~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

February 9, 2017

Mr. Peter P. Sena, III
President and Chief Nuclear Officer
PSEG Nuclear LLC - N09
P.O. Box 236
Hancocks Bridge, NJ 08038

SUBJECT: REGULATORY AUDIT SUMMARY FOR OCTOBER 3 – 6, 2016, AUDIT AT GE HITACHI IN SUPPORT OF LICENSE AMENDMENT REQUEST TO UPGRADE HOPE CREEK GENERATING STATION'S POWER RANGE NEUTRON MONITORING SYSTEM TO A DIGITAL POWER RANGE NEUTRON MONITORING SYSTEM (CAC NO. MF6768)

Dear Mr. Sena:

By letter dated September 21, 2015 (Agencywide Documents Access and Management System (ADAMS) Package Accession No. ML15265A223), as supplemented by letters dated November 19, 2015, and September 23, 2016 (ADAMS Accession Nos. ML15323A268 and ML16270A006, respectively), PSEG Nuclear LLC (PSEG) submitted a license amendment request (LAR) for the Hope Creek Generating Station (HCGS). The proposed amendment would allow for the replacement and upgrade of the existing analog Average Power Range Monitor subsystem of the Neutron Monitoring System with GE Hitachi digital Nuclear Measurement Analysis and Control (NUMAC) Power Range Neutron Monitoring (PRNM) system. The PRNM upgrade also includes Oscillation Power Range Monitor capability and will allow full Average Power Range Monitor, Rod Block Monitor, Technical Specification Improvement Program implementation. This upgrade will also include application of Technical Specification Task Force (TSTF) Traveler TSTF-493, Revision 4, "Clarify Application of Setpoint Methodology for LSSS Functions" (ADAMS Accession No. ML092150990), to affected PRNM functions. By letter dated September 12, 2016 (ADAMS Accession No. ML16256A639), PSEG submitted Phase 2 of the LAR.

To support its review of the LAR, the U.S. Nuclear Regulatory Commission conducted a regulatory audit at the GE Hitachi, Castle Hayne, North Carolina, site from October 3 – 6, 2016, to (1) gain a better understanding of the NUMAC development lifecycle processes to support the staff review of the PRNM system for use at HCGS, and (2) confirm the staff's understanding of this application. In addition, this audit could inform future regulatory actions involving NUMAC product-based safety-related instrumentation and control systems.

Enclosure 1 contains Sensitive Unclassified Information. When separated from Enclosure 1, this letter is DECONTROLLED.

If you have any questions, please contact me at (301) 415-1603 or Carleen.Parker@nrc.gov.

Sincerely,

Carleen J. Parker, Project Manager
Plant Licensing Branch I
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-354

Enclosure:
1. Proprietary Audit Summary
2. Non-Proprietary Audit Summary

cc w/enclosure 2: Distribution via Listserv

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF NUCLEAR REACTOR REGULATION

REGULATORY AUDIT SUMMARY FOR OCTOBER 3 – 6, 2016, AUDIT AT GE HITACHI IN SUPPORT OF LICENSE AMENDMENT REQUEST TO INSTALL A DIGITAL NUCLEAR MEASUREMENT ANALYSIS AND CONTROL POWER RANGE NEUTRON MONITORING SYSTEM FOR PSEG NUCLEAR LLC HOPE CREEK GENERATING STATION DOCKET NO. 50-354

Proprietary information pursuant to Title to of the *Code of Federal Regulations* Section 2.390 has been redacted from this document. Redacted information is identified by blank space enclosed with boldface double brackets as shown here **[[ ]]**.

Background

By letter dated September 21, 2015 (Agencywide Documents Access and Management System (ADAMS) Package Accession No. ML15265A223), as supplemented by letters dated November 19, 2015, and September 23, 2016 (ADAMS Accession Nos. ML15323A268 and ML16270A006, respectively), PSEG Nuclear LLC (PSEG) submitted a license amendment request (LAR) for the Hope Creek Generating Station (HCGS). The proposed amendment would allow for the replacement and upgrade of the existing analog Average Power Range Monitor subsystem of the Neutron Monitoring System with GE Hitachi digital Nuclear Measurement Analysis and Control (NUMAC) Power Range Neutron Monitoring (PRNM) system. The PRNM upgrade also includes Oscillation Power Range Monitor capability and will allow full Average Power Range Monitor, Rod Block Monitor, Technical Specification Improvement Program implementation. This upgrade will also include application of Technical Specification Task Force (TSTF) Traveler TSTF-493, Revision 4, "Clarify Application of Setpoint Methodology for LSSS Functions" (ADAMS Accession No. ML092150990), to affected PRNM functions. By letter dated September 12, 2016 (ADAMS Accession No. ML16256A639), PSEG submitted Phase 2 of the LAR.

Enclosure 2

Regulatory Audit Basis

To support its review of the LAR, the U.S. Nuclear Regulatory Commission (NRC) staff conducted an audit at the GEH facility in Castle Hayne, North Carolina. This audit was conducted in accordance with the Office of Nuclear Reactor Regulation Office Instruction LIC-111, "Regulatory Audits." The purpose of this audit was to (1) gain a better understanding of the NUMAC development lifecycle processes to support the staff's review of the PRNM system for use at HCGS, and (2) confirm the staff's understanding of this application. In addition, this audit could inform future regulatory actions involving NUMAC product-based safety-related instrumentation and control systems. The audit was performed in accordance with the audit plan, which was sent to PSEG on September 28, 2016 (ADAMS Accession No. ML16265A449).

The basis of this audit is the HCGS PRNM system LAR and the following regulations:

- Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, Appendix A, General Design Criteria (GDC) 1, *"Quality standards and records,"* requires structures, systems, and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

- GDC 10, *"Reactor design,"* requires the reactor core and associated coolant, control, and protection systems be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.

- GDC 12, *"Suppression of reactor power oscillations,"* requires the reactor core and associated coolant, control, and protection systems to be designed to assure that power oscillations, which can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.

- GDC 13, *"Instrumentation and control,"* requires that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions, as appropriate, to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

- GDC 20, *"Protective system functions,"* requires the protection system be designed (1) to initiate automatically the operation of appropriate systems, including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences, and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

- GDC 21, *"Protection system reliability and testability,"* requires that the system be designed for high functional reliability and inservice testability, with redundancy and independence sufficient to preclude loss of the protection function from a single failure and preservation of minimum redundancy, despite removal from service of any component or channel.

- GDC 22, "*Protection system independence,"* requires that the system be designed so that natural phenomena, operating, maintenance, testing, and postulated accident conditions do not result in loss of the protection function.GDC 23, "*Protection system failure modes,"* requires that the system be designed to fail to a safe state in the event of conditions such as disconnection, loss of energy, or postulated adverse environments.

- GDC 24, *"Separation of protection and control systems,"* requires that interconnection of the protection and control systems be limited to assure safety in case of failure or removal from service of common components.

- GDC 29, *"Protection against anticipated operational occurrences,"* requires that protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

- 10 CFR 50.55 requires, in part, that structures, systems, and components subject to the standards in 10 CFR 50.55a must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

- 10 CFR 50.55a(h) requires that the protection systems meet the Institute of Electrical and Electronics Engineers (IEEE) Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," Section 4.2, which discusses the general functional requirement for independence of protection systems to assure they satisfy the single failure criterion.

Regulatory Audit Scope

The audit reviewed items to verify, by an independent evaluation, that the NUMAC-based PRNM system to be used at HCGS conforms to applicable regulations, standards, guidelines, plans, and procedures by assessing the implementation of the system's developmental lifecycle process. A review of activities associated with the establishment of a secure development environment was also conducted. A more detailed discussion of items reviewed for this regulatory audit were provided in the regulatory audit plan.

Audit Logistics

The NRC staff who participated in this audit were:

- Richard Stattel, Audit Leader
- Samir Darbali, Technical Reviewer

The GEH and licensee staff who participated in this audit were:

Name	*Role/Title*	*Organization*
Kahlim Miller	Project Manager	GEH
Erin Joy	Controls Manager	GEH
Larry Chi	Chief Consulting Engineer – IVV Lead	GEH
Barry Pagans	Design Technology Engineer	GEH
Randy Eubanks	System Quality Engineer	GEH
Ty Rodgers	I&C Principal Engineer	GEH
Peter Sanza	I&C Principal Engineer	GEH
Frank Novak	PRNM Tech Lead	GEH
Kim Vikara	PRNM Tech Lead (Acting)	GEH
Mark Elliott	Quality Leader	GEH
Lisa Schichlein	Regulatory Affair Engineer	GEH
Tim Enfinger	Regulatory Affair Engineer	GEH
Paul Nichols	I&C Engineering Manager	GEH
David Vreeland	Stability Engineer	GEH
Scott West	Qualification and Test Manager	GEH
Ross Marente	Hope Creek Tech Project Engineer	GEH
Kevin Peters	Cyber Security Engineer	GEH
Jhansi Kandasamy	General Manager, Services Engineering	GEH
Peter Reibe	IV&V Tech Lead	GEH
Keith Swing	PSEG Systems Engineer	PSEG
David Heinig	PSEG Design Engineer	Sargent & Lundy
Robert Gallaher (via phone)	PSEG Project Manager	PSEG
Brian Thomas (via phone)	PSEG Licensing Manager	PSEG

The audit was conducted at the GEH NUMAC development facility in Castle Hayne, North Carolina, from October 3, 2016, to October 6, 2016. Additional activates were performed from NRC headquarters located in Rockville, Maryland.

Audit Activities

1. Entrance Meeting

The NRC staff provided an overview of the audit plan and discussed the objectives for the audit. Facility logistics and the detailed schedule of audit activities were then reviewed and revised to

accommodate availability of participants. Several interviews with key GEH individuals were scheduled for later in the week.

2. Review Central Processing Unit (CPU) Board Anomalies

Before the regulatory audit, GEH notified the NRC staff of a problem observed in one of the boards of the NUMAC PRNM system. During the audit, GEH gave a presentation of the events leading to the anomaly, which resulted in the failure of the auto calibration function of the NUMAC PRNMs. The anomaly was identified after completion of the HCGS factory acceptance test (FAT) and will require new CPU boards to be sent to the licensee for installation prior to system startup.

[[

]]

Subsequent testing of the same design performed for another PRNM system client revealed an anomaly that affected the automatic calibration functions of the PRNM system. A condition report (CR) was then generated and evaluated for potential impact to the HCGS PRNM system. The Condition Review Board determined that the identified condition was not reportable under 10 CFR Part 21 because the effects of the failure were limited to the auto calibrate function of the PRNM system that can only be performed when the associated PRNM channel is placed in the inoperable status. However, the condition was determined and confirmed to be applicable to the HCGS PRNM system, and corrective actions to replace the affected circuit boards in the HCGS system were initiated. Thus, the operating PRNM system channels would not have been affected by the anomaly, but the calibration process to establish operability could have been impacted. Replacement circuit boards that have modified logic designs to prevent auto calibrate failures will be installed into the HCGS PRNM system prior to installation into the plant.

[[

]]

The NRC staff reviewed documentation, including the CRs associated with both the CPU reset issue and the auto calibrate failure anomaly. This review included an assessment of the processes used by GEH to evaluate the extent of condition and applicability to previously installed NUMAC systems. This process includes a daily review conducted by a condition review group (CRG) to perform initial assessment of issues identified and to initiate followup actions as needed.

The NRC staff attended the daily CRG meeting on the morning of October 4, 2016, to observe the tools and processes used for this evaluation. During this meeting, 11 CRs were reviewed, and none were determined to have operability impact or were determined to be reportable. Discussions with the CRG members allowed the NRC staff to gain an understanding of the processes used by GEH to evaluate issues in a timely manner as they are identified.

3. NUMAC Lab and Testing Facility Tour

GEH provided a tour of the NUMAC test facility to demonstrate the auto calibration function that was affected by the programmable logic devices (PLD) timing anomaly discussed above. An auto calibration was performed on a lab system with a circuit analyzer installed to show how the analog test circuits responded to executed test steps.

Though the anomaly could not be reproduced during this demonstration, a detailed discussion of its effects and method of detection were provided. The NRC staff discussed the purpose of the auto calibrate function and confirmed by schematic review that the analog test signals are applied to the detector input circuits, in place of the detectors, in order to assure correct channel calibration. These tests are to be conducted at the plant as part of the required periodic surveillance channel calibration procedure. The licensee representative confirmed that these tests were performed during the HCGS PRNM system FAT and that no test failures were observed.

4. Requirements Thread Reviews

To facilitate performance of thread reviews, the NRC staff asked GEH to assist in creation of a documentation map to illustrate established requirements links between various NUMAC documents. Figure 1 below shows how requirements traceability is accomplished for the HCGS NUMAC system. At the center of this figure are the three primary specification documents that were provided as attachments to the LAR:

- System Requirements Specification (SyRS) (Appendix F Part 1)
- Integrated Performance Specification (IPS) (Appendix F Part 2)
- Average Power Range Monitor (APRM) Functional Controller Software Design Specification (SDS) (Appendix G)

All other documents referenced were made available to the NRC staff during the audit.

Traceability is established using various tools, including DOORS. Traceability matrix tables are included in the specification documents themselves, which allows review of traceability links without the need to directly access the DOORS application.

The NRC staff noted that DOORS is not used exclusively for requirement traceability throughout the development process and that not all referenced documents were imported into the DOORS tool. Establishment of traceability is performed by the design team using DOORS.

For traceability to test documentation, including various test procedures and test results reports, the independent verification and validation (IV&V) team creates tables that are embedded in the test documents. These tables provide traceability between specified requirements and test activities used to verify implementation. Testing traceability is a separate activity from the specification documentation traceability and is performed without the use of the DOORS tool.

[[

]]

Each of these sub-requirements was successfully traced to more specific requirements in the IPS or to the NUMAC licensing topical report (ADAMS Legacy Library No. 9605290009 (non-public - proprietary). Several of these sub-requirements were further traced to requirements in the APRM SDS. The NRC staff then used the test document matrices to locate traceability for these requirements to the verification and validation (V&V) test documents.

The NRC staff notes that there were other links to external documents and to the NUMAC licensing topical reports that were not found in the traceability matrices tables. These links could only be found within the DOORS tool. However, once identified, each of these traces could be followed. The NRC staff successfully traced several sub-requirements to individual validation, module, and integration test cases, and the staff was able to confirm satisfactory implementation and verification of requirement implementation.

[[

]]

This requirement traced directly to a section in the NUMAC licensing topical report. It did not trace to the IPS; however, a word search revealed this requirement exists in the LAR Appendix N, "PRNM System Response Time Analysis Report." The NRC staff then identified a validation test case, "OPRM Trip Response Time," which was used to verify implementation of this safety function timing requirement.

[[

]] The starting point for this requirement was the IPS. This was done to demonstrate traceability to the SyRS in the reverse direction. The NRC staff was able to find the related specification in the SyRS.

The NRC staff noted that several design constraints were used to implement this requirement, but they could not be traced. GEH explained that specifications classified as design constraints (DC) are treated in a similar manner as those designated as requirements; however, they are not directly traceable and are not included in the traceability matrices. For selected design constraint specifications reviewed, the NRC staff was able to confirm that the specification was implemented in the PRNM system design.

[[

]] The starting point for this thread was the Software Requirements Specification. It was chosen to show upward traceability to the SyRS and IPS.

The NRC staff found this specification to be a DC rather than a requirement. As such, there was no reference found in the traceability matrices. However, these DC specifications could be traced through other means, such as word searches and DOOR links.

The NRC staff reviewed test documents to confirm implementation of the associated DCs for this specification (7728DC). Test cases were performed to ensure functions prescribed by the DC specifications operated correctly.

The NRC staff notes that GEH traceability guidance for NUMAC PRNM projects requires objects identified as DCs to be out-linked to IPS requirements. During the audit, however, the NRC was unable to use the embedded traceability matrices to trace threads for the selected DCs. A new open item was initiated to request an explanation of how this procedural requirement is being met, if not through the embedded requirements tables of the SDS and IPS documents.

[[

]]

[[

]] The NRC staff confirmed that traceability was successfully established between the SyRS and the IPS. The NRC staff was able to trace these requirements to the APRM Sub-system Validation Test Procedure and to the Test Procedure Data Sheet, which states that the associated tests were completed and no anomalies were identified.

5. Software Verification and Validation (V&V)

The IV&V portion of the audit was intended to confirm that the NUMAC application software V&V program meets the requirements of IEEE Standard 1012, "IEEE Standard for Software Verification and Validation," and the V&V program is implemented in a manner that reliably verifies and validates the design outputs at each stage of the NUMAC software development process.

This portion of the audit included a discussion of the IV&V processes described in the NUMAC Systems Independent Verification and Validation Plan (IV&VP) for the HCGS PRNM system application software development. The NRC staff discussed the level of IV&V team involvement with the NUMAC development activities and the level of independence between the IV&V team and the design team. The NRC staff made the following observations:

- The IV&V staff is knowledgeable of its roles in the PRNM system application development.
- The IV&V staff was asked to identify examples of issues or conflicts between the IV&V organization and a software design team; it was able to describe how disagreements would be escalated and resolved using existing GEH processes.
- When asked about the relative experience level of the IV&V organization, the NRC staff was presented with a training skills matrix that listed qualification levels for members of the IV&V staff. This matrix is used to ensure that qualified personnel are assigned to perform work activities and a means of identifying training or qualification deficiencies.

The NRC staff performed a review of the qualification and training records for one of the IV&V engineers assigned to the HCGS PRNM project. The NRC staff noted that these individual training records are maintained and used to make work assignments based on qualifications, experience, and past work assignments. These records indicated that the individual did meet the minimum training requirements for the HCGS PRNM team assignment.

IV&V team members explained how identified problems will be documented and addressed using the corrective action processes. GEH provided sample documentation of engineering changes and CRs used during the HCGS project.

The recently submitted HCGS PRNM System Verification and Validation Task Report (Document 001N5721, Revision 5) was reviewed, and it showed a correlation between documented V&V activities performed during each development stage of the HCGS PRNM system and the activities called for in the IV&V plan. An evaluation was also conducted to determine if the GEH IV&V team was sufficiently independent in terms of cost, schedule, and management.

The NRC staff conducted an interview with the Software V&V Engineer to discuss V&V activities and IEEE 1012 compliance. Appendix K of the HCGS LAR contains a compliance matrix showing required mapping of GEH V&V activities with activities defined in IEEE 1012 for SIL 4 software. GEH confirmed that all software associated with the NUMAC PRNM system is

classified and treated as SIL 4 software, and all associated V&V activities are performed to ensure software correctness.

6. Configuration Management

The NRC staff reviewed the configuration management activities established for the HCGS NUMAC system. For this audit activity, the staff reviewed configuration management and design change control procedures, observed how these procedures have been implemented, and interviewed GEH personnel.

GEH uses the Nuclear Product Lifecycle Management (PLM) product data management system as the official repository to maintain and control design documentation and logic files. GEH transitioned from the eMatrix product data management system to PLM between Baselines 1 and 2 of the HCGS NUMAC project. New PLM document numbers were assigned to the configurable items that were originally stored in eMatrix. Although PLM allows for more than one person to work on a document, the tool tracks changes to controlled files. Additionally, every change to a PLM document requires an Engineering Change Order (ECO).

The GEH procedure for a design release (CP-03-100-G400) describes the process for performing ECOs. The ECO identifies Output documents that need to be revised. A description of the proposed change is included in the ECO before the document is changed. Comments to the ECO (provided by the reviewer) and resolutions (provided by the responsible engineer) are documented as part of the document change process. When a document is to be modified, the latest revision's native file (e.g., an MS Word file) is pulled from PLM and edited with tracked changes. Once the document is modified, it is converted into a PDF file, and it becomes a quality record. The latest revision of the document shows when it is released.

The NRC staff reviewed the System Configuration Management Task Report (Appendix C of NEDC-33872P, Revision 0 (ADAMS Accession No. ML16256A648)), which summarizes the configuration management activities performed during each phase of the project and documents conclusions reached. The task report states that anomalies were not identified. Attachment C of the task report includes the system Configuration Status Accounting (CSA) spreadsheet, which identifies the baseline documents and versions at the end of each lifecycle phase. These include plans, specifications, schematics, test procedures, test reports, and source codes. For example, the ECO for Revision 6 of the CSA (ECO-0022695) explains the revision to the IPS was due to the change in the CPU board. This ECO revises the APRM and rod block monitor (RBM) IPS to reflect the use of the new G003 CPU card added to the bill of materials by ECO-0019623. The ECO identifies that Revision 5 of the NUMAC APRM DSS-CD (000N6426), and Revision 2 of the NUMAC RBM (0006612), will be updated to Revisions 6 and 3, respectively, to reflect the updated CPU card part number.

The NRC staff also reviewed the System Quality Assurance Functional Configuration Audit Checklist dated April 25, 2016, which was performed for the test phase (Baseline 5) of development. The checklist identifies that the configuration audit was completed and that changes to previous baseline configurations were approved. The checklist also identifies

documents to be reviewed and approved, including the System Verification and Validation Task Report, the System Configuration Management Task Report, and the CSA.

7. Software Quality Assurance (QA)

The NRC staff reviewed the software QA processes with the GEH quality leader and one of the system quality engineers. These individuals are responsible for evaluating the effectiveness of the QA program in assuring quality of the HCGS PRNM system application software.

The QA leader described the GEH QA program and explained how the NUMAC software quality assurance plan (SQAP), as implemented through work instructions, relates to the overarching GEH Nuclear Quality Assurance (NQA)-1 program. The NRC staff confirmed the quality assurance processes and procedures are subject to the same configuration management, corrective action, and change management activities that apply to NUMAC platform configuration items.

The QA team explained that it performs project-specific audit assessments, reviews, and inspections. These activities are used to assess the quality aspects of the project activities during each phase of the application development lifecycle. The system QA engineer is also a member of the baseline review team and is responsible for performance of functional configuration audits of the product configuration during each lifecycle phase. The results of this audit are documented in the functional configuration audit checklist.

The NRC staff reviewed the implementation phase (Baseline 4) audit checklist for the HCGS PRNM system. It identified task reports for safety analysis, V&V, and Configuration management activities for QA review. Several other project documents, including the project work plan and the four planning documents, were also identified and reviewed by the QA team as part of this baseline.

The NRC staff reviewed and discussed the independence of the QA team from the design and IV&V organizations. As stated in the NUMAC SQAP, the nuclear quality organization is technically, managerially, and financially independent from both the design and IV&V teams. The project team structure organization chart of the system management plan was reviewed, and the reporting structure supports an adequate level of independence between these organizations.

The NRC staff reviewed how problems and anomalies are resolved. The NUMAC system management plan states issues that could affect quality will be promptly escalated for resolution and describes the issue resolution process. The NRC staff reviewed several CRs and observed one daily condition review board meeting during the audit. This audit activity is described in Section 2 of this report.

If resolution of an anomaly requires escalation or identifies a potential reportable condition, a Level 1 escalation process is enacted, which involves project management engagement and includes an extent of condition evaluation of the issue. If the Level 1 process does not resolve the issue, then the issue is further escalated to Level 2, which involves senior management

engagement. A resolution plan is then developed to address the condition, which includes various actions needed to resolve the issue.

The licensee was asked about QA oversight activities performed for the PRNM project. In response, the licensee informed the NRC staff that two audits had been performed. The first was an audit of the equipment supplier Gavial, and the second was an audit of the GEH FAT. The NRC staff requested access to the associated reports for these audits on the document portal.

The NRC staff subsequently reviewed the licensee surveillance reports to evaluate the adequacy of oversight activities performed. The surveillances included detailed descriptions of system development activities, including tests performed and anomalies being addressed by the vendor. The surveillance reports also included surveillance checklists that identify verification activities performed. Several unsatisfactory results were reported for these activities. Surveillance findings were reported to the vendor, and corrective actions were initiated to resolve issues identified by the licensee. A followup surveillance closure activity was then performed, and the licensee accepted corrective actions taken by the vendor to resolve discrepancies.

These reports indicated a high degree of licensee interest and awareness of vendor activities being performed. The surveillance reports indicate that the licensee understood the potential safety implications of issues being addressed by the vendor and that the licensee played an active role in the resolution of these issues.

8. Software Safety

This audit activity was performed to verify that software safety plans, as implemented within the NUMAC SyVVP, and procedures used for safety analysis activities, are adequate to ensure that PRNM software is safe to be used for safety-related nuclear power plant operations.

The GEH system V&V plan identifies processes and activities for incorporating software safety throughout the PRNM system development lifecycle. The NRC staff reviewed software safety processes and procedures used during HCGS PRNM system software development with representatives of the design and IV&V organizations to assess the effectiveness of these programs in achieving the software safety objectives. The audit team observed that the IV&V activities being performed for the PRNM system included safety analysis activities similar to the requirements for software integrity Level 4 software, as defined in the software V&V plan. The safety goals identified in the SyIVVP include mitigation of software-related hazards.

As stated in the SyIVVP, software-related activities are performed by personnel from both the design engineering and IV&V organizations. It was apparent to the audit team that the engineers from these organizations were communicating software safety issues with each other effectively on a regular basis. Personnel interviewed from each organization were found to be knowledgeable and well informed of current and past safety issues pertaining to the PRNM system application.

9. Secure Development Environment

The NRC staff verified that the secure development environment (SDE) established at the GEH facility for the HCGS NUMAC system conforms to the requirements of Regulatory Guide (RG) 1.152, Revision 3, "Criteria for Use Computers in Safety Systems of Nuclear Power Plants" (ADAMS Accession No. ML102870022). For this audit activity, the NRC staff reviewed GEH procedures and guidelines that describe the secure development environmental controls, observed how these security controls have been established, and interviewed key personnel. The NRC staff also reviewed how code reviews were performed to ensure that no unintended code was included in the HCGS NUMAC system.

GEH provided a tour of the design, production, testing, and receipt inspection areas used for the development of the NUMAC system. The NRC staff was able to observe the physical and logical measures implemented to control and monitor access to the NUMAC system to only allow preapproved individuals. The NRC staff also observed how the NUMAC system design and products are secured and tracked throughout the development lifecycle. **[[**

]]

The NRC staff reviewed the following GEH requirements and procedures, which establish the GEH secure development environment for the NUMAC system:

- The Secure Development Environment common procedure (CP-23-314) addresses the establishment of a Secure Development Environment Plan (SDEP) covering security of software, hardware, and documentation, during digital instrumentation and control (I&C) product development lifecycle. The SDEP is to be developed in accordance with RG 1.152 and the applicable portions of RG 5.71, "Cyber Security Programs for Nuclear Facilities." GEH explained that the SDEP came to later be known as the Cyber Security Plan.

- Secure Development Environment Planning work instruction (WI-23-314-01) is intended to implement the SDE planning requirements of CP-23-314 in creating and maintaining either a generic or a project-specific SDEP.

- The Secure Development Environment Susceptibility Assessment work instruction (WI-23-314-10) defines a method to perform susceptibility assessments in accordance with SDE characteristics defined in CP-23-314 and is intended to be used at each stage of the development lifecycle or as required.

- The Secure Development Environment Product Security work instruction (WI-23-314-11) defines processes to implement and assess digital product security, including secure coding practices in accordance with SDE characteristics defined in CP-23-314, including vulnerability assessments, source code analysis, and security flaw tracking and resolution.

- The Secure Development Environment Infrastructure common procedure (CP-23-350) defines the infrastructural security requirements of the SDE, including: secure product handling and delivery, maintaining an SDE during the developmental lifecycle phases, and protecting the developed products from inadvertent or inappropriate alterations during the development lifecycle. The Secure Development Environment Security Operations work instruction (WI-23-350-01) defines processes for implementing the requirements of CP-23-350.

- The NUMAC Systems Cyber Security Plan (002N2752) establishes a process for implementing cyber security requirements into the design and development, integration, and configuration management of safety-related NUMAC products. It describes the NUMAC Digital I&C Development Life Cycle Tasks to be performed by the design team and the IV&V team.

- The PSEG PRNM System Cyber Security Specification (H-1-ZZ-KDS-0512) defines the applicable cyber security control requirements for PSEG Nuclear Digital Technology Systems critical digital assets.

- The HCGS Network Interface Card (NIC) Cyber Security Assessment (DOC-0006-0839) contains the GEH vulnerability assessment of the PSEG security requirements on the HCGS NIC.

The NRC staff also reviewed the Cyber Security Test Procedure for Hope Creek PRNM (002N7269), [[

]]

APRM Code Review

GEH used the Peach Bottom Nuclear Generating Station (Peach Bottom) average power range monitor (APRM) functional software baseline as the starting point for developing the HCGS APRM software code. The controlled Peach Bottom baseline was obtained from the PLM repository and copied to the source code development tool, [[ ]] where it was modified for the HCGS application. GEH explained that although [[ ]] can allow for multiple people to edit the code, typically only one person is assigned to work a particular code project at a time. [[ ]] also assigns the baseline identification numbers and keeps a record of who has edited a baseline file. Before performing the code review, GEH uses a static analysis tool to prevent defects and expose vulnerabilities.

GEH uses an [[ ]] compatible code review tool to verify that the new APRM code meets the application requirements. This tool allows the reviewer to compare different source code baselines by highlighting the differences between the two versions. The tool also allows the reviewer to add comments to be addressed by the responsible engineer. The tool allows for two people to simultaneously review the code. Although the source code review tool is compatible

with [[ ]] it cannot be used to modify the code (i.e., the code can only be modified through [[ ]]

The NRC staff reviewed GEH document 002N6392, Revision 1, "Hope Creek APRM Functional Software Code Review Report." Section 4 of this report documents the code reviews that were performed. Section 5 lists the code reviews that were completed as part of the APRM functional software development and notes that all comments were addressed. The source code review tool output printout is included in Appendix A of the Software Code Review Report.

The NRC staff reviewed the results of a particular code review that covers the source code changes needed to adhere to the HCGS project design specifications. [[

]] which was approved by the NRC staff.

The 002N6392 report includes an instance where the code reviewer identified a portion of the code related to an [[
]]. The responsible engineer agreed with the verifiers' comments and responded that the [[ ]].

The NRC staff reviewed GEH document 002N6397, Revision 1, "Hope Creek APRM Functional Software Test Item Transmittal Report (TITR)," which was prepared by the design team to inform the IV&V team that development of the APRM functional software for the HCGS PRNM has been completed and is ready for independent testing. The Hope Creek APRM Functional Software Code Review Report described above was used as one of the supporting documents for developing the TITR.

PLD Code Review

[[

]]

For the PLD logic modification, GEH used the ECO process to review and document the code review. The ECO process includes a verification scope phase, a comment and resolution phase, and an IV&V comment and resolution phase. The NRC staff reviewed ECO-0021902 and ECO-0021775, which are related to the PLD logic modification, and noted that IV&V had performed a review of the code and that the responsible engineer addressed all comments.

10. Exit Meeting

During the exit meeting, GEH and licensee personnel were provided with a summary of the NRC staff observations made during the audit. The NRC staff also provided a list of documents requested to be placed onto the portal to support the audit summary development. This list was

added to the Open Items List as OI30 and is included below for reference. The Open Items List is available as part of the monthly public meeting summaries (ADAMS Accession Nos. ML16036A154 and ML17012A257).

Request for Documents to be put on Portal:

- PRNM System Validation Test Procedure 002N5897
- APRM IVV Module Test Procedure 002N7588
- APRM Integration Test Cases and Procedures (ITCP) 002N5941
- Licensing Oversight Audit Reports (2), Gavial, and FAT
- CR 13702 (Self Identification of Traceability Issue)
- Functional Software Code Review Report 002N6392
- HCGS APRM Functional Test Item Transmittal Report 002N6397
- ECO-0021902
- ECO-0021775 DBR 0013981
- Quality Control Work Instructions:
    - 23-303-10
    - 23-310-11
    - 23-310-11(G01)

Bibliography

Licensee Documentation:

1. PSEG LAR, dated September 21, 2015 (ADAMS Accession No. ML15265A223)
2. PSEG LAR supplement, dated November 19, 2015 (ADAMS Accession No. ML16172A012)

NRC Guidance:

1. Standard Review Plan (NUREG-0800), Chapter 7, "Instrumentation and Controls"
2. Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
3. Regulatory Guide 1.153, Revision 1, "Criteria for Safety Systems"
4. Regulatory Guide 1.168, Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
5. Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
6. Regulatory Guide 1.173, September 1997, "Developing Software Life-Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Industry Standards:

1. IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

2. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
3. IEEE Standard 828-1990, "IEEE Standard for Software Configuration Management Plans"
4. ANSI/IEEE Standard 1042-1987, "IEEE Guide to Software Configuration Management"
5. IEEE Standard 1012-1998, "IEEE Standard for Software Verification and Validation"
6. IEEE Standard 1028-1997, "IEEE Standard for Software Reviews and Audits"
7. IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes"

If you have any questions, please contact me at (301) 415-1603 or Carleen.Parker@nrc.gov.

Sincerely,

/RA/

Carleen J. Parker, Project Manager
Plant Licensing Branch I
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-354

Enclosure:
1. Proprietary Audit Summary
2. Non-Proprietary Audit Summary

cc w/enclosure 2: Distribution via Listserv

DISTRIBUTION:

PUBLIC	LPL1 R/F	RidsNrrDorlLpl1 Resource
RidsNrrLALRonewicz Resource	RidsNrrPMHopeCreek Resource	RidsACRS_MailCTR Resource
RidsRgn1MailCenter Resource	RidsNrrDeEicb Resource	RStattel, NRR
RidsNrrDorl Resource	RAlvarado, NRR	RidsNrrDssSrxb Resource
SDarbali, NRR	DSaenz, NRR	RidsNrrDssStsb Resource
MChernoff, NRR	RidsNrrDraAphb Resource	VHuckabay, NRR

ADAMS Accession Nos.: PKG: ML16357A080 Enclosure 1 (proprietary): ML16354B237
Enclosure 2 (non-proprietary): ML16363A365 *by e-mail dated

OFFICE	DORL/LPLI/PM	DORL/LPLI/LA	DE/EICB/BC*	DORL/LPLI/BC(A)	DORL/LPLI/PM
NAME	CParker	LRonewicz	MWaters	SKoenick	CParker
DATE	1/26/2017	12/28/2016	12/13/2016	2/9/2017	2/9/2017

OFFICIAL RECORD COPY