Attachments 4 and 8 are to be ~~withheld from public disclosure under 10 CFR § 2.390~~.
When separated from these attachments, this letter is decontrolled.

TVA

Tennessee Valley Authority, Post Office Box 2000, Spring City, Tennessee 37381-2000

May 6, 2011

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

Watts Bar Nuclear Plant, Unit 2
NRC Docket No. 50-391

10 CFR 50.4

Subject: **WATTS BAR NUCLEAR PLANT (WBN) UNIT 2 – INSTRUMENTATION AND CONTROLS STAFF INFORMATION REQUESTS**

Reference: 1. Licensee Open Items to be Resolved for SER Approval List

The purpose of this letter is to provide TVA's responses to NRC's information requests on the "Licensee Open Items to be Resolved for SER Approval List." Enclosure 1 to this letter provides TVA's responses to the information requested by NRC.

Enclosure 2 contains the supporting documents for TVA's responses to NRC's requests/questions provided in Enclosure 1. Enclosure 3 contains a list of references on which TVA's responses are based. Enclosure 4 contains the new regulatory commitments contained in this letter.

Attachments 4 and 8 contain information proprietary to Westinghouse Electric Company LLC (WEC). TVA requests that the WEC proprietary information be withheld from public disclosure in accordance with 10 CFR § 2.390.

If you have any questions, please contact William Crouch at (423) 365-2004.

I declare under penalty of perjury that the foregoing is true and correct. Executed on the 6th day of May, 2011.

Respectfully,

David Stinson
Watts Bar Unit 2 Vice President

D030
NRR

Enclosures:

1. Responses to Licensee Open Items To Be Resolved For SER Approval
2. List of Attachments
3. List of References
4. List of New Commitments

cc (Enclosures):

U. S. Nuclear Regulatory Commission
Region II
Marquis One Tower
245 Peachtree Center Ave., NE Suite 1200
Atlanta, Georgia 30303-1257

NRC Resident Inspector Unit 2
Watts Bar Nuclear Plant
1260 Nuclear Plant Road
Spring City, Tennessee 37381

Enclosure 1
TVA Letter Dated May 6, 2011
Responses to Licensee Open Items to be Resolved for SER Approval

For some NRC requests for additional information (RAIs), this letter provides TVA's initial response. For the other NRC RAIs in this letter, a response has been provided in previous TVA letters to the NRC, and the NRC has subsequently requested additional information. For these requests, the initial TVA response is not repeated below. The additional NRC information requests are identified in this letter as "**Follow-up NRC Requests.**" TVA responses to these items are identified as "**TVA Response to Follow-up NRC Request.**"

The following acronyms/abbreviations are used in this letter:

AC 160	[1]Advant® Controller 160
[2]ANSI™	American National Standards Institute
[3]AP-1000	Westinghouse Generation III+ advanced light water reactor design
[4]BEACON™	Best Estimate Analyzer for Core Operations Nuclear
BISI	Bypass and Inoperable Status Indication
CET	Core Exit Thermocouple
CFR	Code of Federal Regulation
CGI	Commercial Grade Item
[5]DMIMS-DX™	Digital Metal Impact Monitoring System
EDCR	Engineering Document Change Request
EFPD	Effective Full Power Day
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
ENV	European Standard
[6]EPRI®	Electric Power Research Institute®
EQ	Environmental Qualification
FID	Fixed Incore Detector
FSAR	Final Safety Analysis Report
GA-ESI	General Atomic-Electronic Systems Inc.
ICS	Integrated Computer System (aka Plant Computer)
[7]IEEE™	Institute of Electrical and Electronics Engineers
IIS	Incore Instrument System
IITA	Incore Instrument Thimble Assembly
LPMS	Loose Parts Monitoring System
MCR	Main Control Room
MIDS	Movable In-core Detector System
MTP	Maintenance and Test Panel
NDL	Nuclear Data Link
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OI	Open Item (from NRC I&C Open Item Matrix)
OM	Operators Module

[1] Advant is registered trademark of ABB Automation Technology Products Management AG
[2] ANSI is a registered trademark of the American National Standards Institute
[3] AP-1000 is a registered trademark of the Westinghouse Electric Company LLC
[4] BEACON is a registered trademark of the Westinghouse Electric Company LLC
[5] DMIMS-DX is a registered trademark of the Westinghouse Electric Company LLC
[6] EPRI and Electric Power Research Institute are registered service marks of the Electric Power Research Institute Inc.
[7] IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers Inc.

PAMS	Post Accident Monitoring System
PDMS	Power Distribution Monitor System
RAI	Request for Additional Information
RFI	Radio Frequency Interference
RG	Regulatory Guide
RTP	Reactor Thermal Power
SDD	Software Design Document
SE	Safety Evaluation
SPDS	Safety Parameter Display System
SPD	Self Powered Detector
SRP	Standard Review Plan (NUREG-800)
SRS	Software Requirements Specification
SSER	Supplemental Safety Evaluation Report
SWCCF	Software Common Cause Failure
SysRS	System Requirements Specification
TSC	Technical Support Center
TSM	Technical Specification Monitor
TVA	Tennessee Valley Authority
V&V	Verification and Validation
WEC	Westinghouse Electric Company LLC
WBN	Watts Bar Nuclear Plant
[8]WINCISE™	Westinghouse In-Core Information Surveillance & Engineering

1. **NRC Request (Item Number 340)**

Provide test result curves for all EMI/RFI tests listed in Table 3.2.3 (page 3-8) of the Qualification Test Report 04508905-QR. In addition, please provide the standards or the guidance documents used as the source for ENV 50140, ENV 55011 Class A, and EN 55022 Class B.

Follow-up NRC Request

NRC current review guidance is based on compliance with RG 1.180 or equal with justification for variations. TVA is requested to provide the roadmap for compliance to RG 1.180 with justifications for any deviations. Simply following TVA standard specification SS E18.14.01, Rev. 3 is not sufficient.

TVA Response to Follow-up NRC Request

Attachment 1 provides a comparison of the TVA EMC Standard Specification E18.14.01, Revision 3 requirements to Regulatory Guide (RG) 1.180 Revision 1 requirements. The comparison shows that the TVA specification complies with the RG requirements.

[8] WINCISE is a registered trademark of the Westinghouse Electric Corporation LLC

2. **NRC Request (Item Number 346)**

TVA has previously stated in response to open item 319 that RM-1000 System Verification Test Results report, 04507007-1TR is not applicable to WBN-2. However, TVA has not provided a WBN-2 specific test results report. Please identify and provide the appropriate test results reports to complete the review.

Follow-up NRC Request

Report 04507007-1TR, 1999 states in the Test Summary that "Initially the testing was done using the [Sorrento Electronics] safety related production modules that had undergone software V&V testing. The majority of the testing was done by using two of the Sequoyah non-safety related production modules for the TVA contract, substituted for the [Sorrento Electronics] modules." Since the report is based on primarily non safety related components TVA to clarify and justify why NRC should accept this test report for safety related V&V testing.

TVA Response to Follow up NRC Request

GA-ESI has a single process for buying material, assembling, and testing modules. The same safety-related processes are used for any part number, safety-related or not, to avoid having to store the same part number in two different locations and avoid the possibility of mixing them up. Therefore, the Sorrento Electronics "safety-related" production modules and the Sequoyah "non-safety-related" modules are physically identical. Based on the above, the report is acceptable.

3. **NRC Request (Item Number 353)**

Please provide a summary of the [manufacturer's] commercial dedication plan for radiation monitors with references to the guidance document that it follows. Also please include different facets (e.g. receiving, inspection, testing etc.) of the plan.

After additional discussion with the NRC, it was determined that the focus of this question is on dedication of CGI used in the digital safety-related RM-1000 radiation monitors. The specific requirement is contained in NUREG-800, Section 7.0A, Revision 5, which requires that the dedication meet the requirements of EPRI topical report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications", dated October 1996. The topical report requires that dedication of commercial grade items for digital safety systems utilize two or more of the methods described in EPRI guideline NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07)", dated June 1988.

Follow-up NRC Request

(1) TVA to review and satisfy itself with the procedure and provide NRC a copy of the procedure for review.

(2) In addition, TVA and GA-ESI to provide information as to what additional measures were taken by GA-ESI with available documentation to prove that more than one method was followed for commercial dedication.

TVA Response to Follow up NRC Request

(1) TVA has reviewed the revised GA-ESI procedure and determined that the revision brings the GA-ESI commercial grade dedication program into conformance with the requirements of NUREG-800, Section 7.0A, Revision 5 EPRI Topical Report TR-106439 and EPRI guideline NP-5652. Attachment 2 contains GA-ESI Procedure OP-7.3-240, "Safety-Related Commercial Grade Item Parts Acceptance," Revision I.

(2) As stated in Attachment 4 of TVA letter to NRC dated April 15, 2011 (Reference 1), the due date for resolution of this issue is September 15, 2011.

4. **NRC Request (Item Number 362)**

OI #331 requested TVA to provide information regarding how the Loose Parts Monitoring System (LPMS) in-containment components (e.g., Accelerometer (including the integral insulated hardline cable), Softline cable, and Remote Charge Preamplifiers) were qualified for vibration as addressed in regulatory position C.1.g of RG 1.133, Rev. 1. TVA responded by stating that "TVA has reviewed the information provided by Westinghouse describing how the Loose Part Monitoring System (LPMS) sensor is qualified for normal operating conditions provided in Westinghouse letter WBT-D-2782, dated December 17, 2010 (Reference 11) as addressed in regulatory position C.1.g of Reg. Guide 1.133 and found it acceptable. Vibration qualification is not applicable to the softline cable. Due to the installation location (junction boxes mounted to the shield or fan room walls) and previous seismic qualification, vibration qualification of the charge converter/preamplifier is not required. This completes the response to this item."

However, the staff still desires further clarification on this response. (1) Specifically, please provide a documented basis that demonstrates the LPMS in-containment equipment is qualified for normal operating conditions (e.g., test results compared to the equipment qualification specification), including vibration qualification. (2) Also, provide justification for why vibration qualification if the Remote Charge Preamplifier is not required

TVA Partial Response to NRC Request

(1) Attachment 4 contains Westinghouse document "WBT DMIMS-DX™ Seismic Evaluation of the Digital Metal Impact Monitoring System (DMIMS-DX™) for Watts Bar Unit 2," EQ-QR-33-WBT, Revision 0 (proprietary). The non-proprietary version of "WBT DMIMS-DX™ Seismic Evaluation of the Digital Metal Impact Monitoring System (DMIMS-DX™) for Watts Bar Unit 2," EQ-QR-33-WBT, Revision 0 and the affidavit for withholding will be submitted within two weeks of receipt from Westinghouse.

Attachment 5 contains Westinghouse non-proprietary white paper WBT-D-2782, "Westinghouse DMIMS-DX In-Containment equipment environmental specifications."

EQ-EV-71-WBT-P, Revision 1, "Environmental Evaluation and Operating History of the Westinghouse DMIMS-DX Preamplifier and Softline Cable Used at Watts Bar 2," dated February 2011 was submitted in TVA letter to NRC dated February 25, 2011 (Reference 3).

(2) The Remote Charge Preamplifiers are mounted in junction boxes inside containment. The junction boxes are hard mounted either to the crane wall or to a fan room wall. The crane wall and fan room walls are not subject to any significant vibration during normal operation.

5. **NRC Request (Item Number 363)**

OI#199 requested TVA to provide information concerning how TVA plans to meet regulatory criteria for Quality (10 CFR 50.55a(a)(1)) associated with the Technical Support Center and Nuclear Data Link. TVA responded in Letter Dated October 5, 2010, Item 63; however, TVA's response does not address the quality aspects of these system features. A similar question had been asked for Quality Criteria adherence for the SPDS and the BISI functions of the Integrated Computer System. In response to that request (same letter) TVA provided a description of TVA procedures, BISI software development procedures, and various management measures that will be taken to assure high quality in the design, operation, and maintenance of the SPDS and BISI functions of the ICS. Since the TSC and Nuclear Data Link information originates in the SPDS function of the ICS, are there any aspects of the quality measures that apply to the TSC and NDL features developed as part of quality processes for the ICS that are applicable to the data communications features?

Specifically, what is the scope of TVA Procedure SPP-2.6 "Computer Software Control"? How does it apply to the ICS functions of a) SPDS, b) BISI, and c) TSC and NDL functions? Wouldn't there be aspects of the quality procedures that apply to the development, maintenance, and operations of the software needed to support the data communications features. Also, what quality measures will be applied to develop, maintain, and operate the hardware that accomplishes the TSC and NDL functions to ensure that these features will be reliable and available when needed?

TVA Response to NRC Request:

TVA Procedure SPP-2.6 "Computer Software Control," has been superseded by TVA Procedure NPG-SPP-12.7, "Computer Software Control," Revision 0, dated December 17, 2010 (Attachment 3).

To ensure quality, the design, testing, and inspection of all Integrated Computer System (ICS) software including (a) SPDS, (b) BISI and (c) Technical Support Center (TSC) and Nuclear Data Link (NDL) functionality is controlled by qualified personnel in accordance with TVA Procedure NPG-SPP-12.7. The TSC and NDL functions are provided and performed by the ICS and, in the case of NDL, the Central Emergency Control Center (CECC) computers in Chattanooga.

Any changes to ICS software must be documented and controlled using TVA Procedure NPG-SPP-12.7. This includes the (a) SPDS, (b) BISI and (c) TSC and NDL functions. The procedure details controls and processes required for the development, modification, and configuration management of computer software used to support the design, operation, modification, and maintenance of TVA's nuclear power plants consistent with the Nuclear Quality Assurance Plan.

Controls in NPG-SPP-12.7 guide the development and testing of the software changes. Other controls established by this procedure to further maintain quality standards are:

- The application custodian implements controls to prevent unauthorized changes to the software.
- Changes are made in a non-production environment, and validation testing takes place before the change is installed on the ICS when possible.
- Once validation testing begins, the source code is placed under configuration control.
- When the modifications are installed on the ICS, an operability test is performed to demonstrate that the software is installed correctly and is functioning correctly in its operating environment.
- Documentation related to ICS software changes are quality assurance (QA) records.
- The software source code is kept in a physically secure, environmentally controlled space to prevent inadvertent changes.
- Cyber security considerations are also considered in the storage environment.
- The data goes through several validation steps before being presented to the operators.
- When redundant sensors are used, the data received by the computer can be processed by software to determine if the quality of one or more points is questionable.

The hardware involved in the TSC and NDL functionality is verified to be operable on a periodic basis.

In the case of the NDL functionality, the ICS transmits the required data to the CECC on a continuous basis. The CECC monitors the status of the ICS data communications, and alarms are generated when the link is not active. The Emergency Plan (EP) staff conducts a quarterly test that verifies that NDL data is successfully transmitted from each unit to the NRC.

6. **NRC Request (Item Number 364)**

On 5/6/2010 (See Open Item No. 81) the NRC Staff requested an evaluation of the Common Q PAMS against the current staff position.

By letter dated 2/25/11 (ML110620219), TVA docketed a response: TVA performed an analysis and concluded that the Common Q PAMS equipment does not need to meet either IEEE 279-1971 or IEEE 603-1991 and so no analysis was performed or provided.

However, SRP (NUREG-0800 Rev. 2 dated March 2007) Section 7.7, "Information System Important to Safety," specifically identifies IEEE Std 603-1991 as being applicable to *accident monitoring instrumentation. Based upon the review of this item, the staff finds the following open items:*

1. *TVA to demonstrate that the Common Q PAMS meets the applicable regulatory requirements in IEEE Std 603-1991.*

2. *TVA to update FSAR (Amendment 103) Table 7.1-1 to reference IEEE Std 603-1991 for WBN2 Common Q PAMS and Sorrento Containment High Radiation Monitors.*

TVA Partial Response to NRC Request:

2. Table 7.1-1 will be updated to reference IEEE Std 603-1991 for the Common Q PAMS.

   TVA has reviewed the requirements of IEEE Std 603-1991 for the Sorrento Containment High Range Radiation Monitors and determined that IEEE Std 603-1991 is not applicable. IEEE 603-1991 is applicable to actuation systems. While TVA lists the containment high range radiation monitors as RG 1.97 Revision 2 Type A variables, the classification is not based on the RG 1.97 requirements which states:

   "Type A, those variables that provide primary information needed to permit the control room operating personnel to take the specified manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accident event."

   TVA calculation WBN0SG4047, "PAM Type 'A' Variables Determination," uses a broader definition. The calculation definition is:

   "The type 'A' variables will be divided into three groups based on the parameter's purpose. The groups are: (1) event identification, (2) event recovery to plant stabilization, and (3) maintaining the stabilized conditions from event recovery to hot standby. Following a reactor trip, the termination point for transients at WBNP is considered a stabilized condition at hot standby per chapter 15 of the WBN FSAR. Event recovery actions are those manual actions taken to mitigate a design basis accident to a stabilized condition. The plant can be considered stabilized when the plant parameters vary slowly and automatic systems are not being initiated. The diagnostic process consciously performed by the operator via the plant variables to interpret an event indication will be considered as a safety-related operator action regardless of the lack of manual manipulation of equipment. This diagnostic process is necessary to enable the operator to distinguish the 'type' of transient and take the correct mitigating actions."

   A review of TVA calculation WBN0SG4047 and the associated Emergency Instructions found that there are no operator actions that meet the RG 1.97 Revision 2 definition for a Type A variable which are based on the containment high range radiation monitors. Based on this review, IEEE 603 is not applicable to the containment high range radiation monitors.

7. **NRC Request (Item Number 365)**

On 5/6/2010 (See Open Item No. 81) the NRC Staff requested an evaluation of the Common Q PAMS against the current staff position.

By letter dated 2/25/11 (ML110620219), TVA docketed a response: "that WBN2 is not committed in complying with Reg. Guide 1.75...Since WBN2 is not committed to RG 1.75 or IEEE-384, no comparison is required..."

However, WBN2 is committed to RG 1.75 Rev. 2, "Physical Independence of Electric Systems." RG 1.75 Rev. 3 and IEEE Std. 384-1992 are used, in part, to address IEEE Std 603-1991 Clause 5.6.1. The current NRC staff position for RG 1.75 is documented in Rev. 3. Based upon the review of this item, the staff finds the following open item:

1. *TVA to update FSAR (Amendment 103) Table 7.1-1 to include RG 1.75 Rev. 3 for WBN2 Common Q PAMS and the Sorrento Containment High Radiation monitor.*

The Common Q PAMS was designed to meet the requirements of RG 1.75 Rev. 2. WBN2 did not perform an analysis to RG 1.75 Rev. 3. Based upon the review of this item, the staff finds the following open item:

2. *TVA to evaluate Common Q PAMS and the Sorrento Containment High Radiation monitor for conformance with RG 1.75 Rev. 3.*

TVA Response to NRC Request:

The Common Q PAMS and containment high range radiation monitor internal wiring meets the requirements of RG 1.75. The external Common Q PAMS and containment high range radiation monitor cables are routed as 1E, 10 CFR 50.49, trained cables in accordance with WBN Design Criteria WB-DC-30-4, which is not in conformance with RG 1.75 Revision 3 or IEEE Std 384-1992.

As noted in WBN Unit 2 FSAR Section 8.1.5.3, "Compliance to Regulatory Guides and IEEE Standards," note 2, RG 1.75 was issued after the WBN design was complete. Separations criteria for WBN are given in Section 8.3.1.4.2."

FSAR Section 8.3.1.4.2 provides a detailed discussion of the WBN Unit 2 separation requirements and compensatory actions. To ensure that non-1E cables do not degrade 1E cables, non-1E routed in Class 1 structures are evaluated to ensure that they are adequately protected to prevent propagation of damage from the non-1E cables to 1E cables.

The NRC reviewed TVA's separation criteria as supplemented by a breaker testing program in SSER 16 and found it to be acceptable. The same criteria and breaker testing program are applicable to WBN Unit 2.

8. **NRC Request (Item Number 366)**

On 5/6/2010 (See Open Item No. 81) the NRC Staff requested an evaluation of the Common Q PAMS against the current staff position.

By letter dated 2/25/11 (ML110620219), TVA docketed a response: TVA stated that the Common Q PAMS equipment fully meets the RG 1.100 Rev. 0 and is compliant with Rev. 3, with exception of testing above 33 Hz, which is not applicable to Watts Bar.

The WBN2 FSAR (Amendment 103) references Regulatory Guide 1.100 Rev. 1 "Seismic Qualification of Electrical Equipment for Nuclear Power Plants." The Common Q PAMS was designed to meet the requirements of RG 1.100 Rev. 2. RG 1.100 Rev. 3 is the current revision of this guide and is endorsed by the NRC. RG 1.100 Rev. 3 endorses IEEE 344-2004.

Based upon the review of this item, the staff finds the following open item:

1 TVA to update FSAR (Amendment 103) Table 7.1-1 to include RG 1.100 Rev. 3 for WBN2 Common Q PAMS and the Sorrento Containment High Radiation monitor.

or

2 TVA to evaluate Common Q PAMS for conformance with RG 1.100 Rev. 1.

TVA Response to NRC Request:

The Common Q PAMS and RM-1000 radiation monitors comply with IEEE 344-2004 and with RG 1.100 Revision 3 with the exception of issues associated with testing above 33Hz. FSAR Table 7.1-1 will be updated to reflect conformance.

9. **NRC Request (Item Number 367)**

On 5/6/2010 (See Open Item No. 81) the NRC Staff requested an evaluation of the Common Q PAMS against the current staff position.

By letter dated 2/25/11 (ML110620219), TVA docketed a response.

The WBN2 FSAR (Amendment 103) references RG 1.153 Rev. 0, "Criteria for Safety Systems." The Common Q PAMS is designed to meet the requirements of RG 1.153 Rev. 1. By letter dated February 25, 2010 (ML110620219), TVA stated:

"The subject Regulatory Guides [RG 1.153 Rev. 0 & 1] endorse and reference other standards. Common Q PAMS has been evaluated to comply with the requirements of these other endorsed standards ([Comparison report in this letter titled IEEE-279-1971 to IEEE-603-1991 Comparison]). Therefore no additional analysis needs to be performed and no further action is necessary."

However, the "Comparison report in this letter titled IEEE-279-1971 to IEEE-603-1991 Comparison," stated:

"The first of the two standards, IEEE-279, is part of the design basis of WBN2 but is not relevant to Common Q PAMS. The second standard, IEEE-603-1991 is not part of the design basis for the Common Q PAMS for WBN2."

Based on the reasoning quoted above, WBN2 did not evaluate the Common Q PAMS against the criteria of RG 1.153 Rev. 1; therefore, the staff finds the following open item (see also Open Items 364 No. 1 & 2 above.):

1. *TVA to evaluate Common Q PAMS for conformance with RG 1.153 Rev. 1.*

TVA Response to NRC Request:

Common Q PAMS complies with RG 1.153, Revision 1. The response in Attachment 4 of TVA to NRC letter dated February 25, 2011 (Reference 3) was in error.

10. NRC Request (Item Number 368)

On 5/6/2010 (See Open Item No. 81) the NRC Staff requested an evaluation of the Common Q PAMS against the current staff position.

By letter dated 2/25/11 (ML110620219), TVA docketed a response.

The WBN2 FSAR (Amendment 103) references RG 1.152 Rev. 0, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." The Common Q PAMS was designed to meet the requirements of RG 1.152 Rev. 1. RG 1.152 Rev. 2 is the current revision of this guide and is endorsed by the NRC. By letter dated February 25, 2010 (ML110620219), TVA stated:

"RG 1.152 rev 2 endorses ANSI/IEEE-ANS-7-4.3.2-2003, but also provides extra regulatory guidance concerning computer based cyber security. Since this revision was not part of the design basis of WBN2 or Common Q PAMS, the project makes no commitment to the compliance of RG 1.152 rev 2."

Based upon the review of this item, the staff finds the following open item:

1. *TVA to evaluate Common Q PAMS for conformance with RG 1.152, Rev. 2.*

TVA Response to NRC Request:

As documented in Attachment 6, Common Q PAMS is in conformance with RG 1.152, Revision 2, with the exception of the cyber security requirements.

The Common Q PAMS will meet the cyber security requirements for the WBN Unit 2 Nuclear Security Program as mandated by 10 CFR 73.54 via WBN Unit 2 Procedure 25402-3DP-G04G-00508, "Cyber Security Program." This cyber security procedure addresses the security controls identified in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3, which are very similar to the recommended controls endorsed by the NRC in

RG 5.71, "Cyber Security Programs For Nuclear Facilities," Revision 0, and NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6.

11. NRC Request (Item Number 370)

On 5/6/2010 (See Open Item No. 81) the NRC Staff requested an evaluation of the Common Q PAMS against the current staff position.

By letter dated 2/25/11 (ML110620219), TVA docketed a response.

The WBN2 FSAR (Amendment 103) does not reference RG 1.168, IEEE 1012, or IEEE 1028. IEEE Std 7-4.3.2-2003 identifies IEEE Std 1012-1998 as normative. RG 1.168 Rev. 1 endorses, with clarifications, IEEE 1012-1998. The current staff positions are documented in RG 1.168 Rev. 1, IEEE 1012-1998, and IEEE 1020-1997. Based upon the review of this item, the staff finds the following open item:

1. *WBN2 to update FSAR Table 7.1-1 to reference RG 1.168 Rev. 1, IEEE 1012-1998, and IEEE 1020-1997 as being applicable to WBN2 Common Q PAMS and the Sorrento Containment High Radiation monitor.*

TVA Partial Response to NRC Request:

Common Q PAMS is designed in accordance with RG 1.168, Revision 1, IEEE 1012-1998 and IEEE 1020-1997. These references will be added to FSAR Table 7.1-1.

12. NRC Request (Item Number 372)

On 5/6/2010 (See Open Item No. 81) the NRC Staff requested an evaluation of the Common Q PAMS against the current staff position.

By letter dated 2/25/11 (ML110620219), TVA docketed a response.

The requirements in the SysRS and SRS are not traceable back to the design basis (e.g., IEEE Std 603-1991 Section 4) for the system. The SRS does not include any documented evidence that it was ever independently reviewed in accordance with the 10CFR50 Appendix B Criterion III, "Design Control." (Note: It appears that the only Common Q or WBN2 PAMS document that was independently reviewed in accordance with 10 CFR 50 Appendix B requirements is the SysRS.)

Based upon the review of the SysRS and SRS, the staff finds that there is reasonable assurance that the systems fully conform to the applicable guidelines, except for the following open items:

1. *TVA to produce an acceptable description of how the SysRS and SRS implement the design basis requirements of IEEE 603-1991 Clause 4.*

2. *TVA to produce a final SRS that is independently reviewed in accordance with 10 CFR 50 Appendix B, "Criterion III Design Control," requirements.*

TVA Partial Response to NRC Request:

1. Attachment 7 contains the evaluation for how the Common Q PAMS SysRS and SRS implement the design basis requirements of IEEE 603-1991, Clause 4.

13. NRC Request (Item Number 374)

By letter dated October 29, 2010 (ML103120711), TVA docketed a draft technical evaluation associated with an engineering design change (ML103120712) that states the Common Q PAMS will require changes in the technical specifications. The technical specifications (TS) have not been received yet for review. The TS will be reviewed once they are received.

1. *Confirm/Verify Technical Specification changes associated with Common Q PAMS are acceptable.*

TVA Response to NRC Request:

1. The TS changes required by implementation of the Common Q PAMS were made in Revision B of TS Section 3.3.3, "Post Accident Monitoring (PAM) Instrumentation," which were submitted in TVA letter to NRC dated February 2, 2010, "Watts Bar Nuclear Plant (WBN) - Unit 2 - Developmental Revision B of the Technical Specifications (TS), TS Bases, Technical Requirements Manual (TRM), TRM Bases; and Pressure and Temperature Limits Report (PTLR)," ADAMS accession number ML100550326 (Reference 2).

14. NRC Request (Item Number 375)

1. *During the conference call held on 4/12, the staff requested TVA to provide a description of the differences in hardware and/or software design and implementation of the Incore Instrumentation System instrumentation between WBN2 and WBN1. This information was not included in the 4/15 letter. When will this be provided?*

2. *The response for item g provided by TVA does not describe how the regulatory requirements were met. It only listed the criteria and stated that it passed the test. Also, the criteria for IITA does not list criteria for environmental qualifications of safety-related equipment (e.g., RG 1.29, Environmental Equipment Qualifications). Please provide summary test reports.*

3. *Attachment 4 of the TVA letter 4/15 states that the CET and CET cable assembly, as well as mineral insulated cables and IITA connectors, are EQ and class 1E qualified. Please provide the qualification summary test report for these components.*

4. *Attachment 5 of the TVA letter 4/15 provides the hardware description for the WINCISE (WEC document NO-WBT-002). Does this document include a section for Software Description? If so, please provide a copy.*

5. *Attachment 7 of the TVA letter 4/15 describes the functionality of the IIS for Watts Bar unit 2 and the IIS used in AP-1000. The description provided only describes the*

similarity for the core exit thermocouple (CET) and the PAMS system. However, this document does not describe the other components of the IIS (e.g. IITAs). Please clarify if the only similarity between Watts Bar unit 2 and AP-1000 is for the CETs and PAMS, and that there is not similar for the IITAs.

6. *The WCAP-12472-P-A for the BEACON system describes that the system has three operational levels: on line monitoring, tech spec monitor (TSM), and direct margin monitor. For Unit 1, TVA requested approval of the Beacon TSM to be only used as a tech spec monitor for present peaking factor limits. Please confirm that the functionality to be implemented in Unit 2 is the same than the one requested and approved for unit 1. Note Attachment 5 states that the Beacon servers run the Beacon TSM, but it is not clear that this is the only level operating for the IIS.*

7. *The SE for use of the Beacon System in Unit 1 states that the BEACON system will be used when thermal power is greater than 25% RTP. Page 129 of Attachment 4 states that "the WINCISE system will be capable of performing its required core monitoring functions at or above 20%RTP." Please clarify what the intent is for the Beacon system in Unit 2.*

8. *The technical evaluation provided for the Beacon System for unit 1 states that "the movable incore detectors (MIDs) are used for periodic calibration of the PDMS when thermal power is greater than 25% RTP. Additionally, the MIDs are used whenever the PDMS is inoperable or whenever power distribution is below 25%." Please explain how this function will be performed with the fix incore detectors and the Beacon system for unit 2.*

9. *In the NRC SE for WCAP-12472-P-A for the BEACON system, the staff accepted this system but subject to three conditions. In the TVA submittal for use of the Beacon system in unit 1, TVA described how they met these conditions for Unit 1. Please describe how TVA will meet these conditions for Unit 2.*

10. *Please clarify the following statement provided in Attachment 4, Page 25: "During certain accident scenarios, it is possible for the CETs to see temperatures up to 20 deg F different from Unit 1."*

11. *Attachment 4 and 5 explained that the Mineral Insulation cable allows the isolation of the core exit thermocouples (1E) and self-powered neutron detector (non-1E) signals. Please provide the analysis that evaluated this separation, as well as the evaluation that show that failure of the non-1E signal won't affect the 1E signal.*

12. *Page 129 of Attachment 4 states that a minimum of three thermocouples are operable in each quadrant. Table 7.5-2 of the SSER (R.G. 1.97) states that 4 thermocouples should be operable in each quadrant. Please explain if TVA is deviating from the requirements in R.G 1.97, and how this is justified.*

13. *Please provide information regarding the effects of a software common cause failure (SWCCF) on the IIS.*

14. *The FMEA provided by TVA on 4/15 has not been updated. Also, the FMEA provided focus on failures during installation and commissioning and it does not*

identify measures for failures during operation. Last, this FMEA does not address software failures, only component failures and installation failures. Please provide an updated and complete version of the FMEA.

15. *Attachment 4, TVA document "Incore Instrumentation System" describes the system requirements. Therefore, provide a complete system description of the IIS for the staff to evaluate the IIS to be installed in Watts Bar Unit 2. Also, the description for the incore thermocouple system in this TVA document is inconsistent with the description provided in Westinghouse WINCISE Hardware Description (Attachment 5). For example, Section 1.2 of the TVA document states that there are 65 incore thermocouples and Section 2.2.9 describes that the incore thermocouples provide an input signal to the Inadequate Core Cooling Monitor.*

16. *TVA attachment 4 of the 4/15 letter show modifications to the DBE design criteria. Please provide detailed explanation about these modifications.*

17. *Please explain if new penetration and routing were required for IIS' signals. If new penetrations are required, explain how these were qualified. Also, explain the criteria used to route the power/control cables.*

18. *Questions on Technical Specification:*

    (1) The TVA package states that TS 3.1 and TS Bases 3.1 were modified due to WINCISE. Please provide detailed information to evaluate the modifications to the TS.

    (2) The TVA mark up does not define the operating limits in the TS for the reactor power distribution. Please provide detailed information on how the IIS may impact the Technical Specification.

19. *Redundancies are designed and built into the signal processing system to avoid impacting operation in the event of the loss of some SPD signals. The master signal processing rack data interface card provides the output data stream to the Application server. Each cabinet master signal processor rack contains redundant data interface cards. Loss of one data interface card will not result in a loss of data output from the cabinet. Provide detailed description on how this works (e.g., is the switchover software based?)*

20. *The Application Servers receive information from Signal Processing System (SPS Cabinets), Integrated Computer System (ICS), and BEACON. The WINCISE IP Switches provide the main hub for traffic flow from the SPS cabinets, BEACON servers, Application Servers, and ICS. Provide detailed description of the communication among the Integrated Computer System (ICS) and the Beacon System and the WINCISE's Application servers.*

21. *Attachment 4, TVA document "Incore Instrumentation System" describes that the WINCISE system includes a Domain server, which provides a supportive function and is not required for the PDMS to receive needed information from the Application Server. However, the domain server provides an environment for the development and maintenance of application and system software. Please explain how this*

domain server will be configured and used for WINCISE in WBN2. Note that the domain server is not part of the Westinghouse WINCISE Hardware Description (Attachment 5)

22. *Page 52 of Attachment 4, question 1.5 was answered yes, but the I&C calculation to be provided in Sections 4 and 5 is not included. Please explain if this calculation was performed, and if so provide a description.*

23. *Page 52 of Attachment 4, Section 6 does not include the block diagram of the proposed modification to WBN2. Please provide a block diagram of the system, including power sources.*

TVA Partial Response to NRC Request:

1. System differences are described in Engineering Document Construction Release (EDCR) 52321-1 Excerpts (Attachment 4 of TVA letter to NRC dated April 15, 2011 (Reference 1) pages 2 and 3, 7 through 9, and 60 through 113.

2. Please see the response to EQ report request item 3 below. Only the safety-related portion of IITA (namely the CETs and CET cable assemblies) are safety significant and fall under the cited regulatory guide.

3. Please refer to Westinghouse report DAR-ME-09-10, Revision 0, Qualification Summary Report for the WINCISE Cable and Connector Upgrade at Watts Bar Unit 2 (proprietary) (TVA Document Number: 25402-011-V1A-MG00-01949-001-WBT-D-1464) (Attachment 8) for qualification of the associated cable assemblies. The non-proprietary version of DAR-ME-09-10, Revision 0, Qualification Summary Report for the WINCISE Cable and Connector Upgrade at Watts Bar Unit 2 and the affidavit for withholding will be submitted within two weeks of receipt from Westinghouse.

   The qualification report for the IITAs has not been completed. The proprietary and non-proprietary versions and the affidavit for withholding will be submitted within two weeks of receipt from Westinghouse.

5. The IITA are composed of the CET and the self-powered neutron detectors (SPDs). The WBN Unit 2 and AP1000 IITAs have the same function, but are a slightly different design. These differences are necessary because the WBN IITAs are bottom mounted and the AP1000 IITAs are top mounted. Additionally, the IITA are sized appropriately for WBN and AP1000 because the fuel assemblies are different sizes. The WBN IITA design includes 5 self-powered neutron detectors (SPDs) of sequentially increasing length, up to a maximum length of 12 feet. The AP1000 IITA design includes 7 SPDs of sequentially increasing length, up to a maximum of 14 feet.

6. Unit 2 has only been provided with the BEACON TSM function.

7. The BEACON topical report states that BEACON PDMS will be inoperable below 25% RTP. The electrical equipment operability requirements are set below the core power distribution monitoring requirements to ensure that the electronics are operable when needed to support core monitoring.

8. Periodic flux maps using the MIDs (Unit 1) have been replaced by continuous analysis of the permanently installed fixed incore detectors (Unit 2). Data from these fixed incore detectors will periodically be used to generate a set of calibration factors for the BEACON PDMS. The following description was provided in response to an RAI for Addendum 1 of the BEACON topical report:

   "The basic concepts and methodologies used for determining the detector uncertainties and limitations are the same between a BEACON system for a typical Westinghouse plant and a plant that is using SPDs. However, since the basic hardware is different, the actual uncertainties, limitations and restrictions associated with fixed incore detectors are different from the corresponding values associated with the use of incore movable detectors. The prime purpose of the BEACON system is to continuously measure the core peaking factors with high accuracy. In the standard Westinghouse BEACON plant, the incore movable detectors provide periodic (180 EFPD) calibration input to the BEACON System with thermocouple and excore detector readings providing data for continuous power distribution monitoring. The plant specific analysis used to determine the uncertainties in this measurement are described in Section 5 of WCAP-12742-P-A. The fixed incore detector functionality replaces the functionality of the core exit thermocouples, excore detector axial power shape information, and periodic incore movable detector inputs used by the BEACON System continuous monitoring process in Westinghouse design plants. The fixed incore detector uncertainties are analyzed for a specific plant detector configuration using the methodology described in Section 5.0 of Addendum 1 to WCAP-12472-P-A.

   Generally speaking, the more fixed incore detectors are installed, and the higher each detector's measurement accuracy is (smaller measurement variability), the smaller the measured core power peaking factor uncertainty becomes. As described in response to Question 8, the SPD detector design and layout are different for the different NSSS vendors. Furthermore, there are some basic differences in the application of the SPD and moveable detector systems. These include:

   - As plant operation continues, neutron irradiation depletes the detector sensor material and increases the measurement variability. The measurement variability of the incore movable detectors effectively does not change during operation because the movable detector measurements are not present in the core for sufficiently long times to undergo any appreciable depletion of the detector material.

   - Some of the fixed incore detectors may fail during operation, which requires that the power distribution measurement uncertainty be adjusted during plant operation. If an individual incore movable detector fails, the core locations measured by the failed detector can be accessed using one of the other movable detectors, so no uncertainty adjustment is required.

   - If an incore movable detector location access thimble becomes blocked, then the power distribution measurement uncertainty associated with the BEACON calibration data generated from the incore movable detector input is automatically adjusted by the BEACON System. Should the thimble become usable at a later time, BEACON automatically adjusts to this situation. If a FID string cannot be inserted into the thimble during the refueling, the entire string is left out of the core and the uncertainty is adjusted accordingly for the entire cycle.

The BEACON power distribution uncertainty methodology is designed to determining the power peaking factor measurement uncertainty for a wide range of the SPD detector operating conditions. The measure peaking factor uncertainty is defined as a function of the fraction of inoperable detectors and the detector measurement variability as given by Equation 3 and Equation 4 of Addendum 1 to WCAP-12472-P-A. The methodology of the power peaking factor uncertainty determination is described in Section 5 of Addendum 1 to WCAP-12472-P-A.

The constants, variabilities, and coefficients used in the equations described in Section 5 of Addendum 1 to WCAP-12472-P-A are specific for a given reactor core geometry, detector configuration, and installation layout, and can be obtained as described in Section 5. The equations are applicable for a wide range of detector conditions anticipated during the reactor operation.

The behavior of the measured peaking factor uncertainties as a function of the incore detector variability and composite random detector loss levels are shown in Figure 4 and Figure 5 of Addendum 1 to WCAP-12472-P-A for a representative plant. It is seen that the higher the SPD measurement variability and fraction of inoperable detector are, the higher the peaking factor measurement uncertainty becomes.

In most cases, the upper bound of the SPD measurement variability and fraction will be determined for a specified peaking factor measurement uncertainty. Alternatively, the BEACON methodology can be used to support an existing or requested availability requirement for a specific plant."

10. "The CETs are included in the IITA at Unit 2. This means that the Unit 2 CETs are physically located in different areas (radically and axially) than the Unit 1 thermocouples." In other words, this statement points out that a direct comparison of CET readings from Unit 1 and Unit 2 will be of little value. The Unit 2 CETs are located at the top of the active fuel inside the fuel assembly instrument thimble, instead of at the bottom of the upper core plate, so differences in temperature are to be expected between the units. Please note that these differences have been specifically considered in the applicable post-accident monitoring procedures.

12. To clarify, page 129 states that "the WINCISE system shall support two divisions of CET with a minimum of three thermocouples provided in each core quadrant for each division." In other words, there are at least three thermocouples per division per quadrant, or a minimum of six thermocouples per quadrant which exceeds the minimum required by RG 1.97.

13. The IIS software functions are non-safety-related and have no impact on any safety function. Therefore software common mode failure analysis is not required.

15. There are two design changes that impact this system description. The responsible engineers agreed that the WINCISE change package (EDCR 52321) would address everything except the CETs and that the Common Q PAMS change package (EDCR 52351) would address the changes related to the CETS. As previously committed in

TVA letter to NRC dated October 29, 2010 (Reference 4), the final Common Q PAMS EDCR 52351-B excerpts will be submitted within two weeks after the package is issued. Currently the package is scheduled to be issued May 12, 2011.

16. Attachment 4 of TVA letter to NRC dated April 15, 2011, is excerpts from the approved engineering design change package that authorizes a change to the plant (in this case the installation of WINCISE) and provides the detailed basis for the change. It includes the approved document change notices for the impacted documents. Based on prior agreement with the NRC, only excerpts of EDCRs are provided. What is not normally included are the indices, drawing change notices, changes to the Master Equipment List, etc. For this specific item, we included the change paper for the system description and design bases documents as it was felt these were important to the NRC understanding the scope of the change. The Description of Revision for Revision 13 of the design criteria document on Page 115 of the attachment provides the change summary for the document in question. Pages 2 and 3 of the attachment provide the overall change description.

15. NRC Request (Item Number NA)

Provide a non-proprietary description of the Common Q PAMS datastorm test and a summary of the test results.

TVA Response to NRC Request:

Data Storm Test Description

WBN Unit 2 PAMS went through a Data Storm Test to verify that the safety-related functions of the system driven by the Advant Controller 160 (AC160) and the safety-related indications monitored on the Operator Module (OM) located in the Main Control Room (MCR) are not affected when the Ethernet network interface of the Maintenance and Test Panel (MTP) is under data storm conditions. This test was requested by TVA.

The purpose of the data storm test was to test the ability of the MTP to handle the possible volume of traffic generated by a broadcast storm without impacting the safety functions. A broadcast storm occurs when a large number of broadcast packets are received. Forwarding these packets can cause the network to slow down or to time out.

Another objective of the data storm test was to test the ability of the MTP to handle malformed packets possibly generated by a data storm without impacting the safety functions.

The following pass/fail criteria were used to evaluate the success of the data storm test results:

1. During the data storm test, the OM shall continue trending the selected input signal smoothly on the data trend display. The smooth trending was verified by creating a data trend of the point being monitored and comparing it to the data trend observed during the data storm.

2. During the data storm test, the OM shall respond to screen touches (navigation) normally. This was determined by navigating several different screens during the execution of the test.

3. During the data storm, the AC160 user-selectable analog output channel shall generate the analog signal without interruption. The output of the analog channel was captured using a calibrated recording device. A recording of the analog output point being monitored was created before the data storm, and this recording was compared to a recording observed during the data storm.

During the data storm, it was acceptable to have the MTP stop responding because it does not perform a safety function. When this occurred, the following pass/fail criteria were used:

1. The System Trouble Annunciator (digital output from the AC160) to alarm (open contact).

2. The System Trouble Alarm Block on the OM display to indicate alarm (turn to red).

3. The MTP icon on the OM System Health page to indicate alarm or a failure (turn to red or turn to magenta) depending on the type of failure of the MTP.

Test Execution and Test Results

After collecting baseline data, the broadcast storm was applied to the system. While the broadcast storm was in progress the following was observed:

- ➢ The OM was operational throughout the broadcast storm. The trend signal was smooth and all screens were navigational from the directory via touches on the touch screen.

- ➢ The MTP stopped responding for several minutes, and then returned to operational status. While the MTP was inoperable, the system trouble alarm occurred on the OM and annunciator output, and the MTP status was red on the OM. Once the data storm was halted, the MTP began to respond again.

- ➢ The analog output from the AC160 remained operational during the broadcast storm.

The results of the testing determined that the system met the acceptance criteria outlined above.

Enclosure 2
TVA Letter Dated May 6, 2011
Responses to Licensee Open Items to be Resolved for SER Approval

List of Attachments

1. TVA white paper: "Comparison of Regulatory Guide (RG) 1.180, "Guidelines For Evaluating Electromagnetic and Radio-Frequency Interference In Safety-Related Instrumentation and Control Systems," Revision 1 and Tennessee Valley Authority (TVA) Standard Specification (SS) E18.14.01, "Electromagnetic Interference (EMI) Testing Requirements For Electronic Devices," Revision 3, dated April 21, 2011 (Letter Item #1/340)

2. GA-ESI Procedure OP-7.3-240, "Safety-Related Commercial Grade Item Parts Acceptance," Revision I (Letter Item #3/353)

3. TVA Procedure NPG-SPP-12.7, "Computer Software Control," Revision 0, dated December 17, 2010 (Letter Item #5/363)

4. Westinghouse document "WBT DMIMS-DX™ Seismic Evaluation of the Digital Metal Impact Monitoring System (DMIMS-DX™) for Watts Bar Unit 2," EQ-QR-33-WBT, Revision 0 (proprietary) (Letter Item #4/362 [Item 1])

5. Westinghouse non-proprietary white paper WBT-D-2782, "Westinghouse DMIMS-DX In-Containment equipment environmental specifications" (Letter Item #4/362 [Item 1])

6. Evaluation for Common Q PAMS for conformance with RG 1.152 Revision 2 (Letter Item #10/368)

7. Evaluation for how the Common Q PAMS SysRS and SRS implement the design basis requirements of IEEE 603-1991 Clause 4 (Letter Item #12/372)

8. Westinghouse report DAR-ME-09-10, Revision 0, Qualification Summary Report for the WINCISE Cable and Connector Upgrade at Watts Bar Unit 2 (proprietary) (TVA Document Number: 25402-011-V1A-MG00-01949-001-WBT-D-1464) (Letter Item #14/375 [Item 3])

TVA Letter Dated May 6, 2011
Responses to Licensee Open Items to be Resolved for SER Approval

ATTACHMENT 1

TVA white paper: "Comparison of Regulatory Guide (RG) 1.180, "Guidelines For Evaluating Electromagnetic and Radio-Frequency Interference In Safety-Related Instrumentation and Control Systems," Revision 1 and Tennessee Valley Authority (TVA) Standard Specification (SS) E18.14.01, "Electromagnetic Interference (EMI) Testing Requirements For Electronic Devices," Revision 3," dated April 21, 2011 (Letter Item #1/340)

Comparison of
Regulatory Guide (RG) 1.180, "Guidelines For Evaluating Electromagnetic and Radio-Frequency Interference In Safety-Related Instrumentation and Control Systems," Revision 1
and
Tennessee Valley Authority (TVA) Standard Specification (SS) E18.14.01, "Electromagnetic Interference (EMI) Testing Requirements For Electronic Devices," Revision 3
April 21, 2011
Page 1 of 8

- TVA SS E 18.14.01 History and Program Description
  - TVA SS E18.14.01 Revision 0 issued in 1980
  - TVA experience used extensively in Electric Power Research Institute (EPRI®[1]) Topical Report (TR)-102323, "Guidelines for Electromagnetic Interference Testing of Power Plant Equipment"
  - SS E18.14.01Revision 3 updated to reflect EPRI TR-102323 Revision1
  - Nuclear Regulatory Commission (NRC) Safety Evaluation Report (SER) dated April 17, 1996 accepted EPRI TR-102323 Revision 1
  - Test levels conservative to RG 1.180 Revision 1
  - SS allows alternate tests (like RG 1.180 Revision 1)
  - Equipment that requires certification to the SS require reports/testing to be evaluated and approved for the application by the Corporate Electromagnetic Compatibility (EMC) Program Manager
  - SS applied to all electronic equipment - not just digital safety systems
    - Graded approach SS for equipment requirements is shown in sections 1.5 and 1.6
    - Emissions - for all electronic equipment
    - Susceptibility - required for equipment in the RG 1.180 Revision 1 area.
  - Main difference with RG 1.180 - Magnetic Field testing
    - Typically not applicable
    - The location of electronic equipment not in high fields
    - Considered realm of harmonic distortion and not EMI - TVA requires a THD of <5% on sources such as inverters.
    - Testing would be applicable and specified for Cathode Ray Tube (CRT) equipment if installed in magnetic field locations
    - 30 years of evaluating equipment TVA has not seen a failure from the susceptibility testing

[1] EPRI is a registered service mark of the Electric Power Research Institute Incorporated.

Specific comparisons

Emissions SS E18.14.01 Revision 3

- SS 6.7 Radiated Emissions - electromagnetic fields
    - System is required to be configured per the test plan and operable
    - Frequency range is 1 MHz to 1GHz
    - EPRI TR-102323 Figure 7.4 limit is specified
    - Alternate tests are allowed - Industry standard test levels [Federal Communications Commission (FCC), International Special Committee on Radio Interference (CISPR), European Standard (EN)] have more conservative limits over comparable frequency ranges
- SS 6.8 Conducted Emissions
    - The equipment under test (EUT) is required to be configured normally and operable
    - Typically a power line test
    - TVA requires testing on output lines where applicable
    - Frequency range is 10kHz to 400MHz
    - EPRI TR-102323 Figure 7-2 limit is specified
    - Alternate tests are allowed - Military Standard (MIL STD) tests referenced

Emissions RG 1.180 Revision 1

- Radiated Emissions (RE)
    - RE 101 Magnetic Fields 30Hz to 100kHz
    - RE 102 Electric Fields 2 MHz to 1GHz
    - CISPR 11 Electric Field 30MHz to 1GHz
- Conducted Emissions (CE)
    - CE 101 30Hz to 10kHz

    - This frequency range is considered in the power quality distortion requirements of sources and not EMI. The recommendation in EPRI TR-102323 Revision 1 is followed.
    - MIL STD 461F does not require this for Army Ground equipment. The issues for this test relate to ships and aircraft that use the hull/structure for returns
  - CE102 10kHz to 2MHz
    - TVA tests over a greater range and requires testing on output of sources such as DC power supplies
  - CISPR11 150kHz to 30MHz
    - TVA tests require a greater frequency range and requires testing on output of sources such as DC power supplies
  - Alternate or commercial tests
    - The RG as with TVA alternate commercial tests are acceptable when evaluated.

Susceptibility SS E18.14.01 Revision 3

- SS 6.1 Radiated Susceptibility - electric field
  - 10V/meter, 1kHz, 80% sin wave modulated from 10kHz to 1GHz
  - Panel doors are required to be open
  - Alternative tests are allowed - same field strength required
- SS 6.2 Conducted susceptibility - Low frequency
  - 30Hz to 50kHz, 6.3Vrms as calibrated through 50ohm load
  - Typically applied to power input but can be specified on other ports
  - Alternate tests allowed
- SS 6.3 Conducted susceptibility - High Frequency
  - 50kHz to 400MHz, 7Vrms, 1kHz, 80% modulated
  - Required on all cable bundles including power
  - Alternate tests allowed

- SS 6.4 - Surge - High Energy
  - 3kV, asymmetric waveform
  - Power and any conductor / shield that connects to external structures
  - Alternate tests allowed
- SS 6.5 Impulse & Bursts of Impulses (EFT) - Low Energy
  - 3kV, asymmetric wave Power
  - 2kV, asymmetric wave Data/Control
  - Alternate tests allowed
- SS 6.6 Electrostatic Discharge
  - 6kV contact, 8kV air discharge - equivalent to International Electrotechnical Commission (IEC) 61000-4-2 level 3
  - For man-machine interfaces such as switches and push buttons on electronic equipment
  - Alternate tests allowed

<u>Susceptibility RG 1.180 Revision 1</u>

- Radiated Susceptibility
  - RS101 magnetic field
    - 30Hz to 100kHz
    - TVA electronic equipment is not located in areas with strong magnetic fields and per the RG exempted
  - RS103 electric field
    - 30MHz to 1GHz
    - 10V/m per standard
    - This is the same as TVA testing
  - IEC 61000-4-8 - Magnetic Field

        - 50Hz and 60Hz
        - TVA electronic equipment is not located in areas with strong magnetic fields and per the RG exempted
    - IEC 61000-4-9 - Magnetic field
        - 50/60Hz to 50kHz
        - TVA electronic equipment is not located in areas with strong magnetic fields and per the RG exempted
    - IEC 61000-4-10 - Magnetic field
        - 100kHz and 1MHz
        - TVA electronic equipment is not located in areas with strong magnetic fields and per the RG exempted
    - IEC 61000-4-3 - electric field
        - 26Mhz to 1GHz
        - 10V/m per standard
        - This is the same level as TVA testing
- Conducted Susceptibility (CS)
    - Power Leads
        - CS101
            - 30Hz to 150kHz - 136dBµV to 5kHz then decreasing linearly to 106.5dBµV at 150kHz
            - Over the comparable range, TVA testing is equal to or greater than the RG requirements. the range from 50kHz to 150khz is covered by CS - High injection testing
        - CS114
            - 10kHz to 30MHz - 100dBµA from 10kHz to 200kHz then decreasing to 97dBµA from 200kHz to 30MHz
            - TVA test level is 103dBµA from 10kHz to 400MHz enveloping the RG test.

  - IEC 61000-4-6 - 10Vrms into a calibrated 150ohm load
    - TVA test level is 103dBµA from 10kHz to 400MHz enveloping the RG test.
  - IEC 61000-4-13
    - TVA CS-low is equivalent to this test
  - IEC 61000-4-16
    - This test is designed for power harmonics from sources. TVA controls this in the power quality program. Sources such as inverters are required to have a THD <5%. These disturbances are not considered in the EMI program.

- Signal Leads
  - CS114 - 10kHz to 30MHz - 91dBµA
    - TVA testing is at 103dBµA over a wider frequency range
  - CS115 - 2A - impulse
    - This is an alternate test that TVA would accept in lieu of an EFT test
    - The equivalent calibrated voltage level is lower than required by TVA
  - CS116 - 5A - damped sinusoid
    - Damped sinusoidal tests are less intrusive than IEC asymmetric surge wave in both frequency content and energy. Therefore TVA has chosen the IEC surge test. However, on signal and data lines this test is only required on cables that would be subject to this type of surge. Ones that go between structures or go between different ground planes.
  - IEC 61000-4-4 - EFT
    - TVA requires 2kV on signal and data leads. This is the maximum level required by the RG 1.180 Revision 1
  - IEC 61000-4-5 - Surge
    - TVA requires 3kV surge on signal and data lines that connect between external structures and differing ground planes. This is greater than required by RG 1.180 Revision 1
  - IEC 61000-4-6 - conducted radio frequency (RF)

    - This is an alternative test acceptable to TVA

    - TVA requires a higher level test than RG 1.180 Revision 1

- IEC 61000-4-12 - damped sinusoid

    - Damped sinusoidal tests are less intrusive than IEC asymmetric surge wave in both frequency content and energy. Therefore TVA has chosen the IEC surge test. However, on signal and data lines this test is only required on cables that would be subject to this type of surge. Ones that go between structures or go between different ground planes.

- IEC 61000-4-16

    - This test is designed for power harmonics from sources. TVA controls this in the power quality program. Sources such as inverters are required to have a THD <5%. These disturbances are not considered in the EMI program.

Institute of Electrical and Electronic Engineers (IEEE™[2]) C62.41™[3]-1991, "IEEE Recommended Practice for Surge Voltages in Low-Voltage AC Power Circuits"

- The RG discusses various categories for the IEEE surge withstand test. TVA follows the same categories but not the same levels. EPRI TR-102323 Revision 1 defined surge test level of 3kV. This puts the test level between category A and B. This level was approved by the NRC.

- Most equipment will fall in the category A 2kV level. TVA required test levels are typically conservative.

Ring Wave Testing

- TVA does not require ring wave testing. The frequency that a circuit will ring in the plant is determined by the length, resistance, capacitance and inductance due to an impulse generator.

- The IEC surge wave would be such an impulse generator. The IEC pulse has more energy and greater frequency content.

- TVA has determined that the IEC surge impulse test is more severe than the ring wave test.

Radiated susceptibility testing above 1GHz

[2] IEEE is a registered trademark of the Institute of Electrical and Electronics Engineers Incorporated.
[3] C62.41 is a registered trademark of the Institute of Electrical and Electronics Engineers Incorporated.

- TVA does not presently require testing above 1GHz

- Intentional transmitters are approved on a case by case basis. This is for all new frequencies not just above 1GHz.

- This is a legacy issue. Intentional transmitters are evaluated for impact.

- EPRI TR-102323 working group contracted with Wyle labs to show that >1GHz signals are difficult to couple to typical plant equipment. Additionally, the signal loss with distance on cables is high.

- TVA will add a requirement for radiated susceptibility testing above 1GHz in the future.

Conclusion:

TVA meets the intent of the RG 1.180 Revision 1. TVA required tests are typically conservative with the required tests of RG 1.180 Revision 1

TVA has a Corporate EMC Program Manager who reviews and approves vendor test reports to assure that proper testing has been performed on the critical equipment.

All electronic equipment is required to meet emissions standards to assure the susceptibility test envelopes are conservative.

TVA Corporate EMC Program Manager evaluates and approves all intentional radiators on a case by case basis.

TVA's EMC program gives assurance that equipment coming into the plant will perform as needed in the EMC environment that it is subject.

Richard Brehm
Corporate EMC Program Manager
April 21, 2011

TVA Letter Dated May 6, 2011
Responses to Licensee Open Items to be Resolved for SER Approval

ATTACHMENT 2

GA-ESI procedure OP-7.3-240
"Safety-Related Commercial Grade Item Parts Acceptance,"
Revision I (Letter Item #3/353)

BECHTEL POWER CORPORATION	Job Number: 25402

SUPPLIER DOCUMENT REVIEW STATUS

STATUS CODE:

1 ☒ Work may proceed.

1C ☐ Work may proceed. Editorial comments need only be incorporated if revised for other purposes.

2 ☐ Revise and resubmit. Work may proceed subject to incorporation of changes indicated.

3 ☐ Rejected. Revise and resubmit.

4 ☐ Review not required. Work may proceed.

PO 77469 Release 77448

Permission to proceed does not constitute acceptance or approval of design details, calculations, analysis, test methods, or materials developed or selected by the Supplier and does not relieve the Supplier from full compliance with contractual obligations.

Reviewed by	Arch	Civil	CS	Elect	Mech	MET	PD	Constr	Startup	STE
	N/A	N/A	JTT 4/20/11	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Status By: Joe Temples Joe T. Temples

DATE 4/20/11

GENERAL ATOMICS
ELECTRONIC SYSTEMS

OPERATING PROCEDURE	TITLE: SAFETY-RELATED COMMERCIAL GRADE ITEM PARTS ACCEPTANCE			NUMBER: OP-7.3-240
	EFFECTIVE: April 8, 2011		REV: J	Page 1 of 19
RESPONSIBLE DEPARTMENT: RMS ENGINEERING		APPROVED:	DATE: 4/8/2011	

1. SCOPE

This procedure provides the instructions for evaluating commercial grade items (CGI) that have safety related (SR) applications in radiation monitor system (RMS) equipment supplied by General Atomics Electronic Systems Inc. (GA-ESI). A CGI may be furnished as an integral part of RMS equipment at original assembly or as a spare or replacement part for equipment previously assembled and delivered to the customer. This procedure provides the method to determine:

a. whether a part is a CGI;
b. whether a CGI is SR (i.e., SR CGI);
c. whether a SR CGI is fully challenged during equipment assembly and/or testing;
d. whether critical characteristics of a SR CGI must be verified prior to equipment assembly; and
e. whether a SR CGI is equivalent to the item being replaced when sold as a spare or replacement part.

This procedure provides guidelines for establishing verification activities required to assure the SR CGI will successfully perform its intended safety-related function in its qualified assembly.

Verification of an item's critical characteristics is required when dedicating a SR CGI.

2. APPLICABLE DOCUMENTS

IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"

IEEE Std. 344-1975, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"

10CFR50.49, "Environmental Qualification of Electrical Equipment Important to Safety for Nuclear Power Plants"

10CFR21, "Reporting of Defects and Noncompliance"

USNRC Regulatory Guide 1.97 (REV. 3), "Instrumentation For Light Water Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"

ANSI/ASME NQA-1 (1986), "Quality Assurance Program Requirements For Nuclear Power Plants"

OPERATING PROCEDURE	TITLE: SAFETY-RELATED COMMERCIAL GRADE ITEM PARTS ACCEPTANCE		NUMBER: OP-7.3-240
	EFFECTIVE: April 8, 2011	REV: J	Page 2 of 19

EPRI NP-5652 "Guideline For The Utilization Of Commercial Grade Items In Safety Related Applications" (NCIG-07)

NRC Generic Letter 89-02 (March 21, 1989), "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products"

EPRI NP-6406 "Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants" (NCIG-11)

EPRI TR-106439, October 1996, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications"

GA-ESI Procedures:

OP-4.0-130	Engineering Change Orders
OP-4.0-190	Maintenance of RMS Data Base
OP-8.1-110	Processing, Handling and Shipping RMS Spare Parts
OP-8.1-120	Processing Non-Government Customer Furnished Equipment

3. DEFINITIONS

Approved Suppliers List (ASL) - A list of suppliers qualified, controlled and maintained by Product Assurance, that identifies those vendors/suppliers which have an approved Quality Assurance Program applicable to their scope of supply.

Basic Component –

a. A Basic Component means a structure, system, or component, or part thereof that affects its safety function necessary to assure:

1. The integrity of the reactor coolant pressure boundary;

2. The capability to shut down the reactor and maintain it in a safe shutdown condition; or

3. The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to those referred to in paragraphs 50.34 (a)(1), 50.67 (b)(2), or 100.11.

b. Basic Components are items designed and manufactured under a quality assurance program complying with 10CFR50 Appendix B, or CGIs that have successfully completed the dedication process.

Certificate of Conformance (C of C) - A written statement, signed by a qualified party, certifying that items or services conform to specific requirements.

Class 1E - The safety classification of the electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or otherwise are essential in preventing significant release of radioactive material to the environment.

Commercial Grade Item (CGI) –

a. When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, CGI means a structure, system, or component, or part thereof that affects its safety function, that was not designed and manufactured as a basic component. Commercial grade items do not include items where the design and manufacturing process require in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more critical characteristics of the item cannot be verified).

b. When applied to facilities and activities licensed pursuant to 10 CFR Parts 30, 40, 50 (other than nuclear power plants), 60, 61, 63, 70, 71, or 72, CGI means an item that is:

1. Not subject to design or specification requirements that are unique to those facilities or activities;
2. Used in applications other than those facilities or activities; and
3. To be ordered from the manufacturer/supplier on the basis of specifications set forth in the manufacturer's published product description (for example, a catalog).

Commercial Grade Item Engineering Evaluation (CGIEE) – An evaluation form used by ESI engineering to document the verifiable critical characteristics of a SR CGI and to identify end use in customer SR assemblies.

Component - A piece of equipment such as a vessel, piping, pump, valve, or structure which will be combined with other components to form a system.

a. Major Component - That portion of a sub-system whose physical and functional characteristics can be segregated and defined within the overall physical and functional characteristics of that system or sub-system. One or more major components united by some interaction or interdependence comprising a system or sub-system.

b. Subcomponent - That portion of a major component whose physical and functional characteristics can be segregated and defined within the overall physical and functional characteristics of that major component. One or more subcomponents united by some interaction or interdependence comprising a major component.

Conditioning - Any additional work or processing which is imposed on a part which makes it different from nominally similar parts.

Note: Conditioning may include: special calibration, adjustment, tuning, selection testing, "burn-in", heat treatment, machining, and similar processes.

Critical Characteristics (CC) – Those important design, material, and performance characteristics of a CGI that, once verified, will provide reasonable assurance that the item will perform its intended safety function.

Critical Characteristic Acceptance Plan (CCAP) – A form used by GA-ESI Quality Control to document acceptance of SR CGI critical characteristics for a part. A CCAP is implemented based upon a corresponding CGIEE as required for SR CGI material dedication when received or when supplied as a spare or replacement to a customer.

Dedication– Dedication is an acceptance process undertaken to provide reasonable assurance that a CGI to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10CFR50, Appendix B, quality assurance program. This assurance is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery, supplemented as necessary by one or more of the following: commercial grade surveys; product inspections or witness at hold points at the manufacturer's facility, and analysis of historical records for acceptable performance. In all cases, the dedication process must be conducted in accordance with the applicable provisions of 10CFR50, Appendix B. The process is considered complete when the item is designated for use as a basic component.

Equivalency Evaluation - An evaluation performed to confirm that a replacement item, which is not identical to the original item, will satisfactorily perform its intended function once in service. This term is synonymous with "equal-to-or-better-than" evaluation.

Equivalent Item - A replacement item which is not identical to the item that was originally designed and/or installed, but which does not alter the plant's design basis or adversely affect the qualification of the parent equipment and is bounded by the existing design analyses.

Harsh Environments - Environments that may change significantly from the normal expected environment in a sudden or prolonged manner due to the direct effects of a design basis event (i.e. Loss of Coolant Accident [LOCA] or High Energy Line Break [HELB] Accident).

Identical Item – The same part, make and model number, which exhibits the same technical and physical characteristics.

Item - Any level of unit assembly, including structures, systems, subsystems, subassembly, component, part, or material.

Like-for-Like - The replacement of an item with an item that is identical (e.g. replacement in kind).

Mild Environments - An environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated occurrences.

Original Equipment Manufacturer (OEM) - The organization which performed the design, production and fabrication of the original item.

Part - That portion of a major component or subcomponent whose physical characteristics can be segregated and defined within the overall physical characteristics of that major component or subcomponent.

Safety Related - Plant systems, portions of systems, structures, and equipment whose failure or malfunction could cause a release of radio- activity in excess of the criteria specified in 10CFR100. This class also includes equipment that is vital to a safe shutdown of the plant and the removal of decay and sensible heat, or equipment that is necessary to mitigate consequences to the public of a postulated accident. This class includes ASME Code Class 1, 2, and 3 items fabricated, installed, and repaired under ASME Section III or IX and Class 1E Electrical Equipment.

Supplier - Any individual or organization furnishing items or services in accordance with a procurement document. It includes vendor, seller, contractor, subcontractor, manufacturer, and consultant, as well as sub tier levels.

Verification - An act of confirming, substantiating and assuring that an activity or condition has been implemented in accordance with the specified requirements (e.g., a certificate of conformance from an ASL supplier is a verification of compliance with specified requirements. Examinations, inspections and/or tests may be used as verifications).

4. SELECTION OF SR CGI ACCEPTANCE METHODS

Product Assurance Engineering shall use engineering documentation to determine the method(s) to be used for the verification of critical characteristics and acceptance of the part. The following describe the four methods of acceptance and combinations thereof.

a. Method 1- Special Tests and Inspections

This method is used for accepting a CGI by conducting special tests and inspections. The tests and inspections shall be conducted during and after receipt of an item to verify selected critical characteristics. Method 1 shall be used if the technical data are known, test facilities are available, and the items are such that inspection and tests upon receipt are adequate to verify critical characteristics. Method 1 may be used in combination with other acceptance methods.

The critical characteristics shall be verified by a documented plan or checklist. It shall include:

1. Tests and inspections to be performed.
2. Test methods and inspection techniques to be utilized.
3. Acceptance criteria previously derived from the technical evaluation.
4. Documentation requirements for inspection and test results.
5. The sample size to be taken for the verification.
6. Tests and inspections to be performed by facilities determined acceptable by ESI Product Assurance and Engineering.

Once the critical characteristics are verified via special tests and inspections, the part may be accepted. The documentation as a result of the tests and inspections shall become part of the part documentation package that is stored with the purchase order.

b. Method 2- Commercial Grade Survey of Supplier

Method 2 is a means by which the parts may be accepted by taking credit for the commercial quality controls that the supplier may be using. These controls may constitute quality programs, procedures, or practices. Commercial grade surveys can be conducted of suppliers who are original equipment manufacturers, original part manufacturers, or distributors.

A commercial grade survey can be used to accept simple or complex parts. The method is most appropriate for the following.

1. A single supplier of the CGI is being used.
2. Required technical information cannot be obtained from the supplier.

3. A large group of items are repeatedly procured from a supplier for an entire line of components.
4. The CGI is an assembly of many parts.
5. ESI cannot easily verify critical characteristics by inspections or tests.

Where the supplier demonstrates adequate controls, only verification of the part number and the supplier's Certificate of Conformance is required during the standard receipt inspection to complete item acceptance.

Two criteria shall be met when conducting a commercial grade survey. Product Assurance shall confirm that the selected SR CGI's critical characteristics are controlled under the scope of the commercial supplier's quality system activities. Product Assurance shall also be reasonably assured that the commercial supplier's activities adequately control the CGIs supplied. The survey shall be specific to the scope of the particular CGI(s) being purchased.

A CCAP shall be prepared by Product Assurance containing the survey/checklist(s) described above. The plan shall include a list of purchase order requirements necessary for the procurement of the part. Product Assurance shall obtain the necessary information to schedule the verification method(s) in the appropriate time. Purchasing shall be notified of the requirements involving the supplier to allow proper coordination and scheduling.

The results of commercial grade surveys shall be documented in an approved survey plan/checklist that includes:

1. Item or items included within the scope of the survey.
2. Critical characteristics to be controlled by the supplier.
3. Supplier controls to be verified specific to the critical characteristics.
4. Conclusions attesting to the adequacy of the supplier controls.

Once a supplier's controls have been deemed to be adequate, Product Assurance shall invoke or reference the observed commercial or quality controls as a part of the purchase order requirements for the CGI. Care shall be taken not to impose nuclear unique standards on purchase orders for CGIs. Acceptance of the item will be completed by performing a standard receipt inspection with the accompanying supplier's Certificate of Conformance.

c. **Method 3 - Source Verification**

Method 3 involves the verification of critical characteristics by witnessing quality activities before releasing the item for shipment from the supplier. When it is confirmed during a source verification that the supplier adequately controls the critical characteristics, only verification of the part number is required upon receipt. The item is accepted upon completion of the standard receipt inspection and documentation of the source verification results.

The scope of the surveillance may include witnessing fabrication and assembly processes, nondestructive examinations, performance tests, or final inspections. It may also include confirmation of the supplier's design, procurement, calibration, and material control methods employed for the particular CGI being purchased.

The results of the source verification shall be documented in an approved surveillance plan/checklist that includes:

1. Item or items included within the scope of the surveillance.
2. Critical characteristics to be controlled by the supplier.
3. Supplier controls to be verified specific to the critical characteristics.
4. Surveillance methods or verification activities performed with results obtained.
5. Evaluation of the adequacy of the supplier.

The above documentation shall be part of the QA purchase order file and shall constitute objective evidence that control of specific critical characteristics was observed. Acceptance of the item is then completed by standard receipt inspection.

d. <u>Method 4 - Acceptable Supplier/Item Performance Record</u>

This method cannot be used alone for the acceptance of a CGI but may be used in conjunction with one or more other methods to demonstrate a supplier's quality history. Method 4 allows ESI to accept CGIs based upon a confidence in the supplied item achieved through proven performance of the item. It also allows ESI to take credit for item performance based upon historical verification gained from the successful utilization of Methods 1, 2, or 3 or pertinent industry-wide performance data.

Method 4 is best suited for CGIs where results of historical performance can be compiled utilizing:

1. Monitored performance of the item.
2. Industry product tests.
3. National codes and standards (not specific to the nuclear industry)
4. Other industry databases (military, aerospace, etc)

To utilize this method, Product Assurance and/or Engineering shall establish a documented supplier/item performance record using the following sources of information.

1. ESI's historical record. An item's performance record can be determined primarily by monitoring the performance of an item that was purchased from a particular supplier and by monitoring the performance of the parent component in which the part was installed.

2. ESI's historical verification. The successful acceptance of an item using method 1, 2, or 3 over a period of time provides assurance that the supplier has been providing the item specified.

3. Utilization of national codes and standards. When taking credit for an item being manufactured to a national code or standard, Product Assurance shall assure that the item was manufactured in accordance with the code or standard. This assurance can be obtained by:

   (a.) Referencing the national code or standard in the purchase order,
   (b.) Receiving certification from the supplier, or
   (c.) Researching and documenting that it is standard industry practice to manufacture the product to this national code or standard.
   (d.) Verifying manufacturer testing or independent testing with certification.

Product Assurance shall evaluate the supplier/item performance record. The evaluation shall be documented and include the following:

1. Supplier/item being evaluated.
2. Previously established critical characteristics specific to the item or supplier.
3. Identification of utility/industry data examined to evaluate the supplier/item.
4. Basis for determining that industry data substantiates acceptability of the supplier/item.
5. Statement by GA-ESI attesting to the acceptability of the supplier/item.

e. **Combination of Two or More Methods**

The acceptance methods described above may be used in combinations to effectively verify critical characteristics and produce the objective evidence necessary to provide reasonable assurance of acceptability. For complex commercial grade items and commercial grade items for digital safety class systems, method 1 and at least one other method must be utilized. The evaluation of how complex the item is will include identification of such features as the overall architecture, number of functions, inputs and outputs, internal communications among processors or modules, and interfaces with other systems or devices.

f. **Receiving Purchased SR CGI**

1. If the GA-ESI parts/inventory database indicates a CCAP is required at the time a CGI is received, this indicates that critical characteristics are to be verified by QC Receiving and acceptance of the SR CGI shall be in accordance with a CCAP.

2. If a SR CGI does not require a CCAP at receiving, standard QC Receiving inspection methods will be employed.

g. **Storing/Stocking A SR CGI That Requires A CCAP**

1. After an SR CGI requiring a CCAP has been received, inspected and accepted, it may be placed in stock or kitted for an SR assembly.

2. When placed in stock or kitted, a SR CGI requiring a CCAP shall be identified as CCAP accepted to distinguish it from items of the same part number that have not been CCAP accepted.

3. An unverified stocked item requiring a CCAP may be accepted as SR CGI only after it is removed from stock and the critical characteristics have been verified via a CCAP. After verification, it shall be so identified and not be mixed with unverified items of the same part number.

5. PROCEDURE FOR PROJECT ASSEMBLIES

a. **Safety Classification Of Assembly Parts**

GA-ESI has elected to designate all parts incorporated into a SR assembly to be considered SR. This includes all GA-ESI designed and CGI parts, unless separately analyzed and designated otherwise in the assembly's design documents.

b. **Evaluation Of Assembly's Parts For Critical Characteristics Acceptance**

1. Engineering will evaluate each part in an assembly to identify the following:

(a.) The part's SR function(s)
(b.) The part's critical characteristic(s)
(c.) The part's acceptance basis(es) or method(s) of verification

This evaluation will occur at the time of customer order for equipment with SR application and at the time of new design of SR equipment.

2. Engineering will enter the above evaluation information into a Master Evaluation Matrix (MEM) database. Engineering will maintain the database by part number as a basis for review against future customer orders and new designed assemblies.

   Note: The basis for establishing the MEM database will be the Generic Matrix, Form Number SE0206, originally created under GA-ESI Quality Assurance Procedure Number 7-02, Design Control Assurance Of Commercial Grade Items In Nuclear Safety-Related Applications

3. If evaluation determines that critical characteristics be verified at the time SR CGI is received, Engineering will accomplish the following:

   (a.) "Receiving CCAP" will be noted in the MEM database,
   (b.) A CGIEE, listing the characteristics to be verified, will be generated,
   (c.) A copy of the CGIEE will be forwarded to Product Assurance Engineering, and
   (d.) A flag/entry shall be made in the GA-ESI parts/inventory database indicating that a CCAP is required to be implemented when SR CGI is received.

c. **Determination of Critical Characteristics**

A review of the part physically, functionally and materially shall be performed and characteristics identified. These shall be selected on the basis of the environment in which the part is expected to function (Harsh, Mild and seismic). The characteristics which shall be identified are those that are required to meet the safety function of the part that can be verified by one or more of the acceptance methods described in this procedure. The critical characteristics shall be as documented. The responsible engineer shall consult with needed technical interfaces (test, inspection, quality assurance) regarding the critical characteristics to insure that they are measurable and reasonable to perform.

The acceptable value of the critical characteristics shall be determined and documented.

d. **Engineering Review Of Customer Purchase Order For Assembly**

Verify that the purchase order states that the assembly being ordered is SR. If wording within the purchase order leaves doubt, The GA-ESI project manager for the purchase shall contact the customer to verify whether the assembly is to be used for a SR application. If the assembly is SR, proceed with the following steps. If the assembly is not SR, the remainder of this procedure is not applicable.

1. Existing Design

(a.) After customer PO acceptance and prior to commencing assembly, Engineering will compare the assembly parts against the MEM to identify parts not previously entered into the MEM database.

(b.) If a part is listed in the database and part function remains the same, no further engineering effort is required.

(c.) If part performs a different function than the one listed in the database, Engineering will proceed as in procedure step 6.b., above, make an additional entry in the database for the new information, and update the CGIEE as required and forward a copy to Product Assurance Engineering.

2. New Design

After customer PO acceptance and prior to final design review and approval, Engineering will compare the assembly parts against the MEM to identify parts not previously entered into the MEM database. Then proceed as in 6.d.1., above.

e. **Shop Assembly Of SR Equipment For Customer PO**

Prior to assembly, manufacturing staff shall:

1. Verify with Engineering that assembly evaluation of step 6.b. has been performed for assembly in question;

2. Prior to kitting for the given assembly, verify that parts in stock that required CCAP at SR CGI receiving (via parts/inventory database flag) are marked as accepted; and

3. Notify QC Receiving of parts in stock that required CCAP acceptance at receiving but were not so marked.

6. PROCEDURE FOR SPARE AND REPLACEMENT SR CGI

a. SR Determination

Engineering will verify that the purchase order states that the part being ordered is SR. If wording within the purchase order leaves doubt, contact the customer to verify whether the part is SR or to be used in a SR assembly. If the part is SR, proceed with the following steps. If the part is not SR, the remainder of this procedure is not applicable. Annotate goldenrod form accordingly.

b. Determine CGI Status

Verify that the part is not a GA-ESI basic component. If it is an ESI designed and manufactured part, this procedure does not apply. Annotate the goldenrod and process per OP-8.1-110.

c. Determine Dedication Responsibility

Verify the customer PO states or otherwise indicates SR CGI dedication is to be performed by GA-ESI. If the part is not to be dedicated by GA-ESI, the remainder of this procedure is not applicable.

d. Determine If PO Is For Repair

Is the part being returned for repair? If the part is a repair return, the remainder of this procedure is not applicable. Annotate the golden rod and process per OP-8.1-120.

e. Part Changes

Check the part number and description the customer stated in the purchase order to determine whether it is the same as the current part number and description. If there is a difference determine whether the change to the current part from the part that the customer ordered was done by Engineering Change Notice (ECN), if a project specific number is applicable, or by Data Base Change Request (DBCR) or electronic database maintenance (DM) request, if a GA-ESI commercial off the shelf part number.

f. **Previous Dedication Review**

1. Review engineering CGI dedication records to verify if the part has been previously evaluated and dedicated for the customer. If previously done, annotate the golden rod indicating that the part has been previously dedicated.

   Check the purchase order identification of top assemblies and tag numbers and compare them with those previously verified. If they have been previously verified, update the dedication database for the new customer PO and certification of dedication.

2. If the part was previously evaluated and dedicated for a different customer, annotate the goldenrod indicating the part has not been previously dedicated for the customer but does have a dedication plan.

   Note the customer PO and equipment tag numbers to which the part is to be dedicated. The SR part must be identified to a specific ESI nuclear safety-related monitor assembly. Review and identify applicable qualification reports and create a dedication database entry and a CGIEE "Pass Thru" form (SE0159-2A) to document customer tag numbers, applicable qualification test report references, significant comments and notes. This "Pass Thru" form will also be independently verified and approved by Product Assurance.

3. If the part was not previously evaluated and has not been dedicated for any GA-ESI customer, annotate the goldenrod indicating the part has not been previously dedicated for the customer and has no Dedication Plan. Proceed to the next procedure step

g. **Engineering Dedication Documentation**

If the part requires dedication by ESI this will require that ESI maintain its usage for the life of the plant and that defects are reportable in accordance with the requirements of 10CFR21. The qualifying top assemblies, tag numbers and Purchase Order information are documented on the CGIEE forms, and the dedication database is updated.

h. **Technical Evaluation**

1. A technical evaluation shall be made if:

   (a.) the part has not been evaluated before,
   (b.) there are significant changes in the part since the last evaluation or
   (c.) the use of the part differs from that of previous evaluations.

   If the part has been evaluated before and the part number has not changed, no further engineering review is necessary unless the supplier reports changes since the last time the part was evaluated.

2. The evaluation shall include a review of changes and their significance. The evaluation shall be performed as part of the ECN, DBCR or DM process. It may require an equivalency evaluation if the changes are significant. The technical evaluation shall find whether the part is a like-for-like replacement or an alternate replacement.

3. The technical evaluation shall take into account the seismic and environmental qualification of the host. Special emphasis shall be placed on items in harsh environments, such that non-metallic materials are evaluated for safety function. If it is determined that the materials have a safety function, then they shall be tested. Use the Commercial Grade Worksheet form (SE0218) for the evaluation.

4. A part that is not different from the part being replaced or evaluated previously is considered a like-for-like replacement. A like-for-like replacement requires no additional technical evaluation and the next step in this procedure may be taken.

5. If the part has been significantly changed, an equivalency evaluation shall be made. Parts that are equivalent are alternate replacements. If they are not equivalent, an evaluation shall be made to demonstrate the part is an acceptable substitute. Parts that are not acceptable substitutes require additional engineering design. The evaluation shall be documented with an attachment to a DBCR.

i. **Determination of Critical Characteristics**

1. A review of the part physically, functionally and materially shall be performed and characteristics identified. These shall be selected on the basis of the environment in which the part is expected to function (Harsh, Mild and seismic). The characteristics which shall be identified are those that are required to meet the safety function of the part that can be verified by one or more of the acceptance methods described in this procedure.

2. The responsible engineer shall consult with applicable technical interfaces (test, inspection, quality assurance) regarding the critical characteristics to insure that they are measurable and reasonable to perform.

7. ENGINEERING DOCUMENTATION

a. The critical characteristics and their applicable acceptance attributes and/or values shall be documented on a CGIEE Critical Characteristics form, Form No. SE0159-2B. This form shall become part of the engineering package and shall be filed with a database change request (DBCR) form in the document center.

b. The documentation for additional dedications of the same part but for different customers will be documented on CGIEE form, Form SE0159-2A and filed in Quality Assurance records with the QA documentation for the particular customer order.

c. CGIEE form, Form SE0159-2B shall be filed with the corresponding CCAP for SR CGIs requiring acceptance verification at receiving.

8. INDEPENDENT ENGINEERING REVIEW OF CGIEE FORMS

a. When the responsible engineer has completed the CGIEE documentation package, the package shall be independently reviewed by an engineering peer as determined by the Manager of Engineering. The reviewer shall assure that the applicable requirements of this procedure have been met. The independent reviewer will sign the engineering documentation.

b. An additional Product Assurance Engineering review will be conducted to verify that the critical characteristics selected are measurable.

9. 10 CFR 21

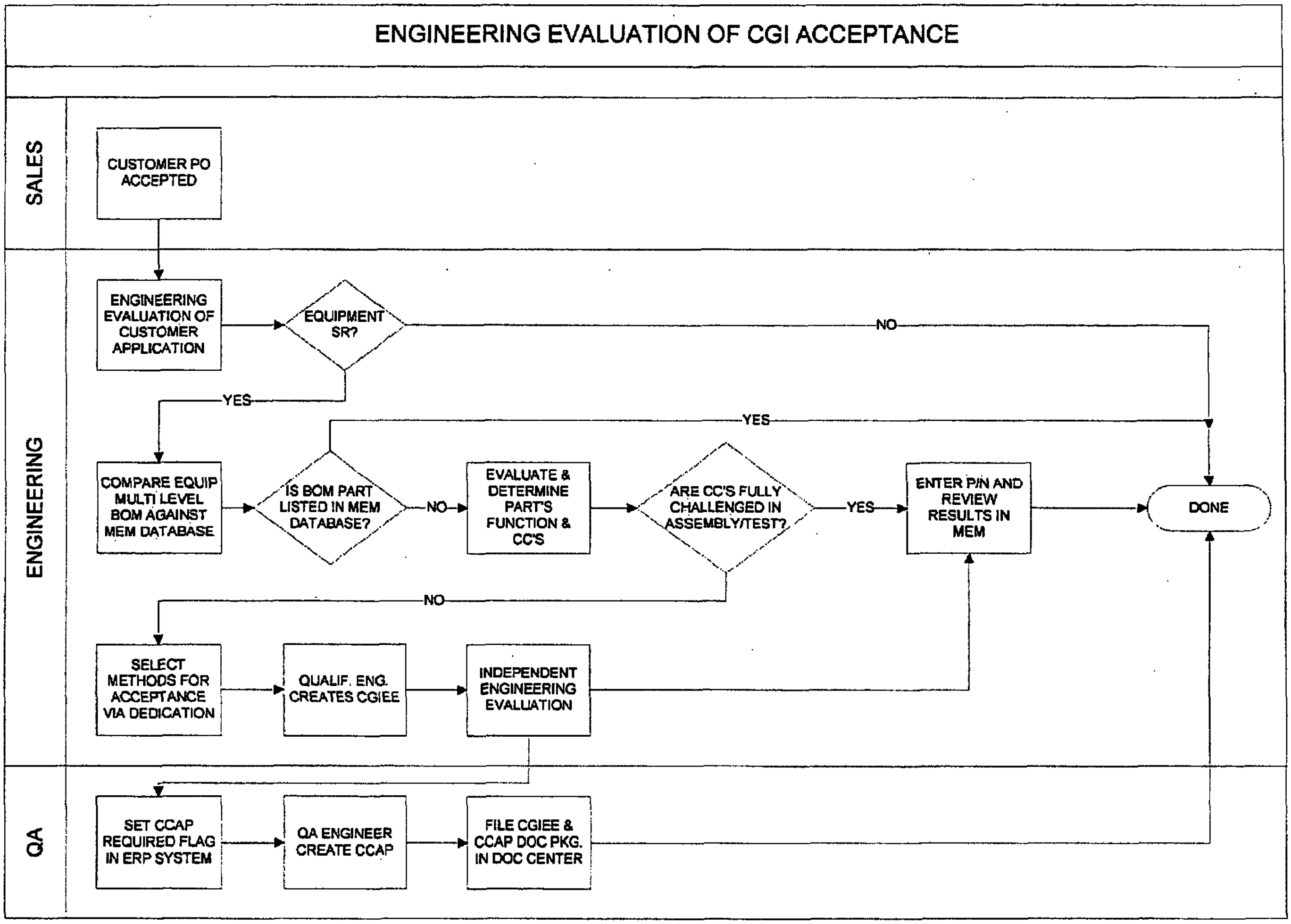
When requested by the customer in the purchase order, ESI will assume responsibility for the 10CFR21 reporting requirements for the part.

10. CERTIFICATIONS

When ESI dedicates a CGI it becomes a SR basic component for use in specific assemblies at the customer's plant. A Certificate of Conformance and a Certificate of Dedication is provided with the shipment. The Certificate of Conformance shall indicate that the item is commercial grade and that the critical characteristics have been verified.

11. FLOWCHARTS

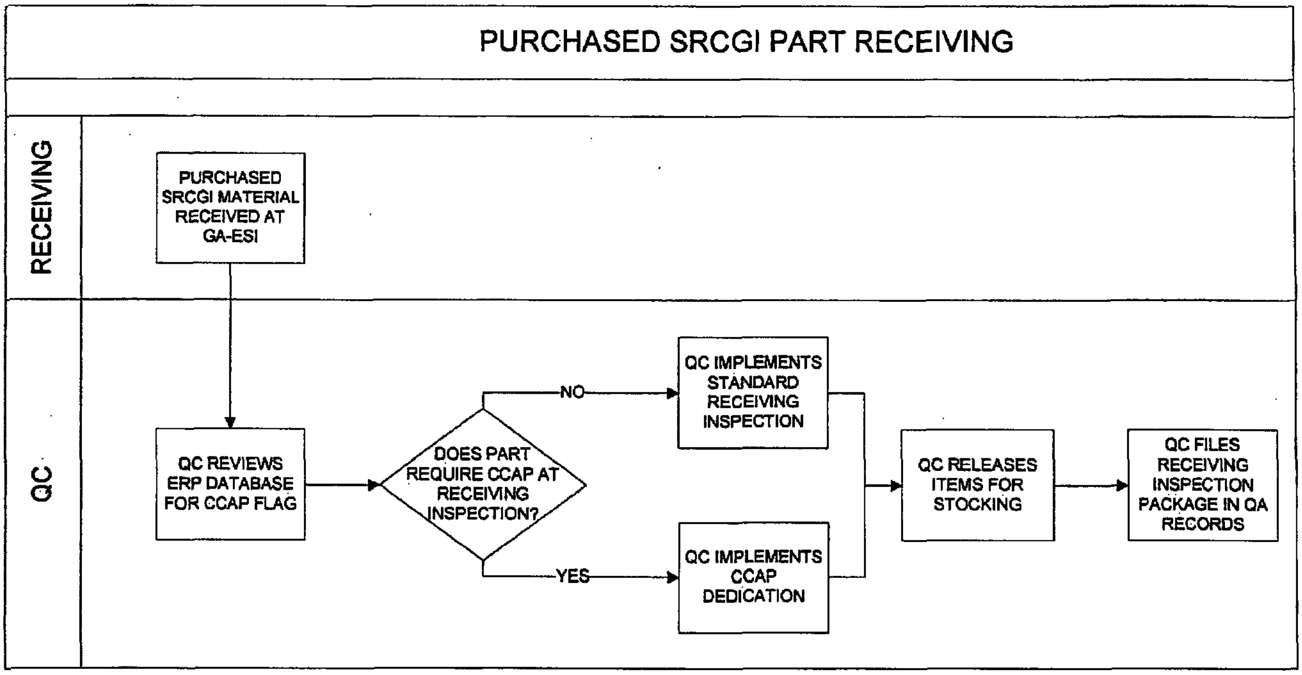
a.


ENGINEERING EVALUATION OF CGI ACCEPTANCE
SALES
ENGINEERING
QA
CUSTOMER PO ACCEPTED
ENGINEERING EVALUATION OF CUSTOMER APPLICATION
EQUIPMENT SR?
NO
YES
YES
COMPARE EQUIP MULTI LEVEL BOM AGAINST MEM DATABASE
IS BOM PART LISTED IN MEM DATABASE?
NO
EVALUATE & DETERMINE PART'S FUNCTION & CC'S
ARE CC'S FULLY CHALLENGED IN ASSEMBLY/TEST?
YES
ENTER P/N AND REVIEW RESULTS IN MEM
DONE
NO
SELECT METHODS FOR ACCEPTANCE VIA DEDICATION
QUALIF. ENG. CREATES CGIEE
INDEPENDENT ENGINEERING EVALUATION
SET CCAP REQUIRED FLAG IN ERP SYSTEM
QA ENGINEER CREATE CCAP
FILE CGIEE & CCAP DOC PKG. IN DOC CENTER

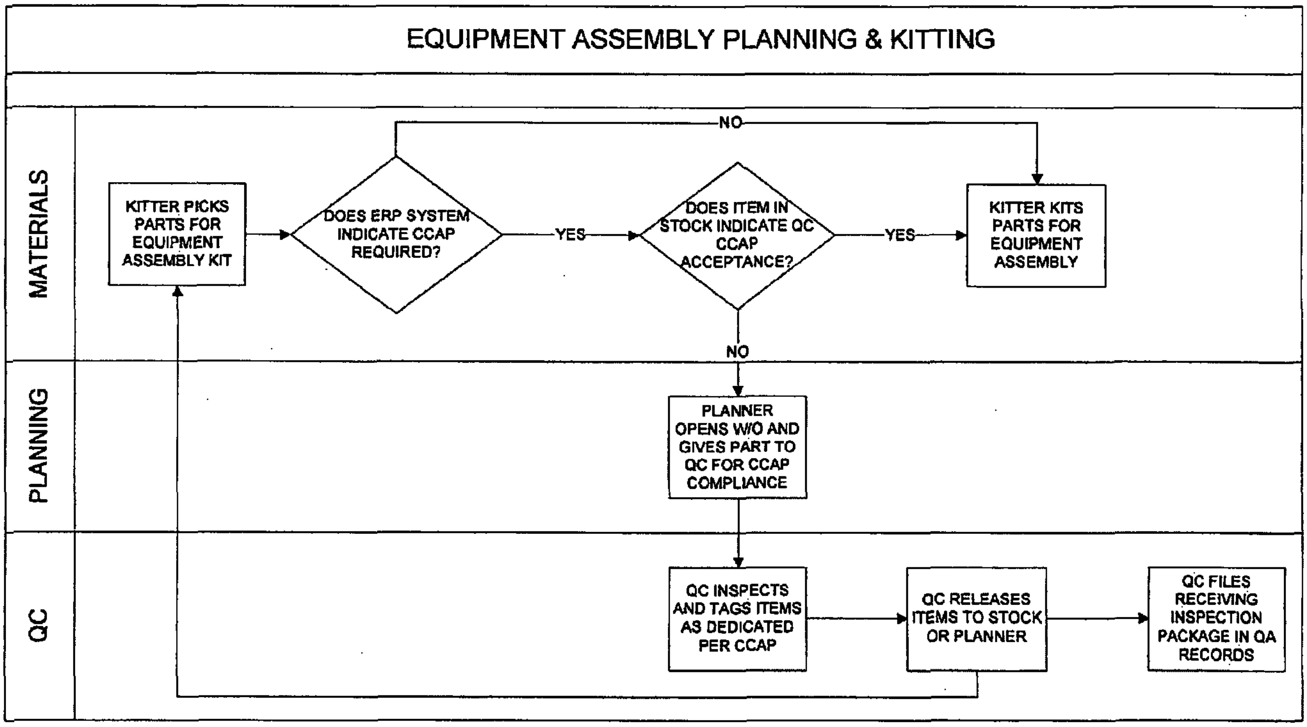
GENERAL ATOMICS
ELECTRONIC SYSTEMS

OPERATING PROCEDURE	TITLE: SAFETY-RELATED COMMERCIAL GRADE ITEM PARTS ACCEPTANCE		NUMBER: OP-7.3-240
	EFFECTIVE: April 8, 2011	REV: J	Page 19 of 19

b.


PURCHASED SRCGI PART RECEIVING
RECEIVING
QC
PURCHASED SRCGI MATERIAL RECEIVED AT GA-ESI
QC REVIEWS ERP DATABASE FOR CCAP FLAG
DOES PART REQUIRE CCAP AT RECEIVING INSPECTION?
NO
YES
QC IMPLEMENTS STANDARD RECEIVING INSPECTION
QC IMPLEMENTS CCAP DEDICATION
QC RELEASES ITEMS FOR STOCKING
QC FILES RECEIVING INSPECTION PACKAGE IN QA RECORDS

c.


EQUIPMENT ASSEMBLY PLANNING & KITTING
MATERIALS
PLANNING
QC
KITTER PICKS PARTS FOR EQUIPMENT ASSEMBLY KIT
DOES ERP SYSTEM INDICATE CCAP REQUIRED?
YES
NO
DOES ITEM IN STOCK INDICATE QC CCAP ACCEPTANCE?
YES
NO
KITTER KITS PARTS FOR EQUIPMENT ASSEMBLY
PLANNER OPENS W/O AND GIVES PART TO QC FOR CCAP COMPLIANCE
QC INSPECTS AND TAGS ITEMS AS DEDICATED PER CCAP
QC RELEASES ITEMS TO STOCK OR PLANNER
QC FILES RECEIVING INSPECTION PACKAGE IN QA RECORDS

TVA Letter Dated May 6, 2011
Responses to Licensee Open Items to be Resolved for SER Approval

ATTACHMENT 3

TVA Procedure NPG-SPP-12.7,
"Computer Software Control,"
Revision 0, dated December 17, 2010 (Letter Item #5/363)

TVA NPG Standard Programs and Processes	TITLE Computer Software Control	NPG-SPP-12.7 Rev. 0000 Page 1 of 56
		Quality Related ☑ Yes ☐ No Effective Date 12-17-2010

Responsible Peer Team/Working Group: Engineering

Approved by: Sam Harvey 8/11/10

Corporate Functional Area Manager Date

Revision Log

Revision or Change Number	Effective Date	Affected Page Numbers	Description of Revision/Change
0	12/17/10	All	Minor/editorial revisions: Due to the conversion of NPG procedures to the new TVA procedure numbering system this procedure replaces SPP-2.6. It also includes the change of "NPG Computer Engineering Group" to "Computer Engineering" and some reformatting due to new procedure format requirements. Added Section 6.0 REFERENCES to incorporate the external Requirements and References document.

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

1.0 PURPOSE

This document describes the quality controls and processes for the development, procurement, modification, and configuration management of computer software used to support the design, operation, modification, and maintenance of TVA's nuclear power plants consistent with the Nuclear Quality Assurance Plan (NQAP).

These controls and processes provide assurance that the computer software within the scope of this procedure performs its intended functions correctly and that the output of the software is correct and can be used without further verification for its intended purpose.

2.0 SCOPE

A. The processes and requirements specified in this SPP apply to all computer application software used in TVA Nuclear Power Group (NPG) with the following exceptions.

1. Computer software integral to devices such as phones, phone systems, radios, beepers, and programmable calculators.

2. Computer software integral to test equipment, test instruments, and lab equipment whose functions can be validated by conventional test methodologies. These methodologies include NPG's measuring and test equipment calibration program or periodic checks against known standards. To meet this exception, the test methodologies must be able to validate all of the device's critical characteristics. If the exception criteria cannot be met, the software must comply with the requirements of this SPP.

3. NPG's nuclear plant simulators. Simulator software is managed in accordance with applicable ANSI standards.

4. System software (computer vendor operating systems and network software) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs.

5. Computer application software that is not owned by NPG and does not meet the criteria for Category B or C software as specified in Appendix A of this SPP.

6. End user software tools, as defined in Section 5.0 of this SPP, TVA "core" applications provided to all TVA employees, and applications available through TVA's InsideNet unless they meet the criteria for Category B or C software as defined in Appendix A of this SPP.

B. Applications utilized internally by contractors performing quality-assured functions for NPG under their own 10 CFR 50 Appendix B Quality Assurance Program shall meet the intent of the requirements of this SPP. Should the contractor deliver computer application software to TVA, then that software is subject to the applicable requirements of this document.

C. This document provides guidance for evaluating the software Quality Assurance Program of suppliers of computer software and software services for inclusion on the NPG Acceptable Suppliers List (ASL).

3.0 INSTRUCTIONS

3.1 Roles and Responsibilities

Application Owner

The individual with administrative and technical responsibility for defining the functional requirements of the computer software. The application owner represents the interests of all users of the application. The application owner is responsible for ensuring software documentation required by NPG-SPP-12.7 has been prepared and approved, and that all required software testing has been completed and that the test results are documented and acceptable. Specific roles and responsibilities of the application owner include the following:

A. Ensuring that the application software is properly classified and documented on the ASD.

B. Ensuring that the application software functional requirements are documented in an SRS. In doing so the application owner represents the interest of the users of the software.

C. Authorizing changes to the application software. All changes to the application software must be approved by the application owner including installation of new releases to previously installed software.

D. Approving software documentation including the software requirements specification, software verification and validation report, software quality assurance and verification and validation plans, if applicable, validation and operability test results, user documentation, and Software Service Requests (SSRs).

E. Ensuring that software documentation is submitted to NPG DCRM for archival within 60 days of the in-service date of the software.

F. Ensuring that purchased application software within the scope of this procedure meets the requirements of this procedure.

G. In conjunction with the software developer; ensuring that software validation and operability test procedures are prepared, and that the test results are documented. Reviews and approves test results.

H. Authorizing installation of validated (tested) application software and software changes.

I. Ensuring that a cyber security assessment has been performed if required.

3.1 Roles and Responsibilities (continued)

NOTE

The application owner ensures that the software documentation listed in the Software Documentation Summary for newly developed/purchased application software in Appendix B is prepared, reviewed, and approved for the new software application. These documents may be prepared by the application owner, application developer, application custodian, or others. However, the application owner must ensure that they have been completed, reviewed, approved, and submitted to Corporate NPG DCRM for archival within 60 days of the in-service (production) date of the software application. Document submittal may be made in hardcopy or as an electronic document and is made using Form NPG-SPP-31.1-2, Document and Record Release Form.

Application Developer

The individual, organization, or vendor responsible for development of a computer software application and associated software documentation and application owner authorized changes to this software. Specific roles and responsibilities of the application developer include the following.

A. Developing and/or modifying the application software as specified by the application owner.

B. Preparing and/or revising software documentation as required by this procedure for application owner approval.

C. Performing and documenting validation and operability testing in conjunction with the application owner.

Application Custodian

The organization, individual, or vendor who ensures the computer software is installed after validation testing has been completed as authorized by the application owner.

A. Ensures that only the validated version of the application software is available for use in the production environment.

B. Ensures software security measures are implemented to prevent unauthorized changes to software.

NPG Point of Contact

Represents NPG's interest in software applications owned by organizations outside NPG, but which are used by NPG in quality-related ways. (Application meets the criteria for Category B or C software.)

A. Ensures NPG's functional requirements are documented in the software documentation.

B. Ensures validation and operability tests are performed and that the results obtained are acceptable. (NPG's functional requirements have been successfully implemented.)

3.1 Roles and Responsibilities (continued)

C. Ensures software changes are documented and tested and that the changes do not adversely affect NPG's use of the application software.

3.2 General Requirements

A. Classification of Computer Software

Computer software is divided into five classifications depending on how the outputs of the application are used. Software classifications are defined in Appendix A of this SPP and may be applied to individual subsystems or subprograms within a particular software application. It is not necessary for all subsystems/subprograms to be classified at the same level. Classifications of component parts of an application must take into account the functions performed by the subsystem/subprogram, their impact on the integrity of the application's outputs, and how the outputs of the software application are used. The classification of computer software is documented on an Application Software Datasheet (ASD), Form 40522 NPG-SPP-12.7-1.

1. An Application Software Datasheet (ASD) shall be completed and submitted to Computer Engineering for review and archival in EDMS for all software applications with the exceptions of end-user software tools as defined in Section 5.0 of this SPP. Classification of the software shall be based on the criteria listed in Appendix A of this SPP.

NOTE

Questions regarding classification of application software should be directed to Computer Engineering.

2. It is the responsibility of the application owner to ensure the computer software is used consistent with its classification. If the manner in which the software is used changes, its classification must be re-evaluated. The ASD must be revised to reflect changes in software classifications.

NOTE

If a software application is reclassified, the controls in effect at the time of its reclassification shall be applied.

3. ASDs are not required for computer application software that is provided to all TVA employees as a TVA "core" application or that is available through TVA's InsideNet unless it meets the criteria for Category B or C software as defined in Appendix A of this SPP.

3.2 General Requirements (continued)

4. ASDs should be updated whenever information on the form changes. This is particularly important for changes in software ownership and changes to software versions.

B. Application software placed in service prior to 7-14-1997 (SPP-2.6 Rev. 0) is required to have software documentation which meets the requirements applicable at the time the software was placed in service. As a minimum, documentation describing the correct use of the software must be available and up-to-date. Retrofitting documentation for these applications is not required. However, the application owner shall ensure that available software documentation has been archived as a record in accordance with Section 4.0 of this SPP. The following sections of this SPP apply to this software.

Requirement	NPG-SPP-12.7 Reference
Changes to Application Software	Section 3.4
Software Validation Testing	Section3.5
Software Operability Testing	Section 3.6
Software Trouble Reporting	Section 3.8
Data Management	Section 3.10
Computer Software Inventory	Section 3.11
Changes to Software Operating Environments	Section 3.12
Software Compatibility Testing	Section 3.13
Retiring Application Software	Section 3.14

C. With the exception of the ASD and any IS required software compatibility testing, Category E software is exempt from all other requirements of this SPP.

3.3 Purchasing or Developing New Application Software or Digital Plant Control Systems/Components

This section of the SPP defines the requirements for purchasing or developing new application software or digital plant control systems/components.

3.3.1 Application Software Datasheet (ASD) - Software Categorization

A. An application owner for the software application or digital control systems to be purchased or developed must be documented on the ASD, Form NPG-SPP-12.7-1. Digital plant components are excluded from this requirement.

NOTE

The application owner for computer software specifically for a particular site is typically an organization at that site. The application owner for computer software used at all sites should be a corporate organization; it is permissible to have joint ownership of a computer application when the software is used at more than one but not all sites.

3.3.1 Application Software Datasheet (ASD) - Software Categorization (continued)

B. The application owner assigns a Software Category to the application software or digital plant control system to be purchased or developed using the Table in Appendix A of this SPP and documents the assigned software category along with the rationale on an Application Software Datasheet, Form NPG-SPP-12.7-1. Categorization of the software must be done before proceeding. End user software tools, as defined in Section 5.0, are Category E by definition and do not require an ASD.

NOTE

Questions regarding classification of application software should be directed to Computer Engineering.

NOTE

Programs/subsystems within an application may be classified individually. If clear distinctions between functions/programs cannot be made or are not practical, then a single classification for the computer application would be appropriate.

C. The Application Owner completes and signs the ASD verifying that the form is complete and the information is correct.

D. The completed ASD is submitted to the Manager, Computer Engineering for review and archival in EDMS. The information is also used by Computer Engineering to update software inventory data.

3.3.2 Purchasing Digital Plant Control Systems/Components

A. Plant digital instrumentation and control systems/components shall be specified, purchased, and implemented, tested, and documented in accordance with Electrical Engineering Standard Specification, SS-E18.15.01 “Software Requirements for Real Time Data Acquisition and Control Computer Systems”. Guidance and useful information on evaluation and acceptance of commercial grade digital equipment in nuclear safety systems may be found in EPRI document TR-106439, “Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications.”

B. System hardening guidelines identified in Appendix I of this SPP must be considered as part of the system implementation.

C. A cyber security assessment is required for purchased plant digital instrumentation and control systems/components. Contact Computer Engineering for assistance in completing the assessment.

NOTE

The remainder of Section 3.3 of this SPP does not apply to digital plant instrumentation and control systems/components purchased and implemented in accordance with Standard Specification, SS-E18.15.01. Plant systems defined to be outside the scope of this specification are purchased or developed in accordance with NPG-SPP-12.7 Section 3.3.3 and 3.3.4, respectively.

3.3.3 Purchasing Computer Software

A. Category E software may be purchased through the IT Online Store and is not subject to further requirements of this section of the SPP. If the IT Online Store does not support procuring the desired category E software, the remainder of this section of the SPP should be followed.

B. When application software is purchased, it shall be procured to the appropriate quality level as noted in the following table. Category A and B application software must be procured from a vendor on NPG's ASL as a qualified supplier of computer software (QA Level 1) or dedicated in accordance with Section 3.7 of this SPP (QA Level 2).

Software Category	Procurement Quality Level
A	1 or 2
B	1, 2, Note 1
C	Note 2
D	0
E	0

NOTE 1

Category B software that is used exclusively for the design, analysis, testing, or acceptance of quality-related and not safety-related plant structures, systems, and components may be procured QA Level 3.

NOTE 2

Software that falls within the scope of NPG-SPP-09.3 shall be procured at the quality level determined by the NPG-SPP-09.3 process. Software used to implement quality related programs listed in section 5.1 of the Nuclear Quality Assurance Plan shall be procured QA level 3. All other category C software shall be procured non-quality.

3.3.3 Purchasing Computer Software (continued)

C. The application owner or designee prepares a procurement request that defines the required deliverables and required vendor activities in accordance with SPP-4.1, "Procurement of Material, Labor, and Services." The request shall state whether or not the application software will be installed as part of a plant system. For applications that are installed as part of a plant system, procurement shall be reviewed by PEG. All other applications will not require a PEG review.

D. Items to be included in the procurement request are noted below:

1. The request shall specify the version and/or versions to be delivered to TVA.
2. Software documentation to be provided.

NOTE

The software documentation that must be available for the completed application software is identified in Appendix B . Any required software documentation not provided by the software vendor must be prepared by TVA or obtained from another source.

NOTE

Documents required by the procurement specification document but considered proprietary by the software supplier must be available to TVA for audit purposes if they are not delivered to TVA.

3. Verification reviews to be performed. The contract should specify the software documentation verification reviews to be performed by the supplier or by TVA.
4. Validation testing required of the software supplier. This includes written validation test procedures and results which demonstrate that the requirements specified in the SRS have been implemented correctly. If features and functionality have been implemented in the software beyond those specified in the SRS, they shall be addressed in the test procedure to demonstrate that they work correctly and that they do not have an unintended impact on the specified requirements. Validation testing required in Section 3.5 must be completed and the results reviewed and approved by the application owner.
5. Contract specifications shall require that changes to the application software be controlled commencing with the software validation test.
6. Any onsite installation support.
7. Training and training materials to be provided.
8. Maintenance support to be provided by the vendor, if any.

3.3.3 Purchasing Computer Software (continued)

9. If TVA does not take delivery of the source code, then consideration should be given to having the software supplier place a copy of the source code in escrow which would be given to TVA in the event the vendor no longer supports the application software.

E. The completed procurement request is processed in accordance with SPP-4.1.

F. A cyber security assessment may be required for the new software application. Contact Computer Engineering for assistance. Assessments are made based on guidance in NEI-04-04, "Cyber Security Program for Power Reactors."

G. Proceed to implement Sections 3.3.5 through 3.3.11 of this SPP.

3.3.4 Developing New Application Software

The following defines the requirements for the development of application software. The extent of the implementation of each requirement is based on the application's classification and its importance to safe and reliable plant operations.

A. Software development shall proceed in a traceable manner. The number of steps in the process and their order depends on the nature and complexity of the software. As such, development may be performed in an iterative or sequential manner.

B. Development of new application software begins with the determination of its classification based on its intended end use. The application owner is responsible for classifying the software and documenting the rationale for its classification. Refer to section 3.3.1 of this SPP.

C. The application owner ensures that the software documentation listed in Appendix B, is prepared, reviewed, and approved for the new software application. These documents may be prepared by the application owner, application developer, application custodian, or others.

Appendix B identifies software documentation by generic document names and provides details on document content. Software documentation may be assigned titles as appropriate to the application. In addition, these documents need not exist as discrete packages but may be combined provided the content requirements are addressed.

D. Additional documentation, as necessary, may be prepared for a given application such as operations and maintenance manuals, system manager's manuals, and training manuals. This documentation shall be reviewed, approved, and issued in a manner similar to the aforementioned documentation.

E. A cyber security assessment is required for purchased plant digital instrumentation and control systems/components. Contact Computer Engineering for assistance in completing the assessment.

3.3.5 Software Documentation

A. The application owner must ensure that all required software documentation has been completed, reviewed, approved, and submitted to Corporate NPG Document Control and Records Management (DCRM) for archival within 60 days of the in-service (production) date of the software application. Document submittal may be made in hardcopy or as an electronic document and is made using Form NPG-SPP-31.1-2, Document and Record Release Form. Software documentation must reflect the "as validated" and installed version of the software.

B. Those documents designated as quality assurance records (refer to Section 4.1) shall be uniquely identified and noted as QA records before they are submitted to Corporate NPG DCRM.

C. Corporate NPG DCRM archives the software documentation. Typically, no controlled hardcopy distribution of the software manuals is made. However, information only copies may be made available as authorized by the application owner. All hardcopy distribution of software documentation is controlled in accordance with NPG-SPP-31.1. For the purposes of this SPP, software documentation excludes plant drawings.

D. Software documentation may be submitted directly to Electronic Document Management System (EDMS) by the software developer provided the documentation is submitted consistent with applicable indexing specifications and with prior approval by the Manager, NPG DCRM.

NOTE

Appendix H contains an NPG-SPP-12.7 to 'Summit' cross-reference of software documentation terminology. Either terminology is acceptable.

3.3.6 Software Interfaces

The application owner shall ensure that the interfaces to other applications are specified, developed, and tested such that the data being used by the application is of the necessary quality. If the data is to be automatically transferred and used without further verification from another application, then the owner is responsible for ensuring that the source applications meet the requirements of this SPP or TVA-SPP-12.5. The owner can establish less automated interfaces that have the appropriate manual checks to ensure the quality of the data being transferred without invoking this SPP. The application owner shall also ensure that configuration control processes are in place to provide notification when changes are made to the source applications and/or interfaces that impact the quality of the transferred data.

3.3.7 Data Migration

If implementation of the application software involves data migration from another application, the requirements of Section 3.10 of this SPP must be addressed.

3.3.8 Software Testing

A. When software development activities are complete, software validation testing shall be performed in accordance with Section 3.5.

B. The validation test procedure and test results are documented in a Software Verification and Validation Report (SVVR).

C. The application owner authorizes software installation after reviewing and approving the validation test results.

> **NOTE**
>
> If the software is to be installed on a standard NPG desktop/laptop computer, then the functional application profile (FAP) must be updated prior to installation of the software and software compatibility testing must be performed by IS.

D. Software operability testing shall be performed in accordance with Section 3.6 of this SPP after it is installed in its production environment but before it is released for use. The operability test and test results are documented in a SVVR.

3.3.9 Software Verification and Validation Report

A Software Verification and Validation Report (SVVR) is prepared to document validation and operability test procedures and test results. (Refer to Appendix F.) It is permissible to include test procedures and results in the SVVR by reference for large test packages.

3.3.10 Software Configuration Control

The TVA application custodian shall store the application's source code and/or executables in a physically secure, environmentally controlled space. The application's source code and/or executables shall be stored in an environment that it is protected from inadvertent changes. Cyber security considerations should be addressed in the storage environment. Cyber security considerations may include protection against source code contamination by malicious codes (viruses, worm Trojans, etc.), protection against code information exploited for malicious intent (i.e., storage area is not connected to a LAN that has internet connectivity), username and password required to access source code, firewall protection to prevent unwanted access, and Intrusion Detection to monitor access.

3.3.11 Installation and Deployment

The process for moving application software from a production to operational environment should include cyber security considerations to ensure it contains no malicious code or software. All applications, binaries, and supporting files transferred from the production to operational environment should include cyber security considerations to ensure they contain no viruses, worms, or other forms of malicious code.

3.4 Changes to Computer Software and Software Integral to Plant Digital Systems/Components

3.4.1 Changes to Software Integral to Plant Digital Systems/Components

A. Software changes purchased or supplied by the equipment vendor shall be implemented, tested, and documented in accordance with Electrical Engineering Standard Specification, SS-E18.15.01 for those systems/components within the scope of that specification.

1. System hardening guidelines identified in Appendix I of this SPP must be considered as part of the change to the plant system/component.

2. A cyber security assessment is required for changes to plant digital instrumentation and control systems/components. Contact Computer Engineering for assistance in completing the assessment.

NOTE

The remainder of this section of this SPP does not apply to software changes supplied by the equipment vendor and implemented under Standard Specification SS-E18.15.01.

B. Changes to the human-machine interface for plant digital systems/components within the scope of SS-E18.15.01 not supplied by the equipment vendor shall be made using the Software Service Request process described in Section 3.4.2 through 3.4.9 of this SPP. In addition, the following items should be addressed:

1. A site impact review shall be performed, documented, and attached to the SSR.

2. A 10 CFR 50.59 evaluation shall be performed and attached to or referenced in the SSR.

3. A human factors review of the proposed change shall be conducted in accordance with NPG-SPP-09.3. The reviewed should be attached to or referenced in the SSR.

C. Software changes for plant systems outside the scope of SS-E18.15.01 shall be made using the software change process defined in Sections 3.4.2 through 3.4.9 of this SPP.

D. Cyber system hardening guidelines identified in Appendix I of this SPP must be considered as part of the software changes in paragraphs B and C above.

E. A cyber security assessment is required for software changes to plant digital instrumentation and control systems/components. Contact Computer Engineering for assistance in completing the assessment.

3.4.2 Changes to Computer Software - Software Service Request (SSR)

A. Changes to application software are documented and controlled using the Software Service Request (SSR). Changes to application software include

1. Those implemented to resolve validation test or operability test deficiencies after the computer software is placed in service,

2. Changes made to add new or enhanced functionality,

3. Vendor supplied software updates, releases, and patches,

4. New versions of software, and

5. Changes to database structure and data files (control code tables) which determine the function of the computer application.

This requirement does not apply to information entered into a database.

B. Changes to application software implemented as part of a change to plant structures, systems, or components which result in changes to Engineering issued system design criteria, the FSAR, or plant technical specifications shall be implemented under the engineering design change process. In these cases, the software change controls defined in NPG-SPP-12.7 guide the development and testing of the computer software. The SSR must be closed prior to the Design Change Notice (DCN) closing and the SSR package must include references to the DCN number.

C. Changes to computer software, control variables, setpoints, and other data constants on digital plant control systems from remote locations are prohibited. Remote locations are defined as any location physically located outside the power plant or not in the same location as the installed control system component.

D. The Software Service Request process applies to Category A, B, C, and D software. SSRs are not required for Category E software.

3.4.3 Initiating A Software Change

A change to application software within the scope of this SPP may be requested by completing Section 1 of the Software Service Request (SSR), Form NPG-SPP-12.7-3, and submitting it to the application owner. An SSR shall be initiated for any of the following:

A. Implementing software changes after the computer software has been placed in service. This includes changes for enhancements, to correct problems, or to resolve outstanding test deficiencies (after the software was placed in service).

B. Installing new releases, new versions, (software updates), patches, or updates of vendor supplied application software.

C. Changes which add or enhance software application functionality.

D. Changes which eliminate software functionality.

3.4.3 Initiating A Software Change (continued)

E. Changes to database structures, files, or software control variables which determine the functions performed by the software.

3.4.4 Software Change Request Approval

The application owner evaluates the request, dispositions the request by completing and signing Section 2 of the SSR form. For applications owned outside of NPG, the application owner forwards a copy of the SSR to the NPG Point of Contact for information. The application owner forwards the approved SSR to the application developer for implementation. Each approved SSR shall be assigned a unique number. Disapproved requests should be returned to the requester along with an explanation for its disapproval.

NOTE

The NPG Point of Contact serves as the NPG "owner" for the software and represents NPG's interest in its functionality and use. See Section 3.1 for Roles and Responsibilities.

3.4.5 Software Implementation

A. The application custodian shall implement controls to prevent unauthorized changes to application software. These controls shall include the following:

1. Prevention of unauthorized or accidental changes to the production (validated) version of the application software.

2. Control of the migration of the software between development/test and production environments.

B. The application developer designs the software change taking into consideration the interfaces with other applications, and modifies the software to implement the approved change.

C. Software changes shall be made to the current, in service version of the software in a nonproduction environment or with the software application in an off-line mode (out of service) unless it is not practical/possible to do so.

D. The application developer evaluates the impact of the software change on the software documentation, updates the software documentation impacted by the change, and notes the results of this evaluation in Section 3 of the SSR. The assessment of software documentation includes the ASD. If the ASD is revised, the form is submitted to the Manager, Computer Engineering for review and archival.

3.4.6 Software Testing

A. When software development activities are complete, validation testing of the software change shall be performed in accordance with Section 3.5 of this SPP. The validation test demonstrates that the modified software correctly implements the requested change.

3.4.6 Software Testing (continued)

B. Following completion of the validation test, Section 4 of the SSR is completed and the validation test and validation test results including any test deficiency reports are attached. It is permissible to reference validation test procedures and results in Section 4 of the SSR rather than attaching them to the SSR.

C. The application owner authorizes software installation only after reviewing and approving the validation test results.

NOTE

If the software is to be installed on a standard NPG desktop/laptop computer, then the functional application profile (FAP) must be updated prior to installation of the software and software compatibility testing must be performed by IS.

D. After installation of the software changes is complete, the application custodian notifies the application owner that the software is ready for operability testing. Operability tests of the software changes shall be performed in accordance with Section 3.6 of this SPP. Operability testing must be complete and results approved by the application owner before the modified software is released for use. A signature on the test documentation denotes approval.

E. The operability test and test results, including any test deficiency reports, are attached to the SSR and Section 5 of this SSR is completed. It is permissible to reference the operability test procedures and results rather than attaching them to the SSR.

3.4.7 Software Service Request Closure

A. The application owner completes Section 6 of the SSR indicating if a cyber security assessment was performed. Contact Computer Engineering for assistance.

B. The application owner completes and signs Section 7 of the SSR releasing the software change for use. If any restrictions are placed on its use, the application owner attaches the restrictions to the SSR or provides a reference for the restrictions and notifies the users of those restrictions.

C. The SSR package includes the following: (1) validation test procedure and test results, and (2) operability test procedure and results or at least references to these documents. Since the operability test may be a site post modification test (PMT), it is permissible to simply reference the PMT or any other post installation test that can be taken credit for as an operability test. If the software change is installed on more than one unit at a site, the SSR package must include the operability test and test results for each unit. If the software change is installed at more than one site, the SSR package must include the operability test and results for each installation unless the software is installed on a standard TVA desktop/laptop computer.

3.4.7 Software Service Request Closure (continued)

NOTE

A SVVR may be prepared for the software change to document the results of software testing. If a SVVR is prepared it should be consistent with requirements of Appendix F and may be attached to or referenced in the SSR.

NOTE

In general, resubmittal of the entire SVVR including revisions is preferred.

D. The application owner is responsible for ensuring that the completed SSR form with any attachments is submitted to Corporate NPG DCRM for archival using transmittal Form NPG-SPP-31.1-2 within 60 days of the in service date of the software change. Revised software documentation is not part of the SSR and is submitted separately to Corporate NPG DCRM for archival in EDMS. |

E. The application owner notifies Corporate NPG DCRM if copies of user documentation are to be distributed and provides the approved distribution.

3.4.8 Software Control Configuration

The TVA application custodian shall store the application's source code and/or executables in a physically secure, environmentally controlled space. The application's source code and/or executables shall be stored in an environment that it is protected from inadvertent changes. Cyber security considerations should be considered in the storage environment. Cyber security considerations may include protection against source code contamination by malicious codes, (viruses, worm Trojans, etc.), protection against code information exploited for malicious intent (i.e., storage area is not connected to a LAN that has internet connectivity), username and password required to access source code, firewall protection to prevent unwanted access, and Intrusion Detection to monitor access.

3.4.9 Installation and Deployment

The process for moving application software from a production to operational environment should include Cyber security considerations to ensure it contains no malicious code or software. All applications, binaries, and supporting files transferred from the production to operational environment should include cyber security considerations to ensure they contain no viruses, worms, or other forms of malicious code.

3.4.10 Emergency Software Changes

Emergency software changes may be made to application software provided the change is approved by the application owner and it is tested prior to use in its production environment. If the change affects plant components or plant operations, notification of the Shift Manager is required before the change is implemented. Within 30 days of installation of the change, a SSR shall be prepared in accordance with the software change control process specified above. In addition, a justification of the emergency change shall be attached to the SSR form.

3.5 Software Validation Testing

The purpose of validation testing is to provide confidence that new or revised applications perform as specified in the SRS or SSR.

A. The application owner ensures that a written validation test procedure that demonstrates that the software requirements specified in an application owner approved software requirements specification (SRS) or Software Service Request (SSR) have been implemented correctly is prepared and executed before the software is installed on the computer on which it will be used. For new Category A software, a traceability matrix shall be prepared that cross references the software functional requirement with the portion/section of the test procedure which tests it. The matrix may be a separate table included in the test report (SVVR), a standalone document which is referenced in the test report, or a cross reference documented in individual steps in the test procedure. To the extent possible, this testing is done off-line or in a non-production environment. If the validation test must be run on the target system, that system shall be declared out of service until the testing is completed. Testing should also consider impact of new software on software already in service and system interfaces.

B. The validation test criteria include the following:

NOTE

Not all of the criteria listed below are applicable to every software application.

1. Functions and features specified in the SRS or SSR work correctly.

2. Software revisions do not adversely affect previously approved and tested functions that were not intended to be within the scope of the change. This criteria may be met by running a test case for the application which demonstrates overall software functionality.

3. Values entered into data control tables to trigger a set of programmatic logic or provide for system functionality have been correctly entered and the output of the logic is correct.

4. Interfaces with software systems/applications with which the application transfers or shares data function properly.

5. Data conversions and migrations are correct. The data sample size included in the test should be commensurate with the magnitude of the data migration. The scope of the test should be commensurate with the complexity of the application.

6. Software responses to abnormal/error conditions.

7. Software response to system loading and expected number of simultaneous users.

8. Software response to other than normally expected sequences of inputs and transactions.

3.5 Software Validation Testing (continued)

9. Software performance at end of period (shift, month, day, year, etc.).

10. Interaction of multiple changes or patches installed at the same time.

C. The application owner approves the validation test procedure.

NOTE

The application owner and application developer/custodian should consider the latest completed validation/functional test, including any test deficiencies, for lessons learned in developing the current validation test plan. The application developer and/or custodian should assist the owner in the development of an adequate validation test, providing input direction, and help as needed.

NOTE

For database applications, the "acceptance" database will be refreshed with a production copy of the data and all database objects. This refresh will be done prior to operability testing. It should be noted that not all software changes require a refresh of the acceptance environment. The refresh will be done at the discretion of the application owner and application custodian based on the magnitude of the software change and the condition of the acceptance environment.

NOTE

Refer to IEEE 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", for additional guidance regarding Category A software validation activities.

D. The validation test procedure is reviewed to ensure that the validation test addresses the items specified in the SRS or SSR. These reviews shall be performed by an independent reviewer for Category A and B software.

E. Prior to initiating software validation testing, the software to be tested shall be placed under configuration control. Once the validation test begins, the software development phase ends and all subsequent changes to the software shall be controlled, including changes necessary to resolve test deficiencies. Software changes are documented on deficiency reports prior to placing the software in service and by software service requests after the software is in use.

F. Validation tests shall be conducted in a non-production environment whenever practical. This environment may include offline development systems, simulators, or systems isolated from the production (in service) system such that the users of the application cannot use the computer software during the test.

G. Validation test results shall be documented. Test deficiencies identified during the validation test as well as their resolution are documented using Form NPG-SPP-12.7-2 or similar document.

3.5 Software Validation Testing (continued)

H. Validation test results, including resolution of test deficiencies, shall be reviewed and approved by the application owner. Approval is denoted by signature on the test documentation. Application owner approval indicates the results are valid and acceptable. In addition, for Category A and B software, the validation test results shall be reviewed by an independent reviewer.

I. Validation test procedure/plan and test results become part of the SVVR for new software applications or the SSR for software changes. Test procedures and results may be included by reference.

3.6 Software Operability Testing

The purpose of operability testing is to ensure that the application has been installed correctly and operates correctly in the production environment.

NOTE

The operability test procedure is run after the software change is installed on the computer system(s) on which it will be used. The purpose for the testing is to verify that the installed software works correctly in its "production" environment. For business process application software, the operability test should address major transactions that may have been affected by the change. For applications run on PCs, an operability test on a representative production system can be used even if the software is installed at multiple sites.

A. The application owner ensures preparation and execution of an operability test procedure which demonstrates that the software performs correctly in its operating environment. This testing is done after software installation on the target system is complete but before the software is released for use. Commencement of the operability testing should be coordinated between the installer of the software and the application owner and users.

B. The operability test procedure should be sufficiently comprehensive to demonstrate (1) that the software installation was correct and (2) that the software is functioning correctly in its operating environment. The operability test procedure may be a plant post modification test, a rerun of the software validation test, or a subset of the validation test depending on the complexity of the software and its interfaces with other systems and equipment. The operability test does not have to be a complete rerun of the software validation test.

C. Operability test results shall be documented, including test deficiencies and their resolution. Operability test deficiencies are documented along with their resolution using Form NPG-SPP-12.7-2 or similar form.

D. Software changes to resolve test deficiencies made prior to placing the software in service are controlled under the test deficiency report. Each software change to resolve test deficiencies must be tested to demonstrate that it resolves the test deficiency.

3.6 Software Operability Testing (continued)

E. Once the software is placed in service (made available for use), all software changes, including those to resolve any remaining (outstanding) test deficiencies, must be controlled in accordance with Section 3.4.

F. The application owner reviews and approves the operability test results after the resolution of any test deficiencies identified during the operability test. Approval is denoted by signature on the test documentation.

G. Operability test procedures and test results become part of the SVVR for new software and the SSR for software changes. Test procedures and results may be included by reference in these documents.

3.7 Software Dedication Process

Category A or B application software procured QA Level 2 must be dedicated as follows unless the software is part of a plant computer system and is dedicated under the DCN process. The application owner is responsible for ensuring that the software dedication is performed when required.

A. A documented evaluation of the industry operating experience with the software being purchased. The review should focus on the same version of the software as much as practical and the software vendor's error reporting process.

B. A documented review of the software vendor's software verification and validation procedure, software development and configuration management procedures, and software error reporting and correction practices. This SPP should be used as guidance for conducting the review.

C. Formal documentation which summarizes the basis for accepting the software for use as a Category A or B computer application. This documentation may be a memorandum or report which summarizes the activities performed and the results which provide the application owner confidence that the computer software is ready for use as a Category A or B application.

D. Software dedication documentation is submitted to Corporate NPG DCRM for archival as a QA record.

E. When new versions of the software are released by the software supplier, installation of the new release is controlled by Section 3.4 of this SPP. The software dedication process is not required for these subsequent releases.

3.8 Software Trouble Reporting

A. Problems identified with computer application software that is part of an in service plant system should be reported directly to the application owner for evaluation. For computer application software that is not part of a plant system, problems should be reported to the Information Technology Customer Center (ITCC) (Help Desk - 751-4357).

B. The ITSC shall report problems with computer application software that they cannot resolve to the application custodian.

3.8 Software Trouble Reporting (continued)

C. The application custodian is responsible for ensuring the reported problem is evaluated for impact to the application software as installed and used.

D. If the software does not perform as specified in the SRS or yields incorrect results, the problem shall be documented and resolved in accordance with NPG's Corrective Action Program.

NOTE

Software changes necessary to resolve a confirmed problem are controlled in accordance with Section 3.4.

E. Error reports received from software suppliers shall be forwarded to the application custodian for screening. The application custodian shall perform the screening and send the results to the application owner within 28 days of receiving the error report. The screening evaluation shall be documented on the "Vendor Software Error Report Evaluation", Form NPG-SPP-12.7-4 and submitted to NPG DCRM for archival in EDMS.

F. If the vendor reported problem is not screened out in Step 3.8E, the application owner shall assess NPG's specific use of the software to determine if the reported error affects the output of the software as used by NPG. If the error does not affect the output, the error report shall be submitted to DCRM as part of the software documentation for the affected application. If the error affects the output, the error shall be documented and resolved in accordance with NPG's Corrective Action Program.

3.9 Software Using Electronic Approvals

Electronic approval is the process where a document or information displayed on a computer display monitor is reviewed, concurred with, and/or approved electronically. This electronic process replaces initials or signature on a hard copy of the document as indication of concurrence or approval. Functional requirements for application software which implement/utilize electronic approvals are contained in NPG Standard Programs and Processes NPG-SPP-31.2, Records Management.

3.10 Data Management

3.10.1 Data Verification Activities

In order for the outputs of Category A-C software to be used without further verification, it is essential that the data used by the software in generating its output be verified and properly managed. It is the responsibility of the application owner to ensure that data verification activities are implemented. Data verification, when required, should be implemented using the following guidelines:

3.10.1 Data Verification Activities (continued)

A. Electronic data may be verified by being compared to a reference source. If large amounts of data need to be verified, statistical sampling of the data is permissible. Should reference sources not be available for verifying the data, the application owner is responsible for documenting the basis for using the unverified data in a process where the output of the quality assured application software will be used without further verification.

B. Electronic data may be transferred from another application (electronic source) in which it has already been verified.

C. Electronic data may be verified electronically through a formal review process including independent checking as appropriate. This type of verification is appropriate for use on electronic documents such as procedures or calculations that are being routed electronically for checking, review, and approval.

D. Data values which are entered into data control tables to trigger a set of programmatic logic or provide for system functionality shall be verified and the logical operation tested within the Verification and Validation process to ensure the data value has been correctly entered and the output of the logic is correct.

3.10.2 Application Software Data Management Requirements

A. For data that has been verified and is being stored within the computer, the software providing the storage environment must ensure that the integrity of the verified data is not compromised either by outside sources or by the computer software providing the storage environment itself.

B. Computer software providing for the transfer of verified data must not compromise the data's integrity while the verified data is being transferred. If the transfer application is performing data conversion, the application software must identify and resolve data which does not successfully pass through the data conversion.

C. Application software that outputs or distributes data must not compromise the integrity of the data while performing that function.

D. Application software generating new data (for example, results of calculations) from verified input data must generate the results correctly.

E. Data shall be protected from unauthorized modifications.

3.11 Computer Application Software Inventory

An inventory of Computer Application Software used in NPG shall be maintained by Computer Engineering. This inventory may be kept in hardcopy form or in an electronic file such as a spreadsheet or database. This inventory contains, as a minimum, the application name, owner, custodian, and software QA classification. Training on the contents and purpose of the inventory is satisfied by training individuals on the requirements of this SPP.

3.12 Changes to Software Operating Environments

NOTE

Whenever system software used by a computer program within the scope of this SPP is upgraded to a major new version, the operating environment under which the computer program was qualified and tested has been changed. Examples include, but are not limited to the following

A. Upgrading computer operating system software.

B. Installing new releases of database management software such as Oracle, or MS Access, etc., which are used by application software within the scope of this procedure.

C. Installing new releases to end-user software tools used by application software within the scope of this procedure, such as Excel, Access, or MathCAD.

A. When changes to the software operating environment have been made (as defined above), an operability test for computer programs (software application) within the scope of this SPP which are to run in the new operating environment is performed. The purpose of this operability test is to verify that the computer program (application software) has not been adversely affected by the change. It is not intended to be a complete rerun of previous application software validation tests.

NOTE

Refer to Section 3.6 for guidance on operability testing.

B. The application developer or custodian evaluates the proposed change to the operating environment and determines the extent of operability testing required to demonstrate that the application software was not adversely affected by the change to the operating environment.

C. The application owner is responsible for ensuring that an operability test, in accordance with the findings of the previous paragraph, is performed and documented before the system software is placed into production. The operability test and test results are documented and submitted to Corporate NPG DCRM for archival using Form NPG-SPP-31.1-2. The Application Owner is responsible for ensuring that identified deficiencies are resolved.

NOTE

The operability test may include (1) rerunning the entire software validation test, (2) running selected test cases or subsets of a previously run validation test, or (3) verifying that the application runs and that data screens/data can be accessed. The extent of the test depends on the nature and scope of the change to the operating environment.

D. In cases where emergency changes to system software must be made, the application owner shall be notified within 24 hours and operability tests conducted and documented within 30 calendar days of the change. The application owner shall identify any required interim control procedures needed until the operability testing is completed and the test results approved.

3.13 Software Compatibility Testing

The purpose of compatibility testing is to provide confidence that new or revised PC-based software does not adversely impact other quality assured software installed on PC desktop computers. It is in addition to software validation and operability testing specified in Sections 3.5 and 3.6. The application owner ensures that appropriate compatibility testing is performed.

A. Software compatibility testing is required for most PC-based software.

Information Services is responsible for making the determination if compatibility testing is required.

B. Information Services determines the appropriate subset of PC-based software applications to be included in the compatibility test and conducts or coordinates the compatibility testing before the new or revised software is installed in its production environment. Information Services works with affected Application Owners and Application Custodians to resolve any identified conflicts.

C. Compatibility testing should be documented to the extent that it identifies when and by whom the test was conducted and the subset of PC-based software included in the test and the test results. Software compatibility testing documentation is the responsibility of Information Services. IS is responsible for submitting this documentation to EDMS.

3.14 Retiring Application Software

Software applications that are no longer needed shall be retired as follows:

A. The Application Software Datasheet (ASD) shall be revised to indicate the software application is retired and the effective date of the retirement. The revised ASD is submitted to Computer Engineering for review and archival to NPG DCRM.

B. The Application Custodian shall remove the application from the production environment and store the source code, executable code, and data files in a physically secure, environmentally controlled space. Code and files shall be protected from unauthorized access and inadvertent use in a production environment.

C. Computer Engineering shall notify the IS FAP Administrator to remove the software from FAPs on which it is listed.

3.15 Plant Control System Boundary Protection Devices

Boundary Protection Devices are used to monitor and control communications at the external boundary of a network to prevent and detect malicious and other unauthorized communications. This section of the SPP applies to firewalls, routers, switches, and network intrusion detection devices managed by NPG.

A. Guideline for configuring Boundary Protection Devices when initially installed.

1. Whenever possible disable, through software or physical disconnection, all unneeded communication ports and removable media drives, or provide engineered barriers.

3.15 Plant Control System Boundary Protection Devices (continued)

2. Examine Boundary Protection Devices for configuration settings such as access control lists, firewall and proxy server settings, inspecting to verify that only authorized network traffic is being allowed through the external boundary interfaces.

3. Firewalls

   a. Provide firewalls and firewall rule sets between network zones.

   b. Provide detailed information on all communications (including protocols) required through a firewall, whether inbound or outbound, and identify each network device initiating a communication.

   c. Provide firewall rule sets or other equivalent documentation. The basis of the rule set shall be "deny all," with exceptions explicitly identified.

4. Network Intrusion Detection Systems (NIDS) provide traffic profiles with expected communication paths, network traffic, and expected utilization boundaries. For signature based NIDSs, provide appropriate signatures.

5. When replacing existing Boundary Protection Devices, if possible, verify that configuration of the new device is the same as the one replaced. If not possible, verify that the configuration is equivalent to the one replaced.

B. Documenting and controlling Boundary Protection Device configurations

1. An Application Software Datasheet (ASD) is not required for a Plant Control System Boundary Protection Device.

2. A Software Service Request (SSR) shall be completed for each Boundary Protection Device when it is initially installed or whenever the configuration of the device is changed. Configuration file(s) shall be obtained from the Plant Control System Boundary Protection Device and attached to the SSR. The configuration file(s) shall be noted in Section 3 of the SSR. No other software documentation is required for Section 3 of the form. For the purposes of completing the SSR, the Boundary Protection Device configuration settings shall be classified Category C on the SSR.

3. A validation test is not applicable or required for the Plant Control System Boundary Protection Device and should be so noted in section 4 of the SSR.

4. An operability test shall be performed on the device once its configuration is finalized. The operability test and test results shall be attached to SSR or included by reference.

3.15 Plant Control System Boundary Protection Devices (continued)

NOTE

The SSR and all related documentation are deemed business sensitive and shall be protected as such according to the Business Practice 29 guidelines. Forward the completed SSR and all attached documentation to Computer Engineering for archival into the EDMS Sensitive Information Vault.

C. Cyber security assessments

A cyber security assessment may be required for Boundary Protection Devices when they are installed or whenever the configuration of the device is changed. Contact Computer Engineering to determine if a cyber security assessment is required. This determination shall be documented in Section 6 of the SSR form. If a cyber security assessment is required, the cyber security assessment shall be performed, completed and submitted to Computer Engineering for review and archival in the EDMS sensitive information vault.

4.0 RECORDS

4.1 QA Records

The following documents are considered QA records for software classified as Category A, B, or C software.

A. Software Requirement Specification

B. Validation and Operability Test Procedures and Results

C. Software Verification and Validation Report

D. Software Service Requests (TVA Form NPG-SPP-12.7-3)

E. Software Quality Assurance Plan (SQAPs)

F. Software Verification and Validation Plan (SVVPs)

G. Documentation of reviews prepared as part of the software dedication process in Section 3.7.

H. Application Software Datasheet (NPG-SPP-12.7-1)

I. Software Verification and Validation Deficiency Form (NPG-SPP-12.7-2)

J. Vendor Software Error Report Evaluation (NPG-SPP-12.7-4)

4.2 Non-QA Records

A. Software documentation not specifically identified in Section 4.1 of this SPP, including Software Design Descriptions, User Documentation, and Maintenance Manuals.

B. Documentation associated with end-user tools or system software as defined in Section 5.0.

C. Software change requests that are not implemented in the production version of the application software.

D. All Category D and E software documentation.

5.0 DEFINITIONS

Application Custodian - The organization or individual who has responsibility for the information technology implementation of a computer software application or software changes.

Application Developer - The individual, organization, or vendor responsible for development of a computer software application and associated software documentation including changes to the software. The application developer develops and tests the computer software.

Application Owner - Individual with administrative and technical responsibility for defining the functional requirements of the computer software. The application owner represents the interests of all users of the application, authorizes changes to the software, and approves software documentation.

Application Software - A logically-related group of computer programs used by the end-user to perform specific and defined functions.

Business Process Application Software - Computer software used to enable critical NPG business processes. Examples include software used to enable the work management, document management, radiation exposure tracking, master equipment list, bill of materials, and equipment clearance control processes.

Commercially Available Software - Software which is procured and used without modification.

Database (Data) - Data collected and managed through a software system (including commercially available software packages); accessed through a computer (including personal computer, minicomputer, or mainframe computer); and used to calculate a result or satisfy a set of information or process requirements.

Data Dictionary - A dictionary that defines the meaning of all the data represented on the data flow. The definitions include **NOT** only the English definitions, but also describes the detailed sub-data elements that comprise the data that are registered on the data flow.

Emergency Software Change - A change made to application software to prevent compromising plant safety systems or safe plant operations whose delays could result in a degradation of plant or personnel safety or result in a reduction of electrical generation.

5.0 DEFINITIONS (continued)

End-User Software Tools - Commercially available software designed to support the development and operation of end-user applications. It includes database programs, spreadsheet programs, report generators, CAD/CAM programs, desktop publishing, word processing programs, graphics programs, terminal emulators, communications programs (i.e., Telnet, FTP, etc.), office equipment device drivers (printers, scanners, etc.), Mathcad or similar programs, Project Management, handbooks, and catalogs. These applications are Category E and do not require an Application Software Data Sheet.

FAP Administrators - Information Services' employees that update and maintain FAPs. The FAP Administrator is available at e-mail address "FAP - Administrator."

Functional Application Profiles (FAPs) - A FAP is a logical grouping of applications associated with performing a specified business function that is managed by a business peer team. FAPs define the appropriate applications an employee is authorized to use in the performance of their job.

Independent Review - A review of software documentation or test procedures and results by an individual other than those who prepared the document, but who may be from the same organization.

NPG Point of Contact - The designated individual responsible for representing NPG's interest in software applications owned by organizations outside NPG, but which are used by NPG in quality-related ways.

Off-the-Shelf Software - Off-the-shelf software is computer software procured and used without modification of any kind. Same as commercially available software.

Operability Tests - A test of a computer program which demonstrates that the validated computer software including changes to the software, performs properly after it is installed in its operating environment.

Plant Systems - A permanent plant system is one that implements an engineering design requirement and is included on an engineering issued drawing.

Software - Computer programs, procedures, rules and data pertaining to the operation of a computer system independent of the media on which it resides (tape, disk, eprom, prom, etc.).

Software Categories - A categorization of software based upon usage of the software that determines the level of software quality assurance that will be applied to the acquisition, development, enhancement, or maintenance of the software.

Software Dedication - An acceptable process undertaken to provide reasonable assurance that computer software from vendors not on the NPG Acceptable Suppliers List will perform its intended function and in this respect is deemed equivalent to computer software developed under a 10CFR50 Appendix B QA program.

Software Modification - Changes to previously validated computer software (1) to eliminate defects, (2) to enhance existing functions/features, or (3) to implement new functions/features in the application software.

5.0 DEFINITIONS (continued)

Software Operating Environment - Those elements of the system hardware and system software which are required for or may affect the successful functioning of the application software which operates in that environment.

Software Quality Assurance Plan (SQAP) - A plan for the development and maintenance of computer software necessary to provide adequate confidence that the software conforms to established requirements. This SPP serves as the software quality assurance plan for all application software within the scope of this procedure except for Category A software.

Software Validation - The test and evaluation of the completed software to ensure compliance with software requirements.

Software Verification - The process of determining whether or not the product of a given phase of the software development cycle fulfills the requirements imposed by the previous phase.

Software Verification and Validation Plan (SVVP) - A document describing the verification (review) and validation (test) activities to be performed. This SPP serves as the SVVP for all application software within the scope of this procedure except for Category A software.

Software Verification and Validation Report (SVVR) - A document containing the results of completed verification and validation activities and identifying any constraints or restrictions placed on the use of the computer software.

Software Design Description (SDD) - A document which provides a technical description of how the computer software design satisfies/addresses the functional requirements specified in the software requirements specification.

Software Requirements Specification (SRS) - A document which defines the requirements the software must satisfy.

System Software - Software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs.

System Version - The numerical designation of a particular version of a computer software system. For new software systems it shall be the integer "1." Existing software systems will maintain their current version until they are modified. Major revisions (e.g., incorporation of significant requirements changes or expansions to the software scope) are identified by incrementing the version to the next highest integer.

User Documentation (User Manual) - An organized compilation of information which explains the use of the application software and/or computer software system.

Validation Test - A test of the completed application software performed before the software is installed in its production environment which demonstrates that the specified requirements have been implemented correctly. If additional features/functions have been implemented in the software and will be used, they must be tested to demonstrate that they work correctly and do not have an unintended impact on the specified requirements.

6.0 REFERENCES

6.1 Source Documents

6.1.1 Business Requirements

None

6.1.2 Requirements Documents

Nuclear Quality Assurance Plan

6.2 Developmental References

ASME NQA2 Part 2.7, “Quality Assurance Requirements of Computer Software for Nuclear Facility Applications”

NUREG/CR-4640, “Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry”

Appendix A
(Page 1 of 1)

Application Software Categories

APPLICATION SOFTWARE CATEGORIES	
Category	Description
A	Application software which is an integral part of a safety-related plant system or component and is essential to the performance of the safety-related function. These systems have direct, active effect on the operation of Class 1E plant systems.
B	Application Software which performs calculations used without further verification for the design and analysis of safety- or quality-related structures, systems, or components or to establish the design basis as described in the final safety analysis report. Application software used without further verification for the design of reactor core loads. Software or portions of software which perform calculations used without further verification to verify compliance with plant technical specifications or nuclear regulatory requirements. Software which performs calculations used without further verification for testing and/or acceptance of safety-related or quality-related plant structures, systems, or components.
C	Software and data which are an integral part of a quality-related but not safety-related plant system or component and are essential to the performance of that function. Software, portions of software, and data essential to the implementation of quality-related programs listed in Section 5.1.B of the Nuclear Quality Assurance Plan, including software used to implement regulatory physical security requirements. Software and data which implements NQAP requirements but not specifically identified as an augmented quality-related program as defined in Section 5.1.B of the NQAP. Software, not associated with a specific plant system, which stores, maintains, controls, distributes or manages data which can be used without further verification in activities which affect safety- or quality- related plant structures, systems, and components. Software, portions of software, and data which are an integral part of a nonsafety-related, non-quality related plant system or component whose failure would significantly impact plant operations. Software used in the design of nonquality-related, nonsafety-related plant structures, systems, and components.
D	Computer software used to enable critical NPG business processes or software not meeting the criteria for Category A-C software. These are considered business process application software.
E	Other application software not meeting any of the criteria identified for Category A, B, C, or D software. Category E includes end user software tools.

Appendix B
(Page 1 of 2)

Software Documentation Summary

	Category						NPG-SPP-12.7
Software Documentation	A	B	C	D	E	Approved By:	Reference
ASD (See note below)	X	X	X	X	X	Application Owner	Form NPG-SPP-12.7-1
Software Quality Assurance Plan (SQAP)	X	O	NR	NR	NR	Application Owner	Appendix C
Software Verification and Validation Plan (SVVP)	X	O	NR	NR	NR	Application Owner	Appendix C
Software Requirements Specification (SRS)	X	X	X	X	NR	Application Owner	Appendix D
Software Design Description (SDD)	X	X	O	NR	NR	Application Developer	Appendix E
Software Verification and Validation Report (SVVR)	X	X	X	X	NR	Application Owner	Appendix F
• Traceability Matrix	X	NR	NR	NR	NR	Application Owner	Section 3.5
• Validation Test Procedure (Part of SVVR)	X	X	X	X	NR	Application Owner	Section 3.5
• Validation Test Results (Part of SVVR)	X	X	X	X	NR	Application Owner	Section 3.5
• Operability Test Procedure (Part of SVVR)	X	X	X	X	NR	Application Owner	Section 3.6
• Operability Test Results (Part of SVVR)	X	X	X	X	NR	Application Owner	Section 3.6
Software Dedication Documentation	X	X	NR	NR	NR	Application Owner	Section 3.7
User Documentation	X	X	X	X	O	Application Owner	Appendix G
Software Service Requests (SSR)	X	X	X	X	NR	Application Owner	Section 3.4

X = Required O = Optional (Discretionary) NR=Not Required

NOTE

All software applications used in NPG are required to have an Application Software Datasheet (ASD) with the exception of end user software tools as defined in Section 5.0 of this SPP and TVA core applications provided to all TVA employees.

NOTE

For applications requiring a software design description (SDD), the SDD may be combined with the SRS into a single document which meets the requirements of both.

Appendix B
(Page 2 of 2)

Software Documentation Summary

NOTE

A SQAP and SVVP is required for Category A software. Appendix C of this SPP provides guidance for contents of these documents. For Category B software, this SPP may serve as the SQAP and SVVP, since it defines the standard processes for managing the development and configuration control of computer software. If requirements unique to a computer application are not adequately addressed by this SPP, a SQAP and SVVP may be developed to address these requirements and/or provide supplemental guidance. However, these documents may not supersede the requirements set forth in this SPP.

NOTE

Software Dedication Documentation is only required for Category A or B software purchased from a vendor not on the Nuclear Assurance maintained NPG Acceptable Suppliers List for software products.

NOTE

If the user documentation is incorporated in the software application as an online help feature, it is controlled as part of the application and is excluded from the user documentation requirements above.

NOTE

For applications that were placed in service prior 7-14/1997 (SPP-2.6 Rev. 0), the backfit of documentation (i.e., SRS, SDD, Initial SVVP) to what is specified in this appendix is not required. The backfit of documentation is also not required for applications that are category E applications as established on 3/31/2003 (SPP-2.6 Rev.8) and were in use on 3/31/2003. However, all changes to the software implemented after 7-14/1997 (SPP-2.6 Rev. 0) must be tested and documented in accordance with the procedure revision in effect at the time the software change is made.

Appendix C
(Page 1 of 2)

Guidelines For SQAPs and SVVPs

1.0 GUIDELINES FOR SQAPS

A software quality assurance plan is required for Category A software. The SQAP should address the following:

A. The software to which the SQAP applies.

B. Roles and responsibilities of those individuals/organizations performing tasks within the scope of the SQAP.

C. Required documentation.

D. Software verification and validation activities for the development and/or maintenance of the software.

E. Software configuration management and change control.

F. Code and Media Control.

G. Problem and error reporting.

H. Supplier Control.

I. Records Collection, Maintenance, and Retention

2.0 GUIDELINES FOR SVVPS

A Software Verification and Validation Plan (SVVP) is required for Category A software. The SVVP should address the following:

A. Software to which the SVVP applies.

B. Roles and responsibilities of those individuals/organizations performing tasks within the scope of the SVVP.

C. A description of the tasks for accomplishing the verification activities for application software development and/or maintenance/modification.

1. A system requirements review to determine if the requirements are correct, complete, consistent and testable.

2. A design review to demonstrate that the stated system requirements are satisfied in the system design.

3. A review of the overall structure of the computer code to verify that the design has been implemented.

4. Verification that the system users manual reflects the proper use of the software and that specified functions are addressed.

Appendix C
(Page 2 of 2)

Guidelines For SQAPs and SVVPs

2.0 GUIDELINES FOR SVVPS (continued)

5. Verification that validation test procedures test system requirements. This includes a traceability matrix for Category A software.

D. A description of software validation activities which demonstrate that the completed software performs its intended functions correctly and has been properly integrated with system hardware.

E. Method for documenting and resolving discrepancies identified during verification and validation activities.

F. Method for documenting the results of the verification and validation activities.

NOTE

IEEE STD 7-4.3.2 may provide guidance for specifying verification and validation requirements for Category A software to ensure appropriate integration of computer system hardware and software.

Appendix D
(Page 1 of 2)

Guidelines For Software Requirements Specifications (SRS)

1.0 REQUIREMENT SPECIFICATIONS

A. The application owner ensures the Software Requirements Specification (SRS) is prepared to document the functions and requirements the computer software must satisfy. Requirements should be specified so that their achievement can be verified and validated. The SRS is required for Category A through D software. The following provides guidance for preparation of the SRS.

1. Title Page

   The SRS should be identified by a title page that contains the following as a minimum:

   a. The words "Software Requirements Specification".

   b. The SRS revision number.

   c. The software name, acronym and release version (if applicable). The name and acronym must match those documented on the Application Software Datasheet (ASD).

   d. The computing system identification, if applicable.

   e. The name and dated signature of the preparer(s) (authors).

   f. The name and dated signature of the SRS reviewer(s).

   g. The name and dated signature of the application owner.

2. Revision Log

3. Functions to be Performed by the Software

4. Calculations, algorithms, or logical operations (if any)

5. Software performance acceptance criteria (for example, response time)

6. Responses to valid and invalid inputs

7. Responses to abnormal situations

8. Data input/output requirements

9. Interfaces/communications with other systems or databases at the application software level

10. User interface

11. Security/access restraints or controls

Appendix D
(Page 2 of 2)

Guidelines For Software Requirements Specifications (SRS)

1.0 REQUIREMENT SPECIFICATIONS (continued)

12. Regulatory requirements, if any, the software is intended to satisfy (implement)

13. Design constraints/restrictions which must be considered

NOTE

It is recommended that the SRS be developed with input/assistance from the application developer or custodian.

NOTE

For Category A software, IEEE STD 7-4.3.2 provides additional guidance for developing and specifying system requirements.

B. The SRS is reviewed for (1) completeness, (2) verifiability, (3) technical feasibility, and (4) consistency by a technically competent individual other than the one that prepared the document. The individual, however, may be from the same organization.

NOTE

A new application software implemented as part of a change to plant structures, systems, or components or which result in changes to Engineering issued system design criteria, the FSAR, or plant technical specifications is implemented under the engineering design change process. In these cases, Section 3.3 of NPG-SPP-12.7 guides the development and testing of the computer software.

C. Approval of the SRS is not a prerequisite for software development activities to proceed. However, it must be recognized that software design and coding activities started before final approval of the SRS could be significantly impacted by changes to the SRS during the review and approval process.

Appendix E
(Page 1 of 2)

Guidelines For Software Design Descriptions (SDD)

1.0 SOFTWARE DESIGN DESCRIPTION (SDD)

A. A software design description (SDD) is prepared to provide a technical description of how the software and/or data base design satisfies the requirements in the SRS. Typically the SDD is prepared by the application developer. The SDD is required for Category A and B software.

Differences between the SDD, SRS and actual available (or practically achievable) software should be resolved by referring to the SRS and revising, if necessary, the SRS. Ultimately the SDD, SRS, and software must agree.

The following provides guidance for the preparation of the SDD. Typical topics to be addressed in the SDD are noted below. The scope of the SDD is determined by the scope and complexity of the software requirements:

1. Title Page

   The SDD will be identified by a title page that contains:

   a. The words "Software Design Description".

   b. The SDD revision number.

   c. The software name, acronym and/or release version (if applicable). The name and acronym must match those documented on the Application Software Datasheet (ASD).

   d. The SDD author(s) name and dated signature.

   e. The name and dated signature of the reviewer(s).

   f. The name and dated signature of the application developer.

2. Revision Log

3. Overall structure of software including major components

4. Technical description of models, algorithms, calculations, and logical operations

5. Description of data and file structure

6. Description of global control structure

7. Description of control and data flow

8. Description of software modules describing their inputs and outputs

9. Design constraints limitations

Appendix E
(Page 2 of 2)

Guidelines For Software Design Descriptions (SDD)

1.0 SOFTWARE DESIGN DESCRIPTION (SDD) (continued)

10. Design assumptions

11. Description of security provisions

NOTE

For Category A software IEEE STD 7-4.3.2 may provide additional guidance for preparation of software design documentation.

B. The SDD is reviewed for (1) technical adequacy, (2) completeness, (3) consistency, and (4) verification that all requirements in the SRS are addressed in the software design. The reviews may include logic, screen designs, data field lists, etc., for which specific application requirements exist. The review is performed by an individual other than the one that prepared the document. The individual, however, may be from the same organization.

C. The finalized SDD, including changes made to resolve reviewer comments, is approved by the application developer.

Appendix F
(Page 1 of 2)

Guidelines For Software Verification And Validation Report (SVVR)

1.0 GUIDELINES FOR SOFTWARE VERIFICATION AND VALIDATION REPORT (SVVR)

A. The application owner ensures that the results of validation and operability testing are documented in a SVVR.

The SVVR has the following characteristics:

1. Reports the results of the verification and validation activities required by NPG-SPP-12.7.

2. Includes objective data and test results, wherever possible.

3. Documents test results that demonstrate the software performs as anticipated over the entire range of predicted use including indication as to whether the product passed or failed specified test criteria.

B. A typical SVVR should include the following:

1. Title page

   a. The word “Software Verification and Validation Report”.

   b. The SVVR revision number.

   c. The software name, acronym and version number (if applicable). The name and acronym must match those documented on the Application Software Datasheet (ASD).

   d. The author’s name and dated signature.

   e. The reviewer(s) name and dated signature.

   f. The application owner’s name and dated signature.

2. Validation test procedure and test results.

3. Validation test deficiency reports.

4. Operability test procedure(s) and results.

5. Operability test deficiency reports.

6. Statement certifying (declaring) the software is ready for use along with identification of any restrictions placed on the use of the software.

Appendix F
(Page 2 of 2)

Guidelines For Software Verification And Validation Report (SVVR)

1.0 GUIDELINES FOR SOFTWARE VERIFICATION AND VALIDATION REPORT (SVVR) (continued)

NOTE

Reference to test procedures which can be retrieved through Records Management or Design Change Packages is an acceptable alternative to attaching test procedure packages to the SVVR.

Appendix G
(Page 1 of 1)

Guidelines For User Documentation

NOTE

The user documentation may be an online help feature of the application, an electronic desktop procedure, an approved hardcopy procedure, or a hardcopy manual.

1.0 GUIDELINES FOR USER DOCUMENTATION

A. The application owner ensures that user documentation is prepared. The following provides guidance for its preparation. User documentation may be prepared by the application developer, application custodian, or application owner.

Suggested topics to address in the user documentation are noted below. However, the extent of the documentation should be determined by the application owner.

1. Title page

   a. The words “User’s Documentation” or similar designation.

   b. Revision number of document.

   c. The software name, acronym and version number (if applicable). The name and acronym must match those documented on the Application Software Datasheet (ASD).

   d. The author’s name and dated signature.

   e. The dated signature of the reviewer(s).

   f. The application owner’s name and dated signature.

2. Revision Log

3. A system overview including purpose and applicability.

4. Description of the purpose and instructions for use of each software function.

5. Restrictions or limitations on use.

6. Description of the user interface with the software including input data requirements with acceptable ranges, interpretation of data outputs, and required responses to system error messages or prompts.

7. Samples of outputs, forms, reports, or displays.

8. Information for obtaining user and maintenance support.

9. Organization to which problems with the software should be reported.

Appendix H
(Page 1 of 1)

Cross-Reference Of NPG-SPP-12.7 And Summit Terminology

The following table provides a cross-reference of software documentation terminology between NPG-SPP-12.7 and the summit methodology used by Information Services. Either terminology may be used provided the requirements of NPG-SPP-12.7 are satisfied.

NPG-SPP-12.7	SUMMIT METHODOLOGY
Software Service Request	Service Request
Software Requirements Specification	System Prospectus
Software Design Description	Technical System Design
Validation Test	Acceptance Test
Operability Test	System Test

Appendix I
(Page 1 of 3)

System Hardening Guidelines

The following cyber security principles should be considered when purchasing, developing, or modifying digital plant control systems/components and their associated network, if any (software, systems, networks). Note that all items are not applicable to every system, component or device.

1.0 REMOVAL OF UNNECESSARY SERVICES AND PROGRAMS

A. All software artifacts should be removed or disabled that are not required for the operation and maintenance of the Control System. The services and software to be removed or disabled should include, but not be limited to:

1. Games
2. Device drivers for network devices not delivered
3. Messaging services
4. Servers or clients for unused Internet services
5. Software compilers in all user workstations and servers except for development workstations and servers
6. Software compilers for languages that are not used in the Control System
7. Unused networking and communications protocols
8. Unused administrative utilities, diagnostics, network management, and system management functions
9. Backups of files, databases, and programs used only during system development
10. All unused data and configuration files
11. Sample programs and scripts
12. Unused document processing utilities, for example, Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.

2.0 CHANGES TO FILE SYSTEMS AND OPERATING SYSTEM PERMISSIONS

The system shall be configured with hosts having the least privileged file and account access necessary to perform the functions of the system.

Appendix I
(Page 2 of 3)

System Hardening Guidelines

3.0 HARDWARE CONFIGURATION

A. Whenever possible, all unneeded communication ports and removable media drives shall be disabled through software or physical disconnection or be protected by other engineered barriers.

B. If technically feasible, the system BIOS shall be password protected from unauthorized changes.

C. Where possible, network devices shall be configured to limit access to/from specific locations.

D. The system shall be configured to allow the system administrators the ability to re-enable devices if they are disabled by software.

4.0 PERIMETER PROTECTION

A. Firewalls and firewall rule sets between network zones shall be implemented.

B. Network Intrusion Detection Systems shall be implemented within the control network.

5.0 ACCOUNT AND SESSION MANAGEMENT

A. All default and guest accounts shall be removed prior to placing the system in service. Vendor owned accounts shall be removed or disabled unless required by the contract.

B. The system should not transmit user credentials in clear text.

C. The system shall not allow applications to retain login information between sessions, nor provide any auto-fill functionality during login, nor allow anonymous logins. User account based logout and timeout settings should be used to the extent practical.

6.0 PASSWORD/AUTHENTICATION POLICY AND MANAGEMENT

To the extent practical the system should have a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout, screen lock by application, and denial of repeated or recycled use of the same password.

7.0 ACCOUNT AUDIT AND LOGGING

The system should have an account activity log that is auditable both from a management (policy) and operational (account use activity) perspective. The audit trails and logging files must be time stamped and access controlled.

Appendix I
(Page 3 of 3)

System Hardening Guidelines

8.0 ROLE-BASED ACCESS CONTROL FOR CONTROL SYSTEM APPLICATIONS

The system shall provide for user accounts with configurable access and permissions associated with the defined user role.

Attachment 1
(Page 1 of 1)

NPG-SPP-12.7-1 Application Software DataSheet (QA Record)

APPLICATION SOFTWARE DATASHEET (QA RECORD)

(1) Application Name *: ______________________ Acronym *: ______________________ Version ____________

(2) Description *: ____
____
____
____

	Application Owner *:	Application Developer *:	Application Custodian *:
Organization:			
Contact (optional)			

Application Software or Subsystems	Software Category*	Basis for Classification

NPG Point of Contact (Non-NPG Owned Applications Only): ______________________________

Reviewers for Software Changes: (Application specific review requirements attached □ Yes □ No)

______________________________ ______________________________
______________________________ ______________________________
______________________________ ______________________________
______________________________ ______________________________
______________________________ ______________________________
______________________________ ______________________________
______________________________ ______________________________

______________________________ ____________
Application Owner (Signature) Date

*Denotes Required Information

Attachment 2
(Page 1 of 1)

NPG-SPP-12.7-2 Software Verification and Validation Deficiency Form

SOFTWARE VERIFICATION AND VALIDATION DEFICIENCY FORM

SOFTWARE APPLICATION:

TEST DEFICIENCY NUMBER OR IDENTIFIER: DATE:

VERIFICATION AND VALIDATION ACTIVITY:

REPORTED BY: DATE:

DESCRIPTION OF DEFICIENCY:

EVALUATION (Impact on Software Output)

RESOLUTION

RESTRICTIONS OF USE OF SOFTWARE (If any)

DEFICIENCY CLOSED: ______________________ (Application Owner) ____________ DATE:

TVA 40524 Page 1 of 1 NPG-SPP-12.7-2 [12-17-2010]

Attachment 3
(Page 1 of 1)

NPG-SPP-12.7-3 Computer Software Service Request (SSR)

COMPUTER SOFTWARE SERVICE REQUEST (SSR)

SSR No. (Assigned by Application Owner or Application Custodian after SSR approval)

Section 1 (Request)

Application Name: ____________ Acronym: ____________ Software Category ____

PER Number: ____________ Need Date ____________

Requested Change (Attach expanded description as required):

____

____

Requested by ____________ Organization ____________ Phone ____________ Date ____________

Section 2 (SSR Approved)

Disapproved □ Approved as Submitted □ Approved as Modified per Attached □

SSR Dispositioned: ____________ Date: ____________

Application Owner

Section 3 (Software Change)

Enter N/A for Revision Number if no revision is required.

Application Documentation	Revision Number	Reference (Optional)
Software Requirements Specification		
Software Design Description		
User Documentation		
Other (Specify)		

Section 4 (Validation Testing)

□ Validation Test Procedures and Results including test deficiencies are attached to the SSR.

□ Validation Test procedures and Results are not attached to the SSR but are included in the following reference.

Reference: ____________

Section 5 (Operability Testing)

□ Operability Test Procedures and Results including test deficiencies are attached to the SSR.

□ Operability Test Procedures and Results are not attached to the SSR but are included in the following reference.

Reference: ____________

Section 6 (Cyber Security Assessment)

Cyber Security Assessment Performed □ Yes □ Not Applicable

____________ ____________

Application Owner Date

Section 7 (Application Owner SSR Closure)

□ Software change is released for use without any restrictions.

□ Software change is released for use with restrictions and users notified. Restrictions are attached to this SSR or are included in the following reference.

Reference: ____________

____________ ____________

Application Owner Date

Distribution:
1. Send completed SSR package to EDMS.
2. If plant system affected, send a copy of the SSR package to Plant Simulator Services organization.
3. If the SSR is for a Plant Control System Boundary Protection Device, contact CE for archival in EDMS Sensitive Information Vault. The SSR and all related documentation are deemed "Business Sensitive".

Attachment 4
(Page 1 of 1)

NPG-SPP-12.7-4 Vendor Software Error Report Evaluation

VENDOR SOFTWARE ERROR REPORT EVALUATION

(A) APPLICABILITY EVALUATION

(1) Software Application Name/Acronym ____________________

(2) Applicability Explanation

(3) Preparer: ____________________ Ext. __________ Date __________

(B) ERROR REPORT ITEM RESPONSE SUMMARY

(1) Item is Applicable: Yes □ No □

(2) PER Initiated: Yes □ No □

(3) Error Report Attached: Yes □ No □

(4) Responsible Manager: ____________________ Ext. __________ Date __________

Source Notes
(Page 1 of 1)

Requirements Statement	Source Document	Implementing Statement
Section 13.2 A	Nuclear Quality Assurance Program	Section 3.3
Section 13.2 B	Nuclear Quality Assurance Program	Section 3.4
Section 13.2 C	Nuclear Quality Assurance Program	Section 3.3.5
Section 13.2 D	Nuclear Quality Assurance Program	Section 3.3.5
Section 13.2 E	Nuclear Quality Assurance Program	Appendix G
Section 13.2 F	Nuclear Quality Assurance Program	Section 3.11
Section 13.2 G	Nuclear Quality Assurance Program	Section 3.5
Section 13.2 H	Nuclear Quality Assurance Program	Section 3.10
Section 13.2 I	Nuclear Quality Assurance Program	Section 3.2 B

TVA Letter Dated May 6, 2011
Responses to Licensee Open Items to be Resolved for SER Approval

ATTACHMENT 5

Westinghouse non-proprietary white paper WBT-D-2782, "Westinghouse DMIMS-DX In-Containment equipment environmental specifications" (Letter Item #4/362 [Item 1])

Response to Request for Loose Parts Monitoring System Qualification Documents

Westinghouse DMIMS-DX In-Containment equipment environmental specifications

The Westinghouse Digital Metal Impact Monitoring System (*DMIMS-DX*) is designed to meet or exceed all the requirements of United States Nuclear Regulatory Commission Regulatory Guide (RG) 1.133, Rev. 1, "Loose Part Detection Program for the Primary System of Light-Water-Cooled Reactors." Section C-1.g of the RG states the following:

> g. *Operability for Seismic and Environmental Conditions.*
> Components of the loose-part detection system within containment should be designed and installed to perform their function following all seismic events that do not require plant shutdown, i.e., up to and including the Operating Basis Earthquake (OBE). Recording equipment need not function without maintenance following the specified seismic event provided the audio or visual alarm capability remains functional. The system should also be shown to be adequate by analysis, test, or combined analysis and test for the normal operating radiation, vibration, temperature, and humidity environment.

The seismic qualification of the *DMIMS-DX* in-containment equipment is summarized in EQ-QR-33-WBT, Rev. 0, "Seismic Evaluation of the Digital Metal Impact Monitoring System (DMIMS-DX) for Watts Bar Unit 2." provided to TVA under Reference 2.

Westinghouse is providing TVA with the *DMIMS-DX* in-containment equipment listed below. The environmental specification for the equipment is listed, along with the normal environmental conditions. The normal environmental conditions for a Westinghouse containment are reported in Tables 6-1 and 6-2 from WCAP 8587 Rev. 6, "Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety Related Electrical Equipment". These tables are attached.

- **5357C52G01 – Accelerometer with 4' integral hardline cable**

Radiation:	Specification: Gamma dose >= 200 R/hr with a TID of 10^8 R
Vibrations:	Specification: 200g (Peak) Maximum
Temperature:	Specification: -65°F to 625°F at sensor face, max of 185°F at connector
Humidity:	Specification: 5% to 95% relative humidity

- **5359C29G44 – 120' soft line cable assembly**

Radiation:	Specification: Radiation resistant, no specification given
Vibrations:	Specification: No specification given
Temperature:	Specification: -140°F to 302°F on the cable, max of 185°F at connectors
Humidity:	Specification: 95%, connector should be the same as the hard line cable.

- **2657C47G01 – Charge Preamplifier**

Radiation:	Specification: Radiation resistant, no specification given
Vibrations:	Specification: No specification given
Temperature:	Specification: 40°F to 212°F
Humidity:	Specification: No specification given

TVA Letter Dated May 6, 2011
Responses to Licensee Open Items to be Resolved for SER Approval

ATTACHMENT 6

Evaluation for Common Q PAMS for conformance with RG 1.152 Revision 2
(Letter Item #10/368)

This table explains the compliance to RG 1.152 Rev. 2 regulatory positions 2.1 through 2.6 for the Common Q PAMS for WBN2.

RG 1.152 Position	RG 1.152 Position Text	WBN2 Compliance Statement
2.1	In the concepts phase, the licensee and developer should identify safety system security capabilities that should be implemented. The licensee and developer should perform security assessment to identify potential security vulnerabilities in the relevant phases of the system life cycle. The results of the analysis should be used to establish security requirements for the system (hardware and software). Remote access to the safety system should not be implemented. Computer-based safety systems may transfer data to other systems through one-way communication pathways.	Security capabilities are defined in the System Requirements Specification (SyRS) and System Design Specification (SDS). Specific communication security capabilities in accordance with ISG-4 are described in Common Q PAMS Licensing Technical Report (LTR) WNA-LI-00058-WBT-P. TVA shall provide a security assessment of potential vulnerabilities throughout the relevant phases of the system life cycle. Refer to WNA-LI-00058-WBT-P for compliance to ISG-4 communication criteria between Post Accident Monitoring System (PAMS) and non-safety systems.
2.2		
2.2.1	*System Features* The licensees and developers should define the security functional performance requirements and system configuration; interfaces external to the system; and the requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance. The security requirements should be part of the overall system requirements. Therefore, the V&V process of the overall system should ensure the correctness, completeness, accuracy, testability, and consistency of the system security requirements. Requirements specifying the use of pre-developed software and systems (e.g., reuse software and commercial off-the-shelf systems) should address the vulnerability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).	Security functional performance and qualification requirements are defined in the SyRS. These get translated into configuration and interface requirements in the SDS. These also get translated in to display design and data definitions defined in the Software Requirements Specification (SRS) and Software Description Documents (SDD). And finally the tech manual for system operation, execution and maintenance. Since the security requirements are defined in the SyRS and SDS, they fall under the Independent Verification and Validation (IV&V) program for the WBN2 PAMS. All pre-developed software has been qualified through commercial dedication or previous IV&V when developed by Westinghouse. All pre-developed software is maintained under configuration control with cyclic redundancy check (CRC) stamps to insure proper configuration.

RG 1.152 Position	RG 1.152 Position Text	WBN2 Compliance Statement
2.2.2	*Development Activities* The development process should ensure the system does not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted and undocumented functions or applications.	All pre-developed software is maintained under configuration control with CRC stamps to insure proper configuration. All Westinghouse developed software undergo an IV&V code review with checklist to ensure all code is requirements driven without undocumented functions or other unwanted features.
2.3	Design Phase	
2.3.1	*System Features* The safety system security requirements identified in the system requirements specification should be translated into specific design configuration items in the system design description. The safety system security design configuration items should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items incorporating pre-developed software into the safety system should address security vulnerabilities of the safety system. Physical and logical access control should be based on the results of cyber-security qualitative risk analyses. Cyber-security risk is the combination of the consequence to the nuclear power plant and the susceptibility of a digital system to internal and external cyber-attack. The results of the analyses may require more complex access control, such as a combination of knowledge (e.g., password), property (e.g., key, smart-card) or personal features (e.g., fingerprints), rather than just a password.	SyRS requirements are decomposed into hardware requirements (SDS) and software requirements (SRS). Physical and logical access, their functionality, and data communication requirements to other systems are defined in these documents. The Common Q Design Restrictions document (WNA-DS-01070-GEN) defines the proper configuration of pre-developed software to address security vulnerabilities. Compliance to WNA-DS-01070-GEN is documented in WNA-AR-00201-WBT. The Common Q PAMS will meet the requirements for the Watts Bar Unit 2 Nuclear Security Program as mandated by 10 CFR 73.54 via Watts Bar Unit 2 procedure 25402-3DP-G04G-00508, "Cyber Security Program." This cyber security procedure addresses the security controls identified in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3 which are very similar to the recommended controls endorsed by the NRC in Regulatory Guide 5.71 "Cyber Security Programs For Nuclear Facilities," Revision 0 and NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors," Revision 6.

RG 1.152 Position	**RG 1.152 Position Text**	**WBN2 Compliance Statement**
2.3.2	*Development Activities* The developer should delineate the standards and procedures that will conform with the applicable security policies to ensure the system design products (hardware and software) do not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications.	IV&V Code Reviews contain checklists to ensure developed code does not include undocumented code. For pre-developed software the Common Q Design Restrictions document (WNA-DS-01070-GEN) defines the proper configuration of the pre-developed software to ensure the safety system is secure. Compliance to WNA-DS-01070-GEN is documented in WNA-AR-00201-WBT.
2.4	Implementation Phase In the system (integrated hardware and software) implementation phase, the system design is transformed into code, database structures, and related machine executable representations. The implementation activity addresses hardware configuration and setup; software coding and testing; and communication configuration and set-up [including the incorporation of reused software and commercial off-the-shelf (COTS) products].	No requirement
2.4.1	*System Features* The developer should ensure that the security design configuration item transformations from the system design specification are correct, accurate, and complete.	All security requirements defined in the SyRS, SDS and SRS are traced through implementation via the Requirements Traceability Matrix (RTM). IV&V performs a requirements traceability analysis to ensure the RTM is complete and accurate.

RG 1.152 Position	RG 1.152 Position Text	WBN2 Compliance Statement
2.4.2	*Development Activities* The developer should implement security procedures and standards to minimize and mitigate tampering with the developed system. The developer's standards and procedures should include testing with scanning as appropriate, to address undocumented codes or malicious functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave beyond the system requirements. The developer should account for hidden functions and vulnerable features embedded in the code, and their purpose and impact on the safety system. If possible, these functions should be disabled, removed, or (as a minimum) addressed (e.g., as part of the failure modes and affects analysis of the application code) to prevent any unauthorized access. Scanning is dependent on the platform and code being used, and may not be available for the specified code and compiler. This may be a difficult task with little assurance that the results will be comprehensive and successful in uncovering hidden problems given the size and complexity of most modern computer systems. Pure application code scanning may be partially successful, but many operating systems, machine code, and callable library function aspects of the system may not be able to be successfully scanned and are just as likely to be where avenues for exploitation exist. COTS systems are likely to be proprietary and generally unavailable for review. It is likely that there is no reliable method to determine security vulnerabilities for Operating systems (for example, Microsoft and other operating system suppliers do not provide access to the source code for operating systems and callable code libraries). In such cases, unless such systems are modified by the application developer, the security effort should be limited to ensuring that the features within the system do not compromise the security requirements of the system, and the security functions should not be compromised by the other system functions.	Westinghouse has work instructions that cover the work of configuration management (including checking in/out software from the library), software installation, releasing software, conducting engineering testing, and creating custom functional elements. These procedures and standards minimize and mitigate tampering with the developed system. At every stage of the software development life cycle there is the IV&V activity of testing and code review. Once IV&V has approved the software module, it is checked into a secure location in the library that only IV&V has write access to. In lieu of scanning, each AC160 software custom element is code reviewed by IV&V with a checklist. Each AC160 function chart is code reviewed with a checklist. The Common Q Design Restrictions document (WNA-DS-01070-GEN) defines the proper usage of pre-developed software that has been commercially dedicated. Each project must complete a compliance matrix to document compliance to the design restrictions.

RG 1.152 Position	RG 1.152 Position Text	WBN2 Compliance Statement
2.5	*Test Phase* The objective of testing security functions is to ensure that the system security requirements are validated by execution of integration, system, and acceptance tests where practical and necessary. Testing includes system hardware configuration (including all external connectivity), software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing.	The PAMS was tested in a full configuration as it would be in the plant. The Common Q platform was type tested for equipment qualification as described in the Common Q PAMS Licensing Technical Report (LTR) WNA-LI-00058-WBT.
2.5.1	*System Features* The security requirements and configuration items are part of validation of the overall system requirements and design configuration items. Therefore, security design configuration items are just one element of the overall system validation. Each system security feature should be validated to verify that the implemented system does not increase the risk of security vulnerabilities and does not reduce the reliability of safety functions.	As described in the requirements phase, all security requirements are defined in the SyRS and SDS. A requirements traceability matrix traces all these requirements through the design phase to the test phase to document the validation process for each security requirement.
2.5.2	*Development Activities* The developer should configure and enable the designed security features correctly. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in OEM features.	The Common Q PAMS Licensing Technical Report (LTR) WNA-LI-00058-WBT describes the external communication compliance to ISG-4 criteria. A data storm test was conducted for the external interface to ensure PAMS integrity during such an event.

RG 1.152 Position	RG 1.152 Position Text	WBN2 Compliance Statement
2.6	*Installation, Checkout, and Acceptance Test* In installation and checkout, the safety system is installed and tested in the target environment. The system licensee should perform an acceptance review and test the safety system security features. The objective of installation and checkout security testing is to verify and validate the correctness of the safety physical and logical system security features in the target environment.	TVA witnessed the factory acceptance test performed at Westinghouse which included testing of security requirements. This test was conducted on the deliverable system in the full configuration that would be at the plant. The Common Q PAMS will meet the requirements for the Watts Bar Unit 2 Nuclear Security Program as mandated by 10 CFR 73.54 via Watts Bar Unit 2 procedure 25402-3DP-G04G-00508, "Cyber Security Program." This cyber security procedure addresses the security controls identified in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3 which are very similar to the recommended controls endorsed by the NRC in Regulatory Guide 5.71 "Cyber Security Programs For Nuclear Facilities," Revision 0 and NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors," Revision 6.
2.6.1	*System Features* The licensee should ensure that the system features enable the licensee to perform post-installation testing of the system to verify and validate that the security requirements have been incorporated into the system appropriately.	The Common Q PAMS will meet the requirements for the Watts Bar Unit 2 Nuclear Security Program as mandated by 10 CFR 73.54 via Watts Bar Unit 2 procedure 25402-3DP-G04G-00508, "Cyber Security Program." This cyber security procedure addresses the security controls identified in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3 which are very similar to the recommended controls endorsed by the NRC in Regulatory Guide 5.71 "Cyber Security Programs For Nuclear Facilities," Revision 0 and NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors," Revision 6.

RG 1.152 Position	RG 1.152 Position Text	WBN2 Compliance Statement
2.6.2	*Development Activities* A licensee should have a digital system security program. The security policies, standards, and procedures should ensure that installation of the digital system will not compromise the security of the digital system, other systems, or the plant. This may require the licensee to perform a security assessment, which includes a risk assessment, to identify the potential security vulnerabilities caused by installation of the digital system. The risk assessment should include an evaluation of new security constraints in the system; an assessment of the proposed system changes and their impact on system security; and an evaluation of operating procedures for correctness and usability. The results of this assessment should provide a technical basis for establishing certain security levels for the systems and the plant.	The Common Q PAMS will meet the requirements for the Watts Bar Unit 2 Nuclear Security Program as mandated by 10 CFR 73.54 via Watts Bar Unit 2 procedure 25402-3DP-G04G-00508, "Cyber Security Program." This cyber security procedure addresses the security controls identified in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3 which are very similar to the recommended controls endorsed by the NRC in Regulatory Guide 5.71 "Cyber Security Programs For Nuclear Facilities," Revision 0 and NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors," Revision 6.

TVA Letter Dated May 6, 2011
Responses to Licensee Open Items to be Resolved for SER Approval

ATTACHMENT 7

Evaluation for how the Common Q PAMS SysRS and SRS implement the design basis requirements of IEEE 603-1991 Clause 4 (Letter Item #12/372)

IEEE 603 Clause 4 Compliance		
Clause	**Requirement**	**How Met**
4. Safety System Designation	A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of ANSI/ANS 51.1–1983 [14] or ANSI/ANS 52.1–1983 [15] and shall document as a minimum:	The design basis is WCAP-16097-P-A, "Common Qualified Platform Topical Report Post Accident Monitoring System (PAMS), Appendix 1" and the Common Qualified platform (Common Q) Phase 3 PAMS, 00000-ICE-30156, "System Requirements Specification for the Common Q Post Accident Monitoring System" and the WBN1 ICCM 86 implementation of RVLIS.
4.1	The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.	The Common Q PAMS is designed for all modes of plant operation. Section 3.1 defines the EMC, Environmental and seismic design basis events under which the WBT PAMS is to function.
4.2	The safety functions and corresponding protective actions of the execute features for each design basis event.	The safety functions for the design basis are described in WCAP-16097-P-A, "Common Qualified Platform Topical Report Post Accident Monitoring System (PAMS), Appendix 1". The Common Qualified platform (Common Q) Phase 3 PAMS, 00000-ICE-30156, "System Requirements Specification for the Common Q Post Accident Monitoring System" define the requirements for meeting those safety functions. WNA-DS-01617-WBT, "Post Accident Monitoring System - Program I&C Projects System Requirements Specification" defines the requirements for the WBN2 PAMS that reference portions of 00000-ICE-30156 and the ICCM 86 RVLIS requirements.
4.3	The permissive conditions for each operating bypass capability that is to be provided.	N/A. There are no operating bypasses in the PAMS
4.4	The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.	The Post Accident Monitoring System does not perform any automatic protective actions. The manual protective actions are based on CETs and subcooled margin indications. The monitored variables are defined in the Common Q PAMS Licensing Technical Report Contract Compliance Matrix. Analytical limits, ranges and rates of change are documented in EOP Setpoints Verification Document WBN-OSG4-188.

IEEE 603 Clause 4 Compliance		
Clause	**Requirement**	**How Met**
4.5	The following minimum criteria for each action identified in 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. See IEEE Std 494–1974 (R1990) [8].[6]	
4.5.1	The points in time and the plant conditions during which manual control is allowed.	N/A. The Post Accident Monitoring System does not contain any manual control functions. It is a safety display system to provide the operator information for manual actions as defined in the EOPs.
4.5.2	The justification for permitting initiation or control subsequent to initiation solely by manual means.	N/A. The Post Accident Monitoring System does not contain any manual control functions. It is a safety display system to provide the operator information for manual actions as defined in the EOPs.
4.5.3	The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.	N/A. The Post Accident Monitoring System does not contain any manual control functions. It is a safety display system to provide the operator information for manual actions as defined in the EOPs.
4.5.4	The variables in 4.4 that shall be displayed for the operator to use in taking manual action.	N/A. The operator information for manual actions as defined in the EOPs.
4.6	For those variables in 4.4 that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.	The Post Accident Monitoring System displays the variables defined in the WBT PAMS SysRS Tables 2.5-4, 2.6-2, 2.6-3, 2.6-4.
4.7	The range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage,frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform.	See WNA-LI-00058-WBT-P for applicability of the WBN2 PAMS qualification to WBN2 environmental requirements.
4.8	The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).	The Post Accident Monitoring System EMC, environmental and seismic qualification criteria is defined in Section 3.1.7. The Post Accident Monitoring System has two independent and separated cabinets to address a fire. The only interface to a non-safety system is the fiber optically isolated data link to the plant computer which cannot fail and adversely impact the system operation.

IEEE 603 Clause 4 Compliance		
Clause	**Requirement**	**How Met**
4.9	The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design.	WBT PAMS SysRS Section 3.3.2 and 3.3.3 define the reliability and availability for the system.
4.10	The critical points in time or the plant conditions, after the onset of a design basis event, including:	
4.10.1	The point in time or plant conditions for which the protective actions of the safety system shall be initiated.	The Post Accident Monitoring System does not perform any protective actions.
4.10.2	The point in time or plant conditions that define the proper completion of the safety function.	The Post Accident Monitoring System does not perform any protective actions. There is no concept of proper completion since it is a passive display system.
4.10.3	The points in time or the plant conditions that require automatic control of protective actions.	The Post Accident Monitoring System does not perform any control of protective actions.
4.10.4	The point in time or the plant conditions that allow returning a safety system to normal.	The Post Accident Monitoring System does not "return to normal". It is always displaying data real time.
4.11	The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.	The Post Accident Monitoring System does not contain any such provisions.
4.12	Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).	Diversity and regulatory criteria are addressed in WNA-LI-00058-WBT.