B. H. Whitley
Director
Regulatory Affairs

Southern Nuclear
Operating Company, Inc.
42 Inverness Center Parkway
Birmingham, AL 35242
Tel 205.992.7079
Fax 205.992.5296

July 28, 2017

Docket Nos.: 52-025
52-026

ND-17-1280
10 CFR 50.90

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

Southern Nuclear Operating Company
Vogtle Electric Generating Plant Units 3 and 4
Request for License Amendment:
Clarify Technical Specification Definition of Actuation Logic Test and
Add New Actuation Logic Output Test (LAR-17-026)

Ladies and Gentlemen:

Pursuant to 10 CFR 52.98(c) and in accordance with 10 CFR 50.90, Southern Nuclear Operating Company (SNC) requests an amendment to the combined licenses (COLs) for Vogtle Electric Generating Plant (VEGP) Units 3 and 4 (License Numbers NPF-91 and NPF-92, respectively). The requested amendment proposes changes to COL Appendix A, Technical Specifications (TS).

The requested amendment proposed changes to TS Section 1.1 Definition of Actuation Logic Test, adding a new TS Section 1.1 Definition of Actuation Logic Output Test (ALOT), revising existing Surveillance Requirements 3.3.15.1 and 3.3.16.1, and adding new Surveillance Requirements 3.3.15.2 and 3.3.16.2 to implement the new ALOT.

Enclosure 1 provides the description, technical evaluation, regulatory evaluation (including the Significant Hazards Consideration) and environmental considerations for the proposed changes in the License Amendment Request (LAR).

Enclosure 2 provides markups depicting the requested changes to the VEGP Units 3 and 4 licensing basis documents.

Enclosure 3 provides conforming Technical Specification Bases changes for information only.

This letter contains no regulatory commitments. This letter has been reviewed and determined not to contain security related information.

SNC requests NRC staff review and approval of the license amendment by March 30, 2018, to support Operator training updates. Delayed approval of this license amendment could result in a delay in Operator training updates. SNC expects to implement the proposed amendment within thirty days of approval. South Carolina Electric & Gas Company (SCE&G) has stated that the current requested approval date for the expected parallel LAR for Virgil C. Summer Nuclear Station (VCSNS) Unit 2 is July 31, 2018.

In accordance with 10 CFR 50.91, SNC is notifying the State of Georgia of this LAR by transmitting a copy of this letter and its enclosures to the designated State Official.

Should you have any questions, please contact Mr. Christopher L. Whitfield at (205) 992-5071.

I declare under penalty of perjury that the foregoing is true and correct. Executed on the 28th day of July 2017.

Respectfully submitted,

Brian H. Whitley
Director, Regulatory Affairs
Southern Nuclear Operating Company

Enclosures

1) Vogtle Electric Generating Plant (VEGP) Units 3 and 4 – Request for License Amendment: Clarify Technical Specification Definition of Actuation Logic Test and Add New Actuation Logic Output Test (LAR-17-026)

2) Vogtle Electric Generating Plant (VEGP) Units 3 and 4 – Proposed Changes to Licensing Basis Documents (LAR-17-026)

3) Vogtle Electric Generating Plant (VEGP) Units 3 and 4 – Conforming Technical Specification Bases Changes (For Information Only) (LAR-17-026)

cc:

Southern Nuclear Operating Company / Georgia Power Company
Mr. S. E. Kuczynski (w/o enclosures)
Mr. M. D. Rauckhorst
Mr. D. G. Bost (w/o enclosures)
Mr. M. D. Meier (w/o enclosures)
Mr. D. H. Jones (w/o enclosures)
Mr. D. L. McKinney (w/o enclosures)
Mr. T.W. Yelverton (w/o enclosures)
Mr. B. H. Whitley
Mr. J. J. Hutto
Mr. C. R. Pierce
Ms. A. G. Aughtman
Mr. D. L. Fulton
Mr. M. J. Yox
Mr. E. W. Rasmussen
Mr. T. R. Takats
Mr. W. A. Sparkman
Ms. A. C. Chamberlain
Mr. M. K. Washington
Ms. A. L. Pugh
Mr. J. D. Williams
Document Services RTYPE: VND.LI.L00
File AR.01.02.06

Nuclear Regulatory Commission
Mr. W. Jones (w/o enclosures)
Ms. J. Dixon-Herrity
Mr. C. Patel
Mr. W. C. Gleaves
Ms. R. Reyes
Ms. J. M. Heisserer
Mr. B. Davis
Mr. P. Kallan
Mr. G. Khouri
Ms. S. Temple
Ms. V. Ordaz
Mr. T. E. Chandler
Ms. P. Braxton
Mr. T. Brimfield
Mr. C. J. Even
Mr. A. Lerch

State of Georgia
Mr. R. Dunn

<u>Oglethorpe Power Corporation</u>
Mr. M. W. Price
Mr. K. T. Haynes
Ms. A. Whaley

<u>Municipal Electric Authority of Georgia</u>
Mr. J. E. Fuller
Mr. S. M. Jackson

<u>Dalton Utilities</u>
Mr. T. Bundros

<u>Westinghouse Electric Company, LLC</u>
Mr. R. Easterling (w/o enclosures)
Mr. G. Koucheravy (w/o enclosures)
Mr. C. D. Churchman (w/o enclosures)
Mr. P. A. Russ
Mr. M. L. Clyde
Mr. C. A. Castell
Ms. K. Chesko
Mr. J. Hopkins
Mr. D. Hawkins

<u>Other</u>
Mr. S. W. Kline, Bechtel Power Corporation
Ms. L. A. Matis, Tetra Tech NUS, Inc.
Dr. W. R. Jacobs, Jr., Ph.D., GDS Associates, Inc.
Mr. S. Roetger, Georgia Public Service Commission
Ms. S. W. Kernizan, Georgia Public Service Commission
Mr. K. C. Greene, Troutman Sanders
Mr. S. Blanton, Balch Bingham
Mr. R. Grumbir, APOG
Mr. N. R. Kellenberger, South Carolina Electric & Gas Company
Mr. D. Kersey, South Carolina Electric & Gas Company
NDDocumentinBox@duke-energy.com, Duke Energy
Mr. S. Franzone, Florida Power & Light

Southern Nuclear Operating Company

ND-17-1280

Enclosure 1

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

Request for License Amendment:
Clarify Technical Specification Definition of Actuation Logic Test and
Add New Actuation Logic Output Test
(LAR-17-026)

(This Enclosure consists of 21 pages, including this cover page.)

Table of Contents

Pursuant to 10 CFR 52.98(c) and in accordance with 10 CFR 50.90, Southern Nuclear Operating Company (SNC) hereby requests an amendment to Combined License (COL) Nos. NPF-91 and NPF-92 for Vogtle Electric Generating Plant (VEGP) Units 3 and 4, respectively.

1. SUMMARY DESCRIPTION

The requested amendment proposes changes to COL Appendix A, Technical Specifications (TS). The proposed changes modify TS Section 1.1 Definition of ACTUATION LOGIC TEST, add a new TS Section 1.1 Definition of ACTUATION LOGIC OUTPUT TEST (ALOT), revise existing Surveillance Requirements (SR) 3.3.15.1 and SR 3.3.16.1, and add new Surveillance Requirements SR 3.3.15.2 and SR 3.3.16.2 to implement the new ALOT.

The requested amendment proposes changes to the COL Appendix A, plant-specific TS as detailed in Section 2. This enclosure requests approval of the license amendment necessary to implement the COL Appendix A changes.

2. DETAILED DESCRIPTION

The objective of this amendment request is to require complete testing on appropriate intervals, within the limitations and conditions of the TS, of all Protection and Safety Monitoring (PMS) actuation circuitry from the sensors to the end devices.

The ACTUATION LOGIC TEST (ALT), by its Technical Specification Definition, would include the logic circuitry downstream of the Bistable Processor Logic (BPL) "such that it [the ALT] provides component overlap with the actuated device." This would include the voting logic within the ESF Local Coincidence Logic (LCL) cabinets, including the signal path from inputs to the LCL, through the LCL voting logic, out to the Integrated Logic Processor (ILP) inputs, through the Component Interface Module (CIM) outputs in the ESF Actuation logic (Integrated Logic Cabinets, or ILCs), and provide overlap with the actuated device (e.g., valve). The frequency of this testing is currently required by SR 3.3.15.1 and SR 3.3.16.1 at 92 days on a STAGGERED TEST BASIS. However, the portion of the logic downstream of the ESF Coincidence Logic (i.e., ILP to CIM actuation path), as well as the actuated device, should not be tested on the same frequency as the ESF Coincidence Logic. Testing the ILP to CIM actuation path, described in more detail below, can result in actuations that will result in undesired plant transients.

In addition, periodic TS functional tests and Inservice Test Program (IST) testing are performed, which during the execution of the testing, verify that the ILP to CIM actuation path is able to perform its specified safety function. For example, ESF response time tests and IST valve stroke tests exercise the component control logic in the Integrated Logic Processor (ILP) subsystem which includes the ILP to CIM pathway.

A revision to the existing TS Definition of ACTUATION LOGIC TEST is proposed and a new TS Definition of ACTUATION LOGIC OUTPUT TEST (ALOT) is added, along with changes to the ALT Surveillance Requirement wording and new ALOT implementing SR 3.3.15.2 and SR 3.3.16.2. These TS changes are needed to perform the required logic testing on appropriate surveillance test frequencies, as discussed further below in Section 3, Technical Evaluation.

Licensing Basis Change Descriptions

The current TS Section 1.1 Definition of ACTUATION LOGIC TEST reads as follows:

"An ACTUATION LOGIC TEST shall be the application of various simulated or actual input combinations in conjunction with each possible interlock logic state required for OPERABILITY of a logic circuit and the verification of the required logic output. The ACTUATION LOGIC TEST shall be conducted such that it provides component overlap with the actuated device."

That Definition is revised to read:

"An ACTUATION LOGIC TEST shall be the application of various simulated or actual input combinations in conjunction with each possible interlock logic state required for OPERABILITY of a logic circuit and the verification of the required logic output. The ACTUATION LOGIC TEST may be performed by means of any series of sequential, overlapping, or total steps."

A new TS Section 1.1 Definition of ACTUATION LOGIC OUTPUT TEST is added as follows:

"An ACTUATION LOGIC OUTPUT TEST shall be the application of simulated or actual logic signals and the verification of the required component actuation output signals up to, but not including, the actuated device. The ACTUATION LOGIC OUTPUT TEST may be performed by means of any series of sequential, overlapping, or total steps."

Existing Surveillance Requirements SR 3.3.15.1 and SR 3.3.16.1 are revised to read:

"Perform ACTUATION LOGIC TEST on ESF Coincidence Logic."

New SR 3.3.15.2 is added to TS 3.3.15, "ESFAS Actuation Logic – Operating," and new SR 3.3.16.2 is added to TS 3.3.16, "ESFAS Actuation Logic – Shutdown," to read as follows:

"Perform ACTUATION LOGIC OUTPUT TEST on ESF Actuation."

The Frequency for the new SR 3.3.15.2 and SR 3.3.16.2 is proposed to be 24 months. The remaining SRs in TS 3.3.15 and TS 3.3.16 are sequentially renumbered (i.e., SRs 3.3.15.3 through 3.3.15.7 and SRs 3.3.16.3 through 3.3.16.5).

Conforming TS Bases changes, provided for information only, reflect clarifying detail of the PMS architecture and address appropriate testing overlap. The TS Bases changes will be incorporated following NRC approval of the amendment request in accordance with TS 5.5.6, Technical Specifications Bases Control Program.

3. TECHNICAL EVALUATION

The Protection and Safety Monitoring System 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 engineered safety feature (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.

<u>PMS Overview</u>

The four divisions of PMS each consist of the following:

- Field Transmitters and Sensors (non-redundant)
- Nuclear Instrumentation System (NIS) - 1 per division (non-redundant)
- Bistable Processor Logic (BPL) System - 2 BPL subsystems per division (redundant)
- Local Coincidence Logic (LCL) System - 2 LCL subsystems per division (redundant)
- ESF Actuation Subsystem Logic (Integrated Logic Cabinet (ILC)) with:
    - Integrated Logic Processor (ILP) System - 2 ILP subsystems per ILC (redundant)
    - Division A - 3 ILCs
    - Division B - 4 ILCs
    - Division C - 2 ILCs
    - Division D - 4 ILCs
    - Component Interface Modules (CIMs) (non-redundant)

PMS equipment duplication within a division (redundancy) is generally provided for active equipment such as processors and communication hardware. Where provided, redundant sets of equipment within a division are not independent and can be subject to common cause failures. This redundancy is provided to increase plant availability and facilitate surveillance testing.

Within each division, the sensor signals and setpoint bistables are processed in the BPL. The results of the bistable logic (partial ESF actuation signals) are communicated to the LCL subsystems in all divisions.

The LCL subsystems perform the divisional ESF Coincidence Logic voting (e.g., two-out-of-four (2oo4) logic) and other associated logic.

ESF system-level actuation outputs from the LCL are inputs to the ESF Actuation Subsystem logic performed in the ILC for generation of logic commands to the actuated components. Each ILC consists of redundant ILPs and non-redundant CIMs. The ILPs decode the system commands and actuate the final equipment through the CIM interlocking logic specific to each component.

Each CIM provides an actuation signal to its associated actuated device.

<u>ESF Actuation Subsystem (Integrated Logic Cabinet (ILC))</u>

Within each division, the LCLs (i.e., the ESF Coincidence Logic) send ESF system-level actuation outputs to the ESF Actuation Subsystem for generation of logic commands to the actuated devices. The ESF Actuation Subsystem consists of internally redundant ILPs and non-redundant CIMs. The ILPs decode the system commands and actuate the final equipment through the CIM logic specific to each actuated device.

Each of the two ILP processors receives inputs from both ESF Coincidence logic processors (LCLs) in a division. Each ILP uses a Safety Remote Node Controller (SRNC) to communicate with the CIMs and perform the component fan-out for each ESF system-level actuation command. As long as the outputs from both ESF Coincidence logic processors (LCLs) agree that an actuation should occur (i.e., two-out-of-two, or 2oo2, logic), the ILPs will generate actuation signals to the CIMs. If one of the LCLs has no output signal, provides a bad quality signal, or is in test, a good quality signal input to the ILP processors from the other LCL is sufficient to maintain ESF Coincidence Logic OPERABILITY. With a good quality signal from only one LCL, the ILP logic becomes one-out-of-one (1oo1).

Each CIM provides an actuation signal to its associated actuated device. Each CIM receives inputs from both ILPs and produces component actuation signals if the input signals agree (i.e., 2oo2 logic). If one of the ILP processors has no output signal or provides a bad quality signal, a good quality signal input to the CIM from the other ILP processor is sufficient to maintain ESF Actuation OPERABILITY. With a good quality signal from only one ILP processor, the CIM logic becomes 1oo1.

Component Interface Modules (CIMs)

The CIM system is designed to interface an actuated device with the Protection and Safety Monitoring System (PMS) and the Plant Control System (PLS). The CIM priority logic function arbitrates between PMS and PLS demands. The CIM component control logic generates an actuated device demand based on the priority logic outputs and field component feedback signals. Each CIM provides an actuation signal to its associated actuated device. Each CIM receives inputs from both ILPs and produces component actuation signals if the input signals agree (i.e., 2oo2 logic).

Communication with the PMS is accomplished with the Safety Remote Node Controller (SRNC) assembly. The SRNC module accepts a high speed link (HSL) connection. The SRNC communicates with each CIM through a safety bus known as the X bus. The X bus is an independent, bidirectional link between the CIM and the SRNC. The PMS communication link to the CIM is known as the X port.

The PMS can send an open, close, or stop demand. In addition to the PMS demands received over the X port, the PMS can also send three configuration commands to the CIM. These commands are Y port enable, maintenance mode, and output test enable. The CIMs also communicate with the PLS through the Y bus.

A manual control located on each CIM provides local maintenance and test features for each field component.

The CIM has two Z port inputs that can be used for connection with a high priority system. Additional details of the CIM design are provided in Reference 3.

Each CIM provides local control switches that allow the operator to manually test a component. This method of testing a component does not verify the entire safety path; only the connection from the CIM to the field component.

When the newly defined ALOT is performed, a test signal is simultaneously injected into both ILPs, satisfying the ILP 2oo2 coincidence logic and causing the CIM to send a component control signal to the component actuator. The ALOT should be performed only when the plant is shut down to preclude actuations of end devices that, in many cases would produce unacceptable plant perturbations such as reactor trip, ESF actuations, and various other plant transient initiators. Testing one ILP in a division at a time which would result in a partial ESF actuation and leave the plant vulnerable to a single failure, could lead to the same unacceptable plant perturbations. During this test, logic signals are injected into the system level commands processed by the ILPs. Since system level commands may feed multiple CIMs in an ILC, more than one CIM may be actuated by this test. To prevent any CIMs that are not the subject of the test from being actuated, they can be placed in local control mode.

PMS Testing

The Engineering Safety Features Actuation System (ESFAS) PMS testing overlap is shown in the table below, for the proposed change that moves a portion of the testing from the ALT to the new ACTUATION LOGIC OUTPUT TEST (ALOT). As currently defined, the ALT scope includes hardware being proposed to be tested in the ALOT row.

Support TS Definition	**Hardware Tested**	**Comments**
CHANNEL CALIBRATION (CAL)	Sensor/Transmitter Analog to Digital (A/D) Converters ESF Bistable Processor Logic (BPL)	Covers signal path from sensor/transmitter, through A/D Converters, through the BPL, to actuation status inputs in each divisional LCL (CAL includes sensor calibration and includes COT testing scope. Overlaps with ALT.)
CHANNEL OPERATIONAL TEST (COT)	ESF Bistable Processor Logic (BPL)	Covers bistable logic (Signal path through the BPL, to actuation status inputs in each divisional LCL)
ACTUATION LOGIC TEST (ALT)	ESF Local Coincidence Logic (LCL)	Covers voting logic (Signal path from inputs to the LCL, through the LCL voting logic, to the ILP inputs. Overlaps with CAL and with ALOT.)
ACTUATION LOGIC OUTPUT TEST (ALOT)	ESF Actuation Subsystem Logic	New ALOT covers ESF Actuation Logic and tests both of the redundant signal paths from inputs to the ILPs through the CIM logic and CIM output driver circuits. Overlaps with ALT and actuated device surveillances.

N/A	Actuated Devices (except squib actuated devices)	Functional tests of actuated devices with overlap via the ACTUATION LOGIC OUTPUT TEST.
N/A	Squib Valves	Continuity check of squib valves performed in accordance with SR 3.4.11.5 and SR 3.5.6.9. Overlaps with ALOT.

Logic Testing Overlap

PMS testing is covered under defined terms and implementing Surveillance Requirements in the Technical Specifications.

The CHANNEL OPERATIONAL TEST is defined as:

> "A COT shall be the injection of a simulated or actual signal into the channel as close to the sensor as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY. The COT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for channel OPERABILITY such that the setpoints are within the necessary range and accuracy. The COT may be performed by means of any series of sequential, overlapping, or total channel steps."

The ACTUATION LOGIC TEST is currently defined as:

> "An ACTUATION LOGIC TEST shall be the application of various simulated or actual input combinations in conjunction with each possible interlock logic state required for OPERABILITY of a logic circuit and the verification of the required logic output. The ACTUATION LOGIC TEST shall be conducted such that it provides component overlap with the actuated device."

To meet the existing TS Section 1.1 Definition, the ACTUATION LOGIC TEST (ALT) is required to test the entire logic circuitry downstream of the BPLs, from the ESF Local Coincidence Logic (LCL) through the Component Interface Module (CIM) outputs in the ESF Actuation logic, and provide overlap with the actuated device. The current ALT Frequency (SR 3.3.15.1 and SR 3.3.16.1) is 92 days on a STAGGERED TEST BASIS. However, testing the ESF Actuation Logic in the ILP to CIM circuitry would result in the actuation of end devices that, in many cases would produce unacceptable plant perturbations (such as reactor trip, ESF actuations, and various other transient initiators). UFSAR Table 3.9-16, Notes 3, 4, 6, 14, 15, 18, 20, 22, 25, 28, 29, 30, and 35 address various actuated devices that defer testing to cold shutdown or refueling to avoid these undesired plant perturbations. As such, the actuated device testing should not be required to be performed as part of the ALT during plant operation on the same frequency as the rest of the ALT.

The ALT testing that can be performed during plant operation on a 92-day frequency (on a STAGGERED TEST BASIS) should only cover the ESF Coincidence Logic (i.e., the voting logic within the redundant LCL subsystems, including the signal path from the inputs to the LCL, through the LCL voting logic, and out to the ILP inputs). Testing the downstream logic in the ILPs and CIMs results in actuations that should not be required to be tested at power. The currently specified surveillance testing of the actuated devices from the output of the CIMs (i.e., surveillances typically specified as being performed on an “actual or simulated actuation signal”) are required on a 24-month Frequency. The overlap point between surveillances performed on a 92-day frequency (on a STAGGERED TEST BASIS), and those performed at 24 months, is proposed to be moved back to the ESF Actuation Logic testing (including the ILP to CIM pathway) such that the ESF Actuation Logic testing is moved to a 24-month Frequency.

A revision to the existing TS Definition of ACTUATION LOGIC TEST is proposed to require testing only the ESF Coincidence Logic. The ESF Actuation Logic is proposed to be tested during the new ACTUATION LOGIC OUTPUT TEST (ALOT), along with new implementing Surveillance Requirements 3.3.15.2 and 3.3.16.2 specified on a 24-month Frequency.

<u>Definition Changes</u>

As discussed above, the existing TS Definition of ACTUATION LOGIC TEST (ALT) and implementing Surveillance Requirements 3.3.15.1 and 3.3.16.1 are revised to require only the ESF Coincidence Logic (i.e., that portion of the PMS logic that may appropriately be tested at power). The new proposed ACTUATION LOGIC OUTPUT TEST (ALOT), with new implementing Surveillance Requirements 3.3.15.2 and 3.3.16.2, verifies the ESF Actuation Logic (i.e., the signal path from the ILP inputs through the CIM logic and CIM output driver circuits).

The new ALOT requires testing the LCL actuation signals through to the actuated devices. As such, the ALOT may be performed in conjunction with other testing (e.g., automatic actuation Surveillance Requirements which verify correct valve positioning on an actual or simulated test signal, ESF RESPONSE TIME testing, IST Program testing, etc.). The new Definition notes that the test boundary does not include the actuated devices. Testing of the actuated devices (except for the circuit breakers and isolation valves covered by the TS 3.3.15 and TS 3.3.16 Surveillance Requirements) is governed by other TS Surveillance Requirements and IST Program testing. Therefore, the last sentence of the ACTUATION LOGIC TEST Definition is deleted. Both the ALT and new ALOT Definitions include the allowance to be performed by means of any series of sequential, overlapping, or total steps. This is for consistency with the SR 3.0.1 Bases and several other test Definitions in TS Section 1.1 (i.e., CHANNEL OPERATIONAL TEST, CHANNEL CALIBRATION, ESF RESPONSE TIME, RTS RESPONSE TIME, and TRIP ACTUATING DEVICE OPERATIONAL TEST).

New Surveillance Requirement Frequency

The proposed ALOT Frequency is 24 months. New SR 3.3.15.2 and new SR 3.3.16.2 will result in the CIMs generating actuation signals to their end devices, several of which, by virtue of their changing state, would result in a plant transient or reactor trip if performed during power operations.

The 24-month Frequency proposed for the ALOT is consistent with the approved Frequencies for testing actuated devices in surveillances typically specified as being performed on an “actual or simulated actuation signal.” In this proposed change, the ILP to CIM pathway is tested on the same interval as the actuated device. The voting logic and output of the ESF Coincidence Logic to the ILPs will continue to be surveilled on a Frequency of 92-days on a STAGGERED TEST BASIS.

One goal of the AP1000 design is to perform the bulk of surveillance testing of the PMS electronics during regular refueling outages. Achievement of this goal is enabled by the high degree of coverage of the continuous self-diagnostics performed in the digital portions of the system, and by the experience of low failure rates of digital I&C equipment.

The reliability of the PMS is such that not testing the ILP to CIM logic pathways and driver output circuits when the reactor is at power will have a net positive impact on ESFAS availability (reduced online testing yields lower unavailability at power). There will also be a reduction in the potential for challenges to the safety systems, coupled with the reduced time that the safety systems are unavailable.

Based on information in Reference 2, the failures identified in the failure modes and effects analysis (FMEA) for the safety-related functions of the ILPs and CIMs are detectable by self-diagnostics (such as deadman timers, cross-check of redundant channels, memory checks, numeric coprocessor checks, and tests of timers, counters and crystal time bases) which result in diagnostic alarms or system fault alarms in the main control room (MCR) or during periodic surveillance testing on the actuated devices performed (TS-required functional tests, IST testing, etc.). There are no undetectable failure modes affecting the ILP to CIM actuation circuitry that would obviate the proposed testing frequency.

These considerations are discussed in greater detail below.

Failure Modes and Effects Analysis (FMEA)

The FMEA (Reference 2) discusses various failure modes and associated detectability classes for the integrated logic cabinets containing the ILPs and CIMs, most of which are detected by self-diagnostics. There are three failure modes which aren't detected by self-diagnostics, all dealing with the CIMs:

- CIM failure mode results in a spurious actuation of its end device. This failure mode is self-revealing and its likelihood is unrelated to the scope of self-diagnostics or planned surveillance testing.

- CIM failure mode results in the inability to effect end device actuation. For this failure mode, the safety function will be carried out by the other PMS divisions. This failure mode is detectable during TS-required functional surveillance tests and Inservice Test Program (IST) testing (e.g., TS surveillance tests that require the verification of proper response to simulated or actual actuation signals; IST fail safe, exercise, and stroke times tests, etc.). The majority of the latter are performed on a quarterly basis.

- CIM Y Port (see Reference 3) failure results in loss of manual control of its associated component from the non-safety Plant Control System (PLS). This affects only the manual control of non-onerous components (i.e., components that may be tested at power without undesirable consequences such as reactor trip, ESF actuation, etc.), with no impact on their automatic actuation. Y port failure modes may result in a self-revealing spurious actuation or the lack of manual control which is detectable during TS-required functional surveillance tests and IST testing. The majority of the latter are performed on a quarterly basis.

Continuous Self-Diagnostics

Automatic self-diagnostic testing is performed during all modes of plant operation. This test is performed continuously to provide early detection of hardware malfunctions. This self-diagnostic testing includes tests such as processor checks, programmable read-only memory block check sums, read/write test of random access memory, check sums of static random access memory data, check sums of shared memory blocks, and data link transmission error detection.

Extensive, detailed FMEA and functional block analyses (FBA) have been performed on the PMS modules to determine the effectiveness of these self-tests. The results indicate that approximately 90 to 99 percent of faults that could occur will be detected by self-diagnostics and cause the system to assume a default state. These results are incorporated into unavailability equations as percentages of faults that are detectable and/or fail-safe.

The PMS self-diagnostics are automatically executed on a continuous basis and provide operator notification in the event of a failure. The types of continuously executed system self-diagnostics include:

- Processor Module Self-Diagnostics – These include watchdog functions and checksums and detect failures of the processor modules (PMs).
- Data Validity Checks – These include range checks and quality checks and detect failures of the sensor, signal conditioning circuits, and signal conversions.
- Communications and I/O Diagnostics – These include “stay-alive” heartbeat signal checks, cyclic redundancy checks, and checksum checks and detect failures of all communication channels.
- Hardware Module Diagnostics – These include self-testing of the component interface modules (CIMs).

These diagnostic tests report system failures to the operator immediately upon detection without needing to wait for periodic functional tests. These diagnostic failures can be seen on the System Health Event Log Display and as a division fault on the Safety Display (SD) System Health Summary Alerts Display.

As mentioned above, the PMS has many self-checking diagnostic features. In all cases where the PMS functionality is challenged, a Division Fault alarm in the main control room provides indication of a detected system failure. The Maintenance and Test Panel System Health displays are then used to isolate the problem to a particular cabinet, process station, module, or module channel.

The Component Interface Module (CIM) and Safety Remote Node Controller (SRNC) have continuous self-diagnostics that indicate the health of the field programmable gate array (FPGA) and the readiness of the module to perform its specified safety function. If the CIM continuous self-diagnostics indicate a failure, the CIM will stop all communication and place the outputs in the default state. If an SRNC failure is detected, the SRNC will halt all high speed link (HSL) and X-bus (safety bus as discussed in Reference 3) communications. These faults can be detected by upstream devices (i.e., if a CIM stops communicating, the SRNC will indicate a CIM timeout, and if the SRNC stops communicating, the component control processor module in the ILP will detect the SRNC timeout condition).

The safety actuation path overlap self-diagnostic testing is comprised of five overlapping CIM and SRNC test features.

The first stage of self-diagnostic testing is addressed by the HSL protocol. The HSL protocol contains a number of features to verify the message integrity. The overlap diagnostic testing of the HSL protocol begins when the HSL data leaves the processor module buffer and ends when the SRNC HSL reception communication function places the data into the communication buffer.

The second stage of self-diagnostic testing is addressed by the SRNC internal self-checking. The SRNC FPGA contains features that verify the FPGA integrity.

The third stage of self-diagnostic testing is addressed by the X bus protocol. The X bus protocol contains a number of features to verify the message integrity. The overlap testing of the X bus protocol begins when the data is read from the buffer by the SRNC X bus transmission communication function, and ends when the CIM X bus reception communication function places that data into a buffer.

The fourth stage of self-diagnostic testing is addressed by the CIM internal self-testing. The CIM FPGA contains test features that verify the integrity of the FPGA. Internal testing in the CIM is required to immediately abort and allow the execution of a PMS command.

The final stage of self-diagnostic testing is addressed by the CIM output test. The CIM output test provides detection for loss of control power (wetting voltage), wire break, defective CIM Field Effect Transistor (FET) output device, and loss of load (open condition only, i.e., a relay coil breaks and the current path is interrupted).

Other Considerations

- Actuation signal diversity is unaffected. There are several types of level, flow, pressure, temperature, delta-T, neutron flux, RCP speed, valve position, and radioactivity sensors that are available to initiate an automatic reactor trip or ESF actuation, as well as manual actuation capabilities.

- Redundancy within the PMS design is unaffected. As discussed in the PMS overview above, there are redundancies built into the number of available input channels, BPLs, LCLs, and ILPs.

- Continuous self-diagnostics are available to detect the overwhelming majority of possible failures.

- The proposed frequency change for the ILP to CIM logic pathway testing results in only half the currently required tests. Under the current TS, an ACTUATION LOGIC TEST is performed every 92 days on a STAGGERED TEST BASIS. As such, one PMS division is tested every 92 days, all four divisions are tested within a one-year interval, and the testing of any single division recurs on a 12-month interval. Under the proposed ACTUATION LOGIC OUTPUT TEST, only the ILP to actuated device portion of the PMS circuitry is affected with respect to its test interval and that specific portion of the circuitry will be tested for all four divisions every 24 months. In lieu of 8 logic tests of that specific circuitry every 24 months, there will be 4, a 50% reduction.

4. REGULATORY EVALUATION

4.1 Applicable Regulatory Requirements/Criteria

10 CFR 52.98(c) requires NRC approval for any modification to, addition to, or deletion from the terms and conditions of a Combined License (COL). This activity involves a change to COL Appendix A, Technical Specifications (TS); therefore, this activity requires NRC approval prior to making the plant-specific changes in this license amendment request.

10 CFR 52, Appendix D, VIII.C.6 states that after issuance of a license, "Changes to the plant specific TS (Technical Specifications) will be treated as license amendments under 10 CFR 50.90." 10 CFR 50.90 addresses the applications for amendments of licenses, construction permits, and early site permits. As discussed above, a change to COL Appendix A is requested, and thus a license amendment request (LAR) (as supplied herein) is required.

Section 182a of the Atomic Energy Act requires applicants for nuclear power plant operating licenses to include TS as part of the license. The TSs ensure the operational capability of structures, systems, and components that are required to protect the health and safety of the public. The U.S. Nuclear Regulatory Commission's (NRC's) requirements related to the content of the TSs are contained in Section 50.36 of Title 10 of the *Code of Federal Regulations* (10 CFR 50.36) which requires that the TSs include items in the following specific categories: (1) safety limits, limiting safety systems settings, and limiting control settings; (2) limiting conditions for operation; (3) surveillance requirements per 10 CFR 50.36(c)(3); (4) design features; and (5) administrative controls.

This amendment application is related to the third category above (SRs) since Surveillance Requirements 3.3.15.1 and 3.3.16.1 are revised and new Surveillance Requirements 3.3.15.2 and 3.3.16.2 are being incorporated into the plant-specific Technical Specifications.

The following regulatory requirements and guidance documents apply to the Protection and Safety Monitoring System:

10 CFR 50, Appendix A, General Design Criterion (GDC) 2 requires that structures, systems, and components important to safety be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without the loss of the capability to perform their safety functions. The proposed amendment does not involve a design change to the Protection and Safety Monitoring System (PMS). The ability to withstand the effects of natural phenomena is unchanged from the compliance discussion in UFSAR Subsection 3.1.1.

10 CFR 50, Appendix A, GDC 4 requires that structures, systems, and components important to safety be designed to accommodate the effects of, and to be compatible with, the environmental conditions associated with the normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures,

systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, discharging fluids that may result from equipment failures, and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping. The proposed amendment does not involve a design change to the PMS. The environmental and missile design basis compliance discussion in UFSAR Subsection 3.1.1 is unaffected.

10 CFR 50, Appendix A, GDC 13 requires that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. The proposed amendment does not involve a design change to the PMS or affect system variable monitoring. The compliance discussion of the instrumentation and control design in UFSAR Subsection 3.1.1 is unaffected.

10 CFR 50, Appendix A, GDC 20 requires that the protection system(s) shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety. The proposed amendment does not involve a design change to the PMS. The compliance discussion of the protection system design in UFSAR Subsection 3.1.1 is unaffected.

10 CFR 50, Appendix A, GDC 21 requires that the protection system(s) shall be designed for high functional reliability and testability. The proposed amendment does not involve a design change to the PMS. There is no change to the reliability and testability design provisions discussed in UFSAR Subsection 3.1.1.

10 CFR 50, Appendix A, GDC 22 through GDC 25 and GDC 29 require various design attributes for the protection system(s), including independence, safe failure modes, separation from control systems, requirements for reactivity control malfunctions, and protection against anticipated operational occurrences. The proposed amendment does not involve a design change to the PMS. None of the GDC compliance discussions for the PMS in UFSAR Subsection 3.1.1 is affected.

Regulatory Guide 1.22, “Periodic Testing of Protection and Safety Actuation Functions,” discusses an acceptable method of satisfying GDC 20 and GDC 21 regarding the periodic testing of protection system actuation functions. These periodic tests should duplicate, as closely as practicable, the performance that is required of the actuation devices in the event of an accident. The proposed amendment establishes frequency-appropriate PMS logic surveillance testing requirements, consistent with this guidance.

10 CFR 50.55a(h) requires that the protection systems meet IEEE 603-1991. Paragraph 3.13 of IEEE 603-1991 discusses the testing and calibration requirements for protection systems. Testing from the sensor inputs to the PMS through to the actuated equipment is accomplished through a series of overlapping sequential tests, and that objective continues to be met by the proposed surveillance testing requirements.

4.2 Precedent

No precedent is identified.

4.3 Significant Hazards Consideration

The requested amendment proposes changes to COL Appendix A, Technical Specifications. The proposed changes revise COL Appendix A, plant-specific Technical Specifications (TS) by modifying the TS Section 1.1 Definition of ACTUATION LOGIC TEST, adding a new TS Section 1.1 Definition of ACTUATION LOGIC OUTPUT TEST (ALOT), revising existing Surveillance Requirements 3.3.15.1 and 3.3.16.1, and adding new Surveillance Requirements 3.3.15.2 and 3.3.16.2 to implement the new ALOT.

An evaluation to determine whether or not a significant hazards consideration is involved with the proposed amendment was completed by focusing on the three standards set forth in 10 CFR 50.92, "Issuance of amendment," as discussed below:

4.3.1 Does the proposed amendment involve a significant increase in the probability or consequences of an accident previously evaluated?

Response: No.

There are no design changes associated with the proposed amendment. All design, material, and construction standards that were applicable prior to this amendment request will continue to be applicable.

The PMS will continue to function in a manner consistent with the plant design basis. There will be no changes to the PMS operating limits. The existing ACTUATION LOGIC TEST Surveillance Requirements are revised such that different portions of the PMS logic circuitry are tested on appropriate surveillance test frequencies.

The proposed change will not adversely affect accident initiators or precursors or adversely alter the design assumptions, conditions, and configuration of the facility, or the manner in which the plant is operated and maintained, with respect to such initiators or precursors.

The proposed changes will not alter the ability of structures, systems, and components (SSCs) to perform their specified safety functions to mitigate the consequences of an initiating event within the assumed acceptance limits.

Accident analysis acceptance criteria will continue to be met with the proposed changes. The proposed changes will not affect the source term, containment isolation, or radiological release assumptions used in evaluating the radiological consequences of any accident previously evaluated. The proposed changes will not alter any assumptions or change any mitigation actions in the radiological consequence evaluations in the Updated Final Safety Analysis Report (UFSAR).

The applicable radiological dose acceptance criteria will continue to be met.

The proposed change revises the frequency of testing certain portions of the PMS logic circuitry, but does not physically alter any safety-related systems.

Therefore, the proposed amendment does not involve a significant increase in the probability or consequences of an accident previously evaluated.

4.3.2 Does the proposed amendment create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No.

With respect to any new or different kind of accident, there are no proposed design changes nor are there any changes in the method by which any safety-related plant SSC performs its specified safety function. The proposed change will not affect the normal method of plant operation or change any operating parameters. No equipment performance requirements will be affected. The proposed change will not alter any assumptions made in the safety analyses.

The proposed change revises the frequency of testing certain portions of the PMS logic circuitry. The proposed change does not involve a physical modification of the plant.

No new accident scenarios, transient precursors, failure mechanisms, or limiting single failures will be introduced as a result of this amendment. There will be no adverse effect or challenges imposed on any safety-related system as a result of this amendment.

Therefore, the proposed amendment does not create the possibility of a new or different kind of accident from any accident previously evaluated.

4.3.3 Does the proposed amendment involve a significant reduction in a margin of safety?

Response: No.

The existing ACTUATION LOGIC TEST Surveillance Requirements are revised such that different portions of the PMS logic circuitry are tested on appropriate surveillance test frequencies. The reliability of the PMS is such that not testing the Component Interface Module (CIM) logic and driver output circuits when the reactor is at power will have a net positive impact on Engineered Safety Feature Actuation System (ESFAS) availability. There will be a reduction in the potential for challenges to the safety systems, coupled with less time that the safety systems are unavailable.

There will be no effect on those plant systems necessary to effect the accomplishment of protection functions.

No instrument setpoints or system response times are affected. None of the acceptance criteria for any accident analysis will be changed.

The proposed change will have no impact on the radiological consequences of a design basis accident.

Therefore, the proposed amendment does not involve a significant reduction in a margin of safety.

Based on the above, it is concluded that the proposed amendment does not involve a significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and, accordingly, a finding of “no significant hazards consideration” is justified.

4.4 Conclusions

In conclusion, based on the considerations discussed above, (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission’s regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public. Pursuant to 10 CFR 50.92, the requested change does not involve a Significant Hazards Consideration.

5. ENVIRONMENTAL CONSIDERATIONS

The requested amendment proposes to amend COL Appendix A, Technical Specifications. The proposed changes revise COL Appendix A, plant-specific Technical Specifications (TS) by modifying the TS Section 1.1 Definition of ACTUATION LOGIC TEST, adding a new TS Section 1.1 Definition of ACTUATION LOGIC OUTPUT TEST (ALOT), revising existing Surveillance Requirements (SR) 3.3.15.1 and SR 3.3.16.1, and adding new Surveillance Requirements SR 3.3.15.2 and SR 3.3.16.2 to implement the new ALOT.

The details of the proposed changes are provided in Sections 2 and 3 of this license amendment request.

This review has determined that the proposed change requires an amendment to the COL. However, a review of the anticipated construction and operational effects of the requested amendment has determined that the requested amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9), in that:

(i) *There is no significant hazards consideration.*

As documented in Section 4.3, Significant Hazards Consideration, of this license amendment request, an evaluation was completed to determine whether or not a significant hazards consideration is involved by focusing on the three standards set forth in 10 CFR 50.92, “Issuance of amendment.” The Significant Hazards Consideration determined that (1) the proposed amendment does not involve a significant increase in the probability or consequences of an accident previously evaluated; (2) the proposed amendment does not create the possibility of a new or different kind of accident from any accident previously evaluated; and (3) the proposed amendment does not involve a significant reduction in a margin of safety. Therefore, it is concluded that the proposed amendment does not involve a significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and accordingly, a finding of “no significant hazards consideration” is justified.

(ii) *There is no significant change in the types or significant increase in the amounts of any effluents that may be released offsite.*

The proposed amendment revises the frequency of testing certain portions of the PMS logic circuitry. The changes are unrelated to any aspects of plant construction or operation that would introduce any changes to effluent types (e.g., effluents containing chemicals or biocides, sanitary system effluents, and other effluents) or affect any plant radiological or non-radiological effluent release quantities. Furthermore, the proposed change does not diminish the functionality of any design or operational features that are credited with controlling the release of effluents during plant operation. Therefore, it is concluded that the proposed amendment does not involve a significant change in the types or a significant increase in the amounts of any effluents that may be released offsite.

(iii) *There is no significant increase in individual or cumulative occupational radiation exposure.*

The proposed amendment revises the frequency of testing certain portions of the PMS logic circuitry. The change does not affect plant radiation zones (addressed in UFSAR Section 12.3), and controls under 10 CFR 20 preclude a significant increase in occupational radiation exposure. Therefore, the proposed amendment does not involve a significant increase in individual or cumulative occupational radiation exposure.

Based on the above review of the requested amendment, it has been determined that anticipated construction and operational effects of the requested amendment do not involve (i) a significant hazards consideration, (ii) a significant change in the types or significant increase in the amounts of any effluents that may be released offsite, or (iii) a significant increase in individual or cumulative occupational radiation exposure. Accordingly, the requested amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Therefore, pursuant to 10 CFR 51.22(b), an environmental impact statement or environmental assessment of the proposed amendment is not required.

6. REFERENCES

1. WCAP-16675-P, “AP1000 Protection and Safety Monitoring System Architecture Technical Report.” [See UFSAR Table 1.6-1 and Reference 19 in UFSAR Subsection 7.1.7.]

2. WCAP-16438-P, “FMEA of AP1000 Protection and Safety Monitoring System.” [See UFSAR Table 1.6-1 and Reference 1 in UFSAR Subsection 7.2.4.]

3. WCAP-17179-P, “AP1000 Component Interface Module Technical Report.” [See UFSAR Table 1.6-1 and Reference 21 in UFSAR Subsection 7.1.7.]

Southern Nuclear Operating Company

ND-17-1280

Enclosure 2

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

Proposed Changes to Licensing Basis Documents

(LAR-17-026)

Insertions Denoted by Blue Underline and Deletions by ~~Red~~ Strikethrough
Omitted text is identified by three asterisks (*...*...*)

(This Enclosure consists of 4 pages, including this cover page)

Revise COL Appendix A, Technical Specifications, TS 1.1 Definitions, as follows:

1.0 USE AND APPLICATION

1.1 Definitions

- NOTE -

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

Term	Definition
	......*
ACTUATION LOGIC TEST	An ACTUATION LOGIC TEST shall be the application of various simulated or actual input combinations in conjunction with each possible interlock logic state required for OPERABILITY of a logic circuit and the verification of the required logic output. The ACTUATION LOGIC TEST ~~shall be conducted such that it provides component overlap with the actuated device~~may be performed by means of any series of sequential, overlapping, or total steps.
ACTUATION LOGIC OUTPUT TEST	An ACTUATION LOGIC OUTPUT TEST shall be the application of simulated or actual logic signals and the verification of the required component actuation output signals up to, but not including, the actuated device. The ACTUATION LOGIC OUTPUT TEST may be performed by means of any series of sequential, overlapping, or total steps.

Revise COL Appendix A (Technical Specifications), TS 3.3.15, Engineered Safety Feature Actuation System (ESFAS) Actuation Logic – Operating, as follows:

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.3.15.1	Perform ACTUATION LOGIC TEST on ESF Coincidence Logic.	92 days on a STAGGERED TEST BASIS
SR 3.3.15.2	Perform ACTUATION LOGIC OUTPUT TEST on ESF Actuation.	24 months
SR 3.3.15.~~2~~3	...*...*...*	*...*...*
SR 3.3.15.~~3~~4	...*...*...*	*...*...*
SR 3.3.15.~~4~~5	...*...*...*	*...*...*
SR 3.3.15.~~5~~6	...*...*...*	*...*...*
SR 3.3.15.~~6~~7	...*...*...*	*...*...*

Revise COL Appendix A (Technical Specifications), TS 3.3.16, Engineered Safety Feature Actuation System (ESFAS) Actuation Logic – Shutdown, as follows:

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.3.16.1	Perform ACTUATION LOGIC TEST on ESF Coincidence Logic.	92 days on a STAGGERED TEST BASIS
SR 3.3.16.2	Perform ACTUATION LOGIC OUTPUT TEST on ESF Actuation.	24 months
SR 3.3.16.~~2~~3	...*...*...*	*...*...*

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE		FREQUENCY
SR 3.3.16.~~3~~4	...*...*...*	*...*...*
SR 3.3.16.~~4~~5	...*...*...*	*...*...*

Southern Nuclear Operating Company

ND-17-1280

Enclosure 3

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

Conforming Technical Specification Bases Changes

(For Information Only)

(LAR-17 -026)

Insertions Denoted by Blue Underline and Deletions by ~~Red~~ Strikethrough
Omitted text is identified by three asterisks (*...*...*)

(This Enclosure consists of 31 pages, including this cover page.)

Technical Specification Bases B 3.1.9, Chemical and Volume Control System (CVS) Demineralized Water Isolation Valves and Makeup Line Isolation Valves

SURVEILLANCE REQUIREMENTS

SR 3.1.9.1

......*

SR 3.1.9.2

Verification that the closure time of each RCS makeup isolation valve is less than that assumed in the safety analysis (i.e., ≤ 30 seconds), is performed by measuring the time required for each valve to close on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance ~~to provide complete testing of the assumed safety function~~. The Frequency is in accordance with the Inservice Testing Program.

SR 3.1.9.3

This SR verifies that each CVS demineralized water isolation valve actuates to the correct position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance ~~to provide complete testing of the assumed safety function~~. 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.

Technical Specification Bases B 3.3.1, Reactor Trip System (RTS) Instrumentation

B 3.3.1

BACKGROUND (continued)

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.~~

BACKGROUND (continued)

~~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 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 required for each plant parameter is specified in Reference 1.~~

~~Selected analog measurements are converted to digital form by digital converters within the Protection and Safety Monitoring System cabinets. Signal conditioning 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:~~

BACKGROUND (continued)

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 (PMS) Cabinets

The Protection and Safety Monitoring System cabinets contain the necessary equipment to (Reference 9):

- Permit acquisition and analysis of the sensor inputs, including plant process sensors and nuclear instrumentation, required for reactor trip and Engineered Safety Features (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 automatic ESF Function;

- Provide data to other systems in the Instrumentation and Control (I&C) architecture;

- Provide additional redundancy (within a single division) for the reactor trips and ESF actuations; and

- Provide separate input isolation 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 2 and 3. If the measured value of a unit parameter exceeds the predetermined setpoint, an output is

BACKGROUND (continued)

generated which is transmitted to the ESF coincidence logic for logic evaluation.

Within the 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, which allows RTB closure. 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.

PMS Overview

The four divisions of PMS each consist of the following:

- Field Transmitters and Sensors (non-redundant)
- Nuclear Instrumentation System (NIS) - 1 per division (non-redundant)

BACKGROUND (continued)

- Bistable Processor Logic (BPL) System - 2 BPL subsystems per division (redundant)
- Local Coincidence Logic (LCL) System - 2 LCL subsystems per division (redundant), each subsystem with two reactor trip processors (non-redundant)
- Reactor Trip Initiation Logic - 2 Reactor Trip Matrices (RTMs) per division (undervoltage (UV) and shunt trip (ST) - redundant)
- Reactor Trip Breakers (RTBs) - 2 per division (non-redundant). See LCO 3.3.7, "RTS Trip Actuation Devices" for further discussion.

The vital buses that power each PMS division are backed up by the battery bank in the same division. See LCO 3.8.1, "DC Sources - Operating" for further discussion.

PMS equipment duplication within a division (redundancy) is generally provided for active equipment such as processors and communication hardware. Where provided, redundant sets of equipment within a division are not independent and can be subject to common cause failures. 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.

Within each division, the sensor signals and setpoint bistables are processed in the BPL. The results of the bistable logic (partial reactor trip signals) are communicated to the LCL subsystems in all divisions. The LCL subsystems perform the divisional voting logic (e.g., two-out-of- four (2oo4) logic) and other associated logic.

Within each division, the LCL reactor trip contact outputs are inputs to two RTMs: one for the RTB undervoltage (UV) mechanism (coil), and one for the shunt trip (ST) mechanism (coil). The RTMs trip the RTBs by deenergizing the UV coils and energizing the ST coils. Each of the four PMS divisions consists of two reactor trip circuit breakers. The reactor is tripped when the RTBs in two or more divisions are opened.

Reactor Trip (RT) Channel

An RT channel extends from the sensor to the output of the associated BPL subsystem and shall include the sensor (or sensors), the signal conditioning, the BPL subsystem, and associated datalinks to the LCL

BACKGROUND (continued)

subsystems. For RT channels containing nuclear instrumentation, the RT channel also includes the signal processing and power supplies for the detectors provided by the NIS. In some cases, sensors provide inputs to more than one RT function. Thus, an inoperability of a shared sensor can affect the OPERABILITY of more than one RT function.

Automatic Trip Logic

The Automatic Trip Logic includes the LCL subsystems and Reactor Trip Initiation logic matrices, including the outputs of the various RT Channels (BPL outputs). It does not include the RTBs.

PMS Division

The PMS consists of four redundant divisions, designated A, B, C, and D. All safety system divisions are physically, functionally, and electrically separated from each other and from non-safety systems. Redundant divisions are provided to satisfy single failure criteria and improve plant availability. Each PMS division actuates two RTBs. Actuation of the RTBs in two divisions will trip the reactor.

Field Transmitters and Sensors

Normally, four redundant measurements using four separate sensors are made for each variable used for reactor trip. One measurement is processed by each division. The use of four channels for protection functions is based on a minimum of two channels being required for a reactor trip (e.g., two-out-of-four (2oo4) voting logic), with one channel in test or bypass, and a single failure on the remaining channel. Minimum requirements for protection 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.

Analog measurements are converted to digital form by analog to digital (A/D) converters within the BPL subsystems. Signal conditioning may be applied to selected inputs following the conversion to digital form. Except for selected dual element resistance temperature detectors (RTDs), the sensors within each division are non-redundant.

BACKGROUND (continued)

Nuclear Instrument System (NIS)

In each division the NIS cabinet provides signal processing and power supplies for the source range, intermediate range, and power range detectors. The analog and digital pulse signals generated are sent to the BPL for processing. Within each division, each transmitter, sensor, and NIS signal is input in parallel to both BPLs.

Bistable Processor Logic (BPL) System

Each PMS division contains two identical and redundant BPL subsystems receiving the same input signals and performing the same calculations and logic. The BPL subsystems receive data from field sensors and manual inputs (such as system-level blocks and resets) from the MCR to perform the protective function calculations.

Within each division, the input from each sensor is provided in parallel to each of the two BPL subsystems' analog or digital input modules. Analog transmitter and sensor measurements are converted from analog to digital form by analog to digital input modules within the BPL subsystems. Signal conditioning may be applied to selected inputs following the conversion to digital form. The subsystems provide signal outputs for MCR indications and, via the Plant Control System (PLS), for non-safety Remote Shutdown Workstation indications.

Following necessary calculations, processing, and logic, the measurements are compared to the applicable setpoints. The basis of the setpoints is described in References 2 and 3. The results of the required calculations and setpoint comparisons determine the partial trip status for each reactor trip function.

The partial reactor trip signals are transmitted to all eight LCLs in the PMS for use in coincidence logic voting. The PMS uses datalinks to communicate the partial trips and related status information calculated in the BPL subsystems to the LCL subsystems. These datalinks are used both locally within a division and externally across divisions. A partial trip signal from either BPL subsystem in a division is interpreted by the LCL coincidence logic as a partial trip signal.

During periodic tests and maintenance performed using the Maintenance and Test Panel and Interface and Test Processor, each BPL subsystem is tested individually. During testing, the LCL processors use the redundant BPL subsystem output for trip status. This permits the division being tested to remain OPERABLE while the testing is being conducted.

BACKGROUND (continued)

Local Coincidence Logic (LCL) System

Each PMS division contains two identical and redundant LCL subsystems receiving the same input signals and performing the same logic. The LCL subsystems perform the logic to combine the partial trip signals from the BPL subsystems and generate a trip output signal to the Reactor Trip Initiation logic.

Eight LCL subsystems are provided in the PMS architecture. Each of the LCL subsystems receives partial reactor trip signals and status signals from each of the eight BPL subsystems. In normal operation, the LCL logic is programmed to assume that a partial trip signal in either BPL subsystem in a given division is equivalent to a partial trip signal.

In the event of a single BPL processor or associated datalink failure in a division is detected by diagnostics, the LCL logic will reject the input from the failed component and use the input from the other BPL subsystem from the affected division as the source of the trip information. This allows the function logic to remain in a 2oo4 logic configuration.

LCL processors will only permit bypass of both BPL inputs of a given function from one division (such as due to a failed sensor). In the event of a division bypass, the LCL reverts to 2oo3 logic in the affected function.

The LCL subsystems act to initiate a reactor trip when the required number of divisions reaches a partial trip state (e.g., 2oo4, 1oo2).

Each LCL subsystem provides four contact outputs to the Reactor Trip Initiation logic, two for the Undervoltage (UV) RTM and two for the Shunt Trip (ST) RTM.

The LCL also provides for the bypass of trip functions to accommodate periodic tests and maintenance. During LCL subsystem testing, each LCL subsystem is tested individually. During testing, the redundant LCL subsystem is available to provide the UV and ST output signals to the RTMs. This permits the division being tested to remain OPERABLE while the testing is being conducted.

Reactor Trip Initiation Logic

The Reactor Trip Matrix (RTM) acts as an interface between the LCL subsystems and the RTBs. The RTM receives contact inputs from the LCL subsystems and performs the logic to determine if a division will issue a reactor trip command.

BACKGROUND (continued)

Each PMS division contains two redundant RTMs; one is configured as a ST matrix and the other a UV matrix. The combination of the two forms the complete RTM for a given division. If the ST logic is satisfied, the RTB ST coils are energized, opening both RTBs in the division. If the UV logic is satisfied, the RTB UV coils are de-energized, opening both RTBs in the division.

The PMS boundary ends at the interposing relay contacts of the RTMs.

Manual RT

A manual reactor trip is initiated from the MCR by redundant momentary switches. The switches directly control the power from the RTM logic, actuating the UV and ST attachments in all four divisions.

Nominal Trip Setpoint (NTS)

The NTS is the nominal value 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 (i.e., ± rack calibration accuracy).

......*

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.

~~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.~~

B 3.3.1

BACKGROUND (continued)

~~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.~~

......*

REFERENCES *...*...*

9. WCAP-16675-P, “AP1000 Protection and Safety Monitoring System Architecture Technical Support.”

Technical Specification Bases B 3.3.4, Reactor Trip System (RTS) Engineered Safety Feature Actuation System (ESFAS) Instrumentation

SURVEILLANCE REQUIREMENTS

SR 3.3.4.1

SR 3.3.4.1 is the performance of a ACTUATION LOGIC TEST every 92 days.

An ACTUATION LOGIC TEST is performed on each required channel to provide reasonable assurance that the entire channel will perform the intended Function. This test demonstrates that the Local Coincidence Logic (LCL) process module that performs the ESF actuation functions for safeguards actuation, ADS Stages 1, 2, and 3 actuation, and CMT actuation also sends a digital signal to the LCL process modules that perform reactor trip actuation functions. That digital signal is sent by way of the global memory feature of the communications interface module. The reactor trip process modules then combine this signal with those from the BPL channel voting logic to generate the outputs sent to the Reactor Trip Switchgear Interface Logic.

Technical Specification Bases B 3.3.6, Reactor Trip System (RTS) Automatic Trip Logic

SURVEILLANCE REQUIREMENTS

SR 3.3.6.1

SR 3.3.6.1 is the performance of an ACTUATION LOGIC TEST every 92 days.

An ACTUATION LOGIC TEST is performed on each channel to provide reasonable assurance that the entire channel will perform the intended Function. The test demonstrates that the Local Coincidence Logic (LCL) performs the required coincidence logic using injected, partial trip signals and communicates reactor trip signals to the Reactor Trip Switchgear Interface Logic.

The LCL to Reactor Trip Matrix (RTM) test provides verification of proper operation of the LCL Reactor Trip (RT) Processor Module (PM) voting logic and digital outputs. Test signals are injected into the voting logic of one of the four redundant LCL RT PMs. Injecting the correct combination of test signals, simulating the partial trip signals from the eight redundant BPL PMs, satisfies the voting logic and actuates the undervoltage and shunt trip outputs of the associated digital output (DO) module. The LCL to RTM test provides overlap with the Reactor Trip Digital Output (RTDO) to Reactor Trip Circuit Breaker (RTCB) test in SR 3.3.7.1 (TADOT). Each RT PM can be individually tested and its output monitored at the RTM without tripping any of the reactor trip breakers.

Technical Specification Bases B 3.3.8, Engineered Safety Feature Actuation System (ESFAS) Instrumentation

B 3.3.8

BACKGROUND (continued)

……*

~~The ESFAS instrumentation is segmented into distinct but interconnected modules.~~

~~Field Transmitters and Sensors~~

~~Normally, four redundant measurements using four separate sensors, are made for each variable used for actuation of Engineered Safety Features (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~~

BACKGROUND (continued)

~~and control are achieved only 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 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. 3). The actual number of channels provided for each plant parameter is specified in Reference 1.~~

~~Engineered Safety Features 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~~Protection and Safety Monitoring System (PMS)

The ~~Plant~~ Protection and Safety Monitoring System contains the necessary equipment to (Reference 8):

- 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;

BACKGROUND (continued)

- Provide data to other systems in the Instrumentation and Control (I&C) architecture; ~~and~~
- Provide additional redundancy (within a single division) for the reactor trips and ESF actuations; and
- Provide ~~separate input~~ isolation 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, 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 2 and 6. 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 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.~~

BACKGROUND (continued)

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 the main control room;
- 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 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.

PMS Overview

The four divisions of PMS each consist of the following:

- Field Transmitters and Sensors (non-redundant)
- Nuclear Instrumentation System (NIS) - 1 per division (non-redundant)
- Bistable Processor Logic (BPL) System - 2 BPL subsystems per division (redundant)

BACKGROUND (continued)

- Local Coincidence Logic (LCL) System - 2 LCL subsystems per division (redundant)
- ESF Actuation Subsystem Logic (Integrated Logic Cabinet (ILC)) with Integrated Logic Processor (ILP) System - 2 ILP subsystems per ILC (redundant)
    - Division A - 3 ILCs
    - Division B - 4 ILCs
    - Division C - 2 ILCs
    - Division D - 4 ILCs
    - Component Interface Modules (CIM) (non-redundant)

The vital buses that power each PMS division are backed up by the battery bank in the same division. See LCO 3.8.1, "DC Sources – Operating" for further discussion.

PMS equipment duplication within a division (redundancy) is generally provided for active equipment such as processors and communication hardware. Where provided, redundant sets of equipment within a division are not independent and can be subject to common cause failures. 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.

Within each division, the sensor signals and setpoint bistables are processed in the BPL. The results of the bistable logic (partial ESF actuation signals) are communicated to the LCL subsystems in all divisions. The LCL subsystems perform the divisional ESF Coincidence Logic voting (e.g., two-out-of-four (2oo4) logic) and other associated logic.

ESF system-level actuation outputs from the LCL are inputs to the ESF Actuation Subsystem logic performed in the ILC for generation of logic commands to the actuated components. Each ILC consists of redundant ILPs and non-redundant CIMs. The ILPs decode the system commands and actuate the final equipment through the CIM interlocking logic specific to each component (Reference 8).

BACKGROUND (continued)

The CIMs provide actuation signals to each of the actuated devices. The PMS boundary ends at the output terminals of the CIMs. The actuated devices are outside the scope of this specification.

Engineered Safety Features (ESF) Channel

An ESF channel extends from the sensor to the output of the associated BPL subsystem and shall include the sensor (or sensors), the signal conditioning, the BPL subsystem, and associated datalinks to the LCL subsystems. For ESF channels containing nuclear instrumentation (e.g., boron dilution block, CVS isolation), the ESF channel also includes the signal processing and power supplies for the detectors provided by the NIS. In some cases, sensors provide inputs to more than one ESF function. Thus, an inoperability of a shared sensor can affect the OPERABILITY of more than one ESF function.

PMS Division

The PMS consists of four redundant divisions, designated A, B, C, and D (with the exception of the Component Interface Modules). All safety system divisions are physically, functionally, and electrically separated from each other and from non-safety systems. Redundant divisions are provided to satisfy single failure criteria and improve plant availability. PMS divisions A and C actuate one train of ESF equipment and divisions B and D actuate the other ESF train.

Field Transmitters and Sensors

Normally, four redundant measurements using four separate sensors are made for each variable used for actuation of ESF. One measurement is processed by each division. The use of four channels for protection Functions is based on a minimum of two channels being required for an ESF actuation (two-out-of-four (2oo4) voting logic), with one channel in test or bypass, and a single failure on the remaining channel. Minimum requirements for protection are achieved only 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 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.

BACKGROUND (continued)

Analog measurements are converted to digital form by analog to digital (A/D) converters within the BPL subsystems. Signal conditioning may be applied to selected inputs following the conversion to digital form. Except for selected dual element resistance temperature detectors (RTDs), the sensors within each division are non-redundant.

Nuclear Instrumentation System (NIS)

In each division the NIS cabinet provides signal processing and power supplies for the source range, intermediate range, and power range detectors. The analog and digital pulse signals generated are sent to the BPL for processing. Within each division, each transmitter, sensor, and NIS signal is input in parallel to both BPLs.

Bistable Processor Logic (BPL) System

Each PMS division contains two identical and redundant BPL subsystems receiving the same input signals and performing the same calculations and logic. The BPL subsystems receive data from field sensors and manual inputs (such as system-level blocks and resets) from the MCR to perform the protective function calculations.

Within each division, the input from each sensor is provided in parallel to each of the two BPL subsystems' analog or digital input modules. Analog transmitter and sensor measurements are converted from analog to digital form by analog to digital input modules within the BPL subsystems. Signal conditioning may be applied to selected inputs following the conversion to digital form. The subsystems provide signal outputs for MCR indications and, via the Plant Control System (PLS), for the non-safety related Remote Shutdown Workstation indications.

Following necessary calculations, processing, and logic, the measurements are compared against the applicable setpoints. The basis of the setpoints is described in References 2 and 6. The results of the required calculations and setpoint comparisons determine the partial actuation status for each ESF actuation function.

The partial ESF actuation signals are transmitted to all eight LCLs in the PMS for use in coincidence logic voting. The PMS uses datalinks to communicate the partial actuations and related status information calculated in the BPL subsystems to the LCL subsystems. These datalinks are used both locally within a division and externally across divisions. A partial actuation signal from either BPL subsystem in a division is interpreted by the LCL coincidence logic as a partial actuation signal.

BACKGROUND (continued)

During periodic tests and maintenance performed using the Maintenance and Test Panel and Interface and Test Processor, each BPL subsystem is tested individually. During testing, the LCL processors use the redundant BPL subsystem for actuation status. This permits the division being tested to remain OPERABLE while the testing is being conducted.

ESF Coincidence Logic (Local Coincidence Logic (LCL) System)

Each PMS division contains two identical and redundant LCL subsystems receiving the same input signals and performing the same logic. The LCL subsystems perform the logic to combine the partial actuation signals from the BPL subsystems, along with automatic and manual permissives, blocks, and resets, and generate an actuation output signal to the ESF Actuation Subsystem Logic (Integrated Logic Cabinet (ILC)).

Eight LCL subsystems are provided in the PMS architecture. Each of the LCL subsystems receives partial ESF actuation signals and status signals from each of the eight BPL subsystems. In normal operation, the LCL logic is programmed to assume that a partial actuation signal in either BPL subsystem in a given division is equivalent to a partial actuation signal.

In the event of a single BPL processor or associated datalink failure in a division is detected by diagnostics, the LCL logic will reject the input from the failed component and use the input from the other BPL subsystem from the affected division as the source of actuation information. This allows the function logic to remain in a 2oo4 logic configuration.

LCL processors will only permit bypass of both BPL inputs of a given function from one division (such as due to a failed sensor). In the event of a division bypass, the LCL reverts to 2oo3 logic in the affected function.

The LCL subsystems act to initiate an ESF actuation when the required number of divisions reaches a partial actuation state (e.g., 2oo4, 1oo2).

The LCL also provides for the bypass of actuation functions to accommodate periodic tests and maintenance. During LCL subsystem testing, each LCL subsystem is tested individually. During testing, the redundant LCL subsystem is available to provide output signals to the ILCs. This permits the division being tested to remain OPERABLE while the testing is being conducted.

Within each division, datalinks transfer the ESF system-level actuations and related status information calculated in the LCL controllers to the ESF

BACKGROUND (continued)

Actuation Subsystem. Actuation signals from both LCL subsystems are transmitted to the redundant ILPs in each ILC.

MCR ESF Manual Controls

Each of the manual system-level actuations is implemented using switches wired to digital input modules included in the LCL. The switch inputs to the LCL produce the ESF system-level actuation signals that are communicated to the ESF Actuation Subsystem.

ESF Actuation Subsystem (Integrated Logic Cabinet (ILC))

Within each division, ESF system-level actuation outputs from the LCLs are inputs to the ESF Actuation Subsystem for generation of logic commands to the actuated components. The ESF Actuation Subsystem consists of internally redundant ILPs and non-redundant CIMs. The ILPs decode the system commands and actuate the final equipment through the CIM logic specific to each component.

Each of the two ILP processors receives inputs from both ESF Coincidence logic processors (LCLs) in a division. The ILPs perform the component fan-out for each ESF system-level actuation command. As long as the outputs from both ESF Coincidence logic processors (LCLs) agree that an actuation should occur (i.e., 2oo2 logic), the ILPs will generate actuation signals to the CIMs. For each Function, if one of the LCLs has no output signal, provides a bad quality signal, or is in test, a good quality signal input to the ILP processors from the other LCL is sufficient to maintain OPERABILITY. With a good quality signal from only one LCL, the ILP logic becomes 1oo1.

Each CIM provides an actuation signal to its associated actuated device.

Each CIM receives inputs from both processors in an ILP and produces component actuation signals if the input signals agree (i.e., 2oo2 logic). If one of the ILP processors has no output signal or provides a bad quality signal, a good quality signal input to the CIM from the other ILP processor is sufficient to maintain OPERABILITY. With a good quality signal from only one ILP processor, the CIM logic becomes 1oo1 .

The PMS boundary ends at the output terminals of the CIMs

Nominal Trip Setpoints (NTSs)

The NTS is the nominal value at which the trip output is set. Any trip output is considered to be properly adjusted when the “as-left” value is

BACKGROUND (continued)

within the band for CHANNEL CALIBRATION, i.e., ± rack calibration accuracy.

......*

REFERENCES

......*

8. WCAP-16675-P, "AP1000 Protection and Safety Monitoring System Architecture Technical Report."

Technical Specification Bases B 3.3.15, Engineered Safety Feature Actuation System (ESFAS) Actuation Logic – Operating

SURVEILLANCE REQUIREMENTS

SR 3.3.15.1

SR 3.3.15.1 is the performance of an ACTUATION LOGIC TEST on the ESF Coincidence Logic. This test, in conjunction with the individual device functional tests throughout the Technical Specifications demonstrate that actuated devices respond to an actual or simulated actuation signal. The ACTUATION LOGIC TEST demonstrates that the ESF Local Coincidence Logic (LCL subsystems) performs the required coincidence logic using injected, partial actuation signals and communicates system actuation signals to the ILP inputs in the ESF Actuation Subsystem Logic (Integrated Logic Cabinets (ILCs)). The ESF coincidence logic and ESF actuation subsystems LCL subsystems within a division are tested every 92 days on a STAGGERED TEST BASIS.

......*

If the ACTUATION LOGIC TEST cannot 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 LCL to ILP test feature provides verification of proper operation of the ESF LCL process modules (PMs), high speed link (HSL) communication, and ILP PMs. The test signal is injected at the ESF LCL PM and monitored at the ILP PMs. The ACTUATION LOGIC TEST provides overlap with the ACTUATION LOGIC OUTPUT TEST in SR 3.3.15.2 by verifying communication of system actuation signals from the ESF Local Coincidence Logic to the ESF Actuation Subsystem ILPs.

......*

B 3.3.15

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.15.2

SR 3.3.15.2 is the performance of an ACTUATION LOGIC OUTPUT TEST (ALOT) on the ESF Actuation. The ALOT demonstrates that both of the redundant signal paths from the inputs to the ILPs through the CIM logic and CIM output driver circuits (ILP to actuator test) in the ESF Actuation Subsystem Logic process injected LCL system actuation signals for the applicable actuation Function. During this test, a signal is sent back to the Maintenance and Test Panel (MTP) subsystem to determine if the CIM 2oo2 logic was satisfied and a component control signal was sent to the actuated device. As such, the ALOT may be performed in conjunction with other testing (e.g., automatic actuation Surveillance Requirements which verify correct valve positioning on an actual or simulated actuation signal).

The CIM can be allowed to actuate its end device in this test. There are certain end devices that are not expected to be actuated, such as the squib valves (ADS Stage 4 squib valves tested under SR 3.4.11.5, IRWST injection and recirculation squib valves tested under SR 3.5.6.9) and the following passive core cooling system motor-operated valves:

- Both accumulator discharge line motor-operated valves;
- Both in-containment refueling water storage tank gravity injection line motor-operated valves; and
- The passive residual heat removal heat exchanger inlet line motor-operated valve.

These motor-operated valves are normally in their required (open) safeguards position, they have redundant position indications and alarms, and they also receive confirmatory open actuation signals. These motor-operated valves have their power removed and locked out, and Surveillance Requirements that verify proper position and power lockout.

The ESF Actuation Subsystem Logic (ILPs and CIMs) within a division is tested every 24 months.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.15.~~2~~3

SR 3.3.15.~~2~~3 demonstrates that the pressurizer heater circuit breakers trip open in response to an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance ~~to provide complete testing of the assumed safety function~~. The OPERABILITY of these breakers is checked by opening these breakers using the Plant Control System.

......*

SR 3.3.15.~~3~~4

SR 3.3.15.~~3~~4 demonstrates that the RCP breakers trip open in response to an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance ~~to provide complete testing of the assumed safety function~~.

......*

SR 3.3.15.~~4~~5

SR 3.3.15.~~4~~5 demonstrates that the CVS letdown isolation valves actuate to the isolation position in response to an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance ~~to provide complete testing of the assumed safety function~~.

......*

SR 3.3.15.~~5~~6

SR 3.3.15.~~5~~6 demonstrates that the main feedwater and startup feedwater pump breakers trip open in response to an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance ~~to provide complete testing of the assumed safety function~~.

......*

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.15.67

SR 3.3.15.67 demonstrates that the auxiliary spray and purification line isolation valves actuate to the isolation position in response to an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance to provide complete testing of the assumed safety function.

Technical Specification Bases B 3.3.16, Engineered Safety Feature Actuation System (ESFAS) Actuation Logic – Shutdown

SURVEILLANCE REQUIREMENTS

SR 3.3.16.1

SR 3.3.16.1 is the performance of an ACTUATION LOGIC TEST on the ESF Coincidence Logic. This test, in conjunction with the individual device functional tests throughout the Technical Specifications demonstrate that actuated devices respond to an actual or simulated actuation signal. The ACTUATION LOGIC TEST demonstrates that the ESF Local Coincidence Logic (LCL subsystems) performs the required coincidence logic using injected, partial actuation signals and communicates system actuation signals to the ILP inputs in the ESF Actuation Subsystem Logic (Integrated Logic Cabinets (ILCs)). The ESF coincidence logic and ESF actuation subsystems LCL subsystems within a division are tested every 92 days on a STAGGERED TEST BASIS.

......*

If the ACTUATION LOGIC TEST cannot 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 LCL to ILP test feature provides verification of proper operation of the ESF LCL process modules (PMs), high speed link (HSL) communication, and ILP PMs. The test signal is injected at the ESF LCL PM and monitored at the ILP PMs. The ACTUATION LOGIC TEST provides overlap with the ACTUATION LOGIC OUTPUT TEST in SR 3.3.16.2 by verifying communication of system actuation signals from the ESF Local Coincidence Logic to the ESF Actuation Subsystem ILPs.

……*

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.16.2

SR 3.3.16.2 is the performance of an ACTUATION LOGIC OUTPUT TEST (ALOT) on the ESF Actuation. The ALOT demonstrates that both of the redundant signal paths from the inputs to the ILPs through the CIM logic and CIM output driver circuits (ILP to actuator test) in the ESF Actuation Subsystem Logic process injected LCL system actuation signals for the applicable actuation Function. During this test, a signal is sent back to the Maintenance and Test Panel (MTP) subsystem to determine if the CIM 2oo2 logic was satisfied and a component control signal was sent to the actuated device. As such, the ALOT may be performed in conjunction with other testing (e.g., automatic actuation Surveillance Requirements which verify correct valve positioning on an actual or simulated actuation signal).

The CIM can be allowed to actuate its end device in this test. There are certain end devices that are not expected to be actuated, such as the squib valves (ADS Stage 4 squib valves tested under SR 3.4.11.5, IRWST injection and recirculation squib valves tested under SR 3.5.6.9) and the following passive core cooling system motor-operated valves:

- Both accumulator discharge line motor-operated valves;
- Both in-containment refueling water storage tank gravity injection line motor-operated valves; and
- The passive residual heat removal heat exchanger inlet line motor-operated valve.

These motor-operated valves are normally in their required (open) safeguards position, they have redundant position indications and alarms, and they also receive confirmatory open actuation signals. These motor-operated valves have their power removed and locked out, and Surveillance Requirements that verify proper position and power lockout.

The ESF Actuation Subsystem Logic (ILPs and CIMs) within a division is tested every 24 months.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.16.~~2~~3

SR 3.3.16.~~2~~3 demonstrates that the RCP breakers trip open in response to an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance ~~to provide complete testing of the assumed safety function~~. 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. The SR is modified by a Note stating that the SR is only required to be met in MODE 5.

SR 3.3.16.~~3~~4

SR 3.3.16.~~3~~4 demonstrates that the CVS letdown isolation valves actuate to the isolation position in response to an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance ~~to provide complete testing of the assumed safety function~~.

......*

SR 3.3.16.~~4~~5

SR 3.3.16.~~4~~5 demonstrates that the Spent Fuel Pool Cooling containment isolation valves actuate to the isolation position in response to an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance ~~to provide complete testing of the assumed safety function~~.

Technical Specification Bases B 3.4.11, Automatic Depressurization System (ADS) - Operating

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.4.11.4

This SR verifies that each Stage 1, 2, and 3 ADS valve actuates to the correct position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance ~~to provide complete testing of the assumed safety function~~.

......*

SR 3.4.11.5

This SR verifies that each Stage 4 ADS valve actuates to the correct position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance to provide complete testing of the assumed safety function. 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.

Technical Specification Bases B 3.5.2, Core Makeup Tanks (CMTs) – Operating

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.5.2.7

This SR verifies that CMT outlet isolation valve actuates to the correct position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance to provide complete testing of the assumed safety function. 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.

Technical Specification Bases B 3.5.4, Passive Residual Heat Removal Heat Exchanger (PRHR HX) – Operating

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.5.4.8

This SR verifies that both PRHR HX air operated outlet isolation valves and both IRWST gutter isolation valves actuate to the correct position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance to provide complete testing of the assumed safety function. 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.

Technical Specification Bases B 3.5.6, In-containment Refueling Water Storage Tank (IRWST) – Operating

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.5.6.9

This SR ensures that each IRWST injection and containment recirculation squib valve actuates to the correct position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance~~ to provide complete testing of the assumed safety function~~. 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 ...*...*...*

Technical Specification Bases B 3.6.3, Containment Isolation Valves

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.6.3.5

Automatic containment isolation valves close on a containment isolation signal to prevent leakage of radioactive material from containment following a DBA. This SR ensures that each automatic containment isolation valve will actuate to its isolation position on a containment isolation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance~~ to provide complete testing of the assumed safety function~~. This surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The 24 month Frequency is based ...*...*...*

Technical Specification Bases B 3.6.6, Passive Containment Cooling System (PCS)

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.6.6.4

This SR requires verification that each automatic isolation valve actuates to its correct position upon receipt of an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap with this Surveillance. This Surveillance is not required for valves that are locked, sealed, or otherwise secured in the required position under administrative controls. The 24 month Frequency is based ...*...*...*

Technical Specification Bases B 3.6.9, Vacuum Relief Valves

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.6.9.3

This SR ensures that each vacuum relief motor operated valve will actuate to the open position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance ~~to provide complete testing of the assumed safety function~~. The Frequency of 24 months is based on the need to ...*...*...*

Technical Specification Bases B 3.7.2, Main Steam Line Flow Path Isolation Valves

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.7.2.4

This SR ensures that each MSIV bypass and steam line drain valve will actuate to its isolation position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance ~~to provide complete testing of the assumed safety function~~. The 24 month Frequency is based on the need to ...*...*...*

Technical Specification Bases B 3.7.3, Main Feedwater Isolation Valves (MFIVs) and Main Feedwater Control Valves (MFCVs)

SURVEILLANCE REQUIREMENTS

SR 3.7.3.1

This SR verifies that the closure time of each MFIV and MFCV is ≤ 5.0 seconds, on an actual or simulated actuation signal. The MFIV and MFCV isolation times are assumed in the accident and containment analyses. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance to provide complete testing of the assumed safety function. This Surveillance is normally performed upon returning the unit to operation following a refueling outage. These valves should not be tested at power, since even a part stroke exercise increases the risk of a valve closure when the unit is generating power. This is consistent with the ASME OM Code (Ref. 2) quarterly stroke requirements during operation in MODE 1 or 2.

Technical Specification Bases B 3.7.6, Main Control Room Emergency Habitability System (VES)

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.7.6.7

Verification that the VBS isolation valves and the Sanitary Drainage System (SDS) isolation valves are OPERABLE and will actuate upon demand is required every 24 months to ensure that the MCRE can be isolated upon loss of VBS operation. The ACTUATION LOGIC OUTPUT TEST provides overlap with this Surveillance.

Technical Specification Bases B 3.7.7, Startup Feedwater Isolation and Control Valves

SURVEILLANCE REQUIREMENTS

......*

SR 3.7.7.2

This SR ensures that each startup feedwater isolation valve and startup feedwater control valve will actuate to its isolation position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlaps with this Surveillance to provide complete testing of the assumed safety function.

Technical Specification Bases B 3.7.10, Steam Generator (SG) Isolation Valves

SURVEILLANCE REQUIREMENTS (continued)

......*

SR 3.7.10.3

This Surveillance verifies that each SG PORV, SG PORV block valve, and SG blowdown isolation valve actuates to the isolation position on an actual or simulated actuation signal. The ACTUATION LOGIC OUTPUT TEST provides overlap~~s~~ with this Surveillance~~ to provide complete testing of the assumed safety function~~.

......*