



U.S. Department of Energy

Office of River Protection

P.O. Box 450
Richland, Washington 99352

SEP 09 2004

04-ESQ-074

Mr. E. S. Aromi, President
and General Manager
CH2M HILL Hanford Group, Inc.
Richland, Washington 99352

Dear Mr. Aromi:

CONTRACT NO. DE-AC27-99RL14047 – REQUEST FOR ACTION ON ASSESSMENT OF INSTRUMENT AND CONTROL (I&C) COMPUTER SOFTWARE

This letter forwards the results of the U.S. Department of Energy, Office of River Protection assessment of CH2M HILL Hanford Group, Inc. (CH2M HILL), control of I&C computer software in the Hanford Tank Farms during the period of August 2 – 6, 2004. The assessment team identified two Findings and made seven Observations. The details of the assessment, including the Findings and Observations, are documented in the assessment report (attachment).

The assessment team found CH2M HILL had made considerable progress in improving its processes for the control of I&C computer software. For example, new procedures and a company standard were implemented to clearly define the processes for the control of I&C software. However, the administrative process for controlling the validation testing of I&C software requires correction. Also, the software change process employed by Fluor Government Group during development of software for the Tank Farms monitoring and control system and the master pump shutdown system were not always followed.

Within 30 days of receipt of this letter, CH2M HILL should respond to the Findings of the assessment. The response should include:

- Admission or denial of the Finding;
- The causes of the Findings if admitted, and, if denied, the reason why;
- The corrective steps that have been taken and the results achieved;
- The corrective steps that will be taken to prevent further Findings; and
- The date when full compliance with the applicable commitments in your quality assurance program will be achieved.

Mr. E. S. Aromi
04-ESQ-074

-2-

SEP 03 2004

The Observations do not identify any deficiencies, but represent experience-based Observations of the team members that CH2M HILL should consider as a source of information for improving their program. In addition to responding to the Findings, CH2M HILL should state the actions it intends to take as a result of the Observations.

If you have any questions, please contact me, or your staff may call Robert C. Barr, Director, Office of Environmental Safety and Quality, (509) 376-7851.

Sincerely,



Roy J. Schepens
Manager

ESQ:DHB

Attachment

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

ASSESSMENT: Control of Tank Farms Instrumentation and Control Computer Software

REPORT: A-04-ESQ-TANKFARM-011

FACILITY: CH2M HILL Hanford Group, Inc.

LOCATION: Richland, Washington

DATES: August 2-6, 2004

ASSESSORS: David H. Brown, DOE-ORP, Lead Assessor
Shivaji S. Seth, DOE-RL Assessor
Clifford A. Ashley, DOE-RL, Assessor

APPROVED BY: P. P. Carrier, Verification and Confirmation Official

Executive Summary

Introduction

From August 2-6, 2004, the U.S. Department of Energy (DOE), Office of River Protection (ORP) assessed the implementation of the Tank Farm contractor's program for controlling instrumentation and control (I&C) computer software. The contractor for the operation and maintenance of the Hanford Tank Farms is CH2M HILL Hanford Group, Inc. (CH2M HILL). The assessment team (Team) evaluated the control of safety software used in the instrumentation and control of safety systems, structures, and components. The Team used criteria, review, and approach documents provided by the DOE Office of Assistant Secretary for Environmental Safety and Health to guide its review of the following areas:

- Validation and Verification;
- Software Design Descriptions;
- Software Requirements Descriptions;
- User Documentation;
- Software Quality Assurance;
- Software Procurement;
- Software Problem Reporting and Corrective Actions; and
- Software Configuration Management.

The assessment team included the following I&C systems in its assessment:

- Tank Farms monitoring and controls system (M&CS), including the master pump shutdown system (MPSS);
- AN Tank Farm primary ventilation instrumentation and control equipment;
- AY/AZ Tank Farms ventilation system monitoring and control equipment;
- SY B-Train exhauster monitoring and control equipment; and
- 242-A Evaporator monitoring and control system.

The M&CS, the MPSS, and the AN Tank Farm primary ventilation system were all in late stages of development by Fluor Government Group, Inc. (FGG), a subcontractor to CH2M HILL. The remaining systems were existing and of varying ages.

Significant Conclusions and Issues

- The Team found CH2M HILL was continuing to improve their processes for the control of computer software. A recent ORP assessment of design and analysis software identified problems in CH2M HILL's implementation of software quality assurance requirements, and these were still being resolved. The current assessment did not identify any new programmatic issues.
- Some CH2M HILL validation testing following maintenance did not provide all documentation required by procedures, and procedures did not define the whole maintenance testing process. (This was an assessment Finding.)
- FGG software change request documents for the M&CS and MPSS development projects were not always controlled in accordance with the process described in the project quality assurance and configuration management plans. (This was an assessment Finding.)

In addition to the Findings, the Team identified several issues that are classified as Observations. Observations are issues based on opinions of the Team rather than contractual noncompliances. ORP may request a response from the contractor on Observations. The Observations addressed the following issues:

- CH2M HILL Engineering had a very small cadre of people trained to develop and maintain software for programmable logic controllers (PLC), particularly Allen-Bradley PLCs. PLCs were playing an increasingly critical role in Tank Farms operations. The assessment team concluded CH2M HILL should enhance the training of existing personnel responsible for PLCs and increase the number of personnel with the necessary skills for changing and testing PLC software;
- FGG's contract with CH2M HILL for development of the M&CS and MPSS software required them to follow CH2M HILL software engineering procedures, but they did not do this. Instead, they followed a reasonable set of processes described in the project quality assurance plan and configuration management plan. The assessment team reviewed the actual work done and concluded these irregularities did not create any questions about the adequacy of the software. However, the assessment team also concluded CH2M HILL should require subcontractors like FGG to develop and follow their own software engineering procedures;
- The technical depth of FGG assessments of software development activities could be improved. While independent surveillance assessments performed by FGG could identify compliance issues, they lacked the technical depth to identify complex process breakdowns;
- The control system software documentation located in the 242-A Evaporator control room was outdated. CH2M HILL should replace it with documentation applicable to the version release installed in the evaporator monitoring and control system control modules;

- CH2M HILL procedures should provide explicit controls for “software forces.” “Software forces” are temporary configurations in control systems that simulate plant conditions. They are required to be controlled like any other temporary modification or temporary bypass; and
- CH2M HILL should have a process for promptly reconciling new safety requirements with ongoing projects. CH2M HILL and FGG were waiting for the operations acceptance testing and accompanying unreviewed safety question processes before comparing documented safety analysis requirements to the M&CS project requirements. The assessment team considers this introduces unnecessary risk from late identification of requirements.

Table of Contents

Executive Summary	ii
Introduction.....	ii
Significant Conclusions and Issues.....	iii
Table of Contents.....	v
List of Acronyms.....	vi
Assessment Purpose and Scope	1
Significant Observations and Conclusions	1
Software Requirements Descriptions (SRD).....	4
User Documentation	4
Software Verification and Validation.....	5
Software Configuration Management.....	5
Software Quality Assurance.....	5
Software Procurements	6
Software Problem Reporting and Corrective Action.....	6
List of Items Opened, Closed, and Discussed.....	7
Signatures	13
Appendix A – Team Biographies	
Appendix B – Assessment Notes	

List of Acronyms

CD	Compact Disc
CH2M HILL	CH2M HILL Hanford Group, Inc.
CFR	Code of Federal Regulations
COTS	Commercial-Off-the-Shelf
CRAD	Criteria, Review, and Approach Document
DNFSB	Defense Nuclear Facilities Safety Board
DOE	U.S. Department of Energy
DSA	Documented Safety Analysis
FGG	Fluor Government Group, Inc.
HMI	Human-Machine Interface
I&C	Instrumentation and Control
M&CS	Monitoring and Control System
Micon	Micon-Powell Process Systems, Inc.
MPSS	Master Pump Shutdown System
NovaTech	NovaTech Process Solutions, LLC
NQA-1	ASME NQA-1-1989, <i>Quality Assurance Program Requirements for Nuclear Facilities</i>
ORP	U.S. Department of Energy, Office of River Protection
PCS	Process Control System
PDS	Project Development Specification
PER	Problem Evaluation Request
PLC	Programmable Logic Controller
QA	Quality Assurance
QAP	Quality Assurance Program
QAPD	CH2M HILL Quality Assurance Program Description
SCADA	Supervisory Control and Data Acquisition
SCM	Software Configuration Management
SCR	Software Change Request
SDD	Software Design Description
SQA	Software Quality Assurance
SQAP	Software Quality Assurance Plan
SRD	Software Requirements Description
SRS	System Requirements Specification
V&V	Verification and Validation
WFO	Waste Feed Operations

Control of Tank Farms Contractor Instrumentation and Control (I&C) Software for the Period of August 2 - 6, 2004

Assessment Purpose and Scope

The assessment team compared the contractor's processes for the control of I&C software to the criteria specified in U.S. Department of Energy, Office of Assistant Secretary for Environmental Safety and Health Criteria, Review, and Approach Document (CRAD) 4.2.3.1, Revision 3, "Criteria and Guidelines for the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities" and the Contractor's Quality Assurance Program Description (QAPD)¹. The CRAD was prepared in response to Defense Nuclear Facilities Safety Board recommendation 2002-1, "Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities."

Significant Observations and Conclusions

The Contractor documented its quality assurance program in TFC-PLN-02, Revision A-3, "Quality Assurance Program Description." The QAPD stated that its requirements were based on American Society of Mechanical Engineers NQA-1-1989, "Quality Assurance Program Requirements for Nuclear Facilities" (NQA-1). While the QAPD addressed computer software, it drew its explicit software control requirements from NQA-1, Supplement 3S-1, "Supplementary Requirements for Design Control," and Supplement 11S-2, "Supplementary Requirements for Computer Program Testing." As discussed in the U.S. Department of Energy, Office of River Protection (ORP) assessment A-04-ESQ-TANKFARM-006, CH2M HILL did not explicitly invoke the requirements of Subpart 2.7, "Quality Assurance Requirements for Computer Software for Nuclear Facility Applications."

Systems Evaluated:

The assessment team reviewed documentation and interviewed responsible personnel for the following I&C systems:

- Tank Farms monitoring and controls system (M&CS), including the master pump shutdown system (MPSS);
- AN Tank Farm primary ventilation instrumentation and control equipment;
- AY/AZ Tank Farms ventilation system monitoring and control equipment;
- SY B-Train exhauster monitoring and control equipment; and

¹ TFC-PLN-02, Revision A-3, *Quality Assurance Program Description*

- 242-A Evaporator monitoring and control system.

Tank Farms M&CS – At the time of the assessment fieldwork, the M&CS was in a late stage of development and deployment. It was a supervisory control and data acquisition system (referred to as a “SCADA system”) intended to automate many Tank Farms operations. In particular, the MPSS component would provide waste transfer routing information, including indication of many valve positions. Transfer pumps were controlled by the system. The MPSS safety function was to automatically shut down transfer pumps and terminate transfers on a signal from any leak detector or signals indicating system configuration anomalies. While there was no control room for the M&CS, human-machine interfaces (HMI) were located at seven nodes. Waste transfers could be planned, initiated, and shut down from any of these HMIs.

The system used programmable logic controllers (PLC) manufactured by RTP Corporation. These were Institute of Electrical and Electronics Engineers class 1E components, designed and sold as nuclear-grade equipment. The M&CS system was designed and assembled by Fluor Government Group Inc. (FGG), and was scheduled for turnover to CH2M HILL in February 2005. At that time, FGG was to have completed all “factory acceptance tests” and CH2M HILL was to begin “operations acceptance tests.”

The software used in the system was Citect (configurable commercial firmware provided by RTP Corp.), NetArrays (commercial communication and HMI software), and custom logic developed by FGG. Development and testing of the logic was a significant effort of the project. FGG performed development work in their Richland office and tested software on the PLCs while they were in Richland. FGG referred to testing in Richland as “qualification testing.” When qualification testing was complete, the PLCs were installed onsite. However, FGG maintained a test bed in Richland where software changes and upgrades were initially tested. Tested software was then copied from the test bed PLCs and uploaded onto the field PLCs.

At the time of the assessment fieldwork the logic developed in Richland had been accepted by FGG, but some configuration changes were continuing. Although field acceptance tests were complete, FGG had scheduled a final round of acceptance tests to address late configuration changes.

AN Tank Farm Ventilation Equipment – The AN Tank Farm ventilation equipment was another system that was being incorporated into the M&CS. Like MPSS, it used RTP Corporation PLCs along with NetArrays, Citect, and locally configured software. The logic and system configuration were developed by the same individuals in FGG who developed the MPSS software. At the time of the assessment fieldwork, FGG and CH2M HILL anticipated that turnover to CH2M HILL would occur in September 2004. Following turnover, CH2M HILL would conduct operations acceptance testing.

The Tank Farms documented safety analysis (DSA) assumed continuous ventilation through the AN Tank Farm. Therefore, there was a technical safety requirement specifying that the AN ventilation system was operating. If the system was not operating, no activities with the potential to ignite flammable gases were allowed. The safety function of the M&CS for the AN Tank Farm would indicate to operators that the ventilation system was operating.

AY/AZ Tank Farms Ventilation System – The AY/AZ Tank Farms ventilation system was based on a M&CS provided by Micon-Powell Process Systems, Inc., (Micon). The system was originally purchased in the late 1980's for a project that was cancelled before the equipment was installed. The equipment was removed from storage and incorporated into the AY/AZ ventilation system when it was built in the mid 1990's. Because the AY and AZ Tank Farms had high decay heat loads, an important function of the system was to provide cooling for the tanks. However, the only safety function with respect to the DSA was to provide indication that the ventilation system was running (and therefore removing flammable gases). The system controlled ventilation fans and monitored a number of system parameters such as temperatures, radiation levels, and valve positions.

CH2M HILL personnel said that Micon was no longer able to fully support all of its customers, and they were afraid that some key support would become unavailable in the future. Therefore, they planned to replace the monitoring and control equipment with a new system using equipment similar to that used in the Tank Farms M&CS.

SY B-Train Exhauster Monitoring and Control Equipment – The SY B-Train system used a single PLC manufactured by Allen-Bradley, a subsidiary of Rockwell Automation. It was one of a pair of filtered ventilation trains used to remove flammable gases from the SY Tank Farm head spaces. (The SY-A ventilation train was not regulated by digital controllers.) The equipment was mounted on a skid that was built in the mid-1990s. Programming access and indication for the PLC were provided by an Allen-Bradley HMI, and custom software developed for the equipment used Allen-Bradley ladder logic. The safety function of the system would provide indication to operators that the ventilation system was operating to remove flammable gasses from the SY tanks.

242-A Evaporator M&CS -- The Evaporator facility monitoring and control equipment was a relatively complex patchwork of systems. While the equipment was intended for operating the Evaporator, it also had the capability of monitoring some transfer leak detectors in the Tank Farms. The only safety function of the systems was to indicate leakage reported by the Tank Farms leak detectors during transfers. However, the new Tank Farms M&CS system was to take over monitoring these leak detectors in the coming months. At that time the equipment at the Evaporator would no longer have a safety function.

Functions specific to the Tank Farms were handled by a control module using software named D/3® running on a Digital Equipment Corp. platform. D/3 was supported by NovaTech Process Solutions, LLC, (NovaTech). In the early 1990s, when the control module was originally delivered, the business unit that manufactured it was owned by Texas Instruments. While the equipment was old, CH2M HILL personnel said NovaTech continued to provide adequate support to CH2M HILL. (A NovaTech motto was, "No D/3 left behind.")

CH2M HILL took over control of the Evaporator from Fluor Hanford, Inc., on May 26, 2003.

Assessment Team Conclusions:

Software Requirements Descriptions (SRD)

The assessment criteria were fully satisfied. The functional and performance requirements for the I&C software were complete, correct, consistent, clear, testable, and feasible. Also, software requirements were documented and consistent with the system safety basis (except as discussed below). SRDs were controlled and maintained. Requirements were identified and defined such that they could be verified and validated.

When the Tank Farms DSA was approved, there was no mechanism for a prompt reconciliation of new requirements with the existing MPSS and M&CS requirements. Instead, CH2M HILL anticipated that the unreviewed safety question process at project turnover would assure that all DSA requirements were satisfied. However, the assessment team was concerned that this approach could provide very late identification of inconsistencies resulting in project delays. Delays place pressure on personnel to cut corners on quality. (Assessment Observation A-04-ESQ-TANKFARM-011-005.)

Except for MPSS and M&CS, all software applications reviewed had a distinct SRD that included a well-defined functional requirements basis at the system level. Considering the nature of the applications involving PLC's and HMI, where the software requirements, design, and implementation life-cycle phases can often be integrated, the SRD along with the software design descriptions (SDD) provided adequate requirements description. In the case of the MPSS and M&CS, the assessors found that the Project Development Specification (PDS) and the SDD generally satisfied the need for software requirements definition and description. However, they also believed that the development of an appropriate software requirements specifications document (e.g., by applying a consensus standard such as IEC-880 or IEEE-830) would have provided greater traceability between system functional requirements and software design implementation, and thereby a greater assurance of reliability. (Assessment Observation A-04-ESQ-TANKFARM-011-006.)

SDDs

The software applications had generally adequate design descriptions consistent with the nature of PLC and HMI applications. The CRAD assessment criteria were met. I&C software-related requirements are implemented in designs, and design elements were traceable to the requirements. Designs were correct, consistent, clearly presented, and feasible.

User Documentation

The criteria of the CRAD were met. User's manuals contained appropriate documentation for their equipment. Documentation provided information to aid the users in the correct operation of the software and to provide assistance for error conditions. Manuals reviewed by the assessors provided adequate guidance on software design and coding requirements.

The control room user's manuals for the D/3 equipment in the 242-A Evaporator were not current. The current documentation was on a compact disc (CD) kept by the system engineer. The assessment team concluded CH2M HILL should print out the documentation from the CD and use it to replace outdated user documentation in the 242A Evaporator control room. (Assessment Observation A-04-ESQ-TANKFARM-011-O02.)

While CH2M HILL has provided appropriate training on most equipment, it has not provided training for personnel maintaining Allen-Bradley PLCs. Also, the number of individuals trained to maintain I&C software was very small. (Assessment Observation A-04-ESQ-TANKFARM-011-O01.)

Software Verification and Validation (V&V)

The CRAD assessment criteria were partially satisfied. CH2M HILL and FGG were verifying software requirements and validating software designs for correct operation. They were also evaluating relevant abnormal conditions for mitigating unintended functions.

However, the assessment team found that CH2M HILL's new key procedure governing control of I&C software referenced invalid procedures for making and testing software changes. Also, the Waste Feed Operations (WFO) Software Quality Assurance Plan (SQAP), and the WFO Software Configuration Management Plan (SCMP) lacked sufficient criteria to consistently test changes to I&C software. (Assessment Finding A-04-ESQ-TANKFARM-011-F01.)

Software Configuration Management

The CRAD assessment criteria were partially satisfied. The assessment team found that CH2M HILL had adequately identified their software components and products, and procedures existed to manage the modification and installation of new versions. However the assessors also found that software change request documentation and temporary modifications to I&C software were not always completed in accordance to plans or procedures. (Assessment Finding A-04-ESQ-TANKFARM-011-F02.)

Software Quality Assurance

The CRAD assessment criteria were generally met. CH2M HILL had significantly improved its Software Quality Assurance (SQA) processes since Defense Nuclear Facilities Safety Board Tech-25 was issued. ORP identified some continuing issues in assessment A-04-ESQ-TANKFARM-006, "Control of Tank Farms Contractor Design and Analysis Computer Software," but CH2M HILL and FGG were resolving them.

CH2M HILL had recently issued a new I&C software engineering procedure and a new I&C software standard. The assessment team found both generally included appropriate guidance and direction. However, the new procedure did not correctly identify procedures for testing software changes made during maintenance. (Assessment Finding A-04-ESQ-TANKFARM-011-F01.) CH2M HILL Waste Feed Engineering had also issued a new SQA plan intended to address I&C

safety software. CH2M HILL was in the process of extending its scope to address safety systems.

In Assessment Report A-04-ESQ-TANKFARM-006, ORP identified deficiencies in the CH2M HILL assessment program with respect to SQA. At the time of the current assessment, ORP and CH2M HILL had not finished closing this issue.

FGG was not explicitly following CH2M HILL software engineering procedures for MPSS development work as specified in the contract between CH2M HILL and FGG. Instead, FGG personnel were following relatively detailed requirements in the MPSS SQA/configuration management plan. Both the SQA/configuration management plan and the CH2M HILL procedures described appropriate software engineering processes, but they were not the same. Therefore, while FGG was not complying with its contractual obligations to CH2M HILL, the assessment team did not identify any resulting problems with the software FGG was developing. The assessment team concluded CH2M HILL should require subcontractors to develop and follow their own implementing procedures. (Assessment Observation A-04-ESQ-TANKFARM-011-O04.)

FGG performed independent surveillance-level assessments of MPSS and M&CS software development activities, but these lacked technical depth. While surveillances could identify compliance issues, they lacked the technical depth to identify more complex process breakdowns. For example, the answers to questions on a surveillance checklist reflected a superficial understanding on the part of the surveillance engineer of the relative roles of different software components. (Assessment Observation A-04-ESQ-TANKFARM-011-O03.)

Software Procurements

The criteria were met for current procurements. CH2M HILL did not have objective evidence that procurements made in the mid-1990s conformed to all requirements, but this problem was identified and resolved previously.

ORP evaluated FGG's software procurements for the Tank Farms M&CS and MPSS in an earlier assessment and found them to be appropriate.

Software Problem Reporting and Corrective Action

While the criteria for problem reporting and corrective action were met, multiple processes existed for different software development and maintenance activities. These were specified in individual quality assurance plans. CH2M HILL said they were in the process of establishing a single, company-wide procedure for software error reporting.

Software errors were reported and resolved using the established systems, both in CH2M HILL and FGG. Some issues with error resolutions are addressed in the configuration management section of this report.

List of Items Opened, Closed, and Discussed

Opened

A-04-ESQ-TANKFARM-011-F01: CH2M HILL plans and procedures did not accurately define the processes for identification and execution of software maintenance and testing.

Requirements:

TFC-PLN-02, Revision A-3, "Quality Assurance Program Description," Section 2.5.2.1 "General Requirements for Work Processes," stated: "All activities that can affect the quality, safety, or the environment of CH2M HILL products and services shall be prescribed by, and performed, in accordance with documented, management-approved procedures, instructions, and design documents that meet the requirements of applicable regulatory requirements, DOE orders, technical standards, and administrative controls."

Discussion:

CH2M HILL was in the process of making extensive improvements in the requirements infrastructure for software engineering, including generation of new procedures and plans. The assessment team reviewed many of these new procedures and plans, and found they were appropriate improvements to CH2M HILL's processes. However, the assessment team found some documents that either contained errors or did not specify the required level of rigor for safety software. The assessment team based its conclusions on the following:

- The key procedure governing maintenance of I&C software did not specify the correct process for testing some changes to I&C software made during maintenance activities. CH2M HILL made procedure TFC-ENG-DESIGN-P-12, Revision A, "Process Control Software Procedure" effective on April 2, 2004, to describe the overall process for developing, documenting, testing, control, and maintenance of I&C software. Despite a statement in the "Purpose and Scope" section of the procedure to include maintenance, there was no section specific to maintenance. Procedure Section 4.6, "Modification of Implemented Software," addressed most software maintenance activities. For testing of completed changes, this section required testing to be conducted in accordance with several testing procedures, including TFC-PRJ-SUT-C-01, "Test Plan Preparation," and TFC-ENG-DESIGN-C-18, "Testing Practices." However, these procedures, along with the other procedures invoked by Section 4.6, contained scope statements that explicitly excluded testing of maintenance work. In this context, "maintenance" would not include software many changes and upgrades, therefore the personnel preparing work packages could be expected to navigate the system successfully. However, there was no procedure to address testing of corrective maintenance required to bring the software into conformance with the system design;
- CH2M HILL WFO SQAP (RPP-2108, Revision 0), Section 4.13 stated: "Testing is performed as described in the WFO SCMP on a case-by-case basis depending upon the magnitude of the changes being made." Neither the SCMP (RPP-21082, Revision 0) nor the