UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION II
245 PEACHTREE CENTER AVENUE NE, SUITE 1200
ATLANTA, GEORGIA 30303-1257

June 19, 2012

Mr. B. L. Ivey
Vice President, Regulatory Affairs
Southern Nuclear Operating Company
P.O. Box 1295
BIN BO22
Birmingham, AL 35201

SUBJECT: SOUTHERN NUCLEAR OPERATING COMPANY VOGTLE ELECTRIC GENERATING PLANT UNITS 3 & 4 - NRC ITAAC INSPECTION - INSPECTION REPORTS 05200025 /2012-009, 05200026/2012-009, AND NOTICE OF VIOLATION

Dear Mr. Ivey:

On May 25, 2012, the U.S. Nuclear Regulatory Commission (NRC) completed an inspection at the Westinghouse Electric Company facility located in Warrendale, Pennsylvania, to review work activities conducted on behalf of Vogtle Electric Generating Plant (VEGP) Units 3 & 4. The enclosed inspection report documents the inspection results that were discussed during an initial exit meeting on April 13, 2012, and during the final exit meeting on May 25, 2012, with members of your staff.

During the inspection, the NRC staff examined activities associated with Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) 2.5.2.11.b and 2.5.2.12 conducted under your combined license (COL) to confirm compliance with the Commission's rules and regulations, and with the conditions of your COL. Within these areas, the inspectors reviewed selected procedures, records, design documents, and conducted interviews.

Based on the results of this inspection, the NRC has identified an issue that was evaluated under the construction significance determination process as having very low safety significance (Green). The NRC has also determined that one violation is associated with this issue.

The violation was evaluated in accordance with the NRC Enforcement Policy, Section 2.3.2 and the temporary enforcement guidance outlined in enforcement guidance memorandum (EGM) 11-006. The current Enforcement Policy is included on the NRC's Web site at (http://www.nrc.gov/about-nrc/regulatory/enforcement/enforce-pol.html). The violation is cited in the enclosed Notice of Violation (Notice) and the circumstances surrounding it are described in

detail in the enclosed report. As described in Section 2.3, “Disposition of Violations,” of the NRC Enforcement Policy, the violation is cited in the Notice, because for reactor facilities under construction in accordance with 10 CFR Part 52, the site corrective action program must have been demonstrated to be adequate prior to the issuance of non-cited violations for NRC-identified violations. As of this inspection, the NRC had not yet made this determination for VEGP Units 3 & 4.

You are required to respond to this letter and should follow the instructions specified in the enclosed Notice when preparing your response. If you have additional information that you believe the NRC should consider, you may provide it in your response to the Notice. The NRC review of your response to the Notice will also determine whether further enforcement action is necessary to ensure compliance with regulatory requirements. If you contest the violation or significance of the NOV, you should provide a response within 30 days of the date of this inspection report, with the basis for your denial, to the Nuclear Regulatory Commission, ATTN: Document Control Desk, Washington DC 20555-0001, with copies to: (1) the Regional Administrator, Region II; (2) the Director, Office of Enforcement, United States Nuclear Regulatory Commission, Washington, DC 20555-0001; and (3) NRC Senior Resident Inspector at VEGP Units 3 and 4. If you disagree with the cross-cutting aspect assigned to the finding in this report, you should provide a response within 30 days of the date of this inspection report, with the basis for your disagreement, to the Regional Administrator, Region II, and the NRC Senior Resident Inspector at VEGP Units 3 and 4.

In accordance with 10 CFR 2.390 of the NRC's "Rules of Practice," a copy of this letter, its Enclosures, and your response will be made available electronically for public inspection in the NRC Public Document Room or from the NRC's document system (ADAMS), accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.html. To the extent possible, your response should not include any personal privacy or proprietary information so that it can be made available to the Public without redaction. If personal privacy or proprietary information is necessary to provide an acceptable response, then please provide a bracketed copy of your response that identifies the information that should be protected, and a redacted copy of your response that deletes such information. If you request that such material is withheld from public disclosure, you must specifically identify the portions of your response that you seek to have withheld and provide in detail the bases for your claim (e.g., explain why the disclosure of information will create an unwarranted invasion of personal privacy, or provide the information required, by 10 CFR 2.390(b), to support a request for withholding confidential commercial or

financial information). If safeguards information is necessary to provide an acceptable response, please provide the level of protection described in 10 CFR 73.21.

Sincerely,

/RA/

Mark S. Lesser, Chief
Construction Inspection Branch 1
Division of Construction Inspection

Docket Nos: 52-00025, 52-00026
Combined Licenses (COL): NPF-91 (Unit 3) and
NPF-92 (Unit 4)

Enclosures:
1. Notice of Violation (Notice)
2. NRC Inspection Report 052-00025/2012-009; 052-00026/2012-009;
   w/Attachment: Supplemental Information

cc w encl: (See Pages 4-7)

financial information). If safeguards information is necessary to provide an acceptable response, please provide the level of protection described in 10 CFR 73.21.

Sincerely,

/RA/

Mark S. Lesser, Chief
Construction Inspection Branch 1
Division of Construction Inspection

Docket Nos: 52-00025, 52-00026
Combined Licenses (COL): NPF-91 (Unit 3) and NPF-92 (Unit 4)

Enclosures:
1. Notice of Violation (Notice)
2. NRC Inspection Report 052-00025/2012-009; 052-00026/2012-009; w/Attachment: Supplemental Information

cc w encl: (See Page 4-7)

Distribution w/encl:
Region II Regional Coordinator, OEDO (M. Kotzalas)
M.Brown, NRO
T. Kozak, NRO
J. Moorman, RII
T. Reis, RII
C. Ogle, RII
J. Yerokun, RII
M. Ernstes, RII
S. Freeman, RII
M. Lesser, RII
K. O'Donohue, RII
G. Khouri, RII
J.Kent, RII
J. Fuller, RII
C. Abbott, RII
C. Huffman, RII
ConE_Resource@nrc.gov
NRO_cROP Resource@nrc.gov
PUBLIC

X PUBLICLY AVAILABLE ☐ NON-PUBLICLY AVAILABLE ☐ SENSITIVE **X** NON-SENSITIVE
ADAMS: **X** Yes ACCESSION NUMBER: ML12171A058 **X** SUNSI REVIEW COMPLETE **X** FORM 665 ATTACHED

OFFICE	RII:DCI	RII:DCI	RII:DCI	NRO, HQ	HOR, HQ	NRO, HQ	
SIGNATURE	MSL for TNF1	TNF1	NDK1	WAR1/via e-mail	WXM4/via e-mail	TRF2/via e-mail	
NAME	L. Castelli	T. Fanelli	N. Karlovich	W. Roggenbrodt	W. Morton	T. Fredette	
DATE	6/ 14 /2012	6/ 14 /2012	6/ 14 /2012	6/ 15 /2012	6/ 18 /2012	6/ 13 /2012	
E-MAIL COPY	**YES** NO	**YES** NO	**YES** NO	**YES** NO	**YES** NO	**YES** NO	

OFFICIAL RECORD COPY DOCUMENT NAME: G:\CCI\INSPECTION REPORTS\NEW REACTORS\VOGTLE\2012 REPORTS\VOG IR 2012009 IR.DOCX

cc w/encl:

Office of Attorney General
Law Department
132 Judicial Building
Atlanta, GA 30312

Resident Manager
Oglethorpe Power Corporation
Alvin W. Vogtle Nuclear Plant
7821 River Road
Waynesboro, GA 30830

Lucious Abram
Commissioner -
Burke's County Commissioner
P. O. Box 1626
Waynesboro, GA 30830

Anne F. Appleby
Olgethorpe Power Corporation
2100 East Exchange Place
Tucker, GA 30084

Ms. Michele Boyd
Legislative Director
Energy Program
Public Citizens Critical Mass Energy
and Environmental Program
215 Pennsylvania Avenue, SE
Washington, DC 20003

County Commissioner
Office of the County Commissioner
Burke County Commission
Waynesboro, GA 30830

Director
Consumer's Utility
Counsel Division
Governor's Office of Consumer Affairs
2 Martin Luther King, Jr. Drive
Plaza Level East, Suite 356
Atlanta, GA 30334-4600

Mr. James C. Hardeman
Environmental Radiation Program Manager
Environmental Protection Division
Georgia Dept. of Natural Resources
4220 International Pkwy, Suite 100
Atlanta, GA 30354-3906

Lisa Higdon
Southern Nuclear Op. Co.
Document Control Coordinator
42 Inverness Center parkway
Attn: B236
Birmingham, AL 35242

Rita Kilpatrick
250 Arizona Ave.
Atlanta, GA 30307

Stephen E. Kuczynski
Chairman, President and CEO
Southern Nuclear
P.O. Box 1295
Birmingham, AL 35201

Mr. Reece McAlister
Executive Secretary
Georgia Public Service Commission
Atlanta, GA 30334

Mr. Joseph A. (Buzz) Miller
Executive Vice President
Southern Nuclear Operating Company
241 Ralph McGill Blvd.
BIN 10240
Atlanta, GA 30308-3374

Resident Inspector
Vogtle Plant
8805 River Road
Waynesboro, GA 30830

cc w/encl: (continued on page 5)

cc w/encl: (continued from page 4)

Elaine Sikes
Burke County Library
130 Highway 24 South
Waynesboro, GA 30830

Mr. Jerry Smith
Commissioner, District 8
Augusta-Richmond County Commission
1332 Brown Road
Hephzibah, GA 30815

Gene Stilp
1550 Fishing Creek Valley Road
Harrisburg, PA 17112

Mr. Robert E. Sweeney
IBEX ESI
4641 Montgomery Avenue
Suite 350
Bethesda, MD 20814

George B. Taylor, Jr.
2100 East Exchange Pl
Atlanta, GA 30084-5336

Email
agaughtm@southernco.com (Amy Aughtman)
agbaker@southernco.com (Ann Baker)
anfaulk@southernco.com (Nicole Faulk)
APH@NEI.org (Adrian Heymer)
awc@nei.org (Anne W. Cottingham)
Bill.Jacobs@gdsassociates.com (Bill Jacobs)
blivey@southernco.com (Pete Ivey)
bob.masse@opc.com (Resident Manager)
bobbie@wand.org (Bobbie Paul)
BrinkmCB@westinghouse.com (Charles Brinkman)
bwwaites@southernco.com (Brandon Waites)
chmahan@southernco.com (Howard Mahan)
crpierce@southernco.com (C.R. Pierce)
cwaltman@roe.com (C. Waltman)
dahjones@southernco.com (David Jones)
danawill@southernco.com (Dana Williams)
david.hinds@ge.com (David Hinds)
david.lewis@pillsburylaw.com (David Lewis)
david.siefken@hq.doe.gov (David Siefken)
dlfulton@southernco.com (Dale Fulton)
ed.burns@earthlink.net (Ed Burns)
edavis@pegasusgroup.us (Ed David)

cc w/encl: (continued on page 6)

cc w/encl: (continued from page 5)

enweathe@southernco.com (Beth Thomas)
erg-xl@cox.net (Eddie R. Grant)
G2NDRMDC@southernco.com (SNC Document Control)
james1.beard@ge.com (James Beard)
jamiller@southernco.com (Buzz Miller)
jbtomase@southernco.com (Janice Tomasello)
jenmorri@southernco.com (Jennifer Buettner)
jim.riccio@wdc.greenpeace.org (James Riccio)
jim@ncwarn.org (Jim Warren)
jlpember@southernco.com (John Pemberton)
Joseph_Hegner@dom.com (Joseph Hegner)
jrjohnso@southernco.com (Randy Johnson)
jtdavis@southernco.com (Jim Davis)
jtgasser@southernco.com (Jeffrey Gasser)
karen.patterson@ttnus.com (Karen Patterson)
kim.haynes@opc.com (Kim Haynes)
KSutton@morganlewis.com (Kathryn M. Sutton)
kwaugh@impact-net.org (Kenneth O. Waugh)
lchandler@morganlewis.com (Lawrence J. Chandler)
maria.webb@pillsburylaw.com (Maria Webb)
mark.beaumont@wsms.com (Mark Beaumont)
markus.popa@hq.doe.gov (Markus Popa)
matias.travieso-diaz@pillsburylaw.com (Matias Travieso-Diaz)
mdrauckh@southernco.com (Mark Rauckhorst)
media@nei.org (Scott Peterson)
mike.price@opc.com (M.W. Price)
mike_moran@fpl.com (Mike Moran)
MSF@nei.org (Marvin Fertel)
nirsnet@nirs.org (Michael Mariotte)
nlhender@southernco.com (Nancy Henderson)
Nuclaw@mindspring.com (Robert Temple)
patriciaL.campbell@ge.com (Patricia L. Campbell)
Paul@beyondnuclear.org (Paul Gunter)
pbessette@morganlewis.com (Paul Bessette)
rhenry@ap.org (Ray Henry)
RJB@NEI.org (Russell Bell)
sabinski@suddenlink.net (Steve A. Bennett)
sblanton@balch.com (Stanford Blanton)
sfrantz@morganlewis.com (Stephen P. Frantz)
sjackson@meagpower.org (Steven Jackson)
skauffman@mpr.com (Storm Kauffman)
sroetger@psc.state.ga.us (Steve Roetger)
stephan.moen@ge.com (Stephan Moen)
taterrel@southernco.com (Todd Terrell)
tcmoorer@southernco.com (Thomas Moorer)
tlubnow@mpr.com (Tom Lubnow)
Tom.Bilik@nrc.gov (Thomas Bilik)
tomccall@southernco.com (Tom McCallum)

cc w/encl: (continued on page 7)

cc w/encl: (continued from page 6)

Vanessa.quinn@dhs.gov (Vanessa Quinn)
Wanda.K.Marshall@dom.com (Wanda K. Marshall)
wasparkm@southernco.com (Wesley A. Sparkman)
whelmore@aol.com (Bill Elmore)

NOTICE OF VIOLATION

Southern Nuclear Operating Company, Inc. (SNC) Docket Nos: 05200025, 05200026
Vogtle Electric Generating Plant (VEGP) Units 3 and 4 License Nos: NPF-91, NPF-92

During an NRC inspection, completed May 25, 2012, one violation of NRC requirements was identified. In accordance with the NRC Enforcement Policy, the violation is listed below:

10 CFR 50 Appendix B Criterion III, Design Control, requires, in part, that measures be established to assure that applicable regulatory requirements and the design basis, as defined in § 50.2 and as specified in the license application, for those structures, systems, and components to which this appendix applies are correctly translated into specifications, drawings, procedures, and instructions.

Vogtle Units 3 & 4 Final Safety Analysis Report Chapter 7 incorporates by reference the AP 1000 Design Control Document (DCD) Revision 19.

DCD Subsection 7.1.2.14.1, "Design Process," states "WCAP-16096-NP-A (Reference 9) … describes design processes that will be used for AP1000." WCAP-16096-NP-A Section 5.1 Software Verification and Validation Plan states that, "This SVVP complies with Reference 8 [IEEE Std. 1012-1998]." IEEE Std. 1012-1998 Subsection 5.4.2 states, in part, that "The V&V effort shall perform, as appropriate for the selected software integrity level, the minimum V&V tasks," including Software Requirements Evaluation, Interface Analysis, Criticality Analysis, Hazard Analysis, and Risk Analysis.

DCD Subsection 7.1.2.14.1, "Design Process," states "Westinghouse Quality Management System (Reference 21) describes design processes that will be used for AP1000." Westinghouse Quality Management System Subsection 4.2.9, Computer Software states, in part, "Computer software developed as a deliverable safety-related product … is developed, controlled, and maintained in accordance with procedures and instructions that comply with ASME NQA-1, (i.e., Part I Supplement 11S-2; Part II, Subpart 2.7)." NQA-1-1994 Subpart 2.7 Section 4 states in part, "Software verification and validation shall be performed by individuals other than those who designed the software."

DCD Subsection 7.1.4.2 , "Conformance with Industry Standards," states, "The instrumentation and control systems are designed in accordance with guidance provided in applicable portions of the following standards…IEEE 1074-1995; "IEEE Standard for Developing Software Life Cycle Processes." IEEE Std. 1074-1995 Section 5 describes the processes that must be performed during the development of a software product and states that "Prior to the distribution of the Preliminary Software Requirements… [and] distribution of the Output Information…[and] distribution of the Software Requirements the following Processes shall be invoked [which includes Verification and Validation]." Moreover Subsection 5.1.3.2 states that, "the developer shall analyze the software requirements to determine traceability, clarity, validity, testability, safety, and any other project-specific characteristics."

DCD Subsection 7.1.7 lists WCAP-16097-NP-A as a Tier 2* reference. WCAP-16097-NP-A, Section 4 identifies compliance to the codes and standards applicable for the Common Q designs and states that it conforms to IEEE Std. 830-1993 as endorsed by Reg. Guide 1.172 and as described in the Common Q SPM. IEEE 830-1993 Subsection 4.3, as

modified by Reg. Guide 1.172, Rev. 0, states the SRS must be complete, unambiguous, and be ranked for importance and/or stability. The SRS is complete if and only if, it includes all significant requirements, whether relating to functionality, performance, design constraints, attributes, or external interfaces. The SRS is unambiguous if, and only if, every requirement stated therein has only one interpretation. The SRS is ranked for importance and/or stability if each requirement in it has an identifier to indicate either the importance or stability of that particular requirement.

Contrary to the above, as of May 25, 2012, the licensee failed to assure that applicable regulatory requirements and the design basis, as defined in § 50.2 and as specified in the license application, for the Protection and Safety Monitoring System, were correctly translated into specifications, drawings, procedures, and instructions in that:

1. The verification and validation (V&V) effort did not adequately perform, the minimum V&V tasks including software requirements evaluation, interface analysis, criticality analysis, hazard analysis, and risk analysis, in that; the required input documents were not available to perform the hazard analysis, criticality analysis, and risk analysis, and the software requirements specification was inadequate to perform the software requirements evaluations and interface analysis.

2. The software V&V activities included individuals who designed the software in that; the V&V team took credit for the design team's activities, thus the V&V activities were not performed independently from the design team.

3. The developer did not analyze the software requirements to determine safety characteristics in that; a software hazard analysis of the software requirements specification was not performed.

4. The reusable software element document (RSED) development did not follow the prescribed software lifecycle process and activities, in that V&V tasks were not invoked. The RSEDs requirements were not analyzed to determine traceability, clarity, validity, testability, safety, or other project specific characteristics.

5. The SRS was ambiguous, not complete, and was not ranked for importance, in that; the software requirement for the reactor coolant flow compensation was incomplete and ambiguous as more than one interpretation of the software requirement could be implemented, the requirements for loss and subsequent restoration of power were incomplete, and no requirements were ranked for importance.

This violation is associated with a Green SDP ITAAC Finding.

Pursuant to the provisions of 10 CFR 2.201, SNC is hereby required to submit a written statement, or explanation, to the U.S. Nuclear Regulatory Commission, ATTN: Document Control Desk, Washington, DC 20555-0001 with a copy to the Regional Administrator, Region II, and a copy to the NRC Resident Inspector for Vogtle Units 3 and 4, within 30 days of the date of the letter transmitting this Notice of Violation (Notice). This reply should be clearly marked as a "Reply to a Notice of Violation," and should include for the violation: (1) the reason for the violation, or if contested, the basis for disputing the violation, (2) the corrective steps that have been taken and the results achieved, (3) the corrective steps that will be taken to avoid further violations, and (4) the date when full compliance will be achieved. Your response may reference, or include, previous docketed correspondence, if the correspondence adequately

addresses the required response. If an adequate reply is not received within the time specified in this Notice, an order or a Demand for Information may be issued as to why the license should not be modified, suspended, or revoked, or why such other action, as may be proper, should not be taken. Where good cause is shown, consideration will be given to extending the response time.

If you contest this enforcement action, you should also provide a copy of your response, with the basis for your denial, to the Director, Office of Enforcement, United States Nuclear Regulatory Commission, Washington, DC 20555-0001.

Because your response will be made available electronically for public inspection in the NRC Public Document Room or from the NRCs document system (ADAMS), accessible from the NRC Web site at http://www.nrc.gov/reading-rm/adams.html, to the extent possible, it should not include any personal privacy, proprietary, or safeguards information so that it can be made available to the public without redaction. If personal privacy or proprietary information is necessary to provide an acceptable response, then please provide a bracketed copy of your response that identifies the information that should be protected, and a redacted copy of your response that deletes such information. If you request withholding of such material, you must specifically identify the portions of your response that you seek to have withheld, and provide in detail the bases for your claim of withholding (i.e., explain why the disclosure of information will create an unwarranted invasion of personal privacy or provide the information required by 10 CFR 2.390(b) to support a request for withholding confidential commercial or financial information). If safeguards information is necessary to provide an acceptable response, please provide the level of protection described in 10 CFR 73.21.

In accordance with 10 CFR 19.11, you may be required to post this Notice within two working days of receipt.

Dated this 19th day of June 2012.

U.S. NUCLEAR REGULATORY COMMISSION
Region II

Docket Nos:	05200025 (Unit 3); 05200026 (Unit 4)
License Nos:	NPF-91 (Unit 3); NPF-92 (Unit 4)
Report Nos:	05200025/2012-009; 05200026/2012-009
Licensee:	Southern Nuclear Operating Company, Inc. (SNC)
Facility:	VEGP Units 3 and 4
Location:	Waynesboro, GA
Inspection Dates:	March 26 through May 25, 2012
Inspectors:	Lisa Castelli, Senior Construction Inspector, DCI/CIB1, Region II Theo Fanelli, Construction Inspector, DCI/CIB1, Region II Nick Karlovich, Construction Inspector, DCI/CIB1, Region II William Roggenbrodt, Electronics Engineer, NRO/DE/ICE, HQ Wendell Morton, Electronics Engineer, NRO/DE/ICE, HQ Tom Fredette, Reactor Operations Engineer, NRO/DCIP, HQ
Accompanying Personnel:	Tomy Nazario, Acting Branch Chief, DCI/CIB1, Region II Jimi Yerokun, Deputy Director, DCI, Region II
Approved by:	Mark S. Lesser, Chief Construction Inspection Branch 1 Division of Construction Inspection

SUMMARY OF FINDINGS

Inspection Report (IR) 05200025/2012009, IR 05200026/2012009; 03/26/2012 through 05/25/2012; Vogtle Electric Generating Plant (VEGP) Units 3 and 4, Digital Instrumentation and Control (DI&C) System/Software Design Acceptance Criteria (DAC) – Related to ITAAC.

This report covers an announced inspection by Region II and Headquarters based inspectors at the Westinghouse Facility located in Warrendale, Pennsylvania. One Green Inspection, Test, Analyses, and Acceptance Criteria (ITAAC) finding which involved a violation was identified. The violation was evaluated in accordance with the NRC Enforcement Policy, Section 2.3.2, and the temporary enforcement guidance outlined in enforcement guidance memorandum (EGM) 11-006. The significance of most findings is indicated by their color (Green, White, Yellow, or Red) using Inspection Manual Chapter (IMC) 2519P, "Construction Significance Determination Process," (SDP). Cross-cutting aspects were determined using IMC 0613P, Appendix F, "Construction Safety Focus Components and Aspects." The Nuclear Regulatory Commission's (NRC's) program for overseeing the safe construction of commercial nuclear power reactors is described in IMC 2506, "Construction Reactor Oversight Process General Guidance and Basis Document."

A. NRC and Self-Revealed Findings

Cornerstone: Design/Engineering

Green. An NRC identified ITAAC finding of very low safety significance (Green) which involved a violation (VIO) of 10 CFR Part 50, Appendix B, Criterion III, "Design Control," was identified by the inspectors on May 25, 2012, regarding the licensee's failure to assure that applicable regulatory requirements and the design basis, as defined in § 50.2 and specified in the license application, for the Protection and Safety Monitoring System (PMS) were correctly translated into specifications, drawings, procedures, and instructions. Specifically:

- The verification and validation (V&V) effort did not adequately perform the minimum V&V tasks including software requirements evaluation, interface analysis, criticality analysis, hazard analysis, and risk analysis;
- The V&V of the System Definition (requirements) phase activities was not performed independently;
- Reusable software element documents (RSED) did not follow the prescribed life cycle activities;
- A software hazard analysis of the software requirements specification (SRS) was not performed;
- The SRS was ambiguous, incomplete and was not ranked for importance.

At the time of the exit meeting for this report, the planned corrective actions for these issues were being evaluated by the licensee. These issues were entered into a corrective action program as Condition Report 438475.

The inspectors determined this issue is more than minor because, if left uncorrected, it represents a failure to implement an adequate process and quality oversight function that could render the quality of the construction activity unacceptable or indeterminate, and it could adversely affect the closing of an ITAAC. The finding affected the objective of the

Design/Engineering Cornerstone, which is to ensure that licensee's processes are adequately developed and implemented for design control. The finding was determined to be an ITAAC Finding because examples of this finding are material to the acceptance criteria of ITAAC 2.5.2.12, in that; software requirements were not ranked for importance and the V&V team was not independent of the design team. The inspectors evaluated the finding using the construction SDP and determined that, because there were no issues identified that would reasonably be expected to impair the design function of the PMS, the finding screened as Green. The finding was cross-cutting in the area of baseline inspection, work practices, because the licensee failed to ensure supervisory and management oversight of work activities associated with the PMS software development such that the construction quality was supported. [A.4(c)]. (Section 1.2503.1).

REPORT DETAILS

1. CONSTRUCTION REACTOR SAFETY

Design/Engineering

2503 ITAAC-Related Inspections

.1 ITAAC No/Family: 2.5.2.11.b / 10F
ITAAC No/Family: 2.5.2.12 / 10F

a. Inspection Scope

The inspectors performed direct inspection of work associated with Inspections, Tests, Analyses and Acceptance Criteria (ITAACs) 2.5.2.11.b and 2.5.2.12. (Attachment, Table 1) using the guidance in Inspection Procedure (IP) 65001.22, "Inspection of Digital Instrumentation and Control (DI&C) System/Software Design Acceptance Criteria (DAC)-Related ITAAC."

65001.22-A1.03.01, Inspection of Software Management Plan
65001.22-A1.03.03, Inspection of Software Configuration Management Plan
65001.22-A1-03.04, Inspection of Software Verification & Validation Plan
65001.22-A2.03.01, Digital I&C System Requirements
65001.22-A2.03.02, Software Requirements
65001.22-A2.03.03, Requirements Phase Documentation
65001.22-A2.03.04, Safety Analysis

System and Software Requirements

The inspectors reviewed the Westinghouse (WEC) AP1000 Design Control Document (DCD) as adopted by Southern Nuclear (SNC) for the Vogtle Electric Generating Plant (VEGP) Units 3&4 Final Safety Analysis Report (FSAR), AP1000 safety analyses, instrumentation and controls (I&C) system specifications, Protection and Safety Monitoring System (PMS)-specific specifications and functional requirements, PMS functional and logic drawings, and the requirements traceability matrix (RTM) to verify that selected I&C reactor trip functions and engineered safety feature (ESF) functions were adequately and accurately translated to discrete digital software requirements as itemized in the PMS Software Requirements Specification (SRS). The SRS document is the output product from the completion of the System Definition (requirements) phase of the digital I&C (DI&C) software life cycle (SLC) development process for the PMS as delineated in the WEC Software Program Manual (SPM) and ITAAC 2.5.2.11.b. The inspectors used the RTM to conduct requirements traceability of a risk-informed sample of PMS protective functions, including pressurizer pressure reactor trip, pressurizer level reactor trip, overpower and overtemperature delta-T (OPΔT/OTΔT) reactor trips, manual channel bypass, and ESF actuation and control functionality, including In-containment Refueling Water Storage Tank initiation. Characteristics of the SRS and selected software requirements were verified against criteria in IEEE Standard (Std.) 830-1993 "IEEE Recommended Practice for Software Requirements Specifications," as endorsed by NRC Regulatory Guide (RG) 1.172 "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Documents

reviewed during this inspection activity are listed in the List of Documents Reviewed section of this report.

Requirements Phase Documentation

The inspectors interviewed personnel and reviewed documentation related to Independent Verification and Validation (IV&V) organization and activities within the licensee's System Definition (requirements activities) phase of the SLC The inspectors reviewed the DCD, FSAR, and SPM for Common Q Systems [WCAP-16096-NP-A, Rev.1A], the Verification & Validation Process for the Common Q System [WNA-PV-00009-GEN, Rev 3] and the AP1000 PMS IV&V Phase Summary Report [APP-PMS-GER-021, Rev 1]. In addition, the inspectors reviewed project specific requirements contained in the Design Process for the AP1000 Common Q Safety Systems Technical Report [WCAP-15927. Rev 2] and AP1000 Conformance with SRP Acceptance Criteria Technical Report [WCAP-15799, Rev 1].

The inspectors reviewed these documents to verify compliance with the criteria in IEEE Std. 1012-1998 "IEEE Standard for Software Verification and Validation," as endorsed by NRC RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." The inspectors assessed whether the IEEE 1012-1998 criteria was adequately implemented for the PMS System Definition phase. The inspectors reviewed the AP1000 PMS IV&V Phase Summary Report [APP-PMS-GER-021] for compliance with IEEE Std. 1012-1998 to determine if the required task inputs were adequately reviewed, assessed, and documented.

The inspectors reviewed various WEC procedures related to the open items (OIs) and the open items tracking system (OITS), and reviewed a set of OIs from the OITS database associated with the RTM. The inspectors conducted interviews with WEC personnel with direct responsibility for the creation and closure of OIs against the PMS Subsystem Requirements Specification, PMS System Design Specification, and the PMS SRS to verify whether changes to requirements processed through the OIs/OITS were accomplished in accordance with approved procedures and the licensee's 10 CFR Part 50 Appendix B program. Documents reviewed during this inspection activity are listed in the List of Documents Reviewed section of this report.

Requirements Safety Analysis

The inspectors reviewed the PMS Software Safety Plan, as incorporated into the Common Q SPM, the preliminary Software Hazards Analysis of the AP1000 PMS, the Project Computer Security Plan, and the Concept Phase Security Assessment to ascertain how the licensee and WEC were capturing and mitigating the impact of specific hazards associated with the development of PMS system and software requirements. The inspectors compared analyses that were performed and documented in the AP1000 PMS IV&V Phase Summary Report to those prescribed in IEEE Std. 1228-1994 (Software Safety Analysis) and the methodologies outlined in NUREG-6430 (Software Hazards Analysis). The inspectors assessed the quality of these analyses against commitments identified in the SPM, AP1000 DCD, and the licensee's FSAR. Documents reviewed during this inspection activity are listed in the List of Documents Reviewed section of this report.

Software Management

The inspectors assessed the quality of the implementation of the licensee's software management program as it affected the software development process against regulatory requirements related to design control to determine if measures have been established for the identification and control of design interfaces and for coordination among participating design organizations and measures to ensure that applicable regulatory requirements and the design basis have been correctly translated into specifications, drawings, procedures, and instructions. The inspectors interviewed responsible WEC personnel and reviewed SLC activities associated with software management. The inspectors assessed if commitments related to software development had been effectively implemented. The inspectors evaluated design control measures established in Tier 2* commitments and requirements identified in the licensee's FSAR and the WEC DCD. Documents reviewed during this inspection activity are listed in the List of Documents Reviewed section of this report.

b. Findings

Introduction: The inspectors identified a Green ITAAC Finding and a cited violation of 10 CFR 50, Appendix B, Criterion III, Design Control, for the licensee's failure to assure that applicable regulatory requirements and the design basis for the Protection and Safety Monitoring System were correctly translated into specifications, drawings, procedures, and instructions. Specifically, the licensee did not ensure the System Definition phase activities met all the regulatory requirements and Tier 2* design criteria in the licensee's FSAR including NQA-1-1994, IEEE Std. 1074-1995, IEEE Std. 830-1993, and IEEE Std. 1012-1998.

Description:

Verification and Validation Adequacy

WCAP-16096-NP-A Section 5.1, "Software Verification and Validation Plan," states that, "This SVVP complies with Reference 8" [IEEE Std. 1012-1998]. IEEE Std. 1012-1998 Subsection 5.4.2 states in part that, "The V&V effort shall perform, as appropriate for the selected software integrity level, the minimum V&V tasks for Requirements V&V." Table 1 of IEEE Std. 1012-1988 describes the minimum V&V tasks, task criteria, and required inputs and outputs. These documents include the criticality task report, software hazards analysis report, prior V&V task reports, the SRS, and the interface requirements specification (IRS).

The inspectors observed that APP-PMS-GER-021 identified no issues of significance related to the System Definition (requirements) phase activities. The criticality task report, software hazards analysis report, and prior V&V task reports could not be provided for the inspectors to review. The inspectors determined that the V&V tasks for the requirements phase were not completed as required by IEEE Std. 1012-1998. The inspectors determined, by review of APP-PMS-GER-021, that the drawings referenced in the SRS as software requirements were not reviewed by V&V.

The inspectors observed that the APP-PMS-J0R-001, "AP1000 Protection and Monitoring System Requirements Traceability Matrix," Rev. 1 (RTM) used by the V&V team listed some software requirements as new or "base" requirements, meaning that these new requirements were not based on predecessor system requirements. Since base requirements are new, compliance to previous system requirements could not be traced. The inspectors determined through interviews with WEC personnel that the base requirements were not part of the V&V review for traceability. The inspectors identified software requirements that were inaccurately identified in the SRS as base requirements for example; the timing requirement PMS_SRS-7605 establishes the timing for the executable structure elements used within the integrated logic processor (ILP) component control processor (CCP). PMS_SRS-7605 is listed as a base requirement in the RTM. The inspectors determined this is not a base requirement because it has a predecessor from APP-PMS-J4-020, "AP1000 PMS Subsystem Design Specification," Revision 3 Section 8, Time Response Requirements. The inspectors determined the V&V team had not adequately traced the base requirements to verify correctness. The inspectors determined the System Definition (requirements) phase V&V tasks were not completed, as no software requirement existed for some system requirements (i.e. functional diagrams) and some software requirements were listed as base requirements, but in fact, had predecessor system requirements.

Through interviews with WEC personnel, the inspectors determined that the V&V team did not evaluate the reusable software element document (RSED) requirements referenced in the SRS. The inspectors determined the documentation produced by V&V for the System Definition (requirements) phase did not serve as adequate technical disclosure for the claims made in APP-PMS-GER-021 Appendix A – Software Verification and Validation Requirements Phase Checklist. This is identified as Example One of VIO 05200025/2012009-01, 05200026/2012009-01, Inadequate Design Control of Software Development.

Independent Verification and Validation

The licensee's FSAR includes design commitments for development of safety-related software for the PMS. The WEC Quality Management System (QMS) Revision 5 requires the quality program for software development to comply with NQA-1-1994, "Quality Assurance Program Requirements for Nuclear Facilities." Generic software development criteria within the FSAR are contained in WCAP-16096-NP-A, which was required to be augmented by project specific constraints, such as applicable regulatory requirements, design bases, and related guidance. The inspectors determined that the independence requirement for safety related verification and validation (V&V) activities was not met.

NQA-1-1994 Subpart 2.7 requires in part, "Software verification and validation shall be performed by individuals other than those who designed the software." The inspectors determined that APP-PMS-GER-021 Section 2.2.2 describes the V&V team using design team peer reviews of safety related software requirements in order to verify correctness of the requirements specifications. The inspectors determined, through interviews with WEC V&V personnel, that they lacked the required skills to review and assess portions of the PMS design, so, they relied on design team personnel for those portions of the V&V review. The inspectors determined the V&V team did not have independence from the design organization in their reviews of safety related software as required by their procedures and regulatory requirements. This example is material to the Acceptance

Criteria of ITAAC 2.5.2.12, that states, in part, that requirements are provided for V&V including requirements for reviewer independence. This is identified as Example Two of VIO 05200025/2012009-01, 05200026/2012009-01, Inadequate Design Control of Software Development.

Software Hazards Analysis

IEEE Std. 1074-1995 Subsection 5.1.3.2 states in part that, the "developer shall analyze the software requirements to determine… safety… characteristics." Sections 3 and 5 of WCAP-16096-NP-A indicate the analysis identifies software contributions to the system hazards and it must identify all software requirements that have safety implications.

The inspectors determined that SPM Subsection 5.5.3.2 assigned responsibility for the System Definition (requirements) phase safety analysis review to the IV&V organization. IEEE 1012-1998 Section 5 clarifies that the design organization is responsible for the safety analysis and the V&V organization provides the body of evidence showing the software product satisfies its requirements. The inspectors determined the design organization did not perform a software hazard analysis for the System Definition phase of software development and therefore the V&V organization could not have verified it. Consequently, no software hazards were identified in the SRS, no documentation was provided identifying the software requirements that have safety implications, and no analysis was performed to identify the contributions that the software requirements would have to system hazards. The inspectors determined that assumptions were used to interpret system requirements and to generate approximately 485 new requirements (as identified in APP-PMS-GER-021) that have no predecessor requirements from the system design (base requirements) in the SRS, which created unanalyzed software hazards. As examples, the use of RSEDs for software requirements introduces extra software code that is not necessary to implement the system requirement. The extra code (dead code) has the potential to expose the PMS to an unexpected fault condition. Additionally, alarms that are consolidated into the same memory register could be exposed to the effects from single errors (e.g., PMS_SRS-7356). Moreover, the inspectors determined that some assumptions made in the SRS do not match the assumptions made in the preliminary Hazard Analysis (PHA) (WCAP-16592-P, "AP1000 PMS Software Hazards Analysis" Revision 2). WCAP-16592-P is considered preliminary because it was developed prior to actual software development. As examples, the PHA requires the main control room (MCR)/remote shutdown room (RSR) transfer switch signal to default to the Main Control Room upon a detected failure of the switch, while SRS requirement PMS_SRS_4549 requires the MCR/RSR transfer switch to hold the last good value, if present, else default to Main Control Room on BAD quality. Upon detection of a failed switch (BAD quality); PMS_SRS_4549 would go to the last known good value which would be either of the two positions the MCR or RSR not the MCR alone. Additionally, the AP1000 DCD Tier 1 Chapter 2, Section 2.5.2 states, "The PMS does not allow simultaneous bypass of two redundant channels." The inspectors determined that the RSED for 2 out of 4 logic contained code associated with parameters not used in this application (dead code) that could be configured to allow two channels to be bypassed simultaneously, which is unanalyzed in the PHA. These safety analyses deficiencies were not documented in APP-PMS-GER-021, and except for a checklist, there is no documentation to support any of the analyses performed by the V&V group to support software safety analysis activities. This is identified as Example Three of VIO 05200025/2012009-01, 05200026/2012009-01, Inadequate Design Control of Software Development.

Software Life Cycle Control of Reusable Software Element Documents (RSEDs)

The licensee's FSAR and AP1000 DCD identify commitments, without condition, to IEEE Std. 1074-1995 "IEEE Standard for Developing Software Lifecycle Processes," as endorsed by RG 1.173. Table 1.6-1 of the DCD captures these commitments in WCAP-16097-P-A, **"**Common Qualified Platform Topical Report**,"** which is referenced as a Tier 2* document for Chapter 7, "Instrumentation and Controls," Section 7.1 within Tier 2 information of the AP1000 DCD. IEEE Std. 1074-1995, as endorsed by RG 1.173, identifies the SLC processes and activities committed to by the licensee. RG 1.173 Section 2 states, in part, "compliance with IEEE Std 1074-1995 means that all mandatory activities are performed, that the requirements described as "shall" are met, and that all the inputs, outputs, activities, pre-conditions, and post-conditions mentioned by IEEE Std 1074-1995 are described or accounted for in the applicant's life cycle model." Additionally, RG 1.173 Section 1.1 states, in part, "The descriptions of input information, life cycle activity, and output information required by IEEE Std. 1074-1995 must identify applicable regulatory requirements, design bases, and related guidance." IEEE Std. 1074-1995 establishes the prescribed SLC processes and their activities that are to be executed in sequence for successive phases of the lifecycle. Section 5 "Development Process," states, "These are the processes that must be performed during the development of a software product." Subsection 5.1 "Requirement Process," requires three iterative activities to complete this process prior to the design phase. These activities are to define and develop software requirements (Subsection 5.1.3), to define and develop interface requirements (Subsection 5.1.4), both from the decomposed system requirements; and then to prioritize and integrate (Subsection 5.1.5) the software and interface requirements into an integrated SRS. V&V process activity (Subsection 7.1.4) is invoked for each of these activities individually before moving to the next activity. Subsection 5.1.3.2 states the (integrated) SRS to be "analyzed to determine traceability, clarity, validity, testability, safety, and any other project-specific characteristics." The inspectors determined that the RSEDs were not developed according to the life cycle processes mentioned above. RSEDs were used to implement complex aspects of the PMS such as; pressurizer water level density compensation, main control room/remote shutdown panel transfer switch override, OPΔT/OTΔT, and squib valve logic. The inspectors determined through interviews with WEC personnel that the RSEDs development did not include the required V&V process activities nor were they analyzed for the characteristics mentioned above. This is identified as Example Four of VIO 05200025/2012009-01, 05200026/2012009-01, Inadequate Design Control of Software Development.

Software Requirements Specification

IEEE Std. 830-1993 as endorsed by Reg. Guide 1.172 states, in part, that the SRS must be complete and unambiguous. The SRS is complete if, and only if, it includes all significant requirements, whether relating to functionality, performance, design constraints, attributes, or external interfaces. IEEE Std. 830-1993 also states that an SRS is unambiguous if, and only if, every requirement stated therein has only one interpretation. The inspectors determined through review of the SRS that portions of the PMS functional software requirements for reactor trip functions incorporated functional diagrams as software requirements. The inspectors determined through interviews that the functional diagrams could be interpreted in multiple ways. The inspectors

determined that the functional diagrams were not fully decomposed and described as discrete software requirements in the SRS.

The reactor coolant low flow reactor trip flow compensation function block is an example of a functional diagram not fully decomposed in the SRS. The SRS has a general requirement that states the system shall function in accordance with the functional diagrams. The inspectors determined that the SRS requirement for reactor flow compensation (PMS_SRS-14832) states only that the flow shall be compensated and provides no software requirements to define how to implement the compensation in the software. The SRS provides a rational statement that references a document which defines the equation for flow compensation; however, this rational statement is not defined as a requirement in the SRS and no other requirement was identified in the SRS that contained the equation. In addition, the referenced document for the equation and the associated functional diagram for flow compensation only defined the inputs associated with the compensation equation as analog, and did not define data types for the inputs. The inspectors determined that because the data type, such as floating point or integer, of the inputs was not defined, the designer would need to make assumptions related to the data type and to the scaling between data types. Due to the lack of guidance or additional software requirements, the inspectors determined the software requirements for the reactor coolant flow compensation were incomplete and ambiguous in that more than one interpretation of the software requirement could be implemented.

The inspectors determined via document evaluation and interviews that some critical high-level requirements accomplished via software are not present within the SRS. The inspectors observed that requirements found within the SRS would be inadequate to address how the software affects the output state of system components and how each must respond during a loss and subsequent restoration of power activity under the full range of applicable conditions delineated in the design basis. IEEE Std. 603-1991, Clause 5.5, “System Integrity” states that the safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Further, Clause 4 requires, in part, that the [critical] point in time or the plant conditions that allow returning a safety system to normal be documented. Although written for system restoration following a design basis event, this scenario must be analyzed and accounted for after a subsequent loss and restoration of power occurrence to a safety channel, division, or system. The inspectors observed that only two software requirements addressed a loss of power condition, specifically, PMS_SRS-6113 addresses loss of power for the source range high voltage power supplies, and PMS_SRS-6117 addresses loss of power to radiation monitoring systems; none accounted for output states.

The inspectors determined the SRS was incomplete in addressing IEEE Std. 603-1991 requirements. Additionally, through examination, the inspectors determined no predecessor or successor requirements were referenced in the RTM for the loss of and subsequent restoration of power activity. Due to the lack of completeness for this requirement, and lack of specificity of the SRS, the inspectors were unable to determine that the PMS SRS contained software requirements necessary to address occurrences related to a loss and subsequent restoration of power condition to meet the requirements of Clause 5.5 of IEEE 603-1991. The inspectors also observed that the design control process for modifying software requirements using Open Items (OIs) is not clearly defined by procedures.

The inspectors determined that SRS requirements were not ranked for importance. RG 1.172 states that software requirements important to safety be identified as such in the SRS. IEEE Std. 830-1993 states, in part, that "the SRS be ranked for importance. An SRS is ranked for importance if each requirement in it has an identifier to indicate the importance of that particular requirement." The inspectors determined that the PMS SRS did not provide the appropriate ranking of software requirements in keeping with their relative safety importance. This issue is material to the Acceptance Criteria for ITAAC 2.5.2.12 which states that a report exists and concludes that the process establishes a method for classifying the PMS software elements according to their relative importance to safety and specifies requirements for software assigned to each safety classification was done. The inspectors found that no method for ranking had been implemented. This is identified as Example Five of VIO 05200025/2012009-01, 05200026/2012009-01, Inadequate Design Control of Software Development.

Analysis: Inadequate design control for the PMS System Definition (requirements) phase is a performance deficiency that was within the licensee's ability to foresee and correct. Specifically the licensee did not ensure the SRS was developed using all the regulatory requirements and Tier 2* design criteria in the licensee's FSAR including NQA-1-1994, IEEE Std. 1074-1995, IEEE Std. 830-1993, and IEEE Std. 1012-1998. The performance deficiency was considered more than minor because it is an issue that, if left uncorrected, represents a failure to implement an adequate software development process and quality oversight function which could render the quality of the construction activity unacceptable or indeterminate; it also could adversely affect the closing of ITAAC 2.5.2.12. The finding was determined to be an ITAAC finding because the inspectors determined that the licensee could not meet the ITAAC 2.5.2.12 acceptance criteria without taking corrective actions to correct the deficiencies associated with the finding. Specifically, the finding was material to the acceptance criteria of ITAAC 2.5.2.12 in that (1) the process did not establish a method for classifying the PMS software elements according to their relative importance to safety and requirements for software assigned to each safety classification and (2) that requirements for V&V did not provide for reviewer independence.

The performance deficiency is associated with the Design/Engineering cornerstone in that it resulted in the PMS software requirements specification not meeting the specified design criteria which adversely affected the cornerstone objective. As a result, the issue was required to be evaluated using the construction SDP. The inspectors assessed the ITAAC finding in accordance with Inspection Manual Chapter (IMC) 2519P Appendix A and determined the following: (1) The risk importance of the PMS is high and (2) the finding is of very low safety significance (Green) because the inspectors did not identify an issue in PMS software requirements that could reasonably have been expected to impair the design function of the PMS at this stage of software development.

The inspectors determined that the ITAAC finding had a cross-cutting aspect in the work practice component of the baseline inspection program because the licensee failed to ensure supervisory and management oversight of work activities associated with the PMS software system development such that the construction quality was supported. [A.4(c)]. This resulted in a lack of coordination between licensing, design, and V&V, which resulted in the failure to flow licensing requirements down to implementing procedures.

Enforcement: 10 CFR 50 Appendix B Criterion III, Design Control, requires in part that measures be established to assure that applicable regulatory requirements and the design basis, as defined in § 50.2 and as specified in the license application, for those structures, systems, and components to which this appendix applies are correctly translated into specifications, drawings, procedures, and instructions.

Vogtle Units 3 & 4 Final Safety Analysis Report Chapter 7 incorporates by reference the AP 1000 Design Control Document (DCD) Revision 19.

DCD Subsection 7.1.2.14.1, "Design Process," states "WCAP-16096-NP-A (Reference 9) … describes design processes that will be used for AP1000." WCAP-16096-NP-A Section 5.1 "Software Verification and Validation Plan," states that, "This SVVP complies with Reference 8 [IEEE Std. 1012-1998]." IEEE Std. 1012-1998 Subsection 5.4.2 states in part the, "The V&V effort shall perform, as appropriate for the selected software integrity level, the minimum V&V tasks" including Software Requirements Evaluation, Interface Analysis, Criticality Analysis, Hazard Analysis, and Risk Analysis.

DCD Subsection 7.1.2.14.1, "Design Process," states "Westinghouse Quality Management System (Reference 21) describes design processes that will be used for AP1000." Westinghouse Quality Management System Subsection 4.2.9, Computer Software, states in part, "Computer software developed as a deliverable safety-related product … is developed, controlled, and maintained in accordance with procedures and instructions that comply with ASME NQA-1, (i.e., Part I Supplement 11S-2; Part II, Subpart 2.7)." NQA-1-1994 Subpart 2.7 Section 4 states in part, "Software verification and validation shall be performed by individuals other than those who designed the software."

DCD Subsection 7.1.4.2, "Conformance with Industry Standards," states, "The instrumentation and control systems are designed in accordance with guidance provided in applicable portions of the following standards…: IEEE Std. 1074-1995; "IEEE Standard for Developing Software Life Cycle Processes". IEEE Std. 1074-1995 Section 5 describes the processes that must be performed during the development of a software product and states that "Prior to the distribution of the Preliminary Software Requirements… [and] distribution of the Output Information…[and] distribution of the Software Requirements the following Processes shall be invoked [which includes Verification and Validation]". Moreover, Subsection 5.1.3.2 states that, "the developer shall analyze the software requirements to determine traceability, clarity, validity, testability, safety, and any other project-specific characteristics."

DCD Subsection 7.1.7 lists WCAP-16097-NP-A as a Tier 2* reference. WCAP-16097-NP-A, Section 4 identifies compliance to the codes and standards applicable for the Common Q designs and states that it conforms to IEEE Std. 830-1993 as modified by Reg. Guide 1.72 and as described in the Common Q SPM. IEEE 830-1993 Subsection 4.3, as modified by Reg. Guide 1.172, Rev. 0 states the SRS must be complete, unambiguous and be ranked for importance and/or stability. The SRS is complete if and only if, it includes all significant requirements, whether relating to functionality, performance, design constraints, attributes, or external interfaces. The SRS is unambiguous if, and only if, every requirement stated therein has only one interpretation. The SRS is ranked for importance and/or stability if each requirement in it has an identifier to indicate either the importance or stability of that particular requirement.

Contrary to the above, as of May 25, 2012, the licensee failed to assure that applicable regulatory requirements and the design basis, as defined in § 50.2, and as specified in the license application, for the Protection and Safety Monitoring System were correctly translated into specifications, drawings, procedures, and instructions in that:

1. The V&V effort did not adequately perform, the minimum V&V tasks including software requirements evaluation, interface analysis, criticality analysis, hazard analysis, and risk analysis, in that; the required input documents were not available to perform the hazard analysis, criticality analysis, and risk analysis, and the software requirements specification was inadequate to perform the software requirements evaluations and interface analysis.

2. The software verification and validation activities included individuals who designed the software in that, the V&V team took credit for the design team's activities, thus the V&V activities were not performed independently from the design team.

3. The developer did not analyze the software requirements to determine safety characteristics in that, a software hazard analysis of the software requirements specification was not performed.

4. The RSEDs development did not follow the prescribed software lifecycle process and activities, in that V&V tasks were not invoked. The RSEDs requirements were not analyzed to determine traceability, clarity, validity, testability, safety, or other project specific characteristics.

5. The SRS was ambiguous, not complete, and was not ranked for importance. In that, the software requirement for the reactor coolant flow compensation was incomplete and ambiguous in that more than one interpretation of the software requirement could be implemented and the requirements for loss and subsequent restoration of power were incomplete, and no requirements were ranked for importance.

The licensee submitted Condition Report 438475.

2. OTHER INSPECTION RESULTS

4OA6 Meetings, including Exit

.1 Exit Meeting Summaries

On April 13, 2012, the regional inspectors presented the interim results of the inspection to Mr. Murray Medlock, other members of his staff, and representatives for the consortium. On May 25, 2012, the regional inspectors re-exited with Mr. Murray Medlock, other members of his staff, and representatives for the consortium. The findings, cross-cutting, and cornerstone attributes associated with the finding provided during the re-exit were acknowledged by Mr. Medlock. The inspectors stated that no proprietary information would be included in the inspection report.

ATTACHMENT: SUPPLEMENTAL INFORMATION

SUPPLEMENTAL INFORMATION

KEY POINTS OF CONTACT

B. Hirmanpour - SNC
W. Odess-Gillettm WEC
L. Erin, WEC
B. Seelman, WEC
C. Scardina-Gazzo, WEC
T. McLaughlin, WEC
M. Uzman, WEC
D. Harris, WEC
S. Mullen, WEC
S. Wang, WEC
K. Murphy, WEC
D. Altman, WEC
S. Emery, WEC
R. Span, WEC
G. Jurecko, WEC
M. Angelini, WEC
J. Faulkner, WEC
D. Stark, WEC
J. Wieseman, WEC
J. Strong, WEC
G. Glen, WEC
S. Karaaslan, WEC
B. Sebesta, WEC
J. Presutti, WEC
L. Lubic, WEC
W. Vaughn - SNC
C. Medlock - SNC

LIST OF ITEMS OPENED, CLOSED, AND DISCUSSED

Item Number	Status	Description
NOV 05200025/2012009-01, 05200026/2012009-01	Open	Inadequate Design Control of Software Development

LIST OF DOCUMENTS REVIEWED

Licensing Documents:

Final Safety Analysis Report - Vogtle Units 3&4, Rev. 5
AP1000 Design Certification Document, Rev. 19

Technical / Topical Reports:

WCAP-15799, "AP1000 Conformance with SRP Acceptance Criteria," Rev. 1
WCAP-15927, "Design Process for the AP1000 Common Q Safety Systems," Rev. 2
WCAP-16096-NP-A, "Software Program Manual for Common Q Systems (SPM)," Rev.1A
WCAP-16097-P-A, "Common Qualified Platform Topical Report," Rev. 0
WCAP-17420, "AP1000 PMS Tracing Methodology for the System Definition Phase," Rev. 0
WCAP-16592-P, "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System," Rev. 2

Calculations:

Calculation Note APP-PXS-M3C-100, "PXS Component Control Requirements," Rev. 9
Calculation Note APP-PXS-M3C-101, "PXS Instrumentation and Mechanical Systems Interface Requirements," Rev. 7

Corrective Action / Nonconformance Records written during the inspection:

CAP Issue Report 12-089-M038 (Software Hazards Analysis Update)
CAP Issue Report 12-090-M050 (IV&V Issues)
CAP Issue Report 12-082-M053 (Traceability Issues)
CAP Issue Report 12-101-M050 (Deficiencies in AP1000 IV&V Summary Report)
CAP Issue Report 12-101-M060 (IV&V for Reusable Software Elements)
CAP Issue Report 12-103-M039 (Document Process for Requirements Change)
CAP Issue Report 12-103-M040 (SRS Requirements Ranking)
CAP Issue Report 12-103-M041 (IEEE 1074 Compliance)
CAP Issue Report 12-104-M024 (Open Items Process Procedure Improvements)

Drawings:

APP-PMS-J1-102, "AP1000 Functional Diagram – Reactor Trip Functions," Rev. 9
APP-PMS-J1-105, "AP1000 Functional Diagram – Core Heat Removal and RCP Trip," Rev. 7

APP-PMS-J1-111, “AP1000 Functional Diagram – Safeguards Actuation,” Rev. 8
APP-PMS-J1-116, “AP1000 Functional Diagram - IRWST Actuations,” Rev. 2
APP-PMS-J3-315, “AP1000 Detailed Functional Diagram - Overtemperature/Overpower Reactor Trips Division A,” Rev. 3
APP-PMS-J3-327, “AP1000 Detailed Functional Diagram RCS Hot Legs 1 and 2 Low-2 Reactor Coolant flow Reactor Trip,” Rev. 3
APP-PMS-J3-307, “AP1000 Detailed Functional Diagram - Reactor Trip Logic,” Rev. 3
APP-PMS-J1-106, “AP1000 Functional Diagram - Primary Overpressure and Loss of Heat Sink Protection,” Rev. 6
APP-PMS-J1-104, “AP1000 Functional Diagram - Nuclear Overpower Protection,” Rev. 7
Requirements for drawing APP-PMS-J1-106
Requirements for drawing APP-PMS-J1-104
APP-PMS-J3-319, “AP1000 Detailed Functional Diagram - PZR Pressure Reactor Trip,” Rev. 3
APP-PMS-J3-320, “AP1000 Detailed Functional Diagram - PZR Level Reactor Trip,” Rev. 3
APP-PMS-J3-314, “AP1000 Detailed Functional Diagram - Power Range Neutron Detector Reactor Trip,” Rev. 3

Miscellaneous:

WNA-PD-00042-WAPP, “AP1000 PMS Software Development Plan,” Rev. 4
NUREG/CR-6430 “Software Safety Hazard Analysis”
APP-GW-J0R-012, “AP1000 PMS Computer Security Plan,” Rev. 1
WNA-PS-00019, “Computer Security Assessment,” Rev. 1
APP-PMS-GER-021, “AP1000 Protection and Safety Monitoring System IV&V Phase Summary Report,” Rev. 1
APP-GW-GLR-137, “Bases of Digital Overpower and Overtemperature Delta-T (OPΔT/OTΔT) Reactor Trips,” Rev. 1
WNA-DS-01663-GEN, “Standard Reusable Software Element Document for Q-Delta T Type Circuit,” Rev. 1
WNA-DS-01709-GEN, “Standard Reusable Software Element Document for Axial Penalty Custom PC Element,” Rev. 4
WNA-DS-02054-GEN, “Standard Reusable Software Element Document for Value and Quality Selection from Redundant Sensor Algorithm Custom PC Element,” Rev. 2
APP-GW-GLR-154, “I&C Licensing Compliance Matrix,” Rev. 0
APP-PMS-J0R-001, “AP1000 Protection and Monitoring System Requirements Traceability Matrix,” Rev. 1
WNA-DS-01491-GEN, “Standard Reusable Software Element Document for Pressurizer Water Level Compensation Custom PC Element,” Rev. 2
WNA-DS-01523-GEN, “Standard Reusable Software Element Document for Vote Two Out of Four Custom PC Element,” Rev. 2
WNA-TR-01438-GEN, “Element Software Test Report for PZWLCOMP Custom PC Element,” Rev. 1
APP-PMS-J8R-003, “AP1000 Protection and Safety Monitoring System Software Release Report,” Rev. 1
WNA-PD-00051-WAPP Rev 2 - Project Plan AP1000 I&C Programs Plan rev2
WNA-PQ-00283-WAPP AP1000 Rev 0 - I&C Programs Project Quality Plan

Procedures:

NABU-DP-00014-GEN, “Design Process for Common Q Safety Systems,” Rev. 3
APP-PMS-J1-014, “AP1000 Protection and Safety Monitoring System Safety Analysis Summary,” Rev. 0
APP-PMS-J1-001, “AP1000 Protection and Safety Monitoring System Functional Requirements,” Rev. 0
(APP-GW-GEP-010, revision 5, “Process & Procedure for AP1000 Internal Open Items and Holds”; WNA-WI-00048-WAPP, rev. 3, “Use of the AP1000 Opens Items Database”)
WNA-PV-00009-GEN, Revision 3, “Verification & Validation Process for the Common Q Safety Systems,”
NA 4.19.9, “Issue Reporting and Resolution,” Rev.0
NA 4.28, Request for Engineering Change, Rev.2
NSNP 3.4.1, Change Control for the AP1000 Program, Rev. 4
WEC 16-2 Rev 3- Westinghouse Procedure Corrective Action Processes
WNA-PD-00051-WAPP Rev 2 - Project Plan AP1000 I&C Programs Plan rev2
WNA-PQ-00283-WAPP AP1000 Rev 0 - I&C Programs Project Quality Plan
WNA-PD-00042-WAPP Rev 4 - AP1000 Protection and Safety Monitoring System Software Development Plan.pdf

Specifications:

APP-GW-J4-001, “AP1000 I&C Design Specification,” Rev. 6
APP-GW-J1-010, “AP1000 I&C Requirements Specification,” Rev. 3
APP-PMS-J4-003, “AP1000 PMS Subsystem Requirements Specification,” Rev. 2
APP-PMS-J4-020, “AP1000 PMS Subsystem Design Specification,” Rev. 3
APP-PMS-J4-102, “AP1000 Protection and Safety Monitoring System Software Requirements Specification,” Rev.3

Design Change Packages:

APP-GW-GEE-2082, “Feedwater/CVS Isolation Logic Deficiency-Undesirable Isolation of SFW and CVS During Fill-Up,” Rev.0
APP-GW-GEE-1908, “PRHR PAM Parameter Recategorization,” Rev. 0

LIST OF ACRONYMS

10 CFR	Title 10 of the *Code of Federal Regulations*
ADAMS	Agency-wide Documents Access & Management System
AP1000	Westinghouse Advanced Passive Pressurized Water Reactor
ASME	American Society of Mechanical Engineers
DAC	Design Acceptance Criteria
DCD	Design Control Document
DI&C	Digital Instrumentation and Control
ESF	Engineered Safety Feature
FSAR	Final Safety Analysis report
IEEE	Institute of Electrical and Electronics Engineers
IMC	Inspection Manual Chapter
IP	Inspection Procedure
IR	Inspection Report
IRS	Interface Requirement Specification
IRWST	In-Containment Refueling Water Storage Tank
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
IV&V	Independent Verification and Validation
No	Number
Notice	Notice of Violation
NRC	Nuclear Regulatory Commission
OI	Open Item
OITS	Open Item Tracking System
OPΔT/OTΔT	Overpower Delta-T / Overtemperature Delta-T
PHA	Preliminary Hazards Analysis
PMS	Protection and Safety Monitoring System
PZR	Pressurizer
QMS	Quality Management System
RCP	Reactor Coolant Pump
Rev	Revision
RG	Regulatory Guide or Reg Guide
RSED	Reusable Software Element Document
RTM	Requirements Traceability Matrix
SDP	Significance Determination Process
SLC	Software Lifecycle
SNC	Southern Nuclear Operating Company, Inc or Southern Nuclear
SPM	Software Program Manual
SRP	Standard Review Plan
SRS	Software Requirements Specification
SVVP	Software Verification and Validation Plan
V&V	Verification and Validation
VEGP	Vogtle Electric Generation Plant
VIO	Violation
WEC	Westinghouse Electric Company LLC

Table 1, ITAAC 2.5.2

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11. The PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages b) System definition phase	Inspection will be performed of the process used to design the hardware and software	A report Exists and concludes that the process defines the organizational responsibilities, activities, and configuration management controls for the following: b) Specification of Functional requirements
12. The PMS software is designed, tested, installed and maintained using a process which incorporated a graded approach according to the relative importance of the software to safety and specifies requirements for: Software management including documentation requirements, standards, review requirements, and procedures for problem reporting and corrective action Software configuration management including historical records of software and control of software changes Verification and validation including requirements for reviewer independence	Inspection will be performed of the process used to design, test install, and maintain the PMS software.	A report exists and concludes that the process establishes a method for classifying the PMS software elements according to their relative importance to safety and specifies requirements for software assigned to each safety classification. The report also concludes that requirements are provided for the following software developments functions: a) Software management including documentation requirements, standards, review requirements, and procedures for problem reporting and corrective action. Software management requirements may be documented in the software quality assurance plan, software development plan, software safety plan, and software operation and maintenance plan; or these requirements may be combined into single software management plan. b) Software configuration management including historical records or software and control of software change. Software configuration management requirements are provided in the software configuration management plan c) V&V including requirements for reviewer independence. V&V requirements are provided in the V&V plan