APPENDIX

U.S. NUCLEAR REGULATORY COMMISSION
REGION IV

Inspection Report: 50-285/94-08

License: DPR-40

Licensee: Omaha Public Power District
Fort Calhoun Station FC-2-4 Adm.
P.O. Box 399, Hwy. 75 - North of Fort Calhoun
Fort Calhoun, Nebraska 68023-0399

Facility Name: Fort Calhoun Station

Inspection At: Blair, Nebraska

Inspection Conducted: February 22 through March 8, 1994

Inspector: R. Mullikin, Senior Resident Inspector

Approved: Thomas F. Stetka
Thomas F. Stetka, Chief, Project Branch D

3/29/94
Date

Inspection Summary

Areas Inspected: Special, announced inspection of the consequences of a supervisory relay failure in the engineered safety features system (ESF).

Results:

- The licensee operated since initial construction with an ESF system that was not single failure proof and, thus, outside of the design basis. This was reported in accordance with 10 CFR 50.72. (Section 1.2)
- The licensee promptly installed temporary modifications to ensure the plant was within the design basis. Compensatory measures for disabled alarm and annunciator features were effective. (Section 2)
- During followup of an ESF supervisory relay failure which caused a reactor trip, the licensee identified the potential for premature change to the recirculation mode of emergency core cooling injection during design basis events. Further evaluation of this condition to determine the scope of the problem will be tracked as Unresolved Item 285/9408-01. (Section 3.2.5)

- The possibility of a supervisory relay short circuit was considered during construction by the architect engineer. The probability was considered remote and no corrective action was deemed necessary. However, because of the recent failure at the Fort Calhoun Station, the age of these relays, and the unknown cause of the failure, this conclusion appears to be invalid. (Section 4.1)

- The licensee reported that the core damage frequency did not increase as a result of adding the probability of an early change to the recirculation mode caused by a single failure of a supervisory relay. While the postulated failure was potentially high risk, it was determined to have a low probability of occurring. (Section 5.1)

- The licensee lacks procedures for recovery from an early recirculation actuation signal initiation. (Section 5.2)

- The licensee failed to discover this design basis deficiency during the Design Basis Reconstitution Program, because of the limited scope of the program (Section 6).

Summary of Inspection Findings:

- Unresolved Item 285/9408-01 was opened. (Section 3.2.5)

- Inspection Followup Item 285/9408-02 was opened. (Section 5.2)

Attachments:

- Attachment 1 - Persons Contacted and Exit Meeting

- Attachments 2, 3, and 4 - Recirculation Actuation Signal Relay Diagrams

DETAILS

1 BACKGROUND

1.1 Reactor Trip

On February 11, at 3:40 p.m., the Fort Calhoun Station experienced a reactor trip due to an inadvertent containment high pressure signal (CHPS). The Channel B CHPS lockout relay (86B/CHPS) actuated causing actuation of safety injection, containment isolation, ventilation isolation, and steam generator isolation signals. The closing of the main steam isolation valves caused a turbine trip and a subsequent reactor trip.

The licensee suspected that a failed supervisory relay (86B/CHPSS) had caused Lockout Relay 86B/CHPS to actuate. A CHPS is designed to be received when containment pressure reaches 5 psig. Actual containment pressure at the time of the trip was approximately .6 psig. The licensee was able to reset the Channel "B" safeguards signal after lifting a lead for Relay 86B/CHPSS under an emergency temporary modification (TM 94-011).

All safety equipment operated as designed. With the steam generators isolated, an automatic start of the electric auxiliary feedwater pump (FW-6) and turbine driven auxiliary feedwater pump (FW-10) occurred. Some of the main steam code safety valves lifted. Primary heat removal was maintained through the two main steam safety valves that have pneumatic controllers. The licensee declared a Notification of Unusual Event at 4 a.m. and downgraded from it at 7:46 a.m.

1.2 Licensee Followup to ESF Relay Failure

The licensee's investigation into the event revealed that Supervisory Relay 86B/CHPSS had shorted, thus causing the CHPS. The licensee planned to send the failed relay off site for an independent evaluation. This relay had been installed since initial operation of the plant and was a General Electric Model HGA17C.

The licensee performed a review of ESF circuits to determine whether the same type of relay failure could result in an unanalyzed condition or a condition outside the plant design basis. On February 18 the licensee reported in accordance with 10 CFR 50.72(b)(1)(ii)(A) and -(B) that a such a scenario existed. A failure of either Supervisory Relay 86A/STLSS or 86B/STLSS occurring simultaneously with a loss of coolant accident, a steam generator tube rupture, or a main steam line break could result in the premature initiation of the recirculation actuation signal (RAS). Premature initiation of the RAS could cause the realignment of the containment spray pumps and the high pressure safety injection pumps on both trains to a dry sump, resulting in loss of suction pressure and damage to the pumps. The premature initiation of the RAS would also trip both low pressure safety injection pumps.

During the inspection the licensee's review continued. On May 3 a second condition outside the design basis was reported in accordance with 10 CFR50.72(b)(1)(ii)(B), when additional relays were discovered to affect the single failure criteria. The licensee determined that single supervisory relay failures had the potential to cause premature closing of one or both high pressure safety injection pump minimum recirculation header valves leading to potential dead heading of the high pressure safety injection pumps and possible pump damage. A short circuit failure of either Supervisory Relay 86A/STLSS or 86B/STLSS occurring during an accident would close both valves (HCV-385 and HCV-386). In addition, the licensee determined that a short circuit failure of another six supervisory relays in the RAS logic would cause one of the high pressure safety injection pump recirculation valves (HCV-385 and HCV-386) to close. Since valves HCV-385 and HCV-386 are in series, closure of either valve disables the minimum recirculation path for both high pressure safety injection pumps and could lead to damage of both pumps under some postulated accident conditions

2 CORRECTIVE ACTIONS

2.1 Temporary Modification Installation

The licensee installed Temporary Modification TM 94-014 on February 18, which lifted one of the leads from Supervisory Relays 86A/STLSS and 86B/STLSS and electrically removed these from the logic circuit. This modification eliminated the single failure concern reported on February 18, since a short circuit of the supervisory relay could no longer occur.

In addition, the licensee reviewed the other supervisory relays in the RAS logic circuit. The licensee installed Temporary Modification TM 94-015 on February 19, to lift a similar lead from six other supervisory relays, as a precautionary measure until the engineering analysis was completed.

The inspector reviewed the temporary modification packages and concluded that the lifted leads would perform the intended function and would not result in any other apparent problems. It was also noted that a proper 10 CFR 50.59 applicability screening was performed and that no unreviewed safety question existed with these modifications.

2.2 Compensatory Measures for Disabled Alarm and Annunciation Features

The effect of the temporary modifications was to disable the control room trouble alarm and annunciation features for the RAS. The licensee still had amber lights on the control room panel which, if extinguished, would indicate a problem in the circuit. Control room operators log hourly readings for various control room indications using Form FC-75, "Control Room Log." The licensee included the monitoring and documenting that these lights were illuminated as part of the hourly log taking using Form FC-75. The inspector verified that the control panel amber lights were being routinely monitored by

control room operators. The inspector also noted that the lights are situated in a manner such that they can be easily viewed by control room personnel.

3 FAILURE ANALYSIS

3.1 RAS Logic Design

Attachments 2 - 4 depict the RAS relay logic for Train A. The Train B logic would be identical except for the component designators.

The typical ESF supervisory circuit consists of a high coil resistance relay and indicating light wired in parallel and then connected in series with the lockout relay coil. For example, in the safety injection and refueling water low signal (STLS) scheme, each train (A and B) has a redundant set of four channel level switches (A/LC, B/LC, C/LC, and D/LC). This allows the closing of any two contacts to initiate an STLS. On each redundant set, a 2-out-of-4 logic exists. Should an actual STLS occur, a 2-out-of-4 matrix is actuated which shorts out the supervisory relay and then actuates the lockout relay. A small amount of current is allowed to travel through the supervisory and lockout relays. This current is enough to pick up the supervisory relay, but not enough to actuate the lockout relay. If power is lost to the circuit, or the lockout relay coil fails in the open condition, the supervisory relay drops out and an alarm and annunciator is actuated to alert control room operators that the lockout relay is not operable. In addition, normally the amber light associated with the supervisory relay is dimly lit verifying that the circuit's power is available and the lockout relay coil has not open circuited. Should power be lost or the lockout relay coil open the indicating light will go out.

3.2 Licensee Failure Analysis

3.2.1 Reactor Trip

The February 11, 1994, CHPS supervisory relay failure was a shorted relay coil. The supervisory relay has a normal coil resistance of approximately 2280 ohms. The shorted coil on February 11 resulted in a coil resistance of approximately 109 ohms, which had the effect of increasing the current through the supervisory and the lockout relays. This, in turn caused the lockout relay to actuate.

3.2.2 Single Failure Requirements

The licensee determined from this event that a single failure of the CHPS supervisory relay caused an ESF actuation of both trains. As the result of this determination, an investigation was performed to determine whether any similar failures could put the plant outside of the design basis. The licensee performed Engineering Analysis EA-FC-94-008 to determine whether a lockout relay actuation caused by the failure of the associated supervisory relay circuitry could place the plant in a condition which is outside of it's design basis as described in the Updated Safety Analysis Report (USAR),

Section 7.3.5, and Appendix G, Criterion 41. The USAR design criteria states that no single failure of an ESF system component, by itself, will result in the failure to achieve a minimum level of engineered safeguard performance acceptable for a design basis accident as discussed in Sections 6 and 14.

3.2.3 Single Failure Review

The licensee evaluated the effect of the failure of a supervisory relay during normal plant operations with no other concurrent failures and during the following design basis accidents: loss-of-coolant accident (LOCA), steam generator tube rupture (SGTR), main steam line break (MSLB), and a fuel handling accident. These events were chosen because they represent the entire spectrum of ESF response to any USAR Section 14, "Safety Analysis," scenario. There were 56 safety-related General Electric Model HGA supervisory relays in operation at the Fort Calhoun Station. The licensee's evaluation considered the effects of any of these relays shorting and causing the inadvertent actuation of its associated lockout relay.

The licensee determined that any transient caused by a single failure of a lockout relay would be bounded by the USAR accident analysis. It was concluded that this would not cause an event outside of the design basis.

3.2.4 Supervisory Relay Failures

Inadvertent lockout relay actuations during design basis events were identified which resulted in failure to achieve a minimum level of engineered safeguard performance acceptable for the design basis accident. A failure of Supervisory Relay 86A/STLSS caused by a short circuit of a relay coil could result in an actuation of Lockout Relay 86A/STLS. If this occurred during a design basis accident with either a low pressurizer pressure signal present or a CHPS present, the lockout relay actuation would result in the initiation of a RAS with the following results:

- Safety Injection and Refueling Water Tank Discharge Valves LCV 383-1 and LCV 383-2 would close.
- Containment Sump Suction Valves LCV 383-3 and LCV 383-4 would open.
- Both low pressure safety injection pumps would trip.
- Both high pressure safety injection pumps' minimum recirculation header isolation valves (HCV-385 and HCV-386) would close.

Train A RAS actuation causes an automatic swap to the recirculation mode for both trains of safety injection and containment spray. If the failure was timed so that the RAS actuation was premature, there would be insufficient net positive suction head for the running pumps. The high pressure safety injection pumps for both trains would be vulnerable to damage. The

It was also concluded that under certain MSLB, SGTR, or small break LOCA conditions high pressure safety injection pump damage could occur due to dead heading. This condition could be caused by either failure of Supervisory Relay 86A/STLSS or three other supervisory relays in the Train A RAS logic: Supervisory Relays 86A/RASS, 86A1/RASS, or 86A1/STLSS.

The above described logic sequence would be identical for the Train B logic. A similar failure of Supervisory Relay 86B/STLSS would result in the actuation of Lockout Relays 86B/STLS, etc. Train B RAS actuation also causes the automatic swap to the recirculation mode for both trains of high pressure injection and containment spray.

3.2.5 Other Potential Single Failures

The licensee determined that the inadvertent actuation of a lockout relay by itself, without the coil being energized, was not a credible event. The licensee based this judgement on the fact that a lockout relay requires a spring loaded latch to be moved by the energized relay coil allowing a second spring to rotate the cam shaft, opening or closing contacts as required. The lockout relay can only be reset by manual operation. The licensee's analysis determined from historical data that the failure mode for these relays has been the failure to actuate, not inadvertent actuation.

In addition, the licensee considered the possibility that a short circuit could occur in the supervisory amber light. The supervisory light assemblies utilize a low voltage lamp and a fixed resistor. The licensee considered a failure of the light circuit that could actuate the lockout relay to not be credible because the fixed resistor would prevent lockout relay actuation.

Should a premature actuation of Lockout Relay 86A/STLS (86B/STLS) for any reason occur, or a short circuit occur across the amber light in parallel with Supervisory Relay 86A/STLSS (86B/STLSS) during accident conditions, the plant could be in a condition which is outside of the plant's design basis as described in the USAR, Section 7.3.5, and Appendix G, Criterion 41. Additional NRC review is planned to determine whether this single failure vulnerability constitutes a violation of NRC requirements. Additional NRC review is also planned to determine if other credible single failure mechanisms exist. This review will be tracked as Unresolved Item 285/9408-01.

4 HISTORICAL DATA

4.1 Early Design Considerations

The inspector reviewed a copy of an internal quality assurance document, dated March 18, 1971, from the architect engineer (Gibbs & Hill, Inc.) that stated a supervisory relay short circuit could cause an unnecessary safeguards actuation. It did provide a solution which was the adding of a 500 ohm, 40 watt resistor in series with the supervisory relay coil. The internal response to this document was dated April 4, 1971, and concluded that the probability of a coil short circuit was so remote that the addition of the

40 watt resistor in series with the supervisory relay coil. The internal response to this document was dated April 4, 1971, and concluded that the probability of a coil short circuit was so remote that the addition of the resistor was not justified. The licensee could not locate any further information on this matter from the architect engineer.

4.2 Model HGA17C Failure History

The licensee researched the failure history within the industry for the Model HGA17C relay and all HGA relays and found that a total of 52 HGA relay failures have occurred in safety-related applications. Of these failures, only one failure had occurred with Model HGA17 relays. The inspector reviewed the narratives of all 52 failures and found that only 1 had a failure attributed to a shorted coil. This failure was in a Model HGA14 relay in 1991.

4.3 Model HEA61C Failure History

The inspector reviewed the licensee provided industry data on failures of the General Electric Model HEA61C relay, which is the type used for the lockout relays. There were a total of 145 documented failures of these types of relays. A computer search resulted in no reported failures attributed to an inadvertent actuation due to mechanical failure. The inspector also inspected a Model HEA61C relay and concluded that a mechanical failure would be unlikely. This supports the licensee's conclusion that this failure would not be credible.

4.4 Prior Generic Communications

In addition, the Office for Analysis and Evaluation of Operational Data performed a review of generic communications on relay failures that were provided to the industry. It was discovered that there was no applicable information available on failures of Model HGA17 relays.

4.5 Design Basis Reconstitution

The inspector questioned the licensee on whether the relay single failure vulnerability should have been discovered during the licensee's Design Basis Reconstitution Program. The inspector interviewed licensee personnel and was told that the program scope was to develop Design Basis Documents (DBDs) for various systems and compile all existing data into one document. The licensee stated that the program made the assumption that single failure criteria was satisfied. It was stated that, when data was missing, the licensee had to recreate this data and that single failure vulnerabilities were considered at that time. In addition, the inspector was informed that, while the architect engineer's March 18, 1971, letter was included in the DBD data base, it was not reviewed during the DBD review process.

5 SAFETY SIGNIFICANCE

5.1 Probabilistic Risk Assessment

The licensee concluded that the overall core damage frequency (1.36E-5/year) did not change as a result of adding the short circuit failure of the STLSS supervisory relays to the probabilistic risk assessment model.

While this event was determined to be a very low probability event, it was a high risk event. A complete loss of high pressure safety injection and containment spray as well as inappropriate termination of low pressure safety injection could occur due to a single failure of one of the STLSS supervisory relays during the early portion of a LOCA, SGTR, or MSLB.

5.2 Recovery from an Early RAS

The initiation of an early RAS was not a planned event and, as a result, the licensee did not have procedures that would provide operators specific guidance on how to recover from such an event. Thus, operator actions may differ from crew to crew and an increased margin of error would be introduced.

Switch CS-A1 (Switch CS-B1) can be used by the operators to restrict the RAS initiation logic so that Train A (Train B) logic will only control Train A (Train B) engineered safeguard features. This would allow for reset of equipment associated with the nonfailed logic train.

The licensee is presently reviewing Abnormal Operation Procedure AOP-23, Reset of Engineered Safeguards, to determine what revisions are needed to provide instructions to operations personnel for recovering from an early RAS signal. The licensee's efforts in this regard will be tracked as Inspection Followup Item 285/9408-02.

6 CONCLUSIONS

The licensee promptly investigated the potential for similar failures of other Model HGA17C relays, after the self-disclosing single failure concern was identified, and as a result identified a potentially significant long-standing design error.

The licensee operated since initial construction with an ESF system that was not single failure proof and, thus, outside of the design basis. This was reported in accordance with 10 CFR 50.72. The scope of this problem is being evaluated as Unresolved Item 285/9408-01.

The actions taken by the licensee to put the plant back within the design basis were prompt and proper. The temporary modification that was installed resolved the technical issue. The measures implemented by the operators to compensate for disabled annunciators were appropriate. The licensee is reviewing Procedure AOP-23 to determine what revisions are needed to assure that adequate instructions are available to mitigate an early RAS initiation.

This issue is being tracked as an inspection followup item. Long-term corrective actions are yet to be proposed.

The architect engineer had identified during plant construction that a supervisory relay short circuit could cause an unnecessary safeguards actuation. The architect engineer concluded that the probability of a relay coil failing in a shorted condition was remote and no corrective action was needed. Because of the recent failure, the age of these relays, and the unknown cause of the failure, this conclusion does not appear valid.

The licensee failed to discover this design basis deficiency during the Design Basis Reconstitution Program, since it was outside of the scope of the program.

ATTACHMENT 1

1 PERSONS CONTACTED

1.1 Licensee Personnel

J. Chase, Manager, Fort Calhoun Station
G. Cook, Supervisor, Station Licensing
R. Jaworski, Manager, Station Engineering
L. Kusek, Manager, Nuclear Safety Review Group
W. Orr, Manager, Quality Assurance and Quality Control
T. Patterson, Division Manager, Nuclear Operations
R. Phelps, Acting Division Manager, Production Engineering
R. Short, Manager, Nuclear Licensing and Industry Affairs
J. Skiles, Acting Manager, Design Engineering
D. Trausch, Acting Manager, Training

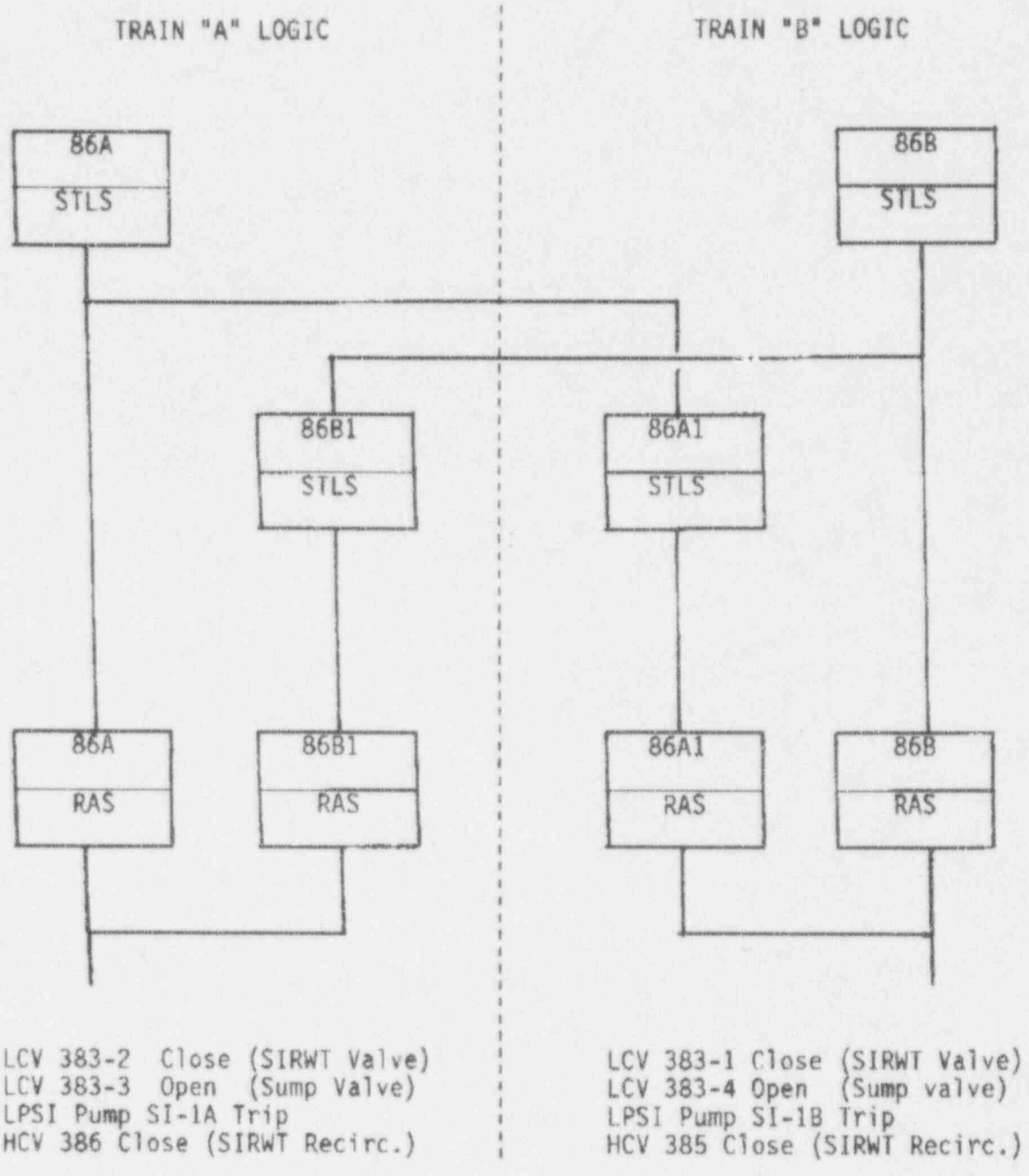
The above personnel attended the exit meeting. In addition to the personnel listed above, the inspector contacted other personnel during this inspection period.

2 EXIT MEETING

An exit meeting was conducted on March 8, 1994. During this meeting, the inspector reviewed the scope and findings of the report. The licensee agreed with the inspection findings presented at the meeting. The licensee did not identify as proprietary any information provided to, or reviewed by, the inspector.

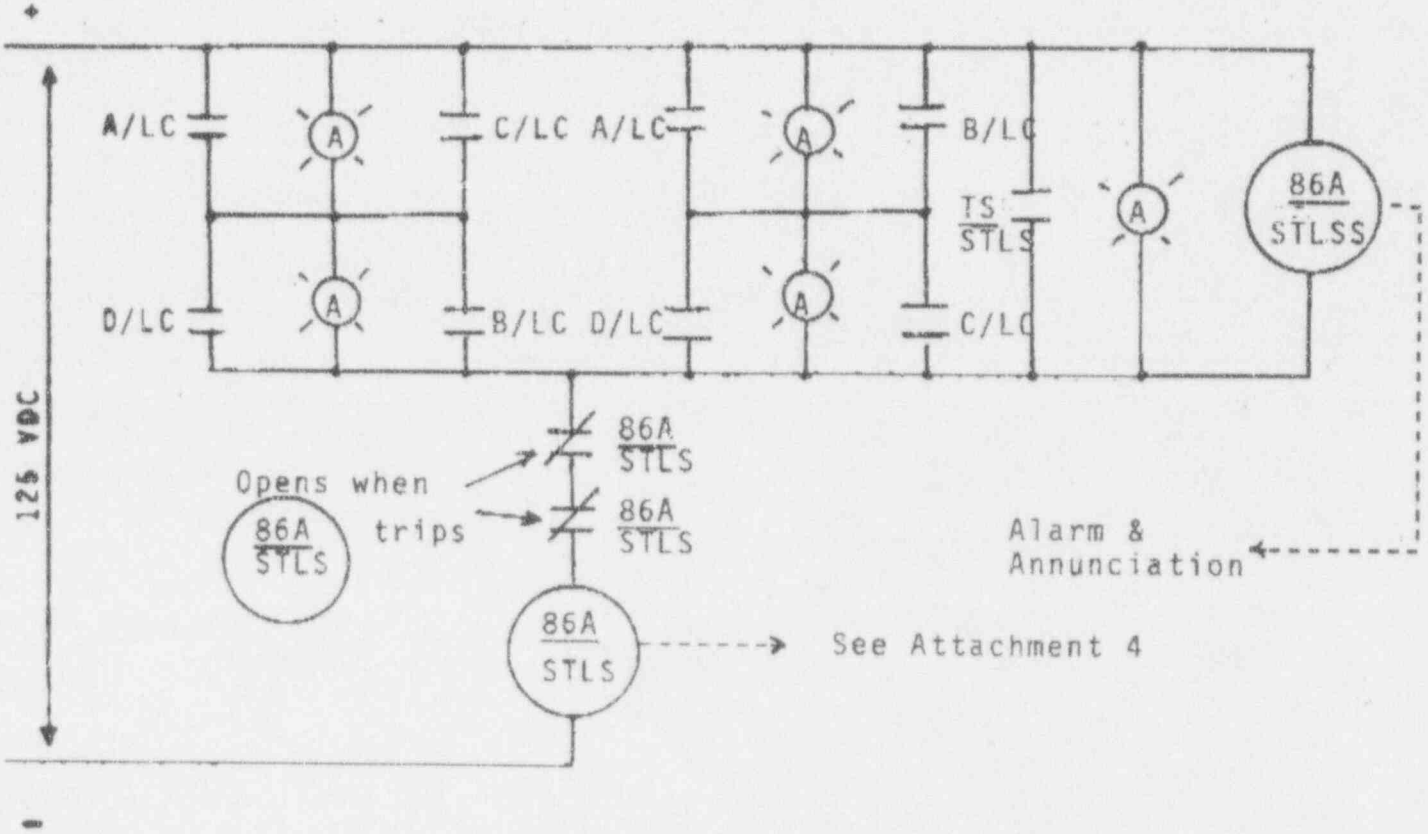
ATTACHMENT 2

STLS/RAS LOGIC



ATTACHMENT 3

STLS TRAIN "A" LOGIC



LS - Safety Injection & Refueling Water Tank Low Signal
S - Recirculation Actuation Signal
PS - Pressurizer Pressure Low Signal
HS - Containment Pressure High Signal

- Normally Open Contact
- Normally Close Contact
- Amber Light (Control Room Panel)
LC - Channel A Level Switch
- Test Switch

86A/STLS - STLS Initiating/Lockout Relay

86A/STLSS - STLS Supervisory Relay

86A/RAS or 86A1/RAS - RAS Initiating/Lockout Relay

86A/RASS or 86A1/RASS - RAS Supervisory Relay

86AX/RAS or 86A1X/RAS - RAS Auxiliary Initiating/Lockout R

ATTACHMENT 4

RAS LOGIC