



U.S. Department of Energy
Office of River Protection

P.O. Box 450, MSIN H6-60
Richland, Washington 99352

FEB 25 2008

08-ESQ-013

Mr. W. S. Elkins, Project Director
Bechtel National, Inc.
2435 Stevens Center Place
Richland, Washington 99354

Dear Mr. Elkins:

CONTRACT NO. DE-AC27-01RV14136 – REQUEST FOR ACTION ON ASSESSMENT REPORT A-07-ESQ-RPPWTP-017, BECHTEL NATIONAL, INC. (BNI) COMPUTER SOFTWARE QUALITY ASSURANCE (SQA)

Reference: 24590-WTP-QA-01-001, Revision 7b, "Quality Assurance Manual."

This letter forwards the results of the U.S. Department of Energy, Office of River Protection (ORP) assessment of BNI SQA conducted during the period of December 3 through 13, 2007, and requests action to correct the issues. The assessment evaluated implementation of the SQA requirements of the BNI Quality Assurance Manual (QAM) (Reference).

The assessment found BNI had an SQA program in place that adequately captured all the key requirements of the BNI QAM. However, the assessment did identify procedure implementation issues and some process and procedure weaknesses that require correcting for BNI to have a fully effective SQA program. The assessment noted that individuals performed appropriately despite the weaknesses in processes and procedures. No evidence was found that any of the weaknesses identified led to errors in calculations or other software output, but this must be confirmed by your evaluation of the findings. The assessment resulted in four findings, three observations, and one Assessment Follow-up Item (AFI).

Within 30 days of receipt of this letter you should respond to the assessment findings. For the findings, your response should include:

- The causes of the findings;
- The corrective actions that have been taken to control or remove any adverse impact from non-compliant conditions (remedial actions) and the results achieved;
- The corrective actions that will be taken to identify the extent of condition, correct the cause(s), and prevent further findings; and
- The date when all corrective actions will be completed, verified, and compliance to applicable requirements achieved.

Mr. W. S. Elkins
08-ESQ-013

-2-

FEB 25 2008

In addition to responding to the findings, you should explain what you will do in response to Observation A-07-ESQ-RPPWTP-017-O01 as it applies to Engineering procedures. ORP will address the AFI in a future visit.

If you have any questions, please contact me, or your staff may contact Samuel A. Vega, Office of Environmental Safety and Quality, (509) 373-1240.

Sincerely,



William J. Taylor, Assistant Manager
Office of Environmental Safety and Quality

ESQ:SAV

Attachment

cc w/attach:

A. M. Austin, BNI
D. J. Jantosik, BNI
D. E. Kammenzind, BNI
D. J. Pisarcik, BNI
R. R. Souther, BNI
D. J. Stroup, BNI
BNI Correspondence

U.S. DEPARTMENT OF ENERGY
Office of River Protection
Environmental Safety and Quality

ASSESSMENT: Bechtel National, Inc., Computer Software Quality Assurance

REPORT: A-07-ESQ-RPPWTP-017

FACILITY: Hanford Tank Waste Treatment and Immobilization Plant

LOCATION: Richland, Washington

DATES: December 3 through 13, 2007

ASSESSORS: Samuel A. Vega, Lead Assessor
David H. Brown, Assessor
Debra R. Sparkman, DOE-HQ Central Technical Authority, Technical Participant
Ronald C. Schrotke, Technical Participant

APPROVED BY: Patrick P. Carier, Lead Verification and Confirmation Team

Executive Summary

The U.S. Department of Energy (DOE), Office of River Protection conducted an assessment of Bechtel National, Inc. (BNI) computer Software Quality Assurance (SQA) from December 3 through 13, 2007. The assessment evaluated BNI's SQA program, SQA procedures, engineering procedures for using software, a sample of engineering calculations that used computer software, the SQA documentation for a sample of commercial computer codes, the development of plant instrument and control software, evidence of oversight, and other evidence of BNI's implementation of SQA requirements. The assessment compared BNI procedures and activities to the requirements of the BNI Quality Assurance Manual (QAM), 24590-WTP-QA-01-001. The QAM implemented DOE O 414.1B, "Quality Assurance," and was based on ASME-NQA-1-1989, "Quality Assurance Requirements for Nuclear Facilities," and ASME-NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications."

The assessment found BNI had a SQA program in place that adequately captured all the key requirements of the BNI QAM. However, the assessment did identify procedure implementation issues and some processes and procedures weaknesses that require correcting for BNI to have a fully effective SQA program. The assessment team found no evidence that any of the identified weaknesses led to errors in calculations or other software output, but this must be confirmed by BNI's evaluation of the findings.

The assessment team identified four findings as follows:

- **Finding A-07-ESQ-RPPWTP-017-F01:** Four spreadsheets used in engineering calculations were not used and controlled in accordance with the requirements of BNI procedures and the QAM;
- **Finding A-07-ESQ-RPPWTP-017-F02:** Computer programs used in engineering calculations were not always verified to show they produced correct solutions within defined limits for each parameter as required by the QAM;
- **Finding A-07-ESQ-RPPWTP-017-F03:** Software life cycle documentation did not comply with requirements of BNI procedures; and
- **Finding A-07-ESQ-RPPWTP-017-F04:** Configuration items were not placed on the baseline at the end of major life cycle phases as required by BNI procedures and the QAM.

The assessment also identified three observations which are discussed within this report. One of the observations identified the need for BNI to re-evaluate its procedure for engineering calculations to assure it specifies an appropriate, systematic process for checking calculations in which spreadsheets are used.

Table of Contents

Executive Summary	ii
Table of Contents	iii
List of Acronyms	iv
1.0 Details.....	5
2.0 Findings and Observations	18
3.0 Conclusion	24
Signatures	25
 Appendix A – Documents Reviewed	
 Appendix B – Personnel Contacted	

List of Acronyms

AFI	Assessment Follow-up Item
AI	Analog Input
BNI	Bechtel National, Inc.
C&I	Control and Instrumentation
CS&A	Civil, Structural, and Architectural
DOE	U.S. Department of Energy
FAT	Factory Acceptance Test
HLW	High-Level Waste
ICN	Integrated Control Network
IHLW	Immobilized High-Level Waste
IT	Information Technology
LAW	Low-Activity Waste
ORP	Office of River Protection
PES	Programmable Electronic System
PIN	Plant Information Network
PJM	Pulse Jet Mixer
PPJ	Programmable Protection System
PTF	Pre-Treatment Facility
QAM	Quality Assurance Manual
QAP	Quality Assurance Program
QAS	Quality Affecting Software
SAT	Software Acceptance Test
SEM	Software Engineering Methodology
SIS	Safety Instrumented System
SPP	Software Project Plan
SQA	Software Quality Assurance
SRS	Software Requirements Specification
SSRS	Safety System Requirements Specification
V&V	Verification and Validation
WESP	Wet Electrostatic Precipitator
WTP	Waste Treatment and Immobilization Plant

**U.S. Department of Energy (DOE), Office of River Protection (ORP)
Assessment of Bechtel National, Inc. (BNI)
Computer Software Quality Assurance (SQA)**

1.0 DETAILS

1.1 Program

Summary

The assessors reviewed computer software control procedures and procedures specifying when and how to use software. They compared the procedures to the requirements for SQA in 24590-WTP-QAM-QA-01-001, "Quality Assurance Manual" (QAM). The assessors found BNI had a SQA program in place that adequately captured all the key requirements of the BNI QAM. However, the assessment did identify procedure implementation issues and some processes and procedures weaknesses that require correcting for BNI to have an effective SQA program. These implementation issues and issues and procedure weaknesses are described in subsequent sections of this report.

SQA Program Preparing for Transition

The BNI QAM was based on ASME-NQA-1-1989, "Quality Assurance Requirements for Nuclear Facilities," and ASME-NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications." BNI was in the process of implementing DOE O 414.1C, "Quality Assurance," and ASME-NQA-1-2000, "Quality Assurance Requirements for Nuclear Facility Applications."

At the time of the assessment, ORP had reviewed BNI's draft Quality Assurance Program (QAP) documents, and determined BNI had resolved most comments satisfactorily. In preparation for approval of the new QAP, the Information Systems and Technology organization was developing a new SQA procedure set. The assessment team did not review or evaluate these procedures because ORP will evaluate them when ORP verifies implementation of DOE O 414.1C.

Procedures Require Improvement

The assessment team identified a number of weaknesses in the existing BNI procedures, including a need to improve the clarity of the process for checking calculations. Also, software life cycle documents prepared by BNI were not always consistent in providing the information required in the life cycle procedure; required information was not provided where the procedures indicated, or required information was missing. Observation A-07-ESQ-RPPWTP-017-O01 provides a complete list of the procedure weaknesses so that BNI may assure that similar weaknesses do not exist in the new procedure set. Despite implementation and procedure weaknesses noted, no evidence was found that any of the noted weaknesses led to errors in calculations or other software output. Interviews with BNI staff indicated BNI was aware of most of these weaknesses and was planning on addressing them in the new procedures.

BNI Conducts Software Oversight

The assessment team found that over the 18 months preceding this assessment BNI conducted one audit of computer SQA during February through March 2007. The audit was conducted by a team of six quality assurance auditors, and it appropriately identified issues. While the BNI audit did not identify the specific issues of this ORP report, it still provided management with an assessment of the overall status of the BNI SQA program. The assessment team also reviewed several surveillances of SQA conducted during the past year. These surveillances were focused on performance and did not assess SQA program effectiveness. The assessors determined BNI's SQA oversight was minimal, but met the QAM requirements.

Personnel Appropriately Trained, But Training Requirements Were Weak

The assessment team evaluated the training BNI provided to personnel who used some commercial software in design work, and found it was adequate. Training requirements were specified in individual training profiles, which were established as a result of management judgment. Minimum training requirements were not specified in SQA procedures and the software project plans did not always provide adequate training requirements. Sections 1.3 and 1.4 of this report contain examples where a desk instruction and some software project plans did not adequately specify training requirements. The problem with not adequately specifying training requirements is described in Observation A-07-ESQ-RPPWTP-017-O02.

Graded Approach in Transition

The assessment team reviewed the processes for applying the graded approach provided in 24590-WTP-GPP-IT-008, "Software Life Cycle Management," interviewed BNI staff and management responsible for implementing the procedure, and reviewed software life cycle documentation. The assessment team also reviewed procurement documentation to determine how grading was applied to the software and the procurements.

The assessment team found the grading criteria applied to SQA activities were inconsistent with the grading criteria in the BNI QAM. Section 3.3 of procedure 24590-WTP-GPP-IT-008 stated, "Grading allows for adjustment of the requirements if the activity does not add value or reduces risk," where the BNI QAM required a much broader consideration by requiring "controls and verifications applied to items and activities to be consistent with their importance to safety, cost, schedule, and success of the program associated with the item or activity. Implementation of DOE O 414.1C will resolve this issue because the implementation guide for safety software provided with this revision provided more direction for grading software. The problem of inconsistent application of the grading criteria is addressed in Observation A-07-ESQ-RPPWTP-017-O01.

1.2 Control and Use of Computer Programs in Engineering Calculations

Summary

The assessment team evaluated 24590-WTP-3DP-G04B-00037, "Engineering Calculations," and a sample of engineering calculations that were performed using both calculational software and compiled code. The Team found procedures did not adequately describe the processes for implementing engineering analysis and software checking requirements. As a result, analysis and checking activities did not always comply with QAM requirements. The assessment team also found four spreadsheet templates that were used as though they had been pre-verified as Quality Affecting Software (QAS) when they were not controlled in accordance with BNI's life cycle management requirements. The assessment team saw no evidence that the weaknesses and non-compliances led to errors in calculations. These procedure and implementation issues and issues are described in subsequent sections of this report.

Computer Programs Not Always Verified for Each Application

The assessors found evidence that not all calculations were verified to assure the application of the calculation program to the applied problems produced valid results. Also, some Verification and Validation (V&V) reports did not include sufficient information for originators and checkers to make the required verification. ASME-NQA-1-1989 and the QAM required that personnel verify applicability of each calculation program to the specific problem application to confirm the calculation program produces valid results.

24590-WTP-3DP-G04B-00037, "Engineering Calculations," Section 3.3.2, "Contents," required engineers preparing calculations to state the basis for applicability of the software to the specific physical problem. BNI management told the assessment team that this implemented the QAM requirement that mathematical models in computer programs be shown to produce valid solutions for the physical problem addressed by the computer programs. The V&V report for PIPE-FLO Professional provided example test cases, but never stated the bounding conditions of the tests. It did not state the range of pipe sizes, fluid pressures, or fluid flow rates for which the code was valid. Without this information, persons preparing calculations could not verify that the code was valid for their particular application. Other V&V reports also did not contain the necessary information. The problem of inadequate calculation verification is described in Finding A-07-ESQ-RPPWTP-017-F02.

Engineering Calculation Procedure Weaknesses

ASME-NQA-2a-1990 and the QAM provided two methods for using software in calculations – either pre-verifying the software or checking the results. This meant that software, such as a spreadsheet, required either a V&V and was subject to other life cycle documentation and controls, or the output had to be checked independently from the spreadsheet when the calculation was checked. There was no provision for mixing the two methods. Mixing the two methods can lead to errors if checkers rely on their own verification of the spreadsheet and are then distracted from independently verifying the accuracy of the results. Also, both methods provide protection from program execution errors like the ones recently identified by Microsoft

Corporation in Excel®¹ calculations, but mixing the two verification methods can defeat this protection.

Section 3.5.1, “Checking Methods” in procedure 24590-WTP-3DP-G04B-00037, “Engineering Calculations,” specified two methods for checking a calculation when the calculation used calculational software that was not pre-verified. These methods were a “mathematical check” and an alternate calculation method. For the mathematical check the procedure required the checker to confirm that all cell formulas, inputs, and outputs were correct. However, ASME-NQA-1-2000 and the QAM required that the checker only verify the inputs and outputs. While the procedure specified more than the minimum QAM requirements for this activity, requiring the checker to review the spreadsheet formulas distracts the checker from the specific requirement to verify the spreadsheet inputs and results. If the checker verifies the inputs and outputs are correct, there is no need to verify the cell formulas, and the checker is not tempted to rely on accuracy of the spreadsheet execution.

The Engineering Calculations procedure was confusing because Section 3.5.1 did not tell the checker what to do for pre-verified computer programs. Section 3.4, “Computer Applications,” discussed the use of pre-verified programs, but there was no link back to the related statement in Section 3.5.1, “Checking Methods.” As a result, an engineer following Section 3.5.1 verbatim for checking a calculation in a pre-verified spreadsheet; a QAS spreadsheets by definition. BNI verified QAS spreadsheets during the V&V process so these resource-consuming actions were unnecessary. The assessment team documented the issue of calculation procedure weaknesses in Observation A-07-ESQ-RPPWTP-017-O01.

Use of Incorrectly Controlled Spreadsheets in Engineering Calculations

The assessment team evaluated a sample of calculations performed using Excel spreadsheets and the Mathcad®² calculation program. Generally, engineers followed the procedure requirements that were specific for this type of calculational software. However, the Civil, Structural, and Architectural (CS&A) discipline had four spreadsheet templates that did not conform to the SQA requirements for documentation, V&V, and configuration management specified in BNI procedures. When the assessment team brought this issue to the attention of BNI, BNI management acted promptly to identify a resolution to the issue in condition report 24590-WTP-CRPT-07-170. The resolution was to develop QAS life cycle documents for the spreadsheet templates.

CS&A maintained the spreadsheet templates for engineers to use for rebar calculations. An example was 24590-PTF-DGC-S13T-00040, “Excel Spreadsheet Methodology and Example for Shear Wall Analysis.” This spreadsheet was complex and extensive, producing output on the order of 70 11” X 14” sheets. The template included documentation describing its method similar to that required for a pre-verified computer program. The CS&A organization maintained the template under an informal configuration management process so that, when an error was actually discovered in the template, CS&A submitted Corrective Action Report 24590-WTP-CRPT-QA-07-327 which provided a process to correct the error.

¹ Excel is a registered trademark of Microsoft Corporation

² Mathcad is a registered trademark of Parametric Technology Corporation

Because CS&A had not developed life cycle documentation nor subjected the spreadsheets to the formal BNI V&V process, the spreadsheet output should have been verified with each use. However, engineers checking calculations using the spreadsheet templates told the assessment team they trusted the spreadsheets and did not check their output. Based on how the spreadsheet templates were managed and used, the assessment team concluded they were actually pre-verified spreadsheets that should have been on the software baseline. They were not listed on the baseline and were not otherwise controlled in accordance with BNI SQA procedures for pre-verified software. The problem of the inadequately controlled spreadsheet templates is described in Finding A-07-ESQ-RPPWTP-017-F01.

1.3 Purchased Design and Analysis Software

Summary

The assessment team evaluated BNI's use of two purchased computer codes, ANSYS®³ and PIPE-FLO®⁴. The assessors found the codes were appropriately documented and controlled as specified in QAM Section 3.13, "Software Developed Not Using this Policy." BNI had issued project plans, V&V plans, and V&V reports for both codes. The vendors of both codes were contractually obligated to provide error notifications as required by ASME-NQA-2a-1990 and the QAM, and BNI evaluated the error notifications for applicability to BNI work. While overlooked in the PIPE-FLO project plan, BNI procedures required BNI to report errors identified by BNI to the vendors. Personnel using these codes were appropriately trained, although the assessment team judged the training requirements specified in project plans were not rigorous. In some cases, calculation packages developed using these codes did not document whether the analyst or checker had verified that the V&V bounded the problem being solved in the calculation as required to meet the requirements of the QAM. The problem of inadequate verification of program applicability is described in Finding A-07-ESQ-RPPWTP-017-F02.

ANSYS

ANSYS was a finite element analysis code that analyzed loads, stresses, temperatures, and other attributes of systems, structures, and components during engineering design activities.

The assessors reviewed a variety of documents, including the ANSYS project plan, ANSYS V&V documentation, procurement documentation, the licensing agreement, and one calculation in which ANSYS was used. They also interviewed management and personnel involved in documenting, using, and conducting configuration management of the application. BNI classified ANSYS as QAS.

Overall, the assessment team found that ANSYS was appropriately documented, was subject to appropriate V&V activities, and was under configuration control as specified in BNI procedures. The license agreement stated that the vendor's QAP implemented ASME-ASME-NQA-1, Subpart 2.7 requirements and provided for error reporting. The BNI ANSYS project plan also

³ Ansys is a registered trademark of Ansys, Inc.

⁴ PIPE-FLO is a registered trademark of Engineered Software, Inc.

provided for reporting of errors to the vendor as required by the BNI QAM. The assessors reviewed several vendor supplied error reports and the BNI review and analysis documentation packages that considered whether the errors impacted BNI activities. BNI's reviews and analyses determined that there was no impact from the error reports on BNI engineering work. BNI had not identified any errors and had not generated any error reports.

The assessors found that a calculation made using ANSYS did not state that it was verified to be valid over the range of parameters employed in the calculation as required by the QAM. The assessors also found that ANSYS users would be unable to find in the BNI ANSYS V&V report the information necessary to determine whether the range of V&V testing performed bounded a user's application. The problem of inadequate verification of program applicability is described in Finding A-07-ESQ-RPPWTP-017-F02.

PIPE-FLO

BNI used PIPE-FLO Professional®⁵ to perform the hydraulic calculations for design of systems carrying incompressible fluids and used PIPE-FLO Compressible®⁶ for designing systems carrying compressible fluids. BNI applied the requirements of QAM Section 3.13, "Software Developed Not Using This Policy," to the purchase the different PIPE-FLO products.

The assessment team evaluated BNI's use of PIPE-FLO Professional and PIPE-FLO Compressible. The assessors reviewed a variety of documents, including the PIPE-FLO project plans, PIPE-FLO V&V documentation, procurement documentation, and a calculation package that used both PIPE-FLO Professional and PIPE-FLO Compressible. They also interviewed management and personnel involved in documenting, using, and conducting configuration management of the applications. BNI classified both PIPE-FLO products as QAS.

Overall, the assessment team found that both PIPE-FLO products were appropriately documented, were subjected to appropriate V&V activities, and were under configuration control as specified in BNI procedures. The BNI PIPE-FLO Professional Project Plan provided for reporting of errors to the vendor as required by the BNI QAM. Mechanical and Process Engineering staff told the assessment team they had not identified any errors in PIPE-FLO Professional or PIPE-FLO Compressible during more than three years of use.

The assessors determined the project plan for PIPE-FLO software did not adequately specify training requirements appropriate for software of this complexity. The project plans stated, "Training is recommended but not required for a first time user." When discussed with BNI, Engineering management assured the assessors that their community of PIPE-FLO users was appropriately trained on the use of the code, and access to the code was limited to trained personnel and that this was just an inadequacy with the software life cycle documentation. The assessors did not have time to completely verify this BNI position. As a result, this problem of inadequately specifying training requirements is described in Observation A-07-ESQ-RPPWTP-017-O02.

⁵ PIPE-FLO Professional is a registered trademark of Engineered Software, Inc.

⁶ PIPE-FLO Compressible is a registered trademark of Engineered Software, Inc.

The PIPE-FLO Compressible Project Plan was missing the “Error Reporting” section required by 24590-WTP-GPP-IT-008, “Software Life Cycle Management.” Although the error reporting requirements were not addressed in the project plan, error reporting procedures were being implemented. BNI received and evaluated error notices from the vendor but had not identified any errors during their own use of the code. The assessment team considered the error reporting requirement missing from the project plan was an isolated situation and did not include it in a finding or observation.

1.4 Plant Instrument and Control Software

Summary

The assessment team evaluated BNI’s SQA, acquisition, development, and use of procedures; reviewed the software life cycle documentation associated with the Pulse Jet Mixer (PJM), Plant Information Network (PIN), Programmable Protection System (PPJ), Integrated Control Network (ICN), and Low-Activity Waste (LAW) Swabbing & Monitoring System Factory Acceptance Testing (FAT) applications; and interviewed personnel involved in development, maintenance, and use of these applications. The assessors found that software life cycle documentation did not meet BNI requirements, and configuration items were not placed on the configuration baseline at the end of major software life cycle phases.

Programmable Protection System

The PPJ is a Programmable Electronic System (PES) for safety applications used for Safety Instrumented Systems (SIS) at the Waste Treatment and Immobilization Plant (WTP). PPJ is a Tricon®⁷ triple modular redundant PES manufactured by Triconex®⁸. PPJ and its associated sensing and control elements will serve as an additional and separate layer of protection that monitors plant operating parameters. If the SIS, including portions of the PPJ, detects that specific plant parameters are not within the predefined set of safe conditions, the SIS will place the system(s) in a safe condition.

BNI divided the PPJ into four major subprojects: 1) Pre-treatment Facility (PTF); 2) LAW; 3) High-Level Waste (HLW); and 4) infrastructure system. The PPJ will be installed in each of the major facilities within the WTP (PTF, HLW, and LAW). PPJ will perform its safety functions independent of each facility’s basic process control system. This basic process control system is commonly referred to as the ICN. Unlike the ICN, the PPJ would perform its safety functions automatically with little or no operator intervention.

PPJ (and ICN) was composed of three computer system architectural layers:

- Application layer;
- Control element layer; and

⁷ Tricon is a registered trademark of Invensys, PLC

⁸ Triconex is a registered trademark of Invensys, PLC

- Computer system layer.

The application layer included custom developed software that will perform data management, complex logic, and user interface functions. The control element layer included reusable standard and user defined functions such as device drivers. BNI will use software within this layer across all facilities. The computer system layer was primarily the procured software that was used to develop the PPJ software and interfaces. This layer was based upon Tristation 1131⁹ and Matrikon¹⁰ software products. BNI was currently developing software for the control element layer.

The assessors reviewed the PPJ procurement package, 24590-QL-POA-JD03-00001, Revision 0, containing the acquisition requirements for Tristation 1131. BNI procured and received the development system environment for Tristation 1131 from the vendor, Triconex, using BNI's Q level procurement designation. The procurement package specified ASME-NQA-2a-1990 quality assurance requirements. BNI originally performed a supplier evaluation of Triconex in October 2002 and placed Triconex on their Approved Supplier List. Supplier Quality updated this qualification in April 2006 and scheduled a triennial audit for April 2009. BNI placed the Tristation 1131 software on the Project Information Technology (IT) baseline with a grading determination of non-QAS. BNI made this determination because the components of Tristation 1131 will not be installed on WTP computer systems. Instead, Tristation will be used to develop software that will be controlled under the QAS software life cycle processes.

The assessors reviewed 24590-WTP-PL-J-01-004, Revision 1, "Software Project Plan for Programmable Protection System." BNI was using 24590-WTP-GPP-IT-008 for PPJ implementation, although instrument and control software was excluded from this procedure's scope. The assessment team documented the issue of procedure inconsistencies in Observation A-07-ESQ-RPPWTP-017-O01.

The PPJ Software Project Plan (SPP) content was not consistent with the instructions provided in 24590-WTP-GPP-IT-008. The assessors observed the similar content inconsistencies in the PIN and ICN software project plans. The assessment team documented the issue of project plan content inconsistencies in Observation A-07-ESQ-RPPWTP-017-O03.

BNI generated SPPs for plant installed systems, including PPJ, early in the software life cycle. However, BNI suspended work on plant installed systems for approximately 18 months, so the PPJ and ICN software project plans required updating. The assessment team identified, and BNI acknowledged, the need for updating these documents. BNI had previously included an update to the ICN software project plan in the ICN Software Restart schedule beginning in December 2007.

The PPJ SPP content was not consistent with the instructions provided in 24590-WTP-GPP-IT-008. The content was confused between the "Objectives," "Purpose," and "Background" sections. The PPJ SPP "Control Element Layer" section (Section 2.2.2) and "Software Quality Assurance" section (Section 6.2.4) did not include the specific International Electrotechnical

⁹ Tristation 1131 is a registered trademark of Invensys, PLC

¹⁰ Matrikon is a registered trademark of Matrikon, Inc.

Commission and Institute of Electrical and Electronics Engineers standards that were specified for use in the development and validation activities by 24590-WTP-GPG-J-015, "Design Guide for Safety Instrumented Systems Implementation."

Procedure 24590-WTP-GPP-IT-008 required an installation plan and software configuration management plan for QAS developed software, but the PPJ SPP omitted these documents from the list of required software life cycle deliverables within the "Scope" section (Section 2.5). When the assessors discussed this with BNI, the contractor showed the assessors where, in other sections, the document explained that the inspection plan would be generated at a later time and as such was not part of the scope of the existing documents. The assessors felt this explanation clarified why the documents did not currently exist, but felt the installation plan was still a project deliverable and should not have been excluded from the list of final project deliverables.

The PPJ SPP also discussed configuration management in Section 7, "Software Configuration Management," where it referenced the use of a generic configuration management plan (as allowed by procedures), but did not include the specific WTP project design control procedures (24590-WTP-GPP-IT-005) that procedure 24590-WTP-GPP-IT-008 indicated must be used in the development phase. When discussed with BNI, the contractor indicated there was no problem because the procedure allowed the use of a generic configuration management plan. It was not clear to the assessors that this substitution allowed in the procedure included not using 24590-WTP-GPP-IT-005, and the team felt a configuration management plan should have been included as a project deliverable regardless of the fact that a generic one was used. The assessors found these documents confusing because 24590-WTP-GPP-IT-008 language clearly specified "required" documentation procedures to be followed, yet BNI allowed deviations not clearly stipulated in the procedures. The assessment team documented the problem of inconsistent software documentation in Observation A-07-ESQ-RPPWTP-017-003.

BNI developed safety system requirements specifications for six of the software applications associated with the PPJ during June through October 2005. The PPJ SPP stated that SIS software requirements would be included in a Safety System Requirements Specification (SSRS) and non-SIS in a Software Requirements Specification (SRS). The assessors reviewed two SSRS documents for compliance with ASME-NQA-2a-1990, Part 2.7 and BNI QAM requirements. BNI developed 24590-LAW-3PS-PPJ-T0010, "Safety System Requirements Specification for LAW Accident Monitoring," and 24590-LAW-3PS-PPJ-T0002, "Safety System Requirements Specification for LAW WESP High Level Interlocks" in accordance with 24590-WTP-GPG-J-015, Revision 0, "Design Guide for Safety Instrumented System Implementation." The LAW Accident Monitoring SSRS included requirements applicable to software control and human-machine interface, while the LAW Wet Electrostatic Precipitator (WESP) High Level Interlocks SSRS includes requirements applicable to software control.

Both of the SSRSs were inconsistent with 24590-WTP-GPP-IT-008, Revision 2, "Software Life Cycle Management," in that they did not include performance, interface, software environment, or data management requirements, nor did they include a requirements traceability matrix, the build/buy decision, user documentation, and testing requirements. The LAW WESP High Level Interlocks SSRS did not uniquely identify requirements, thus BNI will not be able to trace the requirements throughout the software life cycle.

BNI also included incomplete information in the LAW WESP High Level Interlocks SSRS, where they used question marks in place of a reference title. BNI checked, reviewed, and approved both SSRS. BNI had not generated either of these requirement specifications according to 24590-WTP-GPP-IT-008, ASME-NQA-2a-1990 or QAM requirements. The assessment team documented the problem of incomplete life cycle documentation in Finding A-07-ESQ-RPPWTP-017-F03.

ICN

The ICN sub-project managed the development of system-level functionality, configuration, and human-machine interfaces not associated with the specific sub-projects for the PTF, LAW, HLW or balance of facility sub-projects list in 24590-WTP-PL-J-01-003, "Software Project Plan for the Integrated Control Network."

The software life cycle requirements for ICN were specified in 24590-WTP-GPP-IT-008, "Software Life Cycle Management." The assessment team reviewed this procedure and two ICN-related life cycle documents, 24590-WTP-3PS-JD01-T0010, "Software Requirements Specification for ICN," and 24590-WTP-PL-J-01-003 "Software Project Plan for the ICN," and interviewed staff and management responsible for the ICN software.

Procedure 24590-WTP-GPP-IT-008, Appendix 4, explained that the primary goal of a software requirements specification was to develop a basis of mutual understanding between the system owner/user and the system developer/implementers about the application. The procedure also explained that the requirements specification was to provide traceability of requirements throughout the development of the software. To accomplish this, the appendix required requirement statements to have sufficient detail to be verifiable, consistent, and technically feasible.

The SRS for the ICN sub-project, 24590-WTP-3PS-JD01-T0010, described many of the requirements generically but lacked the detail required to ensure they would be verifiable, consistent, and technically feasible. For example, "A robust communications network supporting the control system infrastructure," was a system configuration requirement, and a requirement for alarms specified "Alarms shall be prioritized to ensure that a suitable level of operator attention is achieved." Both examples lacked sufficient detail to accomplish the intent of the requirements specification because they lacked sufficient detail to promote agreement, promote constant application, or allow for verification. Many of the requirement statements in this document had deficiencies similar to these two examples.

Procedure 24590-WTP-GPP-IT-008 contained an appendix for every software life cycle document specified in the procedure. Each appendix then provided a document format and direction as to what each section of the document was to address. The ICN SRS (24590-WTP-3PS-JD01-T0010) did not include all the content required in 24590-WTP-GPP-IT-008, Appendix 4. It did not address the required topics of interfaces, environmental/attributes, data management requirements, and data confidentiality/security. When asked about this, BNI did not provide an explanation of the deviation in the document as required by 24590-WTP-GPP-IT-008.

The ICN project plan (24590-WTP-PL-J-01-003) was another example where a document did not provide the required content. 24590-WTP-GPP-IT-008, Appendix 2 required the project plan to identify the specific standards and Software Engineering Methodology (SEM) that applied. The project plan was to identify the specific standards and SEM in Section 6.2.4, "Standards," but the ICN project plan did not provide or reference any development standards. Another example was in Section 7.0, "Software Configuration Management," of the project plan. WTP-GPP-IT-008, Appendix 2, required software characterized as "developed software" to be managed in accordance with procedure 24590-WTP-GPP-IT-005, "Project IT Change Control Process." The project plan did not specify this requirement.

BNI had developed routines that will be part of the ICN computer system layer which included reusable system components such as device drivers. The assessment team reviewed the life cycle documentation for one of these device drivers, 24590-WTP-3PS-JD01-T0119, Revision 0, "Routine Specification V1E Non Fail Last Position Valves." Document 24590-WTP-PL-J-01-003, Revision 001, "Software Project Plan for the Integrated Control Network," specified that 24590-WTP-GPP-IT-008, Appendix 1, would be used to fulfill the WTP documentation requirements for routines and macros. Document 24590-WTP-3PS-JD01-T0119, Revision 0, "Routine Specification V1E Non Fail Last Position Valves," contained description information, but did not include the requirements for the V1E routine. BNI also did not include the test results or other content associated with the test report section. BNI had checked, reviewed, and approved the V1E document without identifying these errors.

The assessment team documented the problem of incomplete life cycle documentation in Finding A-07-ESQ-RPPWTP-017-F03.

PJM Application

The PJM software will monitor and control the pressure within the PJM. The initial releases of the PJM software were used to establish design and operational parameters for multiple PJMs that will be permanent plant equipment. BNI designed the PJM software to monitor and control up to 12 PJMs each with five flush and five suction pressure transmitters.

Control and Instrumentation (C&I) used a project notebook for the PJM software to demonstrate that the software life cycle methodology was used in producing the software. The PJM project notebook includes sections for software requirements, system design, implementation, test plans and reports, user documentation, installation instructions, and operations and maintenance. C&I invoked a generic software configuration management plan, 24590-WTP-PL-J-01-002, "Control System Configuration Management Plan for Control Systems," for the PJM software. The PJM project notebook references three locations for functional requirements, including emails attached to the project notebook. However, the requirements traceability matrix within the project notebook captured the software requirements in a single section. C&I had organized the software design description section of the PJM project notebook in a similar manner, referencing three other documents and emails. The assessment team found this inconsistency with the guidance of 24590-WTP-IT-008 to be confusing. The PJM project notebook organization did not provide for ease in ensuring all software quality requirements as specified in 24590-WTP-IT-008, "Software Life Cycle Management," were met.

The PJM project notebook described three types of testing: Software Acceptance Testing (SAT), Pre-Factory Acceptance Testing, and FAT. SAT testing for PJM V0.0 was performed by an independent control system engineer with the PJM software developer nearby to respond to questions. The PJM project notebook cover sheet for the SAT included two signatures, both signing below the “Test Passed” and above their names and job position of “Control System Engineer.” The PJM project notebook did not indicate which of the individuals signing the test results performed the SAT. C&I identified the tester signature during interviews, but this was not evident in the test documentation. The assessment team documented the issue of project notebook inconsistencies in Observation A-07-ESQ-RPPWTP-017-O03.

After each SAT test was completed and prior to being placed under configuration management, BNI performed an independent check of the project notebooks. The Project Program Sponsor and Responsible Manager then reviewed and approved the PJM project notebooks after this checking was completed. The PJM notebook, including the documentation generated from each major software life phase, was not approved or placed under configuration management until the completion of the SAT. However, Section 3.10.1 of QAM Policy Q-03.2 required that configuration management be established at the end of earlier development phases. The assessment team documented the configuration management problems in Finding A-07-ESQ-RPPWTP-017-F04.

Test personnel redlined PJM SAT procedures in the PJM project notebook during the testing of PJM V0.0. BNI document the changes to those procedures in 24590-WTP-3PS-JD-0100 Revision 0, Routine Specification for PJM Control Software. BNI subsequently reviewed and approved those changes as typographical errors or minor omissions and/or errors in the test instructions.

C&I tested two of the five PJM routines, V1E and Analog Input (AI), separately from the PJM software acceptance testing documented in the PJM project notebook. The BNI document, 24590-WTP-3PS-JD-1-T0100, “Routine Specification for Pulse Jet Mixer Control Software,” Revision 1, stated “The routine [PJM] is comprised of various instantiations of two baselined routines (V1E and AI) and ... The software objects V1E and AI have been tested under ... and released ...” V1E and AI are device drivers developed by WTP that will be part of the permanent plant reusable library objects for the ICN. C&I was unable to locate the specific versions of V1E or AI included in the PJM application in 24590-WTP-RPT-IT-03-001, Revision 52, “Approved Project IT Software Baseline Report.” BNI did not place the specific versions of V1E or AI that were used in the PJM application on the WTP IT Project Baseline or on the Controls and Instrumentation configuration baseline. The assessment team documented the PJM configuration management problems in Finding A-07-ESQ-RPPWTP-017-F04.

C&I had earlier changed PJM’s designation to QAS and performed a crosswalk to the QAS requirements. C&I incorrectly designated PJM, a collection of five routines, as a routine rather than QAS non-Immobilized HLW (IHLW) software. As a result, they did not perform the required software life cycle processes, including document reviews, and did not generate the required software project plan or its equivalent in the PJM project notebook for developed QAS non-IHLW software. The assessment team documented the problem of inadequate life cycle documentation in Finding A-07-ESQ-RPPWTP-017-F03.

PIN Application

The PIN provides access to a collection of information to support the WTP operation and product data to the customer and regulatory bodies. PIN supports laboratory information management, waste tracking and inventory management, and data warehousing of process and production data. The PIN consists of three major subsystems: Laboratory Information Management System, the Waste Tracking and Inventory System, and the Plant Data Warehousing and Reporting Systems.

The assessors reviewed 24590-WTP-PL-J-01-005, Revision A, "Software Project Plan for Plant Information Network," and found it was not consistent with the requirements of 24590-WTP-GPP-IT-008. The PIN SPP had the same documentation deficiencies as the PPJ and ICN. Also, the PIN SPP "Cost and Schedule" section referenced the completion of PIN FAT in the second-half of 2004, but BNI had not completed the procurement and development of all PIN components at the time of this assessment, December 2007. The assessment team documented this issue of outdated life cycle documentation in Observation A-07-ESQ-RPPWTP-017-003.

LAW Facility Applications

BNI placed over thirty software tool applications on the Project IT baseline that will be used to conduct FAT testing of equipment for the LAW Facility. These applications used the project notebook approach to demonstrate that the software life cycle methodology was used in producing the software. The assessors reviewed one of these project notebooks, 24590-WTP-RPJ-J-0010 Revision A, "Software Project Notebook for ME39-SP-#222A LAW Swabbing & Monitoring System" and compared it to the requirements of 24590-WTP-GPP-IT-008. The LAW Swabbing & Monitoring project notebook included sections for software requirements, system design, implementation, test plans and reports, user documentation, installation instructions, and operations and maintenance. However, it did not include the build/buy decision as specified in the software requirements section of 24590-WTP-GPP-IT-008, Appendix 9, for non-QAS software. The assessment team documented the problem of inadequate life cycle documentation in Finding A-07-ESQ-RPPWTP-017-F03.

The assessors noted redline markup in the SAT section of the LAW Swabbing & Monitoring project notebook, changing the specific version identifier used for the module referred to as the FB_Constants ABB library. C&I investigated this change during the assessment period and determined that the vendor provided a version update to this library module during the year between when the SAT procedure was developed and when it was executed. The assessment team did not determine if this was consistent with QAM document control requirements, but identified the issue for follow-up in Assessment Follow-up Item (AFI) A-07-ESQ-RPPWTP-017-AFI01.

BNI's graded approach specified in 24590-WTP-GPP-IT-008 required the computer hardware and software configurations to be documented in the test report for QAS applications, but it was not specific if this information was required for non-QAS applications. BNI did not include the hardware and software configuration in the LAW Swabbing & Monitoring project notebook. The LAW Swabbing & Monitoring notebook, including the documentation generated from each major software life phase, was not approved or placed under configuration management until the

completion of the SAT. The assessment team documented this deficiency in Finding A-07-ESQ-RPPWTP-017-F04.

2.0 FINDINGS AND OBSERVATIONS

Finding A-07-ESQ-RPPWTP-017-F01: Four spreadsheets used in engineering calculations were not used and controlled in accordance with the requirements of BNI procedures and the QAM.

Requirements:

- a. 24590-WTP-QAM-01-001, Revision 7b, Policy Q-03.1, Section 3.5.6 stated, "...computer program acceptability shall be pre-verified or the results verified with the design analysis for each application."
- b. 24590-WTP-GPP-IT-001, Revision 5, Section 4.2 stated, "This section defines the process for qualifying software for use in performing quality-affecting work. The process ensures that software used in quality-affecting work is limited to software applications obtained from a software configuration management process."

Discussion:

Contrary to these requirements, the CS&A organization had four spreadsheet templates for designing concrete rebar placements that did not have the required BNI software life cycle documentation. CS&A had conducted V&V activities and placed the templates in an ad hoc configuration management process, but these did not conform to the BNI software life cycle documentation requirements and the spreadsheet templates were not on the BNI software baseline.

Engineers who used the templates in facility design said they trusted the validity of the spreadsheets and did not check their output. While CS&A management considered the spreadsheet templates were non-QAS software, their organization was using the software in a manner consistent with documented, pre-verified, and baselined QAS software.

The four spreadsheet templates were:

- 24590-PTF-DGC-S13T-00040, Revision 0d, "Excel Spreadsheet Methodology and Example for Shear Wall Analysis;"
- 24590-HLW-DGC-S13T-00050, Revision 00B, "Excel Spreadsheet Methodology and Example for Shear Wall Analysis;"
- 24590-HLW-DGC-S13T-00051, Revision 00D "Excel Spreadsheet Methodology and Example for Slab Analysis;" and
- 24590-PTF-DGC-S13T-00041, "Excel Spreadsheet Methodology and Example for Slab Analysis."

Finding A-07-ESQ-RPPWTP-017-F02: Computer programs used in engineering calculations were not verified to show they produced correct solutions within defined limits for each parameter as required by the QAM.

Requirements:

- a. 24590-WTP-QAM-01-001, Revision 7b, Policy Q-03.1, Section 3.5.7 stated, “The computer program shall be verified to show it produces correct solutions for the encoded mathematical model within defined limits for each parameter employed. The encoded mathematical model shall be shown to produce a valid solution to the physical problem associated with the particular application.”
- b. 24590-WTP-3DP-G04B-00037, Revision 11, “Engineering Calculations,” Section 3.3.2 stated, “The calculation ... shall identify any computer calculations, including ... the basis (or reference thereto) for supporting applicability of the software application to the specific physical problem.”

Discussion:

Contrary to these requirements, engineers preparing and checking calculation packages did not always verify that V&V testing bounded the problem they were solving. Also, some V&V reports evaluated by the assessment team did not provide sufficient information for engineers using the computer programs to make this determination. The assessment team based its conclusion on the following:

- Calculation package 24590-LAW-M2C-M80T-00001, Revision 00A, “LAW Melter Lid Stress Analysis,” did not provide evidence that the computer program used in the analysis (ANSYS) had been verified within defined limits for each parameter applicable to this calculation. The calculation made reference to the V&V report, but there was no evaluation to establish that limits bounding the calculation were tested or otherwise verified for the code;
- Calculation package 24590-HLW-M6C-PWD-00007, Revision A, “Line Sizing Calculation for the Plant Wash and Disposal System,” did not provide evidence that the computer program used in the analysis (PIPE-FLO Professional) had been verified within defined limits for each parameter applicable to this calculation. The calculation made reference to the V&V report, but there was no evaluation to establish that limits bounding the calculation were tested or otherwise verified for the code;
- Life cycle document 24590-WTP-VV-ENG-03-0001, Revision 3, “Control Valve Sizing for Liquid Service – QAS Routine,” did not state the range of parameter values for which the spreadsheet routine was valid. The routine was tested for parameters such as temperatures, densities, vapor pressures, thermodynamic critical pressures, viscosities, inlet pressures, outlet pressures, and flow rates. However, the assessment team was unable to use the document to verify that testing bounded any specific calculation; and

- The V&V report 24590-WTP-VV-M-01-001, Revision 6, “Verification and Validation Report for PIPE-FLO Professional Version 2005,” did not provide a clear statement regarding the limits of V&V testing for all parameters employed, such as pipe diameters, flow rates, and pressures. The V&V report did provide a clear summary of what was tested, but it did not state if the test values constituted limits on the validity of the software. When testing was conducted for 2”, 10”, and 24” piping, the report did not state if the code was valid, for example, for 28” piping.

Finding A-07-ESQ-RPPWTP-017-F03: Software life cycle documentation did not comply with requirements of BNI procedures.

Requirements:

- a. 24590WTP-GPG-IT-006, Revision 0, “Glossary of Terms for Software Quality,” stated, “Routine – A collection of computer macros or scripts, a spreadsheet application, or other standalone software (either acquired or developed) that operates within Commercial Off The Shelf Software, such as spreadsheets. Routines are software.”
- b. 24590-WTP-GPP-IT-008, Revision 2, “Software Life Cycle Management,” Appendix 4: “Software Requirements Specification,” stated, “Requirements documentation shall be completed, reviewed and approved prior to the approval of Design Specifications.”
- c. 24590-WTP-GPP-IT-008, Revision 2, “Software Life Cycle Management,” Appendix 1, stated, “The following formats are suggested for QAS routines and macros life cycle documents: if an alternative format is used, the content described below is to be included, if applicable. If the content below is determined to not be applicable to the routine, document justification for not including that item that section of the life cycle document. ... 5.0 Test Report ...”
- d. 24590-WTP-GPP-IT-008, Revision 2, “Software Life Cycle Management,” Appendix 4, stated, “The SRS describes all the various requirements for the system, including functionality, performance, network, security, and implementation. This specification should have detailed requirements that are verifiable, consistent, and technically feasible. The following items are requirements for the Software Requirements Specification document...”
- e. 24590-WTP-GPP-IT-008, Revision 2, “Software Life Cycle Management,” Appendix 9, stated, “... If an items listed in the template is omitted, the item label should be included in the document and a justification for omission in that section of the life cycle document. 2.0 Software Requirements Specification ... Build/buy decision.”
- f. 24590-WTP-GPP-IT-008, Revision 2, “Software Life Cycle Management,” Section 3.5.7B, stated, “If new software is being developed for the project (Developed Software): ... Complete the deliverables for one of the following: If QAS - (See Appendix for required format).”

Discussion:

BNI did not develop software project plans, software requirements specifications, and software test documentation according to these requirements. This occurred when Engineering did not use the proper grading determination for the PJM application, and thus did not perform the required reviews.

- C&I did not use the correct software grade determination for PJM and thus did not perform the required software life cycle processes and did not generate the required software project plan.
- C&I issued 24590-LAW-3PS-PPJ-T0010, "Safety System Requirements Specification for LAW Accident Monitoring," and 24590-LAW-3PS-PPJ-T0002, "Safety System Requirements Specification for LAW WESP High Level Interlocks" without implementing the software quality assurance requirements in 24590-WTP-GPP-IT-008.
- C&I did not include the requirements, test results or other content associated with the test report section in V1E Non Fail Last Position Valves project notebook.
- C&I did not include the build/buy decision in the LAW Swabbing & Monitoring project notebook.

Finding A-07-ESQ-RPPWTP-017-F04: Configuration items were not placed on the baseline at the end of major life cycle phases as required by BNI procedures and the QAM.

Requirements:

- a. ASME-NQA-2a-1990, "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications," Part 2.7, Section 5.1 stated, "A configuration baseline shall be defined as the completion of each major phase of the software development."
- b. 24590-WTP-QAM-01-001, Revision 7b, Policy Q-03.2, Section 3.10.1 stated, "A configuration baseline shall be defined at the completion of each major phase of the software development and include appropriate control points within each major phase. Approved changes created subsequent to the baseline shall be added to the baseline ..."
- c. 24590-WTP-QA-01-001, "Quality Assurance Manual," Policy Q-03.2, "Software Quality," Section 3.10.1 stated, "A configuration baseline shall be defined as the completion of each major phase of the software development."
- d. 24590-WTP-GPP-IT-008, Revision 2, "Software Life Cycle Management," Section 3.5.8, stated, "Upon acceptable validation of developed software, the software shall be baselined and controlled per 24590-WTP-GPP-IT-005, 'Project IT Change Control Process.'"

Discussion:

Contrary to these requirements, BNI's C&I organization used project notebooks to collect software life cycle documentation, but did not approve or place the software requirements or software design life cycle phase documentation under configuration management until the completion of the software acceptance testing phase. ASME-NQA-2a-1990, the QAM, and BNI SQA procedures required the configuration items to be placed under control at the end of each major life cycle phase. The assessment team based its conclusion on the following:

- The PJM project notebook contained software life cycle configuration items that were not approved or placed under configuration management at the software requirements, system design, and implementation phases. They were not placed under configuration management until after the software acceptance testing phase;
- BNI did not place the specific versions of VIE or AI that were used in the PJM application on the WTP IT Project Baseline or on the Controls and Instrumentation configuration baseline; and
- The LAW Swabbing & Monitoring notebook was not approved or placed under configuration management at the software requirements, software design, and implementation phases. It was only placed under configuration management at the completion of the software acceptance testing phase.

Observation A-07-ESQ-RPPWTP-017-O01: Procedures contained inconsistencies and ambiguities, and needed information was missing.

Discussion:

The assessment team evaluated the Engineering and IT procedure sets and found a number of ambiguities and inconsistencies. BNI had updated draft procedures but had not issued them prior to the assessment. BNI stated the new procedures would address some of the issues identified by the assessment team, but the assessment team did not review IT's new procedures. The Engineering procedures were not in the scope of BNI's procedural updates and were not addressed by the recent BNI procedure activities. The inconsistencies and ambiguities were:

- 24590-WTP-3DP-G04B-00037, "Engineering Calculations," Section 3.3.2, "Contents," did not fully describe the responsibility of persons preparing and checking calculations to assure computer programs were verified to be valid for the range of parameters employed during the calculation;
- 24590-WTP-3DP-G04B-00037, "Engineering Calculations," Section 3.5.1, "Checking Methods," did not specify the process for checking a calculation made using pre-verified software;
- The 24590-WTP-GPG-IT-006, "Glossary of Terms for Software Quality," the use of the term non-QAS was misleading because it implied that software designated as non-QAS did not affect quality. In fact, the output of some non-QAS software did affect quality, but the

output was subject to independent verification. Also, the application of the term “quality affecting” is not consistent with DOE requirements and Nuclear Quality Assurance;

- The graded approach described in 24590-WTP-GPP-IT-008, “Software Life Cycle Management,” was based upon “adding value” rather than on importance to safety, cost, schedule, and success of the project as specified in the QAM and DOE O 414.1B;
- 24590-WTP-IT-008, “Software Life Cycle Management,” and 24590-WTP-GPP-IT-014 used the title/role of the Chief Information Officer rather than the title/role used in the ORG-HR-01-001, “Project Management Organization;”
- 24590-WTP-QAM-QA-01-001, “Quality Assurance Manual,” used different titles/roles for the Deputy Project Manager, Operations and Assurance and the Deputy Project Manager, Business Services than the titles/roles used in the ORG-HR-01-001, “Project Management Organization;”
- 24590-WTP-GPP-IT-001, “Use of Quality Affecting Software Applications,” specified process steps applicable to all quality affecting software but that were inappropriate for instrument and control system software installed in the plant;
- 24590-WTP-GPP-IT-008, “Software Life Cycle Management,” excluded C&I software, but C&I stated this procedure was required for PPJ and ICN software;
- 24590-WTP-GPP-IT-008, “Software Life Cycle Management,” specified review and approval criteria based on if the software was designated as QAS or non-QAS rather than the grading criteria specified in the BNI QAM; and
- The BNI “List of Qualified Individuals” contained only the first name, last name, and middle initials of individuals. The list did not state what activities or responsibilities personnel were qualified to perform.

Observation A-07-ESQ-RPPWTP-017-O02: Specified training requirements were weak.

Discussion:

The assessment team found that, for the individuals they verified, personnel performing activities affecting software quality were appropriately trained. However, training requirements specified in software project plans were weak and require improvement. The assessment team based its conclusions on the following:

- The C&I organization desk instruction on notebooks stated inappropriately that personnel were adequately trained and qualified simply because they are members of C&I; and
- The project plans for PIPE-FLO Professional and PIPE-FLO Compressible (24590-WTP-PL-M-02-006, Revision 2 and 24590-WTP-PL-M-02-002, Revision 2) stated inappropriately, “Training is recommended but not required for a first time user.”

Observation A-07-ESQ-RPPWTP-017-O03: BNI's Control and Instrumentation software project plans and software project notebooks are out of date and were inconsistent with BNI guidance.

Discussion:

The assessment team identified several BNI implementation documents that were out-of-date, were confusing, or lacked the detail required to effectively perform all phases of the software life cycle development.

- The BNI PJM project notebook organization did not provide ease in ensuring BNI's software quality requirements would be met. Requirements and design descriptions each referenced three separate locations for details. Content of Revision B was changed but sections within the revised document that referenced page numbers prior to the revision were not updated.
- The PJM project notebook did not identify the individuals who performed the acceptance testing.
- The PIN, PPJ, and ICN software project plans were generated prior to a hold being placed on WTP work. They needed to be updated to reflect current schedules.
- The PIN and PPJ software project plans did not follow the organizational and content guidelines in 24590-WTP-GPP-IT-008.

AFI A-07-ESQ-RPPWTP-017-AFI01: Verify that Engineering followed document control requirements during testing of the LAW Swabbing and Monitoring software.

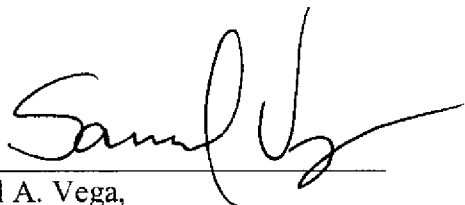
Discussion:

At the time of the assessment fieldwork, it was not clear that all red-lined changes in the LAW Swabbing and Monitoring notebook test procedures were "minor changes" as defined in QAM Policy Q-06.1-3, Section 3.4. Changes that are not minor changes must follow BNI document control procedures. ORP will verify, when DOE O 414.1C safety software implementation is assessed, that these changes in the LAW Swabbing and Monitoring notebook test procedures were adequately incorporated in accordance to BNI document control procedures.

3.0 CONCLUSION

The assessment found BNI had a SQA program in place that adequately captured all the key requirements of the BNI QAM. However, the assessment did identify procedure implementation issues and some processes and procedures weaknesses that require correcting for BNI to have a fully effective SQA program. The assessment team found no evidence that any of the weaknesses identified led to errors in calculations or other software output, but this must be confirmed by BNI's evaluation of the findings.

Signatures



Samuel A. Vega,
Lead Assessor



Patrick P. Carier, Lead
Verification and Confirmation Team

Appendix A
Documents Reviewed

Documents Reviewed

Calculation Packages

- 24590-PTF-DGC-S13T-00040, Revision 0D, “Excel Spreadsheet Methodology and Example for Shear Wall Analysis.”
- 24590-HLW-M6C-PWD-00007, Revision A, “Line Sizing Calculation for the Plant Wash and Disposal (PWD) System.”
- 24590-LAW-M2C-M80T-00001, Revision 00A, “LAW Melter Lid Stress Analysis.”
- 24590-PTF-DGC-S13T-00024, Revision A, “El 56’ Slab Design for PT Building – Bounded by Col Lines 17 thru 24.5.”
- 24590-HLW-DGC-S13T-00113, Revision A, “Design of Concrete Walls El 0’ to 14’ – Bounded by Col Lines 16.5 thru 20 and C thru S.”
- 24590-HLW-M6C-PWD-00007, Revision A, “Line Sizing Calculation for the Plant Wash and Disposal (PWD) System.”
- 24590-LAB-JVC-C2V-00003, Revision A, “Control Valve Calculation Tag No. LAB-C2V-TV-6114B.”
- 24590-LAB-JVC-C2V-00009, Revision B, “Control Valve Calculation Tag No. LAB-C2V-TV-6142B.”
- 24590-LAB-JVC-C2V-00013, Revision B, “Control Valve Calculation Tag No. LAB-C2V-TV-6155.”
- 24590-LAB-JVC-C2V-00014, Revision B, “Control Valve Calculation Tag No. LAB-C2V-TV-6157.”
- 24590-LAB-JVC-C2V-00015, Revision A, “Control Valve Calculation Tag No. LAB-C2V-TV-6159.”
- 24590-LAB-JVC-C5V-00013, Revision B, “Control Valve Calculation Tag No. LAB-C2V-TV-6130.”
- 24590-LAB-JVC-CHW-00001, Revision B, “Control Valve Calculation Tag No. LAB-CHW-FV-6182.”
- 24590-LAW-JVC-PCW-00002, Revision C, “Control Valve Calculation Tag No. PCW-FV-2234.”
- 24590-LAW-M2C-M80T-00001, Revision 00A, “LAW Melter Lid Stress Analysis.”

- 24590-PTF-DGC-S13T-00024, Revision A, “El 56’ Slab Design for PT Building – Bounded by Col Lines 17 thru 24.5.”
- 24590-PTF-DGC-S13T-00040, Revision 0D, “Excel Spreadsheet Methodology and Example for Shear Wall Analysis.”
- 24590-WTP-S0C-S15T-00021, Revision A, “Breakpoint Coupled Analysis.”
- 24590-WTP-S0C-S15T-00023, Revision 0, “Strength Adequacy Evaluation of Bond Between Steel Decking and Concrete Platforms in HLW and PTF Facilities.”

Computer Program Life Cycle Documents

- 24590-ITC-IT-06-0037, Revision 1, “IT Change Request (PJM Control Software V0.0b).”
- 24590-ITC-IT-25-0225, Revision 0, “IT Change Request (PJM Control Software V0.0).”
- 24590-LAW-3PS-PPJ-T0002, Revision A, “Safety System Requirements Specification for LAW WESP High Level Interlocks.”
- 24590-LAW-3PS-PPJ-T0010, Revision A, “Safety System Requirements Specification for LAW Accident Monitoring.”
- 24590-QL-POA-JD03-00001, Revision 0, “Programmable Protection System Procurement Package.”
- 24590-WTP-3PS-JD01-T0010, “Software Requirements Specification for ICN.”
- 24590-WTP-3PS-JD01-T0100, Revision 1, “Routine Specification for Pulse Jet Mixer (PJM) Control Software.”
- 24590-WTP-3PS-JD01-T0119, Revision 0, “Routine Specification V1E Non Fail Last Position Valves.”
- 24590-WTP-ITC-IT-05-0050, Revision 0, IT Change Request for PIPE-FLO Professional 2005.
- 24590-WTP-ITC-IT-05-0081, Revision 0, IT Change Request for Ansys, Version 9.
- 24590-WTP-ITC-IT-05-0175, Revision 0, IT Change Request for PIPE-FLO Compressible 2005.
- 24590-WTP-ITC-IT-06-0105, Revision 0, IT Change Request for Safety Analysis Inputs Database.
- 24590-WTP-ITC-IT-07-0239, Revision 1, IT Change Request for Ansys, Version 11.

- 24590-WTP-ITC-IT-07-0270, Revision 1, IT Change Request, “Component Information System.”
- 24590-WTP-ITC-IT-07-0326, Revision 1, IT Change Request for Flowel.
- 24590-WTP-ITC-IT-07-183, Revision 1, IT Change Request, “Component Information System.”
- 24590-WTP-PL-J-01-002, Revision 1, “Control System Configuration Management Plan for Control Systems.”
- 24590-WTP-PL-J-01-004, Revision 1, “Software Project Plan for Programmable Protection System.”
- 24590-WTP-PL-J-01-005, Revision A, “Software Project Plan for Plant Information Network.”
- 24590-WTP-PL-M-01-0005, Revision 1, “Software Application Test Plan for PIPE-FLO Professional Version 2005.”
- 24590-WTP-PL-M-01-001, Revision 6, “Verification and Validation Report for PIPE-FLO Professional Version 2005.”
- 24590-WTP-PL-M-02-002, Revision 2, “Project Plan for PIPE-FLO Compressible Version 2005.”
- 24590-WTP-PL-M-02-006, Revision 2, “Project Plan for PIPE-FLO Professional Version 2005.”
- 24590-WTP-PL-M-02-007, Revision 2, “Software Requirements Specification for PIPE-FLO Professional Version 2005.”
- 24590-WTP-QAS-IT-02-023, Revision 2, QAS Application Form, PIPE-FLO Compressible 2005.
- 24590-WTP-QAS-IT-03-001, Revision 2, QAS Application Form, PIPE-FLO Professional 2005.
- 24590-WTP-QAS-M-02-003, Revision 3, QAS Application Form, Ansys Version 9.
- 24590-WTP-QAS-M-06-001, Revision 2, QAS Application Form, Ansys Version 11.
- 24590-WTP-RPT-IT-03-001, Revision 52, “Approved Project IT Software Baseline Report.”
- 24590-WTP-RPT-IT-03-002, Revision 44, “Approved Project Software Designation List.”

- 24590-WTP-RPT-J-04-0010, Revision B, “Software Project Notebook for LAW Swabbing & Monitoring System.”
- 24590-WTP-RPT-J-05-172, Revision A, “Software Project Notebook for Pulse Jet Mixer Controls Testing.”
- 24590-WTP-RPT-J-05-172, Revision B, “Software Project Notebook for Pulse Jet Mixer Controls Testing.”
- 24590-WTP-SWLCD-ENG-05-0028-01, Revision 2, “Component Information System Non-QAS Software Lifecycle Documentation.”
- 24590-WTP-SWLCD-ENG-05-0028-02, Revision 2, “Component Information System (Non-QAS) Test Plan and Test Results.”
- 24590-WTP-VV-ENG-03-001, Revision 3, “Control Valve Sizing for Liquid Service – QAS Routine.”
- 24590-WTP-VV-ENG-03-002, Revision 3, “Control Valve Sizing for Gas Service – QAS Routine.”
- 24590-WTP-VV-ENG-03-003, Revision 4, “Control Valve Sizing for Steam Service – QAS Routine.”
- 24590-WTP-VV-PS-02-001, Revision 4, Verification and Validation Plan for “ANSYS.”
- 24590-WTP-VV-PS-02-002, Revision 4, Verification and Validation Report for “ANSYS.”
- 24590-WTP-VV-PS-02-002, Revision 8, Verification and Validation Report for “ANSYS” Version 11.
- 24590-WTP-VV-PS-02-003, Revision 1, “ANSYS Project Plan” (Version 9).
- 24590-WTP-VV-PS-02-003, Revision 3, “ANSYS Project Plan” (Version 11).
- 24590-WTP-VV-PS-07-001, Revision 0, “Individual QAS Computers JO05774 and JO04004 Verification and Validation Report for Ansys Ver. 11.”
- BNI-RPP-WTP ASL Search, “BNI-RPP-WTP Supplier Quality – Invensys-Triconex.”
- CCN: 154224, “CIS Component Information System (Non-QAS) Test Plan and Test Results.”

Condition Reports

- 24590-WTP-CRPT-QA-07-089, Revision 0.
- 24590-WTP-CRPT-QA-07-103, Revision 0.
- 24590-WTP-CRPT-QA-07-104, Revision 0.
- 24590-WTP-CRPT-QA-07-114, Revision 0.
- 24590-WTP-CRPT-QA-07-170, Revision 0.
- 24590-WTP-CRPT-QA-07-172, Revision 0.
- 24590-WTP-CRPT-QA-07-327, Revision 0.

Correspondence

- BNI Internal Memorandum, CCN: 148349, R. R. Souther to Distribution, "Information Technology Change Board Appointments."
- BNI Internal Memorandum, CCN: 166071, R. R. Souther to Distribution, "Plant Installed Software Change Board Appointments and Formation Meeting."
- BNI Internal Memorandum, CCN: 162092, John F. Schneider to Distribution, "Engineering Software Use in Response to CRPT 24590-WTP-CRPT-QA-07-170, Action 9," dated November 15, 2007.
- BNI Internal Memorandum, CCN: 156969, Leslie E. Woodside to Antoinette Austin and Ryan Souther, "Review of WTP Software Licenses January-June, 2007," dated July 16, 2007.
- BNI Internal Memorandum, CCN: 131144, Kirby Oldfather to John Minichiello, "Closure of CAR 06-84, Action 03," dated July 26, 2006.
- BNI Internal Memorandum, CCN: 142093, B. F. Busch to Antoinette Austin, "Closure of CAR 06-84 Action 03," dated July 18, 2006.
- Email April 04, 2005, 9:23am, Billings to Meinert, "RE: Software Object Approval for Placement on the C&I Project Baseline (Element Library Version 1.1-0)."
- Email April 04, 2005, 9:24am, Billings to Meinert, "RE: Software Object Approval for Placement on the C&I Project Baseline (Device Driver Library Version 1.1-0)."
- Email April 04, 2005, 1:04pm, Billings to Meinert, "RE: Software Object Approval for Placement on the C&I Project Baseline (FB_Constants Library Version 1.2-0)."

Internal Assessments

- 24590-WTP-IAR-QA-07-0002, Revision 0, “Internal Audit of Software Quality and Electronic Data Management.”

Miscellaneous

- Calculation procedure compliance checklist for 24590-WTP-S0C-S15T-00021.
- Calculation procedure compliance checklist for 24590-WTP-S0C-S15T-00023.
- Calculation procedure compliance checklist for 24590-WTP-DGC-S13T-00040.
- Calculation procedure compliance checklist for 24590-WTP-DGC-S13T-00113.
- Monthly IT Change Management Review Presentations for March, April, August, September 2007.
- 24590-WTP-RPT-IT-07-002, Revision 3, “Tracked Database List Report,” November 5, 2007.
- BNI Crosswalk, IT-008 to the QAM and Quality Assurance Requirements Document.
- Blanket Master Contract 9951, CH2M HILL Hanford Group, Inc. and Engineered Software, Inc., January 24, 2001, “PIPE-FLO PROFESSIONAL 6 License.”
- ANSYS, Inc. Quality Assurance Service Agreement, effective October 5, 2007.
- Organization Chart, WTP Engineering Organization.
- Augmented Monitoring of Employee Worksheet (for two employees).
- Calculation Checklist for 24590-LAB-JVC-CHW-00001.
- Organization Chart, WTP Project Management.
- 24590-WTP-LQI-001, Revision 137, “List of Qualified Individuals.”
- 24590-WTP-ORG-HR-01-01-001, Revision 45, “Project Management Organization Chart.”
- Primavera Schedule, “ICN Software Restart Schedule,” December 5, 2007.
- Primavera Schedule, “C&I Schedule – All,” December 5, 2007, 10:36.
- 24590-RMCD-01651, “PADC Electronic Media Form.”
- ANSYS, Inc. user training handout material.

Procedures

- 24590-WTP-GPG-ENG-0106, Revision 1, “Augmented Monitoring of New Employees/Employees with New Assignments.”
- 24590-WTP-3DP-G04B-00037, Revision 11, “Engineering Calculations.”
- IS&T Standard Practice, “Tracking RM, PPS, DO, and OM Training,” Revision 0.
- IS&T Standard Practice, “Guidance for Software Change Management Review,” Revision 4.
- 24590-WTP-3DP-G06B-00002, Revision 6, “Subcontracts.”
- 24590-WTP-GPP-IT-005, Revision 4, “Project IT Change Control Process.”
- 24590-WTP-GPP-IT-005, Revision 5, “Project IT Change Control Process.”
- 24590-WTP-GPP-MGT-027, Revision 0, “Plant Installed Software Baseline Change Control.”
- 24590-WTP-GPG-J-015, Revision 0, “Design Guide for Safety Instrumented System Implementation.”
- 24590-WTP-GPG-J-016, Revision 1, “Design Guide for Control Valve Sizing.”
- 24590-WTP-GPG-J-025, Revision 5, “ICN Implementation of the Software Configuration Management Plan for Control Systems.”
- 24590-WTP-3DP-G05B-00034, Revision 4, Engineering Department Project Instructions, “Indoctrination and Training.”
- “Desk Instruction: Software Project Notebook.”
- 24590-WTP-QAM-QA-01-001, Revision 7b, “Quality Assurance Manual.”
- 24590-WTP-GPP-IT-008, Revision 2, “Software Life Cycle Management.”
- 24590-WTP-GPG-J-015, Revision 1, “Design Guide for Safety Instrumented System Implementation.”
- 24590-WTP-GPG-J-015, Revision 0, “Design Guide for Safety Instrumented System Implementation.”
- 24590-WTP-GPP-MGT-026, Revision 0, “Modification of Plant Installed Software and Life Cycle Documentation.”

- 24590-WTP-GPG-IT-006, Revision 0, “Glossary of Terms for Software Quality.”
- 24590-WTP-PL-MGT-07-0002, Revision 0, “Plan for Plant Installed Software Life Cycle Management.”
- 24590-WTP-GPP-IT-001, Revision 5, “Use of Quality Affecting Software Applications.”
- 24590-WTP-GPG-QA-203, Revision 5, “Quality Assurance Glossary of Terms.”
- 24590-WTP-GPP-IT-014, Revision 3, “Acquired Software Packaged with Equipment.”

Software Error Notifications

- 24590-SEN-M-07-002, Revision 0

Surveillance Reports

- 24590-WTP-SV-QA-07-291, Revision 1.
- 24590-WTP-SV-QA-06-014, Revision 0.
- 24590-WTP-SV-QA-06-150, Revision 0.

Appendix B
Personnel Contacted

- Manager, Information Systems and Technology Systems Engineering.
- WTP IT Change Manager.
- Lead, C&I Program.
- Lead, Release Management, Software QAP.
- Lead, C&I Software.
- Engineer, C&I.
- Supervisor, IT Applications.
- IT Data Management Supervisor.
- Lead, CS&A Discipline Support.
- CS&A Discipline Production Engineering Manager.
- Lead, CS&A Concrete Design Production – Rebar.
- Engineer, CS&A Steel Design Production.
- Group Lead, CS&A Steel Design Production.
- Engineer, CS&A Analysis Reanalysis.
- Engineer, CS&A Resident and Site Engineering (Formally CS&A Concrete Design Production – Rebar Group – Engineer, which was the basis of the interview).