stages 1, 2, and 3 Actuation

PRHR is also actuated any time ADS Stages 1, 2, and 3 Actuation is initiated. The PRHR actuation Function requirements for the ADS Stages 1, 2, and 3 actuation are the same as the requirements for the ADS Stages 1, 2, and 3 Actuation Function, but only in MODES 2, 3, and 4, and in MODE 5 with the RCS pressure boundary intact.

13.e. CMT Actuation (Function 2)

PRHR is also actuated by all the Functions that actuate CMT injection. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 2 (CMT Actuation) is referenced for all initiating functions and requirements.

13.f. Pressurizer Water Level – High 3

PRHR is actuated when the pressurizer water level reaches its High 3 setpoint. This signal provides protection against a pressurizer overfill following an inadvertent core makeup tank actuation with consequential loss of offsite power. This Function is automatically unblocked when RCS pressure is above the P-19 setpoint. This Function is required to be OPERABLE in MODES 1, 2, and 3, and in MODE 4 when the RCS is not being cooled by the RNS and above the P-19 (RCS pressure) interlock. This Function is not required to be OPERABLE in MODES 5 and 6 because it is not required to mitigate DBA in these MODES.

14. Steam Generator Blowdown Isolation

The primary Function of the steam generator blowdown isolation is to ensure that sufficient water inventory is present in the steam generators to remove the excess heat being generated until the decay heat has decreased to within the PRHR HX capability.

This Function closes the isolation valves of the Steam Generator Blowdown System in both steam generators when a signal is generated from the PRHR HX Actuation or Steam Generator Narrow Range Water

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Level – Low. This Function is required to be OPERABLE in MODES 1, 2, and 3, and in MODE 4 when the RCS is not being cooled by the RNS. This Function is not required to be OPERABLE in MODE 4 if the steam generator blowdown line is isolated.

14.a. PRHR Heat Exchanger Actuation (Function 13)

Steam Generator Blowdown Isolation is also initiated by all Functions that initiate PRHR actuation. The Steam Generator Blowdown Isolation requirements for these Functions are the same as the requirements for the PRHR Actuation. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 13, PRHR HX Actuation, is referenced for all initiating Functions and requirements.

14.b. Steam Generator Narrow Range Level – Low

The Steam Generator Blowdown isolation is actuated when the Steam Generator Narrow Range Level reaches its Low Setpoint.

The LCO requires four channels per steam generator to be OPERABLE to satisfy the requirements with a two-out-of-four logic. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will

disable this trip Function. Setpoint reflects both steady state and adverse environmental instrument uncertainties as the detectors provide protection for an event that results in a harsh environment.

15. Boron Dilution Block

The block of boron dilution is accomplished by closing the CVS suction valves to demineralized water storage tanks, and aligning the boric acid tank to the CVS makeup pumps. This Function is actuated by Source Range Neutron Flux Doubling and Reactor Trip.

15.a. Source Range Neutron Flux Doubling

A signal to block boron dilution in MODES 2 or 3, when not critical or during an intentional approach to criticality, and MODES 4 or 5 is derived from source range neutron flow increasing at an excessive rate (source range flux doubling).

This Function is not applicable in MODES 4 and 5 if the demineralized water makeup flowpath is isolated. The source range neutron detectors are used for this Function. The LCO requires four divisions to be OPERABLE. There are four divisions and two-out-of-four logic is used. On a coincidence of excessively increasing source range neutron flux in two of the four divisions, demineralized water is isolated from the makeup pumps and reactor coolant makeup is isolated from the reactor coolant system to preclude a boron dilution event. In MODE 6, a dilution event is precluded by the requirement in LCO 3.9.2 to close, lock and secure at least one valve in each unborated water source flow path.

15.b. Reactor Trip (Function 18.ba)

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Demineralized Water Makeup is also isolated by all the Functions that initiate a Reactor Trip. The isolation requirements for these Functions are the same as the requirements for the Reactor Trip Function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead Function 18.ba, (P-4 Reactor Trip Breakers), is referenced for all initiating Functions and requirements.

16. Chemical Volume and Control System Makeup Line Isolation

The CVS makeup line is isolated following certain events to prevent overfilling of the RCS. In addition, this line is isolated on High 2 containment radioactivity to provide containment isolation following an accident. This line is not isolated on a containment isolation signal, to allow the CVS makeup pumps to perform their defense-in-depth functions. However, if very high containment radioactivity exists (above the High 2 setpoint) this line is isolated.

A signal to isolate the CVS is derived from two-out-of-four high steam generator levels on either steam generator, two-out-of-four channels of pressurizer level indicating high or two-out-of-four channels of containment radioactivity indicating high. Four channels are provided to permit one

channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function.

16.a. Steam Generator Narrow Range Water Level – High 2

Four channels of steam generator level are provided for each steam generator. Two-out-of-four channels on either steam generator indicating level greater than the setpoint will close the isolation valves for the CVS. This Function prevents adding makeup water to the RCS during a SGTR. This Function is required to be OPERABLE in MODES 1, 2, 3, and 4 with the RCS not being cooled by the RNS. This Function is not applicable in MODES 3 and 4 if the CVS makeup flowpath is isolated. This Function is not required to be OPERABLE in MODES 5 and 6 because the RCS pressure and temperature are reduced and a steam generator tube rupture event is not credible.

16.b. Pressurizer Water Level – High 1 Coincident with Safeguards Actuation

Four channels of pressurizer level are provided on the pressurizer. Two-out-of-four channels on indicating level greater than the High 1 setpoint coincident with a Safeguards Actuation signal (Function 1) will close the containment isolation valves for the CVS. This Function prevents the pressurizer level from reaching a level that could lead to water relief through the pressurizer safety valves during some DBAs. This Function is required to be OPERABLE in MODES 1, 2, and 3. This function is not required to be OPERABLE in MODES 4, 5, and 6, because it is not required to mitigate a DBA in these MODES. This

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Function is not applicable in MODE 3, if the CVS makeup flowpath is isolated.

16.c. Pressurizer Water Level – High 2

A signal to close the CVS isolation valves is generated on Pressurizer Water Level – High 2. This Function results from the coincidence of pressurizer level above the High 2 setpoint in any two of the four divisions. This Function is automatically blocked when the pressurizer pressure is below the P-11 permissive setpoint to permit pressurizer water solid conditions with the plant cold and to permit level makeup during plant cooldowns. This Function is automatically unblocked when RCS pressure is above the P-19 setpoint. This Function is required to be OPERABLE in MODES 1, 2, and 3 and in MODE 4 when the RCS is not being cooled by the RNS. This Function is not required to be OPERABLE in MODE 4 if the CVS makeup flowpath is isolated. This Function is not required to be OPERABLE in MODES 5 and 6 because it is not required to mitigate a DBA in these MODES.

16.d. Containment Radioactivity – High 2

Four channels of Containment Radioactivity – High 2 are required to be OPERABLE in MODES 1, 2, and 3 when the potential exists for a LOCA, to ensure that the radioactivity inside containment is not released to the atmosphere. This Function is not required to be OPERABLE in MODE 3 if the associated flowpath is isolated. This signal results from the coincidence of containment radioactivity above the High 2 Setpoint in any two of the four divisions. These Functions are not required to be OPERABLE in MODES 4, 5, and 6 because there is no credible release of radioactivity into the containment in these MODES that would result in a High 2 actuation.

16.e. Manual Initiation

Manual Chemical Volume Control System Makeup Isolation is actuated by either of two switches in the main control room.

Either switch closes Chemical Volume Control System Makeup valves. The LCO requires two switches to be OPERABLE.

16.f. Source Range Neutron Flux Doubling (Function 15.a)

Chemical Volume Control System Makeup Isolation is actuated by the Source Range Neutron Flux Doubling Function. The Source Range Neutron Flux Doubling Function requirements are the same as the requirements for Boron Dilution Block Function 15.a, Source Range Neutron Flux Doubling. Therefore, the requirements are not repeated in Table 3.3.2-1, and Function 15.a is referenced for all requirements.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

17. Normal Residual Heat Removal System Isolation

The RNS suction line is isolated by closing the containment isolation valves on High 2 containment radioactivity to provide containment isolation following an accident. This line is isolated on a safeguards actuation signal. However, the valves may be reset to permit the RNS pumps to perform their defense-in-depth functions ~~postaccident~~ **post accident**. Should a high containment radiation signal (above the High 2 setpoint) develop following the containment isolation signal, the RNS valves would re-close. A high containment radiation signal is indicative of a high RCS source term and the valves would re-close to assure offsite doses do not exceed regulatory limits.

17.a. Containment Radioactivity – High 2

A signal to isolate the normal residual heat removal system is generated from the coincidence of containment radioactivity above the High 2 setpoint in two-out-of-four channels. Four channels of Containment Radioactivity – High 2 are required to be OPERABLE in MODES 1, 2, and 3 when the potential exists for a LOCA, to ensure that the radioactivity inside containment is not released to the atmosphere. This Function is not required to be OPERABLE in MODE 3 if the RNS suction line is isolated. These Functions are not required to be OPERABLE in MODES 4, 5, and 6 because no DBA that could release radioactivity into the containment is considered credible in these MODES.

17.b. Safeguards Actuation (Function 1)

This Function is also initiated by all Functions that initiated the Safeguards Actuation signal. The requirements to isolate the normal residual heat removal system are the same as the requirements for the Safeguards Actuation Function.

Therefore, the requirements are not repeated in Table 3.3.2.1. Instead, Function 1 is referenced for all initiating Functions and requirements.

17.c. Manual Initiation

The operator can initiate RNS isolation at any time from the control room by simultaneously actuating two switches in the same actuation set. Because an inadvertent actuation of RNS isolation could have serious consequences, two switches must be actuated simultaneously to initiate isolation. There are two sets of two switches in the control room. Simultaneously actuating the two switches in either set will isolate the RNS in the same manner as the automatic actuation signal. Two Manual Initiation switches in each set are required to be OPERABLE to ensure no single failure disables the Manual Initiation Function.

18. ESFAS Interlocks

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

To allow some flexibility in unit operations, several interlocks are included as part of the ESFAS. These interlocks permit the operator to block some signals, automatically enable other signals, prevent some actions from occurring, and cause other actions to occur. The interlock Functions backup manual actions to ensure bypassable Functions are in operation under the conditions assumed in the safety analyses.

18.a. Reactor Trip Breaker Open, P-3

The P-3 interlock is provided to permit the block of automatic Safeguards Actuation after a predetermined time interval following automatic Safeguards Actuation.

The reactor trip breaker position switches that provide input to the P-3 interlock only function to energize or de-energize (open or close) contacts. Therefore, this Function does not have an adjustable trip setpoint.

18.ba. Reactor Trip, P-4

There are eight reactor trip breakers with two breakers in each division. The P-4 interlock is enabled when the breakers in two-out-of-four divisions are open. Additionally, the P-4 interlock is enabled by all Automatic Reactor Trip Actuations. The Functions of the P-4 interlock are:

- Trip the main turbine
- Block boron dilution
- Isolate main feedwater coincident with low reactor coolant temperature (This function is not assumed in safety analysis therefore, it is not included in the technical specifications.)

The reactor trip breaker 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 ~~t~~rip ~~s~~etpoint.

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 to trip the main turbine, because the main turbine is not in operation.

The P-4 Function does not have to be OPERABLE in MODE 4 or 5 to block boron dilution, because Function 15.a, Source Range Neutron Flux Doubling, provides the required block. In MODE 6, the P-4 interlock with the Boron Dilution Block Function is not required, since the unborated water source flow path isolation valves are locked closed in accordance with LCO 3.9.2.

18.c. Intermediate Range Neutron Flux, P-6

The Intermediate Range Neutron Flux, P-6 interlock is actuated when the respective NIS intermediate range channel increases to

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

approximately one decade above the channel lower range limit. Below the setpoint, the P-6 interlock automatically unblocks the flux doubling function, permitting the block of boron dilution. Normally, this Function is blocked by the main control room operator during reactor startup. This Function is required to be OPERABLE in MODE 2.

18.db. Pressurizer Pressure, P-11

The P-11 interlock permits a normal unit cooldown and depressurization without Safeguards Actuation or main steam line and feedwater isolation. With pressurizer pressure channels less than the P-11 setpoint, the operator can manually block the Pressurizer pressure – Low, Steam Line Pressure – Low, and Tcold – Low Safeguards Actuation signals and the Steam Line Pressure – Low and Tcold – Low steam line isolation signals. When the Steam Line Pressure – Low is manually blocked, a main steam isolation signal on Steam Line Pressure-Negative Rate – High is enabled. This provides protection for an SLB by closure of the main steam isolation valves. Manual block of feedwater isolation on Tavg – Low 1, Low 2, and Tcold – Low is also permitted below P-11. With pressurizer pressure channels \geq P-11 setpoint, the Pressurizer Pressure – Low, Steam Line Pressure – Low, and Tcold – Low Safeguards Actuation signals and the Steam Line Pressure Low and Tcold – Low steam line isolation signals are automatically enabled. The feedwater isolation signals on Tcold – Low, Tavg – Low 1 and Low 2 are also automatically enabled above P-11. The operator can also enable these signals by use of the respective manual reset buttons. When the Steam Line Pressure – Low and Tcold – Low steam line isolation signals are enabled, the main steam isolation on Steam Line Pressure-Negative Rate – High is disabled. The 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 Safeguards Actuation or main steam or feedwater isolation. This Function does not have to be OPERABLE in MODE 4, 5, or 6, because plant pressure must already be below the P-11 setpoint for the requirements of the heatup and cooldown curves to be met.

~~18.c. Intermediate Range Neutron Flux, P-6~~

~~The Intermediate Range Neutron Flux, P-6 interlock is actuated when the respective NIS intermediate range channel goes increases to approximately one decade above the minimum channel reading lower range limit. Below the setpoint, the P-6 interlock automatically unblocks the flux doubling function, permitting the block of boron dilution. Normally, this Function is blocked by the main control room operator during reactor startup. This Function is required to be OPERABLE in MODE 2.~~

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

18.ed. Pressurizer Level, P-12

The P-12 interlock is provided to permit midloop operation without core makeup tank actuation, reactor coolant pump trip, CVS letdown isolation, or purification line isolation. With pressurizer level channels less than the P-12 setpoint, the operator can manually block low pressurizer level signal used for these actuations. Concurrent with blocking CMT actuation on low pressurizer level, ADS 4th Stage actuation on Low 2 RCS hot leg level is enabled. Also CVS letdown isolation on Low 1 RCS hot leg level is enabled. When the pressurizer level is above the P-12 setpoint, the pressurizer level signal is automatically enabled and a confirmatory open signal is issued to the isolation valves on the CMT cold leg balance lines. This Function is required to be OPERABLE in MODES 1, 2, 3, 4, 5, and 6.

18.fe. RCS Pressure, P-19

The P-19 interlock is provided to permit water solid conditions (i.e., when the pressurizer water level is >92%) in lower MODES without automatic isolation of the CVS makeup pumps. With RCS pressure below the P-19 setpoint, the operator can manually block CVS isolation on High 2 pressurizer water level, and block Passive RHR actuation and Pressurizer Heater Trip on High 3 pressurizer water level. When RCS pressure is above the P-19 setpoint, these Functions are automatically unblocked. This Function is required to be OPERABLE IN MODES 1, 2, 3, and 4 with the RCS not being cooled by the RNS. When the RNS is cooled by the RNS, the RNS suction relief valve provides the required overpressure protection (LCO 3.4.14).

18.f. Reactor Trip Breaker Open, P-3

~~The P-3 interlock is provided to permit the block of automatic Safeguards Actuation after a predetermined time interval following automatic Safeguards Actuation.~~

~~The reactor trip breaker position switches that provide input to the P-3 interlock only function to energize or de-energize (open or close) contacts. Therefore, this Function does not have an adjustable Trip Setpoint.~~

19. Containment Air Filtration System Isolation

Some DBAs such as a LOCA may release radioactivity into the containment where the potential would exist for the radioactivity to be released to the atmosphere and exceed the acceptable site dose limits. Isolation of the Containment Air Filtration System provides protection to prevent radioactivity inside containment from being released to the atmosphere.

19.a. Containment Radioactivity – High 1

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Three channels of Containment Radioactivity – High 1 are required to be OPERABLE in MODES 1, 2, 3, and 4 with the RCS not being cooled by the RNS, when the potential exists for a LOCA, to protect against radioactivity inside containment being released to the atmosphere. These Functions are not required to be OPERABLE in MODE 4 with the RCS being cooled by the RNS or MODES 5 and 6, because any DBA release of radioactivity into the containment in these MODES would not require containment isolation.

19.b. Containment Isolation (Function 3)

Containment Air Filtration System Isolation is also initiated by all Functions that initiate Containment Isolation. The Containment Air Filtration System Isolation requirements for these Functions are the same as the requirements for the Containment Isolation. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 3, Containment Isolation, is referenced for initiating Functions and requirements.

20. Main Control Room Isolation and Air Supply Initiation

Isolation of the main control room and initiation of the air supply provides a protected environment from which operators can control the plant following an uncontrolled release of radioactivity. This Function is required to be OPERABLE in MODES 1, 2, 3, and 4, and during movement of irradiated fuel because of the potential for a fission product release following a fuel handling accident, or other DBA.

20.a. Control Room Air Supply Radiation – High 2

Two radiation monitors are provided on the main control room air intake. If either monitor exceeds the High 2 setpoint, control room isolation is actuated.

20.b. Pressurizer Pressure – Low

This signal provides protection against a potential release of radioactivity due to a LOCA.

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). Therefore, the ~~Trip Setpoint~~ NTSPNTS reflects the inclusion of both steady-state and adverse environmental instrument uncertainties.

The LCO requires four channels of Pressurizer Pressure – Low to be OPERABLE in MODES 1, 2, and 3 (above P-11, when the RCS boron concentration is below that necessary to meet the SDM requirements at an RCS temperature of 200°F), to mitigate the consequences of a high energy line rupture inside containment. Four

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure no single random failure will disable this trip Function. This signal may be manually blocked by the operator below the P-11 setpoint.

This Function is not required to be OPERABLE in MODE 3 below the P-11 setpoint.

21. Auxiliary Spray and Purification Line Isolation

The CVS maintains the RCS fluid purity and activity level within acceptable limits. The CVS purification line receives flow from the discharge of the RCPs. The CVS also provides auxiliary spray to the pressurizer. To preserve the reactor coolant pressure in the event of a break in the CVS loop piping, the purification line and the auxiliary spray line are isolated on a pressurizer water level Low 1 setpoint. This helps maintain reactor coolant system inventory.

21.a. Pressurizer Water Level – Low 1

A signal to isolate the purification line and the auxiliary spray line is generated upon the coincidence of pressurizer level below the Low 1 setpoint in any two-out-of-four divisions. This Function is required to be OPERABLE in MODES 1 and 2 to help maintain RCS inventory. In MODES 3, 4, 5, and 6, this Function is not needed for accident detection and mitigation.

21.b. Manual Chemical Volume Control System Makeup Isolation (Function 16.e)

The Auxiliary Spray and Purification Line Isolation is also initiated by the Manual Chemical Volume Control System Makeup Isolation Function. The requirements for this Function are the same as the requirements for Manual Chemical Volume Control System Makeup Isolation (Function 16.e), but only apply in MODES 1 and 2.

Therefore, the requirements are not repeated in Table 3.3.2-1, and Function 16.e is referenced for all requirements.

22. IRWST Injection Line Valve Actuation

The PXS provides core cooling by gravity injection and recirculation for decay heat removal following an accident. The IRWST has two injection flow paths. Each injection path includes a normally open motor operated isolation valve and two parallel lines, each isolated by one check valve and one squib valve in series. Manual initiation or automatic actuation on an ADS Stage 4 actuation signal or a coincident RCS Loops 1 and 2 Hot Leg Level-Low will generate a signal to open the IRWST injection line and actuate IRWST injection.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

22.a. Manual Initiation

The operator can open IRWST injection line valves at any time from the main control room by actuating two IRWST injection actuation switches in the same actuation set. There are two sets of two switches each in the main control room. This Function is required to be OPERABLE in MODES 1, 2, 3, 4, 5, and 6.

22.b. ADS Stage 4 Actuation (Function 10)

An open signal will be issued to the IRWST injection isolation valves when an actuation signal is issued to the ADS Stage 4 valves. The requirements for this function are the same as the requirements for the ADS Stage 4 Actuation Function. Therefore, the requirements are not repeated in Table 3.3.2-1. Instead, Function 10 is referenced for all initiating functions and requirements.

23. IRWST Containment Recirculation Valve Actuation

The PXS provides core cooling by gravity injection and recirculation for decay heat removal following an accident. The PXS has two containment recirculation flow paths. Each path contains two parallel flow paths, one path is isolated by a motor operated valve in series with a squib valve and one path is isolated by a check valve in series with a squib valve. Manual initiation or automatic actuation on a Safeguards Actuation signal coincident with a Low 3 level signal in the IRWST will open these valves.

23.a. Manual Initiation

The operator can open the containment recirculation valves at any time from the main control room by actuating two containment recirculation actuation switches in the same actuation set. There are two sets of two switches each in the main control room. This Function is required to be OPERABLE in MODES 1, 2, 3, 4, 5, and 6.

23.b. ADS Stage 4 Actuation Coincident with IRWST Level – Low 3

A low IRWST level coincident with a ADS Stage 4 Actuation signal will open the containment recirculation valves. Four channels are provided to permit one channel to be in trip or bypass indefinitely and still ensure that no single random failure will disable this trip Function. This Function is required to be OPERABLE in MODES 1, 2, 3, 4, 5, and 6, except when the ADS Stage 4 valves are open or an equivalent relief area is open. The required ADS valves or equivalent relief area are specified in LCO 3.4.12, ADS – Shutdown, RCS Intact and LCO 3.4.13, ADS – Shutdown, RCS Open.

24. Refueling Cavity Isolation

The containment isolation valves in the lines between the refueling cavity and the Spent Fuel Pool Cooling System are isolated on a Low spent fuel pool level.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

24.a. Spent Fuel Pool Level – Low

In the event of a leak in the non-safety Spent Fuel Pool Cooling System, closure of the containment isolation valves on low spent fuel pool level in two of three channels will terminate draining of the refueling cavity. Since the transfer canal is open in MODE 6, the spent fuel pool level is the same as the refueling cavity.

Draining of the spent fuel pool, directly, through a leaking Spent Fuel Pool Cooling System is limited by the location of the suction piping, which is near the top of the pool. Therefore, closure of the containment isolation valves between the refueling cavity and the Spent Fuel Pool Cooling System is sufficient to terminate refueling cavity and spent fuel pool leakage through the Spent Fuel Pool Cooling System. This Function is required in MODE 6 to maintain water inventory in the refueling cavity.

25. ESF Logic

This LCO requires four sets of ESF coincidence logic, each set with one battery backed logic group OPERABLE to support automatic actuation. These logic groups are implemented as processor based actuation subsystems. The ESF coincidence logic provides the system level logic interfaces for the divisions.

25.a. Coincidence Logic

If one division of battery backed coincidence logic is OPERABLE, an additional single failure will not prevent ESF actuations because three divisions will still be available to provide redundant actuation for all ESF Functions. This Function is required to be OPERABLE in MODES 1, 2, 3, 4, 5, and 6.

26. ESF Actuation

This LCO requires that for each division of ESF actuation, one battery backed logic group be OPERABLE to support both automatic and manual actuation. The ESF actuation subsystems provide the logic and power interfaces for the actuated components.

26.a. Actuation Subsystem

If one battery backed logic group is OPERABLE for the ESF actuation subsystem in all four divisions, an additional single failure will not prevent ESF actuations because ESF actuation subsystems in the other three divisions are still available to provide redundant actuation for ESF Functions. The remaining cabinets in the division with a failed ESF actuation cabinet are still OPERABLE and will provide their ESF Functions. This Function is required to be

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

OPERABLE in MODES 1, 2, 3, 4, 5, and 6.

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

27. Pressurizer Heater Trip

Pressurizer heaters are automatically tripped upon receipt of a core makeup tank operation signal or a Pressurizer Water Level – High 3 signal. This pressurizer heater trip reduces the potential for steam generator overfill and automatic ADS Stages 1, 2, and 3 actuation for a steam generator tube rupture event. Automatically tripping the pressurizer heaters reduces the pressurizer level swell for certain non-LOCA events such as loss of normal feedwater, inadvertent CMT operation, and CVS malfunction resulting in an increase in RCS inventory. For small break LOCA analysis, tripping the pressurizer heaters supports depressurization of the RCS following actuation of the CMTs.

27.a. CMT Actuation (Function 2)

A signal to trip the pressurizer heaters is generated on a CMT actuation signal. The requirements for this function are the same as the requirements for the CMT Actuation Function, except this function is only required to be OPERABLE in MODES 1, 2, and 3, and in MODE 4 when the RCS is not being cooled by the RNS and above the P-19 (RCS pressure) interlock. Therefore, the requirements are not repeated in Table 3.3.2.1. Instead, Function 2 is referenced for initiating Functions and requirements and SR 3.3.2.9 also applies.

27.b. Pressurizer Water Level – High 3

A signal to trip the pressurizer heaters is generated when the pressurizer water level reaches its High 3 setpoint. This signal provides protection against a pressurizer overfill following an inadvertent core makeup tank actuation with consequential loss of offsite power. This Function is automatically unblocked when RCS pressure is above the P-19 setpoint. This Function is required to be OPERABLE in MODES 1, 2, and 3, and in MODE 4 when the RCS is not being cooled by the RNS and above the P-19 (RCS pressure) interlock. This Function is not required to be OPERABLE in MODES 5 and 6 because it is not required to mitigate DBA in these MODES.

28. Chemical and Volume Control System Letdown Isolation

The CVS provides letdown to the liquid radwaste system to maintain the pressurizer level. To help maintain RCS inventory in the event of a LOCA, the CVS letdown line is isolated on a Low 1 hot leg level signal in either of the RCS hot leg loops. This Function is required to be OPERABLE in MODE 4 with the RCS being cooled by the RNS. This Function is also required to be OPERABLE in MODE 5, and in MODE 6 with the water level < 23 feet above the top of the reactor vessel flange.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

28.a. Hot Leg Level – Low 1

A signal to isolate the CVS letdown valves is generated upon the occurrence of a Low 1 hot leg level in either of the two RCS hot leg loops. This helps to maintain reactor system inventory in the event of a LOCA. This function can be blocked in Modes 1, 2 and 3 and is automatically reset when P-12 is first activated. This function may be manually reset as well. These letdown valves are also closed by all of the initiating Functions and requirements that generate the Containment Isolation Function in Function 3.

29. SG Power Operated Relief Valve and Block Valve Isolation

The Function of the SG Power Operated Relief Valve and Block Valve Isolation is to ensure that the SG PORV flow paths can be isolated during a SG tube rupture (SGTR) event. The PORV flow paths must be isolated following a SGTR to minimize radiological releases from the ruptured steam generator into the atmosphere. The PORV flow path is assumed to open due to high secondary side pressure, during the SGTR. Dose analyses take credit for subsequent isolation of the PORV flow path by the PORV and/or the block valve which receive a close signal on low steam line pressure. Additionally, the PORV flow path can be isolated manually.

This Function is required to be OPERABLE in MODES 1, 2, 3, and 4 with the RCS cooling not being provided by the Normal Residual Heat Removal System (RNS). In MODE 4 with the RCS cooling being provided by the RNS and in MODES 5 and 6, the steam generators are not being used for RCS cooling and the potential for a SGTR is minimized due to the reduced mass and energy in the RCS and steam generators.

29.a. Manual Initiation

Manual initiation of SG Power Operated Relief Valve and Block Valve Isolation can be accomplished from the control room. There are two switches in the control room and either switch can close the SG PORVs and PORV block valves. The LCO requires two switches to be OPERABLE.

29.b Steam Line Pressure – Low

Steam Line Pressure – Low provides closure of the PORV flow paths in the event of SGTR in which the PORV(s) open, to limit the

radiological releases from the ruptured steam generator into the atmosphere. This Function is anticipatory in nature and has a typical leading/lag ratio of 50/5.

The LCO requires four channels of Steam Line Pressure – Low Function to be OPERABLE in MODES 1, 2, 3, and 4 with the RCS cooling not being provided by the RNS. Four channels are provided in each steam line to permit one channel to be in trip or bypass indefinitely and still ensure that no single random failure will disable this Function.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

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

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. The Completion Time(s) of the inoperable equipment of a Function will be tracked separately for each Function starting from the time the Condition was entered for that Function.

A second Note has been added to provide clarification that, more than one Condition is listed for each of the Functions in Table 3.3.2-1. If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the second Condition shall be entered.

In the event a channel's ~~Nominal Trip Setpoint as found~~ condition is ~~not met outside the as-found tolerance described in the SGPSP, or the channel is not functioning as required~~, or the transmitter, or the Protection and Safety Monitoring System Division, associated with a specific Function is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the LCO Condition(s) entered for the particular protection Function(s) affected. When the Required Channels are specified only on a per steam line, per loop, per SG, basis, then the Condition may be entered separately for each steam line, loop, SG, etc., as appropriate.

When the number of inoperable channels in a trip function exceed those specified in one or other related Conditions associated with a trip function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 in MODES 1 through 4 and LCO 3.0.8 for MODE 5 and 6 should be immediately entered if applicable in the current MODE of operation.

A.1

Condition A is applicable to all ESFAS protection Functions. Condition A addresses the situation where one or more channels/divisions 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 and B.2

With one or two channels or divisions inoperable, one affected channel or division must be placed in a bypass or trip condition within 6 hours. If one channel or division is bypassed, the logic becomes two-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels or divisions will not prevent the protective function.) If one channel or division is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels or divisions will not prevent the protective function.) If one channel or division is

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

bypassed and one channel or division is tripped, the logic becomes one-out-of-two, while still meeting the single failure criterion. The 6 hours allowed to place the inoperable channel(s) or division(s) in the bypassed or tripped condition is justified in Reference 6.

C.1

With one channel inoperable, the affected channel must be placed in a bypass condition within 6 hours. The 6 hours allowed to place the inoperable channel in the bypass condition is justified in Reference 6. If one CVS isolation channel is bypassed, the logic becomes one-out-of-one. A single failure in the remaining channel could cause a spurious CVS isolation. Spurious CVS isolation, while undesirable, would not cause an upset plant condition.

D.1

With one required division inoperable, the affected division must be restored to OPERABLE status within 6 hours.

Condition D applies to one inoperable required division of the P-3 & P-4 Interlocks (Functions 18.a and 18.f). With one required division inoperable, the 2 remaining OPERABLE divisions are capable of providing the required interlock function, but without a single failure. The P-3 & P-4 Interlocks are enabled when RTBs in two divisions are detected as open. The status of the other inoperable, non-required P-3 & P-4 division is not significant, since P-3 & P-4 divisions cannot be tripped or bypassed. In order to provide single failure tolerance, 3 required divisions must be OPERABLE.

Condition D also applies to one inoperable division of ESF coincidence logic or ESF actuation (Functions 25 and 26). The ESF coincidence logic and ESF actuation divisions are inoperable when their associated battery-backed subsystem is inoperable. With one inoperable division, the 3 remaining OPERABLE divisions are capable of mitigating all DBAs, but without a single failure.

The 6 hours allowed to restore the inoperable division is reasonable based on the capability of the remaining OPERABLE divisions to mitigate all DBAs and the low probability of an event occurring during this interval.

E.1

Condition E is applicable to manual initiation of:

- Safeguards Actuation;
- CMT Actuation;
- Containment Isolation;
- Steam Line Isolation;
- Main Feedwater Control Valve Isolation;
- Main Feedwater Pump Trip and Valve Isolation;

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

- ADS Stages 1, 2, & 3 Actuation;
- ADS Stage 4 Actuation;
- Passive Containment Cooling Actuation;
- PRHR Heat Exchanger Actuation;
- CVS Makeup Line Isolation;
- IRWST Injection Line Valve Actuation;
- IRWST Containment Recirculation Valve Actuation;
- Steam Generator PORV Flow Path Isolation.

This Action addresses the inoperability of the system level manual initiation capability for the ESF Functions listed above. With one switch or switch set inoperable for one or more Functions, the system level manual initiation capability is reduced below that required to meet single failure criterion. Required Action E.1 requires the switch or switch set for system level manual initiation to be restored to OPERABLE status within 48 hours. The specified Completion Time is reasonable considering that the remaining switch or switch set is capable of performing the safety function.

F.1, F.2.1, and F.2.2

Condition F is applicable to the Main Control Room (MCR) isolation and air supply initiation function which has only two channels of the initiating process variable. With one channel inoperable, the logic becomes one-out-of-one and is unable to meet single failure criterion. Restoring all channels to OPERABLE status ensures that a single failure will not prevent the protective Function.

Alternatively, radiation monitor(s) which provide equivalent information and control room isolation and air supply initiation manual controls may be verified to be OPERABLE. These provisions for operator action can replace one channel of radiation detection and system actuation. The 72 hour Completion Time is reasonable considering that there is one remaining channel OPERABLE and the low probability of an event occurring during this interval.

G.1

With one switch, switch set, channel, or division inoperable, the system level initiation capability is reduced below that required to meet single failure criterion. Therefore, the required switch, switch set, channel, and division must be returned to OPERABLE status within 72 hours. The specified Completion Time is reasonable considering the remaining switch, switch set, channel, or division is capable of performing manual initiation.

H.1

With one channel inoperable, the inoperable channel must be placed in a trip condition within 6 hours.

Condition H is applicable to the PRHR heat exchangers actuation on SG Narrow

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Range Water Level Low coincident with Startup Feedwater Flow Low (Function 13.b). With one startup feedwater channel inoperable, the inoperable channel must be placed in a trip condition within 6 hours. If one channel is tripped, the interlock condition is satisfied. Condition H is also applicable to Refueling Cavity Isolation (Function 24.a). With one of the three spent fuel pool level channels inoperable, the inoperable channel must be placed in a trip condition within 6 hours. If one channel is tripped, the logic becomes one-out-of-two, while still meeting the single failure criterion. The specified Completion Time is reasonable considering the time required to complete this action.

I.1 and I.2

Condition I applies to IRWST containment recirculation valve actuation on safeguards actuation coincident with IRWST Level Low 3 (Function 23.b). With one or two channels inoperable, one affected channel must be placed in a bypass or trip condition within 6 hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is bypassed and one channel is tripped, the logic becomes one-out-of-two, while still meeting the single failure criterion. The 6 hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference 6.

J.1 and J.2

Condition J applies to the P-6, P-11, P-12, and P-19 interlocks. With one or two required channel(s) inoperable, the associated interlock must be verified to be in its required state for the existing plant condition within 1 hour, or any Function channels associated with the inoperable interlock(s) placed in a bypassed condition within 7 hours. Verifying the interlock state manually accomplishes the interlock role.

If one interlock channel is inoperable, the associated Function(s) must be placed in a bypass or trip condition within 7 hours. If one channel is bypassed, the logic becomes two-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.) If one channel is tripped, the logic becomes one-out-of-three, while still meeting the single failure criterion. (A failure in one of the three remaining channels will not prevent the protective function.)

If two interlock channels are inoperable, one channel of the associated Function(s) must be bypassed and one channel of the associated Function(s) must be tripped. In this state, the logic becomes one-out-of-two, while still meeting the single failure criterion. The 7 hours allowed to place the inoperable channel(s) in the bypassed or tripped condition is justified in Reference 6.

K.1

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

LCO 3.0.8 is applicable while in MODE 5 or 6. Since irradiated fuel assembly movement can occur in MODE 5 or 6, the ACTIONS have been modified by a Note stating that LCO 3.0.8 is not applicable. If moving irradiated fuel assemblies while in MODE 5 or 6, the fuel movement is independent of shutdown reactor operations. Entering LCO 3.0.8 while in MODE 5 or 6 would require the optimization of plant safety, unnecessarily. Condition K is applicable to the MCR Isolation and Air Supply Initiation (Function 20), during movement of irradiated fuel assemblies. If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the plant must suspend movement of the irradiated fuel assemblies immediately. The required action suspends activities with potential for releasing radioactivity that might enter the MCR. This action does not preclude the movement of fuel to a safe position.

L.1

If the required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 3 within 6 hours. The allowed time is reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner without challenging plant systems.

M.1 and M.2

If the Required Action and associated Completion Time of the first condition listed in Table 3.3.2-1 is not met, the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 3 within 6 hours and in MODE 4 within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner without challenging plant systems.

N.1 and N.2

If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 3 within 6 hours and in MODE 4 with the RCS being cooled by the RNS within 24 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner without challenging plant systems.

O.1 and O.2

If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 3 within 6 hours and in MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner without challenging

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

plant systems.

P.1, P.2.1, and P.2.2

If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 cannot be met, the plant must be placed in a condition where the instrumentation Function for valve isolation is no longer needed. This is accomplished by isolating the affected flow path(s) within 24 hours. By isolating the flow path from the demineralized water storage tank to the RCS, the need for automatic isolation is eliminated.

To assure that the flow path remains closed, the flow path shall be isolated by the use of one of the specified means (P.2.1) or the flow path shall be verified to be isolated (P.2.2). A means of isolating the affected flow path(s) includes at least one closed and deactivated automatic valve, closed manual valve, blind flange, or check valve with flow through the valve secured within 7 days. If one of the P.2.1 specified isolation means is not used, the affected flow path shall be verified to be isolated once per 7 days.

This action is modified by a Note allowing the flow path(s) to be unisolated intermittently under administrative control. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the control room. In this way the flow path can be rapidly isolated when a need for flow path isolation is indicated.

Q.1, Q.2.1, and Q.2.2

If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the plant must be placed in a condition where the instrumentation Function for valve isolation is no longer needed. This is accomplished by isolating the affected flow path by the use of at least one closed manual or closed and deactivated automatic valve within 6 hours.

If the flow path is not isolated within 6 hours the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 3 within 12 hours and in MODE 4 within 18 hours.

This action is modified by a Note allowing the flow path(s) to be unisolated intermittently under administrative control. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the control room. In this way the flow path can be rapidly isolated when a need for flow path isolation is indicated.

R.1, R.2.1.1, R.2.1.2, and R.2.2

If the Required Action and associated Completion Time of the first Condition given in Table 3.3.2-1 is not met the plant must be placed in a condition in which the likelihood and consequences of an event are minimized. This is accomplished by placing the plant in MODE 3 within 6 hours and isolating the affected flow path(s) within 12 hours. To assure that the flow path remains closed, the affected flow path shall be verified to be isolated once per 7 days.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

If the flow path is not isolated within 12 hours the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 4 with the RCS cooling provided by the RNS within 30 hours. The allowed Completion Time is reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner without challenging plant systems.

This action is modified by a Note allowing the flow path(s) to be unisolated intermittently under administrative control. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the control room. In this way the flow path can be rapidly isolated when a need for flow path isolation is indicated.

S.1, S.2.1.1, S.2.1.2, S.2.1.3, and S.2.2

If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the plant must be placed in a condition in which the likelihood and consequences of an event are minimized. This is accomplished by placing the plant in MODE 3 within 6 hours and in MODE 4 with the RCS cooling provided by the RNS within 24 hours. Once the plant has been placed in MODE 4 the affected flow path must be isolated within 30 hours. To assure that the flow path remains closed, the affected flow path shall be verified to be isolated once per 7 days.

If the flow path is not isolated within 12 hours, the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 5 within 42 hours. The allowed Completion Time is reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner without challenging plant systems.

This action is modified by a Note allowing the flow path(s) to be unisolated intermittently under administrative control. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the control room. In this way the flow path can be rapidly isolated when a need for flow path isolation is indicated.

T.1.1, T.1.2.1, T.1.2.2, T.2.1, and T.2.2

If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the plant must be placed in a Condition in which the likelihood and consequences of an event are minimized. This is accomplished by isolating the affected flow path within 6 hours and isolating the affected flow path(s) by the use of at least one closed and deactivated automatic valve, closed manual valve, blind flange, or check valve with flow through the valve secured within 7 days or verify the affected flow path is isolated once per 7 days.

If the flow path is not isolated within 6 hours the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 3 within 12 hours and in MODE 5 within 42 hours. The allowed Completion Time is reasonable, based on operating experience, to reach the

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

required plant conditions from full power conditions in an orderly manner without challenging plant systems.

This action is modified by a Note allowing the flow path(s) to be unisolated intermittently under administrative control. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the control room. In this way the flow path can be rapidly isolated when a need for flow path isolation is indicated.

U.1 and U.2

If the Required Action and the associated Completion Time of the first Condition given in Table 3.3.2-1 is not met, and the required switch or switch set is not restored to OPERABLE status within 48 hours, the plant must be placed in a condition in which the likelihood and consequences of an event are minimized. This is accomplished by placing the plant in MODE 5 within 12 hours. Once in MODE 5, action shall be immediately initiated to open the RCS pressure boundary and establish $\geq 20\%$ pressurizer level. The 12 hour Completion Time is a reasonable time to reach MODE 5 from MODE 4 with RCS cooling provided by the RNS (approximately 350°F) in an orderly manner without challenging plant systems. Opening the RCS pressure boundary assures that cooling water can be injected without ADS operation. Filling the RCS to provide $\geq 20\%$ pressurizer level minimizes the consequences of a loss of decay heat removal event.

V.1, V.2.1, and V.2.2

If the Required Action and the associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met and the required channel(s) is not bypassed within 6 hours, the inoperable channel(s) must be restored within 168 hours. The 168 hour Completion Time is based on the ability of the two remaining OPERABLE channels to provide the protective Function even with a single failure.

If the channel(s) is not restored within the 168 hour Completion Time, the plant shall be placed in a condition in which the likelihood and consequences of an event are minimized. This is accomplished by placing the plant in MODE 5 within 180 hours (the next 12 hours). Once in MODE 5, action shall be initiated to open the RCS pressure boundary and establish $\geq 20\%$ pressurizer level. The 12 hours is a reasonable time to reach MODE 5 from MODE 4 with RCS cooling provided by the RNS (approximately 350°F) in an orderly manner without challenging plant systems.

Opening the RCS pressure boundary assures that cooling water can be injected without ADS operation. Filling the RCS to provide $\geq 20\%$ pressurizer level minimizes the consequences of a loss of decay heat removal event.

W.1, W.2, W.3, and W.4

If the Required Action and the associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met while in MODES 5 and 6, the plant must be

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

placed in a MODE in which the likelihood and consequences of an event are minimized. This is accomplished by immediately initiating action to be in MODE 5 with the RCS open and $\geq 20\%$ pressurizer level or to be in MODE 6 with the upper internals removed. The flow path from the demineralized water storage tank to the RCS shall also be isolated by the used of at least one closed and de-activated automatic valve or closed manual valve. These requirements minimize the consequences of the loss of decay heat removal by maximizing RCS inventory and maintaining RCS temperature as low as practical. Additionally, the potential for a criticality event is minimized by isolation of the demineralized water storage tank and by suspension of positive reactivity additions.

X.1, X.2, and X.3

If the Required Action and the associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met while in MODES 5 and 6, the plant must be placed in a MODE in which the likelihood and consequences of an event are minimized. This is accomplished by immediately initiating action to be in MODE 5 with the RCS open and $\geq 20\%$ pressurizer level or to be in MODE 6 with the upper internals removed. These requirements minimize the consequences of the loss of decay heat removal by maximizing RCS inventory and maintaining RCS temperature as low as practical. Additionally, the potential for a criticality event is minimized by suspension of positive reactivity additions.

Y.1, Y.2, Y.3, and Y.4

If the Required Action and the associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met while in MODE 4, with RCS cooling provided by the RNS, MODE 5, or MODE 6, the plant must be placed in a MODE in which the likelihood and consequences of an event are minimized. If in MODE 4, this is accomplished by placing the plant in MODE 5 within 12 hours. The 12 hours is a reasonable time to reach MODE 5 from MODE 4 with RCS cooling provided by the RNS (approximately 350°F) in an orderly manner without challenging plant systems.

If in MODE 4 or 5, Required Action Y.3 requires initiation of action within 12 hours to close the RCS pressure boundary and establish $\geq 20\%$ pressurizer level. The 12 hour Completion Time allows transition to MODE 5 in accordance with Y.2, if needed, prior to initiating action to open the RCS pressure boundary.

If in MODE 6, Required Action Y.4 requires the plant to be maintained in MODE 6 and initiation of action to establish the reactor cavity water level ≥ 23 feet above the top of the reactor vessel flange.

Required Actions Y.2, Y.3, and Y.4 minimize the consequences of a loss of decay heat removal event by optimizing conditions for RCS cooling in MODE 5 using the PRHR HX or in MODE 6 using IRWST injection. Additionally, maximizing RCS inventory and maintaining RCS temperature as low as practical further minimize the consequences of a loss of decay heat removal event. Closing the RCS pressure boundary in MODE 5 assures that PRHR HX cooling

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

is available. Additionally, the potential for a criticality event is minimized by suspension of positive reactivity additions.

Z.1, Z.2.1, and Z.2.2

If the Required Action and associated Completion Time of the first Condition listed in Table 3.3.2-1 is not met, the plant must be placed in a condition where the instrumentation Function for valve isolation is no longer needed. This is accomplished by isolating the affected flow path by the use of at least one closed manual or closed and deactivated automatic valve within 6 hours.

If the flow path is not isolated within 6 hours, the plant must be placed in a MODE in which the LCO does not apply. This is accomplished by placing the plant in MODE 3 within 12 hours and in MODE 4 with RCS cooling provided by the RNS within 30 hours.

This Action is modified by a Note allowing the flow path(s) to be unisolated intermittently under administrative control. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the control room. In this way the flow path can be rapidly isolated when a need for flow path isolation is indicated.

AA.1.1, AA.1.2.1, AA.1.2.2, AA.2.1, AA.2.2, and AA.2.3

If the Required Action and associated Completion Time of the first condition listed in Table 3.3.2-1 is not met, the plant must be placed in a condition where the instrumentation Function for valve isolation is no longer needed. This is accomplished by isolating the affected flow path within 24 hours. By isolating the CVS letdown flow path from the RCS, the need for automatic isolation is eliminated.

To assure that the flow path remains closed, the flow path shall be isolated by the use of one of the specified means (AA.1.2.1) or the flow path shall be verified to be isolated (AA.1.2.2). A means of isolating the affected flow path includes at least one closed and deactivated automatic valve, closed manual valve, blind flange, or check valve with flow through the valve secured, within 7 days. If one of the P.2.1 specified isolation means is not used, the affected flow path shall be verified to be isolated once per 7 days.

This action is modified by a Note allowing the flow path to be unisolated intermittently under administrative control. These administrative controls consist of stationing a dedicated operator at the valve controls, who is in continuous communication with the control room. In this way the flow path can be rapidly isolated when a need for flow path isolation is indicated.

If the flow path cannot be isolated in accordance with Required Actions AA.1.1, AA.1.2.1 and AA.1.2.2, the plant must be placed in a MODE in which the likelihood and consequences of an event are minimized. If in MODE 4, this is accomplished by placing the plant in MODE 5 within 12 hours. The 12 hours is a reasonable time to reach MODE 5 from MODE 4 with RCS cooling provided by

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

the RNS (approximately 350°F) in an orderly manner without challenging plant systems.

If in MODE 4 or 5, Required Action AA.2.2 requires initiation of action, within 12 hours, to establish > 20% pressurizer level. The 12 hour Completion Time allows transition to MODE 5 in accordance with AA.2.1, if needed, prior to initiating action to establish the pressurizer level.

If in MODE 6, Required Action AA.2.3 requires the plant to be maintained in MODE 6 and initiation of action to establish the reactor cavity water level ≥ 23 feet above the top of the reactor vessel flange.

Required Actions AA.2.2 and AA.2.3 minimize the consequences of an event by optimizing conditions for RCS cooling in MODE 5 using the PRHR HX or in MODE 6 using IRWST injection.

BB.1 and BB.2

With one channel inoperable, the inoperable channel must be placed in bypass and the hot leg level continuously monitored.

If one channel is placed in bypass, automatic actuation will not occur. Continuous monitoring of the hot leg level provides sufficient information to permit timely operator action to ensure that ADS Stage 4 actuation can occur, if needed to mitigate events requiring RCS makeup, boration, or core cooling. Operator action to manually initiate ADS Stage 4 actuation is assumed in the analysis of shutdown events (Reference 4410). It is also credited in the shutdown PRA (Reference 4211) when automatic actuation is not available.

SURVEILLANCE REQUIREMENTS

The Surveillance Requirements for each ESF Function are identified by the Surveillance Requirements column of Table 3.3.2-1. A Note has been added to the Surveillance Requirement table to clarify that Table 3.3.2-1 determines which Surveillance Requirements apply to which ESF Functions.

SR 3.3.2.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is 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 even something more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

channel is outside the match criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside ~~its~~ **their corresponding** limits.

The Surveillance Frequency is based on operating experience that demonstrates **that** channel failure is rare. Automated operator aids may be used to facilitate performance of the CHANNEL CHECK.

SR 3.3.2.2

SR 3.3.2.2 is the performance of an ACTUATION LOGIC TEST. This test, in conjunction with the ACTUATION DEVICE TEST, demonstrates that the actuated device responds to a simulated actuation signal. The ESF coincidence logic and ESF actuation subsystems within a division are tested every 92 days on a STAGGERED TEST BASIS.

A test subsystem is provided with the protection and safety monitoring system to aid the plant staff in performing the ACTUATION LOGIC TEST. The test subsystem is designed to allow for complete functional testing by using a combination of system self-checking features, functional testing features, and other testing features. Successful functional testing consists of verifying that the capability of the system to perform the safety function has not failed or degraded.

For hardware functions this would involve verifying that the hardware components and connections have not failed or degraded. Generally this verification includes a comparison of the outputs from two or more redundant subsystems or channels.

Since software does not degrade, software functional testing involves verifying that the software code has not changed and that the software code is executing.

To the extent possible, protection and safety monitoring system functional testing is accomplished with continuous system self-checking features and the continuous functional testing features. The ACTUATION LOGIC TEST shall include a review of the operation of the test subsystem to verify the completeness and adequacy of the results.

If the ACTUATION LOGIC TEST ~~can~~ not be completed using the built-in test subsystem, either because of failures in the test subsystem or failures in redundant channel hardware used for functional testing, the ACTUATION LOGIC TEST can be performed using portable test equipment.

The Frequency of every 92 days on a STAGGERED TEST BASIS provides a complete test of all four divisions once per year. This frequency is adequate based on the inherent high reliability of the solid state devices which comprise this equipment; the additional reliability provided by the redundant subsystems; and the use of continuous diagnostic test features, such as deadman timers, memory checks, numeric coprocessor checks, cross-check of redundant subsystems, and tests of timers, counters, and crystal time basis, which will report a failure within these cabinets to the operator.

SR 3.3.2.3

SR 3.3.2.3 is the performance of a TADOT of the manual actuations, initiations,

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

and blocks for various ESF Functions, the reactor trip breaker open (P-3), and the reactor trip (P-4) input from the IPCs. This TADOT is performed every 24 months.

The Frequency is based on the known reliability of the ESF Functions and the multichannel redundancy available, and has been shown to be acceptable through operating experience.

The SR is modified by a Note that excludes verification of setpoints from the TADOT. The functions have no setpoints associated with them.

SR 3.3.2.4

SR 3.3.2.4 is the performance of a CHANNEL CALIBRATION every 24 months or approximately at every refueling. CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor and the IPC. The test is performed in accordance with the SCPSP. If the actual setting of the channel is found to be outside the as-found tolerance, the channel is considered inoperable. This condition of the channel will be further evaluated during performance of the SR. This evaluation will consist of resetting the channel setpoint to the NTS (within the allowed tolerance), and evaluating the channel's response. If the channel is functioning as required and is expected to pass the next surveillance, then the channel is OPERABLE and can be restored to service at the completion of the surveillance. After the surveillance is completed, the channel as-found condition will be entered into the Corrective Action Program for further evaluation. Transmitter calibration must be performed consistent with the assumptions of the setpoint methodology. The difference between the current as-found values and the previous as-left values must be consistent with the transmitter drift allowance used in the setpoint methodology.

The setpoint methodology requires that 30 months drift be used (1.25 times the surveillance calibration interval, 24 months).

The Frequency is based on operating experience and consistency with the refueling cycle.

This Surveillance Requirement is modified by a Note. The Note states that this test should include verification that the time constants are adjusted to the prescribed values where applicable.

SR 3.3.2.5

SR 3.3.2.5 is the performance of a CHANNEL OPERATIONAL TEST (COT) every 92 days. The test is performed in accordance with the SCPSP. If the actual setting of the channel is found to be outside the as-found tolerance, the channel is considered inoperable. This condition of the channel will be further evaluated during performance of the SR. This evaluation will consist of resetting the channel setpoint to the NTS (within the allowed tolerance), and evaluating the channel's response. If the channel is functioning as required and is expected to pass the next surveillance, then the channel is OPERABLE and can be restored to service at the completion of the surveillance. After the surveillance is completed, the channel as-found condition will be entered into the Corrective

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

Action Program for further evaluation.

A COT is performed on each required channel to provide reasonable assurance that the entire channel will perform the intended ESF Function.

A test subsystem is provided with the protection and safety monitoring system to aid the plant staff in performing the COT. The test subsystem is designed to allow for complete functional testing by using a combination of system self-checking features, functional testing features, and other testing features. Successful functional testing consists of verifying that the capability of the system to perform the safety function has not failed or degraded.

For hardware functions this would involve verifying that the hardware components and connections have not failed or degraded. Generally this verification includes a comparison of the outputs from two or more redundant subsystems or channels.

Since software does not degrade, software functional testing involves verifying that the software code has not changed and that the software code is executing.

To the extent possible, protection and safety monitoring system functional testing is accomplished with continuous system self-checking features and the continuous functional testing features. The COT shall include a review of the operation of the test subsystem to verify the completeness and adequacy of the results.

If the COT can not be completed using the built-in test subsystem, either because of failures in the test subsystem or failures in redundant channel hardware used for functional testing, the COT can be performed using portable test equipment.

The 92 day Frequency is based on Reference 6 and the use of continuous diagnostic test features, such as deadman timers, cross-check of redundant channels, memory checks, numeric coprocessor checks, and tests of timers, counters and crystal time bases, which will report a failure within the integrated protection cabinets to the operator.

During the COT, the protection and safety monitoring system cabinets in the division under test may be placed in bypass.

SR 3.3.2.6

This SR ensures the individual channel ESF RESPONSE TIMES are less than or equal to the maximum values assumed in the accident analysis. Individual component response times are not modeled in the analyses. The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the ~~Trip-Setpoint~~NTS value at the sensor, to the point at which the equipment reaches the required functional state (e.g., valves in full open or closed position).

For channels that include dynamic transfer functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer functions set to one with the resulting measured response time compared to the appropriate Chapter 7 (Ref. 2) response time. Alternately, the response time test can be

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

performed with the time constants set to their nominal value provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

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 sensor 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. WCAP-13632-P-A, Revision 2, "Elimination of Pressure Sensor Response Time Testing Requirements" (Ref. 4012), 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 WCAP. Response time verification for other sensor types must be demonstrated by test.

ESF RESPONSE TIME tests are conducted on a 24 month STAGGERED TEST BASIS. Testing of the 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 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.

SR 3.3.2.7

SR 3.3.2.7 is the performance of an ACTUATION DEVICE TEST. This test, in conjunction with the ACTUATION LOGIC TEST, demonstrates that the actuated device responds to a simulated actuation signal. This Surveillance Requirement is applicable to the equipment which is actuated by the Protection Logic Cabinets except squib valves. The OPERABILITY of the actuated equipment is checked by exercising the equipment on an individual basis.

The Frequency of 24 months is based on the need to perform this surveillance during periods in which the plant is shutdown for refueling to prevent any upsets of plant operation.

This Surveillance Requirement is modified by a Note that states that actuated equipment, that is included in the Inservice Test (IST) Program, is exempt from this surveillance. The IST Program provides for exercising of the safety related

valves on a more frequent basis. The results from the IST Program can therefore be used to verify OPERABILITY of the final actuated equipment.

SR 3.3.2.8

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

SR 3.3.2.8 is the performance of an ACTUATION DEVICE TEST, similar to that performed in SR 3.3.2.7, except this Surveillance Requirement is specifically applicable to squib valves. This test, in conjunction with the ACTUATION LOGIC TEST, demonstrates that the actuated device responds to a simulated actuation signal. The OPERABILITY of the squib valves is checked by performing a continuity check of the circuit from the Protection Logic Cabinets to the squib valve.

The Frequency of 24 months is based on the need to perform this surveillance during periods in which the plant is shutdown for refueling to prevent any additional risks associated with inadvertent operation of the squib valves.

SR 3.3.2.9

SR 3.3.2.9 is the performance of an ACTUATION DEVICE TEST. This test, in conjunction with the ACTUATION LOGIC TEST, demonstrates that the actuated device responds to a simulated actuation signal. This Surveillance Requirement is applicable to the circuit breakers which de-energize the power to the pressurizer heaters upon a pressurizer heater trip. The OPERABILITY of these breakers is checked by opening these breakers using the Plant Control System.

The Frequency of 24 months is based on the need to perform this surveillance during periods in which the plant is shutdown for refueling to prevent any upsets of plant operation. This Frequency is adequate based on the use of multiple circuit breakers to prevent the failure of any single circuit breaker from disabling the function and that all circuit breakers are tested.

REFERENCES

1. Chapter 6.0, "Engineered Safety Features."
2. Chapter 7.0, "Instrumentation and Controls."
3. Chapter 15.0, "Accident Analysis."
4. Institute of Electrical and Electronic Engineers, IEEE-603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," June 27, 1991.
5. 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants."
6. APP-GW-GSC-020, "Technical Specification Completion Time and Surveillance Frequency Justification."
7. 10 CFR 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

ESFAS Instrumentation
B 3.3.2

BASES

8. NUREG-1218, "Regulatory Analysis for Resolution of USI A-47," 4/88.
 9. WCAP-16361-P, "Westinghouse Setpoint Methodology for Protection Systems – AP1000," May 2006 (proprietary).
 10. APP-GW-GLR-004 Rev. 0, "AP1000 Shutdown Evaluation Report." July 2002. ~~ESBU-TB-97-01, Westinghouse Technical Bulletin, "Digital Process Rack Operability Determination Criteria," May 1, 1997.~~
 11. Chapter 19.0, "Probabilistic Risk Assessment," Appendix 19E, "Shutdown Evaluation."
 - ~~112.~~ WCAP-13632-P-A (Proprietary) and WCAP-13787-A (Non-Proprietary), Revision 2, "Elimination of Pressure Sensor Response Time Testing Requirements," January 1996.
-

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Attachment 16.3D

Markup of Sections 7.2.1.2.2 and 7.3.1.5.2

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

7. Instrumentation and Controls

AP1000 Design Control Document

7.2.1.1.12 Bypasses of Reactor Trip Functions

Each channel used in reactor trip can be bypassed, as discussed in subsection 7.1.2.9, except for reactor trips resulting from manual initiations. One channel can be bypassed for an indefinite period of time with the normal two-out-of-four trip logic automatically reverting to a two-out-of-three trip logic. Bypassing two or more channels is not allowed.

7.2.1.2 Design Basis for Reactor Trips

This section provides the design bases information on the reactor trip function, including the information required by Section 4 of IEEE-603-1991. Reactor trip is a protective function generated as part of the protection and safety monitoring system. Those design bases relating to the equipment that initiates and accomplishes reactor trips are contained in WCAP-15776 (Reference 2). The design bases presented here concern the variables monitored for reactor trips, the minimum performance requirements in generating the trips, and the requirements placed on reactor trips during various reactor operating modes.

7.2.1.2.1 Design Basis: Generating Station Conditions Requiring Reactor Trip (Paragraph 4.1 of IEEE-603-1991)

The generating station conditions requiring protective actions are analyzed in Chapter 15. Conditions that result in a reactor trip are listed in Table 15.0-6. This table correlates the accident conditions (II, III, or IV events) to each reactor trip.

7.2.1.2.2 Design Basis: Variables, Levels, Ranges, and Accuracies Used in Reactor Trip Functions (Paragraphs 4.1, 4.2, and 4.4 of IEEE-603-1991)

The variables monitored for reactor trips are:

- Neutron flux
- Reactor coolant pump bearing water temperature
- Pressurizer pressure
- Water level in the pressurizer
- Reactor coolant flow in each loop
- Speed of each reactor coolant pump
- Water level in each steam generator
- Cold leg temperature (T_{cold}) in each loop
- Hot leg temperature (T_{hot}) in each loop
- Status of each manual reactor trip control

The ranges, accuracies, and response times for each variable are listed on Table 7.2-1.

A discussion on levels that require reactor trip is contained in subsection 7.2.1.1.

The reactor trip setpoints are maintained by the setpoint program which is described. ~~The allowable values for the limiting safety-related system settings and the trip setpoint for~~

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

7. Instrumentation and Controls

AP1000 Design Control Document

~~reactor trips are~~ in the technical specifications (Chapter 16).

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

7. Instrumentation and Controls

AP1000 Design Control Document

- Main control room supply air radioactivity level
- Reactor coolant pump bearing water temperature
- Startup feedwater flow
- Spent fuel pool level
- Reactor coolant pressure in each of the two hot legs

Subsections 7.3.1.1 and 7.3.1.2 discuss levels that result in engineered safety features actuation. The ~~allowable values for the limiting conditions for operation and the trip setpoints for~~ engineered safety features actuation and trip setpoints are maintained by the setpoint program which is described ~~are given~~ in the technical specifications (Chapter 16).

Ranges, accuracies, and response times for the variables used in engineered safety features actuation are listed in Table 7.3-4. The time response is the maximum allowable time period for an actuation signal to reach the necessary components. It is based on following a step change in the applicable process parameter from 5 percent below to 5 percent above (or vice versa) the actuation setpoint with externally adjustable time delays set to OFF.

7.3.1.5.3 Design Basis: Spatially Dependent Variables Used for Engineered Safety Features Actuation (Paragraph 4.6 of IEEE 603-1991)

Spatially dependent variables are discussed in subsection 7.2.1.2.3.

7.3.1.5.4 Design Basis: Limits for Engineered Safety Features Parameters in Various Reactor Operating Modes (Paragraph 4.3 of IEEE 603-1991)

During startup or shutdown, various engineered safety features actuation can be manually blocked. These functions are listed in Table 7.3-1.

During testing or maintenance of the protection and safety monitoring system, certain channels used for engineered safety features may be bypassed. Although no setpoints are changed for bypassing, the logic is automatically adjusted, as described in subsection 7.3.1.4. The safeguards channels that can be bypassed in the protection and safety monitoring system are listed in Table 7.3-1.

7.3.1.5.5 Design Basis: Engineered Safety Features for Malfunctions, Accidents, Natural Phenomena, or Credible Events (Paragraph 4.7 and 4.8 of IEEE 603-1991)

The accidents that the various engineered safety features are designed to mitigate are detailed in Chapter 15. Table 15.0-6 contains a summary listing of the engineered safety features actuated for various Condition II, III, or IV events. It relies on provisions made to protect equipment against damage from natural phenomena and credible internal events. Consequently, there are no engineered safety features actuated by the protection and safety monitoring system to mitigate the consequences of events such as fires.

Functional diversity is used in determining the actuation signals for engineered safety features. For example, a safeguards actuation signal is generated from high containment pressure, low pressurizer pressure, and low compensated steam line pressure. Engineered

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

7. Instrumentation and Controls

AP1000 Design Control Document

safety features are not normally actuated by a single signal. The extent of this diversity is