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

July 30, 2010

Mr. Mark McBurnett, Vice President
Oversight and Regulatory Affairs
South Texas Project Nuclear Operating Company
P. O. Box 289
Wadsworth, TX 77483

SUBJECT: SOUTH TEXAS PROJECT ELECTRIC GENERATING PLANT UNITS 3 & 4 - NRC INSPECTION REPORT 05200012/2010001 AND 05200013/2010001

Dear Mr. McBurnett:

On June 21 - 25, 2010, the U.S. Nuclear Regulatory Commission (NRC) completed an inspection of design activities performed for your South Texas Project (STP) Electric Generating Station Units 3 and 4 at Westinghouse's facility in Cranberry Township, PA. The purpose of the inspection was to resolve certain Design Acceptance Criteria associated with your combined license (COL) application, and to evaluate quality assurance program implementation for development of safety-related computer-based software to be used in digital instrumentation and control components of the safety system logic and control system. The enclosed inspection report documents the inspection results that were discussed on June 25, 2010 and July 20, 2010, with Mr. Mike Murray and other members of your staff.

The inspection determined whether activities were conducted in accordance with NRC requirements and your application basis. The inspectors examined activities implemented to accomplish the Planning Phase of the software life cycle as outlined in the Design Acceptance Criteria contained in Table 3.4 of the Advanced Boiling Water Reactor Design Certification Document, which is referenced in your COL application, and Branch Technical Position 7- 14 of the Standard Review Plan (NUREG-0800). The inspectors reviewed selected life cycle planning documents, procedures, and records, and interviewed personnel.

In accordance with 10 CFR 2.390 of the NRC's "Rules of Practice," a copy of this letter, its enclosure, and your response (if any) will be available electronically for public inspection in the NRC Public Document Room or from the Publicly Available Records (PARS) component of NRC's document system (ADAMS).

ADAMS is accessible from the NRC Website at http://www.nrc.gov/reading-rm.html (the Public Electronic Reading Room).

Should you have any questions concerning this letter, please contact me at (404)997-4460.

Sincerely,

/RA/

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

Docket Nos.: 52-012, 52-013

Enclosure:
NRC Inspection Report 05200012/2010001 and 05200013/2010001
w/Attachment: Supplemental Information

cc w/encl: (See next page)

ADAMS is accessible from the NRC Website at http://www.nrc.gov/reading-rm.html (the Public Electronic Reading Room).

Should you have any questions concerning this letter, please contact me at (404)997-4460

Sincerely,

/RA/

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

Docket Nos.: 52-012, 52-013

Enclosure:
NRC Inspection Report 05200012/2010001 and 05200013/2010001
w/Attachment: Supplemental Information

cc w/encl: (See next page)

■ PUBLICLY AVAILABLE □ NON-PUBLICLY AVAILABLE □ SENSITIVE ■NON-SENSITIVE
ADAMS: □ Yes ACCESSION NUMBER:_ML102110291_ ■SUNSI REVIEW COMPLETE

OFFICE	RII:DCI	RII:DCI	RII:DCI	NRO:DCP	RES:DE	NRO:DE	RII:DCP
SIGNATURE	CJ	Via email	JK	T. Fredette for/via email	Via email	Via email	Via email
NAME	C. Jones	L. Castelli	J. Kent	T. Frye	M. Concepcion	D. Taneja	D. Ayres
DATE	7/28/10	7/27/10	7/27/10	7/27/10	7/26/10	7/26/10	7/30/10
E-MAIL COPY?	YES NO	YES NO	YES NO	YES NO	YES NO	YES NO	YES NO

OFFICIAL RECORD COPY DOCUMENT NAME: G:\CCI\INSPECTION REPORTS\NEW REACTORS\SOUTH TEXAS PROJECT\STP INSPECTION REPORT.DOCX

cc w/encl:

Mr. Brian Almon
Public Utility Commission
William B. Travis Build
PO Box 13326
1701 North Congress Avenue
Austin, TX 78701-3326

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

C. M. Canady
City of Austin
Electric Utility Department
721 Barton Springs Road
Austin, TX 78704

Certrec Corporation
4200 South Hulen, Suite 422
Fort Worth, TX 76109

Mr. Ted Enos
4200 South Hulen
Suite 422
Ft. Worth, TX 76109

Ms. Susan M. Jablonski
Office of Permitting, Remediation
and Registration
Texas Comm. on Env. Quality
MC-122
P.O. Box 13087
Austin, TX 78711-3087

Judge
Matagorda County
Matagorda County Courthouse
1700 Seventh Street
Bay City, TX 77414

C. Kierksey
City of Austin
Electric Utility Department
721 Barton Springs Road
Austin, TX 78704

Scott M. Head
Regulatory Affairs Manager
STP Nuclear Operating Company
P.O. Box 289
Wadsworth, TX 77483

Bill Mookhoek
Licensing Supervisor
STP Units 3 and 4
Project Electric Generating Station
P.O. Box 289
Wadsworth, TX 77483

Mr. Terry Parks
Chief Inspector
Texas Department of Licensing
and Regulation
Boiler Division
P.O. Box 12157
Austin, TX 78711

Kathy C. Perkins, RN, MBA
Assistant Commissioner
Division for Regulatory Services
Texas Department of State Health Services
P.O. Box 149347
Austin, Texas 78714-9347

Policy Director
Environmental and Natural Resources
P. O. Box 12428
Austin, TX 78711-3189

Mr. Frank M. Quinn
8 Oak Avenue
Gaithersburg, MD 20877-2705

Regional Administrator, Region IV
U. S. Nuclear Regulatory Commission
611 Ryan Plaza Drive, Suite 400
Arlington, Texas 76011-8064

Alice Hamilton Rogers, P.E.
Inspections Unit Manager
Texas Department of State Health Services
P. O. Box 149347
Austin, Texas 78714-9347

J. J. Sheppard
President & CEO
STP Nuclear Operating Company
P.O. Box 289
Wadsworth, TX 77483

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

Mr. Steve Winn
STP Nuclear Operating Company
1301 McKinney, Suite 2300
Houston, TX 77010

Mr. Jon C. Wood
Cox, Smith, & Matthews
112 East Pecan, Suite 1800
San Antonio, TX 78205

Letter to Mark McBurnett from Mark S. Lesser, dated, July 30, 2010.

SUBJECT: SOUTH TEXAS PROJECT ELECTRIC GENERATING PLANT UNITS 3 & 4 - NRC INSPECTION REPORT 05200012/2010001 AND 05200013/2010001

Distribution w/encl:

D. Ayres, RII
R. Croteau, RII
T. Fredette, NRO
T. Frye, NRO
T. Gody, RII
R. Hannah, Public Affairs Officer, RII
C. Jones, RII
I. Jung, NRO
J. Ledford, Public Affairs Officer, RII
M. Lesser, RII
C. Ogle, RII
L. Plisco, RII
L. Reyes, RII
N. Sanfillippo, OEDO, Region II Regional Coordinator
G. Wunder, NRO
P. Miles, Region II Administrator's Administrative Assistant
S. DuBose, Region II DRAC's Administrative Assistant

U.S. NUCLEAR REGULATORY COMMISSION
Region II

Docket No:	52-012 52-013
License No:	Pre-COL
Report No.:	05200012/2010001 05200013/2010001
Applicant:	South Texas Project Nuclear Operating Company (STPNOC)
Facility:	South Texas Project Electric Generating Station Units 3 & 4
Location:	Cranberry Township, PA
Inspection Dates:	June 21 through June 25, 2010
Inspectors:	C. Jones, Sr. Construction Inspector, RII/CCI L. Castelli, Sr. Construction Inspector, RII/CCI J. Kent, Construction Inspector, RII/CCI M. Concepcion, Sr. I&C Engineer, RES/DE D. Taneja, Sr. Electronics (Digital I&C) Engineer, NRO/DE
Accompanying Personnel:	T. Fredette, Reactor Operations Engineer, NRO/DCIP M. Lesser, Chief, Branch 1 Division of Construction Inspection, RII/CCI

Approved By **/RA/** 7/30/10

Mark S. Lesser, Chief
Construction Inspection Branch 1
Center for Construction Inspection

Date

Enclosure

SUMMARY OF FINDINGS

Inspection Report 052012/2010001; 052013/2010001; 06/21/2010 through 06/25/2010; South Texas Project (STP) Electric Generating Station Units 3 and 4; Inspection of Digital Instrumentation and Control Systems/Software Design Acceptance Criteria.

The report covered an announced inspection to resolve Design Acceptance Criteria associated with the combined license application. Specifically the team reviewed planning activities that have been completed for the development of software to be used in digital computer-based instrumentation and control systems for STP Units 3 & 4.

The Nuclear Regulatory Commission's (NRC's) program for the inspection of construction and operational programs is described in Inspection Manual Chapter 2504, Construction Inspection Program – Inspection of Construction and Operational Programs.

A. NRC-Identified Findings and Licensee Identified/Self-Revealing Violations Evaluated as Findings

   No findings of significance were identified.

B. Licensee-Identified and Self-Revealing Violations Not Evaluated as Findings

   None

REPORT DETAILS

A. ITAAC-RELATED INSPECTIONS

1. Inspection of Digital Instrument & Control Design Acceptance Criteria (DAC)-related ITAAC (IP 35007, as guided by draft IP 65001.xx, Appendix 1)

   The inspectors conducted an inspection of software life cycle planning phase activities related to the development of software for digital computer-based instrumentation and control (I&C) systems at South Texas Project (STP) Units 3 and 4. The inspection was conducted to resolve DAC and to verify the software life cycle was formally defined and planning documents were developed in a manner that incorporated the characteristics outlined in Branch Technical Position 7-14 of the NRC's Standard Review Plan (NUREG-0800).

   Digital I&C systems associated with this inspection scope included two individual system platforms that provide key applications for the STP Advanced Boiling Water Reactor (ABWR) Safety System Logic and Control System:

   - The Reactor Protection and Neutron Monitoring Systems (i.e. the Toshiba Non-Rewritable Field Programmable Gate Array platform), and

   - The Engineered Safeguards Logic Control System (i.e. the Westinghouse Common Q platform).

   The inspection was conducted prior to the completion of NRC's review of the application for a combined license that has been submitted by STP Nuclear Operating Company. Inspection guidance was provided in IP 35007, Quality Assurance Program Implementation during Construction, and draft IP 65001.xx, Inspection of Digital Instrumentation and Control (DI&C) System/Software Design Acceptance Criteria (DAC) - Related ITAAC (attached).

   a. ITAAC No 3.4.07 / Family 16E, Software Quality Assurance

   1) Inspection Scope

      The inspectors reviewed applicant activities in order to verify a quality assurance program was established that defined control processes for software development in accordance with Design Acceptance Criterion (DAC) number 7 in Table 3.4 of the Advanced Boiling Water Reactor (ABWR) Design Certification Document, which is referenced by the STP combined license application. Specifically, the inspectors reviewed quality program documents, software development plans, and quality procedures to verify that they were implemented in accordance with regulatory requirements, met design basis requirements, and were adequate for the work being performed.

      The inspectors' review included U7-P-QP01-QAPD, STP 3 & 4 Quality Assurance Program Description. The program description document was reviewed to verify that the quality assurance program, as supplemented and augmented by U7-PROJ-J-P-EN02-002, Software Program Plan, and WCAP-16096-NP-A, Software Program Manual for Common Q Systems, sufficiently defined controlled processes for software development that were applicable to the complete software life cycle as required by DAC 7.

The inspectors evaluated the quality program description and the two software quality assurance (QA) plans against the inspection attributes identified in (draft) IP 65001.xx. These attributes included evaluation of the following:

- Specific management aspects; including for example, definition of the QA management tasks, QA documentation, QA recordkeeping, QA standards, reviews & audits, corrective action, control of QA tools, and control of vendors.

- Key attributes; including for example, identification of QA-related software products, identification of organization interfaces, establishment of QA independence, identification of QA oversight tasks, identification of QA documents, establishment of requirements for reviews & audits, and establishment of provisions for problem identification and resolution.

2) Findings

No findings of significance were identified.

b. ITAAC No: 3.4.08 / Family 16E, Software Management Plan

1) Inspection Scope

The inspectors reviewed applicant activities in order to verify the planning phase for development of digital I&C systems established a Software Management Plan as prescribed by Design Acceptance Criterion (DAC) 8 in Table 3.4 of the Advanced Boiling Water Reactor (ABWR) Design Certification Document, which is referenced by the STP combined license application. The DAC specified software management plan attributes to be met in order to assure that software be developed, designed, evaluated, and documented per a design development process that addresses, for safety-related software, software safety issues at each defined life-cycle phase of the software development.

Software Management Plan (DAC 8a and 8d)

The inspectors conducted interviews with staff knowledgeable in the STP software management processes, and reviewed project plans and documents to verify the Software Management Program Plan outlined in U7-PROJ-J-P-EN02-002 implemented DAC 8a requirements to define the organization and responsibilities for development of the software design; the procedures to be used in the software development; the interrelationships between software design activities; and the methods for conducting software safety analyses.

Inspectors also reviewed U7-PROJ-J-P-EN02-002 to verify implementation of DAC 8d requirements for planning phase design activities to address software system design requirements and software development plans. Five attributes of this DAC were included in the inspection sample. The attributes require planning phase activities to address:

- DAC 8d(1), the Software Management Plan

- DAC 8d(2), the Software Configuration Management Plan
- DAC 8d(3), the Verification and Validation Plan
- DAC 8d(4), equipment design requirements
- DAC 8d(5), safety analysis of design requirements

The inspectors' evaluation of the Software Management Program Plan was guided by the inspection attributes identified in (draft) IP 65001.xx, Section A1.03.01. These attributes included evaluation of the following:

- Specific management aspects of the software development project; including for example, definition of the management structure, oversight of vendors, independence of QA, and training & qualification.

- Key attributes; including for example, scheduling reviews & audits, defining deliverables, defining organizational responsibilities, identifying constraints impacting safety, and identifying required technical documents.

Software Safety Analysis (DAC 8b)

The inspectors reviewed the STP 3 & 4 Software Safety Program Plan, contained in U7-PROJ-J-P-EN02-002, Software Program Plan. The review was conducted to verify the Software Safety Program Plan established processes and identified activities that will provide an adequate software safety analysis. In addition, the inspectors evaluated whether the Software Safety Program Plan provided a description of the safety efforts that will be carried out by STP 3 & 4 construction project team members and subcontractors on all safety-related software.

The inspectors reviewed the Software Safety Program Plan to confirm that the plan provided an adequate description of the software safety strategy, consistent with staff and industry guidance. The inspectors specifically reviewed the associated project plans and documents to verify the requirements for configuring and conducting software safety analyses were defined as prescribed by DAC 8b. Inspectors also reviewed the Software Program Plan to verify it included plans for implementation of the following additional elements of DAC 8:

- DAC 8d(5), Safety analysis of design requirements
- DAC 8e(5), Safety analysis of the developed design definition.
- DAC 8f(2), Safety analysis of the software design.
- DAC 8g(3), Safety analysis of the software coding.
- DAC 8h(2), Safety analysis of the integration test results.
- DAC 8i(4), Safety analysis of the validation test results

The inspectors' evaluation of the software safety plan was guided by the inspection attributes identified in (draft) IP 65001.xx, Section A1.03.05. These attributes included evaluation of the following:

- Specific management aspects of the software development project; including for example, documentation of safety analyses results, information on safety problems, results of audits, results of safety tests, and records on training.

- Key attributes; including for example, definition of methods for conducting analyses tasks, identification of documents and records to be produced, specification of methods for approving tools, and provision of methods to ensure subcontractor compliance.

2) Findings

a) Description:

Two examples were identified where attributes of Design Acceptance Criteria were not implemented in the manner outlined in Table 3.4 of the ABWR Design Certification Document, which is referenced in the combined license application:

(1) Table 3.4, Acceptance Criterion 8a, of the ABWR Design Certification Document requires the Software Management Plan to define the procedures to be used in software development. During a June 25, 2010 inspection of the applicant's Software Management Plan as detailed in Section 2 of U7-PROJ-J-P-EN02-0002, inspectors found the Software Management Plan did not define the procedures to be used in software development. On July 1, 2010, the applicant issued Condition Report 10-171 to address this finding.

(2) Table 3.4, Acceptance Criterion 8h(2), of the ABWR Design Certification Document requires the Software Management Plan to define the integration phase which shall address equipment testing activities, including safety analysis of the integration test results. During a June 25, 2010 inspection of the applicant's Software Management Plan as detailed in Section 2 of U7-PROJ-J-P-EN02-0002, inspectors found the Software Management Plan did not define requirements for safety analysis of results from integration testing during the Integration Phase of the software life cycle. The applicant issued Condition Report 10-171 to address this finding.

b) Analysis:

The inspectors determined that the omission of information in the Software Management Plan that was specifically prescribed by DAC 8a and DAC 8b will not resolve the Design Acceptance Criteria.

The inspectors noted that a separate plan description entitled Software Development Plan, contained information about procedures to be used for software development; however, the Design Acceptance Criterion specifically called for the information to be placed in the Software Management Plan.

The NRC has not issued a combined license (COL) for STP 3 & 4, and the ABWR Design Acceptance Criteria do not represent NRC requirements for pre-COL activities. As such, a pre-COL inability to resolve Design Acceptance Criteria is not characterized as ITAAC-related. However, the inspectors determined that the applicant's Combined License Application, Rev. 3, and quality program documents require their software development activities to conform to the Design Acceptance Criteria outlined in the ABWR Design Certification Document.

The STP program attributes that were not fully consistent with the Design Acceptance Criteria were identified as examples for an Unresolved Item (URI) and is being tracked as URI 052012/2010-001-01, 052013/2010-001-01: Design Acceptance Criteria cannot be resolved in the manner specified in Table 3.4 of the ABWR Design Certification Document, Examples 1 and 2. The issue is unresolved pending further inspection of compliance with requirements to correctly translate design basis requirements into plant documents and to assure suppliers conform to the requirements of procurement documents.

c. ITAAC No. 3.4.09 / Family 16E, Configuration Management Plan

1) Inspection Scope

The inspectors interviewed responsible applicant staff and reviewed design documents to verify the planning phase for development of digital I&C systems established a Software Configuration Management Plan as prescribed by Design Acceptance Criterion (DAC) 9 in Table 3.4 of the ABWR Design Certification Document, which is referenced by the combined license application. The DAC specified attributes to be met in order to assure the Configuration Management Plan established the methods for maintaining, throughout the software design process, the design documentation, procedures, evaluated software, and the resultant as-installed software.

The inspectors' review included the Software Configuration Management Program Plan (SCMPP) contained in U7-PROJ-J-P-EN02-0002. The review was performed to verify the following attributes were addressed by the SCMPP:

- DAC 9a, identify the specific software products or system scope to which it is applicable
- DAC 9b, define organizational responsibilities for configuration management
- DAC 9c, require the definition of methods for design control; including 9c(1), identifying design interfaces; 9c(3), controlling design changes; 9c(4), processing corrective actions; 9c(5), maintaining status of design; and 9c(6), controlling status of software revisions
- DAC 9e, define the configuration management of tools (e.g. compilers) and procedures
- DAC 9f, provide for dedication of commercial software
- DAC 9g, define methods for tracking error rates during software development
- DAC 9h, specify controls for configuration management records

Inspectors evaluated whether U7-PROJ-J-P-EN02-0002 described and established requirements for the software development life cycle activities, and whether it formed the basis to generate plans for individual digital I&C systems or logical groups of digital I&C systems.

The inspectors' evaluation of the Software Configuration Management Plan was guided by the inspection attributes identified in (draft) IP 65001.xx, Section A1.03.03. The evaluation of these attributes included the following:

- Specific management aspects; including for example, establishment of development baselines; definition of review, approval, and control of changes; establishment of reviews and audits; and control of interfaces.

- Key attributes; including for example, identification of product interfaces; definition of responsibility for baseline changes; description of methods to manage phase-specific activities; establishment of procedures to manage changes; identification of items to be placed under configuration control; establishment of a requirement to conduct a safety assessment; establishment of requirements for periodic reviews and audits; and establishment of provisions to audit suppliers.

2) Findings

a) Description:

Two examples were identified where attributes of Design Acceptance Criteria were not implemented in the manner outlined in Table 3.4 of the ABWR Design Certification Document, which is referenced in the combined license application:

(1) Table 3.4, Acceptance Criterion 9f, of the ABWR Design Certification Document requires the Software Configuration Management Plan to define methods for the dedication of commercial software for safety related usage. During a June 25, 2010 inspection of the applicant's Software Configuration Management Program Plan as detailed in Section 7 of U7-PROJ-J-P-EN02-0002, inspectors found the Software Configuration Management Program Plan did not address dedication of commercial software for safety related usage. The applicant issued Condition Report 10-171 to address this finding.

(2) Table 3.4, Acceptance Criterion 9g, of the ABWR Design Certification Document requires the Configuration Management Plan to define the methods for tracking error rates during software development. During a June 25, 2010 inspection of the applicant's Software Configuration Management Program Plan as detailed in Section 7 of U7-PROJ-J-P-EN02-0002, inspectors found the Software Configuration Management Program Plan did not address methods for tracking error rates during software development. The applicant issued Condition Report 10-171 to address this finding.

b) Analysis:

The inspectors determined the omission of information in the Software Configuration Management Program Plan that was specifically prescribed by DAC 9f and DAC 9g will not resolve the Design Acceptance Criteria.

The NRC has not issued a combined license (COL) for STP 3 & 4, and the ABWR Design Acceptance Criteria do not represent NRC requirements for pre-COL activities. As such, a pre-COL inability to resolve Design Acceptance Criteria is not characterized as ITAAC-related. However, the inspectors determined that the applicant's Combined License Application, Rev. 3, and quality program documents require their software development activities to conform to the Design Acceptance Criteria outlined in the ABWR Design Certification Document.

The STP program attributes that were not fully consistent with the Design Acceptance Criteria were identified as examples for an Unresolved Item (URI) and is being tracked as URI 052012/2010-001-01, 052013/2010-001-01: Design Acceptance Criteria cannot be resolved in the manner specified in Table 3.4 of the ABWR Design Certification Document, Examples 3 and 4. The issue is unresolved pending further inspection of compliance with requirements to correctly translate design basis requirements into plant documents and to assure suppliers conform to the requirements of procurement documents.

d. ITAAC No. 3.4.010 / Family 16E, Verification & Validation Plan

1) Inspection Scope

The inspectors conducted an inspection of applicant activities in order to verify the planning phase for the development of digital I&C systems established a Software Verification and Validation Plan as prescribed by DAC number 10 in Table 3.4 of the ABWR Design Certification Document. The DAC specified attributes to be met in order to assure that developed software are subjected to structured and documented verification reviews and validation testing, including testing of the software that has been integrated into the target hardware.

The inspectors reviewed the Software Verification and Validation Program Plan (SVVPP) contained in STP Document U7-PROJ-J-P-EN02-0002, Software Program Plan. The review was performed to verify the SVVPP met the acceptance criteria specified in DAC 10, including the following attributes:

- DAC 10a, conduct baseline reviews in each phase of the life cycle
- DAC 10c, establish procedural control over use of commercial software and tools
- DAC 10d, verify conformity of design in each phase of the baseline review
- DAC 10e, conduct validation testing of software as-installed in target hardware
- DAC 10f, use knowledgeable and separate personnel for reviews and tests
- DAC 10h, use documented test plan and procedure for validation testing
- DAC 10i, include non-safety related software in baseline reviews
- DAC 10j, document and maintain configuration control of review products
- DAC 10k, define methods to identify, close, and document nonconformances
- DAC 10l, software development is not complete until V&V activities are complete

In addition, the review was performed to verify the SVVPP defined the verification and validation activities for all software development in support of the digital I&C systems. Inspectors determined whether the requirements of the SVVPP were applied to all software intended for use in nuclear safety-related, non-safety related Group 1, and non-safety related Group 2 system applications.

The inspectors' evaluation of the software verification and validation program was guided by Institute of Electrical and Electronics Engineers (IEEE) Standard 1012-1994, NRC Branch Technical Position 7-14, and the inspection attributes identified in (draft) IP 65001.xx, Section A1.03.04. These attributes included evaluation of the following:

- Specific management aspects; including for example, description of methods for managing Life Cycle V&V; and description of methods for verification and validation (V&V) during the requirements phase, design & implementation phase, integration phase, validation & test phase, and installation phase.

- Key attributes; including for example, establishment of references to the configuration management plan and the quality assurance plan; definition of the scope of the V&V effort; definition of a V&V schedule; definition of V&V tools & methods; establishment of methods to handle anomalies; definition of responsibilities of V&V participants; establishment of V&V procedures; and provision of procedures for review and audit.

- Various life cycle phase-specific attributes as defined for each phase in the software life cycle.

2) Findings

No findings of significance were identified.

2. Inspection of Non-ITAAC Digital Instrument & Control Software Development (IP 35007, as guided by draft IP 65001.xx, Appendix 1)

1) Inspection Scope

The inspectors conducted interviews with staff knowledgeable in the STP software management activities and reviewed design documents to verify the planning phase for the development of software for digital I&C systems established an adequate process for software development consistent with Branch Technical Position 7-14 of the NRC's Standard Review Plan (NUREG-0800). Specifically, inspectors reviewed the Software Development Plan and applicable elements of the software program plan to verify they identified the tasks that are to be a part of each life cycle; identified the life cycle inputs and outputs, including the review, verification and validation of those outputs; and listed the international, national, industry, and company standards and guidelines, including regulatory guides, which were to be followed.

The inspectors' review included U7-PROJ-J-P-EN02-002, Software Program Plan. The inspectors' evaluation of the Software Development Plan aspects contained in U7-PROJ-J-P-EN02-002 was guided by the inspection attributes identified in (draft) IP 65001.xx, Section A1.03.06. These attributes included, for example, listing technical milestones, identifying technical documents required, and documenting audits of the software development process.

2) Findings

No findings of significance were identified.

B. EXIT MEETINGS SUMMARY

On June 25, 2010 and July 20, 2010, the inspectors presented the inspection results to Mr. M. Murray and other members of the STP 3 & 4 project staff, who acknowledged the Unresolved Item. The inspectors acknowledged that the applicant desired the material

examined during the inspection to be considered proprietary. The inspectors stated that no proprietary information would be included in the inspection report.

Attachments:
Supplemental Information w/ Appendix

SUPPLEMENTAL INFORMATION

KEY POINTS OF CONTACT

Applicant personnel

J. Cook, STP Licensing Engineer
K. Dittman, STP Principal I&C Engineer
E. Fredrickson, Westinghouse
A. Fukumoto, Toshiba I&C Sr. Fellow
D. Herrell, MPR Associates
K. Kloes, Westinghouse Nuclear Automation Quality Assurance
J. Mauck, STP I&C Licensing
M. Murray, STP I&C Manager
R. Nydes, Westinghouse Program Manager
C. Swanner, MPR Associates
H. Takeda, Toshiba QA Manager
S. Zander, Toshiba America Nuclear Energy I&C Manager

NRC personnel

M. Lesser, Chief, RII/CCI/DCI/Branch 1

LIST OF ITEMS OPENED, CLOSED, AND DISCUSSED

Opened

052012/20102010-001-01, 052013/20102010-001-01	URI	Design Acceptance Criteria cannot be resolved in the manner specified in Table 3.4 of the ABWR Design Certification Document (Sections A.1.b, A.1.c).

LIST OF DOCUMENTS REVIEWED

7A32-3702-0004, Rev. 0, FPGA-Based Safety-Related Systems Logic Development Plan
AS-300A008, Rev. 12, Nonconformance and Corrective Action Procedure
CR 10-171-R0**,** Additional Issues in STP 3 & 4 Software Program Plan
NSNP 3.6.1, Rev. 2, Computer Software Development Process
PP-ES-08-0774, Rev. 1, Project Plan – STP Units 3 & 4 Engineering Support
PQP-ES-08-0774, South Texas Project Units 3 & 4 Project Quality Plan
U7-P-QP01-QAPD, Rev. 4, STP 3 & 4 Quality Assurance Program Description
U7-PROJ-J-GDD-0038, Rev. A, Technical Report for the Toshiba FPGA-based Safety-Related Instrumentation and Control System Design Process
U7-PROJ-J-P-EN02-0002, Rev. 0, Software Program Plan
U7-ELCS-J-PLAN-SW-0001, Rev. 1, ESF Logic and Control System Software Project Plan
WCAP-16096-NP-A, Rev. 1A, Software Program Manual for Common Q Systems
WCAP-16097-NP-A, Rev. 0, Common Qualified Platform Topical Report
WEC 6.1, Rev. 2, Document Control

WNA-PD-00100-TIX/TJX, Rev. 1, Engineered Safety Features Logic and Control System Software Project Plan
WNA-PD-00102-TIX/TJX, Rev. 0, South Texas Project 3 & 4 RRAS ESF Logic and Control (ELCS) Project Plan

LIST OF ACRONYMS

ABWR	Advanced Boiling Water Reactor
BTP	Branch Technical Position
COL	Combined License
Common Q	Common Qualification
DAC	Design Acceptance Criteria
DCD	Design Certification Document
DI&C	Digital Instrumentation and Control
ELCS	Engineered Safeguards Features Logic Control System
FPGA	Field Programmable Gate Array
I&C	Instrumentation and Control
IEEE	Institute of Electrical and Electronics Engineers
IP	Inspection Procedure
ITAAC	Inspection, Test, Analysis, and Acceptance Criteria
NRC	Nuclear Regulatory Commission
QA	Quality Assurance
SCMPP	Software Configuration Management Program Plan
SDP	Software Development Plan
SPP	Software Program Plan
STP	South Texas Project
SVVPP	Software Verification and Validation Program Plan
URI	Unresolved Item
V&V	Verification and Validation

(Continued Next Page)

APPENDIX

ATTACHMENT 65001.XX

INSPECTION OF DIGITAL INSTRUMENTATION AND CONTROL (DI&C) SYSTEM/SOFTWARE DESIGN ACCEPTANCE CRITERIA (DAC)-RELATED ITAAC

PROGRAM APPLICABILITY: 2503

65001.XX-01 INSPECTION OBJECTIVES

01.01 To verify that the combined license (COL) holder (licensee) has developed the digital instrumentation and control (DI&C) system as committed in the licensing basis.

01.02 To confirm by inspection that the COL licensee has adequately implemented the DI&C development process to yield a system that meets the acceptance criteria in the Inspections, Tests, Analyses and Acceptance Criteria (ITAAC).

01.03 To provide implementation guidance for use of the Appendices.

65001.XX -02 INSPECTION REQUIREMENTS AND GUIDANCE

02.01 Background. Inspection of ITAAC associated with a COL is intended to support the Commission finding stipulated in 10 CFR Part 52.103(g), specifically that the COL acceptance criteria (ITAAC acceptance criteria) have been met, and that the facility has been designed and built to conform to the licensing basis. The Commission policy for Design Acceptance Criteria (DAC), defined in SECY-92-053, allowed a licensee to provide implementation details for a Digital Instrumentation and Control (DI&C) design as ITAAC. The DI&C DAC-related ITAAC would be inspected as the development process for the associated systems progresses and the licensee completes the ITAAC throughout the facility post-COL (construction) phase.

02.02 Inspection Requirements and Guidance.

a. General Inspection Requirements. The development of safety-related DI&C systems and software should progress in accordance with a formally defined Life Cycle. Although life cycle activities may differ between licensees, all share certain characteristics. The staff's inspection and acceptance of digital safety system and software functions is based upon: 1) confirmation that acceptable plans were prepared to control software development activities; 2) evidence that the plans were implemented in the software development life cycles; and 3) evidence that the process produced acceptable design outputs.

   Generic inspection attributes and criteria for each DI&C Software Life Cycle Phase are provided within Appendices 1 through 6 of this IP. It is recognized that not all DI&C Life Cycle Phases may be inspected because they may not apply to each licensee's development program/process. The goal of this inspection activity is to examine the governing documents and samples of activities that demonstrate the implementation of these documents in order to provide a comprehensive inspection of the licensee's DI&C development process as delineated in the ITAAC.

   The actual planning and scheduling of the DI&C inspections is dependent on the licensee's development schedule and associated milestones. The guidance contained herein is intended to mirror a typical development life cycle. Inspections should not be planned until the completion of life cycle phases by the licensee can be anticipated and expected completion dates can be

confirmed. All construction inspection activities should be coordinated through the Region II Center for Construction Inspection (RII/CCI).

Specific Guidance. Gather pertinent information and discuss inspection planning and scheduling issues with the CCI Branch Chief, or designee, for example:

- importance/prioritization of activities
- concurrent inspections to be conducted using other IPs
- status of previous NRC findings
- licensee responses to applicable Bulletins, Circulars, and Information Notices sent to licensee
- commitments made in the COL pertaining to digital system/software development activities

Contact the licensee for information needed to prepare the inspection plan, for example:

- status of DI&C development activities, planned activities and schedule (used to focus inspection and determine inspection sample)
- identification of individuals assigned key positions and functions described by the licensee's Software Quality Assurance (QA) and Verification and validation (V&V) program
- availability of licensee personnel during the period tentatively scheduled for the inspection
- changes to Software QA or V&V program since any previous NRC inspection (e.g., policy, personnel , program description, implementing documents)

b. Requirements for Performance of Inspection. The inspection will be performed in accordance with the inspection plan. Adjustments to the inspection plan will be communicated to Region II/CCI to minimize impact to the licensee and to assist in revising inspection planning efforts accordingly. Unexpected events subsequent to approval of the inspection plan may result in changes to the inspection when conducted.

Specific Guidance. Conduct the inspection in accordance with this IP and its associated appendices.

c. Requirements for Inspection Reporting. An inspection report and any findings will be prepared, approved, and released in accordance with Inspection Manual Chapter 0613.

Specific Guidance. No specific guidance.

65001.XX -03 RESOURCE ESTIMATE

TBD

65001.XX-04 REFERENCES

1. 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants"
2. Regulatory Guide 1.206, C.II.1.2.5, "ITAAC for Instrumentation and Controls (SRP Section 14.3.5) and C.III.5, "Design Acceptance Criteria"
3. Regulatory Guide 1.152, Revision 2. "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission,

2006. (ML053070150)

4. Regulatory Guide 1.168, Revision 1. "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2004. (ML040410189)
5. Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997. (ML003740102)
6. Regulatory Guide 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
7. Regulatory Guide 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
8. Regulatory Guide 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
9. Regulatory Guide 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
10. NUREG 0800 (SRP), Section 14.3, “Inspections, Tests, Analyses, and Acceptance Criteria”
11. NUREG 0800 (SRP), Branch Technical Position (BTP) 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”
12. NUREG/CR-6101. "Software Reliability and Safety in Nuclear Reactor Protection Systems"
13. Inspection Manual Chapter 2503, “Construction Inspection Program: Inspections of Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Related Work”
14. Inspection Manual Chapter 0613, “Documenting 10 CFR Part 52 Construction and Test Inspections” (ML082490463).
15. ASME NQA-1, “Quality Assurance Requirements for Nuclear Facility Applications,” American Society for Mechanical Engineers.
16. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
17. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
18. IEEE Std. 730-2002, “IEEE Standard Criteria for Software Quality Assurance Plans”
19. IEEE Std. 828-1990, “IEEE Standard for Configuration Management Plans”
20. IEEE Std. 829-1983, “IEEE Standard for Software Test Documentation”
21. IEEE Std. 830-1993, “IEEE Recommended Practice for Software Requirements Specifications”
22. IEEE Std. 1008-1987, “IEEE Standard for Software Unit Testing”
23. IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation Plans"
24. IEEE Std. 1028-1997, “IEEE Guide to Software Configuration Management”
25. IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes"
26. IEEE Std. 1228-1994, "IEEE Standard for Software Safety Plans"

65001.XX -05 PROCEDURE COMPLETION

Implementation of this IP is considered complete when the planned sample of attributes for each of the specified appendices is complete.

END

Appendices:

1. Inspection Guide for DI&C System/Software Life Cycle - Planning Phase
2. Inspection Guide for DI&C System/Software Life Cycle - Requirements Phase
3. Inspection Guide for DI&C System/Software Life Cycle - Design & Implementation Phase
4. Inspection Guide for DI&C System/Software Life Cycle - Integration Phase
5. Inspection Guide for DI&C System/Software Life Cycle - Validation & Test Phase
6. Inspection Guide for DI&C System/Software Life Cycle - Installation Phase

Attachment:

1. Revision History Sheet for IP 65000.XX

Appendix 1. Inspection Guide for DI&C System/Software Life Cycle – Planning Phase

A1.01 INSPECTION OBJECTIVES

Verify that the licensee's DI&C development process Planning Phase documents are consistent with the ITAAC design commitments and acceptance criteria.

A1.02 SAMPLE SIZE

Inspection of DI&C DAC-related ITAAC will typically rely on selection of a sample of attributes for verification. Given the importance of the various Life Cycle Plans in defining and detailing the high quality design and development process expected for safety-related DI&C systems/software, inspection of a larger representative sample of attributes associated with the Planning Phase documents is appropriate.

A1.03 INSPECTION REQUIREMENTS AND GUIDANCE

General Guidance.

A digital system/software development life cycle provides definition for a deliberate, disciplined, and high quality development process. Implementation of this process should result in a high quality DI&C system and supporting software. Verification of this process should confirm, by evaluation against applicable standards and criteria, that the licensee and vendor procedures and plans are sufficient to accomplish this goal.

The Planning Phase activities will provide documents that will be used to oversee the DI&C development project as it progresses from one Life Cycle Phase to the next. The documents resulting from the Planning Phase include the following minimum set; additional documents may be required by the development organization as part of their standard business procedures.

- Software Management Plan (SMP)
- Software Quality Assurance Plan (SQAP)
- Software Configuration Management Plan (SCMP)
- Software Verification and Validation Plan (SVVP)
- Software Safety Plan (SSP)
- Software Development Plan (SDP)
- Software Integration Plan (SIntP)
- Software Installation Plan (SInstP)

Generally, these Planning documents include management characteristics, implementation characteristics, and resource characteristics. Not all specific characteristics occur for every Plan. Management characteristics for each Plan should include a stated Purpose, identify Organizational and Oversight responsibilities, and account for risk and security management. Implementation characteristics should include Process Metrics as well as guidance on Procedure control and Recordkeeping. Resource characteristics should include details of Special Tools utilized in the development process, Personnel resources and qualification, and

the Standards used to meet regulatory requirements. Inspection should focus on those aspects of the Plans which can impact the safety and quality of the resulting DI&C system/software.

The inspectable attributes identified in the following sections were compiled from many of the references listed in this procedure. Additionally, other attributes may be identified in the Acceptance Criteria of the specific ITAAC. These additional attributes should be included in the scope of the planned inspection. This inspection procedure verifies commitments made in the COL and licensing basis.

Inspection Requirements.

A1.03.01 Inspection of Software Management Plan (SMP).

a. Verify that the SMP addresses the following specific management aspects of the software development project, as committed to in the licensing basis:

    1. Organizational structure is defined. Responsibilities are known and documented, and a management structure exists to keep the SMP up to date through a configuration control process.

    2. Oversight of vendors. The SMP should describe the interaction between licensee and system/software vendors, extension of QA requirements to vendors, what checks and audits the licensee will perform and their impact.

    3. Independence between the software development group and the QA group, system/software safety group, and V&V group. If independence aspects are described in the planning documents of these organizations, such as the V&V Plan, Safety Plan or QA plan, the SMP should provide a pointer to those plans.

    4. Personnel responsible for various items have the experience, training and qualifications to perform those duties.

b. Verify that the SMP includes the following key attributes, as committed to in the licensing basis:

    1. Project schedule includes time allotted for review (management, V&V, etc.) and audit.

    2. Project work products and deliverables are well defined.

    3. Responsibilities documented and communicated to the development organization.

    4. Project constraints that may have an impact on safety are identified.

    5. Known risk factors are identified.

    6. Required reports and technical documents identified.

    7. Training requirements known and documented.

    8. Internal review and audit processes identified.

A1.03.02 Inspection of Software Quality Assurance Plan (SQAP).

a. Many aspects of software quality are described in the various Plans that are implemented for digital system/software development. This includes the Configuration Management Plan, the Software Safety Plan, and the Software Verification and Validation Plan.

The SQAP shall comply with the requirements of 10 CFR Part 50, Appendix B, and the licensee's overall QA program. The SQAP should typically: 1) identify which QA procedures are applicable to specific software processes; 2) identify particular methods chosen to implement QA procedural requirements; and 3) augment and supplement the QA program as needed for software.

Verify that the SQAP addresses the following, as committed to in the licensing basis:

1. SQA Management Tasks
2. Documentation
3. Recordkeeping
4. Standards, Practices, Conventions
5. Reviews and Audits
6. Problem Reporting and Corrective Action
7. Control of Tools, Techniques, and Methodologies
8. Supplier (Vendor) Control

b. Verify that the SQAP includes the following key attributes, as committed to in the licensing basis:

1. SQAP specifies which software products are covered by the Plan.
2. Project elements (organizations) that interact with the SQA organization are listed.
3. SQA organization is independent of the development organization, including cost and schedule.
4. Life Cycle development phases that will be subject to SQA oversight are listed.
5. Required SQA tasks are listed and described.
6. Conflict resolution among organizations is described.
7. Required software documents are listed.
8. Required reviews and audits are listed.

9. Methods by which each review and audit will be carried out is described.

10. SQAP includes provisions to assure that problems will be documented and corrected.

A1.03.03 Inspection of Software Configuration Management Plan (SCMP).

a. Verify that the SCMP addresses the following specific activities, as committed to in the licensing basis:

    1. Production/development baselines are identified and established.

    2. Review, approval, and control of changes is defined.

    3. Tracking and reporting of changes is defined.

    4. Audits and reviews of the evolving products are established.

    5. Control of interface documentation is defined.

b. Verify that the SCMP includes the following key attributes, as committed to in the licensing basis:

    1. Product interfaces that have to be supported within the project are identified.

    2. The required capabilities of the staff needed to perform SCM activities are defined.

    3. The responsibilities for processing baseline changes are defined.

    4. The SCMP specifies who is responsible for each SCM activity.

    5. The organizational interfaces that affect the SCM process are identified.

    6. SCM activities that will be coordinated with other project activities is described.

    7. Describes how phase-specific SCM activities will be managed during the different life cycle phases.

    8. Specific procedures exist to manage the change process.

    9. Audit procedures are defined.

    10. Configuration identification scheme matches the structure of the software product.

    11. SCMP specifies which items will be placed under configuration control (configuration items (CI)).

    12. SCMP describes the authority of the Configuration Control Board (CCB).

    13. CCB authority is sufficient to control safety-related changes to the CI baseline.

14. SCMP requires the Configuration Control Board to assess the safety impact of change requests.

15. Provisions are included for auditing the SCM process.

16. SCMP provides for periodic reviews and audits of the configuration baseline, including physical audits of the baseline.

17. SCMP provides for audits of suppliers and subcontractors, if such are used.

A1.03.04 Inspection of Software Verification & Validation Plan (SVVP).

a. Verify that the SVVP addresses the following specific activities, as committed to in the licensing basis:

1. Management of Life Cycle V&V. The major portion of the V&V Plan will describe the methods in which V&V will be carried out through the life of the development project. In general, the following activities should be required for each phase of the life cycle:

a) Identify the V&V tasks for the life cycle phase.
b) Identify the methods that will be used to perform each task.
c) Specify the source and form for each input item required for each task.
d) Specify the purpose, target and form for each output item required for each task.
e) Specify the schedule for each V&V task.
f) Identify the resources required for each task.
g) Identify the risks and assumptions associated with each V&V task.
h) Identify the organizations or individuals responsible for performing each V&V task.

2. Requirements Phase V&V. The V&V Plan should describe how the various V&V tasks will be carried out for the following:

a) Software Requirements Traceability Analysis
b) Software Requirements Evaluation (Report)
c) Software Requirements Interface Analysis
d) System Test Plan Generation
e) Acceptance Test Plan Generation

3. Design & Implementation Phase V&V. The V&V Plan should describe how the various V&V tasks will be carried out for the following:

a) Software Design Traceability Analysis
b) Software Design Evaluation (Report)
c) Software Design Interface Analysis

d) Test Plan Generation
e) Source Code Traceability Analysis
f) Source Code Evaluation
g) Source Code Interface Analysis
h) Source Code Documentation Analysis

4. Integration Phase V&V. The V&V Plan should describe how the various V&V task will be carried out for the following:

a) Integration Test Procedure Generation
b) Integration Test Procedure Execution

5. Validation & Test Phase V&V. The V&V Plan should describe how the various V&V tasks will be carried out for the following:

a) Acceptance Test Procedure Generation
b) System Test Procedure Execution
c) Acceptance Test Procedure Execution

6. Installation Phase V&V. The V&V Plan should describe how the various V&V tasks will be carried out for the following:

a) Installation Configuration Audit
b) Final V&V Report Generation

b. Verify that the SVVP includes the following key attributes, as committed to in the licensing basis:

1. SVVP references the SMP and/or SQAP.

2. Specific elements of the higher-level plans are addressed in the SVVP.

3. Scope of the V&V effort is defined.

4. V&V organization defined, along with its relationship to the development organization.

5. Schedule defined that provides enough time for V&V activities to be effectively carried out.

6. Tools, techniques, and methods to be used in the V&V process defined.

7. Each task is identified and tied into the project V&V goals.

8. SVVP identifies method of handling anomalies encountered during each activity.

9. V&V schedule and resource requirements are described in detail.

10. SVVP identifies the responsibilities of the V&V participants.

11. Defined procedure for management review of the V&V process.

12. Procedure for the periodic assessment and updating of the V&V procedures, methods, and tools.

13. Defined procedure for correlating V&V results with management and technical review documents.

14. SVVP is coordinated with project Planning documents to ensure early availability of the Planning documents for the V&V effort.

15. SVVP explicitly defines the activities required before the requirements development activities begin.

c. Verify that the SVVP includes the following Life Cycle Phase-specific attributes, as committed to in the licensing basis:

1. Requirements Activities

a) Concept documentation, software requirements specification (SRS), interface requirements, hazards analysis, and user documentation will be complete prior to beginning the V&V requirements analysis.
b) SVVP explicitly defines the activities required during the requirements analysis.
c) SVVP requires the performance of a software requirements traceability analysis that traces elements of software requirements to system and source requirements.
d) SVVP requires that the SRS be evaluated for safety, correctness, consistency, completeness, accuracy, readability, and testability.
e) SVVP requires that the SRS be evaluated for performance issues.
f) SVVP requires that a system test plan and an acceptance test plan be generated during the requirements phase.

2. Design & Implementation Activities

a) SVVP requires the generation and dissemination of anomaly reports.
b) SVVP explicitly defines the activities required during design/implementation phase.
c) SVVP requires the performance of a design traceability analysis that traces elements of the detailed design and coding to elements of the software requirements.
d) SVVP requires a design evaluation (report).
e) SVVP requires a design interface analysis.

f) SVVP requires that the software design document be evaluated against hardware requirements, operator requirements, and software interface requirements documentation.
g) SVVP requires a software component test plan, an integration test plan, and a test design be generated for use in later testing.
h) SVVP requires that the source code be evaluated for correctness, consistency, completeness, accuracy, readability, safety, and testability.
i) SVVP requires generation and use of test cases to help ensure the adequacy of test coverage.
j) SVVP requires the generation of test cases for software component, integration, system, and acceptance testing.

3. Integration, Validation & Test, and Installation Activities

a) SVVP explicitly defines the activities required during the integration and validation analysis and testing.
b) SVVP requires the performance of integration, system, and acceptance testing requirements sufficiently detailed so as to ensure that there is a very low probability of error during operation.
c) SVVP explicitly defines the activities required during the installation analysis and testing.
d) SVVP requires the performance of an installation configuration audit.
e) SVVP requires the generation of a final report.

A1.03.05 Inspection of Software Safety Plan (SSP)

a. Verify, consistent with commitments in the licensing basis, that the SSP addresses the following documentation that will be required as part of the software safety program:

1. Results of all safety analyses
2. Information on suspected or verified safety problems
3. Results of audits performed on software safety program activity
4. Results of safety tests carried out on the software system
5. Records on training provided to software safety personnel and software development personnel

b. Verify that the SSP includes the following key attributes, as committed to in the licensing basis:

1. Software safety organization is described and authority defined; authority sufficient to enforce compliance with safety requirements and practices.
2. SSP provides a mechanism for defining safety requirements, performing software safety analysis tasks, and testing safety-critical features of the DI&C system.

3. SSP describes what safety-related documents will be produced during the development life cycle; contents sufficient to ensure that known safety concerns are addressed in the appropriate places within the development life cycle.

4. SSP identifies the safety-related records that will be generated, maintained, and preserved.

5. SSP specifies the process of approving and controlling software tool use.

6. SSP provides a means to ensure that safety-critical software developed by a subcontractor meets the requirements of the software safety program.

A1.03.06 Inspection of Software Development Plan (SDP)

a. Verify, consistent with commitments in the licensing basis, the following:

1. SDP defines the tasks that are a part of each life cycle.

2. SDP defines life cycle inputs and outputs, including review, verification and validation of those outputs.

3. SDP lists the international, national, industry, and company standards and guidelines, including regulatory guides, which will be followed, and whether or not these standards and guidelines have previously been approved by the NRC staff.

b. Verify that the SDP includes the following key attributes, as committed to in the licensing basis:

1. Technical standards that will be followed are listed.

2. Technical milestones are listed.

3. Milestones are consistent with the schedule provided in the SMP.

4. Technical documents that must be produced are listed.

5. Technical documents are consistent with those listed in the SMP.

6. Milestones, baselines, reviews, and signoffs are listed for each document.

7. Audit reports document that the SDP is being followed.

A1.03.07 Inspection of Software Integration Plan (SIntP)

a. Verify, consistent with commitments in the licensing basis, the following:

1. SIntP describes the general strategy for integrating the software modules together into one or more programs.

2. SIntP integration strategy includes integrating the various software modules together to form single programs.

3. SIntP integration strategy includes integrating the software with the hardware and instrumentation, and testing the resulting integrated product.

b. Verify that the SIntP includes the following key attributes, as committed to in the licensing basis:

1. SIntP specifies the levels of integration required.

2. SIntP is consistent with the software design specification.

3. SIntP describes each step of the integration process.

4. SIntP describes the environment that will be used to perform and test each integration step.

5. Software and hardware tools that will be used to integrate the system are listed.

6. SIntP includes instructions on how to carry out integration steps.

7. SIntP includes a contingency plan in case the integration fails.

8. SIntP includes a requirement for configuration control of the completed product.

A1.03.08 Inspection of Software Installation Plan (SInstP)

a. Verify that the SInstP includes the following key attributes, as committed to in the licensing basis:

1. General procedures for installing the software product are described.

2. Materials required are listed in an Installation Package.

3. Complete step-by-step procedures exist for installation in the operational environment.

4. Expected results from each installation step are described.

5. Known installation error conditions and recovery procedures are described.

6. Installation Plan is fully tested.