DEPARTMENT OF ENERGY
RICHLAND OPERATIONS OFFICE

ASSESSMENT OF FLUOR HANFORD INC.
SAFETY SOFTWARE QUALITY ASSURANCE
March 15 – 31, 2004

A-04-SED-FHI-009

S. Seth, Lead
C. Ashley
D. Brown
J. McCracken
S. Sen

May 2004

U. S. Department of Energy
Richland Operations Office (RL)
Assessment of Fluor Hanford Inc. Safety Software Quality Assurance

Report Approval

Assessment Team:

Shivaji S. Seth, DOE-RL,
Team Lead

Clifford A. Ashley, DOE-RL
Deputy Lead

Dave H. Brown, DOE-ORP

Jim J. McCracken, DOE-RL

Subir Sen, DOE-EH

U. S. Department of Energy
Richland Operations Office (RL)
Assessment of Fluor Hanford Inc. Safety Software Quality Assurance

EXECUTIVE SUMMARY

The DOE Richland Operations Office (RL) conducted an assessment of safety software quality assurance (SQA) processes of its prime contractor, Fluor Hanford Inc. (FHI) during the period March 15 – 31, 2004. The assessment was undertaken to fulfill field office commitments in the DOE's Implementation Plan, *Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities,* for Defense Nuclear Facilities Safety Board Recommendation 2002-1.

The objectives of the assessment were to assess the adequacy of SQA for safety system instrumentation and control (I&C) software and the software used in the safety analysis and design of nuclear facilities. The assessment was based on the criteria and approach documents developed by the DOE Office of Assistant Secretary for Environment, Safety and Health to specifically address these objectives. The following were the eight broad areas of SQA assessment:

- Software Requirements Description
- Software Design Description
- Software User Documentation
- Software Verification and Validation (V&V)
- Software Configuration Management
- Software Quality Assurance
- Software Procurement
- Software Reporting and Corrective Action

The assessment included all I&C software that performs safety functions in nuclear facilities operated by FHI and some additional I&C software application that are not credited with safety functions. The safety analysis and design work for nuclear facilities is mostly performed by Fluor Government Group (FGG) personnel under a staff augmentation agreement with FHI, and through FHI's subcontractor, Duratek Federal Services, Inc. Therefore, the assessment also included a large sample of safety analysis and design computer software controlled and used by personnel from the three organizations, FHI, FGG, and Duratek.

The assessment team found that FHI has established a generally adequate set of computer software requirements based on the nuclear industry's well-recognized and widely used software quality assurance standard, ASME NQA-1 Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications.* It also found that the designated principal users of safety software in all three organizations have excellent qualifications and experience.

The assessment revealed significant weaknesses in FHI's implementation of software quality assurance requirements. A few deficiencies identified during the assessment resulted in FHI taking actions. One of these deficiencies involved the lack of quality assurance requirements in a procurement of fire hazards analysis services, which used the computer code CFAST. FHI issued an occurrence report declaring site-wide potential inadequacy of documented safety analysis. The deficiencies identified did not pose an imminent threat to safety.

The noteworthy practices, findings and observations from this assessment are listed below:

Noteworthy Practices

(1) *FHI requires compliance with the nuclear industry's well-established and comprehensive software quality assurance standard.*

(2) *FHI's procurement of the Spent Nuclear Fuel (SNF) Project Safety Class Instrumentation and Control (SCIC) hardware and software system assures quality and reliability of the equipment.*

(3) *Duratek's upgrading of the computer code RADCALC is a good example of revising software to conform to current software quality assurance requirements.*

(4) *Designated principal users of software have excellent qualifications and experience.*

(5) *Lists of authorized users of software are well maintained.*

(6) *The evaluation, reporting, and tracking of error reports on commercial off-the-shelf (COTS) software by FGG staff working under staff augmentation agreement with FHI is commendable.*

Findings

(F-1) Finding A-04-SED-FHI-009-F01

FGG personnel performing work for FHI in staff augmentation roles do not implement FHI's software quality assurance requirements and procedures, and the software used by them is not controlled under FHI's software quality assurance program.

(F-2) Finding A-04-SED-FHI-009-F02

FHI did not develop software management plans for safety analysis and design software as required by its procedures.

(F-3) Finding A-04-SED-FHI-009-F03

FHI Safety and Health organization did not meet its requirement to bring legacy software into compliance by the established date.

(F-4) Finding A-04-SED-FHI-009-F04

FHI failed to specify quality assurance requirements for subcontractors performing fire hazards analyses of nuclear facilities.

(F-5) Finding A-04-SED-FHI-009-F05

FHI and Duratek do not always adequately implement software V&V and configuration control requirements.

(F-6) Finding A-04-SED-FHI-009-F06

FHI did not adequately implement software quality assurance requirements for legacy MICON I&C software at PFP.

(F-7) Finding A-04-SED-FHI-009-F07

FHI and Duratek do not identify and formally document computer software user qualification and training requirements.

(F-8) Finding A-04-SED-FHI-009-F08

FHI's software quality assurance procedures do not implement the NQA-1, Subpart 2.7 requirements for software procurement and for reporting software errors between FHI and its suppliers.

(F-09) Finding A-04-SED-FHI-009-F09

The FHI assessment program failed to identify inadequacies in its software quality assurance program.

Observations

(O-1) Observation A-04-SED-FHI-009-O01

FHI's software quality assurance requirements cannot be unambiguously determined from the Quality Assurance Program Description.

(O-2) Observation A-04-SED-FHI-009-O02

FHI requirement for controlling access to SRS I&C software at FFTF was compromised.

(O-3) Observation A-04-SED-FHI-009-O03

FHI and Duratek do not require each authorized user of an approved safety analysis or design computer program to maintain a record of computer program use.

TABLE OF CONTENTS

TABLES

LISY OF ACRONYMS

AJHA	Automated Job Hazards Analysis
ASME	American Society of Mechanical Engineers
COTS	Commercial-Off-The-Shelf
CFR	Code of Federal Regulations
CRAD	Criteria, Review, and Approach Document
DSA	Documented Safety Analysis
DNFSB	Defense Nuclear Facilities Safety Board
ESL	Evaluated Suppliers List
FFTF	Fast Flux Test Facility
FGG	Fluor Government Group
FHA	Fire Hazards Analysis
FHI	Fluor Hanford, Inc.
HFD	Hanford Fire Department
I&C	Instrumentation and Control
NQA	Nuclear Quality Assurance
P&ID	Piping and Instrumentation Diagrams
PFP	Plutonium Finishing Plant
PHMC	Project Hanford Management Contract
PISA	Potential inadequacy of documented safety analysis
PLC	Programmable Logic Controller
PTW	Power[*]Tools for Windows (Trademark of SKM, Inc.)
RWP	Radiological Work Permit
SDD	Software Design Description
SNF	Spent Nuclear Fuel
SQA	Software Quality Assurance
SRD	Software Requirements Description
V&V	Verification and Validation
VSS	Vital Safety Systems
QA	Quality Assurance
QAPD	Quality Assurance Program Description

U. S. Department of Energy
Richland Operations Office (RL)
Assessment of Fluor Hanford Inc. Safety Software Quality Assurance

1. INTRODUCTION

This report presents the results of a Richland Operations Office (RL) assessment of safety software quality assurance processes of its prime contractor, Fluor Hanford Inc. (FHI). The assessment was conducted during the period March 15 – 31, 2004. The background and objectives of the assessment are discussed below.

1.1 Background

The DOE Implementation Plan (1) for Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2002-1, *Quality Assurance for Safety-Related Software,* September 2002, defines the actions and processes that are being taken to ensure the quality of safety software at defense nuclear facilities. Safety software includes both safety system software and safety analysis and design software. Commitment 4.2.3.3 of the Implementation Plan is to complete the identification, selection, and assessment of safety system software; and Commitment 4.2.4.3 is to complete the assessments of the processes in place to ensure that safety software currently used to support the analysis and design of defense nuclear facilities is adequate.

As one of RL's prime contractors, FHI is responsible for a significant portion of the cleanup at the Hanford site. The work involves the use of computer software, both instrumentation and control (I&C) software and safety analysis and design computer codes in support of deactivating and decommissioning nuclear and radiological facilities. The present assessment was undertaken to fulfill the above mentioned commitments relative to safety software currently used by FHI, Fluor Government Group (FGG) personnel working as FHI staff augmentation, and FHI subcontractor Duratek Federal Services, Inc. (Duratek).

1.2 Objectives and Criteria

The primary objectives of this assessment follow the objectives and commitments contained in the DOE's Implementation Plan for DNFSB Recommendation 2002-1:

A. Assess the adequacy of software quality assurance (SQA) for safety system I&C software and firmware in nuclear facilities operated by FHI.

B. Assess the adequacy of FHI's SQA processes in place for computer codes, calculation software, and database programs, including custom and commercial off-the-shelf (COTS) software used in the safety analysis and design of nuclear facilities.

The assessment was based on the two criteria and review approach documents [2,3], CRAD – 4.2.3.1 and CRAD – 4.2.4.1, developed by the DOE to specifically address Objectives A and B, respectively.

The objectives and criteria in the CRADs are consistent with DOE 10 CFR 830.120 and DOE Order 414.1A Contractor Requirements Document on Quality Assurance, which are implemented in the Project Hanford Management Contract (PHMC) with FHI through FHI's Quality Assurance Program Description [4] (QAPD). The QAPD is the top-level document of FHI, and compliance is mandatory. Specifically, the QAPD requires compliance with the American National Standard ASME NQA-1, Subpart 2.7 [5]. Implementation of the QAPD is supported by FHI procedures [6,7] on computer software requirements and management. The results of this SQA assessment, therefore, were keyed to FHI's specific requirements.

1.3 Report Organization

The next two sections discuss the scope and approach of the assessment. Tables 1 and 2 in Section 3 identify the specific software items examined. Section 4 presents the significant results in terms of noteworthy practices, findings, and observations. As noted above, the findings and observations reference the specific FHI requirements. Section 5 provides brief summaries of assessment areas mentioned in the DOE CRADs, including whether the specified criteria were met. These summaries cross-reference the findings and observations in Section 4 to indicate issues identified in the assessment areas.

Appendices A-1 and A-2 are lists of documents reviewed and personnel interviewed, respectively, in support of this assessment. Appendix B provides brief biographies of assessment team members relative to their qualifications and experience.

2.0 SCOPE OF ASSESSMENT

All FHI I&C software that performs safety functions was included in the assessment. Additional I&C software was identified and included in the assessment for reasons mentioned in the next section.

Most of FHI's safety analysis and design work is performed by FGG staff under a staff augmentation agreement with FHI, and through FHI's subcontractor, Duratek Federal Services, Inc. Duratek staff perform analyses for FHI in two ways: under task-order contracts using qualifying software under FHI approved NQA-1 QA program and in a staff augmentation role using qualifying software in accordance with FHI requirements and procedures. Therefore, with the objective of assessing all the SQA processes that come into play through the PHMC, a sufficient sample of safety analysis and design codes was examined, which was used by staff from three organizations, FHI, FGG, and Duratek. The assessment of SQA processes also included review of supporting calculation software.

Database programs and other safety management software that has nuclear safety implications was also sampled and examined to a limited extent. Computer software applications of this type are also used by the Pacific Northwest National Laboratory (PNNL) at FHI operated facilities through the Hanford Site shared services agreement with PNNL. Such applications include radiological dose assessment and radiation exposure monitoring. RL intends to conduct a separate assessment of the PNNL SQA processes governing such software applications in May 2004.

3.0 ASSESSMENT APPROACH AND TAILORING

3.1 Software Identification and Selection

An initial step in this assessment, undertaken with FHI's assistance, was the development and review of FHI's and subcontractor's inventory of software that potentially could be classified as safety software using the definitions in DOE CRADs. This enabled selecting all the safety I&C software and a sample of safety analysis and design codes, which was sufficient to provide confidence in the assessment of SQA processes. It also enabled FHI to identify and provide, or to keep ready for review at the facility, a significant portion of the requested documents for the team's review; and to develop a preliminary schedule for interviews with key personnel.

A valuable starting point for identifying the relevant I&C software was the list of vital safety systems (VSS) prepared in support of DOE's Implementation Plan for DNFSB Recommendation 2000-2. However, the VSS included defense-in-depth systems and certain I&C systems that did not rely on their software for their safety functions. The assessment team worked with RL's authorization basis staff to ascertain the role of I&C software applications in various nuclear facilities. Where there was some uncertainty regarding the potential safety role of an I&C system software, that software was at least initially included in the assessment. This resulted in grading or limiting the assessment of a few software applications based on further review and discussion of the safety significance of that software. It also led to including one general service I&C software that is credited with performing a safety-significant function in a documented safety analysis that was approved by RL during the assessment period. Table 1 is a list of the I&C software included in the assessment.

A starting point for identifying the safety analysis and design codes was the results of surveys of such codes completed as part of previous commitments in the DOE Implementation Plan for DNFSB Recommendation 2002-1. A careful selection of computer codes is necessary because several factors affect the applicable SQA processes. These factors include the following: (a) the type of software (COTS, government agency sponsored, or custom); (b) model complexity (affecting user understanding, interaction, documentation, and code validation method); (c) vintage (affecting the nature of available life cycle documentation and how "legacy" software is brought into compliance); and (d) whether the software is "currently used". The consideration of these factors resulted in a

TABLE 1
List of Selected Instrumentation and Control (I&C) Software

Name, Owner and Version	Type of Application	Application/Function
Software Used by Fluor Hanford Inc. (FHI)		
Safety Class Instrument and Control (SCIC)	I&C / Programmable Logic Control	Spent Nuclear Fuel (SNF) Project—Cold Vacuum and Drying Facility (CVDF)/ Safety shutdown of multi-canister over-pack (MCO) valves and tempered water heater on selected process upsets
MICON I&C software [†]	Distributed Control System	Plutonium Finishing Plant (PFP)—various functions, including shutdown of 2736-ZB ventilation on fire alarm
Refueling Closed Loop Ex-Vessel Machine (CLEM) I&C software [*]	I&C / Programmable Logic Controller	Fast Flux Test Facility (FFTF)— CLEM control system
Sodium Removal System (SRS) I&C software [*]	Programmable Logic Controller	Fast Flux Test Facility (FFTF)— SRS control system
Multi-canister Overpack (MCO) Loading System (MLS) I&C software [**]	I&C / Programmable Logic Controller	Spent Nuclear Fuel (SNF) Project— K-Basins / MLS shuttle, basket grapple and gantry, support structure operations
Fuel Retrieval System (FTS) I&C software [**]	I&C / Programmable Logic Controller	Spent Nuclear Fuel (SNF) Project—K-Basins / Fuel retrieval system operations

[†] General service software performing safety-significant function, augmented by special operational controls at the level of technical safety requirements.

[*] Not safety software.

[**] Not safety software; limited review of applicable SQA processes and functionality.

TABLE 2
List of Selected Safety Analysis and Design Software

Name, Owner and Version	Type of Application	Application/Function
Software Controlled/Used by Duratek		
ALGOR (Algor, Inc) Version 14.4	Design and analysis of transportation systems	Structural analysis using differential equations
ORIGEN (RSICC/Duratek) Version 2.1	Safety analysis of transportation	Radionuclide decay and processing
RADCALC (Duratek) Version 3.0	Safety analysis of packaging and transportation	Hydrogen generation, radionuclide decay, and package classification
Software Controlled by Fluor Government Group (FGG)		
ANSYS (Ansys, Inc) Version 7.1	Design and analysis in civil/structural engineering)	Finite element analysis
GXQ (FGG) Version 4.0 Revs. A-F	Safety analysis of nuclear facilities	Atmospheric dispersion modeling and analysis
ORIGEN (RSICC/FGG) Version S.2	Safety analysis of nuclear facilities	Radionuclide decay and processing
Power*Tools for Windows[†] (SKM) Version 4.5.3.0	Electric power system studies	Short circuit, load flow and voltage drop, and arc flash analyses
Software Controlled/Used by Fluor Hanford Inc. (FHI)		
CFAST (NIST) Version 3.1.7	Fire hazards Analysis	Analytical zone modeling and analysis of fires in structures
GXQ (FGG) Version 4.0 Rev. C	Safety analysis of nuclear facilities	Atmospheric dispersion modeling and analysis
AJHA (FHI) Version 5.1.0	Automated job hazards analysis	Identification of radiological and other health, safety, and environmental job hazards and controls

[†] Abbreviated in this report as PTW.

relatively large sample set of software used by staff from three organizations. The list of selected safety analysis and design codes is shown in Table 2.

3.2 Software Assessment

The two DOE CRADs for SQA assessment each identify eight broad areas covering the typical software life cycle:

- Software Requirements Description
- Software Design Description
- Software User Documentation
- Software Verification and Validation (V&V)
- Software Configuration Management
- Software Quality Assurance
- Software Procurement
- Software Reporting and Corrective Action

Each of these areas was covered in the assessment to the extent deemed appropriate. The assessment team's lines of inquiry for each area followed the approach described in the CRADs for that area.

The criteria and approach in the CRADs in certain areas required tailoring. For example, software requirements description and software design description areas do not fully apply to procured COTS software or to certain I&C applications involving programmable logic controllers (PLCs). Similarly, V&V applies differently to COTS, where the assessment focused on installation V&V and proper validation using test problems and cases appropriately matched to the intended software application.

The qualification and training of software users was an important element in this assessment, especially for relatively complex safety analysis and design codes where significant technical expertise is needed for proper code validation, problem modeling, and correct use of the software for diverse applications. The assessment criteria provided in the DOE CRADs do not address this aspect explicitly, although they refer to user training as part of one item in describing the approach for software user documentation assessment area. The assessment team appropriately augmented its lines of inquiry in this assessment area to address software user qualifications and training in greater detail.

Field visits, document reviews, and personnel interviews were the primary means of gathering data and information for the assessment. During the field review of a particular application of software, the team ensured that appropriate DOE and contractor staff were involved. The following provides examples of the types of general and software-specific documents that were reviewed, depending on their applicability to SQA processes and activities; and the types of personnel who were interviewed. The full lists of documents reviewed and personnel interviewed are provided in Appendices A-1 and A-2, respectively.

The following are examples of types of requirements and background documents reviewed:

- DOE and contractor software quality assurance requirements documents
- Facility-specific SQA requirements and procedures
- Self-assessments, audits, and independent assessments
- List of databases that may have safety implications
- List of evaluated suppliers of software and technical services
- List of subcontractors using or developing safety software
- Occurrence reports and corrective action requests/reports

The following are examples of types of software-specific documents reviewed:

- Description of current work relating to the software, including changes
- Software functional and requirements and descriptions
- Software design description
- Software development and management plans covering the entire lifecycle
- Products during and following software development
- Program description manuals, user manuals, guides, and instructions
- Audit reports; problem/resolution and corrective action reports
- User qualification and training requirements/records, and training manual
- List of individuals that performed V&V and their qualifications
- List of authorized users
- Sample input and output files

The following are examples of key personnel interviewed:

- Principal user (also may be referred to as system engineer or design authority)
- Users of software
- Discipline or functional manager
- Individuals responsible for developing and implementing software modifications
- Individuals responsible for software V&V
- Nuclear safety (authorization basis) engineers, as necessary
- I&C system engineer
- Quality assurance manager and staff

During the assessment, FHI initiated or took corrective actions on a few deficiencies identified by the assessment team. One instance involved FHI issuing an occurrence report declaring site-wide potential inadequacy of documented safety analysis (PISA). In these instances, the contractor and the team followed the established procedures. The concerns did not pose an imminent threat to safety.

FHI staff members accompanied the assessment team throughout its field work to facilitate the reviews, provide assistance in obtaining the necessary additional documents, and understand the issues identified. In addition, daily exit meetings with FHI and its subcontractor staff were held. At the completion of its field work, the assessment team provided a comprehensive out-brief to RL and contractor organizations, which presented all the preliminary results of the assessment.

Additional document reviews and discussions with contractor personnel were conducted as necessary to bring closure to open issues and finalize the results. A draft of this report was provided to FHI for a review of factual accuracy. All review comments were addressed in this report.

4.0 ASSESSMENT RESULTS

The following is a discussion of the noteworthy practices, findings, and observations derived from the team's assessment of the safety software quality assurance processes of FHI and Duratek. Most of these results cut across several assessment areas; therefore, all the essential information from relevant assessment areas, which supports a given result, is included with each assessment result. Brief summaries of the assessment areas with references to the results discussed below are provided in the next section.

Overall, the assessment found that FHI has established a generally adequate hierarchy of computer software requirements based on the nuclear industry's well-recognized and widely used software quality assurance standard, ASME NQA-1, Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications.* However, the assessment also revealed significant weaknesses in FHI's implementation of software quality assurance requirements, as indicated by the findings and observations discussed in this section.

The findings and observations presented in Sections 4.2 and 4.3, respectively, are assigned identification numbers and trending categories (shown in parenthesis), as required by RL procedures.

4.1 Noteworthy Practices

(1) *FHI requires compliance with the nuclear industry's well-established and comprehensive software quality assurance standard.*

FHI has a hierarchy of implementing directives addressing software quality assurance. The FHI Quality Assurance Program Description (HNF-MP-599) requires compliance with ASME NQA-1, Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications.* This standard is implemented by HNF-RD-10768, *Computer Software Requirements*, and HNF-PRO-309, *Computer Software Management.* FHI provides adequate criteria for determining which software must meet the requirements.

(2) *FHI's procurement of the SNF Project Safety Class Instrumentation and Control (SCIC) hardware and software system assures quality and reliability of the equipment.*

The procurement of the SCIC equipment and software was executed in accordance with FHI procurement process, assuring that the quality and reliability of the system would meet all requirements. This system is located in the SNF Project's Cold Vacuum Drying Facility (CVDF). FHI/SNF engineering staff properly identified the functional, performance, and quality requirements for the system. They then participated in verifying that the supplier, Framatome ANP, had a quality assurance program that met FHI requirements, and that the vendor was capable of providing the system as specified. The procurement and software life cycle documentation was adequate and well organized.

(3) *Duratek's upgrading of the computer code RADCALC is a good example of revising software to conform to current software quality assurance requirements.*

RADCALC is one of the very few examples of major customized upgrades of safety software completed recently at Hanford. Duratek, the custodian of the software, upgraded the software to conform to the NQA-1, Subpart 2.7 standard for conducting transportation safety analyses. The assessment team found excellent life cycle documentation for the code. The code provides automatic verification and validation during software installation.

(4) *Designated principal users of software have excellent qualifications and experience.*

The assessment team interviewed the designated principal user or the technical authority for each software application selected as part of this assessment. In general, these individuals were knowledgeable, well qualified, and competent. They could be relied upon for providing in-house technical expertise to other authorized users of the software.

(5) *Lists of authorized users of software are well maintained.*

Maintaining a list of authorized users for each application of safety software is essential for software control and access. The assessment team found that FHI, Duratek, and FGG generally had an adequately maintained list of authorized users for the safety software under their control.

(6) *The evaluation, reporting, and tracking of error reports on COTS software by FGG staff working under staff augmentation agreement with FHI is commendable.*

Communication of software errors to software vendors and evaluation of error reports received from the vendors are important because of their potential safety implications.

FGG staff reported to the vendor of PTW software an error in one of the application modules, which the vendor was not aware of. FGG staff also routinely review error notices, such as for ANSYS, and evaluate whether previous calculations in support of safety or design analyses could be affected. Such evaluations are adequately documented.

4.2 Findings

(F-1) Finding A-04-SED-FHI-009-F01

FGG personnel performing work for FHI in staff augmentation roles do not implement FHI's software quality assurance requirements and procedures, and the software used by them is not controlled under FHI's software quality assurance program. **[QA-QAPROG, ISMS-IDHAZ]**

Requirements:

1. 10 CFR 830 Subpart A, *Quality Assurance Requirements,* Paragraph 830.121, *Quality Assurance Program (QAP)*, "(b) The contractor responsible for a DOE nuclear facility must: … (4) Conduct work in accordance with the QAP."

2. HNF-MP-599, Revision 12, *Quality Assurance Program Description,* Section 7.0, Paragraph 2.3.3, "Contractors providing support services used for staff augmentation shall work to the FH QA Program and procedures and need not be evaluated for placement on the FH ESL."

3. HNF-MP-599, Revision 12, *Quality Assurance Program Description,* Section 1.0, Paragraph 2.20, "Software acquisition, development, operations, maintenance, and retirement shall be developed and documented in accordance with procedures based on ASME NQA-1, Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Application*."

Discussion:

FHI described its relationship with FGG as an "affiliate" relationship. As such, FGG employees performing work for FHI served in staff augmentation positions and were therefore required to perform work in accordance with the FHI quality assurance program.

The assessment team reviewed work that FGG personnel were performing with safety computer software. It found that several computer codes were not controlled in accordance with FHI requirements and procedures, but controlled under FGG procedures. FGG staff performing work under staff augmentation agreement with FHI said they follow the FGG procedures [8, 9], Practice 1342000960, *Control of Engineering Software,* and Practice 1342001020, *Engineering Calculations.* The assessment team reviewed the FGG procedures and found that they did not implement the requirements of NQA-1, Subpart 2.7, as required by FHI's Quality Assurance Program Description (QAPD). FGG and FHI management told the assessment team that the FGG procedures were not intended to implement NQA-1, Subpart 2.7.

FHI had neither established nor independently assessed the equivalency of FGG's procedures to FHI's requirements and procedures. For software quality assurance, FHI requirements are provided in HNF-RD-10768 and HNF-PRO-309. FGG itself had identified and documented [10] several gaps and deficiencies in its procedures relative to FHI's procedure HNF-PRO-309, Revision 1. For example, gaps existed in the areas of configuration management, software testing, and user qualifications.

FGG staff use a large number of safety analysis and design computer codes in performing safety analysis and design work for FHI. A part of such work is directly in support of preparing documented safety analyses (DSAs) for nuclear facilities, as required by the Code of Federal Regulations, 10 CFR 830, *Nuclear Safety Management*. The computer codes selected for this assessment included ORIGEN, GXQ, PTW, and ANSYS. All of these codes are examples of safety software that is in use by FGG personnel for FHI work but is not controlled and used in accordance with FHI requirements.

RL Closure Required: YES [X] NO [ ]

(F-2) Finding A-04-SED-FHI-009-F02

***FHI did not develop software management plans for safety analysis and design software as required by its procedures.* [QA-WORKPR, ENG-CM, ISMS-WORK]**

Requirements:

1. HNF-RD-10768, Requirement 12, "Organizations developing or modifying computer software shall develop software management plans and procedures that describe their computer software development, test, and configuration management process."

2. HNF-RD-10768, Requirement 13, "Software Quality Assurance Plans shall, as a minimum, contain the following: …"

3. HNF-PRO-309, Revision 4, *Computer Software Management*, Section 5.1, Step 2, "Prepare a Software Management Plan (SMP) which as a minimum contains the following:… [11 bulleted items, including those below]

   - Software Life Cycle Methodology …
   - Identification of document control and records management processes as required by HNF-RD-8310, *Document Control Program, and HNF-PRO-10588, Records Management Process.*
   - Organizations responsible …

- Configuration Management Methodology, including …
- Methods to verify and validate software
- Process for reporting and documenting software problems, …"

4. HNF-MP-599, Revision 12, Section 5.0, Paragraph 2.6, *Control of Computer Software*, "Computer software used in applications important to safety, health, environmental, and quality aspects of Project Hanford activities, including design calculations and laboratory analysis, shall be subject to appropriate controls, including configuration management, throughout the software life cycle."

Discussion:

FHI requirements and procedures provide for the development and implementation of software management plans to specify how organizations are to comply with the specified software quality requirements.

Contrary to FHI requirements, the assessment team found that there are no software management plans for the large number of safety analysis and design codes used by FGG personnel working under staff augmentation agreement with FHI. Those computer codes are under FGG's management control and procedures, which do not require software management plans. Thus, the use of those codes by FGG staff deviates from the FHI requirements of HNF-RD-10768 and HNF-PRO-309.

The assessment team also reviewed the use of safety software under FHI control. The assessment team requested software management plans and found they did not exist for some safety software. In particular, there were no software management plans addressing GXQ Version 4.0 C and CFAST. These computer codes are used in the development of DSAs and fire hazards analyses for nuclear facilities, respectively.

The ownership of Version 4.0C of GXQ was transferred from FGG to FHI in February 2001, but FHI did not prepare the required software management plan for this code. Later, when it would be classified as legacy software by Revision 4 of HNF-PRO-309, FHI also did not prepare a software implementation plan for bringing it into compliance with the appropriate life cycle documentation and configuration management requirements. The FHI Office of the Chief Information Officer has custody of GXQ Version 4.0 C, but stated that they have no technical capability for actual maintenance of the code. Meanwhile, FGG has continued to develop revisions of its proprietary version of the code; and FGG staff, in staff augmentation roles for FHI, have used different versions of the code for various nuclear facilities at the Hanford site.

The Hanford Fire Department (HFD) personnel use the CFAST fire hazards analysis computer code to review or check the results of fire analyses performed by subcontractors. They may also perform fire hazards analyses for diverse analytical tasks not subcontracted. Such reviews and analyses have the potential to provide, modify, reinterpret, or accept results and information that are used in the DSAs of nuclear facilities or in the safety analyses of radiological, non-nuclear, or industrial facilities.

Since the code can be readily down-loaded from the NIST website, different versions of the code may be used by HFD fire protection engineers assigned to different FHI projects. There are no FHI controls or guidance on the use of CFAST. The HFD does not have an approved software management plan or other quality assurance documentation, such as that reflecting configuration control and V&V of CFAST versions in use.

Furthermore, FHI has not established a formal management system for controlling the baseline and the status of the numerous software management plans and software implementation plans. These software implementation plans provide management controls for bringing into compliance with current FHI requirements all legacy software (software used prior to October 30, 2002) that satisfies the criteria in HNF-PRO-309, Appendix A.

Some software management or implementation plans (e.g., for SNF and FFTF projects) were not issued as controlled documents in accordance with the document control requirements of HNF-RD-8310. These requirements are intended to ensure that all quality assurance documentation, including software management plans, are properly prepared; adequately reviewed and approved; distributed to, and properly used by those responsible for performing the functions described in the document; and revised in a manner that ensures that configuration is maintained and adequately documented.

After the assessment team discussed the inconsistent implementation of document control system for FHI software management plans, the SNF project issued its Software Management and Implementation Plan as a formal document with an HNF reference number. FHI pointed out however that the SNF software management plan, prior to this assessment, was properly approved, issued with a formal letter, and posted on an internal SNF fileserver. Personnel responsible for compliance with the plan were provided specific briefings on their roles and responsibilities as outlined in the plan.

RL Closure Required: YES [X] NO [ ]

(F-3) Finding A-04-SED-FHI-009-F03

FHI Safety and Health organization did not meet its requirement to bring legacy software into compliance by the established date.
[QA-QAPROG, ENG-CM, ISMS-WORK]

Requirements:

1. HNF-RD-10768, Revision 0, *Computer Software Requirements*, Section 2.0, Requirement 3, "Organizations must prepare an implementation plan which outlines their methodology for bringing legacy software into compliance with this procedure, based on safety, security, and risk to the company/project/facility."

2. HNF-PRO-309, Revision 4, Section 3.0, “This document is effective for implementation upon publication. Organizations that cannot be in compliance by March 31, 2003, must submit a *Document Variance* (A-6002-579) in accordance with HNF-PRO-589, *Requirements Management Process*, providing a justification, an implementation plan and schedule. Continue to comply with HNF-PRO-309, Revision 3, and HNF-PRO-2778, *IRM Application Software System Life Cycle Standards*, Revision 0, until this revision is implemented.”

3. HNF-PRO-309, Revision 4, Section 5.1, Step 5, “Prepare Company/Project/ Facility/Function Software Implementation Plan for bringing legacy software into compliance with the appropriate life cycle documentation and configuration management requirements specified in the Software Management Plan. The Software Implementation Plan contains the following, at a minimum: ….”

4. HNF-PRO-309, Revision 4, Section 5.2, “Qualification of Legacy Software,” states, “2. Complete a *Software Evaluation Form* (SEF) (A-6003-405 or equivalent) that describes the adequacy and completeness of design, test and user documentation.”

Discussion:

HNF-PRO-309 mandated compliance of legacy software to the procedure’s requirements by March 31, 2003. The procedure defines legacy software as that used prior to October 30, 2002 and not developed to a recognized national consensus software engineering standard, or whose history of application is unknown. A “document variance” is required if the compliance requirement could not be met. The procedure also requires a software implementation plan to ensure that legacy software has appropriate life cycle documentation and configuration management requirements specified in the software management plan for the particular software.

FHI’s Safety and Health organization has an inventory comprising approximately 45 different software applications. When the organization found it could not meet the March 31, 2003 deadline for bringing software into compliance with the requirements of HNF-PRO-309, it submitted a document variance specifying that all required software would be in compliance by June 30, 2003. At the time of this assessment, the software was still not in compliance with HNF-PRO-309. Also, there was no evidence that the document variance was revised to extend the deadline date for compliance.

RL Closure Required: YES [X] NO [ ]

(F-4) Finding A-04-SED-FHI-009-F04

FHI failed to specify quality assurance requirements for subcontractors performing fire hazards analyses of nuclear facilities. **[QA-PRO, IS-FP&P, ISMS-ANLYZE]**

Requirements:

1. HNF-MP-599, Revision 12, Section 7.0, Paragraph 2.2, "Content of Procurement/Acquisition Documents," states, "1. Procurement/acquisition documents for items or services requiring controls beyond standard commercial practices shall include as applicable: …

    f. QA requirements applicable to the scope of work and commensurate with the importance and/or complexity of the item or service…"

2. HNF-MP-599, Revision 12, Section 7.0, Paragraph 2.3, "Supplier Evaluation and Selection," states, "3. Once selected, suppliers of the following items (…) or services, at a minimum, shall be identified on the FH ESL:

    a. Safety Class or Safety Significant items and associated services."

3. HNF-MP-599, Revision 12, Section 6.0, Paragraph 2.2, Item 9, "Computer software used to originate or verify safety or other risk-significant design solutions during the design process shall be validated, and the status of validation shall be identified and documented prior to use."
4. HNF-RD-10768, Revision 0, Requirement 27, "Software testing shall include development testing, verification testing, and validation testing, when appropriate."
5. HNF-RD-10768, Revision 0, Requirement 28, "Software shall be acceptance tested when installed, after changes, and periodically during use, as appropriate."

Discussion:

The assessment team reviewed the procurement process for an FHI subcontractor, FP2, Inc., performing fire hazard analyses (FHAs) for nuclear facilities. It found that FHI had not evaluated FP2 and had not placed it on the Evaluated Suppliers List (ESL) as required by FHI procedures. FHAs are used in the development of nuclear facility DSAs, so contractors performing this work are required to be listed on the ESL.

Also, the contract statement of work in the FP2 contract did not specify any quality assurance requirements and so did not specify any software quality assurance requirements. FP2 used the computer code CFAST to perform FHAs. However, contrary to FHI requirements, FP2 did not perform installation and validation testing of CFAST.

FHI routinely procures services for preparing FHAs for nuclear facilities, whose results are often used in the DSAs required by 10 CFDR 830, *Nuclear Safety Management*. Subcontractors performing FHAs frequently use CFAST. This code is maintained by the National Institute for Standards and Technology (NIST), and is readily downloaded from the NIST website or purchased on compact discs. While DOE has endorsed the use of this code, it has also evaluated and identified its limitations and weaknesses. Software quality assurance requirements require installation V&V and validation for proper use of the code.

After the assessment team brought this problem to the attention of FHI management, FHI issued an occurrence report, dated April 6, 2004, for FHI site-wide facilities, which declared a potential inadequacy of documented safety analyses (PISA), per requirements of 10 CFR 830.203(g).

RL Closure Required: YES [X] NO [ ]

(F-5) Finding A-04-SED-FHI-009-F05

FHI and Duratek do not always adequately implement software V&V and configuration control requirements. **[CONOPS-INDVER, QA-INSP, ISMS-WORK]**

Requirements:

1. HNF-RD-10768, Revision 0, *Computer Software Requirements*, Section 2.0, Requirement No. 27 states, "Software testing shall include development testing, verification testing, and validation testing, when appropriate."

2. HNF-RD-10768, Revision 0, *Computer Software Requirements,* Section 2.0, Requirement No. 7 states, "Computer software used in applications important to safety, health, environmental, and quality aspects of Project Hanford activities, including design calculations and laboratory analysis, shall be subject to appropriate controls, including configuration management, throughout the software life cycle."

3. HNF-RD-10768, Revision 0, *Computer Software Requirements*, Section 2.0, Requirement No. 38 states, "Software design products shall be verified and validated by individuals other than those who performed the work."

4. HNF-MP-599, Revision 12, Section 8, Paragraph 2.2 (1) states, "inspections and acceptance tests shall be performed by technically qualified personnel, other than those who performed or directly supervised the work, and who have the freedom of access and communication to conduct and report…."

The following FGG requirements are provided only as reference for what served as the basis for FGG personnel. These requirements are not controlling since FGG personnel must perform work to FHI requirements.

- Fluor Federal Services Practice 134 200 0960, *Control of Engineering Software,* section on Approval for Use states, "Before using the program, the authorized user …
    - Ensures that the intended use of program is within program limitations and uses for which it was verified.
    - Confirms an in-use test has been successfully performed …"

- Fluor Federal Services Practice 134 200 0960, *Control of Engineering Software,* section on Verifying Commercial Software, Step 3 states, "The assigned verifier prepares sample problems designed to exercise the program over the whole range of variables. The sample problems are designed to test all of the functions of the program that will be used by FFS engineers in performing design and analysis."

Discussion:

The assessment team reviewed documentation of V&V and found a number of inadequacies. These included (a) a lack of adequate V&V planning and test documentation; (b) a lack of adequate software testing for intended application; (c) a lack of adequate configuration control of computer code versions; and (d) lack of sufficient independence in V&V. The following are examples of conditions that led the assessment team to its conclusions:

- FGG personnel working in staff augmentation roles did not perform the formal V&V of software as required by FHI procedures and did not maintain configuration control of the codes. FGG personnel did not perform V&V of three of the various GXQ revisions, which were used extensively at Hanford facilities. These code revisions provided enhancements, but also corrections to certain errors. The assessment team observed that different versions of the code were used by different staff members over the same period for different applications. Although the use of differing versions of a code with adequate validation does not necessarily present a configuration control issue, the concurrent use of different versions by different FGG staff members, with some versions not subject to V&V, indicated a deficiency in configuration control.

- In the case of the application PTW, an application module was used by FGG in design work, but it was explicitly excluded from V&V testing. The module was for transient motor starting, and was used in September-October 2003. FHI pointed out that the specific PTW module was not relied upon as design analysis or used in the development of a design, and that it was used as an independent check on an existing design and did not affect the design in any way. The assessment team believes that the use of a software module that is not adequately verified and validated for the purpose of independently checking and accepting a design is contrary to FHI requirements.

- Duratek used the computer code ALGOR without adequate validation for the problem they were solving. The problem was the analysis of a cask drop onto a hard surface. The assessment team reviewed the validation test problem (torsional oscillation of a gear shaft) and found that it was not similar to the problem being solved.

- A recent DOE Richland Operations Office surveillance [11] found that the Automated Job Hazards Analysis (AJHA) database software would print out radiation work permits (RWPs) that did not fully and correctly specify the approved entry requirements for some areas. The software has its own life cycle documentation, including software requirements specifications and test requirements. However, inadequacies in requirement specifications and validation testing for the changes resulted in the incorrect outputs. The assessment team acknowledges that the problem was obscure and technically difficult to identify. However, the system inappropriately allowed editing of database records that were in use. Records printed out by users while other individuals were editing them resulted in erroneous RWPs.

- In the case of RADCALC, a computer code upgraded by Duratek, V&V was performed by individuals not independent of the development of the software upgrade. The validation test plan was prepared by the system engineer who was instrumental in the development of the software upgrade. The RADCALC system engineer and programmer were on the V&V software development team, and the V&V testing was performed by some one who was not an approved software user.

- V&V tests for two modifications to the CLEM I&C software at FFTF were conducted by the design authority who directly supervises all changes to the CLEM software. These modifications were two of the three identified in an engineering document change document (HNF-EDC-03-16547, dated 9/29/03).

RL Closure Required: YES [X] NO [ ]

(F-6) Finding A-04-SED-FHI-009-F06

***FHI did not adequately implement software quality assurance requirements for legacy MICON I&C software at PFP.* [CONOPS-EQCTRL, QA-WORKPR, ENG-CHANGE, ISMS-WORK]**

Requirements:

1. HNF-PRO-309, Revision 4, Section 5.2, *Qualification of Legacy Software,* states, “1. Develop a list of Functional Requirements defining critical features,

capabilities and interfaces to be included for each software application assigned in the Software Implementation Plan."

2. HNF-PRO-309, Revision 4, *Computer Software Management*, Section 5.1, Step 2 states, "Prepare a Software Management Plan (SMP) which as a minimum contains the following:…
   - Configuration Management Methodology, including …
   - Methods to verify and validate software…"

3. HNF-MP-599, Revision 12, Section 5.0, Paragraph 2.6, *Control of Computer Software,* states, "Computer software used in applications important to safety, health, environmental, and quality aspects of Project Hanford activities, including design calculations and laboratory analysis, shall be subject to appropriate controls, including configuration management, throughout the software life cycle."

4. HNF-RD-10768, Revision 0, Requirement No. 25, "Change control processes shall provide objective evidence of evaluation, coordination, and approval of changes prior to implementation of the change."

5. HNF-PRO-309, Revision 4, Section 5.6, Step 9, "Determine if a major or minor change to the software is required to meet functional and performance requirements. If a major change is required, go to Section 5.3 and treat change as new development." [For process control software, this subsequently leads to Section 5.4 on software testing.]

Discussion:

HNF-PRO-309, Section 5.2, provides the steps for Qualification of Legacy Software, including the requirements for development of functional requirements and software evaluation. Section 5.1 of that procedure provides for a software management plan that would ensure adequate validation testing and configuration control for changes to software.

For legacy I&C software, the assessment team found deficiencies for the MICON distributed control system software at the Plutonium Finishing Plant (PFP). The MICON system performs an important safety-significant function (tripping the ventilation fans in 2736-ZB on fire alarm to prevent damage to air filters) as well as other functions that have safety implications.

The MICON system is covered by the PFP Software Management and Implementation Plan and has a configuration management plan. However, there is no current list of functional requirements or software specification for the software. The requirements for the system were developed from the existing piping and instrumentation drawings (P&IDs). Both the MICON system and the P&IDs have evolved and the traceability of software requirements to P&IDs is inadequate. There is also no formal listing of control parameters and alarm set-points. (The alarm set-points are provided in the MICON software documentation, HNF-SD-CP-CSWD-16; however that information is part of software listing.) In October 2003, PFP Engineering compiled a design description document that incorporated all the changes made to the software and intended to be comprehensive. However, the associated documentation does not show that a formal V&V plan, test, and report were completed for the significant changes. Also, there is no formal validation of the design description.

The assessment team noted a MICON software change to modify facility instrumentation (annunciation alarm) set points was made in October 2003, which did not have adequate work authorization and V&V test documentation. The design authority for this application said that, "changing the set point did not require a work package, and the acceptance criteria were met by observing the operation of the alarm during normal operations." This is contrary to requirements of QAPD Section 5.0, Paragraph 2.6, and HNF-RD-10768, Requirement 25. When the assessment team brought this issue to the attention of FHI management, PFP issued a surveillance report [12] with two findings on March 31, 2004.

The software implementation plan for MICON, *Computer Software Configuration Management Plan for PFP MICON Automation System,* places the system software in the Software Operation and Maintenance life cycle stage (HNF-PRO-309, Section 5.6). Section 3.2.1 of the plan describes the procedure for making software changes. This procedure does not distinguish between a major and a minor change and is not consistent with the provisions of HNF-PRO-309, Section 5.6. Specifically, a determination of a major change should require application of software testing requirements of HNF-PRO-309, Section 5.4.

RL Closure Required: YES [X] NO [ ]

(F-7) Finding A-04-SED-FHI-009-F07

FHI and Duratek do not identify and formally document computer software user qualification and training requirements. **[QA-TRAIN, ISMS-DEFINE]**

Requirements:

1. HNF-MP-599, Revision 12, *Quality Assurance Program Description,* Section 2.0, Paragraph 2.2, "Training and Indoctrination," states, "1. Training and indoctrination needs for personnel shall be identified and documented, and resources provided."

2. HNF-MP-599, Revision 12, *Quality Assurance Program Description,* Section 2.0, Paragraph 2.2, "Training and Indoctrination," states, "3. Personnel training shall be provided to achieve initial proficiency, continued to maintain proficiency, and adapt to changes in technology, methods, or job responsibilities."

3. HNF-RD-1819, Revision 2, Section 4.1.4 (b) states, "Personnel assigned to design activities shall be qualified individuals who are trained to conduct the assigned activity."

Discussion:

Contrary to the above requirements, FHI and Duratek do not establish formal qualification and training requirements for users of a software application. Such requirements, when properly tailored to the technical complexity of the software, provide an objective basis for qualifying users and maintaining status of their qualification and training (and retraining retraining, as necessary).

Additionally, the principal users of certain computer codes acknowledged that formal training was not given to the authorized users. Examples of such codes (with organizations controlling the software shown in parenthesis) are ORIGEN 2.1 (Duratek), ORIGEN S.2 (FGG), and Power*Tools for Windows (FGG).

RL Closure Required: YES [X] NO [ ]

(F-8) Finding A-04-SED-FHI-009-F8

FHI's software quality assurance procedures do not implement the NQA-1, Subpart 2.7 requirements for software procurement and for reporting software errors between FHI and its suppliers. **[QA-PRO, ISMS-FEEDBK]**

Requirements:

1. HNF-MP-599, Revision 12, *Quality Assurance Program Description,* Section 1.0, Paragraph 2.20, "Software acquisition, development, operations, maintenance, and retirement shall be developed and documented in accordance with procedures based on ASME NQA-1, Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Application*."

2. NQA-1-1994, Subpart 2.7, Section 10, "Contracted Software," specifies requirements for purchasing and contracting computer software.

3. NQA-1-1994, Subpart 2.7, Section 8, "Problem Reporting and Corrective Action," states, "A formal procedure for software problem and corrective action shall be established for software errors and failures. This problem reporting system shall assure the problems are promptly reported to affected organizations to assure formal processing of problem resolutions."

4. NQA-1-1994, Subpart 2.7, Section 10.1, "Contracted Software," states, "The supplier shall report software errors or failures to the purchaser, and the purchaser shall report software errors to the supplier."

Discussion:

Contrary to the above requirements, FHI did not implement the procurement requirements of NQA-1, subpart 2.7. These requirements are not addressed in either HNF-RD-10768 or HNF-PRO-309.

Further, FHI also did not implement a process for either reporting errors to suppliers or for dispositioning errors reported by suppliers, as required by NQA-1, Subpart 2.7. Management of error reporting with suppliers is also not addressed in either HNF-RD-10768 or HNF-PRO-309. In several instances, FHI did not have maintenance contracts with software or firmware vendors, and it could not be assumed that vendors would notify users of errors. The I&C software MICON at PFP, and CLEM and SRS at FFTF are examples of this situation.

FHI managers told the assessment team that specifying technical requirements in contracts was the responsibility of personnel preparing purchase requisitions. An individual preparing a purchase requisition was expected to research the requirements, including those in NQA-1, and make sure that all necessary requirements were in both the purchase requisition and the contract. In the view of the assessment team, the absence of implementing requirements in FHI requirements documents and procedures could be interpreted by personnel preparing purchase requisitions as FHI policy not to implement the specific requirements of NQA-1 for software procurement and software error reporting.

RL Closure Required: YES [X] NO [ ]

(F-9) Finding A-04-SED-FHI-009-F9

> ***The FHI assessment program failed to identify inadequacies in its software quality assurance program.*** **[QA-ASSMNT, ISMS-FEEDBK]**

Requirements:

HNF-MP-599, Revision 12, *Quality Assurance Program Description,* Section 10.0, Paragraph 2.1.2 states, "Independent assessments shall be planned and conducted to measure the adequacy of work performed in complying with applicable requirements and determine the effectiveness of QA Program implementation."

Discussion:

Contrary to the above requirement, the FHI assessment program did not comprehensively assess the implementation of software quality assurance requirements. As a result, significant non-compliances, such as those identified in this report, went undetected.

The following are examples of conditions that led the assessment team to its conclusion:

- The last comprehensive assessment of computer software control was conducted by DOE in 1999. Since 1999, FHI has conducted a number of surveillances and limited-scope independent assessments, but it has not conducted a programmatic assessment of computer software quality assurance.
- FHI has scheduled a company-wide assessment of the FHI software quality assurance program for September 2004, but this is more than two years after HNF-PRO-309, Revision 4 was issued for implementation.
- A number of organizations did not bring their software into compliance with Revision 4 of HNF-PRO-309 by the deadline date of March 31, 2003 and did not have the required approved variance. An FHI independent assessment should have identified this problem before it was identified by this assessment team.
- FGG personnel, working in FHI staff augmentation positions, used computer software that was not controlled in accordance with the FHI software quality assurance program. An FHI independent assessment should have identified this problem before it was identified by this assessment team.

RL Closure Required: YES [X] NO [ ]

4.3 Observations

(O-1) Observation A-04-SED-FHI-009-O01

FHI's software quality assurance requirements cannot be unambiguously determined from the Quality Assurance Program Description. **[QA-QAPROG, ISMS-IDHAZ]**

Requirements:

Referring to the development of quality assurance programs, 10 CFR 830.121(c)(3) states that contractors are to "use voluntary consensus standards in its development and implementation, where practicable and consistent with contractual and regulatory requirements, and identify the standards used."

Discussion:

HNF-PRO-599, Revision 12, *Quality Assurance Program Description* (QAPD), identifies the specific quality assurance requirements that FHI has committed to implement. FHI has chosen to base its quality assurance program on NQA-1, and, in most cases, identifies the NQA-1 requirements that it is implementing. However, in the case of computer software quality assurance, the QAPD, Section 1.0, Paragraph 2.20, simply states, "Software acquisition, development, operations, maintenance, and retirement shall be developed and documented in accordance with procedures based on ASME NQA-1, Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Application*." It does not identify the requirements of Subpart 2.7 that are to be implemented. While there are several passing references to software quality assurance requirements in other parts of the QAPD, these do not systematically identify the requirements to be implemented.

As an example, the requirements for the control of nonconforming items are clearly described in QAPD Section 3.0, *Quality Improvement*, Paragraph 2.4, "Nonconformance Control." Also, Section 6.0, *Design*, Paragraph 2.2, "Design Process," specifies clear requirements for the engineering design process. However, the QAPD lacks this level of clarity for software quality assurance requirements. For example, the requirements of Subpart 2.7 for problem reporting and corrective action are not explicitly addressed in the QAPD.

The situation is confused further by the fact that FHI has not identified the edition of NQA-1 upon which it bases its quality assurance program. While HNF-RD-10768, Revision 0, *Computer Software Requirements*, identifies requirements from NQA-1-1994, FHI personnel said that FHI is not implementing a specific edition of NQ-1. Since the requirements of Subpart 2.7 vary significantly between editions of NQA-1, the specific software quality assurance requirements to which FHI is committed to DOE cannot be reliably determined from the QAPD.

RL Closure Required: YES [ ] NO [X]

(O-2) Observation A-04-SED-FHI-009-O02

FHI requirement for controlling access to SRS I&C software at FFTF was compromised. **[CONOPS-EQCTRL, QA-WORKPR, ISMS-WORK]**

Requirement:

> HNF-RD-10768, Revision 0, Requirement No. 47 state, "Controls shall be established to permit authorized and prevent unauthorized access to a computer system."

The assessment team discovered that the above FHI requirement for access control was significantly compromised for the SRS I&C software at FFTF. The key was checked out more than a year ago with inadequate entry in the key log, and the key was left in the lock. Furthermore, the key to the key box that contains critical keys, such as for the SRS, was found in an unlocked and readily accessible location.

RL Closure Required: YES [ ] NO [X]

(O-3) Observation A-04-SED-FHI-009-O03

FHI and Duratek do not require each authorized user of an approved safety analysis or design computer program to maintain a record of computer program use. **[CONOPS-LOGS, QA-DOC, ISMS-WORK]**

Discussion

The assessors believe that FHI and Duratek should establish a requirement for recording and maintaining the usage of safety analysis and design computer programs. A computer program use record aids significantly in providing traceability between the computer program version used and the specific safety analysis or design application. This would be an important in the event that a software error is identified that could have introduced errors into safety analysis and design work, particularly if the error is identified after the work has been completed. Such a requirement also has other advantages in reviewing the past and anticipated use of a particular computer program.

During its assessment, the assessors noted that FGG has an appropriate requirement for recording computer program usage in its procedure, *Control of Engineering Software*[(8).]. The assessment also revealed several computer programs for which FGG's Engineering Computer Program Use Record forms had not been adequately completed and maintained according to its procedure. When this issue was discussed with FGG, they acknowledged that the use record forms were not being maintained as required. Since this FGG requirement is not controlling for FGG staff working to FHI's software quality assurance requirements under staff augmentation agreement with FHI, the assessment team does not point this out as a finding.

However, the assessment team recommends that FHI and Duratek consider developing and implementing a requirement on recording computer program usage, such as that in FGG's procedure. Separate use record should be maintained for different versions of the same computer program, and user records should be reviewed on a regular basis by the technical lead for the computer program.

RL Closure Required: YES [ ] NO [X]

5.0 SUMMARY OF ASSESSMENT AREAS

The following provides a summary of assessment areas by the eight software quality assurance topics covered in the DOE CRADs. Since the contractor's software requirements address both I&C software and safety analysis and design codes, the summaries provide a combined assessment of these two types of computer software applications. The lists of documents reviewed and personnel interviewed were organized according to organization and the software application selected for assessment. These lists are provided in Appendix A-1 and A-2, respectively.

5.1 Software Requirements Description

Objective:

Software functions, requirements, and their bases are defined and documented.

Criteria:

1. The functional and performance requirements for the software are complete, correct, consistent, clear, testable, and feasible.
2. The software requirements are documented and consistent with the safety basis.
3. The software requirements description is reviewed, controlled and maintained.
4. Each requirement should be uniquely identified and defined such that it can be objectively verified and validated.

Summary:

The criteria were partially met for the software to which they were applicable.

In the case of safety analysis and design computer codes, software requirements description were not available for COTS (ALGOR, ANSYS, PTW) and government agency sponsored software, such as ORIGEN. However, information on software functionality and other requirements were obtainable and found satisfactory. Of the two custom software packages (RADCALC and GXQ), only RADCALC met the criteria for functional and software requirements. The software requirements description for RADCALC adequately addressed attributes such as functionality, performance, design constraints, and interfaces; and the documentation was excellent. In the case of GXQ, FGG continued to modify and update the GXQ code and FGG staff working as staff augmentation for FHI continued to apply the code to Hanford nuclear facilities. However, they did not update the requirements documentation.

In the case of I&C software, the functional requirements for SCIC, CLEM, and SRS were defined in sufficient detail. However, MICON did not have an adequate functional or software requirements document for the present configuration.

Related Noteworthy Practices, Findings and Observations:

Noteworthy Practice: (3)
Finding: (F-6)

5.2 Software Design Description

Objective:

The software design description (SDD) depicting the logical structure, information flow, logical processing steps, and data structures are defined and documented.

Criteria:

1. All software related requirements are implemented in the design.
2. All design elements are traceable to the requirements.
3. The design is correct, consistent, clearly presented and feasible.

Summary:

The criteria were partially met for the software to which they were applicable.

The assessment in this area of software QA was similar to that discussed for software requirements description. The only significant exception was in the case of MICON I&C software, where an updated design description was developed to incorporate all the major software modifications. However, this document lacks an adequate and independent validation. This is considered in the V&V assessment area.

Related Noteworthy Practices, Findings and Observations:

Noteworthy Practice: (3)
Finding: (F-6)

5.3 Software Verification and Validation (V&V)

Objective:

The software V&V process is defined and performed, and related documentation is maintained to ensure that (a) the software adequately and correctly performs all intended functions, and (b) the software does not perform any unintended function.

Criteria:

1. All analysis and design software requirements and software design have been verified and validated for correct operation using testing, observation, or inspection techniques.
2. Relevant abnormal conditions have been evaluated for mitigating unintended functions through testing, observation, or inspection techniques.

Summary:

The criteria were not met.

This assessment identified a lack of adequate V&V planning and test documentation in several instances, covering both safety analysis and design codes, and I&C software; examples include GXQ, CFAST, PTW, and MICON. Where software development and implementation relied on historic knowledge or expertise of a few individuals, as in the case of legacy I&C software and the code RADCALC, the assessment team found that sufficient independence in performing V&V by adequately qualified technical personnel was not achieved. Additionally, in the case of certain relatively complex codes (e.g., ALGOR), validation using properly matched test problems appeared to be lacking. Finally, the requirements for V&V planning and testing applied by FGG personnel working for FHI as staff augmentation were not fully consistent with the requirements of NQA-1 Subpart 2.7, which are embodied in FHI's requirements.

Related Noteworthy Practices, Findings and Observations:

Findings: (F-1), (F-4), (F-5), (F-6)

5.4 Software User Documentation

Objective:

Software documentation is available to guide the user in installing, operating, managing, and maintaining the software.

Criteria:

1. The system requirements and constraints, installation procedures, and maintenance procedures such as database fine-tuning are clearly and accurately documented.
2. Any operational data system requirements and limitations are clearly and accurately documented.
3. Documentation exists to aid the users in correct operation of the software and to provide assistance for error conditions.
4. Appropriate software design and coding documentation to assist in future software modifications is defined and documented.

Summary:

The criteria were generally met. A significant issue is the lack of established software-specific qualification and training requirements for users of safety software.

The assessment covered a diverse body of software in terms of type, ownership, use, and vintage. The assessment team found that the user documentation was generally adequate. It comprised documentation items such as installation procedures, system requirements, user and technical manuals, and built-in messaging for error handling. Vendors of COTS software provided test problems for users to validate software installation and use.

An additional focus of this assessment was the qualification and training of software users. The principal users or custodians of all software covered in the assessment were judged to be well qualified individuals. Also, a list of authorized users was always adequately maintained. However, there was no formal description of qualification and training requirements commensurate with the complexity of software within any of the organizations assessed. The need for establishing such requirements is particularly important in the case of sophisticated software (e.g., ALGOR) used to analyze complex problems. The assessment also identified that users did not receive formal software-specific training in several cases.

Related Noteworthy Practices, Findings and Observations:

Noteworthy Practices: (4), (5)
Finding: (F-7)

5.5 Software Configuration Management

Objective:

Software components, products, and related documentation are identified and maintained; and changes to those items are controlled.

Criteria:

1. All software components and products to be managed are identified.
2. For those components and products, procedures exist to manage the modification and installation of new versions.
3. Procedures for modifications to those components and products are followed.

Summary:

The criteria were not met.

Software configuration management is an important element of the requirements of HNF-PRO-309 for software management plans, and for developing software implementation plans for bringing legacy software into compliance with the requirements.
In the case of FHI's safety analysis and design codes, GXQ Version 4.0C and CFAST, such software management plans did not exist. Also the FHI Safety and Health organization which has numerous software applications that have safety implications did not have software management plans. FGG personnel perform considerable safety analysis and design work for FHI as staff augmentation, using various computer codes controlled by FGG. However, FGG software does not fully comply with the requirements of HNF-PRO-309 and does not have software management plans. FGG has self-identified certain gaps in the area of configuration control and other areas relative to HNF-PRO-309 on behalf of another client, but has not resolved them.

FGG's procedure on the control of engineering software imposes an excellent requirement for maintaining user logs for each computer code; however, the implementation of this requirement was non-uniform and inadequate based on several inconsistencies in the use record forms (e.g. for various versions of GXQ, ORIGEN S.2, and PTW). This is not pointed out as a finding since FGG's requirements are not controlling for FGG staff working for FHI as staff augmentation. FGG's requirement for recording computer usage, however, should be considered for implementation by FHI and its subcontractors since it has several advantages for analyzing the impact of errors discovered, as well as configuration and use control.

All of FHI's I&C software considered in this assessment had software management and implementation plans. However, the configuration controls specified in the software implementation plan for MICON were found to be inadequate allowing changes to be made without adequate V&V. The assessment team found that two significant engineering changes did not have adequate V&V, and one change was made without following the job control process properly and without adequate documentation for change validation. Subsequent to this observation, PFP issued two findings to correct the work package.

Related Noteworthy Practices, Findings and Observations:

Noteworthy Practice: (5)
Findings: (F-1), (F-2), (F-3), (F-5), (F-6)
Observations: (O-2) (O-3)

5.6 Software Quality Assurance

Objective:

SQA activities are evaluated for applicability to the analysis and design software, defined to the appropriate level of rigor, and implemented.

Criteria:

1. SQA activities and software practices for requirements management, software design, software configuration management, procurement controls, V&V (including reviews and testing), and documentation have been evaluated and established at the appropriate level for proper applicability to the software under assessment.

2. SQA activities have been effectively implemented.

Summary:

The criteria were not met.

FHI specifies how it implements 10 CFR 830.120 (the Quality Assurance Rule) in HNF-MP-599, Revision 12, *Quality Assurance Program Description* (QAPD). The QAPD identifies NQA-1, *Quality Assurance Program Requirements for Nuclear Facilities*[i] as the standard FHI applies to nuclear work. Software quality assurance requirements are drawn from NQA-1, Subpart 2.7, *Quality Assurance Requirements of Computer Software for Nuclear Facility Applications*. These FHI requirements, in turn, require software management plans for software that meet a defined set of criteria and software implementation plans for bringing legacy software into compliance with specified requirements.

However, this assessment identified a number of inadequacies in the implementation of FHI's requirements. Those include the following:

- FHI did not specify quality assurance requirements for subcontractors performing fire hazards analyses.
- FHI used subcontractors that were not evaluated in accordance with FHI procurement procedures to perform fire hazards analyses supporting documented safety analyses.
- FGG personnel working under the FHI quality assurance program used computer software that was not controlled under FHI software control procedures.
- Legacy safety software was not always controlled in accordance with the FHI requirements.
- The FHI Safety and Health organization has been delinquent since June 30, 2003 in bringing software into compliance with HNF-PRO-309 requirements.
- The Fire Department used the CFAST code to review and concur with fire analyses even though they did not control CFAST in accordance with HNF-PRO-309.
- The QAPD did not identify the specific software quality assurance requirements FHI was implementing
- FHI did not perform adequate independent assessments to identify the weaknesses in implementation of its software quality assurance requirements.

Related Noteworthy Practices, Findings and Observations:

Noteworthy Practices: (1), (3)
Findings: (F-1), (F-2), (F-3), (F-4), (F-8), (F-9)
Observation: (O-1)

5.7 Software Procurement

Objective:

Vendor-supplied software, either COTS software, custom-developed or modified, requires the appropriate levels of QA commensurate with the level of risk introduced by their use.

Criteria:

1. Procurement documents for acquisition of software programs identify the quality requirements appropriate for the level of risk introduced by their use.

2. Acquired software is verified to meet the identified quality requirements.

Summary:

The criteria were partially met.

For safety software created for FHI, the quality assurance programs for suppliers of software are evaluated; and various activities, such as system testing, provide assurance that the software meets quality requirements. When FHI purchases software licenses from vendors, the contract language specifies a requirement for the vendor to notify FHI of software errors. For example, the contract with Framatome ANP, Inc., specified a requirement that Framatome notify FHI of software errata. However, for some software, such as the MICON I&C system at PFP and the SRS I&C system at FFTF, FHI did not have a maintenance contract with the vendor and so was not routinely notified of software errata.

FHI's requirements documents, HNF-RD-10768 and HNF-PRO-309, do not implement procurement requirements of the NQA-1, Subpart 2.7 standard, as specified in the FHI QAPD.

FHI used subcontractors that were not evaluated in accordance with FHI procurement procedures to perform fire hazards analyses supporting DSAs.

Related Noteworthy Practices, Findings and Observations:

Noteworthy Practice: (2)
Findings: (F-4), (F-8)

5.8 Software Problem Reporting and Corrective Action

Objective:

Formal procedures for software problem reporting and corrective action for software errors and failures are established, maintained, and controlled.

Criteria:

1. Practices and procedures for reporting, tracking, and resolving problems or issues identified in both software items and software development and maintenance processes are defined, documented and implemented.

2. Organizational responsibilities for reporting issues, approving changes, and performing corrective actions are identified and effective.

Summary:

The criteria were generally met.

FHI has documented procedures for reporting, tracking, and resolving problems. FHI procedure HNF-PRO-309 provides a reasonable process for identifying and resolving software problems, and identifies who is responsible for completing each step of the procedure. However, neither HNF-PRO-309 nor any other procedure explicitly addresses reporting errors to software vendors, nor do they explicitly describe a process for dispositioning errors identified by software vendors.

Related Noteworthy Practices, Findings and Observations:

Noteworthy Practice: (6)
Finding: (F-8)
Observation: (O-3)

6.0 LESSONS LEARNED

The following summarizes the lessons learned for improving safety SQA assessment process and approach:

- Complete and accurate software inventory. Assembling and obtaining a correct inventory of all the software that should be considered for the assessment was a far more difficult task than was anticipated. Perhaps a major factor that made this task difficult was insufficient integration of appropriate FHI nuclear facility and nuclear safety staff knowledgeable of safety software during the early planning phase.

- Selected sample of software applications. The selection of safety analysis and design codes properly considered several factors, such as software type, complexity, vintage, current use, and safety significance (e.g., for spreadsheet and database applications with safety implications). However, some modifications were made to the selected sample during the assessment. Additional discussions during the planning would have avoided the changes.

- Role of I&C software in a safety I&C system. The assessment included some I&C software whose safety significance was uncertain at the start of the assessment, although some discussions were held with authorization basis staff. Additional discussions during planning would have helped provide better focus.

- Nature and availability of software life cycle documentation. The availability of software life cycle documentation in terms of its form and location varied considerably depending on the organization and the software itself. A better understanding of how the documentation could be made available for the software applications selected would have resulted in greater efficiency.

7.0 REFERENCES

1. *Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities,* Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1, U.S. Department of Energy, March 13, 2003.

2. *Criteria and Guidelines For the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities,* CRAD – 4.2.3.1, Revision 3, U.S. Department of Energy, October 24, 2003.

3. *Assessment Criteria and Guidelines for Determining the Adequacy of Software Used in the Safety Analysis and Design of Defense Nuclear Facilities,* CRAD – 4.2.4.1, Revision 3, U.S. Department of Energy, October 24, 2003.

4. *Quality Assurance Program Description,* HNF-MP-599, Revision 12, Project Hanford Management System, February 3, 2004.

5. *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications,* ASME NQA-1, Subpart 2.7, The American Society of Mechanical Engineers. [The FHI Quality Assurance Program Description (4), Section 2.20, refers to this document, but does not specify a specific version.]

6. *Computer Software Requirements,* HNF-RD-10768, Revision 0, Project Hanford Management System Requirements Document, June 27, 2002.

7. *Computer Software Management,* HNF-PRO-309, Revision 4, Project Hanford Management System Procedure, October 24, 2002.

8. *Control of Engineering Software,* Practice 134 200 0960, Fluor Federal Services, May 1, 2002.

9. *Engineering Calculations,* Practice 134 200 1020, Fluor Federal Services, March 1, 2002.

10. *Comparison of Fluor Federal Services Practice 134.200.0960, "Control of Engineering Software" to HNF-PRO-309, "Computer Quality Assurance Requirement,"* Fluor Memorandum, from C.T. Narquis to W.A. Holstein, April 30, 2001.

11. *Use of Radiological Work Permits,* Department of Energy Richland Operations Office Surveillance Report, S-04-OOD-SNF-013, March 26, 2004.

12. *Conduct of Operations: Chapter 8.1, Control of Equipment and System Status,* Fluor Hanford Surveillance Report, QA-PPQA-PFP-SURV-04-146, March 31, 2004.

APPENDIX A-1

DOCUMENTS REVIEWED

FLUOR HANFORD INC. (FHI) DOCUMENTS (GENERAL)

HNF-MP-599 Revision 12, *Quality Assurance Program Description* (2/3/04)

HNF-RD-10768 Revision 0, *Computer Software Requirements* (6/27/02)

HNF-PRO-309 Revision 4, *Computer Software Management* (10/24/02)

HNF-RD-10320 Revision 2d, *PHMC Acquisition System Requirements* (1/29/04)

HNF-PRO-123 Revision 10, *Requesting Materials and Services* (1/20/04)

HNF-PRO-268 Revision 12, *Control of Purchased/Acquired Items and Service* (2/2/04)

HNF-PRO-3144 Revision 5, *Supplier Quality Assurance Program Evaluation* (814/03)

HNF-RD-12439 Revision 0, *Data and Information Management Standards* (4/7/03)

HNF-PRO-10588 Revision 2, *Records Management Processes* (4/4/03)

HNF-RD-8310 Revision 2, *Document Control Program* (7/24/03)

HNF-RD-1819 Revision 2, *PHMC Engineering Requirements* (2/6/04)

HNF-RD-12491 Revision 0, *Software Accountability* (4/3/03)

HNF-PRO-311 Revision 2, *Functional Security Requirements/Application Development* (12/18/02)

HNF-PRO-596 Revision 2, *Certifying Sensitive or Essential Computer Applications* (12/18/02)

Safety Class/Safety Significant Systems Listing (2/25/04)

PPQA-INF-SURV-04-028, Surveillance Report: *Computer Software Management* (10/30/03)

WMP03-LW-GA-QA-035, LPCS Worker Assessment Report: *Computer Software Management* (9/30/03)

RL-PHMC-PFP-2001-0028, (Occurrence Report) *PFP Non-destructive Assay Measurement and Calculation Issues* (7/30/02)

FH-09A-01-046, *Portable Non-destructive Assay (NDA) at Nuclear Material Stabilization Project (PFP)* (10/17/01)

ESL Vendor NQA-1 Sub-Part 2.7 (no date)

Spent Nuclear Fuel Project (FHI-SNF)

EN-6-010-03, *Administrative Procedure, Calculations* (1/7/03)

MN-7-001-06, *Administrative Procedure, JCS Preventive Maintenance and Surveillance (PM/S) Module* (7/29/03)

CM-6-040-02, *Administrative Procedure, Verification and Validation of SNF Project Software* (5/2/01)

CM-6-013-05, *Administrative Procedure, Software (Non-Process Automation) Configuration Management* (7/30/03)

CM-6-037-04, *Spent Nuclear Fuel Project, Process Automation Software and Equipment Configuration Management* (7/30/03)

SNF-20678, 03-SNF/JKM-020 Letter, *Spent Nuclear Fuel Project-Software Management and Implementation Plan* (3/20/03)

SNF-6956 Revision 2, *System Configuration Management Implementation Procedure for the Cold Vacuum Drying facility Safety Class Instrumentation and Control System Software* (2/19/02)

FH-QA-03-029, FH-QA-OCRWM Audit-03-02, *Audit of Spent Nuclear Fuel Project* (7/9/03)

NTS-RL-PHMC-GENERAL-2002, *Noncompliance Report, Programmatic Issues with Software Quality Assurance* (1/22/02)

SNF-SURV-FY01-226, *SNF Project Assurance Surveillance Report* (10/1/01)

03-SNF-JKM-020, *Spent Nuclear Fuel Project Software Management and Implementation Plan (3/18/03)*

Fast Flux Test Facility Project (FHI-FFTF)

FFTF-EI-074 Revision 3, (FFTF Engineering Instruction) *Preparation, Release, and revision of Critical System Software* (4/22/03)

A-15 Revision 5F, *FFTF Key Control* (1/8/04)

Memo, *Fast Flux Test Facility Software Management and Implementation Plan* (4/1/03)

FFTF Closed Loop Ex-vessel Machine Control Software Documentation (listing Operating Procedures and Supporting Documents) (no date)

FFTF Qualified Refueling Personnel List which identifies CLEM and SRS users.

Fluor Hanford Safety and Health Software Management Plan (no document number) (7/2/03)

FHI SOFTWARE APPLICATIONS

CFAST (FHI)

Review Comment Record (RCR) for Project PFP/2736-Z-FHA (11/7/2000)

Review Comment Record (RCR) for HNF-SD-CP-FHA-002, Revision 2 (6/17/02)

CFAST *Baseline Software List* (no date)

CFAST *Software Installation and Checkout Form* (3/2/04)

CFAST *Software Quality Assurance Plan* (no document number) (3/2/04)

CFAST *Software Evaluation Form for Consolidated Model for Fire and Smoke Transport* (3/2/04)

SNF-4268 Revision 1, *FAST Input Data* (pages A-93 through A-99) (no date)

HNF-3553 Revision2, Annex B, *Cold Vacuum Drying Facility*, (February 2003)

SNF-4268 Revision 1, *CVDF Fire Scenario 4* (pages A-85 through A-102) (not date)

SNF-4942 Revision 1, *Spent Nuclear Fuel Cold Vacuum Drying Facility Implementation Plan for Fire Hazard Analysis Suggested Actions* (August 2000)

HNF-3673 Revision 2, Section 5.0 *Administrative Controls* (February 2003)

CP-24-001V Revision 0, *Control of Combustible Materials within CVDF* (3/10/04)

SNF-16575 Revision 0, *Cold Vacuum drying facility Analysis of the Fire Hazard Of a Wood Waste Crate in Bay 1* (5/15/03)

ASTM E 1591-00, *Standard Guide for Obtaining Data for Deterministic Fire Models*

CFAST Naming Convention and Product Information (3/8/04)

Explanation of CFAST Model (3/8/04)

Fire Growth and Smoke Transport Modeling with CFAST/FAST (3/8/04)

CFAST Reference Documents (3/8/04)

CFAST Examples of Model (3/8/04)

CFAST/FAST Version History (3/8/04)

CFAST/FAST Version 3 (3/8/04)

CFAST Version 5 Update (8/1/02)

National Institute of Standards and Technology (NIST) Technical Note (TN) 1299, CFAST, the Consolidated Model of Fire and Growth and Smoke Transport

U.S. Department of Commerce Special Publication 921, 2000 Edition, *A User's Guide for FAST\: Engineering Tools for Estimating Fire Growth and Smoke Transport* (January 2000)

NIST TN 1431, *A Technical Reference for CFAST: An Engineering Tool for Estimating Fire and Smoke Transport* (March 2000)

DOE-EH-4.2.1.4 - Interim- CFAST, *The CFAST Computer Code Application Guidance for DOE Documented Safety Analysis* (September 2003)

DOE-EH-4.2.1.3 - Interim- CFAST, *Defense Nuclear Facilities Safety Board Recommendation 2002-1 Software Quality Assurance Implementation Plan Commitment 4.2.1.3: CFAST Gap Analysis Interim Report* (January 2004)

CLEM (FHI-FFTF)

HNF-EDC-03-16547 (Engineering Document Change Control) CLEM software change so that "Jaws should be operable when load range limits are exceeded." (9/29/03)

HNF-EDC-02-12109 (Engineering Document Change Control) CLEM software changes "The grapple over-travel reset value is the calculated over-travel value for all locations." & "Floor valve purge is finished when the purge volume is => the purge set point." (9/17/02)

CLEM JCS Work Packages (as of 3/24/04), includes spread sheet of Work Packages 4F-01-1243, 4F-02-402/T, 4F-03-406 and Description of changes.

CLEM Software use from project start (3/1/97) to software validation (9/18/02).

MICON (FHI-PFP)

HNF-SD-CP-CSWD-16 Revision 3, *PFP-MICON DCS Computer Software Documentation* (12/2/03)

HNF-EDC-03-18388, *Engineering Document Change Control* (10/15/03)

ECN-191457 (Engineering Change Notice), *Supplement Change to SD-CP-CSWD-16 R2C to add 5 Room Temperature Indications to the MICON Cabinet in 2736-ZB to allow Remote Monitoring of Building Temperature*. (1/11/99)

ECN-666931 (Engineering Change Notice), *Supplement Change to SD-CP-CSWD-16 R2C to show changes to Control Logic so that the 300 Bus No Longer Needs to be De-energized to close the breaker.* (4/30/01)

HNF-FMP-03-18072 Revision 0, *PDIC-642 Alarm Setpoint* (10/2/03)

HNF-EDC-03-15989, *Engineering Document Change Control* (5/1/03)

HNF-SD-CP-CSCM-008 Revision 2, *Computer Software Configuration Management Plan for the Plutonium Finishing Plant MICON Automation System*. (5/1/03)

HNF-15941 Revision 0, *Plutonium Finishing Plant (PFP) Software Management and Implementation Plan (5/21/03), documented in HNF-EDC-03-15953* (5/21/03)

HNF-SD-CP-OMM-003 Revision 2, *PFP MICON Maintenance Manual* (2/17/98)

HNF-SD-CP-CSUD-004 Revision 2 *MICON View User Manual* (11/26/96)

HNF-SD-CP-CSCM-008 Revision 2, *Computer Software Configuration Management Plan for the Plutonium Finishing Plant MICON Automated System (5/1/03), documented in HNF-EDC-03-15989* (5/1/03)

HNF-FMP-03-18072 Revision 0, (Facility Modification Package) *Change PDIC-642 Alarm Setpoint* (10/2/03)

WHC-SD-610-ATR-002 Revision 0, *Project B610 Process Control Configuration Acceptance Test Report (6/27/95), documented in EDT 606653* (6/23/95)

HNF-SD-C189-ATR-002 Revision 0, *Acceptance Test Report (4/10/97), documented in EDT-620756* (4/8/97)

HNF-SD-C189-ATR-001 Revision 0, *Acceptance Test Report 2721-Z Upgrades* (2/3/98)

HNF-18060 Revision 0, *Implementation Plan for Compliance with HNF-PRO-309 (2/5/04), documented in HNF-EDC-03-16036* (Engineering Document Change Control) (2/5/04)

QA-PPQA-PFP-SURV-04-146 *Conduct of Operations: Chapter 8.1, Control of Equipment and System Status* (3/31/04)

ITEM011, *ITEM Report Course 200310 Low Level Wastewater Treatment Operations* (3/19/04)

FSP-PFP-5-8 Vol. 2 Revision 6, *Quality Assurance Program Plan 15.1* (12/4/02)

FSP-58, Section 13.4 Revision 23, Change 13, *Work Management Process Description and Job Control System Process* (3/11/04)

Hanford Controlled Vendor Information Package 20068, MICON

SCIC (FHI-SNF)

Framatome #51-5004581-07, STAR SFP1, *Application Software Requirements Specification (SRS) for Hanford SCIC* (10/11/00)

Framatome #51-5005590-04, *STAR SFP1 Hanford SCIC System Design Description (SDD)* (10/11/00)

Framatome #51-5006606-00, *Hanford CVDF SFP1 Software Test Plan* (2/28/00)

Framatome #51-5006907-02, *Test Report for Safety Function Processor 1* (10/11/00)

Framatome #51-50046649-07, *Hanford CVDF STAR SFP1 Tracking Matrix* (10/11/00)

Framatome #51-51-5005739-05, *Hanford CVDF STAR SFP1 Software Requirements Review (SRR) Report*

Framatome #51-5009241-01, *Hanford CVDF STAR SFP1 Software Design Review (SDR) Report* (10/11/00)

Framatome #51-5009415-01, *Hanford CVDF STAR SFP1 Software Code Review (SCR) Report* (10/11/00)

Framatome #51-5003996-07, *STAR Hanford CVDF SCIC SFP2 Software Requirements Specification (SRS)* (9/19/00)

Framatome #51-5003997-07, *STAR Hanford CVDF SCIC SFP2 System Design Description (SDD)* (10/2/00)

Framatome #51-5006106-00, *Hanford CVDF SFP2 Software Test Plan* (2/8/00)

Framatome #51-5006766-02, *Test Report for Safety Function Processor 2* (10/11/00)

Framatome #51-5004712-05, *Hanford CVDF SFP2 Tracking Matrix* (10/3/00)

Framatome #51-5005961-03, *Hanford CVDF STAR SFP2 Software Requirements Review (SRR) Report* (10/3/00)

Framatome #51-5009095-01, *Hanford CVDF STAR SFP2 Software Design Review (SDR) Report* (10/6/00)

Framatome #51-5009613-01, *Hanford CVDF STAR SFP2 Software Code Review (SCR) Report* (10/9/2000)

Framatome #51-5003747-10, *STAR Function Requirements Addendum for the Hanford CVDF SCIC* (8/29/00)

Framatome #51-5003919-00, *Hanford CVDF STAR V&V Plan* (4/14/99)

Framatome #56-1224788-03, *Requested Software V&V Assignment Sheets*

Framatome #51-5010029-00, *Hanford CVDF SCIC Final Report* (10/12/00)

HNF-3229 Revision 2a, *Cold Vacuum Drying Safety Class Instrumentation and Control System Performance Specification* (4/12/99)

SP-93-002V, *Calibration of Bay 4 STAR Processor Module and Analog voltage Input Module (AVIM) (OCRWM)* (6/27/03)

Cold Vacuum Drying, Safety Class Instrumentation and Control System Statement of Work (8/4/99)

SRS (FHI-FFTF)

HNF-FMP-01-9280-R0C (Facility Modification Package) “This change releases the Test Specification for acceptance testing of the SRS control system upgrade.” (1/2/02)

DR-41D-01-001 Revision 0, Test Report - *SRS Control System Upgrade* (3/06/03)

FFTF-5632, Revision 0, Attachment 1, *SRS SW Loop Test Data Sheet* (12/8/00)

FLUOR GOVERNMENT GROUP (FGG) DOCUMENTS (GENERAL)

Practice 1342001020, *Engineering Calculations* (3/1/02)

Practice 134290112, *Technical Peer Reviews* (11/22/99)

Practice 1342000960, *Control of Engineering Software* (5/1/02)

Practice 1340001100, *Quality Management Program* (5/1/02)

SGS 01.001 (letter) *Custodianship of Spray & GXQ Codes* (2/5/01)

CTN-2001-042 (letter) *Comparison of Fluor Federal Services Practice 1342000960 to HNF-PRO-309 Computer Quality Assurance Requirement* (4/30/01)

FGG SOFTWARE APPLICATIONS
(USED BY FGG PERSONNEL IN FHI WORK AS STAFF AUGMENTATION)

ANSYS

HNF-MR-0554 Revision 0, *ANSYS Verification Plan 5.2* (2/7/96)

HNF-MR-0554 Revision 1, *ANSYS Verification Report 5.2* (9/22/97)

ANSYS Release 5.7 *Verification Test Summary for FLAN System Workstation*

ANSYS Release 5.5 *Verification Report*
ANSYS *Error Report Update* (4/10/96 and 9/2/92)

ANSYS ERRATA Sheets From 10/96 to Present

E-NW-193, *Engineering Computer Program Use Records* for ANSYS Versions 7.1, 5.7, and 5.5

PN-R300.50-1, -2, -3, and -4, *ANSYS User's Manual* (12/23/92)

P-NW-304, *ANSYS Administrative Procurement Action Request* (12/3/03)

ANSYS Release Notes for Versions 7.1, 5.7, 5.5, and 5.4.

Invoice # 3074047 From ANSYS Inc., *QA Testing Services Annual Subscription Agreement* 11/24/03

GXQ

RPP-13482 Revision 1, *Atmospheric Dispersion Coefficients and Radiological and Toxicological Exposure Methodology for Use Tank Farm* (7/29/03)

HNF-SD-WM-TI-733 Revision 1, *Supporting Calculations & Assumptions for Use in WESF Analysis (3/7/97), documented in ECN 632064 Engineering Change Notice* (3/7/07)

BEH-97-013 (Interoffice Correspondence) *Authorized User List for Software Code GXQ* (5/16/97)

RJP-04-001 (Memo) *Authorized User List for the Software Code GXQ* (3/8/04)

WHC-SD-GN-SWD-30002 Revision 1, *GXQ 4.0 Program Users Guide* (12/19/94), documented in ECN-609884 Update of GXQ Program Users Guide Version 4.0 (5/10/95)

WHC-SD-GN-SWD-30003 Revision 1, *GXQ 4.0 Program Verification and Validation* (5/9/95), documented in ECN-609885 Update of GXQ Program Verification and Validation for Version 4.0 (5/10/95)

E-NW-193, Engineering Program Use Record for GXQ Re. 4.0, 4.0A, B, C, D & F.

White Paper, *Changes to GXQ Version 4.0* (3/25/04)
White Paper, *Evolution of GXQ Version 4.0* (3/25/04), and
White Paper, *GXQ Validation History* (3/25/04)

ORIGEN 2 Version S.2

HNF-20020 Revision 0, CSER 04-004: *Criticality Safety Evaluation Report for Unirradiated FFTF Fuel Assembly Transfer to and Storage in Interim Storage Vaults* (March 2004), documented in HNF-EDC-04-20284 (Engineering Document Change Control) (2/17/2004)

HNF-8696 Revision 0, *Software Certification Report for ORIGEN Version S.2* (8/28/01)

FDNW-RJP-98-005 (Interoffice Correspondence) *Controlled Software/ORIGEN 2* (1/26/98)

HNF-SW-SNF-TI-061 Revision 1, *Shipping Port Pressurized Water Reactor Core 2 Blanket Assemblies Source Term Calculations Using ORIGEN 2* (8/10/99), documented in ECN 655253 (7/22/99)

SNF-TP-991107/Task Order 99-006B Revision 2, *Single Use Letter Report for the Verification and Validation of the RADNU-2A and ORIGEN 2 S.2 Computer Codes* (4/29/99)

HT-2001-027 (Memorandum) *Authorized User List for Software Code RADNUC 2A* (8/9/01)

HT-2001-026 (Memorandum) *Authorized User List for Software Code ORIGEN2* (8/29/01)

HT-2001-032 (Memorandum) *CDR Backup for ORIGEN 2 and RADNUC 2A* (9/7/01)

White Paper, *RSIC Code Package CCC-217* (1981)

PTW

CALC No. PTW 4.5.3.0, *PTW Verification* (7/29/03)

CALC No. PTW 32v 4530, *PTW Arc Flash Verification* (7/28/03)

CALC No. PTW 4.5.2.3, *PTW Verification* (4/16/03)

CALC No. PTW 4.5.1.1, *PTW Verification* (2/4/03)

CALC No. PTW 3.8.1.0, *PTW Verification* (1/9/01)

CALC No. PTW 3.7.2.0, *PTW Verification* (11/27/00)

CALC No. PUREX - *Short Circuit* (3/9/04)

Power Tools for Windows User Guide (11/16/01)

E-NW-193 Engineering Computer Program Use Records for Versions 4.5.3.0, 4.5.2.3, 4.5.1.1m 4.5.1.0, 4.0.2.6, 4.0.2.4, and 3.8.1.0

PTW User List (e-mail) (11/30/00)

Administrative Procurement Action Request (APAR), Purchase Arc Flash Component of PTW (10/7/02)

Administrative Procurement Action Request (APAR), Maintenance Renewal for PTW software (7/17/01)

Administrative Procurement Action Request (APAR), Maintenance & Support for System Analysis Inc. (SKM) Power Tools Software (8/28/00)

PTW-TMS Problem (e-mail from SKM) (12/13/00)

DURATEK DOCUMENTS (GENERAL)

DFSNW-QAP-001 Revision 5, *Quality Assurance Procedure* (3/10/03)

ICN-01, *Interim Change Notice (ICN) Software Management* (9/10/02)

ICN-01, *Preparation and Checking of Calculation Packages* (10/22/03)

Review of Duratek Federal Services Inc. QAM Adequacy to meet NQA-1 1994, Subpart 2.7 Requirements (no date)

Duratek *Approved Software & Hardware* list (3/18/04)

Duratek *Approved User List* (3/18/04)

Duratek *Software System Engineer* list (3/18/04)

Duratek *Software Quality Plan Revision 1, Level 1 Acquired Computer Codes* (3/16/04)

DURATEK SOFTWARE APPLICATIONS

ALGOR

ALGOR User Guide Revision 5.2, Vol. 1, 2, and 3 (2/10/03)

ALGOR Software Installation CD (2/21/04)

ALGOR Accuracy Verification Examples Manual CD - Part # 709.501 (12/20/02)

DFSNW-ECAL-211 (Engineering Analysis/Design Calculation) *T Plant Macro-encapsulation Container 0006038* (5/20/03)

ALGOR Accuracy verification Examples Manual, Revision 16 (12/20/02)

Duratek Software Installation & Checkout Form for ALGOR (3/4/04)

Duratek Existing Software Evaluation Report (3/1/04)

Duratek Commercial Off-the-Shelf Software Training Acknowledgement (two ALGOR users)

ORIGEN 2.1

CCC-371/ORIGEN 2.1, *RSICC Computer Code Collection* (May 1999)- Also *Software Installation & Checklist Form Version 2.1* (2/10/03)

CCC-371/ORIGEN 2, *RSIC Computer Code Collection* (July 1980)

Software Installation & Checkout Form for Computer #7200027498 (11/19/03), #5648611 (3/10/04), #352QS01 (10/15/03), and #00022 (2/27/02)

Existing Software Evaluation Report ORIGEN 2.1 (3/29/01)

DTS-ECAC-251 (Engineering Analysis/Design Calculation) *222-S Bulk Liquid Scintillation Waste Drum Characterization* (2/11/04)

RADCALC

DTF #1292 (Data Transmittal Form) *RADCALC 3.0 Software Requirements Specification* (5/30/01)

RADCALC Training (Two RADCALC User Training Documentation)

DFNW-VV-014 Revision 0, *RADCALC 3.0 Verification and Validation Test Report* (9/25/01)

DTF #01293 (Data Transmittal Form) for *NTP RADCALC* (8/7/01)

DFSNW-VV-013 Revision 0, *RADCALC 3.0 Verification and Validation Test Procedure* (8/22/01), documented in DTF #01315 (Data Transmittal Form) NTP RADCALC (8/28/01)

DFSNW-RPT-042 Revision 0, *RADCALC 3.0 Volume I: User's Manual* (November 2001)

DTS-RPT-066 Revision 0, *RADCALC 4.0 Software Design Description* (March 2004)

APPENDIX A-2

PERSONNEL INTERVIEWED

FLUOR HANFORD, INC. (FHI)

Karolyn Friday, Information Resources Management
Jack Garvin, Nuclear and Criticality Safety
Scott Spencer, Central Engineering
Katt Thompson, Quality Assurance Programs
Bill Hoogendoorn, Contracting Officer
Dave Fraley, Information Resources Management

FHI I&C SOFTWARE APPLICATIONS

Spent Nuclear Fuel Project (FHI-SNF)

John Dearing, SNF/CVDF Project Manager
Dick Whitehurst, DMJM Technology
Barbara Phillip, COGEMA Systems Engineering
John Diehl, SNF QA

Fast Flux Test Facility Project (FHI-FFTF)

George Ruge, FFTF Engineering Team Lead, Fuel Handling I&C

Plutonium Finishing Plant (PFP) Project

Keith Bonser, Plateau Projects Quality Assurance
Nathan Cathy, Manager, Nuclear Safety
Jim Daniels, Facility Engineering
Keith Hampton, Lead, Facility Engineering
Mel Higginson, PFP Chief Information Officer
William Doggett, (PFP PTW application)
Tom Ibson, LMIT, PFP Analytical Lab Software Management and Implementation Plan

CLEM (FHI-FFTF)

Mike Anglesey, User
John Logan, FFTF Engineering Electrical, and Design Authority for CLEM

MICON (FHI-PFP)

Greg Silvan, MICON Cognizant Engineer, Design Authority for HVAC

SCIC (FHI-SNF)

Dick Whitehurst, DMJM Technology
Barbara Phillip, COGEMA Systems Engineering

SRS (FHI-FFTF)

Lowell Hill, FFTF Engineering Design Authority for SRS
Duane Lenkersdorfer, User

FHI SAFETY ANALYSIS AND DESIGN AND OTHER SOFTWARE

AJHA

Miles Jaeger, AJHA Program Administrator
Mark Hermanson, AJHA System Analyst

CFAST (FHI)

Dave Mertz, Fire Prevention
Jim Robanske, Information Services
Al Ramble, FHI Nuclear Safety Manager
Stan Wallace, FHI Fire Protection Engineer

LANMAS

Aaron Greenhalgh, Technical Authority
Gary Hulse, Technical Support

SAFETY AND HEALTH SOFTWARE

Lanette Adams, Technical Authority

FLUOR GOVERNMENT GROUP (FGG)

Dwight Brayton, River Protection Project (RPP)
Cliff Narquis, RPP QA/QC Manager
Raymond Puigh, Manager, Nuclear Safety Group
Jay Lan, Criticality & Shielding

FGG SOFTWARE APPLICATIONS (FGG MANAGERS AND PERSONNEL PERFORMING FHI WORK AS STAFF AUGMENTATION)

ANSYS

Susan Farmworth, Civil/Structural Engineering Manager, User
K. C. Tu, Principal User

GXQ

Brit Hey, Former Principal User
Paul Rittman, Principal User
Raymond Puigh, Manager Nuclear Safety Group

ORIGEN 2 Version S.2

Ray Puigh, User
Kevin Schwinkendorf, Code Custodian, User
Hans Toffer, Manager, Criticality and Shielding
Jay Lan, Nuclear Criticality Safety
Warren Wittekind, Safety Analysis and Nuclear Engineering

PTW

Elliot Ahola, Principal User
Greg McDonald, Electrical Engineering Manager, User
Keith Newhouse, User

DURATEK

Sid Ailes, Quality Assurance Manager
Dave Bergmann, Engineering Analysis Manager
John Reeves, Project Engineering Services Manager
Tina Romano, Software System Manager (software administrator)

DURATEK SOFTWARE APPLICATIONS

ALGOR

Doug Reid, Software System Engineer & User
Jeff Scott, User

ORIGEN 2.1

Tony Savino, Software System Engineer & User

RADCALC

Tony Savino, User

Appendix B

ASSESSMENT TEAM QUALIFICATIONS AND EXPERIENCE

Dr. Shivaji S. (Shiv) Seth, Team Leader – Dr. Seth is Senior Technical Advisor for Nuclear Safety at the DOE Richland Operations Office. He has reviewed the nuclear safety authorization basis and operational safety of several nuclear facilities at the Hanford site, including those where safety software is deployed both in safety systems and in analyzing facility safety. As a member of a DOE team responding to DNFSB Recommendation 2002-1, Dr. Seth was a contributor to the development of the DOE qualification standard for software engineers and the CRADs for safety software assessments. In February 2004, he was a member of the DOE software quality assurance inspection team for the Waste Treatment Plant under design and construction at Hanford.

Prior to joining DOE in 1996, Dr. Seth managed and guided several safety and systems engineering projects at the MITRE Corporation in support of the USNRC and DNFSB. He was the principal investigator of a major project for the USNRC for developing the guidelines, technical basis, and research needs for high-integrity (safety) software in nuclear power plant safety systems. This work (NUREG/CR-6263) has been cited as a resource in various USNRC Regulatory Guides.

Dr. Seth's 35 years of work in the nuclear field also includes nuclear reactor core design and analysis, optimization of the reactor fuel cycle, and safety and probabilistic risk analyses. These involved considerable programming and use of computers. His experience at a national laboratory includes planning and analyzing reactor critical experiments for investigating the design and safety of fast reactors and supervising reactor operations. These involved the use of digital instrumentation and control systems.

Dr. Seth holds Master's and Doctor's degrees in Nuclear Engineering from the Massachusetts Institute of Technology, Cambridge, Massachusetts, and has authored over 80 technical publications.

Clifford A. Ashley, Deputy Team Leader – Mr. Ashley has been leading and participating in quality assurance assessments and surveillances during the last 13 years for the US DOE. This includes nine years experience as a DOE Facility Representative, as well as service as subject matter expert and various quality assurance positions with the New Production Reactor Project and the Tank Waste Remediation System Project. Several assessments included or were focused on computer software quality assurance. In February 2004, Mr. Ashley actively participated as an assessor in a software quality assurance assessment of Bechtel National Inc., where safety design, analysis, instrument and control software applications were reviewed.

During 1979 to 1981, Mr. Ashley's primary responsibility was to program a HP-1000 computer to record and extract critical test data from DOD sidewinder missile servomechanisms.

Mr. Ashley holds a baccalaureate degree in electrical engineering from Washington State University (1975), and a Master of Science degree in Electrical Engineering from North Dakota State University (1976).

David H. Brown – Mr. Brown has been leading and participating in quality assurance assessments for 17 years. Several of these have included or been focused on computer software quality assurance. He has been certified as a Lead Auditor in accordance with the requirements of NQA-1, *Quality Assurance Program Requirements for Nuclear Facilities*, since June, 1987. Mr. Brown holds a baccalaureate degree in nuclear science from the State University of New York, Maritime College (1971). He received formal training in computer software quality assurance from the Pacific Northwest National Laboratory in May, 1992. He participated in development of the following DOE directives and documents:

- The DOE response to DNFSB Recommendation 2002-1, *Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities*.
- CRAD 4.2.3.1, *Criteria and Guidelines for the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities*
- CRAD 4.2.4.1, *Assessment Criteria and Guidelines for Determining the Adequacy of Software Used in the Safety Analysis and Design of Defense Nuclear Facilities*
- DOE-STD-1172-2003, *Safety Software Quality Assurance Functional Area Qualification Standard*

James J. McCracken – Mr. McCracken holds a Master Degree in Nuclear Engineering, is a Licensed Professional Engineer in Washington and California, and has extensive experience with computer software. He has been the Computer system Administrator for the process computer system in a large commercial nuclear power plant (Diablo Canyon, California). In addition, he has programmed in Unix and DOS environments using Fortran, C, and assembly language. He has used nuclear criticality codes LANL MCNP, PNNL MCNP Visual Editor and PNNL 1DB. He is also proficient in Microsoft Access and Excel programming, including the RL Office Radidose Accident Analysis Software.

Subir K. Sen – Currently with the DOE's Office of Environment, Safety and Health, Office of Quality Assurance Programs (EH-31), Dr. Sen has significant experience in the use and development of design and analysis computer software for commercial nuclear power plants and DOE nuclear facilities. Dr. Sen has participated in design review and preparation of safety evaluation reports for a number of DOE facilities where computer software was used extensively, such as Hanford Spent Nuclear Fuel Project and Savannah River Site's F&H Canyons' seismic vulnerability study. He has been a participant in and led independent assessment and inspection teams that conducted safety analysis reviews, studied ES&H vulnerabilities of DOE's nuclear material storage facilities, conducted inspections of nuclear D&D operational activities and functioning of essential safety systems. Dr. Sen was the project manager for the DOE sponsored and completed software KBERT that analyzes the ex-facility and in-facility consequence of an accident involving radioactive materials.

Dr. Sen has significant involvement in DOE's response to DNFSB's Recommendation 2002-1. Dr. Sen participated in the development of the DOE implementation plan and the software functional area qualification standard, and in the preparation of the two criteria, requirements, and approach documents used in DOE software quality assurance assessments.

During his 24 years of industrial and research experience, Dr. Sen led engineering teams in the design and analysis of nuclear and fossil power plants, in the use and validation of commercial software, and in the development of computer programs for design and research work.

Dr. Sen holds MS and D.Sc. degrees in structural engineering from Washington University in St. Louis. He is a member of the American Society of Civil Engineers and the Earthquake Engineering Research Institute. He is also a registered professional engineer. He has published in many technical journals and is trained in ISO 9000.