

the team, the design authority appeared to consider critical characteristics to be limited to those demonstrable by an operational test procedure. The team concluded that because operational test procedures are typically limited to a functional test of the system as a "black box," these tests would not be expected to address critical characteristics such as device ratings. Functional tests are necessary but not always sufficient to identify and demonstrate conformance to all critical characteristics of a safety significant structure, system, or component.

Issues:

- a. The design description document for safety class leak detection circuits and initial software release packages for safety significant saltwell PIC skid programmable logic controllers had not been subject to design verification. (Finding 12)
- b. The design description and commercial grade item (CGI) dedication for leak detection relay circuits did not identify or address all critical characteristics. (Finding 13)

Appraisal Form

Transfer Leak Detection System

Topical Area: Configuration Management	Criteria Met
Date: February 26, 2002	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Objective:

Changes to safety basis-related requirements, documents, and installed components are controlled.

Criterion:

2. Limited technical walkdown of selected system components verifies that the actual physical configuration of these components conforms to documented design and safety basis documents for the system.

Approach:

Records Review:

N/A

Interviews:

N/A

Observations:

- 2-1 Walk down selected system components and compare the actual physical configuration of these components to system documents such as design basis and safety/authorization basis documents, system design descriptions, and system drawings such as piping and instrumentation diagrams. Identify any temporary changes, or configuration discrepancies that call into question (1) the operability or reliability of the system or (2) the adequacy of the change control or document control processes, including drawing revision, applied to the system.

Process:

Records Reviewed:

- a. HNF-SD-WM-ER-736, Rev 0. *Intrinsically Safe Leak Detector Circuit Design Description*, Rev. 0 1998
- b. Dwg H-14-103791 *Skid P Pump and Instr Control Arrangement*
- c. Dwg H-2-34965 *Leak Detector Assembly Typical Details*

- d. Dwg H-2-69162 *Elect. Leak Detection and Misc. Diagram*
- e. Dwg H-2-73822 and H-2-73823 *Electrical Leak Detector Elementary Diagrams*

Personnel/ Positions Interviewed:

Field walkdowns were accompanied by system engineers for single shell tank leak detection systems, interim stabilization leak detection systems, cross site transfer leak detection systems, and site electricians and instrument technicians as needed for equipment access.

Evolutions/Operations/Shift Performance Observed:

- a. Field walkdown of interim stabilization leak detection system in A and AX Tank Farms
- b. Field walkdown of transfer leak detection system in A and AX Tank Farms
- c. Field walkdown of transfer leak detector equipment in U Tank Farm
- d. Field walkdown of transfer leak detector equipment in TX Tank Farms
- e. Field walkdown of cross site transfer system continuous leak detector stations and cross
- f. site transfer control room in 242S
- g. Field walkdown of Tank Farm transfer leak detector annunciator panel in 242S control room

Results:

Discussion of Results:

A and AX Tank Farms, interim stabilization and single shell tank intrinsically safe leak detection equipment

The AX Tank Farm saltwell pumping (interim stabilization) intrinsically safe leak detector conformed to the design description, including controls and switches, with one exception. Interim stabilization used a modification to the general intrinsically safe leak detector design. A 120-volt output relay was omitted in the interim stabilization design as the detection signal was sent to a programmable logic controller (PLC) for output. This modification was not reflected in the intrinsically safe leak detector circuit design description located in the interim stabilization system engineers notebook. However, it was depicted correctly on the support drawing *Skid "P" Pumping & Instr. Control Arrangement*. Otherwise the system was as described in the design description, including controls and switches. Intrinsically safe wiring and components were separated and

clearly marked. There was a small amount of loose debris including a small wire jumper laying in the bottom of the cabinet.

The AX Tank Farm transfer line intrinsically safe leak detector and the A-AX interim stabilization leak detection systems agreed with their respective wiring, arrangement, and detail drawings. The general condition of the transfer line and the saltwell pumping intrinsically safe equipment was good, and internal and external wiring was properly identified, routed, and terminated. One of the AX Tank Farm old style inductive relay leak detectors was also opened, and it's condition was also generally good.

A stand-alone Micro Logic 1000 PLC enclosure in AX Tank Farm did not have a connection from the enclosure to earth ground. Dwg H-2-69162 did not show an enclosure ground connection. The system engineer stated that he thought the enclosure was grounded through the power cable ground conductor approximately 20 feet back to the main panel. The system engineer for the cross site transfer leak detection system also sits on the local committee for the national electrical code. When asked about this condition he stated that this was a separate enclosure per the NEC and that a separate earth ground at the enclosure was required.

U and TX Tank Farm inductive relay leak detection equipment

The older inductive style leak detectors in the U and TX Tank Farms varied in their material condition. In general, internal wire leads were not well marked with wire numbers. In one case, terminal board terminal numbers were written in with pencil on masking tape. In some cases internal wiring was routed haphazardly and joined using wire nuts rather than connecting at a terminal board. In a U farm sump leak detector, an approx. 5 watt carbon resistor had been attached to a terminal board terminal on one lead with the other lead spliced directly into a nearby wire, rather than attaching both leads to terminal board terminals. The function of the carbon resistor was unknown. This equipment was obviously some of the oldest transfer leak detection equipment on site.

At U Tank Farm leak detector LDE-241-151-U, the cable going from the leak detector station down to the leak detector element had a split in the outer cable sheath about half the circumference of the cable at the high point of a bend, exposing the inner lead wires. The system engineer and electrician stated that a PER would be written and the condition repaired. When asked if cable minimum bend radius criteria were used when cables were installed the electrician stated that bend radius criteria are adhered to for new installations, but that practice was relatively recent.

At TX Tank Farm, two enclosures labeled LDE-241-152-TX and LDE-241-155-TX were situated adjacent to each other. LDE-241-152-TX housed older style leak detector circuit components. LDE-241-155-TX housed an item which appeared to be some sort of canned transformer. This device did not appear on system drawings. Both the installation of the unit itself and wiring to the unit was haphazard, with no internal wire lead identifiers, and was obviously old work. Neither the system engineer nor the electrician could identify the component or it's function.

Concerning the West Tank Farms leak detection equipment evaluated by the assessment team, both the system engineers and craft personnel acknowledged that much of it was in generally poor condition. With the exception of some specific deficiencies they have been aware of these general conditions. When asked about the apparent discrepancy between East and West Tank Farm equipment the term "run to failure" was used to describe the methodology in place for maintenance of some West Tank Farms equipment rather than the program of periodic inspections and repairs. The system engineers indicated they would like to upgrade equipment but have been limited by funding. Engineering management echoed the position on funding.

Installation of leak detector annunciator equipment on the indicating panel in the 242S control room looked good. Although a lot of the equipment on this panel was relatively old there was also some newer equipment on the panel. Rear panel wire runs, wire and cable identification, terminations, treeing, and equipment installation was good.

Cross-site transfer leak detection equipment

The assessment team inspected two of the five leak detector stations for the continuous cross site transfer leak detection system and the maintenance and operations computers in the cross site transfer control room. This was new equipment composed primarily of *printed circuit boards slotted on a motherboard, with signal outputs routed to PLCs.* Equipment installation and condition at the leak detector stations and the PLC cabinets was very good, and all wiring was properly identified, routed, and terminated. However, installation of the fiber optic communication line connecting the various PLCs to each other and to the control room computers was poor.

Cross-site transfer fiber optic equipment communications line

Installation of the fiber optic communications line was very sloppy, with the individual fiber optic leads loosely strung over to the front terminals on the PLC input/output module. These fiber optic leads were fragile, and the way they are routed and strung made it difficult to work inside the PLC cabinet without damaging them. At the control room end this fiber optic cable entered the room under the false ceiling and was strung under the ceiling to the opposite wall. It dropped down the wall to about knee height where it drooped over unsupported approximately two feet to the rear of the operations computer console. This was an obvious equipment and tripping hazard for anyone accessing the area between the rear of the computer console and the wall.

The system engineer stated that the fiber optic link had been installed by a low bid vendor, that operations had accepted the work and that he was to some extent stuck with it because he did not have the funds available to correct it. He was aware of some other cable routing issues at the rear of the computer console and planned to correct those as funds and schedule permit.

The continuous leak detection system is classified as defense in depth.

Conclusion:

Although not all of the site transfer leak detection equipment was opened and inspected by the assessment team, a large disparity in material condition clearly existed between the newer equipment put in place in the last 5 to 10 years and some of the older leak detection equipment. Much of the older equipment dates to the early days of site operation and is located in the West Tank Farms. The newer, intrinsically safe leak detection equipment installed in some of the East Tank Farm transfer lines, the SY Tank Farm, and in the salt well pumping skids used for interim stabilization generally reflected good industry practice for electrical equipment installation, wire and cabling installation, and wire terminations and identification.

The cross site transfer system was also generally in very good condition, with the exception of the PLC fiber optic communication line. The installation techniques and practices used on the fiber optic line were poor, to the point where tripping hazards to personnel and potential hazards to equipment during maintenance were created by the installation.

The most serious examples of poor material conditions were seen in much of the older equipment installed in the West Tank Farms. This equipment suffered from poor installation practices, damaged cabling, undocumented modifications and other problems such as dirt and debris. The maintenance strategy for this equipment was run to failure with no program for periodic inspection and repair. Many of the deficiencies noted, such as damaged cabling, would likely have been detected and repaired under a program of preventive maintenance. The technical personnel responsible for both the West Tank Farm leak detection equipment and the Cross Site Transfer equipment were generally aware of the poor conditions but considered themselves limited by lack of funding and direction.

Issues:

The Tank Farms contractor and the Department of Energy are aware of the generally poor condition of much of the transfer leak detection equipment, particularly in the West Tank Farms. Therefore no specific findings or observations have been written on this matter to avoid re-stating existing issues.

Appraisal Form

Transfer Leak Detection System

Topical Area: Configuration Management	Criteria Met
Date: February 26, 2002	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Objective:

Changes to safety basis-related requirements, documents, and installed components are controlled.

Criterion:

3. Changes to system safety basis requirements, documents, and installed components conform to the approved safety/authorization basis (safety envelope) for the facility, and the appropriate change approval authority is determined using the unreviewed safety question (USQ) process.

Approach:

Records Review:

- 3-1 Review documentation, such as change travelers and changes packages, and interview individuals responsible for processing selected changes made to the system requirements, installed equipment, and associated documents. Determine whether:
 - Changes to the system are reviewed to ensure that system requirements and performance criteria are not affected in a manner that adversely impacts the ability of the system to perform its safety functions
 - The USQ process (i.e., USQ screens and USQ safety evaluations/determinations) is being appropriately used

Interviews:

N/A

Observations:

N/A

Process:

Records Reviewed:

- a. HNF-IP-0842 Vol. 4 "Engineering" Section 4.29 *Engineering Document Change Control Requirements*

- b. HNF-IP-0842 Vol. 4 "Engineering" Section 5.4 *Unreviewed Safety Questions*
- c. ECN 649790 to drawing H-2-34965 *Power for Leak Detector Panels*
- d. ECN 657931 to drawing H-2-34965 *Leak Detector System*
- e. ECN 644388 to drawing H-2-73823 *Tank Waste Remediation*

Personnel/ Positions Interviewed:

- a. G. J. Coleman, system engineer, Interim Stabilization
- b. J. B. Roberts, system engineer, Cross Site Transfer
- c. J. A. Bewick, system engineer, Single Shell Tanks

Evolutions/Operations/Shift Performance Observed:

Results:

Discussion of Results:

Requirements to perform unreviewed safety question (USQ) determinations in conjunction with changes to engineering documents were included both in the procedure for USQs and in the procedure for engineering document change control requirements. Review of a sample of engineering change notices (ECNs) for the transfer leak detection systems showed that the USQ process was being followed.

During interviews, system engineers explained that if an ECN was being issued which resulted in system modifications the ECN originator accessed a network web site to obtain a unique USQ screening number. If the results of the USQ screen showed that a USQ determination was required then the USQ screen number was retained and became the USQ determination number. This number was to be referenced on the ECN. Review of completed ECNs by the assessment team showed that this process was being followed.

ECN forms contained a signature block for approval of the change by the safety organization. Signatures from the safety organization had been obtained on those ECNs for which safety organization approval was required.

During interviews, systems engineers who process changes to their engineering documents said that they were familiar with the USQ process requirements. The system engineer for interim stabilization stated he routinely used the USQ process during preparation of engineering change notices on his systems. He estimated that often up to 50 percent of his time was spent researching and processing USQ determinations and USQ related issues. The system engineers for single shell tanks and the cross site transfer

system also stated that they understood the USQ process used during preparation of an ECN, and that they were very familiar with it. They also stated that they routinely processed USQ determinations associated with their ECNs.

The assessment team reviewed the training records for all of the primary and back-up system engineers and found that all of the system engineers had received USQ training and that the training was current.

Conclusion:

The requirement to consider USQ determinations while processing changes to engineering documents was included in the procedures governing the USQ process and engineering change control. Review of completed ECN forms showed that the USQ determination process was being followed. Technical personnel were trained on the procedures and requirements governing the USQ process and they considered it a routine part of their duties to comply with those requirements. This criterion will be assessed in more depth during the upcoming vital safety system assessments for primary leak detection and tank ventilation, both of which are safety class systems.

Issues: None

Appraisal Form

Transfer Leak Detection System

Topical Area: Configuration Management	Criteria Met
Date: February 26, 2002	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Objective:

Changes to safety basis-related requirements, documents, and installed components are controlled.

Criterion:

4. Facility procedures ensure that changes to the system safety basis requirements, documents, and installed components are adequately integrated and coordinated with those organizations affected by the change.

Approach:

Records Review:

N/A

Interviews:

- 4-1 Determine whether engineering (including the design authority and technical disciplines for process control, electrical, mechanical, chemical, HVAC, nuclear, criticality, structural, etc.), operations, and maintenance organizations are made aware of system changes that affect them, and are appropriately involved in the change process. Verify integration and coordination with other organizations that could logically be affected by the change such as facility training, document control, construction, radiological control, OSHA occupational safety, industrial hygiene, occupational medicine, hazard analysis/safety basis, safeguards and security, and fire protection.

Observations:

N/A

Process:

Records Reviewed:

- a. ECN 649790 to drawing H-2-34965 *Power for Leak Detector Panels*
- b. ECN 657931 to drawing H-2-34965 *Leak Detector System*

- c. ECN 644388 to drawing H-2-73823 *Tank Waste Remediation*

Personnel/ Positions Interviewed:

- a. E. R. Hamm, manager, Tank Farms configuration management
- b. G. J. Coleman, system engineer, Interim Stabilization
- c. J. B. Roberts, system engineer, Cross Site Transfer
- d. J. A. Bewick, system engineer, Single Shell Tanks
- e. M. G. Al-Wazani, design authority, Design Engineering
- f. R. P. Raven, operating engineer, Tank Farms Central Command and Control

Evolutions/Operations/Shift Performance Observed:

N/A

Results:

Discussion of Results:

The engineering change control process included provisions on the engineering change notice (ECN) form for indicating the impact of the change to a comprehensive list of other affected documents and procedures across the Tank Farms complex. For the documents that were reviewed, signatures indicating approval of the change were obtained from Quality Assurance, Safety, Environmental, design authorities and cognizant engineers. Signatures were also obtained from the organizations responsible for any other specific documents affected by the change.

The assessment team interviewed system engineers for several systems and found that they were aware of changes to their system. System engineers were involved in the change control process, and were aware of configuration issues as reported in occurrence reports.

The Design Engineering design authority stated that, with the implementation of system engineers, his responsibility for system changes to the transfer leak detection system had been transferred to the system engineer. Review of ECNs processed prior to the onset of the system engineering program showed that the design authorities have been involved in system changes to equipment.

The assessment team interviewed the duty operating engineer in the tank farms Central Command and Control station on the subject of access to current and correct essential drawings. Since the total number of tank farm essential drawings was too large to keep at the station the operating engineer did not keep essential drawings on file. Rather, she

relied on retrieving drawings as needed by computer from the Hanford document control system. The operating engineer did keep a file of selected drawings on hand, but not the full set of essential drawings, and she did not necessarily keep them current. She understood that the most current versions were available through the Hanford document control system and relied on the system to provide access.

The assessment team discussed the procedure for processing changes to engineering documents with the manager for Tank Farms configuration management. He stated that a completely rewritten procedure for management of changes was due for release in summer 2002. The new procedure was intended to be more in line with commercial nuclear practice, consisting of five separate change procedures in the areas of design, documentation, modifications, requests for engineering assistance, and equivalency substitutions.

Conclusion:

Processes were in place in the existing change control system to disseminate information concerning system changes to other organizations affected by the change. Schedule constraints during the assessment of vital safety systems transfer leak detection equipment prevented a complete evaluation of the existing process. This area will be evaluated again in the upcoming vital safety systems assessments on primary leak detection and tank ventilation. Also, since the engineering change control procedures were scheduled for complete revision in the near future it may be premature to assess the effectiveness of the existing change control process for future operations. This is an area in which it would be appropriate to hold a follow-on assessment of configuration management practices some time after the new change control procedures have come into effect

Issues:

None

Appraisal Form

Transfer Leak Detection System

Topical Area: Configuration Management	Criteria Met
Date: February 25, 2002	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Objective:

Changes to safety basis-related requirements, documents, and installed components are controlled.

Criterion:

5. Software used in system instrumentation and control (I&C) components that perform functions important to safety is subject to a software quality process consistent with 10 CFR 830.120.

Approach:

Records Review:

- 5-1 For software used by safety system I&C components, request the facility staff to identify:
 - The applicable software quality assurance requirements,
 - The software quality assurance standards/controls applied to software development, procurement, acceptance, and testing
 - The basis for acceptance of these standards/controls as providing adequate assurance that the software is acceptable for performing its associated safety functions
- 5-2 Review software quality assurance requirements, procedures, and records. Determine whether:
 - Software quality assurance documentation exists for software in use
 - Configuration management procedures exist for updates, changes, and version control of software and related documentation such as software design documents and a list of software configuration items installed on computer-based components
 - An appropriate degree of independence exists between those responsible for software development and quality assurance functions
 - A process is in place and used to identify, evaluate, and resolve operational problems that are attributable to software

Interviews:

- 5-3 Interview facility engineering and operations staff to determine their awareness of software quality assurance requirements for system software under their cognizance.

Observations:

N/A

Process:

Records Reviewed:

- a. HNF-SD-WM-SAR-067, Revision 3, Table 3.3.2.4.7-3, "Summary of Safety Structures, Systems, and Components for Waste Transfer Leak."
- b. HNF-SD-WM-SAR-067, Revision 3, Section 4.4.7, "Transfer Leak Detection System."
- c. HNF-PRO-309, *Computer Software Quality Assurance Requirements*, Revision 1, March 23, 2000.
- d. HNF-PRO-2778, *IRM Application Software System Life Cycle Standards*, Revision 0, February 12, 1999.
- e. Certified Vendor Information (CVI) File 22726 [Allen-Bradley vendor manual sections for saltwell PIC skid PLCs].
- f. RPP-7142, "Saltwell Leak Detector Station Programmable Logic Controller (PLC) Software Configuration Management Plan (SCMP)," Revision 0, November 20, 2000.
- g. RPP-5775, "PLC/DTAM Software Programs for Pumping Instrumentation and Control [PIC] Skid 'P'," Revision 1, July 19, 2001.
- h. HNP-5283, "Operational Test Report (OTR) for SX-104 Pumping, Instrumentation and Control (PIC) Skid," Revision 0, November 5, 1999.
- i. ECN 667416 [Incorporated nine prior completed ECNs into RPP-5775], July 19, 2001.
- j. ECN 669317 [Added an active mode to communications allowing each PIC skid PLC to verify that the other on-line PLCs are actively communicating], July 24, 2001.

- k. ECN 669379 [Added alarm numbers to titles for DTAM displays], November 16, 2001.
- l. ECN 670685 [Disabled input from leak detector AN-101 because of change in transfer route], October 5, 2001.
- m. USQ-TF-01-0474, "U/S/SX/A and AX PIC Skid Software Changes," Revision 3, July 2001.
- n. USQ-TF-01-0768, "Software Disable of AN-101 Leak Detector Input to Tank 241-A-101 PIC Slid 'P' PLC," Revision 0, October 2001.
- o. RPP routine work request WS-01-00411/1 [241-U-102 saltwell shutdown with no alarms activated on DTAM or OCS; unable to determine cause], June 27, 2001.
- p. PER-2001-0865 [Develop or migrate FDH procedures (HNF-PRO-309 and HNF-PRO-2778) as CHM procedures], July 12, 2001.
- q. PER-2001-1711 [No available documentation for a test plan and acceptance criteria for PLC operability or functionality test after installation of the software per WP-2W-01-00140M], October 31, 2001.
- r. PER-2001-1947 [various configuration errors identified during and prior to operational test for U-108 saltwell system], November 12, 2001.
- s. PER-2001-2178 [ECN had not been formally added to a work package prior to being worked for PIC Skid K PLC], November 30, 2001.
- t. PER-2002-0555 [Approval designator had been incorrectly assigned for Engineering Data Transmittal of PLC software release package for leak detector station No. 5], January 31, 2002.
- u. "Interim Stabilization Engineering (ISE) PIC Skid PLC Software Audit," [informal self-check report] Floyd M. Maiden, April 10, 2001.
- v. Specification W-058-P2 [Replacement cross-site transfer system control system].
- w. HNF-2544, "Software Configuration Management Plan for the Replacement Cross-Site Transfer System Control System," Revision 1, April 12, 2001.
- x. HNF-2563, "Project W-058 System Overviews," Chapter 1, "Monitor and Control System," Revision 0, April 10, 1998.

- y. HNF-2346, "Project W-058 Monitor and Control System Logic," Revision 0, March 11, 1998.
- z. Vendor Information (VI) File 22798 Supplement 48, "System Documentation," Submittal Item #5, "Factory Test Procedure," Submittal Item #7, "Data Package."

Personnel/ Positions Interviewed:

- a. F. M. Maiden, software custodian, leak detection station and saltwell PIC skid programmable logic controllers.
- b. B. R. Johns, design agent, leak detection station and saltwell PIC skids.
- c. W. F. Zuroff, design authority, interim stabilization.
- d. J. Roberts, software custodian, replacement cross-site transfer control system programmable logic controllers.
- e. C. DeFigh-Price, Director, System Engineering

Evolutions/Operations/Shift Performance Observed: N/A.

Results:

Discussion of Results:

Assessment scope

For this assessment, the team selected the software for the saltwell leak detector station programmable logic controllers (PLCs) and the replacement cross-site transfer system control system PLCs. The team assessed a sample of the documentation available for elements of the software life cycle for each application. The software documentation included available requirements documents and procurement specifications (HNF-2563 and specification W-058-P2 for the cross-site transfer application); software configuration management plans (SCMPs) (RPP-7142, HNF-2544); vendor files (CVI File 22726 and VI File 22798); detailed software release packages (RPP-5775 and HNF-2346); a sample of four engineering change notices (ECNs); and five retrievable problem evaluation reports (PERs). For the saltwell pumping, instrumentation and control (PIC) skid PLCs, the team also reviewed a self-assessment of software configuration control performed by the software custodian in April 2001, and two unreviewed safety question (USQ) screening/determinations that supported ECNs.

The team reviewed the appropriate documentation against 10 CFR 830.120(c)(2)(ii), *Design* and 10 CFR 830.120(c)(2)(iii), *Procurement*.

The team also selectively reviewed the documentation against the FSAR and software

quality assurance procedures HNF-PRO-309 and HNF-PRO-2778. The team focused on assessing whether there was reasonable assurance of adequate performance and configuration control, rather than on strict procedural compliance. For assessing performance, the team selected certain functional requirements (e.g., trip of the saltwell pumps when a leak is detected) and other performance attributes such as response to power/communication failure scenarios, protection of configuration integrity, and control of software forces. (A software force is a maintenance tool that is the equivalent of a hardware jumper.) The documents were reviewed in part against these attributes, and discussed in interviews. The cross-site transfer application was not reviewed in as much detail as the saltwell PIC skid PLCs.

Safety/quality classification of software

FSAR 4.4.7, "Transfer Leak Detection System" stipulates that the transfer leak detection systems are safety-significant. Contrary to the FSAR, the software configuration management plan (SCMP) for the leak detector stations (RPP-7142 Revision 0) states that "The leak detector station PLC system and software used for the Hanford saltwell interim stabilization are general service, defense-in-depth."

In an interview, the design authority stated that the "general service, defense in depth" classification stipulated in the software configuration management plan (SCMP) of record was believed correct when the SCMP was issued November 28, 2000, but that the current FSAR requires a "safety significant" classification. During the assessment, the team was unable to identify any PERs or pending engineering change notices (ECNs) that would change the safety/quality classification of the software or programmable logic controller (PLC) to reflect the higher classification stipulated in the FSAR.

The design authority said that the leak detector station PLC and software will be reclassified as safety-significant when the safety equipment list is updated (due February 28, 2002), following which the design authority would prepare an implementation plan to reconcile gaps in qualification to the higher classification. This would include, for example, gaps in documentation of requirements analysis and verification & validation (V&V).

For the cross-site transfer PLCs, SCMP HNF-2544 did not explicitly identify a safety or quality classification. However, the introduction to the SCMP stated that "The computer operating system provides control of all cross-site equipment and is used for normal plant operations. Safety shutdowns of the transfer system are performed by hardwire components." This suggested that the software would not be "safety class" or "safety-significant," because credit was taken only for the hardwired circuits. Based on review of the FSAR and discussions with the design authority and software custodian, the assessment team concluded that the contractor considered the software and the software function to be "general service."

Application of software quality assurance and controls

HNF-PRO-309, *Computer Software QA Requirements*, Section 2.1, "Software Life Cycles, Baselines, and Controls," requires in part that: "Software previously developed and not in accordance with this procedure...shall conform to the following:

Perform, document, and provide for an independent review and evaluation:

- Its adequacy to support software operation and maintenance
- Test plans and tests cases required to validate the software for acceptability..."

Section 2.3, "Documentation," requires in part that "Review of software baselines shall be performed and documented at each of the software life cycle control points."

Contrary to the requirements of HNF-PRO-309, documentation of most of the saltwell PLC software life cycle was generally not retrievable, despite past attempts by the design authority to find it. This included requirements analysis, design, code construction/acquisition, integration and system factory testing, installation, and acceptance stages (as defined in HNF-PRO-2778). According to the design authority, DOE did this PLC procurement in 1994. It was unusual for DOE, rather than the contractor, to accomplish the procurement, but this was apparently done to expedite the project.

The design authority stated that they had been unsuccessful in finding this documentation or verifying that it existed. They had searched DOE procurement files and vendor files, and were only able to recover fragmented documentation. The team confirmed that certified vendor information (CVI) file 22726 was comprised primarily of Allen-Bradley generic vendor manual sections, and did not include or reference the expected software life cycle products such as a system requirements document, procurement specification, V&V plans/reports, or a factory acceptance test report.

CHG lacked documentation to demonstrate conformance with 10 CFR 830.120(c)(2)(ii), *Design*; 10 CFR 830.120(c)(2)(iii), *Procurement*; HNF-PRO-309; and HNF-PRO-2778 for the major portions of the software life cycle for the saltwell PLC applications. This condition is also inconsistent with ASME NQA-1, "QA Requirements for Nuclear Facility Applications," Subpart 2.7.

Notwithstanding the contractor's baselined software configuration management program, this absence of life cycle documentation was inadequate as-found to satisfy quality assurance requirements for software classified as "safety significant."

As an example of the possible consequences of missing or deficient software requirements analysis/documentation, the team noted a "revealed requirement" regarding communication between skids. For the purposes of this assessment, a "revealed requirement" is one that had not been documented in the design process, but was revealed by the consequences (or potential consequences) of an operational event. Had the revealed requirement been incorporated in the original design, the consequences would

have been precluded. Such an event involving lockup of a PLC CPU in June 2001 revealed that if a skid PLC locked up, other interfacing skids would not recognize the condition. The design authority fixed this (ECN-669317) by allowing each skid to verify that the other on-line PLCs are actively communicating. If a PLC that is expected to be on-line fails to communicate properly, then the sensing PLC will shut down the saltwell pump. Had more than one skid been active when the event had occurred under the original configuration, the pump on the interfacing skid would not have tripped as required if a leak had occurred.

The contractor's configuration management (CM) organization believed that the saltwell PIC skid PLCs would be an outlier, and they expected other applications to have adequate software documentation. CM believed that these PLCs were exceptions because they had been procured directly by DOE rather than by a contractor. Apparently, DOE did not obtain and provide the expected software documentation.

In contrast to the saltwell PIC skid PLCs, readily retrievable documentation for the cross-site transfer project included a detailed procurement specification (W-058-P2), requirements document (HNF-2563 Chapter 1), and vendor documentation (VI 22798). The vendor documentation included a comprehensive and detailed factory acceptance test procedure and report as well as a detailed data package for configuration items. The team accepted this without further review as objective evidence of software life cycle documentation from specification through factory acceptance, and adequate for software classified as "general service."

Software configuration management

For control of software changes (software configuration management), the design authority had baselined the saltwell PIC skid PLC software configuration "as-found" in 1999. The baseline configuration was captured in considerable detail in a baseline software release document "PLC/DTAM Software Programs for Pumping Instrumentation and Control (PIC) Skid 'D'" (for SX-104). The design authority selected this baseline because it was believed to be the earliest software delivered, and because it appeared to be a configuration generally applicable to many skids, modifiable for specific skid applications. In the absence of available and reliable documentation, the design authority identified FSAR/TSR requirements levied on the software (e.g., trip pumps upon detection of a leak), documented the software requirements, and "reverse-engineered" other software requirements from the as-found configuration.

The design authority then used the software release document for skid 'D' as the configuration baseline, without critical review or special tests beyond operational test report (OTR) HNP-5283. The team notes that an OTP/OTR is typically a surveillance limited to operational tests of hardware performance, and generally not designed to comprehensively exercise software functions (such as communication functions and network performance). The design authority took this approach in part because it was believed that the performance history of the software used at the Tank Farms had been adequate. To generate software release documentation for other skids, they prepared and

issued a similar document for each skid.

The design authority and software custodian stated that the software release package document described above contained sufficient detail to restore the system configuration if the installed software and all backup copies were destroyed. This conclusion seemed reasonable to the team, based on the level of detail provided in this package. The software custodian had also retrofit comment annotations in the ladder logic software. This practice facilitated review of the detailed software code, and provided some traceability to the software requirements. The design authority and software custodian stated that there were little or no such annotations or other software documentation when they inherited the system. Based on a cursory review, the team concluded that the design authority's effort to document and control the baseline configuration appeared effective in capturing the as-found configuration, notwithstanding the lack of design basis and other early life cycle documentation required for safety significant software.

The design authority used a software configuration management plan (SCMP) to control software or configuration changes. An example was RPP-7142, "SCMP for the Saltwell Leak Detector Stations." The governing procedure for this SCMP was HNF-PRO-309 Rev. 1, *Computer Software Quality Assurance*, Sec. 2.4, "Software Configuration Management." The team concluded that RPP-7142 appeared to generally comply with the software configuration management aspects of HNF-PRO-309.

Based on a limited vertical slice review of the software documentation for skid 'P' PLCs (RPP-5775), the team concluded that the leak detection/pump trips for the selected sample were being correctly implemented. Review of the ECNs sampled did not identify any problems. In reviewing USQ-TF-01-0474 (July 2001) and USQ-TF-01-0768 (October 2001), the team concluded that the earlier USQ screening/evaluation was incomplete because it did not evaluate potential failure modes and consequences. However, the team did not expect that the USQ conclusion would have been different, and noted that the more recent USQ determination was substantially more thorough. Interviews with the author of the two USQ determinations suggested to the team that the contractor's organization had benefited from lessons learned from earlier unsatisfactory USQ screenings and determinations. The software custodian said that current practice conservatively requires that a USQ determination (not a USQ screening) be performed for all ECNs.

For the cross-site transfer PLCs, SCMP HNF-2544 was similar in content to SCMP RPP-7142, but there were differences in content and format. For example: RPP-7142 identified the quality class (albeit obsolete) of the software but HNF-2544 did not; HNF-2544 presented and referenced specific requirements for logging software forces but RPP-7142 did not; RPP-7142 stipulated an objective to conduct assessments to ensure that the SCMP is effective in establishing and maintaining the technical requirements but HNF-2544 did not mention assessments; HNF-2544 identified specific training requirements and access levels for personnel authorized to make changes but RPP-7142 did not; RPP-7142 identified and prescribed the use of software change requests (SCRs) per HNF-PRO-2778 but HNF-2544 did not. However, both SCMPs appropriately required the

ECN process to be used for any software changes. In the case of assessments to ensure effectiveness in establishing and maintaining software technical requirements for the cross-site transfer system, contracts had been put in place to have the original vendor provide that service.

The assessment team believed that a uniform format and content should be established for software configuration management plans governed by HNF-PRO-309. For example, in interviews, both projects appeared to describe reasonable practices for control of software forces and for protection of data from viruses or other corruption. (A software force is a maintenance tool that is the equivalent of a hardware jumper.) However, these practices were formally documented in the software configuration management plans (SCMPs) for one of the projects but not the other. Therefore, formal procedural controls for maintaining configuration integrity were not always evident.

The software custodian for the PIC skid PLCs provided a copy of an "audit" he had performed in April 2001. Because the audit was actually an informally documented self-check by the software custodian of records he had generated or was responsible for, the effort could not be considered independent, and the report contained only his name as author.

Notwithstanding this lack of independence and oversight, the team concluded that the technical effort was reasonable for determining the effectiveness of software configuration management and achieving his objectives. The purpose of the self-check was to verify that all applicable ECNs written against the PIC skid PLC software had been implemented, that associated software change requests (SCRs) had been completed and placed in the SCR book, and that electronic copies of the PIC skid PLC software held by the software custodian and in the fire-rated file cabinet were up to date.

The software custodian chose seven active skids at random (S-102; SX-101, -103, -105; U-105, -106, -109) and software was uploaded from each active skid. Display (DTAM) software was excluded at that time, because the active skids would need to be shut down to upload the DTAM software. The software custodian's report recommended that the DTAM software should be similarly audited when conditions permitted. The software custodian said this would probably be done in the next "audit" planned for about April 2002, and that use of an independent reviewer might be considered.

For the self-check, the software custodian obtained ECN information was obtained from the site document database, and:

- Compared it against SCRs to verify an SCR had been written for each ECN;
- Compared in 100% detail to the software uploads to verify the changes had been implemented; and
- Compared the electronic backup copies of the software to the uploaded PIC skid software to verify they were all up to date.

The results of the self-check were:

- Three ECNs (written after the September 11, 2000 requirement for SCRs) did not have an associated SCR;
- All changes listed in the ECNs had been implemented in the PLC software uploaded from the PLC skids; and
- All copies of the PIC skid PLC software were verified as up to date as of April 10, 2001.

Independence of design verification

10 CFR 830.120(c)(2)(ii), *Design*, requires in part that “The adequacy of design products shall be verified or validated by individuals or groups other than those who performed the work. Verification and validation work shall be completed before approval and implementation of the design.”

Contrary to these requirements, there was no available documented evidence of this independent design verification for most of the software life cycle design documents. This included the un-retrievable original requirements and procurement specifications for the PIC skid PLC software as well as the initial issues of the software release packages (for example, RPP-5775).

Approvals for initial software releases appeared limited to administrative or management authorizations, rather than technical verification and validation. However, changes to software identified in ECNs (for example, ECN 667416) contained an “informal review” signature. In the ECNs sampled by the team, the informal review signature was not the cognizant engineer who had prepared the ECN.

Based on interviews the team expected that the informal reviewer identified on the ECN would have the technical skills and experience for adequate design verification. However, there was no record supporting these informal reviews (for example, a record of comments and their resolution). The team understands that the informal review process is no longer used and has been replaced by a more structured, rigorous, and formally documented design verification process as governed by HNP-IP-0842, Volume IV, “Engineering,” Section 4.24, *Design Verification*.

The team observed the foregoing design verification practice for hardware design as well as software design. For example, design description documents for hardware did not include evidence of design verification, and the same ECN process and informal reviews had been used for hardware changes.

Resolution of software errors and operational problems

The team tried to identify and retrieve a record of software errors and operational problems for Tank Farm programmable logic controller (PLC) applications. The problem evaluation report (PER) process began in the first half of 2001. Prior to the PER

process, non-conforming conditions had been formally identified using only the nonconformance report (NCR) process, which is still in use. In interviews, CHG management said that personnel used NCRs to identify observable configuration discrepancies, such as a discrepancy between as-found equipment and a drawing. NCRs were thus identifiable by equipment identification numbers or drawing numbers. The NCR process was not used to capture software performance history because personnel focused it on observable hardware configuration discrepancies relative to drawings. Therefore, prior to the current PER process, the team concluded there was no uniform process applied to formally identify, evaluate, trend, and correct software problems.

In assessing the effectiveness of the current PER process, the team found difficulty in identifying and retrieving a reliable sample of PERs involving software conditions. For example, the contractor performed a search of the PER database and identified/retrieved four PERs involving PLC software. However, a substantial PER (2001-1947) identified by the software custodian (based on his personal knowledge) did not appear in the group retrieved.

The team also identified a noteworthy example of a significant software problem which had not been dispositioned by the PER process, presumably because the process was still new to the contractor's organization. This example was the June 27, 2001 event involving lockup of a PLC CPU. This revealed that the communication configuration would not recognize that the PLC for an interfacing skid had locked up, potentially defeating the pump trip if a leak were detected. The solution to the consequences of this problem was documented by ECN 669317 and USQ-TF-01-0474. However, investigation of the locked-up CPU which had initiated the event had only been sparsely documented by RPP routine work request (RWR) WS-01-00411/1. This RWR did not specifically describe the initiating condition, determine the cause, or suggest trending. The work request record was also difficult for the software custodian to identify and retrieve for the team, despite the fact that he was generally familiar with the event.

The team expects that more aggressive use of the current PER process will result in more effective condition identification, condition evaluation (root or apparent cause, extent of condition, condition trending), and appropriateness of corrective action

Other results

The team asked the software custodian to identify controls in place to preclude corruption of the processor files downloaded to the PLC processor (such as corruption from viruses, worms, corrupt data, etc.). The software custodian stated that dedicated laptop PCs are used. These PCs contain no network cards, and uses other than for PLC configuration are prohibited. Current virus protection software is installed on the laptop. The virus protection software runs under Windows 98 and is the same as used on the network.

However, the only governing formal procedure for control of the laptop PCs used for configuration is the generic property management procedure HNF-IP-0842, Volume 15, "Property Management," Section 3.9, "Management and Control of Automated Data

Processing and Communications Equipment,” which is limited to protection of property from loss, unauthorized use, or misappropriation. The practices used by the contractor appeared adequate as described, but there was no formal procedure that supported the reported practice, and it was not addressed in the software configuration management plan.

Conclusion:

Software used in system I&C components that perform functions important to safety is subject to a quality process consistent with 10 CFR 830.122. However, there are examples of software items that do not conform to the CHG process:

- The PLC software supporting the saltwell transfer leak detector stations was not classified as “safety significant,” as stipulated in the FSAR. The design authority stated that the software and PLCs would be reclassified as safety-significant when the safety equipment list is updated (due February 28, 2002), following which the design authority would prepare an implementation plan to reconcile gaps in qualification to the higher classification
- Documentation was lacking to demonstrate complete conformance to 10 CFR 830.120(c)(2)(ii), *Design*; 10 CFR 830.120(c)(2)(iii), *Procurement*; HNF-PRO-309; and HNF-PRO-2778 for the major portions of the software life cycle for the safety significant saltwell PIC skid PLC applications. Notwithstanding the contractor’s baselined software configuration management program, this absence of critical life cycle documentation was inadequate for software classified as “safety significant.”
- There was no documented evidence of independent design verification for most of the software life cycle design documents. This included the un-retrievable original requirements, procurement specifications, and vendor V&V documentation for the PIC skid PLC software as well as the initial issues of the design authority’s software release packages. However, changes to the as-found software baseline implemented by engineering change notices did include an undocumented “informal review” by a qualified reviewer who had not performed the work. This observed practice for design verification did not appear limited to software design. The team understands that the informal review process is no longer used and has been replaced by a more structured, rigorous, and formally documented design verification process governed by HNP-IP-0842.
- There was an incomplete formal record of the software operational history (defect reporting/resolution, errors, anomalies, problem reports, etc.) for the saltwell PIC skid PLCs. This was due in part to the absence of a formalized problem evaluation reporting (PER) process until about mid-2001, and an NCR process that was not used to address software anomalies. The team expects that more aggressive use of the current PER process will result in more effective condition identification, condition evaluation (root or apparent cause, extent of condition,

condition trending), and appropriateness of corrective action.

For tracking software development as well as operational performance, the team notes that industry standards such as IEEE Std 1044-1993, *IEEE Standard Classification for Software Anomalies* can provide specific guidelines for recording, classifying, identifying impact, investigating, and dispositioning software anomalies.

The assessment team concluded that there was reasonable assurance that software configurations were being adequately controlled with respect to changes to the baseline software established by the design authority.

The scope of software configuration management plans (SCMPs) in place for the applications reviewed was generally adequate, and consistent with governing procedures. However, the team observed that a uniform format and content should be established for software configuration management plans governed by HNF-PRO-309. Based on interviews, the two projects assessed herein both appeared to use good practices, but the procedures governing these practices had not always been uniformly documented in the SCMP or other project procedures.

In this limited review, the team did not identify any discrepancies in the baseline software configuration or in subsequent modifications. Interviews with the design authority and software custodians for the saltwell PIC skid PLCs suggested to the team that personnel responsible for software changes were making a conscientious and effective effort at software configuration control, including informally documented self-checks of the configuration.

Issues:

- a. The "safety significant" classification stipulated in the FSAR for the transfer leak detection system was not reflected in the software configuration management plan for the leak detector stations. (Finding 10)
- b. Vendor, procurement, verification, and validation documentation for the safety significant software supporting the saltwell pumping instrumentation and control skid programmable logic controllers was not retrievable. (Finding 11)
- c. The design description document for safety class leak detection circuits and initial software release packages for safety significant saltwell PIC skid programmable logic controllers had not been subject to design verification. (Finding 12)
- d. There was an incomplete formal record of the software operational history for the saltwell PIC skid programmable logic controllers. (Finding 9)
- e. A specific and uniform format and content should be established for software configuration management plans governed by HNF-PRO-309. (Observation 3)

Appraisal Form

Transfer Leak Detection System

Topical Area: Safety Function Definition	Criteria Met
Date: February 27, 2002	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Objective:

Safety basis-related technical, functional, and performance requirements for the system are identified/defined in appropriate safety documents.

Criterion:

1. Safety/Authorization Basis documents identify and describe:
 - a. The system safety functions and the safety functions of any essential supporting systems, and
 - b. The system requirements and performance criteria that the system must meet to accomplish its safety functions.

Review Approach:

Records Review: -

1. Review the appropriate safety/authorization basis documents, such as safety analysis reports, basis for interim operations, technical safety requirements, safety evaluation reports, and hazards and accident analyses, to determine if the definition/description of the system safety functions includes:
 - The specific role of the system in detecting, preventing, or mitigating analyzed events
 - The associated conditions and assumptions concerning system performance
 - Requirements and performance criteria for the system and its active components, including essential supporting systems, for normal, abnormal, and accident conditions relied upon in the hazard or accident analysis.

Interviews:

N/A

Observations:

N/A

Process:

Records Reviewed:

- a. HNF-SD-WM-SAR-067, Revision 3a, Tank Farms Final Safety Analysis Report
- b. HNF-SD-WM-TSR-006, Revision 2g, Tank Farms Technical Safety Requirements
- c. RPP-5667, Revision 0c, Stochastic Consequence Analysis for Waste Leaks
- d. Draft Double Shell Tank Transfer Leak Detection Safety Equipment List
- e. OSD-T-151-00031, Revision D-6, Operating Specifications for Tank Farm Leak Detection and Single Shell Tank Intrusion Detection, Section 31.2.4, Transfer Leak Detection
- f. Assessment of Operational Readiness of the Safety Significant Transfer Leak Detection System (Vital Safety System Phase I assessment)
- g. Authorization Basis Clarification Request Log Number 02-005, Revision 0, regarding whether integrity of a leak detection pit is required to meet leak detector functional requirements.
- h. Certified vendor information (CVI) file 22726 [Allen-Bradley vendor manual for saltwell PIC skid programmable logic controllers (PLCs)]

Personnel/ Positions Interviewed:

- a. R. R. Bafus, System Engineering
- b. E. C. Heubach, Nuclear Safety & Licensing
- c. F. M. Maiden, software custodian, saltwell PIC skid PLCs
- d. D. W. Reberger, System Engineering
- e. R. D. Smith, Nuclear Safety & Licensing
- f. D. A. White, System Engineering

Evolutions/Operations/Shift Performance Observed:

N/A

Results:

Discussion of Results:

System and Safety Function Description

According to the Tank Farm FSAR, "the safety function of the safety-significant transfer leak detection system is to detect waste transfer system leaks in waste-transfer associated structures and to provide an alarm to alert operators to take mitigative action to shut down the transfer pump (or other motive force) and to take response actions to limit exposure to onsite and facility workers, thus limiting the volume of waste leaked and the time that workers are exposed to the leaked waste, thereby decreasing the consequences of the Waste Transfer Leak accident."

The FSAR also identified that the safety-significant piping encasements were necessary to accomplish the function of the transfer leak detectors. The tank farm electrical distribution system was identified as a supporting system as it provided power for leak detection alarm and control circuitry.

The FSAR did not adequately describe all major safety-significant components of the transfer leak detection system. Specifically, the FSAR did not discuss the design of the leak detectors in the replacement cross-site transfer system diversion box and vent station, nor the weight factor instrumentation in the Aging Waste Facility (AWF) transfer leak detection pits. The nuclear safety management rule and referenced standard required detailed information and performance criteria for these components.

The predominant type of safety-significant transfer leak detector in tank farms was the dual-electrode conductivity probe installed on the bottom of transfer pits and diversion boxes. The FSAR did appropriately describe the basic operation of this type of leak detector. There were however, as mentioned briefly above, two additional types of transfer leak detectors that the FSAR does not mention at all.

The first is the new style of leak detector used in the replacement cross-site transfer system diversion box 6241-A and vent station 6241-V. These detectors employ resistance temperature detectors and circuitry that send a signal when the probe is immersed. Although the end result is the same, the principle of detection and testing procedures are sufficiently different to warrant discussion in the FSAR and technical safety requirements (TSR). For example, due to an analyzed potential failure mode, there must be two redundant leak detector elements in a given location for the leak detection system to be operable. This redundancy was unique to waste transfer structures 6241-A and 6241-V.

The second type was the AWF weight factor transfer leak detection systems. These level monitoring systems, located only in 241-AY and 241-AZ tank farms, resided in leak detection pits that collect leakage from the side-fill transfer line encasements. Chapter 2 of the FSAR mentioned weight factor monitoring and leak detection pits, but only in the

context of collecting and measuring double-shell tank annulus leakage.

Despite the lack of information in the FSAR, the TSR limiting condition of operation (LCO) 3.1.3, "Transfer Leak Detection Systems," mentioned the AWF weight factor transfer leak detection system when it prescribed a semi-annual surveillance:

SR 3.1.3.2 Perform FUNCTIONAL TEST on the weight factor leak detection systems used in AWF leak detection pits.

This level monitoring system in the transfer leak detection pits was also briefly mentioned in the TSR bases for LCO 3.1.3, but there were no *performance* criteria, either here or in FSAR Chapter 4, *Safety Structures, Systems, and Components*, to adequately define operability.

The lack of FSAR documentation contributed to a poor understanding of actual leak detection system configuration on the part of the assigned double-shell tank leak detection instrumentation system engineers and at least one nuclear safety and licensing (NS&L) engineer. The assessor found that the system engineers responsible for this system had never heard of the weight factor instrumentation in AWF transfer leak detection pits.

The assessor also found an authorization basis clarification request (Log number 02-005, Rev. 0) and discussed the resolution with the applicable NS&L engineer. This engineer was also unaware of the unique aspects of the AWF transfer leak detection pits. The resolution was based on assumptions made regarding conductivity leak detectors in transfer related structures, and may not be correct for the actual configuration.

Performance Criteria

The TSR bases for transfer leak detection system surveillances identified RPP-5667, *Stochastic Consequence Analysis for Waste Leaks*, as the accident analysis document that provided the assumptions regarding leak detector probe placement in the waste transfer-related structures. The FSAR mentioned that the conductivity leak detector probes were placed so as to alarm prior to waste accumulation in the pit exceeding 5% of the pit volume. RPP-5667 demonstrated that waste could fill 50% of the pit before an alarm was actuated without significantly increasing the consequences.

One potential shortcoming is that the FSAR did not explicitly list performance criteria for the transfer leak detection system in terms of how the accident analysis assumes the system would perform under normal, abnormal, and accident conditions. However, this division of performance criteria between normal, abnormal and accident conditions appeared to the assessor to have no basis in the nuclear safety management rule and referenced standard for development of the documented safety analysis.

In attempting to identify the authorization basis/FSAR requirements for degraded voltage conditions at the tank farms (for the purpose of determining what voltage tolerances should be used as design inputs for hardware), the team noted that FSAR Chapter 4, Section 4.5.1, "Tank Farm Electrical Distribution System" addressed complete loss or interruption of electrical power, but was silent on addressing the effects of degraded voltage or degraded power quality. The FSAR also did not stipulate any requirements for degraded voltage protection. Nuclear safety and licensing stated that degraded voltage conditions had not been specifically addressed in the hazard analysis.

Notwithstanding the conclusion in FSAR Chapter 4, Section 4.5.1.4 that "Electrical power systems in the tank farms do not appear to be major contributors to the failures of safety SSCs," degraded voltage was not addressed. Degraded voltage events can complicate accident scenarios by overheating and subsequent failure of motors, selective drop-out (or selective pickup failures) of contactors and relays, and other disruptions. Other degraded power conditions could include surges and excessive harmonic content (waveform distortion).

One area of specific interest during this assessment was the impact on programmable logic controller (PLC) functions under degraded power conditions, because the impact might be selective and unpredictable. The following scenario was of interest to the team, based on our interpretation of vendor technical information in the Allen-Bradley PLC manuals (CVI File 22726).

Upon a loss of external power to the PLC chassis, there could be a holdup time of about 20 msec to 3 seconds, depending on the I/O module configuration and current states of the modules. Upon degradation to a set limit, the power supply will signal the processor to initiate a power supply shutdown. The turn-on/turn-off times of the input modules can be less than the power holdup time. Therefore, the input state changes that occur when power is removed or degraded may be captured by the processor before the power supply shutdown occurs. If this scenario were to occur, the team could not readily determine if this postulated scenario would always result in "fail-safe" consequences for safety significant functions.

In an interview, the software custodian for the saltwell PIC skid PLCs stated that failure modes and effects for such postulated conditions were acceptable for waste transfer leak detection functions, based on the failure modes and effects of the PLC inputs and the timing of the scan cycles. The team did not confirm this in detail. The software custodian also said that ECN 669317 added an active mode to communications, allowing each PIC skid PLC to verify that the other on-line PLCs are actively communicating. The software custodian stated that this improvement provided "fail safe" consequences from communication failures postulated to result from loss or degradation of power, because the communication failure would trip the transfer pumps.

However, of greater concern would be other types of loads not in the scope of this assessment, such as critical ventilation fans required to run continuously and continuous air monitors (CAMs). Degraded voltage/power conditions represent a potential common

cause failure mode which could result in challenging the timely identification, diagnosis, repair, and replacement of multiple components that had failed as a result of the condition. If the risk presented by these effects were analyzed and found unacceptable, then appropriate electrical protection might be required and prescribed as a part of the Authorization Basis.

Human factors program of FSAR chapter 13 not implemented

DOE approved the current final safety analysis report on February 2, 1999. However, the DOE safety evaluation report (SER) recognized that implementation of the FSAR sections describing programs (chapters 6-17) was incomplete. During this assessment, the assessment team noted that some features of these chapters were still not implemented. For example, the human factors program described in chapter 13 was not implemented, although the SER had required the contractor to complete implementation "as directed by fiscal year planning."

The Nuclear Safety and Licensing organization had a schedule for achieving implementation of the human factors program, but the ORP Environment, Safety, Health, and Quality Assurance organization told the assessment team that it did not meet their expectations. In the view of the assessment team, there were program features that should have been implemented, even if fiscal year planning had not yet allowed for full program development. For example, human-machine interface checklists described in the FSAR should be used during the design of new and modified tank farm systems.

Conclusion:

The FSAR does not properly describe some major components of the transfer leak detection system. The lack of such description contributed to inadequate system knowledge on the part of system engineers. The FSAR must also define performance criteria for these major components. While it did so for conductivity leak detection probes, it did not for the replacement cross-site structure leak detectors or the AWF leak detection pit weight factor instrumentation.

The FSAR and hazard analysis must consider all credible hazards to the facility, evaluate their risk, and identify any necessary controls (such as design features or operating limits) for managing the risk to an acceptable level. Specifically, 10 CFR 830.2021, *Safety Basis*, paragraph (b)(4) and (b)(5) required in part that the contractor responsible for the facility must "...prepare a documented safety analysis for the facility and establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment." Contrary to this requirement, degraded voltage or degraded power conditions were not considered or addressed in the FSAR or hazards analysis.

In addition to implementing a human factors program responsive to chapter 13 of the FSAR, CHG should begin performing some of the activities of a human factors program. For example, CHG should be employing the human-machine interface checklists

described in the FSAR for modifications and new systems.

Issues:

- a. The tank farms FSAR did not adequately describe all safety-significant components of the transfer leak detection system. (Finding 8)
- b. In describing the operability of the safety structures, systems, and components, the tank farms FSAR did not explicitly provide performance criteria relied upon in the accident analysis during normal, abnormal, and accident conditions. (Observation 5)
- c. Degraded voltage or degraded power conditions were not addressed in the FSAR or hazards analysis. (Finding 5)
- d. CHG has not instituted the human factors program described in the FSAR. (Observation 7)

Appraisal Form

Transfer Leak Detection System

Topical Area: System Maintenance	Criteria Met
Date: February 26, 2002	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Objective:

The system is maintained in a condition that ensures its integrity, operability and reliability.

Criterion:

1. Maintenance processes consistent with the system safety classification are in place for prescribed corrective, preventive, and predictive maintenance, and to manage the maintenance backlog.

Approach:

Records Review:

- 1-1 Verify that maintenance for the system satisfies system requirements and performance criteria in safety basis documents or other local maintenance requirements.

Note: The following approach statements 1-2 and 1-3 need to be reviewed only once for common site or facility-specific implementation of maintenance management processes or programs.

- 1-2 Evaluate maintenance of aging system equipment and components.
 - Determine whether there are criteria in place to accommodate aging-related system degradation that could affect system reliability or performance.
 - Review the plans and schedules for monitoring, inspecting, replacing, or upgrading system components needed to maintain system integrity, including the technical basis for such plans and schedules
- 1-3 Determine whether maintenance source documents such as vendor manuals, industry standards, DOE Orders, and other requirements are used as technical bases for development of system maintenance work packages.

Interviews:

Maintenance managers, production control personnel, system engineering managers and system engineers

Observations:

N/A

Process:

Records Reviewed:

- a. HNF-IP-0842, Volume 5 – *Production Control*, Section 7.1, REV 9b, “Tank Farm Contractor Work Control”
- b. HNF-IP-0842, Volume 5 – *Production Control*, Section 7.3, REV 6a, “Preventive Maintenance”
- c. RPP-MP-624, REV 0, “Maintenance Excellence Plan”
- d. HNF-IP-0842, Volume 4 – *Engineering*, Section 2.21, REV 0b, “Conduct of System Engineering”
- e. HNF-SD-WM-SAR-067, Tank Farm FSAR, Chapter 2 REV 3a, “Facility Description”
- f. HNF-SD-WM-SAR-067, Tank Farm FSAR, Chapter 4 REV 3a, “Safety Structures, Systems, and Components”
- g. HNF-SD-WM-SAR-067, Tank Farm FSAR, Chapter 10 REV 3a, “Initial Testing, In-Service Surveillance, and Maintenance”
- h. HNF-SD-WM-SAR-067, Tank Farm FSAR, Chapter 11 REV 3a, “Operational Safety”
- i. 3-LDD-055, REV C6, Tank Farm Maintenance Procedure, “Troubleshooting and Repair of Liquid Detector”
- j. 3-LDD-042, REV G15, Tank Farm Maintenance Procedure, “Testing of Liquid Detector”
- k. HNF-IF-0842, “RPP Administration,” Conduct of Operations Manual
- l. RPP-9848, REV 0, “System Health Report For Waste Transfer Instrumentation”
- m. RPP-9878, REV 0, “System Health Report For Saltwell Electrical and Instrumentation”
- n. RPP-9960, REV 0, “System Health Report for the Single Shell Tank Waste Transfer Instrumentation System”

Personnel/ Positions Interviewed:

- a. C. Defigh-Price, Manager, System Engineering
- b. M. R. Koch, Single Shell Tank System Engineering
- c. M. J. Sutey, Single Shell Tank Engineering
- d. B. L. Sharer, Production Control Manager
- e. G. P. Graves, production control
- f. J. A. Bewick, system engineer
- g. J. B. Roberts, system engineer
- h. R. E. Larson, design authority/design engineer
- i. D. H. Shuford, Reliability/Maintenance Manager
- j. M. G. Al-Wazani, design authority/design engineer
- k. R. L. Schlosser, engineer
- l. T. J. Bowman, design engineer
- m. T. L. Hissong, Maintenance Manager
- n. K. E. Drakulich, Electrical Supervisor

Evolutions/Operations/Shift Performance Observed:

N/A

Results:

Discussion of Results:

1-1 The required 92-day TSR surveillances of transfer leak detection system were timely in 2001, but two surveillances were performed late in 2000. The surveillances that were past due in 2000 were within the grace period for the 92-day TSR surveillance. There was not a formal prescribed corrective, preventive, or predictive maintenance program for the transfer leak detection system. In discussion with the assessors, maintenance managers explained that maintenance or system engineering typically identified equipment and systems requiring prescribed corrective, preventive, or predictive maintenance and that they had not requested these type of maintenance activities for the

transfer leak detection system.

On February 7, during a 92-day surveillance of leak detectors LDE-DB-U-151 and LDE-DB-U-152 the associated transmitter panel LDT-15 electrical-mechanical components had accumulated a significant quantity of dirt and sand. This equipment failed to function correctly during the surveillance test. The dirt appeared to be a major contributor to the surveillance failure. The transfer panel used for this transfer leak detection system was older and only used in three locations throughout the tank farms. Additionally, the condition of transmitter panel LDT-15 was poor and justified special maintenance focus. For example, dust and sand entered the panel because the cover had no sealing gasket.

FSAR section 2.4.14 stated that to minimize and control corrosion, most encasement piping associated with the DST in 200E was protected by an impressed-current cathodic protection system. Additionally, section 3.3.2.4.7, "Waste Transfer Leaks," stated that corrosion was a major contributor to leaks in the transfer lines. The transfer lines were classified as safety significant. Yet the cathodic protection system was not classified as safety class, safety significant, or defense-in-depth.

The system engineers stated that an independent verification performed by the QA department during maintenance might be warranted for lifted DC wiring for the impressed-current cathodic protection system. Reverse landing of the positive and negative leads on the impressed-current cathodic protection system during maintenance would accelerate rather than suppress the piping corrosion rate. Safety classification is an important influence on selection of QC inspections.

System engineers also said that there was not documentation of the decision process for classification on record for the impressed-current cathodic protection system. The impressed-current cathodic protection system classification evaluation was performed prior to implementation of Procedure HNF-IF-0842, "RPP Administration," which required formal documentation of control decision records.

1-2 The contractor had a process for evaluating historic maintenance and surveillance activities to gain insight on failure modes and areas for improvement. However, the process used a computer database that required extensive sorts to gain insight on historic surveillance and maintenance information to determine aging-related system degradation that could affect system reliability or performance. As discussed in a system maintenance appraisal deficiency form and section 2-3, the current practice to build in maintenance activities to fix failed surveillances in surveillance work packages obscured the computer generated equipment history because maintenance and post surveillance activities were not captured. Additionally, there was a lack of clear guidance on the type of as-found conditions and field observations to document in surveillance and maintenance work packages. On February 7, the assessors observed several transfer leak detection surveillances and noted that the craft did not document the as-found conditions of the equipment. This included the LDT-15 transmitter panel that had a significant accumulation of dust and dirt.

The new system engineering program required system engineers to walk down assigned systems for which they were responsible. The first system health report had been issued for the transfer leak detection system during the assessment period and identified the three transfer panels as the least reliable and in need of replacement. However, as noted in section 1.1 above, there were no additional compensatory maintenance activities to ensure that the LDT-15 transmitter panel equipment remained operable.

1-3 Assessors observed that the LDT-15 transmitter panel enclosure did not provide a level of protection against blowing dust and moisture. Specifically, the transmitter enclosure door was missing a seal to provide a degree of protection against blowing dust and moisture, and sand and dust had accumulated within the LDT-15 transmitter panel enclosure. Craft explained that absence of the enclosure door seal was a major contributor to the accumulation of dirt and dust in the LDT-15 transmitter panel enclosure. Dust and dirt interferes with proper operations of safety significant relays inside the enclosures.

The assessors reviewed the contractor's foreign material exclusion (FME) program used during maintenance and surveillance activities. On February 7, the assessors observed the 151-U and 152-U 92-day TSR surveillance and saw no provisions for FME. Specifically, the work package did not address weather conditions (wind) before starting or other FME considerations during maintenance or surveillance activities. Field supervision and craft explained they were unaware of a formal FME program but expressed concern that the results of high winds could degrade exposed systems. In a follow-up discussion with the assessors, the production control manager explained that there was not a formal FME program for Tank Farm activities and stated the need for one was warranted. The contractor issued PER-2002-1134 to document the FME issue.

Conclusions:

Maintenance processes consistent with the system safety classification were in place for prescribed corrective, preventative, and predictive maintenance, and to manage the maintenance backlog. However, there were weaknesses in the execution of these processes.

Preventive maintenance might be warranted for some older components such as the transfer leak detection electrical-mechanical components. The assessor questioned the lack of safety classification for the impressed-current cathodic protection system.

The conduct of maintenance and surveillance activities does not provide accurate feedback to gain insight on the degradation or reliability of the transfer leak detection equipment. The system engineering program included a process to assess equipment conditions and this process was being implemented.

CHG was maintaining a safety system panel enclosure. Outdoor electrical equipment should be protected from the effect of weather, such as rain and wind. The lack of a gasket in an outdoor enclosure appeared to be significant contributor for the failure of the

151-U and 152-U 92-day TSR surveillance. Additionally, the assessors concluded that the need for a formal FME program was warranted.

Issues:

- a. Lack of a safety classification for the impressed-current cathodic protection system has the potential to accelerate deterioration of protected piping. (Observation 2)
- b. The condition of transfer leak detection system's LDT-15 transmitter panel enclosure allowed the accumulation of dust and sand within the panel that was a significant contributor to the failure of the 151-U and 152-U 92-day TSR surveillance. (Observation 6)
- c. Lack of a foreign material exclusion program for maintenance and surveillance activities can adversely affect equipment and system operability. (Observation 4)

Appraisal Form

Transfer Leak Detection System

Topical Area: System Maintenance	Criteria Met
Date: February 20, 2002	<input type="checkbox"/> Yes' <input checked="" type="checkbox"/> No

Objective:

The system is maintained in a condition that ensures its integrity, operability and reliability.

Criterion:

2. The systems are periodically walked down in accordance with maintenance requirements to assess its material condition.

Approach:

Records Review:

- 2-1 Verify that the systems are inspected periodically according to maintenance requirements.
- 2-3 Review system or component history files for selected system components for the past three years.
 - Identify whether excessive component failure rates were identified.
 - Determine how failure rates were used in establishing priorities and schedules for maintenance or system improvement proposals.
- 2-4 Review the procedure and process for performing walk downs of the system.

Interviews:

- 2-4a Verify through manager and worker interviews that personnel performing walk downs understand operational features, safety requirements and performance criteria for the system.

Observations:

- 2-2 On a sample basis, perform a walkdown inspection of the systems with emphasis on the material condition of installed equipment, components, and operating conditions. Identify and document any observed conditions that could challenge the ability of the system to perform its safety function (e.g., leaks, cracks, deterioration, or other degraded or abnormal conditions). Determine whether observed deficiencies have been identified and addressed in a facility condition assessment or deficiency tracking system.

Process:

Records Reviewed:

- a. HNF-IP-0842, Volume 5 – *Production Control*, Section 7.1, REV 9b, “Tank Farm Contractor Work Control”
- b. HNF-IP-0842, Volume 5 – *Production Control*, Section 7.3, REV 6a, “Preventive Maintenance”
- c. RPP-MP-624, REV 0, “Maintenance Excellence Plan”
- d. HNF-IP-0842, Volume 4 – Engineering, Section 2.21, REV 0b, “Conduct of System Engineering”
- e. HNF-SD-WM-SAR-067, Tank Farm FSAR, Chapter 2 REV 3a, “Facility Description”
- f. HNF-SD-WM-SAR-067, Tank Farm FSAR, Chapter 4 REV 3a, “Safety Structures, Systems, and Components”
- g. HNF-SD-WM-SAR-067, Tank Farm FSAR, Chapter 10 REV 3a, “Initial Testing, In-Service Surveillance, and Maintenance”
- h. HNF-SD-WM-SAR-067, Tank Farm FSAR, Chapter 11 REV 3a, “Operational Safety”
- i. 3-LDD-055, REV C6, Tank Farm Maintenance Procedure, “Troubleshooting and Repair of Liquid Detector”
- j. 3-LDD-042, REV G15, Tank Farm Maintenance Procedure, “Testing of Liquid Detector”
- k. HNF-IF-0842, “RPP Administration” Conduct of Operations Manual
- l. RPP-9848, REV 0, “System Health Report For Waste Transfer Instrumentation”
- m. RPP-9878, REV 0, “System Health Report For Saltwell Electrical and Instrumentation”
- n. RPP-9960, REV 0, “System Health Report for the Single Shell Tank Waste Transfer Instrumentation System”

Personnel/ Positions Interviewed:

- a. C. Defigh-Price, Manager, System Engineering
- b. M. R. Koch, Single Shell Tank System Engineering
- c. M. J. Sutey, Single Shell Tank Engineering
- d. J. A. Bewick, system engineer
- e. J. B. Roberts, system engineer
- f. R. E. Larson, design authority/design engineer
- g. D. H. Shuford, Reliability/Maintenance Manager
- h. M. G. Al-Wazani, design authority/design engineer
- i. R. L. Schlosser, design engineer
- j. T. J. Bowman, engineer
- k. T. L. Hissong, Maintenance Manager
- l. K. E. Drakulich, Electrical Supervisor

Evolutions/Operations/Shift Performance Observed:

- a. Replacement of a failed leak detector local alarm panel strobe light fixture

Results:

Discussion of Results:

2-1 The transfer leak detection system was not included in the maintenance inspection program. Maintenance management explained that the maintenance inspection program was invoked when systems were failing surveillances, were requiring abnormal maintenance, or when requested by engineering. In a discussion with the assessors, a maintenance engineer explained there was no indication from the review of past 92-day TSR surveillances that any reliability or operability concerns existed with transfer leak detection systems. As discussed the section 2-2 below, the current maintenance practice that allows maintenance activities to be included in surveillance work packages, coupled with problems in the conduct of maintenance activities, obscured identifying reliability or operability concerns. This conclusion was based on the review of all the 2000 and 2001 work packages queried from the database of J-5 reports.

2-2 and 2-3 On February 7, the assessors observed the 92-day TSR LDE-DB-U151 and LDE-DB-U152 transfer leak detection surveillance to gain first hand knowledge of the system's condition and to observe maintenance activities. The details of this surveillance were documented in System Surveillance and Testing appraisal form in this report. However, based on discussions with select craft supervision, field craft, and system engineering, the assessors elected to perform in-depth review of year 2000 and 2001 system and component maintenance records associated with the LDE-DB-U151 and LDE-DB-U152 transfer leak detection system. This review was because craft supervision, field craft, and system engineers told the assessors that the electrical-mechanical components inside LDT-15 transmitter panel were cleaned with compressed air during the surveillance.

The assessors learned through discussions with craft supervisors, field craft personnel, and system engineers that maintenance craft personnel were performing troubleshooting and maintenance activities on the LDT-15 transmitter panel without a procedure and without documenting their activities. Specifically, the assessors noted that the maintenance records for the leak detector LDE-DB-U-151 and LDE-DB-U-152 92-day TSR surveillance identified one failed surveillance (2W-00-01207P, performed on October 23, 2000) for the eight surveillances conducted between December 2000 and August 2001. However, some craft supervision, craft personnel, and system engineers told the assessors that the LDT-15 transmitter panel would not operate properly during the first surveillance attempt. This was based on their previous experience with this test. Failure of the test would be due to the accumulation of dust and dirt in the electro-mechanical components. The assessors learned that instead of using the appropriate work controls, craft were cleaning the LDT-15 transmitter panel internal components and then re-testing the system to satisfactorily complete the 92-day TSR surveillances for LDE-DB-U-151 and LDE-DB-U-152. This practice was leading to the conclusion that the leak detectors LDE-DB-U-151 and LDE-DB-U-152 had been working properly when they actually might not have performed their safety function.

Through discussions with the craft supervisor and maintenance craft personnel, the assessors learned that the craft believed their past troubleshooting activities for the LDT-15 transmitter panel were performed in accordance with Procedure 3-LDD-055, *Troubleshooting and Repair of Liquid Detector*. TSR Surveillance Procedure 3-LDD-042, *Testing of Liquid Detector* directed craft personnel to use 3-LDD-055 to troubleshoot and repair certain specific problems identified during TSR surveillances of liquid detection equipment.

Procedure 3-LDD-055 authorized troubleshooting on panels LDE-DB-U-151 and LDE-DB-U-152, not for the LDT-15 transmitter panel. Also, it did not authorize cleaning any panel to assist in passing a TSR surveillance test.

Any work outside the scope of 3-LDD-055 required the use of engineering drawings and logical troubleshooting techniques. Because of the safety significance of this leak detection system, any such work required a properly approved procedure and/or work package. Even if the work on LDT-15 transmitter panel was included in the scope of

procedure 3-LDD-055, workers failed to document their findings and repairs in the work package and to obtain engineering approvals as required by 3-LDD-055.

Unauthorized and undocumented maintenance, especially when performed to complete TSR surveillance requirements, defeats the reliability and system engineering processes that would identify aging and failure-prone equipment. It also obscures accurate knowledge of the operability of safety systems. Waste transfer procedures do not re-perform TSR surveillances prior to transfers, but rather rely on a review of surveillance documentation. CHG assumes that equipment that successfully passed its last surveillance will remain operable throughout the surveillance interval. Finally, failure to properly document all surveillance failures can result in inappropriate surveillance frequencies. The TSR bases for this surveillance state, "This FUNCTIONAL TEST Frequency has been established based on operating experience and the maintenance recall system."

2-4 The newly implemented system engineering program procedures required system engineers to perform walk-downs to evaluate the field condition of assigned systems. These walk-downs were an essential part of system performance monitoring. Weekly, system engineers were to perform routine walk-downs with a focused review of data, observation of work activities, and inspection of the general conditions of critical equipment, housekeeping, and safety. Quarterly, a comprehensive walk-down was to be performed to verify the as-found physical configuration was correct, to identify any discrepancies, to maintain awareness of system condition, and to gather data related to system performance.

The assessment team noted that the walk-down process described in procedure NF-IF-0842, Volume 4, Section 2.21, Rev 0b, "Conduct of System Engineering," included all the attributes for system engineers to gain insight on the condition of equipment and systems for which they were responsible. The assessment team noted that the transfer leak detection initial system health report for the single shell tanks identified the transmitter panels and Gamewell® components of the transfer leak detection system were unreliable and in need of replacement.

CHG management told the assessment team that they were having trouble fully implementing their system walkdown process. This was largely due to the burden of work on system engineers. So far, the quarterly walkdowns were compilations of many smaller walkdowns that occurred over the quarter.

The assessment team interviewed system engineers and reviewed the records of their walkdowns. Team members also traveled with system engineers during some walkdowns. The assessment team agreed that there was room for further progress on implementing the walkdown requirement. For one thing, it appeared from their records that system engineers were not making their walkdowns, but it was clear that they did not always know when to record an activity as a walkdown. CHG management clarified this with the system engineers during the time of the assessment fieldwork.

The assessors did not see any field enhancements made to the transfer leak detection system that had resulted from the implementation of the new system engineering program. The assessors noted that the system engineering program was still under development, and it would have been inappropriate to assess the effectiveness of the program at the time of the assessment.

Conclusion:

Systems are periodically walked down in accordance with maintenance requirements to assess material condition. However, this process is not fully implemented, largely because system engineers are burdened with many duties. Some system engineers did not understand that some of their activities were valid walkdowns, and so did not record them as such. Also, quarterly walkdowns were not yet a discreet activity, but were instead a compilation of many smaller walkdowns. This could be a problem because there is no mechanism to assure that the many smaller walkdowns result in visits to the entire system.

Some aspects of the way maintenance activities are conducted obscure problems with the reliability and operability of safety equipment.

The assessors noted that the contractor repeatedly performed unauthorized and undocumented maintenance on a transfer system leak detector transmitter panel. This obscured an actual operability problem with this safety significant component.

The newly implemented system engineering program has the structure to gain accurate insight on the operability of tank farm systems and equipment. CHG must continue its development.

Issues:

- a. TSR surveillance work packages include corrective maintenance that could obscure the maintenance and surveillance history of equipment. (Observation 1)
- b. The contractor performed unauthorized and undocumented maintenance on a transfer system leak detector transmitter panel, obscuring an actual operability problem. This was a safety significant component, and the problem occurred repeatedly over a period of two years. (Finding 3)

Appraisal Form

Transfer Leak Detection System

Topical Area: System Engineer Program	Criteria Met
Date: February 14, 2002	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Objective:

A viable system engineer program exists.

Criterion:

1. Systems have been identified whose safety significance warrants the assignment of a safety engineer.

Approach:

Records Review:

- 1-1. Review contractor procedures and verify that a system engineer program is documented.
- 1-2. Review independent and management assessment reports that address the system engineer program. Determine whether program weaknesses are being identified and resolved.
- 1-3. Review the system engineer program procedures and documents to determine if a current list of vital safety systems exist to which the system engineer program is applied.
- 1-4. Review system engineer assignments and the contractors vital safety system list. Verify that at least one system engineer is assigned to each system.

Interviews:

System engineering managers and system engineers

Observations:

N/A

Process:

Records Reviewed:

- a. HNF-IP-0842, Volume 4 – *Engineering*, Section 2.20, REV 1, “Operability Evaluations”
- b. HNF-IP-0842, Volume 4 – *Engineering*, Section 2.21, REV 1, “Conduct of System Engineering”
- c. Management Assessment (System Engineering Manager) dated February 6, 2001
- d. ORP letter 01-OPD-026, Ami B. Sidpara to M. P. DeLozier, CHG, “Direction to Provide a List of System Engineers to Meet the Defense Nuclear Facilities Safety Board Recommendation 2000-2,” dated March 21, 2001
- e. ORP memorandum 01-TOD-T008, Dana C. Bryson to Michael J. Oldham, EM-3, “Transmittal of the Vital Safety System Information (Commitment 5) for the River Protection Project,” dated August 8, 2001

Personnel/ Positions Interviewed:

- a. Cherri Defigh-Price, Manager, System Engineering
- b. Michael Koch, Manager, Single Shell Tank System Engineering
- c. Michael Sutey, Manager, Single Shell Tank Engineering
- d. J. A. Bewick, system engineer
- e. J. B. Roberts, system engineer
- f. D. A. White, system engineer
- g. R. R. Bafus, system engineer
- h. C. Rupp, ESG, Inc.
- i. T. C. Oten, Manager, Double Shell Tanks System Engineering

Evolutions/Operations/Shift Performance Observed:

N/A

Results:

Discussion of Results:

- 1-1 A system engineering program is established and documented. The documentation is achieved through the two procedures, "Conduct of System Engineering" and "Operability Evaluations." These procedures are not very old, and still have some "bugs" in them. CHG management told the assessment team that as they go through the first year of applying the procedures, problems are being identified for correction.
- 1-2 At the time of this assessment, the system engineering manager was just completing an extensive management assessment of her program. The assessment had not yet been formally issued, but it appeared to be thorough. It identified problems in the program, the correction of which should significantly enhance the program. For example, the CHG assessment found that system engineers believed that reporting problems with their systems would reflect negatively on them professionally. CHG management said they were acting to change this perception.
- 1-3 There does not appear to be a formal agreement between ORP and CHG identifying the vital safety systems. Following an informal dialogue with CHG, ORP submitted a list to HQ and shared the list with CHG. CHG has used the list to assure themselves that at least one system engineer is responsible for each system. Since the ORP list was submitted to HQ, ORP has changed this list, but only identified the change by e-mail correspondence.
- 1-4 CHG has identified system engineers for all systems they consider vital safety systems. The manager of System Engineering told the assessment team that they have also verified that all systems identified by ORP as vital safety systems have an assigned system engineer. The assignments are posted on an internal web site.

Conclusion:

Systems have been identified whose safety significance warrants the assignment of a safety engineer. CHG management conducts management assessments of their program to identify issues for correction. At the time of this assessment only one comprehensive management assessment has been performed and the final report has not been issued. However, it is reasonable that CHG would be performing its first management assessment at this stage in the development of this program.

At the time the assessment began, CHG and DOE-ORP each believed the other organization was controlling the formal list of vital safety systems. DOE provided a list of vital safety systems in a letter dated March 21, 2001. CHG considered this list to be authoritative, but DOE personnel thought CHG was maintaining a more definitive list.

Issues:

- a. There is no controlled list of vital safety systems recognized by both DOE and CHG. (Finding 7)

Implementation Plan for Phase II VSS Assessment of the Transfer Leak Detection System

Results:

Discussion of Results:

Conclusion:

Issues:

Inspector: _____ Date: _____	Approved: _____ Team Leader Date: _____
---------------------------------	-----------------------------------------------

Appraisal Form

Transfer Leak Detection System

Topical Area: System Surveillance and Testing	Criteria Met
Date:	<input type="checkbox"/> Yes <input type="checkbox"/> No

Objective:

Surveillance and testing of the safety system demonstrates that it is capable of accomplishing its safety functions and continues to meet applicable system requirements and performance criteria.

Criteria:

1. Requirements for surveillance and testing are adequate for demonstrating overall system reliability and operability, and are linked to the technical safety basis.
2. Surveillance and test procedures confirm that key operating parameters for the overall system and its major components are maintained within operating limits.
3. Instrumentation and measurement and test equipment for the system are calibrated and maintained.

Approach:

Records Review:

- 1-1 Identify the acceptance criteria from the surveillance test procedures used to verify that the system is capable of performing its safety functions. Compare the acceptance criteria with the safety functions, functional requirements, performance criteria, assumptions and operating characteristics discussed in safety documents. Verify that there is a clear linkage between the test acceptance criteria and the safety documentation, and that the acceptance criteria are capable of confirming that safety/operability requirements are satisfied.
- 2-1 Review surveillance and testing procedures for the system's major components. Review a sample of the test results and verify:
 - Validity of test results
 - System performance meets system requirements
 - Performance criteria are appropriate for current facility mission life-cycle
 - Parameters that demonstrate compliance with the safety requirements can be measured