APPENDIX B

U.S. NUCLEAR REGULATORY COMMISSION
REGION IV

NRC Inspection Report: 50-498/94-11
50-499/94-12

Operating License: NPF-76
NPF-80

Licensee: Houston Lighting & Power Company
P.O. Box 1700
Houston, Texas 77251

Facility Name: South Texas Project Electric Generating Station,
Units 1 and 2

Inspection At: Matagorda County, Texas

Inspection Conducted: March 10 through April 14, 1994

Inspectors: D. P. Loveless, Senior Resident Inspector
D. M. Garcia, Resident Inspector
J. M. Keeton, Resident Inspector

Approved: W. D. Johnson 4/22/94
W. D. Johnson, Chief, Project Branch A Date

Inspection Summary

Areas Inspected: Unannounced, special, reactive inspection of the events and circumstances surrounding the safety injection actuation and subsequent loss of decay heat removal that occurred on March 10, 1994.

Results:

- Management controls were insufficient to prevent surveillance testing that had the potential to cause a loss of decay heat removal while the reactor was in midloop operations (Sections 2.2, and 2.7).

- One violation with two examples was identified for failure of reactor operators to follow surveillance procedures. This failure led to a safety injection actuation and loss of decay heat removal while the reactor was in midloop operations (Section 2.3).

- The shift supervisor had indications that reactor operators were not properly controlling the surveillance test; however, he did not adequately evaluate the situation (Section 2.3).

- Although investigation and troubleshooting did not identify the specific reason for the safety injection actuation, the inspector determined that the solid state protection system was left in an operable condition and that the licensee engineers' hypotheses were reasonable (Section 2.4).

- The licensee's corrective actions for this event were comprehensive and included generic actions to improve management controls of significant testing and maintenance activities (Section 2.5).

- The operational procedures provided adequate guidelines for midloop operations and met the licensee's commitments in response to Generic Letter 88-17, "Loss of Decay Heat Removal" (Section 2.6).

- Although the safety significance of the event was considered low, the failure to control testing that could have a negative impact on core cooling or personnel safety was considered significant (Section 2.7).

Summary of Inspection Findings:

- Violation 498/94012-01 was opened (Section 2.3).

Attachment:

- Persons Contacted and Exit Meeting

DETAILS

1 PLANT STATUS

1.1 Unit 1 Plant Status

At the time of the event on March 10, 1994, the Unit 1 reactor was in Mode 5, with the reactor coolant system drained to midloop in support of repairs to a leaking tube plug in Steam Generator C. The primary manways of Steam Generator C had been removed and the nozzle dams were not in place.

2 REVIEW OF THE CIRCUMSTANCES SURROUNDING THE SAFETY INJECTION ACTUATION AND SUBSEQUENT LOSS OF DECAY HEAT REMOVAL (93702)

2.1 System Overview

The solid state protection system (SSPS) was designed to trip the reactor to prevent unsafe operations that could lead to accident conditions. If an accident were to occur, a safety injection signal generated by the SSPS would actuate engineered safety features designed to mitigate the consequences of the accident.

The SSPS is comprised of two logic trains, designated R and S. Four input bays in each logic train receive signals from the process instrument racks, nuclear instrumentation, and field contacts throughout the plant. These signals are processed by the logic trains to determine if the appropriate logic for that parameter has been satisfied. Once the logic is satisfied, the logic train provides the respective actuation signal.

The output from SSPS Logic Trains R and S supply power for the undervoltage relay of the respective reactor trip breaker and the undervoltage coil of the opposite train bypass trip breaker. This allows on-line testing of the reactor trip breakers. Upon loss of this power, the reactor trip breakers will open. The R and S train outputs also provide signals to the three safety injection actuation trains designated A, B, and C.

Each logic train has a logic test panel. The panels allow for on-line testing of that train. With one logic train in test, a valid reactor trip or safety injection signal on the other train is sufficient to cause the requisite safety system response. However, the output of the train in test is inhibited and will not cause a reactor trip or safety injection.

Because safety system actuations are not required in all operational modes, certain safeguards actuation signals are provided with an operator initiated block. One example is the main steam line low pressure safety injection signal, which may be blocked to permit a controlled cooldown of the reactor and secondary plant.

2.2 Background

Prior to March 10, 1994, in order to support the ongoing work in Steam Generator C, licensed operators had drained the reactor coolant system to midloop in accordance with Plant Operating Procedure OPOP03-ZG-0009, "Mid-loop Operations."

The inspectors reviewed the plan-of-the-day agenda issued by licensee personnel on the morning of March 10. The planned activities included returning the reactor to midloop operations for removal of the steam generator nozzle dams. The inspectors noted that there were no shutdown risk assessment concerns noted in the appropriate section of the plan, even though entry into midloop operations was anticipated.

Additionally, on the Unit 1 scope table, management had delineated station surveillances as a high priority item. The operators were aware that Mode 4 restraints needed to be completed prior to returning the unit to power. During shift turnover from night to day shift on March 10, the shift supervisors discussed the need to perform Plant Surveillance Procedure OPSP03-SP-0005S, "SSPS Logic Train S Functional Test." The inspectors noted that this test was not included on the weekly Unit 1 surveillance schedule, nor was the activity listed on the planned activities list.

Senior licensee management stated that their reviews of activities to be performed while the reactor was in midloop operations had been limited to physical work. Routine surveillance activities were not considered a threat to nuclear safety. In addition, Procedure OPSP03-SP-0005S had not been performed when originally scheduled several days before. Therefore, the procedure was not on the weekly schedule and was being performed to ensure that surveillance requirements for Mode 4 were met.

The inspectors reviewed Plant Operating Procedure OPOP03-ZG-0009, Revision 8, "Mid-loop Operations," and Plant General Procedure OPGP03-ZO-0035, Revision 2, "Reduced RCS Inventory Operations." These procedures required the shift supervisor and midloop coordinator to review and remain cognizant of all work activities that may have affected the residual heat removal system capability. Again, management stated that this review only included a review of work activities and not surveillance testing. The shift supervisor and midloop coordinator did review the surveillance activity and determined that, if performed properly, the procedure would not be a risk. However, the review failed to identify that working in the logic train cabinets could negatively impact the reliability of the residual heat removal system.

The shift supervisor did identify that Procedure OPOP03-ZG-0009, Step 3.2.8, required that the operators ensure that the control rods were fully inserted and that the reactor trip breakers were open. Surveillance Procedure OPSP03-SP-0005S required the reactor trip breakers to be closed during certain testing evolutions. Therefore, the shift supervisor issued Field Change 94-0545 to Procedure OPOP03-ZG-0009 to allow the operators to

close the reactor trip breakers during this testing evolution. This action effectively bypassed a management administrative barrier.

At approximately 3:30 p.m., a pretest brief was conducted by the test coordinator. This briefing was general in nature, did not cover the specific details of the procedure, and, most notedly, the duty outage manager was not present nor aware that this testing was to be performed.

The inspectors concluded that senior management was not aware that this critical test was to be performed. Additionally, management controls were inadequate to inform senior management that testing was being performed, nor did these controls restrict surveillance testing during midloop operations.

2.3 Description of the Event

On March 10, 1994, while the plant was in midloop operations, licensed operators performed Plant Surveillance Procedure OPSP03-SP-0005S, "SSPS Logic Train S Functional Test." Section 5.1, "Setup for Test," required the operators to perform indication verifications and switch manipulations in protection system Logic Cabinets R and S, alternately. Step 5.3.1 required the operators to verify the condition of a test light in Logic Cabinet R. Similar verifications are then made in Logic Cabinet S in accordance with Step 5.3.2. Following Step 5.3.2 a note stated:

> Unless noted, all of the following steps are conducted at "PROTECTION SYSTEM LOGIC TRAIN S, LOGIC CABINET" (SSPS)(ZRR008), "LOGIC TEST PANEL."

The operators inadvertently began performing the following test steps in Protection System Logic Cabinet R. During an interview, the lead reactor operator stated that the procedure repeatedly transitioned from one logic cabinet to the other and that they had transitioned the final time instead of remaining in the Train S logic cabinet. The failure to perform the procedural steps in the cabinet specified is a violation (498/94012-01).

Prior to the performance of Step 5.18, the operators questioned a procedural note that required the memories check of the logic to be conducted in the Train S logic cabinet. This note was a repeat of the one quoted above. The operators stated that they originally believed the note to contain a typographical error. The operators indicated that they were aware that the test could not be performed in both logic trains at once.

The operators stopped work and informed the shift supervisor that the procedure was in error and required them to perform testing in both logic cabinets at the same time. The shift supervisor and the midloop coordinator reviewed the procedure, determined that it was adequate, and told the operators to complete the test. In interviews, the shift supervisor and the midloop coordinator stated that, at the time, they were unaware that the test was being performed in the wrong train. However, the inspector noted that the shift supervisor should have more fully reviewed the reactor operators'

questions, because they indicated that the operators did not understand and were not properly controlling the testing evolution.

Upon returning to the instrument cabinets, the operators determined that they had been working in the wrong logic cabinet. They decided jointly to back out of Logic Cabinet R using Section 5.20, "Restoration and Documentation." Although Precaution 3.6 stated that, if testing was terminated for any reason the shift supervisor was to be immediately notified, the reactor operators proceeded with the recovery without informing the shift supervisor. The failure to notify the shift supervisor, in accordance with plant procedures, is considered a second example of Violation 498/94012-01.

As part of the recovery actions, the operators attempted to perform Step 5.20.8.c that required the operators to place Turbine Trip Test Switch S-128 to normal. This action did not reset the turbine trip because the Train S reactor trip breaker was open. The operators repeatedly and in rapid succession attempted to reset the turbine trip by turning Test Switch S-128 to the normal position. During this effort, a full safety injection signal was received.

The control room operators responded to the event appropriately. All equipment functioned as expected, with the exception of Essential Chiller 11C that tripped on low oil pressure. The safety injection pumps had been disabled in the pull-to-lock position as required during shutdown conditions. As designed, the residual heat removal system pumps were stripped from the safety busses. This resulted in the loss of decay heat removal from the reactor. The pumps were restarted within 5 minutes, and reactor cooling was restored. During this evolution, the reactor temperature increased by 1°F.

During the evolution, reactor water level increased by approximately 1 1/2 inches. During normal operation of the residual heat removal system, the suction of the low-head safety injection system pumps is aligned to the refueling water storage tank. In this configuration, the pressure of the residual heat removal system kept the low-head safety injection pump discharge check valve closed. Upon loss of the residual heat removal system, the discharge check valves opened allowing a gravity feed path from the refueling water storage tank via the low-head safety injection system to the reactor vessel. The resultant level increase did not cause water level to increase above the normal midloop operations level band.

Following the actuation, the inspectors responded to the site to ensure that the transient had stabilized and that adequate reactor core cooling was established. The reactor core temperature was determined to be stable and the residual heat removal system was in service. Additionally, the shift supervisor had restricted any activities in the SSPS cabinets until an investigation of the event could be completed. A walkdown of the procedures was performed, including interviews with the reactor operators involved in the testing.

2.4 Analysis of the Event

Although the reactor operators had been performing testing in the wrong SSPS logic cabinet, there was no clear indication of the specific cause of the safety injection. The investigation determined that, prior to returning Logic Train R to service, a reactor operator stationed in the control room blocked the low pressure/low power safeguards actuation signals. This was the first indication that an operator in the control room was aware that testing had been performed on the wrong train. This operator indicated during interviews that he had failed to inform the lead reactor operator of the problem.

The licensee engineers' investigation initially indicated that the SSPS had malfunctioned and that the operators' actions had not caused the event. At the time of the event, the testing was being performed in Actuation Train B. Activities in this train should not have caused a full safeguards actuation of all three trains. Licensee engineers determined that both the safety injection low pressure blocks had released simultaneously.

The licensee engineers developed an extensive troubleshooting plan that was delineated in Temporary Engineering Procedure 0TEP07-SP-0005R, "SSPS Logic Train R Special Functional Test." The inspector reviewed the results of the test with the engineers. No problems with the SSPS circuitry, hardware, nor logic had been identified.

The engineers stated that the most likely cause of the actuation was a noise spike in Actuation Train B. The inspector noted that this could have been caused by the repeated operations of Turbine Trip Test Switch S-128 by the reactor operators as documented in Section 2.3 of this inspection report. Actuation Train B and Logic Train R were supplied power from the same distribution panel. Therefore, a noise spike at Switch S-128 in Actuation Train B could backfeed to the inverter and cause an electrical disturbance in Logic Train R.

The inspector reviewed the logic diagrams for the system and concurred that a spike at the power supply could have caused a full actuation signal to be generated in Logic Train R. The SSPS vendor also confirmed this finding.

As a result of these investigations, interviews with personnel involved, and a review of administrative controls, the following causes were identified:

- The reactor operators were working in the wrong train of the solid state protection system.
- The operators failed to perform self-verification and dual-verification of the SSPS logic cabinet designators prior to actuating switches.
- Upon discovery of their errors, the reactor operators failed to adequately communicate the problem to shift supervision.

- Shift managers failed to recognize that the conduct of this surveillance test during midloop operations could have resulted in a loss of decay heat removal and could have caused an uncontrolled release of reactor coolant system inventory.

- Shift supervision failed to provide oversight in the field when the operators presented a potential problem.

- Multiple procedural and management expectation barriers were bypassed by shift managers, shift supervision, and operators.

2.5 Review of the Licensee's Corrective Actions

As initial corrective action, control room operators reset the safety injection actuation system and restored reactor cooling by restarting the residual heat removal pumps. This action was accomplished in approximately 5 minutes. The individual operators and supervisors directly involved in this event were removed from shift. Personnel actions were taken in accordance with the constructive discipline program. The operators who were directly involved in the event developed a crew training briefing based on their experience. The briefing was presented to all operations personnel. Senior management expectations were reinforced and delineated by discussions with shift managers and shift supervisors.

Other administrative measures were implemented to prevent recurrence of this or similar events. Procedure OPOP03-ZG-0009 was revised to incorporate lessons learned. A work risk assessment document, to be completed prior to giving work start approval for surveillances, preventive maintenances, service requests, or postmaintenance testing, was developed and implemented. The inspectors reviewed examples of usage of this document and found that it appeared to be an effective tool as reported in NRC Inspection Report 50-498/94-10; 50-499/94-10. The corrective actions taken and proposed appeared to be sufficient to prevent recurrence of this event.

2.6 Review of Industry Operational Experience

Generic Letter 88-17, "Loss of Decay Heat Removal", dated October 17, 1988, provided recommended licensee actions to prevent and, if necessary, to respond to a loss of decay heat removal during operations with the reactor coolant system partially drained.

The licensee's programmed enhancements in response to Generic Letter 88-17 were reviewed and inspected as documented in NRC Inspection Report 50-498/90-17; 50-499/90-17. In that inspection report, the inspector concluded that the licensee's procedures and administrative controls appeared adequate to minimize reactor coolant system perturbations. The procedures associated with reduced inventory operations were also reviewed and generally supported the commitments made in the response to Generic Letter 88-17.

The inspector reviewed Plant Operating Procedure OPOP03-ZG-0009, Revision 8, "Mid-Loop Operation," and concluded that the procedure continued to provide adequate guidelines for midloop operations and meet the Generic Letter 88-17 commitments. However, as documented in Sections 2.2 and 2.7 of this inspection report, these guidelines were not well implemented.

2.7 Safety Significance

The inspectors reviewed the safety significance of this event. The residual heat removal system was lost approximately 5 minutes during this event. The reactor temperature only increased 1°F, and analysis indicated that it would have taken approximately 5 hours without cooling to begin reactor coolant boiling. However, as documented in Generic Letter 88-17, operating a plant with a reduced reactor coolant system water inventory was a particularly sensitive condition, and a loss of decay heat removal capability while at midloop could lead to fuel damage.

Additionally, at the time of the event, contractor personnel were working in and around the steam generator manways. During the evolution, reactor water level increased by approximately 1 1/2 inches, and remained within normal band for midloop operations. However, an inadvertent increase in the reactor coolant system inventory, such as a continued gravity drain, or the start of a safety injection pump, could have resulted in personnel injury and an uncontrollable radiological spill inside containment.

Although the overall safety significance of the technical aspects of this event was considered low, one aspect of this event was of concern. A lack of proper management controls allowed the SSPS surveillance test to be performed while the reactor was in midloop operations, as documented in Section 2.2 of this inspection report. Senior management failed to delineate the expectation that all activities, including surveillance testing, should have been restricted while the reactor coolant system water level was at midloop. This test clearly had the potential to affect the reliable operation of the residual heat removal system and, yet, management controls did not prevent its performance during the midloop evolution.

2.8 Conclusions

The inspectors concluded that management controls did not prevent the performance of critical testing while the reactor coolant system was drained to midloop. Senior management did not restrict the performance of surveillance testing during midloop operations, nor were they aware that SSPS testing was to be performed. Additionally, the shift supervisor and midloop coordinator failed to identify that testing the SSPS could negatively impact the reliable operation of the residual heat removal system.

Two examples of a procedural violation were identified. The first occurred when operators performed the steps of the procedure in Logic Train R as opposed to the required Logic Train S. Additionally, the self verification program failed to identify this error. The second example occurred when the

reactor operators determined that they were in the wrong logic cabinet and terminated the test without informing the shift supervisor, as required by a precaution in the procedure. However, the inspectors noted that the shift supervisor had indications that the reactor operators were not properly controlling the testing evolution and did not fully pursue the answers to their questions.

The operators responded appropriately to the safety injection actuation and restored core cooling in a timely manner. Additionally, the gravity feed path from the refueling water storage tank to the reactor was secured.

Licensee engineers concluded that no problems with the SSPS circuitry, hardware, or logic existed. The cause of the actuation was determined to be a noise spike in the Actuation Train B circuitry. The inspectors determined that the investigation results were reasonable and based on sound troubleshooting techniques.

The inspectors reviewed the midloop operations procedures and determined that the licensee's Generic Letter 88-17 commitments were still being met. However, procedural controls were not well implemented.

The overall safety significance of this specific event was considered low. However, the loss of residual heat removal system pumps and the resultant increase in reactor coolant system inventory with the steam generator manways open was of concern. Additionally, senior management failed to adequately delineate the expectation that all activities, including surveillance testing, should have been restricted while the reactor coolant system water level was at midloop.

ATTACHMENT

1 PERSON CONTACTED

1.1 Licensee Personnel

H. Butterworth, Manager, Plant Operations
M. Coughlin, Staff Licensing Engineer
D. Daniels, Administrator, Corrective Action Group
J. Groth, Vice President, Nuclear Generation
D. Keating, Director, Independent Safety Engineering Group
B. MacKenzie, Corrective Action Group, Staff
L. Martin, General Manager, Nuclear Assurance
B. Masse, General Manager, Generation Support
L. Myers, Plant Manager
J. Sheppard, General Manager, Nuclear Licensing

The personnel listed above attended the exit meeting. In addition to the personnel listed above, the inspectors contacted other personnel during this inspection period.

2 EXIT MEETING

An exit meeting was conducted on April 14, 1994. During this meeting, the inspectors reviewed the scope and findings of the report. The inspectors addressed the significance of management's failure to properly delineate expectations to plant employees and of the shift supervisor's failure to provide adequate oversight of the reactor operators. The licensee acknowledged the information presented at the exit meeting. The Vice President, Nuclear Generation stated that he concurred with the findings and that a management lessons learned document had been prepared to address corrective actions needed for improved senior management oversight. The licensee did not identify as proprietary any information provided to, or reviewed by, the inspectors.