Summary of Vendor Oversight Activities and Planning

The section below summarizes the Vendor Oversight Plan (VOP) and it is to be included in the license amendment request (LAR). This VOP summary meets the intent of the prerequisite in DI&C ISG-6 Section C.2.2.1. Note that this paragraph will not be included in the LAR / VOP summary.

Assumptions Regarding VOP Summary

This VOP Summary is written assuming the underlying VOP was written for the Oconee Project based on the current understanding of the DI&C-ISG-06 Revision 2 Alternate Review process and its use of the VOP. This VOP Summary is not based on an actual VOP. The Oconee project had the following project characteristics:

1. *Use of an NRC-approved digital platform (TELEPERM XS)*
2. *Vendor (Areva) had a quality assurance program compliant with 10 CFR Part 50 Appendix B and was on the licensee's approved supplier list.*
3. *No software program manual existed that defined an approved application development process*

Vendor Oversight Plan

A Vendor Oversight Plan (VOP) was developed to describe the series of interactions that occur at key milestones to ensure that process and technical requirements are maintained throughout the project lifecycle. The VOP scope, which includes both hardware and software elements of digital equipment, ensures vendor compliance with their processes, verification and validation, requirements traceability, configuration management, testing, Secure Development and Operational Environment (SDOE), and applicable Plant Specific Action Items (PSAI).

Software quality assurance shall also be confirmed for consistency with the 2015 version of NQA-1 (Reference 1), Part II Subpart 2.7, "Quality Assurance Requirements for Computer Software for Nuclear Facility Applications." The VOP assures that the vendor operates in compliance with their software lifecycle processes, in accordance with ISG-06, Section C.2.2.1, as implemented in the vendor's 10 CFR 50 Appendix B Quality Assurance Program.

Inputs to the VOP include Purchase Specification, Operating Experience, Nuclear Procurement Issues Committee Audit Checklist (NUPIC) or Licensee audit reports, NRC/INPO/EPRI reports, technical reviews, and applicable vendor oversight guidelines. The results of each visit are documented in one or more reports that are maintained by the licensee and available for NRC audit or inspection.

This VOP is adapted to project-specific activities described in this LAR and consists of the following steps:

1. Identify stakeholders and their roles
2. Development and assessment of potential risk factors
3. Determine performance measures and acceptance criteria
4. Implement appropriate oversight methods
5. Perform corrective actions as needed

1. Identify stakeholders and their roles

Project stakeholders, identified below, have a working knowledge of the supply chain involved in producing digital equipment intended the for plant and/or understanding of the technical requirements and expectations from the vendor. Selected licensee stakeholders attend the vendor oversight visits. The vendor (Areva) has responsibility for both the development of the protection system equipment and the associated project integration activities. As such, their representatives participate in vendor oversight visits, as necessary. The project status and covered topics identify those stakeholders that need to be present for the visit being planned, as well as questions to be answered from stakeholders not present.

The stakeholders and their VOP-specific roles for this project are identified as follows:

Licensee:

Project Manager – This individual, who serves as the project manager for the overall project, is responsible for coordinating, scheduling, organizing, and chairing vendor oversight visits and ensuring the appropriate stakeholders are present, depending on the purpose of the specific visit. The licensee project manager is ultimately responsible for controlling and managing change to minimize project resources.

Quality Manager – This individual is familiar with 10 CFR 50 Appendix B and responsible for reviewing and accepting the current vendor's Nuclear Procurement Issues Committee Audit (NUPIC) report. This individual ensures the vendor's internal quality processes (for platform application development and system integration) are being executed properly for the project.

Subject Matter Expert – Individual(s) who served a role in the conceptual design / scoping phase of the project and responsible for ensuring that project requirements are understood and met.

Responsible Engineer – Responsible for understanding all technical aspects of the Engineering Change. Considering that this project is being designed, manufactured, and integrated by a single vendor, the Responsible Engineer is also responsible for performing/coordinating an owner's acceptance review of the Engineering Change.

Digital Engineer – Responsible for digital engineering aspects of the project that involve plant computer programs, digital equipment, software and/or firmware. This individual reviews deliverables that focus on hardware and software including schematics, software verification and validation, digital configuration management plan, disaster recovery plan, etc. This individual is familiar with the engineering methods used for platform application development and manufacturing to ensure the vendor is being properly evaluated. Although the Digital Engineer performing the activities resides with the vendor's integration organization, the licensee remains overall responsible and provides owner's acceptance of the documents.

Cyber Security Engineer – Responsible for performing Cyber Security Assessments for the new equipment and identifying Cyber Security design requirements. This individual ensures that the vendor is providing proper controls in the design to prevent or at least mitigate Cyber Security vulnerabilities in the Secure Operational Environment, as provided by the system and installed in the plant.

System Manager/Engineer – Owner of the system for which the equipment belongs and understands the requirements of the new equipment and impact to other systems.

Licensing Engineer – Responsible for ensuring that the system being designed remains within the bounds of the license, including UFSAR system description and UFSAR accident analyses.

Human Factors Engineer – Responsible for evaluating the appropriate human factors concerns for the modification and potential impacts on Operations, Maintenance, and Engineering staff.

Maintenance Engineer – Ensures that the system as implemented supports surveillance testing, calibration, troubleshooting, and other maintenance activities to ensure that the applicable maintenance procedures are updated appropriately for the new system.

Operations Representative – Responsible for conveying all Operations decisions to the project team and the Operations staff. Responsible for ensuring that Operations procedures are updated appropriately for the new system.

Vendor Integration Organization:

Project Manager – This individual is responsible for ensuring that the vendor integration organization remains on track for meeting schedule commitments, coordinating the vendor integration stakeholders to attend or to support the VOP visit, resolving each issue identified in the integration scope or ensuring that the vendor resolves issues in the vendor's scope, and controlling and managing change to minimize the impact on project resources.

Responsible Integration Engineer – Responsible for leading the team that develops the Engineering Change and the quality of the Engineering Change. This individual is responsible for coordinating of all technical aspects of the Engineering Change throughout the Engineering Change process.

Design Engineers – Provides design engineering for the various disciplines required to implement the Engineering Change (Digital, Electrical, Mechanical, Structural, etc.).

Platform Application Development Organization:

Project Manager – This individual coordinates vendor oversight visits at their facility, makes arrangements for the necessary vendor personnel to ensure adequate participation, tracks schedule and budget and reporting schedule and budget compliance within the vendor's organization (as well as initiating recovery actions as necessary), resolves each issue identified in the vendor's scope, and controls and manages change to minimize the impact on project resources.

Quality Manager – Maintains quality documentation or oversees maintenance of quality documentation and vendor process compliance, including Hardware and Software Design Process, Configuration Control, Software Verification and Validation (V&V), etc. This individual ensures that products meet the required level of quality.

Design Engineers – These hardware, software, and human factors engineers design, develop, implement, and test the project-specific equipment.

Test Engineers and Software V&V Engineers – Responsible to ensure the software is adequately tested and documented.

2. Development and Assessment of Potential Risk Factors

Potential Risk Factors were considered in accordance with EPRI Report 3002011816, Digital Engineering Guide (Reference 3), Table 5-1. The following topics were used to assess risk:

- Schedule – Schedule is reasonable with sufficient float to account for uncertainties **LOW RISK**
- Technical Staff – Familiar with plant and/or equipment, highly experienced with nuclear projects, low turnover **LOW RISK**
- Conceptual Design – Some deviations or exceptions from specification, some unique or First-of-a-Kind, and moderate complexity **MODERATE RISK**
- Hazards - Some hazards can lead to trips or transients **MODERATE RISK**
- Procurement - Several (3-5) internal or subvendor organizations **MODERATE RISK**
- Human Factors Engineering Vendor has an HFE program or plan that complies with applicable requirements, guides and standards **LOW RISK**

- Data Communications - Uses standard interfaces and protocols but has interchannel communication interfaces **MODERATE RISK**
- Cyber Security - Minor deviations from applicable cyber requirements, guides and standards; some compensating controls required **MODERATE RISK**
- Plant Integration Design - Uses standard interfaces, installation or construction methods **LOW RISK**
- Testing - Has proven test facilities and the system is designed to be testable and observable **LOW RISK**
- Configuration Management - Has a program that complies with applicable requirements, guides and standards **LOW RISK**

The above risks are continuously reassessed throughout the course of the project and changed as necessary.

3. <u>Determine performance measures and acceptance criteria</u>

Performance measures and acceptance criteria are comprised of **General Performance Measures**, based on the guidance in EPRI Report 1025283, Commercial-Grade Digital Equipment for High-Integrity Applications (Reference 2) and **Project-Specific Performance Measures** based on project-specific attributes that warrant vendor oversight.

General and Project-Specific Performance Measures are both evaluated during each vendor oversight visit and classified as Acceptable, Marginal, or Unacceptable. These results are then used as input to the appropriate level of oversight and oversight methods.

General Performance Measures

EPRI Report 1025283, Table 3-2, provides suggested vendor performance measures and acceptance criteria under the topics listed below.

<u>Hardware Design Control</u> – Verify there are no component issues found during inspection or test; no significant wiring, cabling or separation issues; no hardware-related design changes are necessary.

<u>Software/Firmware Lifecycle, V&V</u> – Reasonable lifecycle and effective V&V are demonstrated; few software changes evident and minor corrections only.

<u>Failure Analysis</u> - Failure analysis is timely and effective, and results confirmed via evaluation or test.

<u>Documentation</u> - No missing or conflicted documents and documents are clear and up to date.

Configuration Control - Hardware and software configuration items are identified; intended changes are timely and effective and no unintended or uncontrolled changes.

Corrective Actions - Low initiation threshold for Condition Reports (CR); corrective actions timely and complete and strong causal analysis.

Reporting - All hardware and software issues that could impact safety or critical functions are identified and reported in a timely manner.

Sub-Vendor Control - Effective and timely QA audits, surveys and surveillances and strong vendor oversight.

Project-Specific Performance Measures

Project Specific Performance Measures, identified below, are included in vendor oversight. The scope of vendor oversight is expected to continuously evolve during the project. For example, the vendor maintains a "Project Risk Mitigation" worksheet to identify risk, problem, and mitigation strategies. Project Specific Performance Measures that warrant vendor oversight are updated as this list changes.

Change control and management – Effective management of change to minimize schedule, budget, resource, and rework impacts. The assessment should include validating the commitments in the LAR for configuration management as described in DI&C-ISG-06 Section D.4.2.5, "Configuration Management Processes".

Quality Assurance - Verify that the Quality Assurance (QA) program used for logic implementation is effective in controlling the development process to assure quality of the application. The assessment should include validating the commitments in the LAR for software quality assurance as described in DI&C-ISG-06 Section D.4.2.3, "Software Quality Assurance Processes".

Regulatory Obligations – Ensure that vendors and their sub-suppliers explicitly comply with the requirements of Appendix B to 10 CFR Part 50 and 10 CFR Part 21 to control the quality of safety-related materials, equipment, and services. The assessment should include validating the commitments in the LAR for the I&C system development processes as described in DI&C-ISG-06 Section D.4, "I&C System Development Processes".

Plant Specific Action Items – Ensure that PSAIs identified in the Topical Report are implemented as part of the design as dispositioned in the LAR as described in DI&C-ISG-06, Section D.5.1.2, "Resolution of Topical Report Plant-Specific Action Items".

Time Response – Review relation between the specified time response requirements and the safety analysis response time assumptions listed in the UFSAR.

Accuracy and Uncertainty – Review the accuracy requirements and ensure that operating margin remains between normal operating conditions and protective limits, as driven by the relative accuracy and uncertainty of the equipment.

Configuration Verification - Verify that correct logic implementation is installed into the control system logic boards. Determine if this verification activity can be done with the system operable and if surveillance tests are performed to periodically verify correct logic implementation.

Software V&V - Verify that the application software V&V program complies with the V&V program approved by NRC for the LAR as described in DI&C-ISG-06, Section D.4.2.4, "Software Verification and Validation Processes", and that the V&V program is implemented in a manner that reliably verifies and validates the design outputs of each stage of the design process.

ASME NQA-1-2015, Subpart 2.7 – Review the requirements for the acquisition, development, operation, maintenance, and retirement of software for consistency with NQA-1-2015, Subpart 2.7.

Secure Development Environment (SDE) – Verify that the vendor has a development environment that complies with the requirements of Regulatory Guide (RG) 1.152, Revision 3, as approved by NRC for the LAR and associated vendor topical report (see DI&C-ISG-06, Section D.8, "Secure Development and Operational Environment"). Some key attributes to a SDE includes having a method for identifying the origin of critical components and ensuring that all critical asset components are compliant with the supplier's security requirements and free of counterfeits. Distribution paths shall use known, traceable, and reputable suppliers and distributors throughout the supply chain from component fabrication through delivery to the acquirer. Surplus, open box, or bid sites are considered untrusted sources. Ensure that the SDE and the vendor's design process produces a cyber-Secure Operational Environment (SOE).

Cyber Security - Review of activities associated with addressing system and services acquisition controls as set forth in the licensee's NRC-approved Cyber Security Plan, and in accordance with Section 73.54, "Protection of digital computer and communication systems and networks." This evaluates the SOE defined in RG 1.152, Revision 3, as approved by NRC for the LAR and associated vendor topical report (see DI&C-ISG-06, Section D.8, "Secure Development and Operational Environment").

4. Implement Appropriate Oversight Methods

Vendor oversight is based on risk and performance measures. Most of the vendor oversight activities occur after submittal of this LAR. Therefore, the amount and specific focus of the oversight activities vary as the project evolves. Vendor oversight occurs based on the various risk factors and performance measures described above.

LOW RISK factors (Section 2) and/or **ACCEPTABLE PERFORMANCE MEASURES** (Section 3) that indicate continued use of routine oversight methods, such as:

- Initial Audit
- Periodic Surveillances
- Routine Design Reviews
- Routine Project Meetings

MEDIUM RISK factors (Section 2) or **DEGRADED PERFORMANCE MEASURES** (Section 3) that indicate a need for supplemental oversight methods, such as:

- Increased surveillance frequency
- Interim design reviews
- Challenge boards
- Increased frequency of project meetings

HIGH RISK factors (Section 2) or **UNACCEPTABLE PERFORMANCE MEASURES** (Section 3) that indicate a need for extraordinary oversight methods, such as:

- Placement of oversight staff inside the vendor's organization
- Management intervention
- Stop work order and recovery plan

5. <u>Perform Corrective Actions</u>

Condition reports for entry into the corrective action program document vendor performance or quality that is in question. The following conditions, as a minimum, trigger a condition report:

- Vendor noncompliance with the vendor's own quality program, software processes, or hardware processes
- Nuclear safety may be adversely impacted if the digital item is installed and operated
- Unit generation may be adversely impacted if the digital item is installed and operated
- Digital item quality simply cannot be assured
- Digital item quality cannot be assured without a significant project delay
- Digital item quality is not assured, and identical or similar digital items are already installed in the facility, in other applications, and are considered operable or available

- The vendor has been awarded other POs or contracts to deliver other digital items, and performance measures indicate that the quality of the other items may not be assured

If the Project team or Vendor Oversight team identifies degraded or unacceptable performance or issues, oversight would be enhanced to include:

- Periodic meetings to discuss and resolve issues
- Additional technical reviews or surveillances
- Management Intervention
- Stop work and recovery plan

6. References

1. American Society of Mechanical Engineers (ASME), NQA-1:2015, Quality Assurance Requirements for Nuclear Facility Applications
2. Electric Power Research Institute (EPRI) Report 1025283, Commercial-Grade Digital Equipment for High-Integrity Applications, August 28, 2013
3. EPRI Report 3002011816, Digital Engineering Guide