Office of the Assistant Manager for Environment, Safety, Health and Quality; U.S. Department of Energy, Office of River Protection

Assessment A-02-AMSQ-TANKFARM-002, Phase II Vital Safety System Assessment, Transfer Leak Detection System

Issued: March 2002

Executive Summary

This report provides the results of the phase II assessment of the tank farms transfer leak detection system. The Office of River Protection (ORP) performed the assessment in response to a DOE commitment to the Defense Nuclear Facilities Safety Board (DNFSB) for DNFSB recommendation 2000-2, *Configuration Management, Vital Safety Systems*, concerning degrading conditions of vital safety systems (VSSs). The phase I assessment of the Hanford Tank Farms was performed by CHG and DOE during an extended period of CY 2001.

Material condition varied from good to poor.

The material condition of equipment varied considerably throughout the Tank Farms. For example, wiring in some electrical junction boxes was well laid out and properly labeled. In other boxes, however, labels and wiring were in poor condition. Outdoor boxes sometimes lacked weather seals on their doors so that during bad weather, water and dirt would enter these boxes. In some cases, cable sheathing had deteriorated and the internal wires (insulated) were exposed. That there are areas of poor material condition in the Tank Farms is a well-known situation stemming in part from traditional funding practices for the Tank Farms. The assessment team was concerned that living with poorly maintained equipment could desensitize both DOE and contractor personnel to the role of the equipment in fulfilling its safety function.

CHG had made good progress on developing the system engineer program.

CHG had established a system engineer program and was in the process of implementing it. Procedures had been prepared and issued. System engineers had been trained, qualified (interim), and assigned to systems. CHG was continuing to develop the program, and progress during the preceding year was good.

The tank farms had an approved FSAR, but implementation was incomplete.

The final safety analysis report (FSAR) described the transfer leak detection system and identified it as safety significant. A technical safety requirement (TSR) required the system to be operable during transfers, and some surveillance activities were specified to verify operability. The assessment team found that the FSAR description of the transfer leak detection system was incomplete in some areas. Also, implementation of some parts of the FSAR was incomplete, such as the human factors program described in chapter 13.

CHG was working to improve configuration management.

Historically, the Tank Farms have suffered from poor configuration management. One result has been poor documentation of facility design. In April 2000, CHG issued a plan regarding how to recover documentation and control of facility design, as well as for dealing with equipment aging issues. CHG appeared to be making progress on carrying out their plan.

CHG has procedures for control of computer software, including control of commercial off-the-shelf software and legacy software. However, software for a safety significant system was not classified as safety significant and configuration management over the complete software life cycle was not consistent with standards for safety significant software.

Some surveillance tests were not performed correctly.

CHG had a surveillance testing program based on the TSRs. Surveillance items were accomplished in accordance with a formal schedule, but the assessment team found problems with execution of some surveillance tests. The assessment team found that operations outside a test procedure actually invalidated the test so that the test did not accurately represent the operability of the equipment.

Primary Issues

The assessment team's primary issues were:

- Procedure violations invalidated a TSR-related surveillance test.
- Eight months after identifying a TSR violation, CHG failed to perform the required root cause analysis and develop a corrective action plan.
- There was no controlled list of VSSs in either DOE or CHG.
- There was no technical training for system engineers, and oral examinations may not have accurately measured system engineer candidates' knowledge.
- System engineers were unaware of some components within their responsibility.
- The effects of degraded voltage were not considered by the FSAR.
- The FSAR did not adequately describe the transfer leak detection system.
- Some programs and activities described in the FSAR were not implemented.

Table of Issues

Issue No.	Description	Topical Area
Finding 1	Contractor personnel violated administrative procedures during and after a TSR functional test.	System Surveillance and Testing
Finding 2	During some transfer leak detector quarterly functional tests, the tank farm contractor did not perform a verification described in the TSR bases. The contractor self-identified this issue as a TSR violation eight months ago but had not completed root cause analysis and corrective action planning and implementation.	System Surveillance and Testing
Finding 3	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.	System Maintenance
Finding 4	Contractor personnel did not properly report two failed saltwell transfer leak detector TSR surveillances to the Central Command and Control Station.	System Surveillance and Testing
Finding 5	Degraded voltage or degraded power conditions were not addressed in the FSAR or hazards analysis.	Safety Function Definition
Finding 6	System engineers were not provided with systematic technical training on the final safety analysis report, the technical safety requirements, and the design features of their systems.	System Engineer Program
Finding 7	There was no controlled list of vital safety systems recognized by both DOE and CHG.	System Engineer Program
Finding 8	The tank farms FSAR did not adequately describe all safety-significant components of the transfer leak detection system.	Safety Function Definition
Finding 9	There was an incomplete formal record of the software operational history for the saltwell PIC skid programmable logic controllers.	Configuration management
Finding 10	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.	Configuration management

Finding 11	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.	Configuration management
Finding 12	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.	Configuration management
Finding 13	The design description and commercial grade item (CGI) dedication for leak detection relay circuits did not identify or address all critical characteristics.	Configuration management
Observation 1	TSR surveillance work packages include corrective maintenance that could obscure the maintenance and surveillance history of equipment.	System Maintenance
Observation 2	Lack of a safety classification for the impressed-current cathodic protection system has the potential to accelerate deterioration of protected piping.	System Maintenance
Observation 3	A specific and uniform format and content should be established for software configuration management plans governed by HNF-PRO-309.	Configuration management
Observation 4	Lack of a foreign material exclusion program for maintenance and surveillance activities can adversely affect equipment and system operability.	System Maintenance
Observation 5	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.	Safety Function Definition
Observation 6	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.	System Maintenance
Observation 7	CHG has not instituted the human factors program described in the FSAR.	Safety Function Definition

Signatures

David H. Brown,
Team Lead

Courtney A. Blanchard,
Assessor

for James M. Leivo
per telecon
3/11/02 0735

James M. Leivo,
Assessor

Stephen H. Pfaff,
Assessor

Dale H. Splett,
Assessor

Table of Contents

I. Introduction

A. Objectives of the Evaluation

In March 2000, the Defense Nuclear Facilities Safety Board (DNFSB) issued Recommendation 2000-2, *Configuration Management, Vital Safety Systems*, concerning degrading conditions of vital safety systems (VSSs). The DNFSB recommended that DOE assess the condition of VSSs, develop programs for contractor and federal technical personnel, and improve the self-assessment processes that evaluate the condition of VSSs.

In October 2000, DOE issued the *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2000-2*. This plan specified a phased approach to the evaluation of confinement ventilation systems and other vital safety systems. During the initial phase of the plan (phase I), assessments were performed on a set of VSSs at "priority" facilities. (VSSs include safety class, safety-significant, fire protection, and other defense-in-depth systems.) The phase I assessment of the Hanford Tank Farms was performed by CHG and DOE during an extended period of CY 2001.

DOE also committed to the DNFSB that it would perform phase II assessments focusing more directly on field conditions of VSSs. These were to follow the phase I assessments, building on their results.

This report provides the results of the phase II assessment of the Tank Farms transfer leak detection system. It applied a set of criteria and review approach documents (CRADs) that were developed from a model set of CRADs provided by DOE-HQ. DOE-HQ developed the model CRADs for assessments of VSSs in DOE defense nuclear facilities.

This assessment was intended to provide an understanding and characterization of system operability and reliability issues, including those identified during the phase I assessment. While the phase I assessment focused on documentation, the phase II assessment focused primarily on actual hardware and system performance. It also evaluated the newly implemented CHG system engineering program as applied to this VSS.

B. Review Process and Methods

The phase II assessment team performed an independent review that provided evidence of the operability of the transfer leak detection system. It was accomplished through sampling by document reviews, personnel interviews, and field observations to determine if the equipment was operable. It was also to determine if documentation, maintenance activities, and personnel were capable of assuring continued operability.

Assessment team members used the review approaches described in the CRADs to guide their evaluations. The CRADs were documented in the implementation plan, *ORP DNFSB Recommendation 2000-2 Phase II Assessment of the Hanford Tank Farms Transfer Leak Detection System.*

Topical Areas

The assessment addressed five topical areas:

- Safety function definition,
- Configuration management,
- System maintenance,
- System surveillance and testing, and
- The CHG system engineering program.

Process Boundaries

Equipment subject to the assessment were leak detectors and associated electrical equipment within the following system boundaries:

Waste Transfer Containment

- The waste transfer containment system, including waste transfer lines (direct buried lines, pipe in pipe, hose in hose etc.), waste transfer pits, diversion boxes and clean-out boxes, cover blocks and cover plates for pits and waste transfer lines;

- Waste transfer piping and encasements;

- Process pits and jumpers;

- The over-ground transfer lines pipe encasements and cover blocks and piping encasements;

Waste Transfer Instrumentation

- Master pump shutdown system (a vital safety system) with the various leak detectors, interlocks and alarm functions.

C. Team Composition

Team members carried out the following assignments as described in the implementation plan:

David H. Brown	Team Lead, System Engineering Program
Courtney A. Blanchard	System Maintenance, System Surveillance and Testing
Stephen H. Pfaff	Safety Function Definition, System Surveillance and Testing
Dale H. Splett	Configuration Management
James M. Leivo	Safety Function Definition, Configuration Management (computer software control)

Qualifications of the team members were described in the assessment implementation plan.

II. Assessment Results

A. Material Condition

Material condition varied from good to poor.

The material condition of equipment varied considerably throughout the Tank Farms. For example, wiring in some electrical junction boxes was well laid out and properly labeled. In other enclosures, however, labels and wiring were in poor condition. These enclosures were often outdoors and, in at least one case, lacked weather seals on the doors. During windy or wet weather water and dirt would enter these boxes. In some cases, cable sheath had deteriorated and the internal (insulated) wires were exposed. That there are areas of poor material condition in the Tank Farms is a well-known situation stemming in part from traditional funding practices for the Tank Farms.

Another example of poor material condition was from the U and TX Tank Farm inductive relay leak detection equipment. There, 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 other 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 resister 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 resister was unknown.

There were also problems with the cross-site transfer optic equipment communications line. Installation of the fiber optic line was very sloppy, with the individual fiber optic leads loosely strung over to the front terminals on the programmable logic controller (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 the 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.

CHG personnel were complacent regarding some poorly maintained equipment.

Generally, equipment in the East Tank Farms was in much better material condition than equipment in the West Tank Farms single shell tanks. CHG managers said that this stemmed from historic funding practices in DOE and its contractors wherein work in East Tank Farms was prioritized above work in the West Tank Farms. When money ran out, some work was never performed, especially in the West Tank Farms. The result is that both contractor and DOE personnel were simply accepting that equipment in the West Tank Farms would not be well maintained. However, when the assessment team identified the lack of a seal on an electrical enclosure cover, CHG was able to promptly correct this condition.

There is a large amount of equipment in the Tank Farms for which maintenance and upgrade funding has been historically meager. The assessment team was concerned that living with poorly maintained equipment could desensitize both DOE and contractor personnel to the role of the equipment in fulfilling its safety function. Because it is unlikely that the Tank Farm funding will ever allow upgrading equipment to nuclear facility standards, overcoming this complacency is a particularly difficult challenge.

System health reports were off to a good start.

An important and promising element of the new system engineering program was the system health report process. Each system engineer was required to develop a report documenting the condition of his or her system. System engineers were then required to report on their systems to a panel that included the CHG chief engineer and the system engineering manager. The overall results were then presented to the CHG Senior Facility Review Board and the facility directors. This systematic approach to assessing system operability promises to be a useful tool form making maintenance and funding decisions. Presentations provided important opportunities for system engineers to discuss problems with their systems with management. Some of these problems might otherwise not come to management attention.

B. System Engineer Program

CHG had established a system engineer program and was in the process of implementing it. Procedures had been prepared and issued. System engineers had been trained, qualified (interim), and assigned to systems. CHG was continuing to develop the program, and progress during the preceding year had been good.

Procedures were in place.

The system engineer program was based on two procedures in HNF-IP-0842, Volume 4 – *Engineering*. They are Section 2.20, *Operability Evaluation*, and Section 2.21, *Conduct* *of System Engineering*. Both procedures appeared to provide coherent direction to system engineers.

Training was developed and accomplished.

System engineer training is comprised of three courses: "Determining System Operability," "Performance Monitoring," and "Reliability-Centered Maintenance." These courses are managed and presented by the CHG training department, using training department procedures.

There was no technical training on either the FSAR or on the Tank Farm systems. CHG management said that this was acceptable because system engineers were drawn from the cadre of cognizant engineers who were considered to be technically knowledgeable. Under the organization that existed before creation of the system engineer role, cognizant engineers were responsible for routine engineering work. Many (but not all) had extensive experience in the Tank Farms.

An important distinction between the cognizant engineer system and system engineers is in how responsibilities were assigned. Cognizant engineers were usually assigned to ongoing engineering duties for a single farm, while system engineers were now responsible for a single facility system running through many farms. Therefore, under the cognizant engineer system, a mechanical engineer might be responsible for the electronics engineering in instrumentation and control equipment for his or her farm.

CHG management said that they verified the technical knowledge of system engineer candidates in the qualification process. Also, system engineers received training in how to use the FSAR to perform USQ determinations. The FSAR training used, for example, the technical safety requirements (TSRs) in making practice USQ determinations, but it did not systematically train system engineers on the requirements of the FSAR and TSRs.

The assessment team noted one weakness in system engineer knowledge in that some system engineers were unfamiliar with some leak detectors addressed in the FSAR and TSRs. These were leak detectors located in the Aging Waste Facility transfer leak detection pits and air-purged encasement leak detectors. This indicated a need for improvement in the system engineer training and qualification program.

Qualification requirements were established and completion documented.

CHG established two "qualification cards" for system engineers, an interim qualification and a final qualification. A third qualification card for system engineering managers had recently been issued. All system engineers and backup system engineers with current assignments had completed the interim qualification card. Each of them was recently issued a final qualification card that was to be completed by August 2002. CHG had also recently distributed the qualification card for system engineer managers so that they could begin documenting their qualification process.

The qualification process for system engineers included completion of classroom training, required reading, and an oral examination. A board of CHG managers administered the oral examination. The oral board usually included the chief engineer and the director of system engineering. System engineers were asked a variety of questions, many of which were designed to determine the technical knowledge of the candidate. For example, candidates were usually asked to draw a schematic of their system.

While the design of the qualification process was generally appropriate, it included an important weakness. During the examination, the oral board members did not have available to them verified answers to the questions. While CHG managers responsible for system engineers are experienced and knowledgeable regarding tank farm systems, it is unlikely that any of them know all of the systems to the level of detail required of a system engineer. Therefore, they might not always recognize incorrect answers to oral board questions.

C. Safety Function Definition

The tank farms had an approved FSAR, but implementation was incomplete.

The FSAR described the transfer leak detection system and identified it as safety significant. A TSR required the system to be operable during transfers, and some surveillance activities were specified to verify operability. The assessment team found that the FSAR description was incomplete in that it focused solely on conductivity leak detectors and did not adequately describe the weight factor instrumentation in the Aging Waste Facility leak detection pits or their function in transfer leak detection. It also did not describe the unique leak detectors in the replacement cross-site transfer system diversion box and vent station.

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.

The safety equipment list was undergoing revision.

CHG generally defined the nuclear safety classification in the FSAR at the system level, and the safety equipment list (SEL) was intended to then identify the classification of individual components. At the time of this assessment, CHG was preparing a major revision to the SEL that would increase its level of detail. In the meantime, it was sometimes necessary for engineers to make individual decisions on the classification of individual components.

Other issues

While the impressed-EMF cathodic protection system was outside of the transfer leak detection system, the assessment team still questioned whether it was correctly classified. CHG classified the system as general service, but it prevented corrosive deterioration of safety significant piping. Incorrect configuration of the equipment could actually accelerate deterioration of the piping. This was encasement piping, forming a secondary barrier against release of waste to the environment should the primary piping fail.

Also, the FSAR did not clearly identify requirements and performance criteria for the transfer leak detection system beyond normal operation. Operations under abnormal and accident condition are not specifically addressed for any system.

D. Configuration Management

CHG was working to improve configuration management performance.

CHG had a configuration management system that was described in HNF-1900, *Configuration Management Plan for the Tank Farm Contractor*. This document was published in April 2000 and CHG had been working to implement it. CHG planned to issue revision 2 in the period following this assessment. The program was administered by a configuration management organization within the engineering organization.

At the time of this assessment, the configuration management organization was working to significantly upgrade CHG's performance in this area. This was necessary because configuration of the Tank Farm systems had not been properly maintained during significant periods of Tank Farms history.

Some important features of the configuration management plan were for design reconstitution, material condition management, and aging management. These are important features intended to overcome the historic problem of inadequate design control.

Computer software configuration management was coherent but had weaknesses.

CHG had established processes for the development and control of computer software. These were generally consistent with industry norms, but there were some weaknesses.

The assessment team used the computer software associated with programmable logic controllers to evaluate software control. While control of configuration of the ladder logic was important, the assessment team also evaluated control of the underlying operating system that applied the ladder logic to control of the transfer leak detection system.

The assessment team concluded that there was reasonable assurance that safety significant software was being adequately controlled with respect to changes to the baseline software that had been established by the design authority. The software configuration management plans were generally adequate and consistent with governing procedures.

In a sample of software configuration items, the assessment team did not find any software configuration discrepancies. However, the team identified several deficiencies with the overall software life cycle quality process for the transfer leak detection system. For example, software supporting the waste transfer leak detection system was not classified as "safety significant," as stipulated in the FSAR. This was commercial off-the-shelf software, and the configuration baseline had been documented as-found in considerable detail by the contractor. However, there were some problems with it. These were:

- There was no retrievable documentation of the requirements basis, procurement specifications, factory acceptance tests, or verification and validation records;
- There was no evidence of independent design verification for most of the software life cycle design documents including initial releases; and
- There was an incomplete formal record of the software operational history.

Notwithstanding the effective efforts by the contractor to document the as-found baseline configuration, the absence of critical life cycle documentation and design verification was contrary to the documentation standard for safety significant software.

Other Issues

Some other conditions discussed in Appendices C and D of this report were:

- Critical characteristics were not adequately identified and verified for leak detector relay CGI dedication.
- The leak detector circuit design description was not subject to design verification.

E. System Maintenance

The assessment team reviewed a sample of maintenance activities. This included checking programmatic issues, such as the status of maintenance backlog and the effectiveness of the deficiency reporting process.

The maintenance system was defined, but it had weaknesses.

While CHG had a coherent maintenance program, the assessment team identified several weaknesses:

- Discipline in the problem evaluation request (PER) process was not mature. PERs are the method required by CHG's procedures to document most types of deficiencies. However, personnel sometimes initiated corrective action for a problem without documenting the problem on a PER. As a result, visibility on problems and classes of problems could be lost. For example, input to the trending process relies on consistent use of PERs.

  The PER process had only been in place for about a year, and it was not surprising that it would have some growing pains. CHG management had already recognized weaknesses in PER reporting and said they were working to improve performance on PERs. The following are examples of problems observed by the assessment team that were not documented on PERs:

  - Failed TSR surveillances of leak detector equipment were not documented.
  - A bad strobe light in West Tank Farms transfer leak detection system was replaced without a PER. Maintenance personnel and the system engineer had difficulty obtaining the proper replacement part.
  - The lack of a weather seal on a leak detector transmitter enclosure cover was recognized but not documented.

- Aside from the lack of PERs there were other feedback mechanisms that were not always working properly. For example, CHG procedures required that problems occurring during maintenance were to be entered in the "comments" section of the work package, but this was not always done.

- CHG did not have coherent foreign material exclusion guidance in maintenance procedures. This came to the attention of the assessment team when it saw that dirt had entered an outdoor electrical panel and interfered with operation of some relays.

- CHG's current practice of including maintenance activities in surveillance work packages to address equipment problems occurring during surveillances diminished the opportunity to identify component reliability issues.

F. System Surveillance and Testing

CHG had a surveillance testing program based on TSR requirements. Surveillance items were accomplished in accordance with a formal schedule, but the assessment team found problems with execution of some surveillance tests.

Unauthorized work was performed during a TSR surveillance.

The assessment team observed execution of procedure 3-LDD-042, "Testing of Liquid Detector." Personnel performing the test anticipated that it might fail. When it did fail, they manipulated components in a manner not authorized by the procedure. This surveillance was eventually recorded as unsatisfactory, but craft personnel, craft supervision, and system engineers said that cleaning of leak detector transmitter panels had occurred during previous surveillances to enable satisfactory completion of the surveillance tests. This cleaning removed dirt that interfered with proper operation of mechanisms within the enclosure. In the view of the assessment team, the test may sometimes pass only because of this type of unauthorized work. (This practice is sometimes referred to as "preconditioning" the equipment.) Consequently, the test results did not accurately represent the operability of the equipment.

A surveillance procedure did not satisfy the TSR bases.

The assessment team reviewed recent TSR surveillance packages and found that many were missing a requirement described in the TSR bases. The basis for TSR LCO 3.1.3 required a verification that previous maintenance activities had not affected leak detector probe positions. The interim stabilization group properly included this verification in their surveillance procedure, but the remainder of the Tank Farms organizations did not.

IV. Lessons Learned

- The assessment was accomplished with an appropriate level of planning using experienced assessors. However, the assessors were not able to complete all of their fieldwork in one week. This was due partly to the fact that some of the assessors had no previous exposure to the Tank Farms but also to the amount of work required to gather all of the information specified in the CRADs. All things considered, the best approach to this would have been establishing a fieldwork period of two weeks, rather than one week. The next two assessments for this series will generally use the same personnel, and it should go more quickly, because they now have a reasonable level of tank farms field experience. Also, a lot of the information gathered in the first assessment will also be applicable to the next two assessments. But if assessors are unable to perform their fieldwork in one week it has not been a problem to simply extend the fieldwork period.

- The CHG audit center was very valuable as a base of operations. It was equipped with sufficient desk space and new computers to accommodate the assessment team. It would have been difficult to accomplish the assessment in the time allotted without a central location like the audit center.

- The assessment team chose to follow a format for the assessment much like an operational readiness review (ORR). CRADs were provided in the assessment implementation plan, and assessors performed fieldwork in line with the review approaches specified in the CRADs. The assessors prepared appraisal forms in the same manner is for an ORR, and they submitted findings and observations on deficiency forms.

  As issues were identified, the team provided CHG with draft deficiency forms. This is typical for ORRs where contractors must move quickly to resolve issues that may be in the critical path for an important event. However, it does not provide as much time for the assessors to synthesize information among them into more meaningful issues. In a conventional assessment, the team more carefully considers issues before they are shared with the contractor. (An exception is a deficiency in which there is an imminent hazard. These situations are immediately brought to the attention of contractor management.)

In future assessments, assessment teams should continue to brief contractor and DOE management on potential issues as fieldwork proceeds. However, draft issues should not be provided to the contractor in writing until the whole draft report is ready for the comment/review cycle.

- Identifying issues that were already understood was awkward. In the case of conventional assessments, issues that have been previously identified and have a reasonable action plan are not identified as findings. However, an important purpose of this assessment was to describe the current condition of the system. Therefore, issues that were already documented might be identified again for this assessment. This could create a situation in which the assessment identifies issues that are already well known, but causes the contractor to expend resources to respond to them again. The assessment team should be cautious in identifying previously known issues so that responding to the assessment does not require an unnecessary expenditure of the contractor's resources.

Appendix A

Implementation Plan

Implementation Plan

ORP DNFSB Recommendation 2000-2 Phase II Assessment of the Hanford Tank Farms Transfer Leak Detection System

February 4, 2002

Table of Contents

1.0 Introduction/Background

In March 2000, the Defense Nuclear Facilities Safety Board (DNFSB) issued Recommendation 2000-2, *Configuration Management, Vital Safety Systems*, concerning degrading conditions of vital safety systems (VSSs). The DNFSB recommended that DOE assess the condition of VSSs, develop programs for contractor and federal technical personnel, and improve the self-assessment processes that evaluate the condition of VSSs.

In October 2000, DOE issued the *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2000-2.* This plan specifies a phased approach to the evaluation of confinement ventilation systems and other vital safety systems. During the initial phase of the Plan (phase I), assessments were performed on a set of VSSs at "priority" facilities. (VSSs include safety class, safety-significant, fire protection, and other defense-in-depth systems.) The phase I assessment of the Hanford Tank Farms was performed by CHG and DOE during an extended period of CY 2001.

The phase I assessment of the Hanford Tank Farms found weaknesses in the design, maintenance, and operation of some VSSs. Subjects for the phase II assessment were chosen from among the systems that displayed weaknesses during the phase I assessment.

This implementation plan addresses performance of phase II assessments for the transfer leak detection system, the primary tank leak detection system, and the AN tank farm ventilation system. The DOE developed a set of model assessment criteria and review approach documents (CRADs) for assessment of VSSs in DOE defense nuclear facilities. These model CRADs form the basis for the assessment approach applied for this phase II assessment.

This plan describes the scope, activities, method of accomplishment, and schedule for the performance of the phase II assessment of the transfer leak detection system. The report of the assessment will be submitted through ORP to DOE-HQ for ultimate transmittal to the DNFSB. Additional phase II assessments will be performed on other systems when this assessment is complete.

2.0 Purpose

This document provides the plan for the Office of River Protection (ORP) phase II assessment of the transfer leak detection system. The assessment is intended to provide an understanding and characterization of system operability and reliability issues, including those identified during the phase I assessment. While the phase I assessment focused on documentation, the phase II assessment will focus on actual hardware and system performance. It will also evaluate the newly implemented CHG system engineering program, as applied to this VSS.

3.0 Scope

3.1 Topical Areas

The assessment will address five topical areas:

- Safety function definition,
- Configuration management,
- System maintenance,
- System surveillance and testing, and
- The CHG system engineer program.

The results of the phase I assessment will serve as a starting point for issues, although fieldwork may identify additional issues.

3.2 Process Boundaries

Activities subject to the assessment are within the following system boundaries:

a. **Waste Transfer Containment**
   - The waste transfer containment system includes waste transfer lines (direct buried lines, pipe in pipe, hose in hose etc.), waste transfer pits, diversion boxes and clean-out boxes, cover blocks and cover plates for pits and waste transfer lines also provide waste containment functions.
   - Waste transfer piping and encasements; process pits and jumpers
   - Vital safety components include: The over ground transfer lines pipe encasements and cover blocks and piping encasements.
   - These are broken down further (w/in tank farms) by DST, SST and interim stabilization ("hose-in-hose").

b. **Waste Transfer Instrumentation**
   - Master pump shutdown system (a vital safety system) with the various leak detectors, interlocks and alarm functions. This is broken down further by SST (which includes the cross site transfer), DST, and interim stabilization.

4.0 Approach

The phase II assessment team will perform an independent review that provides evidence of the operability of the transfer leak detection system. This will be accomplished by document reviews, personnel interviews, and field observations to confirm that all required equipment, documentation, and personnel are capable of sustained operation.

Assessment team members will use the review approaches described in the CRADs to guide their evaluations. Upon completion of the fieldwork, the assessment team will document its conclusions in a report.

5.0 Preparation

While team members have been chosen for their skills and knowledge in the areas of their assignments, each team member must identify in advance what material they will need in order to conduct their evaluation. For example, team members should identify and review the appropriate CHG procedures applicable to their area before the assessment begins. (The assessment team leader will facilitate obtaining material and other needs once identified by the team members).

The assessment team leader will arrange with CHG for the team's logistical needs during the assessment. These will include office space, telephones, and computers.

The assessment team leader will assure that all security and access issues are resolved prior to beginning the fieldwork. Team members will require access to tank farms equipment, although this may be with an escort.

Prior to beginning the assessment, the assessment team will prepare lines of inquiry that address their areas of responsibility. These will be in a checklist format as specified by the assessment team lead that verify the criteria of the CRADs are satisfied. Team members will provide copies of their lines of inquiry to the team leader before the fieldwork begins.

6.0 Processes

The assessment will be carried out in accordance with Reference 9.1. Team members will review documents, conduct interviews, review equipment, and observe activities during the fieldwork period. They will perform verifications in accordance with the attached appraisal forms and lines of inquiry. Deficiencies will be documented on deficiency forms. Team members will submit their completed appraisal forms and deficiency forms to the team leader prior to the end of the fieldwork period.

6.1 Guiding Principles

The assessment will be guided by the following principles, as discussed in Reference 9.1:

- Line management will be notified immediately when the team identifies a condition that poses an immediate threat to personnel or facility safety;
- The assessment team will review the phase I assessment and other reports, but it will not duplicate other activities;
- The assessment will include inspections to determine physical material condition and consistency of system configuration with documentation;
- Procedures and records for system surveillance testing and maintenance will be evaluated to determine whether they are appropriate and are being used to verify that system requirements and performance criteria described in the safety documentation are satisfied;
- Software quality assurance will be within the scope of the assessment;
- Reviews of site-wide or tank farm-wide processes and programs that directly affect continued integrity, reliability, and availability of different systems may be combined;
- Results of the assessment will be discussed in an exit meeting and be described in an assessment report;
- Items worthy of DOE-wide dissemination will be entered into the DOE lessons learned system; and
- If observers and trainees accompany the assessment team, they shall not interfere with the conduct of the assessment.

7.0 Team Organization

Team assignments are described in Table 1.

Team member resumes are provided in Appendix A.

8.0 Reporting

During the conduct of the assessment, documentation of assessment issues and the assembly of objective evidence of operability will be the responsibility of the individual team members.

The appraisal form will be used to document the methods and actions of a team member taken in their criteria evaluation process. Each form 1 will be complete enough to allow an outside agency reviewing the form to follow the inspection logic and means used to verify operability of the system.

The write-up will clearly describe the approach taken to review the criteria. If for some reason the approach used does not exactly match the approach described in the appraisal form, the reason will be documented. The conclusion will specify if the criteria for the particular review approach have been met. Appraisal forms may include observations that are either recognition of excellent practices that are considered noteworthy or are minor deficiencies not considered significant enough to be findings.

The deficiency form is used to document issues identified during the criteria evaluation process. A separate deficiency form should be generated for each issue related to a particular review approach. For instance, in reviewing an area, a team member will generate a single appraisal form that describes the methods used in the investigation. It identifies the conditions found and states the issues involved. If one distinct issue is discovered, the assessment team member will generate a deficiency form to detail the deficiency. If three distinct findings are identified the assessment team member will then generate three deficiency forms. A single deficiency form may be used to identify a generic problem for which a number of individual examples are listed.

9.2 Lessons Learned

The team leader will report any problems or successes specific to the conduct of this assessment and document them as lessons learned to aid future assessments. These lessons learned will be submitted to the DOE lessons learned program.

9.3 Final Report

With the assistance of the assessment team, the team leader will develop a report to document the results of the assessment. Team members will be requested to concur in the final report for the areas or their specific responsibility. Dissenting opinions that have not been resolved will be appropriately addressed in the report. The assessment team leader will transmit the final report to the ORP office manager, the director of the Technical Operations Division and other interested parties. The director of the Technical Operations Division will be responsible for transmitting the report to the contractor and obtaining resolution on the assessment issues.

Dissenting opinions give the individual team members an opportunity to voice concerns they believe were not adequately addressed in the report.

9.0 References

9.1 DOE-EH memorandum, Steven V. Cary to Assistant Secretary for Environmental Management, et. al., *Model Assessment Criteria and Guidelines for Performing Phase II Assessments of Safety Systems at Defense Nuclear Facilities*, November 30, 2001

Approval

David H. Brown,
Assessment Team Leader

Delmar L. Noyes,
Director, Technical Operations Division

Table 1

Team Member Assignments

David H. Brown	Team Lead, System Engineer Program
Courtney A. Blanchard	Mechanical Systems, Authorization Basis
Stephen H. Pfaff	Mechanical Systems, Authorization Basis
Dale H. Splett	Instrumentation and Control
James M. Leivo	Instrumentation and Control, Computer Software Control

Appendix A

Team Member Resumes

David H. Brown – Assessment Team Leader

Mr. Brown has 30 years of experience in nuclear work. Fourteen of these years were in startup and testing work on submarine reactors at a naval shipyard. For the past 15 years he has worked at DOE-RL and DOE-ORP, primarily in the area of quality assurance and nuclear safety assessments. He holds a Bachelor of Science degree in nuclear science from the State University of New York Maritime College.

Mr. Brown is qualified as a lead auditor under the ORP NQA-1 qualification program, having held a DOE lead auditor certification since 1987. He has led many audits, assessments, surveillances, and employee concerns investigations, as well as two accident investigations. He has also led four ORRs and participated as a team member in several others.

Dale H. Splett – I&C

Mr. Splett has over 27 years of experience in nuclear reactor operations, instrumentation & control systems, and in project management for nuclear material storage and handling facilities. He was a qualified nuclear power plant electrical operator with the U.S. Navy and later performed instrumentation, control, and electric power equipment installation and troubleshooting of nuclear systems at Puget Sound Naval Shipyard. Mr. Splett earned a Bachelor of Science degree in electrical engineering from Seattle University in 1990 and worked as an instrumentation & control systems engineer in the Puget Sound Shipyard Nuclear Engineering Department.

Mr. Splett joined the Department of Energy in 1994 and performed project engineering, management and facility operations oversight duties for the Hanford Spent Nuclear Fuel Project through 2001. In addition to new project development he was also responsible for issues concerning the Spent Nuclear Fuel authorization basis, review of the final safety analysis report, unreviewed safety questions and technical safety requirement violations, and has performed readiness assessments and operational readiness reviews for systems and facility startup. This work also included configuration control and management oversight of systems in facilities at or near their design life. He is currently a construction project manager with the DOE Office of River Protection.

Stephen H. Pfaff -- Authorization Basis/Mechanical Systems

Mr. Pfaff has 16 years of experience in nuclear reactor operations and nuclear facility oversight. Seven years were devoted to naval nuclear propulsion plant operations and maintenance on two ships. For the past nine years, he has served as a Department of Energy Facility Representative in plutonium facilities at the Rocky Flats Site and in the Tank Farms at the Hanford Site. Mr. Pfaff earned a Bachelor of Science degree in Business Administration with minors in Science and Naval Science in 1983 from Oregon State University. Mr. Pfaff is qualified as a lead auditor under the ORP NQA-1 qualification program and has led or participated in many assessments and surveillances.

Courtney Blanchard -- Authorization Basis/Mechanical Systems

Mr. Blanchard has 21 years of industrial experience including 8 years in the nuclear field. In May of 2001, he transferred to the Department of Energy from the Nuclear Regulatory Commission (NRC) were his last assignment was Senior Resident Inspector at the Paducah Gaseous Diffusion Plant located in Paducah, Kentucky. Mr. Blanchard is a graduate of Michigan Technological University and has a professional engineering license in the State of Washington. His work experience includes construction engineering with Owens Illinois, design engineering and management with Puget Sound Naval Shipyard, as well as industrial and radiological inspection activities with the NRC. He presently works on technical interfaces for the Assistant Manager of System Requirements (AMSR) at ORP.

Mr. Blanchard was a qualified fuel cycle inspector and resident inspector with the NRC, now performs performance/compliance reviews of interface activities for AMSR, and has performed an inspection for the ORP Office of Safety Regulation. At the NRC he led several performance inspections and was a member of the ORR inspection for increasing the Paducah Gaseous Diffusion Plant assay enrichment.

James M. Leivo, P. E. -- I&C, Computer Software Technical Specialist,

Mr. Leivo has over 34 years of experience in the nuclear industry, including technical direction of the design and retrofit of instrumentation, control, electrical, and computer systems for nuclear power plants and facilities. His experience includes design, regulatory submittal, regulatory inspections, and independent design inspections/assessments. His career includes 14 years with Westinghouse Nuclear Energy Systems Divisions; three years with NUS Corporation and Los Alamos Technical Associates; and 17 years as an independent consultant to the NRC I&C Branch, NRC Inspection Programs, nuclear utilities, and DOE. He holds a BSEE from Carnegie Mellon University, and completed various graduate level courses as a part of the Florida Institute of Technology Digital Systems Option.

Since 1986, Mr. Leivo has supported over 50 independent assessments of nuclear facilities, including design inspections for NRC and design assessments for nuclear utilities. This included thread audits and assessments of safety-related and critical computer-based systems retrofitted to operating plants. Examples of utility assessments include: the auto-essential feedwater control system at Davis-Besse; and the digital feedwater control system, switchyard SCADA system, and automatic test interface for the diesel generator load sequencer at Salem. Examples of NRC audits or inspections of digital systems include the reactor protection systems at D. C. Cook and Haddam Neck; thermal margin monitor at Palisades; and the plant safety monitoring system at Beaver Valley. He also supported preparation of safety evaluation reports for the DOE WERF and WSF facilities at INEL. Mr. Leivo has also served as team leader on several design assessments performed for nuclear utilities.

Appendix B

Criteria Review and Approach Appraisal Forms

Criteria And Approach

The *Criteria, Review and Approach* section is divided into topical areas: (1) safety function definition, (2) configuration management, (3) system maintenance, and (4) system surveillance and testing. Each of these topical areas includes:

- *Objective* describes the intent that the topical area should contribute to assessment of the safety system
- *Criteria* characteristics of a system that should be verified
- *Approach* collection of information needed to assess the condition of the system according to the criteria. The items in the *Approach* section are to guide the assessment team; however, the assessment team may choose to select another approach to meet assessment-specific needs.

For each topical area, the criteria and approach items are numbered for easy reference. The items under the *Approach* subsection are numbered such that the items can be readily linked back to the most applicable criterion (e.g., item number 2-1 under the Approach is most directly linked to Criterion 2). However, the evaluation of each criterion should consider all relevant information collected during the assessment (not only information related to the linked items).

The 2000-2 phase I assessment or other reviews of the system being assessed may satisfy some of the objectives and criteria that follow. Previous reviews may also contain information relevant to this assessment, which can be cited and used in this assessment. In such situations, this assessment should be limited to objectives and criteria not covered in previous assessments and should not unnecessarily duplicate previous assessments.

Criteria review and approach appraisal forms are to be completed by team members and submitted to the team leader for approval. They will then become part of the final report.

Appraisal Form

Transfer Leak Detection System

Topical Area: Safety Function Definition	Criteria Met
Date:	[ ] Yes [ ] No

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

Criteria:
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:

Personnel/ Positions Interviewed:

Evolutions/Operations/Shift Performance Observed:

Results:

Discussion of Results:

Conclusion:

Issues:

Inspector: ______________________ Date: ______________________	Approved: ______________________ Team Leader Date: ______________________

Appraisal Form

Transfer Leak Detection System

Topical Area: Configuration Management Date:	Criteria Met [ ] Yes [ ] No

Objective:

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

Criteria:

1. Changes to system safety basis requirements, documents, and installed components are designed, reviewed, approved, implemented, tested, and documented in accordance with controlled procedures. Consistency is maintained among system requirements and performance criteria, installed system equipment and components, and associated documents as changes are made.

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.

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.

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.

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:

1-1 On a sample basis, review and evaluate the change control process and procedures and associated design change packages and work packages to determine whether the change control process and procedures are adequate and effectively implemented. Determine whether:

- SSCs and documents affected by the change are identified
- Changes are accurately described, reviewed and approved as appropriate

- Installation instructions, post-modification testing instructions and acceptance criteria for turnover to facility operations are specified, and
- Important documents affected by the change (e.g., operating and test procedures, Master Equipment List, etc.) are revised in a timely manner.

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

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:

1-2 Interview a sample of cognizant line, engineering, QA managers and other personnel to verify their understanding of the change control process and commitment to manage changes affecting design and safety basis in a formal, disciplined and auditable manner.

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.

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

Observations:

2-1 Walkdown 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:

Personnel/ Positions Interviewed:

Evolutions/Operations/Shift Performance Observed: -

Results:

Discussion of Results:

Conclusion:

Issues:

Inspector: ____________________ Date: ____________________	Approved: ____________________ Team Leader Date: ____________________

Appraisal Form

Transfer Leak Detection System

Topical Area: System Maintenance Date:	Criteria Met [ ] Yes [ ] No

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

Criteria:

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.

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

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.

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:

2-1 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:

Personnel/ Positions Interviewed:

Evolutions/Operations/Shift Performance Observed:

The team noted that ECNs supporting changes to these documents had been subject to an "informal review." However, documentation of the scope and disposition for these informal reviews was not retrievable. The "informal review" process was described in a CHG procedure that was subsequently cancelled.

In interviews, the design authority and CHG management said that the scope of informal reviews typically was at the discretion of the document author, and there was apparently no requirement to document an informal review and retain records of the comments and their resolution. HNF-IP-0842, Vol. IV, "Engineering," Section 4.24, *Design Verification* prescribes specific requirements for design verification and its documentation.

Determination of critical characteristics - Design description documents

The design description for the intrinsically safe leak detector circuit (HNF-SD-ER-736 Revision 0, May 8, 1998) identified the circuit as "safety class." However, the design description did not include critical electrical design inputs and characteristics such as tolerances for supply voltage, frequency, and harmonic content as well as device ratings such as surge withstand capability, contact ratings, and diode ratings.

The design description purported to delineate the requirements for the leak detector circuit and demonstrate compliance to the requirements presented. It was generally comprehensive and traceable to design inputs that appeared valid at the time the document was written. However, some authorization basis references were obsolete as was the "safety class" classification. For example, reference to HNF-SD-WM-BIO-001 for the safety basis was no longer valid. The current FSAR stipulates "safety significant," not "safety class" for this equipment.

In interviews with the cognizant engineer for the document and the design authority for the system, they said that the anticipated system design description program was expected to revisit these types of requirements. They expected the system design description program and the safety equipment list update to provide a more complete identification of the design basis and design inputs/requirements that might have been missing in earlier design documents.

The assessment team also discussed the larger issue of system design descriptions with the manager for Tank Farms configuration management. General system design descriptions did not currently exist for Tank Farm systems, but were under development. Approximately 55 design description documents were scheduled to be completed this year. The lack of these documents made it difficult for the assessment team to understand the functions of the various transfer leak detection systems. The lack of a comprehensive listing of the essential drawings for each system also contributed to this difficulty, although the Tank Farm contractor published a Tank Farm-wide list of essential drawings. The essential drawings for each system, along with the system description, were to be included in the release of the design description documents. These documents were expected to greatly aid the system engineers and anyone needing to understand a particular system.

CGI dedication

The CGI dedication for leak detection relays and circuits (HNF-4275, Revision 8, September 25, 2001) also did not include critical electrical design inputs and characteristics. These included characteristics such as tolerances for supply voltage, frequency, and harmonic content as well as device ratings such as surge withstand capability, contact ratings, and diode ratings. The document was limited to a functional test of the leak detection relay circuits as a "black box." In interviews, the design authority said he believed this approach was typical of CGI dedications. The team concluded that functional tests are necessary but not always sufficient to identify and demonstrate conformance to all critical characteristics of an SSC.

The design authority stated that the anticipated system design descriptions are expected to be the formal documentation of all critical characteristics for the system of interest and its equipment.

Conclusion:

The Tank Farms contractor had a system of procedures in place to control changes to engineering documents through the configuration management program. The technical and management personnel responsible for making changes to transfer leak detection documentation as well as managing the change control process itself were aware of the applicable procedures and requirements. These requirements were for the most part correctly applied and followed. However, improvements to the system could be made, such as in the areas of timely completion of work, and system descriptions. CHG was taking steps to improve the configuration management program, notably new procedures for processing engineering changes and development of system design descriptions.

Some particular problem areas included the following:

- Initial issues of safety significant hardware and software design documents had not been subject to design verification as required by 10 CFR 830.122(f)(4).

- Subsequent changes to safety significant hardware and software design documents implemented by ECNs appear to have been subject to an informal review process, as specifically requested by the author of the change. However, there was no retrievable record of the scope of the informal review or disposition of the reviewer's comments as required by current design verification procedures.

- The design description and commercial grade item (CGI) dedications for leak detection relay circuits did not identify or address all critical characteristics, as required by HNF-IP-0842, Volume 4, Section 3.11. For the documents reviewed by