Westinghouse Energy Systems

Westinghouse Energy Systems

WCAP-11736-A WESTINGHOUSE PROPRIETARY CLASS 3
Volume I

RESIDUAL HEAT REMOVAL SYSTEM AUTOCLOSURE INTERLOCK REMOVAL REPORT FOR THE WESTINGHOUSE OWNERS GROUP

Revision 0.0

October 1989

N. B. Closky
K. J. King
P. M. McHale
C. A. Marmo

Prepared by Westinghouse Electric Corporation for use by members of the Westinghouse Owners Group. Work performed under Shop Order MUHP-2054, under the direction of the Technical Specification Subcommittee.

Westinghouse Electric Corporation
Power Systems
P.O. Box 355
Pittsburgh, Pennsylvania 15230

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

August 8, 1989

Mr. Roger A. Newton, Chairman
Westinghouse Owners Group
2310 W. Michigan Avenue
Milwaukee, Wisconsin 53201

Dear Mr. Newton:

SUBJECT: ACCEPTANCE FOR REFERENCING WCAP-11736 REV. 0.0, "RESIDUAL HEAT REMOVAL SYSTEM AUTOCLOSURE INTERLOCK (ACI) REMOVAL REPORT" IN PLANT SPECIFIC SUBMITTALS

We have completed our review of the subject topical report submitted with your letter of April 22, 1988. We have concluded that the information in this report can be used to supplement plant specific requests to remove the ACI from the Westinghouse plants covered by this report. However, the attached SER does not grant permission to remove the ACI for any plant; such permission must be requested on a plant-specific basis.

We do not intend to repeat our review of the matters described in the reports and found acceptable when the reports appear as references in license applications except to assure that the material presented is applicable to the specified plant involved. Our acceptance applies only to the matters described in the reports.

In accordance with procedures established in NUREG-0390, it is requested that Westinghouse publish accepted proprietary and non-proprietary versions of this topical report within 3 months of receipt of this letter. The accepted versions should incorporate this letter and the enclosed evaluation between the title page and the abstract. The accepted versions shall include an -A (designated accepted) following the report identification symbol.

Should our criteria or regulations change, such that our conclusions as to the acceptability of the reports are invalidated, Westinghouse and/or the licensees referencing the topical reports will be expected to revise and resubmit their respective documentation, or submit justification for the continued effective applicability of the topical reports without revision of their respective documentation.

Sincerely,

Ashok Thadani, ~~Assistant Director~~ Director
for Systems
Division of Engineering & Systems Technology
Office of Nuclear Reactor Regulation

Enclosure:
Safety Evaluation
WCAP-11736

cc w/enclosure:
J.A. Triggiani, Westinghouse

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

ENCLOSURE 1

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION
RELATING TO REMOVAL OF AUTO CLOSURE INTERLOCK FUNCTION
WESTINGHOUSE OWNERS GROUP
WCAP-11736, VOLUME I AND II

1.0 INTRODUCTION

By letters dated April 22, 1988 and January 3, 1989 (References 1, 2) the Westinghouse Owners Group (WOG) requested that the staff review WCAP-11736 Volume I and II, "Residual Heat Removal System Auto Closure Interlock Removal Report." The staff review of this issue has focused on assuring that this generic report is consistent with the staff position on the removal of the autoclosure interlock, as set forth in the staff's safety evaluation for Diablo Canyon (Reference 3).

2.0 EVALUATION

2.1 WCAP-11736 Summary

WCAP-11736 was written with the support and funding of WOG. It provides an evaluation of the removal of the autoclosure interlock (ACI) from suction/isolation valves in the residual heat removal system (RHRS) at four reference plants: Salem Unit 1, Callaway Unit 1, North Anna Unit 1, and Shearon Harris Unit 1. The WOG plants participating in the program were categorized into one of four groups based on RHRS configuration and design characteristics that were similar to one of the four reference plants. The plants listed by group are:

Group 1 - Salem Unit 1

Salem Unit 2
D.C. Cook Units 1 & 2
Indian Point Unit 3
McGuire Units 1 & 2
Sequoyah Units 1 & 2
Watts Bar Units 1 & 2
Zion Units 1 & 2

Group 2 - Callaway Unit 1

Braidwood Units 1 & 2
Byron Units 1 & 2
Catawba Units 1 & 2
Comanche Peak Units 1 & 2
Trojan Unit 1
Seabrook Unit 1
Vogtle Units 1 & 2
Wolf Creek Unit 1
Millstone Unit 3
South Texas Units 1 & 2

Group 3 - North Anna Unit 1

H.B. Robinson Unit 2
Turkey Point Units 3 & 4
Beaver Valley Unit 1
Prairie Island Units 1 & 2
North Anna Unit 2

Group 4 - Shearon Harris Unit 1

Farley Units 1 & 2
Beaver Valley Unit 2
V.C. Summer Unit 1

The choice of the four particular reference plants was intended to provide the maximum number of the other WOG members with the best possible fit should they choose to delete the ACI in the future and reference WCAP-11736. It is expected that, should a plant desire to delete the ACI, a plant-specific analysis would still be required, but that substantially less resources would need to be expended to produce and review this analysis if reference were made to WCAP-11736.

The staff agrees with this approach and gives some guidance by summarizing the WOG position for what is expected in the plant-specific response.

2.2 Hardware Changes

WCAP-11736 proposes to remove the ACI function from the RHR suction valves. The open permissive interlock will remain intact. An alarm will be added to each valve which will actuate if the valve is open. The setpoint for the alarm is a plant-specific concern. A general rule for establishing the alarm setpoint, is that the setpoint pressure be greater than the open permissive setpoint and less than the RHR system design pressure minus the RHR pump head pressure. In addition, the status lights on the operator's panel, which indicate that these valves are open or closed, will remain functional after power has been removed from these valves.

2.3 Procedural Changes

WCAP-11736 proposes the following for generic procedural requirements:

Each plant will be expected to review its operating procedures to determine the continued applicability of the procedures and to make any changes necessary, to ensure continued safe operation without the ACI. Plant operating procedures should be reviewed to determine the effect of removing the ACI and installing a control room alarm. Listed below are a few of the general procedures that may require modification.

- RHRS operating procedure
- Plant startup from cold shutdown operating procedure(s)
- Plant shutdown from hot standby operating procedure(s)
- Alarm surveillance procedures (to include the new alarm)
- Leak rate testing procedures (caution regarding alarms and power removal from RHR suction valves)

In addition, the alarm response procedure used during plant startup should be modified to reflect the appropriate (new) alarm recognition and responses for the added alarm. The procedure should be revised to direct the operator to take the necessary actions to close the open RHR suction valve(s), if they are not closed following alarm actuation during normal startup operations. If this is not possible, the operator should be instructed to not pressurize further and return to the safe-shutdown mode of operation.

The staff agrees with this generic guidance assuming a surveillance procedure for the RHR suction valve alarms is added to ensure these alarms remain operable, but in addition, the staff believes that further protection can be achieved by removing power from the RHR suction valves before they are leak-checked in order to ensure that they remain in the tested configuration. If this is not feasible for a particular plant, the reasons for not performing this procedure should be justified in the plant-specific submittal.

2.4 Reasons for Removing Autoclosure Interlock

The main reasons for removing ACI have been previously elucidated by the staff in the AEOD report, "Decay Heat Removal Problems at U.S. Pressurized Water Reactors" (Reference 4). This report points out that of the 130 loss-of-RHR events that were documented at U.S. pressurized water reactors (PWRs) between 1976 and 1983, 37 were caused by the automatic closure of the suction/isolation valves. The AEOD report also quotes a Sandia Laboratory study (Reference 5) that evaluated the competing risks associated with RHR suction/isolation valve closure and Event V. Sandia concluded that:

> "The lowest core melt frequency due to the combination of loss of RHR suction during cold shutdown and V-LOCAs is obtained when there are no autoclosure interlocks on the RHR suction valves...removing the overpressure interlocks from the RHR suction valves gives the best RHR suction arrangement for PWRs based upon this analysis.

> ...when interlocks are present, loss of RHR suction is the largest contributor to core melt frequency for all assumed values of P(CM-LRHRs). However, when the interlocks are not present, the core melt frequency due to loss of RHR suction is comparable to or less than the V-LOCA core melt frequency for the "best estimate" cases."

The AEOD report concluded that even though it was most likely a good idea to remove ACI, the effects of ACI removal upon plant safety must be evaluated on a plant-by-plant basis because of numerous plant-specific differences. The WOG submittal (Reference 1) contains such a plant-specific analyses for four different groups of plants.

An additional benefit associated with removal of ACI is that the isolation valves will remain open during low-temperature overpressurization (LTOP) events which allows the RHR relief valves to relieve pressure and aid in the LTOP protection of the RCS.

2.5 Safety Function of the Autoclosure Interlock

The WOG has shown in Reference 1 that the RHR relief valves have adequate capacity to mitigate pressure transients that occur during RHR operation. Therefore, the purpose of ACI is to ensure that there is a double barrier between the RCS and the RHRS when the plant is at normal operating conditions (hot and pressurized) and not in the RHRS cooling mode. The ACI function is to preclude conditions that could lead to a LOCA outside of containment, Event V, due to operator error. The sequence that concerns the staff in particular is that case in which the operator closes one of the isolation valves and not the other, since if both valves were left open, the operator would not be able to pressurize the plant.

2.6 Probabilistic Risk Assessment of the Event V Sequence and Safety Analyses of Transients

WCAP-11736 provides a plant-specific probabilistic risk assessment (PRA) for the four lead plants (Salem, Callaway, North Anna, Shearon Harris); these analyses follow the PRA format previously reviewed by the staff for Diablo Canyon (Reference 3). The results of these analyses agree with the Diablo Canyon finding that the proposed configuration with the ACI removal and an alarm added will result in a lower probability for the Event V sequence than the present plant configuration. The staff has no requirements based on the absolute values in the PRA analyses and will not require a plant-specific PRA from each licensee proposing to remove the ACI. However, the licensee should do sufficient PRA and safety analyses to ensure that its plant will not show results that will invalidate the conclusions of WCAP-11736.

3.0 STAFF POSITION

The staff finds that the removal of the ACI for Westinghouse plants covered by WCAP-11736 can produce a net safety benefit provided that the following five key improvements are in place. Furthermore, the staff finds that WCAP-11736 may be referenced in the licensee's plant-specific submittals to show compliance with those items that are not plant specific. However, this SER does not grant permission to remove the ACI for any plant.

Plant Improvements

(1) An alarm will be added to each RHR suction valve which will actuate if the valve is open and the pressure is greater than the open permissive setpoint and less than the RHR system design pressure minus the RHR pump head pressure [justified by WCAP-11736].

(2) Valve position indication to the alarm must be provided from the stem-mounted limit switches (SMLSs) and power to the SMLSs must not be affected by power lockout of the valve [justified by WCAP-11736].

(3) The procedural improvements described in WCAP-11736 should be implemented. Procedures themselves are plant specific.

(4) Where feasible, power should be removed from the RHR suction valves prior to their being leak-checked [plant specific].

(5) The RHR suction valve operators should be sized so that the valves cannot be opened against full system pressure [plant specific].

4.0 REFERENCES

(1) N. L. Burns (et al.), "Residual Heat Removal System Autoclosure Interlock Removal Report for the Westinghouse Owners Group," February 1988, WCAP-11736, Revision 0.0.

(2) Letter, Roger A. Newton (WOG) to M. W. Hodges (NRC), January 3, 1989.

(3) Letter, Harry Rood (NRC) to J. D. Shiffer (PGE), "Safety Evaluation of Removal of RHR Autoclosure Interlock Function and Installation of an Alarm at Diablo Canyon Units 1 & 2," February 17, 1988.

(4) H. O. Ornstein, "Decay Heat Removal Problems at U.S. Pressurized Water Reactors," December 1985, AEOD/C503.

(5) D. R. Gallup, D. M. Kunsman, M. P. Bohr; Sandia National Laboratories, "Potential Benefits Obtained by Requiring Safety-Grade Cold Shutdown Systems," NUREG/CR-4335, July 1985.

WOG

Westinghouse Owners Group

OG-89-01

January 3 1989

U.S. Nuclear Regulatory Commission
Washington, DC 20555

Attention: Document Control Desk

Attention: Mr. Marvin W. Hodges, Reactor Systems Branch Chief
Division of Engineering & System Technology

Subject: Westinghouse Owners Group
<u>Transmittal of Responses to NRC Questions on Topical Report WCAP-11736 Volume I & II Residual Heat Removal System Autoclosure Interlock Removal Report</u>

References: 1) Letter OG-88-17, 4/22/88.
2) Telecon with G. Schwenk, 12/1/88.
3) Telecon with G. Schwenk, 12/16/88.

Dear Mr. Hodges:

Reference 1 transmitted the following report:

1. WCAP-11736 Volume I Residual Heat Removal System Autcclosure Interlock Removal Report Revision 0.0 February 1988

2. WCAP-11736 Volume II Residual Heat Removal System Autoclosure Interlock Removal Report Revision 0.0 February 1988.

This topical report was transmitted to you for your information at the request of the Westinghouse Owners Group Technical Specification Subcommittee to provide the results of a Westinghouse Owners Group sponsored program to justify the deletion of the Residual Heat Removal (RHR) Suction/Isolation Valve Autoclosure Interlock (ACI). We anticipate that utilities will reference this report as part of plant specific license amendment applications for deletion of the RHR Suction Valve ACI.

WOG

Westinghouse Owners Group

OG-89-01

January 3 1989

U.S. Nuclear Regulatory Commission
Washington, DC 20555

Attention: Document Control Desk

Attention: Mr. Marvin W. Hodges, Reactor Systems Branch Chief
Division of Engineering & System Technology

Subject: Westinghouse Owners Group
Transmittal of Responses to NRC Questions on Topical Report WCAP-11736 Volume I & II Residual Heat Removal System Autoclosure Interlock Removal Report

References: 1) Letter OG-88-17, 4/22/88.
2) Telecon with G. Schwenk, 12/1/88.
3) Telecon with G. Schwenk, 12/16/88.

Dear Mr. Hodges:

Reference 1 transmitted the following report:

1. WCAP-11736 Volume I Residual Heat Removal System Autoclosure Interlock Removal Report Revision 0.0 February 1988

2. WCAP-11736 Volume II Residual Heat Removal System Autoclosure Interlock Removal Report Revision 0.0 February 1988.

This topical report was transmitted to you for your information at the request of the Westinghouse Owners Group Technical Specification Subcommittee to provide the results of a Westinghouse Owners Group sponsored program to justify the deletion of the Residual Heat Removal (RHR) Suction/Isolation Valve Autoclosure Interlock (ACI). We anticipate that utilities will reference this report as part of plant specific license amendment applications for deletion of the RHR Suction Valve ACI.

This letter documents conversations between the Westinghouse Owners Group Technical Specification Subcommittee and NRC staff reviewer, Mr. George Schwenk. Several telephone conferences (References 2 and 3) were held to discuss NRC concerns and questions regarding the report. The attachment to this letter contains the WOG responses to the NRC questions identified by Mr. Schwenk and indicates several changes that will be made to the topical report. These changes will be submitted to the NRC following issuance of the SER.

Should you have any questions or require additional information, please contact either Mr. Gregg Sinders, Carolina Power and Light Company, Chairman WOG Technical Specification Subcommittee, at 919-362-3260 or
Mr. Mike Shannon, Westinghouse Electric Corporation, at 412-374-5590.

Very truly yours

Roger A. Newton

Roger A. Newton, Chairman
Westinghouse Owners Group

RAN/dac

attachment

0544G

ATTACHMENT

NRC Question 1. The WOG Report recommends that the reference plants, which have the RHRS located outside of containment, install an alarm to alert the operator of an improperly positioned RHRS isolation valve. Page 9-4 of the Report indicates that the alarm setpoint corresponds to the current ACI setpoint (Salem = 700 psig, Callaway = 682 psig, Shearon Harris = 700 psig and North Anna = 582 psig). Is it possible to revise the alarm setpoint to a pressure that is significantly lower than the current ACI setpoint?

WOG Response. The Westinghouse Owners Group has determined that establishing a setpoint for the alarm to alert the operator of an improperly positioned (i.e. open) RHR suction valve during startup operations, is a plant-specific concern. It is dependent on the open permissive pressure setpoint, the RHR system design pressure, and the operating pressure at which a plant isolates the RHRS during startup operations. The alarm setpoint can be set to a pressure significantly lower than the current ACI setpoint. A general rule for establishing the alarm setpoint, is that the setpoint pressure be within the range of the open permissive setpoint pressure and, the RHR system design pressure minus the RHR pump head pressure.

P (open permissive setpoint) < P (alarm setpoint) < [P (RHR system design pressure) - P (RHR pump discharge head)]

Following issuance of the SER, the A version of the Report will reflect the revised alarm setpoint.

NRC Question 2. Does removal of the RHR ACI have any impact on the Low Temperature Overpressurization (LTOP) issue?

WOG Response. The RHR ACI was designed to ensure that all RHR suction isolation valves are closed during normal full-power operation. The RHR suction valve closure time of approximately two minutes, and the ACI setpoint which is above the RHR design pressure, prevent the ACI from being an effective system for low temperature overpressure mitigation. Low temperature overpressure mitigation capability is provided by the pressurizer PORVs and/or the RHR suction relief valves. Removing the ACI helps ensure that the RHR suction relief valves are available to mitigate potential overpressure transients. In addition, removing the ACI reduces the potential for the inadvertent isolation of the RHRS. Inadvertent isolation of the RHRS can cause a LTOP transient (reduced letdown combined with a loss of decay heat removal) while also isolating an overpressure mitigation path (the RHR RVs). Removing the RHR ACI thus, has a positive impact on low temperature overpressure mitigation.

The Westinghouse Owners Group confirms that the LTOP issue is not adversely affected by the RHR ACI removal.

NRC Question 3. The plants that implement the RHR ACI Removal will require procedural changes to insure that the RHR valves are closed during start-up. However, it is not evident whether these procedure requirements should be generic or plant-specific.

WOG Response. Each plant will be expected to review their operating procedures to determine the continued applicability of the procedures and to make any changes necessary, to ensure continued safe operation without the ACI. A review of plant operating procedures should be conducted to determine the effect of removing the autoclosure interlock and installing a control room alarm. Listed below are a few of the general procedures that may require modification.

- RHRS operating procedure.
- Plant startup from cold shutdown operating procedure(s).
- Plant shutdown from hot standby operating procedure(s).
- Alarm surveillance procedures (to include the new alarm).
- Leak rate testing procedures (caution regarding alarms and power removal from RHR suction valves).

In addition, the alarm response procedure used during startup of the plant should be modified to reflect the appropriate (new) alarm recognition and responses for the added alarm. The procedure should be revised to direct the operator to take the necessary actions to close the open RHR suction valve(s), if they are not closed following alarm actuation during normal startup operations. If this is not possible, the operator should be instructed to not pressurize further and return to the safe shutdown mode of operation.

The A version of the Report will reflect the above statements concerning procedure reviews and modifications that are required to ensure that the RHR valves are closed during start-up.

NRC Question 4. The NRC has concluded that alarms will be required on all plants regardless of whether the RHRS is located inside or outside of containment. Approval will not be granted unless this requirement is met. Thus, the WOG Report should be consistent with this requirement.

WOG Response. The Westinghouse Owners Group believes that an alarm is not required for plants whose RHRS is inside containment. The risk of an interfacing system LOCA and thus, a direct containment bypass with severe risk consequences, is precluded since the RHRS is located entirely inside containment. Thus, the alarm serves only as additional protection against potential RHRS overpressurization and a subsequent LOCA inside containment. The consequences from an interfacing system LOCA are greater than the consequences from a LOCA inside containment. Therefore, the addition of an alarm for plants with a RHRS located inside containment, does not significantly impact overall plant safety.

The Westinghouse Owners Group has decided that this discussion is best continued at the plant specific level. The report will be revised to reflect the alarm for all plants.

ABSTRACT

A review and analysis has been performed which justifies the deletion of the autoclosure interlock associated with the Residual Heat Removal System suction/isolation valves for four reference plants. The open permissive circuitry is unaffected, but an alarm is added to notify the operator of an incorrectly positioned RHRS suction/isolation valve. A probabilistic analysis was used to demonstrate that the deletion of the autoclosure interlock is acceptable from both a core safety and RHR System overpressurization standpoint.

TABLE OF CONTENTS

Volume I

TABLE OF CONTENTS (CONTINUED)

Volume I

TABLE OF CONTENTS (CONTINUED)

Volume I

TABLE OF CONTENTS (CONTINUED)

Volume II

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES (CONTINUED)

LIST OF FIGURES (CONTINUED)

LIST OF FIGURES (CONTINUED)

EXECUTIVE SUMMARY

This report was written with the support and funding of the Westinghouse Owner's Group (WOG). It provides an evaluation of the removal of the autoclosure interlock (ACI) on the Residual Heat Removal System (RHRS) suction/isolation valves at four reference plants: Salem Unit 1, Callaway Unit 1, North Anna Unit 1 and Shearon Harris Unit 1. The WOG plants participating in the program were categorized into one of four groups based on similar RHR System configurations and design characteristics. The plants listed by Group are:

<u>Group 1 - Salem Unit 1</u>
Salem Unit 2
D.C. Cook Units 1 & 2
Indian Point Unit 3
McGuire Units 1 & 2
Sequoyah Units 1 & 2
Watts Bar Units 1 & 2
Zion Units 1 & 2

<u>Group 2 - Callaway Unit 1</u>
Braidwood Units 1 & 2
Byron Units 1 & 2
Catawba Units 1 & 2
Comanche Peak Units 1 & 2
Trojan Unit 1
Seabrook Unit 1
Vogtle Units 1 & 2
Wolf Creek Unit 1
Millstone Unit 3
South Texas Units 1 & 2

<u>Group 3 - North Anna Unit 1</u>
H.B. Robinson Unit 2
Turkey Point Units 3 & 4
Beaver Valley Unit 1
Prairie Island Units 1 & 2
North Anna Unit 2

<u>Group 4 - Shearon Harris Unit 1</u>
Farley Units 1 & 2
Beaver Valley Unit 2
V.C. Summer Unit 1

The choice of the four particular reference plants was made based on providing the maximum number of the other WOG members with the best possible fit should they choose to delete the ACI in the future and reference this document. It is expected that, should a plant desire to delete the ACI, a plant specific analysis would still be required but the resources expended to produce and review it should be substantially less with reference to this document than without it.

A literature review of decay heat removal problems indicates that approximately 28 percent of the recent loss of RHRS events were caused by inadvertent automatic closure of the RHRS suction/isolation valves. In an effort to reduce the frequency of these inadvertent automatic suction/isolation valve closures, several plants have taken one or more of the following steps: 1) power lockout of these valves during plant shutdown, 2) maintenance procedures which require de-energizing these valves in the open position before conducting setpoint calibration or work on the inverters and 3) modifications to technical specification surveillance requirements involving verification of open suction/isolation valves when credit is taken for RHRS relief valves for cold overpressure protection mitigation. The literature recognizes that corrective actions are necessary to minimize the risk associated with loss of decay heat removal capability caused by actuation of the ACI, but also highlights concerns associated with intersystem Loss-Of-Coolant Accidents (LOCA) and RHRS relief capacity.

During the 1960s and 1970s two closed valves in series isolated the RHRS from the RCS while the RCS was at normal operating temperature and pressure. Both valves were to have power disconnected via administrative procedures except when the valves were to be stroked. An Open Permissive Interlock (OPI) was provided to one of the valves to prevent opening until the RCS pressure was below RHRS design pressure. In 1971 the AEC requirements had evolved to require an Auto Closure Interlock on increasing pressure. A meeting between the industry and the NRC in 1974 brought about three acceptable methods of preventing RHRS overpressurization while the RHRS is in operation or when returning the RCS to operation: 1) automatic closure interlocks on the RHRS suction/isolation valves, 2) sufficient capacity of the RHRS suction line relief valves to mitigate a pressure transient, or 3) a combination of the two.

This agreement was short lived and in 1975 the NRC required in its SER for RESAR-41 that RHRS suction isolation valves be equipped with the ACI feature. The current NRC position is stated in Branch Technical Position RSB 5-1 of July 1981 which requires that the RHRS suction/isolation valves shall be interlocked to protect against one or both valves being open during an RCS increase above the design pressure and that adequate relief capacity shall be provided during the time period while the valves are closing. There has been more recent discussion within the NRC on this issue. In 1984 an internal NRC ICSB memo recommended that action should be taken to modify the design of the RHRS interlocks. A 1985 NRC internal memo stated that a request by a plant to remove the ACI feature should be substantiated by proof that the change is a net improvement to safety and should, as a minimum address the following:

1. The means available to minimize Event V concerns.

2. The alarms available to alert the operator of an improperly positioned valve.

3. Adequacy of the RHRS relief capacity.

4. Means other than the ACI to ensure both MOVs are closed (e.g., single switch actuating both valves).

5. Assurance that the function of the open permissive circuitry is not affected by the proposed change.

6. Assurance that MOV position indication will remain available in the control room.

7. Assessment of the proposed changes effect on RHRS reliability, as well as on Low Temperature Overpressure (LTOP) concerns.

This report provides, for each of the four reference plants, the supporting: 1) RHR System description, 2) current RHRS suction/isolation valve control circuity description, 3) proposed ACI deletion hardware changes, 4) proposed suction/isolation valve alarm circuitry addition, 5) RHRS unavailability analysis, 6) interfacing systems LOCA analysis, and 7) overpressurization analysis.

CONCLUSIONS

The report recommends the deletion of the autoclosure for all WOG plants. The installation of a control room alarm is recommended for all plants to warn the operator that a series suction/isolation valve(s) is not fully closed when RCS pressure is above the alarm setpoint. The results of the intersystem LOCA analysis show that the frequencies of the the Event V decreases with the removal of the ACI feature. The results of the RHRS unavailability analysis show that the removal of the ACI feature increases the RHRS availability. The results of the overpressurization analysis show that removal of the ACI feature will have no effect on the heat input transients and will result in a slight increase in frequency of occurrence for some categories of the mass input transients with a decrease in others. The net effect of the ACI feature removal is considered to be a net improvement in plant safety.

1.0 INTRODUCTION

This section states the purpose of this report and defines its intended use by participating utilities. It also presents, as background, a description of a typical newer vintage Residual Heat Removal System and autoclosure interlock.

1.1 Purpose

Recently, the Nuclear Regulatory Commission (NRC) and the nuclear industry has expressed interest in the acceptability of removing the autoclosure interlock (ACI) on the Residual Heat Removal System (RHRS) suction/isolation valves. This interest is in response to growing concerns about the loss of residual heat removal capability during cold shutdown and refueling operations due to inadvertent isolation of the RHRS caused by failure of the ACI circuitry. Isolation of the RHRS while operating has resulted in a loss of decay heat removal capability at several operating plants. It is also a potential contributor to overpressurization of the Reactor Coolant System (RCS) with possible Power-Operated Relief Valve (PORV) challenge and RHRS pump damage.

This report was written with the support of the Westinghouse Owner's Group (WOG). It provides an evaluation of the removal of the ACI on the RHRS suction/isolation valves at the following four reference plants: Salem Unit 1, Callaway Unit 1, North Anna Unit 1 and Shearon Harris Unit 1. These four plants are designated as lead plants for the program. The WOG plants participating in the program were categorized into four (4) groups based on similar RHR System configuration and design characteristics. It is intended that other members of the WOG will be able to reference one of these lead plants for applicable information and with a plant specific analyses remove the RHRS ACI in the future at a reduced cost impact.

This report reviews the basis for the interlock in terms of current regulations and justifies removal of the ACI based on a safety evaluation of the effect of ACI removal on low temperature overpressure protection, RHRS availability and interfacing system LOCA potential. Additionally, the report proposes basic logic changes to implement the ACI deletion, provides proposed Technical Specification revisions and presents a WOG position with regard to the RHRS ACI removal. A description of each lead plant's RHR System is provided to allow comparison with other plants and to support the current evaluation.

1.2 Background

During normal and emergency conditions, it is necessary to keep low pressure systems that are connected to the high pressure Reactor Coolant System (RCS) properly isolated from each other in order to avoid damage by overpressurization or potential for loss of integrity of the low pressure system and potential radioactive releases to the environment. The Residual Heat Removal System (RHRS) is a low pressure system, with a typical design pressure of 600 psia, with an interface to the high pressure RCS, normal operating pressure of 2250 psia.

The primary function of the RHRS is to remove heat energy from the RCS during plant cooldown and refueling operations. As a secondary function, the RHRS is used to transfer refueling water between the Refueling Water Storage Tank (RWST) and the refueling cavity at the beginning and end of refueling operations. Parts of the RHRS also may serve as part of the Emergency Core Cooling System (ECCS) during a Loss-of-Coolant Accident (LOCA).

Figure 1-1 is a simplified flow diagram showing a typical newer RHR System design. The system consists of two parallel flow paths. Each path takes suction from a separate RCS hot leg. Each flow path contains a residual heat removal pump, a residual heat exchanger and associated piping, valves and instrumentation required for operational control.

During system operation, reactor coolant flows from the RCS to a residual heat removal pump, through the tube side of a residual heat exchanger, and back to the Reactor Coolant System through the Safety Injection System (SIS) cold leg injection header. Heat is transferred from the reactor coolant to the component cooling water, which is circulating through the shell side of the residual heat exchangers.

Two inlet suction/isolation valves are provided in each inlet line from the RCS. These motor-operated, gate valves are normally-closed except when the RHRS is in operation and function to keep the low pressure RHR System isolated from the high pressure RCS. Each of these valves is provided with manual control (OPEN/CLOSE) on the main control board and has two automatic interlocks associated with its control circuitry: the AutoClose Interlock (ACI) and the Open Permissive Interlock (OPI).

The OPI prevents inadvertent opening of the suction/isolation valves when the RCS pressure is above the design pressure of the RHRS considering RHR pump discharge pressure. The pressure setpoint is normally about 400 psig when instrument uncertainties are included. Additionally, the OPI includes interlocks to prevent opening the suction/isolation valves if either of the other suction/isolation valves to the containment sump or the RWST are open or the valves in the recirculation lines from the residual heat exchanger outlets to the charging and safety injection pumps are open.

The ACI ensures that both isolation valves are fully closed when the RCS is pressurized above the RHRS design pressure. Both valves will close automatically if the pressure increases above the bistable setpoint of approximately 700 psig.

A detailed description of each of the four lead plants RHRS is provided in Section 5.0 of this report.

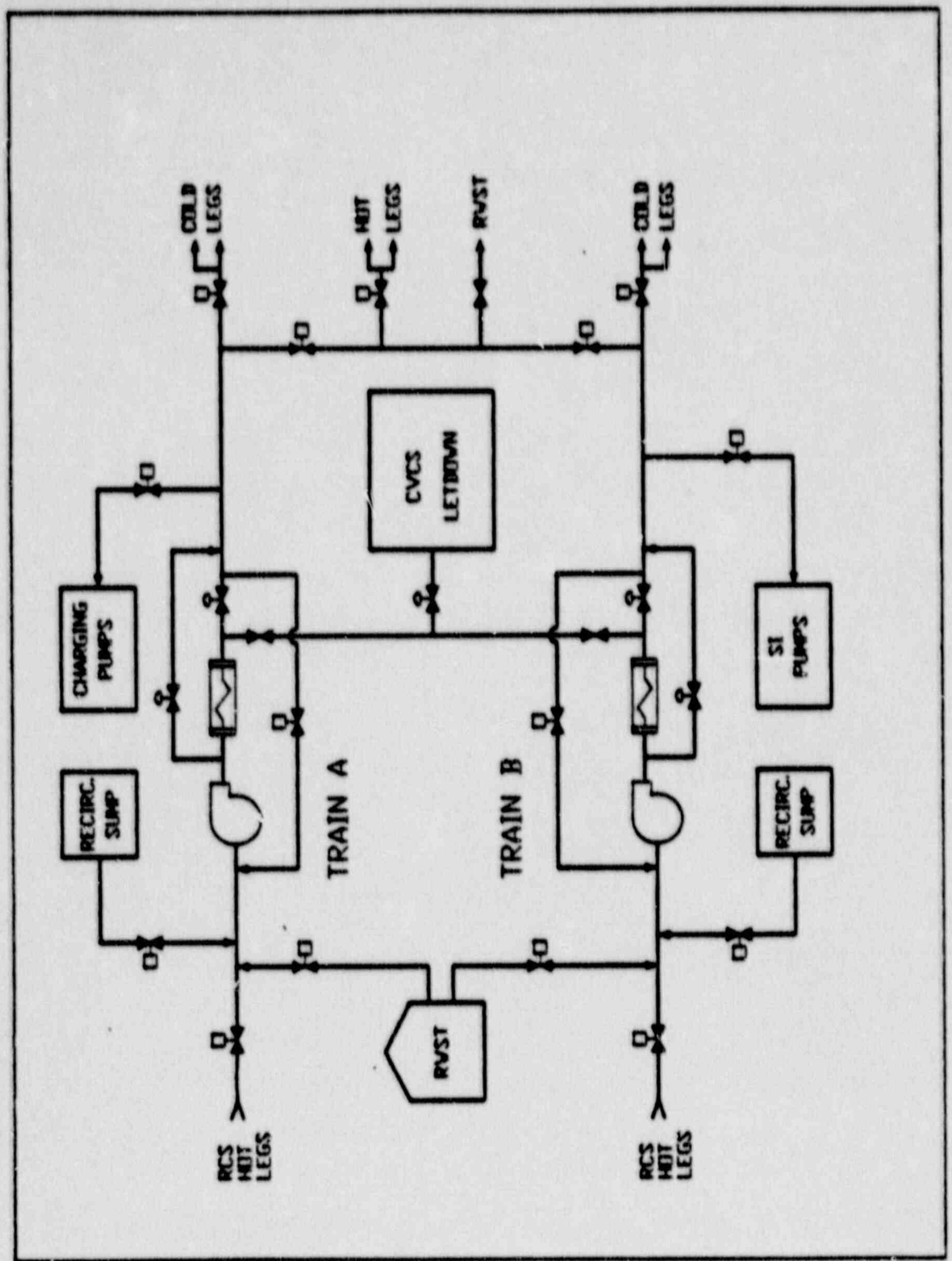


Figure 1-1. Simplified Typical Residual Heat Removal System

2.0 RECENT LITERATURE REVIEW

The following sections provide a summary of the history and background of literature concerned with loss of Residual Heat Removal events and the autoclosure interlock feature of the RHR suction/isolation valves. NRC Case Study reports and Sandia Laboratories Risk Assessment analysis conclusions are presented.

2.1 History and Background

A U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of Operational Data, Case Study Report AEOD/C503, "Decay Heat Removal Problems at U.S. Pressurized Water Reactors", (Reference 1) analyzed U.S. pressurized water reactor (PWR) experiences involving loss of an operating RHRS. This report indicated that 130 loss of decay heat removal events were reported between 1976 and 1983. In addition, analysis of operating data revealed that an underlying or root cause of most loss of RHRS events are human factors deficiencies involving procedural inadequacies and personnel error. Most errors were committed during maintenance, testing, repair operations and at a time when the RHRS is in operation.

The report further stated that the consequences of a total loss of the RHRS under certain conditions could lead to bulk boiling, core uncovery, and resultant fuel damage. The time margin for restoring the RHRS, or establishing alternate methods of decay heat removal prior to the onset of core uncovery has been calculated to begin, under worst conditions, as soon as one hour after the loss of the RHRS. The actual time would depend upon several factors such as RCS temperature, the decay heat rate and the amount of RCS inventory.

Reference 1 lists summaries of 45 loss of RHRS events that occurred during 1982 and 1983 as obtained from LERs and NRC reports. A Nuclear Safety Analysis Center/Electric Power Research Institute Report NSAC/52, "Residual Heat Removal Experience Review and Safety Analysis, Pressurized Water

Reactors" (Reference 2) identified loss of RHRS events for the period 1976 through 1981. Table 1-1 is a listing of these events reproduced from Reference 1. It provides a tabulation of 130 RHRS loss of function events for 33 plants during the period of 1976 through 1983[1]. The leading category of loss of RHRS events (37 of 130) was an inadvertent automatic closure of the RHRS suction isolation valves. Most of these events were caused by human error. Table 1-2 is also reproduced from Reference 1. It tabulates the 130 events based on the failure that caused the loss of function. The table illustrates that 28.5% of the events were caused by inadvertent automatic closure of suction isolation valves. Only two of the 37 ACI valve closure events were legitimate responses to valid signals which were correctly generated based on RCS pressure exceeding the isolation valve setpoint.

The authors of Reference 1 view the many losses of decay heat removal events at PWRs as a significant group of precursors and conclude that corrective actions are required to minimize the risk associated with decay heat removal losses. The report makes six recommendations to the office of Nuclear Reactor Regulation (NRR) based upon the potential safety significance of loss of decay heat removal events. Recommendation 5 states that the NRR should consider the removal of autoclosure interlocks to minimize loss of decay heat removal events:

> "In order to prevent inadvertent RHRS suction/isolation valve closures (during RHR System operation) it is recommended that NRR consider either requiring the removal of the autoclosure interlocks to the RHR suction/isolation valves, or requiring removal of power to the RHR suction/isolation valves when valve motion is not required. Prior to implementing this recommendation, it is necessary to ensure that there is adequate relief capacity to prevent overpressurization of the RHRS."

---

1. The reader is directed to Reference 2 appendices for summary information on RHRS losses that occurred from 1976 to 1981. For the period of 1982 through 1983, Reference 1, Appendix A provides additional summary information on RHRS losses.

The Institute of Nuclear Power Operations discusses loss of residual heat removal capability in Significant Operating Experience Report (SOER) 85-4 (Reference 3). The SOER summarizes loss of residual heat removal capability events due to the following causes: 1) low reactor vessel level, 2) automatic RHR suction valve closure, 3) loss of running RHR pump and 4) air binding of an RHR pump due to vortexing. Four events caused by automatic RHRS suction valve closure occuring during 1983 are described in the following paragraph.

One event occurred while maintenance personnel were performing a surveillance test on the cold overpressure protection system while the plant was in cold shutdown. The test simulated high RCS pressure which closed the suction/isolation valve and resulted in the operator tripping the RHR pump. The other three events involved automatic closure of the suction/isolation valve due to a closed signal being "sealed-in" while the motor control center was out of service for inspection. When the power was restored to the motor control center, the suction/isolation valve closed.

SOER 85-4 notes that, due to the potential for the loss of residual heat removal capability through inadvertent isolation of the RHR suction/isolation valves, both the AEOD report (Reference 1) and the NSAC report (Reference 2) recommend disabling the suction/isolation valves during certain phases of RHR operation. The SOER states its position on this matter as follows:

> "Suction valve closure interlocks should not be disabled without a careful analysis of low temperature overpressurization and containment integrity concerns. Since not all plants have adequate relief through the RHRS, additional relief capacity may be necessary prior to disabling the autoclosure interlock...
>
> Removing power from the suction valve motor operator is an undesirable method of avoiding inadvertent suction valve closure, since such action compromises the ability to quickly isolate RHR suction from the RCS in the event of an RHR System LOCA."

The SOER also makes the following recommendation concerning the RHR suction/isolation autoclose interlock design:

"The automatic RHR suction/isolation valve closure interlock that isolates the RHR System from the RCS should be disabled when the reactor vessel head is removed. In addition, plants that have adequate overpressure protection through the RHR system should disable the automatic closure interlock during all phases of RHR system operation."

The Reference 1 case study report has stimulated much interest in the subject of autoclosure interlocks. Based upon an earlier (1984) draft of this case study report, Sandia Laboratories performed a risk assessment analysis as part of Task A-45 evaluating the competing risks associated with RHRS suction/isolation valve closures and Event V. The RHRS Loss Of Coolant Accident (LOCA), or "Type V" LOCA, is a non-mitigable LOCA outside of containment and results in core melt. It is presumed to occur if the valves in the RHRS suction line fail open when the RCS is at normal operating pressure and results in RHRS overpressurization with failure of the RHRS pressure boundary.

The Sandia report, NUREG/CR-4335, SAND84-1339, "Potential Benefits Obtained by Requiring Safety-Grade Cold Shutdown Systems" (Reference 4), was generated specifically for the Calvert Cliffs Unit 2 plant configuration. Subsequent to their quantification of risks, Sandia concluded[2] the following:

"The lowest core melt frequency due to the combination of loss of RHRS suction during cold shutdown and V-LOCAs is obtained when there are no autoclosure interlocks on the RHRS suction valves...removing the overpressure interlocks from the RHRS suction valves gives the best RHRS suction arrangement for PWRs based upon this analysis.

2. The reader is directed to Appendix C of Reference 4 for the details of the calculations made in this analysis.

...when interlocks are present, loss of RHRS suction is the largest contributor to core melt frequency for all assumed values of probability of core melt given that RHRS suction is lost. However, when the interlocks are not present, the core malt frequency due to loss of RHRS suction is comparable to or less than the V-LOCA core melt frequency for the "best estimate" cases.

...Finally, we believe that the "best" RHRS suction valve arrangement is to have a single suction line without primary system over-pressure interlocks on the valves."

In response to the earlier draft of this case study, NRR reviewed the issue of "RCS/RHRS Suction Line Interlocks on PWRs". NRR performed a prioritization evaluation (a simplified risk and cost assessment). As a result, on August 13, 1985, in Reference 5, the Director of NRR forwarded a copy of his staff's prioritization of this issue, assigned it a "HIGH" priority ranking, and directed the Director of the Division of Systems Integration to take the actions necessary to resolve this issue.

In an effort to reduce the frequency of inadvertent suction/isolation valve closures, several plants have taken steps to allow the removal of power (power lockout) from these valves during certain modes of plant operation. Some plants, having repeated decay heat removal system losses, have amended their technical specifications to allow removal of power from the RHRS suction/isolation valves during plant shutdown in order to preclude their inadvertent closure. Other plants have maintenance procedures which call for deenergizing these valves in the open position before conducting setpoint calibration and prior to conducting work on inverters. Both of these actions were made in order to preclude their inadvertent closure.

Additionally, recently licensed plants have been granted technical specifications which allow the RHRS suction relief valves to meet the Limiting Condition for Operation (LCO) requirements for the Overpressure Protection System in the lower modes. These plants were required to include an additional technical specification surveillance requirement which ensures that a single failure will not cause an inadvertent suction/isolation valve closure. This surveillance involves verifying at least once per 31 days that one of the RHRS suction/isolation valves is open with power removed and verifying at least once per 12 hours that the other RHRS suction/isolation valve in the same drop line is open when credit is taken for that drop line's RHRS relief valve.

It is also important to note that two plants, Kewaunee and Diablo Canyon, have recently requested alterations in their RHRS suction/isolation valve control circuitry to remove the ACI.

Kewaunee is a two loop Westinghouse PWR with two RHRS drop lines from the RCS hot legs. In December, 1983 the utility requested NRR acceptance of complete removal of the ACI. This was based on the utility's belief that the ACI presents a high potential for inadvertent RHRS isolation and for their particular plant, a loss of the Low Temperature Overpressure Protection System (LTOPS). Westinghouse evaluated Kewaunee's proposal for removing the autoclosure interlocks on the RHRS suction valves. The Westinghouse evaluation considered the various events which could lead to RHRS overpressurization. The events considered included the following transients: 1) premature opening of the RHRS, 2) isolation of letdown while charging continues at a constant rate, 3) charging/safety injection pump actuation, 4) opening of an accumulator discharge isolation valve, 5) startup of an inactive RCS loop, 6) pressurizer heaters actuation, 7) rod withdrawal, and 8) loss of an RHRS cooling train. The evaluation showed that for transients 1,3,6,7 and 8 the removal of the autoclosure feature had little or no effect on the transient, for transients 4 and 5 the removal may be beneficial and for transient 2 the removal may preclude the transient or reduce its severity.

The NRC commenting in a memorandum for Reactor Systems Branch members concerning "Auto Closure Interlocks for PWR Residual Heat Removal (RHR) Systems" (Reference 6) notes that the Westinghouse analysis concluded that for Kewaunee the proposed modification would be a safety improvement. NRR has subsequently approved the modification for Kewaunee.

Diablo Canyon is a four loop Westinghouse PWR with only a single RHRS drop line from the RCS hot leg. As a result of NRC review during the licensing process, the staff found that the plant should retain power available to the RHRS suction/isolation valve motor operators when the RHR System is in operation. Additionally, the staff requested that the utility address the possibility of removal of the ACI. WCAP-11117, "Residual Heat Removal System Auto Closure Interlock Removal Report for Diablo Canyon Nuclear Power Plant" (Reference 7), provides justification for ACI removal based on the same methodology as presented in this report. The request to remove the ACI at Diablo Canyon has been approved by the NRC and a SER was issued in February, 1988 (Reference 27).

As noted in Reference 5, the effects of autoclosure interlock removal upon plant safety must be evaluated on a plant by plant basis because of numerous plant-specific differences and the plant specific data needed as input to the analyses.

Table 1-1
Frequency of DHR Losses
(1976 - 1983)

	1976	1977	1978	1979	1980	1981	1982	1983	Total
Davis-Besse			4	1	9	2			16
Beaver Valley - 1			1	1	4	2	1	1	10
Calvert Cliffs - 2			2	1		2	3		10
Salem - 2						2		8	10
Crystal River		3	2	2	2				9
Calvert Cliffs - 1			2		5		1	1	9
Trojan		1	5			1			7
North Anna - 1				1	2		2	2	7
North Anna - 2							4	3	7
Salem - 1	1			3			1		5
Farley - 1			2		2	1			5
McGuire - 1							2	1	3
Millstone - 2				1		1	1		3
ANO - 2				2					2
Ginna								2	2
Maine Yankee						2			2
Palisades			1			1			2
Rancho Seco						1	1		2
St. Lucie - 1			1					1	2
Sequoyah - 1						1	1		2
Turkey Point - 3								2	2
Turkey Point - 4						2			2
Indian Point - 3	1								1
Fort Calhoun		1							1
San Onofre - 1					1				1
Oconee - 1						1			1
Oconee - 2						1			1
Zion - 1							1		1
Surry - 1								1	1
Sequoyah - 2								1	1
Farley - 2								1	1
McGuire - 2								1	1
Summer - 1								1	1
									130
Annual Frequency of DHR Losses (# of events) / (# of Operating PWRs)	.06	.1	.5	.3	.6	.5	.35	.5	

Reproduced from Reference 1

Table 1-2

Categories of 130 Reported Total DHR System

Failures When Required to Operate (Loss of Function)

at U.S. PWRs 1976-1983

	No. of Events	(% of Events)
Automation Closure of Suction/ Isolation Valves	37	(28.5)
Loss of Inventory		
Inadequate RCS Inventory Resulting in Loss of DHR Pump Suction	26	(20.0)
Loss of RCS Inventory Through DHR System Necessitating Shutdown of DHP System	10	(7.7)
Component Failures		
Shutdown or Failure of DHR Pump	21	(16.2)
Inability to Open Suction/Isolation Valve	8	(6.1)
Others	28	(21.5)
Total	130	(100.0)

Reproduced from Reference 1

3.0 LICENSING BASIS

The removal of the autoclosure interlock feature must be reviewed within the framework of the regulatory and industry safety standard criteria. Since the evaluation of this licensing basis spans over twenty-five years, a description of the history as well as the current regulations is presented in the sections that follow.

3.1 History of Regulations

During the 1960s and 1970's, the typical RHRS configuration for a Westinghouse PWR consisted of two residual heat removal trains with a common suction line from the RCS hot leg line. Two closed valves in series isolated the RHRS from the RCS while the RCS was at normal operating temperature and pressure. A combination of interlocks and administrative procedures were used to prevent overpressurization of the RHRS. An open permissive interlock was provided on the valve adjacent to the RCS to prevent opening until the RCS pressure was reduced below the RHRS design pressure. Both valves were to have power disconnected via administrative procedures except when the valves were to be stroked. As an additional design feature, the suction/isolation valve motor operators were sized with insufficient opening torque to move the valve disc with a pressure differential greater than approximately 600 psi. Finally, a relief valve set to prevent RHRS overpressure was located just downstream of the suction/isolation valves.

The early 1970's saw the Atomic Energy Commission's (AEC) interest in the suction/isolation valve interlock develop. Initially this was manifested in the AEC stating its concern for the need for a pressure interlock on both valves. The AEC position on this issue was extended to four suction isolation valves as the newer two suction line designs were starting to make their appearance. Other AEC positions that evolved at that time (1971) were 1) interlocks for automatic closure on increasing pressure, 2) use of diverse principles for interlocks, and 3) commitment to IEEE-279. Table 3-1 provides a brief review of the impact of these requirements and some of the plants affected.

The introduction of the autoclose interlock heightened a previous industry concern regarding RCS pressure control during RHRS operation. Spurious closure of the RHR suction/isolation valves would isolate the RCS from both the RHR suction line relief valves and the low pressure letdown connection to the Chemical and Volume Control System (CVCS). Without the low pressure letdown line, plant operation in the water solid mode is difficult. Additionally, should a pressure transient occur, automatic closure of the suction valves prevents the relief valve from performing its function (overpressure protection), thus aggravating the transient.

A joint meeting between industry (W, B&W, and CE) and the AEC in March, 1974 attempted to clarify the AEC's requirement for the interlocks. This discussion brought about three acceptable methods of preventing RHRS overpressurization while the RHRS is in operation or when returning the RCS to operation: 1) automatic closure interlocks on the RHR suction/isolation valves, 2) sufficient capacity of the RHR suction line relief valves to mitigate a pressure transient, or 3) a combination of the two.

It was pointed out at the meeting that the AEC representative on the ANS Committee 32.4 (Overpressure Protection of Low Pressure Systems Connected to the Reactor Coolant Pressure Boundary) said he would not accept removal of the autoclosure interlock. While the AEC replied that a committee member speaks only as an individual and not for the AEC, the AEC representative's position was later adopted as their official position.

Over the next 1-1/2 years, Westinghouse performed several analyses in support of the RESAR-3 and RESAR-41 applications. These analyses demonstrated that adequately sized relief valves were sufficient by themselves in protecting the RHRS from overpressure, and that the autoclosure feature was not needed.

In parallel with the RESAR-41 application and NRC staff review, the NRC formalized their position and released it as Branch Technical Position (BTP) ICSB 3, "Isolation of Low Pressure Systems From the High Pressure Reactor Coolant System" (Reference 8), in the summer of 1975. BTP ICSB 3 presented six measures which should be incorporated in designs of the interfaces between low pressure systems and the high pressure Reactor Coolant System. Of special interest is measure 2 which states:

"For system interfaces where both valves are motor-operated, the valves should have independent and diverse interlocks to prevent both from opening unless the primary system pressure is below the subsystem design pressure. Also, the valve operators should receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure."

Faced with the requirement for retaining both the open permissive interlock and the autoclosure interlock, discussion with the NRC centered on raising the setpoint such that the autoclosure feature did not prematurely isolate the RHRS on a pressure transient. At the same time, the setpoints for the RHRS suction line relief valves were lowered to 450 psig from 500 psig. The raised autoclosure setpoint, however, would not preclude transients initiated by a spurious closure of the valves such as was experienced during testing at Kewaunee Nuclear Power Plant on September 26, 1974 (Reference 9).

The Safety Evaluation Report (SER) for the RESAR-41 (Reference 10) application provided the final NRC position on the issue. While BTP ICSB 3 stated that "the valve operators <u>should</u> receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure," the RESAR-41 SER stated:

"In particular, the Residual Heat Removal System inlet isolation valves <u>will</u> be equipped with autoclosure and prevent-open interlocks to prevent possible exposure of the residual heat removal system to excessive pressures. The interlocks <u>will</u> be designed to prevent the occurrence of a situation where there is only a single barrier protection against a possible loss-of-coolant accident outside containment.

The autoclosure interlock will close the system isolation valves when the Reactor Coolant System pressure increases to 750 pounds per square inch. This pressure is greater than the Residual Heat Removal System relief valve set pressure plus accumulation, thus assuring that the relief valves will provide some overpressure protection to the Reactor Coolant System when in the cold shutdown condition.

Westinghouse has designed the relief valves for the Residual Heat Removal System to prevent inadvertent overpressurization during plant cooldown or startup, considering normal operating conditions, infrequent transients, and abnormal occurrences. As part of our review of the final design for RESAR-41, we will require that Westinghouse provide a detailed analysis that demonstrates the adequacy of the capacity of the system relief valves to prevent overpressurization during plant cooldown or startup."

When the NRC recognized an autoclosure setpoint above the RHRS design pressure it separated the autoclosure feature LOCA concerns from pressure transient mitigation concerns. The requirement, then, was to demonstrate the adequacy of the relief valves. This is demonstrated by the NRC's acceptance of the use of the pressurizer power-operated relief valves in conjunction with the RHRS relief valves at Maine Yankee Atomic Power Station to meet single failure criteria for the overpressure protection system. While the NRC did recognize a higher than RHRS design pressure setpoint for the ACI, they stopped short of permitting the removal of the autoclosure feature as discussed in a letter to Yankee Atomic Electric Company dated August 22, 1977 (Reference 11).

The industry-experienced problem, that of loss of RHRS capability and possible pump damage following closure of the RHRS isolation valves due to a failure of the autoclosure interlock, was reviewed in conjunction with the RESAR-3S application (Reference 12). Actions taken by several utilities were to remove power from one or more of the suction valves during the time frame when the RHR pumps are most susceptible to damage due to loss of suction (i.e. refueling or testing). Westinghouse recommended this approach via "Westinghouse Nuclear Service Division Technical Bulletin 77-7" in July, 1977 (Reference 13).

Various other publications during this time period also dealt with these issues, among them; "Staff Discussion of 15 Technical Issues Listed in Attachment to November 3, 1976 Memo from Director, NRR to NRR Staff" (Reference 14) and "Operating Experiences: Reactor Vessel Pressure Transients" (Reference 15).

In 1977, Working Group ANS-56.3 (previously ANS-32.4 and ANS-55.4) finished work on ANSI/ANS-56.3-1977, "Overpressure Protection of Low Pressure Systems Connected to the Reactor Coolant Pressure Boundary" (Reference 16). This standard permitted the RHRS designer a choice between a suction valve isolation or the use of pressure reduction (flow limitation).

The isolation scheme of this standard required independent interlocks to prevent the suction valves from being opened unless the RCS is below the RHRS design pressure. Additionally, to protect the low pressure system against accidental overpressure when both valves are open, an independent signal for power actuation was required for each valve to automatically close should the pressure in the RCS increase to a value exceeding the RHRS design pressure.

The alternate pressure reduction scheme would require some sort of pressure reducing device (i.e., orifice, throttling valve, or drag valve) to control the pressure to a predetermined value and a pressure relieving device (i.e., RHRS relief valve) in the RHRS. The design required pressure relief protection with sufficient capacity for the worst case pressure transient.

The standard also stated: " Control Room indication shall be provided to indicate when isolation is necessary."

The issue remained quiet through the remainder of the 1970's.

In 1982, a study, "Evaluation of Events Involving Decay Heat Removal Systems in Nuclear Power Plants", was published by Oak Ridge National Laboratory detailing the review and evaluation of events placed in the Nuclear Safety Information Center (NSIC) file involving the removal of decay heat in US BWRs and PWRs from June, 1979 through June, 1981 (Reference 17). The Oak Ridge study reported that during the two-year period "the most frequent event involving a significant problem with decay heat removal (DHR) system was the cavitation of RHR pumps". Five events were traced to closure of the suction valves due to spurious signals from their autoclosure interlocks.

Shortly thereafter, an EPRI report (Reference 2) also detailed events where RHRS operation was curtailed due to inadvertant suction valve closure . Twenty-four events (occurring over five years) that involved inadvertent loss of RHRS cooling due to the autoclosure interlock failing were identified.

3.2 Current Regulations

The removal of the autoclosure interlock feature must be reviewed within the framework of the applicable and current regulatory and industry safety standard criteria. While the following discussion is not meant to be inclusive it presents a summary of the current licensing considerations associated with the RHRS ACI.

ANSI/ANS 56.3-1977

ANSI/ANS 56.3-1977, "Overpressure Protection of Low Pressure Systems Connected to the Reactor Coolant Pressure Boundary", Section 3, describes several methods of protection that "shall be used" to prevent overpressurization of the RHRS. Specifically, Section 3.2.1 permits the designer a choice between the use of an autoclose feature or pressure relief sized on the basis of the most extreme pressure transient anticipated to occur during the plant operating condition when the two valves separating the RCS from the RHRS suction are open. Figure 3-1 is a reproduction of Figure 1 of the standard and depicts the methods acceptable to the standard.

Current RHRS design is more conservative than either method 1(a) or 1(b) in the figure in the sense that it requires both the ACI and the OPI in addition to the RHRS relief valve sized to mitigate the most limiting pressure transient. Following removal of the ACI, overpressure protection would be provided by method 1(b) which consists of two suction/isolation valves in series interlocked with an OPI and an adequately sized RHRS relief valve.

Regulatory Guide 1.139

The U.S. NRC Office of Standards Development issued Regulatory Guide 1.139, "Guidance For Residual Heat Removal" with the intent of describing a method acceptable to the NRC staff for complying with the Commission's regulations with regard to the removal of decay heat and sensible heat after a reactor shutdown. The regulatory position on RHRS isolation states that the RHRS should satisfy the following functional guidance in relation to the RHRS suction/isolation valves.

1. Isolation of the suction side of the RHR System should be provided by at least two power-operated valves in series.

2. Alarms in the control room should be provided to alert the operator if either valve is open when the RCS pressure exceeds the RHR System design pressure.

3. The valves should have independent diverse interlocks to prevent them from being opened unless the RCS pressure is below the RHR System design pressure.

Regulatory Guide 1.139 also provides the following functional guidance to protect the RHRS against accidental overpressurization when it is not isolated from the RCS.

1. Pressure relief in the RHRS should be provided with relieving capacity in accordance with the ASME boiler and Pressure Vessel Code.

2. The most limiting pressure transient during the plant operating condition when the RHRS is not isolated from the RCS should be considered when selecting the pressure relieving capacity of the RHRS relief valve(s).

3. If interlocks are provided to automatically close the isolation valves when the RCS pressure exceeds the RHRS design pressure, adequate relief capacity should be provided during the time that the valves are closing.

Standard Review Plan (SRP)

The NRC position is stated in two branch technical position papers: ICSB 3 and RSB 5-1 found in "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plant", NUREG-0800, July, 1981. Branch Technical Position ICSB 3, "Isolation of Low Pressure Systems From the High Pressure Reactor Coolant System" position B.2. states:

"For system interfaces where both valves are motor-operated, the valves should have independent and diverse interlocks to prevent both from opening unless the primary system pressure is below the subsystem design pressure. Also, the valve operators should receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure."

Branch Technical Position RSB 5-1, "Design Requirements of the Residual Heat Removal System" position B.1 states:

"The following shall be provided in the suction side of the RHRS to isolate it from the RCS.

A. Isolation shall be provided by at least two power-operated valves in series. The valve positions shall be indicated in the control room.

B. The valves shall have independent diverse interlocks to prevent the valves from being opened unless the RCS pressure is below the RHRS design pressure. Failure of a power supply shall not cause any valve to change position.

C. The valves shall have independent diverse interlocks to protect against one or both valves being open during an RCS increase above the design pressure of the RHRS."

The major difference between the two BTPs is in the use of the words "should" and "shall". ICSB 3 uses "should" while RSB 5-1 uses "shall". The implication is that "shall" is interpreted as a requirement while "should" generally is interpreted as only a recommendation. Another difference is that the ICSB 3 position makes no mention of relief valves, while position C of RSB 5-1 states:

"The RHRS shall satisfy the pressure relief requirements listed below.

1. To protect the RHRS against accidental overpressurization when it is in operation (not isolated from the RCS), pressure relief in the RHRS shall be provided with relieving capacity in accordance with the ASME Boiler and Pressure Vessel Code. The most limiting pressure transient during the plant operating condition when the RHRS is not isolated from the RCS shall be considered when selecting the pressure relieving capacity of the RHRS. For example, during shutdown cooling in a PWR with no steam bubble in the pressurizer, inadvertent operation of an additional charging pump or inadvertent opening of an ECCS accumulator valve should be considered in selection of the design bases.

2. Fluid discharged through the RHRS pressure relief valves must be collected and contained such that a stuck open relief valve will not:

(a) Result in flooding of any safety-related equipment.

(b) Reduce the capability of the ECCS below that needed to mitigate the consequences of a postulated LOCA.

(c) Result in a non-isolatable situation in which the water provided to the RCS to maintain the core in a safe condition is discharged outside of the containment.

3. If interlocks are provided to automatically close the isolation valves when the RCS pressure exceeds the RHRS design pressure, adequate relief capacity shall be provided during the time period while the valves are closing."

The RSB position goes on to state:

D. Pump Protection Requirements

"The design and operating procedures of any RHRS shall have provisions to prevent damage to the RHRS due to overheating, cavitation or loss of adequate pump suction fluid."

The inconsistency in branch positions (one requires the autoclosure interlock while the other only recommends it) is seemingly confounded by the NRC's acceptance of the autoclosure setpoint above RHRS design pressure. Close inspection of the BTPs indicates that the ACI isolation function is provided to assure that there is a double barrier (two closed valves) between the RCS and the RHRS when the plant is at normal operating conditions, and not to protect the low pressure RHRS piping from higher RCS pressure. If neither suction/isolation valve are closed, the RHRS relief valves would preclude the capability to pressurize the primary system above the relief valve setpoint during startup. RSB 5-1 Item C above clearly assigns the protection of the RHRS from overpressurization events to the RHRS pressure relief valves. With the proper function of both the RHRS suction/isolation valve ACI and the relief valves clearly in mind it is not difficult to see how the current ACI setpoint can be above the RHRS design pressure as long as the relief valves are suitably sized.

An April 17, 1984 NRC ICSB internal memorandum on "RHRS Interlocks for Westinghouse Plants" (Reference 18) discussed a clarification of the design basis of RHRS interlocks. Also discussed was a concern centered on the safety implications of the failure mode of interlocks due to a loss of an instrument bus which results in automatic closure of the RHRS suction/isolation valves and a subsequent loss of RHRS decay heat removal capability. The reference concludes:

> "In summary, the aspects of the RHRS interlocks which can result in automatic closure of the RHRS suction valves on a loss of an instrument bus make a negligible contribution to the design basis for which they are provided. However, the potential for a complete loss of decay heat removal capability by the RHRS is greatly increased by this design. Therefore, it is recommended that in the interest of plant safety, action should be taken to modify the design of RHRS interlocks for Westinghouse plants such that a loss of an instrument bus will not result in a loss of RHRS cooling."

An NRC internal memorandum of January, 1985 (Reference 6) stating the RSB position states that:

> "The issue of RHRS ACI reliability is being prioritized by SPEB. In the meantime, proposals to change the RHRS isolation valve controls should be carefully considered, especially in light of the many overlapping concerns."
>
> "There is no reason, as yet, to allow or even encourage whole scale removal of the ACI. The request by each plant should be reviewed on a case-by-case basis. As a minimum, however, any proposal to remove the ACI should be substantiated by proof that the change is a net improvement in

safety. For example, requests for removal of power or the ACI should assess as a minimum, the following:

1. The means available to minimize Event V concerns.

2. The alarms to alert the operator of an improperly positioned RHRS MOV.

3. The RHRS relief valve capacity must be adequate.

4. Means other than the ACI to ensure both MOVs are closed (e.g., single switch actuating both valves).

5. Assurance that the function of the open permissive circuitry is not affected by the proposed change.

6. Assurance that MOV position indication will remain available in the control room, regardless of the proposed change.

7. An assessment of the proposed change's effect on RHRS reliability, as well as on LTOPs concerns."

10CFR50.59

This paragraph of the Code of Federal Regulations allows the utility to make a change in the facility as described in the FSAR without prior NRC approval if the change does not involve a change in the plant's technical specifications or constitute an unreviewed safety question. Otherwise, the utility must submit an application for license amendment pursuant to 10CFR50.90 and provide to the Commission its analysis, using the standards in 10CFR50.92, about the issue of no significant hazards considerations.

The change "shall be deemed to involve an unreviewed safety question (i) if the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report may be increased; or (ii) if a possibility for an accident or malfunction of a different type than any evaluated previously in the safety analysis report may be created; or (iii) if the margin of safety as defined in the basis for any technical specification is reduced."

The "Standard Technical Specifications for Westinghouse Pressurized Water Reactors", NUREG-0452, DRAFT Rev. 5, requires that verification of automatic isolation and interlock action of the RHRS from the RCS be conducted at least once per 18 months in accordance with surveillance requirement 4.5.2.d.1. The Technical Specifications for each reference plant will be reviewed in Section 8.0 of this report to determine if a similar surveillance exists. If the technical specifications require modification, an amendment to the operating license will be necessary per 10CFR50.90 with the accompanying 10CFR50.92 significant hazards evaluation. For those plants whose technical specifications do not contain a similar surveillance requirement the impact of the removal of the ACI on 10CFR50.59 is limited to determining if the removal constitutes an unreviewed safety question as discussed above.

The first question to be addressed is if an increase in the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report occurs.

Section 9.0 of this report concludes that based on three areas of probabilistic analysis: 1) the frequency of an Event V, 2) the availability of the RHRS, and 3) the effect on overpressure transients, there is an overall increase in safety due to removal of the autoclosure interlock. While it is true that the frequency of the consequences of the overpressurization event does increase, the increase is considered to be insignificant and offset by the reduction in frequency of Event V and the increase in RHRS availability. The demonstrated improvement in RHRS availability will further reduce the probability of the accidents for which RHRS failure during shutdown cooling is an initiating event. Therefore, this change does not involve an increase in the probability or consequences of accidents previously evaluated.

The second question to be addressed is: Has the possibility of an accident or malfunction of a different type than any evaluated previously in the safety analysis report been created?

Each Final Safety Analysis Report should be reviewed to determine the commitment to the analysis of an RHRS overpressurization accident (requested in Reg. Guide 1.70, Rev. 1) with reference to the RHRS interlocks. In general, the effect of an overpressure transient at cold shutdown conditions will not be altered by removal of the ACI. With or without removal of the ACI, the RHRS will be subject to overpressure for which the RHR System relief valves must be relied upon to limit pressure to within RHRS design parameters. This follows from the fact that, while it is true that the interlocks provide an automatic closure to the RHRS suction valves on high RCS pressure, overpressure protection of the RHRS is provided by the RHRS relief valves and not by the slow acting suction/isolation valves that isolate the RHRS from the RCS. The purpose of the interlocks is to assure that there is a double barrier (two closed valves) between the RCS and the RHR System when the plant is at normal operating conditions, i.e., pressurized and not in the RHRS cooling mode. Thus, the interlock safety function is to preclude conditions that could lead to a LOCA outside of containment due to an operator error. The interlock safety function is not to isolate the RHRS from the RCS when the RHRS is operating in the decay heat removal mode.

There are several levels of defense which would assure that there is a double barrier between the RCS and RHRS when the plant is at normal operating conditions. The first level would be the plant operating procedures which instruct the operator to isolate the RHRS during plant heatup. The second level would be the installation of an alarm that sounds given a "valve not full closed" signal in conjuntion with a "RCS pressure - high" signal. The intent of the alarm would be to alert the operator that either of the RCS-RHRS isolation valves is not fully closed, and that double isolation is not intact. The third level of defense would be revised alarm response guidelines and operator training. It should be noted that the open permissive interlock is not changed and it would still function to prevent opening of either RHRS suction/isolation valve when the RCS is above RHRS design pressure.

The third question regarding reduction in margin of safety as defined in the basis for any Technical Specification would or would not apply depending upon the plant's particular technical specifications.

10CFR50.92

The Code of Federal Regulations requires that, at the time a licensee requests an amendment to the license, it must provide to the Commission a significant hazards report using the standards of 10CFR50.92 to meet the notice for public comment requirements of 10CFR50.91. This requirement is met by determining if operation of the facility in accordance with the proposed amendment would not: 1) involve a significant increase in the probability or consequences of an accident previously evaluated; or 2) create the possibility of a new or different kind of accident from any accident previously evaluated; or 3) involve a significant reduction in a margin of safety.

The first question that needs to be addressed, as defined above is: would operation without the RHRS ACI involve a significant increase in the probability or consequences of an accident previously evaluated? The answer to this question is similar to the discussion presented in Section 3.2.3 in regard to 10CFR50.59 unreviewed safety question Item (i) which responded to the question: is there an increase in the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report? As stated in the previous section, based on three areas of probabilistic analysis: 1) the frequency of Event V, 2) the availability of RHRS, and 3) the effect on overpressure transients, there is an overall increase in safety due to removal of the autoclosure interlock. Therefore the deletion of the RHRS ACI does not pose a significant hazard in the sense that it would involve a significant increase in the probability or consequences of an accident previously evaluated.

The second question to be addressed is: would operation without the RHRS ACI create the possibility of a new or different kind of accident from any accident previously evaluated? The answer to this question is similar to the discussion presented in Section 3.2.3 in regard to 10CFR50.59 unreviewed safety question Item (ii) which responded to the question: is the possibility of an accident or malfunction of a different type than any evaluated previously in the safety analysis report created? As stated in the previous section, each plant's Final Safety Analysis Report should be reviewed to determine the committment to the analysis of an RHRS overpressurization accident (requested in Reg. Guide 1.70, Rev. 1) with reference to the RHRS interlocks. In general, the effect of an overpressure transient at cold shutdown conditions will not be altered by removal of the RHRS ACI. For normal plant operating conditions, when the plant is pressurized and not in the RHRS cooling mode, there are several levels of defense which would assure that there is a double barrier between the RCS and RHRS. Therefore, the deletion of the RHRS ACI does not pose a significant hazard in the sense that it would create the possibility of a new or different kind of accident from any accident previously evaluated.

The third question to be addressed is: would operation without the RHRS ACI reduce the margin of safety as defined in the basis for any technical specification? The "Standard Technical Specifications for Westinghouse Pressurized Water Reactors", NUREG-0452, DRAFT Rev. 5, requires that verification of automatic isolation and interlock action of the RHRS from the RCS be conducted at least once per 18 months in accordance with surveillance requirement 4.5.2.d.1. The corresponding bases for Emergency Core Cooling Systems (ECCS) states:

> "The Surveillance Requirements provided to ensure OPERABILITY of each component ensures that at a minimum, the assumptions used in the safety analysis are met and that the subsystem OPERABILITY is maintained."
>
> "The OPERABILITY of two independent ECCS subsystems ensures that sufficient emergency core cooling capability will be available in the event of a LOCA assuming the loss of one subsystem through the single failure consideration."

No mention is specifically made in the technical specification bases concerning the RHRS ACI. However, the conclusion can be made that, since the probabilistic analysis in Section 9.0 indicates an increase in RHRS availability due to the RHRS ACI removal, the margin of safety has actually increased.

Fire Protection: 10CFR50.48 and Appendix R

10CFR50.48 states that nuclear power plants licensed to operate after January 1, 1979, shall complete all fire protection modifications needed to satisfy Criterion 3 of Appendix A to 10CFR50 in accordance with the provisions of their licenses. Appendix R of 10CFR50 governs the fire protection program for nuclear power facilities operating prior to January 1, 1979. Appendix R states: "When considering the effects of fire, those systems associated with achieving and maintaining safe shutdown conditions assume major importance to safety because damage to them can lead to core damage resulting from loss of coolant through boiloff." Since the RHR System is associated with achieving and maintaining safe shutdown conditions, any change to the system has possible impact on the fire protection requirements of Appendix R. In particular, Appendix R requires under Part II, General Requirements, subsection B, "Fire Hazards Analysis", that a fire hazards analysis be performed to, among other things, determine the consequences of fire in any location in the plant on the ability to safely shut down the reactor or on the ability to minimize and control the release of radioactivity to the environment.

Since the deletion of the RHRS ACI is in part based on a probabilistic risk analysis which justifies the removal based on a criterion of increased availability and reliability, this change is not expected to adversely impact the lead plants current Appendix R, Fire Protection Safety Analysis Reports. Of course, changes made as part of the autoclosure interlock deletion must be reviewed by each lead plant and must be made in accordance with the Appendix R requirements that apply to the provisions of their particular license, such as train separation, fire barriers, fire hazards analysis, etc.

TABLE 3-1

AEC INSPIRED MODIFICATIONS TO RHRS SUCTION VALVING

Original Design	Required Modifications	Plants Affected
1. Group I		
a. Two valves in series in the single suction line:	a. Maintain items 1a and 1b and add additional features:	2 Loop Plants Kewaunee Prairie Island 1 & 2
(1) One valve adjacent to RCS was interlocked with a pressure control signal derived from a pressure transmitter to prevent its opening whenever the system pressure is greater than about 425 psig.	(1) A second wide range pressure channel was added to provide a pressure control signal to interlock the valve located adjacent to the RHRS. This is used to prevent its opening whenever the system pressure is greater than about 425 psig.	3 Loop Plants North Anna 1 & 2 Beaver Valley 1 4 Loop Plants
(2) One valve adjacent to RHRS was administratively locked closed by locking off the motor controlled power supply.	This second pressure transmitter is connected by a separate connection into the RHR suction line inside the containment. Therefore, the suction line	Zion 1 & 2 D. C. Cook 1 & 2 Salem 1 & 2 Diablo Canyon 1 & 2 Trojan

TABLE 3-1 (continued)

AEC INSPIRED MODIFICATIONS TO RHRS SUCTION VALVING

Original Design	Required Modifications	Plants Affected
b. One pressure transmitter was provided to provide control signal for valve 1.a (1) above. The pressure transmitter was taken off the reactor coolant loop which contained the RHR suction line. The pressure transmitter was connected into the suction line inside the containment.	contains two separate connections, one for each pressure transmitter. (2) Added control circuitry to automatically close both suction line valves if they haven't been manually closed by the time the reactor coolant pressure reaches 600 psig.	Sequoyah 1 & 2 Watts Bar 1 & 2 McGuire 1 & 2
2. Group II		
a. Two valves in series in each of two separate suction lines: (1) In each line one valve adjacent to RCS was interlocked with a pressure control signal derived from the pressure transmitter in its associated line to	a. A control signal from one of the two pressure channels is used to interlock the opening of the two suction line valves adjacent to the RCS and a control signal from the other pressure channel is used to interlock the opening of the two suction line valves adjacent to the RHRS.	2 Loop Plants Future Plants 3 Loop Plants Farley 1 & 2 Virgil Summer

TABLE 3-1 (continued)

AEC INSPIRED MODIFICATIONS TO RHRS SUCTION VALVING

Original Design	Required Modifications	Plants Affected
prevent its opening whenever the system pressure is greater than about 425 psig.		Shearon Harris, 1,2,3,4
	b. Added control circuitry to automatically close both valves in each suction line if they haven't been manually closed by the time the reactor coolant pressure reaches 600 psig.	Future Plants 4 Loop Plants Byron 1 & 2 Vogtle 1 & 2 Millstone 3 Future Plants
(2) One valve in each line adjacent to RHRS was administratively locked closed by locking off the motor controller power supply.		
b. Each of the two separate suction lines had one pressure transmitter which provided a control signal for its respective valve 2.a.(1) above. Each suction line was taken off a different reactor coolant loop. The pressure transmitter was connected into its respective suction line inside the containment.		

TABLE 3-1 (continued)

AEC INSPIRED MODIFICATIONS TO RHRS SUCTION VALVING

Original Design	Required Modifications	Plants Affected
3. Group III		
Same as Group 1	No change	2 Loop Plants
		Point Beach 1 & 2
		3 Loop Plants
		Surry 1 & 2 Turkey Point 4
		4 Loop Plants
		Indian Point 2

Source: Westinghouse letter, R. I. Hayford, Subject: Control Features Required for Critical Function Motor Operated Valves, E-EPS-737, May 10, 1972.

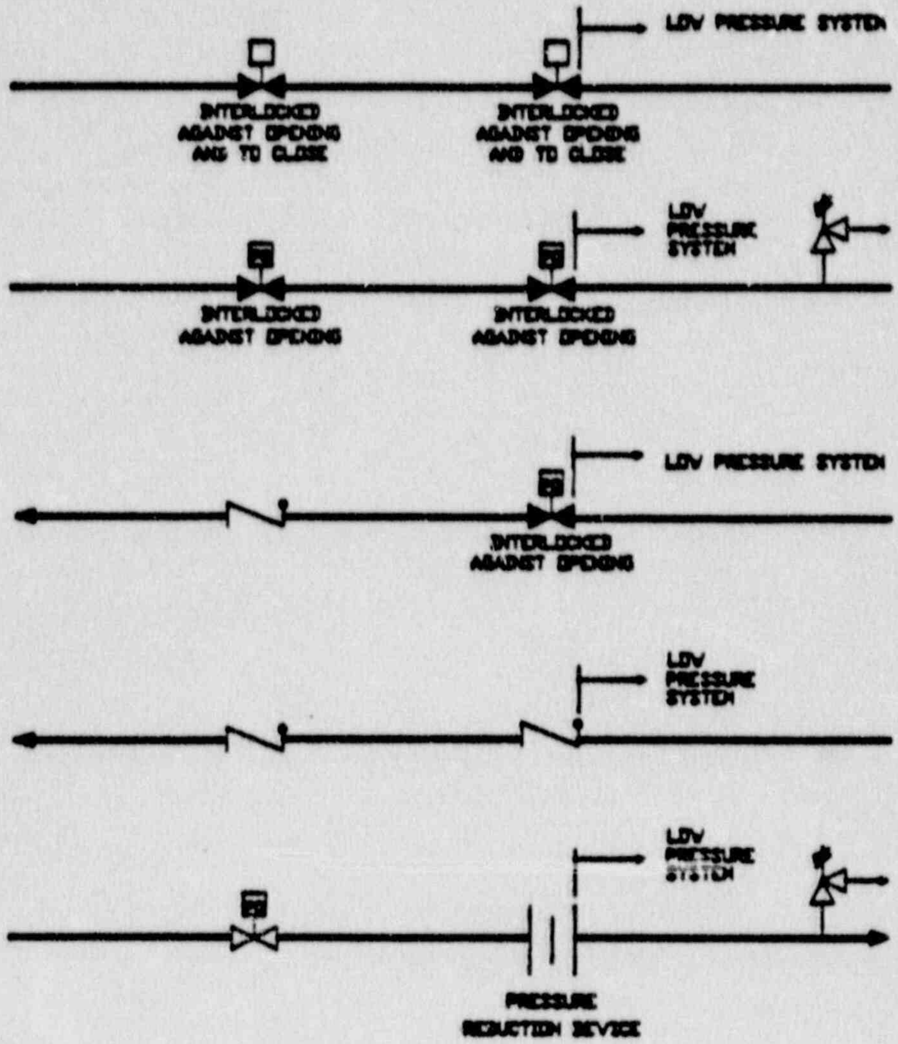


Figure 3-1. ANSI/ANS-56.3-1977 METHODS OF OVERPRESSURE PROTECTION

4.0 WOG PLANT CATEGORIZATION

In order to facilitate the application of the analyses and the results to each plant in the Westinghouse Owner's Group (WOG), the WOG plants were categorized based on certain characteristics that required distinction in order to assure that each plant would be fairly well represented by the analyses performed. Information from the Final Safety Analysis Reports (FSARs), Precautions, Limitations and Setpoints (PLSs), Technical Specifications, and other sources was collected for each plant and then the plants were categorized based on RHR System characteristics. The following sections describe the criteria used to categorize the WOG plants, the groupings that were established, and the lead plants selected for each group.

4.1 Criteria

The WOG plants were categorized based on criteria which would distinguish the plants. The grouping was based mainly on RHR System design. Operating practices at the plants were not utilized in the determination of the groupings. The plants were categorized into four groups based on the following characteristics: 1) number of RCS loops, 2) number of RHR hot leg suction lines, 3) RHR suction valve arrangement, and 4) RHR System design. The general criteria used to group the plants are discussed below:

1. Number of RCS loops - The plants were first categorized based on whether it was a two-loop, three-loop, or four-loop plant design. Plant response characteristics and design characteristics are usually grouped based on the number of RCS loops. This distinction was also made because the number of RHR inlet and outlet paths from and to the RCS are generally dependent on the number of loops available for suction and injection. Also, the success criteria used in the probabilistic portion of the analyses is dependent on the number of injection paths available.

2. Number of RHR Inlet Lines - This criterion is utilized to determine how many RCS hot leg suction paths to the RHR System are available. Some plants have one suction line while other plants have two separate suction lines while still another plant has three RHR inlet lines. This criterion impacts the reliability of the RHR System and the interfacing systems LOCA frequency.

3. RHR Suction Valve Arrangement - The WOG plants were distinguished based on the number of valves in each suction line and the ranges of autoclosure setpoints and open permissive setpoints.

4. RHR System Design - This criterion was the driving force in the categorization of the WOG plants. This criterion encompassed the above criteria and also provided information on train separation, the presence of crossties, the ability of the RHR System to be reconfigured given failure of a component in one train, the location of the CVCS letdown path (used to control the RCS pressure during cold shutdown), and the number and location of the RHR relief valves.

Information with regard to the above criteria was gathered for each WOG plant from available FSARs, PLSs, and other internal Westinghouse information. Table 4-1 shows the information collected for each plant involved in the program. The plants were then grouped based on these criteria as described in the following section.

4.2 Final Grouping

Of the 55 plants represented by the membership of the WOG Technical Specification Subcommittee, 43 of the plants have the RHRS autoclosure interlock feature and 12 plants do not have the RHRS autoclosure interlock feature. Eight plants chose not to participate in the program. The 43 plants having the ACI and participating in the program were categorized into four groups. A description of the distinguishing characteristics of each group and a list of the plants in each group is presented below.

Group 1

This group consists of four loop plants which have one RHRS suction line from the RCS with a single RHR relief valve located between the RHRS suction/isolation valves and the RHR pumps on the common drop line. The common drop line has both an inner and outer suction/isolation valve. Additionally, all the plants in this group have a cross-tie line connecting the two RHRS trains at a point between the RHR pump and the RHR heat exchanger. The cross-tie is significant since with this arrangement each RHR pump can feed either RHR heat exchanger for long term core cooling. Figure 4-1 shows the general RHRS design for Group 1.

The lead Plant for Group 1 is Salem Unit 1. A detailed description of the Salem Unit 1 RHRS is presented in Section 5.1 of this report. The plants in this group are:

D.C. Cook Unit 1
D.C. Cook Unit 2
Indian Point Unit 3
McGuire Unit 1
McGuire Unit 2
Salem Unit 1
Salem Unit 2
Sequoyah Unit 1
Sequoyah Unit 2
Watts Bar Unit 1
Watts Bar Unit 2
Zion Unit 1
Zion Unit 2

Group 2

This group consists of four loop plants which have a separate RHRS suction line from the RCS for each RHR train with one RHR relief valve located between the RHRS suction/isolation valves and the RHR pump on each train. Each drop line has both an inner and outer RHRS suction/isolation valve. The plants in this group do not have a cross-tie line connecting the RHRS trains at a point between the RHR pump and the RHR heat exchanger. The lack of this cross-tie is significant since with this arrangement each RHR pump can only feed its own RHR heat exchanger for long term core cooling. Figure 4-2 shows the general RHRS design for Group 2.

The South Texas Units differ from the other units in this group in that each of the South Texas Units has three independent trains of RHRS while the other plants in this group only have two. Millstone Unit 3 is similar to the other units except that it has added a third RHRS suction/isolation valve in each drop line. The third suction/isolation valve is not interlocked. Trojan Unit 1 differs from the other units in this group in the sense that it does not have multiple drop lines. These differences would be addressed in plant specific analysis should one of these plants reference this report. The general Group 2 results would be applicable to all plants in this group.

The lead plant for this group is Callaway Unit 1. A detailed description of the Callaway Unit 1 RHRS is presented in Section 5.2 of this report.

The plants in this group are:

- Braidwood Unit 1
- Braidwood Unit 2
- Byron Unit 1
- Byron Unit 2
- Callaway Unit 1
- Catawba Unit 1
- Catawba Unit 2
- Comanche Peak Unit 1
- Trojan Unit 1
- Seabrook Unit 1
- Vogtle Unit 1
- Vogtle Unit 2
- Wolf Creek Unit 1
- Millstone Unit 3
- South Texas Unit 1
- South Texas Unit 2
- Comanche Peak Unit 2

Group 3

Group 3 consists of both two and three loop plants and, with the exception of the Prairie Island Units, the plants selected in this group all have a single RHRS suction line from the RCS with one or more RHR relief valve located between the RHRS suction/isolation valves and the RHR pumps or at the discharge side of the RHRS heat exchanger. The Prairie Island plants have two drop lines that are headered together. Each drop line has both an inner and outer RHRS suction/isolation valve. All the plants in this group have a cross-tie line connecting the two RHRS trains at a point between the RHR pump and the RHR heat exchanger. The cross-tie is significant since with this arrangement each RHR pump can feed either RHR heat exchanger for long term core cooling. Figure 4-3 shows the general RHRS design for Group 3.

The lead plant for this group is North Anna Unit 1. A detailed description of the North Anna Unit 1 RHRS is presented in Section 5.3 of this report.

The plants in this group are:

H.B. Robinson Unit 2	Prairie Island Unit 1
Turkey Point 3	Prairie Island Unit 2
Turkey Point 4	North Anna Unit 1
Beaver Valley Unit 1	North Anna Unit 2

Group 4

Group 4 consists of three loop plants which have either one or two separate RHRS suction lines from the RCS with one RHR relief valve located between the RHRS suction/isolation valves and each RHR pump. Each drop line has both an inner and outer RHRS suction/isolation valve. The plants in this group do not have a cross-tie line connecting the two RHRS trains at a point between the RHR pump and the RHR heat exchanger. The lack of this cross-tie is significant since with this arrangement each RHR pump can only feed its own RHR heat exchanger for long term core cooling. Figure 4-4 shows the general RHRS design for Group 4.

The lead plant for this group is Shearon Harris Unit 1. A detailed description of the Shearon Harris Unit 1 RHRS is presented in Section 5.4 of this report.

The plants in this group are:

Farley Unit 1	Beaver Valley Unit 2
Farley Unit 2	V.C. Summer Unit 1
Shearon Harris Unit 1	

Plants Participating in the Program Without Autoclosure Interlock

The following four plants representing utilities supporting this report have indicated that they do not have an RHRS autoclosure interlock feature.

- Yankee Rowe
- Connecticut Yankee
- Surry Unit 1
- Surry Unit 2

YANKEE ROWE

The Yankee Rowe FSAR states that the unit has four motor operated isolation valves inside the vapor container which are key locked closed while the shutdown cooling system is not in use. The valves have no automatic interlock or actuation features.

CONNECTICUT YANKEE

The Connecticut Yankee FSAR states that the unit has remotely operated double valving to isolate the RHRS inlet and outlet piping from the RCS. All four of isolation valves have an open permissive interlock which prevents them from being opened when the RCS pressure exceeds RHRS design pressure. Key control switches provide administrative control against improper operation of the outboard set of valves.

SURRY UNITS 1 AND 2

The Surry updated FSAR indicates that the units have remotely operated double valving to isolate the RHRS inlet piping from the RCS. The isolation valves have an open permissive interlock which prevents it from being opened when the RCS pressure exceeds RHRS design pressure. The FSAR states that the entire RHRS is located inside of the containment, with the exception of the line penetrating the containment that connects to the RWST.

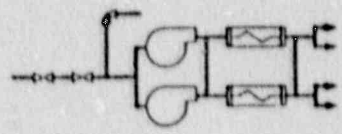
Plants Not Participating In The Program

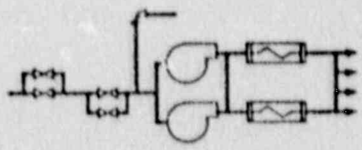
The following eight plants representing Utilities not supporting this report have indicated that they do not have an RHRS autoclosure interlock feature.

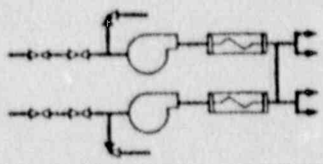
Ginna Unit 1	San Onofre Unit 1
Indian Point Unit 2	Kewaunee Unit 1
Point Beach Unit 1	Point Beach Unit 2
Diablo Canyon Unit 1	Diablo Canyon Unit 2

RHR GROUPING	PLANT	NO. LOOPS	# RHR INLET LINES	RHR OPERATING PARAMETERS	RHR ISOLATION VALVES	PREVENT OPEN SETPOINT	AUTOCLOSE SETPOINT	RHR RELIEF VAL SETPOINT/FLOWR
1	DC COOK 1	4	1 (HL LOOP 2)	400 PSIG 350 F	2 MOVS	369 PSIG	526 PSIG	450 PSIG 900 G
1	DC COOK 2	4	1 (HL LOOP 2)	400 PSIG 350 F	2 MOVS	369 PSIG	700 PSIG	450 PSIG 900 G
1	INDIAN PT 3	4	1 (HL LOOP 2)	400 PSIG 350 F	2 MOVS	450 PSIG	600 PSIG	450 PSIG 400 G
1	ZION 1	4	1 (HL LOOP 4)	425 PSIG 350 F	2 MOVS	425 PSIG	600 PSIG	450 PSIG 900 G
1	ZION 2	4	1 (HL LOOP 4)	425 PSIG 350 F	2 MOVS	425 PSIG	600 PSIG	450 PSIG 900 G
1	MCGUIRE 1	4	1 (HL LOOP 3)	425 PSIG 350 F	2 MOVS	385 PSIG	555 PSIG	450 PSIG 900 G
1	MCGUIRE 2	4	1 (HL LOOP 3)	425 PSIG 350 F	2 MOVS	385 PSIG	555 PSIG	450 PSIG 900 G
1	SALEM 1	4	1 (HL LOOP 1)	350 PSIG 350 F	2 MOVS	390 PSIG	570 PSIG	375 PSIG 840 G
1	SALEM 2	4	1 (HL LOOP 1)	350 PSIG 350 F	2 MOVS	390 PSIG	570 PSIG	375 PSIG 840 G
1	SEQUOYAH 1	4	1 (HL LOOP 4)	425 PSIG 350 F	2 MOVS	380 PSIG	700 PSIG	450 PSIG 900 G
1	SEQUOYAH 2	4	1 (HL LOOP 4)	425 PSIG 350 F	2 MOVS	380 PSIG	700 PSIG	450 PSIG 900 G
1	WATTS BAR 1	4	1 (HL LOOP 4)	400 PSIG 350 F	2 MOVS	380 PSIG	750 PSIG	450 PSIG 900 G
1	WATTS BAR 2	4	1 (HL LOOP 4)	400 PSIG 350 F	2 MOVS	425 PSIG	750 PSIG	450 PSIG 900 G
2	BRAIDWOOD 1	4	2 (HL LOOPS 1&3)	400 PSIG 350 F	2 MOVS	400 PSIG	700 PSIG	450 P-475 GPM
2	BRAIDWOOD 2	4	2 (HL LOOPS 1&4)	400 PSIG 350 F	2 MOVS	400 PSIG	700 PSIG	450 P-475 GPM
2	BYRON 1	4	2 (HL LOOPS 1&3)	400 PSIG 350 F	2 MOVS	400 PSIG	700 PSIG	450 P-475 GPM
2	BYRON 2	4	2 (HL LOOPS 1&3)	400 PSIG 350 F	2 MOVS	400 PSIG	700 PSIG	450 P-475 GPM
2	CALLAWAY	4	2 (HL LOOPS 1&4)	425 PSIG 350 F	2 MOVS	425 PSIG	750 PSIG	450 P-475 GPM
2	CATAWBA 1	4	2 (HL LOOPS B&C)	385 PSIG 350 F	2 MOVS	385 PSIG	600 PSIG	450 PSIG 900
2	CATAWBA 2	4	2 (HL LOOPS B&C)	385 PSIG 350 F	2 MOVS	385 PSIG	600 PSIG	450 PSIG 900
2	COMANCHE PEAK 1	4	2 (HL LOOPS 1&4)	425 PSIG 350 F	2 MOVS	425 PSIG	750 PSIG	450 PSIG 900
2	COMANCHE PEAK 2	4	2 (HL LOOPS 1&4)	425 PSIG 350 F	2 MOVS	425 PSIG	750 PSIG	450 PSIG 900
2	SEABROOK 1	4	2 (HL LOOPS 1&4)	365 PSIG 350 F	2 MOVS	365 PSIG	660 PSIG	450 PSIG 900
2	VOGTLE 1	4	2 (HL LOOPS 1&4)	400 PSIG 350 F	2 MOVS	425 PSIG	750 PSIG	450 PSIG 900
2	VOGTLE 2	4	2 (HL LOOPS 1&4)	400 PSIG 350 F	2 MOVS	425 PSIG	750 PSIG	450 PSIG 900
2	WOLF CREEK	4	2 (HL LOOPS 1&4)	425 PSIG 350 F	2 MOVS	425 PSIG	750 PSIG	450 P-475 GPM

?VE DESIGN ?ATE	COMS DESIGN CRITERIA # VALVES	COMMENTS	RHR SYSTEM DESIGN
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
?PM	2 PORVS		
375 F/675 G	2 PORVS		
375 F/675 G	2 PORVS		
375 F/675 G	2 PORVS		
375 F/675 G	2 PORVS		
375 F/770 G	2 PORVS & RHR RELIEF		
GPM	2 PORVS		
GPM	2 PORVS		
GPM	2 PORVS		
GPM	2 PORVS		
GPM	2 PORVS		
GPM	2 PORVS		
GPM	2 PORVS		
375 F/770 G	2 PORVS		







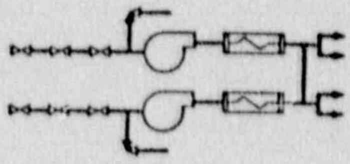
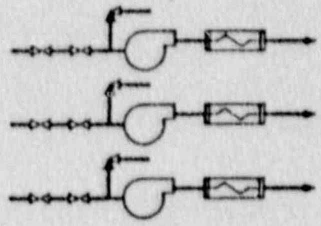
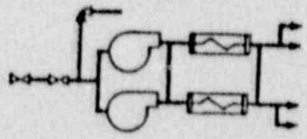
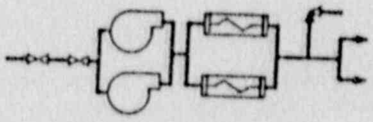
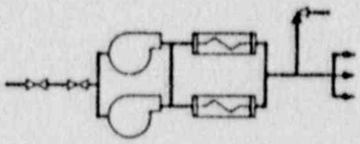
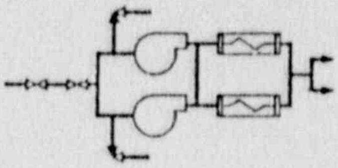
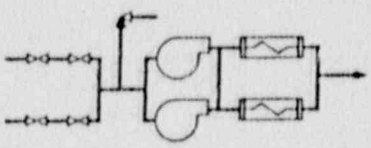
SI
APERTURE
CARD

Also Available On
Aperture Card

8911150026-01

RHR GROUPING	PLANT	NO. LOOPS	# RHR INLET LINES	RHR OPERATING PARAMETERS	RHR ISOLATION VALVES	PREVENT OPEN SETPOINT	AUTOCLOSE SETPOINT	RHR RELIEF VALVE SETPOINT/FLOWRAT
2	MILLSTONE 3	4	2 (HL LOOPS 1&4)	375 PSIG 350 F	2 MOVS/2INT	375 PSIG	750 PSIG	450 PSIG 800 GPM
2	SOUTH TEXAS 1	4	3 (HL LOOP 1,2,3)	350 PSIG 350 F	2 MOVS	350 PSIG	700 PSIG	600 PSIG 810 GPM
2	SOUTH TEXAS 2	4	3 (HL LOOP 1,2,3)	350 PSIG 350 F	2 MOVS	350 PSIG	700 PSIG	600 PSIG 810 GPM
2	TROJAN	4	1 (HL LOOP 4)	400 PSIG 350 F	2 MOVS	425 PSIG	600 PSIG	450 PSIG 900 GPM
3	BEAVER VALLEY 1	3	1 (HL LOOP 1)	400-450 P 350 F	2 MOVS	425 PSIG	600 PSIG	600 PSIG 1133 GP
3	HB ROBINSON 2	3	1 (HL LOOP 2)	450 PSIG 350 F	2 MOVS	465 PSIG	465 PSIG	600 PSIG 500 GPM
3	TURKEY POINT 3	3	1 (HL LOOP A)	450 PSIG 350 F	2 MOVS	465 PSIG	465 PSIG	600 PSIG 500 GPM
3	TURKEY POINT 4	3	1 (HL LOOP A)	450 PSIG 350 F	2 MOVS	465 PSIG	465 PSIG	600 PSIG 500 GPM
3	NORTH ANNA 1	3	1 (HL LOOP 1)	450 PSIG 350 F	2 MOVS	418 PSIG	582 PSIG	467 PSIG 900 GPM
3	NORTH ANNA 2	3	1 (HL LOOP 1)	450 PSIG 350 F	2 MOVS	418 PSIG	582 PSIG	467 PSIG 900 GPM
3	PRAIRIE ISLAND 1	2	2 (HL LOOP 1 & 2)	425 PSIG 350 F	2 MOVS	425 PSIG	600 PSIG	500 PSIG 607 GPM
3	PRAIRIE ISLAND 2	2	2 (HL LOOP 1 & 2)	425 PSIG 350 F	2 MOVS	425 PSIG	600 PSIG	500 PSIG 607 GPM

(Continued)

DESIGN E	COMS DESIGN CRITERIA # VALVES	COMMENTS	RHR SYSTEM DESIGN
	2 PORVS		
	2 PORVS 2 PORVS		
	2 PORVS		
	2 PORVS	LOCATED IN CONTAIN.	
	2 PORVS		
	2 PORVS 2 PORVS	LOCATED IN CONTAIN. LOCATED IN CONTAIN.	
	2 PORVS 2 PORVS		

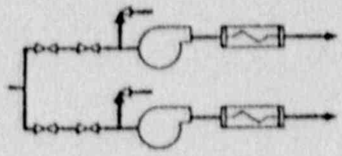
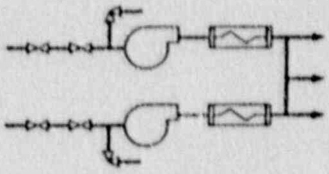
RHR GROUPING	PLANT	NO. LOOPS	# RHR INLET LINES	RHR OPERATING PARAMETERS	RHR ISOLATION VALVES	PREVENT OPEN SETPOINT	AUTOCLOSE SETPOINT	RHR RELIEF VALV SETPOINT/FLOWRA
4	BEAVER VALLEY 2	3	1 (2) (HL LOOP 1)	400 PSIG 350 F	2 MOVS	360 PSIG	700 PSIG	450 PSIG 900 GP
4	FARLEY 1	3	2 (HL LOOP 1&3)	425 PSIG 350 F	2 MOVS	402 PSIG	700 PSIG	450 PSIG 475 GP
4	FARLEY 2	3	2 (HL LOOP 1&3)	425 PSIG 350 F	2 MOVS	402 PSIG	700 PSIG	450 PSIG 475 GP
4	SHEARON HARRIS	3	2 (HL LOOP 1&3)	425 PSIG 350 F	2 MOVS	363 PSIG	700 PSIG	450 PSIG 900 GP
4	V C SUMMER	3	2 (HL LOOP 1&3)	425 PSIG 350 F	2 MOVS	425 PSIG	700 PSIG	450 PSIG 900 GP

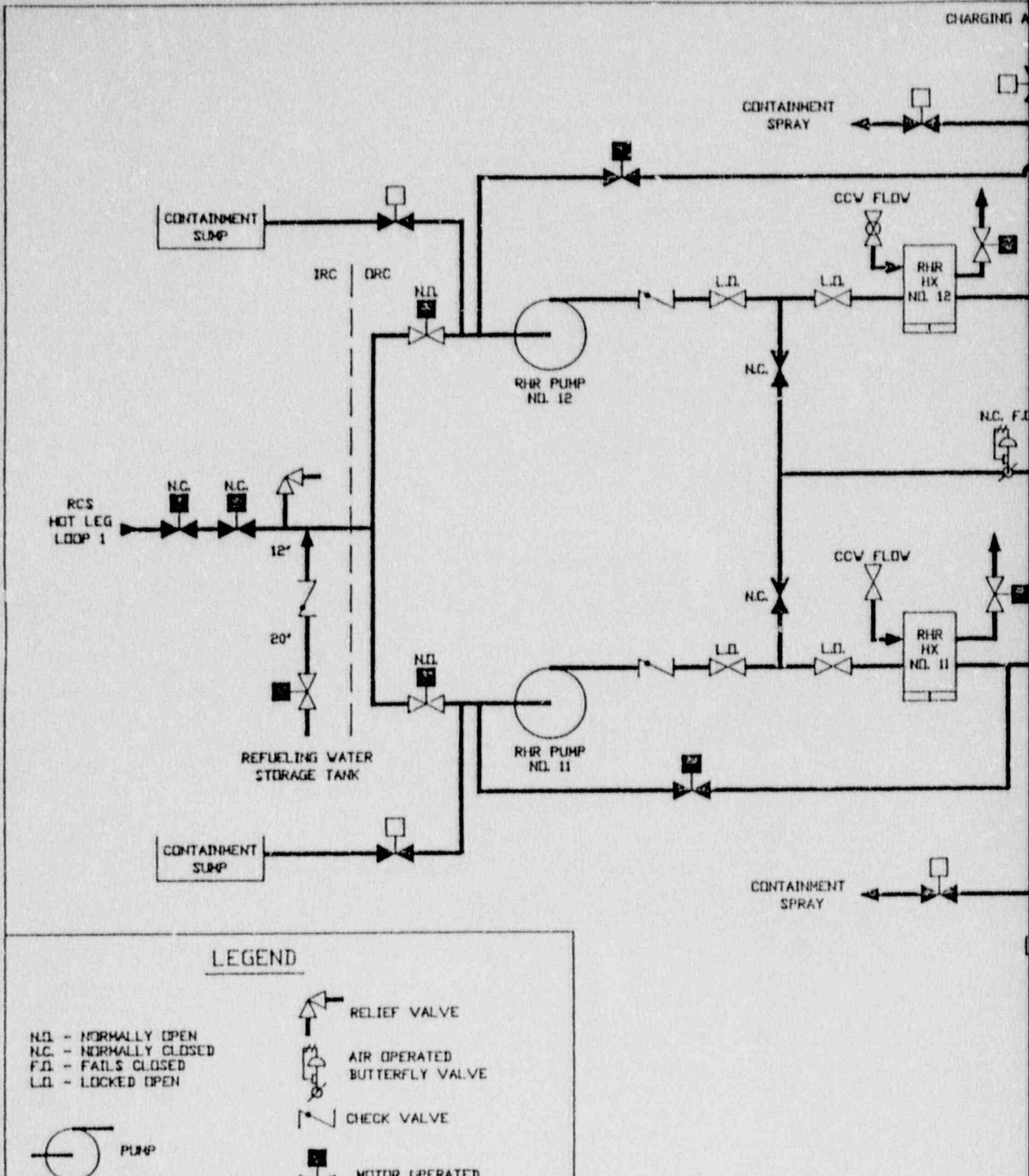
PARTICIPATING PLANTS WITHOUT AUTO CLOSURE FEATURE

YANKEE ROWE
CONN YANKEE
SURRY 1
SURRY 2

PLANTS NOT IN PROGRAM

GINNA
SAN ONOFRE 1
POINT BEACH 1&2
KEWAUNEE
DIABLO CANYON 1&2
INDIAN POINT 2

E DESIGN	COMS DESIGN CRITERIA	COMMENTS	RHR SYSTEM DESIGN
TE	8 VALVES		
	2 PORVS	LOCATED IN CONTAIN.	
1	RHR RELIEF VALVES		
1	RHR RELIEF VALVES		
1	2 PORVS		
1	RHR RELIEF VALVES		



RESIDUAL HEAT

FIGU

1/16/88

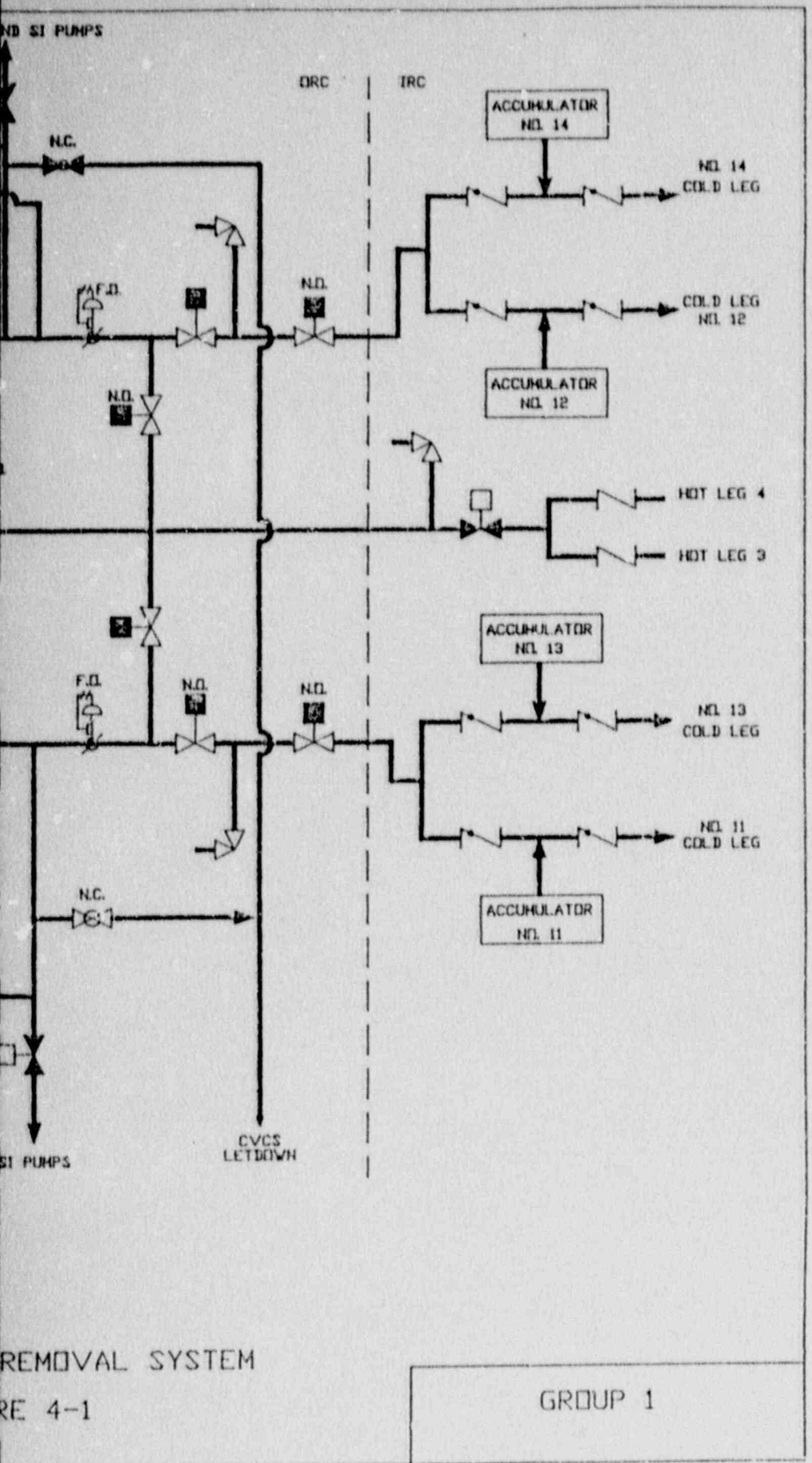


Figure 4-1

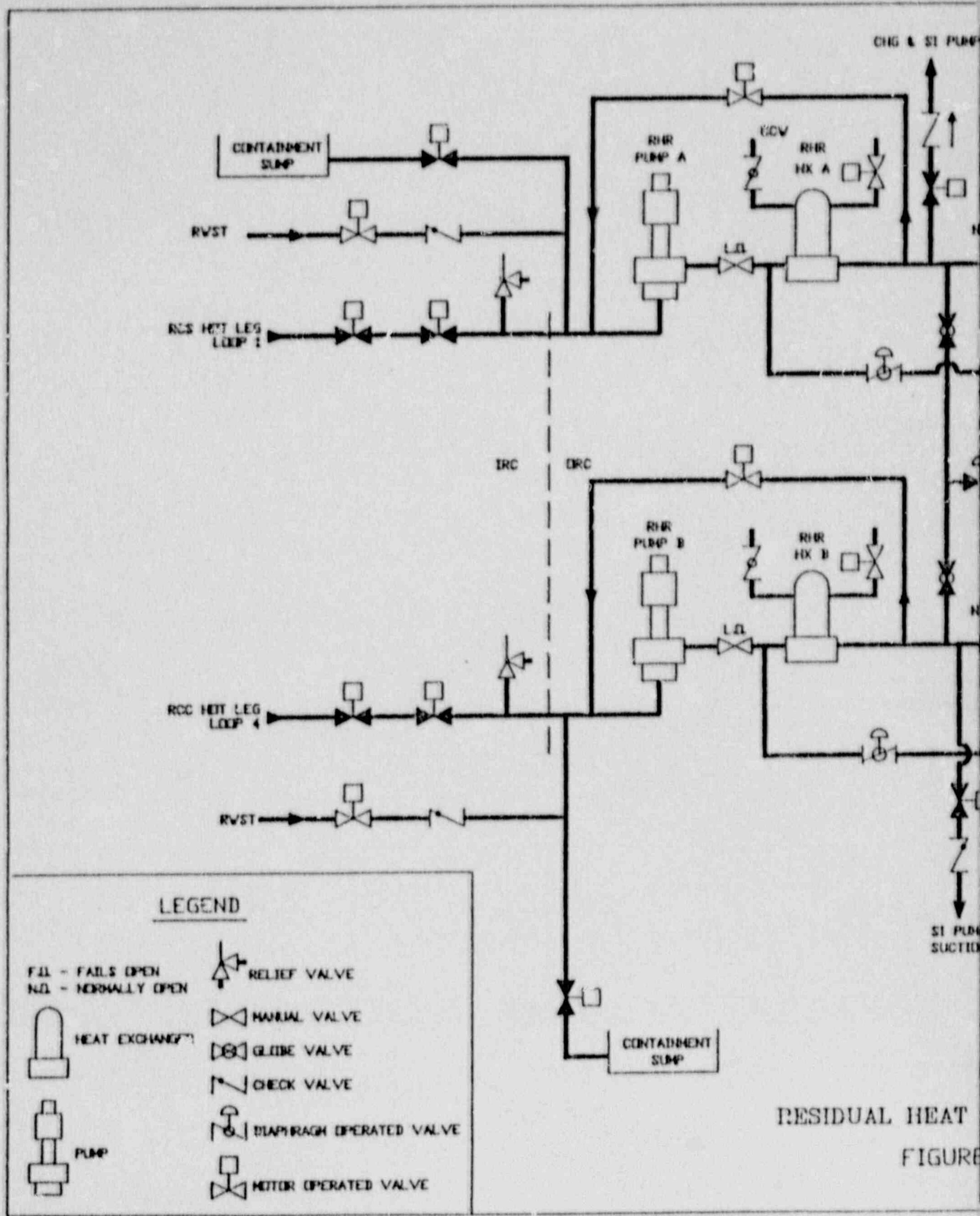
General RHR Design

For Group 1 Plants

SI
APERTURE
CARD

Also Available On
Aperture Card

8911150026-04

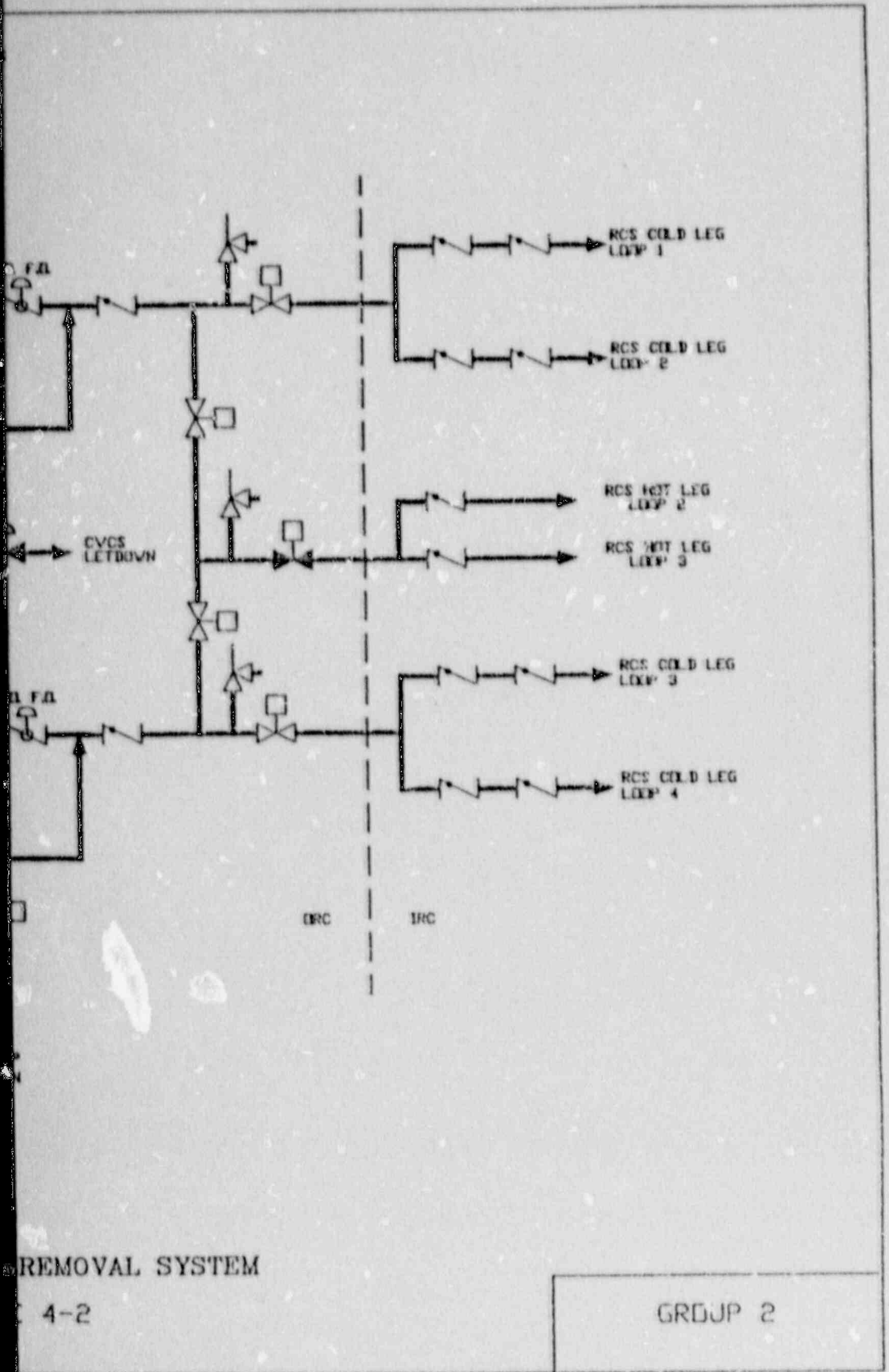


RESIDUAL HEAT

FIGURE

RHRCALM

2/11/88



SI
APERTURE
CARD

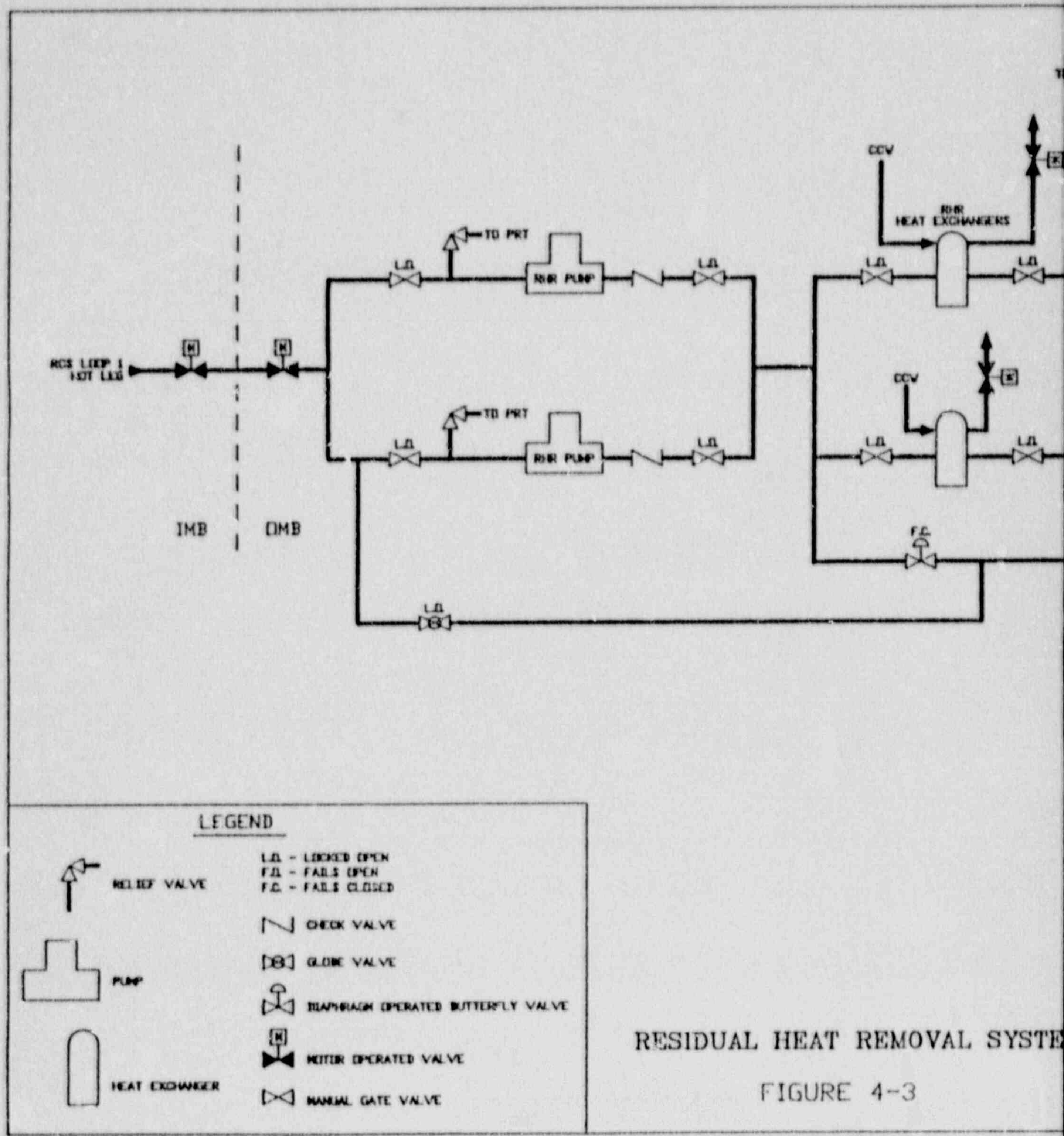
Also Available On
Aperture Card

Figure 4-2.

General RHR Design

For Group 2 Plants

8911150026-05



RESIDUAL HEAT REMOVAL SYSTE

FIGURE 4-3

RHR_NA

2/11/88

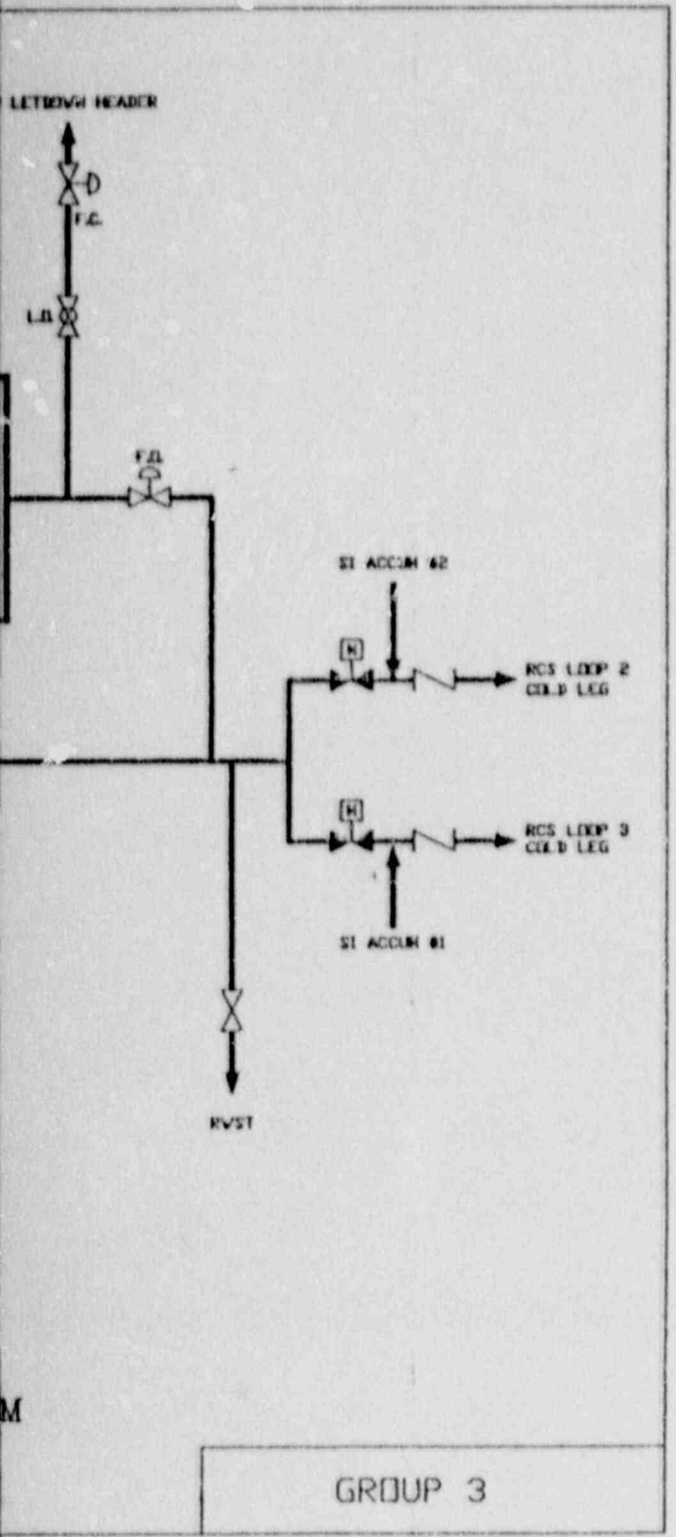
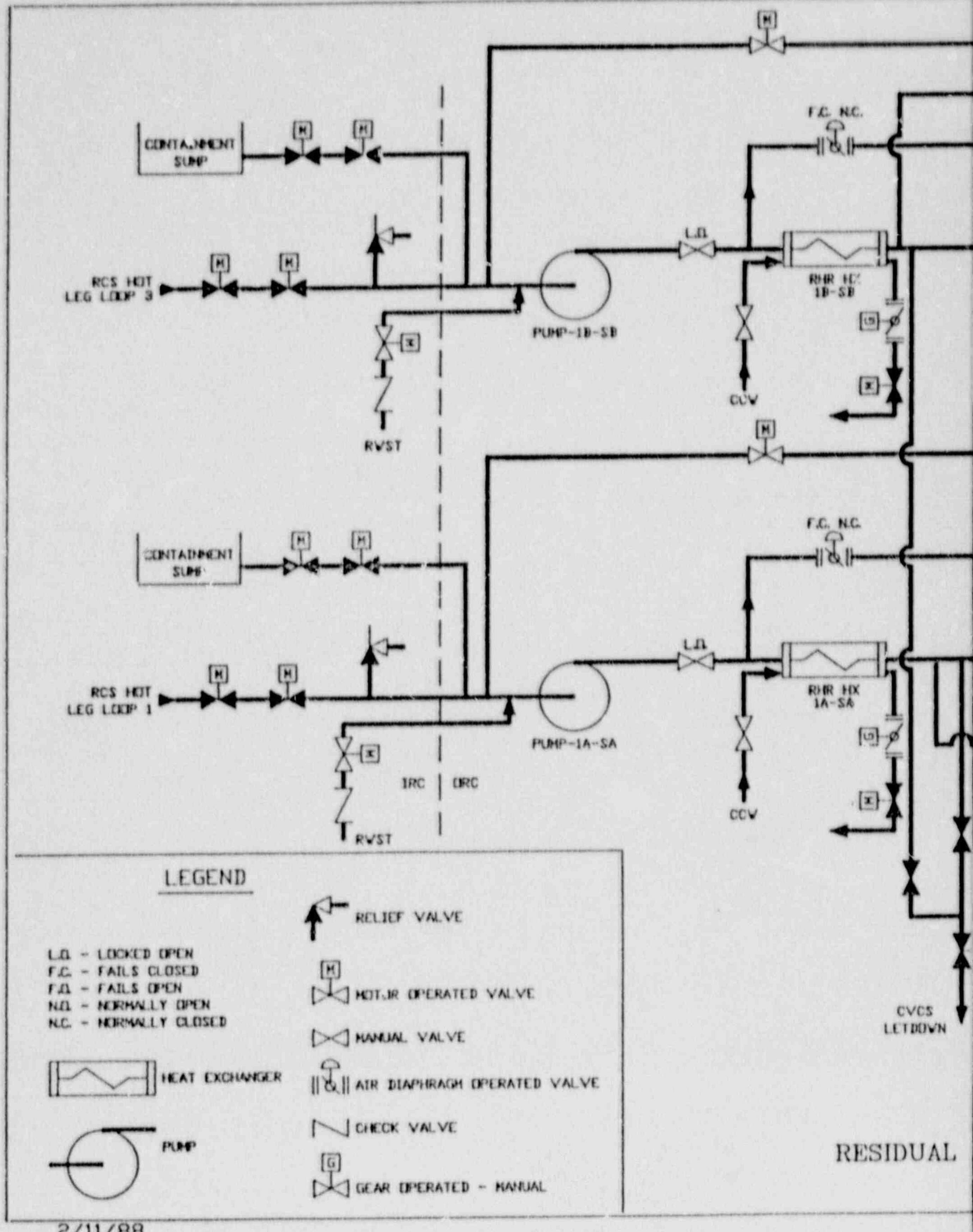


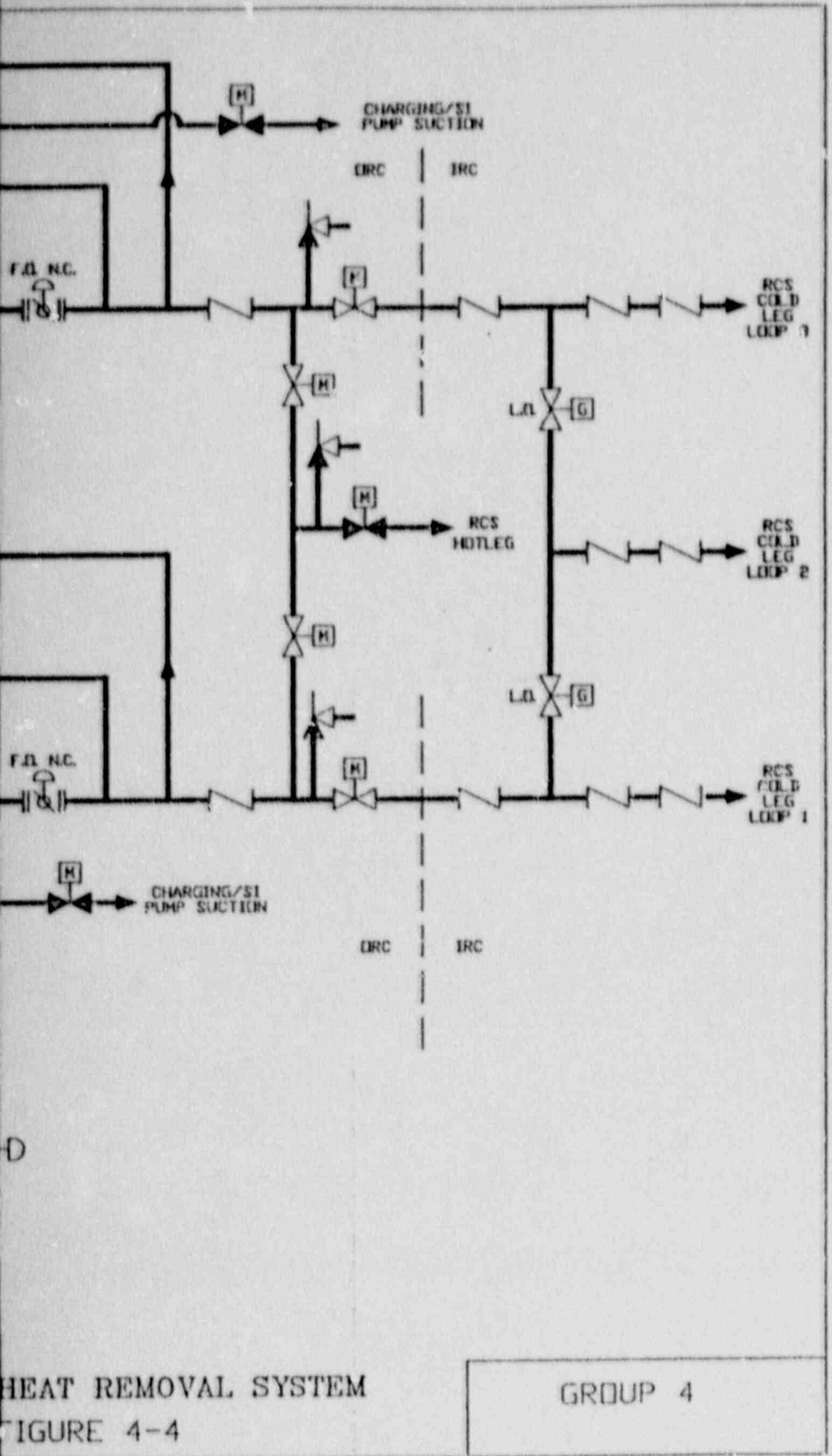
Figure 4-3.

General RHR Design For Group 3 Plants


CONTAINMENT SUMP
RCS HOT LEG LOOP 3
RWST
PUMP-1B-SB
L.O.
F.C. N.C.
RHR HX 1B-SB
CCW
CONTAINMENT SUMP
RCS HOT LEG LOOP 1
RWST
IRC
ORC
PUMP-1A-SA
L.O.
F.C. N.C.
RHR HX 1A-SA
CCW
CVCS LETDOWN
LEGEND
L.O. - LOCKED OPEN
F.C. - FAILS CLOSED
F.O. - FAILS OPEN
N.O. - NORMALLY OPEN
N.C. - NORMALLY CLOSED
HEAT EXCHANGER
PUMP
RELIEF VALVE
MOTOR OPERATED VALVE
MANUAL VALVE
AIR DIAPHRAGM OPERATED VALVE
CHECK VALVE
GEAR OPERATED - MANUAL
RESIDUAL

RHR_SH

2/11/88



SI
APERTURE
CARD

Also Available On
Aperture Card

Figure 4-4.

General RHR Design For Group 4 Plant

8911150026-07

5.0 LEAD PLANT DESCRIPTIONS

The following sections provide a general description of each lead plant and describe in detail each lead plant's RHRS. Included in the RHRS description is a discussion of the RHR System operation during the various reactor operating modes from refueling through cold shutdown and power operation. A detailed description of the major RHRS components is provided along with the plant specific setpoints and normal valve positions. Valve identification includes both the plant-specific tag number and the Westinghouse valve number. In addition, a description of each lead plant's current interlocks is presented along with a detailed discussion of the RHRS suction/isolation valve description down to the relay level. The intent of this section is to provide sufficient detail to support the probabilistic analysis presented in Section 7 of this report.

5.1 Salem Unit 1

The following sections provide a description of the Group 1 lead plant, Salem Unit 1.

5.1.1 General Description

Salem Units 1 & 2 are essentially identical Westinghouse PWRs. The unit was granted a full power operating license on June 4, 1977. The Nuclear Steam Supply System (NSSS) consists of a 3411 MWt core with four (4) reactor coolant loops. Each loop contains a Westinghouse Model 51 improved steam generator and a Westinghouse Model 93A reactor coolant pump.

The containment is a reinforced concrete structure with a cylindrical wall, a hemispherical dome, and a flat foundation slab. The inside surface of the structure is lined with carbon steel plates welded together to form a barrier which is essentially leak tight.

The power conversion system consists of a Westinghouse tandem-compound turbine having one high-pressure and three low-pressure elements. Design output is 1090 MWe (net), and steam dump to the condenser is rated at 40-percent full load. Four main steam lines carry steam from the top of the steam generators, through four main steam isolation valves (one in each line), to the turbine stop valves at the inlet to the turbine generator. Each main steam line is also equipped with five code safety valves and one power-operated relief valve.

Emergency Core Cooling System (ECCS) components include 4 cold leg accumulators, 2 centrifugal charging pumps (CHG/HHSI), 2 safety injection pumps, 2 residual heat removal pumps (RHR/LHSI) and associated valves and piping. Three redundant onsite emergency diesels assure electric power supply to vital equipment. The borated refueling water storage facility consists of a large outside storage tank (RWST) which is the suction source for the ECCS pumps during the injection phase.

5.1.2 Residual Heat Removal System

Function

The primary function of the Residual Heat Removal System (RHRS) is to remove decay heat from the core and Reactor Coolant System (RCS) during plant cooldown and refueling operations. The RHRS transfers heat from the RCS to the Component Cooling Water System (CCWS) to reduce reactor coolant temperature to the cold shutdown temperature. The cold shutdown temperature is maintained until the plant is started up again.

The RHRS also serves as part of the Safety Injection System (SIS) to provide Low Head Safety Injection (LHSI) emergency core cooling in the event of a break in either the RCS or steam system. Also, since the containment spray pumps do not take suction from the containment sump, the RHR/LHSI pumps continue containment spray during the post-accident recirculation phase, if required. As a secondary function, the RHRS is used to transfer refueling water between the Refueling Water Storage Tank (RWST) and the refueling cavity before and after refueling operations.

Overview

A basic flow diagram of the RHRS is shown in Figure 5-1. The RHRS consists of two separate RHR trains of equal capacity, each independently capable of meeting the safety analysis design bases. Each train consists of one heat exchanger, one motor-driven pump and the associated piping, valves and instrumentation necessary for operational control. The inlet line to each train of the RHRS is connected to a common letdown line from the hot leg of reactor coolant loop 1, while the return lines are connected to the cold legs of all four reactor coolant loops via the SIS accumulator discharge lines (downstream of the cross-connect, train A discharges to loops 1 and 3, and train B discharges to loops 2 and 4).

The RHRS is normally isolated from the RCS by two, series, motor-operated, suction/isolation valves in the single letdown line connecting the low pressure RHRS to the high pressure RCS. The RHRS discharge lines are isolated from the RCS by two check valves in series for each line. The RHRS suction/isolation valves, the inlet line pressure relief valve, the return lines to the RCS cold legs downstream of valves 11SJ49/12SJ49 (8809A/B) and the hot leg injection lines from valves 1RH25 (8708) and 1RH26 (8703) are located inside containment while the remainder of the system is located outside containment.

During normal RHR System operations, reactor coolant flows from RCS hot leg 1 to the RHR pumps, through the tube side of the RHR heat exchangers and back to the RCS cold legs through the safety injection accumulator discharge lines. The reactor coolant heat is transferred by the RHR heat exchangers to the component cooling water which circulates through the shell side of the RHR heat exchangers.

Coincident with RHRS normal cooldown operations, a portion of the reactor coolant flow may be diverted from downstream of the RHR heat exchangers to the Chemical and Volume Control System (CVCS) low-pressure letdown line for cleanup and/or pressure control. By regulating the diverted flowrate and the charging flow, the RCS pressure can be controlled during water solid plant operations. Pressure regulation is necessary to maintain the pressure range dictated by the reactor vessel fracture prevention criteria requirements and by the RCP No. 1 seal differential pressure and NPSH requirements.

The RCS cooldown rate is manually controlled by regulating both the reactor coolant flow through the tube side of the RHR heat exchangers and the reactor coolant flow bypassing the heat exchangers. Instrumentation is provided to monitor system pressure, temperature and total flow.

System Operation

A discussion of RHRS operation during various reactor operating modes follows:

Reactor Startup

Generally, during cold shutdown, the RHRS operates to remove residual heat from the reactor core. The number of pumps and heat exchangers in service depends on the RHRS heat load at the time. At initiation of plant startup, the RCS is completely filled (water-solid), and the pressurizer heaters are energized. At least one RHR pump is operating with a portion of its discharge directed to the CVCS for purification and/or pressure control via a line that is connected to a cross-connect header downstream of the RHR heat exchanger. Once a steam bubble is formed in the pressurizer, the RHRS is isolated, and RCS pressure/ inventory control are provided by the pressurizer spray, pressurizer heaters, normal letdown and charging systems.

Power Generation and Hot Standby Operation

The RHRS is not used during hot standby or power operations when the RCS is at normal pressure and temperature. Under these conditions, the RHRS is aligned for operation as part of the ECCS. Upon initiation of a safety injection signal ("S" signal), the RHR pumps take suction from the

RWST and inject borated water into the reactor vessel via the Safety Injection System accumulator cold leg injection headers. When the water in the RWST is depleted, the RHR pumps are manually aligned to take suction from the containment recirculation sump. The RHR heat exchangers then cool the sump fluid being recirculated by the RHR pumps and deliver the cooled water to the reactor vessel cold legs. Hot leg recirculation is initiated approximately 22.5 hours after the accident following ECCS initiation. The flow path for this condition consists of both RHR pumps taking suction from the recirculation sump, with one pump discharging through its discharge cross connect valve and common discharge valve to the RCS hot legs 3 and 4. The RHR pumps (being the only ECCS pumps which take suction directly from the sump) also feed the suctions of the safety injection pumps and the CHG/HHSI pumps and continue containment spray (if required) during the post-accident recirculation phase.

Reactor Shutdown

With the RCS borated to the cold shutdown concentration (approximately 2000 ppm), the initial phase of reactor cooldown is accomplished by transferring heat from the RCS to the Steam and Power Conversion System (SPCS) through the use of the RCS steam generators and the SPCS steam dump valves or the SPCS atmospheric power-operated relief valves. When the reactor coolant nominal temperature and pressure are reduced to 350°F and less than 360 psig, approximately 4 hours after reactor shutdown, the second phase of cooldown starts with the RHRS being placed in operation.

The reactor cooldown rate is limited by RCS equipment cooling rates based on allowable stress limits, as well as the operating temperature limits of the Component Cooling Water System (CCWS). As the reactor coolant temperature decreases, the reactor coolant flow through the RHR heat exchangers is increased to maintain a constant cooldown rate.

As cooldown continues, the pressurizer is filled with water and the RCS is operated in the water-solid condition. At this stage, pressure is controlled by regulating the charging flow rate and the letdown rate to the CVCS from the RHRS. After the Reactor Coolant System is depressurized, cooled to ≤140°F, and purged to reduce dissolved hydrogen concentration to a safe level, the reactor vessel head may be removed for refueling or maintenance.

Refueling

One RHR pump is utilized during refueling to transfer borated water from the RWST to the refueling cavity. During this operation, the isolation valves in the inlet line of the RHRS are closed, and the isolation valves from the refueling water storage tank are opened. After the water level in the refueling cavity reaches normal refueling level, the inlet isolation valves are opened, the RWST supply valves are closed, and normal RHRS operation resumes.

During refueling, the RHRS remains in service with the number of pumps and heat exchangers in operation as required by the heat load and plant technical specifications. Additionally, a portion of the RHRS flow is directed to the CVCS for purification and eventual return to the RCS via the charging system.

Following refueling, an RHR pump drains the refueling cavity to the top of the reactor vessel flange by pumping water from the RCS to the RWST.

<u>Component Description</u>

This section describes the major components of the RHR System.

RHR Pumps

Two pumps are installed in the RHR System. The pumps are sized to deliver sufficient reactor coolant flow through the RHR heat exchangers to meet the plant cooldown requirements. The use of two pumps ensures that cooling capacity is only partially lost should one pump become inoperable.

The RHR pumps are protected from overheating and loss of suction flow by miniflow bypass lines, located on the heat exchanger outlet, that diverts part of the flow back to the pump suction. A control valve located in each miniflow line is regulated by a signal from the flow transmitters located in each pump discharge header. The control valves open to divert flow back to the pump suction when the discharge flow is less than 500 gpm and close when it exceeds 1000 gpm. This arrangement ensures that the RHR pump does not overheat or vibrate when the discharge line is closed or when the RCS pressure exceeds the pump shutoff head.

A pressure transmitter in each pump discharge header provides pressure indication with a high pressure alarm in the main control room.

The two RHR pumps are vertical, centrifugal units with mechanical shaft seals. All pump surfaces in contact with reactor coolant are austenitic stainless steel or equivalent corrosion resistant material.

RHR Heat Exchangers

Two RHR heat exchangers are installed in the RHRS. The heat exchanger design is based on heat load and temperature differences between reactor coolant and component cooling water existing 20 hours after reactor shutdown when the temperature difference between the two systems is small. The installation of two heat exchangers ensures that the heat removal capacity of the system is only partially lost if one heat exchanger becomes inoperative. The heat exchangers are of the shell and U-tube type. Reactor coolant circulates through the tubes, while component cooling water circulates through the shell. The tubes are welded to the tubesheet to prevent leakage of reactor coolant.

RHRS Valves

The following sections describe the Salem Unit 1 RHRS valves. To facilitate other plants in this grouping referencing this discussion, corresponding Westinghouse valve I.D. numbers are provided in parentheses.

Inlet Isolation Valves 1RH-1 (8702) and 1RH-2 (8701)

These valves are motor-operated, gate valves which are normally-closed except when the RHRS is in operation. Both valves are provided with a manual control (open/closed) on the main control board and will fail in the "as-is" position.

Valve 1RH-1 (8702) is interlocked with RCS pressure transmitter PT-403 and valve 1RH-2 (8701) is interlocked with PT-405. These interlocks prevent the inadvertent opening of the valves when RCS pressure is above 360 psig. The valves also close automatically when RCS pressure is higher than 580 psig. A more detailed description of the interlocks is provided in Section 5.1.3.

Pump Suction Isolation Valves 11RH-4 (8700A) and 12RH-4 (8700B)

These valves are motor-operated, gate valves which are normally-open except when the RHRS is used as part of the SIS during the recirculation phase following a LOCA. An interlock is provided between valve 11RH-4 (8700A) and its associated RHR pump suction line to containment sump isolation valve 11SJ44 (8982A) to prevent opening of the pump suction valve without closing the sump line. 12RH-4 (8700B) is similarly interlocked with 12SJ44 (8982B).

Heat Exchanger Flow Control Valves 11RH-18 (HCV-638) and 12RH-18 (HCV-640)

The reactor coolant flow rate through the RHR heat exchangers is adjusted by air-operated, butterfly, discharge valves 11RH-18 (HCV-638) and 12RH-18 (HCV-640). Positioning of these valves from the control room regulates the reactor coolant flow and temperature exiting the heat exchangers. These valves are normally full open during power operation.

Bypass Flow Control Valve 1RH-20 (HCV-670)

This valve, located in the common heat exchanger bypass line, is an air-operated, butterfly valve which may be positioned from the main control room. By adjusting this valve, the bypass flow around the RHR heat exchangers may be changed to regulate the return flow temperature, and in conjunction with valves 11RH-18 (HCV-638) and 12RH-18 (HCV-640) the total return flow.

Miniflow Stop Valves 11RH-29 (FCV-641A) and 12RH-29 (FCV-641B)

These normally-closed valves are motor-operated globe valves which are located in the residual heat removal pump miniflow line. This miniflow line ensures that the RHR pump does not overheat or vibrate when the discharge line is closed or when RCS pressure exceeds the pump shutoff head. The valves are controlled by flow transmitters FIC-641A and FIC-641B, respectively, which are located in the RHR pump discharge line. These valves will open when their respective pumps are operating, and the flow is less than 500 gpm. When the pump flow exceeds 1000 gpm, or a residual heat removal pump stops, the corresponding valve will close.

Loop Isolation Valves 11RH-19 (8716A) and 12RH-19 (8716B)

These motor-operated stop valves, located in the piping crosstie downstream of the residual heat exchangers, are open during both normal plant and RHRS operation. They allow RHRS flow from both trains to inject to all 4 cold legs during ECCS injection. These valves are closed during the post-accident recirculation phase to provide system separation for passive failure protection. Additionally, they provide a flow path to return water to the RWST during refueling operations and injection to loops 3 and 4 hot legs during ECCS hot leg recirculation. These valves are controlled from the main control board and fail "as is."

RHRS Return Line Check Valves 11SJ43 (8818A), 12SJ43 (8818B), 13SJ43 (8818C) and 14SJ43 (8818D)

One check valve is located in each branch of the RHRS return line to prevent backflow from the safety injection pumps, and to serve as a backup in the event of leakage of the check valves on the SIS Accumulator cold leg injection lines.

Accumulator Cold Leg Injection Line Check Valves 11SJ56 (8948A), 12SJ56 (8948B), 13SJ56 (8948C) and 14SJ56 (8948D)

There is one check valve in each accumulator cold leg discharge line segments (closest to the RCS and in common with the RHRS/LHSI and safety injection pumps discharge paths) which serves as an RCS pressure boundary valve and prevents backflow to the ECCS.

Gate Valve 11SJ49 (8809A) and 12SJ49 (8809B)

There is an eight-inch, normally-open, motor-operated, gate valve in each parallel discharge line from the residual heat removal pump, downstream of the heat exchanger and discharge crosstie header. These valves are used to isolate the RHRS from the cold legs during hot leg recirculation or during refueling operations when returning water to the RWST.

Crosstie Valves 11RH17 (8734A) and 12RH17 (8734B)

These two, normally-closed, manual valves are used to line up a portion of the RHR pump discharge to be directed to the CVCS. This flow path is used during a plant cooldown and during water solid plant operations where the CVCS is used for RCS pressure control and purification.

Gate Valve 1RH105 (8804A)

Gate Valve 1RH105 (8804A) isolates a flow path from the RHR/LHSI pump (downstream of the RHR heat exchanger) to the safety injection pump during recirculation. 1RH105 (8804A) is normally-closed and is interlocked with the RHRS suction isolation valves (see section 5.1.3), the SI pump miniflow valves, and the sump isolation valves.

Gate Valve 12SJ45 (8804B)

Gate Valve 12SJ45 (8804B) isolates a flow path off the discharge of the RHR heat exchanger No. 2, which supplies water to the suction of the centrifugal charging pumps and safety injection pumps during the recirculation phase of safety injection. 12SJ45 (8804B) is normally-closed and is interlocked with the RHRS suction/isolation valves (see Section 5.1.3), the SI pump miniflow valves, and the sump isolation valves.

Gate Valve 1RH-26 (8703)

During hot leg recirculation RHR pumps are realigned to discharge through discharge cross connect valves 11RH-19 (8716A) and 12RH-19 (8716B), and common discharge valve 1RH-26 (8703). This realignment is initiated at approximately 22.5 hours after the accident and ECCS initiation. Hot leg recirculation prevents crystallization of boric acid in the core and quenches the steam bubble in the top of the core.

RWST Isolation Valves 1SJ69 and 1SJ70 (8980 and 8981)

Check valve 1SJ70 (8981) and gate valve 1SJ69 (8980) are located in the common suction line from the RWST to the RHR/LHSI pumps. These valves isolate the RWST from the RHRS during normal cooldown and post-accident recirculation operations.

Sump Isolation Valves 11SJ44 and 12SJ44 (8982A and 8982B)

There is one motor-operated gate isolation valve in each RHR/LHSI pump suction line from the sump. These valves are interlocked with 11RH-4 and 12RH-4 (8700A/B).

Containment Spray Header Isolation Valves 11CS36 and 12CS36 (9003A and 9003B)

These valves isolate the flow paths from the RHRS/LHSI pumps discharges to the containment spray headers. This path allows the RHR/LHSI pumps to continue containment spray following the switchover operations to recirculations. These valves are interlocked with the RHR suction isolation valves and the sump isolation valves.

RHRS Discharge Relief Valves 11SJ48, 12SJ48 and 1RH25 (8856A/B and 8708)

A relief valve is located in each RHR/LHSI cold leg and hot leg injection header. These valves protect against overpressurization of the piping due to any RCS backleakage or thermal expansion of trapped water.

Relief Valve 1RH-3 (8707)

There is one, 3-inch relief valve (inside containment) in the RHR pumps common suction line from the RCS hot leg. The valve is located immediately downstream of the RHRS suction/isolation valve 1RH-2 (8701). This relief valve prevents RHRS overpressurization by discharging to the Pressurizer Relief Tank when pressures within the RHRS suction line exceed 375 psig. These valves have a design capacity of 840 gpm at the 375 psig setpressure.

5.1.3 Currant RHRS Suction Isolation Valves Interlocks and Functional Requirements

The following sections provide a description of the Salem suction/isolation valve interlocks and valve control circuits.

5.1.3.1 Currant Interlocks

There are two, normally-closed, motor-operated, series, isolation valves in the RHR pump suction line from the RCS hot leg. The valve, 1RH-1 (8701), located inside the missile barrier is designed as the inner isolation valve, while the valve outside the missile barrier, 1RH-2 (8702), is designated as the outer isolation valve. The interlock features provided for the inner isolation valve are identical to those provided for the outer isolation valve.

Each valve is interlocked against opening unless the following condition is met:

1. The RCS pressure, as measured by the appropriate pressure channels, is less than 390 psig. This assures that the RHRS cannot be overpressurized by aligning it to the RCS when RCS pressure plus RHRS pump head would exceed the RHRS design pressure.

In addition to the above interlock feature, the suction isolation valves are also interlocked to automatically close on increasing RCS pressure greater than 700 psig.

The current interlocks for valves 1RH-1 (8702) and 1RH-2 (8701) are shown functionally on Figures 5-2 and 5-3.

5.1.3.2 RHRS Common Suction Isolation Valve Description

The RHR common suction isolation valves are motor-operated valves that can be opened or closed from the main control board. The valves will automatically close on increasing reactor coolant system pressure. On decreasing reactor coolant system pressure, the valve control circuit receives an interlock signal that allows the valve to be opened using the main control board switch. On reactor coolant pressure above the setpoint, the valve control circuit is disabled and the valve cannot be opened.

The valve control circuit consists of control switches, limit switches, contactors, relays, indicating lights, a 3 phase, 230 VAC motor and a pressure control loop. The control switches are located in the main control room. The limit switches are located in the valve motor operator and provide indication of the position of the valve. Relays are used for providing control signals. The contactor, located in the motor control center, is switched on and off to provide the power to the valve motor to change the position of the valve. The contactor also provides contacts that are used in the valve control circuit. There are red and green indicating lights are on the Main Control Board to show the valve's position. The valve motor operator is located at the valve and is used to change the position of the valve. The pressure control loop measures Reactor Coolant System pressure and provides output signals to the valve control circuit, based on the RCS pressure, that allows the valve to be opened from the control switch or automatically closed.

The following provides a detailed description of the valve control circuit for 1RH-1. Operation of valve 1RH-2 is similar. Figures 5-4 and 5-5 show the appropriate detail of the circuits.

Closing the Valve from the Main Control Room

With the valve in the full open position, the valve can be closed from the control switch in the main control room as described in the following steps:

1. Placing the control board switch to the CLOSE position will pick up closing relay coil 5/CSV2. When relay 5/CSV2 picks up, the associated relay contact closes in the valve closing control circuit. This relay contact is in series with a limit switch contact (33/CVO), which is closed when the valve is open, a limit switch contact (33/OVC), which is closed when the valve is open, and a contactor contact (9/O) which is closed when the opening contactor is not energized.

2. With all the contacts in Step 1 closed, the closing contactor (9/C) is now energized with 118 VAC power from the 230/118 VAC control power step down transformer. The closing contactor contact (9/C) in the motor circuit close which supply 230 VAC to the valve motor operator and the valve begins to close. The closing contactor simultaneously opens another contact (9/C) in the opening contactor circuit which prevents the opening contactor from picking up while the valve is closing (i.e. the opening contactor is interlocked with the closing contactor to prevent both contactors from being energized at the same time). An additional closing contactor, contact (9/C), closes and energizes relay 9X/C which picks up and closes contact

9X/C in the closing contactor circuit. Contact 9X/C, which is in parallel with the closing relay coil, contact (5/CSV2), seals in the closing contactor circuit and the control board switch can now be released and the valve will continue to close. When the control board switch is released, closing relay coil, 5/CSV2, will de-energize and the associated contact in the valve closing control circuit will open.

3. The valve continues to close until the valve limit switch contact (33/OVC), opens when the valve is fully closed. When the limit switch opens, the closing contactor de-energizes and all the 9/C contacts open which in turn de-energizes the valve motor, de-energizes relay 9X/C which opens contact 9X/C which in-turn resets the closing coil lock-in circuit. When the valve is fully closed, a limit switch, contact (33/CVC), closes and energizes relay 33Y/CSV2 which lights a green indicating light on the main control board to indicate that the valve is closed. During the time the valve is closing, if the valve should encounter difficulties in closing, a torque switch in the closing contactor circuit will open and de-energize the closing contactor as described above.

<u>Opening the Valve from the Main Control Room</u>

With the valve in the closed position as described, the valve can be opened from the control switch in the main control room as follows:

1. The opening of the RHR valve is controlled by the Reactor Coolant System pressure. If the RCS pressure is below the valve opening setpoint (390 psig), the valve can be opened using the Main Control Board switch as described in Steps 2 through 4 below. The valve is not automatically opened on RCS pressure below the valve opening setpoint. If the RCS pressure is above the valve opening setpoint, the valve cannot be opened. When the RCS pressure is above the opening setpoint, Reactor Coolant Auxiliary relay 63X/RCP is de-energized and its associated contact 63X/RCP in the

valve opening contactor circuit is open. When contact 63X/RCP is open, the valve control circuit cannot be energized and the valve cannot be opened. Turning the control board switch to open when the valve is below the opening setpoint will pickup the opening relay coil 6/CSV2 and close contact 6/CSV2 in the opening contactor circuit. However, since contact 63X/RCP is open (i.e. relay 63X/RCP is de-energized) the valve is prevented from opening. If the RCS pressure is below the opening setpoint the valve will operate as discussed below.

2. If the Reactor Coolant System pressure is below the valve opening setpoint (390 psig), a contact from relay 63X/RCP (Reactor Coolant Pressure Auxiliary Relay) will be closed in the valve opening contactor circuit (i.e. Reactor Coolant Pressure Auxiliary relay 63X/RCP is energized). Placing the control switch to the OPEN position will pick up the opening relay coil 6/CSV2 and close a contact in the valve opening contactor circuit. The relay contact is in series with the RCS Pressure Auxiliary relay contact (63X/RCP), a valve limit switch contact (33/OVC), which is closed when the valve is closed, and a closing contactor contact (9/C), which is closed when the closing contactor is not energized.

3. With all the contacts in Step 2 closed, the opening contactor (9/O) is now energized with 118 VAC from the control power step down transformer. The opening contactor, contact (9/O), closes which supplies 230 VAC to the valve motor operator and the valve begins to open. The 9/O motor contacts connect the three phase power such that the motor rotation direction is reversed from the closing direction. The opening contactor simultaneously opens another contact (9/O) in the closing contactor circuit which prevents the closing contactor from picking up while the valve is opening (i.e. the closing contactor is interlocked with the opening contactor to prevent both contactors from being energized at the same time). An additional opening contactor, contact (9/O), closes and energizes relay 9X/O which closes contact 9X/O in the opening contactor circuit. Contact

9X/O, which is in parallel with the opening relay coil contact (6/CSV2), seals in the opening contactor circuit and the control switch can now be released and the valve will continue to open. When the control board switch is released, opening relay coil 6/CSV2 will de-energize and the associated contact will open.

4. The valve continues to open until the valve limit switch, contact (33/OVO), opens when the valve is fully open. When the limit switch opens, the opening contactor de-energizes and all the 9/O contacts open which de-energizes the valve motor, de-energizes relay 9X/O which opens contact 9X/O which in-turn resets the opening coil lock-in circuit. When the valve is fully open, a limit switch contact (33/CVO) closes and energizes relay 33X/CSV2 which lights a red indicating light on the main control board to indicate that the valve is open.

   During the time the valve is opening, unlike the closing circuit, the valve opening control circuit is not protected from an over-torque condition since the torque switch (33/OVO) is jumpered out.

<u>Automatic Closing of the RHR Suction Isolation Valve</u>

When the pressure goes below the valve opening setpoint (390 psig), the valve can be opened or closed from the control switch in the main control room as described above. When the valve is open, increasing RCS pressure will automatically close the valve and prevent it from opening as described below.

1. With the valve open, increasing RCS pressure above the valve closing setpoint (700 psig) will de-energize the Reactor Coolant Pressure Auxiliary Relay 63Y/RCP and close contact 63Y/RCP in the valve closing contactor circuit. When contact 63Y/RCP closes, the valve automatically begins to close. Contact 63Y/RCP, which is in parallel with the control board closing relay coil contact 5/CSV2, energizes the valve control circuit in the same manner as described above in

the "Closing the Valve from the Main Control Room" section above. The valve will continue to operate until the valve is fully closed as described in the referenced section above. After the valve is fully closed, it cannot be opened because the opening circuit is locked out as described above in the "Opening the Valve from the Main Control Room" section.

Reactor Coolant System Pressure Control Loop

The Reactor Coolant System hot leg pressure channel, PT-403 is used to provide the interlock signals for the RHR common suction isolation valve 1RH-1. PT-405 is used to interlock valve 1RH-2. The pressure control loop consists of the pressure transmitter (PT-403), a loop power supply, a dual circuit signal comparator, a current to voltage module, a signal isolator and various test points and test jacks. The pressure transmitter measures the RCS pressure and provides a current output signal that is proportional to the measured pressure. The purpose of the loop power supply is to provide the current source (4 to 20 milliamps) to drive the instrument loop. The dual circuit signal comparator is used to compare the pressure signal to a given setpoint. The comparator provides a 118 VAC signal or a 0 VAC signal depending if the pressure signal is above or below the setpoint. The current to voltage or I/V module takes the loop current signal developed by the pressure transmitter and the loop power supply and converts the current signal to a proportional voltage signal (1 to 5 V). The voltage signals are used as input signals to the signal comparator module and the signal isolator. The signal isolator modules are used to provide electrical isolation between the input and the output signals. In this application, the signal isolator is used to provide separation between the safety and non-safety related portions of the pressure loop. The various test points and jacks are used during maintenance and calibration of the instrument loop.

As discussed above, the dual circuit signal comparator is used to provide bistable output signals (either on or off) depending on whether the measured signal is above or below the setpoint. Specifically, for the RHR valve interlock circuit, whenever the RCS pressure measured by the pressure loop exceeds the valve closing setpoint (700 psig), the dual comparator output circuit (2) will de-energize (0 VAC) which, in-turn, de-energizes the Reactor Coolant Pressure Auxiliary relay 63Y/RCP. This relay in-turn closes the associated contact 63Y/RCP in the valve closing contactor circuit causing the valve to close as discussed above. Whenever the RCS pressure is below the valve closing setpoint, the comparator output circuit will provide a 118 VAC that will energize the Reactor Coolant System pressure Auxiliary relay 63Y/RCP and open the associated contact 63Y/RCP in the valve closing contactor circuit.

Similarly for the valve opening comparator output, whenever the RCS pressure exceeds the valve opening setpoint (390 psig), the dual comparator output circuit (1) will de-energize (0 VAC), which de-energizes the Reactor Coolant Pressure Auxiliary relay 63X/RCP which opens contact 63X/RCP in the valve opening contactor circuit and prevents the valve from being opened as discussed above. Whenever the RCS pressure is below the valve opening setpoint, the comparator output circuit will provide a 118 VAC output signal that will energize Reactor Coolant Pressure Auxiliary relay 63X/RCP which closes contact 63X/RCP in the valve opening circuit which permits the valve to be opened from the main control board control switch.

5.2 Callaway

The following sections provide a description of the Group 2 lead plant, Callaway.

5.2.1 General Description

Callaway is the first of 2 identical PWR units built to the Standardized Nuclear Unit Power Plant System design (SNUPPS). The unit was granted a full power operating license on October 18, 1984. The Nuclear Steam Supply System (NSSS) consists of a 3411 MWt core with four (4) reactor coolant loops. Each loop contains a Westinghouse Model F improved steam generator and a Westinghouse Model 93A1 reactor coolant pump.

The containment is a prestressed, post-tensioned concrete structure with a cylindrical wall, a hemispherical dome, and a flat foundation slab. The inside surface of the structure is lined with carbon steel plates welded together to form a barrier which is essentially leak tight.

The power conversion system consists of a General Electric tandem-compound turbine having one high-pressure and three low-pressure elements. Design output is 1186 MWe (net), and steam dump to the condenser is rated at 40-percent full load. Four main steam lines carry steam from the top of the steam generators, through four main steam isolation valves (one in each line), to the turbine stop valves at the inlet to the turbine generator. Each main steam line is also equipped with five code safety valves and one power-operated relief valve.

Emergency Core Cooling System (ECCS) components include 4 cold leg accumulators, 2 centrifugal charging pumps (CHG/HHSI), 2 safety injection pumps, 2 residual heat removal pumps and associated valves and piping. Two redundant onsite emergency diesels assure electric power supply to the vital equipment. The borated refueling water storage facility consists of a large outside storage tank (RWST) which is the suction source for the ECCS pumps during the injection phase.

5.2.2 Residual Heat Removal System

Function

The primary function of the Residual Heat Removal System (RHRS) is to remove decay heat from the Reactor Coolant System (RCS) during plant cooldown and refueling operations. The RHRS transfers heat from the RCS to the Component Cooling Water System (CCWS) to reduce reactor coolant temperature to the cold shutdown temperature. The cold shutdown temperature is maintained until the plant is started up again.

As a secondary function, the RHRS is used to transfer refueling water between the Refueling Water Storage Tank (RWST) and the refueling cavity before and after refueling operations. The RHRS also serves as part of the Safety Injection System to provide Low Head Safety Injection emergency core cooling in the event of a break in the RCS.

Overview

A basic flow diagram of the RHRS is shown in Figure 5-6. The RHRS consists of two separate RHR trains of equal capacity, each independently capable of meeting the safety analysis design bases. Each train consists of one heat exchanger, one motor-driven pump and the associated piping, valves and instrumentation necessary for operational control. The inlet line to each train of the RHRS is connected to a RCS hot leg, while the return lines are connected to the cold legs of each of the reactor coolant loops via the accumulator discharge lines.

Each RHRS suction line is normally isolated from the RCS by two, series, motor-operated valves, while the discharge lines are isolated by two check valves in each line. The RHRS suction/isolation valves, and the inlet line pressure relief valve, and the discharge lines downstream of valves 8809A/B and 88?0 are located inside containment, while the remainder of the system is located outside containment.

During normal plant cooldown operations, reactor coolant flows from the RCS hot legs 1 and 4 to the RHR pumps, through the tube side of the RHR heat exchangers and back to the RCS cold legs through the safety injection accumulator discharge lines. The reactor coolant heat is transferred by the RHR heat exchangers to the component cooling water which circulates through the shell side of the RHR heat exchangers.

Coincident with RHRS normal cooldown operations, a portion of the reactor coolant flow may be diverted from downstream of the RHR heat exchangers to the Chemical and Volume Control System (CVCS) low-pressure letdown line for cleanup and/or pressure control. By regulating the diverted flowrate and the charging flow, the RCS pressure can be controlled during water solid-plant operations. Pressure regulation is necessary to maintain the pressure range dictated by the reactor vessel fracture prevention criteria requirements and by the RCP No. 1 seal differential pressure and NPSH requirements.

The RCS cooldown rate is manually controlled by regulating the reactor coolant flow through the tube side of the RHR heat exchangers. Instrumentation is provided to monitor system pressure, temperature and total flow.

System Operation

A discussion of RHRS operation during various reactor operating modes follows:

Reactor Startup

Generally, during cold shutdown, the RHRS operates to remove residual heat from the reactor core. The number of pumps and heat exchangers in service depends on the RHRS heat load at the time.

At initiation of plant startup, the RCS is completely filled, and the pressurizer heaters are energized. At least one RHR pump is operating with a portion of its discharge directed to the CVCS for purification and/or pressure control via a line that is connected to a cross-connect header downstream of the RHR heat exchanger. Once a steam bubble is formed in the pressurizer, the RHRS is isolated, and RCS pressure/inventory control are provided by the pressurizer spray, pressurizer heaters, normal letdown and charging systems.

Power Generation and Hot Standby Operation

The RHRS is not used during hot standby or power operations when the RCS is at normal pressure and temperature. Under these conditions, The RHRS is aligned for operation as part of the ECCS. Upon initiation of a safety injection signal ("S" signal), the RHR pumps take suction from the RWST and inject borated water into the reactor vessel via the Safety Injection System accumulator cold leg injection headers. When the water in the RWST is depleted, the RHR pumps are automatically aligned to take suction from the containment recirculation sump. The RHR heat exchangers then cool the sump fluid being recirculated by the RHR pumps and deliver the cooled water to the reactor vessel cold legs. Hot leg recirculation is initiated approximately 24 hours after the accident and ECCS initiation. The flow path for this condition consists of both RHR pumps taking suction from the recirculation sump, discharging through the discharge cross connect valves and common discharge valve to the RCS hot legs 2 and 3. Since the CHG/HHSI and the safety injection pumps do not take suction from the containment sump, the RHR/LHSI pumps also supply the suctions of these pumps during recirculation.

Reactor Shutdown

With the RCS borated to the cold shutdown concentration (approximately 2000 ppm), the initial phase of reactor cooldown is accomplished by transferring heat from the RCS to the Steam and Power Conversion System (SPCS) through the use of the RCS steam generators and the SPCS steam dump valves or the SPCS atmospheric power-operated relief valves. When the reactor coolant nominal temperature and pressure are reduced to 350°F and less than 360 psig, approximately 4 hours after reactor shutdown, the second phase of cooldown starts with the RHRS being placed in operation.

The reactor cooldown rate is limited by RCS equipment cooling rates based on allowable stress limits, as well as the operating temperature limits of the CCWS. As the reactor coolant temperature decreases, the reactor coolant flow through the RHR heat exchangers is increased to maintain a constant cooldown rate.

As cooldown continues, the pressurizer is filled with water, and the RCS is operated in the water-solid condition. At this stage, pressure is controlled by regulating the charging flow rate and the letdown rate to the CVCS from the RHRS. After the Reactor Coolant System is depressurized, cooled to ≤140°F, and purged to reduce dissolved hydrogen concentration to a safe level, the reactor vessel head may be removed for refueling or maintenance.

Refueling

Both RHR pumps are utilized during refueling operations to pump borated water from the RWST to the refueling cavity. During this operation, the isolation valves in the inlet line of the RHRS are closed, and the isolation valves from the refueling water storage tank are opened. After the water level in the refueling cavity reaches normal refueling level, the inlet isolation valves are opened, the RWST supply valves are closed, and normal RHRS operation resumes.

During refueling, the RHRS remains in service with the number of pumps and heat exchangers in operation as required by the heat load and plant technical specifications. Additionally, a portion of the RHRS flow is directed to the CVCS for purification and eventual return to the RCS via the charging system.

Following refueling, the RHR pumps drain the refueling cavity to the top of the reactor vessel flange by pumping water from the RCS to the RWST.

Component Description

This section describes the major components of the RHR System.

RHR Pumps

Two pumps are installed in the RHR System. Each pump is sized to deliver one-half the total reactor coolant flow through the RHR heat exchangers to meet the plant cooldown requirements. The use of two pumps ensures that cooling capacity is only partially lost should one pump become inoperable.

The RHR pumps are protected from overheating and loss of suction flow by miniflow bypass lines, located on the heat exchanger outlet, that diverts part of the flow back to the pump suction. A control valve located in each miniflow line is regulated by a signal from the flow transmitters located in each pump discharge header. The control valves open to divert flow back to the pump suction when the discharge flow is less than approximately 816 gpm at 300°F (783 gpm at 680°F) and close when it exceeds approximately 1650 gpm at 300°F (1582 gpm at 68°F). This arrangement ensures that the RHR pump does not overheat or vibrate when the discharge line is closed or when the RCS pressure exceeds the pump shutoff head during the ECCS injection phase.

A pressure transmitter in each pump discharge header provides pressure indication with a high pressure alarm in the main control room.

The two RHR pumps are vertical, centrifugal units with mechanical shaft seals. All pump surfaces in contact with reactor coolant are austenitic stainless steel or equivalent corrosion resistant material.

RHR Heat Exchangers

Two residual heat exchangers are installed in the RHR System. The heat exchanger design is based on heat load and temperature differences between reactor coolant and component cooling water existing 20 hours after reactor shutdown when the temperature difference between the two systems is small. The installation of two heat exchangers ensures that the heat removal capacity of the system is only partially lost if one heat exchanger becomes inoperative. The heat exchangers are of the shell and U-tube type. Reactor coolant circulates through the tubes, while component cooling water circulates through the shell. The tubes are welded to the tubesheet to prevent leakage of reactor coolant.

RHRS Valves

The following sections describe the Callaway RHRS valves. To facilitate other plants in this grouping referencing this discussion, corresponding

Westinghouse valve I.D. numbers are provided in parentheses. (For those valves where no tag numbers are provided in parentheses, the plant-specific tag numbers are identical to the Westinghouse tag numbers).

Inlet Isolation Valves HV-8701A, HV-8701B, HV-8702A and HV-8702B

These valves are motor-operated, gate valves which are normally-closed except when the RHRS is in operation. Both valves are provided with a manual control (open/closed) on the main control board and will fail in the "as-is" position.

Valves HV-8701A and HV-8701B are interlocked with RCS pressure transmitter PT-405 and valves HV-8702A and HV-8702B are interlocked with pressure transmitter PT-403. These interlocks prevent the inadvertent opening of the valves when RCS pressure is above 360 psig. The valves also close automatically when the RCS pressure is higher than 682 psig. A more detailed description of the valves interlocks is provided in Section 5.2.3.

Heat Exchanger Flow Control Valves HCV-606 and HCV-607

The reactor coolant flow rate through the RHR heat exchangers is adjusted by air-operated, butterfly valves HCV-606 and HCV-607. Positioning of these valves from the control room regulates the reactor coolant flow exiting the heat exchangers. These valves are normally full open during power operation.

Bypass Flow Control Valves FCV-618 and FCV-619

These valves, located in the heat exchanger bypass lines, are air-operated butterfly valves. The valve may be positioned automatically from its associated flow transmitter (FT-618 or FT-619) or manually from the control room. As the operator positions HCV-606 to regulate the plant cooldown rate, bypass valve FCV-618 automatically repositions itself to maintain a constant return flow to the RCS. HCV-607 and FCV-619 act in a similar manner.

Miniflow Stop Valves FCV-610 and FCV-611

These normally-closed valves are motor-operated, gate valves which are located in the residual heat removal pump miniflow line. This miniflow line ensures that the RHR pump does not overheat or vibrate when the discharge line is closed or when RCS pressure exceeds the pump shutoff head. The valves are controlled by flow transmitters FT-610 and FT-611, respectively, which are located in the discharge line of the RHR pump. These valves will open when the pump discharge flow is less than approximately 816 gpm at 300°F (783 gpm at 68°F). When the pump flow exceeds approximately 1650 gpm at 300°F (1582 gpm at 68°F) the corresponding valve will close. (When the RHR/LHSI pumps are stopped, these valves remain open.)

Crosstie Valves HV-8716A and HV-8716B

These motor-operated valves, located in the piping crosstie downstream of the residual heat exchangers, are open during both normal plant and RHRS operation. They allow RHRS flow from both trains to inject to all 4 cold legs during ECCS injection. These valves are closed during the post-accident recirculation phase to provide system separation for passive failure protection. Additionally they provide a flow path to return water to the RWST and injection to loops 2 and 3 hot legs during ECCS hot leg recirculation. These valves are controlled from the main control board and fail "as is."

Accumulator Cold leg Injection Line Check Valves 8948A, 8948B, 8948C, and 8948D

There is one check valve in each accumulator cold leg discharge line segments (closest to the RCS and in common with the RHRS/LHSI and safety injection pumps discharge paths) which serves as an RCS pressure boundary valve and prevents backflow to the ECCS.

RHRS Return Line Check Valves 8818A, 8818B, 8818C, and 8818D

One check valve is located in each branch of the RHRS return line to prevent backflow from the safety injection pumps, and to serve as a backup in the event of leakage of the check valve on the cold leg injection line.

Gate Valve 8809A and 8809B

There is a ten-inch, normally-open, motor-operated, gate valve in each parallel discharge line from the residual heat removal pump, downstream of the heat exchanger and discharge crosstie header. These valves are used to isolate the RHRS from the cold legs during hot leg recirculation or during refueling operation when returning water to the RWST.

Crosstie Valves V001 and V002 (8734A & B)

These two, normally-closed, manual valves are used to line up a portion of the RHR pump discharge to be directed to the CVCS. Throttle valve HCV-128 is used to control this flow. This flow path is used during a plant cooldown and during water solid plant operations when the CVCS is used for RCS pressure control and purification.

Gate Valve HV-8804A

Gate Valve HV-8804A isolates a flow path off the discharge of the "A" train RHRS heat exchanger which supplies water to the suction of the centrifugal charging pumps and the "A" train safety injection pump during the recirculation phase of safety injection. HV-8804A is normally-closed and is interlocked with the RHRS suction/isolation valves.

Gate Valve HV-8804B

Gate valve HV-8804B isolates a flow path from the "B"-train RHR/LHSI pump (downstream of the RHR heat exchanger) which supplies the suction of the

"B"-train safety injection pump during recirculation. HV-8804B is normally-closed and is interlocked with the RHRS suction isolation valves (see Section 5.2.3).

Gate Valve HV-8840

During hot leg recirculation the RHR pumps are realigned to discharge through cross-connect valves HV-8716A, HV-8716B, and common discharge valve HV-8840. This realignment is initiated at approximately 24 hours after accident initiation. Hot leg recirculation prevents crystallization of boric acid in the core and quenchs the steam bubble in the top of the core.

RWST Isolation Valves 8958A, 8958B, HV-8812A, and HV-8812B

Check valves 8958A/B and motor-operated gate valves HV-8812A and B isolate the RWST from each RHR/LHSI pump's suction. Gate valves HV-8812A and B are interlocked with the RHRS suction isolation valves.

Sump Isolation Valves HV-8811A and HV-8811B

There is one, motor-operated gate isolation valve in each RHR/LHSI pump suction line from the sump. These valves are normally-closed and are automatically opened (from a low-low RWST level signal coincident with an 'S'-Signal) during the switchover operations from injection to recirculation. Valves 8811A/B are also interlocked with the RHRS suction isolation valves.

RHRS Discharge Relief Valves 8856A, 8856B, and 8842

A 3/4-inch relief valve is located in each RHR/LHSI cold leg and hot leg discharge header. These valves protect against overpressurization of the piping due to any RCS backleakage or thermal expansion of trapped water. The design capacity of these valves is 20 gpm at the setpressure of 600 psig.

Relief Valve 8708A and 8708B

There is one, 3-inch relief valve (inside containment) in each RHRS suction line from the RCS hot leg. The relief valves are located immediately downstream of the RHRS suction/isolation valves 8701A and 8701B. These relief valves prevent RHRS overpressurization by discharging to the Pressurizer Relief Tank (PRT) when pressures within the RHRS suction line exceed 450 psig. The design capacity of these valves at the 450 psig setpressure is 475 gpm at inlet temperature of 375°F and 770 gpm at inlet temperatures less than 200°F.

5.2.3 Current RHRS Suction Isolation Valves Interlocks and Functional Requirements

The following sections provide a description of the Callaway suction isolation valve interlocks and valve control circuits.

5.2.3.1 Current Interlocks

There are two, normally-closed, motor-operated, series, isolation valves in each of the two RHR pump suction lines from the RCS hot legs. The two valves inside the missile barrier, 8702A & B, are designated as the inner isolation valves, while the two valves outside the missile barrier, 8701A & B, are designated as the outer isolation valves. The interlock features provided for the inner isolation valves are identical to those provided for the outer isolation valves.

Each valve is interlocked against opening unless the following conditions are met:

1. The RCS pressure, as measured by the appropriate wide range pressure channel, is less than 360 psig. This assures the RHRS cannot be overpressurized by aligning it to the RCS when RCS pressure plus RHR pump head would exceed the RHRS design pressure.

2. The corresponding RHR pump/RWST suction isolation valve is closed. This assures positive isolation of the RWST and RHRS/RWST suction piping before initiating a normal cooldown.

3. The corresponding recirculation line to the charging/high-head safety injection pumps isolation valve is closed. This assures the suction of the high-head safety injection system (design pressure = 210 psig) cannot be overpressurized by normal cooldown flow via an open recirculation line isolation valve.

4. The corresponding containment sump isolation valve is closed. This assures normal cooldown flow cannot be discharged to the containment sump via an open sump isolation valve.

In addition to the above interlocks each valve is also interlocked to automatically close on increasing RCS pressure greater than 682 psig. This feature assures that both isolation valves will be closed during a plant startup prior to reaching operating conditions, if one valve had been inadvertently left open by the operator. The operator may close the suction/isolation valve at any time.

The current interlocks for valves 8701A & B and 8702A & B are shown functionally on Figures 5-7 and 5-8.

5.2.3.2 RHRS Common Suction Isolation Valve Description

The RHR Common Suction Isolation Valves are motor operated valves that can be opened or closed from the main control board. The valve will automatically close on increasing Reactor Coolant System pressure. On decreasing Reactor Coolant System pressure, the valve control circuit receives an interlock signal that allows the valve to be opened using the main control board switch. On reactor coolant pressure above the setpoint, the valve control circuit is disabled and the valve cannot be opened.

The valve control circuit consists of control switches, limit switches, torque switches, contactors, relays, indicating lights, a 3 phase, 480 VAC motor and a pressure control loop. The control switches are located in the main control room. The limit switches are located in the valve motor operator and provide indication of the position of the valve. Relays are used for providing control signals. The contactor, located in the motor control center, is switched on and off to provide the power to the valve. The contactor also provides contacts that are used in the valve control circuit. There are red and green indicating lights are on the Main Control Board to show the position of the valve. The valve motor operator is located at the valve and is used to change the position of the valve. The pressure control loop measures Reactor Coolant System pressure and provides output signals to the valve control circuit based on the system pressure that allows the valve to be opened from the control switch or automatically closed.

The following provides a detailed description of the valve control circuit for HV-8702B. Operation of valves HV-8701A, HV-8701B and HV-8702A is similar. Figures 5-9 through 5-12 show the appropriate detail of the circuits.

Closing the Valve from the Main Control Room

With the valve in the full open position, the valve can be closed from the control switch in the main control room as described in the following steps:

1. Placing the control board switch to the CLOSE position will energize the closing contactor coil (42 C). The control board switch (HIS/close) is in series with a limit switch contact (ZS/1), which is closed when the valve is open, a torque switch contact (WS/17) which is in parallel with ZS/1, and a contact (42 O/b) which is closed when the opening contactor coil (42 O) is not energized.

2. With all the contacts in Step 1 closed, the contactor closing coil 42 C is energized with 120 VAC power from the 480/120 VAC control power step down transformer. The closing contactor contacts (42 C) in the motor circuit close and supply 480 VAC to the valve motor operator and the valve begins to close. The closing contactor simultaneously opens another contact (42 C/b) in the opening control circuit which prevents the opening contactor relay from picking up while the valve is closing (i.e. the opening control circuit is interlocked with the closing control circuit to prevent both contactor relays from being energized at the same time). An additional closing contactor contact (42 C/a) closes. Contact 42 C/a, which is in parallel with the control board switch, seals-in the closing circuit so that the control board switch can be released and the valve will continue to close. As the valve begins to close, limit switch contact ZS/3 closes turning on the green indicating light on the main control board. The red indicating light is controlled by limit switch contact ZS/15 and is on when the valve is open or during travel (i.e. both lights are on during travel).

3. Limit switch contacts ZS/1 open as the valve begins to close, leaving only the parallel torque switch contact (WS/17) to complete the circuit. The valve continues to close until the valve torque switch contact (WS/17) opens indicating the valve is torqued closed. When the torque switch contact opens, the contactor coil de-energizes and all the 42 C contacts open which in-turn de-energize the valve motor. Contact 42 C/a opens which resets the closing seal-in circuit. Contact 42 C/b closes to allow the valve opening control circuit to actuate. When the valve is fully closed, a limit switch contact (ZS/15) opens which turns off the red indicating light on the main control board, leaving the green indicating light on the main control board to show that the valve is closed. During the time the valve is closing, if the valve should encounter difficulties in closing, the torque switch contact (WS/17) in the closing contactor circuit will open and de-energize the closing contactor as described above.

Opening the Valve from the Main Control Room

With the valve in the closed position as described above, the valve can be opened from the control switch in the main control room as follows:

1. The opening of the RHR valve is restricted by the Reactor Coolant System pressure. If the RCS pressure is below the valve opening setpoint (360 psig), the valve can be opened using the Main Control Board switch as described in Steps 2 through 4 below. The valve is not automatically opened on RCS pressure below the valve opening setpoint. If the RCS pressure is above the valve opening setpoint, the valve cannot be opened (See Figure 5-7). When the RCS pressure is above the opening setpoint, the Reactor Coolant Pressure interlock contact (K-734) in the valve opening circuit is open. When contact K-734 is open, the valve opening contactor circuit cannot be energized and the valve cannot be opened. If the RCS pressure is below the setpoint the valve will operate as discussed below.

2. If the Reactor Coolant System pressure is below the valve opening setpoint (360 psig), contact K-734 (Reactor Coolant Pressure interlock) will be closed in the valve opening contactor circuit. Operating the Main Control Board switch to OPEN the valve will energize the opening contactor relay coil 42 O. The Control Board switch is in series with the following contacts:

   - RCS Pressure interlock contact (K-734)
   - Two valve limit switch contacts (ZS/5 & ZS/4) which are closed when the valve is closed
   - A torque switch contact (WS/13), in parallel with ZS/5
   - A RHR pump/RWST suction valve interlock contact (33/bc)
   - A recirculating line to the charging/safety injection pump isolation valve interlock contact (33/bc)
   - A containment sump isolation valve interlock contact (33/bc).

   Each of the three interlocking valves must be closed to close the series contacts noted above.

3. With all the contacts in Step 2 closed, the opening contactor relay coil (42 O) is energized with 120 VAC from the control power step down transformer. The opening contactor contacts (42 O) close and supply 480 VAC to the valve motor operator and the valve begins to open. The 42 O contacts connect the three phase power phases such that the motor rotation direction is reversed from the closing direction. The opening contactor simultaneously opens another contact (42 O/b) in the closing contactor circuit which prevents the closing contactor from picking up while the valve is opening (i.e. the closing contactor is interlocked with the opening contactor to prevent both contactors from being energized at the same time). An additional opening contactor contact (42 O/a) closes. Contact 42 O/a, which is in parallel with the opening Main Control Board switch contact, seals-in the opening contactor circuit so that the control switch can be released and the valve will continue to open. The seal-in contact is also in parallel with the RCS pressure contact, and the three interlocking valve contacts. As the valve begins to open, limit switch contact ZS/15 closes turning on the red indicating light on the Main Control Board. The green indicating light is controlled by limit switch contact ZS/3 and is lit when the valve is closed or during travel.

4. The valve continues to open until the valve limit switch contact (ZS/4) opens and the valve is fully open. When the limit switch opens, the opening contactor relay coil de-energizes and all the 42 O contacts open, de-energizing the valve motor. Contact 42 O/a opens which resets the opening seal-in circuit. Also, when the valve is fully open, a limit switch contact (ZS/3) opens and the green indicating light on the Main Control Board is turned off. The red indicating light on the Main Control Board remains lit to indicate that the valve is open.

During the time the valve is opening, the valve and the valve opening control circuit are protected from a over-torque condition since the torque switch contact WS/13 is in series with the seal-in contact 42 O/a.

Automatic Closing of the RHR Valve

When the RCS pressure goes below the valve opening setpoint (360 psig) the valve can be opened or closed from the control switch in the Main Control Room as described above. When the valve is open, an increasing RCS pressure will automatically close the valve and prevent it from opening as described below.

1. With the valve open, an increasing RCS pressure above the valve closing setpoint (682 psig) will close contact K-735 in the valve closing contactor circuit. Limit switch contact ZS/8, which is in series with contact K-735, is closed except when the valve is fully closed. When contact K-735 closes, the valve automatically begins to close. Contact K-735, which is in parallel with the Control Board closing switch contact, energizes the valve control circuit in the same manner as described above in the "Closing the Valve from the Main Control Room." The valve will continue to close until the valve is torqued closed as described in the referenced section above. When the valve is fully closed, limit switch contact ZS/8 will open preventing the re-actuation of the closing contactor from contact K-735 due to the reset of the torque switch contact (WS/17). After the valve is fully closed, it cannot be opened because the opening circuit is locked out as described above in the "Opening the Valve from the Main Control Room" section.

Reactor Coolant System Pressure Control Loop

The Reactor Coolant System hot leg pressure channel, PT-405 is used to provide the interlock signals for the RHR Inlet Isolation Valves HV-8701A and HV-8701B. PT-403 is used to provide the interlock signals for RHR Inlet Isolation Valves HV-8702A and HV-8702B. Each pressure control loop consists of the pressure transmitter (PT-403 or PT-405), two channel test cards, a loop power supply/current to voltage transformer, and a dual circuit signal comparator. The pressure transmitter measures the RCS pressure and provides a current output signal that is proportional to the measured pressure. The loop power supply takes the 4 to 20 mA current signal from the pressure transmitter and converts it to a 0 to 10 V proportional voltage signal. The non-isolated output of the loop power supply is input into the dual comparator. The dual comparator compares the pressure signal (input voltage) to the given setpoints. The comparator outputs are 0 VDC or 24 VDC depending on the signal to setpoint comparison. The 0/24 VDC outputs control relays which open and close the valve contactor K-734 and K-735 contacts. The A comparator output is 24 VDC when the pressure is above 360 psig which energizes the K-734 relay, opening the K-734 contacts. The B comparator output is 24 VDC when the pressure is above 682 psig which energizes the K-735 relay, closing the K-735 contacts. The various test points and jacks are used during maintenance and calibration of the instrument loop.

As discussed above, the dual circuit signal comparator is used to provide bistable output signals (either on or off) depending on whether the measured signal is above or below the setpoint.

Specifically, for the RHR valve interlock circuit, whenever the RCS pressure measured by the pressure loop exceeds the valve closing setpoint (682 psig), the dual comparator output circuit (B) will energize the K-735 relay closing the associated contact K-735 in the valve closing contactor circuit causing the valve to close as discussed above. Whenever the RCS pressure is below the valve closing setpoint, the comparator output circuit will de-energize the K-735 relay opening the associated contact K-735 in the valve closing contactor circuit, allowing the valve to remain open.

Similarly, for the valve opening comparator output, whenever the RCS pressure exceeds the valve opening setpoint (360 psig), the dual comparator output circuit (A) will energize the K-734 relay opening contact K-734 in the valve opening contactor circuit and prevent the valve from being opened as discussed above. Whenever the RCS pressure is below the valve opening setpoint, the comparator output circuit will de-energize, closing contact K-734 in the valve opening circuit, permitting the valve to be opened from the Main Control Board control switch.

Emergency Core Cooling System (ECCS) components include 3 cold leg accumulators, 3 centrifugal charging/HHSI pumps and 2 residual heat removal pumps (RHR/LHSI) and associated valves and piping. Two redundant on-site emergency diesels assure electric power supply to vital equipment. The borated refueling water storage facility consists of a large outside storage tank (RWST) which is the suction source for the ECCS pumps during the injection phase.

5.3 North Anna Unit 1

The following sections provide a description of the Group 3 lead plant, North Anna Unit 1.

5.3.1 General Description

North Anna Units 1 and 2 are identical Westinghouse PWR's. Unit 1 was granted a full power operating license in April 1978, and Unit 2 followed in August 1980. The Nuclear Steam Supply System (NSSS) consists of a 2893 MWt core with three (3) reactor coolant loops. Each loop contains Westinghouse Model 51 steam generator and a Model 93A reactor coolant pump.

The containment is a steel-lined, reinforced concrete structure with a cylindrical wall, hemispherical dome, flat foundation slab, and a sub-atmospheric environment.

The power conversion system consists of a Westinghouse tandem-compound turbine having one high-pressure and two low-pressure elements. Design output is 925 MWe (net), and steam dump to the condenser is rated at 40 percent of full load. Three main steam lines carry steam from the steam generators, through three main steam isolation valves (one in each line) to the turbine stop valves at the inlet to the turbine generator. Each main steam line is also equipped with five code safety valves and one power-operated relief valve.

Emergency Core Cooling System (ECCS) components include 3 cold leg accumulators, 3 safety injection/charging pumps, 2 low head safety injection pumps and associated valves and piping. Two redundant onsite emergency diesels assure electric power supply to vital equipment. The borated refueling water storage facility consists of a large outside storage tank (RWST) which provides a borated water suction source for the ECCS pumps. A Boron Injection Tank (BIT) contains a nominal 8% concentrated boric acid solution and is connected to the discharge of the centrifugal charging pumps which flush the BIT contents into the RCS on a safety injection signal ("S" signal).

5.3.2 Residual Heat Removal System

The primary function of the Residual Heat Removal System is to remove heat energy from the reactor core and the Reactor Coolant System during plant cooldown and refueling operations. The RHRS transfers heat from the RCS to the Component Cooling Water System (CCWS) to reduce the reactor coolant temperature to the cold shutdown temperature. The RHRS is kept in service to maintain the RCS at cold shutdown conditions until the plant is started up again.

As a secondary function, the RHRS is used to transfer water from the reactor refueling cavity and transfer canal to the RWST following refueling operations.

The RHR System does not function following a loss of coolant accident (LOCA). The low head safety injection pumps in conjunction with the high head safety injection pump provide injection flow to the core during the injection and recirculation phases of a LOCA.

Overview

A basic flow diagram of the RHRS is shown in Figure 5-13. The RHRS consists of two trains of equal capacity, each independently capable of meeting the safety design bases. Each train consists of one RHR heat exchanger, one motor-driven pump and the associated piping, valves and instrumentation necessary for operational control. The inlet line to each RHRS train is connected to a single drop line from the RCS hot leg loop 1, while the return lines are connected to the cold legs of two separate reactor coolant loops via the accumulator discharge lines.

There are two motor-operated suction/isolation valves, in series, in the single letdown line connecting the low pressure RHRS to the high pressure RCS. Each RHRS cold leg discharge line is isolated from the RCS by one of the accumulator discharge check valves (in the common segment closest to the cold leg) and one normally-closed, motor-operated, gate valve. All of the North Anna RHRS piping and equipment is located inside containment.

During normal RHRS operation, reactor coolant flows from RCS hot leg loop 1 to the RHR pumps, through the tube side of the RHR heat exchangers and back to the RCS cold legs (Loops 2 and 3) through the safety injection accumulator discharge lines. The reactor coolant heat is transferred by the RHR heat exchanger to the component cooling water circulating through the shell side of the heat exchangers.

Coincident with RHRS normal operations, a portion of the reactor coolant flow may be diverted from downstream of the RHR heat exchangers to the Chemical and Volume Control System (CVCS) low-pressure letdown line for cleanup and/or pressure control. By regulating the diverted flowrate and the charging flow, the RCS pressure can be controlled during water-solid plant operations. Pressure regulation is necessary to maintain the pressure range dictated by the reactor vessel fracture prevention criteria requirements and by the RCP No. 1 seal differential pressure and NPSH requirements.

The RCS cooldown rate is manually controlled by regulating reactor coolant flow through the tube side of the RHR heat exchangers. Instrumentation is provided to monitor system pressure, temperature and total flow.

System Operation

A discussion of the RHRS operation during various reactor operating modes follows:

Reactor Startup

Generally, during cold shutdown, the RHRS operates to remove residual heat from the reactor core. The number of RHR pumps and RHR heat exchangers in service depends on the RCS heat load at the time. At the initiation of plant startup, the RCS is completely filled (water-solid) and the pressurizer heaters are energized. At least one RHR pump is operating with a portion of its discharge directed to the CVCS for purification and/or pressure control via a line that is connected to a cross-connect header downstream of the RHR heat exchanger. Once a steam bubble is formed in the pressurizer, the RHRS is isolated, and RCS pressure/inventory control are provided by the pressurizer spray, pressurizer heaters, normal letdown and charging systems.

Power Generation and Hot Standby Operation

The RHRS is not used during hot standby or power operations when the RCS is at normal pressure and temperature.

Reactor Shutdown

The initial phase of plant shutdown is accomplished by transferring heat from the RCS, steam generators to the main steam atmospheric relief valves or to the condenser steam dump valves. When the reactor coolant temperature and pressure are reduced to approximately 350°F and less than 418 psig, approximately 4 hours after reactor shutdown, the second phase of shutdown starts with the RHRS being placed in operation.

The reactor cooldown rate is limited by RCS equipment cooling rates based on allowable stress limits, as well as the operating temperature limits of the Component Cooling Water System (CCWS). As the reactor coolant temperature decreases, the reactor coolant flow through the RHR heat exchanger is increased to maintain a constant cooldown rate.

As shutdown continues, the pressurizer is filled with water, and the RCS is operated in the water-solid condition. At this time, pressure is controlled by regulating the letdown rate to the CVCS from the RHRS. After the reactor coolant system is depressurized, cooled to ≤140°F, and purged to reduce dissolved hydrogen concentration to a safe level, the reactor vessel head may be removed for refueling or maintenance.

Refueling

Both RHR pumps are used during refueling to pump borated water from the RWST to the refueling cavity. During this operation, the isolation valves in the inlet line of the RHRS are closed and the isolation valves from the refueling water storage tank are opened. After the water level reaches normal refueling level, the RWST supply valves are closed, the inlet isolation valves are opened, and normal RHRS operation resumes.

During refueling, the RHRS remains in service with the number of pumps and heat exchangers in operation as required by the heat load and plant technical specifications. Additionally, a portion of the RHRS flow is directed to the CVCS for purification and eventual return to the RCS via the charging system.

Following refueling, the RHR pumps drain the refueling cavity to the top of the reactor vessel flange by pumping water from the RCS to the RWST.

<u>Component Description</u>

This section describes the major components of the Residual Heat Removal System.

RHR Pumps

Two pumps are installed in the RHRS. The pumps are sized to deliver sufficient reactor coolant flow through the RHR heat exchangers to meet the plant cooldown requirements. The use of two pumps ensures that cooling capacity is only partially lost should one pump become inoperative.

The RHR pumps are protected from overheating and loss of suction flow by a common, normally open, miniflow bypass line, located on the RHR heat exchangers discharge piping common header, that diverts flow back to the pump suction. The common miniflow line is sized for minimum recirculation flow; however, when the RHRS is in normal operation, the line resistance is sufficient to minimize this recirculated flow.

The two RHR pumps are vertical, centrifugal units with mechanical shaft seals. All pump surfaces in contact with reactor coolant are austenitic stainless steel or equivalent corrosion resistant material.

RHR Heat Exchangers

Two RHR heat exchangers are installed in the RHRS. The RHR heat exchanger design is based on heat load and temperature differences between the reactor coolant and component cooling water existing 20 hours after reactor shutdown when the temperature difference between the two systems is small. The installation of two heat exchangers ensures that the heat removal capacity of the RHRS is only partially lost if one heat exchanger becomes inoperative. The heat exchangers are of the shell and U-tube type. Reactor coolant circulates through the tubes, while component cooling water circulates through the shell.

The tubes are welded to the tube sheet to prevent leakage of reactor coolant into the component cooling water system.

RHRS Valves

The following sections describe the North Anna Unit 1 RHRS valves. The plant-specific I.D. numbers are followed by the Westinghouse tag numbers in parenthesis.

Inlet Isolation Valves MOV 1700 and 1701 (700 and 701)

These valves are motor-operated, gate valves which are normally closed except when the RHRS is in operation. Both valves are provided with a manual control (open/closed) on the main control board and will fail in the "as-is" position.

Inlet isolation valves 1700 and 1701 (700 and 701) are interlocked with RCS pressure transmitter PT-402 and PT-403, respectively. These interlocks prevent the inadvertent opening of the valves when RCS pressure is above 418 psig. The valves also close automatically when RCS pressure is higher than 582 psig. A more detailed description of the interlocks is provided in Section 5.4.3.

Gate Valves 1720A and 1720B (720A and 720B)

There is a ten-inch, normally-closed, motor-operated, gate valve in each RHR return line to the SIS accumulator cold leg discharge lines. These valves are used to isolate the RHRS from the RCS cold legs when the RHRS is not in operation.

Heat Exchanger Bypass Flow Control Valves FCV-1605 (FCV-605)

This valve, located in the RHR heat exchanger bypass line, is an air operated, butterfly valve. The valve is positioned automatically by flow transmitter FT-605 or manually from the main control room. As the operator positions HCV-758 to regulate the plant cooldown rate, bypass valve FCV-1605 (FCV-605) automatically repositions itself to maintain a constant return flow to the RCS.

Heat Exchanger Flow Control Valve HCV-1758 (HCV-758)

The reactor coolant flowrate through the RHR heat exchangers is adjusted by air-operated, butterfly valve HCV-1758 (HCV-758) located in the heat exchanger common discharge header. Positioning of this valve from the main control room regulates the reactor coolant flow through the heat exchangers and thus the plant cooldown rate. The valve is normally open to a set position, but has a fail-open feature.

CVCS Purification Line Isolation Valve 1RH-31 (717)

This normally-closed, manual, globe valve is used to line up a portion of the RHR pump discharge flow to be directed to the CVCS. Throttle valve HCV-1142 (HCV-142) is used to control this flow. This flowpath is used during plant cooldown operations and during water-solid plant operations where the CVCS is used for RCS pressure control and purification.

Accumulator Cold Leg Injection Line Check Valves 1-SI-144 and 1-SI-161 (875B and 875C)

The North Anna RHRS discharges to the SIS accumulator discharge lines of RCS cold legs 2 and 3; therefore, the accumulator discharge line check valves 1-SI-144 and 1-SI-161, in conjunction with gate isolation valves MOV-1702A and MOV-1702B, serve as RCS pressure boundary valves and prevent backflow from the RCS to the RHRS.

Relief Valve RV-1721A and RV-1721B (721A and 721B)

There is one relief valve in each RHR pump suction line from the RCS hot leg. These relief valves prevent RHRS overpressurization by discharging to the pressure relief tank (PRT) when pressures within the RHR System suction line exceeds 467 psig. These valves have a design capacity of 900 gpm at the 467 psig setpressure.

5.3.3 Current RHRS Suction Isolation Valves Interlocks and Functional Requirements

The following sections provide a description of the North Anna suction/isolation valve interlocks and valve control circuits.

5.3.3.1 Current Interlocks

There are two normally closed motor operated series isolation valves in the RHR pump suction line from the RCS hot leg. Valve MOV-1700 located inside the missile barrier is designated as the inner isolation valve, while the valve outside the missile barrier, MOV-1701, is designated as the outer isolation valve. The interlock features provided for the inner isolation valve is similar to those provided for the outer isolation valve.

Each valve is interlocked against opening unless the following condition is met:

1. The RCS pressure, as measured by the appropriate pressure channels, is less than 418 psig. This feature assures the RHR System cannot be overpressurized by aligning it to the RCS when RCS pressure plus RHR pump head would exceed the RHR System design pressure.

In addition to the above interlock feature, each suction isolation valve is also interlocked to automatically close on increasing RCS pressure greater than 582 psig.

The current interlocks for valves MOV-1700 and MOV-1701 are shown functionally on Figures 5-14 and 5-15. Figure 5-16 and 5-17 show the appropriate detail of the circuits.

5.3.3.2 RHRS Common Suction Isolation Valve Description

The RHR Common Suction Isolation Valves are motor operated valves that can be opened or closed from the main control board. The valve will automatically close on increasing Reactor Coolant System pressure. On decreasing Reactor Coolant System pressure, the valve control circuit receives an interlock signal that allows the valve to be opened using the Main Control Board switch. On reactor coolant pressure above the setpoint, the valve control circuit is disabled and the valve cannot be opened.

The valve control circuit consists of control switches, limit switches, torque switches, contactors, relays, indicating lights, a 3 phase, 480 VAC motor and a pressure control loop. The control switches are located in the main control room. The limit switches are located in the valve motor operator and provide indication of the position of the valve. Relays are used for providing control signals. The contactor, located in the motor control center, is switched on and off to provide the power to the valve. The contactor also provides contacts that are used in the valve control circuit. There are red and green indicating lights on the Main Control Board to show the position of the valve. The valve motor operator is located at the valve and is used to change the position of the valve. The pressure control loop measures Reactor Coolant System pressure and provides output signals to the valve control circuit based on the system pressure that allows the valve to be opened from the control switch or automatically closed.

The following provides a detailed description of the valve control circuit MOV-1701 (701). Operation of MOV-1700 (700) is similar. Figures 5-16 and 5-17 show the appropriate detail of the circuits.

Closing the Valve from the Main Control Room

With the valve in the full open position, the valve can be closed from the control switch in the main control room as described in the following steps:

1. Pushing the control board pushbutton to CLOSE will energize the closing contactor coil (52/C). The control board pushbutton closing contacts are in series with the following contacts:

   - Limit switch contact (LS-1) is closed when the valve is full open, and LS-8 is closed except when the valve is full closed.
   - Torque switch contact (TS-17) which is in parallel with LS-1.
   - Control board open contact which is open except when the OPEN pushbutton is depressed.
   - Contact (52/O) is closed when the opening contactor coil (52/O) is energized.

2. With all the contacts in Step 1 closed, the contactor closing coil 52/C is energized with 120 VAC power from the 480/120 VAC control power step down transformer. The closing contactor contacts (52/C) in the motor circuit close and supply 480 VAC to the valve motor operator and the valve begins to close. The closing contactor simultaneously opens another contact (52/C) in the opening control circuit which prevents the opening contactor relay from picking up while the valve is closing (i.e., the opening control circuit is interlocked with the closing control circuit to prevent both contactor relays from being energized at the same time). An additional closing contactor contact (52/C), which is in parallel with the control board switch, seals-in the closing circuit so that the control board switch can be released and the valve will continue to close. As the valve begins to close, limit switch contact LS-3 closes, turning on the green indicating light on the main control board. The red indicating light is controlled by limit switch contact LS-7 and is lit whenever the valve is not full closed.

3. Limit switch contact LS-1 opens as the valve begins to close, leaving only the parallel torque switch contact (TS-17) to complete the circuit. The valve continues to close until the limit switch contact (LS-8) opens indicating the valve is closed. When the limit switch contact opens, the contactor coil de-energizes and the motor 52/C contacts open which in-turn de-energize the valve motor. The

52/C seal-in contacts open, resetting the closing seal-in circuit. The 52/C contact in the opening control circuit closes to allow the valve opening control circuit to actuate. When the valve is fully closed, a limit switch contact (LS-7) opens which turns off the red indicating light on the Main Control Board, leaving the green indicating light on the Main Control Board to show that the valve is closed. During the time the valve is closing, if the valve should encounter difficulties in closing, the torque switch contact (TS-17) in the closing contactor circuit will open and de-energize the closing contactor as described above.

Opening the Valve from the Main Control Room

With the valve in the closed position as described above, the valve can be opened from the control pushbuttons in the main control room as follows:

1. The opening of the RHR valve is restricted by the Reactor Coolant System pressure. If the RCS pressure is below the valve opening setpoint (418 psig), the valve can be opened using the main control board switch as described in Steps 2 through 4 below. The valve is not automatically opened on RCS pressure below the valve opening setpoint. If the RCS pressure is above the valve opening setpoint, the valve cannot be opened (See Figure 5-16). When the RCS pressure is above the opening setpoint, the Reactor Coolant Pressure interlock contact (PC-1403 X1) in the valve opening circuit is open. When contact PC-1403 X1 is open, the valve opening contactor circuit cannot be energized and the valve cannot be opened. If the RCS pressure is below the setpoint the valve will operate as discussed below.

2. If the Reactor Coolant System pressure is below the valve opening setpoint (418 psig), contact PC-1403 X1 (Reactor Coolant Pressure interlock) will be closed in the valve opening contactor circuit. Depressing the control room pushbutton, will energize the opening contactor relay coil 52/O. The control board switch opening contacts are in series with the following contacts:

- RCS Pressure interlock contact (PC-1403 X1)
- Valve limit switch contact (LS-4) is open when the valve is full open; and LS-5 is closed when the valve is full closed.
- A torque switch contact (TS-18), in parallel with TS-5.
- Control board close contact is open except when the CLOSED pushbutton is depressed.

3. With all the contacts in Step 2 closed, the opening contactor relay coil (52/O) is energized with 120 VAC from the control power step down transformer. The opening contactor motor contacts (52/O) close and supply 480 VAC to the valve motor operator and the valve begins to open. The 52/O contacts connect the three phase power phases such that the motor rotation direction is reversed from the closing direction. The opening contactor simultaneously opens another contact (52/O) in the closing contactor circuit which prevents the closing contactor from picking up while the valve is opening i.e. the closing contactor is interlocked with the opening contactor to prevent both contactors from being energized at the same time. An additional opening contactor contact (52/O), which is in parallel with the opening main control room pushbutton, seals-in the opening contactor circuit so that the control switch can be released and the valve will continue to open. The seal-in contact is in series with the RCS pressure contact (PC-1403 1X). As the valve begins to open, limit switch contact LS-5 opens leaving the parallel torque switch contact (TS-18) to complete the circuit. Also, as the valve begins to open, limit switch contact LS-7 closes, turning on the red indicating light on the main control board. The green indicating light is controlled by limit switch contact LS-3 and is lit when the valve is not full open.

4. The valve continues to open until the valve torque switch contact (TS-18) opens. When the limit switch opens, the opening contactor relay coil de-energizes and all the 52/O motor contacts open, de-energizing the valve motor. The 52/O seal-in contacts open resetting the opening seal-in circuit. Also, when the valve is fully open, torque switch contact (TS-18) opens and the green indicating

light on the main control board is turned off. The red indicating light on the main control board remains lit to indicate that the valve is open.

During the time the valve is opening, the valve and the valve opening control circuit are protected from a over-torque condition by the torque switch contact TS-18 which is in series with the seal-in contact 52/O.

Automatic Closing of the RHR Valve

When the RCS pressure goes below the valve opening setpoint (418 psig) the valve can be opened or closed from the control switch in the Main Control Room as described above. When the valve is open, an increasing RCS pressure will automatically close the valve and prevent it from opening as described below.

1. With the valve open, an increasing RCS pressure above the valve closing setpoint (582 psig) will close contact PC-1403 2X in the valve closing contactor circuit. Limit switch contact LS-8, which is in series with contact PC-1403, is closed except when the valve is fully closed. When contact PC-1403 2X closes, the valve automatically begins to close. Contact PC-1403 2X, which is in parallel with the control board closing switch contact and with the control board opening switch contact, energizes the valve control circuit in the same manner as described above in the "Closing the Valve from the Main Control Room." The valve will continue to close until the valve is closed as described in the referenced section above. When the valve is fully closed, limit switch contact LS-8 will open preventing the re-actuation of the closing contactor from contact PS-1403 2X. After the valve is fully closed, it cannot be opened because the opening circuit is locked out as described above in the "Opening the Valve from the Main Control Room" section.

Reactor Coolant System Pressure Control Loop

The Reactor Coolant System hot leg pressure channels, PT-1402 and PT-1403 are used to provide the interlock signals for the RHR Inlet Isolation Valves MOV-1700 and 1701 (700 AND 701), respectively. Each pressure control loop consists of a pressure transmitter (PT-1402 or PT-1403), a channel test card, a loop power supply/current to voltage transformer, a dual circuit signal comparator, a comparator trip switch and two aux relays (PC-1402-1X and -2X or PC-1403-1X and -2X). The pressure transmitter measures the RCS pressure and provides a current output signal that is proportional to the measured pressure. The loop power supply takes the 4 to 20 mA current signal from the pressure transmitter and converts it to a 0 to 10 V proportional voltage signal. The non-isolated output of the loop power supply is input into the dual comparator. The dual comparator compares the pressure signal (input voltage) to the given setpoints. The comparator outputs are 0 VDC or 24 VDC depending on the signal to setpoint comparison. The 0/24 VDC outputs control the PC-1402 and PC-1403 aux relays which control the 118 VAC contactor 1X (opening) and 2X (closing) contacts. The dual comparator 1X output is 24 VDC when the pressure is below 418 psig, which energizes the aux relay, closing the 1X contacts. The dual comparator 2X output is 24 VDC when the pressure is below 582 psig, which energizes the aux relay, closing the 2X contacts. The channel test switch, various test points and jacks and the comparator trip switch are used during maintenance and calibration of the instrument loop.

As discussed above, the dual circuit signal comparator is used to provide bistable output signals (either on or off) depending on whether the measured signal is above or below the setpoint.

Specifically, for the RHR valve closing comparator circuit, whenever the RCS pressure measured by the pressure loop exceeds the valve closing setpoint (582 psig), the dual comparator 2X output circuit will de-energize the aux relay, closing the associated 2X contact in the valve closing contactor circuit, causing the valve to automatically close as discussed above. Whenever the RCS pressure is below the valve closing setpoint, the dual comparator 2X output circuit will energize the aux relay, opening the associated 2X contact in the valve closing contactor circuit, allowing the valve to remain open.

Similarly, for the RHR valve opening comparator circuit, whenever the RCS pressure exceeds the valve opening setpoint (418 psig), the dual comparator 1X output circuit will de-energize the aux relay, opening contact 1X in the valve opening contactor circuit and preventing the valve from being opened as discussed above. Whenever the RCS pressure is below the valve opening setpoint, the dual comparator 1X output circuit will energize the aux relay, closing contact 1X in the valve opening circuit, permitting the valve to be opened from the main control board control switch.

5.4 Shearon Harris

The following sections provide a description of the Group 4 lead plant, Shearon Harris.

5.4.1 General Description

Shearon Harris was granted a full power operating license on May 2, 1987. The Nuclear Steam Supply System (NSSS) consists of a 2775 MWt core with 3 reactor coolant loops. Each loop contains a Westinghouse Model D-4 steam generator and a Westinghouse Model 93A reactor coolant pump. The Shearon Harris plant NSSS is essentially identical to the Beaver Valley and North Anna Units. The major difference between the plants is the containment systems; Beaver Valley and North Anna have sub-atmospheric containments while Shearon Harris has an atmospheric containment.

The Shearon Harris containment is a steel lined reinforced concrete structure with a cylindrical wall, a hemispherical dome, and a flat foundation slab. The inside surface of the structure is lined with carbon steel plates welded together to form a barrier which is essentially leak tight.

The power conversion system consists of a Westinghouse tandem-compound turbine having one high-pressure and two low-pressure elements. Design output is 900 MWe (net), and steam dump to the condenser is rated at 70-percent full load. Three main steam lines carry steam from the top of the steam generators, through three main steam isolation valves (one in each line), to the turbine stop valves at the inlet to the turbine generator. Each main steam line is also equipped with five code safety valves and one power-operated relief valve.

Emergency Core Cooling System (ECCS) components include 3 cold leg accumulators, 3 centrifugal charging/HHSI pumps and 2 residual heat removal pumps (RHR/LHSI) and associated valves and piping. Two redundant on-site emergency diesels assure electric power supply to vital equipment. The borated refueling water storage facility consists of a large outside storage tank (RWST) which is the suction source for the ECCS pumps during the injection phase.

5.4.2 Residual Heat Removal System

Function

The primary function of the Residual Heat Removal System (RHRS) is to remove sensible heat from the Reactor Coolant System (RCS) during plant cooldown and refueling operations. This sensible heat load consists of residual decay heat from the reactor core and heat from operating reactor coolant pumps. The RHRS transfers heat from the RCS to the Component Cooling Water System (CCWS) to reduce reactor coolant temperature. The cold shutdown temperature is maintained until the plant is started up again.

As a secondary function, the RHRS is used to transfer refueling water between the Refueling Water Storage Tank (RWST) and the refueling cavity before and after the refueling operations. The RHRS also serves as part of the Safety Injection System to provide Low-Head-Safety-Injection (LHSI) emergency core cooling in the event of a break in either the RCS or steam system.

Overview

A basic flow diagram of the RHRS is shown in Figure 5-18. The RHRS consists of two separate trains of equal capacity, each independently capable of meeting the safety analysis design bases. Each train consists of one heat exchanger, one motor-driven pump and the associated piping, valves and instrumentation necessary for operational control. The inlet line to each train of the RHRS is connected to a reactor coolant loop hot leg, while the return lines are connected to the cold legs of each of the reactor coolant loops.

Each RHRS suction line is normally isolated from the RCS by two, series, motor-operated valves, while the cold leg and hot leg discharge lines are isolated by two check valves in each line. The RHRS suction/isolation valves, the inlet line pressure relief valve, and the discharge lines downstream of valves 1SI-341/340 (8888A/B) and 1SI-359 (8889) are located inside containment while the remainder of the system is located outside containment.

During normal RHRS operation, reactor coolant flows from the RCS hot legs 1 and 3 to the RHR pumps, through the tube side of the RHR heat exchangers and back to the RCS through the Safety Injection System (SIS) cold leg injection lines. The reactor coolant heat is transferred by the RHR heat exchangers to the component cooling water which circulates through the shell side of the RHR heat exchangers.

Coincident with RHRS normal operations, a portion of the reactor coolant flow may be diverted from downstream of the RHR heat exchangers to the Chemical and Volume Control System (CVCS) low-pressure letdown line for cleanup and/or pressure control. By regulating the diverted flowrate and the charging flow, the RCS pressure can be controlled during water-solid plant operations. Pressure regulation is necessary to maintain the pressure range dictated by the reactor vessel fracture prevention criteria requirements and by the RCP No. 1 seal differential pressure and NPSH requirements.

The RCS cooldown rate is manually controlled by regulating the reactor coolant flow through the tube side of the RHR heat exchangers. Instrumentation is provided to monitor system pressure, temperature and total flow.

System Operation

A discussion of RHRS operation during various reactor operating modes follows:

Reactor Startup

Generally, during cold shutdown, the RHRS operates to remove residual heat from the reactor core. The number of pumps and heat exchangers in service depends on the RHRS heat load at the time.

At initiation of plant startup, the RCS is completely filled, and the pressurizer heaters are energized. At least one RHR pump is operating with a portion of its discharge directed to the CVCS for purification and/or pressure control via a line that is connected to a cross-connect header downstream of the RHR heat exchanger. Once a steam bubble is formed in the pressurizer, the RHRS is isolated, and RCS pressure/inventory control are provided by the pressurizer spray, pressurizer heaters, normal letdown and charging systems.

Power Generation and Hot Standby Operation

The RHRS is not used during hot standby or power operations when the RCS is at normal pressure and temperature. Under these conditions, the RHRS is aligned for operation as part of the ECCS. Upon initiation of a safety injection signal ("S" signal), the RHRS pumps take suction from the RWST and inject borated water into the reactor vessel via the Safety Injection System cold leg injection headers. When the water in the RWST is depleted, the RHR pumps are automatically aligned to take suction from the containment recirculation sump. The RHR heat exchangers then cool the fluid being recirculated from the sump by the RHR pumps and deliver the cooled water to the reactor vessel cold legs. Hot leg recirculation is initiated approximately 24 hours after the accident and ECCS initiation. The flow path for this condition consists of both RHR pumps taking suction from the recirculation sump, discharging through the discharge cross connect valves and common discharge valve to the RCS hot legs 1 and 2. Since the CHG/HHSI pumps do not take suction from the containment sump, the RHR/LHSI pumps also supply the suctions of these pumps during recirculation.

Reactor Shutdown

The initial phase of reactor cooldown is accomplished by transferring heat from the RCS to the Steam and Power Conversion System (SPCS) through the use of the RCS steam generators and the SPCS steam dump valves or the SPCS atmospheric power-operated relief valves. When the reactor coolant temperature and pressure are reduced to 350°F and less than 363 psig, approximately 4 hours after reactor shutdown, the second phase of cooldown starts with the RHRS being placed in operation.

The reactor cooldown rate is limited by RCS equipment cooling rates based on allowable stress limits, as well as the operating temperature limits of the CCWS. As the reactor coolant temperature decreases, the reactor coolant flow through the RHR heat exchangers is increased to maintain a constant cooldown rate.

As cooldown continues, the pressurizer is filled with water and the RCS is operated in the water-solid condition. At this stage, pressure is controlled by regulating the charging flow rate and the letdown rate to the CVCS from the RHRS. After the Reactor Coolant System is depressurized, cooled to ≤140°F, and purged to reduce dissolved hydrogen concentration to a safe level, the reactor vessel head may be removed for refueling or maintenance.

Refueling

Both RHR pumps are utilized during refueling operations to pump borated water from the RWST to the refueling cavity. During this operation, the isolation valves in the inlet line of the RHRS are closed, and the isolation valves from the refueling water storage tank are opened. After the water level in the refueling cavity reaches normal refueling level, the inlet isolation valves are opened, the RWST supply valves are closed, and normal RHRS operation resumes.

During refueling, the RHRS remains in service with the number of pumps and heat exchangers in operation as required by the heat load and plant technical specifications. Additionally, a portion of the RHRS flow is directed to the CVCS for purification and eventual return to the RCS via the charging system.

Following refueling, the RHR pumps drain the refueling cavity to the top of the reactor vessel flange by pumping water from the RCS to the RWST.

Component Description

This section describes the major components of the RHR System.

RHR Pumps

Two pumps are installed in the RHR System. The pumps are sized to deliver sufficient reactor coolant flow through the RHR heat exchangers to meet the plant cooldown requirements. The use of two pumps ensures that cooling capacity is only partially lost should one pump become inoperable.

The RHR pumps are protected from overheating and loss of suction flow by miniflow bypass lines, located on the heat exchanger outlet, that diverts part of the flow back to the pump suction. A control valve located in each miniflow line is regulated by a signal from the flow transmitters located in each pump discharge header. The control valves open to divert flow back to the pump suction when the discharge flow is less than approximately 746 gpm at 350°F (713 gpm at 68°F) and close when it exceeds approximately 1402 gpm at 350°F (1339 gpm at 68°F). This arrangement ensures that the RHR pump does not overheat or vibrate when the discharge line is closed or when the RCS pressure exceeds the pump shutoff head during the ECCS injection phase.

A pressure transmitter in each pump discharge header provides pressure indication with a high pressure alarm in the main control room.

The RHR pumps, are vertical, centrifugal units with mechanical shaft seals. All pump surfaces in contact with reactor coolant are austenitic stainless steel or equivalent corrosion resistant material.

RHR Heat Exchangers

Two residual heat exchangers are installed in the RHR System. The heat exchanger design is based on heat load and temperature differences between reactor coolant and component cooling water existing 20 hours after reactor shutdown when the temperature difference between the two systems is small. The installation of two heat exchangers ensures that the heat removal capacity of the system is only partially lost if one heat exchanger becomes inoperative. The heat exchangers are of the shell and U-tube type. Reactor coolant circulates through the tubes, while component cooling water circulates through the shell. The tubes are welded to the tubesheet to prevent leakage of reactor coolant.

RHRS Valves

The following sections describe the Shearon Harris RHRS valves. To facilitate other plants in this grouping referencing this discussion, corresponding Westinghouse valve I.D. numbers are provided in parenthesis.

Inlet Isolation Valves 1RH-2, 1RH-40, 1RH-1 and 1RH-39 (8701A & B and 8702A & B)

These valves are twelve-inch, motor-operated, gate valves which are normally-closed except when the RHRS is in operation. Both valves are provided with a manual control (open/closed) on the Main Control Board and will fail in the "as-is" position.

Valves 1RH-1 (8702A) and 1RH-39 (8702B) are interlocked with RCS pressure transmitter PT-403 and valves 1RH-2 (8701A) and 1RH-40 (8701B) are interlocked with pressure transmitter PT-402. These interlocks prevent the inadvertent opening of the valves when the RCS pressure is above 363 psig. The valves also close automatically when the RCS pressure is higher than 700 psig. A more detailed description of the interlocks is provided in Section 5.3.3.

Heat Exchanger Flow Control Valves 1RH-30 and 1RH-66 (HCV-603A and HCV-603B)

The reactor coolant flow rate through the RHR heat exchangers is adjusted by ten-inch, air-operated, butterfly valves 1RH-30 (HCV-603A) and 1RH-66 (HCV-603B). Positioning of these valves from the control room regulates the reactor coolant flow and temperature exiting the heat exchangers. These valves are normally full open during power operation.

Bypass Flow Control Valves 1RH-20 and 1RH-58 (FCV-605A and FCV-605B)

These valves, located in the heat exchanger bypass lines, are eight-inch, air-operated, butterfly valves. The valve may be positioned automatically from its associated flow transmitter (FT-605A or FT-605B) or manually from the control room. As the operator positions 1RH-30 (FCV-603A) to regulate the plant cooldown rate, bypass valve 1RH-20 (FCV-605A) automatically repositions itself to maintain a constant return flow to the RCS. 1RH-66 (HCV-603B) and 1RH-58 (FCV-605B) act in a similar manner.

Miniflow Stop Valves 1RH-31 and 1RH-69 (FCV-602A and FCV-602B)

These normally-closed valves are three-inch, motor-operated, gate valves which are located in the residual heat removal pump miniflow line. This miniflow line ensures that the RHR pump does not overheat or vibrate when the discharge line is closed or when RCS pressure exceeds the pump shutoff head. The valves are controlled by flow transmitters FT-602A and FT-602B respectively, which are located in the discharge line of the RHR pump. These valves will open when the pump discharge flow is less than approximately 746 gpm at 350°F (713 gpm at 68°F). When the pump flow exceeds approximately 1402 gpm at 350°F (1339 gpm at 68°F), the corresponding valve will close. (When the RHR/LHSI pumps are stopped, these valves remain open.)

Crosstie Valves SI-326 and SI-327 (8887A and 8887B)

These motor-operated valves, located in the piping crosstie downstream of the residual heat exchangers. These valves are open during normal cooldown operations and the ECCS injection phase; however, they are closed to provide train separation during cold leg recirculation, and at least one is re-opened for hot leg recirculation.

Cold leg Injection Line Check Valves 1SI-356, 1SI-357, 1SI-358, 1SI-81, 1SI-82 and 1SI-83 (8973A,B,C and 8998A,B,C)

There are two check valves in each branch of the cold leg injection line to prevent backflow from the RCS.

RHRS Return Line Check Valves 1SI-346 and 1SI-347 (8974A and 8974B)

One check valve is located in each branch of the RHRS return line to prevent backflow to an idle RHRS/LHSI pump during cold leg recirculation.

Gate Valve 1SI-340 and 1SI-341 (8888A and 8888B)

There is a ten-inch, normally-open, motor-operated, gate valve in each parallel discharge line from the residual heat removal pump, downstream of the heat exchanger and hot leg recirculation crosstie header. These valves are used to isolate the RHRS from the cold legs during hot leg recirculation or during refueling operations when returning water to the RWST.

Crosstie Valves 1RH-26 and 1RH-64 (8720A and 8720B)

These two, normally-closed, manual valves are used to line up a portion of each RHR pump discharge to be directed to the CVCS letdown. Throttle valve 1CS-28 (HCV-142) is used to control this flow. This flow path is used during a plant cooldown and during water-solid plant operations when the CVCS is used to control RCS pressure.

Gate Valves 1RH-25 and 1RH-63 (8706A and 8706B)

Gate Valves 1RH-25 (8706A) and 1RH-63 (8706B) isolate the flow paths (connected to the discharge of the RHR heat exchangers) which supply water to the suction of the centrifugal charging pumps during the recirculation phase of safety injection. 1RH-25 (8706A) and 1RH-63 (8706B) are normally-closed and are interlocked with the RHRS suction/isolation valves.

Gate Valve 1SI-359 (8889)

During hot leg recirculation the RHR pumps are aligned to deliver flow through cross-connect valves 1SI-327 (8887A) and 1SI-326 (8887B), and common discharge valve 1SI-359 (8889). This realignment is initiated at approximately 24 hours after accident initiation. Hot leg recirculation prevents crystallization of boric acid in the core and quenchs the steam bubble in the top of the core.

RWST Isolation Valves 1SI-320/321 and 1SI-322/323 (8958A/B and 8809A/B)

Check valves 1SI-320/321 (8958A/B) and motor-operated gate valves 1SI-322/323 (8809A/B) isolate the RWST from each RHR/LHSI pump's suction. Gate valves 1SI-322/323 (8809A/B) are interlocked with the RHRS suction isolation valves.

Sump Isolation Valves 1SI-300/301 and 1SI-310/311 (8811A/B and 8812A/B)

There are two, series, motor-operated gate isolation valves in each RHR/LHSI pump suction line from the sump. These valves are normally closed and are automatically opened (from a low-low RWST level signal coincident with an 'S'-signal) during the switchover operations from injection to recirculation.

RHRS Discharge Relief Valves 1SI-328/329 and 1SI-330 (8864A/B and 8865)

A 3/4-inch relief valve is located in each RHR/LHSI cold leg and hot leg discharge header. These valves protect against overpressurization of the piping due to any RCS backleakage or thermal expansion of trapped water. The design capacity of these valves is 20 gpm at 600 psig.

Relief Valves 1RH-7 and 1RH-45 (8708A and 8708B)

There is one, 3-inch relief valve (inside containment) in each RHRS suction line from the RCS hot leg. The relief valves are located immediately downstream of the RHRS suction/isolation valve 1RH-2 and 1RH-40 (8701A and 8701B). These relief valves prevent RHRS overpressurization by discharging to the Pressurizer Relief Tank (PRT) when pressures within the RHRS suction line exceed 450 psig. These valves have a design capacity of 900 gpm at the 450 psig setpressure.

5.4.3 Current RHRS Suction Isolation Valves Interlocks and Functional Requirements

The following sections provide a description of the Shearon Harris suction/isolation valve interlocks and valve control circuits.

5.4.3.1 Current Interlocks

There are two, normally-closed, motor-operated, series, isolation valves in each of the two RHR pump suction lines from the RCS hot legs. The two valves inside the missile barrier, 1RH-1 and 1RH-39 (8702A & B), are designated as the inner isolation valves, while the two valves outside the missile barrier, 1RH-2 and 1RH-40 (8701A & B), are designated as the outer isolation valves. The interlock features provided for the inner isolation valves are identical to those provided for the outer isolation valves.

Each valve is interlocked against opening unless all of the following conditions are met:

1. The RCS pressure, as measured by the appropriate wide range pressure channel, is less than 363 psig. This assures that the RHRS cannot be overpressurized by aligning it to the RCS when RCS pressure plus RHRS pump head would exceed the RHRS design pressure.

2. The corresponding RHRS pump/RWST suction isolation valve is closed. This assures positive isolation of the RWST and RHRS/RWST suction piping before initiating a normal cooldown.

3. The corresponding recirculation line to the charging/high-head safety injection pumps isolation valve is closed. This assures the suction of the high-head safety injection system cannot be overpressurized by the RHR/LHSI pump's discharge pressure during normal cooldown operation ($P<400$ psig).

In addition to the above interlocks each valve is also interlocked to automatically close on increasing RCS pressure greater than 700 psig. This feature assures that both isolation valves will be closed during a plant startup prior to reaching operating conditions, if one valve had been inadvertently left open by the operator. The operator may close the suction/isolation valve at any time.

The current interlocks for valves 1RH-2 and 1RH-40 (8701A & B) and 1RH-1 and 1RH-39 (8702A & B) are shown functionally on Figure 5-19.

5.4.3.2 RHRS Common Suction Isolation Valve Description

The RHR common suction isolation valves are motor-operated valves that can be opened or closed from the Main Control Board. The valve will automatically close on increasing reactor coolant system pressure. On decreasing Reactor Coolant System pressure, the valve control circuit receives an interlock signal that allows the valve to be opened using the Main Control Board switch. On reactor coolant pressure above the setpoint, the valve control circuit is disabled and the valve cannot be opened.

The valve control circuit consists of control switches, limit switches, torque switches, contactors, relays, indicating lights, a 3 phase, 480 VAC motor and a pressure control loop. The control switches are located in the main control room. The limit switches are located in the valve motor operator and provide indication of the position of the valve. Relays are used for providing control signals. The contactor, located in the motor control center, is switched on and off to provide the power to the valve. The contactor also provides contacts that are used in the valve control circuit. There are red and green indicating lights on the Main Control Board to show the position of the valve. The valve motor operator is located at the valve and is used to change the position of the valve. The pressure control loop measures Reactor Coolant System pressure and provides output signals to the valve control circuit based on the system pressure that allows the valve to be opened from the control switch or automatically closed.

The following provides a detailed description of the valve control circuit for 1RH2. Operation of valves 1RH1, 1RH39 and 1RH40 is similar. Figures 5-20 through 5-23 show the appropriate details of the circuits.

Closing the Valve from the Main Control Room

With the valve in the full open position, the valve can be closed from the control switch in the main control room as described in the following steps:

1. Placing the control board switch to the CLOSE position will energize the closing contactor coil (42/S). The control board switch closing contacts 2B1-2B2 are in series with a limit switch contact (20/1), which is closed when the valve is open, a torque switch contact (20/17) which is in parallel with 20/1, and a contact (42/O) which is closed when the opening contactor coil (42/O) is not energized.

2. With all the contacts in Step 1 closed, the contactor closing coil 42/S is energized with 120 VAC power from the 480/120 VAC control power step down transformer. The closing contactor contacts (42/S) in the motor circuit close and supply 480 VAC to the valve motor operator and the valve begins to close. The closing contactor simultaneously opens another contact (42/S) in the opening control circuit which prevents the opening contactor relay from picking up while the valve is closing (i.e., the opening control circuit is interlocked with the closing control circuit to prevent both contactor relays from being energized at the same time). An additional closing contactor contact (42/S), which is in parallel with the control board switch, seals-in the closing circuit so that the control board switch can be released and the valve will continue to close. As the valve begins to close, limit switch contact 20/3 closes, turning on the green indicating light on the Main Control Board. The red indicating light is controlled by limit switch contact 20/15 and is lit when the valve is open or during travel (i.e., both lights are lit during travel).

3. Limit switch contacts 20/1 open as the valve begins to close, leaving only the parallel torque switch contact (20/17) to complete the circuit. The valve continues to close until the valve torque switch contact (20/17) opens indicating the valve is torqued closed. When the torque switch contact opens, the contactor coil de-energizes and the motor 42/S contacts open which in-turn de-energize the valve motor. The 42/S seal-in contacts open, resetting the closing seal-in circuit. The 42/S contact in the opening control circuit closes to allow the valve opening control circuit to actuate. When the valve is fully closed, a limit switch contact (20/15) opens which turns off the red indicating light on the main control board, leaving the green indicating light on the main control board to show that the valve is closed. During the time the valve is closing, if the valve should encounter difficulties in closing, the torque switch contact (20/17) in the closing contactor circuit will open and de-energize the closing contactor as described above.

Opening the Valve from the Main Control Room

With the valve in the closed position as described above, the valve can be opened from the control switch in the main control room as follows:

1. The opening of the RHR valve is restricted by the Reactor Coolant System pressure. If the RCS pressure is below the valve opening setpoint (363 psig), the valve can be opened using the Main Control Board switch as described in Steps 2 through 4 below. The valve is not automatically opened on RCS pressure below the valve opening setpoint. If the RCS pressure is above the valve opening setpoint, the valve cannot be opened. When the RCS pressure is above the opening setpoint, the Reactor Coolant Pressure interlock contact (K-734) in the valve opening circuit is open. When contact K-734 is open, the valve opening contactor circuit cannot be energized and the valve cannot be opened. If the RCS pressure is below the setpoint the valve will operate as discussed below.

2. If the Reactor Coolant System pressure is below the valve opening setpoint (363 psig), contact K-734 (Reactor Coolant Pressure interlock) will be closed in the valve opening contactor circuit. Operating the Main Control Board switch to OPEN the valve will energize the opening contactor relay coil 42/O. The Control Board switch opening contacts (1A1-1A2) are in series with the following contacts:

   - RCS Pressure interlock contact (K-734)
   - Two valve limit switch contacts (20/5 & 20/4) which are closed when the valve is closed
   - A torque switch contact (20/18), in parallel with 20/5
   - A RHR RWST suction valve (1-8809) interlock contact (20-1/bc)
   - A RHR to CVCS recirculating line valve (1-8706) interlock contact (20-1/bc).

   Both of the interlocking valves must be closed to close the series contacts noted above.

3. With all the contacts in Step 2 closed, the opening contactor relay coil (42/O) is energized with 120 VAC from the control power step down transformer. The opening contactor motor contacts (42/O) close and supply 480 VAC to the valve motor operator and the valve begins to open. The 42/O contacts connect the three phase power phases such that the motor rotation direction is reversed from the closing direction. The opening contactor simultaneously opens another contact (42/O) in the closing contactor circuit which prevents the closing contactor from picking up while the valve is opening (i.e., the closing contactor is interlocked with the opening contactor to prevent both contactors from being energized at the same time). An additional opening contactor contact (42/O), which is in parallel with the opening Main Control Board switch contact, seals-in the opening contactor circuit so that the control switch can be released and the valve will continue to open. The seal-in contact is also in parallel with the RCS pressure contact (K-734), and the two

interlocking valve contacts. As the valve begins to open, limit switch contact 20/5 opens leaving the parallel torque switch contact (20/18) to complete the circuit. Also, as the valve begins to open, limit switch contact 20/15 closes, turning on the red indicating light on the Main Control Board. The green indicating light is controlled by limit switch contact 20/3 and is lit when the valve is closed or during travel.

4. The valve continues to open until the valve limit switch contact (20/4) opens and the valve is fully open. When the limit switch opens, the opening contactor relay coil de-energizes and all the 42/O motor contacts open, de-energizing the valve motor. The 42/O seal-in contacts open resetting the opening seal-in circuit. Also, when the valve is fully open, a limit switch contact (20/3) opens and the green indicating light on the Main Control Board is turned off. The red indicating light on the Main Control Board remains lit to indicate that the valve is open.

   During the time the valve is opening, the valve and the valve opening control circuit are protected from a over-torque condition by the torque switch contact 20/18 which is in series with the seal-in contact 42/O.

Automatic Closing of the RHR Valve

When the RCS pressure goes below the valve opening setpoint (363 psig) the valve can be opened or closed from the control switch in the Main Control Room as described above. When the valve is open, an increasing RCS pressure will automatically close the valve and prevent it from opening as described below.

1. With the valve open, an increasing RCS pressure above the valve closing setpoint (700 psig) will close contact K-735 in the valve closing contactor circuit. Limit switch contact 20/8, which is in series with contact K-735, is closed except when the valve is fully

closed. When contact K-735 closes, the valve automatically begins to close. Contact K-735, which is in parallel with the Control Board closing switch contact, energizes the valve control circuit in the same manner as described above in the "Closing the Valve from the Main Control Room." The valve will continue to close until the valve is torqued closed as described in the referenced section above. When the valve is fully closed, limit switch contact 20/8 will open preventing the re-actuation of the closing contactor from contact K-735 due to the reset of the torque switch contact (20/17). After the valve is fully closed, it cannot be opened because the opening circuit is locked out as described above in the "Opening the Valve from the Main Control Room" section.

Reactor Coolant System Pressure Control Loop

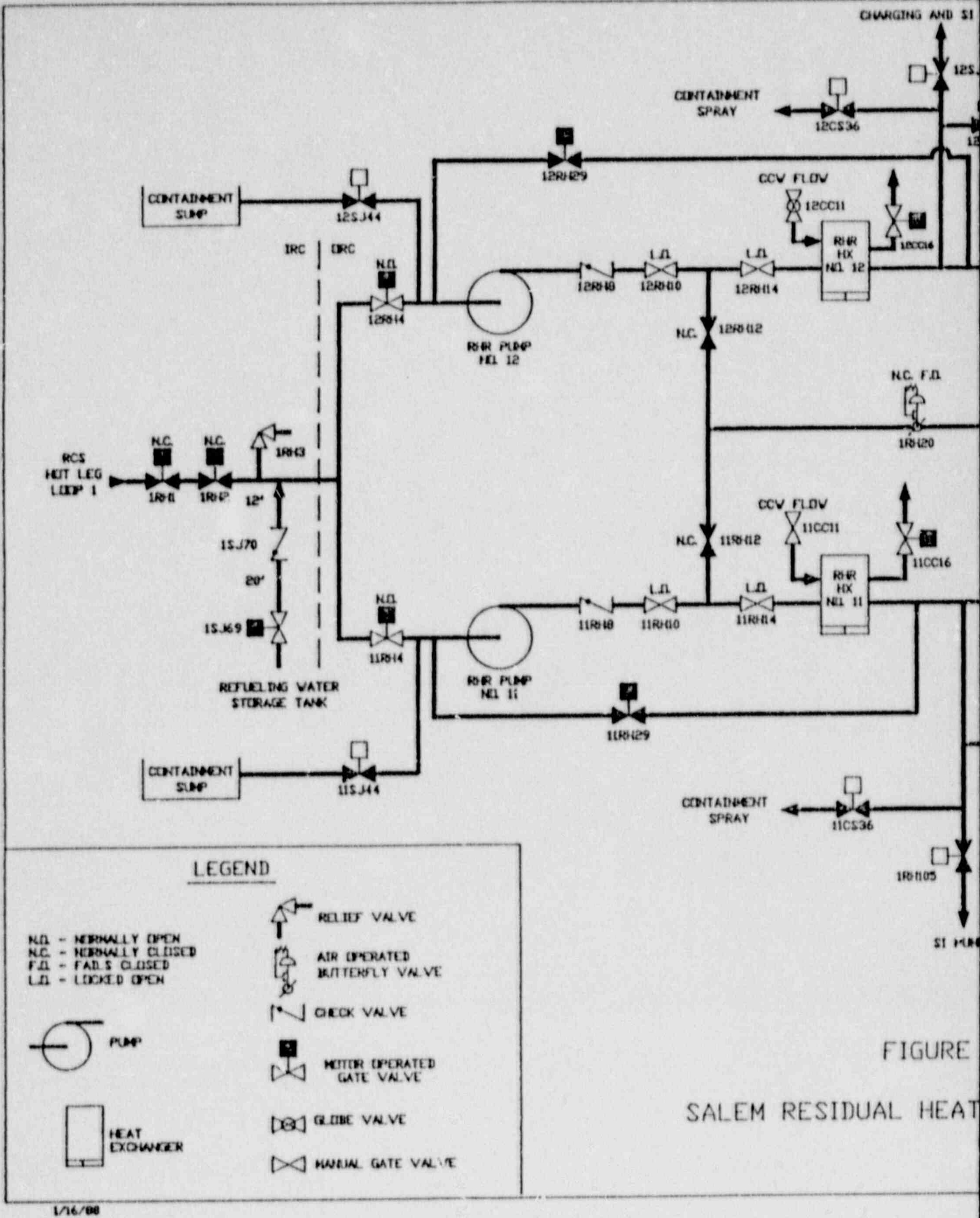
The Reactor Coolant System hot leg pressure channel, PT-402 is used to provide the interlock signals for the RHR inlet isolation valves 1-8701A and 1-8701B. PT-403 is used to provide the interlock signals for RHR inlet isolation valves 1-8702A and 1-8702B. Each pressure control loop consists of the pressure transmitter (PT-402 or PT-403), a channel test card, a loop power supply/current to voltage transformer, a signal isolator, a dual circuit signal comparator, and two aux relays. The pressure transmitter measures the RCS pressure and provides a current output signal that is proportional to the measured pressure. The loop power supply takes the 4 to 20 mA current signal from the pressure transmitter and converts it to a 0 to 10 V proportional voltage signal. The non-isolated output of the loop power supply is input into the signal isolator and into the dual comparator. The dual comparator compares the pressure signal (input voltage) to the given setpoints. The comparator outputs are 0 VDC or 24 VDC depending on the signal to setpoint comparison. The 0/24 VDC outputs control the aux relays which control the 118 VAC K-734 and K-735 relays. The K-734 and K-735 relays open and close the valve contactor K-734 and K-735 contacts. The A comparator output is 24 VDC when the pressure is below 363 psig, which energizes the aux relay, which energizes the K-734 relay, closing the K-734 contacts.

The B comparator output is 24 VDC when the pressure is above 700 psig, which energizes the aux relay, which energizes the K-735 relay, closing the K-735 contacts. The various test points and jacks are used during maintenance and calibration of the instrument loop.

As discussed above, the dual circuit signal comparator is used to provide bistable output signals (either on or off) depending on whether the measured signal is above or below the setpoint.

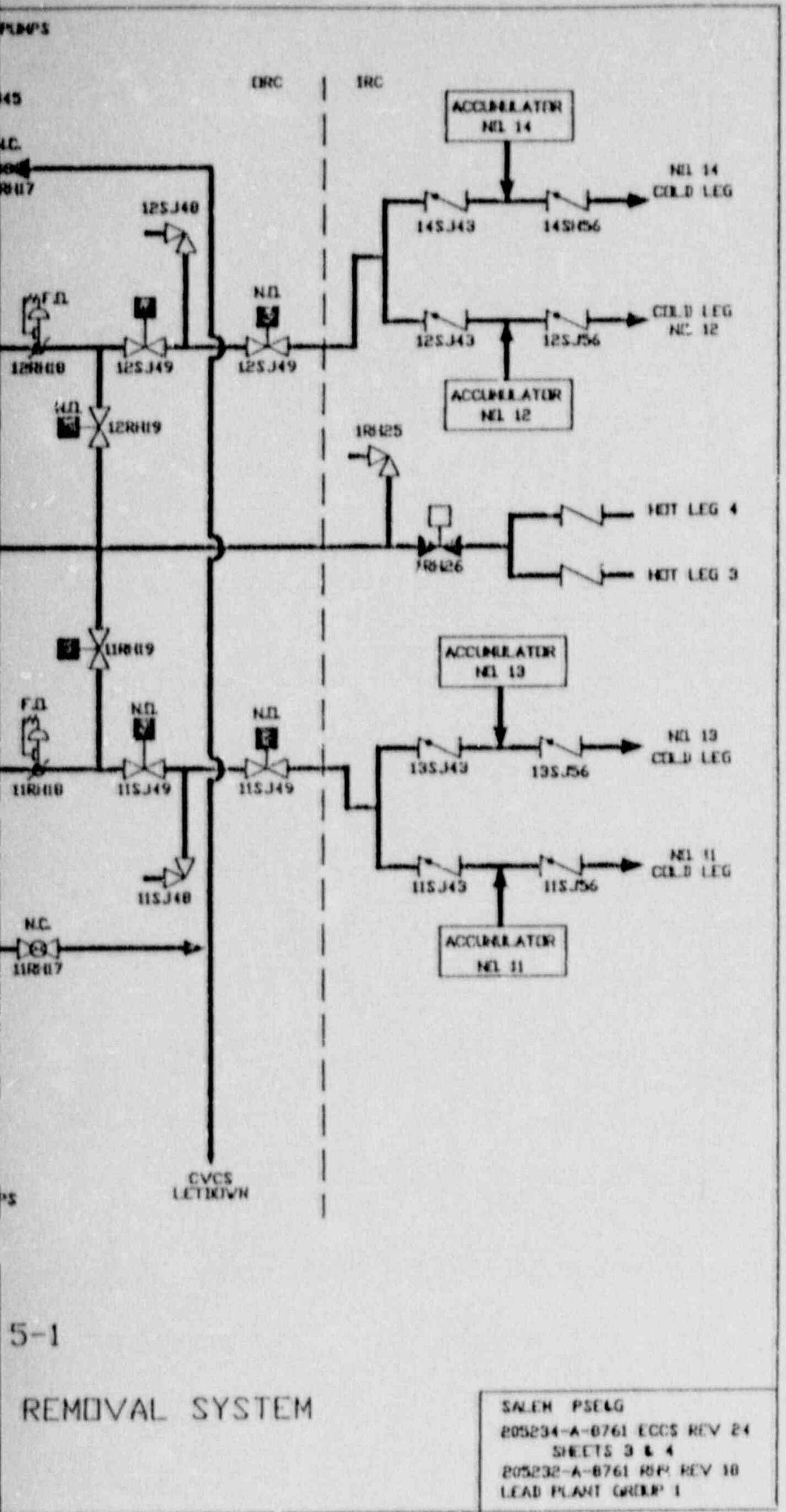
Specifically, for the RHR valve interlock circuit, whenever the RCS pressure measured by the pressure loop exceeds the valve closing setpoint (700 psig), the dual comparator output circuit (B) will energize the aux relay, which energizes the K-735 relay closing the associated contact K-735 in the valve closing contactor circuit, causing the valve to close as discussed above. Whenever the RCS pressure is below the valve closing setpoint, the comparator output circuit will de-energize the aux relay, which de-energizes the K-735 relay, opening the associated contact K-735 in the valve closing contactor circuit, allowing the valve to remain open.

Similarly, for the valve opening comparator output, whenever the RCS pressure exceeds the valve opening setpoint (363 psig), the dual comparator output circuit (A) will de-energize the aux relay, which de-energizes the K-734 relay, opening contact K-734 in the valve opening contactor circuit and preventing the valve from being opened as discussed above. Whenever the RCS pressure is below the valve opening setpoint, the comparator output circuit (A) will energize the aux relay, which energizes the K-734 relay, closing contact K-734 in the valve opening circuit, permitting the valve to be opened from the Main Control Board control switch.



FIGURE

SALEM RESIDUAL HEAT



SI APERTURE CARD

Also Available On Aperture Card

Figure 5-1

Salem Residual Heat Removal System

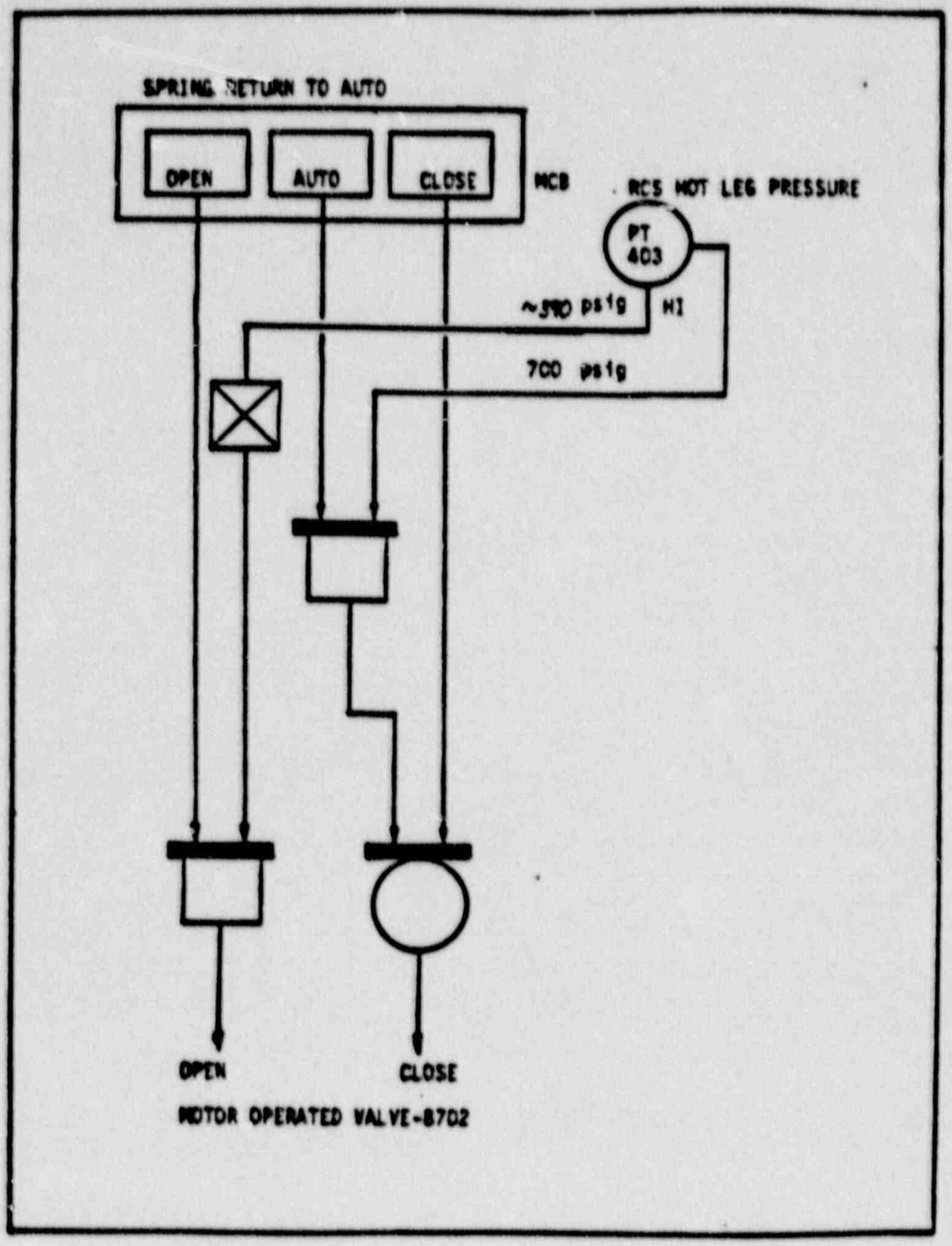


Figure 5-2. Salem Current Interlock-MOV-8702 (1RH-1)

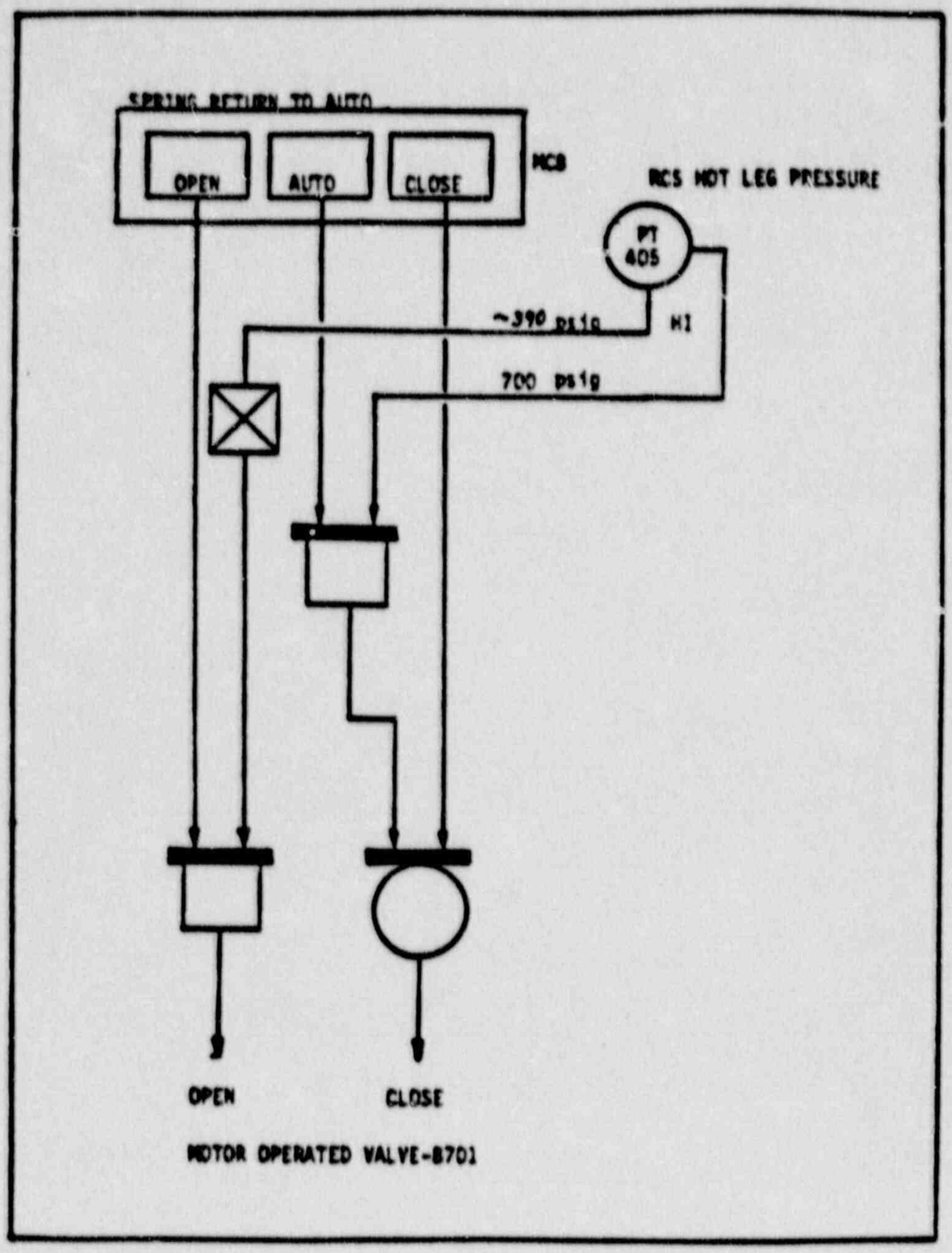
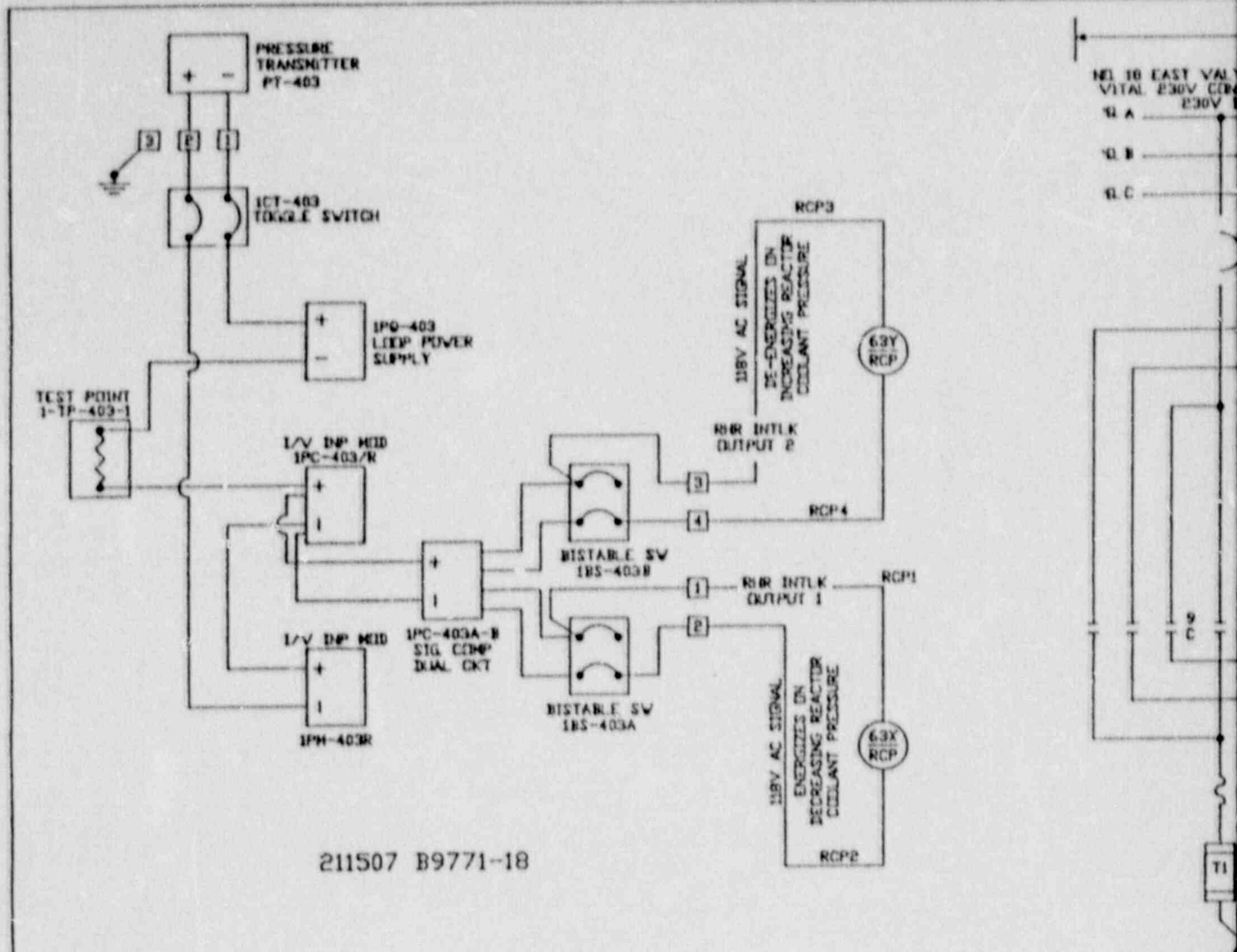


Figure 5-3. Salem Current Interlock-MOV-8701 (1RH-2)



211507 B9771-18

LEGEND

- CONTROL CIRCUIT BREAKER
- FUSE
- DIODE
- CONTACT OPEN
- CONTACT CLOSED
- THERMAL OVERLOADS
- (R) INDICATING LIGHTS R - RED G - GREEN
- VOLTAGE TRANSFORMER

NOTES

5 / CSV2	CLOSING RELAY COIL
6 / CSV2	OPENING RELAY COIL
33 / OVO	VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY OPEN
33 / OVC	VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY CLOSED
33 / CVO	VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY OPEN
33 / CVC	VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY CLOSED
9 / O	REVERSING CONTACTOR OPENING
9 / C	REVERSING CONTACTOR CLOSING
63Y / RCP	REACTOR COOLANT PRESSURE AUX RELAY
63X / RCP	REACTOR COOLANT PRESSURE AUX RELAY
9X / C	AUX RELAY TO CONTACTOR CLOSING COILS
9X / O	AUX RELAY TO CONTACTOR OPENING COILS
33X / CSV2	VALVE FULLY OPEN AUX RELAY
33Y / CSV2	VALVE FULLY CLOSED AUX RELAY

28V DC SUPPLY AT CONTROL CABINET

RHR_1RH1

2/1/88

SALEM RHR SUCTION ISOLATION VALVE 1RH1 CONTROL CIRCUITRY

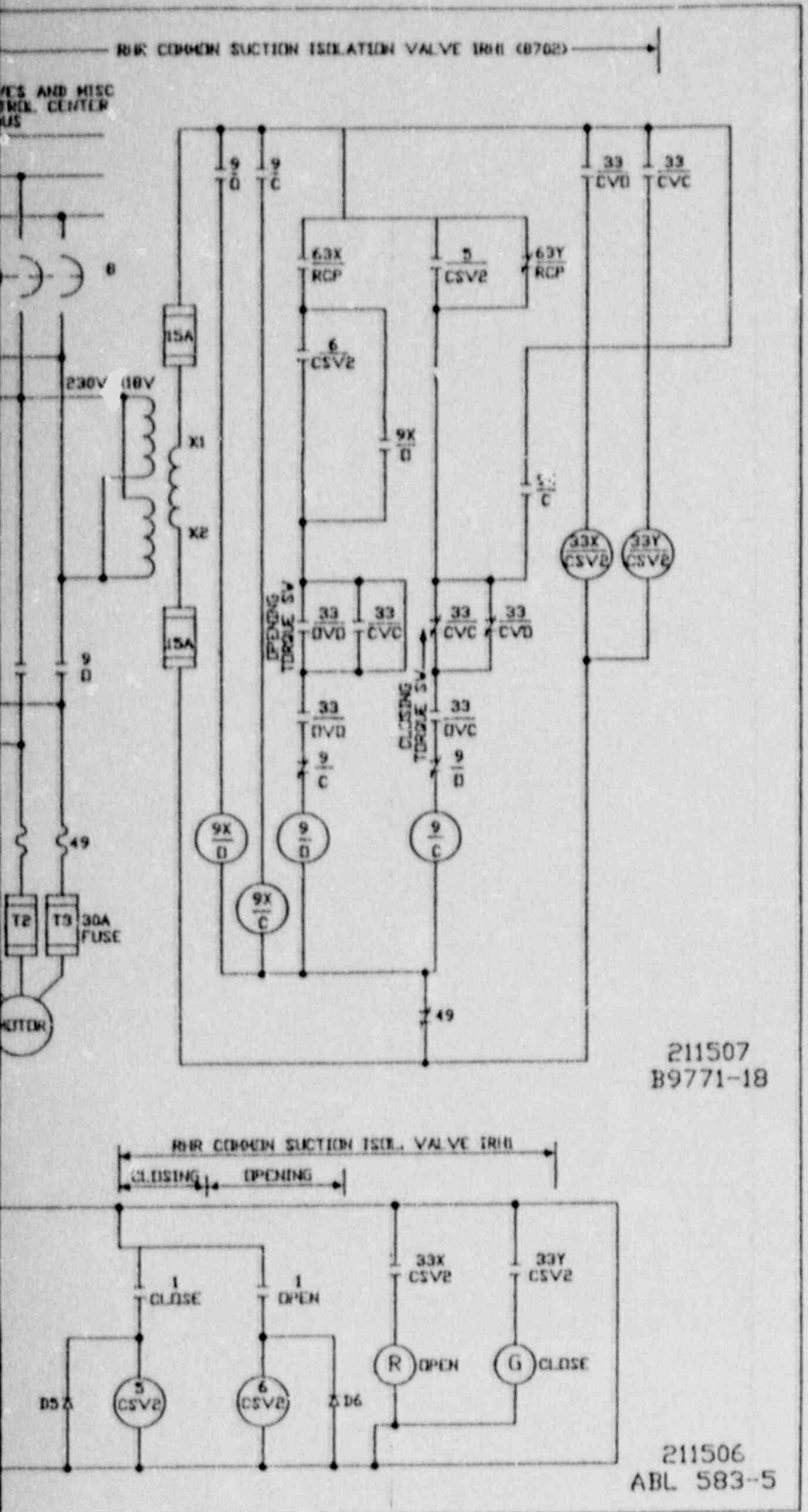
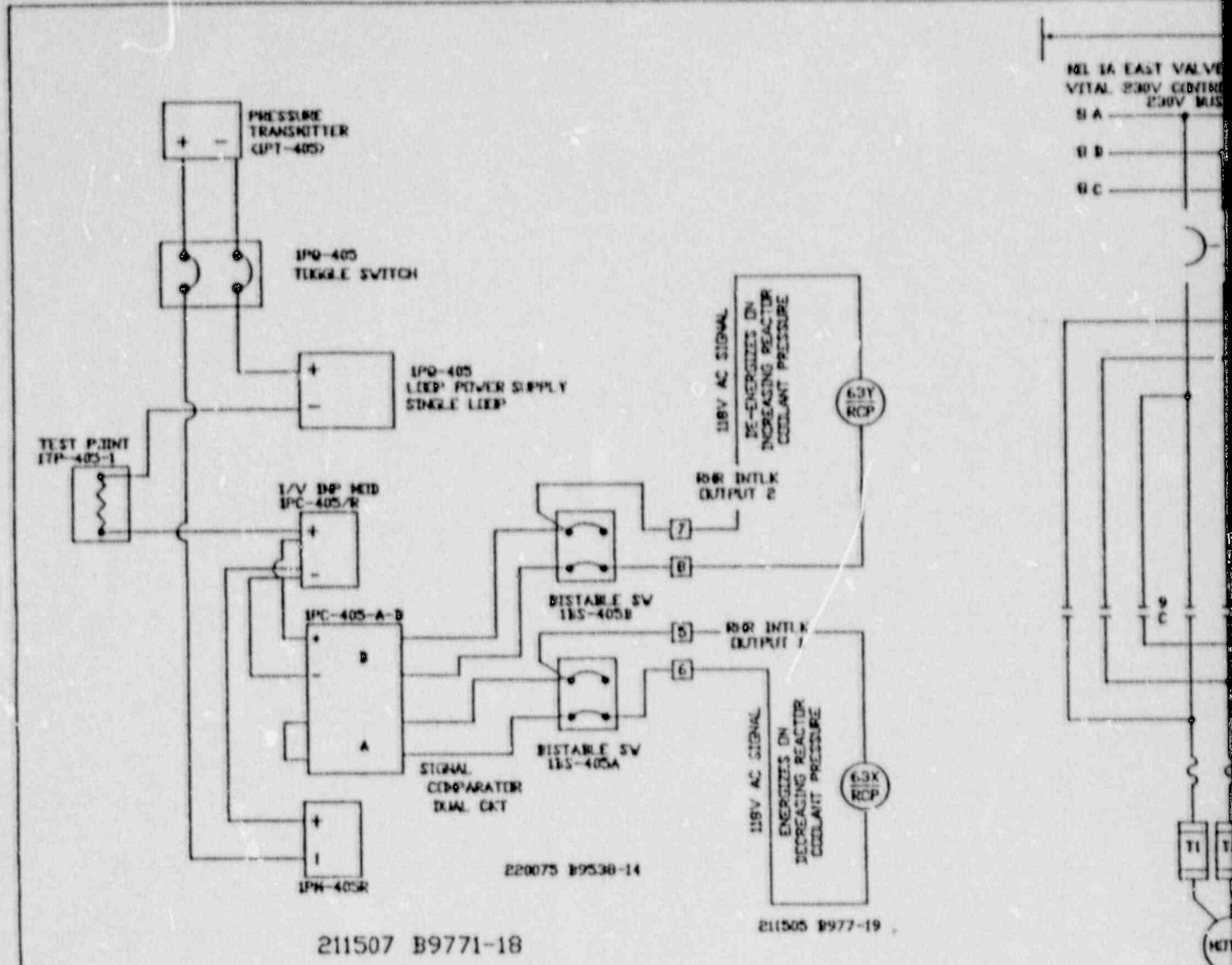


Figure 5-4

Salem RHRS Suction/Isolation Valve Control Circuitry MOV-8702 (1RH-1)



LEGEND

-))) CONTROL CIRCUIT BREAKER
- FUSE
- "A" DIODE
- CONTACT OPEN
- CONTACT CLOSED
- THERMAL OVERLOADS
- (R) INDICATING LIGHTS R - RED G - GREEN
- VOLTAGE TRANSFORMER

NOTES

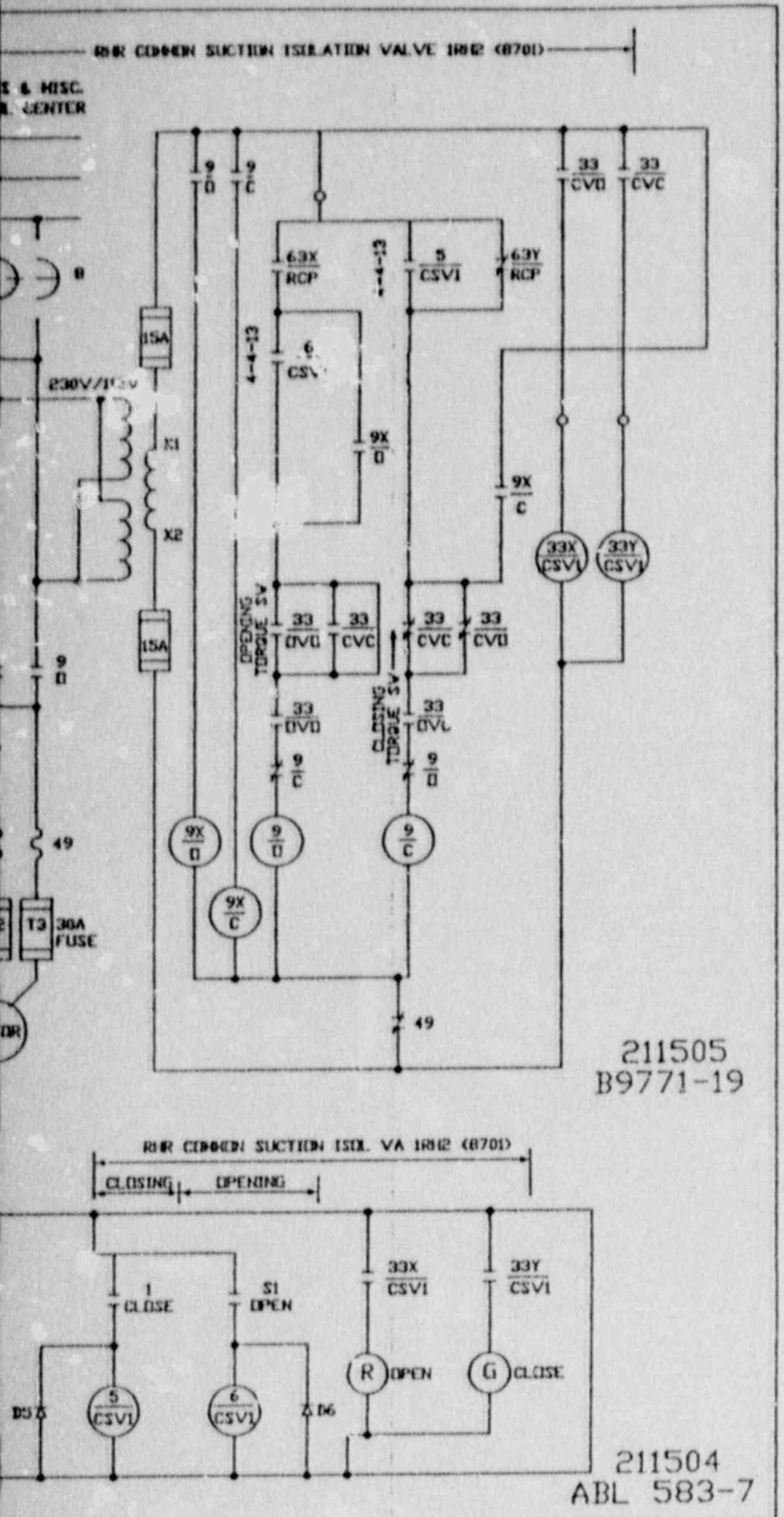
- 5/CSV1 CLOSING RELAY COIL
- 6/CSV1 OPENING RELAY COIL
- 33/DVO VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY OPEN
- 33/DVC VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY CLOSED
- 33/CVO VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY OPEN
- 33/CVC VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY CLOSED
- 9/O REVERSING CONTACTOR OPENING
- 9/C REVERSING CONTACTOR CLOSING
- 63Y/RCP REACTOR COOLANT PRESSURE AUX RELAY
- 63X/RCP REACTOR COOLANT PRESSURE AUX RELAY
- 9X/C AUX RELAY TO CONTACTOR CLOSING COILS
- 9X/O AUX RELAY TO CONTACTOR OPENING COILS
- 33X/CSV1 VALVE FULLY OPEN AUX RELAY
- 33Y/CSV1 VALVE FULLY CLOSED AUX RELAY

28V DC SUPPLY AT CONTROL CABINET

RHR_1RH2

6/26/87

SALEM RHR SUCTION
ISOLATION VALVE 1RH2
CONTROL CIRCUITRY

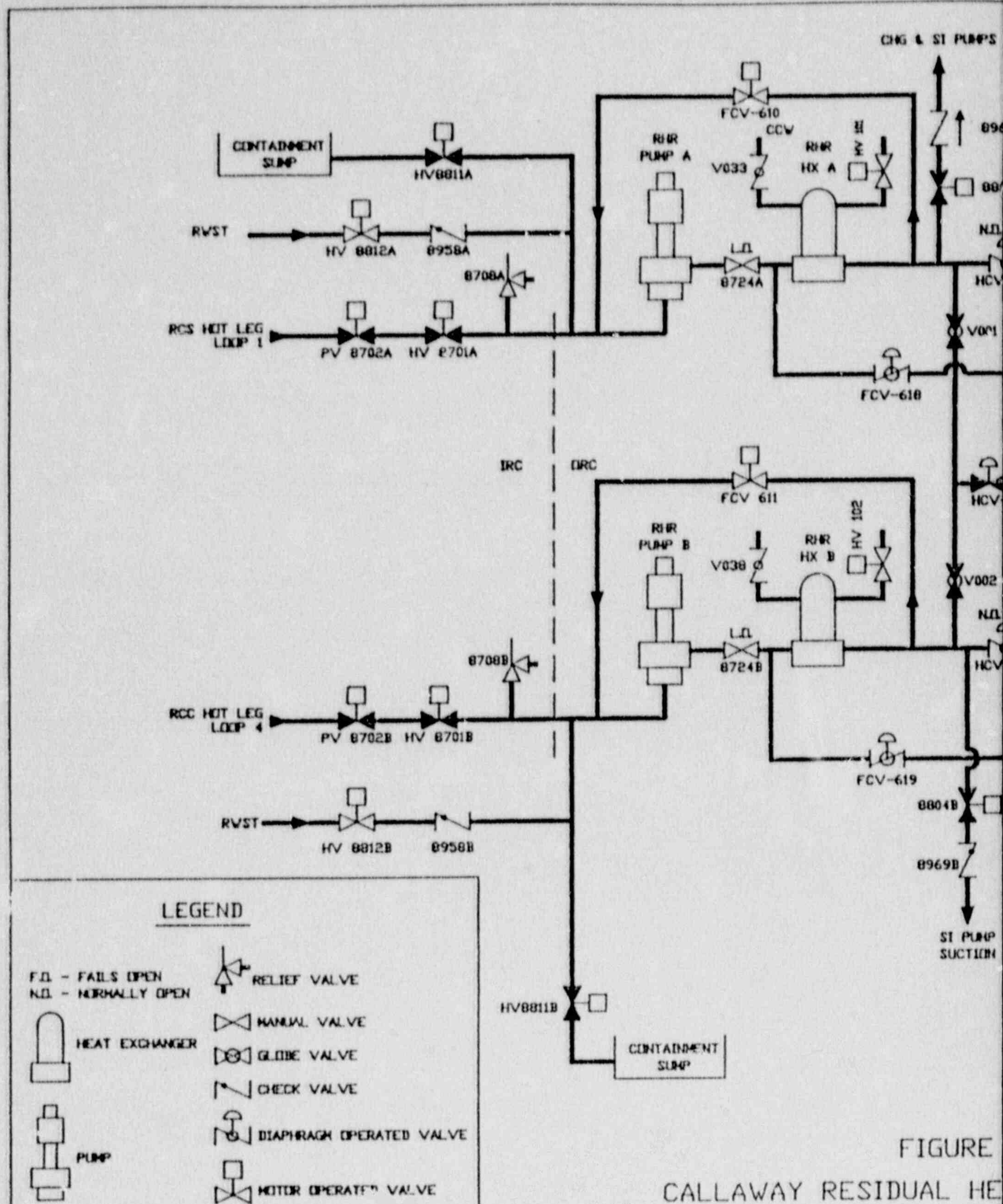


SI APERTURE CARD

Also Available On Aperture Card

Figure 5-5

Salem RHRS Suction/Isolation Valve Control Circuitry MOV-8701 (1RH-2)

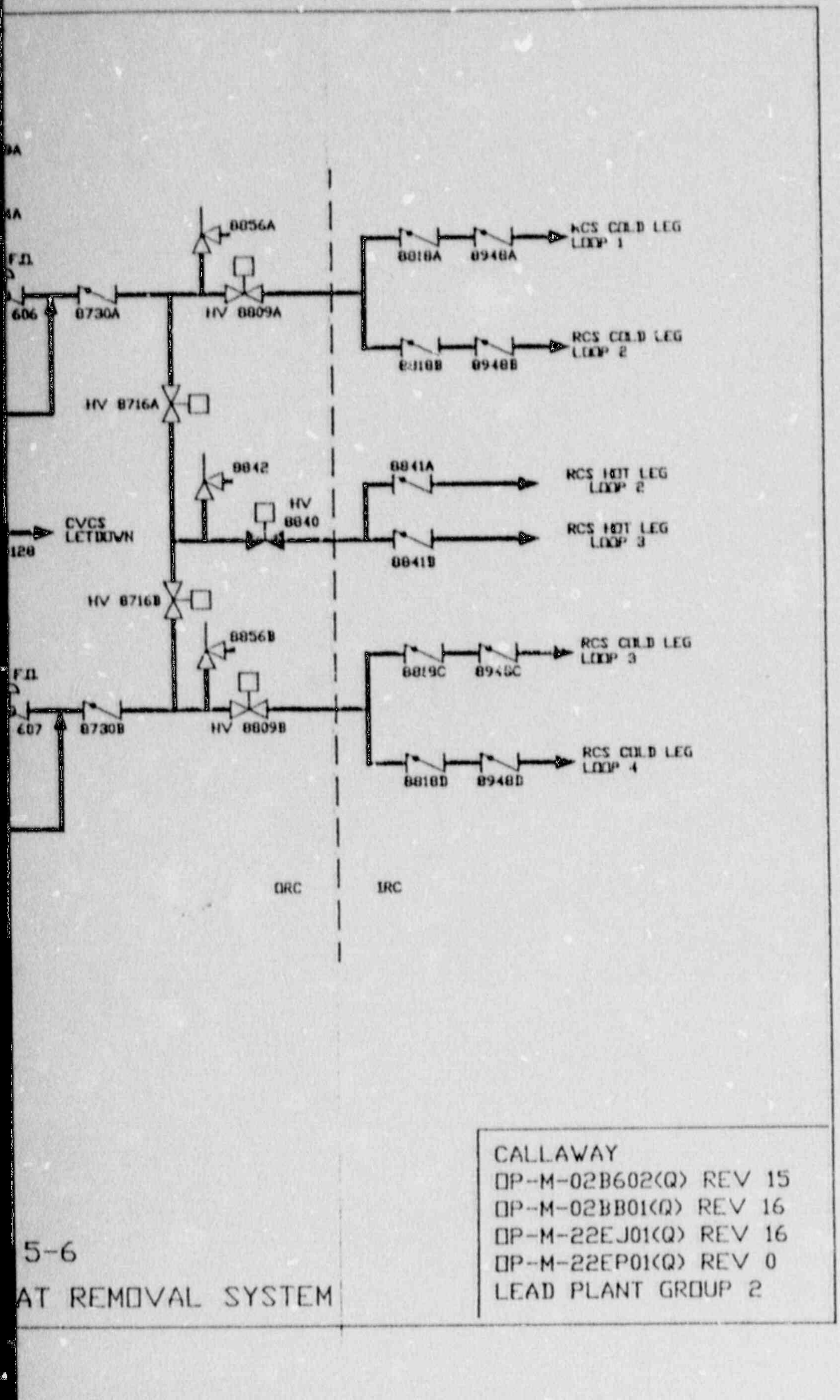


FIGURE

CALLAWAY RESIDUAL HE

RHRCALM

2/11/88



SI APERTURE CARD

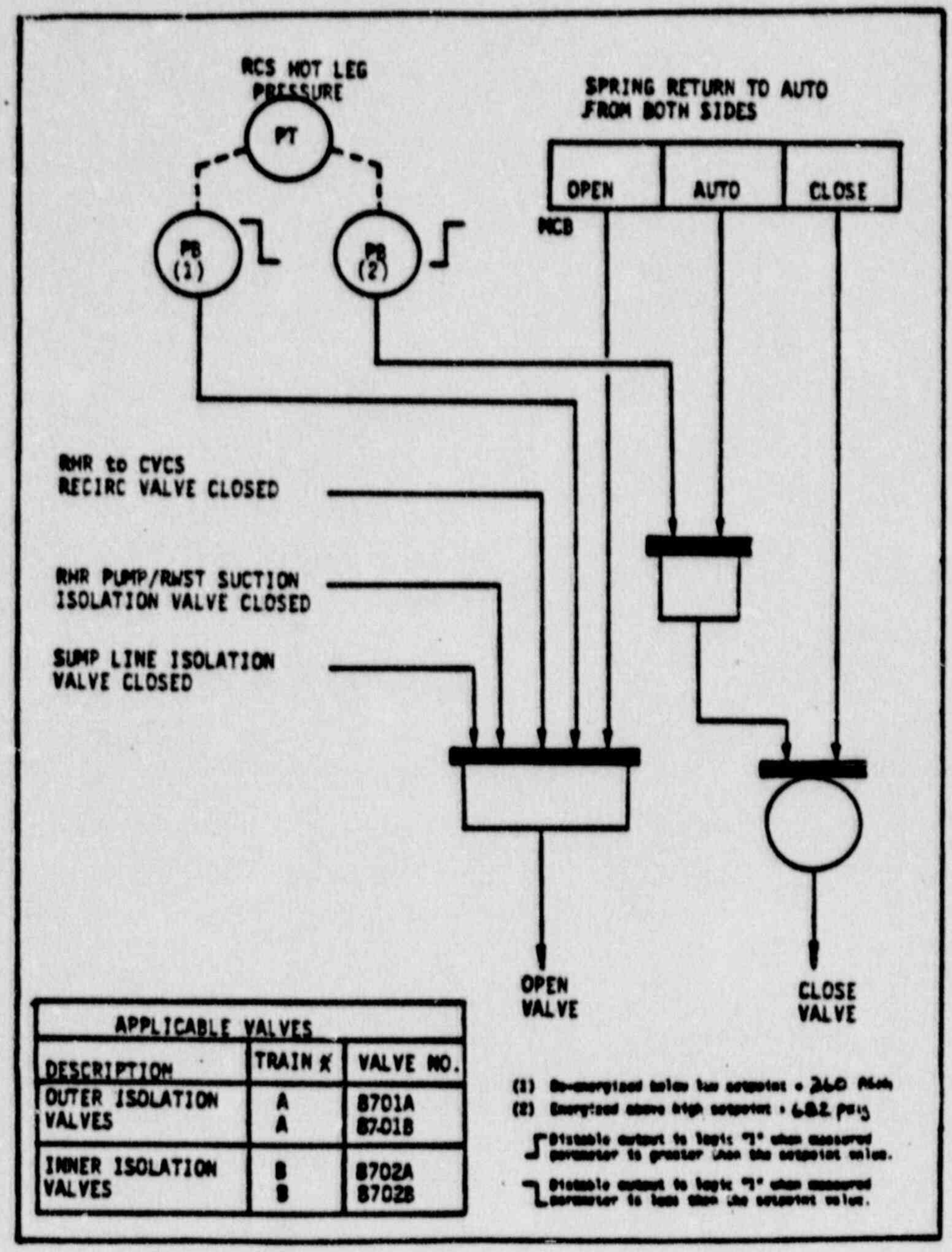
Also Available On Aperture Card

Figure 5-6

Callaway

Residual Heat Removal System

8911150026-11



DESCRIPTION	TRAIN *	VALVE NO.
OUTER ISOLATION VALVES	A A	8701A 8701B
INNER ISOLATION VALVES	B B	8702A 8702B

*Power train assignment

Figure 5-7. Callaway Current Interlock-MOV's-8701A&B, 8702A&B Sheet 1

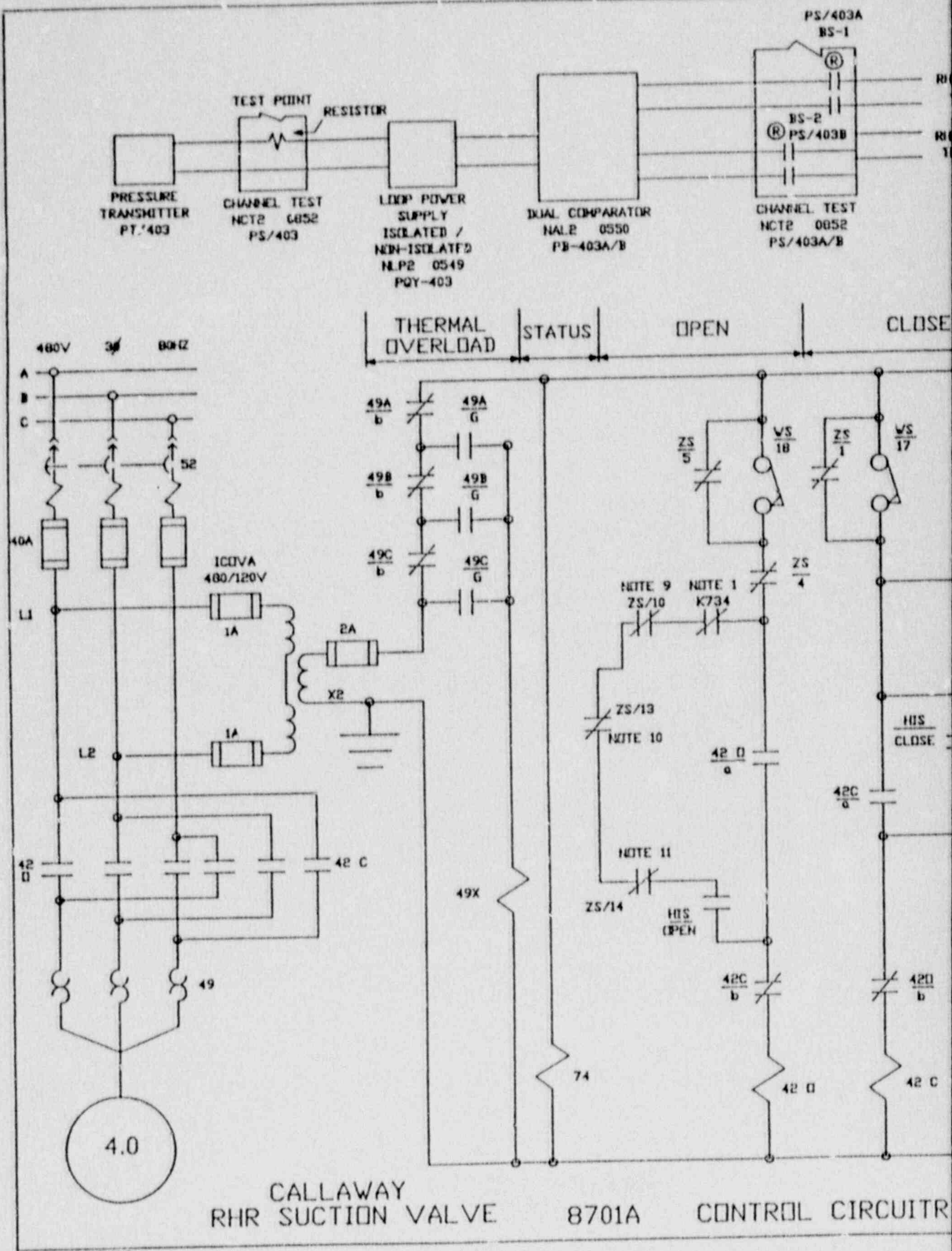
INTERLOCK TABLE - RHR OUTER ISOLATION VALVES		
PLANT	412	
Valve / Interlock with	8701A	8701B
RCS Hot Leg Pressure Channel	PT-405	PT-405
Recirculation Valve Closed/Limit Switch	8804A/#1	8804B/#2
RWST Suction Valve Closed/Limit Switch	8812A/#1	8812B/#2
Sump Line Valve Closed/ Limit Switch	8811A/#1	8811B/#2

LIMIT SWITCH #1 IS THE NORMAL POSITION SWITCH AND IS USED FOR POSITION SIGNALS BETWEEN VALVES ASSIGNED TO THE SAME TRAIN.

LIMIT SWITCH #2 IS THE STEM MOUNTED POSITION SWITCH AND IS USED FOR SIGNALS BETWEEN VALVES ASSIGNED TO OPPOSITE TRAINS.

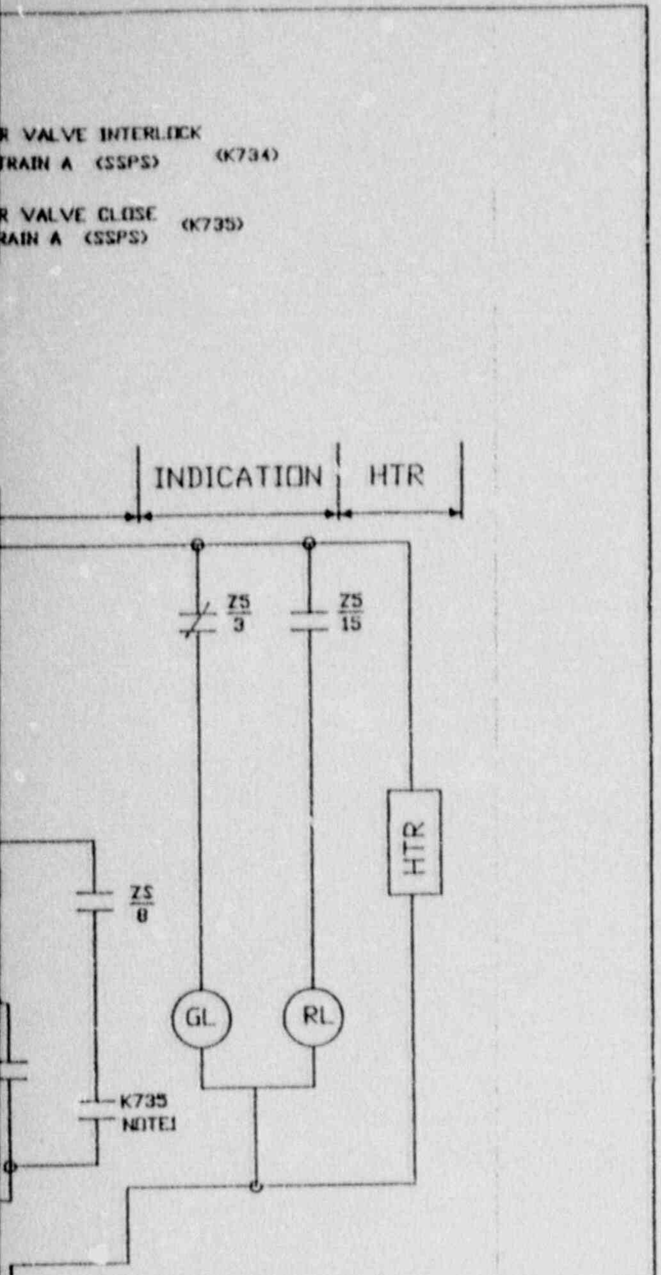
INTERLOCK TABLE - RHR INNER ISOLATION VALVES		
PLANT	412	
Valve / Interlock with	8702A	8702B
RCS Hot Leg Pressure Channel	PT-403	PT-403
Recirculation Valve Closed/Limit Switch	8804A/#2	8804B/#1
RWST Suction Valve Closed/Limit Switch	8812A/#2	8812B/#1
Sump Line Valve Closed/ Limit Switch	8811A/#2	8811B/#1

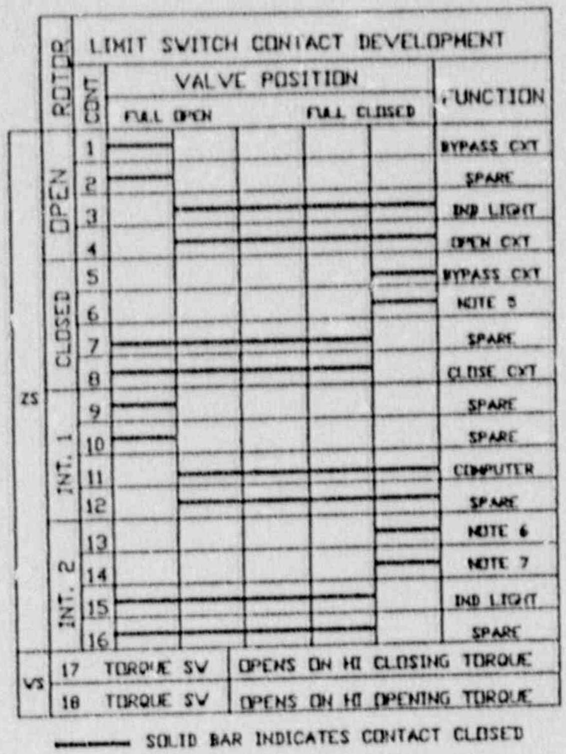
Figure 5-8. Callaway Current Interlock - MOV's-8701A&B, 8702A&B Sheet 2



PS/403A
BS-1
TEST POINT
RESISTOR
BS-2
PS/403B
PRESSURE
TRANSMITTER
PT-403
CHANNEL TEST
NCT2 0852
PS/403
LOOP POWER
SUPPLY
ISOLATED /
NON-ISOLATED
NLP2 0549
PQY-403
DUAL COMPARATOR
NAL2 0550
PB-403A/B
CHANNEL TEST
NCT2 0852
PS/403A/B
THERMAL
OVERLOAD
STATUS
OPEN
CLOSE
480V 3Ø 60HZ
A
B
C
52
40A
100VA
480/120V
1A
2A
X2
L1
L2
49A b
49A G
49B b
49B G
49C b
49C G
ZS 5
WS 18
ZS 1
WS 17
ZS 4
NOTE 9
ZS/10
NOTE 1
K734
ZS/13
NOTE 10
42 O a
HIS CLOSE
42C a
NOTE 11
ZS/14
HIS OPEN
42 O
42 C
49X
49
42C b
42O b
74
42 O
42 C
4.0
RHRCAL1A
CALLAWAY
RHR SUCTION VALVE 8701A CONTROL CIRCUITR

1/23/88





OPEN	
GL.	RL.
CLOSE	

CUTLER-HAMMER TYPE E30 JY9 WITH TWO KLA3 CONTACT BLOCKS

CONTACT	POSITION NORM	POSITION CLOSE	POSITION OPEN
1 o─┤├─o 1T	X	X	
3 o─┤├─o 3T			X
2 o─┤├─o 2B	X		X
4 o─┤├─o 4B		X	

HAND INDICATING SWITCH
HIS - SEE TABLE A
MOMENTARY CONTACT

NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
9. CONTACT CLOSED ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
10. CONTACT CLOSED ON SUMP TO NO. 1 RHR PUMP VALVE CLOSED
11. CONTACT CLOSES ON RHR PUMP 1 TO CHARGING PUMP VALVE CLOSED

5. INTERLOCK TO SCH. IEJG04A
6. INTERLOCK TO SCH. IEJG06A
7. RWST LEVEL TEST CKT.

REFERENCES:

BECHTEL	WESTINGHOUSE
E-23EJ05A(Q) REV 0	8809D50 SHEET 32

Y

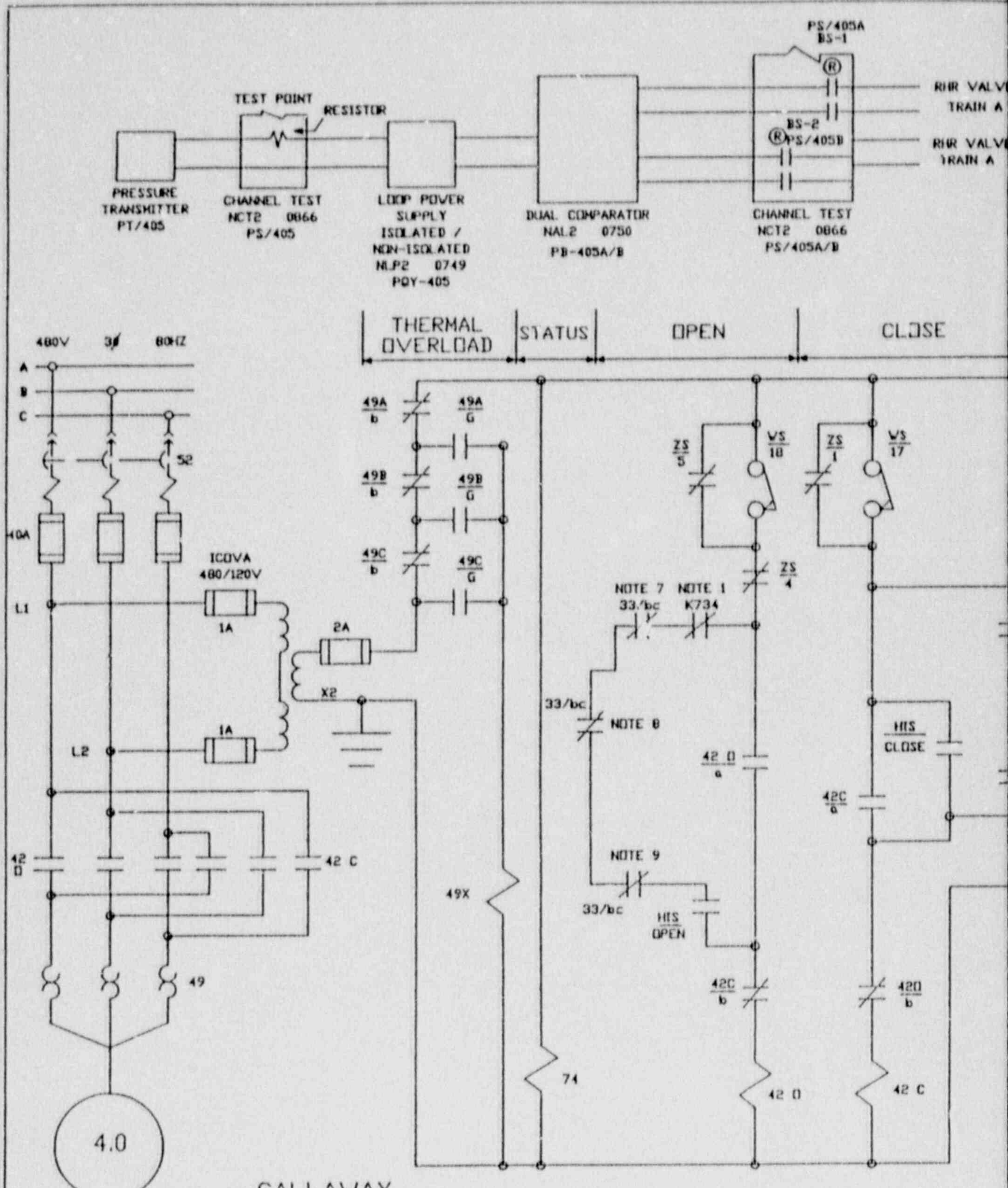
SI
APERTURE
CARD

Also Available On
Aperture Card

Figure 5-9

Callaway RHRS Suction/Isolation Valve Control Circuitry - MOV-8701A

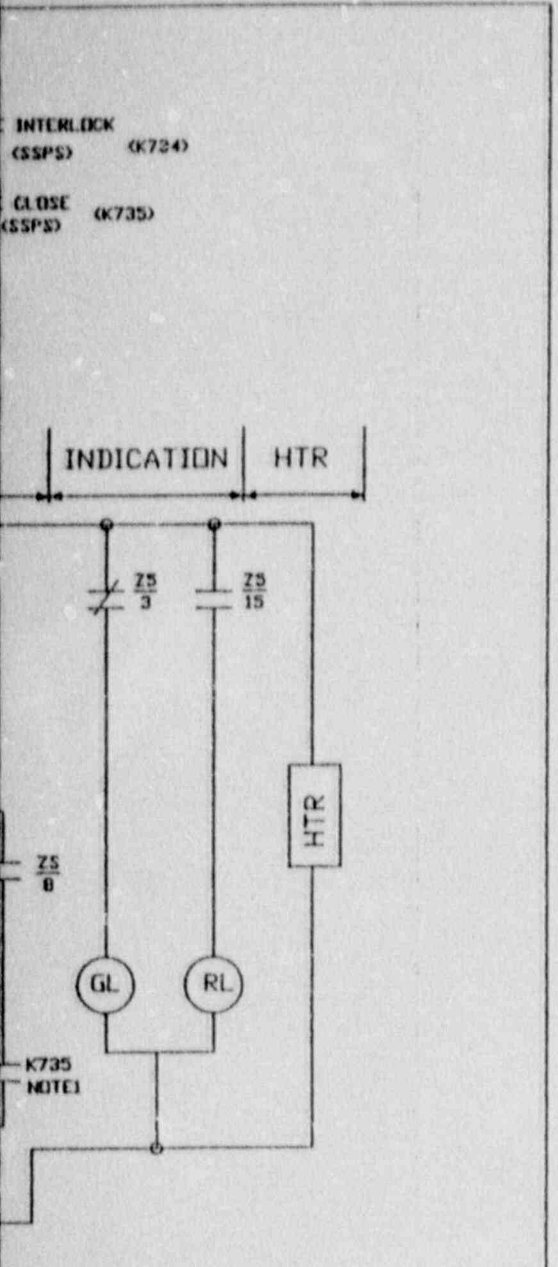
8911150026-12



CALLAWAY
RHR SUCTION VALVE 8701B CONTROL CIRCUITRY

RHRCAL1B

2/11/88



NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
7. CONTACT CLOSES ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
8. CONTACT CLOSES ON SUMP TO NO. 2 RHR PUMP VALVE CLOSED
9. CONTACT CLOSES ON RHR PUMP 2 TO CHARGING PUMP VALVE CLOSED

REFERENCES:

BECHTEL E-23EJ05B(Q) REV 1

WESTINGHOUSE 8809D51 SHEET 45

LIMIT SWITCH CONTACT DEVELOPMENT

	ROTOR	CONT	VALVE POSITION: FULL OPEN				FULL CLOSED	FUNCTION
ZS	OPEN	1	▬					BYPASS CXT
ZS	OPEN	2	▬					SPARE
ZS	OPEN	3		▬	▬	▬	▬	IND LIGHT
ZS	OPEN	4		▬	▬	▬	▬	OPEN CXT
ZS	CLOSED	5					▬	BYPASS CXT
ZS	CLOSED	6					▬	SPARE
ZS	CLOSED	7	▬	▬	▬	▬		SPARE
ZS	CLOSED	8	▬	▬	▬	▬		CLOSE CXT
ZS	INT. 1	9	▬					SPARE
ZS	INT. 1	10	▬					SPARE
ZS	INT. 1	11		▬	▬	▬	▬	COMPUTER
ZS	INT. 1	12		▬	▬	▬	▬	SPARE
ZS	INT. 2	13					▬	SPARE
ZS	INT. 2	14					▬	SPARE
ZS	INT. 2	15	▬	▬	▬	▬		ANN. CKT
ZS	INT. 2	16	▬	▬	▬	▬		SPARE
VS	17	TORQUE SW	OPENS ON HI CLOSING TORQUE					
VS	18	TORQUE SW	OPENS ON HI OPENING TORQUE					

▬ SOLID BAR INDICATES CONTACT CLOSED

OPEN	
GL	RL
CLOSE	

CUTLER-HAMMER TYPE E30 JY9 WITH TWO KLA3 CONTACT BLOCKS

CONTACT	POSITION: NORM	CLOSE	OPEN
1 o—| |—o 1T	X	X	
3 o—| |—o 3T			X
2 o—| |—o 2B	X		X
4 o—| |—o 4B		X	

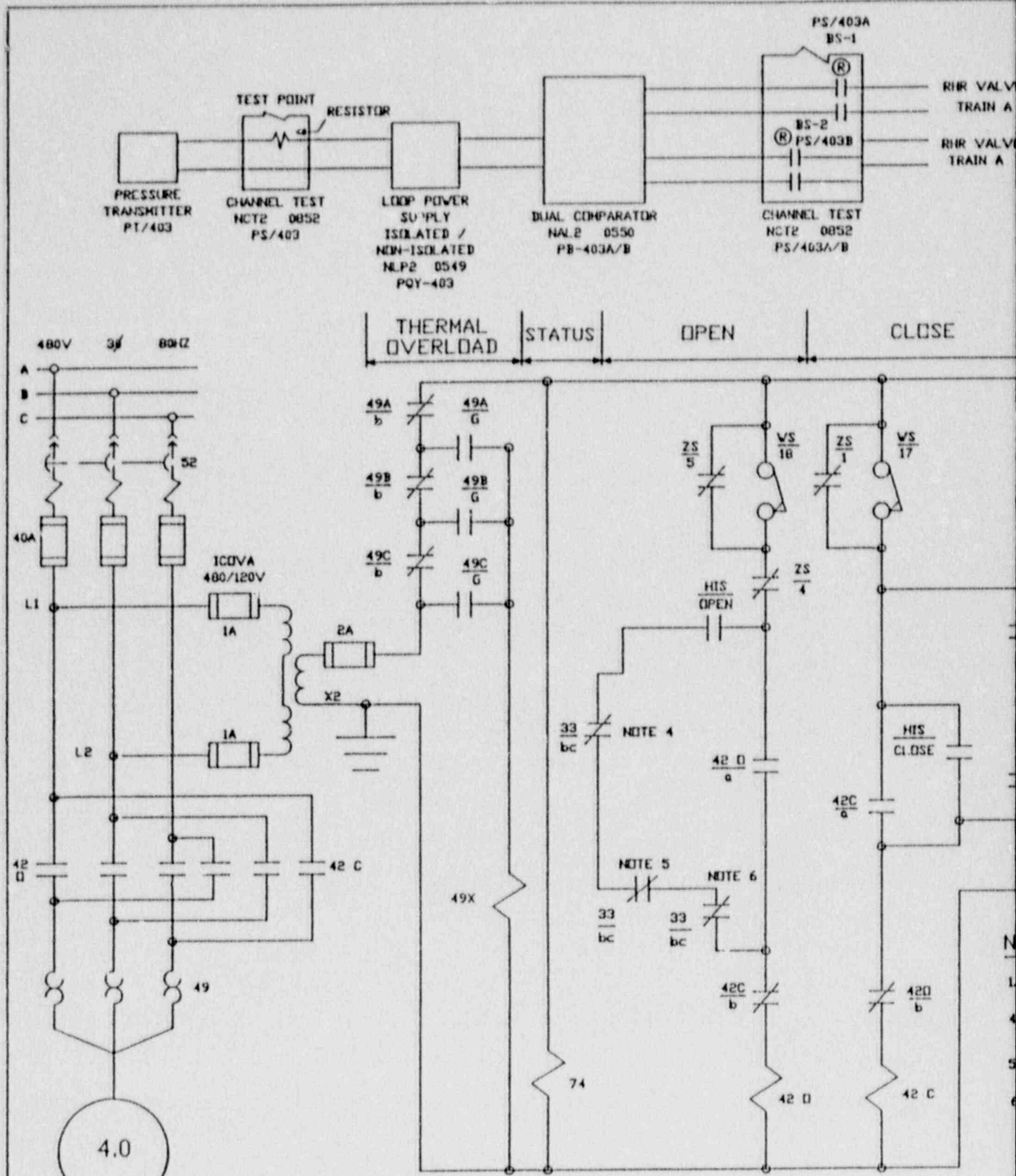
H ND INDICATING SWITCH HS - SEE TABLE A MOMENTARY CONTACT

SI APERTURE CARD

Also Available On Aperture Card

Figure 5-10

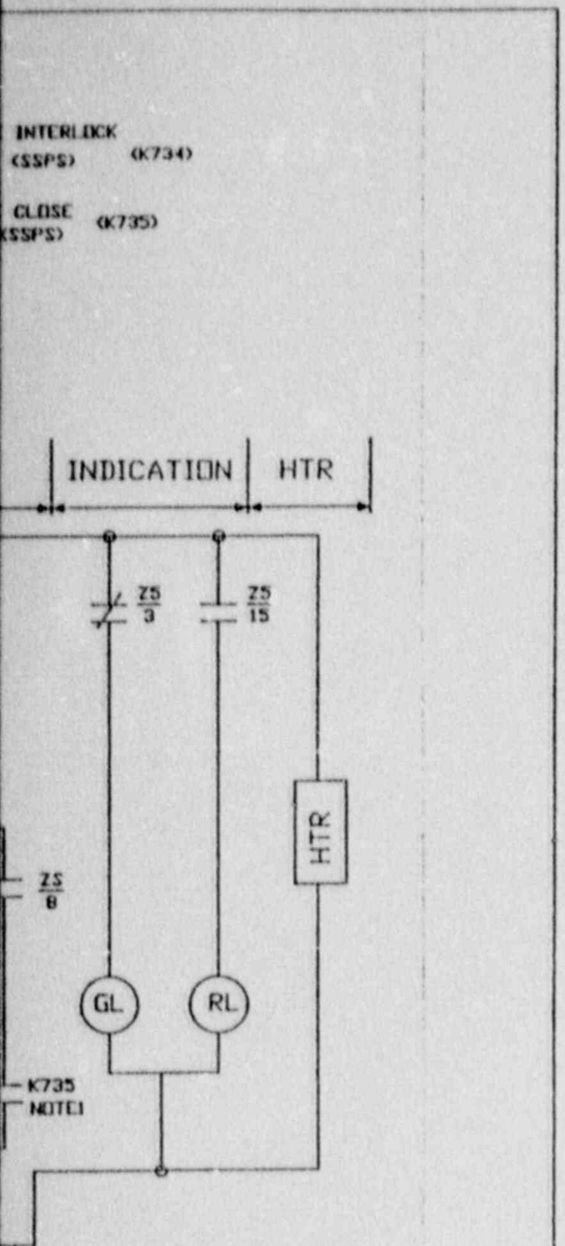
Callaway RHRS Suction/Isolation Valve Control Circuitry - MOV-8702B



CALLAWAY
RHR SUCTION VALVE 8702A CONTROL CIRCUITRY

RHRCAL2A

2/11/88



ROTOR	CONT	FULL OPEN				FULL CLOSED	FUNCTION
LIMIT SWITCH CONTACT DEVELOPMENT		VALVE POSITION					
ZS OPEN	1	▬					BYPASS CXT
ZS OPEN	2	▬					SPARE
ZS OPEN	3		▬	▬	▬	▬	IND LIGHT
ZS OPEN	4		▬	▬	▬	▬	OPEN CXT
ZS CLOSED	5					▬	BYPASS CXT
ZS CLOSED	6					▬	SPARE
ZS CLOSED	7	▬	▬	▬	▬		SPARE
ZS CLOSED	8	▬	▬	▬	▬		CLOSE CXT
ZS INT. 1	9	▬					SPARE
ZS INT. 1	10	▬					SPARE
ZS INT. 1	11		▬	▬	▬	▬	NOTE 7
ZS INT. 1	12		▬	▬	▬	▬	SPARE
ZS INT. 2	13					▬	SPARE
ZS INT. 2	14					▬	SPARE
ZS INT. 2	15	▬	▬	▬	▬		IND LIGHT
ZS INT. 2	16	▬	▬	▬	▬		ANN. CKT
VS	17	TORQUE SW	OPENS ON HI CLOSING TORQUE				
VS	18	TORQUE SW	OPENS ON HI OPENING TORQUE				

▬ SOLID BAR INDICATES CONTACT CLOSED

CUTLER-HAMMER TYPE E30 JY9 WITH TWO KLA3 CONTACT BLOCKS

CONTACT	POSITION NORM	POSITION CLOSE	POSITION OPEN
1 o—| |—o 1T	X	X	
3 o—| |—o 3T			X
2 o—| |—o 2B	X		X
4 o—| |—o 4B		X	

HAND INDICATING SWITCH
HIS - SEE TABLE A
MOMENTARY CONTACT

NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
2. CONTACT CLOSES ON SUMP TO NO. 1 RHR PUMP VALVE CLOSED
3. CONTACT CLOSES ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
4. CONTACT CLOSES ON RHR PUMP 1 CHARGING PUMP VALVE CLOSED

REFERENCES:

BECHTEL	WESTINGHOUSE
3-23BB12A(Q) REV 2	8809D50 SHEET 32

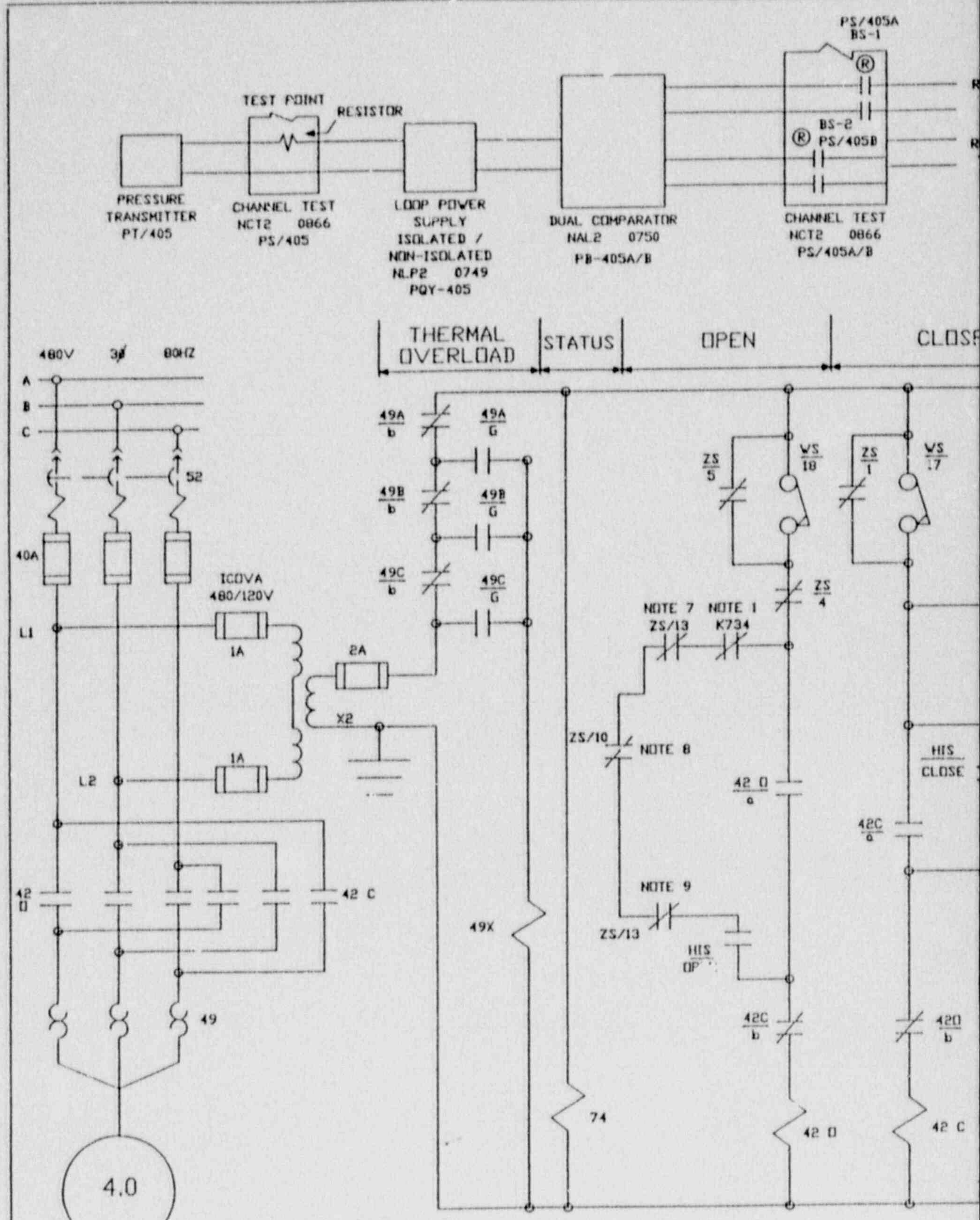
SI
APERTURE
CARD

Also Available On
Aperture Card

Figure 5-11

Callaway RHRS Suction/Isolation Valve Control Circuitry - MOV-8702A

8911150026-14

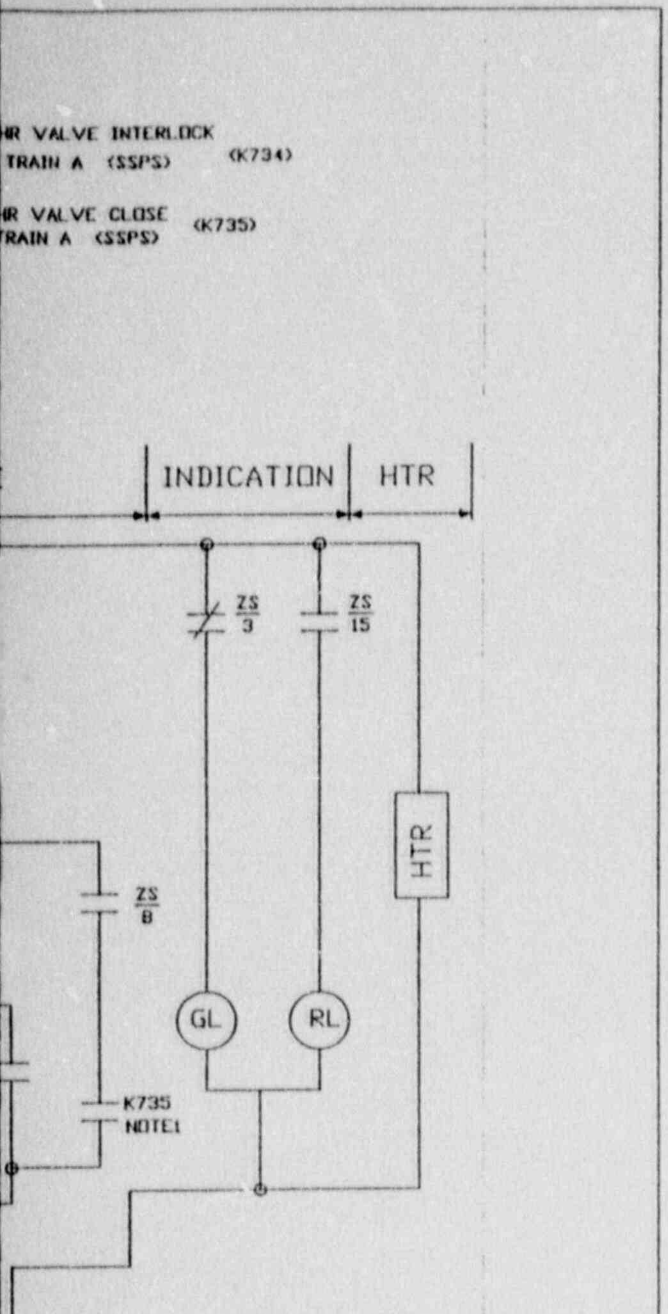


CALLAWAY

RHR SUCTION VALVE 8702B CONTROL CIRCUITR

RHRCAL2B

1/23/88



NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
7. CONTACT CLOSES ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
8. CONTACT CLOSES ON SUMP TO NO. 2 RHR PUMP VALVE CLOSED
9. CONTACT CLOSES ON RHR PUMP 2 TO CHARGING PUMP VALVE CLOSED

REFERENCES:

BECHTEL E-23BB12B(Q) REV 0

WESTINGHOUSE 8809D51 SHEET 45

LIMIT SWITCH CONTACT DEVELOPMENT

	ROTOR	CONT	VALVE POSITION: FULL OPEN				FULL CLOSED	FUNCTION
ZS	OPEN	1	—					BYPASS CXT
ZS	OPEN	2	—					SPARE
ZS	OPEN	3		—	—	—	—	IND LIGHT
ZS	OPEN	4		—	—	—	—	OPEN CXT
ZS	CLOSED	5					—	BYPASS CXT
ZS	CLOSED	6					—	NOTE 2
ZS	CLOSED	7	—	—	—	—		SPARE
ZS	CLOSED	8	—	—	—	—		CLOSE CXT
ZS	INT. 1	9	—					SPARE
ZS	INT. 1	10	—					SPARE
ZS	INT. 1	11		—	—	—	—	NOTE 10
ZS	INT. 1	12		—	—	—	—	SPARE
ZS	INT. 2	13					—	NOTE 3
ZS	INT. 2	14					—	NOTE 4
ZS	INT. 2	15	—	—	—	—		IND LIGHT
ZS	INT. 2	16	—	—	—	—		SPARE
VS	17 TORQUE SW		OPENS ON HI CLOSING TORQUE					
VS	18 TORQUE SW		OPENS ON HI OPENING TORQUE					

—— SOLID BAR INDICATES CONTACT CLOSED

OPEN	
GL	RL
CLOSE	

CUTLER-HAMMER TYPE E30 JY9 WITH TWO KLA3 CONTACT BLOCKS

CONTACT	POSITION: NORM	CLOSE	OPEN
1 o—‖—o 1T	X	X	
3 o—‖—o 3T			X
2 o—‖—o 2B	X		X
4 o—‖—o 4B		X	

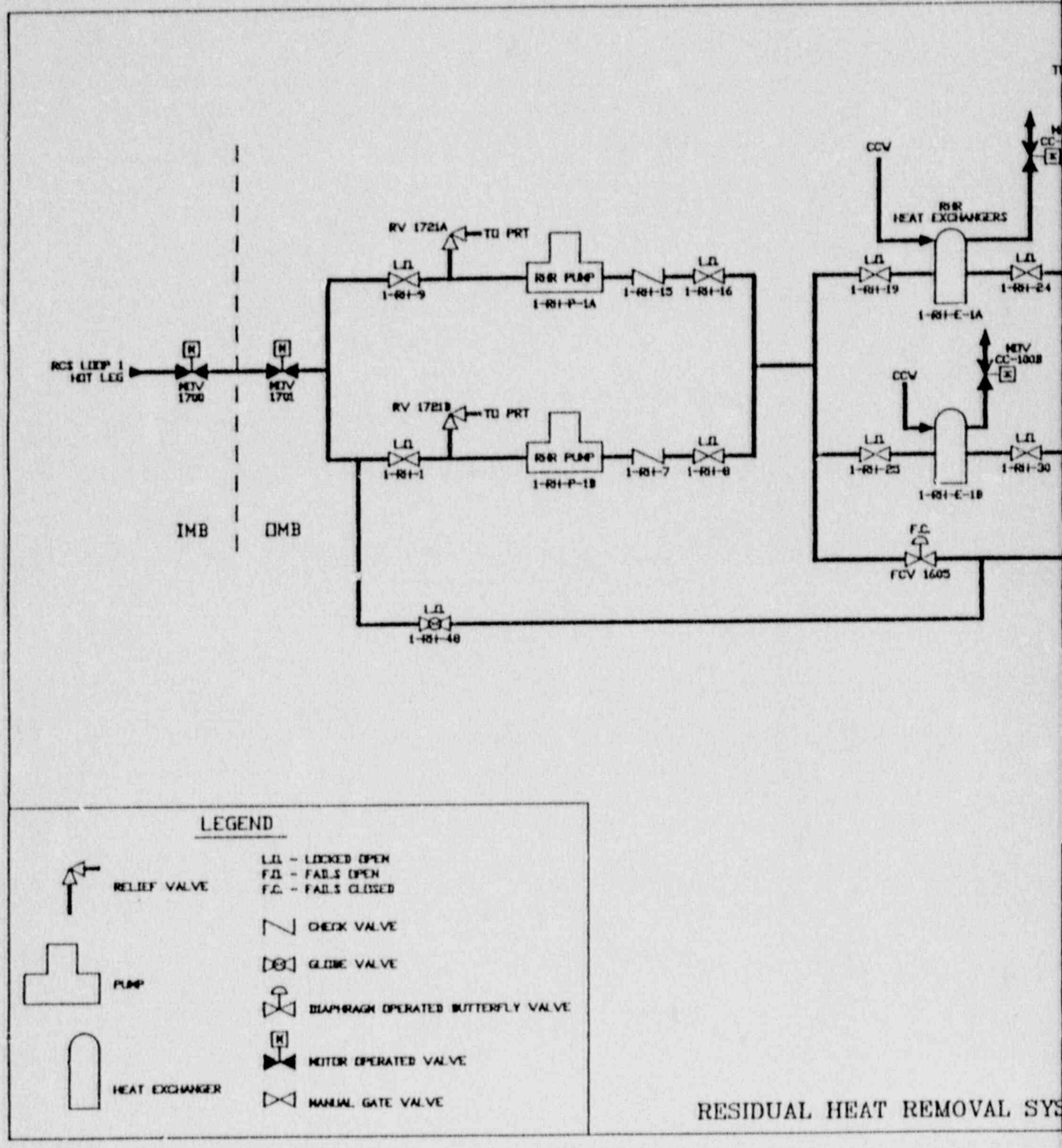
HAND INDICATING SWITCH HIS - SEE TABLE A MOMENTARY CONTACT

SI APERTURE CARD

Also Available On Aperture Card

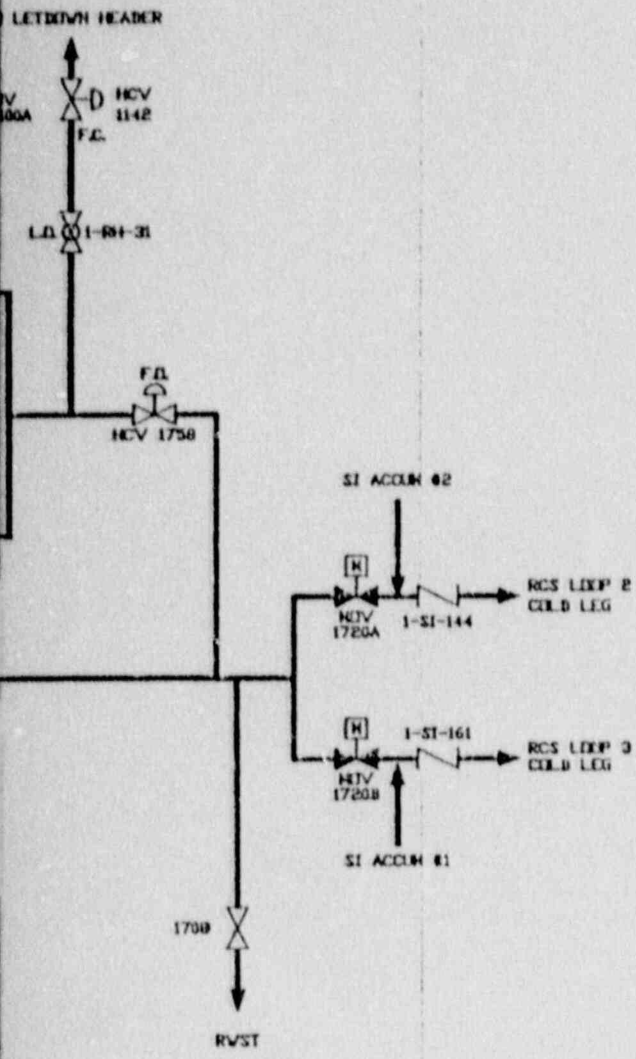
Figure 5-12

Callaway RHRS Suction/Isolation Valve Control Circuitry - MOV-8702B


RCS LOOP 1 HOT LEG
MOV 1700
MOV 1701
IMB
OMB
RV 1721A
TO PRT
L.O.
1-RH-9
RHR PUMP
1-RH-P-1A
1-RH-15
1-RH-16
RV 1721B
1-RH-1
1-RH-P-1B
1-RH-7
1-RH-8
1-RH-48
CCV
RHR HEAT EXCHANGERS
1-RH-19
1-RH-E-1A
1-RH-24
MOV
CC-100B
1-RH-25
1-RH-E-1B
1-RH-30
F.C.
FCV 1605
LEGEND
RELIEF VALVE
PUMP
HEAT EXCHANGER
L.O. - LOCKED OPEN
F.O. - FAILS OPEN
F.C. - FAILS CLOSED
CHECK VALVE
GLOBE VALVE
DIAPHRAGM OPERATED BUTTERFLY VALVE
MOTOR OPERATED VALVE
MANUAL GATE VALVE
RESIDUAL HEAT REMOVAL SYS
RHR_NA

2/11/88

WESTINGHOUSE PROPRIETARY CLASS 3



VIRGINIA POWER
NORTH ANNA POWER STATION
DRAWING NO. 11715-FM-94A-11
11715-FM-41B-15
11715-FM-40C-12
FM-95C
FM-96B
FM-40C
FM-41B
GROUP 3 PLANT

TEM

SI
APERTURE
CARD

Also Available On
Aperture Card

Figure 5-13

North Anna Residual Heat Removal System

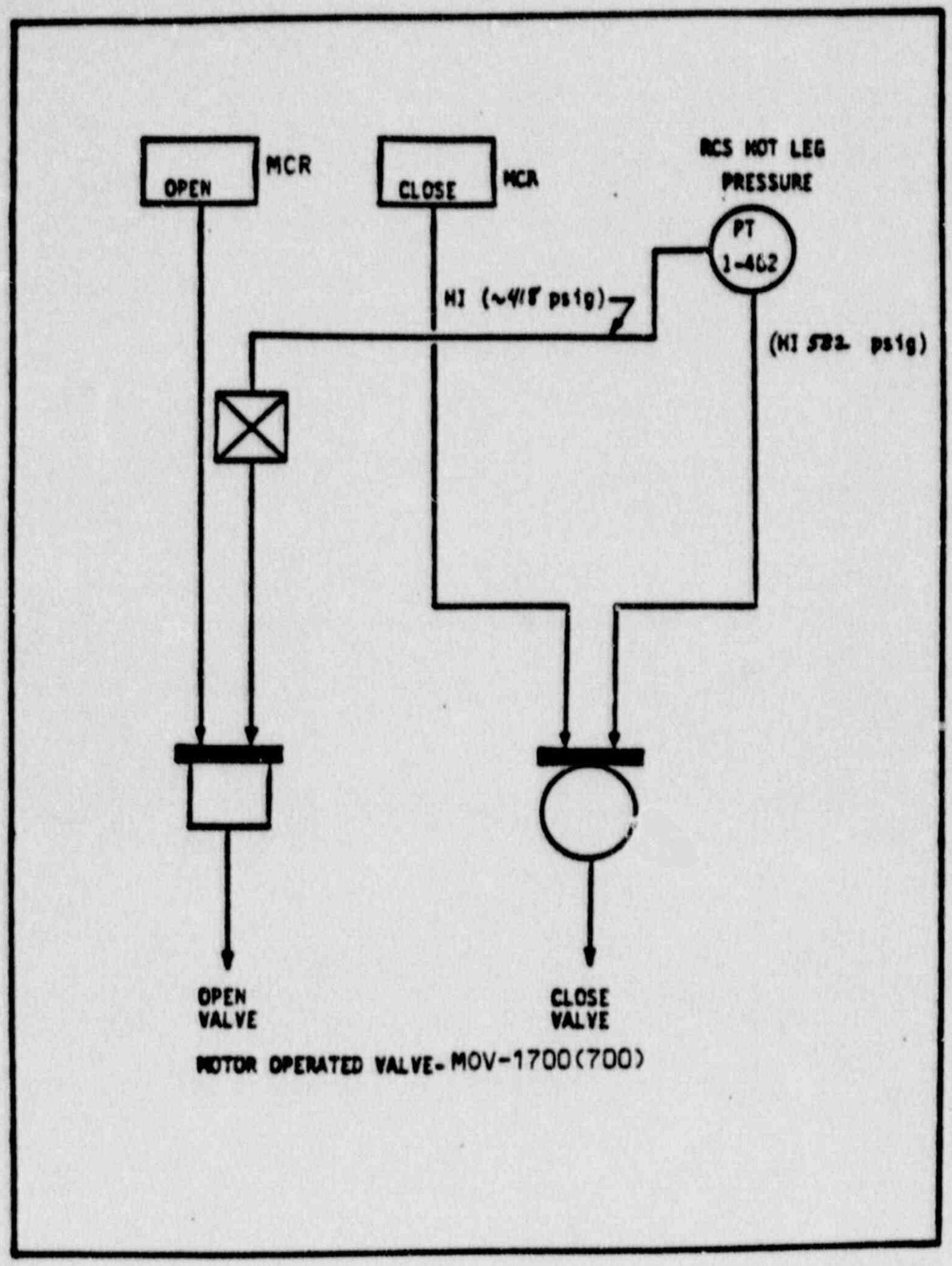


Figure 5-14. North Anna Current Interlock-MOV-1700

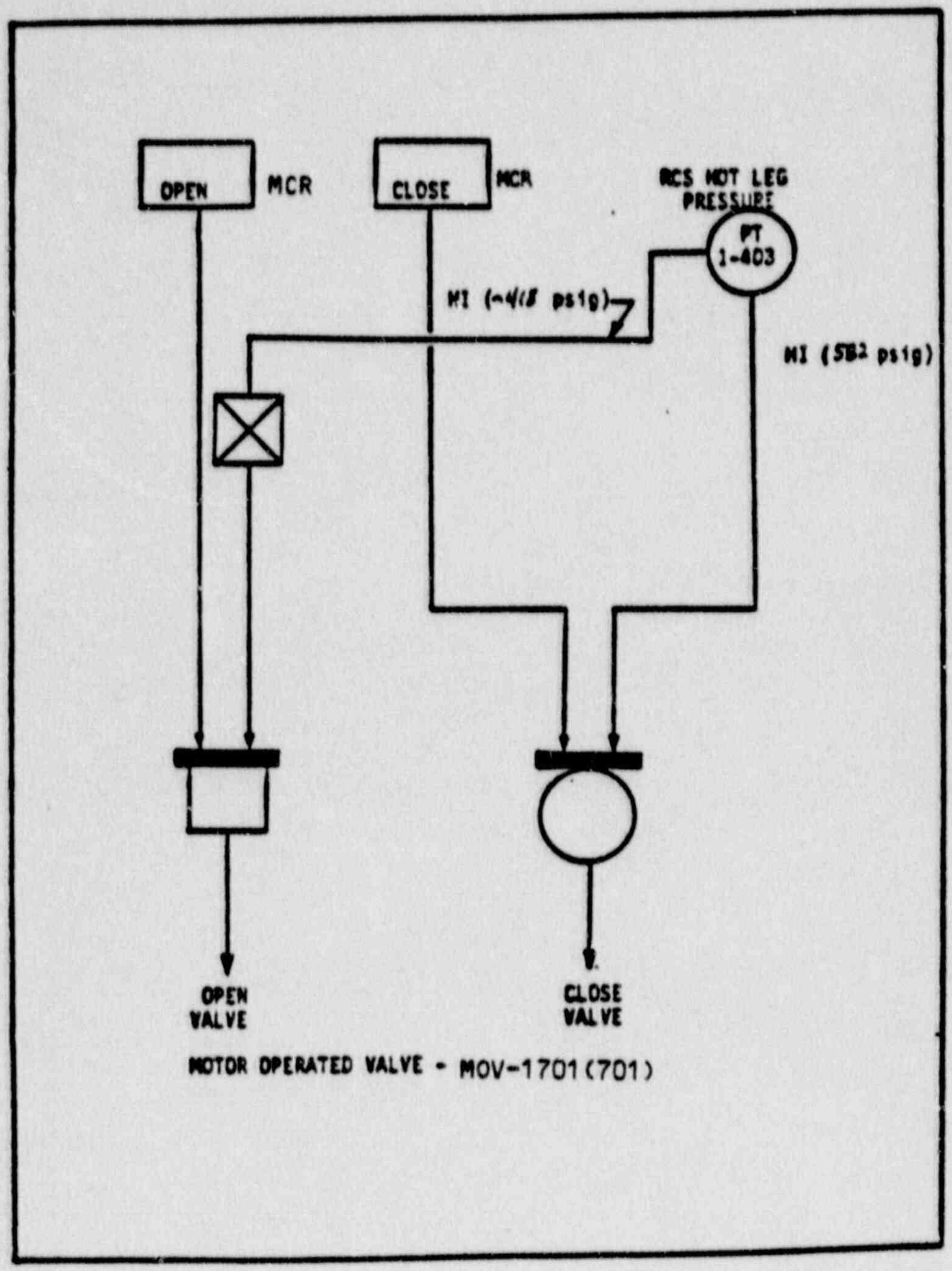
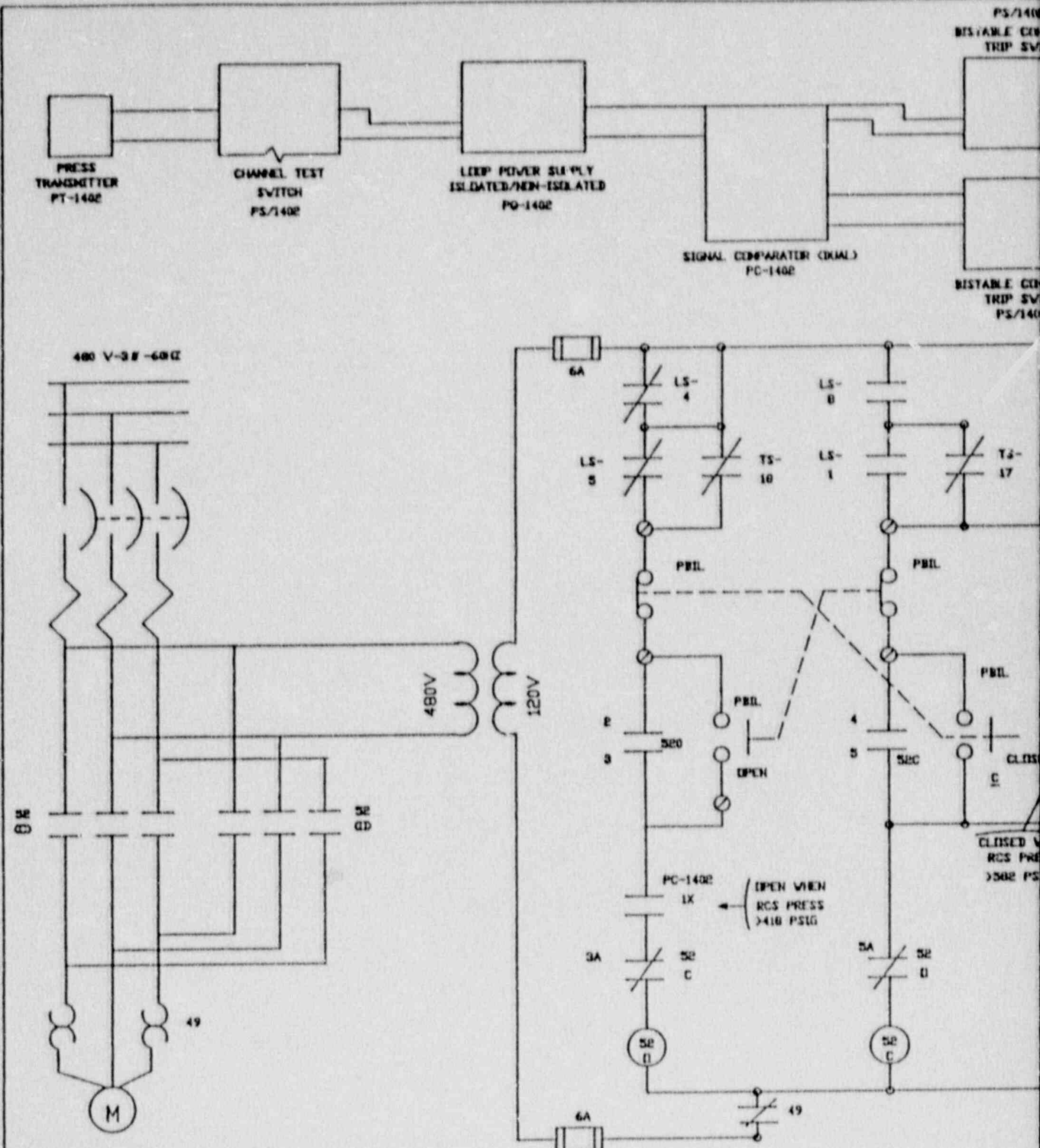


Figure 5-15. North Anna Current Interlock-MOV-1701

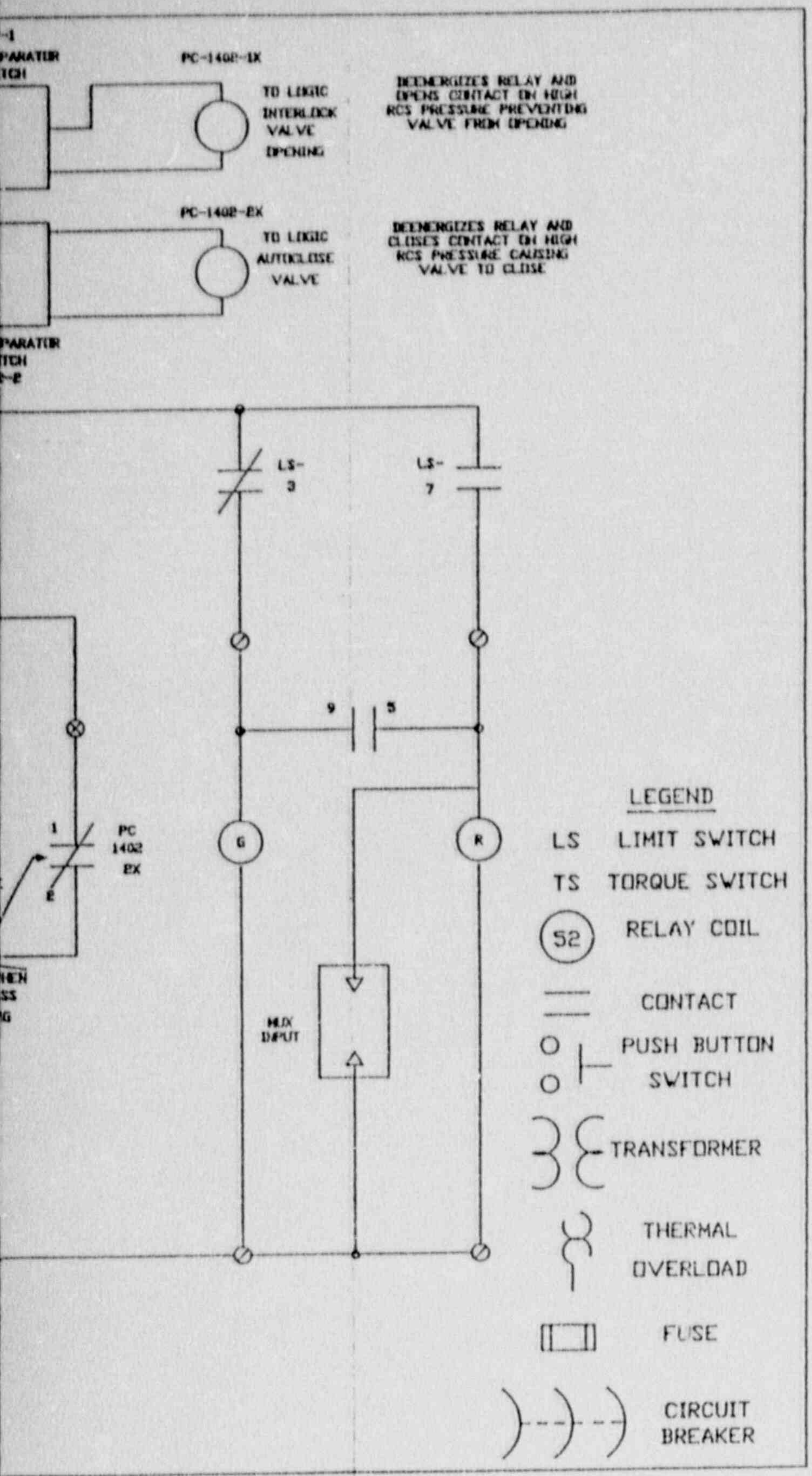


REFERENCES
S&W P-1403 REV 11
W 501B248 SHEET 160 REV 5
W 6007D10
S&W 11715-ESK-6DT SHEET 42 REV 12
S&W 11715-ESK-3H

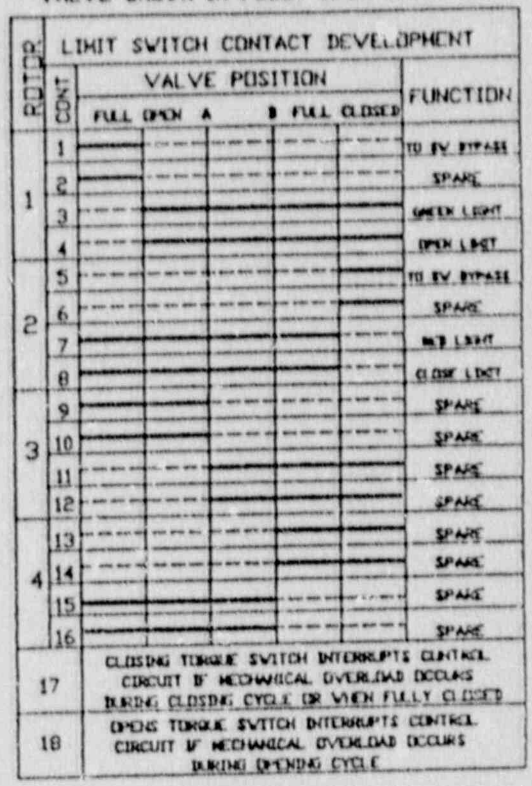
NORTH ANNA
CONTROL WIRING DIAGRAM
MOV-1700

CVD_NA

2/11/88



VALVE SHOWN IN FULLY OPEN POSITION



NOTES

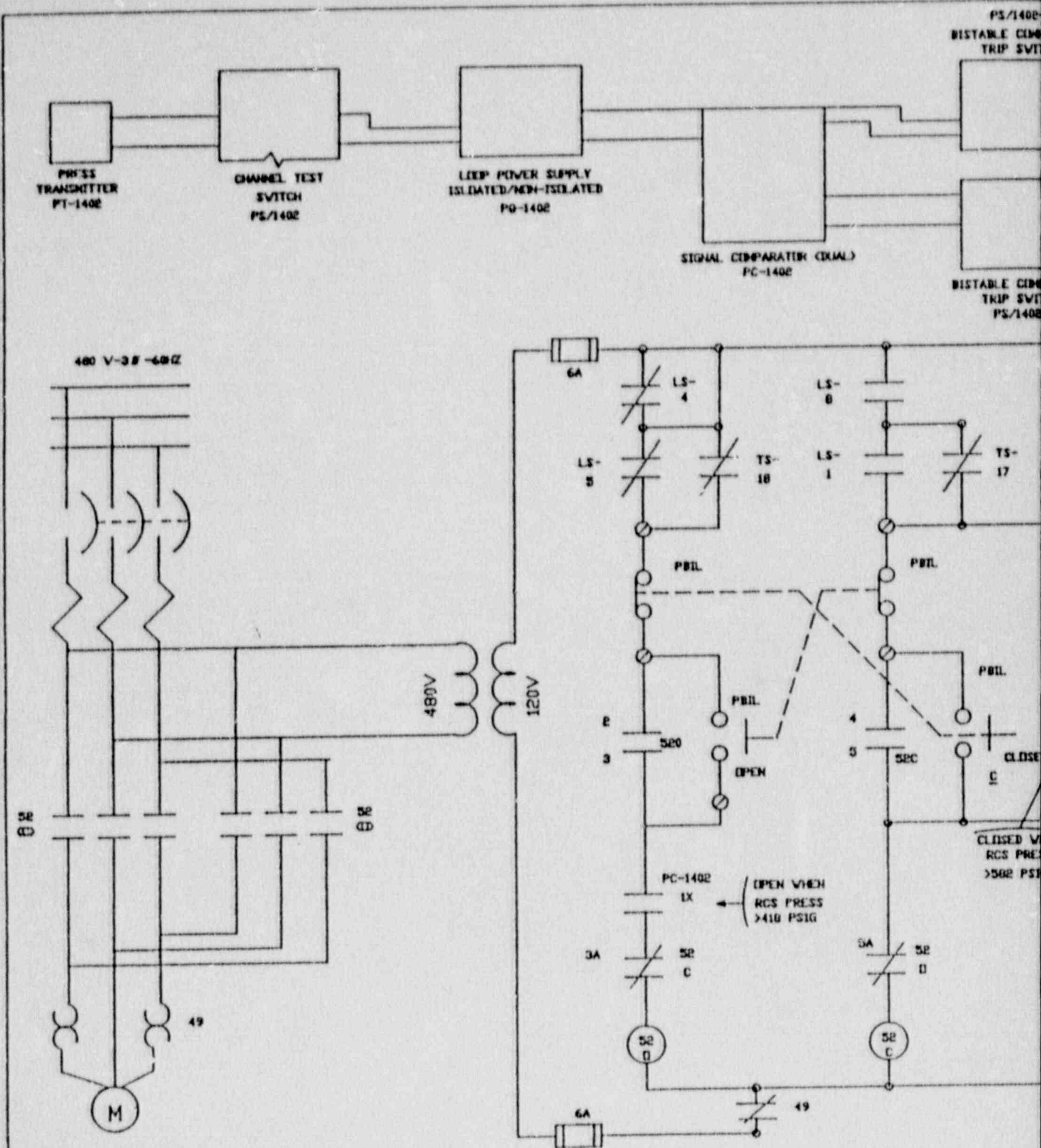
——— INDICATES CONTACT CLOSED

- - - - INDICATES CONTACT OPEN

ROTORS 3 & 4 ARE ADJUSTABLE AND CAN BE SET AT VALVE POSITION FULLY OPEN FULLY CLOSED OR ANY POSITION INBETWEEN

Figure 5-16

North Anna RHRS Suction/Isolation Valve Control Circuitry - MOV-1700

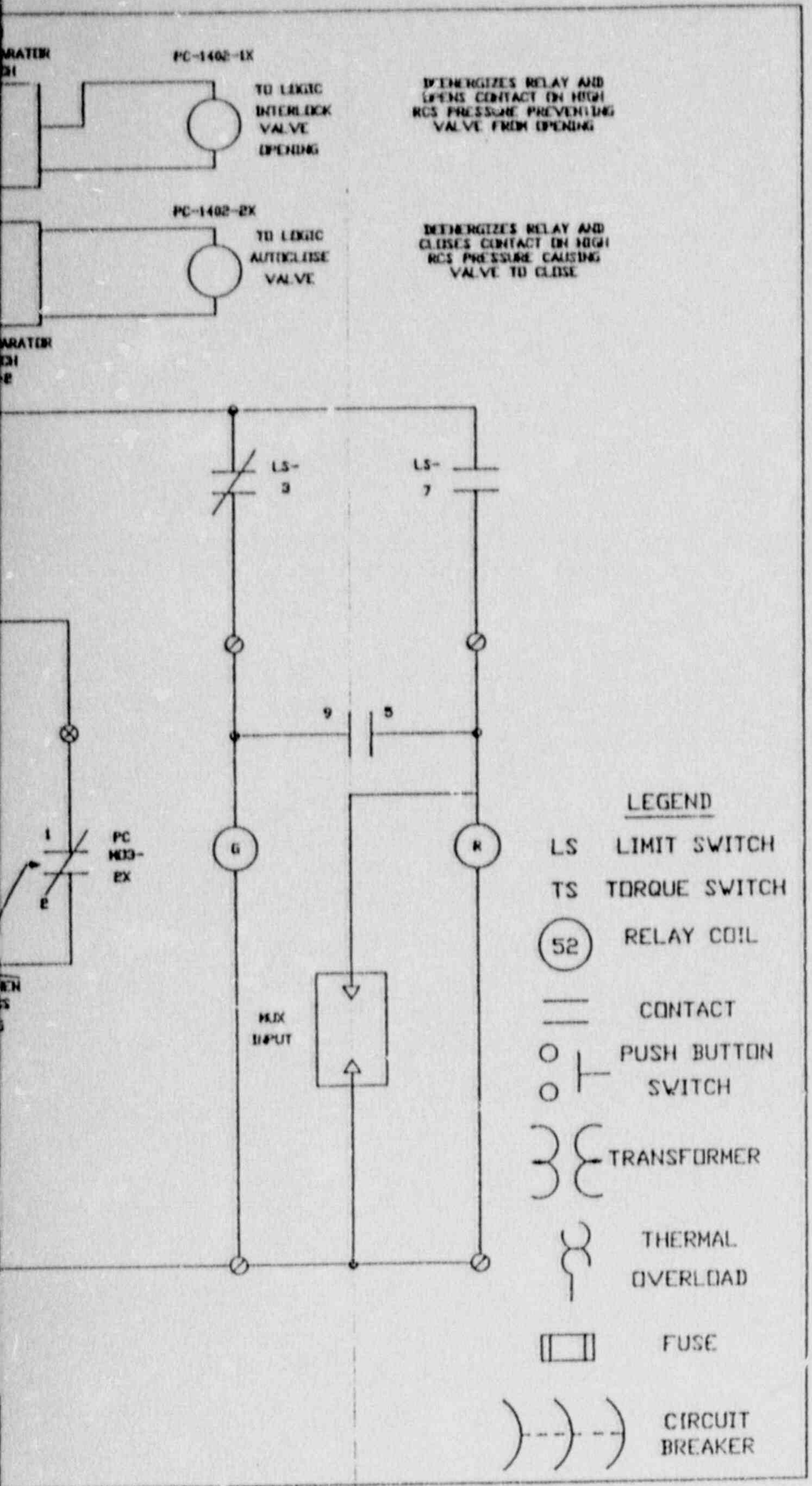


REFERENCES
S&W P-1403 REV 11
W 501B248 SHEET 160 REV 5
W 6007D10
S&W 11715-ESK-6DT SHEET 42 REV 12
S&W 11715-ESK-3H

NORTH ANNA
CONTROL WIRING DIAGRAM
MOV-1701

CWD_NA01

2/11/88



VALVE SHOWN IN FULLY OPEN POSITION

ROTOR	LIMIT SWITCH CONTACT DEVELOPMENT						
	CONT	VALVE POSITION: FULL OPEN	A		B	FULL CLOSED	FUNCTION
1	1	——	- - -	- - -	- - -	- - -	TO BV BYPASS
1	2	——	- - -	- - -	- - -	- - -	SPARE
1	3	- - -	——	——	——	——	GREEN LIGHT
1	4	- - -	——	——	——	——	OPEN LIMIT
2	5	- - -	- - -	- - -	- - -	——	TO BV BYPASS
2	6	- - -	- - -	- - -	- - -	——	SPARE
2	7	——	——	——	——	- - -	RED LIGHT
2	8	——	——	——	——	- - -	CLOSE LIMIT
3	9	——	——	- - -	- - -	- - -	SPARE
3	10	——	——	- - -	- - -	- - -	SPARE
3	11	- - -	- - -	——	——	——	SPARE
3	12	- - -	- - -	——	——	——	SPARE
4	13	- - -	- - -	- - -	——	——	SPARE
4	14	- - -	- - -	- - -	——	——	SPARE
4	15	——	——	——	- - -	- - -	SPARE
4	16	——	——	——	- - -	- - -	SPARE
17	CLOSING TORQUE SWITCH INTERRUPTS CONTROL CIRCUIT IF MECHANICAL OVERLOAD OCCURS DURING CLOSING CYCLE OR WHEN FULLY CLOSED						
18	OPENS TORQUE SWITCH INTERRUPTS CONTROL CIRCUIT IF MECHANICAL OVERLOAD OCCURS DURING OPENING CYCLE						

NOTES

—— INDICATES CONTACT CLOSED

- - - - INDICATES CONTACT OPEN

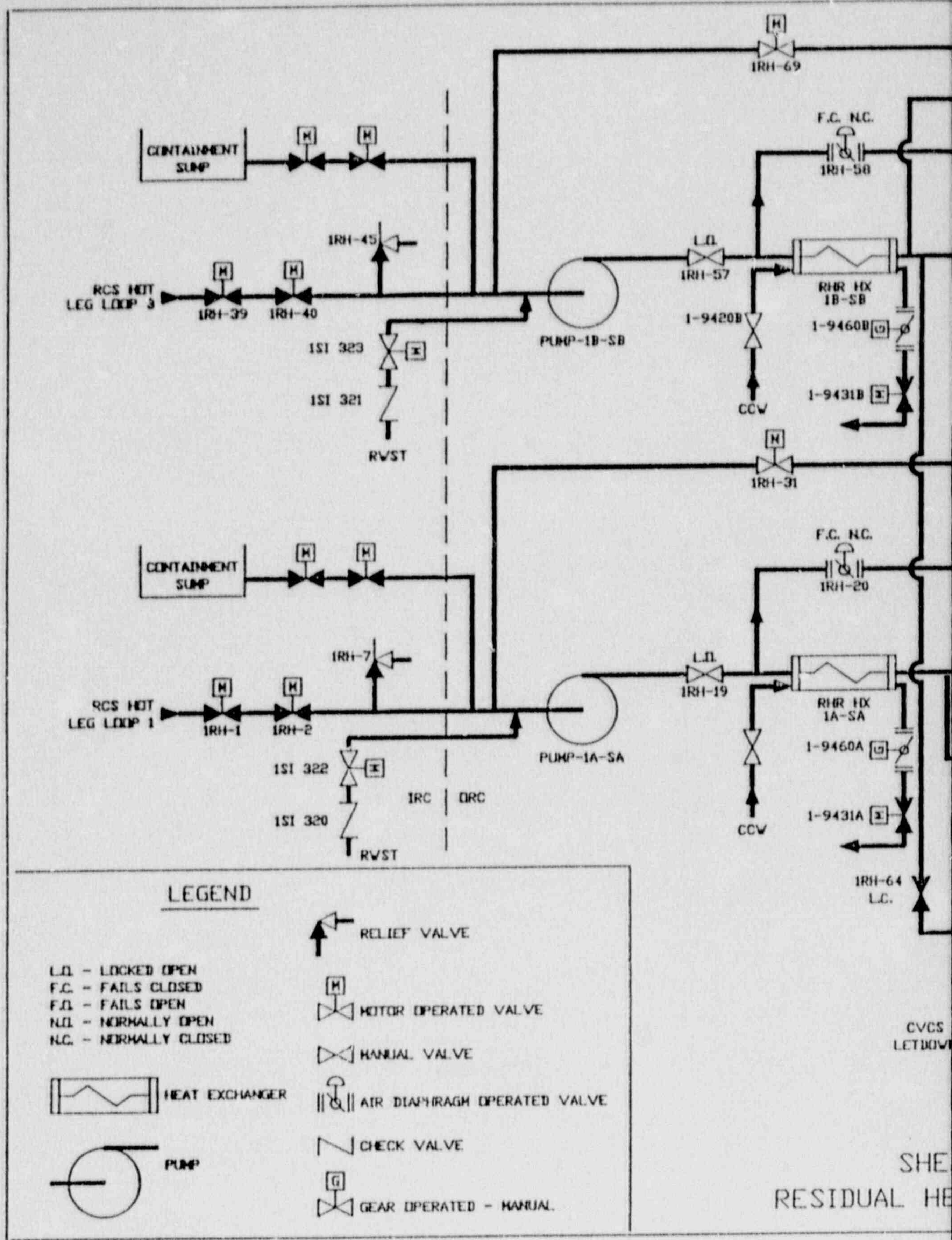
ROTORS 3 & 4 ARE ADJUSTABLE AND CAN BE SET AT VALVE POSITION FULLY OPEN FULLY CLOSED OR ANY POSITION INBETWEEN

SI APERTURE CARD

Also Available On Aperture Card

Figure 5-17

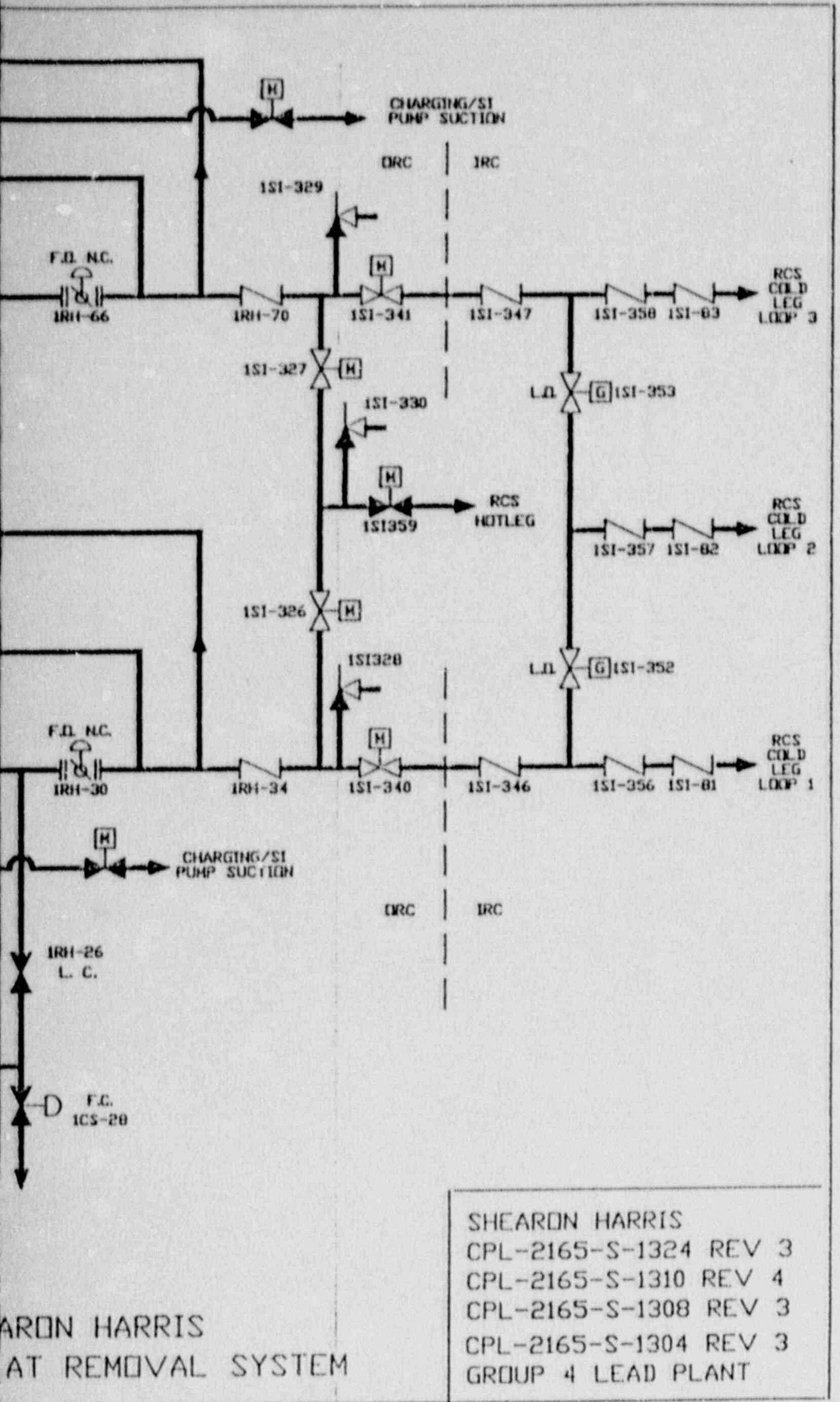
North Anna RHRS Suction/Isolation Valve Control Circuitry - MOV-1701



1RH-69
F.C. N.C.
1RH-58
CONTAINMENT SUMP
1RH-45
RCS HOT LEG LOOP 3
1RH-39
1RH-40
L.O.
1RH-57
RHR HX 1B-SB
PUMP-1B-SB
1-9420B
1-9460B
1SI 323
1SI 321
1-9431B
CCW
RWST
1RH-31
F.C. N.C.
1RH-20
CONTAINMENT SUMP
1RH-7
L.O.
1RH-19
RCS HOT LEG LOOP 1
1RH-1
1RH-2
RHR HX 1A-SA
1-9460A
PUMP-1A-SA
1SI 322
IRC
ORC
1SI 320
1-9431A
CCW
RWST
1RH-64 L.C.
LEGEND
RELIEF VALVE
L.O. - LOCKED OPEN
F.C. - FAILS CLOSED
F.O. - FAILS OPEN
N.O. - NORMALLY OPEN
N.C. - NORMALLY CLOSED
MOTOR OPERATED VALVE
MANUAL VALVE
HEAT EXCHANGER
AIR DIAPHRAGM OPERATED VALVE
CHECK VALVE
PUMP
GEAR OPERATED - MANUAL
CVCS LETDOW
SHE
RESIDUAL HE

RHR_SH

2/11/88



SI
APERTURE
CARD

Also Available On
Aperture Card

Figure 5-18

Shearon Harris

Residual Heat Removal System

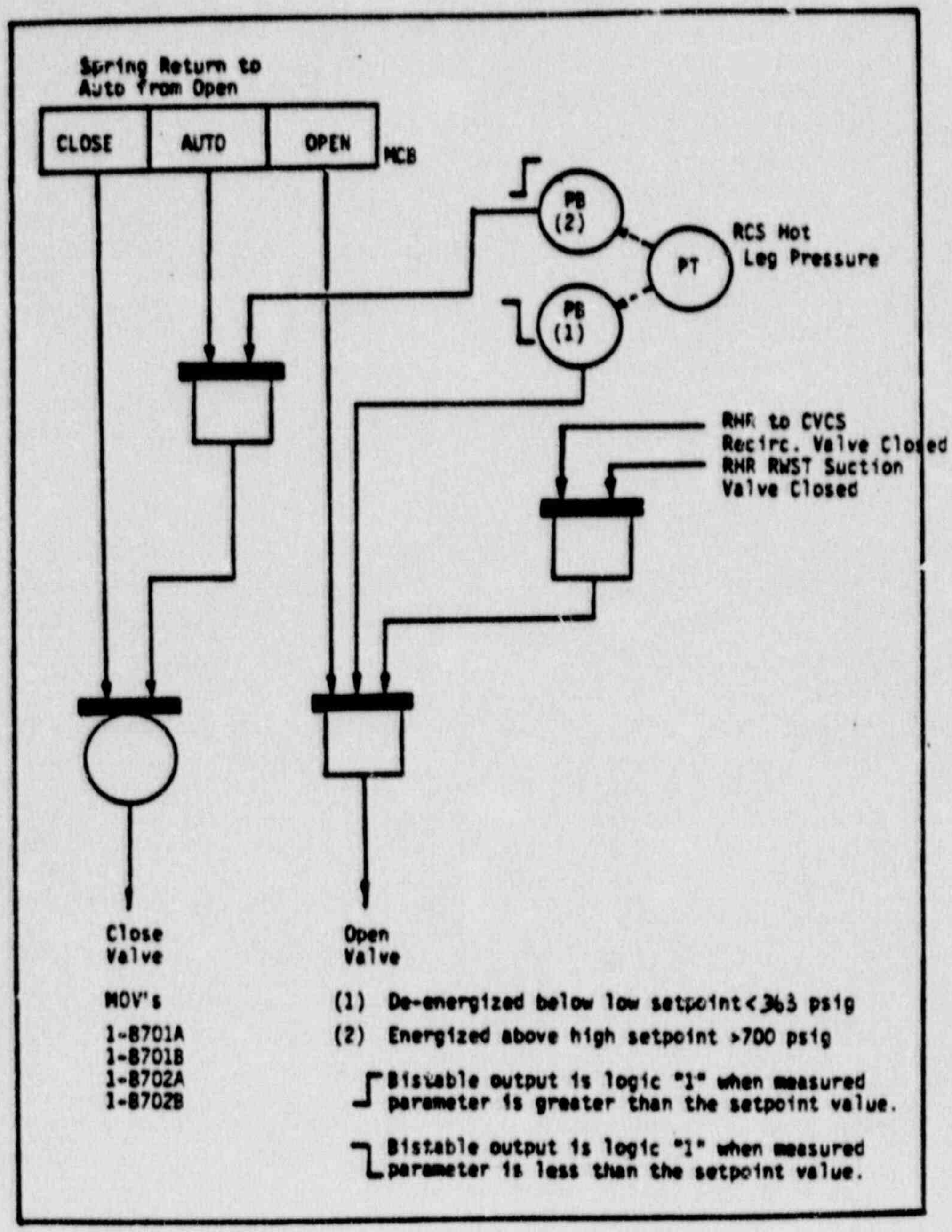


Figure 5-19. Shearon Harris Current Interlock Logic-MOVs-8701A&B, 8702A&B (1RH1, 1RH2, 1RH-39, 1RH-40) Sheet 1 of 2

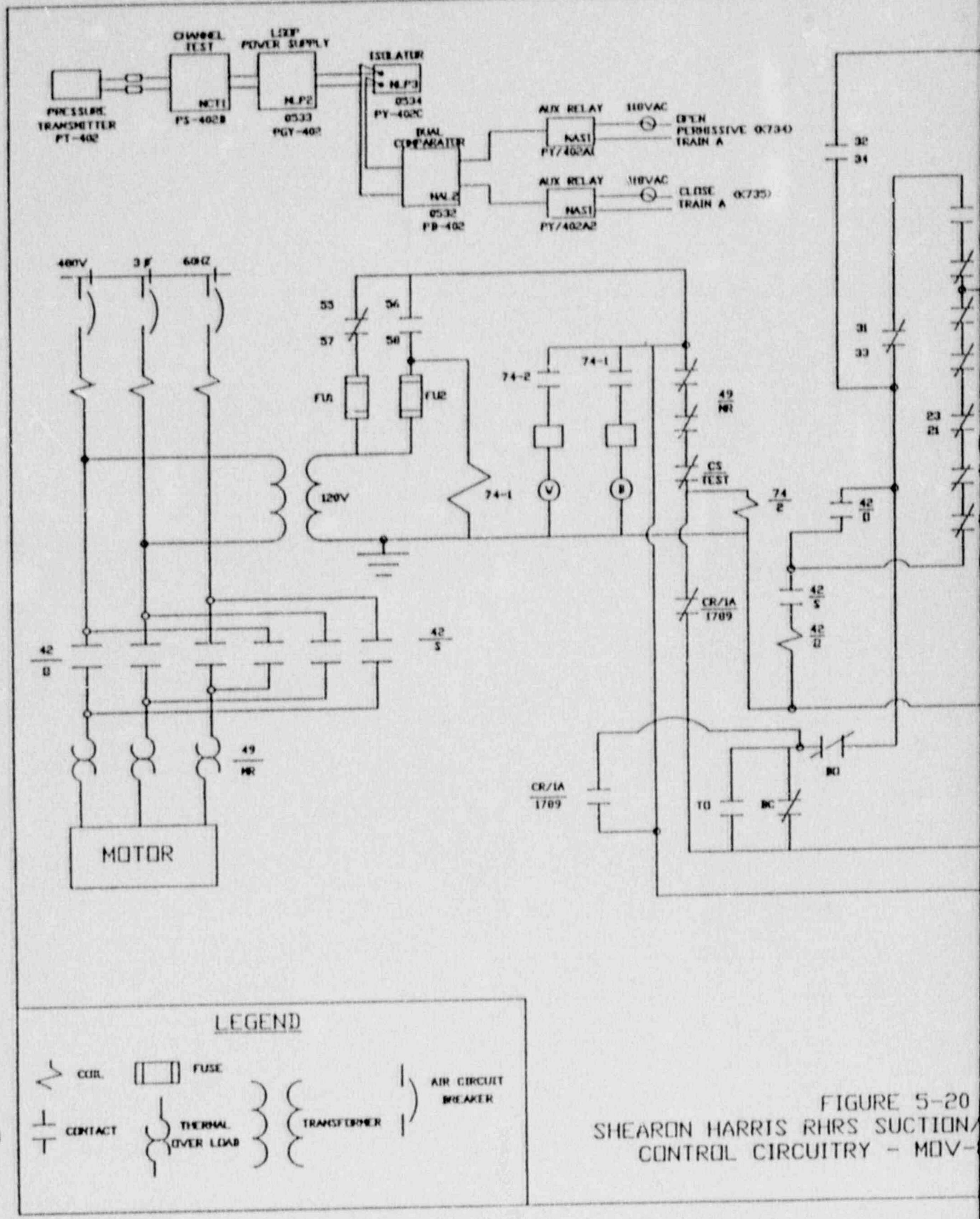
Interlock with \ Valve	1-8701 A (Train A)	1-8701 B (Train A)	1-8702 A (Train B)	1-8702 B (Train B)
PT RCS Hot Leg Pressure	402 (Train A)	402 (Train A)	403 (Train B)	403 (Train B)
RHR to CVCS Rec. Valve	1-3706 A SW. #1 (Train A)	1-8706 B SW. #2 (Train A)	1-8706 A SW. #2 (Train B)	1-8706 B SW. #1 (Train B)
RHR RWST Suction Valve	1-8809A SW. #1 (Train A)	1-8809B SW. #2 (Train A)	1-8809A SW. #2 (Train B)	1-8809B SW. #1 (Train B)

SW = Switch

NOTE: SW #1 - Torque switch powered by same train as valve.

SW #2 - Stem mounted limit switch powered by train different from valve power.

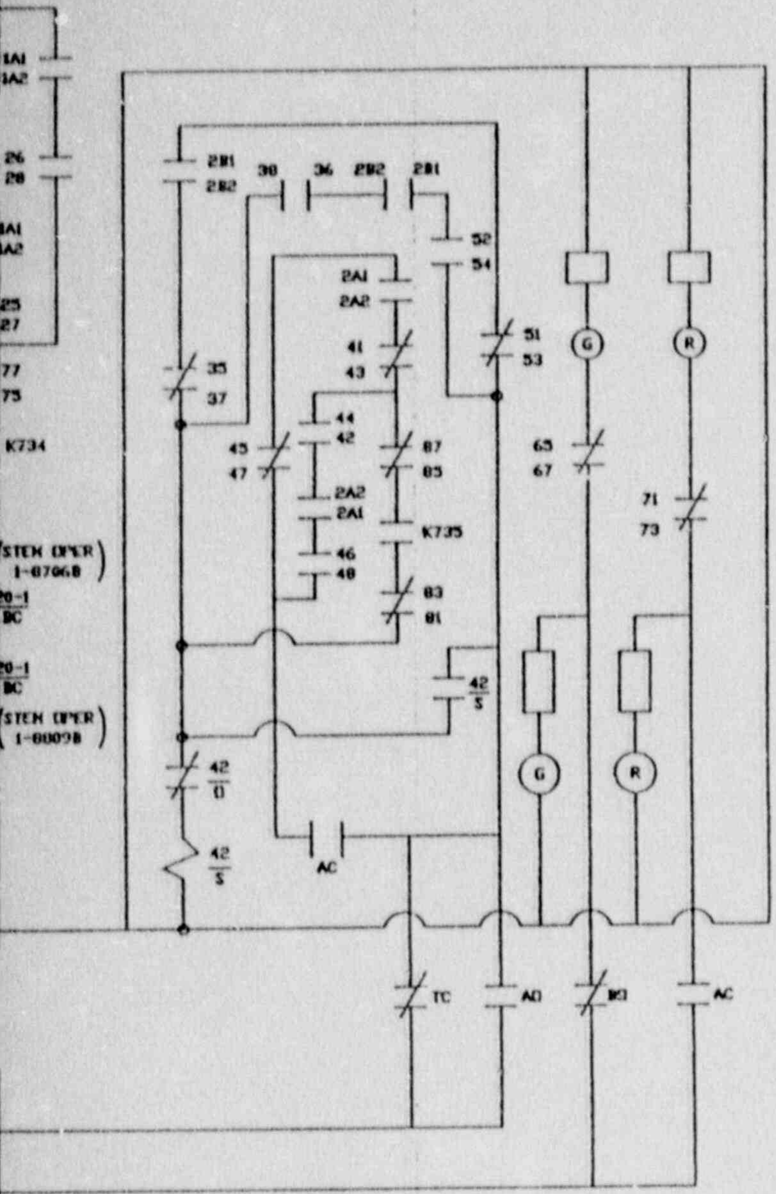
Figure 5-19. Shearon Harris Current Interlock Logic-MOVs-8701A&B, 8702A&B (1RH1, 1RH2, 1RH-39, 1RH-40) Sheet 2 of 2



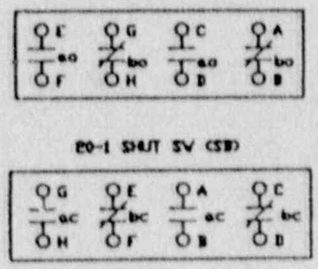
RCS_SH20

FIGURE 5-20
SHEARON HARRIS RHRS SUCTION/
CONTROL CIRCUITRY - MOV-

2/11/88



20-1 OPEN SV (SB)



20-1 SHUT SV (SB)

SHOWN FOR VALVE SHUT

CONTACTS		POSITION		
		SHUT	NORMAL	OPEN
1A1 O-||-O 1A2	A			X
1B1 O-||-O 1B2	B		X	
2A1 O-||-O 2A2	A		X	
2B1 O-||-O 2B2	B	X		

SPRING RETURN TO NORMAL
X-CONTACT CLOSED

NOTE
1. K734 CLOSES AT RCS PRESS< 425 PSIG AND K735 CLOSES AT RCS PRESS > 700 PSIG

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0 – 100)	CWD SH
bo	4			■
ac		8		■
bo	3			■
ac		7		
ao	2			
bc		6		
ao	1			■
bc		5		■
ac		16		
bo	12			
ac		15		■
bo	11			
bc		14		
ao	10			
bc		13		
ao	9			
tc	17		OPENS ON OVLD ON CLOSE STRK	■
to	18		OPENS ON OLVD ON OPEN STRK	■
——— = CONT CLOSED ■ = THIS SHEET				

ISOLATION VALVE
8701B (1RH-40)

SI
APERTURE
CARD

Also Available On
Aperture Card

REF.
CAR 2166 B-401 SH 326
V 2034578 SH 11

8911150026-29

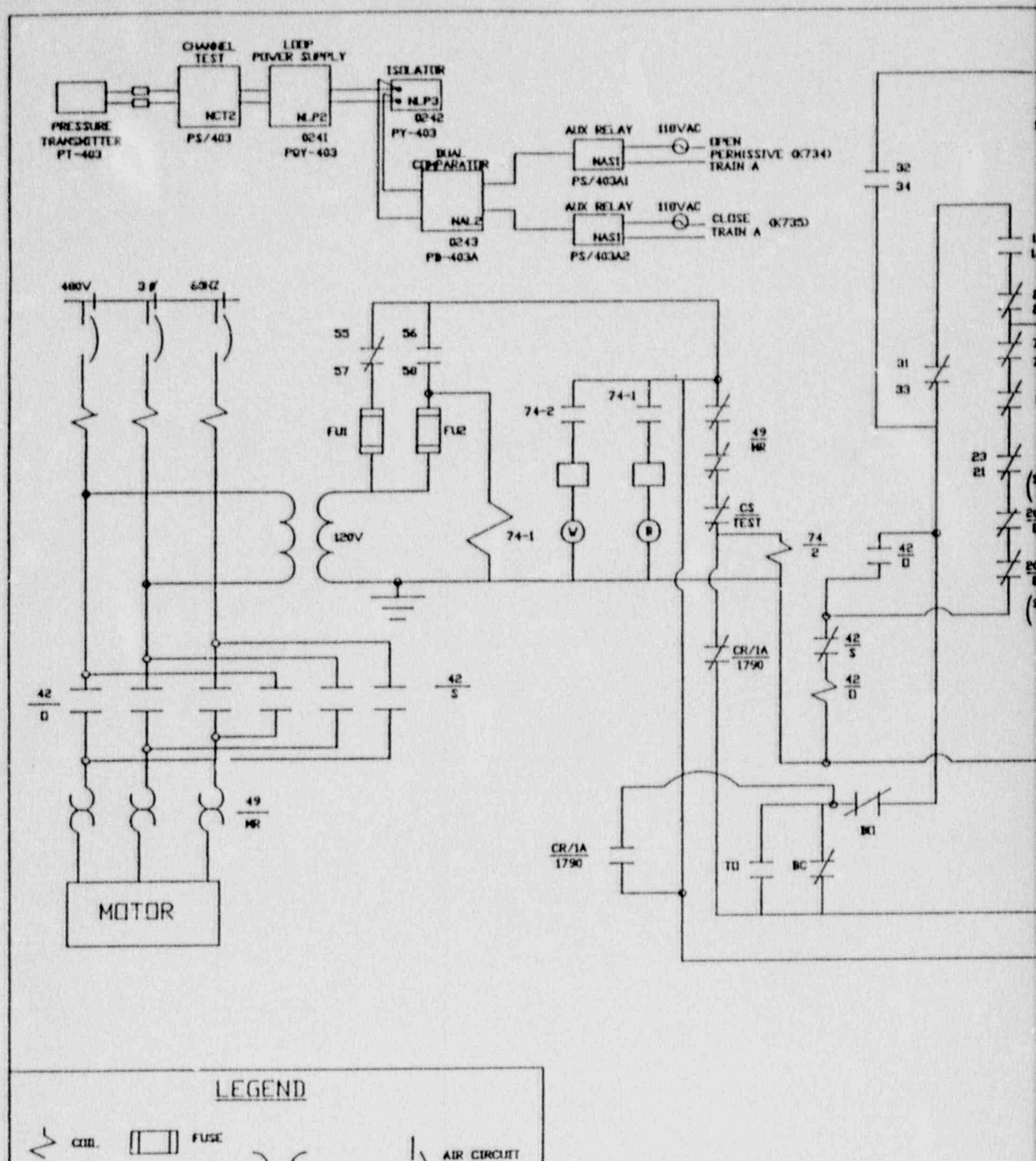
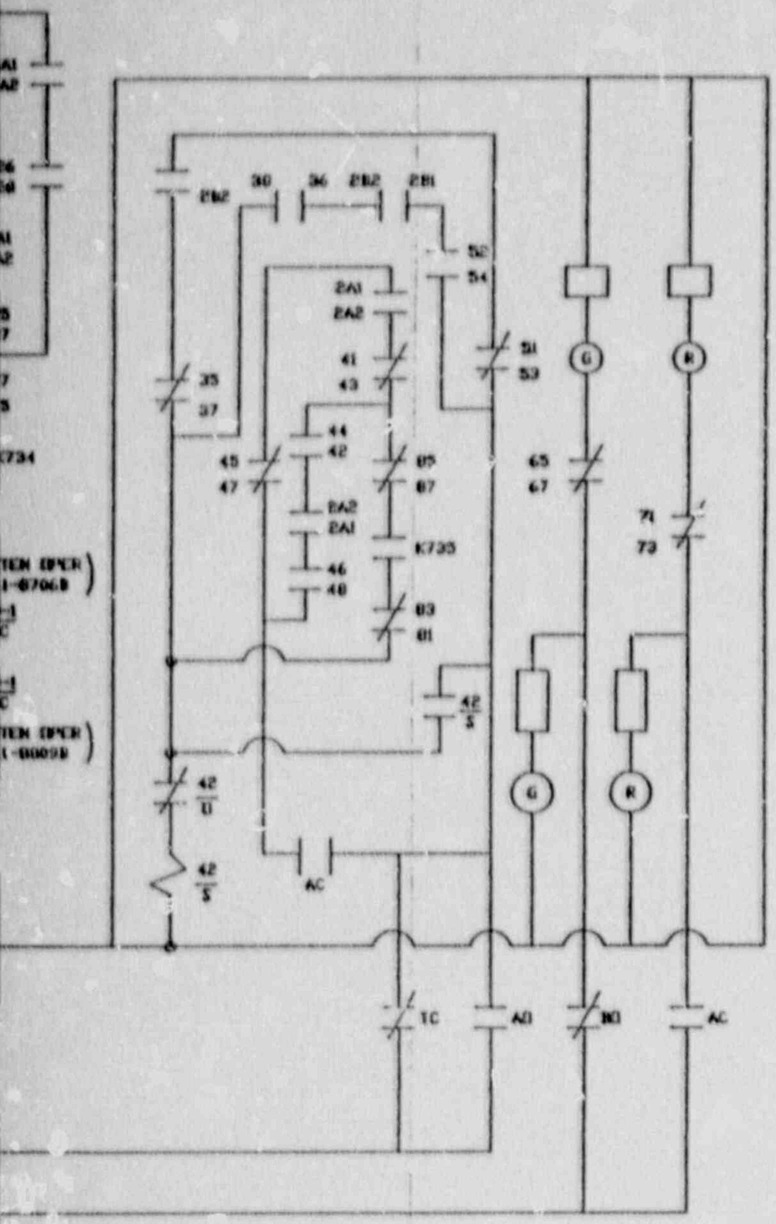


FIGURE 5-21
SHEARON HARRIS RHRS SUCTION/I
CONTORL CIRCUITRY - MOV-8702

RCS_SH21

2/11/88



CONTACTS		POSITION		
		SHUT	NORMAL	OPEN
1A1 O-||-O 1A2	A			X
1B1 O-||-O 1B2	B		X	
2A1 O-||-O 2A2	A		X	
2B1 O-||-O 2B2	B	X		

SPRING RETURN TO NORMAL
X-CONTACT CLOSED

NOTE
1. K734 CLOSES AT RCS PRESS< 425 PSIG AND K735 CLOSES AT RCS PRESS > 700 PSIG

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0 — 100)	CWD SH
bo	4		——— (0 to ~80)	•
ac		8	——— (~20 to 100)	•
bo	3		——— (0 to ~80)	•
ac		7	——— (~20 to 100)	
ao	2		——— (~80 to 100)	
bc		6	——— (0 to ~20)	
ao	1		——— (~80 to 100)	•
bc		5	——— (0 to ~20)	•
ac		16	——— (~20 to 100)	
bo	12		——— (0 to ~80)	
ac		15	——— (~20 to 100)	•
bo	11		——— (0 to ~80)	
bc		14	——— (0 to ~20)	
ao	10		——— (~80 to 100)	
bc		13	——— (0 to ~20)	330
ao	9		——— (~80 to 100)	
tc	17		OPENS ON OVLD ON CLOSE STRK	•
to	18		OPENS ON OLVD ON OPEN STRK	•

——— = CONT CLOSED • = THIS SHEET

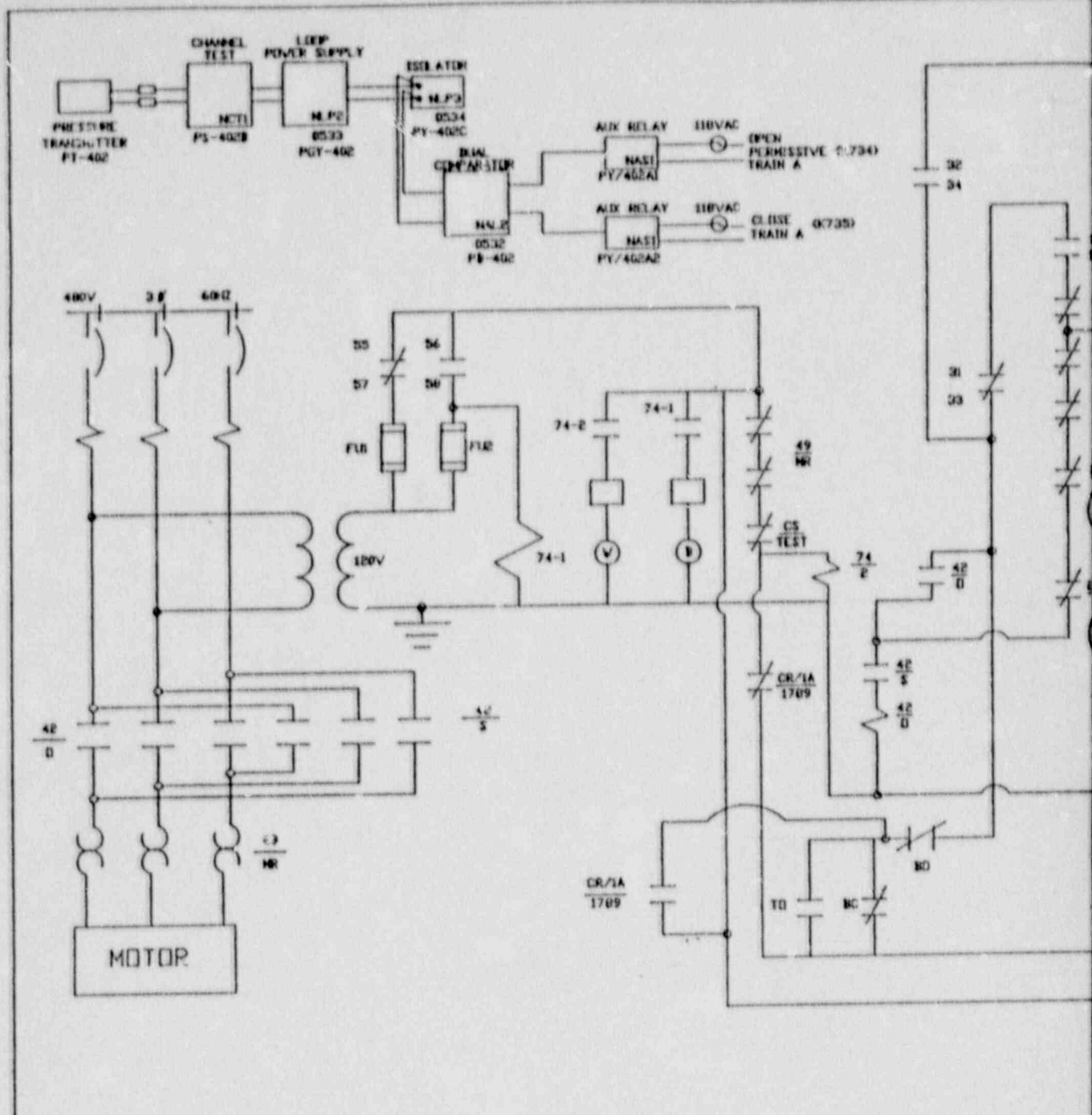
REF.
CAR 2166 B-401 SH 32B
V 2445044 SH 8

SOLATION VALVE
B (1RH-39)

SI
APERTURE
CARD

Also Available On
Aperture Card

8911150026-21



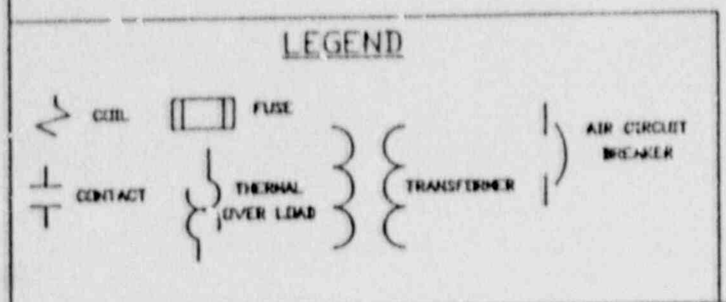
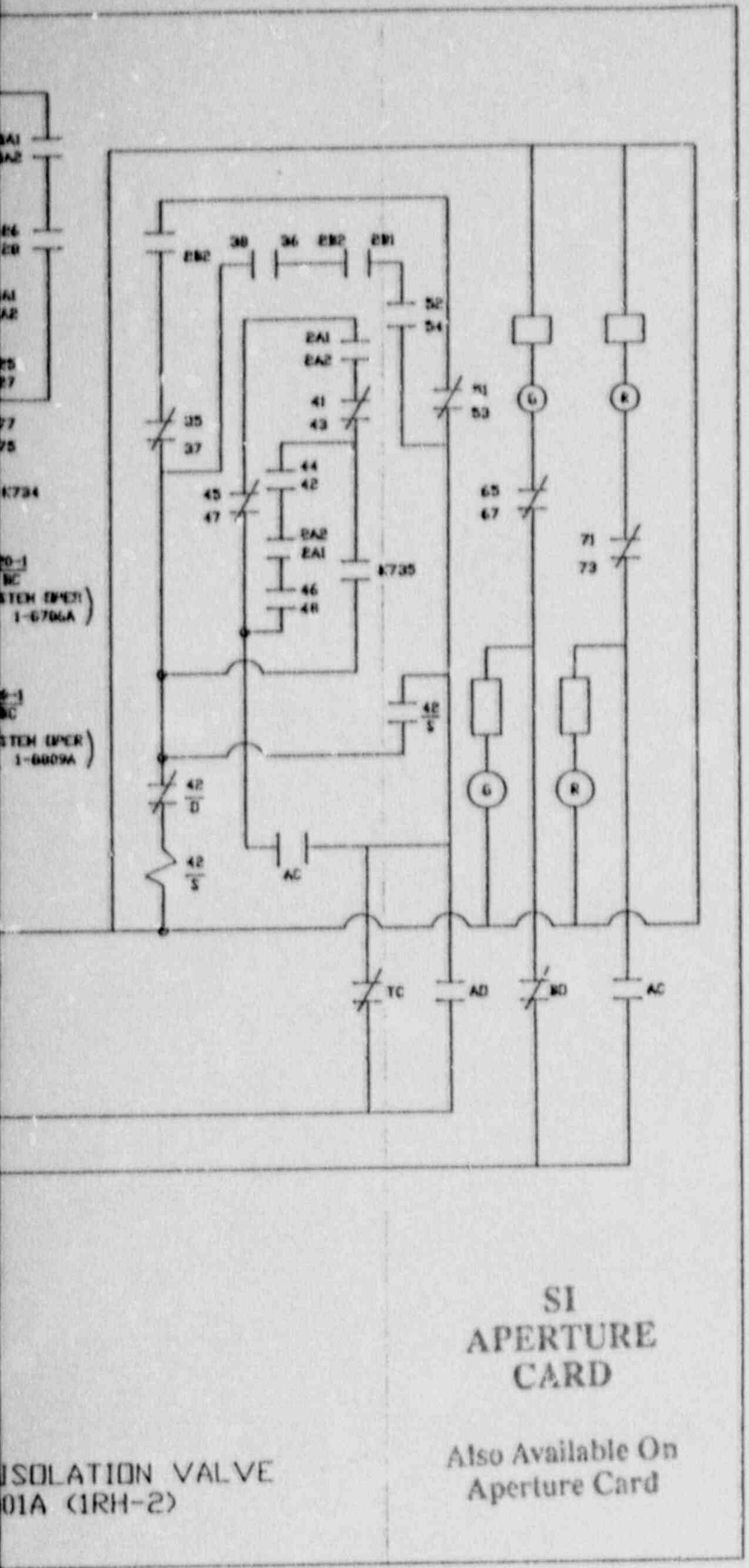


FIGURE 5-22
SHEARON HARRIS RHRS SUCTION/
CONTROL CIRCUITRY - MOV-87

RCS_SH22

2/11/88



CONTACTS		POSITION		
		SHUT	NORMAL	OPEN
1A1 O-||-O 1A2	A			X
1B1 O-||-O 1B2	B		X	SPARE
2A1 O-||-O 2A2	A		X	
2B1 O-||-O 2B2	B	X		

SPRING RETURN TO NORMAL
X-CONTACT CLOSED

NOTE

1. K734 CLOSES AT RCS PRESS< 425 PSIG AND K735 CLOSES AT RCS PRESS > 700 PSIG

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0 – 100)	CWD SH
bo	4			■
ac		8		■
bo	3			■
ac		7		
ao	2			
bc		6		
ao	1			■
bc		5		■
ac		16		
bo	12			
ac		15		■
bo	11			
bc		14		
ao	10			
bc		13		
ao	9			
tc	17		OPENS ON OVLD ON CLOSE STRK	■
to	18		OPENS ON OLVD ON OPEN STRK	■

——— = CONT CLOSED ■ = THIS SHEET

REF.
CAR 2166 B-401 SH 325
V 2034578 SH 11

8911150026-22

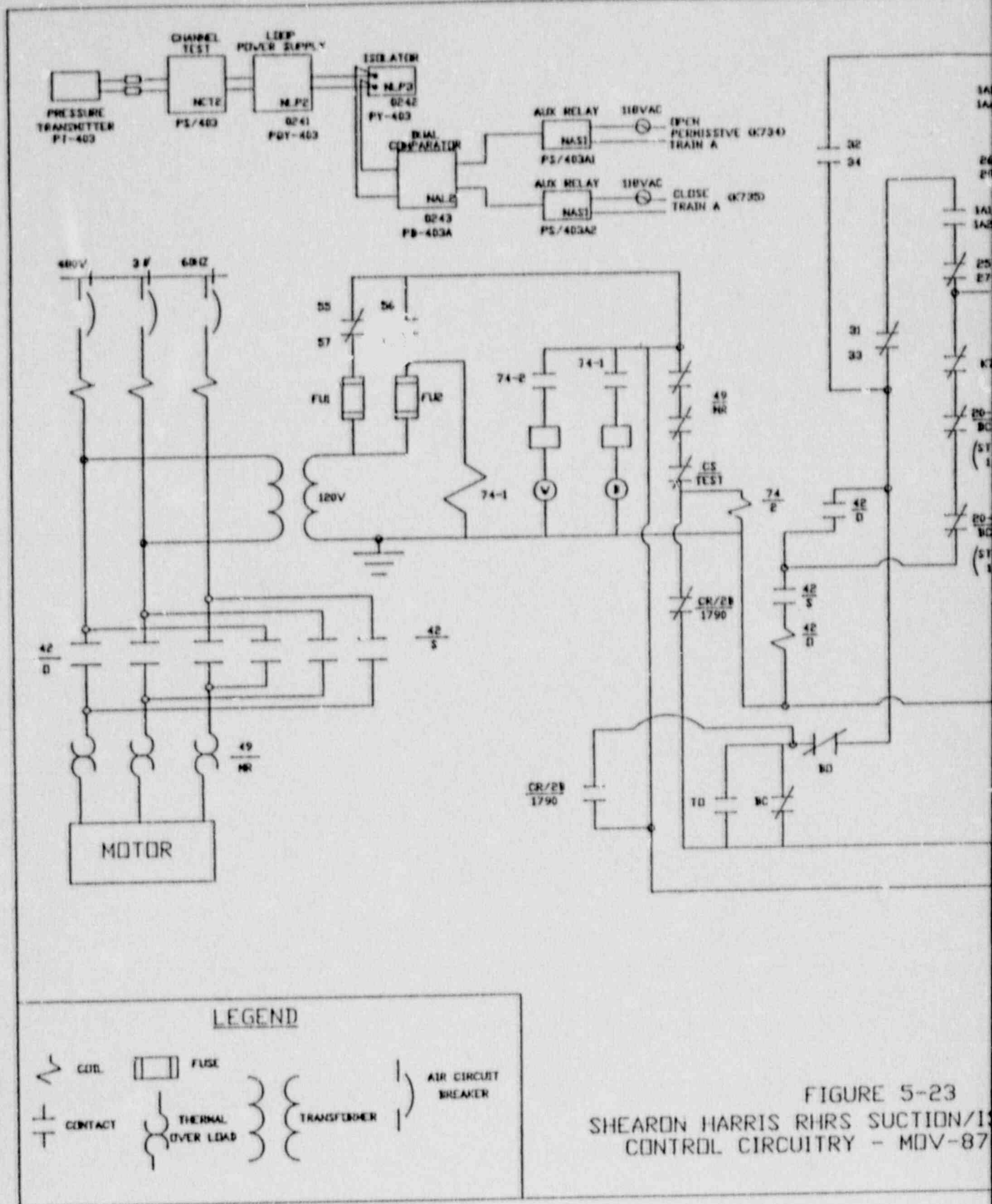
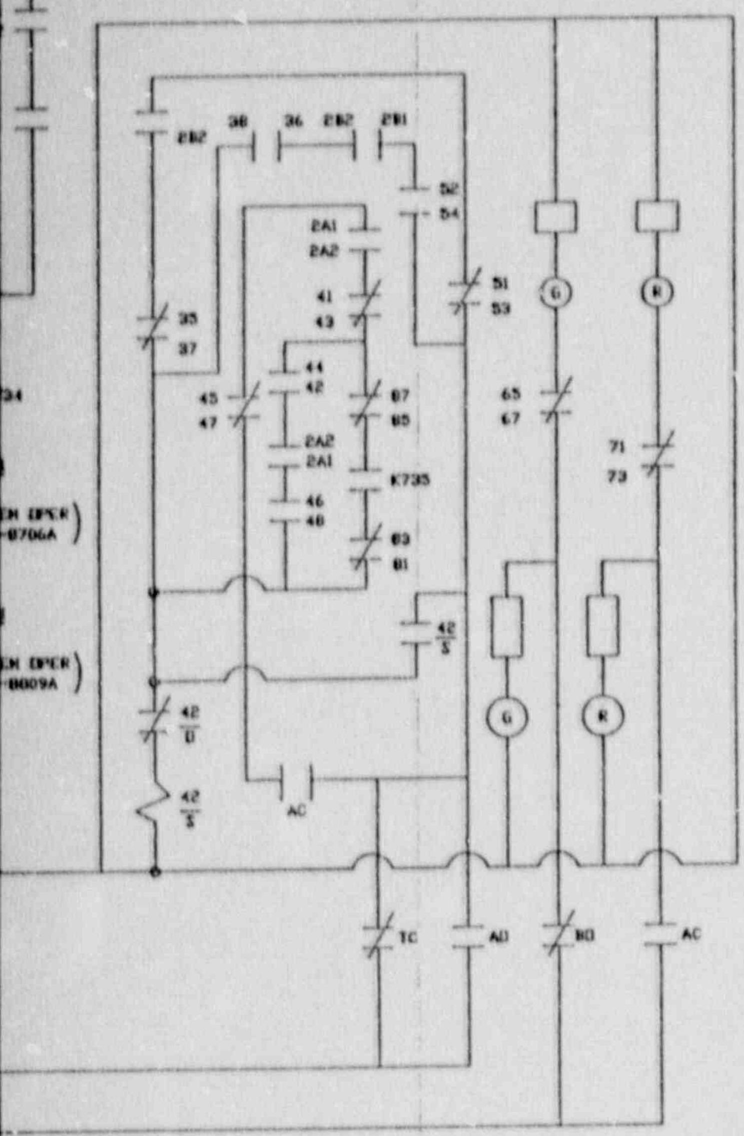
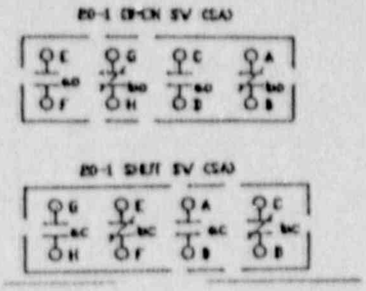


FIGURE 5-23
SHEARON HARRIS RHRS SUCTION/I
CONTROL CIRCUITRY - MOV-87

RCS_SH23

2/11/88





SHOWN FOR VALVE SHUT

CONTACTS		POSITION		
		SHUT	NORMAL	OPEN
1A1 O-||-O 1A2	A			X
1B1 O-||-O 1B2	B		X	
2A1 O-||-O 2A2	A		X	
2B1 O-||-O 2B2	B	X		

SPRING RETURN TO NORMAL
X-CONTACT CLOSED

NOTE

1. K734 CLOSES AT RCS PRESS< 425 PSIG AND K735 CLOSES AT RCS PRESS > 700 PSIG

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0–100)	CWD SH
bo	4		——	•
ac		8	——	•
bo	3		——	•
ac		7	——	
ao	2		——	
bc		6	——	
ao	1		——	•
bc		5	——	•
ac		16	——	
bo	12		——	
ac		15	——	•
bo	11		——	
bc		14	——	
ao	10		——	
bc		13	——	
ao	9		——	
tc	17		OPENS ON OVLD ON CLOSE STRK	•
to	18		OPENS ON OLVD ON OPEN STRK	•
—— = CONT CLOSED • = THIS SHEET				

SOLATION VALVE
02A (1RH-1)

SI
APERTURE
CARD

Also Available On
Aperture Card

REF.
CAR 2166 B-401 SH 327
V 2445/44 SH 8

8911150026-23

6.0 PROPOSED BASIC LOGIC CHANGE

To incorporate the removal of the autoclosure interlock (ACI) from the RHRS suction isolation valves, certain modifications must be made to the plant. These changes fall into two categories: modifications to the RHRS suction isolation valves electrical design, and modifications to plant operating procedures. The following text defines the functional requirements for these changes for each of the four lead plants. The fault tree model used in the probabilistic analysis for the lead plants is based on implementation of these proposed modifications. The final modifications made to the lead plants or a plant referencing a lead plant, must meet the given functional requirements to ensure validity of the results of this report. The reader is reminded that a description of each lead plants current RHRS suction/isolation valve interlocks and functional requirements is provided in Section 5.0.

6.1 Proposed Interlocks and Functional Requirements for Salem Unit 1

The proposed interlock change for Salem Unit 1 removes the autoclosure interlock feature from the RHRS suction/isolation valves (8701, 8702). All other valve interlock features described in Section 5.1.3 of this report remain in place. With removal of the autoclosure interlock feature, valve 1RH-1 (8702) and 1RH-2 (8701) will not close automatically on increasing RCS pressure greater than 700 psig. However, as shown on Figures 6-1 and 6-2 alarms have been added (for each RHRS suction/isolation valve) that actuate in the main control room given a "VALVE NOT FULLY CLOSED " signal in conjunction with a "RCS PRESSURE-HIGH" signal. The intent of the alarms is to alert the operator that a RCS-RHRS, series, suction/isolation valve(s) is not fully closed, and that double valve isolation from the RCS to the RHRS is not being maintained. Valve position indication to the alarm must be provided from the valve stem mounted limit switches (SMLS) and power to the SMLS must not be affected by power lockout to the valve. As with other power lockout valves, there is no requirement for opposite train power for the SMLS, only that power to the SMLS is not affected by the power lockout (see Figure 6-3).

The proposed interlocks for valves 1RH-1 (8702) and 1RH-2 (8701) are shown functionally on Figures 6-1 and 6-2. In addition, the proposed valve interlock changes are shown on the elementary wiring diagrams in Figures 6-4 and 6-5. The only change to the valves interlock and circuitry is to remove the autoclosure portion of the interlock and add a control room alarm; the valves open permissive circuit will not be altered.

In addition to changing the valves interlock circuitry, the Salem Unit 1 "Heatup from Cold Shutdown to Hot Standby" operating procedure must be modified to reflect the appropriate (new) alarm recognition and responses for the added alarms. The procedure should be revised to direct the operator to take the necessary actions to close the open RHRS suction/isolation valve (if it is not closed) following alarm actuation, or if this is not possible, to return to the safe shutdown mode of operation.

In summary, the proposed Salem Unit 1 interlock changes provide deletion of the autoclosure interlock feature from the RHRS suction/isolation valves (8701, 8702), while still meeting the regulatory requirements to retain the open permissive portion of the interlock. In addition, the changes provide a control room alarm to alert the operator if a RHRS suction/isolation valve is not fully closed.

6.2 Proposed Interlocks and Functional Requirements for Callaway

The proposed interlock change for Callaway removes the autoclose interlock feature from the RHRS suction/isolation valves (8701, 8702). All other valve interlock features described in Section 5.2.3 of this report remain in place. With removal of the autoclosure interlock feature, valves 8701A & B and 8702A & B will not close automatically on increasing RCS pressure greater than 682 psig. However, as shown on Figure 6-6 alarms have been added (for each valve in the RHRS suction line) that actuate in the Main Control Room (MCR) given a "VALVE NOT FULL CLOSED " signal in conjunction with a "RCS PRESSURE-HIGH" signal. The intent of the alarms is to alert the operator that a RCS-RHRS, series, suction/isolation valve(s) is not fully closed, and that double valve isolation from the RCS to the RHRS is not being maintained. Valve position indication to the alarm must be provided from the valve stem mounted limit switches (SMLS) and power to the SMLS must not be affected by power lockout to the valve. As with other power lockout valves, there is no requirement for opposite train power for the SMLS, only that power to the SMLS is not affected by the power lockout (see Figure 6-7).

The proposed interlocks for valves 8701A & B and 8702A & B are shown functionally on Figure 6-6. In addition, the proposed valve interlock changes are shown on the elementary wiring diagrams in Figures 6-8, 6-9, 6-10 and 6-11. The only change to the valves interlock and circuitry is to remove the autoclosure portion of the interlock and add a control room alarm; the valves open permissive circuit will not be altered.

In addition to changing the valves interlock circuitry, the Callaway "Heatup from Cold Shutdown to Hot Standby" operating procedure must be modified to reflect the appropriate (new) alarm recognition and responses for the added alarms. The procedure should be revised to direct the operator to take the necessary actions to close the open RHRS suction/isolation valve (if it is not closed) following alarm actuation, or if this is not possible, to return to the safe shutdown mode of operation.

In summary, the proposed Callaway interlock changes provide deletion of the autoclosure interlock feature from the RHRS suction/isolation valves, while still meeting the regulatory requirements to retain the open permissive portion of the interlock. In addition, the changes provide a control room alarm to alert the operator if a RHRS suction/isolation valve is not fully closed.

6.3 Proposed Interlocks and Functional Requirements for North Anna Unit 1

The proposed interlock change for North Anna removes the autoclosure interlock feature from the RHRS suction/isolation valves, MOV-1700 and MOV-1701 (700, 701). All other interlock features described in Section 5.3.3 remain in place. With removal of the autoclosure interlock feature, valves MOV-1700 and MOV-1701 will not close automatically on increasing RCS pressure greater than 582 psig. However, as shown on Figures 6-12 and 6-13 alarms have been added (for each RHRS suction/isolation valve) that actuate in the main control room given a "VALVE NOT FULLY CLOSED" signal in conjunction with a "RCS PRESSURE-HIGH" signal. The intent of the alarms is to alert the operator that a RCS-RHRS, series, suction/isolation valve(s) is not fully closed and that double valve isolation from the RCS to the RHRS is not being maintained.

The proposed North Anna interlock changes for valves MOV-1700 and MOV-1701 (700, 701) are shown functionally on Figures 6-12 and 6-13. In addition, the proposed valve interlock changes are shown on the elementary wiring diagrams in Figures 6-14 and 6-15. The only change to the valve's interlock and circuitry is to remove the autoclosure portion of the interlock and add a control room alarm; the valves open permissive circuit will not be altered.

In summary, the proposed changes provide deletion of the autoclose interlock feature from the RHRS suction isolation valves, while still meeting the regulatory requirement to retain the open permissive portion of the interlock. In addition, the changes provide installation of a control room alarm to alert the operator if a RHRS suction/isolation valve is not fully closed.

6.4 Proposed Interlocks and Functional Requirements for Shearon Harris

The proposed interlock change for Shearon Harris removes the autoclosure interlock feature from the RHRS suction/isolation valves (8701, 8702). All other valve interlock features described in Section 5.4.3 remain in place. With removal of the autoclosure interlock feature, valves 1RH-1, 1RH-2, 1RH-39 and 1RH-40 (8701A&B and 8702A&B) will not close automatically on increasing RCS pressure greater than 700 psig. However, as shown on Figure 6-16 alarms have been added (for each RHRS suction/isolation valve) that actuate in the main control room given a "VALVE NOT FULL CLOSED" signal in conjunction with a "RCS PRESSURE-HIGH" signal. The intent of the alarms is to alert the operator that a RCS-RHRS, series, suction/isolation valve(s) is not fully closed, and that double valve isolation from the RCS to the RHRS is not being maintained. Valve position indication to the alarm must be provided from the valve stem mounted limit switches (SMLS) and power to the SMLS must not be affected by power lockout to the valve. As with other power lockout valves, there is no requirement for opposite train power for the SMLS, only that power to the SMLS is not affected by the power lockout (see Figure 6-17).

The proposed interlocks for valves 1RH-1, 1RH-2, 1RH-39 and 1RH-40 (8701A&B and 8702A&B) are shown functionally on Figure 6-16. In addition, the proposed valve interlock changes are shown on the elementary wiring diagrams in Figures 6-18, 6-19, 6-20 and 6-21. The only change to the valves interlock and circuitry is to remove the autoclosure portion of the interlock and add a control room alarm; the valves open permissive circuit will not be altered.

In addition to changing the valves interlock circuitry, the Shearon Harris "Heatup from Cold Shutdown to Hot Standby" operating procedure must be modified to reflect the appropriate (new) alarm recognition and responses for the added alarms. The procedure should be revised to direct the operator to take the necessary actions to close the open RHRS suction/isolation valve (if it is not closed) following alarm actuation, or if this is not possible, to return to the safe shutdown mode of operation.

In summary, the proposed Shearon Harris interlock changes provide deletion of the autoclosure interlock feature from the RHRS suction/isolation valves, while still meeting the regulatory requirements to retain the open permissive portion of the interlock. In addition, the changes provide a control room alarm to alert the operator if a RHRS suction/isolation valve is not fully closed.

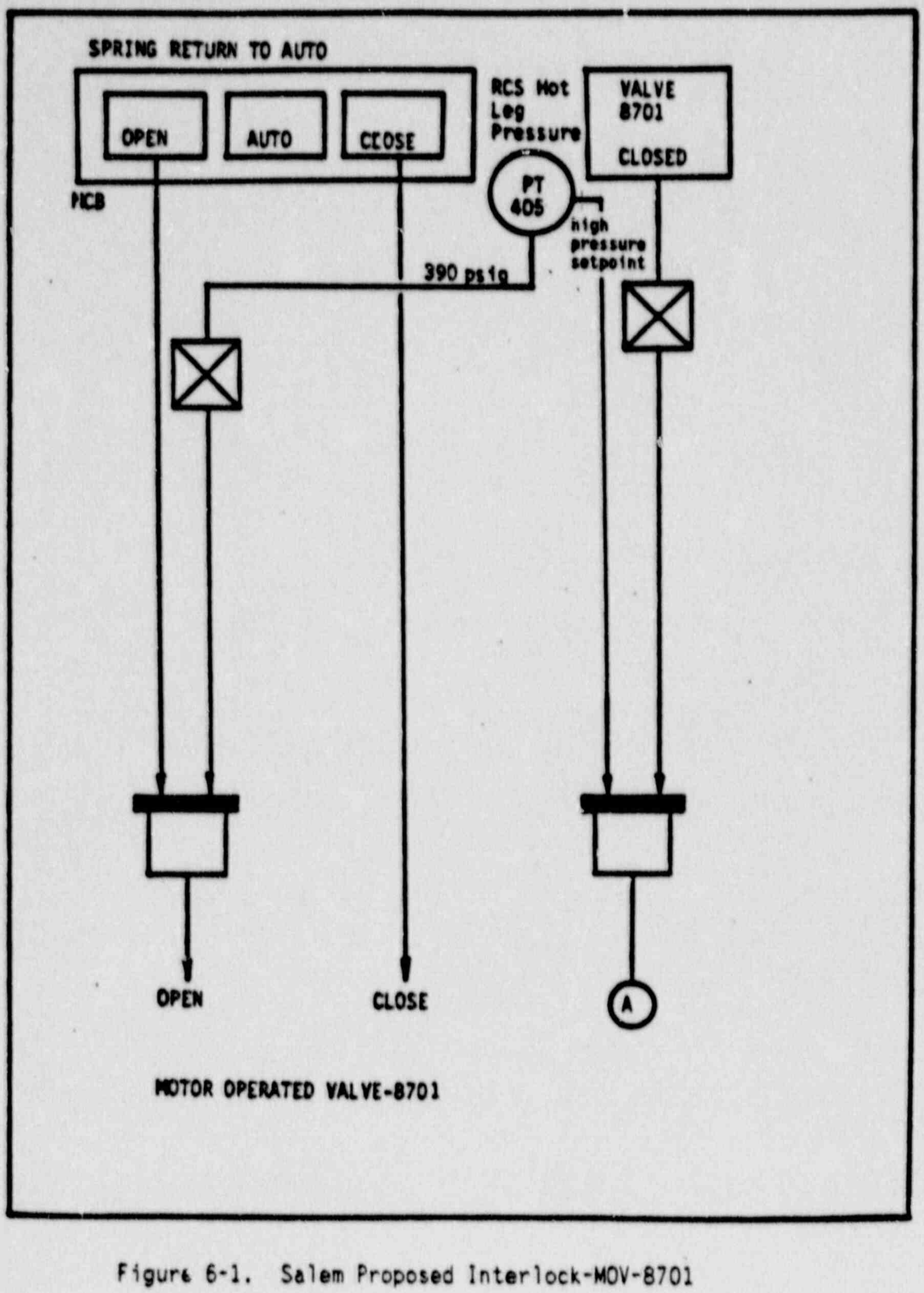


Figure 6-1. Salem Proposed Interlock-MOV-8701

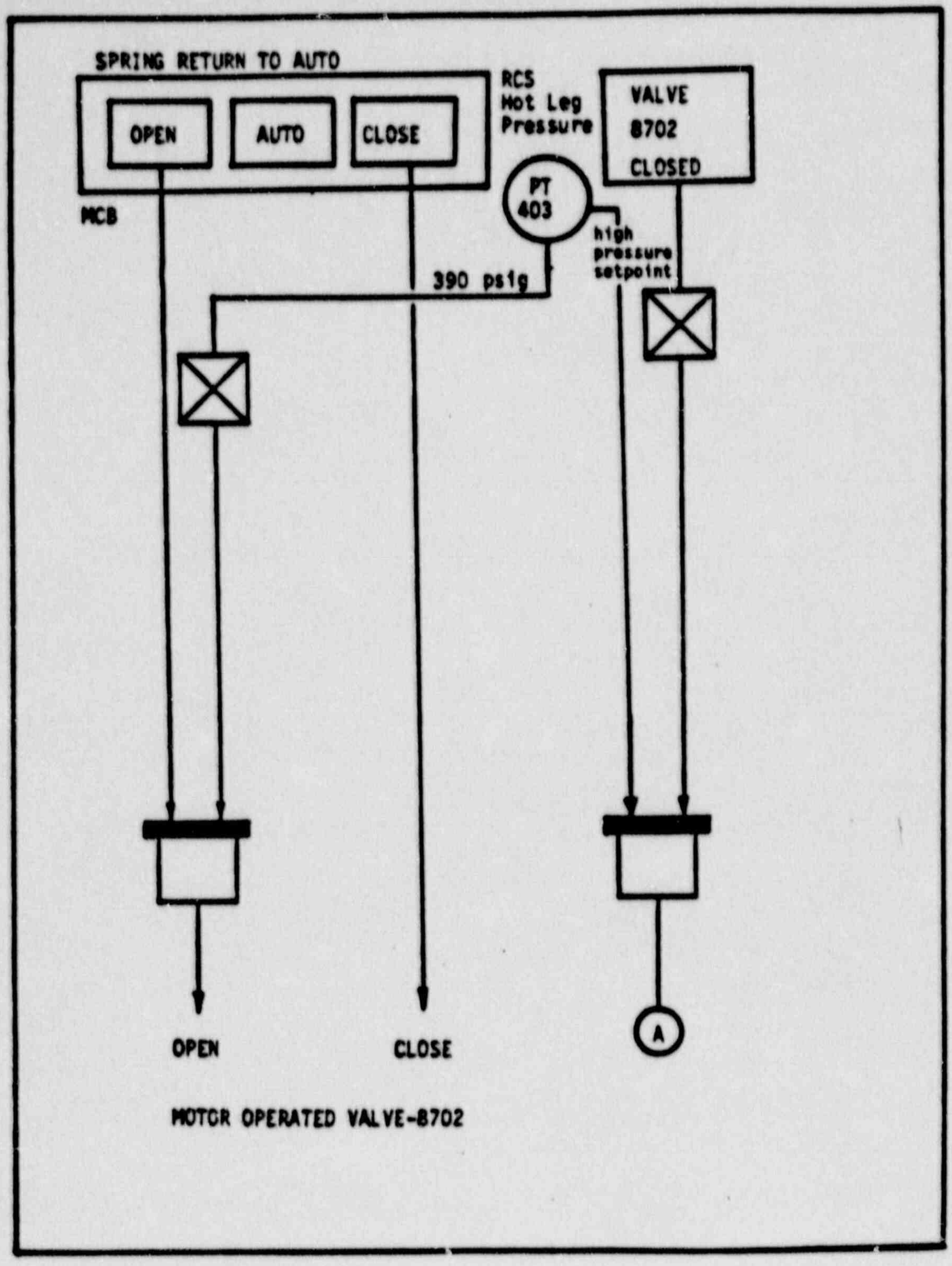


Figure 6-2. Salem Proposed Interlock-MOV-8702

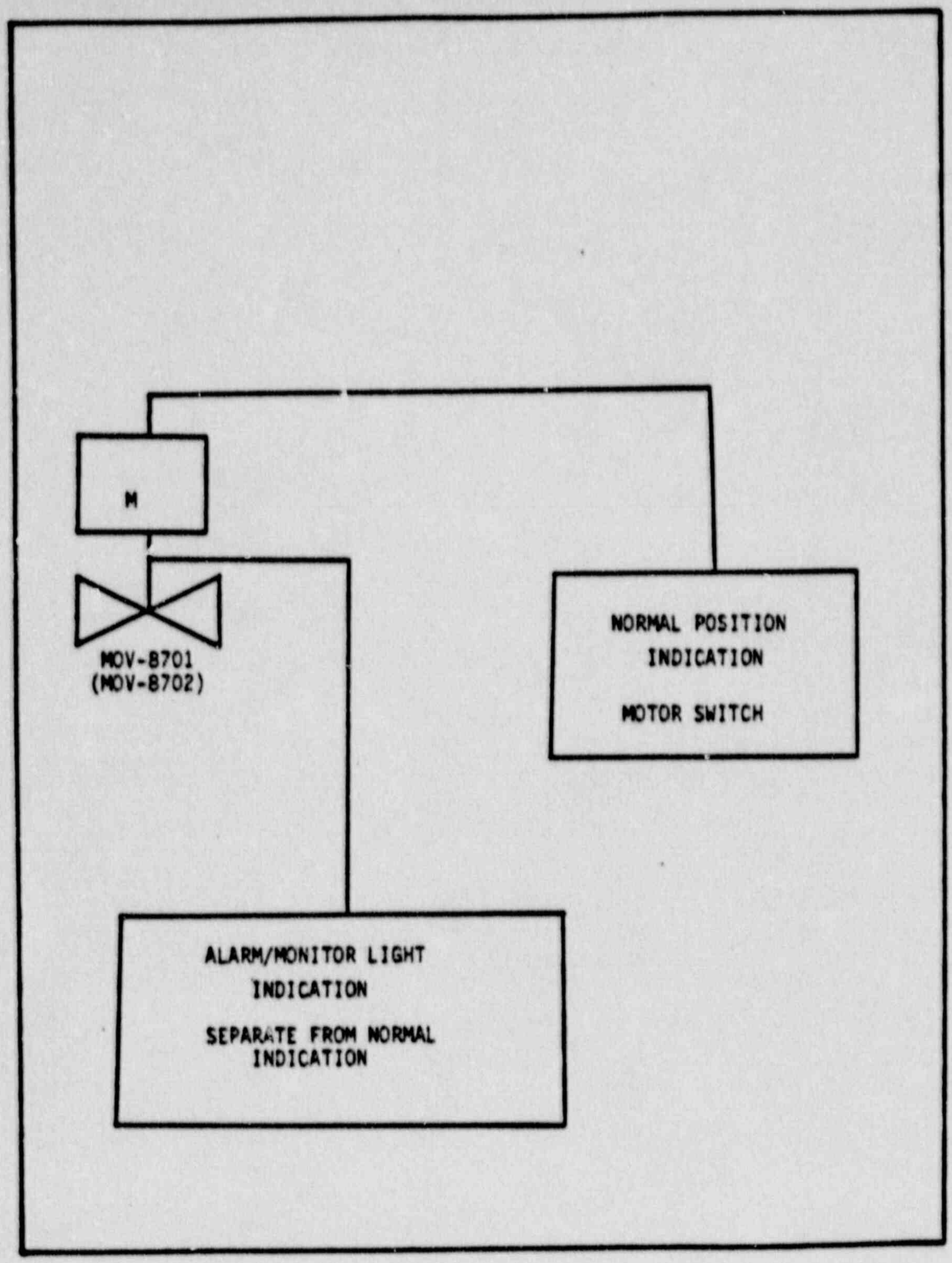
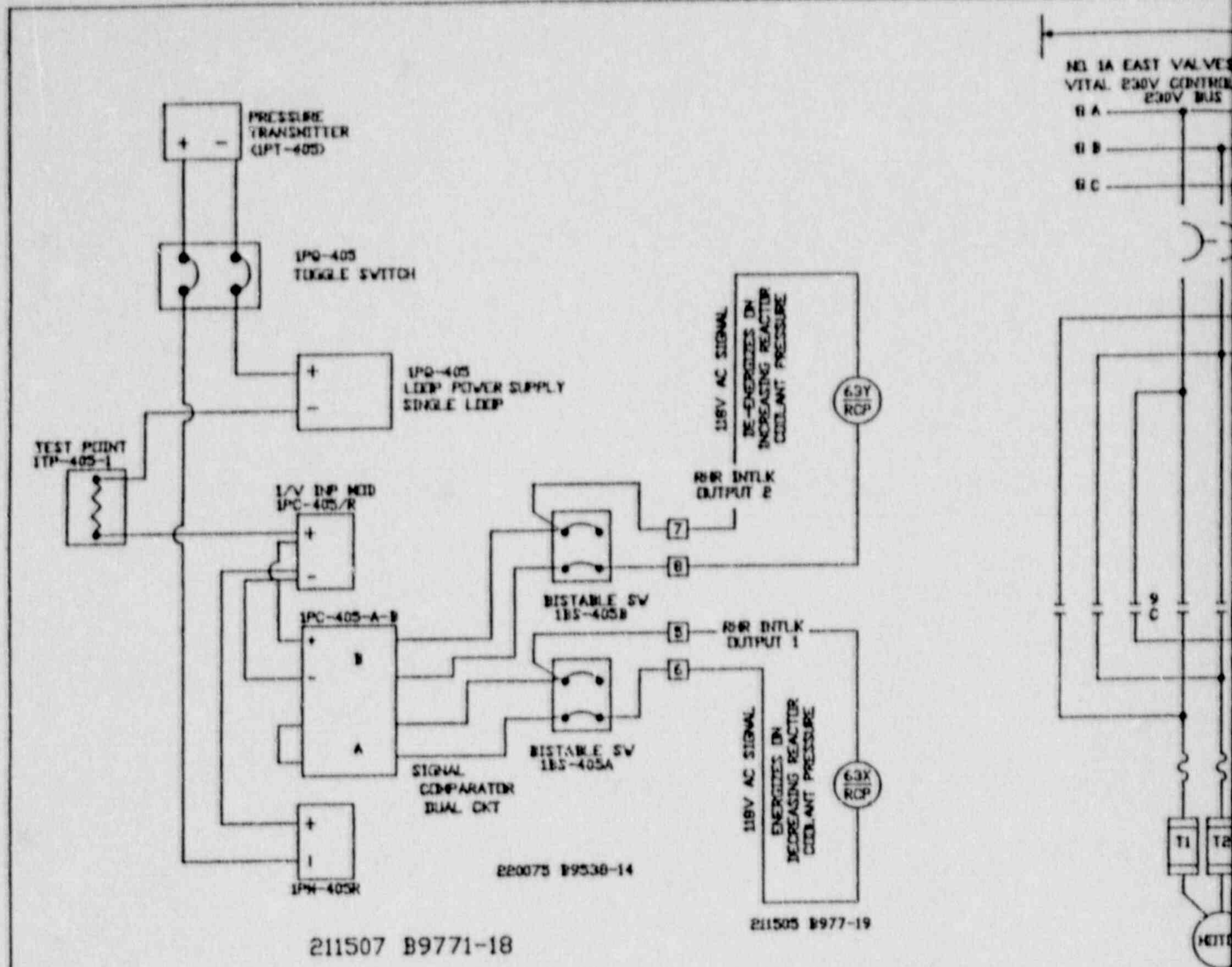


Figure 6-3. Salem Position Indication-MOV-8701 (8702)



LEGEND

- CONTROL CIRCUIT BREAKER
- FUSE
- DIODE
- CONTACT OPEN
- CONTACT CLOSED
- THERMAL OVERLOADS
- (R) INDICATING LIGHTS R - RED G - GREEN
- VOLTAGE TRANSFORMER

NOTES

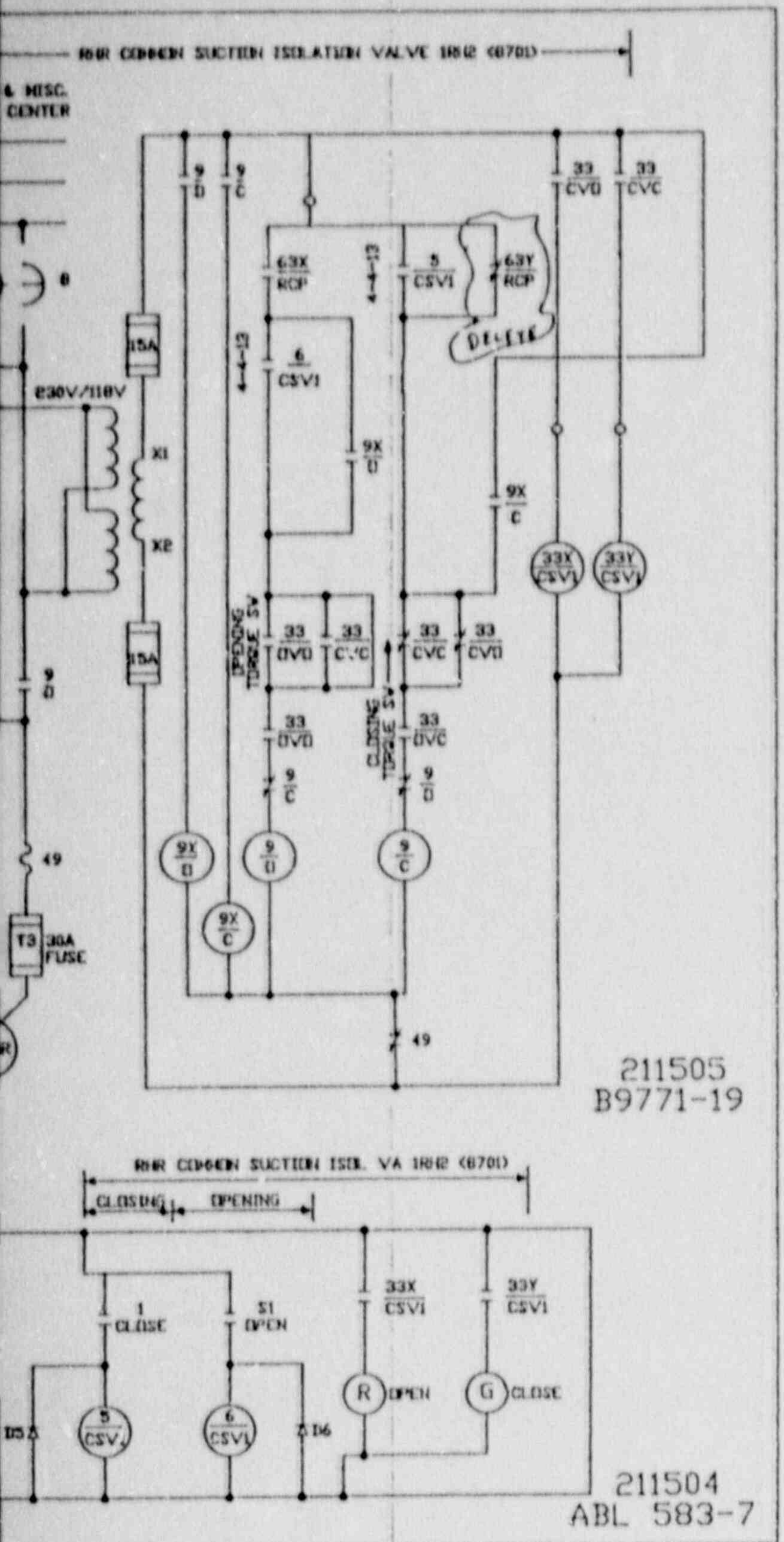
- 5/CSV1 CLOSING RELAY COIL
- 6/CSV1 OPENING RELAY COIL
- 33/OVO VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY OPEN
- 33/OVC VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY CLOSED
- 33/CVO VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY OPEN
- 33/CVC VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY CLOSED
- 9/O REVERSING CONTACTOR OPENING
- 9/C REVERSING CONTACTOR CLOSING
- 63Y/RCP REACTOR COOLANT PRESSURE AUX RELAY
- 63X/RCP REACTOR COOLANT PRESSURE AUX RELAY
- 9X/C AUX RELAY TO CONTACTOR CLOSING COILS
- 9X/O AUX RELAY TO CONTACTOR OPENING COILS
- 33X/CSV1 VALVE FULLY OPEN AUX RELAY
- 33Y/CSV1 VALVE FULLY CLOSED AUX RELAY

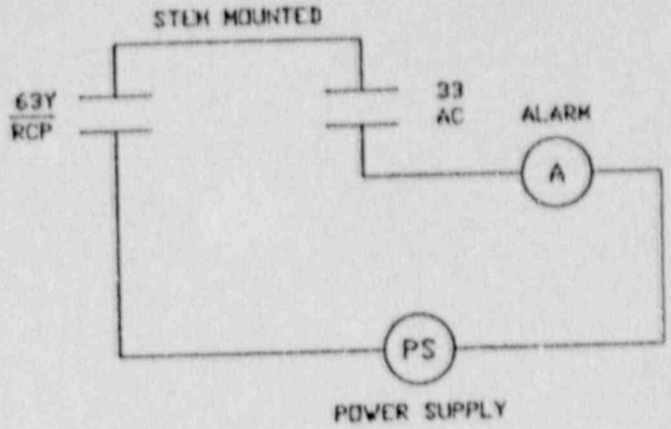
28V DC SUPPLY AT CONTROL CABINET

RHR_1RH2

1/26/88

SALEM RHR SUCTION
ISOLATION VALVE 1RH2
CONTROL CIRCUITRY





TO BE DELETED

PROPOSED CHANGE

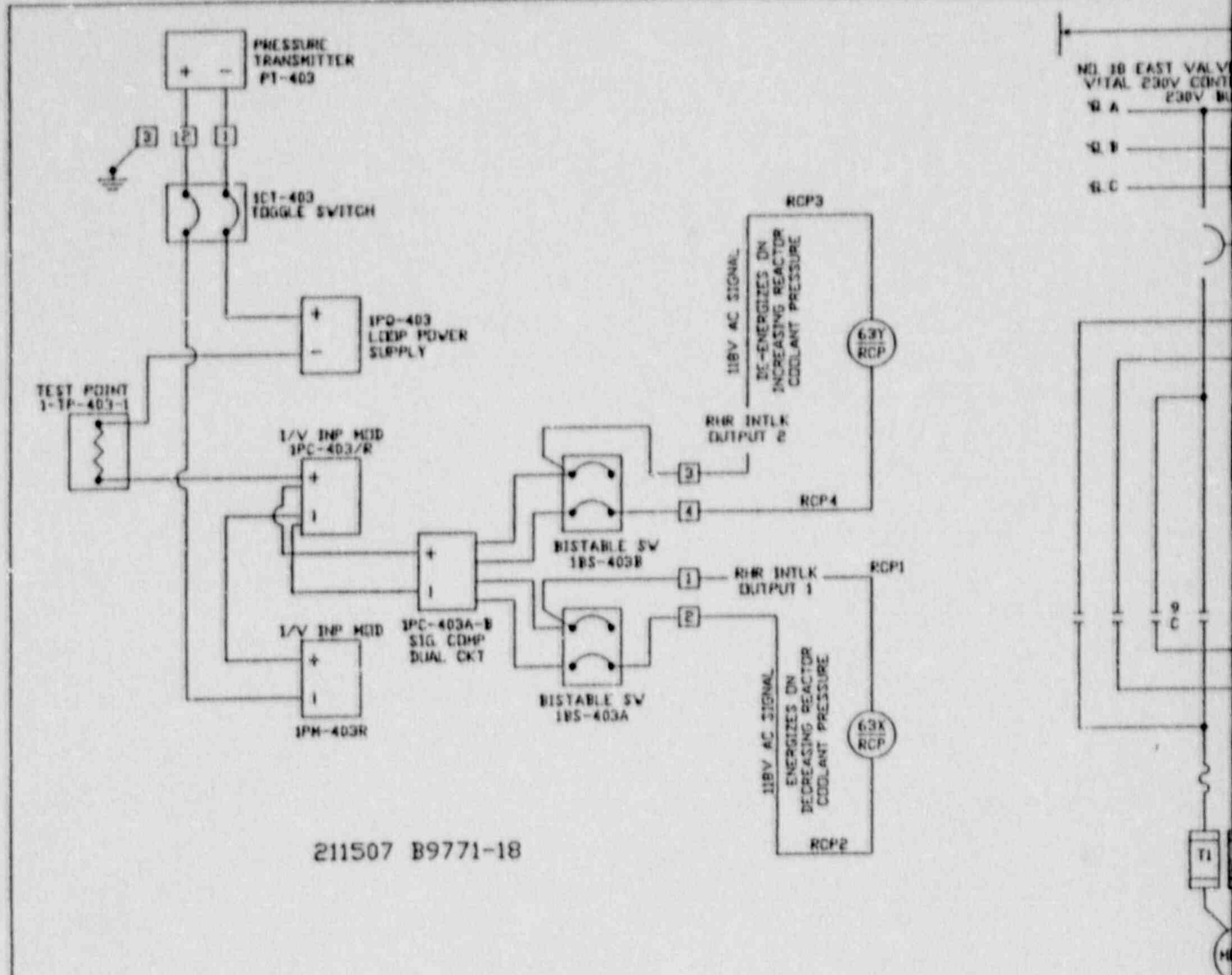
SI
APERTURE
CARD

Also Available On
Aperture Card

Figure 6-4

Salem MOV-8701 Elementary Wiring Diagram
– Proposed

8911150026-24



LEGEND

- CONTROL CIRCUIT BREAKER
- FUSE
- DIODE
- CONTACT OPEN
- CONTACT CLOSED
- THERMAL OVERLOADS
- (R) INDICATING LIGHTS R - RED G - GREEN
- VOLTAGE TRANSFORMER

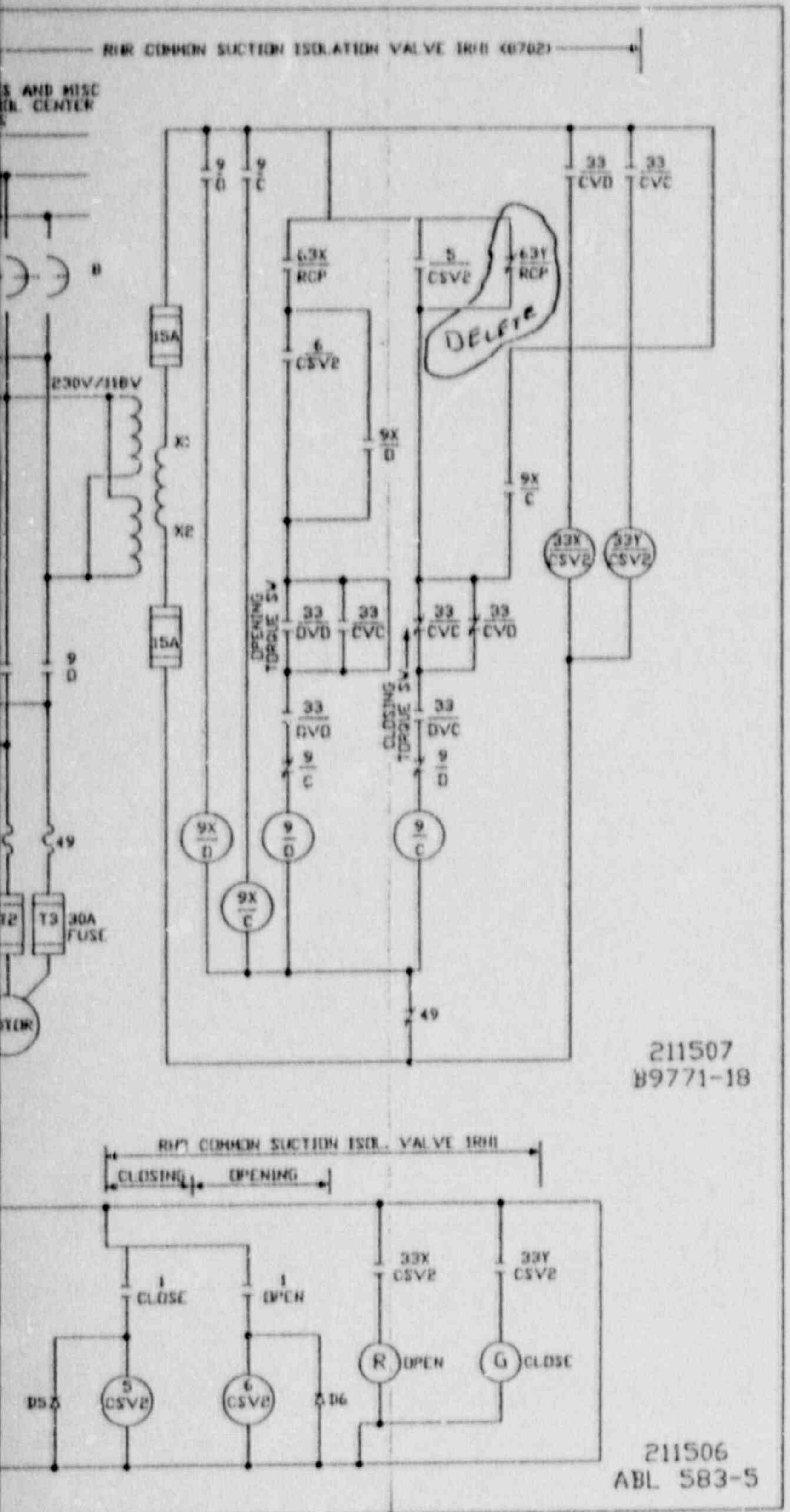
NOTES

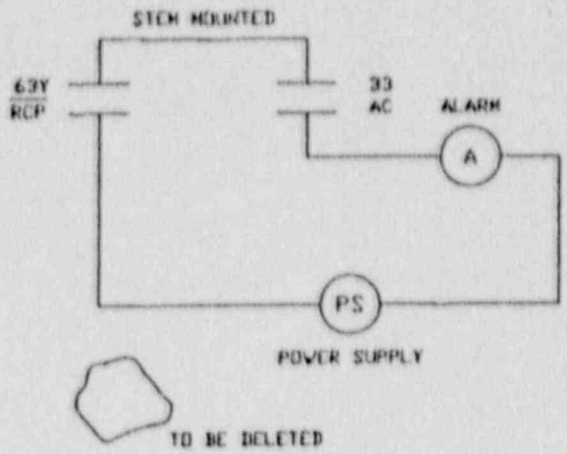
5/CSV2	CLOSING RELAY COIL
6/CSV2	OPENING RELAY COIL
33/OVO	VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY OPEN
33/OVC	VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY CLOSED
33/CVO	VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY OPEN
33/CVC	VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY CLOSED
9/O	REVERSING CONTACTOR OPENING
9/C	REVERSING CONTACTOR CLOSING
63Y/RCP	REACTOR COOLANT PRESSURE AUX RELAY
63X/RCP	REACTOR COOLANT PRESSURE AUX RELAY
9X/C	AUX RELAY TO CONTACTOR CLOSING COILS
9X/O	AUX RELAY TO CONTACTOR OPENING COILS
33X/CSV2	VALVE FULLY OPEN AUX RELAY
33Y/CSV2	VALVE FULLY CLOSED AUX RELAY

RHR_1RH1

2/1/88

SALEM RHR SUCTION
ISOLATION VALVE 1RH1
CONTROL CIRCUITRY

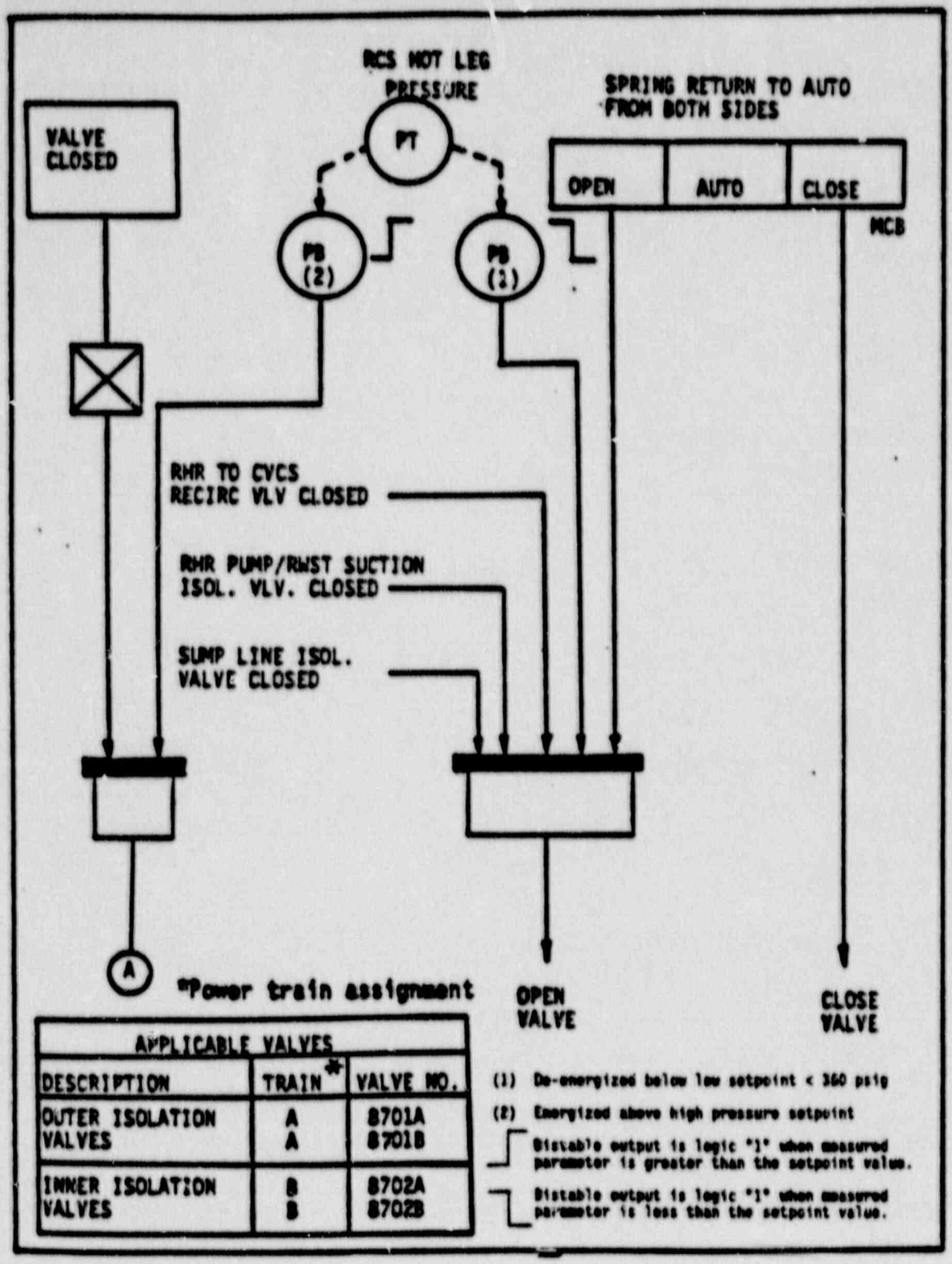




PROPOSED CHANGE

Figure 6-5

Salem MOV-8702 Elementary Wiring Diagram - Proposed



APPLICABLE VALVES		
DESCRIPTION	TRAIN*	VALVE NO.
OUTER ISOLATION VALVES	A A	8701A 8701B
INNER ISOLATION VALVES	B B	8702A 8702B

Figure 6-6. Callaway Proposed Interlock-MOV's-8701A&B, 8702A&B (Sheet 1 of 2)

INTERLOCK TABLE - RHR OUTER ISOLATION VALVES		
PLANT	412	
Interlock with \ Valve	8701A	8701B
RCS Hot Leg Pressure Channel	PT-405	PT-405
Recirculation Valve Closed/Limit Switch	8804A/#1	8804B/#2
RWST Suction Valve Closed/Limit Switch	8812A/#1	8812B/#2
Sump Line Valve Closed/ Limit Switch	8811A/#1	8811B/#2

LIMIT SWITCH #1 IS THE NORMAL POSITION SWITCH AND IS USED FOR POSITION SIGNALS BETWEEN VALVES ASSIGNED TO THE SAME TRAIN.

LIMIT SWITCH #2 IS THE STEM MOUNTED POSITION SWITCH AND IS USED FOR SIGNALS BETWEEN VALVES ASSIGNED TO OPPOSITE TRAINS.

INTERLOCK TABLE - RHR INNER ISOLATION VALVES		
PLANT	412	
Interlock with \ Valve	8702A	8702B
RCS Hot Leg Pressure Channel	PT-403	PT-403
Recirculation Valve Closed/Limit Switch	8804A/#2	8804B/#1
RWST Suction Valve Closed/Limit Switch	8812A/#2	8812B/#1
Sump Line Valve Closed/ Limit Switch	8811A/#2	8811B/#1

Figure 6-6. Callaway Proposed Interlock-MOV's-8701A&B, 8702A&B (Sheet 2 of 2)

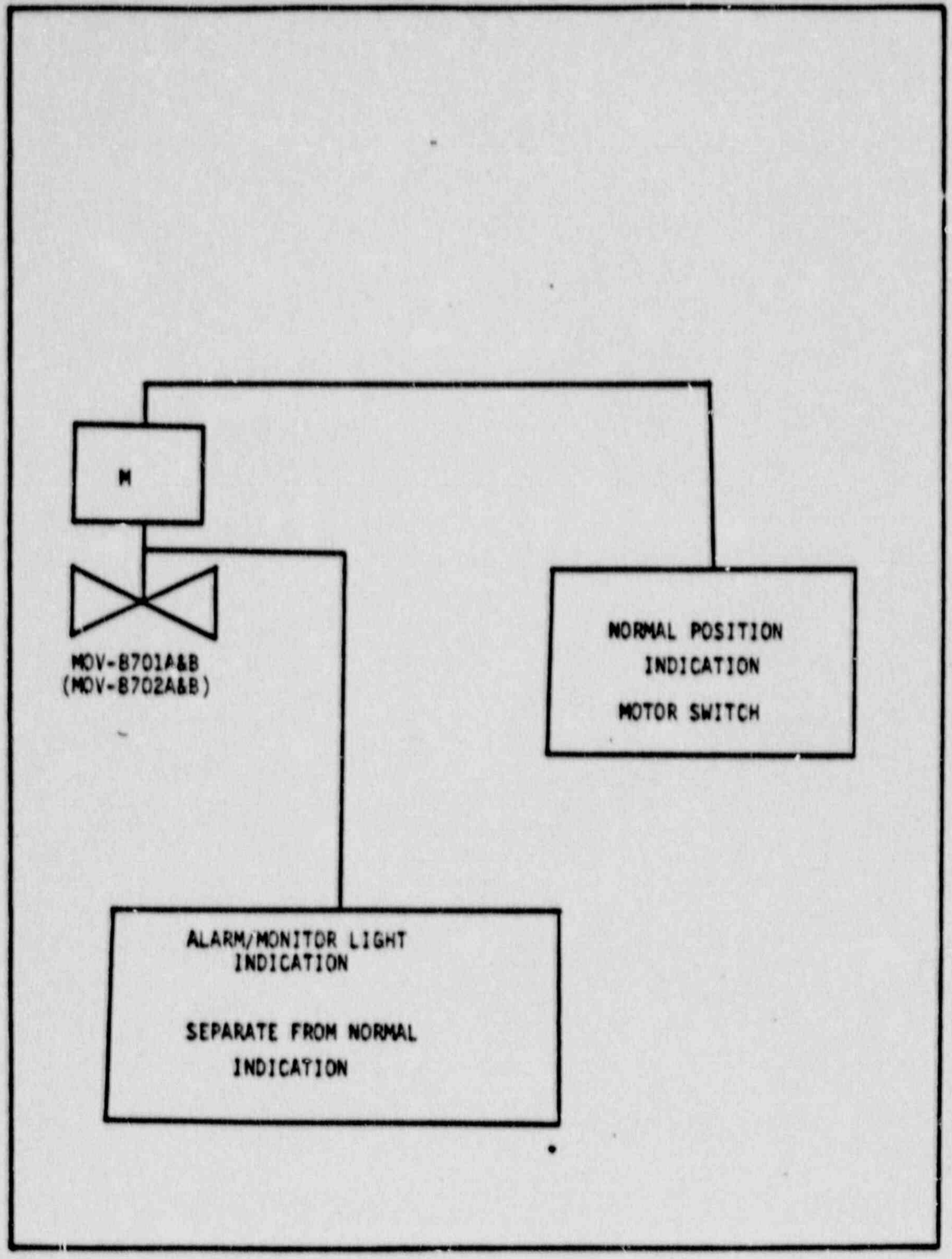
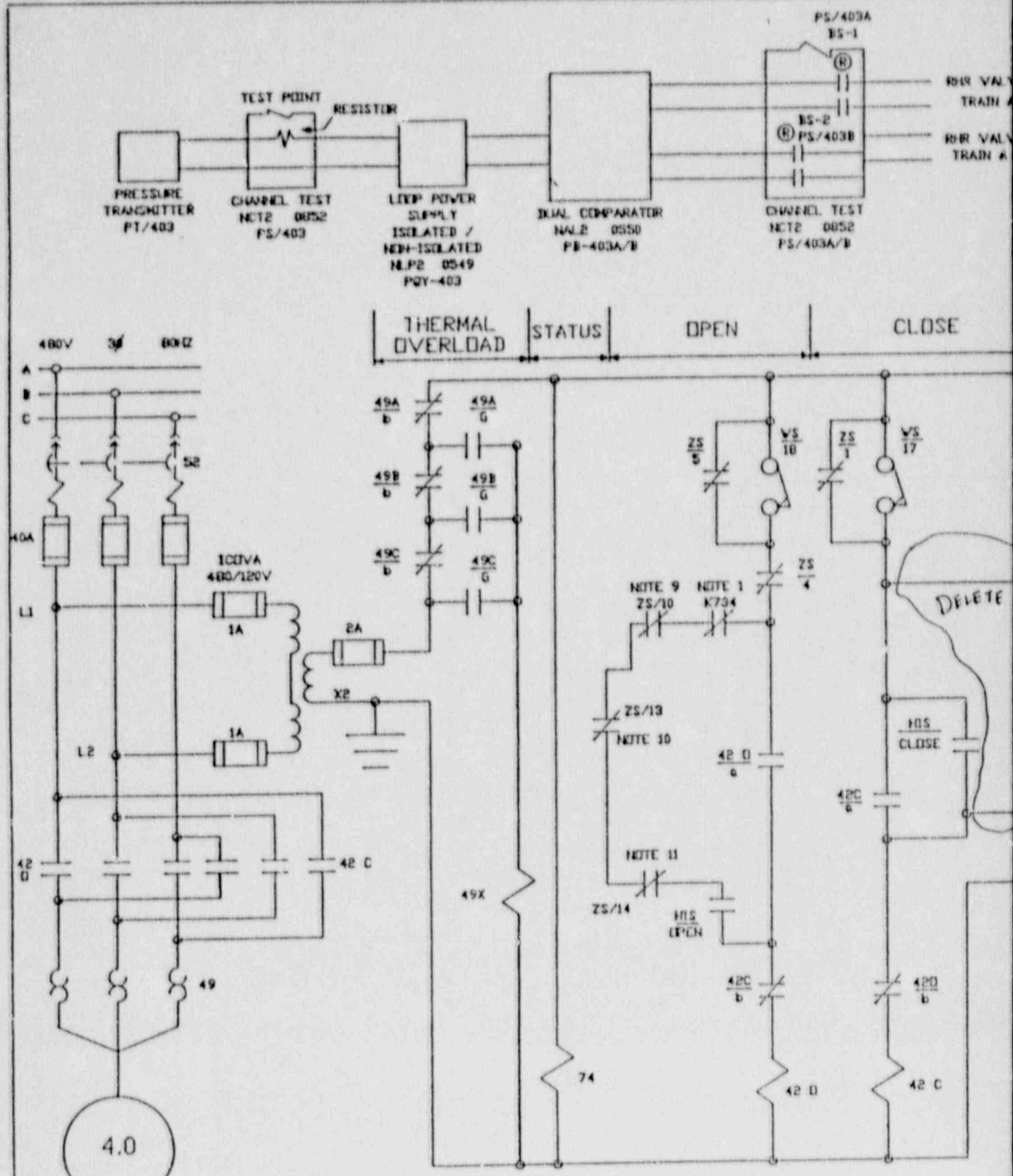


Figure 6-7. Callaway Proposed Indication
MOV's-8701A,B & 8702A,B



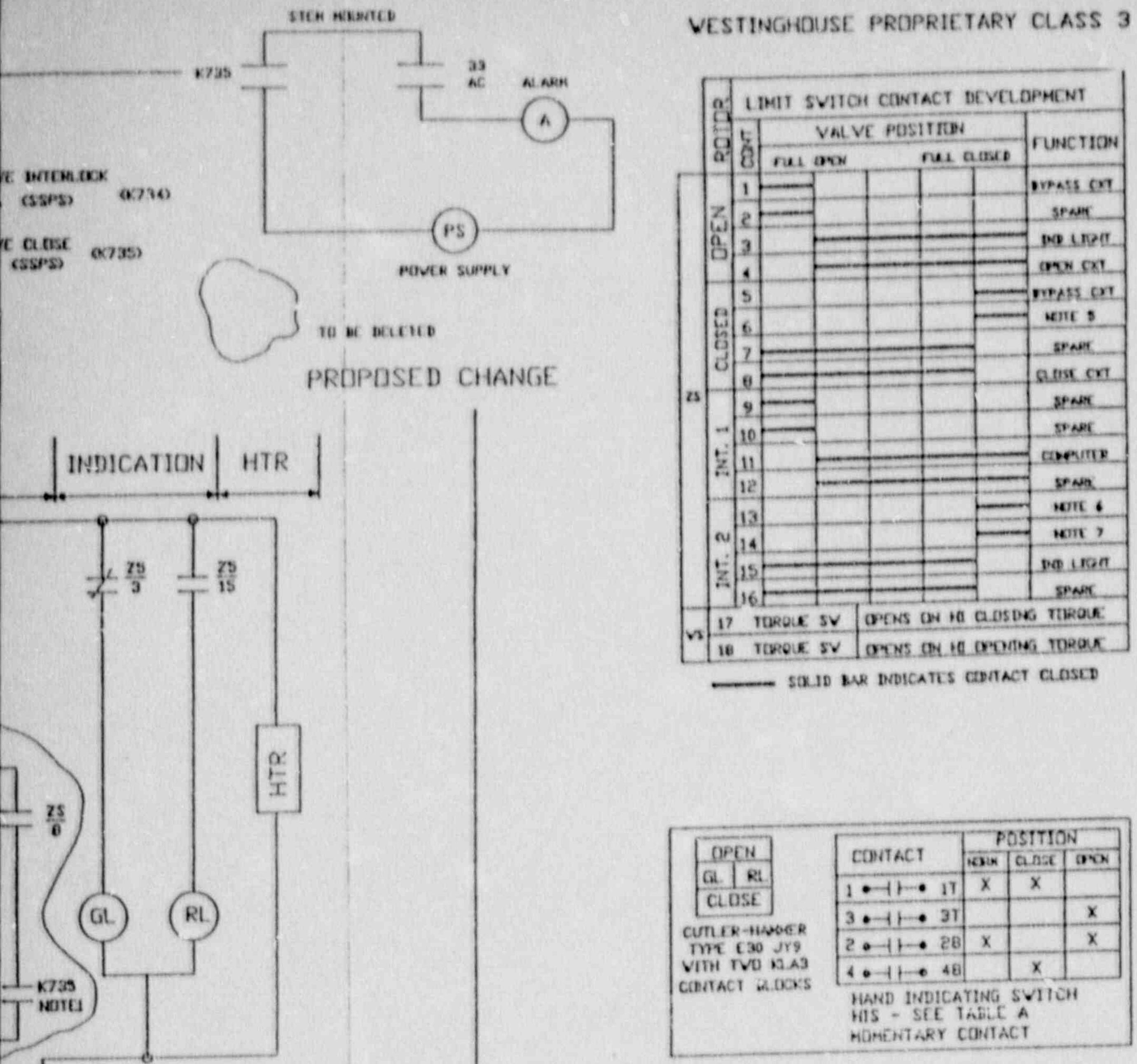
CALLAWAY

RHR SUCTION VALVE 8701A CONTROL CIRCUITRY

RHRCAL1A

1/23/88

WESTINGHOUSE PROPRIETARY CLASS 3



NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
9. CONTACT CLOSED ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
10. CONTACT CLOSED ON SUMP TO NO. 1 RHR PUMP VALVE CLOSED
11. CONTACT CLOSES ON RHR PUMP 1 TO CHARGING PUMP VALVE CLOSED

5. INTERLOCK TO SCH. IEJG04A
6. INTERLOCK TO SCH. IEJG06A
7. RWST LEVEL TEST CKT.

REFERENCES:

BECHTEL	WESTINGHOUSE
E-23EJ05A(Q) REV 0	8809D50 SHEET 32

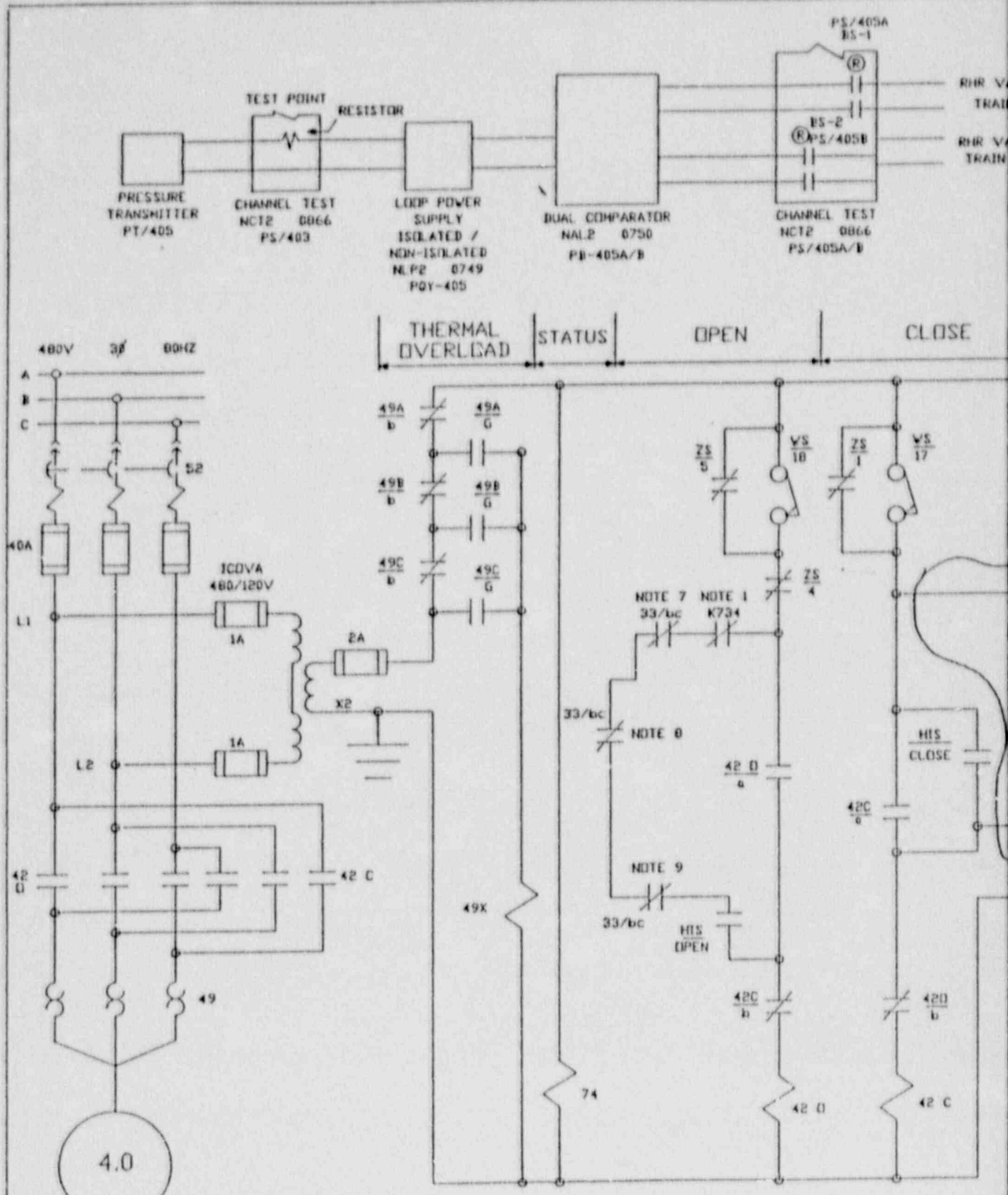
SI APERTURE CARD

Also Available On Aperture Card

Figure 6-8

Callaway Elementary Wiring Diagram Changes for MOV-8701A

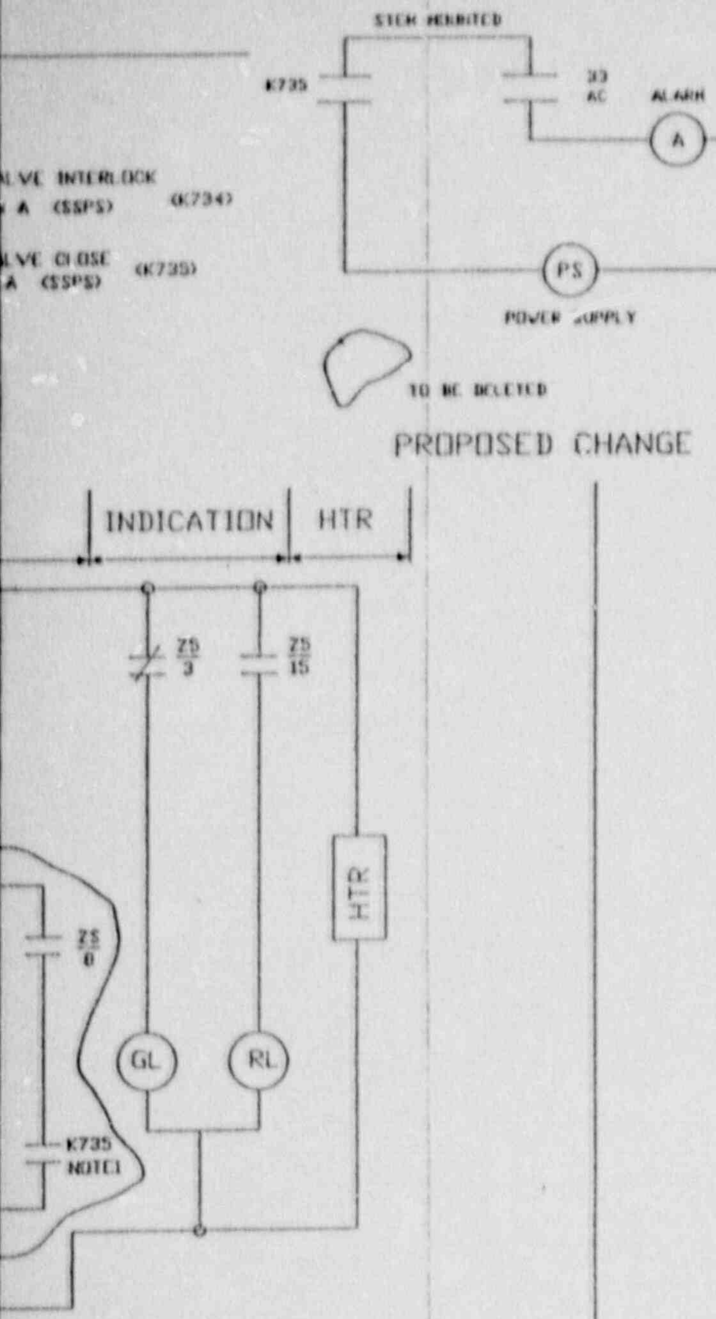
8911150026-26



CALLAWAY
RHR SUCTION VALVE 8701B CONTROL CIRCUITRY

RHRCAL1B

1/23/88



ROTOR	CONT	FULL OPEN				FULL CLOSED	FUNCTION
		LIMIT SWITCH CONTACT DEVELOPMENT					
		VALVE POSITION					
ZS OPEN	1	—					BYPASS CXT
ZS OPEN	2	—					SPARE
ZS OPEN	3		—	—	—	—	IND LIGHT
ZS OPEN	4		—	—	—	—	OPEN CXT
ZS CLOSED	5					—	BYPASS CXT
ZS CLOSED	6					—	SPARE
ZS CLOSED	7	—	—	—	—		SPARE
ZS CLOSED	8	—	—	—	—		CLOSE CXT
ZS INT. 1	9	—					SPARE
ZS INT. 1	10	—					SPARE
ZS INT. 1	11		—	—	—	—	COMPUTER
ZS INT. 1	12		—	—	—	—	SPARE
ZS INT. 2	13					—	SPARE
ZS INT. 2	14					—	SPARE
ZS INT. 2	15	—	—	—	—		ANN CXT
ZS INT. 2	16	—	—	—	—		SPARE
VS	17	TORQUE SW	OPENS ON HI CLOSING TORQUE				
VS	18	TORQUE SW	OPENS ON HI OPENING TORQUE				

▬▬ SOLID BAR INDICATES CONTACT CLOSED

OPEN
GL | RL
CLOSE

CUTLER-HAMMER TYPE E30 JY9 WITH TWO KLA3 CONTACT BLOCKS

CONTACT	POSITION: NORM	POSITION: CLOSE	POSITION: OPEN
1 o—||—o 1T	X	X	
3 o—||—o 3T			X
2 o—||—o 2B	X		X
4 o—||—o 4B		X	

HAND INDICATING SWITCH
HIS - SEE TABLE A
MOMENTARY CONTACT

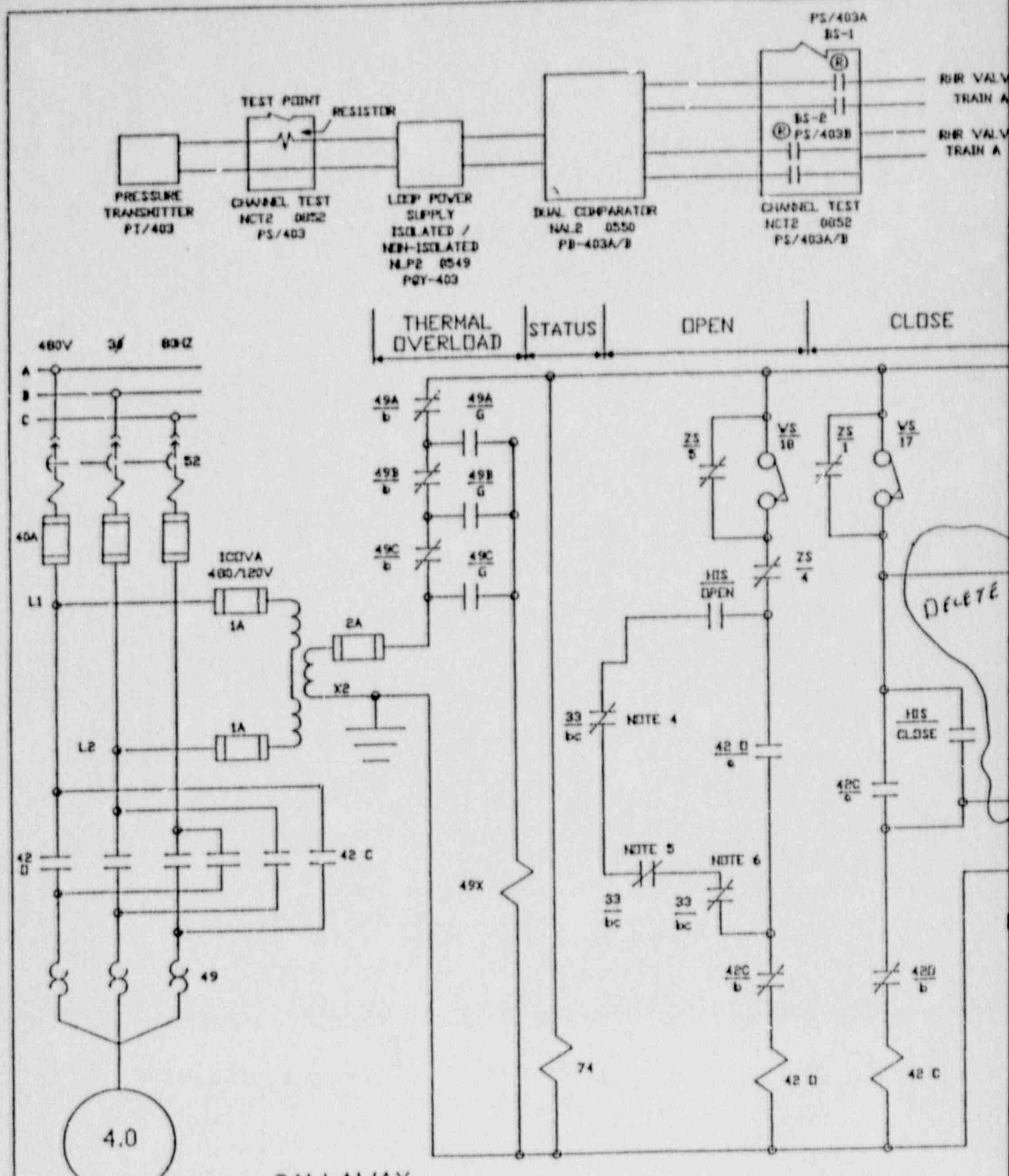
NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
7. CONTACT CLOSES ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
8. CONTACT CLOSES ON SUMP TO NO. 2 RHR PUMP VALVE CLOSED
9. CONTACT CLOSES ON RHR PUMP 2 TO CHARGING PUMP VALVE CLOSED

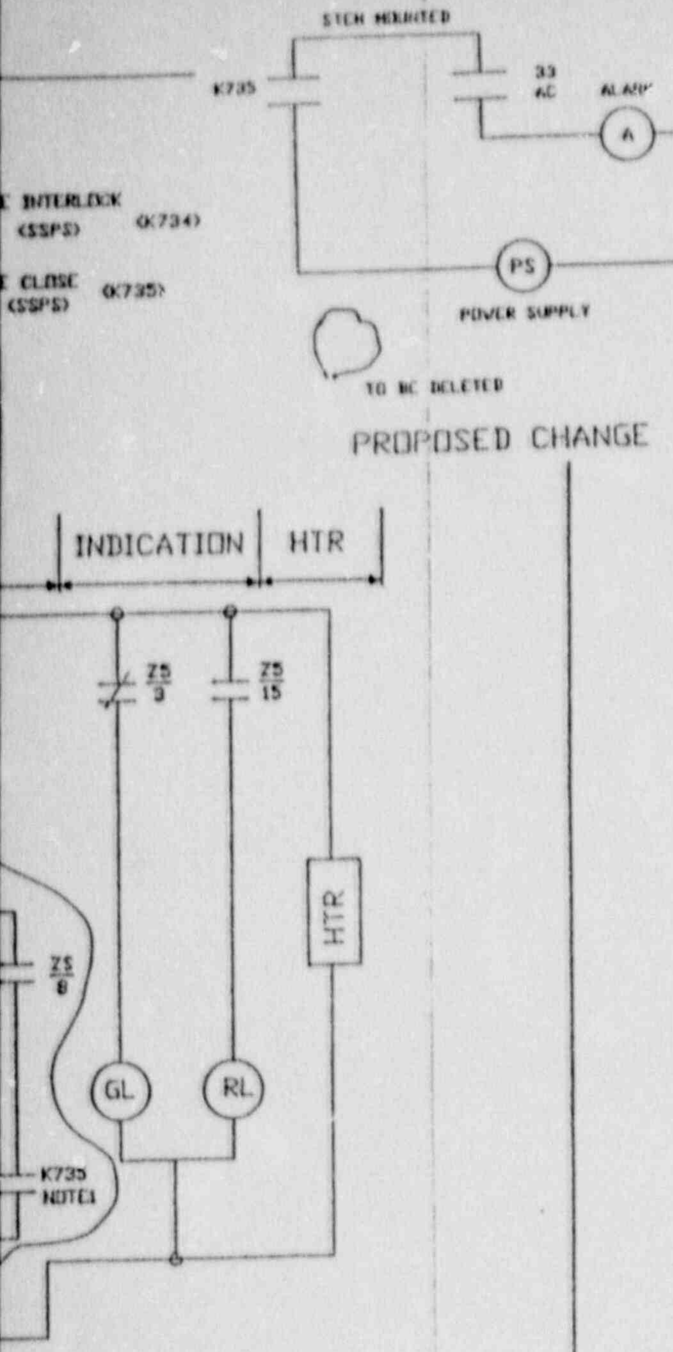
REFERENCES:
BECHTEL E-23EJ05B(Q) REV 1
WESTINGHOUSE 8809D51 SHEET 45

Figure 6-9

Callaway Elementary Wiring Diagram Changes for MOV-8701B



CALLAWAY
RHR SUCTION VALVE 8702A CONTROL CIRCUITRY



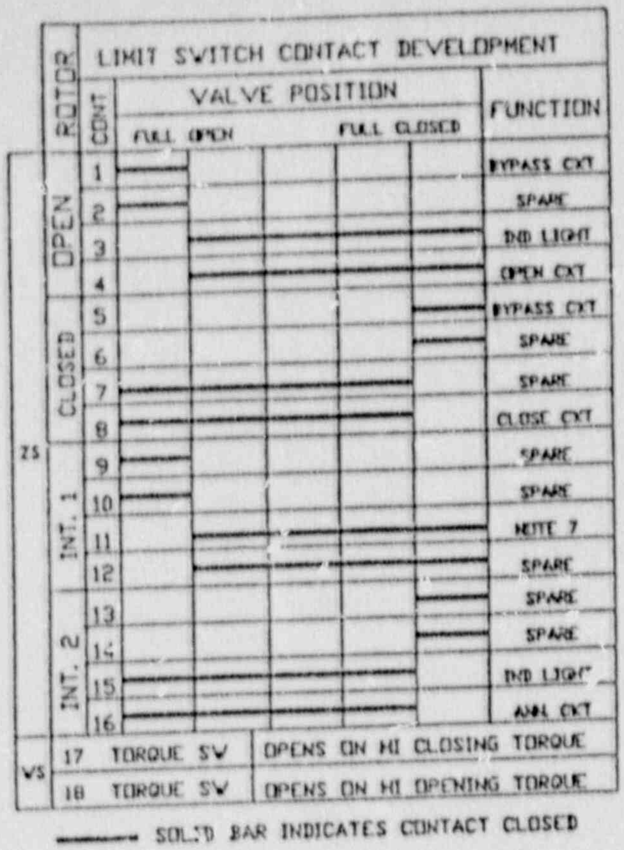
NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
4. CONTACT CLOSES ON SUMP TO NO. 1 THT PUMP VALVE CLOSED
5. CONTACT CLOSES ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
6. CONTACT CLOSES ON RHR PUMP 1 CHARGING PUMP VALVE CLOSED

REFERENCES:

BECHTEL 3-23BB12A(Q) REV 2

WESTINGHOUSE 8809D50 SHEET 32



SOLID BAR INDICATES CONTACT CLOSED

CUTLER-HAMMER TYPE E30 JY9 WITH TWO KLA3 CONTACT BLOCKS

CONTACT	POSITION		
	NORM	CLOSE	OPEN
1 o–||–o 1T	X	X	
3 o–||–o 3T			X
2 o–||–o 2B	X		X
4 o–||–o 4B		X	

HAND INDICATING SWITCH
HIS - SEE TABLE A
MOMENTARY CONTACT

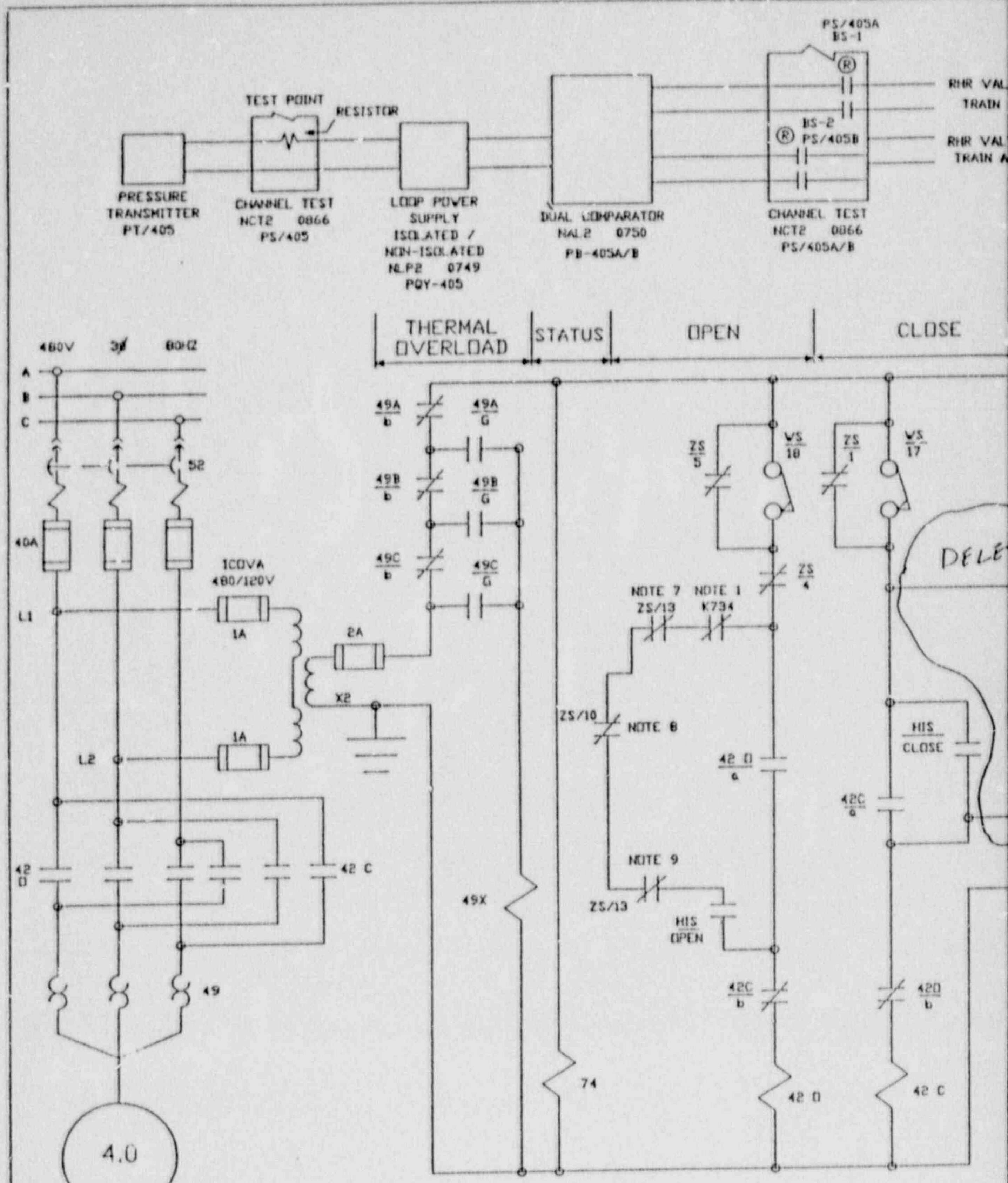
SI APERTURE CARD

Also Available On Aperture Card

Figure 6-10

Calloway Elementary Wiring Diagram Changes for MOV-8702A

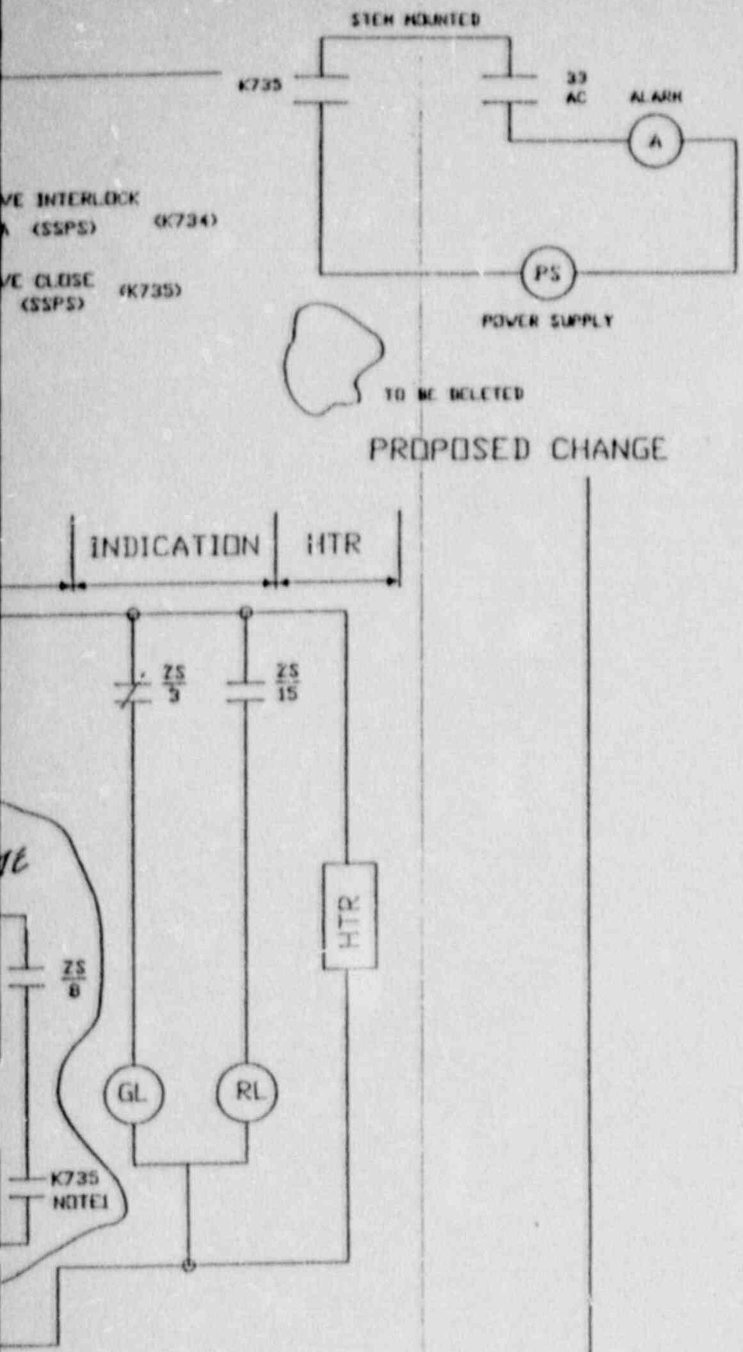
8911150026 -28

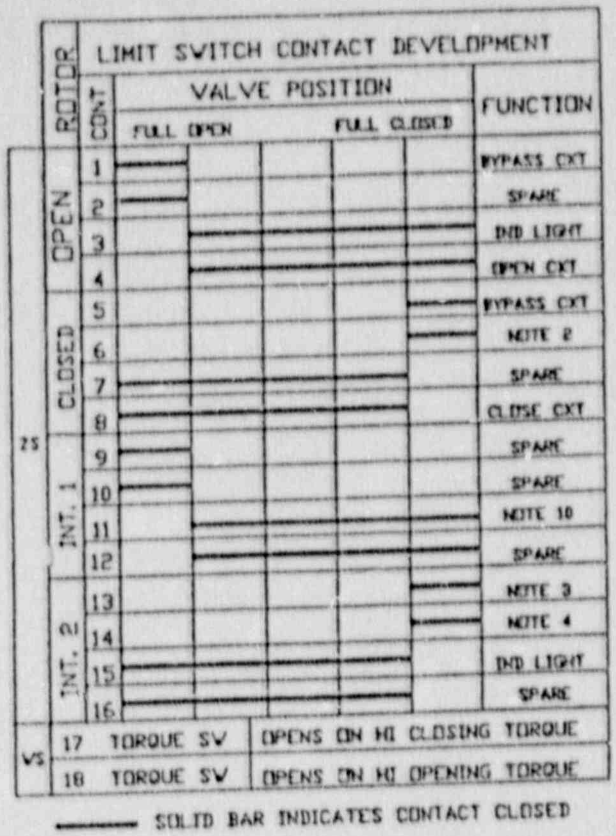


CALLAWAY
RHR SUCTION VALVE 8702B CONTROL CIRCUITRY

RHRCAL2B

1/23/38





CUTLER-HAMMER
TYPE E30 JY9
WITH TWO KLA3
CONTACT BLOCKS

CONTACT	POSITION		
	NORM	CLOSE	OPEN
1 o-||-o 1T	X	X	
3 o-||-o 3T			X
2 o-||-o 2B	X		X
4 o-||-o 4B		X	

HAND INDICATING SWITCH
HIS - SEE TABLE A
MOMENTARY CONTACT

NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
7. CONTACT CLOSES ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
8. CONTACT CLOSES ON SUMP TO NO. 2 RHR PUMP VALVE CLOSED
9. CONTACT CLOSES ON RHR PUMP 2 TO CHARGING PUMP VALVE CLOSED

REFERENCES:

BECHTEL
E-23BB12B(Q)
REV 0

WESTINGHOUSE
8809D51 SHEET 45

Figure 6-11

Callaway Elementary Wiring Diagram Changes for MOV-8702B

8911150026-29

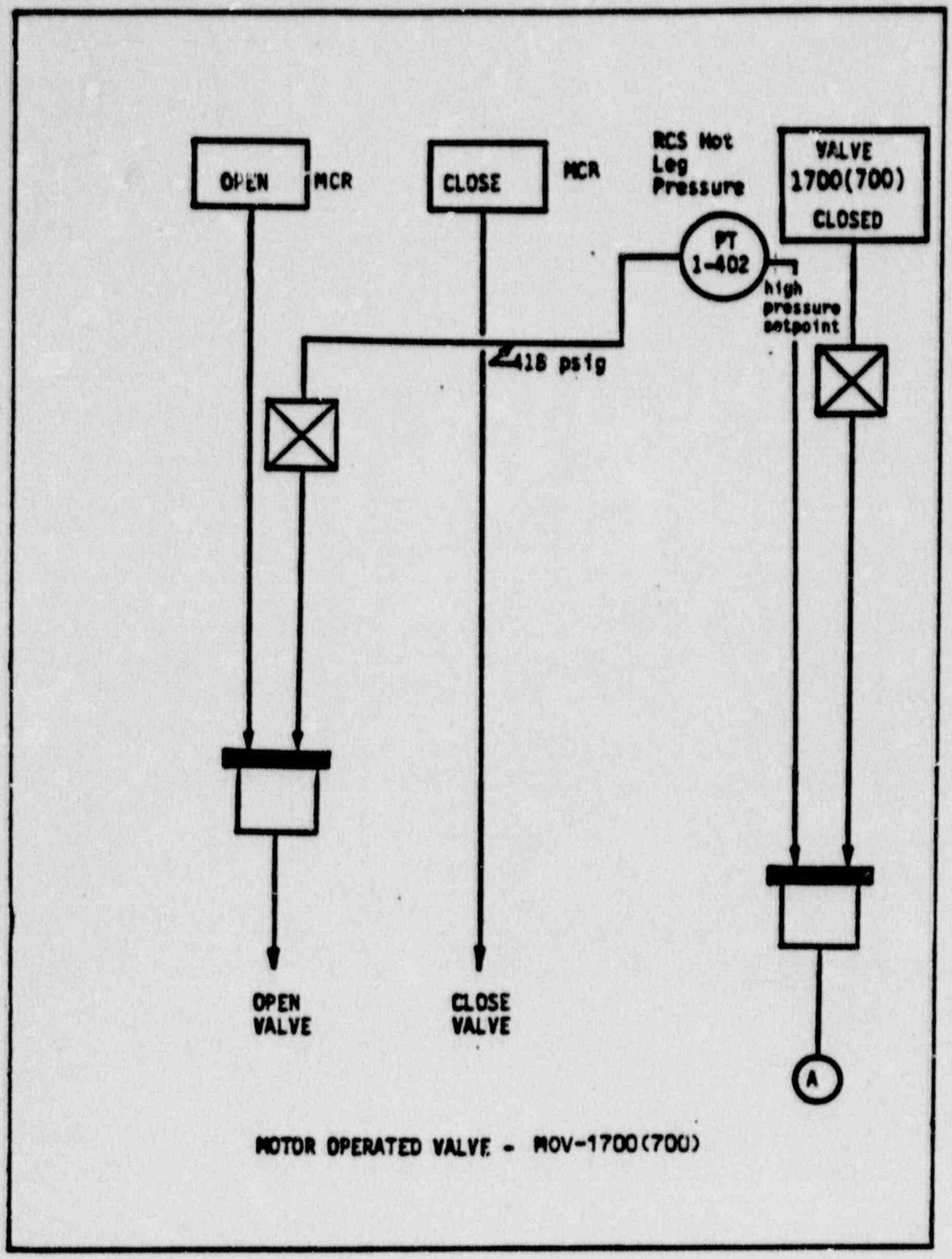


Figure 6-12. North Anna Proposed Interlo MOV-1700(700)

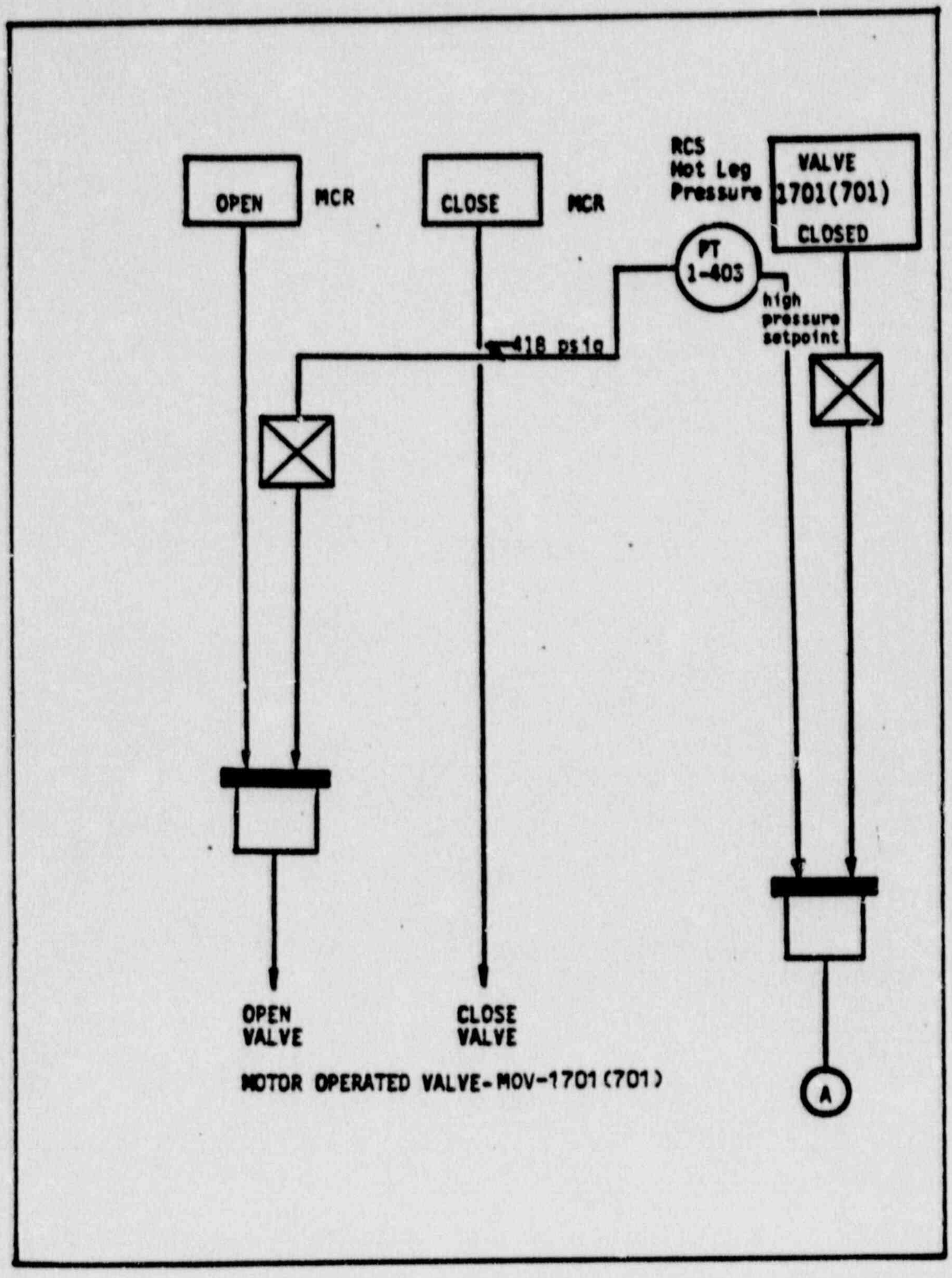
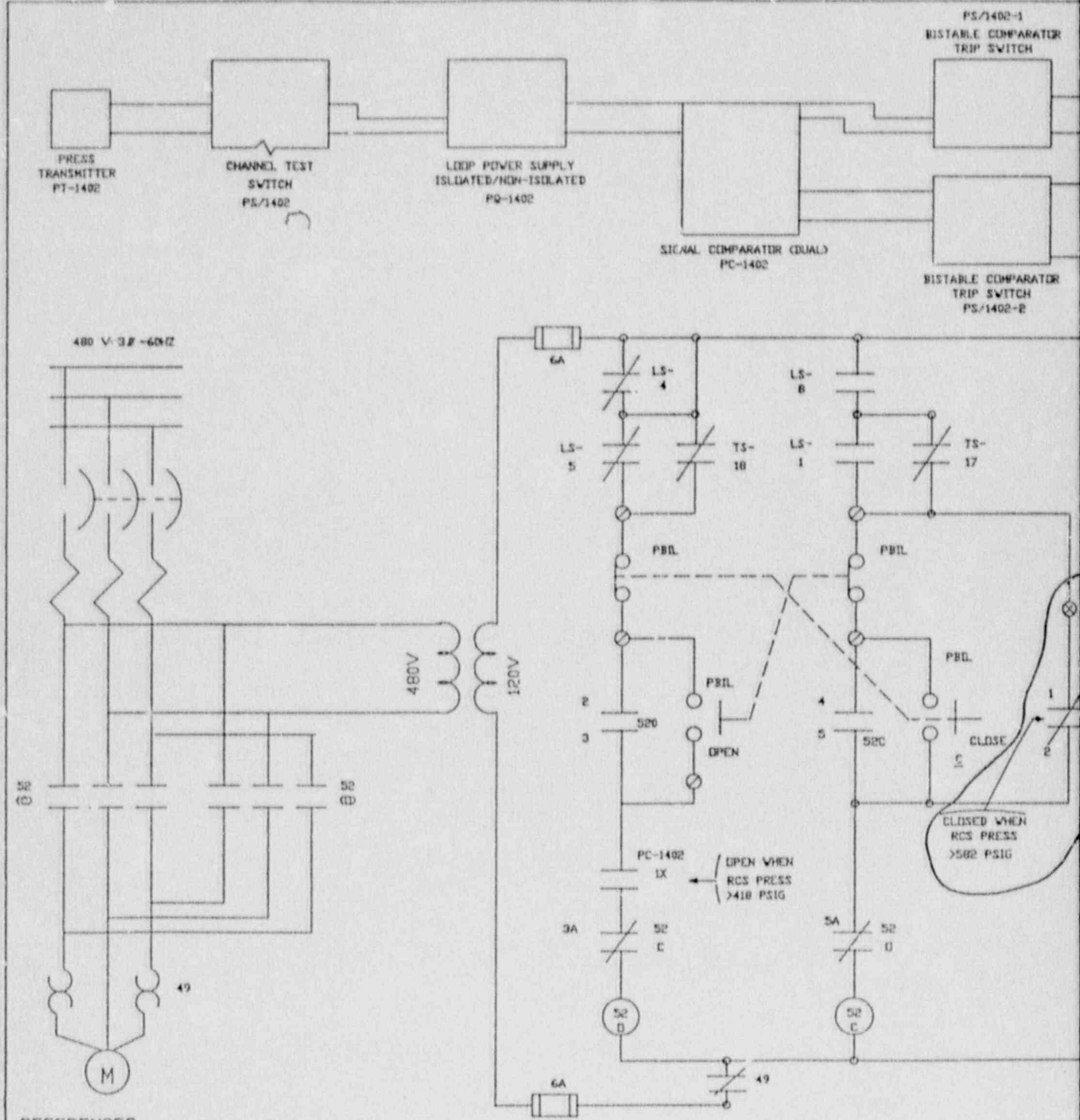


Figure 6-13. North Anna Proposed Interlock MOV-1701(701)

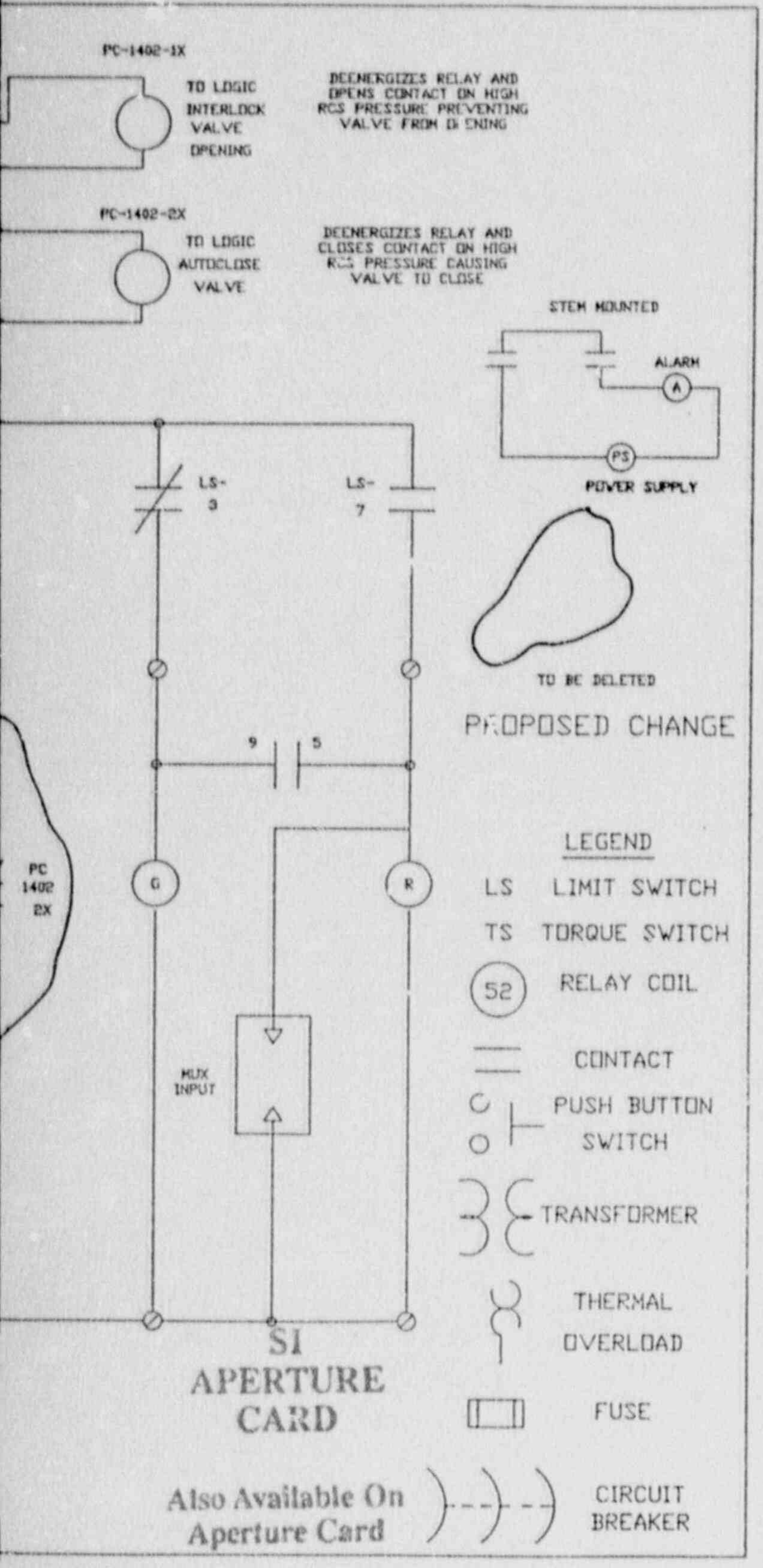


REFERENCES
S&W P-1403 REV 11
W 501B248 SHEET 160 REV 5
W 6007D10
S&W 11715-ESK-6DT SHEET 42 REV 12
S&W 11715-ESK-3H

NORTH ANNA
CONTROL WIRING DIAGRAM
MOV-1700

CWD_NA

2/11/88 PORI388 10/16/89-ADA



WESTINGHOUSE PROPRIETARY CLASS 3

VALVE SHOWN IN FULLY OPEN POSITION

ROTOR	CONT	VALVE POSITION					FUNCTION
		FULL OPEN		A	B	FULL CLOSED	
1	1	——	----	----	----	----	TO 'V BYPASS
	2	——	----	----	----	----	SPARE
	3	----	——	——	——	——	GREEN LIGHT
	4	----	——	——	——	——	OPEN LIMIT
2	5	----	----	----	----	——	TO SV BYPASS
	6	----	----	----	----	——	SPARE
	7	——	——	——	——	----	RED LIGHT
	8	——	——	——	——	----	CLOSE LIMIT
3	9	——	——	----	----	----	SPARE
	10	——	——	----	----	----	SPARE
	11	----	----	——	——	——	SPARE
	12	----	----	——	——	——	SPARE
4	13	----	----	----	——	——	SPARE
	14	----	----	----	——	——	SPARE
	15	——	——	——	----	----	SPARE
	16	——	——	——	----	----	SPARE
17		CLOSING TORQUE SWITCH INTERRUPTS CONTROL CIRCUIT IF MECHANICAL OVERLOAD OCCURS DURING CLOSING CYCLE OR WHEN FULLY CLOSED					
18		OPENS TORQUE SWITCH INTERRUPTS CONTROL CIRCUIT IF MECHANICAL OVERLOAD OCCURS DURING OPENING CYCLE					

NOTES

—— INDICATES CONTACT CLOSED

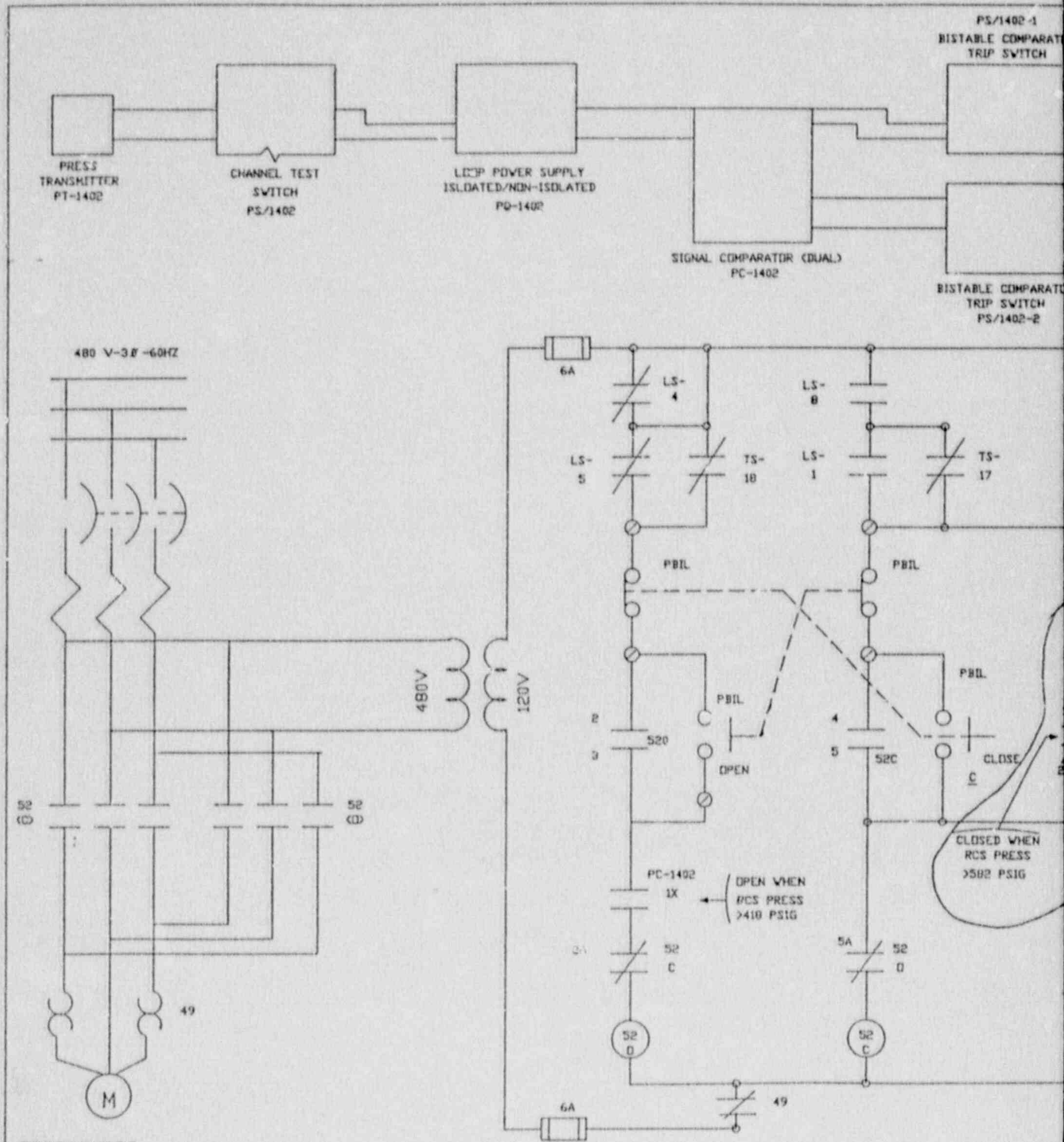
----- INDICATES CONTACT OPEN

ROTORS 3 & 4 ARE ADJUSTABLE AND CAN BE SET AT VALVE POSITION FULLY OPEN FULLY CLOSED OR ANY POSITION INBETWEEN

Figure 6-14

North Anna Elementary Wiring Diagram Changes for MOV-1700 (700)

8911150026-30

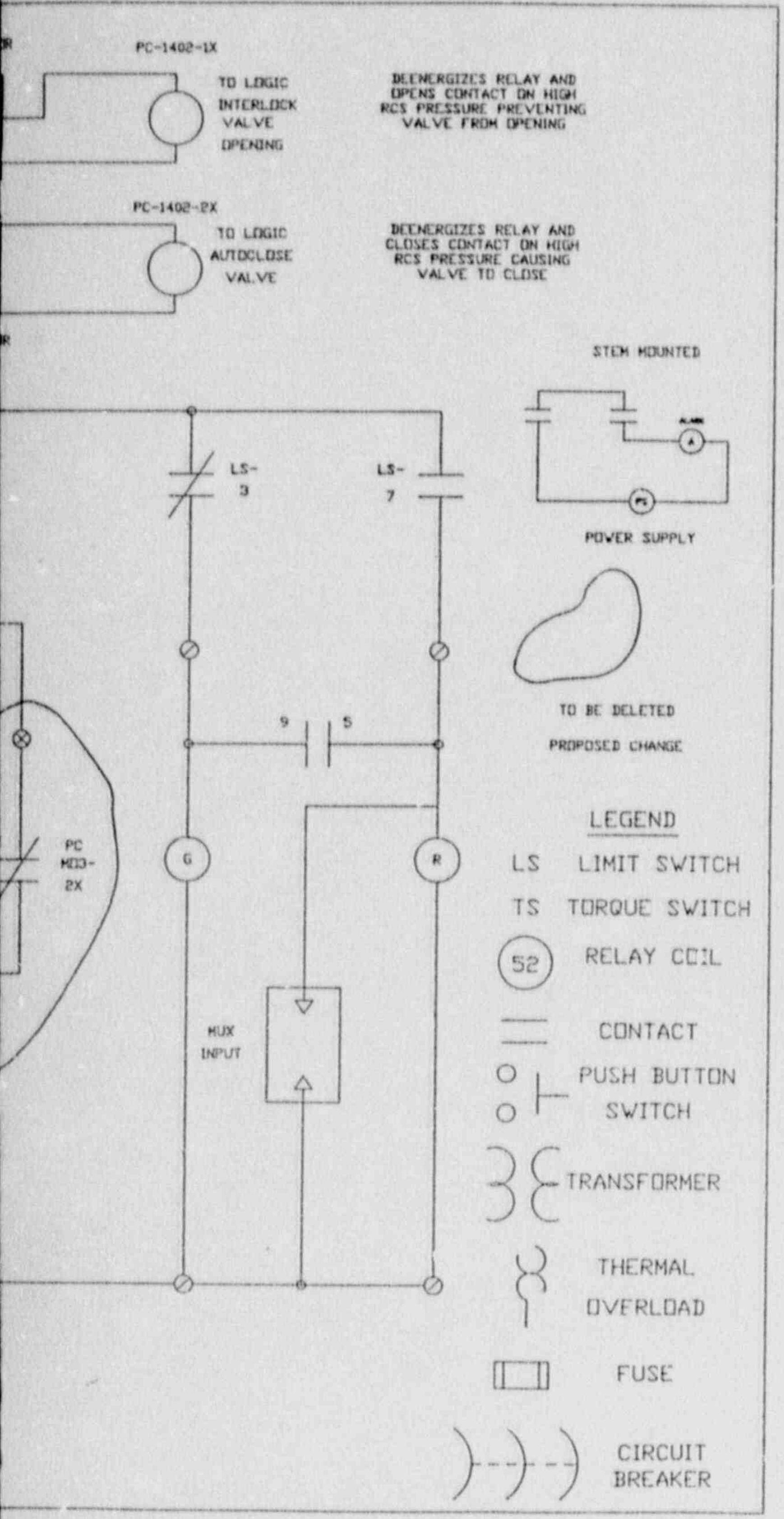


REFERENCES
S&W P-1403 REV 11
W 501B248 SHEET 160 REV 5
W 6007D10
S&W 11715-ESK-6DT SHEET 42 REV 12
S&W 11715-ESK-3H

NORTH ANNA
CONTROL WIRING DIAGRAM
MOV-1701

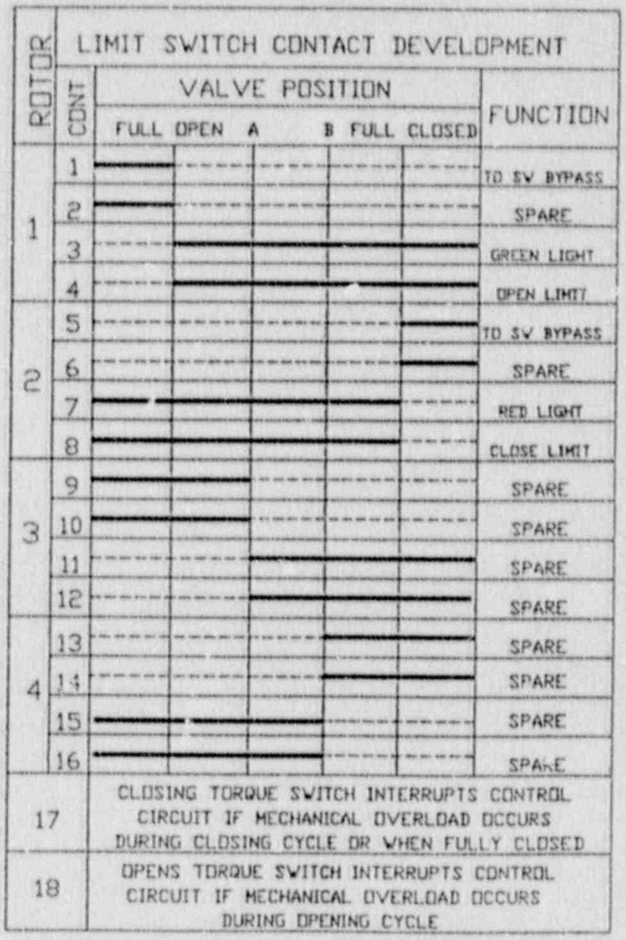
CWD_NA01

2/11/88 PORI389 10/17/89-ADA



WESTINGHOUSE PROPRIETARY CLASS 3

VALVE SHOWN IN FULLY OPEN POSITION



LIMIT SWITCH CONTACT DEVELOPMENT

ROTOR	CONT	VALVE POSITION (FULL OPEN — A — B — FULL CLOSED)	FUNCTION
1	1		TO SV BYPASS
	2		SPARE
	3		GREEN LIGHT
	4		OPEN LIMIT
2	5		TO SV BYPASS
	6		SPARE
	7		RED LIGHT
	8		CLOSE LIMIT
3	9		SPARE
	10		SPARE
	11		SPARE
	12		SPARE
4	13		SPARE
	14		SPARE
	15		SPARE
	16		SPARE
17		CLOSING TORQUE SWITCH INTERRUPTS CONTROL CIRCUIT IF MECHANICAL OVERLOAD OCCURS DURING CLOSING CYCLE OR WHEN FULLY CLOSED	
18		OPENS TORQUE SWITCH INTERRUPTS CONTROL CIRCUIT IF MECHANICAL OVERLOAD OCCURS DURING OPENING CYCLE	

NOTES

——— INDICATES CONTACT CLOSED

------ INDICATES CONTACT OPEN

ROTORS 3 & 4 ARE ADJUSTABLE AND CAN BE SET AT VALVE POSITION FULLY OPEN FULLY CLOSED OR ANY POSITION INBETWEEN

SI APERTURE CARD

Figure 6-15

Also Available On Aperture Card

North Anna Elementary Wiring Diagram Changes for MOV-1701 (701)

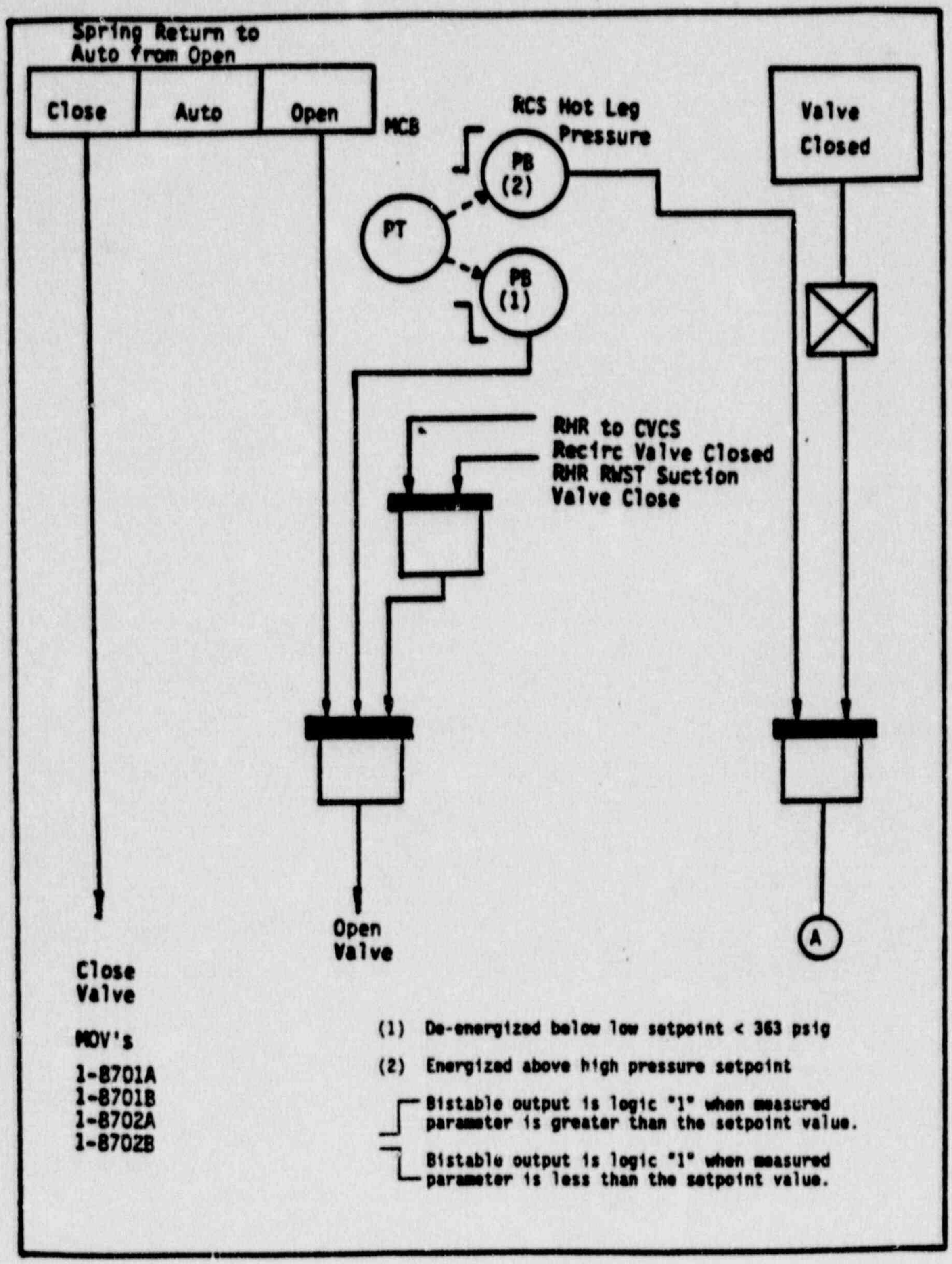


Figure 6-16. Shearon Harris Proposed Interlock-MOV-8701A&B, 8702A&B (Sheet 1 of 2)

Valve / Interlock with	1-8701 A (Train A)	1-8702 B (Train A)	1-8702 A (Train B)	1-8702 B (Train B)
PT RCS Hot Leg Pressure	402 (Train A)	402 (Train A)	403 (Train B)	403 (Train B)
RHR to CVCS Rec. Valve	1-8706 A SW. #1 (Train A)	1-8706 B SW. #2 (Train A)	1-8706 A SW. #2 (Train B)	1-8706 B SW. #1 (Train B)
RHR RWST Suction Valve	1-8809A SW. #1 (Train A)	1-8809B SW. #2 (Train A)	1-8809A SW. #2 (Train B)	1-8809B SW. #1 (Train B)

SW = Switch

NOTE: SW #1 - Torque switch powered by same train as valve.

SW #2 - Stem mounted limit switch powered by train different from valve power.

Figure 6-16. Shearon Harris Proposed Interlock-MOV 8701A&B, 8702A&B (Sheet 2 of 2)

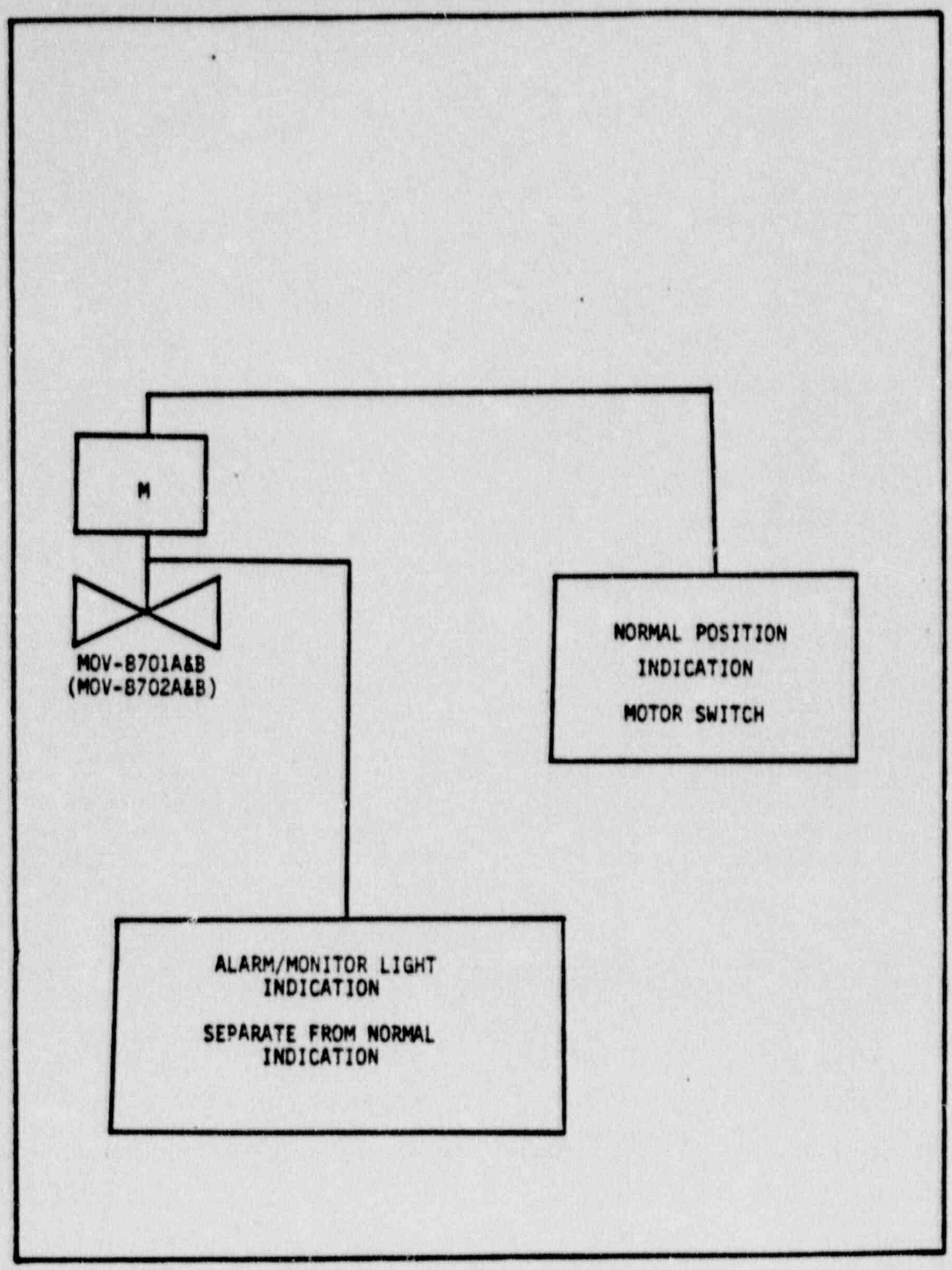


Figure 6-17. Shearon Harris Proposed Position Indication MOV's-8701A,B & 8702A,B

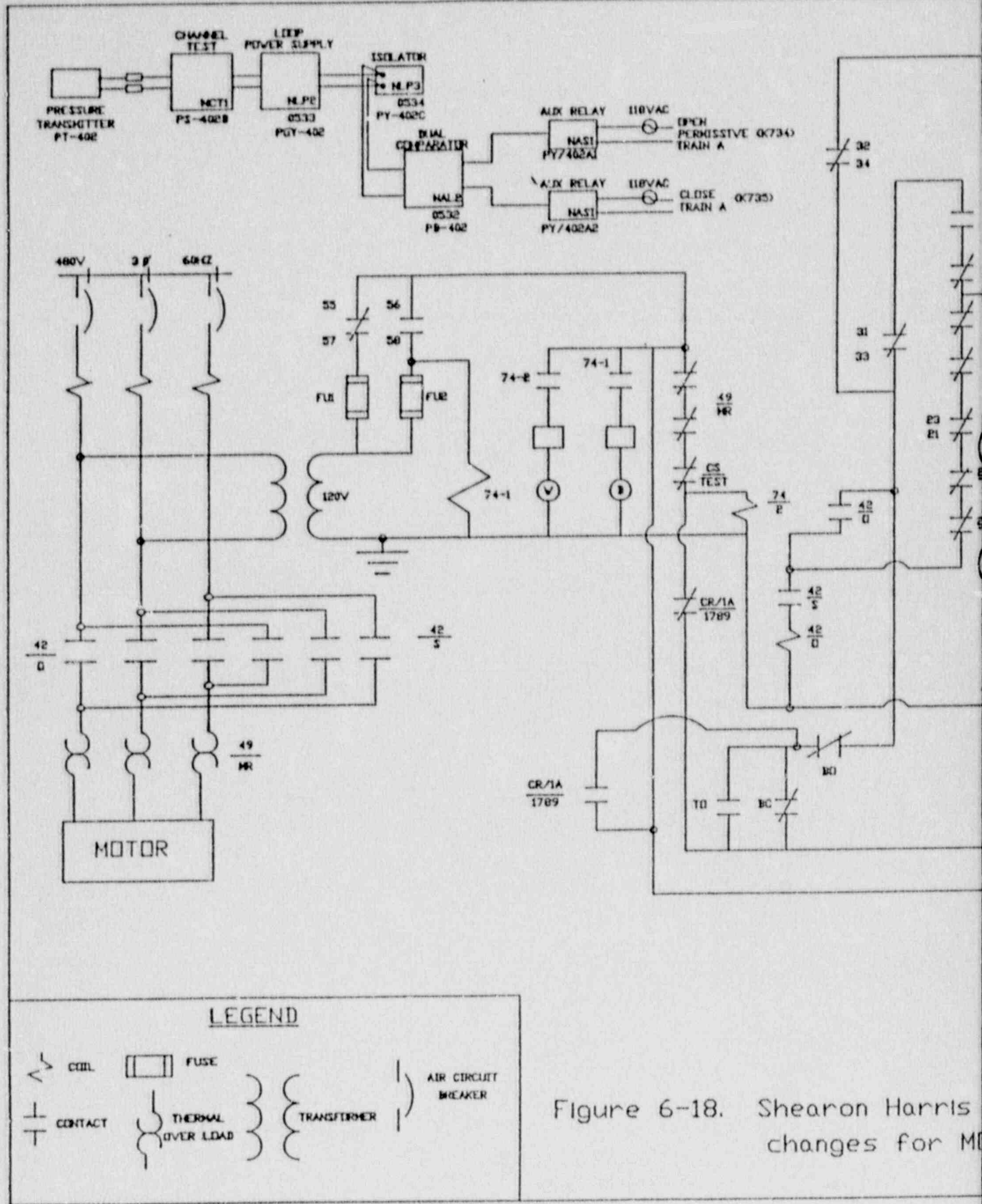
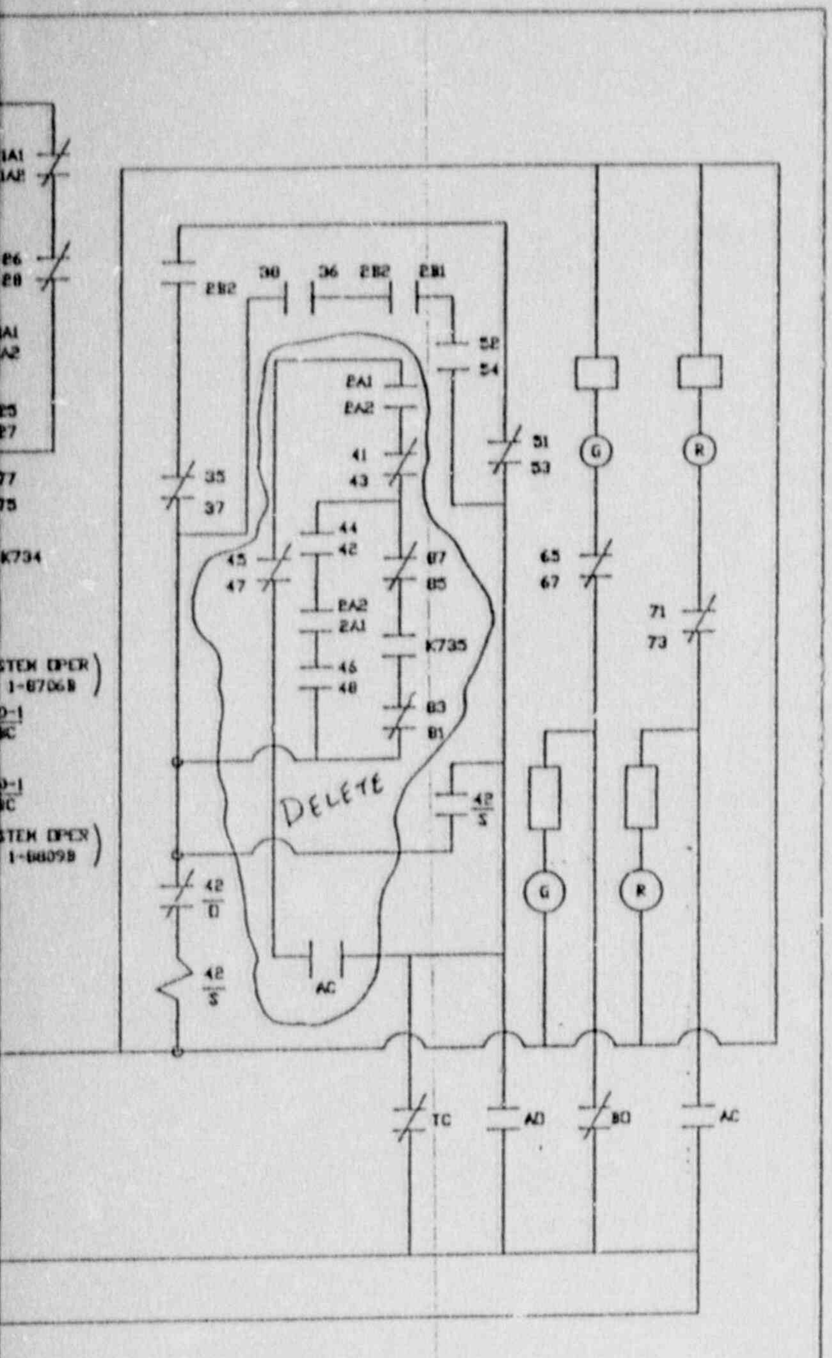


Figure 6-18. Shearon Harris
changes for M

RCS_SH22

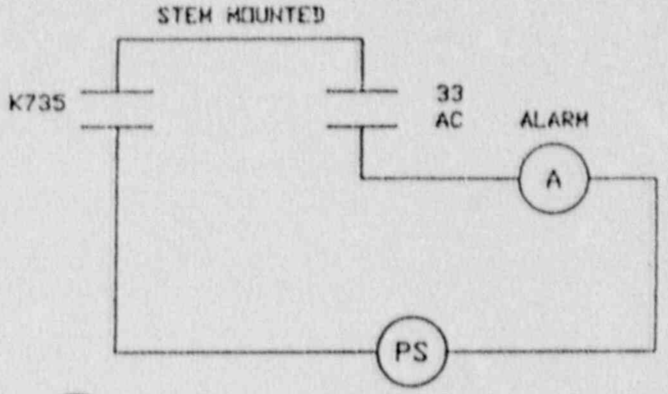
1/19/88

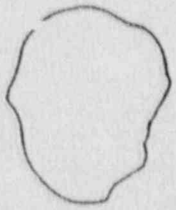


SI APERTURE CARD

Elementary Wiring Diagram
OV-8701A

Also Available On Aperture Card





TO BE DELETED

PROPOSED CHANGE

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % 0 100	CWD SH
bo	4			•
ac		8		•
bo	3			•
ac		7		
ao	2			
bc		6		
ao	1			•
bc		5		•
ac		16		
bo	12			
ac		15		•
bo	11			
bc		14		
ao	10			
bc		13		
ao	9			
tc	17		OPENS ON OVLD ON CLOSE STRK	•
to	18		OPENS ON OLVD ON OPEN STRK	•
—— = CONT CLOSED • = THIS SHEET				

REF.
CAR 2166 B-401 SH 325
V 2034578 SH 11

8911150026-32

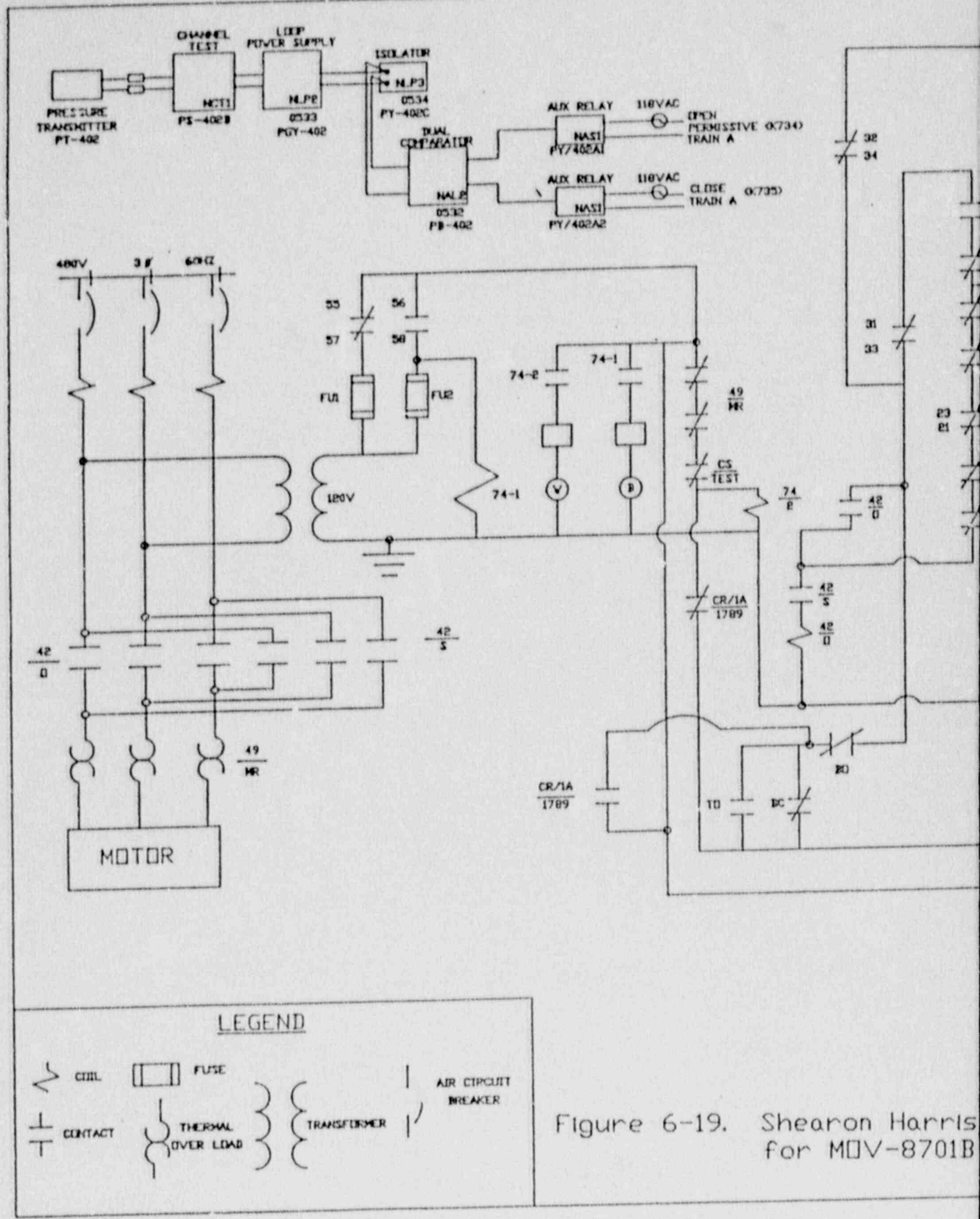
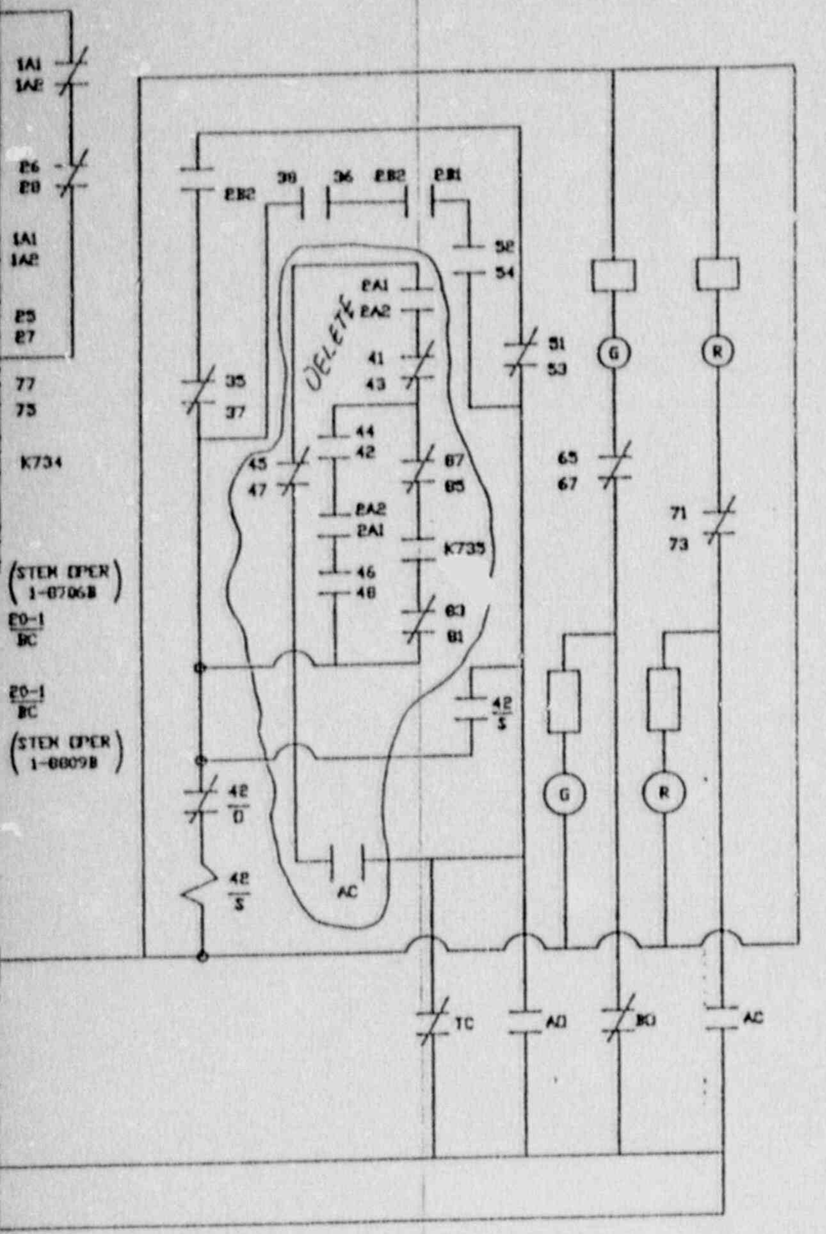


Figure 6-19. Shearon Harris
for MOV-8701B

RCS_SH20

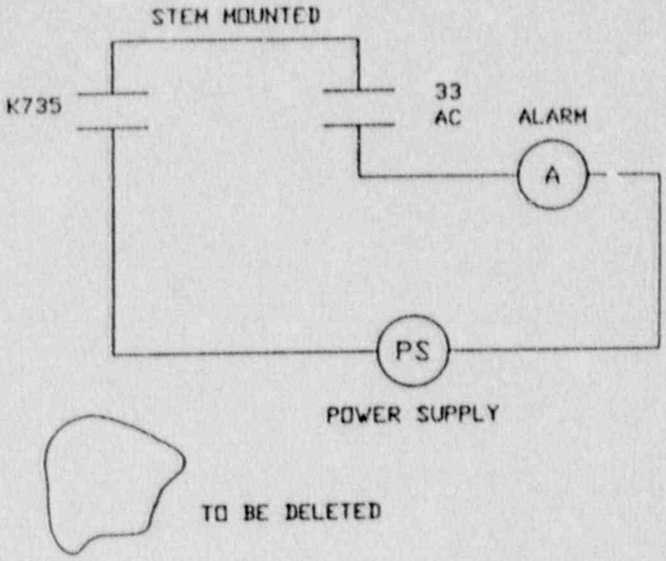
1/19/88



SI
APERTURE
CARD

Also Available On
Aperture Card

Elementary Wiring Diagram Changes



PROPOSED CHANGE

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0 – 100)	CVD SH
bo	4			▪
ac		8		▪
bo	3			▪
ac		7		
ao	2			
bc		6		
ao	1			▪
bc		5		▪
ac		16		
bo	12			
ac		15		▪
bo	11			
bc		14		
ao	10			
bc		13		
ao	9			
tc	17		OPENS ON OVLD ON CLOSE STRK	▪
to	18		OPENS ON OLVD ON OPEN STRK	▪
—— = CONT CLOSED ▪ = THIS SHEET				

REF.
CAR 2166 B-401 SH 326
W 2034578 SH 11

8911150026-33

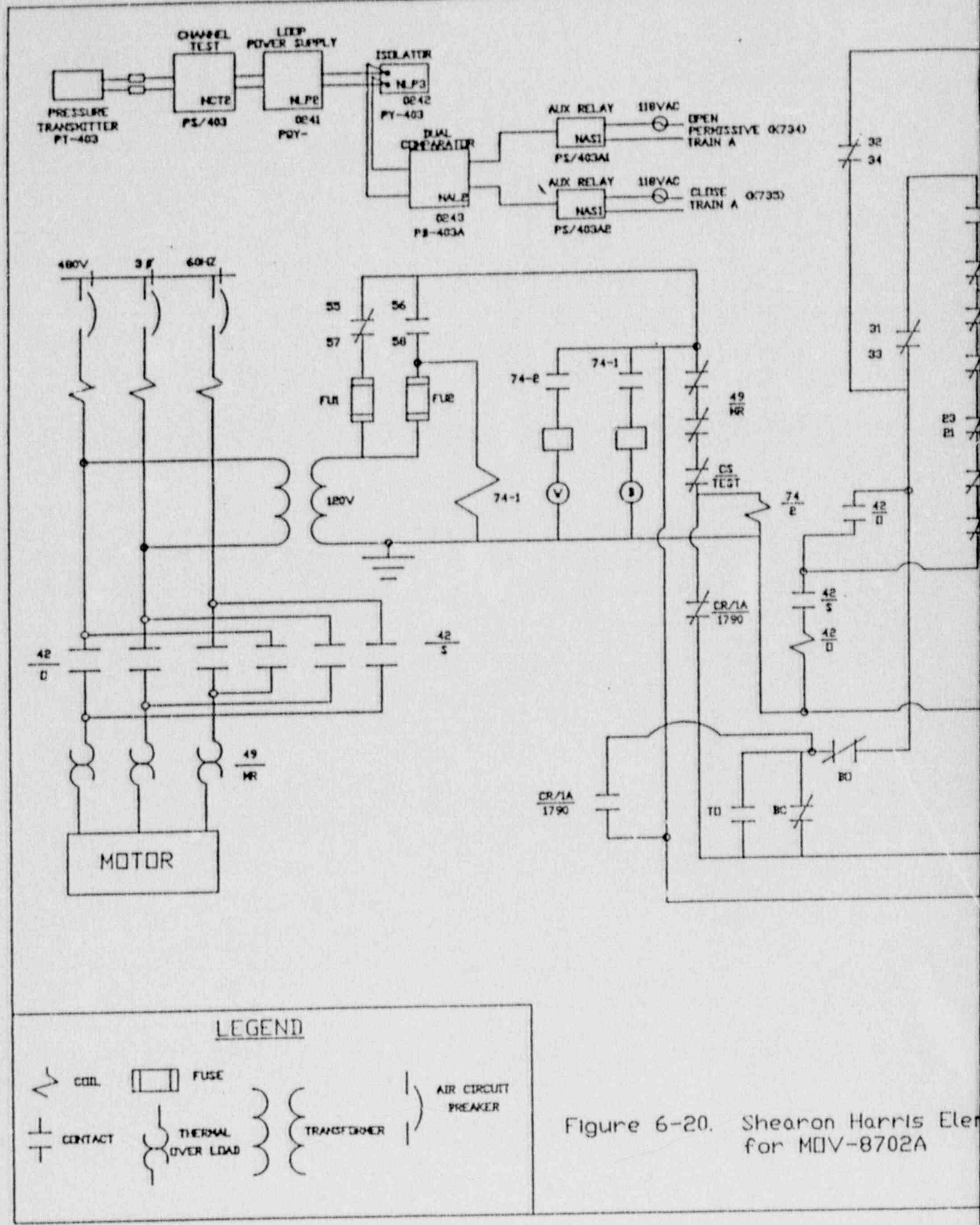
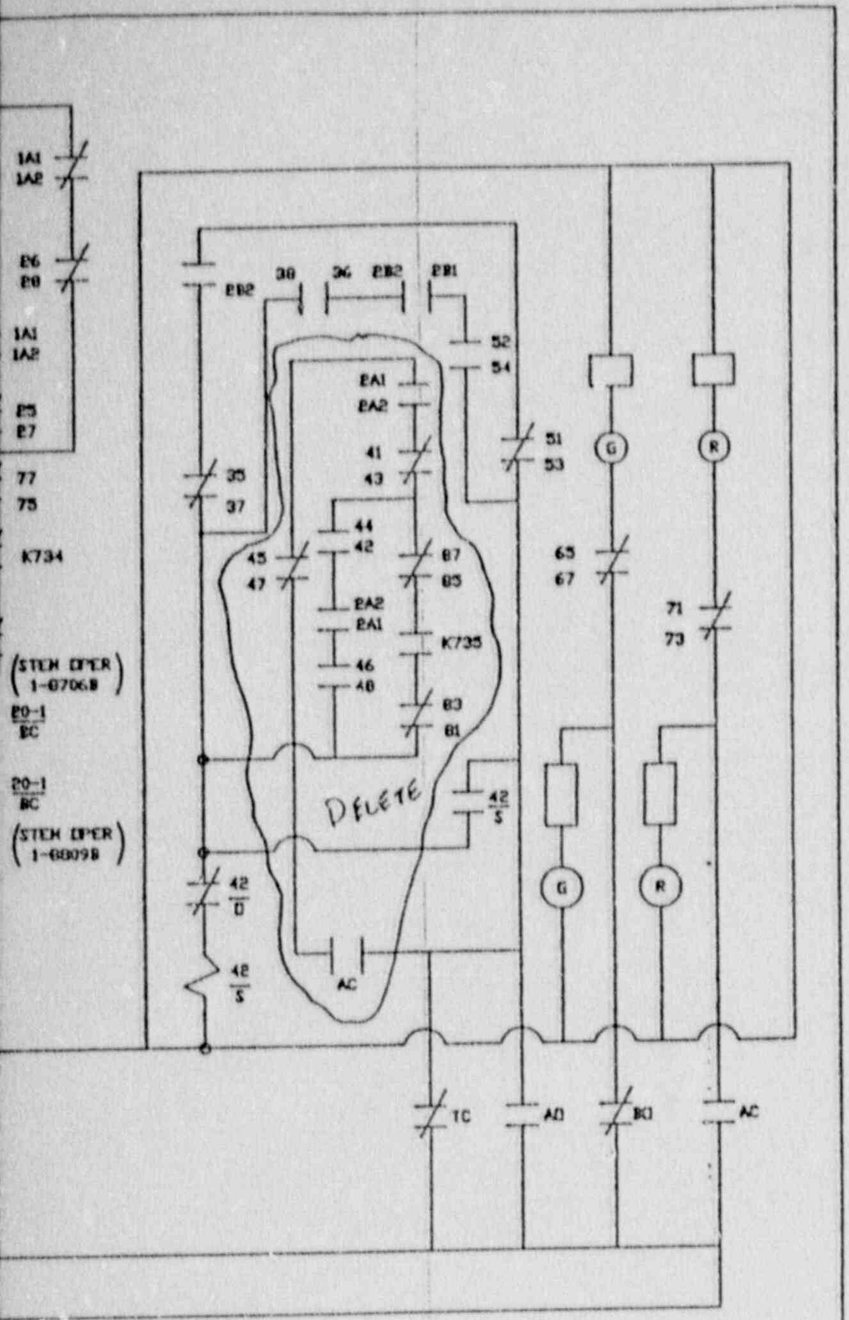


Figure 6-20. Shearon Harris Ele
for MOV-8702A

RCS_SH23

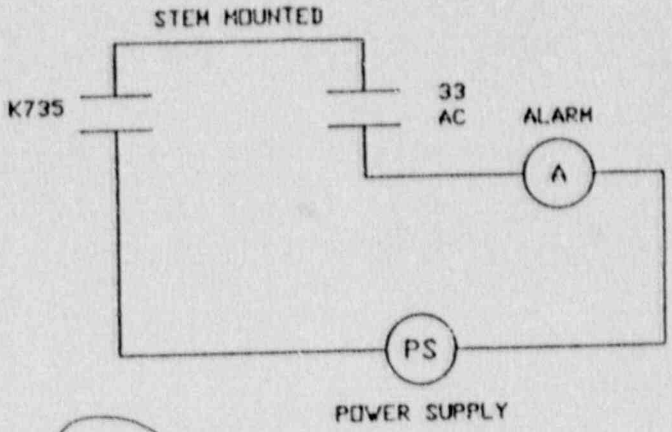
1/19/88

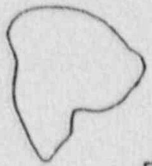


SI
APERTURE
CARD

Also Available On
Aperture Card

mentary Wiring Diagram Changes





TO BE DELETED

PROPOSED CHANGE

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0 – 100)	CVD SW
bo	4			•
ac		8		•
bo	3			•
ac		7		
ao	2			
bc		6		
ao	1			•
bc		[illegible]		•
ac		16		
bo	12			
ac		15		•
bo	11			
bc		14		
ao	10			
bc		13		
ao	9			
tc	17		OPENS ON OVLD ON CLOSE STRK	•
to	18		OPENS ON OLVD ON OPEN STRK	•

—— = CONT CLOSED ■ = THIS SHEET

REF.
CAR 2166 B-401 SH 327
V 2445044 SH 8

8911150026-34

7.0 PROBABILISTIC ANALYSIS

7.1 Introduction

This section describes the probabilistic analysis performed to justify removal of the RHRS suction isolation valve autoclosure interlock for the four reference plants. Three different areas were examined in this analysis: 1) the likelihood of an interfacing system LOCA; 2) RHRS availability and 3) low temperature overpressurization concerns. Each of the three areas was analyzed utilizing the current control circuitry configuration and then with the proposed modification to the control circuitry. The net change in each area was determined and the overall net detriments and benefits were weighed to determine the acceptability of removal of the autoclosure interlock from a probabilistic standpoint.

7.2 Data

The data used in this analysis was derived primarily from two documents - NUREG/CR-2815 Rev. 1, "Probabilistic Safety Analysis Procedures Guide" (Reference 21) and IEEE-500, "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations," (Reference 22). The component failure data is presented in Table 7-1.

Testing information was obtained from the Technical Specifications for each reference plant while maintenance information was extracted from the "Individual Plant Evaluation Methodology for Pressurized Water Reactors," (Reference 20).

The mean human error probabilities were calculated utilizing the medians and error factors from NUREG/CR-1278 (Reference 19) and assuming a lognormal distribution. Each human error calculation is explained in the individual analyses and is shown in the Appendices.

7.3 Interfacing Systems LOCA Analysis

An interfacing systems LOCA, referred to as an Event V in WASH-1400, is a breach of the high pressure Reactor Coolant System (RCS) boundary at an interface with the low pressure piping system. This breach has the potential to cause a LOCA in which the containment and containment safeguards radionuclide protective barriers are bypassed.

An RHR LOCA is classified as a non-mitigable LOCA outside containment. It is assumed to occur if the valves in the RHRS suction line fail open when the RCS is at normal operating pressure (2250 psia). Since the RHR System is designed for a much lower pressure (typically 600 psig or less), the result of both suction/isolation valves failing open is overpressurization of the RHR System. This is assumed to lead to gross failure of the RHR boundary. Since most RHR Systems are located outside of containment, gross failure of the RHRS boundary is assumed to result in an uncontained LOCA.

In this section, the frequency of an interfacing system LOCA is calculated for the RHRS-RCS system interface for two cases: 1) with the present interlock configuration, and 2) with the proposed control circuitry modification. Appendix B provides the detailed calculations for each of the four reference plants.

Typically, RHRS suction paths are the dominant V-sequence source. Usually there are two motor operated valves in series on the RHR suction line from the RCS. Failure of these normally closed valves during power operation (at high pressures) would expose the low pressure piping upstream of the valves to the existing RCS pressure. The suction line configurations for each of the reference plants is shown in Figure 7-1.

In this analysis, several failure combinations are considered which would result in both suction valves being in the "OPEN" position. These failure modes are defined as: 1) rupture of the two series motor-operated valves in the RHR suction line and 2) failure to have closed one suction valve (or spurious opening of the valve) and subsequent rupture of the other valve. The latter failure mode actually includes two combinations - the failure to close the valve closer to the RCS (or spurious opening of the valve) and subsequent rupture of the valve closer to the RHR System and vice versa. Failure to close both RHR suction valves during startup is not considered a credible failure mode because the condition would become apparent and corrective action would be taken. (The RHRS relief valve would lift as the RCS pressure increased, an alarm would sound, and the RCS pressure would increase more slowly than if the suction valves were closed.)

The general expression used to calculate the frequency of an Event V (F(VSEQ)) utilizing the above failure modes is:

$$F(VSEQ) = X \left[(\lambda)_2 \, Q(V_1) + (\lambda)_1 \, Q(V_2) + (\lambda)_2 \, Q(V_1R) \right]$$

where

X	=	the number of RHR suction lines (1 or 2)
$(\lambda)_2$	=	failure rate of RCS valve (due to rupture)
$(\lambda)_1$	=	failure rate of RHR valve (due to rupture)
$Q(V_1)$	=	probability that RHR valve is open
$Q(V_2)$	=	probability that RCS valve is open
$Q(V_1R)$	=	probability of rupture of RHR valve

The following boundary conditions and assumptions were applied in each of the analyses:

1. The calculation is based on an occurrence when the plant is in Mode 1, 2, or 3.

2. The valve closest to the RCS is at RCS pressure and the valve closer to the RHR System is at RCS pressure only if the valve closest to the RCS fails open.

3. No common cause rupture of the valves is considered.

4. The term "valve rupture" is defined as catastrophic internal leakage. The failure rate is the same for either valve given that the valve is exposed to RCS pressure.

5. All electrical power to the control circuitry (i.e. 480 V AC bus) is assumed to be available with a probability 1.0.

6. A refueling outage occurs approximately every 18 months (assumed to be the only time at which the plant will be in cold shutdown, on average).

Fault trees were developed to determine the probability that one of the RHRS suction valves is open at power conditions ($Q(V_1)$ or $Q(V_2)$). These fault trees (shown in Appendix B) were developed in detail to show the failures down to the control circuitry component level. The scenarios examined in the fault tree for the case with the autoclosure interlock are: 1) the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but due to some component failure, the valve does not close) and the autoclosure interlock fails to perform its function and does not close the valve and an operator fails to detect that the valve is not closed during startup or power operation.

For the case with the autoclosure interlock removed, the scenarios developed in the fault tree are: 1) the operator fails to remove power to the valve by racking cut the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but it does not close) and the operator fails to detect that the valve is not closed via the presence of an alarm (or the alarm fails to operate).

The probabilities generated from the fault trees were input into the equation for the frequency of an interfacing system LOCA for each of the four reference plants. The frequencies were calculated for the case with the autoclosure interlock present and without the autoclosure interlock and with an alarm (the proposed change). The frequencies are shown in Table 7-2 along with the percent change in the frequency for each plant.

In each case the frequency of an Event V decreases with removal of the ACI. The main contributor to the frequencies in each case is a rupture of the RCS valve followed by rupture of the RHR valve (frequency of 5.75E-07/year). The deletion of the ACI has no impact on this contributor. The frequency of a double rupture dominates in each case while the other contributor (the rupture of one valve while the other valve has failed open) does not contribute as significantly in the case in which the ACI has been deleted than in the case in which the autoclosure interlock is present. This causes an overall reduction in the frequency of a V-sequence.

Furthermore, several factors were not considered in the analyses but are worth mentioning:

1) Both RHR suction valves have the power removed from the operators during Modes 1, 2, and 3. The four reference plants all have procedures that require that power be removed from the control circuitry by opening and locking the circuit breakers. This prevents opening of the valves during these modes.

2) The suction valves have open permissive interlocks that prevent the valves from being opened whenever the RCS pressure is greater than setpoint of the open permissive (usually around 400 psig). Thus, an operator error in which he inadvertently opens the valves is not very likely.

3) It is highly unlikely that a suction valve could move against the high differential pressure across the valve when the plant is in Modes 1, 2, or 3 because the valve motor size is inadequate to open the valve given the high differential pressure.

4) If an Event V should occur, the RHRS relief valve would operate. This relief valve discharges inside containment to the pressurizer relief tank. This relief valve would decrease the consequences of an Event V.

5) An IDCOR analyses for Zion in Reference 24, "Technical Report 23.5, Evaluations of Containment Bypass and Failure to Isolate Sequences for the IDCOR Reference Plants," found that if the two RHR suction valves fail open such that the release of high pressure fluid into the low pressure piping is sufficiently large, the low pressure piping could be exposed to pressures of approximately 2250 psia. However, "the hoop stress developed by internal pressurization would be at a level much less than the yield stress. ..." "Thus, a slow pressurization would not result in a failure of the piping system, but could eventually overpressurize other parts of the system such as the pump seals. ... , the inadvertent opening of these valves would not create a hydrodynamic transient sufficient to threaten the integrity of the piping. Rather, it would create a 'slow overpressurization' of the low pressure system since the valve opening and thus the pressure transient would be slow compared to the acoustic transit times of tens of milliseconds. Consequently, this would likely result in failure of the pumps seals." Thus the most likely failure mode after the failing open of the RHR suction valves is failure of the, RHRS pumps seals. If this occurred, water would spill onto the floor of the pump compartment. In most plants, each RHRS pump is in a separate, shielded compartment that drains to a sump. Gross leakage from the RHRS can be accommodated in the pump compartments. Thus, the consequences to the public are considerably less than originally postulated in most PRA studies.

Thus, from a probabilistic standpoint, the deletion of the autoclosure interlock and the inclusion of a control room alarm is beneficial in reducing the frequency of an interfacing systems LOCA and the potential for a significant radionuclide release outside containment.

7.4 Residual Heat Removal System Unavailability Analysis

The availability of the RHRS during cold shutdown has been of increasing concern in the nuclear industry. Many events have occurred in which the ability to remove decay heat has been lost, either because of a loss of flow in the RHRS or because of a loss of the heat sink. Abnormal events that occur shortly after initiation of the RHRS, while the decay heat generation rate is high, can cause bulk boiling conditions if decay heat removal is lost and not restored by the operator in a time period as short as twenty minutes. The RHRS for each of the four reference plants was analyzed to determine the unavailability of the system to remove decay heat and the impact of removal of the autoclosure interlock on this unavailability due to spurious closure of the suction valves. Appendix C provides the detailed descriptions of the analysis.

The availability of the RHRS to remove decay heat is considered in three phases in this analysis. First, the RHR System must be placed into service and go through a warm-up period in order to minimize the thermal shock to the system. Secondly, during the initial phase of cooldown, the decay heat load is high. For this phase, two trains of RHR (two pumps and two heat exchangers) are assumed to be required for 72 hours. The final phase of cooldown is long term decay heat removal. The decay heat load is low and only one train of RHRS (one pump and one heat exchanger) is required to be in operation. Six weeks was the time period assumed for this phase (based on the average refueling outage time period).

Fault trees were constructed for each of the three phases. The components in the RHRS were modeled in the fault tree including valves, heat exchangers and pumps. Separate fault trees were developed, with and without the RHR suction/isolation valves autoclosure interlock, in order to show the change in RHR System unavailability due to the removal of the autoclosure interlock. These RHR suction/isolation valves from the Reactor Coolant System hot legs were modeled in detail down to the control circuitry level in order to show the change in unavailability.

The following boundary conditions and assumptions were utilized in the analysis for each of the four reference plants.

1. Two trains of RHR are required for 72 hours following initiation of the RHR System.

2. One train of RHR is required for 6 weeks (representative of the time of a refueling outage).

3. Injection into two cold legs (of 3 or 4 cold legs) is required for the initial RHR cooldown phase (72 hours).

4. Injection into two cold legs (of 3 or 4 cold legs) is required for the long term RHR cooldown phase (6 weeks).

5. No testing or maintenance operations are assumed to occur during the initial phase of cooldown using the RHR System (first 72 hours).

6. During the warm-up period of the RHRS, both RHR pumps are started and must run for approximately two hours before injection into the RCS cold legs.

7. All electric power (AC and DC) is assumed to be available with a probability of 1.0.

8. For long term cooling, it is assumed that the Train A pump is operating and the Train B pump is in standby and thus must start and run should the Train A pump fail. No switching of trains during long term cooling is assumed.

9. No common cause failure of components is considered.

The three phases of cooldown are described below:

Failure to Initiate RHR

A single fault tree was developed for this phase of RHR operation to identify those faults that could impact the initiation of the RHR System, which is defined as being approximately the first two hours of operation. An additional fault tree was not developed because this phase of operation is not dependent on the autoclosure interlock but on the prevent-open interlock, which has remained unchanged.

The basis for the fault tree development for this phase was provided by the operating procedures for initiating decay heat removal by the RHRS. Each of the steps modeled in the RHR initiation fault tree involved an operator error or a component failure or both, as appropriate. For example, the opening of CCW valves to the RHR heat exchangers could involve the operator failing to open the valve or the valve failing to open due to mechanical or electrical malfunctions.

Failure of Short Term Cooling

The fault trees developed for this phase of cooldown reflect that both RHR trains are required to be in operation to provide adequate cooling. Injection into any two of three or four RCS cold legs is required for success in this phase or inversely, failure to supply cooling flow from two RHR trains to the cold legs constitutes RHR System failure. The short term cooling fault tree for each reference plant primarily features spurious closing of various valves and failure of RHR pumps to run over the 72 hour period. Spurious closure of the RHRS suction isolation valves due to the autoclosure interlock is explicitly modeled in the fault trees.

Failure of Long Term Cooling

Only one RHR pump and heat exchanger are required to operate for six weeks in the long term cooling phase to provide adequate cooling. Injection into any two of three or four RCS cold legs is required for success in this phase or inversely, failure to supply cooling flow from either of two RHR trains to the cold legs results in RHR System failure.

For each reference plant, the long term cooling fault tree shows spurious closing of various valves over the six week period along with failure of the one train RHR pump to continue running and upon failure of the running pump, failure of the second RHR pump to start, run or be unavailable due to test or maintenance.

Results

The fault trees for each phase were quantified to determine the unavailabilities for each reference plant. The results are shown in Table 7-3.

For the failure of initiation fault trees, the dominant failure mode is operator error. The operator failing to energize the circuit breakers to the RHR suction valves or the operator failing to open the RHR suction valves dominate the failure modes for this phase of cooldown. The deletion of the autoclosure interlock has no impact on the failure probability for RHRS initiation since the autoclosure interlock does not affect the valve's opening.

The failure probability for the short term cooling phase is reduced between 10 to 13 percent with the deletion of the ACI for the reference plants. The dominant failure mode for the fault trees (with and without the autoclosure interlock) is the failure of either of the two operating pumps to run for 72 hours (both pumps are required for success in this phase).

For each of the reference plants, the failure of both pumps to run for six weeks is the dominant contributor to the unavailability in the long term cooling phase. With the ACI present, the other failure modes involve the single failure of a component associated with the ACI such as the power supply, signal comparator, bistable switch or pressure transmitter which causes spurious closure of one of the RHR suction valves.

For Callaway and Shearon Harris, a single failure of a component associated with the ACI causes spurious closure of one of the RHR valves on each suction line, thereby isolating the RHR System and causing the failure of long term cooling. Since North Anna and Salem have only one suction line, a single failure in the ACI isolates the entire RHR System.

The results of the quantification of the RHR unavailability fault trees show a trend that the autoclosure interlock becomes more of a determining and detrimental factor as the length of time in which the RHRS is required to operate increases. In summary, the deletion of the autoclosure interlock reduces the number of spurious closures of the RHR suction valves, and thus, increases the availability of the RHRS for the reference plants.

7.5 Overpressurization Transients

A number of events have occurred in which the temperature - pressure limits in the Technical Specifications have been exceeded. A majority of these events have occurred during startup or shutdown conditions and have been caused by either equipment malfunction, procedural deficiencies or incorrect operator action. These pressure transients are of concern because the RHRS may be subject to this overpressure, the reactor vessel material is more brittle at relatively low temperatures than at operating temperatures, and the requirements of 10CFR50 Appendix G may be exceeded.

The effect of an overpressure transient at cold shutdown conditions will be altered by removal of the autoclosure interlock. With removal of the interlock, the RHRS may also be subject to overpressure. However, the RHRS relief valve(s) will be available to help mitigate the transient. The trade-offs between these two must be considered in the analysis of the RHRS autoclosure interlock.

The overpressurization analysis uses event trees to model the mitigating actions (both automatic and manual) following the occurrence of low temperature overpressurization events. These mitigating actions affect the severity of the overpressurization events and reduce the possibility of damage to the plant. The analysis is divided into two parts: 1) determination of the frequency of cold overpressure events and 2) the effect of mitigation on the transients. Each part is discussed below. More detail is provided in Appendix D.

7.5.1 INITIATING EVENTS

Many past reports have characterized the different types of transients possible at cold shutdown. The following lists the overpressure transients which have been examined:

1. Premature opening of the RHRS.
2. Rod withdrawal.
3. Failure to Isolate RHRS During Startup.
4. Pressurizer Heaters Actuation.
5. Startup of Inactive Loop. (Startup of a RCP.)
6. Loss of RHRS Cooling Train.
7. Opening of Accumulator Discharge Isolation Valves.
8. Letdown Isolation
   a) RHRS operable
   b) RHRS isolated.
9. Charging/Safety Injection Pump Actuation.

The transients described above were researched in order to determine the frequency of these events based on past experience. Appendix D details the events that have occurred and the quantification of the frequencies of these transients. Table 7-4 lists the transients and the frequencies calculated based on operating experience.

These events have been grouped into two general categories which describe their effect on the plant: 1) events that affect the balance between mass addition and mass letdown, and 2) events that affect the heat input/heat removal balance. These types of events have actually occurred and the NRC has expressed concern over the frequency of these events. This section describes the heat input transients and then the mass input transients along with its effect on the RHR System.

HEAT INPUT TRANSIENTS

Premature Opening of the RHRS

Overpressurization of the RHRS could occur if the RHRS is opened prior to reducing the RCS pressure below the RHRS design pressure. However, the RHRS isolation valves are equipped with "prevent-open" interlocks. These interlocks prevent the opening of the suction valves before the RCS pressure is below a given setpoint. Furthermore, the valve motor operator is sized with insufficient torque to raise the stem with a pressure differential across the valve greater than 500 psi.

To date, this type of event has not occurred, although attempts to access the RHRS prior to reduction of the RCS pressure have resulted in valve motor failures. Because of the design features on the RHRS isolation valves, this type of event is not considered plausible and was not analyzed.

Rod Withdrawal

A rod withdrawal accident is defined as an uncontrolled addition of reactivity to the reactor core caused by withdrawal of one or more banks of control rods, resulting in a power excursion. The transient would be terminated by the automatic features of the Reactor Protection System such as the source range neutron flux trips. Rod withdrawal during shutdown would have only a minor effect on the RCS and the RHRS.

Westinghouse analyses of this event for the RESAR-3 and -41 designs (References 10 and 12) utilized the following assumptions:

1) Reactor is subcritical by 1% $\Delta k/k$.
2) One loop of the RHRS is isolated from service.
3) RCS temperature and pressure are 350°F and 425 psig prior to the event.

It was determined that the event produced one of the least severe transients of those analyzed and would not overpressurize the RHRS (pressure would not exceed 110% of RHRS design pressure). The RHRS relief valve would also be available to help mitigate this transient. The removal of the autoclosure interlock has no effect on this transient. Thus, this event was not considered a critical event (it would be bounded by other events) and was removed from the analysis.

Failure to Isolate RHRS During Startup

During plant startup, the RCS is completely filled, and the pressurizer heaters are energized. The RHRS pumps are operating, but the discharge is directed to the CVCS. After the RCPs are started, pressure control via the RHRS and the low-pressure letdown line is continued until the pressurizer steam bubble is formed. Indication of steam bubble formation is provided in the control room by the damping out of the RCS pressure fluctuations and by pressurizer level indication. Following pressurizer steam bubble formation, the RHRS is isolated from the RCS.

If the RHRS is not isolated by the operator, RCS pressure would increase to that of the RHRS suction relief valve(s) setpoint. Discharge through the relief valve(s) would prevent the pressure from increasing further. Failure to close both RHR suction valves during startup is not considered a credible failure mode because the condition would become apparent and corrective action would be taken. (The RHRS relief valve(s) would lift as the RCS pressure increased, an alarm would sound, and the RCS pressure would increase more slowly than if the suction valves were closed.)

If only one of the suction valves is closed on each suction line, RCS pressure can be raised to operating pressure. Should the operator fail to close the remaining valve, a loss-of-coolant accident could occur if the closed valve opens or ruptures. This condition is analyzed as part of the interfacing systems LOCA analysis described in Section 7.3.

Thus, this event was not analyzed as an overpressurization concern.

Pressurizer Heaters Actuation

During startup, all of the pressurizer heaters are energized and letdown is initiated (or increased) in order to form a steam bubble in the pressurizer. If the pressurizer heaters are inadvertently actuated, the same conditions result. The expansion rate due to boiling in the pressurizer is greater than that due to merely heating the pressurizer water. If the RHRS is not isolated, the pressure increase is limited by the relief valve on the RHRS suction line. However, if the relief valve failed, the RCS pressure would increase above the RHRS design pressure. The transient will continue until the decreasing pressurizer water level actuates an automatic heater cutoff (at approximately 10% of pressurizer volume).

To date, Westinghouse plants have not experienced this type of transient. Furthermore, the operating procedures for most plants require that the pressurizer heaters be de-energized during the mode transition from Hot Standby to Cold Shutdown. Also, since this transient is very slow, the operator should recognize and terminate the transient.

Startup of an Inactive Loop

The startup of an inactive reactor coolant pump is another heat input transient. This transient occurs when the reactor coolant pumps have been stopped (usually below 160°F) during the cooldown sequence. When the RCPs have been stopped, the isothermal conditions in the RCS no longer exist. The steam generator water may remain at a relatively constant temperature greater than the RCS temperature since there is little circulation through the steam generator tubes. Therefore, a significant temperature asymmetry between the steam generator water and the reactor coolant may develop. If a reactor coolant pump were to be started, the sudden heat input into the reactor coolant from the steam generators would cause a rapid increase in reactor coolant temperature.

Another case could occur if a reactor coolant pump is stopped during plant heatup but the cold charging and seal injection water is continued in service. This would cause a relatively cold volume of water to develop in the vertical pipe loop below the reactor coolant pumps. When the inactive reactor coolant pump is restarted, the cold water would be suddenly heated and would mix with the coolant and the cold water expands as its density decreases. This expansion results in an increase in RCS pressure.

This transient is considered in the RHRS overpressure analysis.

Loss of RHRS Cooling Train

Loss of an RHRS cooling train may occur at any time during RHRS operation. However, such a loss would have its greatest impact if it were to occur immediately following RHRS initiation during plant cooldown. At this time, the heat generation rate exceeds the heat removal capability of the remaining cooling train. The continual release of core residual heat into the reactor coolant with no heat rejection would cause a slow rise in the coolant temperature and pressure. Since this transient is slow, the operator should respond and restore the RHRS or limit the RCS pressure by venting the pressurizer.

MASS INPUT TRANSIENTS

Opening of Accumulator Discharge Isolation Valve

When the pressure is less than approximately 1000 psig, plant procedures require that the accumulator motor-operated discharge valves be closed and the power supply to these valves be de-energized and locked out. If an accumulator discharge valve was opened, water would be forced into an already water-solid RCS. This causes a pressure transient. The peak pressure reached during this event will be between the initial RCS pressure and the accumulator nitrogen pressure.

Letdown Isolation

For most Westinghouse plants, during cold shutdown, a letdown path is established through the RHR System in order to control the pressure in the RCS. If this letdown path is isolated, pressure control is lost. Isolation of letdown could occur in several ways: 1) closure of the letdown control valve, 2) isolation of the RHRS/CVCS crossover path or 3) closure of the RHRS inlet isolation valves. Of these, the pressure transient associated with the third event is greater in that the mass addition transient is coupled with a heatup transient because isolation of the RHRS precludes the use of the RHRS relief valve in mitigating the pressure rise and places this action on the COM System.

Charging/Safety Injection Pump Actuation

During the transition from hot standby to cold shutdown, the safety injection actuation signal is blocked to prevent full system actuation while in the water-solid mode. Also, power is locked out to the high head safety injection pumps and usually all but one charging pump. This is due to the fact that under stable pressure conditions, the inadvertent actuation of a charging pump or safety injection pump results in coolant addition and without an increase in letdown, a pressure transient will occur.

7.5.2 ANALYSIS

Based on the discussion of low temperature overpressure initiating events, the following describes the analysis conducted to determine the impact of removal of the autoclosure interlock. The first section describes the heat input analysis while the latter section details the mass input analysis.

HEAT INPUT ANALYSIS

The investigation of reported cold overpressurization events showed these heat addition mechanisms:

1) inadvertent operation of all the pressurizer heaters,
2) heat addition from core decay heat at 12 hours following an extended period of operation, and
3) inadvertent startup of a reactor coolant pump with temperature asymmetry between the reactor coolant system and the steam generator.

Past analyses assessed the effect of these transients in terms of the change in RCS pressure associated with each transient (Reference 26). Figure 7-2 was generated from these analyses.

This figure shows that heat input transients occur quickly in time. The figure also shows that given the RCS temperature and pressure are below 350°F and 450 psig, the RCS pressure change is less than approximately 200 psi for the decay heat addition and pressurizer heaters actuation. For these cases, the RHRS suction valve autoclosure interlock would not be activated (the setpoint is approximately 600 psig). Furthermore, the COM System and RHRS suction relief valves are capable of mitigating these transients.

For the startup of an inactive reactor coolant pump with a temperature asymmetry between the RCS and the steam generator, the peak pressure change is approximately 1500 psi and occurs in roughly 90 seconds with no relief valve actuation. Because the RHRS motor-operated valves closing time is approximately two minutes, the RHRS would be subjected to the high pressure before the valve could close. This could lead to the possibility of an interfacing systems LOCA. However, the probability of this event is small because the RHRS relief valve and the COM System must both fail in order for this event to occur.

From this discussion, the removal of the autoclosure interlock will have no effect on heat input/removal transients that occur during cold shutdown.

MASS INPUT ANALYSIS

In order to depict the slower mass input transients (relative to the heat input transients), event trees were utilized to model the mitigating actions that occur following the transients. Operator actions and mitigating systems are included in the event trees.

Event trees were constructed to determine the consequences of the mass input transients. The safety functions, i.e. the event tree top events, for the event trees are defined below:

1. Initiating Event (IE): The mass input initiator that could lead to overpressurization and/or possible RHRS damage.

2. RHRS isolated (RI): The RHRS will be isolated during certain periods of shutdown. This dictates whether or not the RHRS relief valve is available to mitigate the transient and if the possibility exists for damage to the RHRS.

3. RHRS Suction Relief Valves Lift (RV): If the RHRS is not isolated, the spring loaded relief valves will open at the setpoint pressure.

4. COM System Operates (COM): The low temperature overpressure protection system consists of two redundant and independent systems utilizing the pressurizer PORVs. When the system is enabled and reactor coolant temperature is below a given setpoint, a high pressure signal (above the COMS setpoint) will trip the system automatically and open a PORV until the pressure drops below the reset value.

5a. RHRS Suction/Isolation Valves Automatically Close (RS): When the pressure increases to the autoclosure setpoint pressure, the autoclosure interlock receives a pressure signal that actuates the circuitry and closes the motor-operated valve. This node is addressed in the present configuration case only.

5b. Operator Detects Overpressure Alarm and Isolates the RHRS (OD): For the modification case, an alarm would sound when the high pressure setpoint is reached. Through a revision in operating procedures, it is assumed that the operator will detect the overpressure and isolate the RHRS before the pressure reaches 150% of the RHRS design pressure.

6. Operator Secures Running Pump (OA1): Given an alarm, either by actuation from the RHRS relief valve opening to the pressurizer relief tank (PRT), or from the operation of at least one train of COMS, or from an RHRS pump low flow alarm (on autoclosure of the RHRS suction valves) or from the high pressure alarm on the RHRS suction

valves (in the modification case only), the operator will stop the extra running pump (either an SI or charging pump). If the operator stops the running pump, the overpressure event is terminated.

7. Operator Opens a PORV (OA2): Given an alarm, if no or one relief valve operates successfully and the pressure still continues to rise, the operator may open a PORV in order to reduce the pressure. The operator may also open a PORV if he fails to stop the running pump in order to increase the time available to mitigate the transient.

8. RHRS Relief Valve Reseats (RVR): Given that the RHRS relief valve successfully operated and the transient was terminated, the relief valve must reseat or coolant would be lost to the PRT. If the transient is not stopped, the relief valve will cycle open and closed and is assumed to eventually fail open.

9. Pressurizer PORVs Reseat (POR): Given that one or more of the PORVs has opened and the transient has been stopped, the valve must close in order to avert a loss of coolant condition. If the transient is not stopped, the valve(s) will cycle until failure occurs.

Success criteria for each event tree top event were developed and system/component failure probabilities were calculated for each of the nodes for each of the four reference plants. The calculation of these probabilities is detailed in Appendix D.

The event tree sequences were classified into discrete consequence categories. Each consequence category then represents a number of individual sequences that all have similar characteristics associated with them. The consequence categories are listed in Table 7-5.

The event trees were quantified using system/component failure probabilities along with the initiating event frequencies to determine the frequency of the consequence categories for the present configuration and the modification case. Each initiating event is discussed below. More detail is provided in Appendix D.

Opening of Accumulator Discharge Isolation Valve

This event does not require an event tree analysis. The opening of an accumulator discharge isolation valve would produce a pressure peak between the initial RCS pressure and the accumulator nitrogen pressure. At cold shutdown conditions, the RCS pressure is below approximately 450 psig. The accumulator design pressure is approximately 700 psig and the normal operating pressure is about 650 psig. Therefore, the maximum pressure possible would be less than 650 psig. This pressure would not damage the RHRS. The RHRS autoclosure interlock may close for this case but this would only occur if the RHRS relief valve and the COM System failed to operate. Therefore, the interlock has no effect on this transient.

Letdown Isolation/RHRS Operable

The success criteria for the letdown isolation cases was determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. Because the charging pump was assumed to operate at its maximum flow rate, it was assumed that only one RHR relief valve, or one PORV must operate to mitigate the transient. The following assumptions were utilized in the letdown isolation case.

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves (assumed to be representative of the average time for a refueling outage).

An event tree for the letdown isolation RHR operable case is shown in Figure 7-3.

The event tree was quantified for the configuration with the autoclosure interlock and without the autoclosure interlock. When the two cases were compared for Callaway, the consequence category LSCI decreased slightly while the HOPV category increased to 3E-15/shutdown year while for Salem, the consequence category MSCI decreased slightly while the HOPV category increased to 1.5E-11/shutdown year. The consequence categories LSCI and MSCI decreased slightly for Shearon Harris while the HOPV category increased to 3E-15/shutdown year with removal of the autoclosure interlock. For North Anna, the HOPV consequence category increased to 4.5E-15/shutdown year.

The consequence category HOPV is defined as a high overpressure transient with the RHR System open to the RCS which results in an interfacing systems LOCA at cold shutdown. Although the frequency increases for all four reference plants, the occurrence of such an event is highly unlikely as shown by the small frequency. For this transient to result in an HOPV, the RHR relief valves, the COM System, and any operator mitigating action would have to fail. Thus, the increase of an interfacing LOCA at shutdown for this transient is not significant.

Letdown Isolation/RHRS Isolated

This event puts the transient's overpressure effects on the RCS and not on the RHRS. Thus, the removal of the RHPS autoclosure interlock does not affect the mitigating systems available to stop the transient.

However, the initiating event itself causes this transient. Spurious closure of the isolation valves initiates the overpressure transient. If the autoclosure interlock is removed, the initiator frequency would be reduced. Thus it was conservatively assumed that the frequency of this transient would be reduced by one half (from 4.45E-01/shutdown year to 2.22E-01/shutdown year). (The removal of the interlock would essentially decrease the frequency by much more than one half. However, to account for some unknown spurious closure events, the frequency was conservatively estimated to be reduced by one half.) The result of the reduction in initiator frequency decreases the challenges to the mitigating systems in the RCS and reduces the frequencies of all of the consequences categories.

Charging/Safety Injection Pump Actuation

The success criteria for the event trees for this transient was determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. Because the charging pump maximum flow rate and the safety injection pump maximum flow rate combined is approximately 1200-1300 gpm (conservative assumption that both pumps operate at maximum flow rates), it was assumed that two PORVs or one PORV and one RHR relief valve or two RHR relief valves (where appropriate) are required to mitigate the transient. The following assumptions were also utilized in the analysis of the charging/safety injection mass input transient:

1. No credit is taken for the RCS vents.
2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves (assumed to be representative of the average time for a refueling outage).

Figure 7-4 illustrates an event tree for the charging/safety injection initiating event.

The event tree was quantified for the configuration with the autoclosure interlock and without the autoclosure interlock. When the two cases were compared for Salem, consequence categories MSFO, MSCO, and HOPV increased. However, the increase is in the range of 1E-10 to 1E-11/shutdown year. For Callaway, consequence categories MSFO, MSCO, and HOPV increased in the range of 1E-11 to 1E-12/shutdown year. Consequence categories MSFO, MSCO, and HOPV increased in the range of 1E-11 to 1E-12/shutdown year for Shearon Harris. For North Anna, consequence categories MSFO, MSCO, and HOPV increased. The increase is in the range of 1E-14 to 1E-15/shutdown year. These are very insignificant increases in the frequency of these outcomes.

Although the frequency for the consequence category HOPV increases for all four reference plants, the occurrence of such an event is highly unlikely as shown by the small frequency. For this transient to result in an HOPV, the

RHR relief valves, the COM System, and any operator mitigating action would have to fail. Thus, the increase of an interfacing LOCA at shutdown for this transient is not significant.

Based on the analysis of the mass input transients, the removal of the autoclosure interlock has a small impact on the frequency of an interfacing systems LOCA. Furthermore, the removal of the autoclosure interlock will increase the availability of the RHR suction relief valves to mitigate low temperature overpressure transients, thereby reducing the challenges to the pressurizer power operated relief valves.

It should be understood that the autoclosure interlock was not installed to mitigate overpressure transients. The RHR suction valves are slow-acting and take approximately two minutes to close. The autoclosure interlock will not protect the RHR System from a fast-acting overpressure transient such as the startup of a reactor coolant pump.

The major impact with respect to overpressure concerns is that removal of the autoclosure interlock will significantly reduce the number of letdown isolation transients.

TABLE 7-1

COMPONENT FAILURE RATE DATA

COMPONENT	FAILURE MODE	FAILURE RATE	SOURCE
Air operated valve	Failure to operate	1.0E-05/hr	2815
Check valve	Failure to open	2.0E-07/hr	2815
Check valve	Failure to close	2.0E-06/hr	2815
Motor operated valve	Failure to open	1.0E-05/hr	2815
Motor operated valve	Fail to remain open	2.0E-07/hr	2815
Motor operated valve	Fail to close	1.0E-05/hr	2815
Motor operated valve	Catastrophic	1.0E-07/hr	2815
Manual valve	Failure to operate	2.0E-07/hr	2815
Motor driven pump	Failure to start	1.0E-05/hr	2815
Motor driven pump	Failure to run	1.0E-04/hr	2815
Thermal Overload	Premature open	1.5E-07/hr	Fuse Rate
Diode (Std quality)	All	7.56E-09/hr	MIL HDBK
Resistor (Std quality)	All	4.90E-09/hr	MIL HDBK
Relay	All	8.7E-08/hr	MIL HDBK
Bistable	High Output	2.40E-06/hr	MIL HDBK
Bistable	Low Output	1.65E-06/hr	MIL HDBK
Pressure Sensors	All	2.80E-06/hr	MIL HDBK
Loop Power Supply	All	5.80E-06/hr	MIL HDBK
Comparator	All	2.90E-06/hr	MIL HDBK
Annunciator	All	4.25E-06/hr	IEEE
Torque Switch	Failure to operate	2.00E-07/hr	2815
Current Transformer	All	3.50E-07/hr	IEEE
Relay Contacts	Fail to transfer	1.00E-06/hr	2815
Relay Coil	All	3.00E-06/hr	2815
Circuit Breaker	Fail to close	3.00E-08/hr	IEEE
Circuit Breaker	Fail to open	2.00E-08/hr	IEEE
Circuit Breaker	Open w/o command	1.00E-08/hr	IEEE
Push button switch	All	1.22E-06/hr	IEEE
Rotary switch	All	8.10E-07/hr	IEEE
Toggle switch	All	2.33E-07/hr	IEEE
Fuse	All	1.50E-07/hr	IEEE
Limit switch	All	7.22E-06/hr	IEEE
Motor Starter contacts	Spurious operation	3.00E-08/hr	IEEE
Relay Contacts	Spurious operation	2.00E-08/hr	IEEE
Relief Valve	Fail to open	3E-04/demand	IPE
Relief Valve	Fail to close	3E-02/demand	IPE
I-E Converter	All	2.00E-07/hr	IEEE
Isolator E-E converter	All	4.8E-07/hr	IEEE
Pressure Transmitter	All	1.73E-06/hr	IEEE

Notes:
IEEE - Reference 22
2815 - Reference 21
MIL HDBK- Reference 23
IPE - Reference 24

TABLE 7-2
INTERFACING SYSTEM LOCA FREQUENCIES
WITH AND WITHOUT AUTOCLOSURE INTERLOCK

	WITH AUTOCLOSURE INTERLOCK	WITHOUT AUTOCLOSURE INTERLOCK	PERCENT CHANGE
SALEM	8.35E-07/YEAR	5.77E-07/YEAR	-31
CALLAWAY	1.52E-06/year	1.16E-06/year	-24
SHEARON HARRIS	1.45E-06/YEAR	1.16E-06/YEAR	-20
NORTH ANNA	9.28E-07/YEAR	5.77E-07/YEAR	-38

TABLE 7-3
RHR SYSTEM UNAVAILABILITY RESULTS

PLANT	WITH AUTOCLOSURE INTERLOCK	WITHOUT AUTOCLOSURE INTERLOCK	PERCENT CHANGE
SALEM			
RHR INITIATION	3.20E-02	3.20E-02	0
SHORT TERM COOLING	1.60E-02	1.40E-02	-13
LONG TERM COOLING	3.60E-02	1.20E-02	-67
CALLAWAY			
RHR INITIATION	3.62E-02	3.62E-02	0
SHORT TERM COOLING	1.64E-02	1.44E-02	-12
LONG TERM COOLING	3.91E-02	1.17E-02	-70
SHEARON HARRIS			
RHR INITIATION	3.74E-02	3.74E-02	0
SHORT TERM COOLING	1.61E-02	1.45E-02	-10
LONG TERM COOLING	3.45E-02	1.16E-02	-66
NORTH ANNA			
RHR INITIATION	1.90E-02	1.90E-02	0
SHORT TERM COOLING	1.65E-02	1.46E-02	-12
LONG TERM COOLING	4.14E-02	1.39E-02	-66

TABLE 7-4

FREQUENCY OF OVERPRESSURE TRANSIENTS

	TOTAL NUMBER OF OCCURRENCES	FREQUENCY (EVENTS/SHUTDOWN YEAR)
OPENING OF ACCUMULATOR DISCHARGE ISOLATION VALVES	4	3.56E-02
STARTUP OF INACTIVE LOOP	11	9.79E-02
ISOLATION OF LETDOWN WHILE CHARGING CONTINUES	14	1.25E-01
CHARGING/SAFETY INJECTION	14	1.25E-01
ISOLATION OF LETDOWN WHILE CHARGING CONTINUES RHR ISOLATED	50	4.45E-01
TOTAL	93	8.27E-01

TABLE 7-5
TRANSIENT EVENT OUTCOME DESCRIPTIONS

CATEGORY	OUTCOME DESCRIPTION
LSFO	Low pressure with small loss of coolant and the RHRS is open to the RCS. The running pump has been stopped but one of the relief valves has failed to reseat. The operator must take action to reseat the valve or isolate it and then must add makeup.
LSFI	Low pressure with small loss of coolant and the RHRS is isolated from the RCS. The running pump has been stopped but one of the relief valves has failed to reseat. The operator must take action to reseat the valve or isolate it and then must add makeup. He must also reinitialize RHR operation.
LSCO	Low pressure with small loss of coolant and the RHRS is open to the RCS. The running pump has not been stopped and coolant is exiting via one relief valve. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely.
LSCI	Low pressure with small loss of coolant and the RHRS is isolated from the RCS. The running pump has not been stopped and coolant is exiting via one relief valve. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely.
LLFO	Low pressure with large loss of coolant and the RHRS is open to the RCS. The running pump has been stopped but two or more of the relief valves have failed to reseat. The operator must take action to reseat the valves or isolate them and then must add makeup.
LLFI	Low pressure with large loss of coolant and the RHRS is isolated from the RCS. The running pump has been stopped but two or more of the relief valves have failed to reseat. The operator must take action to reseat the valves or isolate them and then must add makeup. He must also reinitialize RHR operation.
LLCO	Low pressure with large loss of coolant and the RHRS is open to the RCS. The running pump has not been stopped and coolant is exiting via two or more relief valves. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely. The operator must also be aware of possible deadheading or air entrainment of the RHR pumps.

TABLE 7-5 (cont.)
TRANSIENT EVENT OUTCOME DESCRIPTIONS

CATEGORY	OUTCOME DESCRIPTION
LLCI	Low pressure with large loss of coolant and the RHRS is isolated from the RCS. The running pump has not been stopped and coolant is exiting via two or more relief valves. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely.
MSFO	Medium pressure with small loss of coolant and the RHRS is open to the RCS. The running pump has been stopped but one of the relief valves has failed to reseat. The operator must take action to reseat the valve or isolate it and then must add makeup. He must also reduce the RCS pressure and check on the integrity of the RHR System.
MSFI	Medium pressure with small loss of coolant and the RHRS is isolated from the RCS. The running pump has been stopped but one of the relief valves has failed to reseat. The operator must take action to reseat the valve or isolate it and then must add makeup. He must also reduce the RCS pressure and then reinitialize RHR operation.
MSCO	Medium pressure with small loss of coolant and the RHRS is open to the RCS. The running pump has not been stopped and coolant is exiting via one relief valve. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely. He must also reduce the RCS pressure and check on the integrity of the RHR System.
MSCI	Medium pressure with small loss of coolant and the RHRS is isolated from the RCS. The running pump has not been stopped and coolant is exiting via one relief valve. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely.
MLFO	Medium pressure with large loss of coolant and the RHRS is open to the RCS. The running pump has been stopped but two or more of the relief valves has failed to reseat. The operator must take action to reseat the valves or isolate them and then must add makeup. He must also reduce the RCS pressure and check on the integrity of the RHR System.

TABLE 7-5 (cont.)
TRANSIENT EVENT OUTCOME DESCRIPTIONS

CATEGORY	OUTCOME DESCRIPTION
MLFI	Medium pressure with large loss of coolant and the RHRS is isolated from the RCS. The running pump has been stopped but two or more of the relief valves has failed to reseat. The operator must take action to reseat the valves or isolate them and then must add makeup. He must also reduce the RCS pressure and then reinitialize RHR operation.
MLCO	Medium pressure with large loss of coolant and the RHRS is open to the RCS. The running pump has not been stopped and coolant is exiting via two or more relief valves. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely. The operator must also be aware of possible deadheading or air entrainment of the RHR pumps. He must also reduce the RCS pressure and check on the integrity of the RHR System.
MLCI	Medium pressure with large loss of coolant and the RHRS is isolated from the RCS. The running pump has not been stopped and coolant is exiting via two or more relief valves. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely. He must also reduce the RCS pressure.
MOPI	Medium overpressure with the RHRS isolated from the RCS. The running pump has been stopped but no relief valves have actuated. The operator must reduce the RCS pressure and then reinitialize RHR operation.
HOPI	High overpressure with the RHRS isolated from the RCS. The running pump has been stopped but no relief valves have actuated. The operator must reduce the RCS pressure, possibly through the RCS vents or pressurizer safety valves.
HOPV	High overpressure with the RHRS open to the RCS. The running pump has not been stopped and no relief valves have actuated. The RHR System integrity is assumed to be lost and an interfacing systems LOCA has occurred. The operator must attempt to isolate the RHR System.

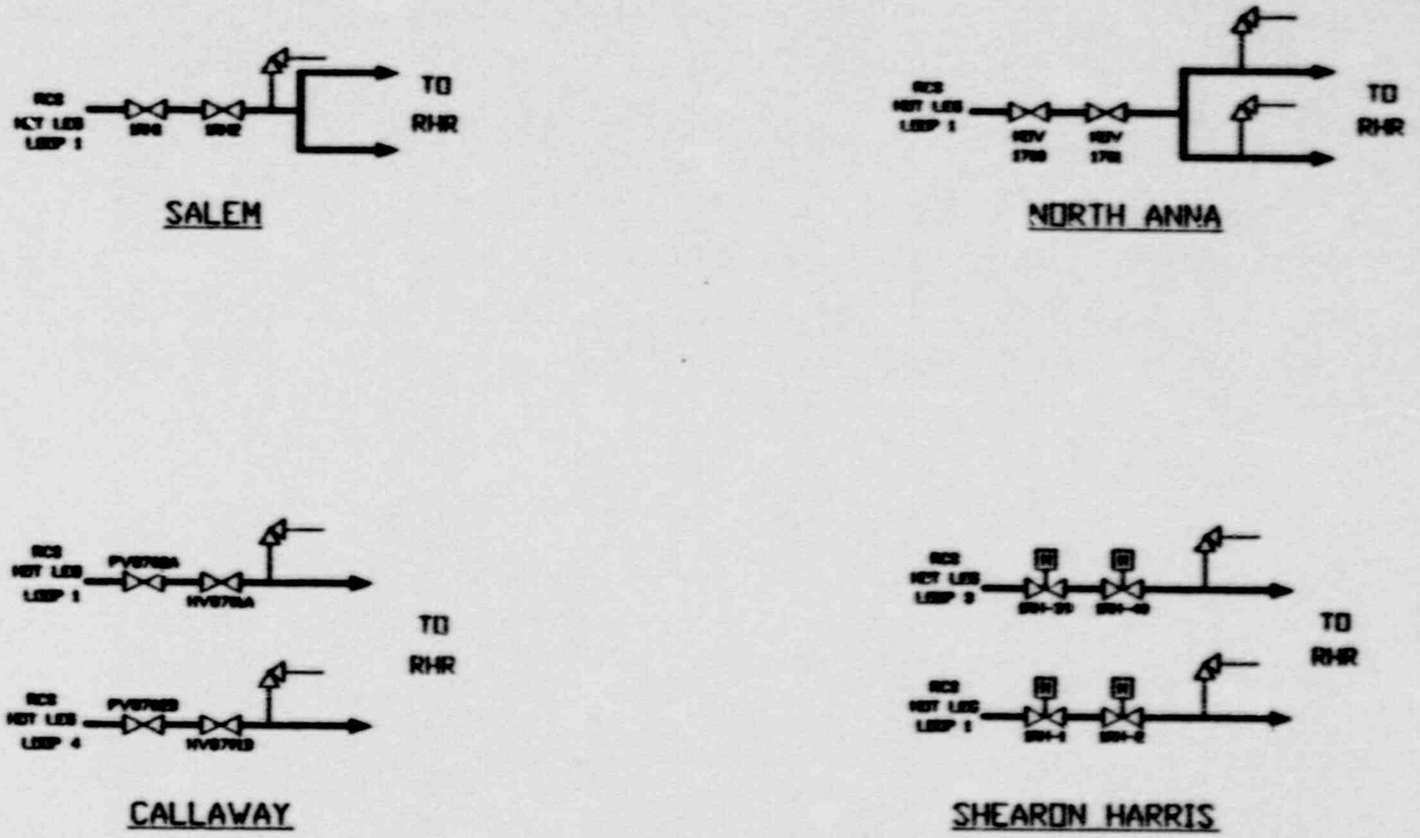


FIGURE 7-1
RHR SUCTION LINE
CONFIGURATIONS

2/8/88

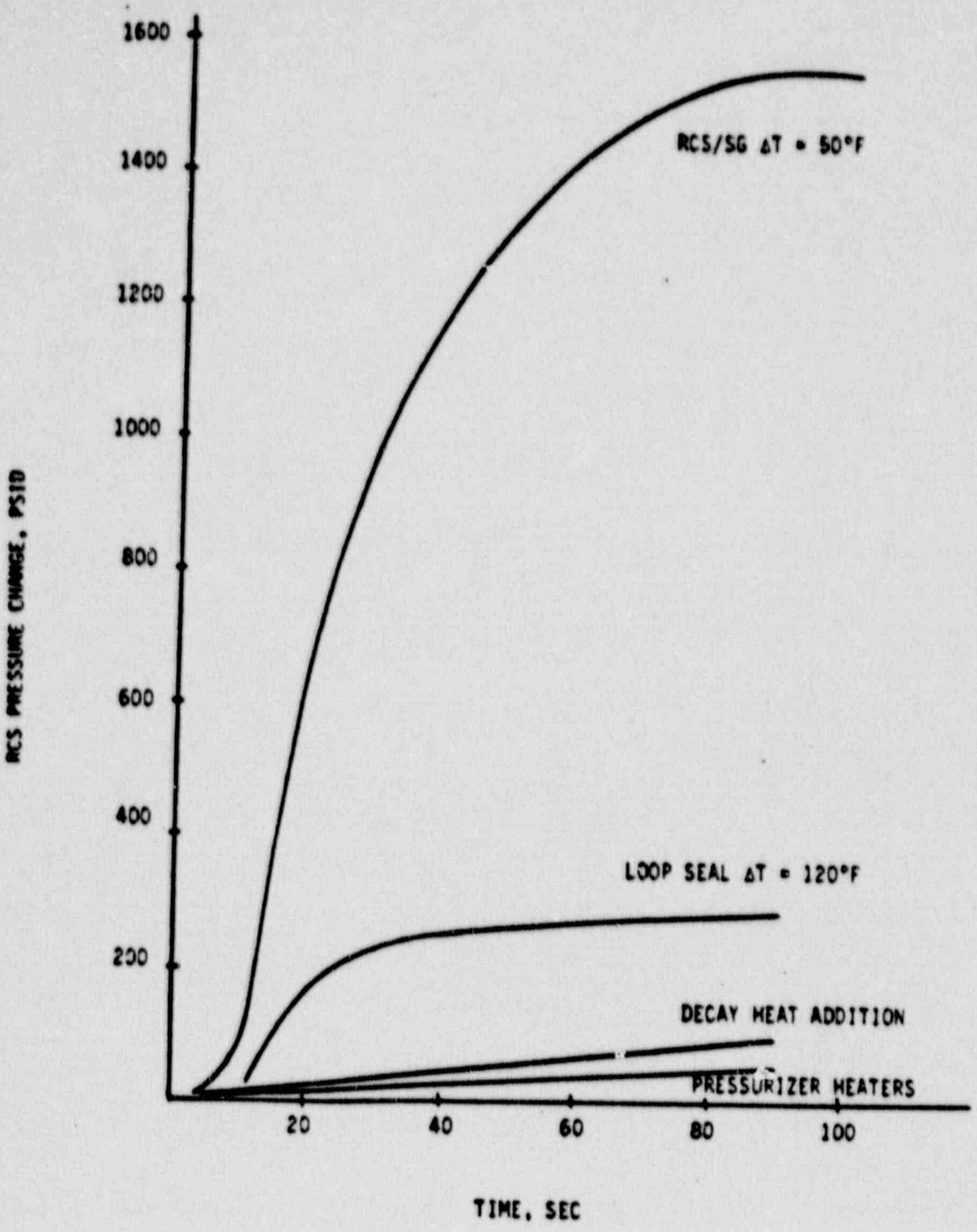


FIGURE 7-2
HEAT INPUT TRANSIENTS

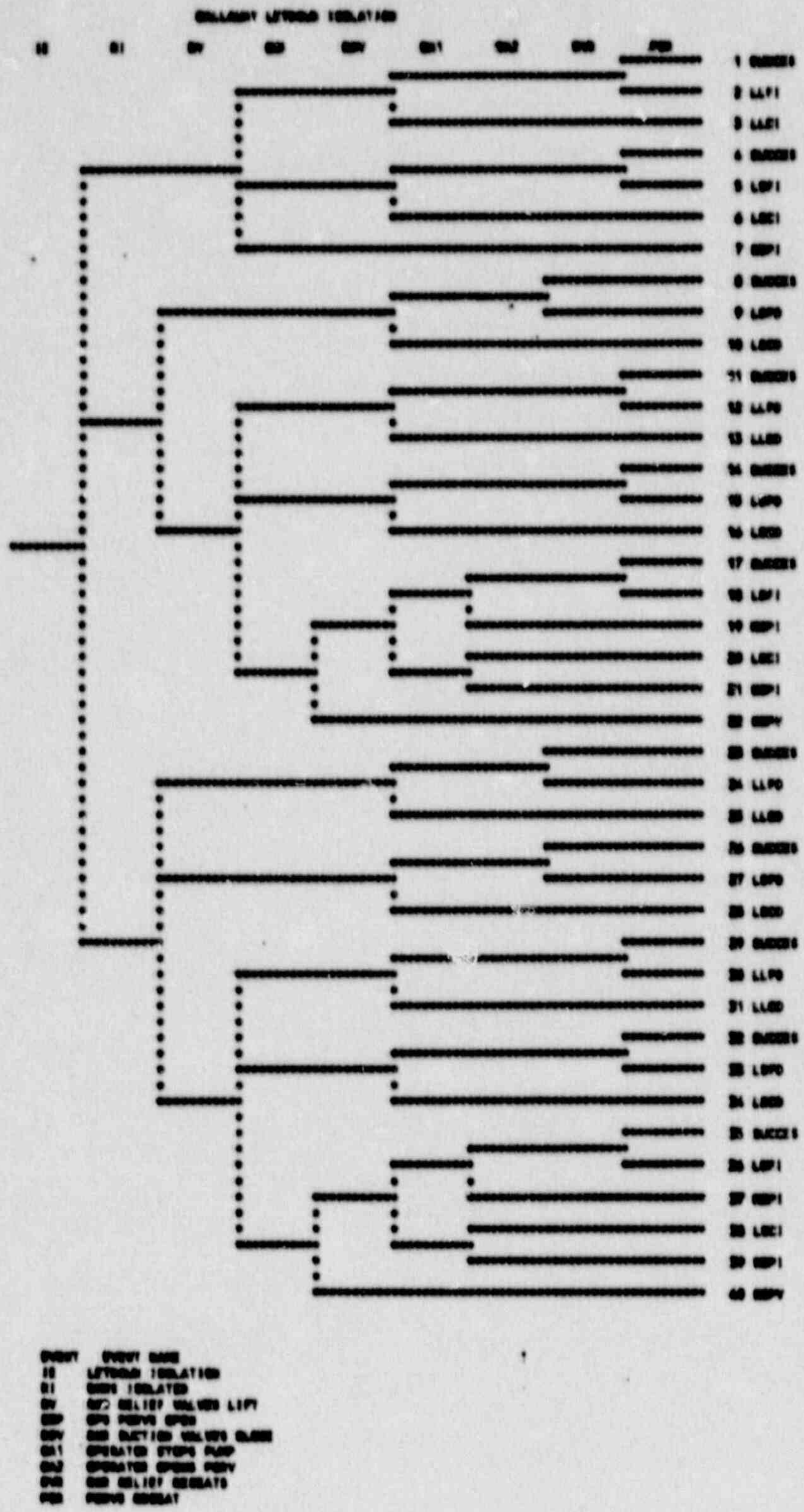


FIGURE 7-3
LETDOWN ISOLATION RHR OPERABLE EVENT TREE

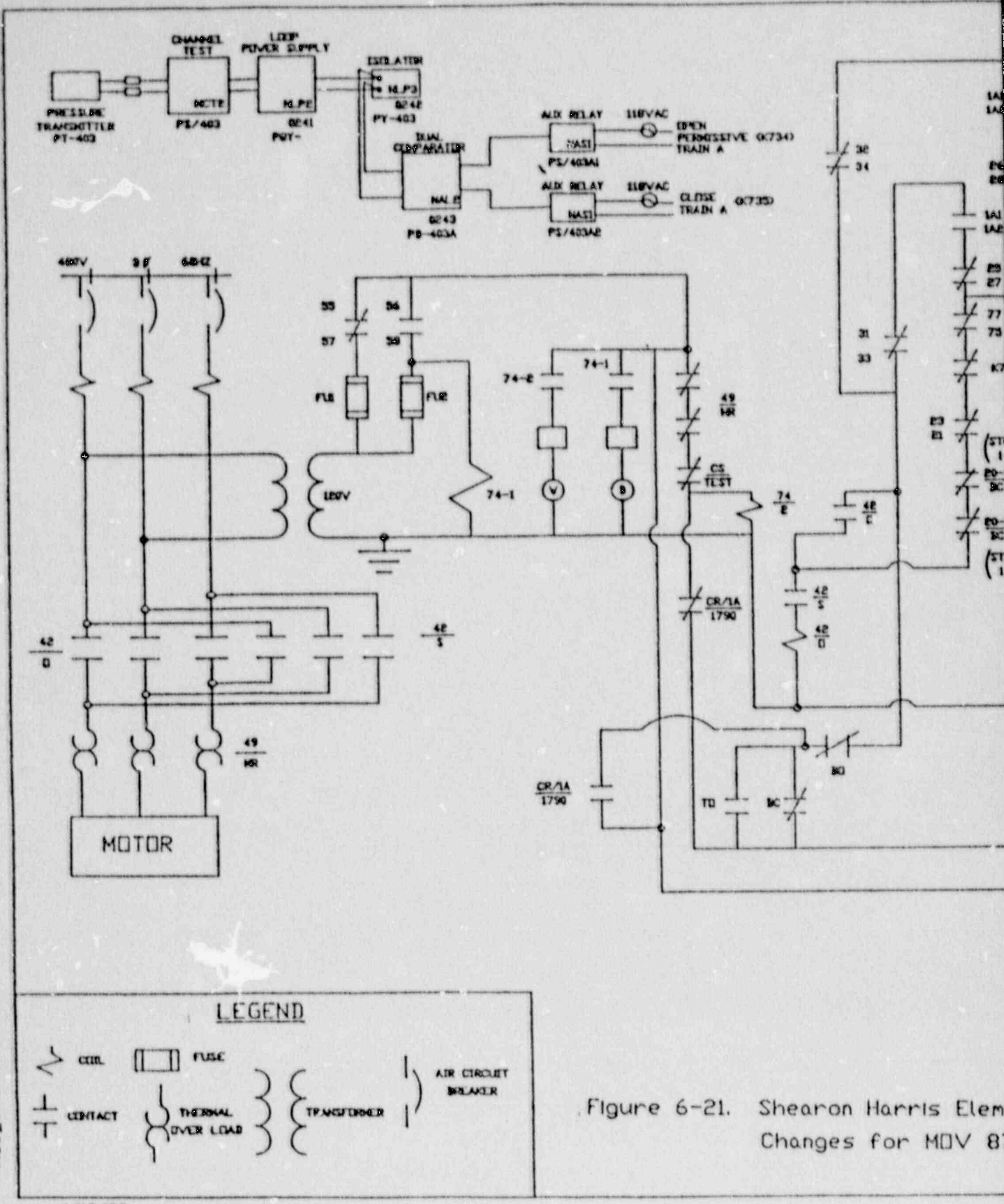
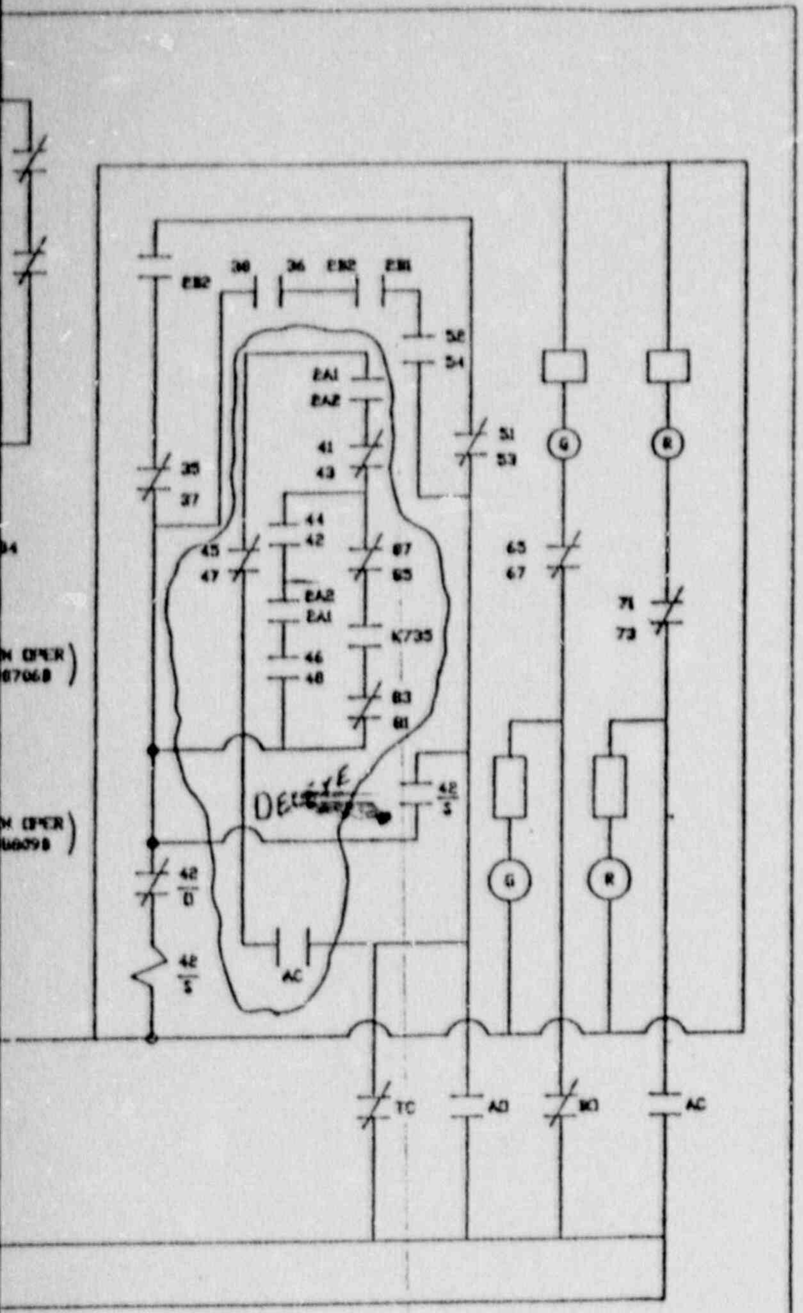
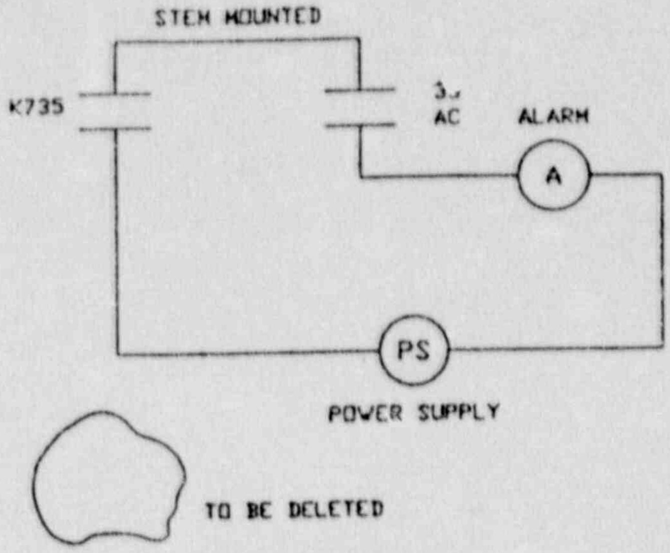


Figure 6-21. Shearon Harris Eleme
Changes for MOV 87

1/19/88



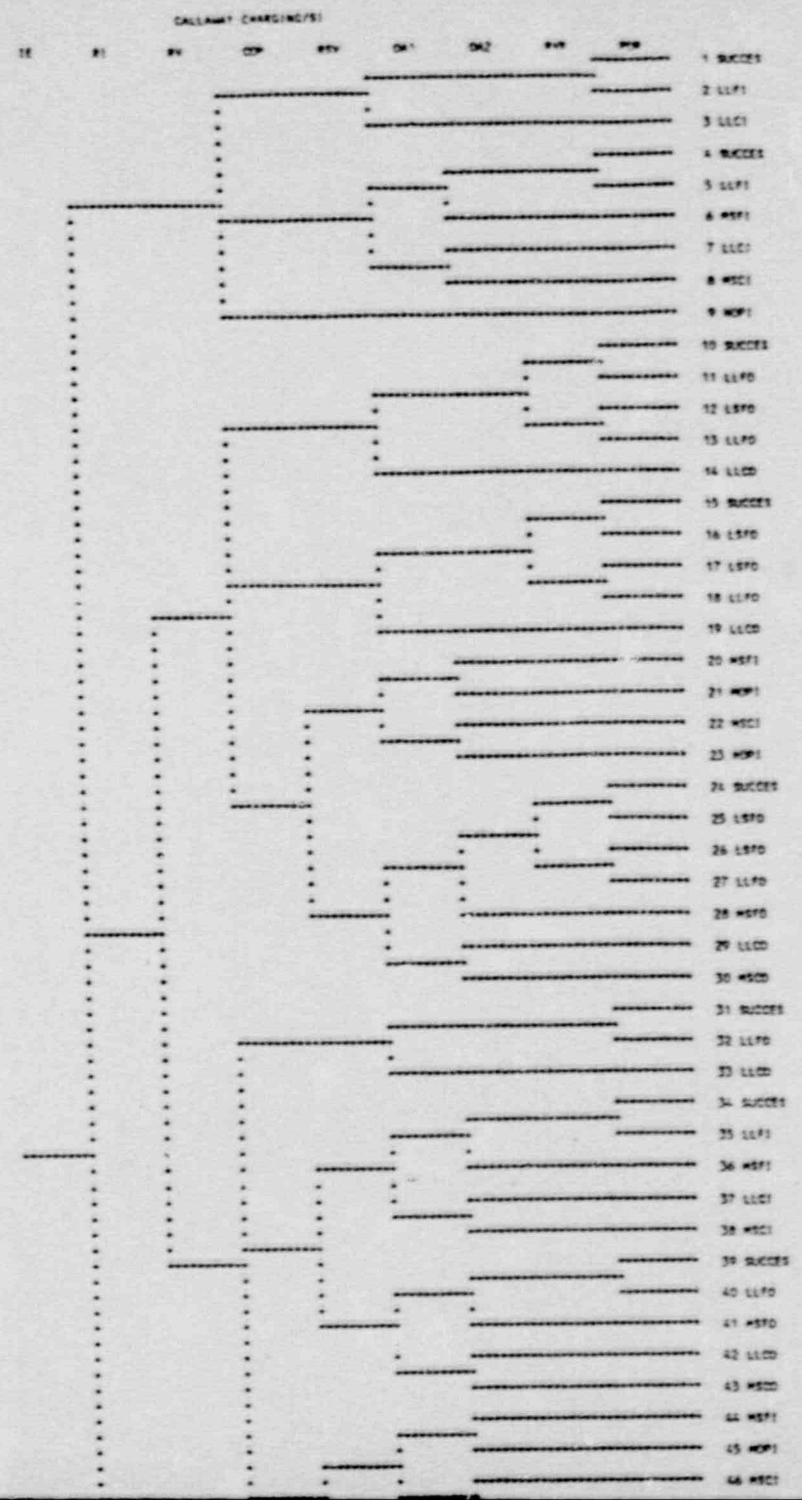
ntary Wiring Diagram
02B



PROPOSED CHANGE

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0 — 100)	CVD SH
bo	4		—	•
ac		8	—	•
bo	3		—	•
ac		7	—	
ao	2		—	
bc		6	—	
ao	1		—	•
bc		5	—	•
ac		16	—	
bo	12		—	
ac		15	—	•
bo	11		—	
bc		14	—	
ao	10		—	
bc		13	—	330
ao	9		—	
tc	17		OPENS ON OVLD ON CLOSE STRK	•
to	18		OPENS ON OLVD ON OPEN STRK	•
—— = CONT CLOSED • = THIS SHEET				

REF.
CAR 2166 B-401 SH 328
V 2443044 SH 8


CALLAWAY CHARGING/SI
1 SUCCES
2 LLF1
3 LLC1
4 SUCCES
5 LLF1
6 MSF1
7 LLC1
8 MSC1
9 MOF1
10 SUCCES
11 LLF0
12 LSF0
13 LLF0
14 LLC0
15 SUCCES
16 LSF0
17 LSF0
18 LLF0
19 LLC0
20 MSF1
21 MOF1
22 MSC1
23 MOF1
24 SUCCES
25 LSF0
26 LSF0
27 LLF0
28 MSF0
29 LLC0
30 MSC0
31 SUCCES
32 LLF0
33 LLC0
34 SUCCES
35 LLF1
36 MSF1
37 LLC1
38 MSC1
39 SUCCES
40 LLF0
41 MSF0
42 LLC0
43 MSC0
44 MSF1
45 MOF1
46 MSC1

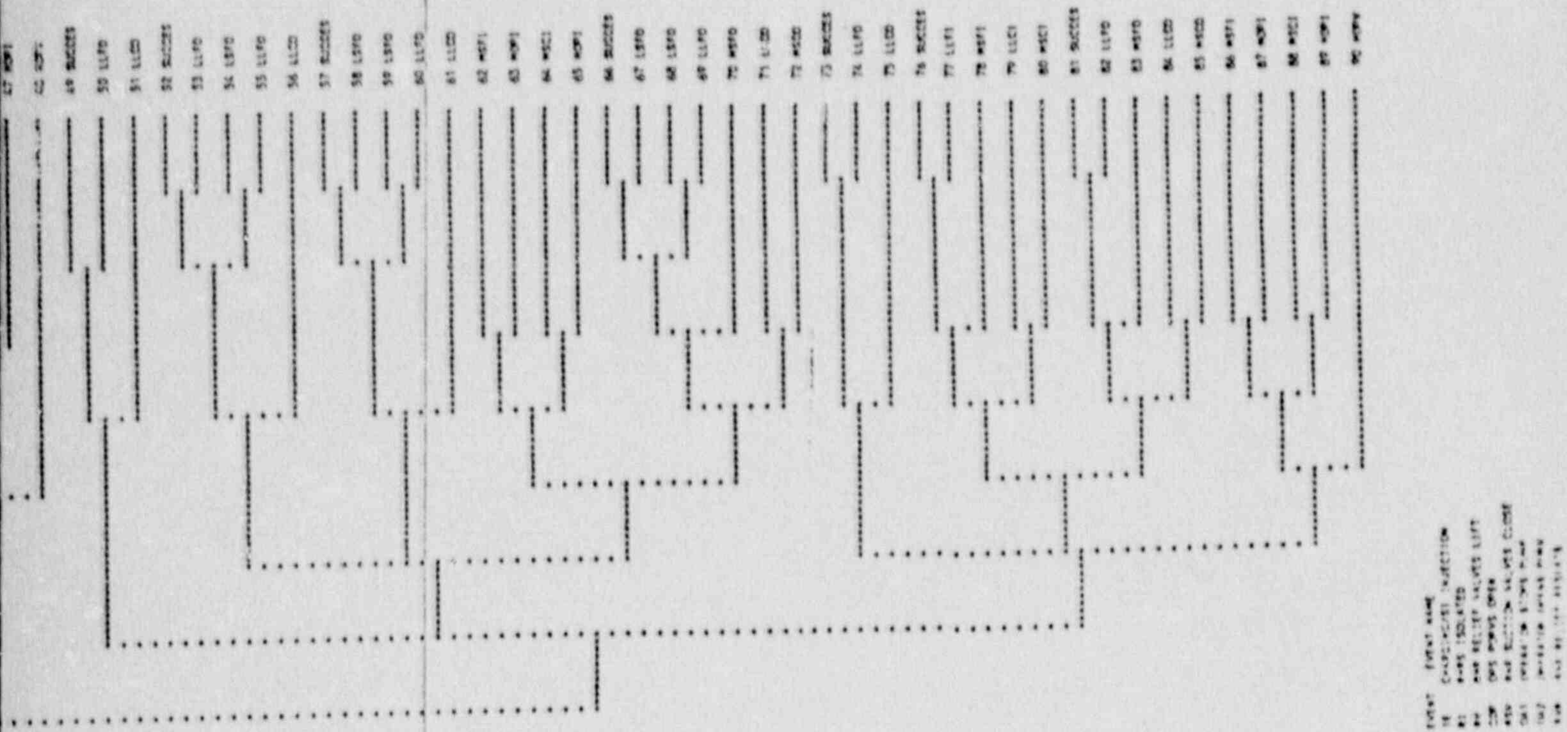


FIGURE 7-4

CHARGING/SAFETY INJECTION PUMP
ACTUATION EVENT TREE

SI
APERTURE
CARD

Also Available On
Aperture Card

8911150026-36

8.0 TECHNICAL SPECIFICATIONS

This section provides a discussion of the technical specifications with reference to the RHRS auto closure interlock feature. Proposed revisions to the technical specifications upon removal of the auto closure interlock are provided as well as marked up examples for each of the lead plants.

8.1 Current Technical Specifications

The "Standard Technical Specifications for Westinghouse Pressurized Water Reactor", NUREG-0452, DRAFT REVISION 5, is the basis for the plant specific technical specifications issued by the Commission since 1985. Plants which were licensed prior to 1985 were issued technical specifications based on earlier revisions of NUREG-0452 or had custom technical specifications. Of the four lead plants, Shearon Harris was issued technical specifications based on NUREG-0452, DRAFT REVISION 5 and the three other lead plants (Salem, North Anna and Callaway) were based on earlier revisions of NUREG-0452. None of the lead plants has custom technical specifications.

The RHRS autoclosure interlock has the potential to impact the NUREG-0452 based technical specifications in the following two places.

1. Surveillance Requirement 4.5.2.d.1 (NUREG-0452, DRAFT REVISION 5) which is required to demonstrate ECCS subsystem OPERABILITY.

2. Surveillance Requirement in the Overpressure Protection Systems specification for those plants which take credit for the RHRS suction relief valves as a means of cold overpressure protection.

ECCS OPERABILITY

Surveillance Requirement 4.5.2.d.1 (NUREG-0452, DRAFT REVISION 5) is required to demonstrate ECCS subsystem OPERABILITY. The surveillance requires that the automatic isolation and interlock function of the RHR suction/isolation valves be demonstrated OPERABLE on an 18 month interval. The Surveillance Requirement as it appears in DRAFT REVISION 5 is presented below.

4.5.2 Each ECCS subsystem shall be demonstrated OPERABLE:

a. ...

b. ...

c. ...

d. At least once per 18 months by:

1) Verifying automatic isolation and interlock action of the RHR System from the Reactor Coolant System by ensuring that:

a) With a simulated or actual Reactor Coolant System pressure signal greater than or equal to 425 psig the interlocks prevent the valves from being opened, and

b) With a simulated or actual Reactor Coolant System pressure signal less than or equal to 750 psig the interlocks will cause the valves to automatically close.

The reference plants' technical specifications have an 18 month surveillance similiar to the to the DRAFT REVISION 5 version presented above. The Salem Unit 1 Surveillance Requirement 4.5.2.i is shown in Figure 8-1. The Callaway Unit 1 Surveillance Requirement 4.5.2.d.1 is shown in Figure 8-2. The North Anna Unit 1 Surveillance Requirement 4.7.9.1.a is shown in Figure 8-3. The Shearon Harris Surveillance Requirement 4.5.2.d.1 is shown in Figure 8-4.

OVERPRESSURE PROTECTION

NUREG-0452, DRAFT REVISION 5, Specification 3/4.4.9.3, "OVERPRESSURE PROTECTION SYSTEMS", does not take credit for the RHR System suction relief valve to meet the Limiting Condition for Operation (LCO). However, several recently licensed plants have included the RHR System suction relief valves as an optional cold overpressure protection system to meet the requirements of the LCO of specification 3/4.4.9.3. When the RHR System suction relief valves are used for cold overpressure protection, an additional surveillance requirement may be necessary to ensure that a single failure of a pressure transmitter could not isolate both RHR System relief valves from the RCS when only the RHR relief valves are providing overpressure protection.

Callaway is the only reference plant that takes credit for the RHR System suction relief valves for cold overpressure protection. As such it has added Surveillance Requirement 4.4.9.3.2 which verifies that a single failure of a pressure transmitter (PT-403 or PT-405) would not isolate both drop lines of the RHR System. Figure 8-5 shows a simplified drawing of the Callaway RHR System. Each of the two drop lines from the RCS to the RHR System contain an inner isolation valve (8702A or B), an outer isolation valve (8701A or B) and a relief valve (8708A or B). The inner isolation valves are defined as those valves closest to the RCS and the outer isolation valves are defined as those valves closest to the RHR System.

The current Callaway interlock table for MOVs 8701A and B and 8702A and B is shown on Figure 8-6 (Sheet 2 of 2). The interlock functional diagrams for these valves are shown on Figure 8-6 (Sheet 1 of 2). As shown on Figure 8-6, Pressure Transmitter PT-405 serves the autoclosure interlock function for both RHRS drop line outer isolation valves while Pressure Transmitter PT-403 serves the autoclosure interlock function for both RHRS drop line inner isolation valves. With this type of arrangement, and without the added Surveillance Requirement 4.4.9.3.2, the plant could find itself in a position where the two RHRS relief valves were providing overpressure protection and a single failure of one of the pressure transmitters could isolate both drop lines and the associated RHRS relief valves.

The current Callaway Surveillance Requirement 4.4.9.3.2 (Figure 8-7) requires that the inner isolation valve for train A and the outer isolation valve for train B be open and power removed from the valve operator. This leaves the outer isolation valve for train A operable and the inner isolation valve for train B operable. The operable valves retain the RHRS autoclosure feature and will isolate on an overpressurization transient, but a single failure of a pressure instrument will not isolate both drop lines.

8.2 Proposed Revision of Technical Specifications

This section provides the technical specification revisions necessary to implement the removal of the RHRS autoclosure interlock feature at each of the four reference plants.

SALEM

The portion of the 18 month surveillance contained in specification 4.5.2.i associated with verifying that the RHRS suction/isolation valves automatically close on a RCS pressure signal should be deleted as shown in Figure 8-8. With the removal of the autoclosure interlock function, there is no longer a need to retain this surveillance requirement. It should be noted that the RHRS open permissive interlock surveillance requirement remains unchanged.

CALLAWAY

The portion of the 18 month surveillance contained in specification 4.5.2.d.1.b associated with verifying that the RHRS suction/isolation valves automatically close on a RCS pressure signal should be deleted as shown in Figure 8-9. With the removal of the autoclosure interlock function there is no longer a need to retain this surveillance requirement. It should be noted that the RHRS open permissive interlock surveillance requirement remains unchanged.

The 31 day surveillance contained in Specifications 4.4.9.3.2.a.1 and 4.4.9.3.2.b.1, verifying that the RHRS suction/isolation valve is open with power removed to the valve operator, should be deleted as shown in Figure 8-10. With the removal of the autoclosure interlock circuitry on the RHRS suction/isolation valve a failure of a pressure transmitter can not result in the valves stroking closed. Thus the postulated occurance of a single failure isolating both RHRS trains while the RHRS relief valves are providing cold overpressure protection can not occur and the surveillance requirement to open and lock-out power to the valves is redundant.

The RHRS suction/isolation valves which had been in the 31 day surveillance should be added to the 12 hour surveillance which requires the valve to be verified open as shown in Figure 8-10. This is necessary to insure that free communication exists between the RCS and the RHRS when the RHRS relief valves are providing cold overpressure protection to the RCS.

Additionally, the 12 hour surveillance interval of specification 4.4.9.3.2.a.2 and 4.4.9.3.2.b.2 should be changed to be consistent with the surveillance interval of specification 4.4.9.3.1.c for verifying that the PORV isolation valves are open when the PORV is used for overpressure protection. The change is shown in Figure 8-10.

Bases section 3/4.4.9 should be modified to delete the discussion on removing power to the RHRS suction/isolation valves as shown in Figure 8-11.

NORTH ANNA UNIT 1

The 18 month surveillance contained in Specification 4.7.9.1.a associated with verifying that the RHRS suction/isolation valves automatically close on a RCS pressure signal should be deleted as shown in Figure 8-12. With the removal of the autoclosure interlock function, there is no longer a need to retain this surveillance requirement.

SHEARON HARRIS

The portion of the 18 month surveillance contained in specification 4.5.2.d.1 associated with verifying that the RHRS suction/isolation valves automatically close on a RCS pressure signal should be deleted as shown in Figure 8-13. With the removal of the autoclosure interlock function there is no longer a need to retain this surveillance requirement. It should be noted that the RHRS open permissive interlock surveillance requirement remains unchanged.

i. The automatic isolation and interlock function of the RHR System shall be verified within the seven (7) days prior to placing the RHR System in service for cooling of the Reactor Coolant System. This shall be done by verifying that valves RH1 and RH2 close upon insertion of a test signal corresponding to a reactor coolant pressure of 580 psig or less, and that, with a test signal corresponding to a reactor coolant pressure of 580 psig or greater, that the valves cannot be opened.

SALEM UNIT 1 3/4 5-5b Amendment No. 44

Figure 8-1. Current Salem Surveillance Requirement 4.5.2.i

EMERGENCY CORE COOLING SYSTEMS

REVISION 1

SURVEILLANCE REQUIREMENTS

4.5.2 Each ECCS subsystem shall be demonstrated OPERABLE:

a. At least once per 12 hours by verifying that the following valves are in the indicated positions with power to the valve operators removed:

Valve Number	Valve Function	Valve Position
EM-HV-8813	Safety Injection to RWST Isolation Vlv	Open
EM-HV-8802A(B)	SI Pump Discharge Hot Leg Iso Vlvs	Closed
EM-HV-8835	Safety Injection Cold Leg Iso Valve	Open
EJ-HV-8840	RHR/SI Hot Leg Recirc Iso Valve	Closed
EJ-HV-8809A	RHR to Accum Inj Loops 1 & 2 Iso Vlv	Open
EJ-HV-8809B	RHR to Accum Inj Loops 3 & 4 Iso Vlv	Open

b. At least once per 31 days by:

1) Verifying that the ECCS piping is full of water by venting the ECCS pump casings and accessible discharge piping high points, and

2) Verifying that each valve (manual, power-operated, or automatic) in the flow path that is not locked, sealed, or otherwise secured in position, is in its correct position.

c. By a visual inspection which verifies that no loose debris (rags, trash, clothing, etc.) is present in the containment which could be transported to the containment sump and cause restriction of the pump suctions during LOCA conditions. This visual inspection shall be performed:

1) For all accessible areas of the containment prior to establishing CONTAINMENT INTEGRITY, and

2) Of the areas affected within containment at the completion of each containment entry when CONTAINMENT INTEGRITY is established.

d. At least once per 18 months by:

1) Verifying automatic isolation and interlock action of the RHR System from the Reactor Coolant System by ensuring that:

a) With a simulated or actual Reactor Coolant System pressure signal greater than or equal to 425 psig the interlocks prevent the valves from being opened, and

b) With a simulated or actual Reactor Coolant System pressure signal less than or equal to 750 psig the interlocks will cause the valves to automatically close.

CALLAWAY - UNIT 1 3/4 5-4

Figure 8-2. Current Callaway Surveillance Requirement 4.5.2.d.1

PLANT SYSTEMS

3/4.7.9 RESIDUAL HEAT REMOVAL SYSTEM

RHR OPERATING

LIMITING CONDITION FOR OPERATION

3.7.9.1 Two residual heat removal subsystems shall be OPERABLE.

APPLICABILITY: MODES 1, 2 and 3.

ACTION:

With one residual heat removal subsystem inoperable, restore the inoperable subsystem to OPERABLE status within 7 days or be in HOT SHUTDOWN within the next 24 hours.

SURVEILLANCE REQUIREMENTS

4.7.9.1 Each residual heat removal subsystem shall be demonstrated OPERABLE:

a. At least once per 18 months by verifying automatic isolation of the RHR system from the Reactor Coolant System when the RCS pressure is above 660 psig.

b. At least once per 18 months during shutdown by cycling each of the valves in the subsystem flow path not testable during plant operation through one complete cycle of full travel.

c. At least once per 18 months by verifying that each residual heat removal pump develops a differential pressure of ≥ 123 psi.

Figure 8-3. Current North Anna Unit 1 Surveillance Requirement 4.7.9.1.a

EMERGENCY CORE COOLING SYSTEMS

SURVEILLANCE REQUIREMENTS (Continued)

d. At least once per 18 months by:

1. Verifying automatic isolation and interlock action of the RHR system from the Reactor Coolant System by ensuring that:

a) With a simulated or actual Reactor Coolant System pressure signal greater than or equal to 425 psig the interlocks prevent the valves from being opened, and

b) With a simulated or actual Reactor Coolant System pressure signal less than or equal to 750 psig the interlocks will cause the valves to automatically close.

2. A visual inspection of the containment sump and verifying that the subsystem suction inlets are not restricted by debris and that the sump components (trash racks, screens, etc.) show no evidence of structural distress or abnormal corrosion.

e. At least once per 18 months, during shutdown, by:

1. Verifying that each automatic valve in the flow path actuates to its correct position on safety injection actuation test signal and on safety injection switchover to containment sump from an RWST Lo-Lo level test signal, and

2. Verifying that each of the following pumps start automatically upon receipt of a safety injection actuation test signal:

a) charging/safety injection pump.
b) RHR pump.

f. By verifying that each of the following pumps develops the required differential pressure when tested pursuant to Specification 4.0.5:

1. charging/safety injection pump (Refer to Specification 4.1.2.4)
2. RHR pump ≥ 100 psid at a flow rate of at least 3663 gpm.

g. By verifying that the locking mechanism is in place and locked for the following ECCS throttle valves:

1. Within 4 hours following completion of each valve stroking operation or maintenance on the valve when the ECCS subsystems are required to be OPERABLE, and

2. At least once per 18 months.

SHEARON HARRIS - UNIT 1 3/4 5-5

Figure 8-4. Current Shearon Harris Surveillance Requirement 4.5.2.d.1

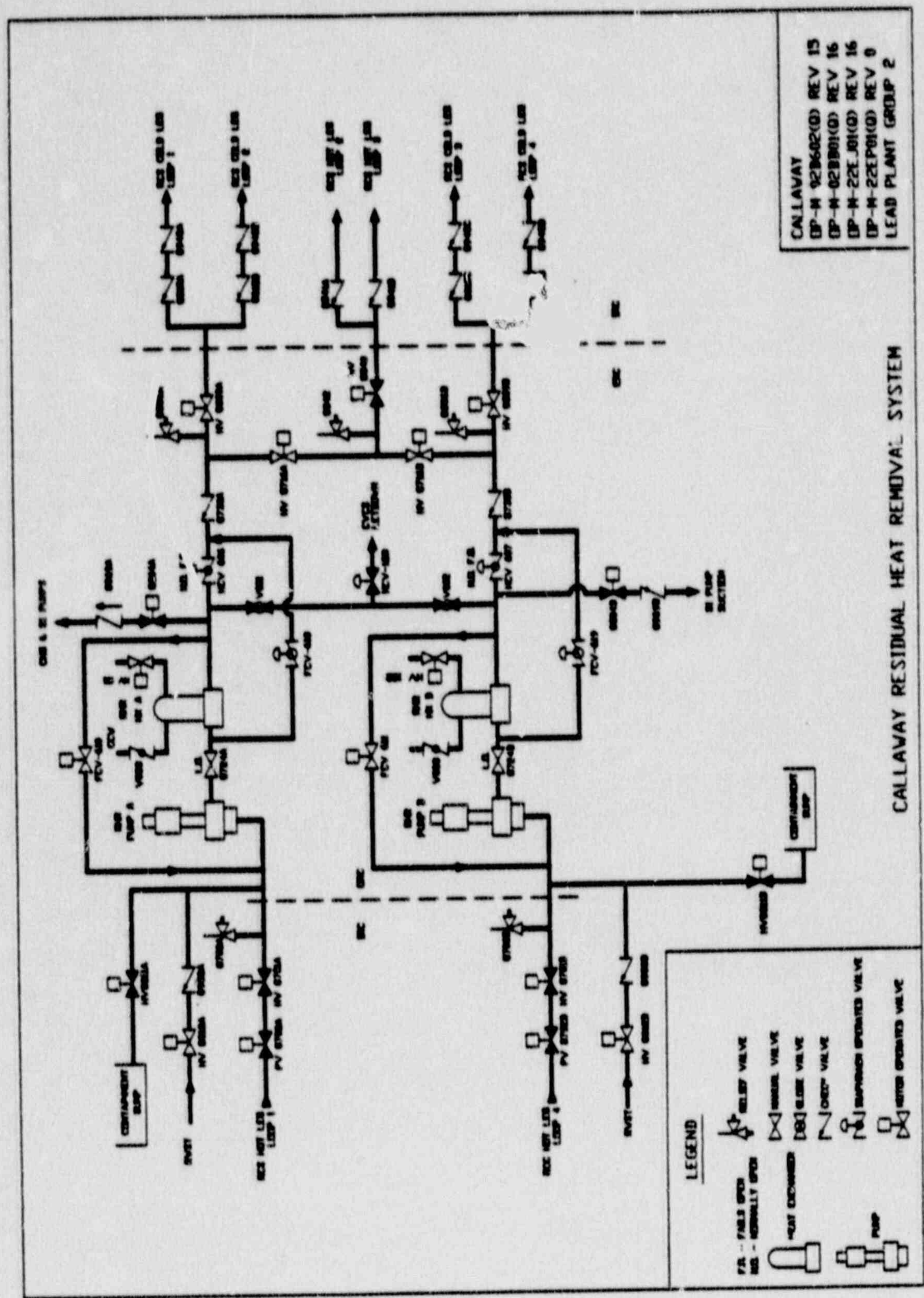
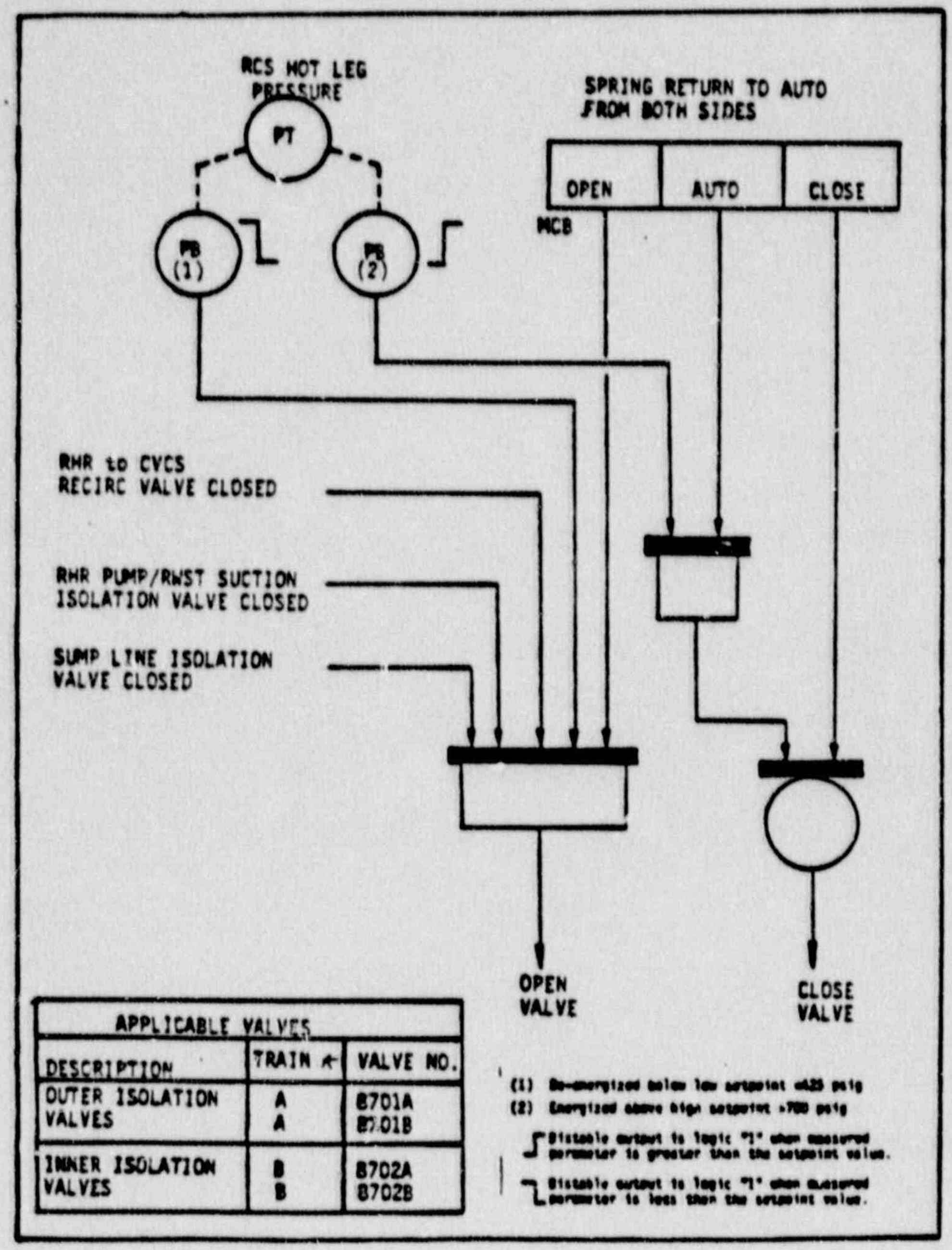


Figure 8-5. Callaway Residual Heat Removal System



APPLICABLE VALVES		
DESCRIPTION	TRAIN *	VALVE NO.
OUTER ISOLATION VALVES	A A	8701A 8701B
INNER ISOLATION VALVES	B B	8702A 8702B

*Power train assignment

Figure 8-6. Callaway Functional Diagram - Current Interlock MOVs - 8701A & B, 8702A & B (Sheet 1 of 2)

INTERLOCK TABLE - RHR OUTER ISOLATION VALVES		
PLANT	412	
Valve / Interlock with	8701A	8701B
RCS Hot Leg Pressure Channel	PT-405	PT-405
Recirculation Valve Closed/Limit Switch	8804A/#1	8804B/#2
RWST Suction Valve Closed/Limit Switch	8812A/#1	8812B/#2
Sump Line Valve Closed/ Limit Switch	8811A/#1	8811B/#2

LIMIT SWITCH #1 IS THE NORMAL POSITION SWITCH AND IS USED FOR POSITION SIGNALS BETWEEN VALVES ASSIGNED TO THE SAME TRAIN.

LIMIT SWITCH #2 IS THE STEM MOUNTED POSITION SWITCH AND IS USED FOR SIGNALS BETWEEN VALVES ASSIGNED TO OPPOSITE TRAINS.

INTERLOCK TABLE - RHR INNER ISOLATION VALVES		
PLANT	412	
Valve / Interlock with	8702A	8702B
RCS Hot Leg Pressure Channel	PT-403	PT-403
Recirculation Valve Closed/Limit Switch	8804A/#2	8804B/#1
RWST Suction Valve Closed/Limit Switch	8812A/#2	8812B/#1
Sump Line Valve Closed/ Limit Switch	8811A/#2	8811B/#1

Figure 8-6. Callaway Functional Diagram - Current Interlock MOVs - 8701A & B, 8702A & B (Sheet 2 of 2)

REVISION 1

REACTOR COOLANT SYSTEM

SURVEILLANCE REQUIREMENTS

4.4.9.3.1 Each PORV shall be demonstrated OPERABLE by:

a. Performance of an ANALOG CHANNEL OPERATIONAL TEST on the PORV actuation channel, but excluding valve operation, within 31 days prior to entering a condition in which the PORV is required OPERABLE and at least once per 31 days thereafter when the PORV is required OPERABLE;

b. Performance of a CHANNEL CALIBRATION on the PORV actuation channel at least once per 18 months; and

c. Verifying the PORV isolation valve is open at least once per 72 hours when the PORV is being used for overpressure protection.

4.4.9.3.2 Each RHR suction relief valve shall be demonstrated OPERABLE when the RHR suction relief valves are being used for cold overpressure protection as follows:

a. For RHR suction relief valve 8708B:

1) By verifying at least once per 31 days that RHR RCS Suction Isolation Valve (RRSIV) 8701B is open with power to the valve operator removed, and

2) By verifying at least once per 12 hours that RRSIV 8702B is open.

b. For RHR suction relief valve 8708A:

1) By verifying at least once per 31 days that RRSIV 8702A is open with power to the valve operator removed, and

2) By verifying at least once per 12 hours that RRSIV 8701A is open.

c. Testing pursuant to Specification 4.0.5.

4.4.9.3.3 The RCS vent(s) shall be verified to be open at least once per 12 hours* when the vent(s) is being used for overpressure protection.

*Except when the vent pathway is provided with a valve which is locked, sealed, or otherwise secured in the open position, then verify these valves open at least once per 31 days.

CALLAWAY - UNIT 1 3/4 4-35

Figure 8-7. Current Callaway Surveillance Requirement 4.4.9.3.2

i. The automatic ~~[illegible]~~ interlock function of the RHR System shall be verified within ~~the~~ seven (7) days prior to placing the RHR System in service for cooling of the Reactor Coolant System. This shall be done by verifying ~~that valves RH1 and RH2 close upon insertion of a test signal corresponding to a reactor coolant pressure of 580 psig or less, and that,~~ with a test signal corresponding to a reactor coolant pressure of 580 psig or greater, that ~~the~~ valves RH1 and RH2 cannot be opened.

SALEM UNIT 1 | 3/4 5-5b | Amendment No. 44

Figure 8-8. Proposed Salem Surveillance Requirement 4.5.2.i

REVISION 1

EMERGENCY CORE COOLING SYSTEMS

SURVEILLANCE REQUIREMENTS

4.5.2 Each ECCS subsystem shall be demonstrated OPERABLE:

a. At least once per 12 hours by verifying that the following valves are in the indicated positions with power to the valve operators removed:

Valve Number	Valve Function	Valve Position
EM-HV-8813	Safety Injection to RWST Isolation Vlv	Open
EM-HV-8802A(B)	SI Pump Discharge Hot Leg Iso Vlvs	Closed
EM-HV-8835	Safety Injection Cold Leg Iso Valve	Open
EJ-HV-8840	RHR/SI Hot Leg Recirc Iso Valve	Closed
EJ-HV-8809A	RHR to Accum Inj Loops 1 & 2 Iso Vlv	Open
EJ-HV-8809B	RHR to Accum Inj Loops 3 & 4 Iso Vlv	Open

b. At least once per 31 days by:

1) Verifying that the ECCS piping is full of water by venting the ECCS pump casings and accessible discharge piping high points, and

2) Verifying that each valve (manual, power-operated, or automatic) in the flow path that is not locked, sealed, or otherwise secured in position, is in its correct position.

c. By a visual inspection which verifies that no loose debris (rags, trash, clothing, etc.) is present in the containment which could be transported to the containment sump and cause restriction of the pump suctions during LOCA conditions. This visual inspection shall be performed:

1) For all accessible areas of the containment prior to establishing CONTAINMENT INTEGRITY, and

2) Of the areas affected within containment at the completion of each containment entry when CONTAINMENT INTEGRITY is established.

d. At least once per 18 months by:

1) Verifying automatic [illegible] interlock action of the RHR System from the Reactor Coolant System by ensuring that:

a) With a simulated or actual Reactor Coolant System pressure signal greater than or equal to 425 psig the interlocks prevent the valves from being opened. and

b) With a simulated or actual Reactor Coolant System pressure signal less than or equal to 750 psig the interlocks will cause the valves to automatically close.

CALLAWAY - UNIT 1 3/4 5-4

Figure 8-9. Proposed Callaway Surveillance Requirement 4.5.2.d.1

REVISION 1

REACTOR COOLANT SYSTEM

SURVEILLANCE REQUIREMENTS

4.4.9.3.1 Each PORV shall be demonstrated OPERABLE by:

a. Performance of an ANALOG CHANNEL OPERATIONAL TEST on the PORV actuation channel, but excluding valve operation, within 31 days prior to entering a condition in which the PORV is required OPERABLE and at least once per 31 days thereafter when the PORV is required OPERABLE;

b. Performance of a CHANNEL CALIBRATION on the PORV actuation channel at least once per 18 months; and

c. Verifying the PORV isolation valve is open at least once per 72 hours when the PORV is being used for overpressure protection.

4.4.9.3.2 Each RHR suction relief valve shall be demonstrated OPERABLE when the RHR suction relief valves are being used for cold overpressure protection as follows:

a. For RHR suction relief valve 8708B:

~~1) By verifying at least once per 31 days that RHR RCS Suction Isolation Valve (RRSIV) 8701B is open with power to the valve operator removed, and~~

~~2)~~ 1) By verifying at least once per ~~12~~ 72 hours that RRSIV 8701B and 8702B valves ~~is~~ are open.

b. For RHR suction relief valve 8708A:

~~1) By verifying at least once per 31 days that RRSIV 8702A is open with power to the valve operator removed, and~~

~~2)~~ 1) By verifying at least once per ~~12~~ 72 hours that RRSIV 8701A and 8702A valves ~~is~~ are open.

c. Testing pursuant to Specification 4.0.5.

4.4.9.3.3 The RCS vent(s) shall be verified to be open at least once per 12 hours* when the vent(s) is being used for overpressure protection.

*Except when the vent pathway is provided with a valve which is locked, sealed, or otherwise secured in the open position, then verify these valves open at least once per 31 days.

CALLAWAY - UNIT 1 3/4 4-35

Figure 8-10. Proposed Callaway Surveillance Requirement 4.4.9.3.2

REVISION 1

REACTOR COOLANT SYSTEM

BASES

HEATUP (Continued)

The use of the composite curve is necessary to set conservative heatup limitations because it is possible for conditions to exist such that over the course of the heatup ramp the controlling condition switches from the inside to the outside and the pressure limit must at all times be based on analysis of the most critical criterion.

Finally, the composite curves for the heatup rate data and the cooldown rate data are adjusted for possible errors in the pressure and temperature sensing instruments by the values indicated on the respective curves.

Although the pressurizer operates in temperature ranges above those for which there is reason for concern of nonductile failure, operating limits are provided to assure compatibility of operation with the fatigue analysis performed in accordance with the ASME Code requirements.

The OPERABILITY of two PORVs, or two RHR suction relief valves, or an RCS vent opening of at least 2 square inches ensures that the RCS will be protected from pressure transients which could exceed the limits of Appendix G to 10 CFR Part 50 when one or more of the RCS cold legs are less than or equal to 368°F. Either PORV or either RHR suction relief valve has adequate relieving capability to protect the RCS from overpressurization when the transient is limited to either: (1) the start of an idle RCP with the secondary water temperature of the steam generator less than or equal to 50°F above the RCS cold leg temperatures, or (2) the start of a centrifugal charging pump and its injection into a water-solid RCS.

RHR/RCS suction isolation valves 8701A and B are interlocked with an "A" train wide range pressure transmitter and valves 8702A and B are interlocked with a "B" train wide range pressure transmitter. Removing power from valves 8701B and 8702A, prevents a single failure from inadvertently isolating both RHR suction relief valves while maintaining RHR isolation capability for both RHR flow paths.

In addition to opening RCS vents to meet the requirement of Specification 3.4.9.3c., it is acceptable to remove a pressurizer Code safety valve, open a PORV block valve and remove power from the valve operator in conjunction with disassembly of a PORV and removal of its internals, or otherwise open the RCS.

COLD OVERPRESSURE

The Maximum Allowed PORV Setpoint for the Cold Overpressure Mitigation System (COMS) is derived by analysis which models the performance of the COMS assuming various mass input and heat input transients. Operation with a PORV setpoint less than or equal to the maximum setpoint ensures that Appendix G criteria will not be violated with consideration for 1) a maximum pressure overshoot beyond the PORV setpoint which can occur as a result of time delays in signal processing and valve opening; 2) a 50°F heat transport effect made

Figure 8-11. Proposed Callaway Bases Section 3/4.4.9

PLANT SYSTEMS

3/4.7.9 RESIDUAL HEAT REMOVAL SYSTEM

RHR OPERATING

LIMITING CONDITION FOR OPERATION

3.7.9.1 Two residual heat removal subsystems shall be OPERABLE.

APPLICABILITY: MODES 1, 2 and 3.

ACTION:

With one residual heat removal subsystem inoperable, restore the inoperable subsystem to OPERABLE status within 7 days or be in HOT SHUTDOWN within the next 24 hours.

SURVEILLANCE REQUIREMENTS

4.7.9.1 Each residual heat removal subsystem shall be demonstrated OPERABLE:

~~a.~~ ~~At least once per 18 months by verifying automatic isolation of the RHR system from the Reactor Coolant System when the RCS pressure is above 660 psig.~~

a ~~b.~~ At least once per 18 months during shutdown by cycling each of the valves in the subsystem flow path not testable during plant operation through one complete cycle of full travel.

b ~~c.~~ At least once per 18 months by verifying that each residual heat removal pump develops a differential pressure of ≥ 123 psi.

Figure 8-12. Proposed North Anna Unit 1 Surveillance Requirement 4.7.9.1.a

EMERGENCY CORE COOLING SYSTEMS

SURVEILLANCE REQUIREMENTS (Continued)

d. At least once per 18 months by:

1. Verifying automatic ~~isolation and~~ interlock action of the RHR System from the Reactor Coolant System by ensuring that~~:~~

~~a)~~ With a simulated or actual Reactor Coolant System pressure signal greater than or equal to 425 psig the interlocks prevent the valves from being opened, ~~and~~

~~b) With a simulated or actual Reactor Coolant System pressure signal less than or equal to 750 psig the interlocks will cause the valves to automatically close.~~

2. A visual inspection of the containment sump and verifying that the subsystem suction inlets are not restricted by debris and that the sump components (trash racks, screens, etc.) show no evidence of structural distress or abnormal corrosion.

e. At least once per 18 months, during shutdown, by:

1. Verifying that each automatic valve in the flow path actuates to its correct position on safety injection actuation test signal and on safety injection switchover to containment sump from an RWST Lo-Lo level test signal, and

2. Verifying that each of the following pumps start automatically upon receipt of a safety injection actuation test signal:

a) charging/safety injection pump,
b) RHR pump.

f. By verifying that each of the following pumps develops the required differential pressure when tested pursuant to Specification 4.0.5:

1. charging/safety injection pump (Refer to Specification 4.1.2.4)
2. RHR pump ≥ 100 psid at a flow rate of at least 3663 gpm.

g. By verifying that the locking mechanism is in place and locked for the following ECCS throttle valves:

1. Within 4 hours following completion of each valve stroking operation or maintenance on the valve when the ECCS subsystems are required to be OPERABLE, and

2. At least once per 18 months.

SHEARON HARRIS - UNIT 1 3/4 5-6

Figure 8-13. Proposed Shearon Harris Surveillance Requirement 4.5.2.d.1

9.0 CONCLUSIONS AND RECOMMENDATIONS

This section addresses the seven concerns expressed in the NRC internal memorandum (Reference 6) of January, 1985 stating the RSB position on requests for removal of the RHRS ACI. The memorandum stated that any proposal to remove the ACI should be substantiated by proof that the change is a net improvement in safety and should assess as a minimum the following:

1. The means available to minimize Event V concerns.
2. The alarms to alert the operator of an improperly positioned RHRS MOV.
3. The RHRS relief capacity must be adequate.
4. Means other than the ACI to ensure both MOVs are closed (e.g., single switch actuating both valves).
5. Assurance that the function of the open permissive circuitry is not affected by the proposed change.
6. Assurance that MOV position indication will remain available in the control room regardless of the proposed change.
7. Assessment of the proposed change's effect on RHRS reliability, as well as on Low Temperature Overpressure (LTOP) concerns.

Each of the seven items above will be commented on separately and reference will be made to supporting analysis contained in this report where applicable.

<u>Means Available To Minimize A LOCA Outside The Containment</u>

An interfacing systems LOCA, referred to as an Event V in WASH-1400, is a breach of the high pressure RCS pressure boundary at an interface with the low pressure piping system. An RHR System LOCA is classified as a non-mitigable LOCA outside containment. It is assumed to occur if the valves in the RHRS suction line fail open when the RCS is at normal operating pressure (2250 psia). Since the RHR System is designed for a much lower pressure (600 psig for the four reference plants), the result of both suction/isolation valves failing open is overpressurization of the RHR System. The RHR System for three of the reference plants (Harris, Salem and Callway) are located outside of containment. A gross failure of the RHR System pressure boundary for these plants is assumed to result in an uncontained LOCA. The North Anna RHR System is located inside containment and would not result in the uncontained LOCA scenario.

Each of the four reference plants has two motor operated suction/isolation valves on the hot leg suction line from the RCS. These valves on each suction line serve as the primary Reactor Coolant System pressure boundary. They are remotely operated from the Main Control Room, and are powered by separate Class 1E electrical power sources. Continuous valve position indication is provided from the valve stem mounted limit switches with indication in the Main Control Room. Plant operating procedures instruct the operator to isolate the RHRS during plant heatup, so the likelihood of these valves being left open is remote. Additionally, this report recommends the installation of a Main Control Room alarm to alert the operator if a RHRS suction/isolation valve is not fully closed in conjunction with a "RCS PRESSURE HIGH" signal (see sections 6.1 through 6.4).

The following factors were among those not considered in the supporting frequency of an interfacing systems LOCA analysis in Modes 1, 2 and 3, but are worth mentioning as they contribute to the means available to minimize a LOCA outside of containment.

1. Both RHRS suction/isolation valves have the power removed from the operators during Modes 1, 2 and 3. The four reference plants all have procedures that require that the power be removed from the control circuitry by opening and locking open the circuit breakers. This prevents opening of the valves in these modes.

2. The suction/isolation valves retain the Open Permissive Interlocks (Sections 5.1.3.1, 5.2.3.1, 5.3.3.1 and 5.4.3.1) which prevent the valves from being opened whenever the RCS pressure is greater than the plant specific setpoint (Salem = 390 psig, Callaway = 360 psig, Shearon Harris = 363 psig, and North Anna = 418 psig). This interlock precludes operator error associated with inadvertently opening the suction/isolation valves in Modes 1, 2 and 3.

3. It is highly unlikely that a suction/isolation valve motor operator is of sufficient size to stroke the valve open against the high differential pressure developed across the valve when the plant is at normal operating pressures in Modes 1, 2, or 3.

Should a pressure peak occur in the RCS while the RHRS suction/isolation valves are open, the pressure effect on the low pressure RHR System would be mitigated by the RHRS suction line relief valves. These relief valves discharge inside containment to the pressurizer relief tank (PRT). A discharge would be detected by high temperature, level, and pressure alarms in the PRT. The deletion of the ACI feature has no effect on the ability of the RHR System to survive pressure transients when the RHRS is connected to the RCS, since the RHRS suction/isolation valves are slow acting and no credit is currently taken for their actuation.

The frequency of an interfacing systems LOCA in modes 1, 2 and 3 without the ACI feature is reduced for all the reference plants. The interfacing system LOCA frequencies, with and without the ACI feature, for the four reference plants are presented in Table 7-2 and the analysis is described in Section 7.3. The reduction in the frequencies for the four reference plants are:

Plant	Percent Change
SALEM	-31
CALLAWAY	-24
NORTH ANNA	-38
SHEARON HARRIS	-20

As mentioned above, North Anna's RHR System is located inside containment; thus, no LOCA would occur outside containment even with removal of the autoclosure interlock.

In conclusion, sufficient means are available to minimize a LOCA outside of containment and removal of the ACI feature is desirable in that it reduces the frequency of interfacing systems LOCA in Modes 1, 2 and 3.

Alarms To Alert The Operator Of An Improperly Positioned RHRS Isolation Valve

The proposed interlocks and functional requirements for the four reference plants (Sections 6.1, 6.2, 6.3 and 6.4) recommends the addition of an alarm for each suction/isolation valve that will actuate in the Main Control Room given a "VALVE NOT FULLY CLOSED" signal in conjunction with a "RCS PRESSURE-HIGH" signal. The proposed Elementary Wiring Diagram modifications to the individual valve control circuitry is presented in Section 6. The intent of the alarms is to alert the operator that a RCS-RHRS, series, suction/isolation valve(s) is not fully closed, and that double valve isolation from the RCS to the RHRS is not being maintained. Valve position indication to the alarm should be provided from the valve stem mounted limit switches (SMLS) and power to the SMLS must not be affected by power lockout to the valve. As with other power lockout valves, there is no requirement for opposite train power for the SMLS, only that power to the SMLS is not affected by the power lockout.

This alarm meets the intent of the requirements of Regulatory Guide 1.139, "Guidance For Residual Heat Removal" which states that it is the regulatory position on RHRS isolation that..."Alarms in the control room should be provided to alert the operator if either valve is open when the RCS pressure exceeds RHR System design pressure". Establishing a setpoint for the alarm to alert the operator of an improperly positioned (i.e. open) RHR suction valve during startup operations, is a plant-specific concern. It is dependent on the open permissive pressure setpoint, the RHR system design pressure, and the operating pressure at which a plant isolates the RHRS during startup operations. The alarm setpoint can be set to a pressure significantly lower than the current ACI setpoint. A general rule for establishing the alarm septoint, is that the setpoint pressure be within the range of the open permissive setpoint pressure and, the RHR system design pressure minus the RHR pump head pressure.

P (open permissive setpoint) < alarm setpoint) <
[P (RHR system design pressure) - P (RHR pump discharge head)]

Verification Of The Adequacy Of RHRS Relief Valve Capacity

The intent of this section of the report is to review the RHRS relief valves' sizing design basis and verify that the relief valves provide RHRS overpressure protection for the design basis event. Additional potential RHRS/RCS overpressurization transients will be evaluated as part of the WOG COMS Deletion Program. Refer to WCAP-11640 for additional RHRS/RCS overpressurization analyses.

RHRS RELIEF VALVE CAPACITY - SALEM

The Salem Residual Heat Removal System (RHRS) is protected from inadvertent overpressurization by various code relief valves located in the system. Of these, primary protection is provided by the suction line relief valve, located in the suction line from the RCS hot leg. The main purpose of the RHRS relief valve in the RHRS suction header is to protect the RHRS from overpressurization during residual heat removal operation. The relief valves' sizing design basis assumed the following limiting RHRS overpressurization event: the RCS is water solid, and the control valves in the charging and seal injection lines fail fully open and the letdown line control valve fails closed. This causes a mass addition to the RCS, thus pressurizing the RCS and RHRS. Based on this event, the RHRS relief valve was sized to relieve the combined flow of all the charging pumps (which is 2 for Salem) at the valve set pressure. The set pressure of the relief valve is 450 psig with a 10% accumulation. This set point considers the additional pressure boost of the downstream RHRS pumps in maintaining the 660 psig (110% of design pressure as required by the ASME Code Section NC-7311) design overpressure limit of the RHR System.

Based on the above discussion the Salem relief valves are designed to relieve 900 gpm of 400°F water, relieving to a maximum allowable backpressure of 50 psig at a valve setpressure of 450 psig (plus 10% accumulation).

Calculations have determined that the maximum flowrate into the RCS through the charging lines from the centrifugal charging pumps

(2 pumps) is 227,278 lb/hr at the RHRS relief valve setpressure (495 psig = 450 psig + 10% accumulation). Under cold conditions (i.e., 100°F) 227,278 lb/hr is equivalent to 457 gpm. Under hot conditions (i.e., 450 psig at 400°F) 227,278 lb/hr is equivalent to 527 gpm. The RHRS relief valve provided for Salem is therefore sufficient to limit system overpressurization for the valve design basis event provided the valve design conditions are met (e.g., 450 psig setpressure, 50 psig maximum allowable backpressure).

RHRS RELIEF VALVE CAPACITY - CALLAWAY

The Callaway Residual Heat Removal System (RHRS) is protected from inadvertent overpressurization by various code relief valves located throughout the system. Of these, primary protection is provided by individual suction line relief valves, located in each subsystem's RHRS pump suction line from the associated RCS hot leg. The main purpose of the RHRS relief valves is to protect the RHRS from overpressurization during residual heat removal operation. The relief valves' sizing design basis assumed the following RHRS overpressurization event: two events were analyzed in determining the RHRS suction relief valves' sizing requirements. The first case evaluated the Reactor Coolant System (RCS) in the initial phase of RHRS cooldown. RCS temperature and pressure are 350°F and 450 psig respectively and one charging pump is in operation. The operator initiates RHRS operation by opening one suction line and starts the pump. At this point a complete loss of plant air occurs, and the charging line flow control valve fails open and the letdown flow control valve fails closed. The second case evaluated the RCS in the last part of cooldown. RCS temperature and pressure are less than 200°F and 450 psig respectively and two charging pumps are in operation. Only one RHRS train is on line and a loss of plant air occurs causing the charging line flow control valve to fail open and the letdown flow control valve to fail closed.

These two postulated events cause a mass addition to the RCS, thus pressurizing the RCS and RHRS. Based on these events, the RHRS relief valve was sized to pass the flow obtained with one charging pump operation at hot conditions, or two charging pumps operating at cold conditions.

Based on the above requirements the Callaway relief valves are designed to relieve 1) 475 gpm of 375°F water, relieving to a maximum allowable backpressure of 185 psig at a valve setpressure of 450 psig (plus 10% accumulation) or 2) 770 gpm of <200°F water, relieving to a maximum allowable backpressure of 120 psig at a valve setpressure of 450 psig (plus 10% accumulation). The set pressure of the relief valve, 450 psig with 10% accumulation, considers the additional pressure boost of the downstream RHRS pumps in maintaining the 660 psig (110% if design pressure as required by the ASME Code Section NC-7311) design overpressure limit on the RHR System.

Calculations have determined that the maximum flowrate into the RCS through the charging lines from one charging pump is 204,899 lb/hr at the RHRS relief valve setpressure (495 psig = 450 psig x 1.1). Under the relief valves' design basis "hot" condition (375°F and 450 psig) 204,899 lb/hr is equivalent to 467 gpm. Therefore, for the first RHRS relief valve design case (one charging pump flow at hot conditions), the relief valve design flowrate of 475 gpm at 375°F exceeds the required flowrate of 467 gpm and therefore prevents system overpressurization.

It has also been estimated that the maximum flowrate into the RCS through the charging lines from two charging pumps is approximately 266,567 lb/hr. Under the relief valves' design basis "cold" condition (200°F and <450 psig) 266,567 lb/hr is equivalent to 552 gpm. Therefore, for the second RHRS relief valve design case (two charging pumps flow at cold conditions), the relief valve design flowrate of 770 gpm at <200°F exceeds the required flowrate of 552 gpm, and therefore, prevents system overpressurization.

RHRS RELIEF VALVE CAPACITY - NORTH ANNA

The North Anna Residual Heat Removal System (RHRS) is protected from inadvertent overpressurization by code relief valves located on each RHRS pumps suction line from the RCS hot leg. The main purpose of the RHRS relief valves in the RHRS pump suction headers is to protect the RHRS from overpressurization during residual heat removal operation. The relief valves' sizing basis assumed the following limiting RHRS overpressurization event: the RCS is water solid, and the control valves in the charging and seal injection lines fail fully open and the letdown line control valve fails closed. This causes a mass addition to the RCS, thus pressurizing the RCS and RHRS. Based on this event, the RHRS relief valve was sized to relieve the combined flow of all charging pumps (which is 3 for North Anna) at the valve setpressure. The set pressure of the relief valve is 467 psig with a 10% accumulation. This set point considers the additional pressure boost of the downstream RHRS pumps in maintaining the 660 psig (110% of design pressure as required by the ASME Code Section 7311) design overpressure limit of the RHR System.

In order to meet the above criteria the North Anna relief valves are each designed to relieve 900 gpm of 400°F water, relieving to a maximum allowable backpressure of 50 psig at a valve setpressure of 467 psig (plus 10% accumulation).

RHRS RELIEF VALVE CAPACITY - SHEARON HARRIS

The Shearon Harris Residual Heat Removal System (RHRS) is protected from inadvertent overpressurization by various code relief valves located throughout the system. Of these, primary protection is provided by individual suction line relief valves, located in each subsystem's RHRS pump suction line from the associated RCS hot leg. The main purpose of the RHRS relief valve is to protect the RHRS from overpressurization during residual heat removal operation. The relief valves' sizing design basis assumed the following limiting RHRS overpressurization event: the RCS is water solid, and the control valves in the charging and seal injection lines fail fully open and the letdown line control valve fails closed. This causes a mass addition to the RCS, thus pressurizing the RCS and RHRS. Based on this event, the RHRS relief valves were sized to relieve the combined flow of all the charging pumps (which is 3 for Shearon Harris) at the relief valve setpressure. The setpressure of the relief valves is 450 psig with a 10% accumulation. This setpoint considers the additional pressure boost of the downstream RHRS pumps in mainintaining the 660 psig (110% of design pressure as required by the ASME Code Section NC-7311) design overpressure limit of the RHR System.

Based on the above requirements the Shearon Harris relief valves are designed to relieve 900 gpm of 400°F water, relieving to a maximum allowable backpressure of 50 psig at a valve setpressure of 450 psig (plus 10% accumulation).

Calculations have determined that the maximum flowrate into the RCS through the charging lines from the centrifugal charging pumps (3 pumps) is 333,209 lb/hr at the RHRS relief valve setpressure (495 psig = 450 psig x 1.1). Under cold conditions (i.e., 100°F) 333,209 lb/hr is equivalent to 670 gpm. Under hot conditions (450 psig at 400°F) 333,209 lb/hr is equivalent to 773 gpm. The RHRS valve on each RHRS pump suction header is therefore sufficient to limit system overpressurization for the valve design basis event provided the valve design conditions are met (e.g., 450 psig setpressure, 50 psig maximum allowable valve backpressure).

<u>Means Other Than Autoclose Interlocks to Ensure Both Isolation Valves Are Closed (e.g. Single Switch Actuating Both Valves)</u>

Current operating instructions, along with redundant position indication and the proposed alarm, are sufficient to insure isolation. The addition of a single switch to close both valves would prevent the cycling of individual suction/isolation valves. This could require some plants to lift leads and add jumpers during surveillance leak testing as required by technical specifications or valve maintenance. The location of the hand switches (for both valves) is generally such that they are near enough to each other on the Main Control Board to ensure timely operator action. Additionally, verification of valve closure could be better obtained by procedural controls such as removing power to the valves before conducting leak tests on both valves. This procedural control would provide positive assurance that the valves remain closed during pressurization to normal operating conditions.

Each plant will be expected to review their operating procedures to determine the continued applicability of the procedures and to make any changes necessary, to ensure continued safe operation without the ACI. A review of plant operating procedures should be conducted to determine the effect of removing the autoclosure interlock and installing a control room alarm. Listed below are a few of the general procedures that may require modification.

- RHRS operating procedure.
- Plant startup from cold shutdown operating procedure(s).
- Plant shutdown from hot standby operating procedure(s).
- Alarm surveillance procedures (to include the new alarm).
- Leak rate testing procedures (caution regarding alarms and power removal from RHR suction valves).

In addition, the alarm response procedure used during startup of the plant should be modified to reflect the appropriate (new) alarm recognition and responses for the added alarm. The procedure should be revised to direct the operator to take the necessary actions to close the open RHR suction valve(s), if they are not closed following alarm actuation during normal startup operations. If this is not possible, the operator should be instructed to not pressurize further and return to the safe shutdown mode of operation.

<u>Assurance That the Open Permissive Circuitry is Neither Removed or Affected by the Proposed Change</u>

The proposed design change as described in Sections 6.1 through 6.4 of this report leaves the open permissive circuit intact. Hardware changes are limited to removal of the ACI portion of the valve control circuitry and the addition of an alarm. Neither one of these changes should affect the operation of the RHRS open permissive interlock.

<u>Assurance That Isolation Valve Position Indication Will Remain Available in the Control Room Regardless of the Proposed Change</u>

The proposed design change as described in Sections 6.1 through 6.4 of this report leaves the valve position indication at the main control board intact. This indication will be provided by two means:

1) continuous valve position indication (MCB status lights)

2) absence of the alarms provided with the autoclosure interlock removal.

<u>Assessment of the Effect of the Proposed Change on RHRS Availability, as Well as Low Temperature Overpressure Protection</u>

RHRS UNAVAILABILITY ANALYSIS

The availability of the RHRS to remove decay heat was considered in three phases for the RHRS Unavailability Analysis for each of the four reference plants. The first phase covers the period during which the RHRS is placed into service and goes through a warm-up period needed to minimize the thermal shock to the system and insure boron mixing. The second phase covers the initial period of cooldown when the decay heat load is high. During this phase, two trains of RHRS (two pumps and two heat exchangers) are assumed to be required for 72 hours. The third phase covers the final long-term period of cooldown when the heat load is smaller. For this phase only one train of RHRS (one pump and one heat exchanger) is required to be in operation. Six weeks was the time period assumed for this phase (based on the average refueling outage time period). The failure probabilities of RHRS unavailability without the ACI feature are reduced for all four reference plants for two of three phases and remains constant for the RHRS initiation phase. The failure probabilities of RHRS, with and without the ACI feature, for the four reference plants are presented in Table 7-3 and the analysis is described in Section 7.4. The reduction in the failure probabilities for the four reference plants are:

Plant	Percent Change
SALEM	
RHR INITIATION	0
SHORT TERM COOLING	-13
LONG TERM COOLING	-67
CALLAWAY	
RHR INITIATION	0
SHORT TERM COOLING	-12
LONG TERM COOLING	-70
NORTH ANNA	
RHR INITIATION	0
SHORT TERM COOLING	-12
LONG TERM COOLING	-66
SHEARON HARRIS	
RHR INITIATION	0
SHORT TERM COOLING	-10
LONG TERM COOLING	-66

The removal of the autoclosure interlock increases the availability of the RHRS to remove decay heat during cold shutdown for all four reference plants. This increase is due to the reduction in spurious closures of the suction valves due to the autoclosure interlock. This effect is particularly critical during long term decay heat removal.

OVERPRESSURIZATION ANALYSIS

The effect of an overpressure transient at cold shutdown conditions will be altered by the removal of the RHRS ACI feature. An overpressurization analysis was conducted (Section 7.5) which used event trees to model the mitigating actions (both automatic and manual) following the occurrence of low temperature overpressurization events. These mitigating actions affect the severity of the overpressurization events and reduce the possibility of damage to the plant. The analysis was conducted in two parts: 1) determination of the frequency of cold overpressurization events and 2) the effect of mitigation on the transients. Ten initiating events which fell into two broad categories, heat input transients and mass input transients, were considered (Section 7.5.1).

For the heat input transients considered the pressure peak is either acceptably low with reference to the RHRS suction relief valves or the transient proceeds so quickly that the RHRS ACI could not cause the slow acting RHRS suction/isolation valve to close in time to affect the transient. The analysis concludes that the removal of the RHRS ACI feature will have no effect on the heat input transients.

For the slower mass input transients event trees were utilized to model the mitigating actions that occur following the transients. Operator actions and mitigating systems were included in the event trees. Success criteria for each event tree top event were developed and system/component failure probabilities were calculated for each of the four reference plants (Appendix D).

For the mass input transients there was a slight increase in some consequence categories for all four reference plants, but the increases were in the range of 1E-10 to 1E-12 per shutdown year. These frequency increases are not considered significant. The major impact with respect to overpressure concerns is that the removal of the RHRS ACI feature will significantly reduce the number of letdown isolation transients, which is a desired result for plants using the RHRS and the CVCS for pressure control when in solid plant operation.

10.0 APPLICABILITY OF RESULTS TO OTHER WOG PLANTS

The intent of this section is to describe how the analyses and results for the four reference plants can be utilized by other WOG plants. The objective of the utilization of four reference plants is to obtain NRC acceptance (SER) of the concept and methodology to justify removal of the autoclosure interlock. It is expected that NRC approval of this program would then greatly facilitate any plant specific effort which could reference one of the lead plants' analyses and conclusions.

The basic information presented in this report can be utilized in any plant specific effort. The literature review and licensing basis remain the same for all WOG plants. The probabilistic models and data base can be utilized as a basis for the plant specific effort. The recommended changes to the technical specifications may be also pertinent. The only aspects that require review are the differences between the plant under review and the reference plant for its category. The following describes the process for comparison of the plant and the applicable reference plant.

The first step involves the determination of the differences between the plant under review and the reference plant for its category. This includes an examination of the control wiring diagrams for the RHR suction valves, the suction valves' logic diagrams, the RHR system configuration and other information. Differences such as components within the control circuitry should be noted along with differences in the system configuration such as additional valves, crossties, etc. This step is necessary because each component is included in the probabilistic models. Some of the examples include:

1) utilization of pressurizer vapor space temperature in the interlock circuitry;

2) presence of alarms indicating position of RHR suction valves;

3) no use of the pressurizer PORVs for cold overpressure protection;

4) presence of three motor operated valves on the RHR suction line;

5) presence of three trains of RHR.

Differences in operating procedures and technical specifications should also be noted.

Another aspect that must be reviewed are the assumptions utilized in the probabilistic analyses. The applicability of these assumptions to the plant can greatly impact the results. If these assumptions are not applicable, some reanalysis would be required.

After the differences between the plant and the reference plant have been identified, the extent of any additional analyses can be determined. If only minor differences have been identified, the reference plant analyses may be bounding and no probabilistic requantification would be necessary. However, if the differences would adversely impact the probabilistic analyses, some reanalysis and requantification would have to be performed.

The following provides an example of what the plant specific analyses should entail.

ANY ADDITIONAL LOGIC MODIFICATIONS

If any new logic other than the recommended generic logic modification is needed, it must be prepared along with the recommended changes to the elementary wiring diagrams. This step is crucial because the recommended wiring diagram changes provide the basis for the probabilistic analyses and this analysis will be the determining factor in any recommendation for removal of the autoclosure interlock.

INTERFACING SYSTEMS LOCA MODEL

The model developed in the generic phase of this program must be reviewed against the plant's configuration to determine if the generic analyses is applicable to the plant. Any discrepancies between the generic plant configuration and the plant must be incorporated into the model and the frequency of an interfacing systems LOCA with and without the autoclosure interlock must then be recalculated.

ADEQUATE RHR RELIEF VALVE CAPACITY

If the autoclosure interlock is removed, the RHRS should not be overpressurized if the pressure increases during cold shutdown. The RHR relief valves should provide adequate protection for the RHRS. Applicable design base analyses of the adequacy of the RHR relief valve must be reviewed and a determination as to the validity of this information should be made.

LOW TEMPERATURE OVERPRESSURE TRANSIENTS

The transients identified as potential overpressure sources must be examined in order to determine if any abnormal events could occur at the plant if the autoclosure interlock are removed. The detailed analysis should employ the utilization of the probabilistic models to show the impact of the transients. Event trees depicting the initiating transient and the systems available to mitigate the overpressure transient (both manual and automatic) should be restructured and requantified, if necessary. Assumptions with respect to the possibility of an interfacing systems LOCA occurring must also be incorporated into the event trees. The event trees must be quantified for the present configuration and for the proposed modification in order to evaluate the trade-offs involved in the autoclosure modification.

RHRS AVAILABILITY

The models developed in the generic program should be modified to show any differences in plant configurations between the plant being analyzed and the WOG reference plant. The availability of the RHR system must be quantified for three phases of RHR operation - startup of the RHR system, short term cooling and long term cooling to allow for a detailed assessment of the spurious closure of the isolation valves over different time spans.

TECHNICAL SPECIFICATIONS

The plant's technical specifications must be reviewed to determine the impact of removal of the autoclosure interlock.

REPORT DOCUMENTATION

A detailed report should be provided summarizing the findings and conclusions reached in the analyses. As a minimum, the report should contain the following information:

1. Description of the differences between the plant and the reference plant in the generic portion.

2. Summary of potential initiating overpressurization transients.

3. Quantification of initiating frequencies for overpressurization transients.

4. Critical assumptions used in analysis.

5. Data used for all calculations.

6. Overpressurization event tree modeling with and without autoclosure feature.

7. Results of overpressurization event tree quantification.

8. Results of interfacing systems LOCA assessment.

9. Results of the evaluation on RHR system availability.

10. Recommendations concerning removal of the RHRS autoclosure feature.

11. Recommended logic changes and additions.

12. Results of the verification regarding the adequacy of the RHR relief valve to mitigate overpressure transients.

13. Written documentation that will insure the open permissive circuitry is neither removed or affected by the proposed change and that isolation valve position indication will remain available in the control room.

14. Responses to the seven NRC issues mentioned earlier in this report and Reference 6.

15. Revised technical specifications.

11.0 REFERENCES

1. U.S. Nuclear Regluatory Commisssion, Office for Analysis and Evaluation of Operational Data, Case Study Report AEOD/C503 "Decay Heat Removal Problems at U.S. Pressurized Water Reactors", December 1985.

2. Nuclear Safety Analysis Center/Electric Power Research Institute, "Residual Heat Removal Experience Review and Safety Analysis, Pressurized Water Reactors," NSAC-52, January 1983.

3. Institute of Nuclear Power Operations, "Loss or Degradation of Residual Heat Removal Capability in PWRs: Significant Operating Experience Report 85-4," August 1985.

4. D.R. Gallup, D.M. Kunsman, M.P. Bohn, Sandia National Laboratories, "Potential Benefits Obtained by Requiring Safety-Grade Cold Shutdown Systems," USNRC Report NUREG/CR-4335, November 1985.

5. Memorandum from H.R. Denton, NRC to R.M. Bernero, "Schedule for Resolving and Completing Generic Issue No. 99--RCS/RHRS Suction Line Interlocks on PWRs," August 13, 1985.

6. Memorandum from B.W. Sheron, NRC to RSB members, "Auto Closure Interlocks for PWR Residual Heat Removal (RHR) Systems," January 28, 1985.

7. WCAP-11117, Revision 1, "Residual Heat Removal System Autoclosure Interlock Removal Report For Diablo Canyon Nuclear Power Plant", N.L. Burns, T.J. Gerlowski, R.M. Malinchak, November 1986.

8. "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-75/087, Branch Technical Position ICSB-3, September 1975.

9. Wisconsin Public Service Corporation letter, E. W. James to J.F. O'Leary (AEC), Subject: Abnormal Occurrence Report, Docket 50-305, October 4, 1974.

10. "Safety Evaluation Report by the Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, in the Matter of Westinghouse Electric Company Reference Safety Analysis Report RESAR-41, Docket No. STN 50-480," NUREG-75/103, December 31, 1975, pp 5-17 to 5-19, 7-15, 7-16, and Appendix C.

11. Nuclear Regulatory Commission letter, R. W. Reid to R. H. Grace (Yankee Atomic Electric Company), Docket 50-309, August 22, 1977.

12. Advisory Committee on Reactor Safeguards letter, D. W. Moeller, Chairman to M. A. Rowden (Chairman NRC), Subject: Report on Westinghouse Electric Corporation Reference Safety Analysis Report, RESAR-3S, July 14, 1976.

13. Westinghouse Nuclear Service Division Technical Bulletin, Subject: Residual Heat Removal Pump, NSD-TB-77-7, Pittsburgh, Pennsylvania, July 15, 1977.

14. "Staff Discussion of Fifteen Technical Issues listed in attachment to November 3, 1976 memorandum from Director, NRR, to NRR Staff," NUREG-0138, U.S. Nuclear Regulatory Commission, November 1976, Issue 15.

15. Casto, William R., "Reactor-Vessel Pressure Transients," Nuclear Safety, Vol. 18, No. 4, July-August 1977, pp 513-519.

16. American National Standard, "Overpressure Protection of Low Pressure Systems Connected to the Reactor Coolant Pressure Boundary," ANSI/ANS-56.3-1977, American Nuclear Society, LaGrange Park, Illinois, April 7, 1977.

17. Haried, J. A., "Evaluation of Events Involving Decay Heat Removal Systems in Nuclear Power Plants," NUREG/CR-2799 (ORNL/NSIC-209), Oak Ridge National Laboratory, Oak Ridge, Tennessee, July 1982.

18. Nuclear Regulatory Commission Memorandum, to R. Mattson, "RHRS Interlocks for Westinghouse Plants," April 17, 1984.

19. A. D. Swain and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application," NUREG/CR-1278, August 1983.

20. IDCOR, "Individual Plant Evaluation Methodology for Pressurized Water Reactors," Technical Report 86.3A1, April 1987.

21. R. A. Bari, et. al., "Probabilistic Safety Analysis Procedures Guide," NUREG/CR-2815, Volume 1, Revision 1, August 1985.

22. IEEE, "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability DAta for Nuclear-Power Generating Stations," IEEE Std. 500-1984.

23. "Military Handbook, Reliability Prediction of Electronic Equipment," MIL-HDBK-217D, January 15, 1982.

24. IDCOR, "Evaluations of Containment Bypass and Failure to Isolate Sequences for the IDCOR Reference Plants," Technical Report 23.5, August 1986.

25. "Licensed Operating Reactors, Status Summary Report, Data as of 11-30-86," NUREG-0020, Vol. 10, No. 12, December 1986.

26. R. W. Fleming, "COMS - Cold Overpressure Mitigating System," WCAP-10529, February 1984 [Proprietary].

27. Letter from Harry Rood (NRC) to J. D. Shiffer (PG&E), "Safety Evaluation of Removal of RHR Autoclosure Interlock Function and Installation of an Alarm at Diablo Canyon Units 1 and 2, February 17, 1988.

RESIDUAL HEAT REMOVAL SYSTEM AUTOCLOSURE INTERLOCK REMOVAL REPORT FOR THE WESTINGHOUSE OWNERS GROUP

Revision 0.0

October 1989

N. B. Closky
K. J. King
P. M. McHale
C. A. Marmo

Prepared by Westinghouse Electric Corporation for use by members of the Westinghouse Owners Group. Work performed under Shop Order MUHP-2054, under the direction of the Technical Specification Subcommittee.

Westinghouse Electric Corporation
Power Systems
P.O. Box 355
Pittsburgh, Pennsylvania 15230

TABLE OF CONTENTS

Volume 1

TABLE OF CONTENTS (CONTINUED)

Volume I

TABLE OF CONTENTS (CONTINUED)

Volume 1

TABLE OF CONTENTS (CONTINUED)
Volume II

APPENDIX A

OVERVIEW OF FAULT TREE AND EVENT TREE QUANTIFICATION

APPENDIX A

OVERVIEW OF FAULT TREE AND EVENT TREE QUANTIFICATION

This appendix is intended to provide an overview of fault trees and event trees and their quantification for those unfamiliar with probabilistic techniques. The sections to follow describe aspects of probabilistic analyses pertinent to the understanding of the PRA analysis appendices. The first section describes fault trees and the models used to quantify the fault trees. The second section details event trees while the final section describes the computer codes used in the PRA analyses quantification.

A.1 Fault Trees

A fault tree analysis can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with component hardware failures, human errors, or any other pertinent events that can lead to the undesired event. A fault tree depicts the logical interrelationships of basic events that lead to the undesired event--which is the top event of the fault tree.

A fault tree is not a model of all possible system failures or all possible causes for system failure. A fault tree is tailored to its top event which corresponds to some particular system failure mode, and the fault tree includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive--they cover only the most credible faults as assessed by the analyst.

A fault tree is a complex of entities known as "gates" which serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationships of events needed for the occurrence of a "higher" event. The "higher" event is the "output" of the gate; the "lower" events are the "inputs" to the gate. The gate symbol denotes the type of relationship of the input events required for the output event. Gates are somewhat analogous to switches in an electrical circuit or two valves in a piping layout. Figure A-1 shows the type of gates commonly used in fault tree analyses.

The basic events identified in the fault trees are divided into four categories: 1) hardware failure unavailability 2) maintenance outage unavailability, 3) test outage contribution and 4) human error probability. The sections below describe these four categories.

A.1.1 Hardware Failure Unavailability

In fault tree development two types of contribution to component average unavailability are considered:

- o Hardware Failure
- o Hardware Outages

The hardware failure contribution arises because the component may fail prior to or during its operation. The outage contribution arises when the component is removed from operation for testing, preventative maintenance, and/or repair.

Two important considerations are made when evaluating component failure contribution. The component may be operating or it may be in a standby mode. If the component is part of a standby system, the average unavailability is estimated using either a time-based failure rate or a demand failure probability for the component failure modes being assessed.

A time-based failure rate is applicable when the failure mechanism causing the failure mode is related to the time the component is in service between checks of its operability. The time between tests is thus an important part of the unavailability calculations for such component failure modes. A demand failure probability is appropriate for component failure modes that do not depend on the test period length, but rather are related to the number of times that the component is "demanded" to operate. The length of test period is irrelevant for a component whose failure mode is truly demand dependent. The component average unavailability using a time-based failure is given by the expression:

$$q_c = 1/2\ (\lambda)\ T_t \qquad (1)$$

where q_c is the component average unavailability, (λ) is the standby failure rate (failures per hour), and T_t is the length of time between tests (hours). An estimate obtained using this expression is adequate assuming an exponential failure distribution and if the product of $(\lambda)*T_t \leq 0.1$.

The demand failure probability is given directly by the data base and thus:

$$q_c = q_d \qquad (2)$$

with q_c defined as before and q_d is the demand failure probability.

A more appropriate model for calculation of the unavailability of components in standby assumes that such components have both time-dependent and demand failure contributions given by:

$$q_c = q_d + 1/2\ (\lambda)\ T_t \qquad (3)$$

with the parameters q_c, q_d, (λ) and T_t are as previously defined. Data is usually available to estimate both the time-dependent and demand related portion of component unavailabilities.

When a component test period is relatively small (e.g., on the order of three months or less) either expression (1) or expression (2) may be used to estimate the unavailability of standby components without introducing sufficient error in the results obtained in fault tree quantification.

The calculation model to compute the unavailability (unreliability) of non-repairable components in an operating system is given by the expression:

$$q_c = (\lambda) T_m \qquad (4)$$

with q_c as previously defined, (λ) is the operating failure rate (failures per hour) and T_m is the total defined mission time. Again, the expression is adequate assuming an exponential failure distribution and if the product of $(\lambda) T_m \leq 0.1$.

In standby safety related systems, components once actuated may fail to perform for the desired mission time (e.g., a pump fails to start and run for a desired time). The unavailability calculation model for such components is given as:

$$q_c = q_d + (\lambda) T_m \qquad (5)$$

or

$$q_c = 1/2 (\lambda) T_t + (\lambda) T_m \qquad (6)$$

with each parameter for both of the above expressions as previously defined. The selection of which expression to use for the quantification being performed is dependent on the type of data given by the selected data bank being used. Depending on a particular component's operating failure rate and total mission time used, the last term of expression (5) may be dropped from being considered as the calculated operating failure probability may be much less than the component's demand failure probability.

A.1.2 Maintenance Outage Unavailability

As stated previously, component outages can occur when components are removed from service for test, preventative maintenance, and/or repair. These are generally classified as:

- o Scheduled outages resulting from periodic tests and scheduled preventative maintenance.
- o Unscheduled outages resulting from a need to repair a failed component.

Scheduled preventative maintenance may be performed by some utilities on major safeguards equipment during normal plant operation. When scheduled preventative maintenance removes a component from service, then a scheduled maintenance outage contribution to component unavailability occurs.

Unscheduled outage occurs when a component fails and is in need of repair to continue system operation. For standby component, this usually happens during a periodic test when a component is discovered to be in a failed state.

Often repair ensues when a component is found to be degraded but operable (i.e., leaky pump and valves seals, excessive back leakage through check valves, etc.) as well as when a catastrophic type failure occurs. Thus the frequency with which unscheduled repair occurs should be at least as large as the component's failure rate, which in many reported data banks, includes only catastrophic failures.

The unscheduled repair (maintenance) outage contribution to component unavailability due to failure detected during test is given by the expression:

$$q_{RM} = f_R (\tau_R / T_t) \qquad (7)$$

where q_{RM} is the component unavailability due to unscheduled repair, f_R is the frequency (per test period) with which repair is expected to occur, τ_R is the mean component repair time (hours) and T_t is the test period.

For this analysis, the mean component repair time (τ_R) is used to compute repair outage unavailabilities for failed components detected during scheduled tests. The mean value selected should be in accordance with a plant's technical specification outage limit. Test period data covers monthly and quarterly testing and the data is given as events per hour. Therefore Q_{RM} can be directly calculated using the data by the expression:

$$q_{RM} = \text{(Events/Hr)} (\tau_R) \qquad (8)$$

A.1.3 Test Outage Contribution

Most testing of safeguards equipment during normal plant operation will not prevent such equipment from carrying out its intended safety function if an accident happens while the equipment is undergoing testing in accordance with the plant's technical specification. If a test procedure results in a component being removed from active service for all or a portion of a test, then a test outage occurs. The unavailability of a component due to testing is given by the expression:

$$q_t = (\tau)_t / T_T \qquad (9)$$

where q_t is the average unavailability from the test outage, $(\tau)_t$ is the average duration of test (hours) and T_t is the interval between test in hours. This data can be extracted from the Technical Specifications.

A.1.4 Human Error Probability

Both event tree and fault tree modeling presented consider operator error as an input parameter. Considerable work has been done by Swain, Bell, and Guttman to develop techniques and procedures for conducting human error reliability analysis. Their work along with examples is documented in NUREG/CR-1278, "Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications" (Reference 19).

A task analysis of each task operator contributing to an event tree sequence and/or system unavailability quantification using fault trees was performed. This formed the basis for the development of human reliability analysis probability trees. Tasks given by emergency operating procedures, test procedures, and maintenance procedures are broken down into smaller units (steps) of human behavior. These individual units of performance constitute elements of behavior for which potential errors are identified. The details in task analysis and the amount of information recorded are used to obtain human error probability (HEP) estimates.

Once the breakdown of tasks steps are completed, errors likely to be made by the operator are identified for each step. The steps are listed in chronological order. Based on the actual performance situation, the analyst determines which types of error the operator is likely to make and which he is not. Errors of commission and omission are to be considered.

Human reliability analysis (HRA) probability trees are then developed for each task identified by accident event trees and system fault trees. In the development of the HRA probability tree, each likely error defined in the task analysis is entered as the right limb in a binary branch of the tree. Chronologically, in the order of their potential occurrence, the resultant branches of errors form the limbs of the HRA tree, with the first potential error starting at the highest point of the tree.

Any given task appears as a two-limb branch of a HRA probability tree, with each left limb representing the probability of success and each right limb that of failure. Once a task is diagrammed as having been completed successfully (or unsuccessfully) another task is considered. The binary branch describing the probability of the success (or failure) of the second task extends from the left (or right) limb of the first branch. This process is repeated until all tasks are included in the development of the HRA tree. When completed, every limb of the tree following the initial branching will depict a conditional probability.

A HRA probability tree is quantified by assigning nominal human error probabilities to each task limb on the tree. Error probabilities assigned are obtained from Chapter 20 of NUREG/CR-1278. To use the values given by Chapter 20, the analyst categorizes all tasks based upon the operator manipulating valves, performing a check of another operator's work, using a written procedure, or attempting some other type of task. Values are then selected from Chapter 20 that most closely approximates the description of a task being considered. In some cases the description on Chapter 20 will detail a scenario only slightly different from the one in analysis, thus the analyst can use the Chapter 20 values for the scenario.

Once human error probability values are assigned to each task limb of a HRA tree, the unavailability of an operator to perform a particular procedure can be obtained by summing the conditional failure probabilities of failed branches representing failed tasks associated with the procedure.

A.1.5 Fault Tree Component Identification Codes

Table A.1-1 describes the coding system used in the fault tree analysis to identify components, trains and failure modes.

A.2 Overview of Event Tree Quantification

Event trees are inductive logic methods for identifying the various possible outcomes of a given initiating event. In risk analysis applications, the initiating event of an event tree is typically a system failure, and the subsequent events are determined by the system characteristics.

An event tree begins with a defined accident-initiating event. This event could arise from failure of a system component, or it could be initiated externally to the system. Different event trees must be constructed and evaluated to analyze a set of accidents.

Once an initiating event is defined, all the safety systems that can be utilized after the accident must be defined and identified. These safety systems are then structured in the form of headings for the event tree.

Once the systems for a given initiating event have been identified, the set of possible failure and success states for each system must be defined and enumerated. Careful effort is required in defining success and failure states for the systems to ensure that potential failure states are not included in the success definitions; much of this analysis is done using fault tree techniques.

Once the system failure and success states have been properly defined the states are then combined through the decision-tree branching logic to obtain the various accident sequences that are associated with the given initiating event. The initiating event is depicted by the initial horizontal line and the system states are then connected in a stepwise, branching fashion; system success and failure states have been denoted by S and F, respectively. The format follows the standard tree structure characteristic of event tree methodology.

The accident sequences that result from the structure are shown in the last column. Each branch of the tree yields one particular accident sequence. The system states on a given branch of the event tree are conditional on the previous states having already occurred.

Once the final event tree has been constructed so that the results associated with each accident sequence have been defined, the final task is to compute the probabilities of system failure. Fault tree analyses are used to calculate the conditional probabilities needed for each branch of the event tree. Multiplication of the conditional probabilities for each branch in a sequence gives the probability of that sequence. (Reference: McCormick, Norman J., Reliability and Risk Analysis, Academic Press, New York, 1981.)

A.3 Computer Codes

This section describes the computer codes used in the analysis to quantify the fault trees and event trees. The GRAFTER code package was used in the fault tree analysis and the SUPER code package was used in the event tree analysis.

A.3.1 GRAFTER CODE SYSTEM (Fault Trees)

The GRAFTER code system is a menu-driven, interactive code system for all aspects of fault tree analysis. It performs the following functions:

- o Draws, stores, and prints fault trees.
- o Uses a master data bank to automatically update fault trees with new data.
- o Quantifies system unavailability and identifies single and multiple failures (cutsets).

GRAFTER is a computer code system written in FORTRAN and ASSEMBLER languages to construct and analyze fault trees interactively on an IBM-AT computer. The code can construct fault trees containing up to 2064 boxes (gate or basic event). A menu of commands is provided to construct the faults trees. The computer keyboard is used to move to different locations of the fault tree.

The data management functions of the GRAFTER system are as follows:

1. Calculate and tabulate basic event failure probabilities and variances. If requested, this option will place the probabilities and variances in a fault tree which has been generated by GRAFTER and calculate minimal cutsets and quantify the mean failure probabilities for the top gate and any specified lower gates.

2. Calculate and tabulate a basic event probability mean and variance which is composed of multiple failure modes.

3. Update and print the contents of a master data file which contains the failure rate means and variances of all failure modes considered in an analysis.

Incorporated into the GRAFTER code system is a master data bank. This data bank contains component random failure data, as well as common cause failure, human error, and test and maintenance unavailability data.

Another function of the GRAFTER code system is to identify minimal cutsets of a fault tree. It also quantifies the mean failure probability and variance of the top event and other specified lower level events.

For each gates specified when generating the input for cutset identification, the code will identify and print the cutsets. The cutsets are listed in order of decreasing probability. The mean and variance for the requested gates are also calculated and printed.

A.3.4 SUPER CODE SYSTEM (Event Trees)

The SUPER code system is a menu-driven, interactive codes system to perform event tree modeling. It performs the following functions:

- o Draws and quantifies event trees for accident scenario probabilities and prints event trees.
- o Identifies dominant accident sequences.

SUPER is written in FORTRAN to run on an IBM-AT computer. SUPER can construct and quantify event trees with 25 nodes and 325 branches. Each node may have up to 8 branches, thus allowing more realistic modeling of system states than is possible with conventional YES/NO binary logic. Consequence categories for the event sequences can be defined and the frequencies of the event sequences can be automatically sorted into consequence categories. The code can also process conditional probabilities defined for specially identified branches.

The output of the codes consists of:

- o Event tree picture
- o Probability/frequency of individual event sequences
- o Probability/frequency of consequence categories
- o Output file for dominant event sequences
- o Output file for consequence categories

The SUPER code system also uses a data bank for automatically updating the event tree node probabilities. The event tree master data bank contains system failure probabilities, operator action failure probabilities, and other phenomenological occurrence probabilities.

TABLE A-1
FAULT TREE COMPONENT IDENTIFICATION CODES

Nine or ten character codes identify component failures (basic events) in the fault trees. The following lists the codes used in this evaluation.

COMPONENT IDENTIFICATION CODE

Code Letters	Component Identification
System	
RH	Residual Heat Removal System
Train	
1	Train #1
2	Train #2
Mechanical Components	
AS	Valve, Relief Solenoid Operated
AV	Valve, Air (Pneumatic) Operated
CV	Valve, Check
HE	Heat Exchanger
HV	Valve, Hydraulic Operated
MV	Valve, Motor Operated
PM	Motor Driven Pump
SV	Valve, Solenoid Operated
XV	Valve, Manual

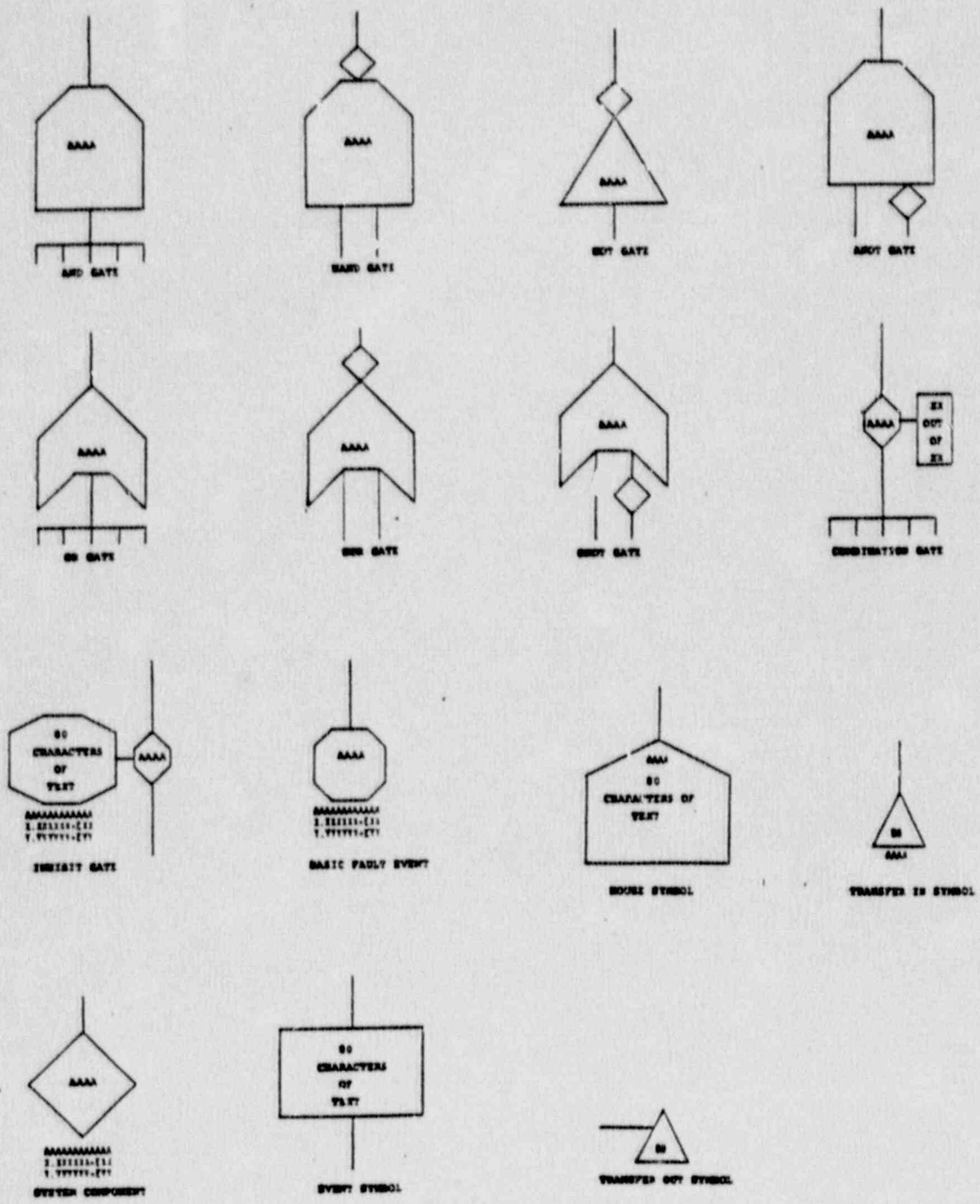
TABLE A-1 (Cont)
COMPONENT IDENTIFICATION CODE

Code Letters	Component Identification
	Electrical Components
AN	Annuciator
BI	Bistable Switch
CB	Circuit Braaker
CM	Signal Comparator
CN	Relay or Switch Contact
CO	Coil
CS	Control Switch
CT	Transformer, Current
DE	Diode
FU	Fuse
IV	Current/Voltage Module
LO	Lockout Relay or Switch
LS	Limit Switch
MO	Motor
MS	Motor Starter
OL	Thermal Overload Element
PS	Power Supply
QS	Switch, Torque
RE	Relay
RL	Relay (Latching Type)
RS	Resistor
SR	Manual Switch (Rotary)
ST	Toggle Switch
SW	Manual Switch (Pushbutton)
TP	Transmitter, Pressure
TT	Transmitter, Temperature

TABLE A.1-1 (Cont)
FAILURE MODE IDENTIFICATION CODE

Code Letters	Failure Mode
A	Does Not Start
B	Open Circuit
C	Closed
D	Does Not Open
F	Loss of Function (Does not operate/start/run)
J	Degraded
K	Does Not Close
H	Fails High
L	Fails Low
N	No Input
O	Open
P	Plugged
Q	Short Circuit
R	Rupture
S	Short to Ground
U	Spurious Opening
V	Spurious Closing
X	Does Not Run
VS	Visual Detection
ST	Status Lignt
OE	Operator Error
TST	Test
MAIN	Maintenance

FIGURE A-1
FAULT TREE SYMBOLS



APPENDIX B

EVENT V ANALYSIS

APPENDIX B
EVENT V ANALYSIS

This appendix details the calculations performed to determine the change in the frequency of an interfacing systems LOCA due to removal of the autoclosure interlock for the four reference plants. An interfacing systems LOCA is an important safety concern because a direct release of radionuclides to the atmosphere may occur. The frequency of an Event V via the RHR suction path is calculated for two cases: 1) with the present interlock configuration and 2) with the proposed modification.

A RHR LOCA is a non-mitigable LOCA outside containment. It is assumed to occur if the valves in the RHR suction line fail open when the RCS is at operating pressure (2250 psia). Because the RHR system is designed for a much lower pressure (600 psig or less), the result of both valves failing open is overpressurization of the RHR system. This is assumed to lead to gross failure of the RHR boundary. Because most RHR systems are located outside of containment, gross failure of the RHR boundary is assumed to lead directly to release of radionuclides into the atmosphere.

In this analysis, several failure combinations are considered in which both suction valves would be in the "OPEN" position. These failure modes include: 1) rupture of the two series motor-operated valves in the RHR suction line and 2) one suction valve failing open and subsequent rupture of the other valve. The latter failure mode actually includes two combinations - the valve closest to the RCS failing open and subsequent rupture of the valve closest to the RHR system and vice versa. Failure to close both RHR suction valves during startup is not considered a credible failure mode because the condition would become apparent and corrective action would be taken. (The RHR relief valve would lift as the RCS pressure increased, an alarm would sound, and the RCS pressure would increase more slowly than if the suction valves were closed.)

The general expression used to calculate the frequency of an Event V (F(VSEQ)) for one RHR suction line utilizing the above failure modes is:

$$F(VSEQ) = (\lambda)_2\, Q(V_1) + (\lambda)_1\, Q(V_2) + (\lambda)_2\, Q(V_1R) \quad (1)$$

where

$(\lambda)_2$ = failure rate of RCS valve (due to rupture)
$(\lambda)_1$ = failure rate of RHR valve (due to rupture)
$Q(V_1)$ = probability that RHR valve is open
$Q(V_2)$ = probability that RCS valve is open
$Q(V_1R)$ = probability of rupture of RHR valve

The following boundary conditions and assumptions were applied in each of the analyses:

1. The calculation is based on an occurrence when the plant is at power, not in the shutdown mode.

2. The valve closest to the RCS is at RCS pressure and the valve closest to the RHR system is at RCS pressure only if the valve closest to the RCS fails open.

3. No common cause rupture of the valves is considered. This is based on the fact that no common cause ruptures of valves have actually occurred.

4. The frequency of valve rupture is that of catastrophic internal leakage. The failure rate is the same for either valve given that the valve is exposed to RCS pressure.

5. All electrical power to the control circuitry (i.e. 480 V AC bus) is assumed to be available with a probability 1.0.

6. A refueling outage occurs approximately every 18 months (assumed to be the only time at which the plant will be in cold shutdown, on average).

The next sections describe the plant specific analyses performed for each reference plant.

B.1 SALEM

In order to determine the probabilities of the motor-operated suction valves being "OPEN" ($Q(V_1)$ and $Q(V_2)$ in equation 1), a detailed fault tree for the Salem control circuitry associated with these valves was developed.

Utilizing the present control circuitry diagrams shown in Figures B-1 and B-2 for suction valves 1RH1 and 1RH2 and the procedures for terminating the RHR system in preparation for startup, a fault tree was developed that considered how either suction valve would be "OPEN" at power conditions. Component failures and human errors were included in the fault tree. The fault tree developed for valve 1RH1 is shown in Figure B-3. (Because the control circuitry for the valves is identical except for component ID's, only one fault tree was developed to calculate the failure probability.)

The scenarios examined in the fault tree for the case with the autoclosure interlock are: 1) the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but due to some component failure, the valve does not close) and the autoclosure interlock fails to perform its function and does not close the valve and an operator fails to detect that the valve is not closed during startup or power operation.

For the deletion of the autoclosure interlock and the addition of an alarm as shown in Figure B-4 for valve 1RH1, a detailed fault tree was also developed. The scenarios developed for this case are: 1) the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but it does not close) and the operator fails to detect that the valve is not closed via the presence of an alarm (or the alarm fails to operate). The fault tree developed for this case is shown in Figure B-5.

In each case (with the autoclosure interlock and without the autoclosure interlock), the first scenario is the same; only the second scenario differs due to the proposed modification.

For the Salem analysis, the following assumptions and boundary conditions were utilized:

1. The operator closes the RHR suction valves utilizing a push-button type switch.

2. The shift supervisor verifies the RHR suction valves are closed before signing the check off sheet.

3. The indicating lights associated with the RHR suction valves do not have alarms associated with them.

4. A component failure would be detected in a 24 hour interval if it caused the suction isolation valve to spuriously open or fail to close.

In order to quantify the fault trees developed for these cases, each basic event probability was calculated and then input into the appropriate fault tree. For a component failure, the following formula was used:

$$Q(\text{component}) = (\lambda)\, \frac{T_{detect}}{2} \qquad (2)$$

where

Q(component) = basic event probability

λ = failure rate for the component

T_{detect} = detection interval

Table B-1 shows the basic event probabilities for each component utilizing a 24 hour detection interval.

The human error probabilities were calculated using "The Handbook for Human Reliability Analysis," Reference 19, and Salem's operating procedures for terminating the RHR system in preparation for startup. The calculations of the human error probabilities are shown in Table B-2.

SALEM RESULTS

The probabilities for $Q(V_1)$ and $Q(V_2)$, the probability that the isolation valve is open, for each case are shown below:

	With Autoclosure Interlock	Without Autoclosure Interlock
$Q(V_1)$	1.48E-04	1.10E-06
$Q(V_2)$	1.48E-04	1.10E-06

The major cutsets (failure combinations) and the probabilities of the cutsets for each case (with and without the autoclosure interlock) are shown in Tables B-3 and B-4. For the case with the ACI (Table B-3), the dominant contributors are a component failure which causes the valve not to close along with the operator failing to detect that the valve did not close during startup and another operator failure to detect the wrong position during power operation.

For the ACI deletion case, the dominant contributors are: the operator fails to close the valve during startup along with the operator failing to detect that the valve is not closed during startup and either operator failure to detect via the alarm or the alarm fails to operate.

The frequency of an interfacing system LOCA, given these probabilities is calculated using:

$$F(VSEQ) = (\lambda)_2\, Q(V_1) + (\lambda)_1\, Q(V_2) + (\lambda)_2\, Q(V_{1R})$$

where

$(\lambda)_2$ = failure rate of RCS valve (due to rupture)
$(\lambda)_1$ = failure rate of RHR valve (due to rupture)
$Q(V_1)$ = probability that RHR valve is open
$Q(V_2)$ = probability that RCS valve is open
$Q(V_{1R})$ = probability of rupture of RHR valve

The failure rate due to rupture of a motor-operated valve is 1.0E-7 per hr ($(\lambda)_1$ and $(\lambda)_2$). The quantity $Q(V_{1R})$ is determined by assuming that the total defined mission time is the time between refueling outages (i.e., every 18 months). The rupture of motor-operated valve is assumed to occur randomly in the time interval 0 - T_M where T_M is the total defined mission time. Therefore the probability of the valve rupturing is:

$$Q(V_{1R}) = (\lambda) \frac{T_M}{2}$$

$$= \frac{1E\text{-}07}{hr} \quad \frac{(8760 \text{ hrs/year} * 1.5 \text{ years})}{2}$$

$$= 6.57E\text{-}04$$

Entering the failure probabilities leads to the following frequency for an interfacing system LOCA for the case with the ACI:

$$F(VSEQ) = (\lambda)_2 Q(V_1) + (\lambda)_1 Q(V_2) + (\lambda)_2 Q(V_{1R})$$
$$= 1E\text{-}07/hr *(1.48E\text{-}04) + (1E\text{-}07/hr)*(1.48E\text{-}04) + 1E\text{-}07/hr *(6.57E\text{-}04)$$
$$= 1.48E\text{-}11/hr + 1.48E\text{-}11/hr + 6.57E\text{-}11/hr$$
$$= 9.53E\text{-}11/hr * (8760 \text{ hrs/year})$$
$$= 8.35E\text{-}07/year$$

The same method was applied in the case without the ACI. The following summarizes the frequencies:

	With Autoclosure Interlock	Without Autoclosure Interlock
F(VSEQ)	8.35E-07/year	5.77E-07/year

The frequency of an Event V decreases by approximately 31 percent with removal of the ACI. The main contributor to the frequencies in each case is a double rupture of MOV 1RH2 then 1RH1 (frequency of 5.75E-07/year in both cases). The deletion of the ACI has no impact on this contributor. As can be seen, the frequency of a double rupture dominates the second case while the other contributor (the rupture of one valve while the other valve has failed open) does not contribute significantly in the case in which the ACI has been deleted. (The frequency for the rupture of one valve while the other is open decreases from 1.30E-7/year (1.48E-11/hr *8760 hrs/year) for the case with the ACI to 9.64E-10/year (1.10E-13/hr * 8760 hrs/year) for the case with the ACI deleted.) This is a significant decrease in the occurrence of an Event V by this failure mode. Thus, the deletion of the autoclosure interlock and the inclusion of an alarm is beneficial in reducing this contribution.

TABLE B-1
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1RHFU30PHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHCBOE	OE	OPERATOR FAILS TO RE	1.600E-03	---	1.60E-03
1RHOECLOSE	OE	OPERATOR FAILS TO CL	1.200E-03	---	1.20E-03
1RHOEDET2	OE	SECOND OPERATOR FAIL	9.800E-01	---	9.80E-01
1RHMVMECH	MV	FAILURE TO CLOSE	1.000E-05	1.200E+01	1.20E-04
1RHOEDETAC	OE	SECOND OPERATOR FAIL	9.800E-01	---	9.80E-01
1RHFU30PHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHFU30PHC	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHCN9CPHA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHCN9CPHB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHCN9CPHC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHOL49PHA	OL	PREMATURE OPEN	1.500E-07	1.200E+01	1.80E-06
1RHOL49PHB	OL	PREMATURE OPEN	1.500E-07	1.200E+01	1.80E-06
1RHOL49PHC	OL	PREMATURE OPEN	1.500E-07	1.200E+01	1.80E-06
1RHCB8	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
1RHCT230	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
1RHFU15A1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHFU15A2	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHOLCN49	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHRECO9C	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
1RHRECN9O	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHQS17	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06

TABLE B-1 (CONT.)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1RHCN9XC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHCN9C	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHRECO9XC	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
CNCLOSE	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
RECO5CSV2	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
RECN5CSV2	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
DED5	DE	DIODE STANDARD QUALI	7.560E-09	1.200E+01	9.07E-08
PS28VDC	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
IVPC403R	IV	I-E CONVERTER ALL FA	2.000E-07	1.200E+01	2.40E-06
IVPM403R	IV	I-E CONVERTER ALL FA	2.000E-07	1.200E+01	2.40E-06
TPRS403	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
PSPQ403	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
STCT403	ST	TOGGLE SWITCH ALL MO	2.330E-07	1.200E+01	2.80E-06
TP403	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
RECO63Y	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
RECN63Y	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
BI403B	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
PS118VAC	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
CM403AB	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
1RHCN9/OQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
1RHCN63XQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHIVPMF	IV	I-E CONVERTER ALL FA	2.000E-07	1.200E+01	2.40E-06
1RHIVPCF	IV	I-E CONVERTER ALL FA	2.000E-07	1.200E+01	2.40E-06

TABLE B-1 (CONT.)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1RHPT405	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
1RHPSPQ405	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
1RHCM405	CR	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
1RHCNS1Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHCNSCSVQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
1RHCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
1RHCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
1RHOEDETAN	OE	OPERATOR DETECT ANNU	2.660E-04	---	2.66E-04
1RH1AN1	AN	ANNUCIATOR ALL MODES	4.250E-06	1.200E+01	5.10E-05
1RHPSAN	PS	ANNU POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
1RHSTEMLS	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05

TABLE B-2

SALEM
HUMAN ERROR CALCULATIONS

TASK: 1RH1 and 1RH2 must be closed and the power supplies cleared and tagged prior to RCS pressure exceeding '5 psig. Complete checkoff sheet of OP II-6.3.4.

REFERENCE: Steps 5.1.5 step f) and 5.1.6 step c) in operating procedure OP II-6.3.3 Revision 10 - Terminating RHR.

BREAKDOWN OF TASK:

1. Omission error - Operator fails to clear and tag open power supply breaker

Median HEP = 0.003	Table 20-7	Long list > 10 items
Mean HEP = 3.75E-03		When procedures with checkoff
Error Factor = 3		provisions are correctly used

2. Commission error - Operator selects wrong circuit breaker

Median HEP = 0.005	Table 20-12	Select wrong circuit breaker in a
Mean HEP = 6.25E-03		group of circuit breakers densely
Error Factor = 3		grouped and identified by labels
		only

3. Recovery error -Shift supervisor fails to detect error by others

Median HEP = 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP = 0.16		using written materials
Error Factor = 5		

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(6.25E-3)(0.16) + 3.75E-03(0.16) \\
&= 9.96E-04 + 6.0E-04 \\
&= 1.596E-03 \\
&= 1.60E-03
\end{aligned}
$$

Fault Tree Identifiers: 1RHCBOE

TABLE B-2
(Cont.)

SALEM
HUMAN ERROR CALCULATIONS

TASK: CLOSE 1RH1 and 1RH2. Complete checkoff sheet of OP II-6.3.4 and Checkoff Sheet 1 of Terminating RHR.

REFERENCE: Steps 5.1.5 step f) and 5.1.6 step c) in operating procedure OP II-6.3.3 Revision 10 - Terminating RHR.

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated suction valve using push-button switch

Median HEP	= 0.003	Table 20-7	Long list > 10 items
Mean HEP	= 3.75E-3		When procedures with checkoff
Error Factor	= 3		provisions are correctly used

2. Commission error - Operator fails to push button to close valve

Median HEP	= 0.003	Table 20-12	Select wrong control on a panel
Mean HEP	= 3.75E-3		from an array of similar-
Error Factor	= 3		appearing controls identified
			by labels only

3. Recovery error - Shift supervisor fails to detect error by others

Median HEP	= 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP	= 0.16		using written materials
Error Factor	= 3		

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(3.75E-03)(0.16) + 3.75E-03(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&\approx 1.20E-03
\end{aligned}
$$

Fault Tree Identifiers: 1RHOECLOSE

TABLE B-2
(Cont.)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Operator fails to detect wrong valve position

REFERENCE:

BREAKDOWN OF TASK:

1. Omission error - Operator fails to detect wrong valve position

   HEP = 0.98 Table 20-25 Legend light
   Other than annuciator light

P_{OE} = 0.98

Fault Tree Identifiers: 1RHOEDET2 and 1RHOEDETAC

TABLE B-2
(Cont.)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Operator fails to detect wrong valve position via annuciator

REFERENCE:

BREAKDOWN OF TASK:

1. Omission error - Operator fails to detect wrong valve position via annuciator and initiate some kind of corrective action

   Median HEP = 0.0001 Table 20-23 One annuciator
   Mean HEP = 2.66E-04
   Error Factor = 10

   P_{OE} = 2.66E-04

   Fault Tree Identifiers: 1RH EDETAN

TABLE B-3

SALEM DOMINANT CUTSETS

FOR $Q(V_1)$

PROBABILITY THAT MOV 1RH1 IS OPEN

WITH ACI CASE

MEAN PROBABILITY OF FAILURE = 1.48E-04

	PROBABILITY	CUTSET DESCRIPTION
1.	3.46E-05	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 RELAY COIL 9X/C FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
2.	3.46E-05	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 RELAY COIL 9/C FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
3.	1.15E-05	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 CONTACT 9/C FAILS TO TRANSFER (TO 9X/C COIL) OPERATOR FAILS TO DETECT OPEN MOV 1RH1
4.	1.15E-05	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 CONTACT 9X/C FAILS TO CLOSE OPERATOR FAILS TO DETECT OPEN MOV 1RH1
5.	1.15E-05	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 CONTACTOR FAILS TO CLOSE (9/C) PHASE C OPERATOR FAILS TO DETECT OPEN MOV 1RH1
6.	1.15E-05	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 CONTACTOR FAILS TO CLOSE (9/C) PHASE B OPERATOR FAILS TO DETECT OPEN MOV 1RH1
7.	1.15E-05	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 CONTACTOR FAILS TO CLOSE (9/C) PHASE A OPERATOR FAILS TO DETECT OPEN MOV 1RH1
8.	4.03E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 230V/118V TRANSFORMER FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
9.	2.30E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 CLOSING TORQUE SWITCH FAILS OPEN (17) OPERATOR FAILS TO DETECT OPEN MOV 1RH1
10.	1.73E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 15 AMP FUSE #2 FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1

TABLE B-3 (CONT.)
SALEM DOMINANT CUTSETS
FOR $Q(V_1)$
PROBABILITY THAT MOV 1RH1 IS OPEN
WITH ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
11.	1.73E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 15 AMP FUSE # 1 FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
12.	1.73E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 THERMAL OVERLOAD FAILS PHASE C OPERATOR FAILS TO DETECT OPEN MOV 1RH1
13.	1.73E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 THERMAL OVERLOAD FAILS PHASE B OPERATOR FAILS TO DETECT OPEN MOV 1RH1
14.	1.73E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 THERMAL OVERLOAD FAILS PHASE A OPERATOR FAILS TO DETECT OPEN MOV 1RH1
15.	1.73E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 30 AMP FUSE PHASE C FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
16.	1.73E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 30 AMP FUSE PHASE B FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
17.	1.73E-06	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 30 AMP FUSE PHASE A FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
18.	2.30E-07	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 CONTACT S/O SPURIOUSLY OPENS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
19.	2.30E-07	SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 THERMAL OVERLOAD CONTACT FAILS OPEN (49) OPERATOR FAILS TO DETECT OPEN MOV 1RH1
20.	1.38E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 MECHANICAL FAILURE OF MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1

TABLE B-4
SALEM DOMINANT CUTSETS
FOR $Q(V_1)$
PROBABILITY THAT MOV 1RH1 IS OPEN
ACI DELETION CASE

MEAN PROBABILITY OF FAILURE = 1.10E-06

	PROBABILITY	CUTSET DESCRIPTION
1.	3.13E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
2.	1.02E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 VALVE STEM MOUNT LIMIT SWITCH FAILS TO OPERATE
3.	8.18E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 POWER SUPPLY TO ANNUCIATOR FAILS
4.	8.18E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 118 V AC POWER SUPPLY FAILS
5.	8.18E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 LOOP POWER SUPPLY 1-PQ-403 FAILS
6.	6.00E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 ANNUCIATOR FAILS TO OPERATE
7.	4.23E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 RELAY COIL 63Y/RCP FAILS
8.	4.09E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 SIGNAL COMPARATOR DUAL CIRCUIT FAILS 1PC403AB
9.	3.95E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 PRESSURE TRANSMITTER PT-403 FAILS
10.	2.33E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 BISTABLE SWITCH 1BS-403B FAILS

TABLE B-4 (CONT.)

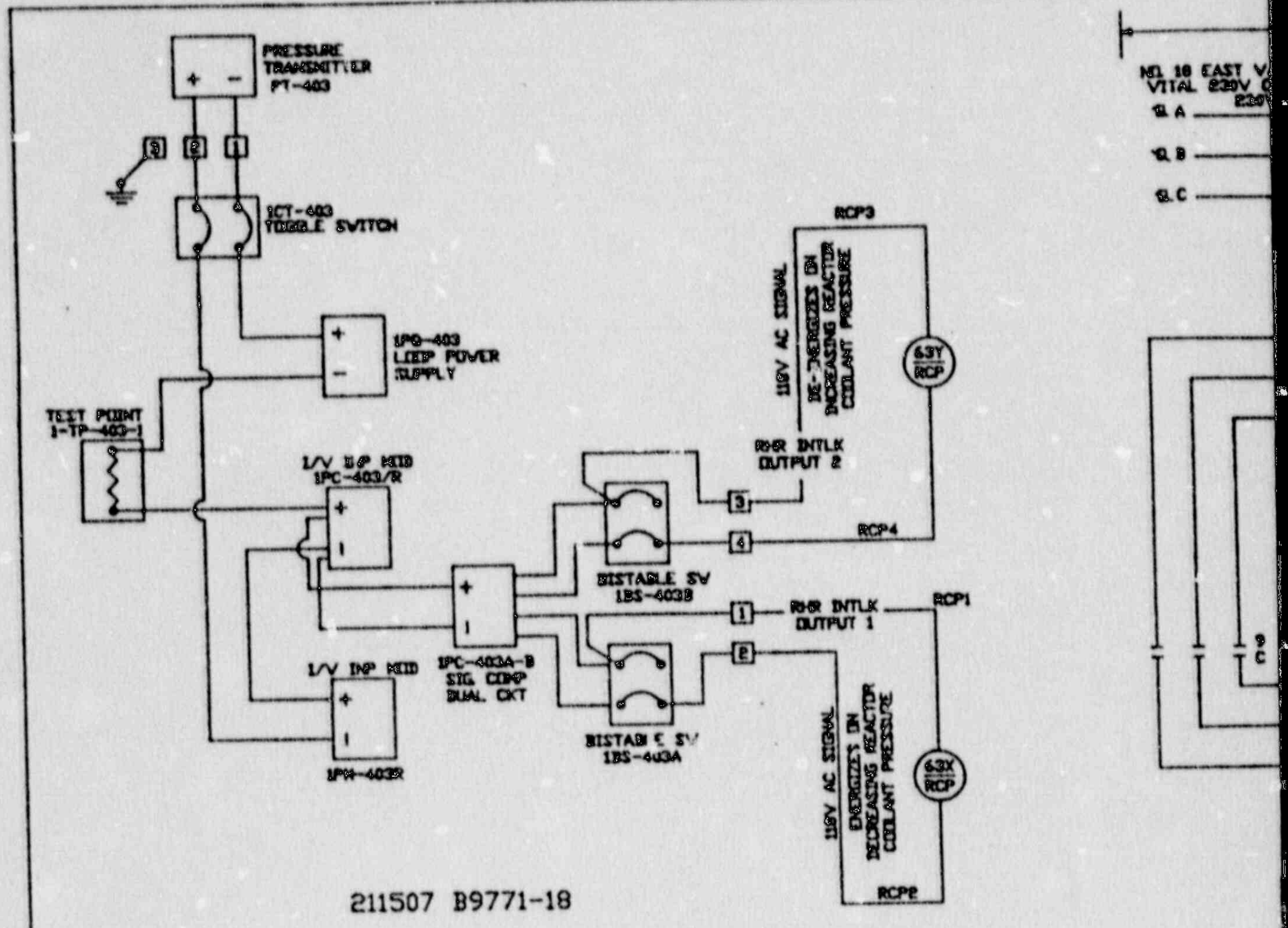
SALEM DOMINANT CUTSETS

FOR $Q(V_1)$

PROBABILITY THAT MOV 1RH1 IS OPEN

ACI DELETION CASE

	PROBABILITY	CUTSET DESCRIPTION
11.	1.81E-08	28 V DC POWER SUPPLY FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
12.	1.41E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 RELAY COIL CONTACT 63Y/RCP FAILS
13.	9.38E-09	RELAY COIL 9X/C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
14.	9.38E-09	RELAY COIL 9/C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
15.	9.38E-09	RELAY COIL 5/CSV2 FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
16.	5.91E-09	28 V DC POWER SUPPLY FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 VALVE STEM MOUNT LIMIT SWITCH FAILS TO OPERATE
17.	4.75E-09	28 V DC POWER SUPPLY FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 POWER SUPPLY TO ANNUCIATOR FAILS
18.	4.75E-09	28 V DC POWER SUPPLY FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 118 V AC POWER SUPPLY FAILS
19.	4.75E-09	28 V DC POWER SUPPLY FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 LOOP POWER SUPPLY 1-PQ-403 FAILS
20.	3.48E-09	28 V DC POWER SUPPLY FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 ANNUNCIATOR FAILS TO OPERATE



211507 B9771-18

LEGEND

- CONTROL CIRCUIT BREAKER
- FUSE
- DIODE
- CONTACT OPEN
- CONTACT CLOSED
- THERMAL OVERLOADS
- (R) INDICATING LIGHTS R - RED G - GREEN
- VOLTAGE TRANSFORMER

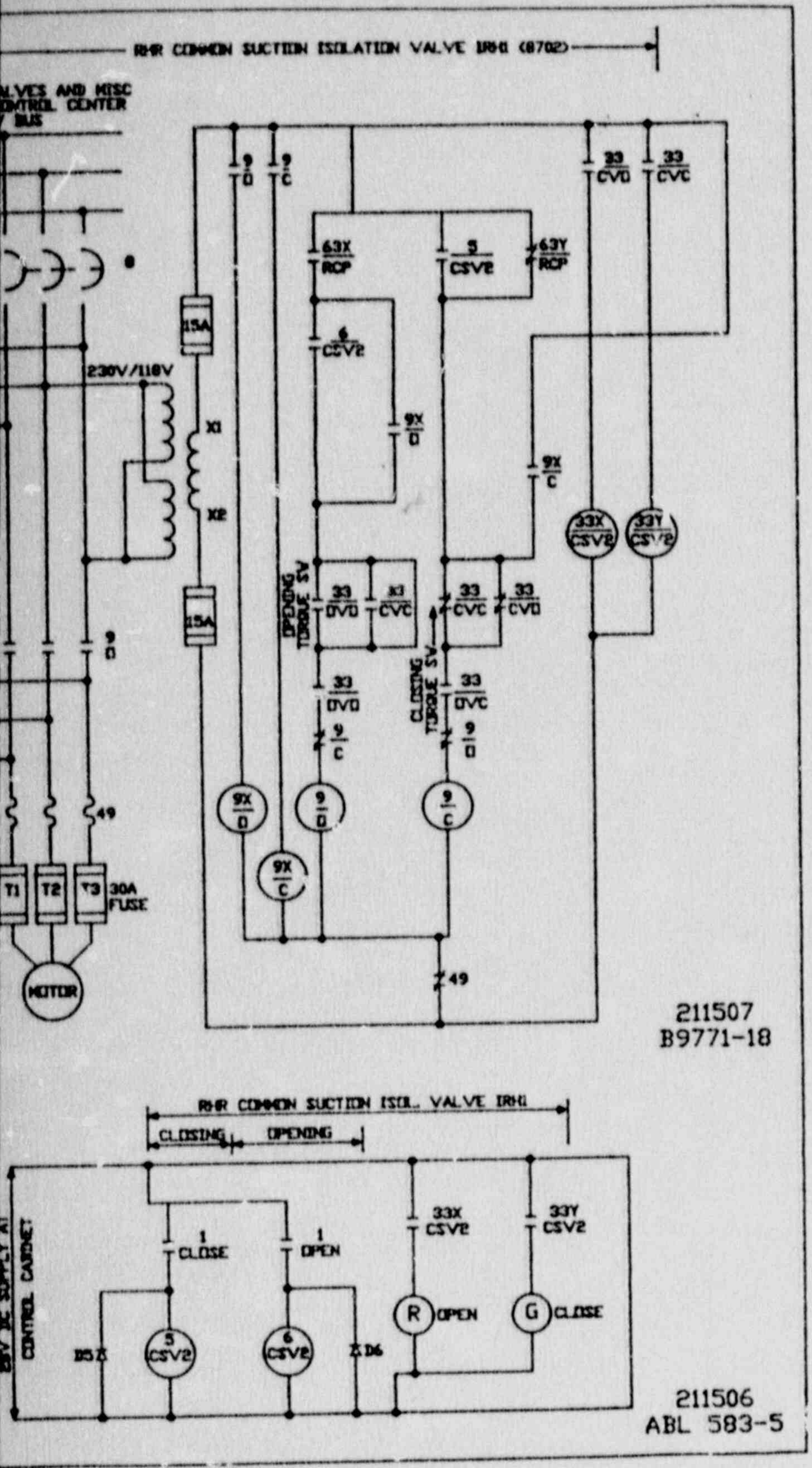
NOTES

5/CSV2	CLOSING RELAY COIL
6/CSV2	OPENING RELAY COIL
33/OVO	VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY OPEN
33/OVC	VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY CLOSED
33/CVO	VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY OPEN
33/CVC	VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY CLOSED
9/O	REVERSING CONTACTOR OPENING
9/C	REVERSING CONTACTOR CLOSING
63Y/RCP	REACTOR COOLANT PRESSURE AUX RELAY
63X/RCP	REACTOR COOLANT PRESSURE AUX RELAY
9X/C	AUX RELAY TO CONTACTOR CLOSING COILS
9X/O	AUX RELAY TO CONTACTOR OPENING COILS
33X/CSV2	VALVE FULLY OPEN AUX RELAY
33Y/CSV2	VALVE FULLY CLOSED AUX RELAY

2/1/88

SALEM RHR SUCTION
ISOLATION VALVE 1RH1
CONTROL CIRCUITRY

WESTINGHOUSE PROPRIETARY CLASS 3



S1
APERTURE
CARD

Also Available On
Aperture Card

FIGURE B-1

Salem RHRS Suction/Isolation Valve Control Circultry MOV-8702 (IRH-1)

1

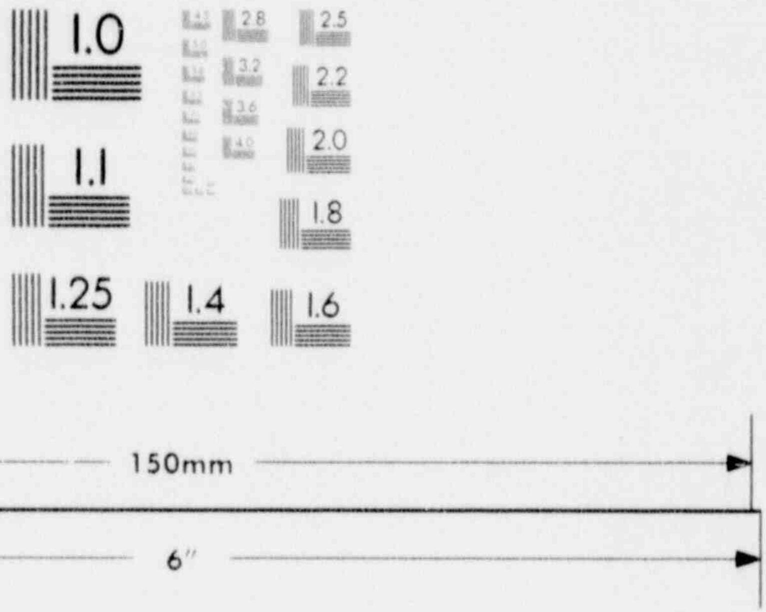
IMAGE EVALUATION TEST TARGET (MT-3)

150mm

6"

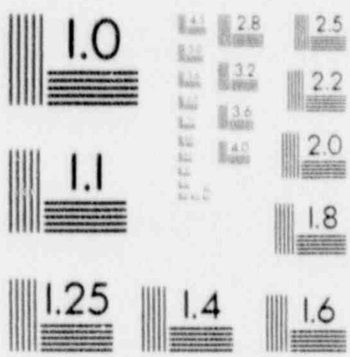
1

IMAGE EVALUATION TEST TARGET (MT-3)



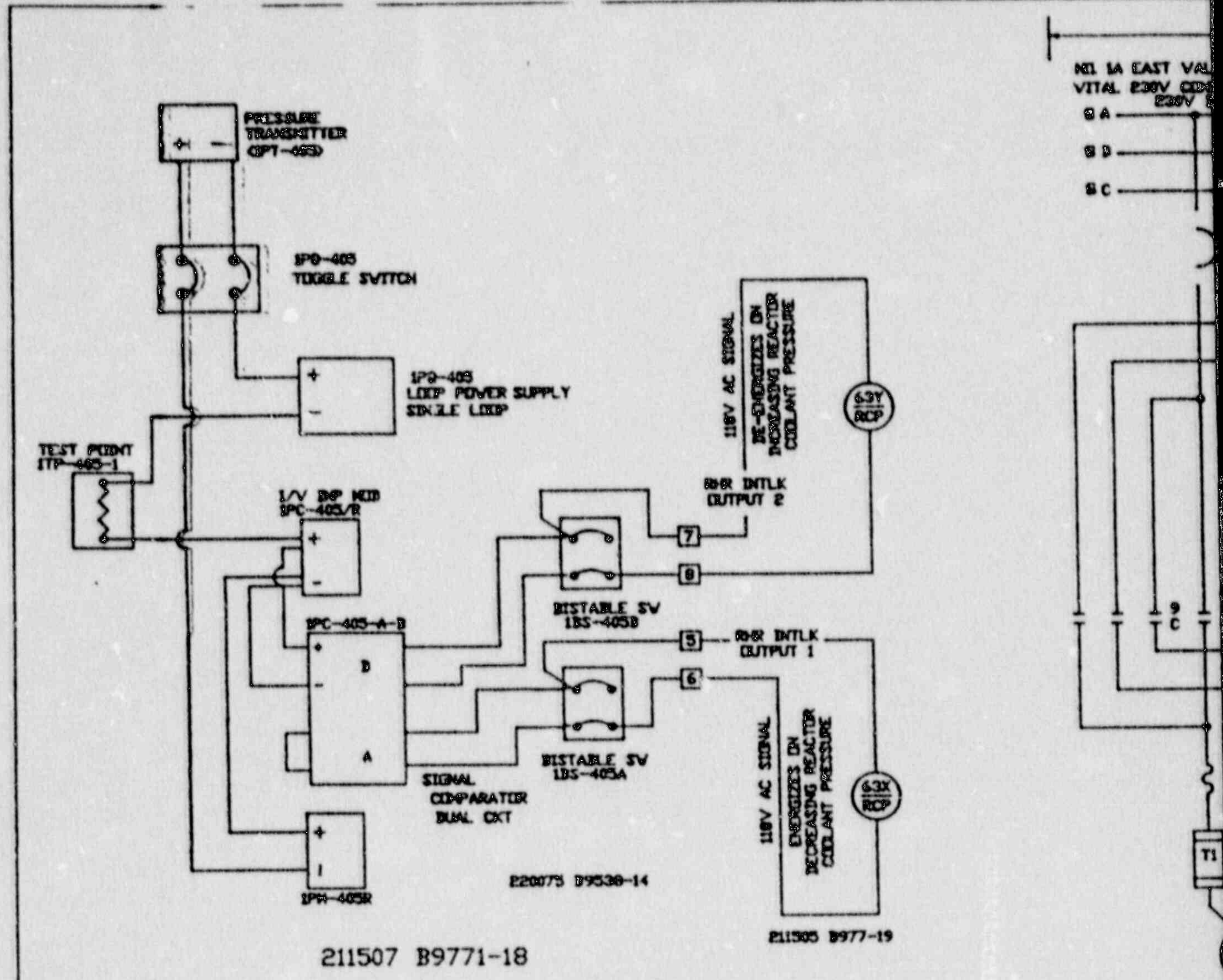
1

IMAGE EVALUATION TEST TARGET (MT-3)



150mm

6"



LEGEND

- CONTROL CIRCUIT BREAKER
- FUSE
- DIODE
- CONTACT OPEN
- CONTACT CLOSED
- THERMAL OVERLOADS
- INDICATING LIGHTS R - RED G - GREEN
- VOLTAGE TRANSFORMER

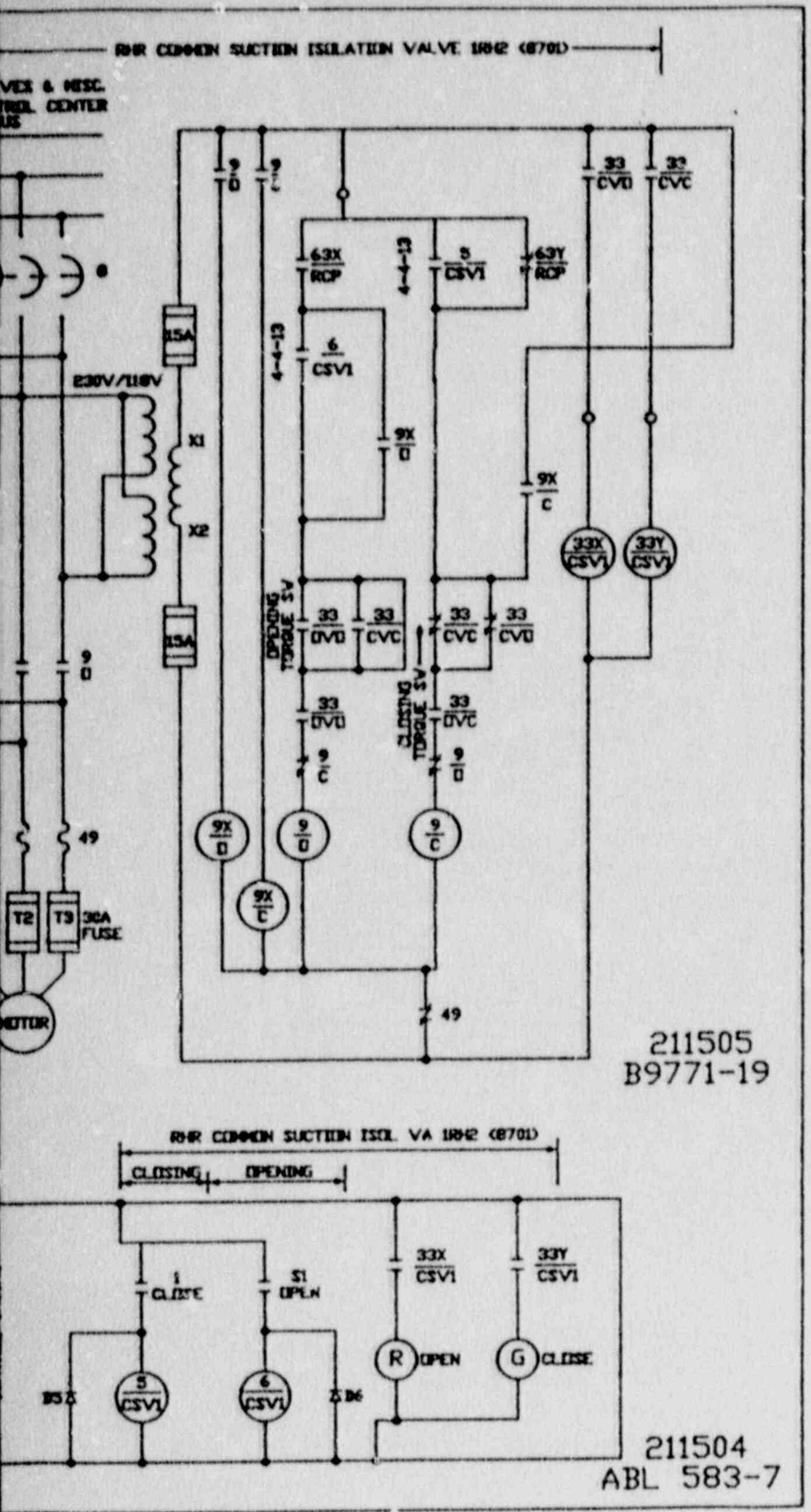
NOTES

- 5/CSV1 CLOSING RELAY COIL
- 6/CSV1 OPENING RELAY COIL
- 33/OVO VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY OPEN
- 33/OVC VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY CLOSED
- 33/CVO VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY OPEN
- 33/CVC VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY CLOSED
- 9/O REVERSING CONTACTOR OPENING
- 9/C REVERSING CONTACTOR CLOSING
- 63Y/RCP REACTOR COOLANT PRESSURE AUX RELAY
- 63X/RCP REACTOR COOLANT PRESSURE AUX RELAY
- 9X/C AUX RELAY TO CONTACTOR CLOSING COILS
- 9X/O AUX RELAY TO CONTACTOR OPENING COILS
- 33X/CSV1 VALVE FULLY OPEN AUX RELAY
- 33Y/CSV1 VALVE FULLY CLOSED AUX RELAY

RHS_1RH2

6/26/87

SALEM RHR SUCTION
ISOLATION VALVE 1RH2
CONTROL CIRCUITRY

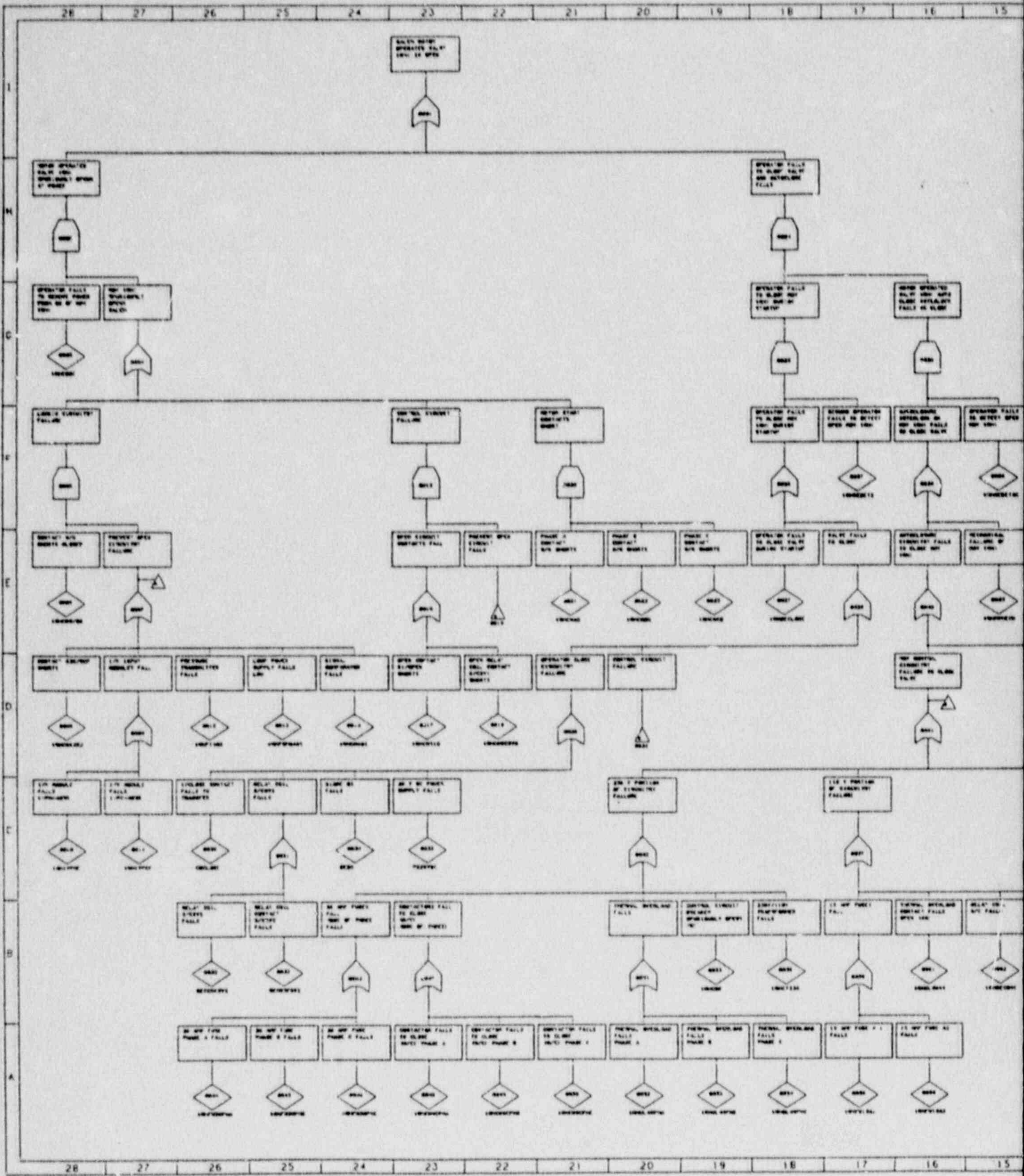


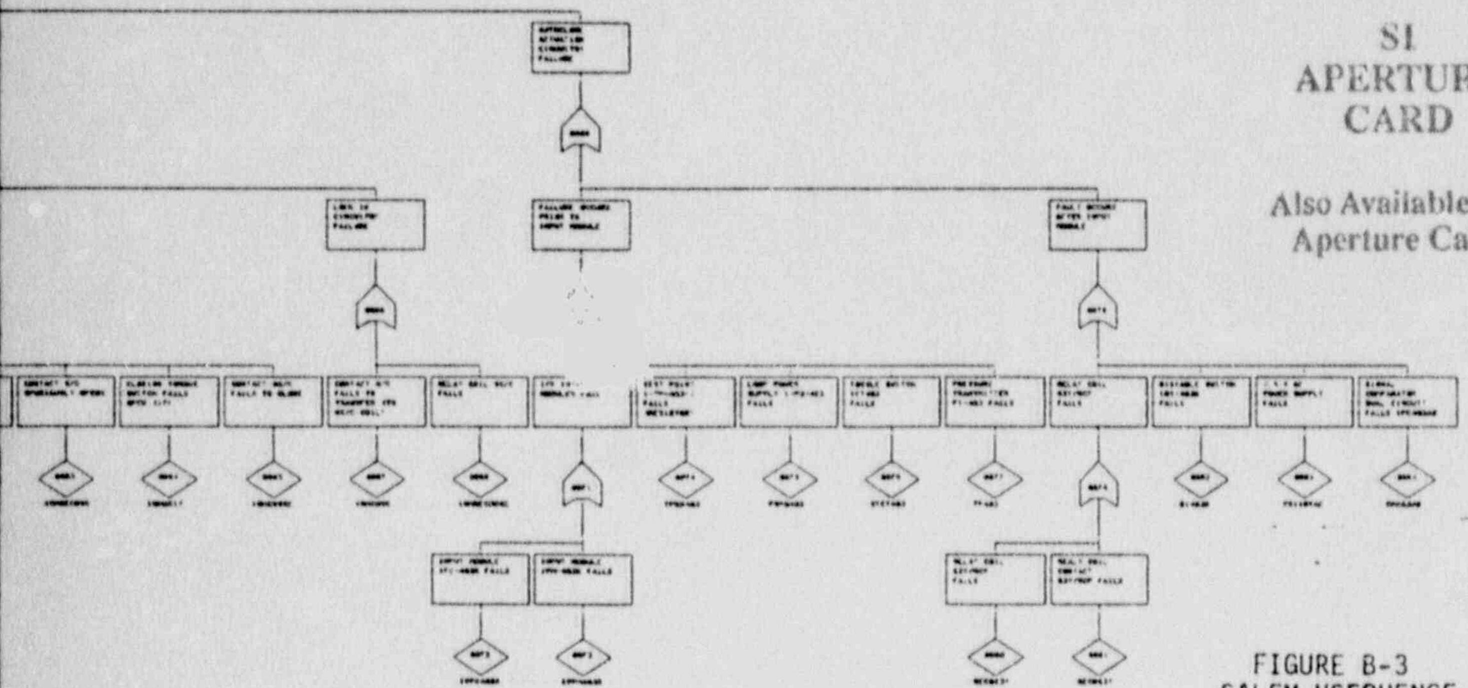
SI
APERTURE
CARD

Also Available On
Aperture Card

FIGURE B-2

Salem RHRS Suction/Isolation Valve Control Circultry MOV-8701 (IRH-2)

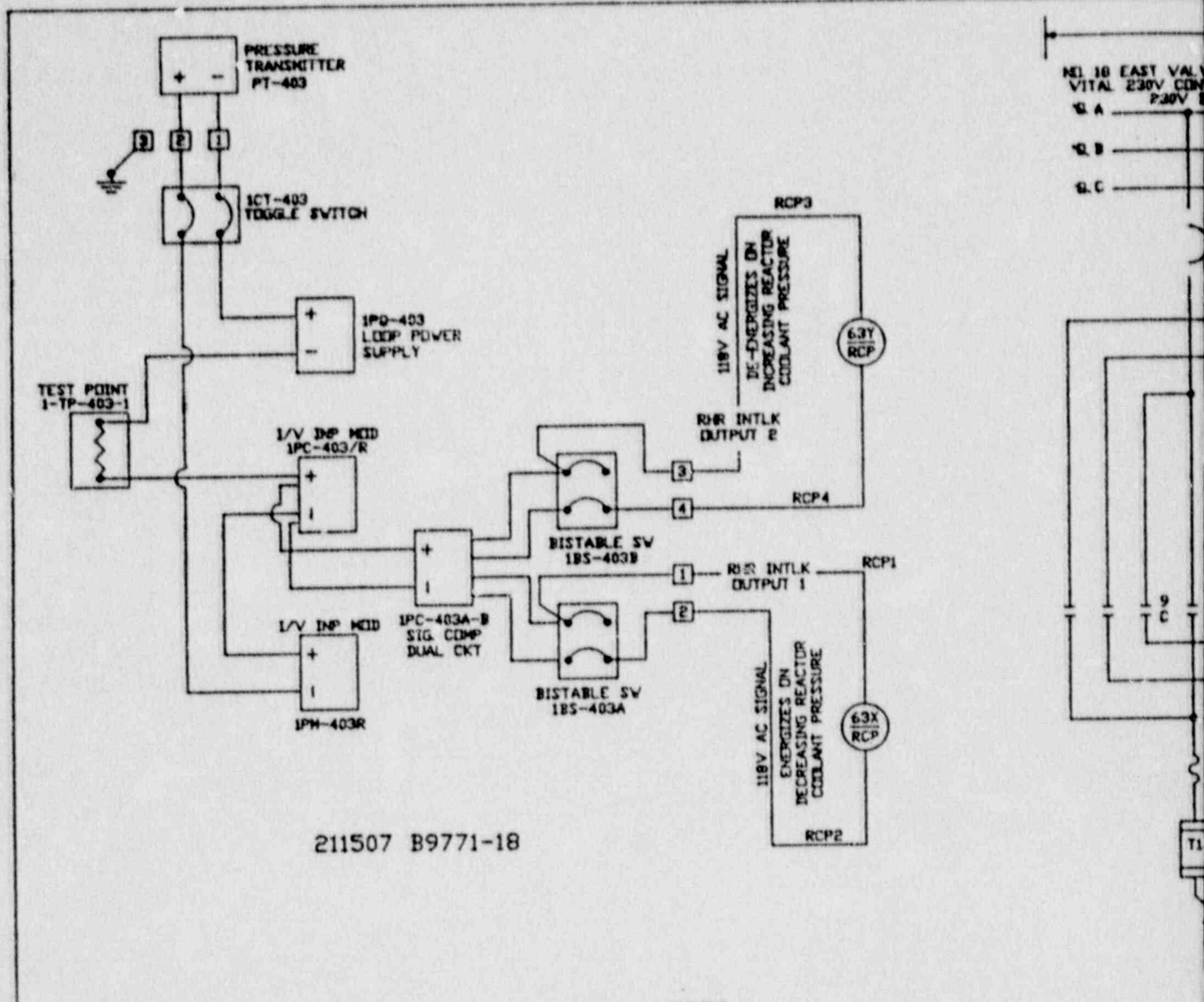

28
27
26
25
24
23
22
21
20
19
18
17
16
15
I
H
G
F
E
D
C
B
A



SI
APERTURE
CARD

Also Available On
Aperture Card

FIGURE B-3
SALEM VSEQUENCE
WITH ACI



LEGEND

- CONTROL CIRCUIT BREA...
- FUSE
- DIODE
- CONTACT OPEN
- CONTACT CLOSED
- THERMAL OVERLOADS
- (R) INDICATING LIGHTS R - RED G - GREEN
- VOLTAGE TRANSFORMER

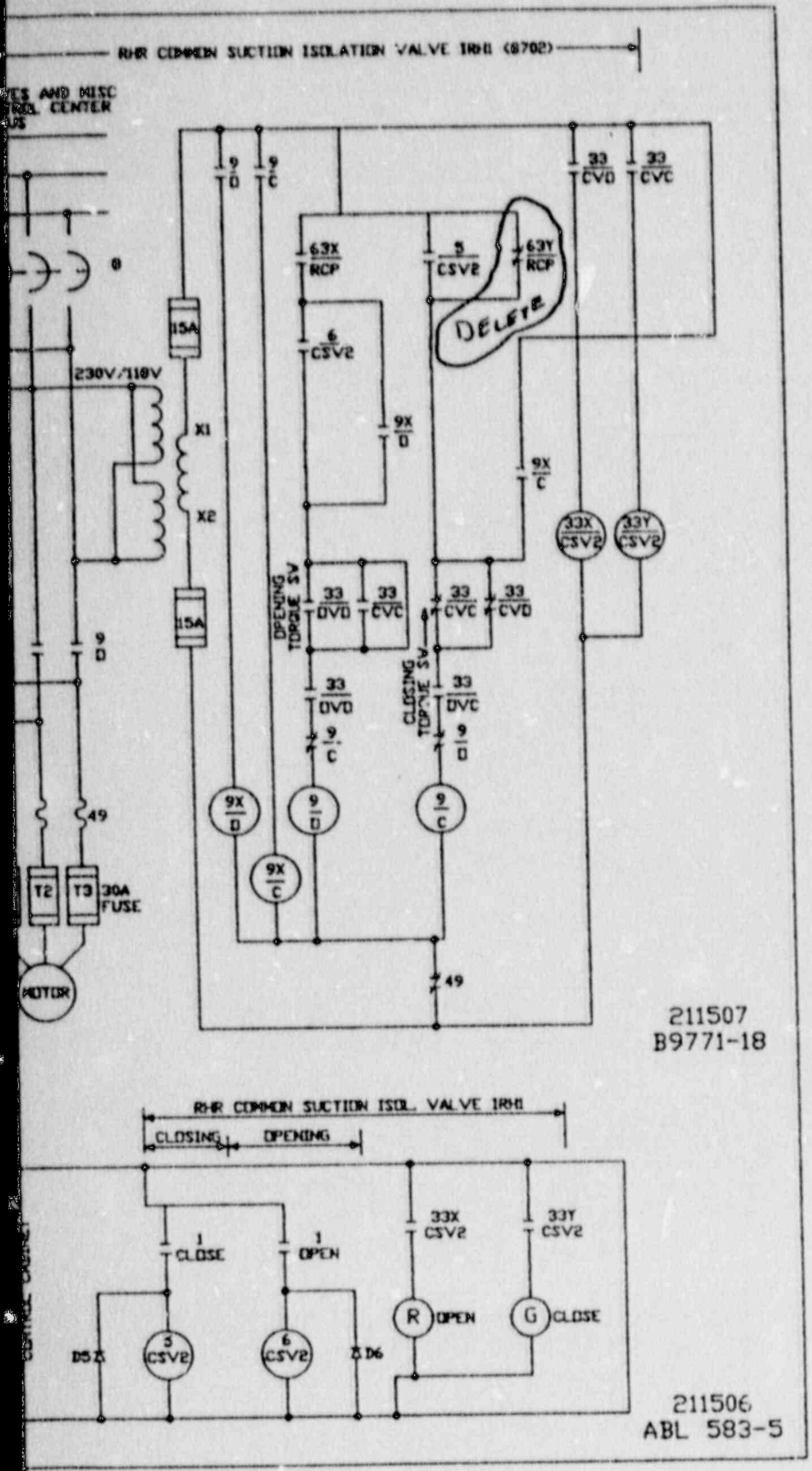
NOTES

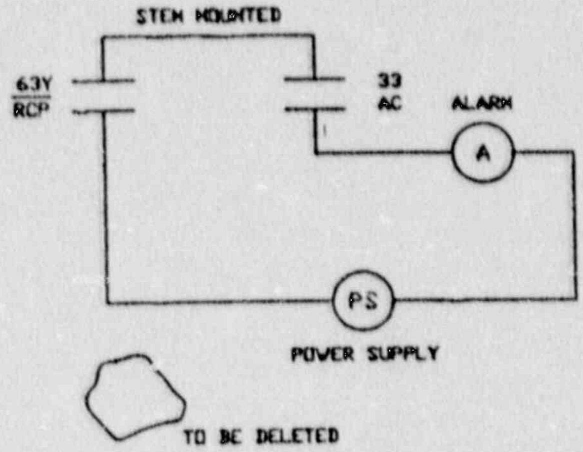
5/CSV2	CLOSING RELAY COIL
6/CSV2	OPENING RELAY COIL
33/OVO	VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY OPEN
33/OVC	VALVE LIMIT SWITCH OPEN WHEN VALVE IS FULLY CLOSED
33/CVO	VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY OPEN
33/CVC	VALVE LIMIT SWITCH CLOSED WHEN VALVE IS FULLY CLOSED
9/O	REVERSING CONTACTOR OPENING
9/C	REVERSING CONTACTOR CLOSING
63Y/RCP	REACTOR COOLANT PRESSURE AUX RELAY
63X/RCP	REACTOR COOLANT PRESSURE AUX RELAY
9X/C	AUX RELAY TO CONTACTOR CLOSING COILS
9X/O	AUX RELAY TO CONTACTOR OPENING COILS
33X/CSV2	VALVE FULLY OPEN AUX RELAY
33Y/CSV2	VALVE FULLY CLOSED AUX RELAY

RHR_1RH1

2/1/88

SALEM RHR SUCTION
ISOLATION VALVE 1RH1
CONTROL CIRCUITRY

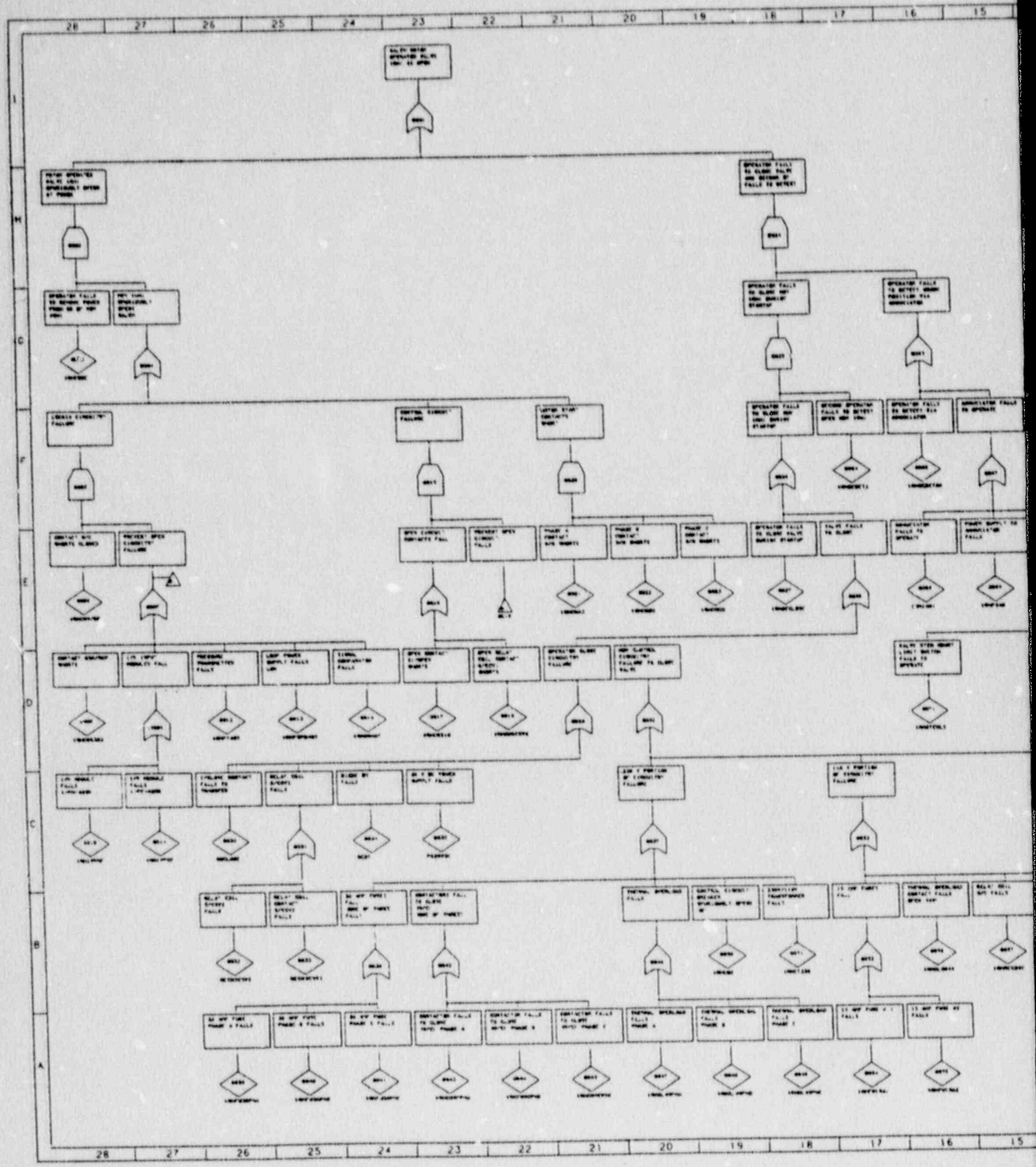




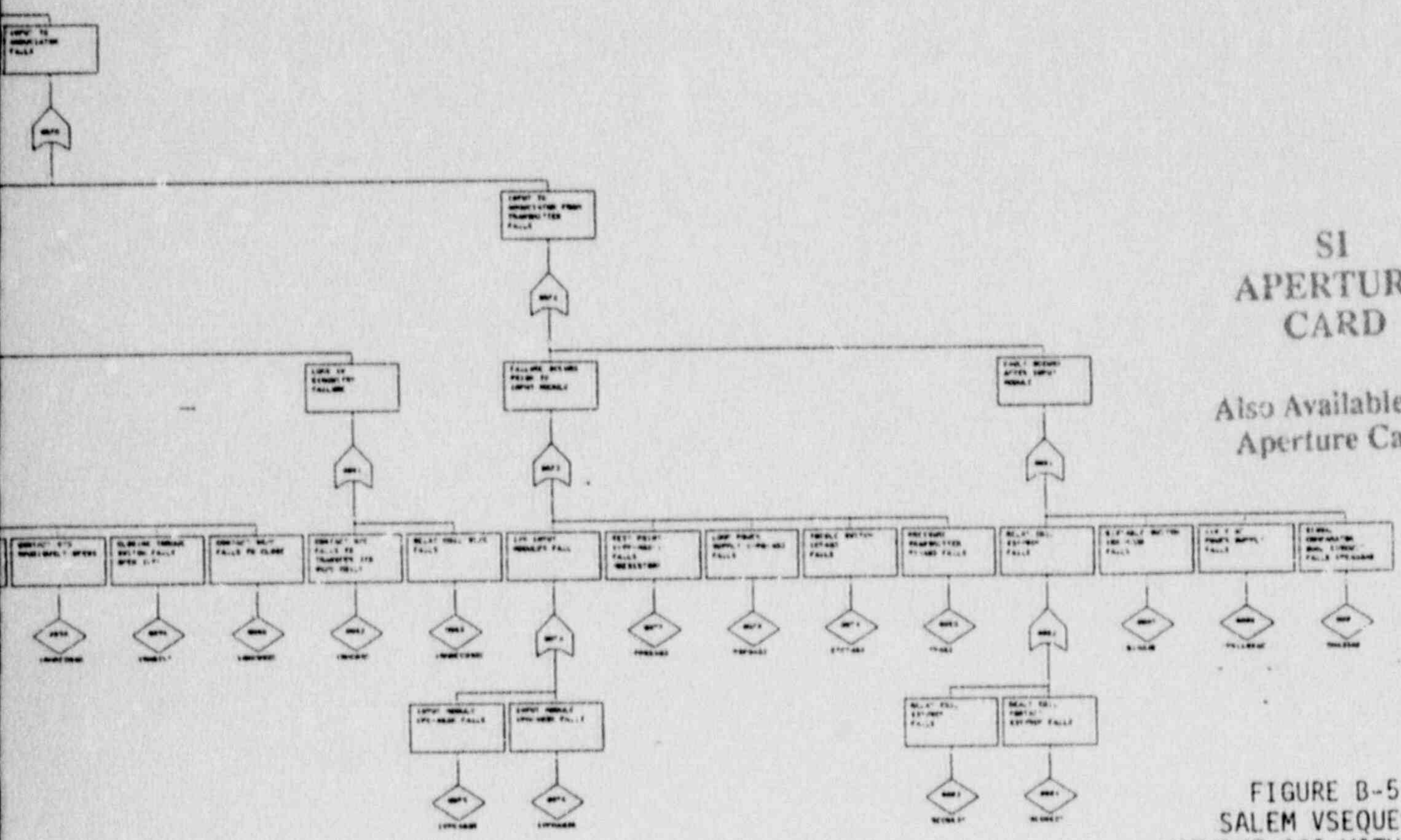
PROPOSED CHANGE

FIGURE B-4

Salem MOV-8702 Elementary Wiring Diagram - Proposed



28
27
26
25
24
23
22
21
20
19
18
17
16
15
I
H
G
F
E
D
C
B
A



SI
APERTURE
CARD

Also Available On
Aperture Card

FIGURE B-5
SALEM VSEQUENCE
WITHOUT ACI WITH ALARM

B.2 CALLAWAY

In order to determine the probabilities of the motor-operated suction valves being "OPEN" ($Q(V_1)$ and $Q(V_2)$ in equation 1), a detailed fault tree for the Callaway control circuitry associated with these valves was developed.

Utilizing the present control circuitry diagram shown in Figure B-6 for suction valves EJ-HV-8701A, EJ-HV-8701B, BB-PV-8702A, and BB-PV-8702B and the procedures for terminating the RHR system in preparation for startup, a fault tree was developed that considered how either suction valve would be "OPEN" at power conditions. Component failures and human errors were included in the fault tree. The fault tree developed for valve EJ-HV-8701A is shown in Figure B-7. (Because the control circuitry for the valves is identical except for component ID's, only one fault tree was developed to calculate the failure probability.)

The scenarios examined in the fault tree for the case with the autoclosure interlock are: 1) the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but due to some component failure, the valve does not close) and the autoclosure interlock fails to perform its function and does not close the valve and an operator fails to detect that the valve is not closed during startup or power operation.

For the deletion of the autoclosure interlock and the addition of an alarm as shown in Figure B-8 for valve EJ-HV-8701A, a detailed fault tree was also developed. The scenarios developed for this case are: 1) the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but it does not close) and the operator fails to detect that the valve is not closed via the presence of an alarm (or the alarm fails to operate). The fault tree developed for this case is shown in Figure B-9.

In each case (with the autoclosure interlock and without the autoclosure interlock), the first scenario is the same; only the second scenario differs due to the proposed modification.

For the Callaway analysis, the following assumptions and boundary conditions were utilized:

1. The operator closes the RHR suction valves utilizing a two-position type switch.

2. The operating supervisor verifies the RHR suction valves are closed before signing the checklist.

3. The indicating lights associated with the RHR suction valves do not have alarms associated with them.

4. A component failure would be detected in a 24 hour interval if it caused the suction isolation valve to spuriously open or fail to close.

In order to quantify the fault trees developed for these cases, each basic event probability was calculated and then input into the appropriate fault tree. For a component failure, the following formula was used:

$$Q(\text{component}) = (\lambda) \frac{T_{detect}}{2}$$

where

$Q(\text{component})$ = basic event probability

λ = failure rate for the component

T_{detect} = detection interval

Table B-5 shows the basic event probabilities for each component utilizing a 24 hour detection interval.

The human error probabilities were calculated using "The Handbook for Human Reliability Analysis," Reference 19, and Callaway's operating procedures for terminating the RHR system in preparation for startup. The calculations of the human error probabilities are shown in Table B-6.

CALLAWAY RESULTS

The probabilities for $Q(V_1)$ and $Q(V_2)$, the probability that the isolation valve is open, for each case are shown below:

	With Autoclosure Interlock	Without Autoclosure Interlock
$Q(V_1)$	1.04E-04	2.05E-06
$Q(V_2)$	1.04E-04	2.05E-06

The major cutsets (failure combinations) and the probabilities of the cutsets for each case (with and without the autoclosure interlock) are shown in Tables B-7 and B-8. For the case with the ACI (Table B-7), the dominant contributors are a component failure which causes the valve not to close along with the operator failing to detect that the valve did not close during startup and another operator failure to detect the wrong position during power operation.

For the ACI deletion case, the dominant contributors are: the operator fails to close the valve during startup along with the operator failing to detect that the valve is not closed during startup and either operator failure to detect via the alarm or the alarm fails to operate.

The frequency of an interfacing system LOCA, given these probabilities is calculated using:

$$F(VSEQ) = 2 \left[(\lambda)_2 Q(V_1) + (\lambda)_1 Q(V_2) + (\lambda)_2 Q(V_{1R}) \right]$$

where

2 = the number of RHR suction lines

$(\lambda)_2$ = failure rate of RCS valve (due to rupture)

$(\lambda)_1$ = failure rate of RHR valve (due to rupture)

$Q(V_1)$ = probability that RHR valve is open

$Q(V_2)$ = probability that RCS valve is open

$Q(V_{1R})$ = probability of rupture of RHR valve

The failure rate due to rupture of a motor-operated valve is 1.0E-7 per hr ($(\lambda)_1$ and $(\lambda)_2$). The quantity $Q(V_{1R})$ is determined by assuming that the total defined mission time is the time between refueling outages (i.e., every 18 months). The rupture of motor-operated valve is assumed to occur randomly in the time interval 0 - T_M where T_M is the total defined mission time. Therefore the probability of the valve rupturing is:

$$Q(V_{1R}) = (\lambda)\ \frac{T_M}{2}$$

$$= \frac{1E\text{-}07}{hr}\ \frac{(8760\ hrs/year * 1.5\ years)}{2}$$

$$= 6.57E\text{-}04$$

Entering the failure probabilities leads to the following frequency for an interfacing system LOCA for the case with the ACI:

$$\begin{aligned} F(VSEQ) &= 2[\ (\lambda)_2\ Q(V_1) + (\lambda)_1\ Q(V_2) + (\lambda)_2\ Q(V_{1R})\ ] \\ &= 2[\ 1E\text{-}07/hr *(1.04E\text{-}04) + (1E\text{-}07/hr)*(1.04E\text{-}04) + \\ &\quad 1E\text{-}07/hr *(6.57E\text{-}04)\ ] \\ &= 2[\ 1.04E\text{-}11/hr + 1.04E\text{-}11/hr + 6.57E\text{-}11/hr\ ] \\ &= 2[\ 8.65E\text{-}11/hr\ * (8760\ hrs/year)\ ] \\ &= 1.52E\text{-}06/year \end{aligned}$$

The same method was applied in the case without the ACI. The following summarizes the frequencies:

	With Autoclosure Interlock	Without Autoclosure Interlock
F(VSEQ)	1.52E-06/year	1.16E-06/year

The frequency of an Event V decreases by approximately 24 percent with removal of the ACI. The main contributor to the frequencies in each case is a double rupture of MOV EJ-HV-8701B then EJ-HV-8701A (or BB-PV-8702A then BB-PV-8702B) (frequency of 5.75E-07/year in both cases). The deletion of the ACI has no impact on this contributor. As can be seen, the frequency of a double rupture dominates the second case while the other contributor (the rupture of one valve while the other valve has failed open) does not contribute significantly in the case in which the ACI has been deleted. (The frequency for the rupture of one valve while the other is open decreases from 9.11E-8/year (1.04E-12/hr *8760 hrs/year) for the case with the ACI to 1.80E-09/year (2.05E-13/hr * 8760 hrs/year) for the case with the ACI deleted.) This is a significant decrease in the occurrence of an Event V by this failure mode. Thus, the deletion of the autoclosure interlock and the inclusion of an alarm is beneficial in reducing this contribution.

TABLE B-5
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
MV8701CBOE	OE	OPERATOR FAILS TO RE	1.600E-03	---	1.60E-03
UCNK734	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
UTPPT405	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
UPSPQY405	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
UCMPB405A	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
UBIPS405A	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
UCN33BCRWS	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
UCN33BCSUM	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
UCN33BCCHA	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
UCNHISOPEN	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
UCN420A	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
UMSCN420A	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
UMSCN420B	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
UMSCN420C	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
MVOECLOSE	OE	OPERATOR FAILS TO CL	3.200E-03	---	3.20E-03
CNCLOSE	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
CN42C/A	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
CB52	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
40AMPFUPHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
40AMPFUPHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
40AMPFUPHC	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
OL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06

TABLE B-5 (CONT.)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
OL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
OL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
MSCN42CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
MSCN42CB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
MSCN42CC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1AMPFUPHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1AMPFUPHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
CT480V120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
2AMPFU	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
OLCN49A/B	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
OLCN49B/B	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
OLCN49C/B	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
QSWS17	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
CN420/B	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
MSRECO42C	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
MVOEDETEC2	OE	SECOND OPERATOR FAIL	9.800E-01	---	9.80E-01
MVOEDETAC	OE	SECOND OPERATOR FAIL	9.800E-01	---	9.80E-01
LSZS8	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
CNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
RSPS405	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
CMPB405B	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
PSPQY405	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05

TABLE B-5 (CONT.)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
BIPS405B	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
TPPT405	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
MOVOEDETAN	OE	OPERATOR FAILS TO DE	2.660E-04	---	2.66E-04
MOV1AN1	AN	ANNUCIATOR ALL MODES	4.250E-06	1.200E+01	5.10E-05
MOVPSAN	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
MOVSTEMLS	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05

TABLE B-6

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Open and lock the power supply breakers for the RHR inlet valves EJ-HV-8701A, EJ-HV-8701B, BB-PV-8702A, BB-PV-8702B. Complete checklist, first and second checker.

REFERENCE: Step 4.5.7 in operating procedure OTN-EJ-00001 Residual Heat Removal System Revision 4, Section 4.5, Placing the RHR System in the Safety Injection Standby Lineup.

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open and lock power supply breaker

Median HEP = 0.003	Table 20-7	Long list > 10 items
Mean HEP = 3.75E-03		When procedures with checkoff
Error Factor = 3		provisions are correctly used

2. Commission error - Operator selects wrong circuit breaker

Median HEP = 0.005	Table 20-12	Select wrong circuit breaker in a
Mean HEP = 6.25E-3		group of circuit breakers densely
Error Factor = 3		grouped and identified by labels only

3. Recovery error - Second checker or Operating Superviser fails to detect error by others

Median HEP = 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP = 0.16		using written materials
Error Factor = 5		

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(6.25E-03)(0.16) + 3.75E-03(0.16) \\
&= 9.96E-04 + 6.0E-04 \\
&= 1.596E-03 \\
&= 1.60E-03
\end{aligned}
$$

Fault Tree Identifiers: MV8701CBOE

TABLE B-6
(Cont.)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: CLOSE BB-PV-8702A(B) and EJ-HV-8701A(B), RHR Suctions from the RCS. Perform Checklist 3 (RHR System Main Control Board Lineup for Safety Injection Standby) as listed, first and second checker.

REFERENCE: Step 4.6.2 and 4.5.5 in operating procedure OTN-EJ-00001 Residual Heat Removal System Revision 4, Section 4.5, Placing the RHR System in the Safety Injection Standby Lineup and Section 4.6, Cooldown of the RHR System, Post RCS Cooldown.

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated suction valve using two-position switch

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to turn control to close valve

Median HEP = 0.01 Mean HEP = 1.61E-02 Error Factor = 5	Table 20-12	Turn two position switch in wrong direction when design violates a strong populational stereotype and operating conditions are normal by labels only

3. Recovery error - Shift supervisor fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$P_{OE} = (1-3.75E-03)(1.61E-02)(0.16) + 3.75E-03(0.16)$$
$$= 2.556E-03 + 6.0E-04$$
$$= 3.166E-03$$
$$= 3.20E-03$$

Fault Tree Identifiers: MVOECLOSE

TABLE B-6
(Cont.)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Operator fails to detect wrong valve position

REFERENCE:

BREAKDOWN OF TASK:

1. Omission error - Operator fails to detect wrong valve position

   Median HEP = 0.98 Table 20-25 Legend light
   Other than annuciator light

   P_{OE} = 0.98

   Fault Tree Identifiers: MVOEDETEC2 and MVOEDETAC

TABLE B-6
(Cont.)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Operator fails to detect wrong valve position via annuciator

REFERENCE:

BREAKDOWN OF TASK:

1. Omission error - Operator fails to detect wrong valve position via annuciator and initiate some kind of corrective action

   Median HEP = 0.0001 Table 20-23 One annuciator
   Mean HEP = 2.66E-04
   Error Factor = 10

   P_{OE} = 2.66E-04

   Fault Tree Identifiers: MOVOEDETAN

TABLE B-7
CALLAWAY DOMINANT CUTSETS
FOR $Q(V_1)$
PROBABILITY THAT MOV EJ-HV-8701A IS OPEN
WITH ACI CASE

MEAN PROBABILITY OF FAILURE = 1.04E-04

	PROBABILITY	CUTSET DESCRIPTION
1.	3.46E-05	MOTOR START RELAY COIL 42 C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
2.	1.15E-05	LOCKIN CONTROL CIRCUIT CONTACT 42C/A FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
3.	1.15E-05	MOTOR START RELAY CONTACT 42C PHASE C FAILS TO TRANSFR SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
4.	1.15E-05	MOTOR START RELAY CONTACT 42C PHASE B FAILS TO TRANSFR SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
5.	1.15E-05	MOTOR START RELAY CONTACT 42 C PHASE A FAILS TO TRANSFR SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
6.	4.03E-06	CURRENT TRANSFORMER 480V/120V FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
7.	2.30E-06	TORQUE SWITCH WS/17 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
8.	1.73E-06	2 AMP FUSE FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
9.	1.73E-06	1 AMP FUSE PHASE B FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE

TABLE B-7 (Cont.)

CALLAWAY DOMINANT CUTSETS

FOR $Q(V_1)$

PROBABILITY THAT MOV EJ-HV-8701A IS OPEN

WITH ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
10.	1.73E-06	1 AMP FUSE PHASE A FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
11.	1.73E-06	THERMAL OVERLOAD 49 PHASE C SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
12.	1.73E-06	THERMAL OVERLOAD 49 PHASE B SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
13.	1.73E-06	THERMAL OVERLOAD 49 PHASE A SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
14.	1.73E-06	40 AMP FUSE PHASE C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
15.	1.73E-06	40 AMP FUSE PHASE B FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
16.	1.73E-06	40 AMP FUSE PHASE A FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
17.	2.66E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN MOV LIMIT SWITCH CONTACT ZS/8 FAILS TO TRANSFER
18.	2.30E-07	CONTACT 420/B SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
19.	2.30E-07	THERMAL OVERLOAD CONTACT 49C/B SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE

TABLE B-7 (Cont.)

CALLAWAY DOMINANT CUTSETS

FOR $Q(V_1)$

PROBABILITY THAT MOV EJ-HV-8701A IS OPEN

WITH ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
20.	2.30E-07	THERMAL OVERLOAD CONTACT 49B/B SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE
21.	2.30E-07	THERMAL OVERLOAD CONTACT 49A/B SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT OPEN VALVE

TABLE B-8

CALLAWAY DOMINANT CUTSETS

FOR $Q(V_1)$

PROBABILITY THAT MOV EJ-HV-8701A IS OPEN

WITHOUT ACI CASE

MEAN PROBABILITY OF FAILURE = 2.05E-06

	PROBABILITY	CUTSET DESCRIPTION
1.	8.34E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT VIA ANNUCIATOR
2.	2.72E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV VALVE STEM MOUNT LIMIT SWITCH FAILS TO OPERATE
3.	2.18E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV POWER SUPPLY TO ANNUCIATOR FAILS
4.	2.18E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV LOOP POWER SUPPLY PQY-405 FAILS
5.	1.60E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV ANNUCIATOR FAILS TO OPERATE
6.	1.09E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV DUAL COMPARATOR PB405B FAILS
7.	1.05E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV PRESSURE TRANSMITTER PT-405 FAILS LOW
8.	6.21E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV BISTABLE SWITCH PS/405B FAILS
9.	9.38E-09	MOTOR START RELAY COIL 42 C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT VIA ANNUCIATOR

TABLE B-8 (CONT.)
CALLAWAY DOMINANT CUTSETS
FOR $Q(V_1)$
PROBABILITY THAT MOV EJ-HV-8701A IS OPEN
WITHOUT ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
10.	3.13E-09	OPERATOR CLOSE CIRCUITY HIS/CLOSE FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT VIA ANNUCIATOR
11.	3.13E-09	LOCKIN CONTROL CIRCUIT CONTACT 42C/A FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT VIA ANNUCIATOR
12.	3.13E-09	MOTOR START RELAY CONTACT 42C PHASE C FAILS TO TRANSFR SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT VIA ANNUCIATOR
13.	3.13E-09	MOTOR START RELAY CONTACT 42C PHASE B FAILS TO TRANSFR SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT VIA ANNUCIATOR
14.	3.13E-09	MOTOR START RELAY CONTACT 42 C PHASE A FAILS TO TRANSFR SECOND OPERATOR FAILS TO DETECT OPEN MOV OPERATOR FAILS TO DETECT VIA ANNUCIATOR
15.	3.06E-09	MOTOR START RELAY COIL 42 C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV VALVE STEM MOUNT LIMIT SWITCH FAILS TO OPERATE
16.	2.46E-09	MOTOR START RELAY COIL 42 C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV POWER SUPPLY TO ANNUCIATOR FAILS
17.	2.46E-09	MOTOR START RELAY COIL 42 C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV LOOP POWER SUPPLY PQY-405 FAILS
18.	1.80E-09	MOTOR START RELAY COIL 42 C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV ANNUCIATOR FAILS TO OPERATE

TABLE B-8 (CONT.)

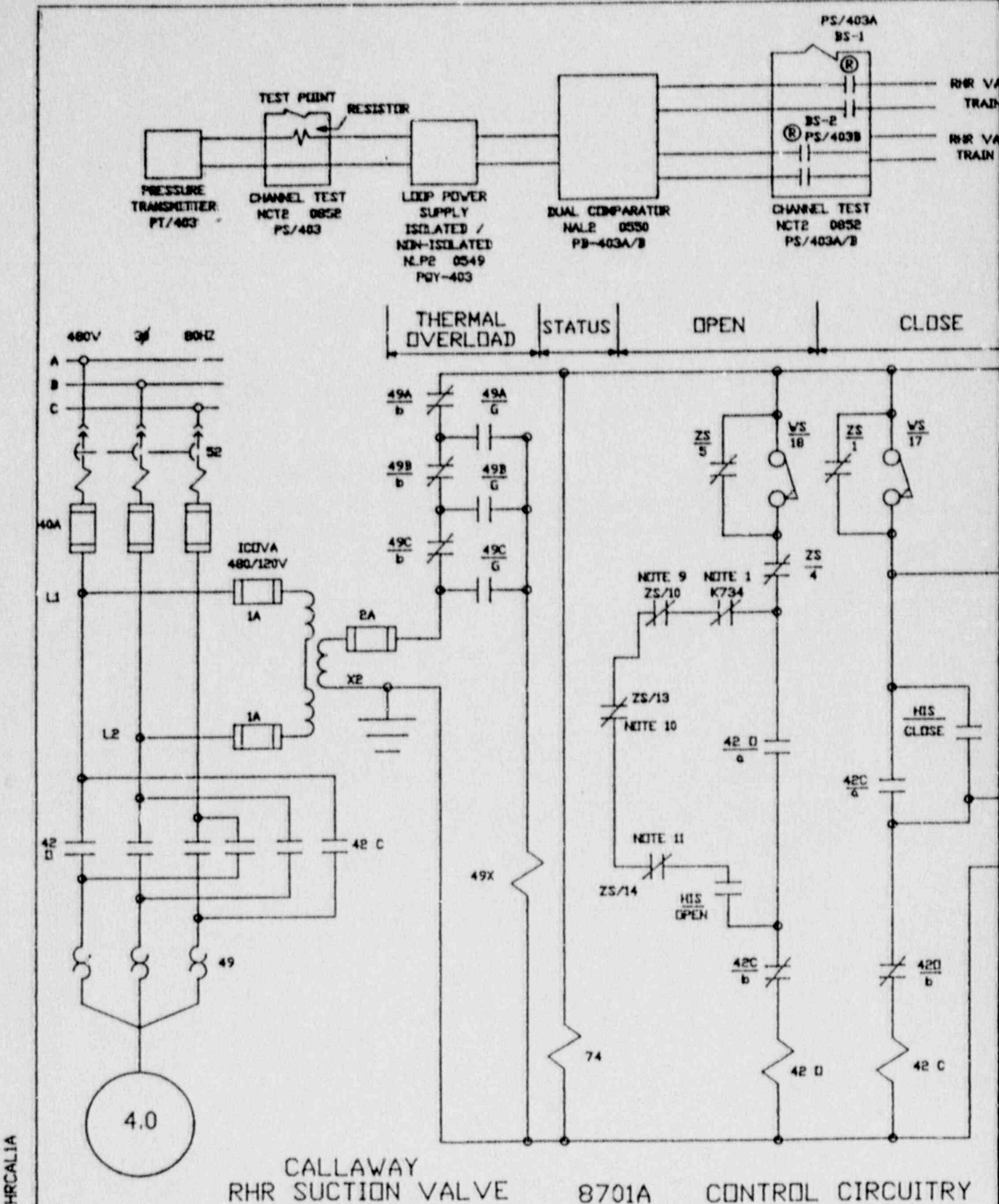
CALLAWAY DOMINANT CUTSETS

FOR $Q(V_1)$

PROBABILITY THAT MOV EJ-HV-8701A IS OPEN

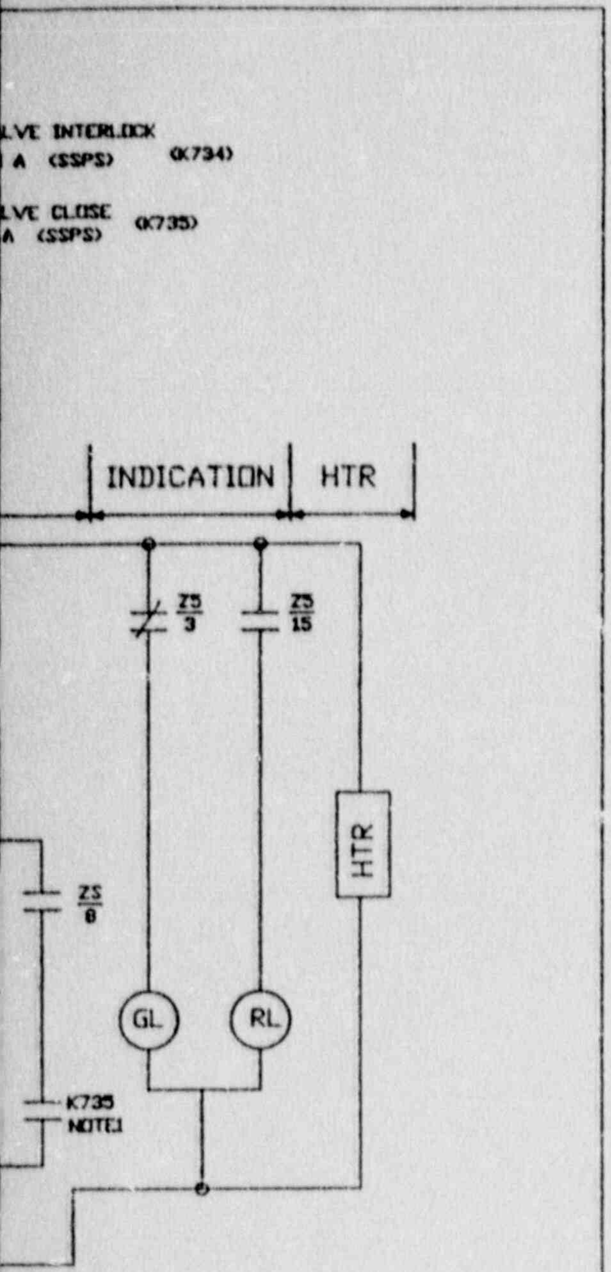
WITHOUT ACI CASE

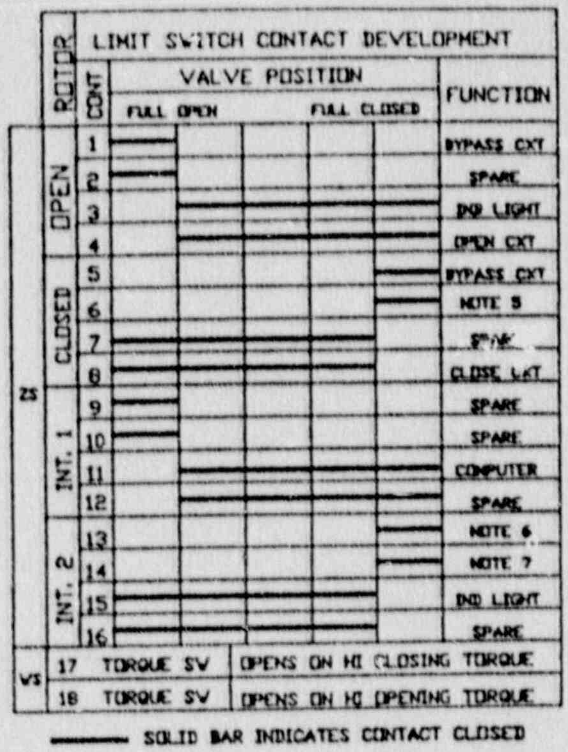
	PROBABILITY	CUTSET DESCRIPTION
19.	1.23E-09	MOTOR START RELAY COIL 42 C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV DUAL COMPARATOR PB405B FAILS
20.	1.19E-09	MOTOR START RELAY COIL 42 C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV PRESSURE TRANSMITTER PT-405 FAILS LOW



CALLAWAY
RHR SUCTION VALVE 8701A CONTROL CIRCUITRY

1/23/88





OPEN
GL | RL
CLOSE

CUTLER-HAMMER TYPE E30 JY9 WITH TWO KLA3 CONTACT BLOCKS

CONTACT	POSITION NORM	POSITION CLOSE	POSITION OPEN
1 •–| |–• 1T	X	X	
3 •–| |–• 3T			X
2 •–| |–• 2B	X		X
4 •–| |–• 4B		X	

HAND INDICATING SWITCH
HIS - SEE TABLE A
MOMENTARY CONTACT

NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
9. CONTACT CLOSED ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
10. CONTACT CLOSED ON SUMP TO NO. 1 RHR PUMP VALVE CLOSED
11. CONTACT CLOSES ON RHR PUMP 1 TO CHARGING PUMP VALVE CLOSED

5. INTERLOCK TO SCH. IEJG04A
6. INTERLOCK TO SCH. IEJG06A
7. RWST LEVEL TEST CKT.

REFERENCES:

BECHTEL	WESTINGHOUSE
E-23EJ05A(Q) REV 0	8809D50 SHEET 32

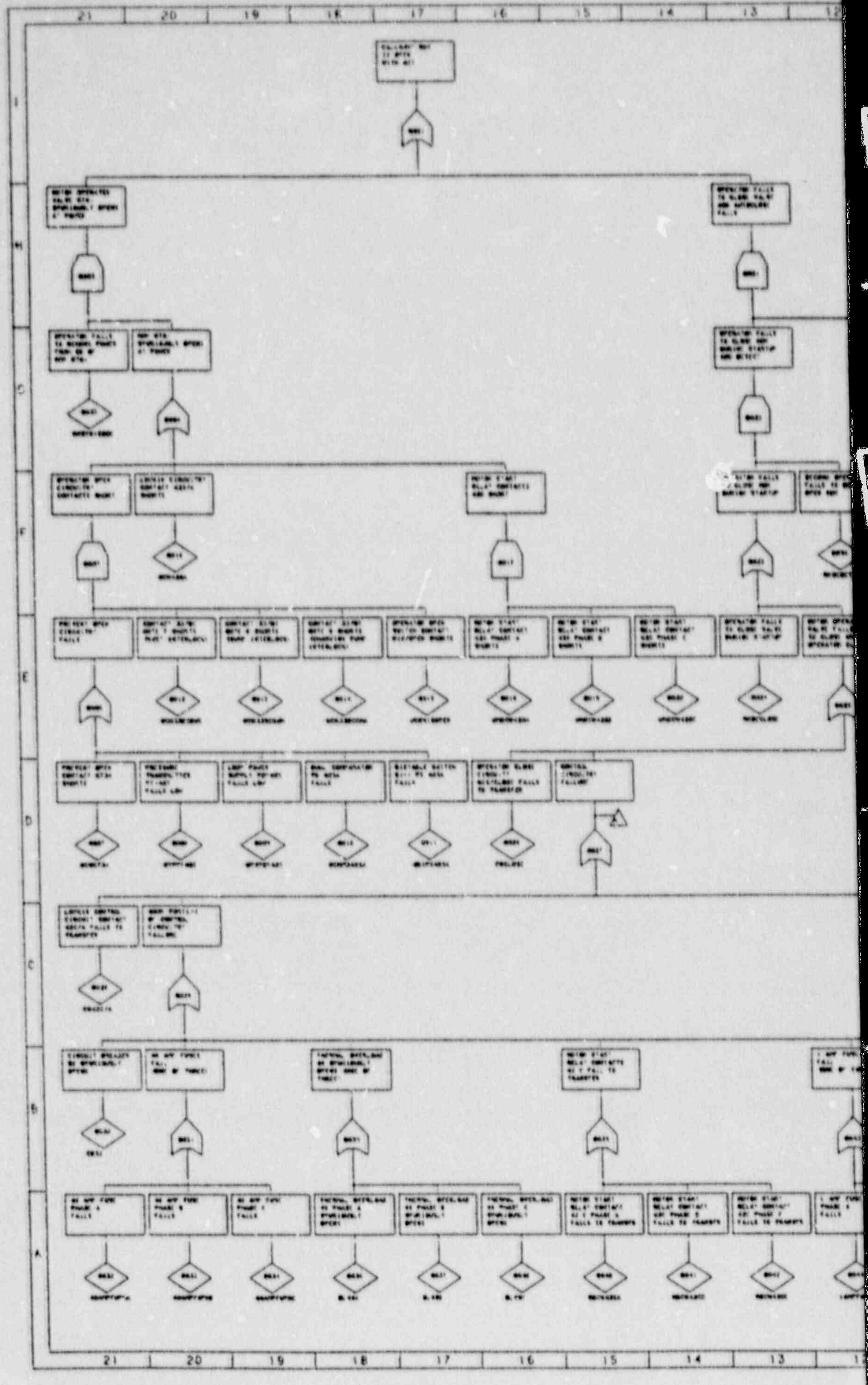
SI APERTURE CARD

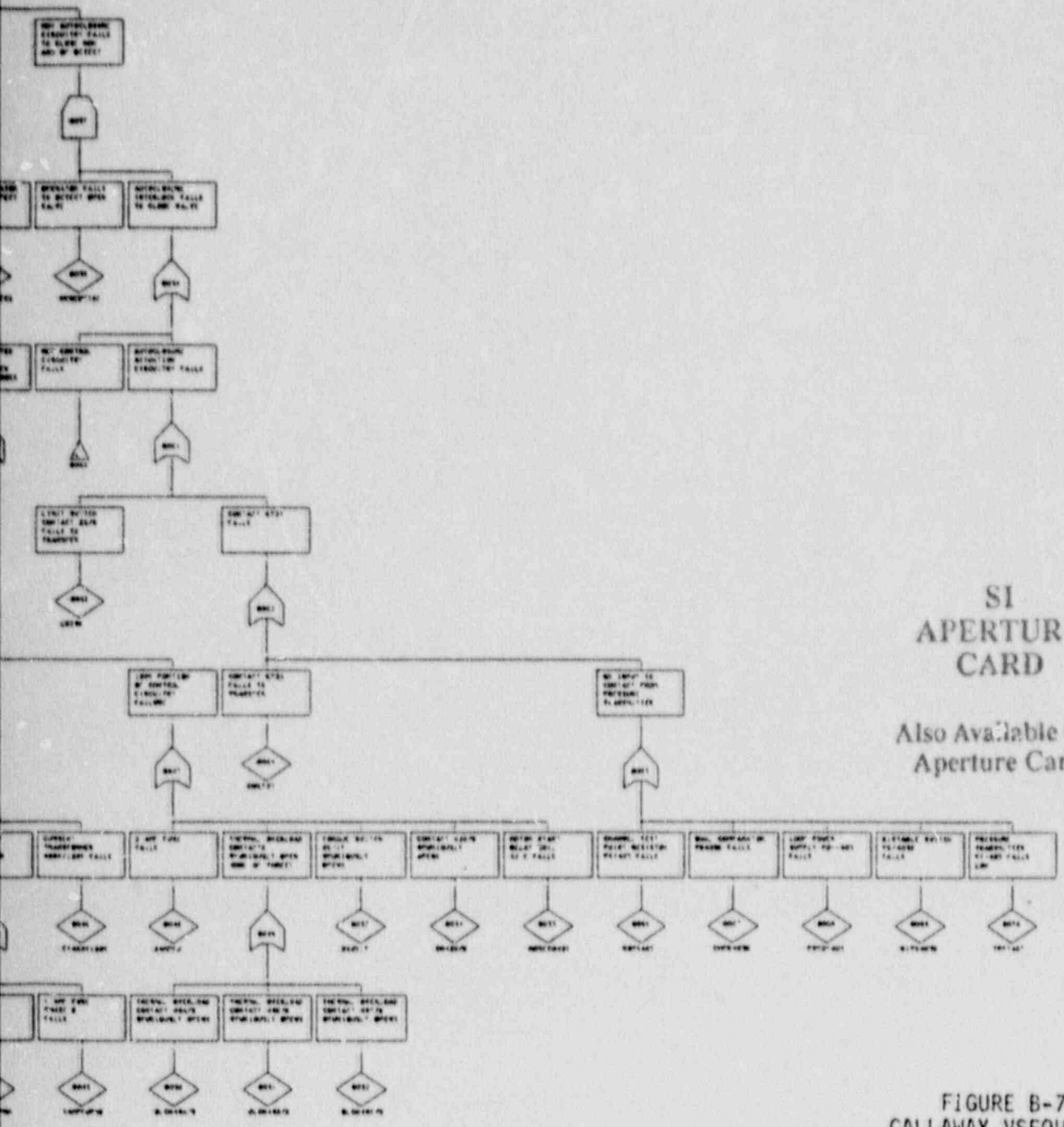
Also Available On Aperture Card

FIGURE B-6

Callaway RHRS Suction/Isolation Valve Control Circuitry - MOV-8701A

8911150026-42

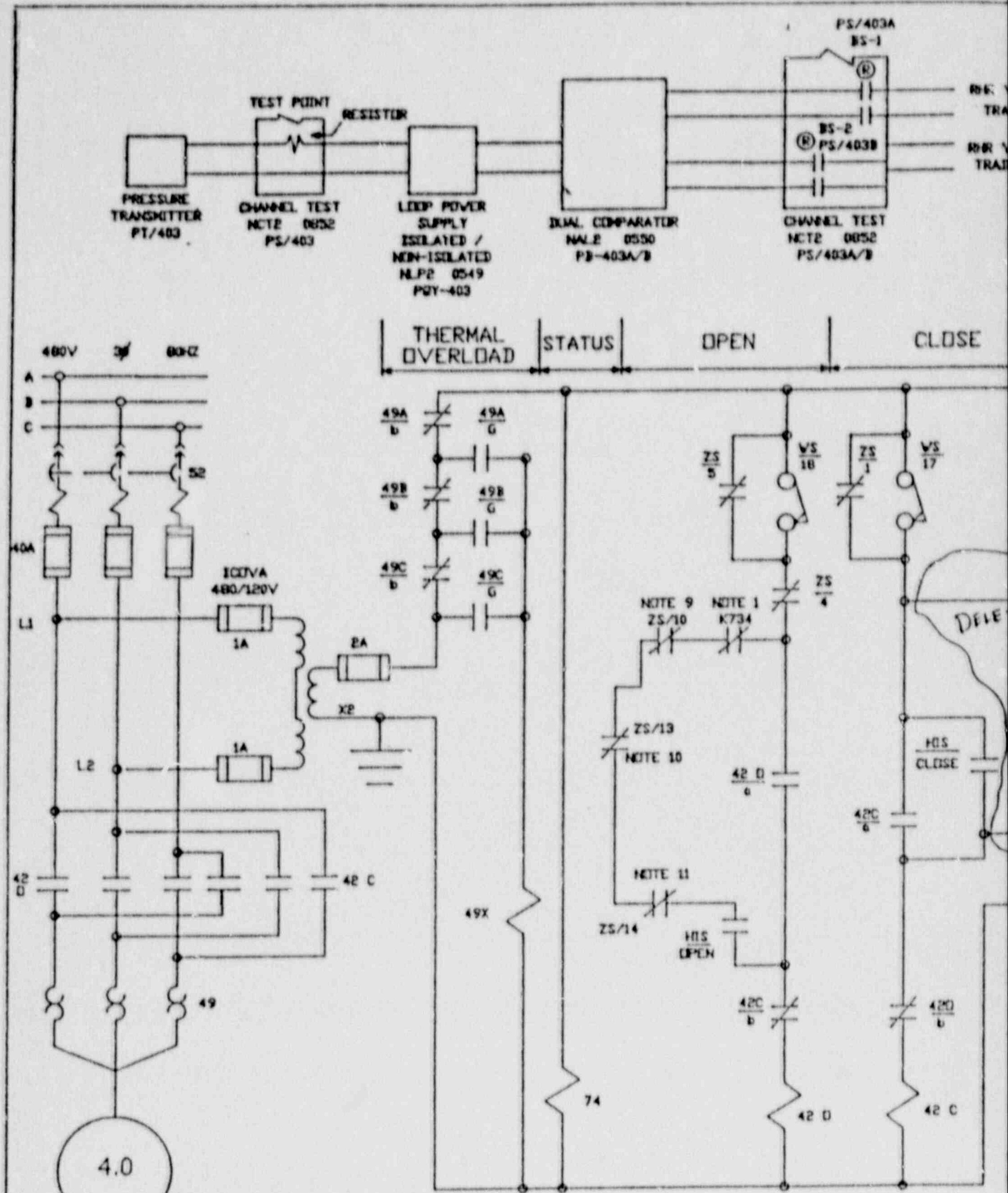




SI
APERTURE
CARD

Also Available On
Aperture Card

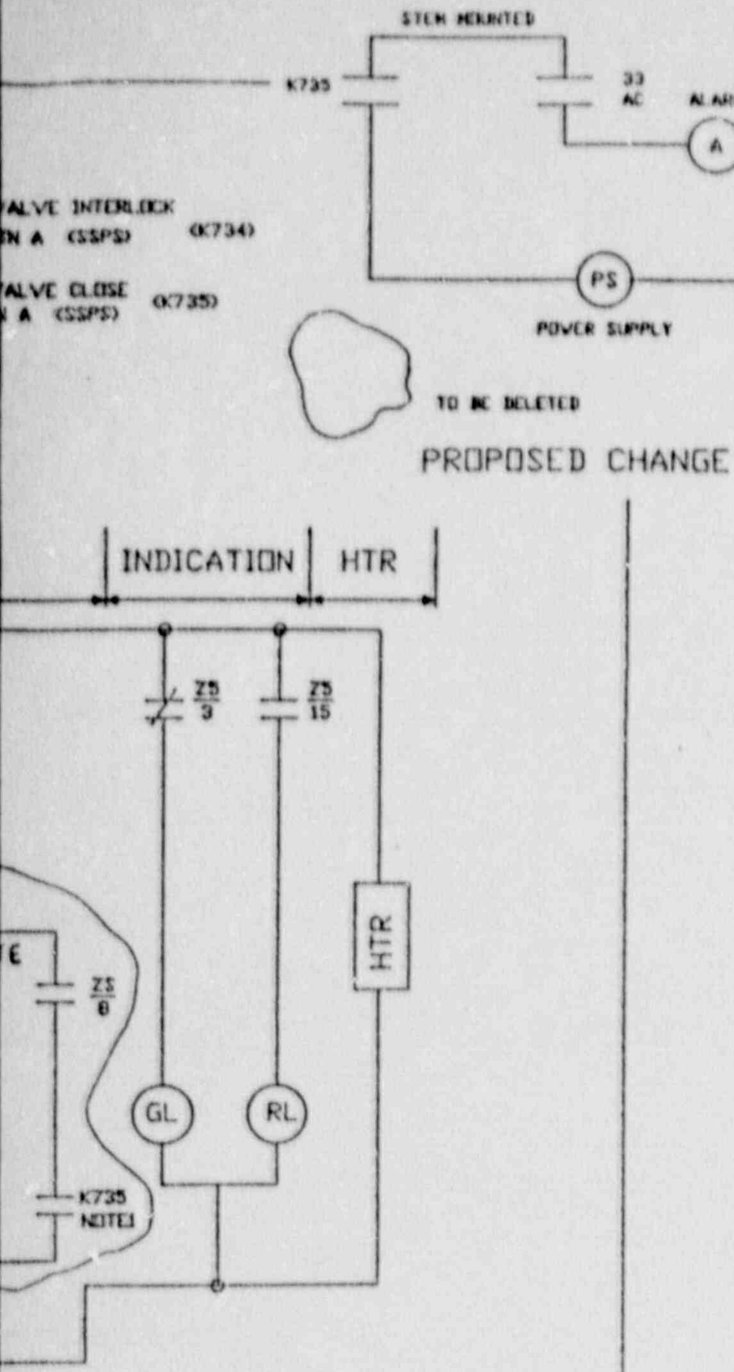
FIGURE B-7
CALLAWAY VSEQUENCE
WITH ACI



CALLAWAY
RHR SUCTION VALVE 8701A CONTROL CIRCUITRY

RHRCALIA

1/23/88



LIMIT SWITCH CONTACT DEVELOPMENT

	ROTOR	CONT	FULL OPEN				FULL CLOSED	FUNCTION
ZS	OPEN	1	—					BYPASS CKT
		2	—					SPARE
		3		—	—	—	—	IND LIGHT
		4		—	—	—	—	OPEN CKT
	CLOSED	5					—	BYPASS CKT
		6					—	NOTE 5
		7	—	—	—	—		SPARE
		8	—	—	—	—		CLOSE CKT
	INT. 1	9	—					SPARE
		10	—					SPARE
		11		—	—	—	—	COMPUTER
		12		—	—	—	—	SPARE
	INT. 2	13					—	NOTE 6
		14					—	NOTE 7
		15	—	—	—	—		IND LIGHT
		16	—	—	—	—		SPARE
VS		17	TORQUE SW		OPENS ON HI CLOSING TORQUE			
		18	TORQUE SW		OPENS ON HI OPENING TORQUE			

——— SOLID BAR INDICATES CONTACT CLOSED

OPEN
GL | RL
CLOSE

CUTLER-HAMMER TYPE E30 JY9 WITH TYPE [illegible]A3 CONTACT BLOCKS

CONTACT	NORM	CLOSE	OPEN
1 •—┤├—• 1T	X	X	
3 •—┤├—• 3T			X
2 •—┤├—• 2B	X		X
4 •—┤├—• 4B		X	

HAND INDICATING SWITCH
HIS - SEE TABLE A
MOMENTARY CONTACT

SI
APERTURE
CARD

Also Available On
Aperture Card

NOTES:

1. CONTACT K-734 OPENS ON HIGH-1 AND K-735 CLOSES ON HIGH-2 RCS PRESSURE
5. INTERLOCK TO SCH. IEJG04A
6. INTERLOCK TO SCH. IEJG06A
7. RWST LEVEL TEST CKT.
9. CONTACT CLOSED ON REFUELING WATER STORAGE TANK TO RHR PUMP MOV CLOSED
10. CONTACT CLOSED ON SUMP TO NO. 1 RHR PUMP VALVE CLOSED
11. CONTACT CLOSES ON RHR PUMP 1 TO CHARGING PUMP VALVE CLOSED

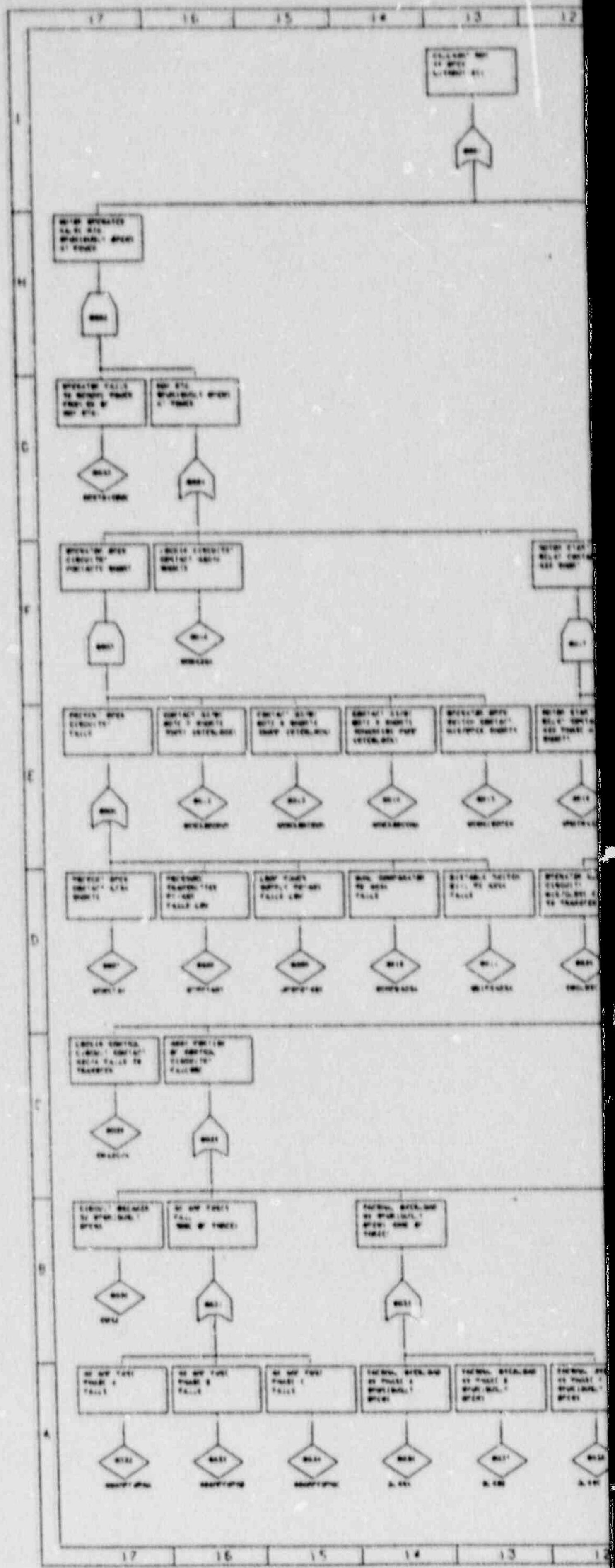
REFERENCES:

BECHTEL	WESTINGHOUSE
E-23EJ05A(Q) REV 0	8609D50 SHEET 32

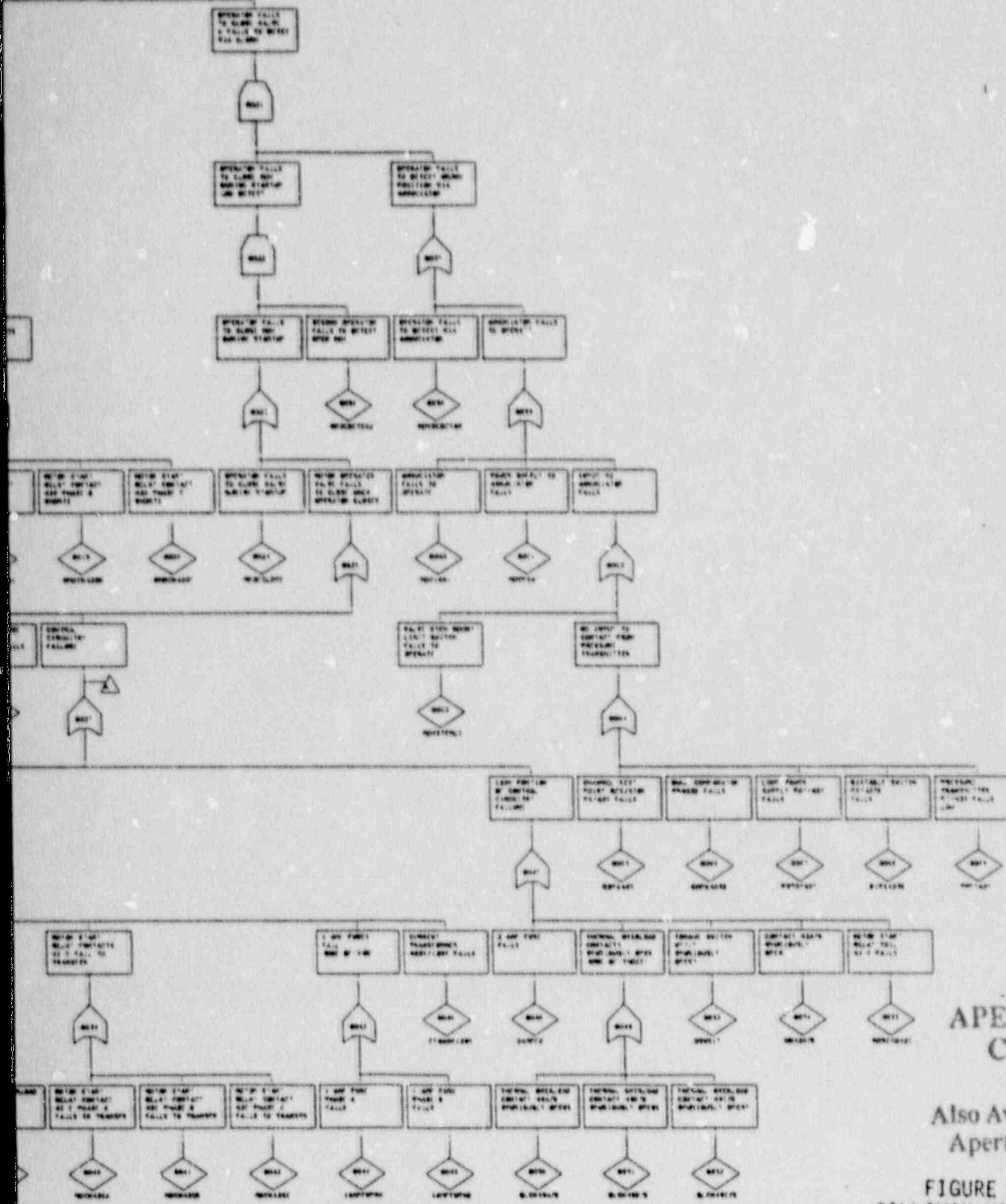
FIGURE B-8

Callaway Elementary Wiring Diagram Changes for MOV-8701A

8911150026-44



17
16
15
14
13
12
I
H
G
F
E
D
C
B
A



SI
APERTURE
CARD

Also Available On
Aperture Card

FIGURE B-9
CALLAWAY VSEQUENCE
WITHOUT ACI WITH ALARM

B.3 NORTH ANNA

In order to determine the probabilities of the motor-operated suction valves being "OPEN" ($Q(V_1)$ and $Q(V_2)$ in equation 1), a detailed fault tree for the North Anna control circuitry associated with these valves was developed.

Utilizing the present control circuitry diagram shown in Figure B-10 for suction valves MOV 1700 and MOV 1701 and the procedures for terminating the RHR system in preparation for startup, a fault tree was developed that considered how either suction valve would be "OPEN" at power conditions. Component failures and human errors were included in the fault tree. The fault tree developed for valve MOV 1700 is shown in Figure B-11. (Because the control circuitry for the valves is identical except for component ID's, only one fault tree was developed to calculate the failure probability.)

The scenarios examined in the fault tree for the case with the autoclosure interlock are: 1)the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but due to some component failure, the valve does not close) and the autoclosure interlock fails to perform its function and does not close the valve and an operator fails to detect that the valve is not closed during startup or power operation.

For the deletion of the autoclosure interlock and the addition of an alarm as shown in Figure B-12 for valve MOV 1700, a detailed fault tree was also developed. The scenarios developed for this case are: 1) the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but it does not close) and the operator fails to detect that the valve is not closed via the presence of an alarm (or the alarm fails to operate). The fault tree developed for this case is shown in Figure B-13.

In each case (with the autoclosure interlock and without the autoclosure interlock), the first scenario is the same; only the second scenario differs due to the proposed modification.

For the North Anna analysis, the following assumptions and boundary conditions were utilized:

1. The operator closes the RHR suction valves utilizing a push-button type switch.

2. The shift supervisor verifies the RHR suction valves are closed before signing the check off sheet.

3. The indicating lights associated with the RHR suction valves do not have alarms associated with them.

4. A component failure would be detected in a 24 hour interval if it caused the suction isolation valve to spuriously open or fail to close.

In order to quantify the fault trees developed for these cases, each basic event probability was calculated and then input into the appropriate fault tree. For a component failure, the following formula was used:

$$Q(\text{component}) = (\lambda)\,\frac{T_{detect}}{2}$$

where

$Q(\text{component})$ = basic event probability

λ = failure rate for the component

T_{detect} = detection interval

Table B-9 shows the basic event probabilities for each component utilizing a 24 hour detection interval.

The human error probabilities were calculated using "The Handbook for Human Reliability Analysis," Reference 19, and North Anna's operating procedures for terminating the RHR system in preparation for startup. The calculations of the human error probabilities are shown in Table B-10.

NORTH ANNA RESULTS

The probabilities for $Q(V_1)$ and $Q(V_2)$, the probability that the isolation valve is open, for each case are shown below:

	With Autoclosure Interlock	Without Autoclosure Interlock
$Q(V_1)$	2.01E-04	9.55E-07
$Q(V_2)$	2.01E-04	9.55E-07

The major cutsets (failure combinations) and the probabilities of the cutsets for each case (with and without the autoclosure interlock) are shown in Tables B-11 and B-12. For the case with the ACI (Table B-11), the dominant contributors are a component failure which causes the valve not to close along with the operator failing to detect that the valve did not close during startup and another operator failure to detect the wrong position during power operation.

For the ACI deletion case, the dominant contributors are: the operator fails to close the valve during startup along with the operator failing to detect that the valve is not closed during startup and either operator failure to detect via the alarm or the alarm fails to operate.

The frequency of an interfacing system LOCA, given these probabilities is calculated using:

$$F(VSEQ) = (\lambda)_2\, Q(V_1) + (\lambda)_1\, Q(V_2) + (\lambda)_2\, Q(V_{1R})$$

where

$(\lambda)_2$ = failure rate of RCS valve (due to rupture)
$(\lambda)_1$ = failure rate of RHR valve (due to rupture)
$Q(V_1)$ = probability that RHR valve is open
$Q(V_2)$ = probability that RCS valve is open
$Q(V_{1R})$ = probability of rupture of RHR valve

The failure rate due to rupture of a motor-operated valve is 1.0E-7 per hr ($(\lambda)_1$ and $(\lambda)_2$). The quantity $Q(V_{1R})$ is determined by assuming that the total defined mission time is the time between refueling outages (i.e., every 18 months). The rupture of motor-operated valve is assumed to occur randomly in the time interval $0 - T_M$ where T_M is the total defined mission time. Therefore the probability of the valve rupturing is:

$$Q(V_{1R}) = (\lambda)\,\frac{T_M}{2}$$

$$= \frac{1E\text{-}07}{hr}\;\frac{(8760\ hrs/year * 1.5\ years)}{2}$$

$$= 6.57E\text{-}04$$

Entering the failure probabilities leads to the following frequency for an interfacing system LOCA for the case with the ACI:

$$\begin{aligned} F(VSEQ) &= (\lambda)_2\, Q(V_1) + (\lambda)_1\, Q(V_2) + (\lambda)_2\, Q(V_{1R}) \\ &= 1E\text{-}07/hr * (2.01E\text{-}04) + (1E\text{-}07/hr) * (2.01E\text{-}04) + \\ &\quad 1E\text{-}07/hr * (6.57E\text{-}04) \\ &= 2.01E\text{-}11/hr + 2.01E\text{-}11/hr + 6.57E\text{-}11/hr \\ &= 1.06E\text{-}10/hr * (8760\ hrs/year) \\ &= 9.28E\text{-}07/year \end{aligned}$$

The same method was applied in the case without the ACI. The following summarizes the frequencies:

	With Autoclosure Interlock	Without Autoclosure Interlock
F(VSEQ)	9.28E-07/year	5.77E-07/year

The frequency of an Event V decreases by approximately 38 percent with removal of the ACI. The main contributor to the frequencies in each case is a double rupture of MOV 1700 then MOV 1701 (frequency of 5.75E-07/year in both cases). The deletion of the ACI has no impact on this contributor. As can be seen, the frequency of a double rupture dominates the second case while the other contributor (the rupture of one valve while the other valve has failed open) does not contribute significantly in the case in which the ACI has been deleted. (The frequency for the rupture of one valve while the other is open decreases from 1.76E-7/year (2.01E-11/hr *8760 hrs/year) for the case with the ACI to 8.37E-10/year (9.55E-14/hr * 8760 hrs/year) for the case with the ACI deleted.) This is a significant decrease in the occurrence of an Event V by this failure mode. Thus, the deletion of the autoclosure interlock and the inclusion of an alarm is beneficial in reducing this contribution.

TABLE B-9

NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
MV1700CBOE	OE	OPERATOR FAILS TO RE	1.600E-03	---	1.60E-03
UCN520Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
USWQ	SW	PUSH BUTTON SWITCH A	1.220E-06	1.200E+01	1.46E-05
UCN14021XQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
UBIPS14021	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
UCMPC1402	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
UPSPQ1402	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
UTP1402	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
UMSCN520A	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
UMSCN520B	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
UMSCN520C	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
1RHOECLOSE	OE	OPERATOR FAILS TO CL	1.200E-03	---	1.20E-03
CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
OL49AF	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
OL49CF	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
MSCN52CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
MSCN52CB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
MSCN52CC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
CT480/120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
FU6AMP1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
FU6AMP2	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
OLCN40U	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05

TABLE B-9 (CONT.)
NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
LS8U	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
QSTS17U	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
CN520U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
RECO52CF	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
CN52CK	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
SWK	SW	PUSH BUTTON SWITCH A	1.220E-06	1.200E+01	1.46E-05
1RHOEDET2	OE	SECOND OPERATOR FAIL	9.800E-01	---	9.80E-01
MV1700MECH	MV	FAILURE TO CLOSE	1.000E-05	1.200E+01	1.20E-04
PT1402F	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
RSPS1402	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
PSPQ1402	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
CMPC1402	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
BIPS14022	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
RECO14022X	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
RECN14022X	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHOEDETAC	OE	SECOND OPERATOR FAIL	9.800E-01	---	9.80E-01
1RHOEDETAN	OE	OPERATOR DETECT ANNU	2.660E-04	---	2.66E-04
1RH1AN1	AN	ANNUCIATOR ALL MODES	4.250E-06	1.200E+01	5.10E-05
1RHPSAN	PS	POWER SUPPLY ANNUCIA	5.800E-06	1.200E+01	6.96E-05
1RHSTEMLS	LS	STEM LIMIT SWITCH AL	7.220E-06	1.200E+01	8.66E-05

TABLE B-10

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Close MOV-1700. Close MOV-1701. De-energize MOV-1700 and MOV-1701 and LOCK OPEN the breakers. Signoff by verifier.

REFERENCE: Steps 4.2.6 , 4.2.7 and 4.2.8 in operating procedure I-OP-14.0/14.1(4/87)- Residual Heat Removal System- Section 4.2 Removing the RHR System from operation.

BREAKDOWN OF TASK:

1. Omission error - Operator fails to clear and lock open power supply breaker

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator selects wrong circuit breaker

Median HEP = 0.005 Mean HEP = 6.25E-03 Error Factor = 3	Table 20-12	Select wrong circuit breaker in a group of circuit breakers densely grouped and identified by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$P_{OE} = (1-3.75E-03)(6.25E-03)(0.16) + 3.75E-03(0.16)$$
$$= 9.96E-04 + 6.0E-04$$
$$= 1.596E-03$$
$$= 1.60E-03$$

Fault Tree Identifiers: MV1700OE

TABLE B-10
(Cont.)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Operator fails to detect wrong valve position

REFERENCE:

BREAKDOWN OF TASK:

1. Omission error - Operator fails to detect wrong valve position

   HEP = 0.98 Table 20-25 Legend light
   Other than annuciator light

$P_{OE} = 0.98$

Fault Tree Identifiers: 1RHOEDET2 and 1RHOEDETAC

TABLE B-10
(Cont.)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: CLOSE MOV-1700 and MOV-1701. Initialize signoff sheet. Complete and verify.

REFERENCE: Steps 4.2.6 and 4.2.7 in operating procedure 1-OP-14.0/14.1 (4/30/87) - Removing the RHR system from operation.

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated suction valve using push-button switch

Median HEP = 0.003	Table 20-7	Long list > 10 items
Mean HEP = 3.75E-03		When procedures with checkoff
Error Factor = 3		provisions are correctly used

2. Commission error - Operator fails to push button to close valve

Median HEP = 0.003	Table 20-12	Select wrong control on a panel
Mean HEP = 3.75E-03		from an array of similar-
Error Factor = 3		appearing controls identified
		by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP = 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP = 0.16		using written materials
Error Factor = 5		

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(3.75E-03)(0.16) + 3.75E-03(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.20E-03
\end{aligned}
$$

Fault Tree Identifiers: 1RHOECLOSE

TABLE B-10
(Cont.)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Operator fails to detect wrong valve position via annuciator

REFERENCE:

BREAKDOWN OF TASK:

1. Omission error - Operator fails to detect wrong valve position via annuciator and initiate some kind of corrective action

   Median HEP = 0.0001 Table 20-23 One annuciator
   Mean HEP = 2.66E-4
   Error Factor = 10

   P_{OE} = 2.66E-04

   Fault Tree Identifiers: 1RHOEDETAN

TABLE B-11

NORTH ANNA MAJOR CUTSETS

FOR Q(V1)

PROBABILITY THAT MOV 1RH1 IS OPEN

WITH ACI CASE

MEAN PROBABILITY OF FAILURE = 2.01E-04

	PROBABILITY	CUTSET DESCRIPTION
1.	8.32E-05	LIMIT SWITCH LS8 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
2.	3.46E-05	RELAY COIL 52C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
3.	3.46E-05	THERMAL OVERLOAD CONTACT 49 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
4.	1.15E-05	MOTOR START CONTACT 52C PHASE C FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
5.	1.15E-05	MOTOR START CONTACT 52C PHASE B FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
6.	1.15E-05	MOTOR START CONTACT 52C PHASE A FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
7.	4.03E-06	480/120 V TRANSFORMER FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
8.	2.30E-06	TORQUE SWITCH TS-17 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
9.	1.73E-06	6 AMP FUSE # 2 FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
10.	1.73E-06	6 AMP FUSE # 1 FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700

TABLE B-11 (CONT.)
NORTH ANNA MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITH ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
11.	1.73E-06	THERMAL OVERLOAD PHASE C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
12.	1.73E-06	THERMAL OVERLOAD PHASE A FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
13.	2.30E-07	CONTACT 520 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
14.	1.38E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 MECHANICAL FAILURE TO CLOSE MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
15.	1.15E-07	CIRCUIT BREAKER SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT OPEN MOV 1700
16.	8.02E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 LOOP POWER SUPPLY FAILS PQ-1402 OPERATOR FAILS TO DETECT OPEN MOV 1700
17.	4.15E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 RELAY COIL FAILURE PC-1402-2X OPERATOR FAILS TO DETECT OPEN MOV 1700
18.	4.01E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 SIGNAL COMPARATOR FAILS PC-1402 OPERATOR FAILS TO DETECT OPEN MOV 1700

TABLE B-11 (CONT.)
NORTH ANNA MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITH ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
19.	3.87E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 PRESSURE TRANSMITTER PT-1402 FAILS LOW OPERATOR FAILS TO DETECT OPEN MOV 1700
20.	2.28E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 BISTABLE TRIP SWITCH FAILS LOW PS1402-2 OPERATOR FAILS TO DETECT OPEN MOV 1700

TABLE B-12

NORTH ANNA MAJOR CUTSETS

FOR Q(V1)

PROBABILITY THAT MOV 1RH1 IS OPEN

WITHOUT ACI CASE

MEAN PROBABILITY OF FAILURE = 9.55E-07

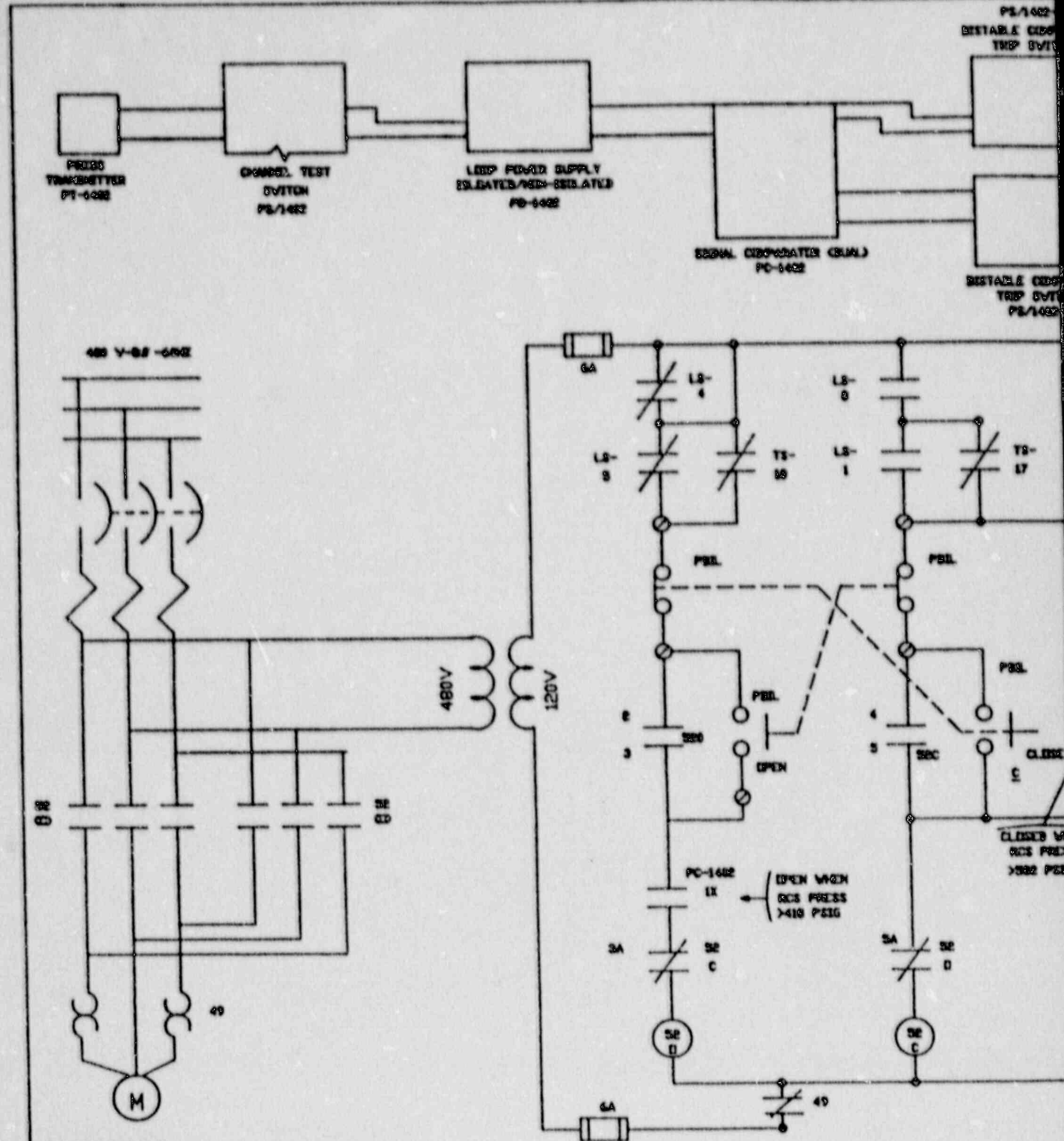
	PROBABILITY	CUTSET DESCRIPTION
1.	3.13E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
2.	1.02E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 VALVE STEM MOUNT LIMIT SWITCH FAILS TO OPERATE
3.	8.18E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 POWER SUPPLY TO ANNUCIATOR FAILS
4.	8.18E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 LOOP POWER SUPPLY FAILS PQ-1402
5.	6.00E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 ANNUCIATOR FAILS TO OPERATE
6.	4.23E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 RELAY COIL FAILURE PC-1402-2X
7.	4.09E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 SIGNAL COMPARATOR FAILS PC-1402
8.	3.95E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 PRESSURE TRANSMITTER PT-1402 FAILS LOW
9.	2.33E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 BISTABLE TRIP SWITCH FAILS LOW PS1402-2

TABLE B-12 (CONT.)
NORTH ANNA MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITHOUT ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
10.	2.26E-08	LIMIT SWITCH LS8 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
11.	1.41E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 RELAY CONTACT FAILS TO TRANSFER PC-1402-2X
12.	9.38E-09	RELAY COIL 52C FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
13.	9.38E-09	THERMAL OVERLOAD CONTACT 49 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
14.	7.35E-09	LIMIT SWITCH LS8 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 VALVE STEM MOUNT LIMIT SWITCH FAILS TO OPERATE
15.	5.91E-09	LIMIT SWITCH LS8 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 POWER SUPPLY TO ANNUCIATOR FAILS
16.	5.91E-09	LIMIT SWITCH LS8 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 LOOP POWER SUPPLY FAILS PQ-1402
17.	4.33E-09	LIMIT SWITCH LS8 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 ANNUCIATOR FAILS TO OPERATE
18.	3.81E-09	PUSHBUTTON SWITCH FAILS TO CLOSE SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT VIA ANNUNCIATOR

TABLE B-12 (CONT.)
NORTH ANNA MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITHOUT ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
19.	3.13E-09	52C CONTACT FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
20.	3.13E-09	MOTOR START CONTACT 52C PHASE C FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1700 OPERATOR FAILS TO DETECT VIA ANNUNCIATOR



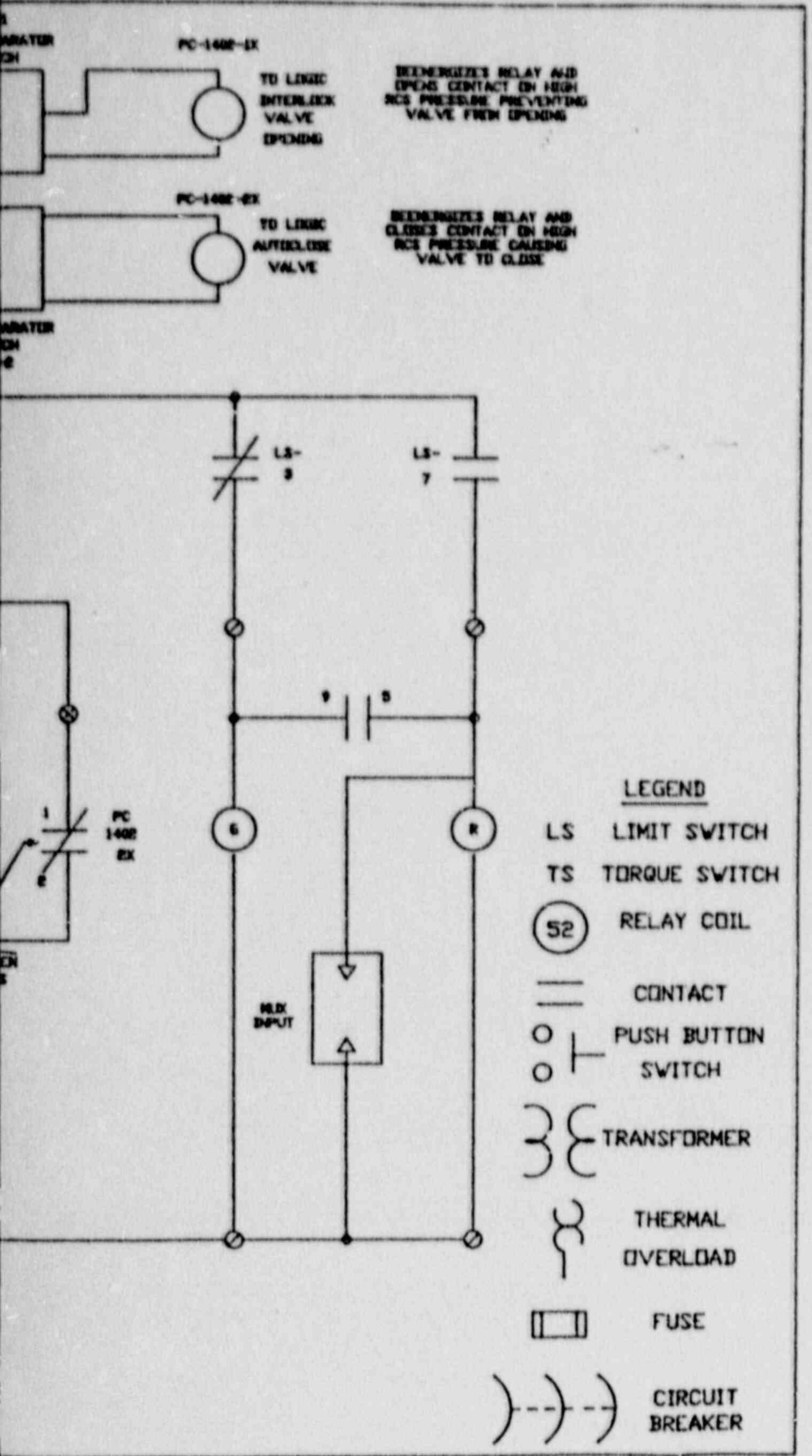
REFERENCES
S&W P-1403 REV 11
W 501B248 SHEET 160 REV 5
W 6007D10
S&W 11715-ESK-6DT SHEET 42 REV 12
S&W 11715-ESK-3H

NORTH ANNA
CONTROL WIRING DIAGRAM
MOV-1700

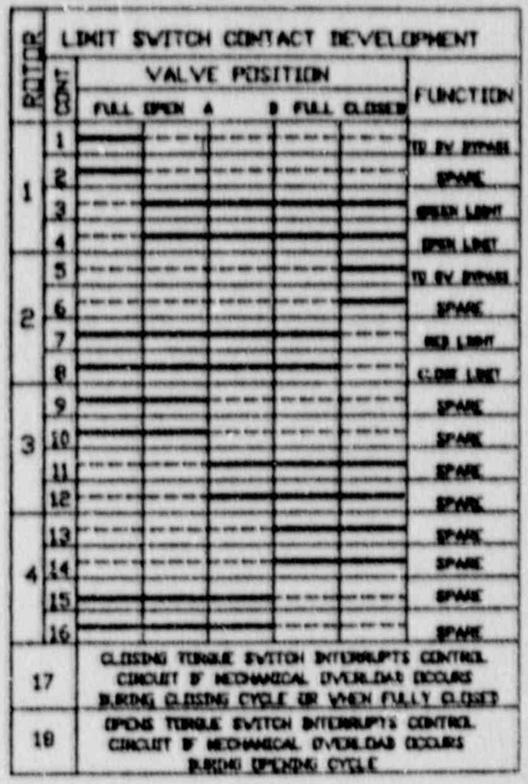
CWD_NA

2/11/88

WESTINGHOUSE PROPRIETARY CLASS 3



VALVE SHOWN IN FULLY OPEN POSITION



NOTES

——— INDICATES CONTACT CLOSED

- - - - INDICATES CONTACT OPEN

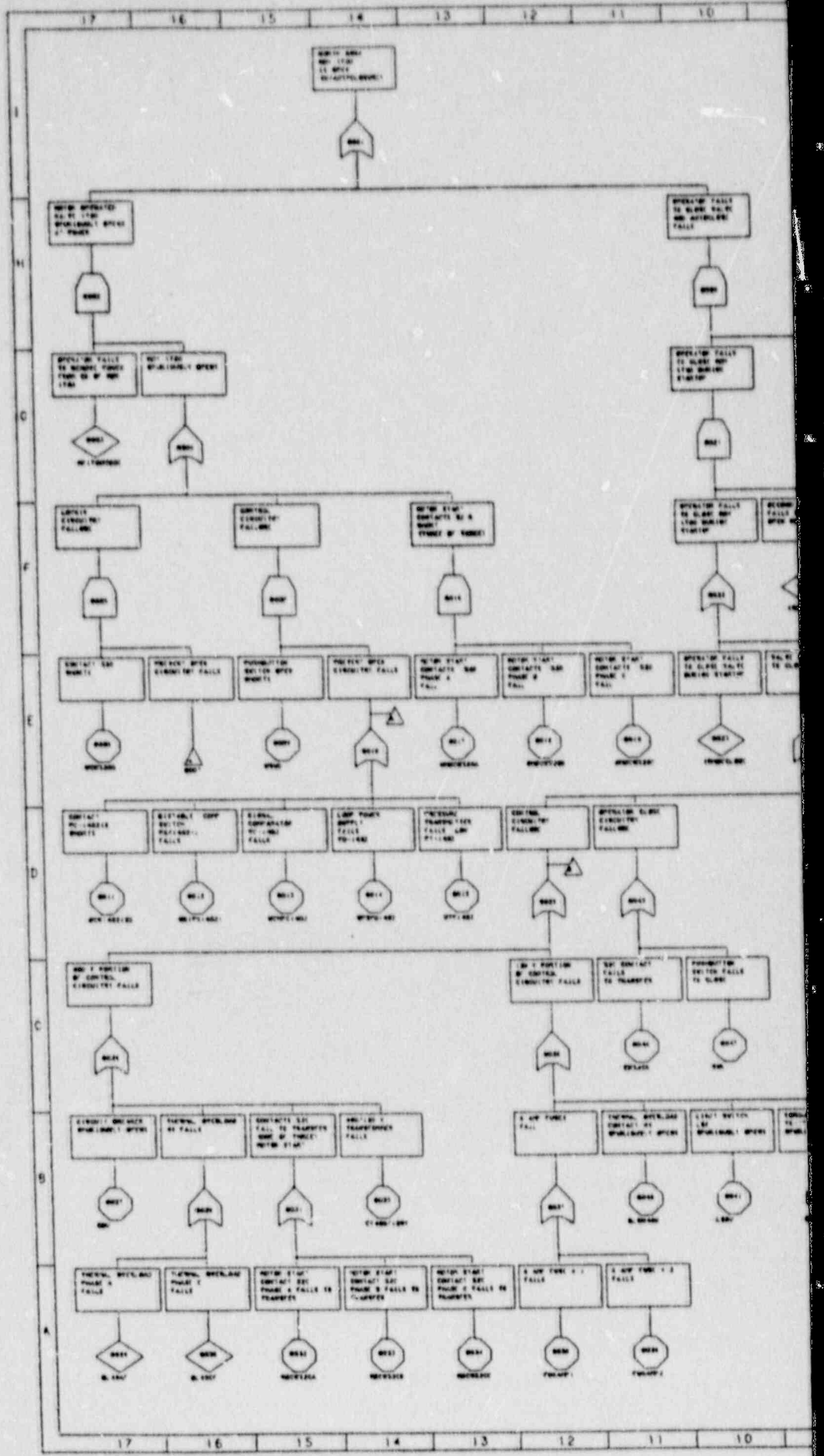
ROTORS 3 & 4 ARE ADJUSTABLE AND CAN BE SET AT VALVE POSITION FULLY OPEN FULLY CLOSED OR ANY POSITION INBETWEEN

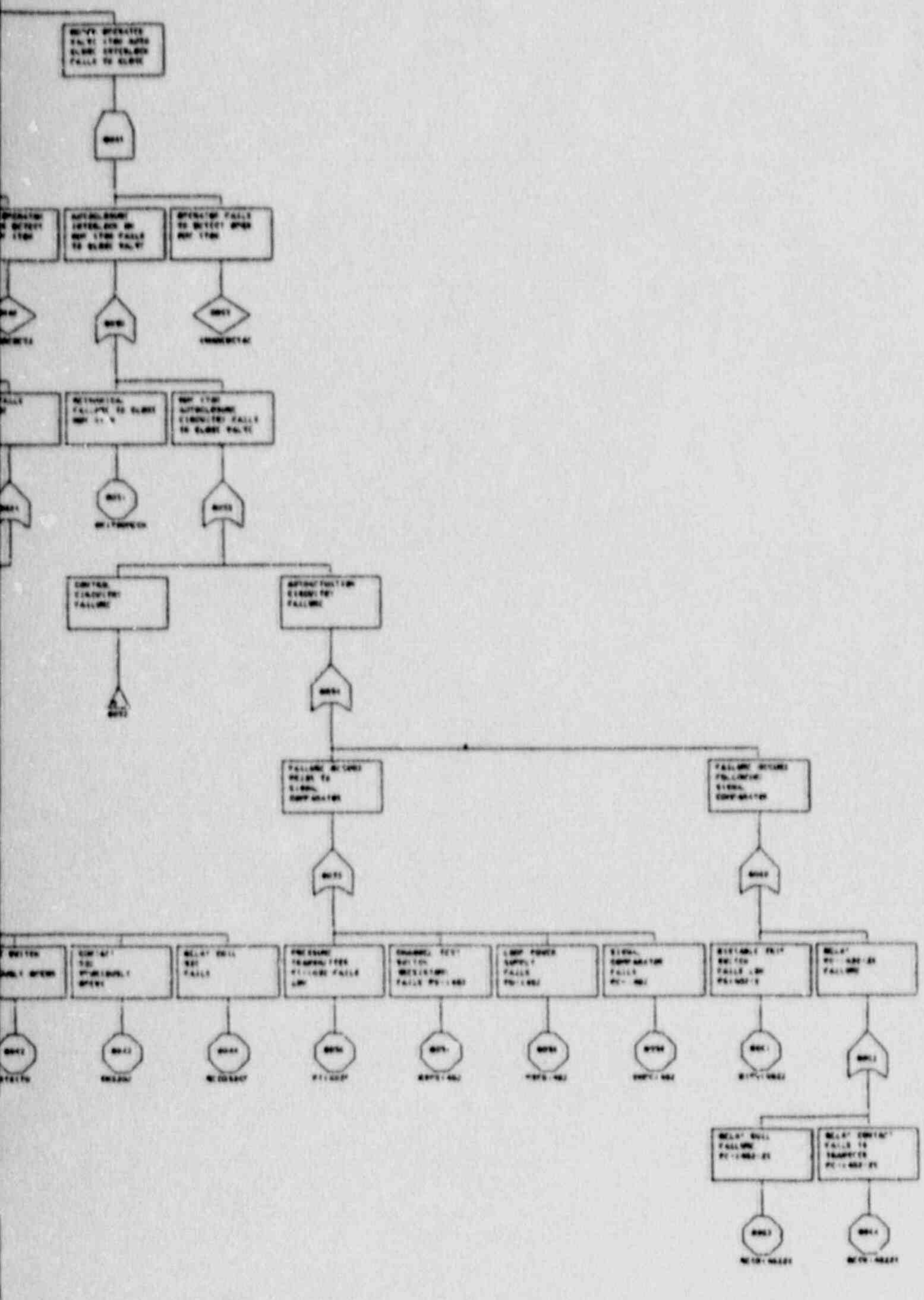
SI APERTURE CARD

Also Available On Aperture Card

FIGURE B-10

North Anna RHRS Suction/Isolation Valve Control Circultry - MOV-1700

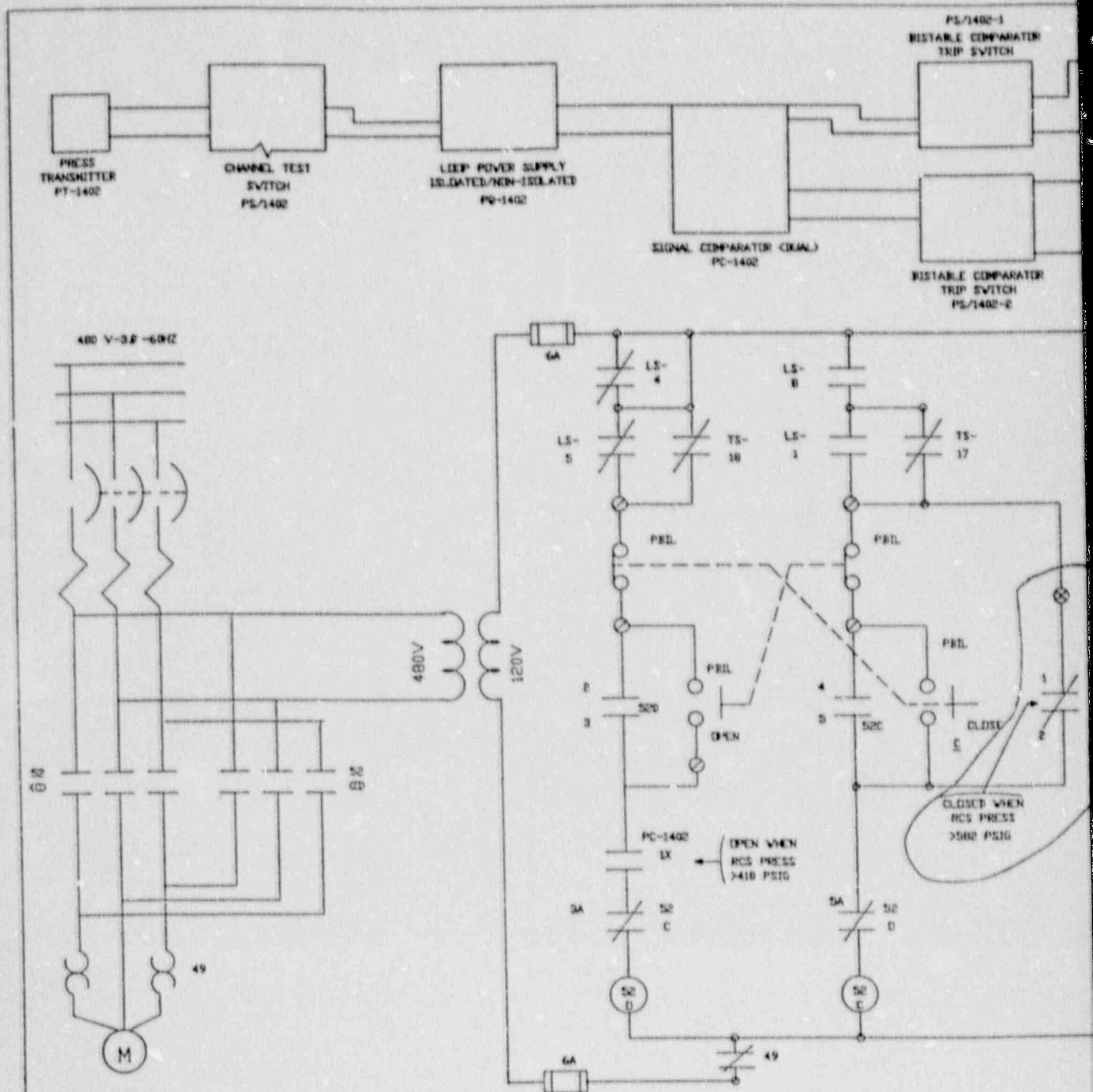




SI
APERTURE
CARD

Also Available On
Aperture Card

FIGURE B-11
NORTH ANNA VSEQUENCE
WITH ACI

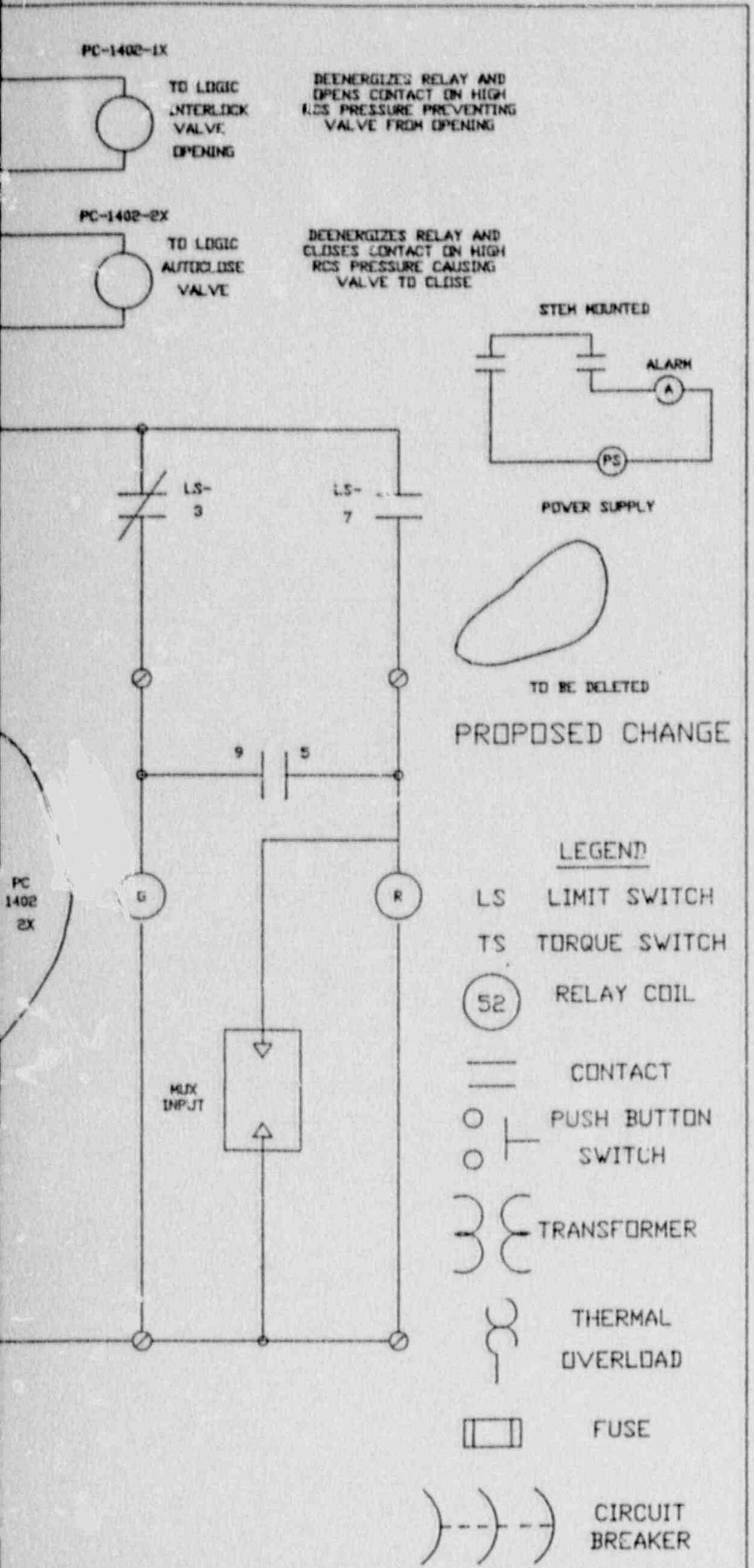


REFERENCES
S&W P-1403 REV 11
W 501B248 SHEET 160 REV 5
W 6007D10
S&W 11715-ESK-6DT SHEET 42 REV 12
S&W 11715-ESK-3H

NORTH ANNA
CONTROL WIRING DIAGRAM
MOV-1700

CWD_NA

2/11/88 PORI391 10/16/89-ADA



WESTINGHOUSE PROPRIETARY CLASS 3

VALVE SHOWN IN FULLY OPEN POSITION

ROTOR	CONT	FULL OPEN		A	B	FULL CLOSED	FUNCTION
		LIMIT SWITCH CONTACT DEVELOPMENT — VALVE POSITION					
1	1	———	-----	-----	-----	-----	TO SW BYPASS
	2	———	-----	-----	-----	-----	SPARE
	3	-----	———	———	———	———	GREEN LIGHT
	4	-----	———	———	———	———	OPEN LIMIT
2	5	-----	-----	-----	-----	———	TO SW BYPASS
	6	-----	-----	-----	-----	———	SPARE
	7	———	———	———	———	-----	RED LIGHT
	8	———	———	———	———	-----	CLOSE LIMIT
3	9	———	———	-----	-----	-----	SPARE
	10	———	———	-----	-----	-----	SPARE
	11	-----	-----	———	———	———	SPARE
	12	-----	-----	———	———	———	SPARE
4	13	-----	-----	-----	———	———	SPARE
	14	-----	-----	-----	———	———	SPARE
	15	———	———	———	-----	-----	SPARE
	16	———	———	———	-----	-----	SPARE
17		CLOSING TORQUE SWITCH INTERRUPTS CONTROL CIRCUIT IF MECHANICAL OVERLOAD OCCURS DURING CLOSING CYCLE OR WHEN FULLY CLOSED					
18		OPENS TORQUE SWITCH INTERRUPTS CONTROL CIRCUIT IF MECHANICAL OVERLOAD OCCURS DURING OPENING CYCLE					

NOTES

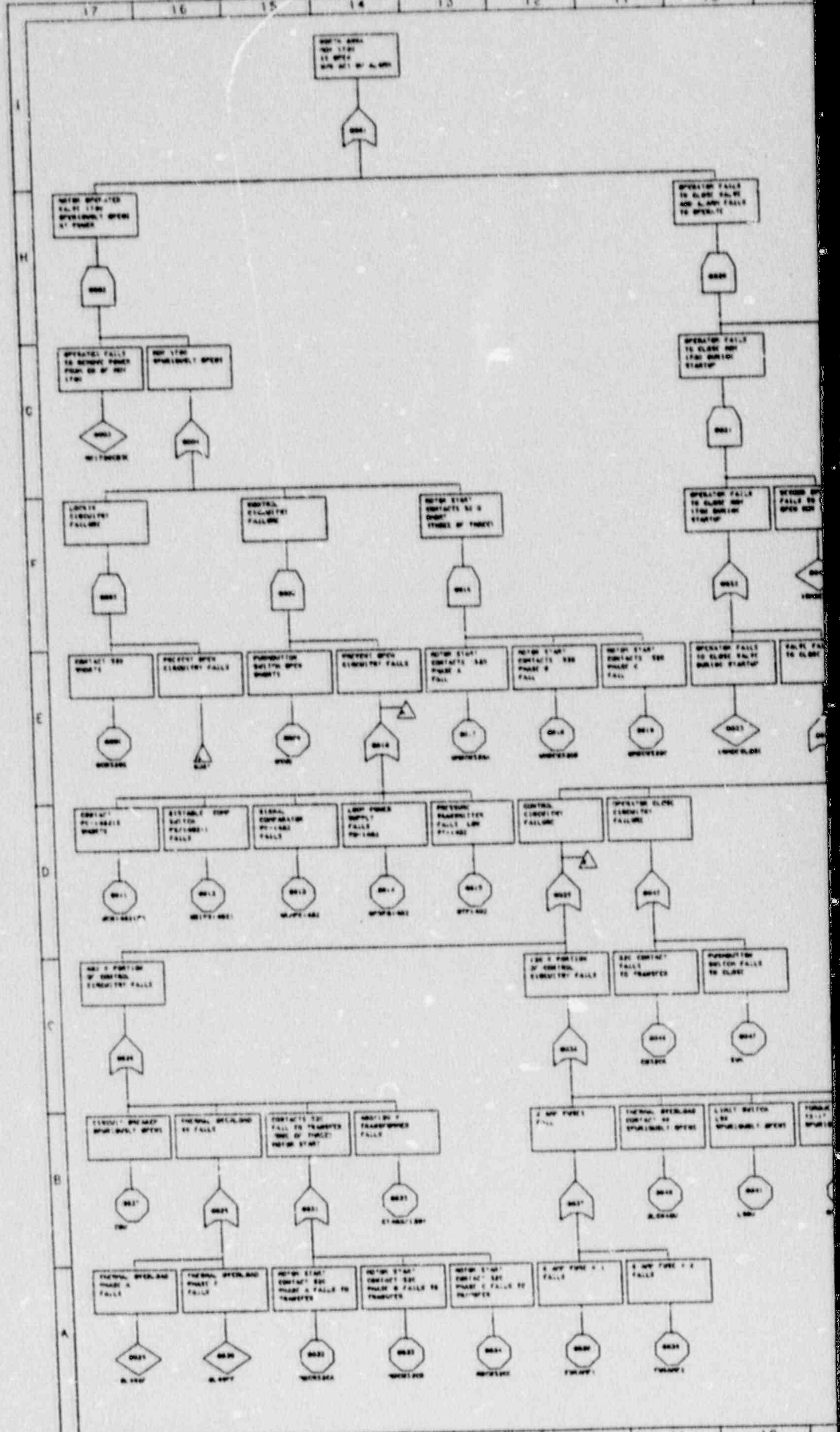
——— INDICATES CONTACT CLOSED

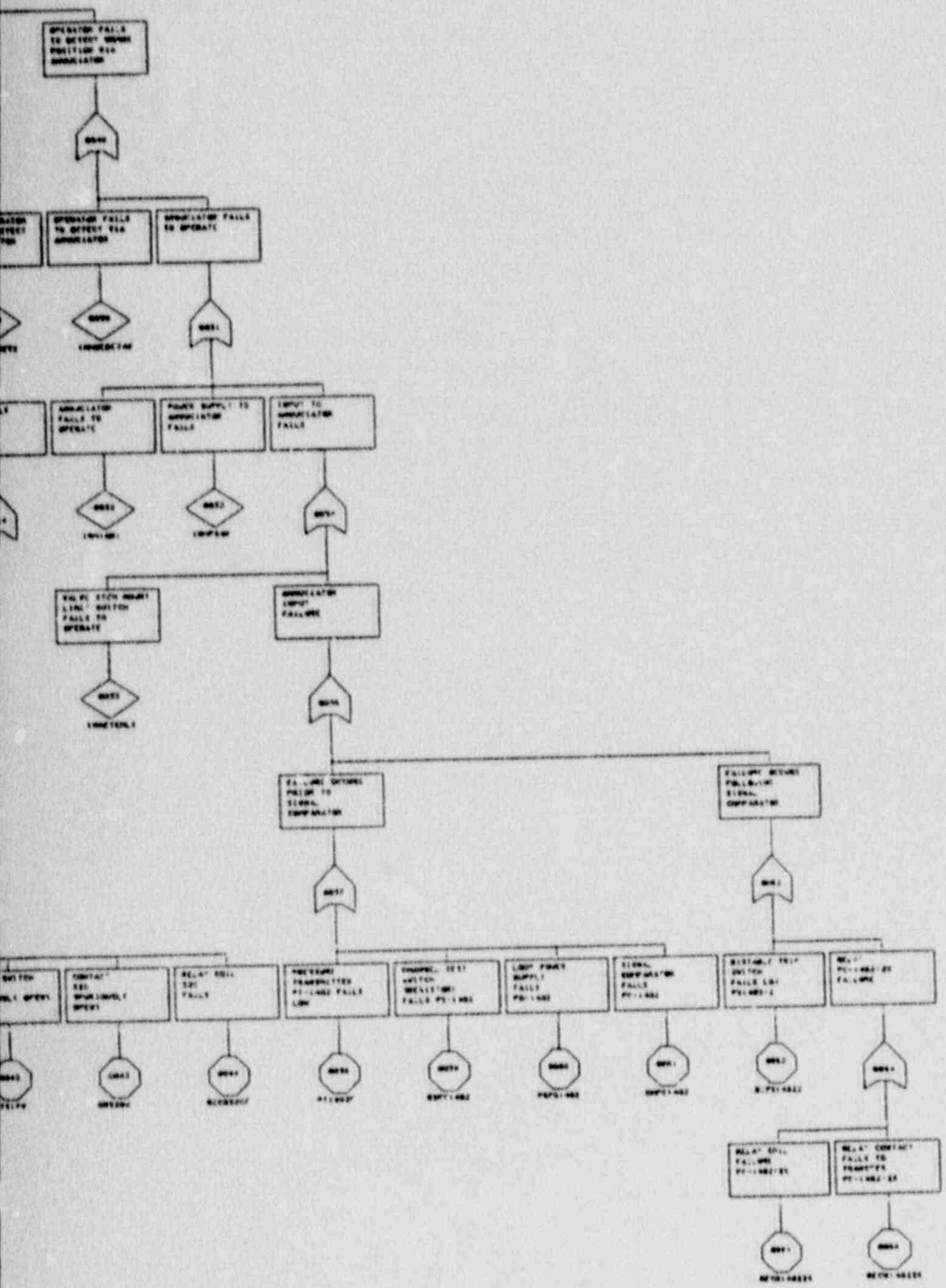
----- INDICATES CONTACT OPEN

ROTORS 3 & 4 ARE ADJUSTABLE AND CAN BE SET AT VALVE POSITION FULLY OPEN FULLY CLOSED OR ANY POSITION INBETWEEN

Figure B-12

North Anna Elementary Wiring Diagram Changes for MOV-1700 (700)





SI
APERTURE
CARD

Also Available On
Aperture Card

FIGURE B-13
NORTH ANNA VSEQUENCE
WITHOUT ACI WITH ALARM

B.4 SHEARON HARRIS

In order to determine the probabilities of the motor-operated suction valves being "OPEN" ($Q(V_1)$ and $Q(V_2)$ in equation 1), a detailed fault tree for the Shearon Harris control circuitry associated with these valves was developed.

Utilizing the present control circuitry diagram shown in Figure B-14 for suction valves 1RH1, 1RH2, 1RH39 and 1RH40 and the procedures for terminating the RHR system in preparation for startup, a fault tree was developed that considered how either suction valve would be "OPEN" at power conditions. Component failures and human errors were included in the fault tree. The fault tree developed for valve 1RH1 is shown in Figure B-15. (Because the control circuitry for the valves is identical except for component ID's, only one fault tree was developed to calculate the failure probability.)

The scenarios examined in the fault tree for the case with the autoclosure interlock are: 1) the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but due to some component failure, the valve does not close) and the autoclosure interlock fails to perform its function and does not close the valve and an operator fails to detect that the valve is not closed during startup or power operation.

For the deletion of the autoclosure interlock and the addition of an alarm as shown in Figure B-16 for valve 1RH1, a detailed fault tree was also developed. The scenarios developed for this case are: 1) the operator fails to remove power to the valve by racking out the circuit breaker and subsequently the valve spuriously opens during power operation or 2) the operator fails to close the valve during startup (or the operator attempts to close the valve but it does not close) and the operator fails to detect that the valve is not closed via the presence of an alarm (or the alarm fails to operate). The fault tree developed for this case is shown in Figure B-17.

In each case (with the autoclosure interlock and without the autoclosure interlock), the first scenario is the same; only the second scenario differs due to the proposed modification.

For the Shearon Harris analysis, the following assumptions and boundary conditions were utilized:

1. The operator closes the RHR suction valves utilizing a two-position type switch.

2. The shift foreman verifies the RHR suction valves are closed before signing the checklist.

3. The indicating lights associated with the RHR suction valves do not have alarms associated with them.

4. A component failure would be detected in a 24 hour interval if it caused the suction isolation valve to spuriously open or fail to close.

In order to quantify the fault trees developed for these cases, each basic event probability was calculated and then input into the appropriate fault tree. For a component failure, the following formula was used:

$$Q(\text{component}) = (\lambda)\ \frac{T_{detect}}{2}$$

where

Q(component) = basic event probability

λ = failure rate for the component

T_{detect} = detection interval

Table B-13 shows the basic event probabilities for each component utilizing a 24 hour detection interval.

The human error probabilities were calculated using "The Handbook for Human Reliability Analysis," Reference 19, and Shearon Harris's operating procedures for terminating the RHR System in preparation for startup. The calculations of the human error probabilities are shown in Table B-14.

SHEARON HARRIS RESULTS

The probabilities for $Q(V_1)$ and $Q(V_2)$, the probability that the isolation valve is open, for each case are shown below:

	With Autoclosure Interlock	Without Autoclosure Interlock
$Q(V_1)$	8.53E-05	2.33E-06
$Q(V_2)$	8.53E-05	2.33E-06

The major cutsets (failure combinations) and the probabilities of the cutsets for each case (with and without the autoclosure interlock) are shown in Tables B-15 and B-16. For the case with the ACI (Table B-15), the dominant contributors are a component failure which causes the valve not to close along with the operator failing to detect that the valve did not close during startup and another operator failure to detect the wrong position during power operation.

For the ACI deletion case, the dominant contributors are: the operator fails to close the valve during startup along with the operator failing to detect that the valve is not closed during startup and either operator failure to detect via the alarm or the alarm fails to operate.

The frequency of an interfacing system LOCA, given these probabilities is calculated using:

$$F(VSEQ) = 2 \, [\, (\lambda)_2 \, Q(V_1) + (\lambda)_1 \, Q(V_2) + (\lambda)_2 \, Q(V_{1R}) \,]$$

where

2 = the number of RHR suction lines

$(\lambda)_2$ = failure rate of RCS valve (due to rupture)

$(\lambda)_1$ = failure rate of RHR valve (due to rupture)

$Q(V_1)$ = probability that RHR valve is open

$Q(V_2)$ = probability that RCS valve is open

$Q(V_{1R})$ = probability of rupture of RHR valve

The failure rate due to rupture of a motor-operated valve is 1.0E-7 per hr ($(\lambda)_1$ and $(\lambda)_2$). The quantity $Q(V_{1R})$ is determined by assuming that the total defined mission time is the time between refueling outages (i.e., every 18 months). The rupture of motor-operated valve is assumed to occur randomly in the time interval 0 - T_M where T_M is the total defined mission time. Therefore the probability of the valve rupturing is:

$$Q(V_{1R}) = (\lambda)\ \frac{T_M}{2}$$

$$= \frac{1E\text{-}07}{hr}\ \frac{(8760\ hrs/year * 1.5\ years)}{2}$$

$$= 6.57E\text{-}04$$

Entering the failure probabilities leads to the following frequency for an interfacing system LOCA for the case with the ACI:

$$\begin{aligned}
F(VSEQ) &= 2[\ (\lambda)_2\ Q(V_1) + (\lambda)_1\ Q(V_2) + (\lambda)_2\ Q(V_{1R})\ ] \\
&= 2[\ 1E\text{-}07/hr * (8.53E\text{-}05) + (1E\text{-}07/hr) * (8.53E\text{-}05) + \\
&\quad 1E\text{-}07/hr * (6.57E\text{-}04)\ ] \\
&= 2[\ 8.53E\text{-}12/hr + 8.53E\text{-}12/hr + 6.57E\text{-}11/hr\ ] \\
&= 2[\ 8.276E\text{-}11/hr\ * (8760\ hrs/year)\ ] \\
&= 1.45E\text{-}06/year
\end{aligned}$$

The same method was applied in the case without the ACI. The following summarizes the frequencies:

	With Autoclosure Interlock	Without Autoclosure Interlock
F(VSEQ)	1.45E-06/year	1.16E-06/year

The frequency of an Event V decreases by approximately 20 percent with removal of the ACI. The main contributor to the frequencies in each case is a double rupture of MOV 1RH2 then 1RH1 (or 1RH39 then 1RH40) (frequency of 5.75E-07/year in both cases). The deletion of the ACI has no impact on this contributor. As can be seen, the frequency of a double rupture dominates the second case while the other contributor (the rupture of one valve while the other valve has failed open) does not contribute significantly in the case in which the ACI has been deleted. (The frequency for the rupture of one valve while the other is open decreases from 7.47E-8/year (8.53E-12/hr *8760 hrs/year) for the case with the ACI to 2.04E-9/year (2.33E-13/hr * 8760 hrs/year) for the case with the ACI deleted.) This is a significant decrease in the occurrence of an Event V by this failure mode. Thus, the deletion of the autoclosure interlock and the inclusion of an alarm is beneficial in reducing this contribution.

TABLE B-13
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
RHCBOE	OE	OPERATOR FAILS TO RE	1.600E-03	---	1.60E-03
CN1A11A2Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
CNK734Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
UREPY402A1	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
UCMPB402	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
UISEEPV402	EE	ISOLATOR E-E CONVERT	4.800E-07	1.200E+01	5.76E-06
UPSPGY402	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
UTPPT402	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
MSCN420AQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
MSCN420BQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
MSCN420CQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
CN420Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHOECLOSE	OE	OPERATOR FAILS TO CL	3.200E-03	---	3.20E-03
CN2B12B2U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
CT480V120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
RECN42SA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
RECN42SB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
RECN42SC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05

TABLE B-13 (CONT.)

SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
QSTCU	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
CN420U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
REC042S	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
CNCR1A1789	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
FU1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
OLCN49MR2	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHOEDET2	OE	SECOND OPERATOR FAIL	9.800E-01	---	9.80E-01
LSACU	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
PS118VAC	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
REPY402A2	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
CMPB402	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
ISEEPV402C	EE	ISOLATOR E-E CONVERT	4.800E-07	1.200E+01	5.76E-06
PSPGY402	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
RSPS402B	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
TPPT402	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
CN2A12A2U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
CNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
MV1RH1MECH	MV	FAILURE TO CLOSE	1.000E-05	1.200E+01	1.20E-04
1RHOEDETAC	OE	SECOND OPERATOR FAIL	9.800E-01	---	9.80E-01

TABLE B-13 (CONT.)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1RHOEDETAN	OE	OPERATOR DETECT ANNU	2.660E-04	---	2.66E-04
1RH1AN1	AN	ANNUCIATOR ALL MODES	4.250E-06	1.200E+01	5.10E-05
1RHPSAN	PS	POWER SUPPLY ANNUCIA	5.800E-06	1.200E+01	6.96E-05
1RHSTEMLS	LS	STEM LIMIT SWITCH AL	7.220E-06	1.200E+01	8.66E-05

TABLE B-14

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: 1RH1 and 1RH2 (or 1RH39 and 1RH40) must be closed and the power supplies opened and locked. Complete Attachment III of OP-111.

REFERENCE: Step 15 in operating procedure OP-111 Revision 2 - Residual Heat Removal System Section 7.0 Shutdown.

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open and lock open power supply breaker

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator selects wrong circuit breaker

Median HEP = 0.005 Mean HEP = 6.25E-03 Error Factor = 3	Table 20-12	Select wrong circuit breaker in a group of circuit breakers densely grouped and identified by labels only

3. Recovery error -Foreman fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(6.25E-03)(0.16) + 3.75E-03(0.16) \\
&= 9.96E-04 + 6.0E-04 \\
&= 1.596E-03 \\
&= 1.60E-03
\end{aligned}
$$

Fault Tree Identifiers: 1RHCBOE

TABLE B-14
(Cont.)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Operator fails to detect wrong valve position

REFERENCE:

BREAKDOWN OF TASK:

1. Omission error - Operator fails to detect wrong valve position

   HEP = 0.98 Table 20-25 Legend light
   Other than annuciator light

   P_{OE} = 0.98

   Fault Tree Identifiers: 1RHOEDET2 and 1RHOEDETAC

TABLE B-14
(Cont.)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: CLOSE 1RH1 and 1RH2 and 1RH39 and 1RH40. Complete Attachment III checklist.

REFERENCE: Step 4 in operating procedure OP-111 Revision 2 - Residual Heat Removal System.

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated suction valve using two-position switch

Median HEP	= 0.003	Table 20-7	Long list > 10 items
Mean HEP	= 3.75E-03		When procedures with checkoff
Error Factor	= 3		provisions are correctly used

2. Commission error - Operator fails to turn control to close valve

Median HEP	= 0.01	Table 20-12	Turn two position switch in wrong direction when design violates a strong populational stereotype and operating conditions are normal by labels only
Mean HEP	= 1.61E-02		
Error Factor	= 5		

3. Recovery error - Shift supervisor fails to detect error by others

Median HEP	= 0.1	Table 20-22	Checking routine tasks, checker using written materials
Mean HEP	= 0.16		
Error Factor	= 5		

P_{OE} = (1-3.75E-03)(1.61E-2)(0.16) + 3.75E-03(0.16)
= 2.556E-03 + 6.0E-04
= 3.166E-03
= 3.25-03

Fault Tree Identifiers: 1RHOECLOSE

TABLE B-14
(Cont.)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Operator fails to detect wrong valve position via annuciator

REFERENCE:

BREAKDOWN OF TASK:

1. Omission error - Operator fails to detect wrong valve position via annuciator and initiate some kind of corrective action

   Median HEP = 0.0001 Table 20-23 One annuciator
   Mean HEP = 2.66E-04
   Error Factor = 10

   P_{OE} = 2.66E-04

   Fault Tree Identifiers: 1RHOEDETAN

TABLE B-15
SHEARON HARRIS MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITH ACI CASE

MEAN PROBABILITY OF FAILURE = 8.53E-05

	PROBABILITY	CUTSET DESCRIPTION
1.	3.46E-05	RELAY COIL 42/S FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
2.	1.15E-05	RELAY CONTACT PHASE C 42/S FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
3.	1.15E-05	RELAY CONTACT PHASE B 42/S FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
4.	1.15E-05	RELAY CONTACT PHASE A 42/S FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
5.	4.03E-06	480V/120V TRANSFORMER FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
6.	2.30E-06	TORQUE SWITCH TC SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
7.	1.73E-06	FUSE FU1 FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
8.	1.73E-06	THERMAL OVERLOAD PHASE C 49/MR FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
9.	1.73E-06	THERMAL OVERLOAD PHASE B 49/MR FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1

TABLE B-15 (CONT.)
SHEARON HARRIS MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITH ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
10.	1.73E-06	THERMAL OVERLOAD PHASE A 49/MR FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
11.	3.69E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 MECHANICAL FAILURE OF MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
12.	2.66E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 LIMIT SWITCH AC SPURIOUSLY OPENS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
13.	2.30E-07	CONTACT 42/O SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
14.	2.30E-07	CONTACT 55-57 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
15.	2.30E-07	CONTACT CR/1A/1789 SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
16.	2.30E-07	CONTACT 49/MR (3) SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
17.	2.30E-07	CONTACT 49/MR (2) SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1
18.	2.30E-07	CONTACT 49/MR (1) SPURIOUSLY OPENS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT OPEN MOV 1RH1

TABLE B-15 (CONT.)
SHEARON HARRIS MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITH ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
19.	2.14E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 LOOP POWER SUPPLY PGY-402 FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1
20.	2.14E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 118 V AC POWER SUPPLY FAILS OPERATOR FAILS TO DETECT OPEN MOV 1RH1

TABLE B-16

SHEARON HARRIS MAJOR CUTSETS

FOR Q(V1)

PROBABILITY THAT MOV 1RH1 IS OPEN

WITHOUT ACI CASE

MEAN PROBABILITY OF FAILURE = 2.33E-06

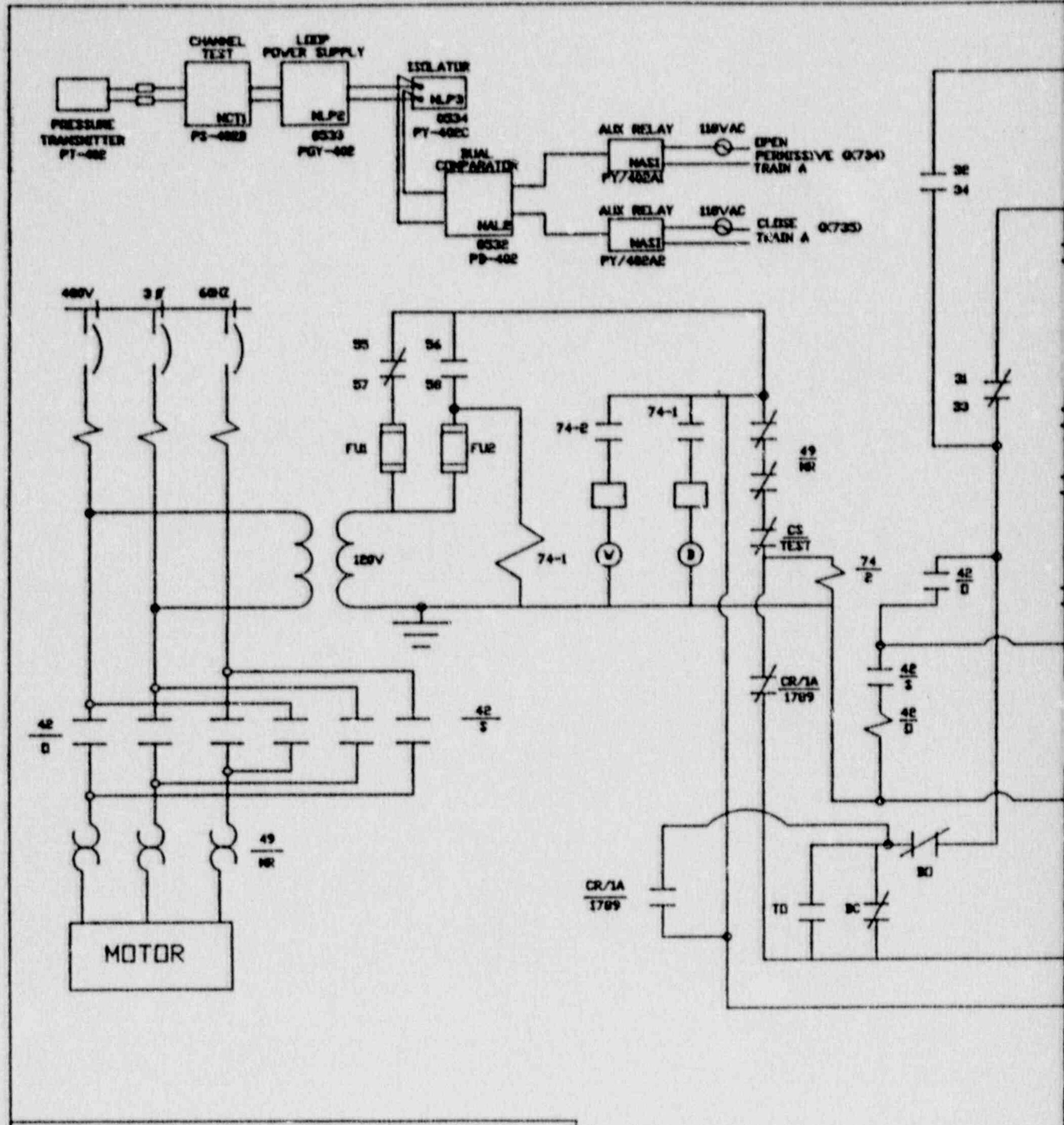
	PROBABILITY	CUTSET DESCRIPTION
1.	8.34E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
2.	2.72E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 VALVE STEM MOUNT LIMIT SWITCH FAILS TO OPERATE
3.	2.18E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 POWER SUPPLY TO ANNUCIATOR FAILS
4.	2.18E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 LOOP POWER SUPPLY PGY-402 FAILS
5.	2.18E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 118V AC POWER SUPPLY FAILS
6.	1.60E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 ANNUCIATOR FAILS TO OPERATE
7.	1.13E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 AUXILIARY RELAY PY/402A2 FAILS
8.	1.09E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 DUAL COMPARATOR PB-402 FAILS

TABLE B-16 (CONT.)
SHEARON HARRIS MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITHOUT ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
9.	1.05E-07	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 PRESSURE TRANSMITTER PT-402 FAILS
10.	1.81E-08	OPERATOR FAILS TO CLOSE VALVE DURING STARTUP PER 7.1.2 (4) SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 ISOLATOR PV-402C FAILS
11.	9.38E-09	RELAY COIL 42/S FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
12.	3.13E-09	RELAY CONTACT PHASE C 42/S FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
13.	3.13E-09	RELAY CONTACT PHASE B 42/S FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 OPERATOR FAILS TO DETECT VIA ANNUCIATOR
14.	3.13E-09	RELAY CONTACT PHASE A 42/S FAILS TO TRANSFER SECOND OPERATOR FAILS TO DETECT OPEN MOVE 1RH1 OPERATOR FAILS TO DETECT VIA ANNUNCIATOR
15.	3.06E-09	RELAY COIL 42/S FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 VALVE STEM MOUNT LIMIT SWITCH FAILS TO OPERATE
16.	2.46E-09	RELAY COIL 42/S FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 POWER SUPPLY TO ANNUCIATOR FAILS
17.	2.46E-09	RELAY COIL 42/S FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 LOOP POWER SUPPLY PGY-402 FAILS
18.	2.46E-09	RELAY COIL 42/S FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 118V AC POWER SUPPLY FAILS

TABLE B-16 (CONT.)
SHEARON HARRIS MAJOR CUTSETS
FOR Q(V1)
PROBABILITY THAT MOV 1RH1 IS OPEN
WITHOUT ACI CASE

	PROBABILITY	CUTSET DESCRIPTION
19.	1.80E-09	RELAY COIL 42/S FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 ANNUCIATOR FAILS TO OPERATE
20.	1.27E-09	RELAY COIL 42/S FAILS SECOND OPERATOR FAILS TO DETECT OPEN MOV 1RH1 AUXILIARY RELAY PY/402A2 FAILS



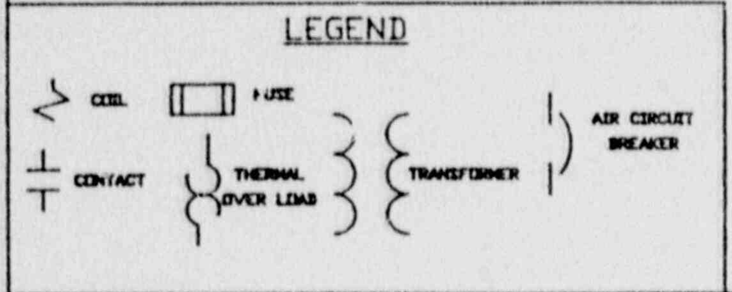
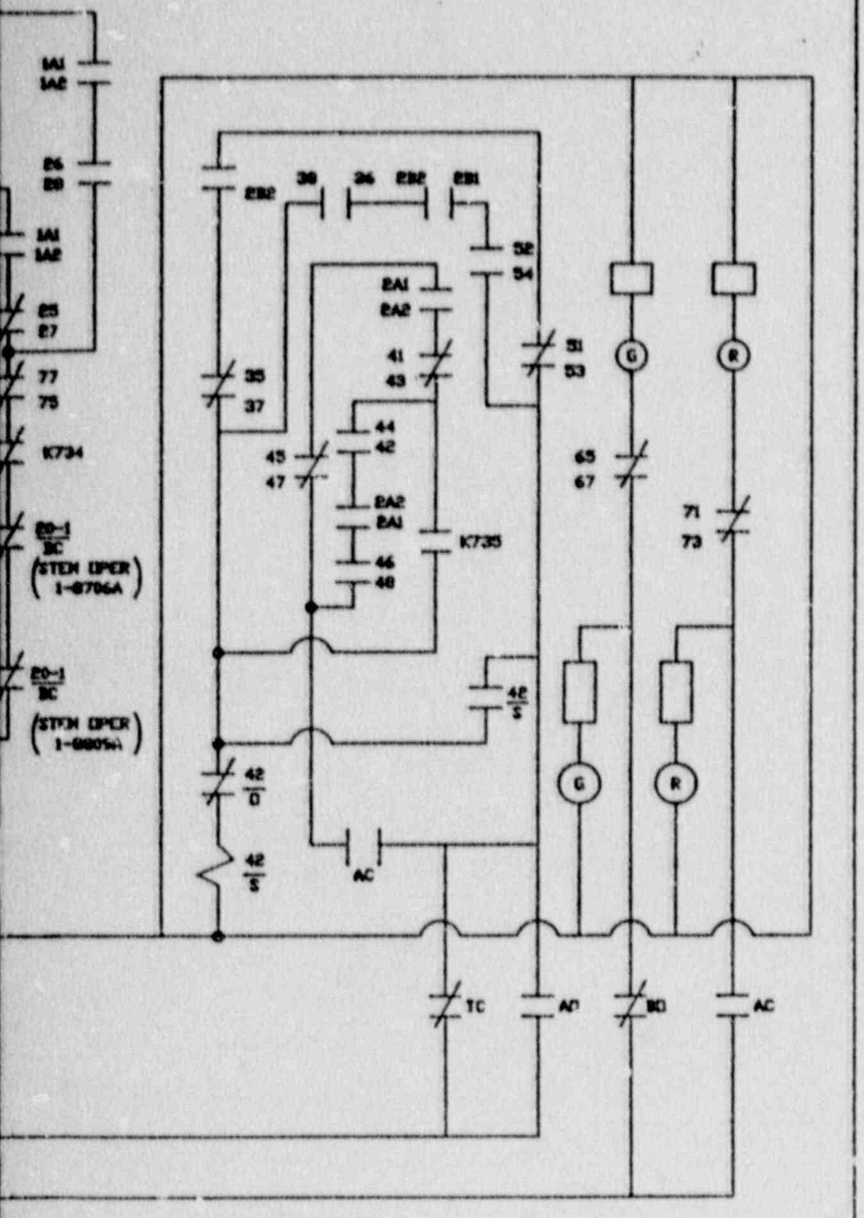


FIGURE B-14

Shearon Harris RHRS Suction/Isola
Control Circultry - MOV-8701A (

RCS_SH22

2/11/88



tion Valve
(RH-2)

CONTACTS		POSITION		
		SHUT	NORMAL	OPEN
1A1 O-II-O 1A2	A			X
1B1 O-II-O 1B2	B		X	SPARE
2A1 O-II-O 2A2	A		X	
2B1 O-II-O 2B2	B	X		

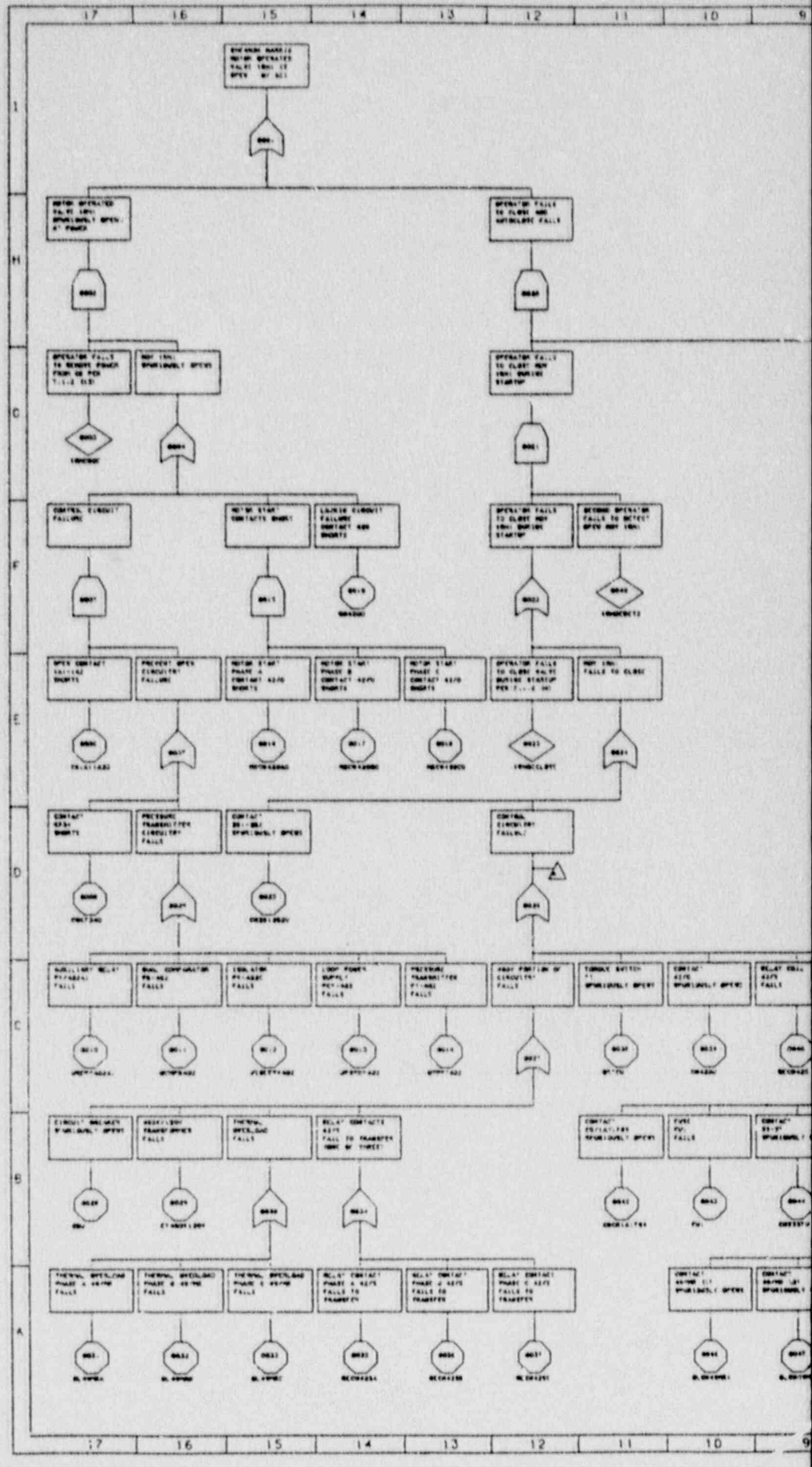
SPRING RETURN TO NORMAL
X-CONTACT CLOSED

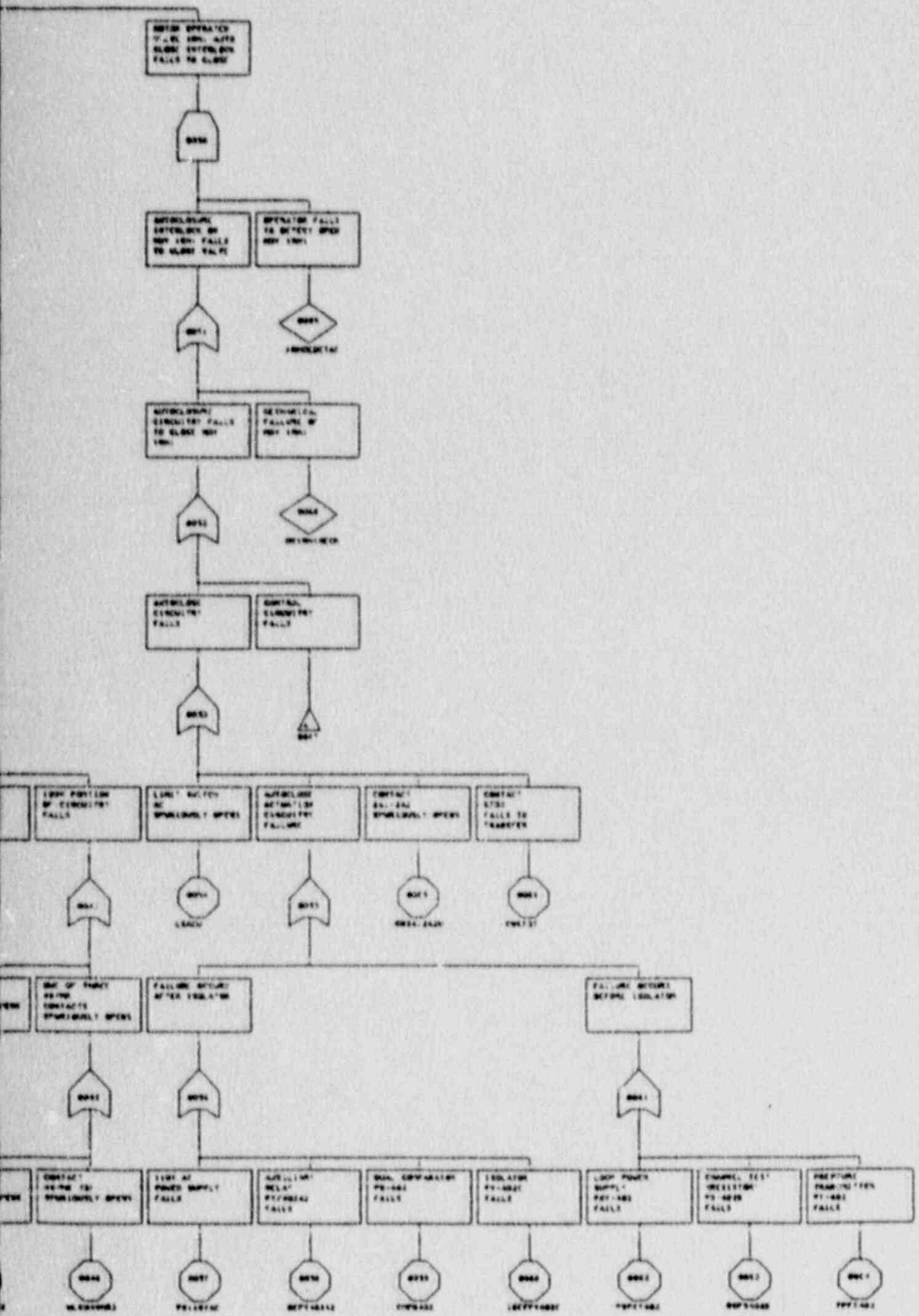
NOTE
1. K734 CLOSES AT RCS PRESS< 425 PSIG AND K735 CLOSES AT RCS PRESS > 700 PSIG

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0 – 100)	CVD SH
bo	4			■
ac		8		■
bo	3			■
ac		7		
ao	2			
bc		6		
ao	1			■
bc		5		■
ac		16		
bo	12			
ac		15		■
bo	11			
bc		14		
ao	10			
bc		13		
ao	9			
tc	17		OPENS ON OVLD ON CLOSE STRK	■
to	18		OPENS ON OLVD ON OPEN STRK	■

—— = CONT CLOSED ■ = THIS SHEET

REF.
CAR 2166 B-401 SH 325
W 2034578 SH 11

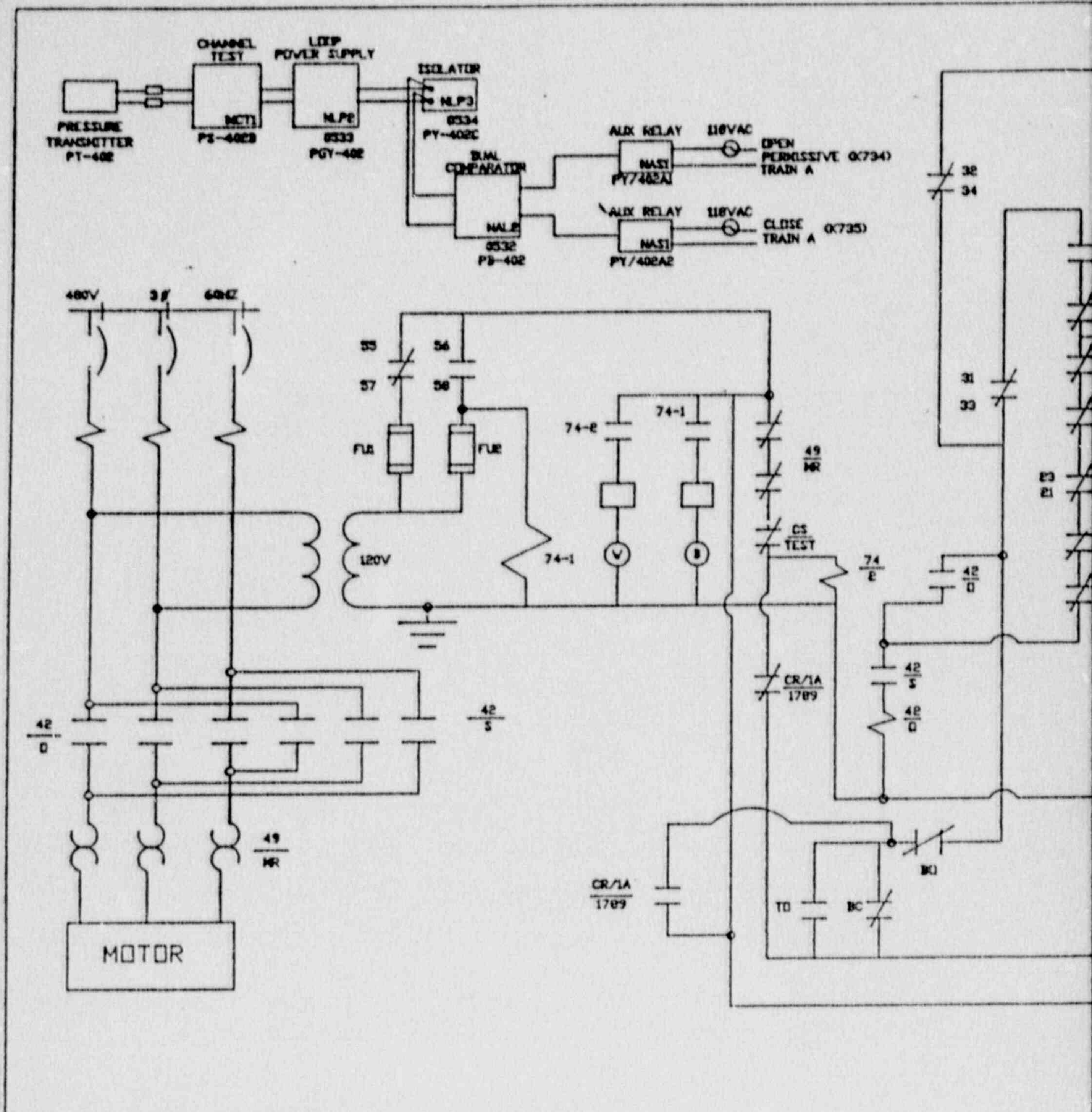




SI
APERTURE
CARD

Also Available On
Aperture Card

FIGURE B-15
SHEARON HARRIS VSEQUENCE
WITH ACI



LEGEND

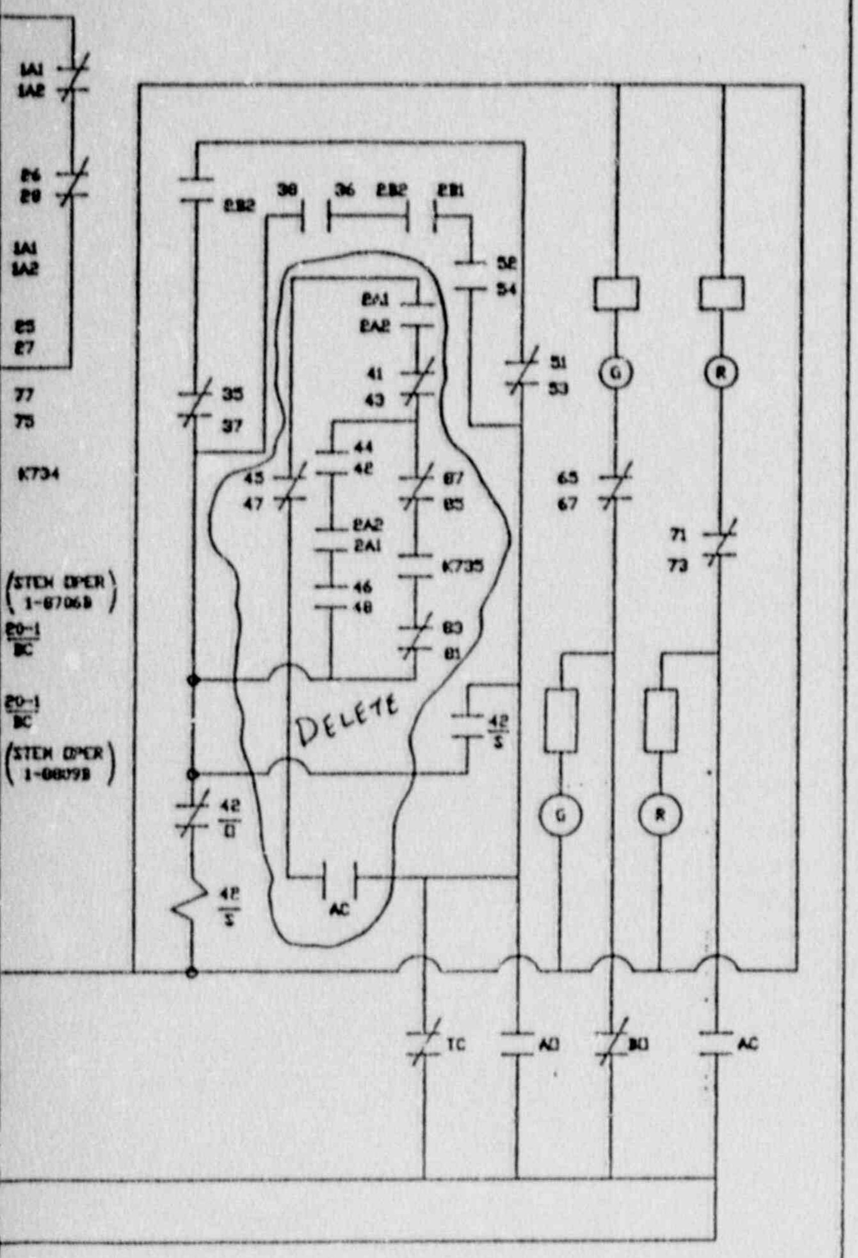
COIL
FUSE
AIR CIRCUIT BREAKER
CONTACT
THERMAL OVER LOAD
TRANSFORMER

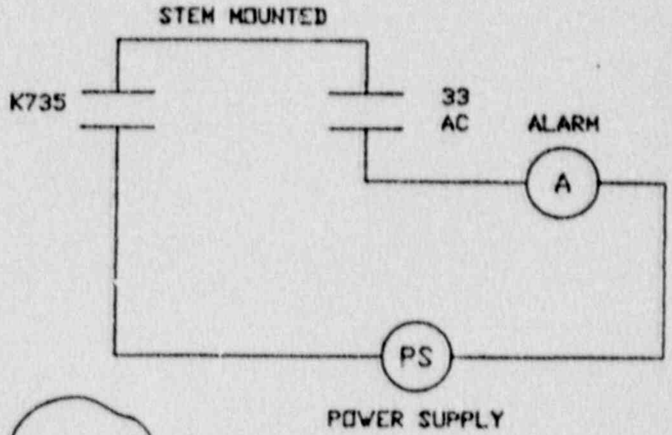
FIGURE B-16

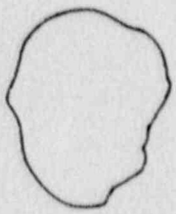
Shearon Harris Elementary Wi
Changes for MOV-87

RCS_SH22

1/19/88







TO BE DELETED

PROPOSED CHANGE

20/ LIMIT SW DEVELOPMENT				
EBASCO SYM	CONT		VALVE OPNG % (0 — 100)	CWD SH
bo	4			■
ac		8		■
bo	3			■
ac		7		
ao	2			
bc		6		
ao	1			■
bc		5		■
ac		16		
bo	12			
ac		15		■
bo	11			
bc		14		
ao	10			
bc		13		
ao	9			
tc	17		OPENS ON OVLD ON CLOSE STRK	■
to	18		OPENS ON OLVD ON OPEN STRK	■
—— = CONT CLOSED ■ = THIS SHEET				

REF.
CAR E166 B-401 SH 325
V 2034578 SH 11

ring Diagram
01A

SI
APERTURE
CARD

Also Available On
Aperture Card

8911150026-52

OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 1

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH

APPENDIX C

RESIDUAL HEAT REMOVAL SYSTEM (RHRS)

AVAILABILITY ANALYSIS

APPENDIX C
RHRS AVAILABILITY ANALYSIS

C.1 Introduction

The Residual Heat Removal System for each of the four reference plants was analyzed to determine the unavailability of the system to remove decay heat and the impact of removal of the autoclosure interlock on this unavailability due to spurious closure of the suction valves. Fault trees were used to determine unavailability for startup of the RHR System, for short term cooling (72 hours) and long term cooling (6 weeks). This appendix describes the calculations and fault tree quantifications used to determine the RHR System unavailabilities.

C.2 Analyses

Guidelines were used in the construction of the fault trees to simplify and reduce the overall size of the fault trees since certain events are often not included owing to their low probability of occurrence relative to other events.

The following describe the guidelines.

A. The "local faults of piping" in a fluid system segment were not included in the fault tree model construction, since their contribution to the probability of system failure, compared to the contribution from the other components, is insignificant.

B. Random mechanical failure of <u>locally</u> locked open manual valves were not included in fault tree development since the probability of failure is not significant relative to other valve faults. The only credible random valve failure that might occur is plugging of an open valve, but this is only significant if the source of water or other fluid is untreated (e.g., service water, etc.) and if the likelihood is comparable or greater than other system faults. Failures of unlocked manual valves were included in fault tree development along with locked open active valves (which are rare) that are locked at the control board. Misposition of locked open manual valves due to human error is considered unlikely due to locking mechanisms employed (e.g., chained locked or other mechanical devices) on most valves.

C. Normally open manual, air and motor-operated valves that are not required to change state during operation were treated as if they are locally locked open. However, misposition of the valve prior to operation due to human error and/or a spurious control signal were considered as a credible event if applicable.

D. Potential flow diversion paths of fluid system that are isolated from the main flow path by one or more locally locked closed valves were not considered as faults of the system.

E. Potential flow diversion paths isolated from the main flow path by normally closed manual, air, and motor-operated, and check valves were not treated as faults of the system. However, valve misposition prior to operation due to human error and/or spurious control signal was considered a system fault, if credible.

F. Check valves failing closed to flow in the forward direction and failing open to flow in the reverse direction were included as credible events. An exception is made for the case of two check valves in series being used as isolation valves to block flow. These were not included in fault tree development since their combined probability of failure to isolate flow would be of low probability relative to other system faults.

G. Failure of heat exchangers (coolers) to transfer heat due to plugging of the tube side and leakage (primary to secondary) were not considered credible faults. An exception was made for the case of heat exchangers plugging when the tube side flow of coolant transfer medium is untreated. Plugging was considered as a credible event for such cases if the coolant medium is untreated.

The following boundary conditions and assumptions were utilized during the analysis for each of the four reference plants.

1. Two trains of RHR are required for 72 hours following initiation of the RHR system.

2. One train of RHR is required for 6 weeks (representative of the time of a refueling outage).

3. Injection into two cold legs (of 3 or 4 cold legs) trains is required for the initial RHR cooldown phase (72 hours).

4. Injection into two cold legs (of 3 or 4 cold legs) is required for the long term RHR cooldown phase (6 weeks).

5. No testing or maintenance operations are assumed to occur during the initial phase of cooldown using the RHR System (first 72 hours).

6. During the warm-up period of the RHRS, both RHR pumps are started and must run for approximately two hours before injection into the RCS cold legs.

7. All electric power (AC and DC) is assumed to be available with a probability of 1.0.

8. For long term cooling, it is assumed that the Train A pump is operating and the Train B pump is in standby and thus must start and run should the Train A pump fail. No switching of trains during long term cooling is assumed.

C.3 QUANTIFICATION

The availability of the Residual Heat Removal System to remove decay heat is considered in three phases in this analysis. First, the RHR System must be placed into service and go through a warm-up period in order to minimize the thermal shock to the system. Secondly, during the initial phase of cooldown, the decay heat load is high. For this phase, two trains of RHR were assumed to be required for 72 hours. The final phase of cooldown is long term decay heat removal. Six weeks was the time period assumed for this phase (based on the average refueling outage time period).

The following describes the RHR availability analysis for each of the four lead plants.

C.3.1 SALEM

Three basic fault trees were developed to model the Residual Heat Removal System unavailability for the Salem. These fault trees were developed from the system flow diagrams and control wiring diagrams shown and described in Section 5.1 for Salem. The three fault trees are startup of the RHR System, short term cooling (72 hours) and long term cooling (6 weeks). The short term and long term fault trees were constructed both with and without the autoclosure feature of the RHR suction valves in order to show the change in RHR System unavailability due to the removal of the autoclosure interlock. These RHR suction valves to the Reactor Coolant System hot legs were modeled in detail down to the control circuitry level in order to show the change in RHR System unavailability due to the removal of the autoclosure interlock.

Failure to Initiate RHR

A single fault tree was developed for this phase of RHR operation to identify those faults that could impact the initiation of the RHR System, which is defined as being from startup through the first two hours of operation. An additional fault tree was not needed because this phase of operation is not dependent on the autoclosure feature but on the prevent-open interlock.

The fault tree for the Salem RHR Initiation is shown in Figure C-1. The basis for fault tree development was the Salem Operating Procedure OP II-6.3.2, "Initiating Residual Heat Removal". RHR initiation proceeds as follows:

1. Remove administrative controls and activate valves 1SJ49, RHR suction from the Refueling Water Storage Tank, 11SJ49 and 12SJ49, RHR discharge to RCS cold legs, 11RH18 and 12RH18, RHR heat exchanger outlets, and 1RH1 and 1RH2, common suction valves.

2. Open valves 11CC16 and 12CC16 to establish Component Cooling Water flow through the RHR heat exchangers.

3. Open valve 1SJ69 to establish RHR suction from the RWST.

4. Open valves 11RH12 and 12RH12, the RHR heat exchanger bypass isolation valves.

5. Close valves 11RH18 and 12RH18, the RHR heat exchanger outlet valves.

6. Close valves 11SJ49 and 12SJ49, the RHR discharge to the RCS cold legs.

7. Start and run the RHR pumps #11 and #12.

8. Open valves 1RH1 and 1RH2, the RHR common suction valves to the RCS hot legs.

9. Close valve 1SJ69, the RHR suction from the RWST.

10. Open valves 11SJ49 and 12SJ49, the RHR discharge to the RCS cold legs.

11. Crack open, then slowly open 1RH20, the RHR heat exchanger bypass valve to control RHR System temperature.

12. Slowly open valves 11RH18 and 12RH18, the RHR heat exchanger outlet valves, while closing 1RH20, the RHR heat exchanger bypass valve, to maintain the necessary RHR flow to the RCS cold legs while controlling the RHR System temperature.

Each of these steps was modeled in the Salem RHR initiation fault tree to involve an operator error or a component failure or both as appropriate. For example, the second step requires the opening of CCW valves to the RHR heat exchangers. Failure of this step could involve the operator failing to open the valve or the valve failing to open. Operator error modeling includes the possibility of recovery from the operator error by a checker.

Failure of Short Term Cooling

The fault trees developed for this phase of cooldown reflect that both RHR pump trains are required to be in operation to provide adequate cooling. Injection into any two of four RCS cold legs is required for success in this phase and inversely, failure to supply cooling flow from two RHR pump trains to three of four cold legs constitutes RHR System failure.

The short term cooling fault tree primarily features spurious closing of various valves and failure of the RHR pumps to run over the 72 hour period. The fault tree for the Salem Short Term Cooling - With Autoclosure Interlock is shown in Figure C-2. The fault tree for the Salem Short Term Cooling - Without Autoclosure Interlock is shown in Figure C-3.

Failure of Long Term Cooling

Only one RHR pump is required to operate for 6 weeks in the long term cooling phase to provide adequate cooling. Injection into any two of four RCS cold legs is required for success in this phase and inversely, failure to supply cooling flow from either of two RHR pump trains to three of four cold legs constitutes RHR System failure.

The long term cooling fault tree primarily features spurious closing of various valves over the six week period along with failure of the first RHR pump to continue running and failure of the second RHR pump to start and run upon failure of the running pump. The fault tree for the Salem Long Term Cooling - With Autoclosure Interlock is shown in Figure C-4. The fault tree for the Salem Long Term Cooling - Without Autoclosure Interlock, is shown in Figure C-5.

The fault trees were quantified for the case with and without the autoclosure interlock. The basic event probabilities (component unavailabilities and human error probabilities) are shown in Table C-2. The equation used to calculate the component unavailability is:

$$Q = (\lambda)\ T_M$$

where

Q = component failure probability

(λ) = failure rate for component

T_M = total defined mission time in which the component must operate.

The human error probability calculations for Salem are shown in Table C-3.

The unavailability of the Train B pump due to test is based on the Technical Specification 3.4.1.4 which states: "One RHR loop may be inoperable for up to 2 hours for surveillance testing provided the other RHR loop is OPERABLE and in operation." Assuming that pump testing occurs on a monthly basis (every 720 hours), the unavailability due to test is calculated by:

$$Q_{test} = (T)/T_T$$

where T = average duration of test (hours)

T_T = interval between tests (hours)

For Salem, the test unavailability is:

$$Q_{test} = (T)/T_T$$
$$= (2\ \text{hours}) / (720\ \text{hours})$$
$$= 2.78E\text{-}03$$

The unavailability due to maintenance was extracted from Reference 20, "Individual Plant Evaluation Methodology for Pressurized Water Reactors," April 1987, Section 2.4, Table 2.4-2 Generic Maintenance Durations for a standby pump tested monthly or quarterly and a component inoperability time limit of 72 hours. Therefore the unavailability due to maintenance is:

$$Q_{main} = (f_r)\ (T)_R$$
$$= (8.42E\text{-}05\ \text{events/hour})\ (18.7\ \text{hours/ event})$$
$$= 1.57E\text{-}03$$

where f_r = frequency of maintenance (events/hour)
$(T)_R$ = mean component repair time (hours/event)

Results

The results of the Salem quantification are shown in Table C-1. The major cutsets for each fault tree are shown in Tables C-4 to C-8.

For the failure of initiation fault tree, the dominant failure mode is operator error. The operator failing to energize the circuit breakers to the RHR suction valves 1RH1 and 1RH2 are the major cutsets. The deletion of the autoclosure interlock has no impact on the failure probability for RHRS initiation.

The failure probability of the short term cooling phase for Salem is reduced by 13 percent with the deletion of the ACI. The dominant failure mode for each fault tree (with and without the autoclosure interlock) is the failure of either pump to run for 72 hours (both pumps are required for success in this phase). For the case with the autoclosure interlock, failure of components associated with the ACI contribute approximately 1.7E-03 to the failure probability.

In the long term cooling phase for Salem, the failure of both pumps to run for six weeks is the dominant contributor to the unavailability. For the case with the ACI present, the other cutsets involve the single failure of a component associated with the ACI such as the power supply, signal comparator and pressure transmitter which causes spurious closure of one of the RHR suction valves. The deletion of the ACI for this phase of cooldown reduces the unavailability by 67 percent.

The results of the quantification of the Salem RHR unavailability fault trees show a trend that the autoclosure interlock becomes more of a determining and detrimental factor as the length of time in which the RHRS is required to operate increases. The deletion of the autoclosure interlock reduces the number of spurious closures of the RHR suction valves and thus increases the availability of the RHRS.

TABLE C-1
SALEM
RHR SYSTEM UNAVAILABILITY RESULTS

FAULT TREE PHASE	WITH AUTOCLOSURE	WITHOUT AUTOCLOSURE	PERCENT CHANGE
INITIATION	3.20E-02	3.20E-02	0
SHORT TERM	1.60E-02	1.40E-02	-13
LONG TERM	3.60E-02	1.20E-02	-67

TABLE C-2

SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
RHR INITIATION					
MV1690POE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
MV1690PD	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
XV11RH12OE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
XV11RH12D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
XV12RH12OE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
XV12RH12D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
AV1118ASOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
AV1118CLOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
AV1118CLD	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV1218ASOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
AV1218CLOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
AV1218CLD	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
MV1149CPOE	OE	OPERATOR FAILS TO PO	1.210E-03	---	1.21E-03
MV1149CLOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
MV1149CLD	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MV1249CPOE	OE	OPERATOR FAILS TO PO	1.210E-03	---	1.21E-03
MV1249CLOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
MV1249CLD	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
PM11S	PM	FAILURE TO START	1.000E-05	2.000E+00	2.00E-05
PM11R	PM	FAIL TO RUN,GIVEN ST	1.000E-04	2.000E+00	2.00E-04
PM12S	PM	FAILURE TO START	1.000E-05	2.000E+00	2.00E-05

TABLE C-2 (Cont)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
PM12R	PM	FAIL TO RUN,GIVEN ST	1.000E-04	2.000E+00	2.00E-04
MV1RH1CBOE	OE	OPERATOR FAILS TO EN	1.610E-03	---	1.61E-03
MV1RH1OE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
1RH1MECH	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
1RECO6CSVF	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
1RECN6CSVF	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1DED6F	DE	DIODE STANDARD QUALI	7.560E-09	2.000E+00	1.51E-08
1CNS1OPENF	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1RHFU30PHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1RHFU30PHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1RHFU30PHC	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1RHCN90PHA	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1RHCN90PHB	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1RHCN90PHC	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1RHOL49PHA	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1RHOL49PHB	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1RHOL49PHC	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1RHCB8	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
1RHCT230	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
1RHFU15A1	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1RHFU15A2	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07

TABLE C-2 (Cont)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1RHOLCN49	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1RHRECO9C	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
1RHRECN9O	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1RHQS	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
1RHCN9XC	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1RHCN9C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1RHRECO9XC	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
1RECO63XF	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
1RECN63XF	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1PS118VACF	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
1BIF05AF	BI	BISTABLE HIGH OUTPUT	2.400E-06	2.000E+00	4.80E-06
1CMPC405AB	CM	COMPARATOR ALL MODES	2.900E-06	2.000E+00	5.80E-06
1PM405RF	IV	I-E CONVERTER ALL FA	2.000E-07	2.000E+00	4.00E-07
1PC405RF	IV	I-E CONVERTER ALL FA	2.000E-07	2.000E+00	4.00E-07
1RS4051F	RS	RESISTOR STANDARD QU	4.900E-09	2.000E+00	9.80E-09
1PS405F	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
1ST405F	ST	TOGGLE SWITCH ALL MO	2.330E-07	2.000E+00	4.66E-07
1TP405F	TP	PRESSURE SENSORS ALL	2.800E-06	2.000E+00	5.60E-06
MV1RH2CBOE	OE	OPERATOR FAILS TO EN	1.610E-03	---	1.61E-03
MV1RH2OE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
2RH1MECH	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
2RECO6CSVF	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06

TABLE C-2 (Cont)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2RECN6CSVF	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2DED6F	DE	DIODE STANDARD QUALI	7.560E-09	2.000E+00	1.51E-08
2CNS1OPENF	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2RHFU30PHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2RHFU30PHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2RHFU30PHC	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2RHCN90PHA	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2RHCN90PHB	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2RHCN90PHC	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2RHOL49PHA	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2RHOL49PHB	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2RHOL49PHC	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2RHCB8	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
2RHCT230	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
2RHFU15A1	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2RHFU15A2	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2RHOLCN49	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2RHRECO9C	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
2RHRECN90	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2RHQS	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
2RHCN9XC	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06

TABLE C-2 (Cont)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2RHCN9C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2RHRECO9XC	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
2RECO63XF	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
2RECN63XF	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2PS118VACF	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
2BIF03AF	BI	BISTABLE HIGH OUTPUT	2.400E-06	2.000E+00	4.80E-06
2CMPC403AB	CM	COMPARATOR ALL MODES	2.900E-06	2.000E+00	5.80E-06
2PM403RF	IV	I-E CONVERTER ALL FA	2.000E-07	2.000E+00	4.00E-07
2PC403RF	IV	I-E CONVERTER ALL FA	2.000E-07	2.000E+00	4.00E-07
2RS4031F	RS	RESISTOR STANDARD QU	4.900E-09	2.000E+00	9.80E-09
2PS403F	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
2ST403F	ST	TOGGLE SWITCH ALL MO	2.330E-07	2.000E+00	4.66E-07
2TP403F	TP	PRESSURE SENSORS ALL	2.800E-06	2.000E+00	5.60E-06
MV169CBOE	OE	OPERATOR FAILS TO EN	1.610E-03	---	1.61E-03
MV1SJ690E	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
MV169CLD	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MV11490POE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
MV11490PD	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
MV12490POE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
MV12490PD	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
AV1200POE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03

TABLE C-2 (Cont)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
AV120OPD	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV1118OPOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
AV1118OPD	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV1218OPOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
AV1218OPD	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV120CLOE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
AV120CLD	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
MV11CC16OE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
MV11CC16D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
MV12CC16OE	OE	OPERATOR FAILS TO OP	1.210E-03	---	1.21E-03
MV12CC16D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
SHORT TERM COOLING					
CV14SJ56D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV14SJ43D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
MV12SJ49V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
MV12RH19V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
MV11RH19V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
MV12CC16V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
PM12X	PM	FAIL TO RUN,GIVEN ST	1.000E-04	7.200E+01	7.20E-03
MV12RH4V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CV12RH8D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05

TABLE C-2 (Cont)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1RHCN9/CQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1RHCN63XQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1RHIVPMF	IV	I-E CONVERTER ALL FA	2.000E-07	7.200E+01	1.44E-05
1RHIVPCF	IV	I-E CONVERTER ALL FA	2.000E-07	7.200E+01	1.44E-05
1RHPT405	TP	PRESSURE SENSORS ALL	2.800E-06	7.200E+01	2.02E-04
1RHPSPQ405	PS	LOOP POWER SUPPLY AL	5.800E-06	7.200E+01	4.18E-04
1RHCM405	CM	COMPARATOR ALL MODES	2.900E-06	7.200E+01	2.09E-04
1RHCNCLOSE	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1RHCN5CSVQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1RHCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1RHCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1RHCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2RHCN9/CQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2RHCN63XQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2RHIVPMF	IV	I-E CONVERTER ALL FA	2.000E-07	7.200E+01	1.44E-05
2RHIVPCF	IV	I-E CONVERTER ALL FA	2.000E-07	7.200E+01	1.44E-05
2RHPT405	TP	PRESSURE SENSORS ALL	2.800E-06	7.200E+01	2.02E-04
2RHPSPQ405	PS	LOOP POWER SUPPLY AL	5.800E-06	7.200E+01	4.18E-04
2RHCM405	CM	COMPARATOR ALL MODES	2.900E-06	7.200E+01	2.09E-04
2RHCNCLOSE	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2RHCN5CSVQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06

TABLE C-2 (Cont)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2RHCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2RHCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2RHCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
CV12SJ43D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV12SJ56D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV13SJ43D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV13SJ56D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
MV11SJ49V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
MV11CC16V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
PM11X	PM	FAIL TO RUN,GIVEN ST	1.000E-04	7.200E+01	7.20E-03
MV11RH4V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CV11SJ43D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV11SJ56D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV11RH8D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
LONG TERM COOLING					
MV12SJ49V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
MV12RH19V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
MV11RH19V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
MV12CC16V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
CV12RH8D	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04
MV12RH4V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04

TABLE C-2 (Cont)

SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
PM12TEST	TE	TEST UNAVAILABILITY	2.780E-03	---	2.78E-03
PM12MAIN	MA	MAINTENANCE UNAVAILA	1.570E-03	---	1.57E-03
PM12A	PM	FAILURE TO START	1.000E-05	1.008E+03	1.01E-02
PM12X	PM	FAIL TO RUN,GIVEN ST	1.000E-04	1.008E+03	1.01E-01
1RHCN9/CQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1RHCN63XQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1RHIVPMF	IV	I-E CONVERTER ALL FA	2.000E-07	1.008E+03	2.02E-04
1RHIVPCF	IV	I-E CONVERTER ALL FA	2.000E-07	1.008E+03	2.02E-04
1RHPT405	TP	PRESSURE SENSORS ALL	2.800E-06	1.008E+03	2.82E-03
1RHPSPQ405	PS	LOOP POWER SUPPLY AL	5.800E-06	1.008E+03	5.85E-03
1RHCM405	CM	COMPARATOR ALL MODES	2.900E-06	1.008E+03	2.92E-03
1RHCNCLOSE	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1RHCN5CSVQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1RHCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1RHCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1RHCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2RHCN9/CQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2RHCN63XQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2RHIVPMF	IV	I-E CONVERTER ALL FA	2.000E-07	1.008E+03	2.02E-04
2RHIVPCF	IV	I-E CONVERTER ALL FA	2.000E-07	1.008E+03	2.02E-04
2RHPT405	TP	PRESSURE SENSORS ALL	2.800E-06	1.008E+03	2.82E-03

TABLE C-2 (Cont)
SALEM BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2RHPSPQ405	PS	LOOP POWER SUPPLY AL	5.800E-06	1.008E+03	5.85E-03
2RHCM405	CM	COMPARATOR ALL MODES	2.900E-06	1.008E+03	2.92E-03
2RHCNCLOSE	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2RHCN5CSVQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2RHCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2RHCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2RHCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
MV11SJ49V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
MV11CC16V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
PM11X	PM	FAIL TO RUN GIVEN ST	1.000E-04	1.008E+03	1.01E-01
MV11RH4V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04

TABLE C-3

SALEM
HUMAN ERROR CALCULATIONS

TASK: Select "valve operable" position on the control power lockout switch to 1SJ69. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.1(a) of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to select "valve operable" position of the control power lockout switch to motor operated RHR suction valve from RWST (1SJ69).

HEP median = 0.003 HEP mean = 3.75E-03 Error Factor = 3	Table 20-7(2)	Long List > 10 items; when procedures with checkoff provisions are correctly used.

2. Commission error - Operator selects wrong lockout switch in place of the switch for the RHR suction valve from RWST (1SJ69).

HEP median = 0.003 HEP mean = 3.75E-03 Error Factor = 3	Table 20-12(2)	Select wrong control on a panel from an array of similar appearing controls identified by labels only.

3. Recovery error - Shift supervisor fails to detect error by others.

HEP median = 0.1 HEP mean = 1.61E-01 Error factor = 5	Table 20-22(1)	Checking routine tasks, checker using written materials.

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)
P_{OE} = 1.21-03

Fault Tree Identifier: MV169CBOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Select "valve operable" position of control power lockout switch to 11SJ49 or 12SJ49. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.1(b) of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to select "valve operable" position of the control power lockout switch to motor operated RHR discharge to cold legs valve (11SJ49 or 12SJ49).

   Table 20-7(2) — Long List > 10 items; when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong lockout switch in place of the switch for an RHR discharge to cold legs valve (11SJ49 or 12SJ49).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

$$P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)$$
$$P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)$$
$$P_{OE} = 1.21-03$$

Fault Tree Identifiers: MV1149CPOE, MV1249CPOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Remove Shift Supervisors tag from air supply valve to 11RH18 or 12RH18 and open the air supply valve. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.1(c) of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to remove shift supervisors tag from the air supply valve and to open the air supply valve to air operated RHR heat exchanger outlet valve (11RHR18 or 12RH18).

   Table 20-7(2) — Long List > 10 items; when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong air supply valve in place of the valve for an RHR heat exchanger outlet valve (11RHR18 or 12RH18).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

$P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)$
$P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)$
$P_{OE} = 1.21-03$

Fault Tree Identifiers: AV1118ASOE, AV1218ASOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Remove Shift Supervisors tags from power supply to 1RH1 or 1RH2 and energize the valve. Complete "Check Off Sheet 1" of OP II 6.3.2.

REFERENCE: Step 5.1.1(d) of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to remove supervisors tag from power supply and energize motor operated RHR common suction valve (1RHR1 or 1RH2).

   Table 20-7(2) — Long List > 10 items; when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator removes tag and energizes wrong valve in place of an RHR common suction valve (1RH1 or 1RH2).

   Table 20-12(11) — Select wrong circuit breaker in a group of circuit breakers densely grouped and identified by labels only.

   HEP median = 0.005, error factor = 3
   HEP mean = 6.25E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](6.25E-03)(1.61E-01)
P_{OE} = 1.61-03

Fault Tree Identifiers: MV1RH1CBOE, MV1RH2CBOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Open 11CC16 and 12CC16. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.2(a) of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open a motor operated RHR heat exchanger outlet valve (11CC16 or 12CC16).

   Table 20-7(2) Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of an RHR heat exchanger outlet valve (11CC16 or 12CC16).

   Table 20-12(2) Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)
P_{OE} = 1.21-03

Fault Tree Identifiers: MV11CC16OE, MV12CC16OE

TABLE C-3 (Cont)

HUMAN ERROR CALCULATIONS - SALEM

TASK: Open 11RH12 or 12RH12. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.5 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open a manually operated RHR heat exchanger bypass isolation valve (11RHR12 or 12RH12).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of an RHR heat exchanger bypass isolation valve (11RH12 or 12RH12).

   Table 20-13(2) — Select wrong valve from a group of clearly and unambiguously labeled valves similar in one of the following: size and shape, state and presence of tags.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)
P_{OE} = 1.21-03

Fault Tree Identifiers: XV11RH12OE, XV12RH12OE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Close 11RH18 and 12RH18. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.7 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close an air operated RHR heat exchanger outlet valve (11RH18 or 12RH18).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of an RHR heat exchanger outlet valve (11RH18 or 12RH18).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)
P_{OE} = 1.21-03

Fault Tree Identifiers: AV1118CLOE, AV1218CLOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Close 11SJ49 or 12SJ49. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Complete step 5.1.8 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close a motor operated RHR discharge to cold leg valve (11SJ49 or 12SJ49).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of an RhR discharge to cold leg valve (11SJ49 or 12SJ49).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)
P_{OE} = 1.21-03

Fault Tree Identifiers: MV1149CLOE, MV1249CLOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Open 1RH1 or 1RH2. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.13 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open a motor operated RHR common suction valve (1RHR1 or 1RH2).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of an RHR common suction valve (1RH1 or 1RH2).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

$$P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)$$
$$P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)$$
$$P_{OE} = 1.21-03$$

Fault Tree Identifiers: MV1RH1OE, MV1RH2OE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Close 1SJ69. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.14 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close the motor operated RHR suction valve from RWST (1SJ69).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of the RHR suction valve from RWST (1SJ69).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

$P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)$
$P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)$
$P_{OE} = 1.21-03$

Fault Tree Identifier: MV1SJ69OE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Open 11SJ49 or 12SJ49. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.16 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open a motor operated RHR discharge to cold leg valve (11SJ49 or 12SJ49).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of an RHR discharge ot cold leg valve (11SJ49 or 12SJ49).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)
P_{OE} = 1.21-03

Fault Tree Identifiers: MV1149OPOE, MV1249OPOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Slowly open 1RH20. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE. Steps 5.1.17 and 5.1.18 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open the air operated RHR heat exchanger bypass valve (1RH20).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong air control valve in place of the RHR heat exchanger bypass valve (1RH20).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

$P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)$
$P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)$
$P_{OE} = 1.21-03$

Fault Tree Identifiers: AV120OPOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Slowly open 11RH18 and 12RH18. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.19 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open an air operated RHR heat exchanger outlet valve (11RH18 or 12RH18).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of an RHR heat exchanger outlet valve (11RH18 or 12RH18).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   Q2 mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   Q3 mean = 1.61E-01

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)
P_{OE} = 1.21-03

Fault Tree Identifiers: AV1118OPOE, AV1218OPOE

TABLE C-3 (Cont)

SALEM
HUMAN ERROR CALCULATIONS

TASK: Close 1RH20. Complete "Check Off Sheet 1" of OP II-6.3.2.

REFERENCE: Step 5.1.19 of OP II-6.3.2 Revision 11, "Initiating Residual Heat Removal".

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close an air operated RHR heat exchanger bypass valve (1RH20).

   Table 20-7(2) — Long List > 10 items, when procedures with checkoff provisions are correctly used.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

2. Commission error - Operator selects wrong valve in place of an RHR heat exchanger bypass valve (1RH20).

   Table 20-12(2) — Select wrong control on a panel from an array of similar appearing controls identified by labels only.

   HEP median = 0.003, error factor = 3
   HEP mean = 3.75E-03

3. Recovery error - Shift supervisor fails to detect error by others.

   Table 20-22(1) — Checking routine tasks, checker using written materials.

   HEP median = 0.1, error factor = 5
   HEP mean = 1.61E-01

P_{OE} = (Q1)(Q3) + (1-Q1)(Q2)(Q3)
P_{OE} = (3.75E-03)(1.61E-01) + [1-(3.75E-03)](3.75E-03)(1.61E-01)
P_{OE} = 1.21-03

Fault Tree Identifiers: AV120CLOE

TABLE C-4

SALEM
DOMINANT CONTRIBUTORS
RHR INITIATION

MEAN PROBABILITY OF FAILURE = 3.20E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.61E-03	OPERATOR FAILS TO ENERG. CB TO MOTOR OPERATED VALVE 1RH2
2.	1.61E-03	OPERATOR FAILS TO ENERG. CB TO MOTOR OPERATED VALVE 1RH1
3.	1.61E-03	OPERATOR FAILS TO ENERG. CB TO MOTOR OPERATED VALVE 1SJ69
4.	1.21E-03	OPERATOR FAILS TO OPEN MOTOR OPERATED VALVE 12CC16
5.	1.21E-03	OPERATOR FAILS TO OPEN MOTOR OPERATED VALVE 11CC16
6.	1.21E-03	OPERATOR FAILS TO CLOSE AIR OPERATED VALVE 1RH20
7.	1.21E-03	OPERATOR FAILS TO OPEN AIR OPERATED VALVE 12RH18
8.	1.21E-03	OPERATOR FAILS TO OPEN AIR OPERATED VALVE 11RH18
9.	1.21E-03	OPERATOR FAILS TO OPEN AIR OPERATED VALVE 1RH20
10.	1.21E-03	OPERATOR FAILS TO OPEN MOTOR OPERATED VALVE 12SJ49
11.	1.21E-03	OPERATOR FAILS TO OPEN MOTOR OPERATED VALVE 11SJ49
12.	1.21E-03	OPERATOR FAILS TO CLOSE MOTOR OPERATED VALVE 1SJ69
13.	1.21E-03	OPERATOR FAILS TO OPEN MOTOR OPERATED VALVE 1RH2
14.	1.21E-03	OPERATOR FAILS TO OPEN MOTOR OPERATED VALVE 1RH1
15.	1.21E-03	OPERATOR FAILS TO CLOSE MOTOR OPERATED VALVE 12SJ49
16.	1.21E-03	OPERATOR FAILS TO POSITION CP L/O SWITCH FOR VALVE 12SJ49
17.	1.21E-03	OPERATOR FAILS TO CLOSE MOTOR OPERATED VALVE 11SJ49
18.	1.21E-03	OPERATOR FAILS TO POSITION CP L/O SWITCH FOR VALVE 11SJ49
19.	1.21E-03	OPERATOR FAILS TO CLOSE AIR OPERATED VALVE 12RH18
20.	1.21E-03	OPERATOR FAILS TO OPEN AIR SUPPLY VALVE TO AV 12RH18

TABLE C-5

SALEM
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.60E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	7.20E-03	RHR PUMP NO. 12 FAILS TO RUN FOR 72 HOURS
2.	7.20E-03	RHR PUMP NO. 11 FAILS TO RUN FOR 72 HOURS
3.	4.18E-04	LOOP POWER SUPPLY FAILS HIGH
4.	4.18E-04	LOOP POWER SUPPLY FAILS HIGH
5.	2.09E-04	SIGNAL COMPARATOR FAILS
6.	2.09E-04	SIGNAL COMPARATOR FAILS
7.	2.02E-04	PRESSURE TRANSMITTER FAILS
8.	2.02E-04	PRESSURE TRANSMITTER FAILS
9.	1.44E-05	I/V MODULE FAILS 2-PC-405R
10.	1.44E-05	I/V MODULE FAILS 2-PM-405R
11.	1.44E-05	I/V MODULE FAILS 1-PC-405R
12.	1.44E-05	I/V MODULE FAILS 1-PM-405R
13.	1.44E-05	PUMP DISCHARGE CHECK VALVE 12RH8 FAILS TO OPEN
14.	1.44E-05	PUMP SUCTION VALVE 12RH4 SPURIOUSLY CLOSES (MOV)
15.	1.44E-05	RHR HEAT EXCH. 12 FAILS TO REMOVE HEAT (CCW VALVE SPURIOUS CLOSE)
16.	1.44E-05	PUMP DISCHARGE CHECK VALVE 11RH8 FAILS TO OPEN
17.	1.44E-05	PUMP SUCTION VALVE 11RH4 SPURIOUSLY CLOSES (MOV)
18.	1.44E-05	RHR HEAT EXCH. 11 FAILS TO REMOVE HEAT (CCW VALVE SPURIOUS CLOSE)
19.	1.44E-05	CROSSTIE VALVE 11RH19 (MOV) SPURIOUSLY CLOSES
20.	1.44E-05	CROSSTIE VALVE 12RH19 (MOV) SPURIOUSLY CLOSES

TABLE C-6

SALEM
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.40E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	7.20E-03	RHR PUMP NO. 12 FAILS TO RUN FOR 72 HOURS
2.	7.20E-03	RHR PUMP NO. 11 FAILS TO RUN FOR 72 HOURS
3.	1.44E-03	PUMP DISCHARGE CHECK VALVE 12RH8 FAILS TO OPEN
4.	1.44E-05	PUMP SUCTION VALVE 12RH4 SPURIOUSLY CLOSES (MOV)
5.	1.44E-05	RHR HEAT EXCH. 12 FAILS TO REMOVE HEAT (CCW VALVE SPURIOUS CLOSE)
6.	1.44E-05	PUMP DISCHARGE CHECK VALVE 11RH8 FAILS TO OPEN
7.	1.44E-05	PUMP SUCTION VALVE 11RH4 SPURIOUSLY CLOSES (MOV)
8.	1.44E-05	RHR HEAT EXCH. 11 FAILS TO REMOVE HEAT (CCW VALVE SPURIOUS CLOSE)
9.	1.44E-05	CROSSTIE VALVE 11RH19 (MOV) SPURIOUSLY CLOSES
10.	1.44E-05	CROTTIES VALVE 12RH19 (MOV) SPURIOUSLY CLOSES
11.	1.44E-06	LOCKIN CIRCUITRY FAILURE CONTACT 9/C SHORTS CLOSED
12.	1.44E-06	CLOSE RELAY COIL CONTACT 5/CSV1 FAILS
13.	1.44E-06	CLOSE CONTACT 1/CLOSE SHORTS
14.	1.44E-06	LOCKIN CIRCUITRY FAILURE CONTACT 9/C SHORTS CLOSED
15.	1.44E-06	CLOSE RELAY COIL CONTACT 5/CSV1 FAILS
16.	1.44E-06	CLOSE CONTACT 1/CLOSE SHORTS
17.	2.07E-10	RHR DISCHARGE VALVE 12SJ49 SPURIOUSLY CLOSES (MOV) RHR DISCHARGE VALVE 11SJ49 SPURIOUSLY CLOSES
18.	2.07E-10	CHECK VALVE 12SJ56 FAILS TO OPEN RHR DISCHARGE VALVE 11SJ49 SPURIOUSLY CLOSES

TABLE C-6 (Cont)

SALEM
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.40E-02

	PROBABILITY	CUTSET DESCRIPTION
19.	2.07E-10	CHECK VALVE 12SJ43 FAILS TO OPEN RHR DISCHARGE VALVE 11SJ49 SPURIOUSLY CLOSES
20.	2.07E-10	CHECK VALVE 14SJ43 FAILS TO OPEN RHR DISCHARGE VALVE 11SJ49 SPURIOUSLY CLOSES

TABLE C-7

SALEM
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 3.60E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.02E-02	PUMP NO. 12 FAILS TO RUN FOR SIX WEEKS PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
2.	5.85E-03	LOOP POWER SUPPLY FAILS HIGH (1RH1)
3.	5.85E-03	LOOP POWER SUPPLY FAILS HIGH (1RH2)
4.	2.92E-03	SIGNAL COMPARATOR FAILS (1RH1)
5.	2.92E-03	SIGNAL COMPARATOR FAILS (1RH2)
6.	2.82E-03	PRESSURE TRANSMITTER FAILS (1RH1)
7.	2.82E-03	PRESSURE TRANSMITTER FAILS (1RH2)
8.	1.02E-03	PUMP NO. 12 FAILS TO START ON DEMAND PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
9.	2.81E-04	PUMP NO. 12 UNAVAILABLE DUE TO TEST PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
10.	2.02E-04	RHR DISCHARGE VALVE 11SJ49 SPURIOUSLY CLOSES
11.	2.02E-04	RHR DISCHARGE VALVE 12SJ49 SPURIOUSLY CLOSES (MOV)
12.	2.02E-4	I/V MODULE FAILS (1RH1) (PC)
13.	2.02E-04	I/V MODULE FAILS (1RH2) (PC)
14.	2.02E-04	I/V MODULE FAILS (1RH1) (PM)
15.	2.02E-04	I/V MODULE FAILS (1RH2) (PM)
16.	1.59E-04	PUMP NO. 12 UNAVAILABLE DUE TO MAINTENANCE PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
17.	2.04E-05	PUMP SUCTION VALVE 12RH4 SPURIOUSLY CLOSES PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS

TABLE C-7 (Cont)

SALEM
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 3.60E-02

	PROBABILITY	CUTSET DESCRIPTION
18.	2.04E-05	PUMP DISCHARGE CHECK VALVE 12RH8 FAILS TO OPEN PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
19.	2.04E-05	HEAT EXCH. 12 FAILS TO REMOVE HEAT (CCW VALVE SPURIOUS CLOSE) PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
20.	2.04E-05	PUMP NO. 12 FAILS TO RUN FOR SIX WEEKS PUMP SUCTION VALVE 11RH4 SPURIOUSLY CLOSES

TABLE C-8

SALEM
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.20E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.02E-02	PUMP NO. 12 FAILS TO RUN FOR SIX WEEKS PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
2.	1.02E-03	PUMP NO. 12 FAILS TO START ON DEMAND PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
3.	2.81E-04	PUMP NO. 12 UNAVAILABLE DUE TO TEST PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
4.	2.02E-04	RHR DISCHARGE VALVE 11SJ49 SPURIOUSLY CLOSES
5.	2.02E-04	RHR DISCHARGE VALVE 12SJ49 SPURIOUSLY CLOSES (MOV)
6.	1.59E-04	PUMP NO. 12 UNAVAILABLE DUE TO MAINTENANCE PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
7.	2.04E-05	PUMP SUCTION VALVE 12RH4 SPURIOUSLY CLOSES PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
8.	2.04E-05	PUMP DISCHARGE CHECK VALVE 12RH8 FAILS TO OPEN PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
9.	2.04E-05	HEAT EXCH. 12 FAILS TO REMOVE HEAT (CCW VALVE SPURIOUS CLOSE) PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
10.	2.04E-05	PUMP NO. 12 FAILS TO RUN FOR SIX WEEKS PUMP SUCTION VALVE 11RH4 SPURIOUSLY CLOSES
11.	2.04E-05	PUMP NO. 12 FAILS TO RUN FOR SIX WEEKS HEAT EXCH. 11 FAILS TO REMOVE HEAT (CCW VALVE SPURIOUS CLOSE)
12.	2.04E-05	CROSSTIE VALVE 11RH19 SPURIOUSLY CLOSES PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
13.	2.04E-05	CROSSTIE VALVE 12RH19 SPURIOUSLY CLOSES PUMP NO. 11 FAILS TO RUN FOR SIX WEEKS
14.	2.04E-05	CROSSTIE VALVE 11RH19 SPURIOUSLY CLOSES PUMP NO. 12 FAILS TO RUN FOR SIX WEEKS

TABLE C-8 (Cont)

SALEM
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.20E-02

	PROBABILITY	CUTSET DESCRIPTION
15.	2.04E-05	CROSSTIE VALVE 12RH19 SPURIOUSLY CLOSES PUMP NO. 12 FAILS TO RUN FOR SIX WEEKS
16.	2.02E-05	LOCKIN CIRCUITRY FAILURE CONTACT 9/C SHORTS CLOSED (1RH1)
17.	2.02E-05	CLOSE RELAY COIL CONTACT 5/CSV1 FAILS (1RH1)
18.	2.02E-05	CLOSE CONTACT 1/CLOSE SHORTS (1RH1)
19.	2.02E-05	LOCKIN CIRCUITRY FAILURE CONTACT 9/C SHORTS CLOSED (1RH2)
20.	2.02E-05	CLOSE RELAY COIL CONTACT 5/CSV1 FAILS (1RH2)

OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 5

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH

C.3.2 CALLAWAY

Three fault trees were developed to model the RHR System unavailability for Callaway. These fault trees were developed from the system flow diagrams and control wiring diagrams shown and described in Section 5.2 for Callaway. Each fault tree is discussed below. The RHR suction valves EJ-HV-8701A, EJ-HV-8701B, BB-PV-8702A, and BB-PV-8702B were modeled in detail down to the control circuitry level to explicitly show the change in unavailability due to removal of the autoclosure interlock.

Failure during RHR Initiation

The fault tree developed for this phase of cooldown (Figure C-6) details the failure during initiation of the RHR System. The fault tree was developed based on the RHR System Operating Procedure OTN-EJ-00001, Revision 4, Section 4.3, "Placing the RHR System in Service for Normal Cooldown." The steps for RHR initiation are summarized below:

1. Close RHR heat exchanger bypass control valve EJ-FCV-618 and EJ-FCV-619.

2. Close RHR heat exchanger flow control valve EJ-HCV-606 and EJ-HCV-607.

3. Unlock and close the supply breakers for the RHR System, loop suction valves, EJ-HV-8701A, EJ-HV-8701B, BB-PV-8702A, and BB-PV-8702B.

4. Open the CCW inlet valves to the RHR heat exchanger, EG-HV-101 and EG-HV-102.

5. Close RHR pump suction valves from RWST, BN-HV-8812A and BN-HV-8812B.

6. Open the RHR loop inlet isolation valves, EJ-HV-8701A, EJ-HV-8701B, BB-PV-8702A, and BB-PV-8702B.

7. Start RHR pump, PEJ01A and PEJ01B.

8. Close EJ-HV-8716A and EJ-HV-8716B.

9. Slowly open RHR heat exchanger bypass valve EJ-HCV-618 and EJ-FCV-619.

10. Open RHR heat exchanger flow control valve EJ-HCV-606 and EJ-HCV-607.

Each of these steps was modeled in the fault tree to involve an operator error or a component failure. For example, the fourth step requires the opening of a CCW valve to the RHR heat exchanger. Failure of this step could involve: 1) the operator failing to open the valve or 2) the valve failing to open. This phase of cooldown is not dependent on the auto closure interlock but on the prevent-open interlock. Thus, only one fault tree was developed.

Loss of Short Term Cooling

The fault tree developed for this phase of cooldown (Figure C-7 with ACI and Figure C-8 without ACI) requires that both trains of RHR be in operation. Injection into two of four cold legs for 72 hours is required for success in this phase. The RHR suction valves are modeled in detail to show how the valves could spuriously close. With the autoclosure interlock present, a spurious pressure signal could cause the suction valves to spuriously close. With the autoclosure signal removed from the circuit, the valves are less likely to spuriously close.

Loss of Long Term Cooling

For this phase of plant cooldown, only one RHR train (pump and heat exchanger) are required to be operating for a period of six weeks. Injection into two of four cold legs is the success criteria. The fault tree developed for the case with the ACI is shown in Figure C-9, while the case without the ACI is shown in Figure C-10.

The fault trees were quantified for the case with and without the autoclosure interlock. The basic event probabilities (component unavailabilities and human error probabilities) are shown in Table C-10. The equation used to calculate the component unavailability is :

$$Q = (\lambda)\ T_M$$

where

Q = component failure probability

(λ) = failure rate for component

T_M = total defined mission time in which the component must operate.

The human error probability calculations for Callaway are shown in Table C-11.

The unavailability of the Train B pump due to test is based on the Technical Specification 3.4.1.4.1 which states: "One RHR loop may be inoperable for up to 2 hours for surveillance testing probided the other RHR loop is OPERABLE and in operation." Assuming that pump testing occurs on a monthly basis (every 720 hours), the unavailability due to test is calculated by:

$$Q_{test} = (T)/T_T$$

where T = average duration of test (hours)

T_T = interval between tests (hours)

For Callaway, the test unavailability is:

$$Q_{test} = (T)/T_T$$
$$= (2 \text{ hours}) / (720 \text{ hours})$$
$$= 2.78E\text{-}03$$

The unavailability due to maintenance was extracted from Reference 20, "Individual Plant Evaluation Methodology for Pressurized Water Reactors," April 1987, Section 2.4, Table 2.4-2 Generic Maintenance Durations for a standby pump tested monthly or quarterly and a component inoperability time limit of 72 hours. Therefore the unavailability due to maintenance is:

$$\begin{aligned} Q_{main} &= (f_r)\,(T)_R \\ &= (8.42E\text{-}05 \text{ events/hour})\,(18.7 \text{ hours/ event}) \\ &= 1.57E\text{-}03 \end{aligned}$$

where f_r = frequency of maintenance (events/hour)
$(T)_R$ = mean component repair time (hours/event)

Results

The results of the quantification are shown in Table C-9. The major cutsets for each fault tree are shown in Tables C-12 to C-16.

For the failure of initiation fault tree, the dominant failure mode is the operator failing to open the suction valves from the RCS to the RHRS. The deletion of the autoclosure interlock has no effect on the failure probability for RHRS initiation.

The failure probability of the short term cooling mode for Callaway is reduced by 12 percent with the deletion of the ACI. The dominant failure mode for each fault tree (with and without the autoclosure interlock) is the failure of either pump to run for 72 hours (both pumps are required for success in this phase). For the case with the autoclosure interlock, failure of components associated with the ACI contribute approximately 2.0E-03 to the failure probability.

In the long term cooling phase for Callaway, the failure of both pumps is the dominant contributor to unavailability. The pump failure modes considered included pump A failing to run and pump B failing to start or run given pump A has failed. The other dominant contributors involve failure of the ACI. The deletion of the ACI for this phase of cooldown reduces the unavailability by 70 percent.

The results of the quantification of the Callaway RHR unavailability fault trees show a trend that the longer the RHR system is in operation, the more likely it becomes that the RHRS suction valves will spuriously close. Thus, the availability of the RHRS increases with the deletion of the autoclosure interlock because the suction valves are less likely to spuriously close.

TABLE C-9

CALLAWAY
RHR SYSTEM UNAVAILABILITY
RESULTS

FAULT TREE PHASE	WITH AUTOCLOSURE	WITHOUT AUTOCLOSURE	PERCENT CHANGE
INITIATION	3.62E-02	3.62E-02	-
SHORT TERM	1.64E-02	1.44E-02	-12
LONG TERM	3.91E-02	1.17E-02	-70

TABLE C-10

CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
RHR INITIATION					
AV618CLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV618K	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV619CLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV619K	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV606CLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV606K	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV607CLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV607K	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
MV812ACLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MV8812AK	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MV812BCLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MV8812BK	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MV701ACBOE	OE	OPERATOR FAILS TO EN	1.600E-03	---	1.60E-03
MV8701AOE	OE	OPERATOR FAILS TO OP	3.200E-03	---	3.20E-03
1ATPPT405	TP	PRESSURE SENSORS ALL	2.800E-06	2.000E+00	5.60E-06
1APSPQY405	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
1ACMPB405A	CM	COMPARATOR ALL MODES	2.900E-06	2.000E+00	5.80E-06
1ABIPS405A	BI	BISTABLE HIGH OUTPUT	2.400E-06	2.000E+00	4.80E-06
1ARSPS405	RS	RESISTOR STANDARD QU	4.900E-09	2.000E+00	9.80E-09
1ACNK734	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06

TABLE C-10 (Cont)

CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1ACN33BCRW	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1ACN33BCSU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1ACN33BCCH	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1ACNHISOPE	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1ACN420/A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1ACN42C/BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1ARECO420F	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
1ACB52U	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
1AFU40APHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1AFU40APHB	FU	FUSE ALL MODES	1.500E [illegible]	2.000E+00	3.00E-07
1AFU40APHC	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1AOL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1AOL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1AOL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1AMSCN420A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1AMSCN420B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1AMSCN420C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1AFU1APHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1AFU1APHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1ACT480120	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
1AFU2AMP	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07

TABLE C-10 (Cont)

CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1AOLCN49AB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1AOLCN49BB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1AOLCN49CB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1AQSWS18	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
MV702ACBOE	OE	OPERATOR FAILS TO EN	1.600E-03	---	1.60E-03
MV8702AOE	OE	OPERATOR FAILS TO OP	3.200E-03	---	3.20E-03
2ACNK734	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2ACN33BCRW	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2ACN33BCSU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2ACN33BCCH	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2ACN[illegible]SOPE	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2ACN420/A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2ACN42C/BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2ARECO420F	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
2ACB52U	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
2AFU40APHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2AFU40APHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2AFU40APHC	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2AOL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2AOL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2AOL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07

TABLE C-10 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2AMSCN420A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2AMSCN420B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2AMSCN420C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2AFU1APHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2AFU1APHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2ACT480120	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
2AFU2AMP	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2AOLCN49AB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2AOLCN49BB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2AOLCN49CB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2AQSWS18	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
MV701BCBOE	OE	OPERATOR FAILS TO EN	1.600E-03	---	1.60E-03
MV8701BOE	OE	OPERATOR FAILS TO OP	3.200E-03	---	3.20E-03
1BTPPT403	TP	PRESSURE SENSORS ALL	2.800E-06	2.000E+00	5.60E-06
1BPSPQY403	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
1BCMPB403A	CM	COMPARATOR ALL MODES	2.900E-06	2.000E+00	5.80E-06
1BBIPS403A	BI	BISTABLE HIGH OUTPUT	2.400E-06	2.000E+00	4.80E-06
1BRSPS403	RS	RESISTOR STANDARD QU	4.900E-09	2.000E+00	9.80E-09
1BCNK734	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1BCN33BCRW	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1BCN33BCSU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08

TABLE C-10 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1BCN33BCCH	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1BCNHISOPE	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1BCN420/A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1BCN42C/BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1BRECO420F	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
1BCB52U	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
1BFU40APHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1BFU40APHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1BFU40APHC	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1BOL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1BOL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1BOL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1BMSCN420A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1BMSCN420B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1BMSCN420C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1BFU1APHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1BFU1APHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1BCT480120	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
1BFU2AMP	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1BOLCN49AB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1BOLCN49BB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1BOLCN49CB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08

TABLE C-10 (Cont)

CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1BQSWS18	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
MV702BCBOE	OE	OPERATOR FAILS TO EN	1.600E-03	---	1.60E-03
MV8702BOE	OE	OPERATOR FAILS TO OP	3.200E-03	---	3.20E-03
2BCNK734	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2BCN33BCRW	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2BCN33BCSU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2BCN33BCCH	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2BCNHISOPE	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2BCN42O/A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2BCN42C/BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2BRECO42OF	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
2BCB52U	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
2BFU40APHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2BFU40APHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2BFU40APHC	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2BOL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2BOL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2BOL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2BMSCN420A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2BMSCN420B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2BMSCN420C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2BFU1APHA	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07

TABLE C-10 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2BFU1APHB	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2BCT480120	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
2BFU2AMP	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2BOLCN49AB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2BOLCN49BB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2BOLCN49CB	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2BQSWS1B	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
PMAA	PM	FAILURE TO START	1.000E-05	2.000E+00	2.00E-05
PMAX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	2.000E+00	2.00E-04
PMBA	PM	FAILURE TO START	1.000E-05	2.000E+00	2.00E-05
PMBX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	2.000E+00	2.00E-04
AV618OPOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV618D	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV619OPOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV619D	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV606OPOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV606D	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV607OPOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV607D	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
MV716ACLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MV8716AK	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MV716BCLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03

TABLE C-10 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
MV8716BK	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MV101OPOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MV101D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
MV102OPOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MV102D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
SHORT TERM COOLING					
CV8948AD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV8818AD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
PMAX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	7.200E+01	7.20E-03
2ACNCLOSEQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2ACN42CAQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2AMSCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2AMSCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2AMSCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2ACNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1BIPS405H	BI	BISTABLE HIGH OUTPUT	2.400E-06	7.200E+01	1.73E-04
1CMPB405F	CM	COMPARATOR ALL MODES	2.900E-06	7.200E+01	2.09E-04
1PSPQY405F	PS	LOOP POWER SUPPLY AL	5.800E-06	7.200E+01	4.18E-04
1TPPT405H	TP	PRESSURE SENSORS ALL	2.800E-06	7.200E+01	2.02E-04
1ACNCLOSEQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1ACN42CAQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06

TABLE C-10 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
M1AMSCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1AMSCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1AMSCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1ACNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
MVHV8809AV	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CV8730AD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
HXACCWMVV	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CV8948BD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV8818BD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV8948CD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV8818CD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
PMBX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	7.200E+01	7.20E-03
2BCNCLOSEQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2BCN42CAQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2BMSCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2BMSCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2BMSCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2BCNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2BIPS403H	BI	BISTABLE HIGH OUTPUT	2.400E-06	7.200E+01	1.73E-04
2CMPB403F	CM	COMPARATOR ALL MODES	2.900E-06	7.200E+01	2.09E-04
2PSPQY403F	PS	LOOP POWER SUPPLY AL	5.800E-06	7.200E+01	4.18E-04
2TPPT403H	TP	PRESSURE SENSORS ALL	2.800E-06	7.200E+01	2.02E-04

TABLE C-10 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1BCNCLOSEQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1BCN42CAQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1BMSCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1BMSCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1BMSCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1BCNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
MVHV8809BV	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CV8730BD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
HXBCCWMVV	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CV8948DD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CV8818DD	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
LONG TERM COOLING					
PMAX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	1.008E+03	1.01E-01
2ACNCLOSEQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2ACN42CAQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2AMSCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2AMSCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2AMSCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2ACNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1BIPS405H	BI	BISTABLE HIGH OUTPUT	2.400E-06	1.008E+03	2.42E-03
1CMPB405F	CM	COMPARATOR ALL MODES	2.900E-06	1.008E+03	2.92E-03

TABLE C-10 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1PSPQY405F	PS	LOOP POWER SUPPLY AL	5.800E-06	1.008E+03	5.85E-03
1TPPT405H	TP	PRESSURE SENSORS ALL	2.800E-06	1.008E+03	2.82E-03
1ACNCLOSEQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1ACN42CAQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1AMSCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1AMSCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1AMSCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1ACNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
MVHV8809AV	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
HXACCWMVV	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
CV8948CD	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04
CV8818CD	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04
PMBA	PM	FAILURE TO START	1.000E-05	1.008E+03	1.01E-02
PMBX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	1.008E+03	1.01E-01
PMBTEST	TE	PUMP TEST UNAVAILABI	2.780E-03	---	2.78E-03
PMBMAIN	MA	PUMP MAINTENANCE UNA	1.570E-03	---	1.57E-03
2BCNCLOSEQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2BCN42CAQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2BMSCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2BMSCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2BMSCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05

TABLE C-10 (Cont)

CALLAWAY BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2BCNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2BIPS403H	BI	BISTABLE HIGH OUTPUT	2.400E-06	1.008E+03	2.42E-03
2CMPB403F	CM	COMPARATOR ALL MODES	2.900E-06	1.008E+03	2.92E-03
2PSPQY403F	PS	LOOP POWER SUPPLY AL	5.800E-06	1.008E+03	5.85E-03
2TPPT403H	TP	PRESSURE SENSORS ALL	2.800E-06	1.008E+03	2.82E-03
1BCNCLOSEQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1BCN42CAQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1BMSCNAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1BMSCNBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1BMSCNCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1BCNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
MVHV8809BV	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
CV8730BD	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04
HXBCCWMVV	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
CV8948DD	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04
CV8818DD	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04

TABLE C-11

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Close RHR heat exchanger bypass control valve EJ-FCV-618 and EJ-FCV-619.

REFERENCE: Step 4.2.7.4 of OTN-EJ-00001 Revision 4, "Normal Operating Procedure -Residual Heat Removal System," Section 4.2, "Borating the RHR System Prior to Placing in Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close air operated heat exchanger bypass control valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Second checker or Operating Supervisor fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$P_{OE} = (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16)$$
$$= 5.9775E-04 + 6.0E-04$$
$$= 1.198E-03$$
$$= 1.2E-03$$

Fault Tree Identifiers: AV618CLOE and AV619CLOE

TABLE C-11 (Cont)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Close RHR heat exchanger flow control valve EJ-HCV-606 and EJ-HCV-607.

REFERENCE: Step 4.2.7.2 of OTN-EJ-00001 Revision 4, "Normal Operating Procedure -Residual Heat Removal System," Section 4.2, "Borating the RHR System Prior to Placing in Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close air operated heat exchanger flow control valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error -Second checker or Operating Supervisor fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

P_{OE} = (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16)
= 5.9775E-04 + 6.0E-04
= 1.198E-03
= 1.2E-03

Fault Tree Identifiers: AV606CLOE and AV607CLOE

TABLE C-11 (Cont)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Unlock and close the supply breakers for the RHR system, loop suction valves, EJ-HV-8701A, EJ-HV-8701B, BB-PV-8702A, and BB-PV-8702B.

REFERENCE: Step 4.3.3 in operating procedure OTN-EJ-00001 Residual Heat Removal System Revision 4, Section 4.3, "Placing the RHR System In Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to unlock and close power supply breaker

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator selects wrong circuit breaker

Median HEP = 0.005 Mean HEP = 6.25E-03 Error Factor = 3	Table 20-12	Select wrong circuit breaker in a group of circuit breakers densely grouped and identified by labels only

3. Recovery error -Second checker or Operating Superviser fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-3)(0.00625)(0.16) + 0.00375(0.16) \\
&= 9.96E-04 + 6.0E-04 \\
&= 1.596E-03 \\
&= 1.6E-03
\end{aligned}
$$

Fault Tree Identifiers: MV701ACBOE, MV701BCBOE, MV702ACBOE, and MV702BCBOE

TABLE C-11 (Cont)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Open the CCW inlet valves to the RHR heat exchanger, EG-HV-101 and EG-HV-102.

REFERENCE: Step 4.3.4 of OTN-EJ-00001 Revision 4, "Normal Operating Procedure -Residual Heat Removal System," Section 4.3, "Placing the RHR System In Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open motor operated CCW heat exchanger valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Second checker or Operating Supervisor fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MV101OPOE and MV102OPOE

TABLE C-11 (Cont)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Close RHR pump suction valves from RWST, BN-HV-8812A and BN-HV-8812B.

REFERENCE: Step 4.3.6 of OTN-EJ-00001 Revision 4, "Normal Operating Procedure -Residual Heat Removal System," Section 4.3, "Placing the RHR System in Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated suction from RWST valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error -Second checker or Operating Supervisor fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MV812ACLOE and MV812BCLOE

TABLE C-11 (Cont)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Open the RHR loop inlet isolation valves, EJ-HV-8701A, EJ-HV-8701B, BB-PV-8702A, and BB-PV-8702B.

REFERENCE: Step 4.3.7 of OTN-EJ-00001 Revision 4, "Normal Operating Procedure -Residual Heat Removal System," Section 4.3, "Placing the RHR System in Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open motor operated suction valve using two-position switch

Median HEP	= 0.003	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used
Mean HEP	= 3.75E-03		
Error Factor	= 3		

2. Commission error - Operator fails to turn control to open valve

Median HEP	= 0.01	Table 20-12	Turn two position switch in wrong direction when design violates a strong populational stereotype and operating conditions are normal by labels only
Mean HEP	= 1.61E-02		
Error Factor	= 5		

3. Recovery error -Shift supervisor fails to detect error by others

Median HEP	= 0.1	Table 20-22	Checking routine tasks, checker using written materials
Mean HEP	= 0.16		
Error Factor	= 5		

P_{OE} = (1-3.75E-03)(0.016)(0.16) + 0.00375(0.16)
= 2.556E-03 + 6.0E-04
= 3.166E-03
= 3.2E-03

Fault Tree Identifiers: MV8701AOE, MV8701BOE, MV8702AOE, and MV8702BOE

TABLE C-11 (Cont)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Close EJ-HV-8716A and EJ-HV-8716B.

REFERENCE: Step 4.3.15 of OTN-EJ-00001 Revision 4, "Normal Operating Procedure -Residual Heat Removal System," Section 4.3, "Placing the RHR System in Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated crosstie to RCS hot leg valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error -Second checker or Operating Supervisor fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MV716ACLOE and MV716BCLOE

TABLE C-11 (Cont)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Slowly open RHR heat exchanger bypass valve EJ-HCV-618 and EJ-FCV-619.

REFERENCE: Step 4.3.16 of OTN-EJ-00001 Revision 4, "Normal Operating Procedure -Residual Heat Removal System," Section 4.3, "Placing the RHR System in Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open air operated heat exchanger bypass control valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Second checker or Operating Supervisor fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: AV618OPOE and AV619OPOE

TABLE C-11 (Cont)

CALLAWAY
HUMAN ERROR CALCULATIONS

TASK: Open RHR heat exchanger flow control valve EH-HCV-606 and EJ-HCV-607.

REFERENCE: Step 4.3.18 of OTN-EJ-00001 Revision 4, "Normal Operating Procedure -Residual Heat Removal System," Section 4.3, "Placing the RHR System in Service for Normal Cooldown."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open air operated heat exchanger flow control valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error -Second checker or Operating Supervisor fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: AV606OPOE and AV607OPOE

TABLE C-12

CALLAWAY
DOMINANT CONTRIBUTORS
RHR INITIATION

MEAN PROBABILITY OF FAILURE = 3.62E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	3.20E-03	OPERATOR FAILS TO OPEN RHR SUCTION VALVE 8702B
2.	3.20E-03	OPERATOR FAILS TO OPEN RHR SUCTION VALVE 8701B
3.	3.20E-03	OPERATOR FAILS TO OPEN RHR SUCTION VALVE 8702A
4.	3.20E-03	OPERATOR FAILS TO OPEN RHR SUCTION VALVE 8701A
5.	1.60E-03	OPERATOR FAILS TO UNLOCK AND ENERGIZE CIRCUIT BREAKER 8702B
6.	1.60E-03	OPERATOR FAILS TO UNLOCK AND ENERGIZE CIRCUIT BREAKER 8701B
7.	1.60E-03	OPERATOR FAILS TO UNLOCK AND ENERGIZE CIRCUIT BREAKER 8702A
8.	1.60E-03	OPERATOR FAILS TO UNLOCK AND ENERGIZE CIRCUIT BREAKER 8701A
9.	1.20E-03	CCW TO RHR HX VALVE EG-HV-102 FAILS TO OPEN OPERATOR ERROR
10.	1.20E-03	CCW TO RHR HX VALVE EG-HV-101 FAILS TO OPEN OPERATOR ERROR
11.	1.20E-03	RHR CROSSTIE VALVE HV-8716B FAILS TO CLOSE OPERATOR ERROR
12.	1.20E-03	RHR CROSSTIE VALVE HV-8716A FAILS TO CLOSE OPERATOR ERROR
13.	1.20E-03	RHR HX FLOW VALVE EJ-HCV-607 FAILS TO OPEN OPERATOR ERROR
14.	1.20E-03	RHR HX FLOW VALVE EJ-HCV-606 FAILS TO OPEN OPERATOR ERROR
15.	1.20E-03	RHR HX BYPASS VALVE EJ-FCV-619 FAILS TO OPEN OPERATOR ERROR
16.	1.20E-03	RHR HX BYPASS VALVE EJ-FCV-618 FAILS TO OPEN OPERATOR ERROR
17.	1.20E-03	RHR SUCTION VALV FROM RWST 8812B FAILS TO CLOSE OPERATOR ERROR
18.	1.20E-03	RHR SUCTION VALV FROM RWST 8812A FAILS TO CLOSE OPERATOR ERROR
19.	1.20E-03	RHR HX FLOW VALVE EJ-HCV-607 FAILS TO CLOSE OPERATOR ERROR
20.	1.20E-03	RHR HX FLOW VALVE EJ-HCV-606 FAILS TO CLOSE OPERATOR ERROR

TABLE C-13

CALLAWAY
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.64E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	7.20E-03	RHR PUMP B FAILS TO RUN FOR 72 HOURS
2.	7.20E-03	RHR PUMP A FAILS TO RUN FOR 72 HOURS
3.	4.18E-04	LOOP POWER SUPPLY PQY-403 FAILS
4.	4.18E-04	LOOP POWER SUPPLY PQY-405 FAILS
5.	2.09E-04	DUAL COMPARATOR PB-403A/B FAILS
6.	2.09E-04	DUAL COMPARATOR PB-405A/B FAILS
7.	2.02E-04	PRESSURE TRANSMITTER PT-403 FAILS HIGH
8.	2.02E-04	PRESSURE TRANSMITTER PT-405 FAILS HIGH
9.	1.73E-04	BISTABLE SWITCH PS-403B FAILS HIGH
10.	1.73E-04	BISTABLE SWITCH PS-405B FAILS HIGH
11.	1.44E-05	HEAT EXCHANGER B FAILS TO REMOVE HEAT (CCW VALVE SPURIOUSLY CLOS)
12.	1.44E-05	CHECK VALVE 8730B FAILS TO OPEN
13.	1.44E-05	MOV HV8809B SPURIOUSLY CLOSES
14.	1.44E-05	HEAT EXCHANGER A FAILS TO REMOVE HEAT (CCW VALVE SPURIOUSLY CLOS)
15.	1.44E-05	CHECK VALVE 8730A FAILS TO OPEN
16.	1.44E-05	MOV HV8809A SPURIOUSLY CLOSES
17.	1.44E-06	CONTACT 42C/A SHORTS HV8701B
18.	1.44E-06	HIS/CLOSE CONTACT SHORTS HV8701B
19.	1.44E-06	CONTACT K735 SHORTS HV8701B
20.	1.44E-06	CONTRACT 42C/A SHORTS PV8702B

TABLE C-14

CALLAWAY
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.44E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	7.20E-03	RHR PUMP B FAILS TO RUN FOR 72 HOURS
2.	7.20E-03	RHR PUMP A FAILS TO RUN FOR 72 HOURS
3.	1.44E-05	HEAT EXCHANGER B FAILS TO REMOVE HEAT (CCW VALVE SPURIOUSLY CLOS)
4.	1.44E-05	CHECK VALVE 8730B FAILS TO OPEN
5.	1.44E-05	MOV HV8809B SPURIOUSLY CLOSES
6.	1.44E-05	HEAT EXCHANGER A FAILS TO REMOVE HEAT (CCW VALVE SPURIOUSLY CLOS)
7.	1.44E-05	CHECK VALVE 8730A FAILS TO OPEN
8.	1.44E-05	MOV HV8809A SPURIOUSLY CLOSES
9.	1.44E-06	CONTACT 42C/A SHORTS HV8701B
10.	1.44E-06	HIS/CLOSE CONTACT SHORTS HV8701B
11.	1.44E-06	CONTACT 42C/A SHORTS PV8702B
12.	1.44E-06	HIS/CLOSE CONTRACT SHORTS PV8702B
13.	1.44E-06	CONTACT 42C/A SHORTS HV8701A
14.	1.44E-06	HIS/CLOSE CONTACT SHORTS HV8701A
15.	1.44E-06	CONTACT 42C/A SHORTS PV8702A
16.	1.44E-06	HIS/CLOSE CONTACT SHORTS PV8702A
17.	2.07E-10	DISCHARGE CHECK VALVE 8818C FAILS TO OPEN DISCHARGE CHECK VALVE 8818D FAILS TO OPEN
18.	2.07E-10	DISCHARGE CHECK VALVE 8818C FAILS TO OPEN DISCHARGE CHECK VALVE 8948D FAILS TO OPEN

TABLE C-14 (Cont)

CALLAWAY
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.44E-02

	PROBABILITY	CUTSET DESCRIPTION
19.	2.07E-10	DISCHARGE CHECK VALVE 8948C FAILS TO OPEN DISCHARGE CHECK VALVE 8818D FAILS TO OPEN
20.	2.07E-10	DISCHARGE CHECK VALVE 8948C FAILS TO OPEN DISCHARGE CHECK VALVE 8948D FAILS TO OPEN

TABLE C-15

CALLAWAY
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 3.91E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.02E-02	RHR PUMP A FAILS TO RUN FOR SIX WEEKS RHR PUMP B FAILS TO RUN FOR SIX WEEKS
2.	5.85E-03	LOOP POWER SUPPLY PQY-405 FAILS
3.	5.85E-03	LOOP POWER SUPPLY PQY-403 FAILS
4.	2.92E-03	DUAL COMPARATOR PB-405A/B FAILS
5.	2.92E-03	DUAL COMPARATOR PB-403A/B FAILS
6.	2.82E-03	PRESSURE TRANSMITTER PT-405 FAILS HIGH
7.	2.82E-03	PRESSURE TRANSMITTER PT-403 FAILS HIGH
8.	2.42E-03	BISTABLE SWITCH PS-405B FAILS HIGH
9.	2.42E-03	BISTABLE SWITCH PS-403B FAILS HIGH
10.	1.02E-03	RHR PUMP A FAILS TO RUN FOR SIX WEEKS RHR PUMP B FAILS TO START
11.	2.81E-04	RHR PUMP A FAILS TO RUN FOR SIX WEEKS RHR PUMP B UNAVAILABLE DUE TO TEST
12.	1.59E-04	RHR PUMP A FAILS TO RUN FOR SIX WEEKS RHR PUMP B UNAVAILABLE DUE TO MAINTENANCE
13.	2.04E-05	HEAT EXCHANGER A FAILS TO REMOVE HEAT (CCW VALVE SPURIOUSLY CLOS) RHR PUMP B FAILS TO RUN FOR SIX WEEKS
14.	2.04E-05	MOV HV8809A SPURIOUSLY CLOSES RHR PUMP B FAILS TO RUN FOR SIX WEEKS
15.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS HEAT EXCHANGER B FAILS TO REMOVE HEAT (CCW VALVE SPURIOUSLY CLOS)

TABLE C-15 (Cont)

CALLAWAY
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 3.91E-02

	PROBABILITY	CUTSET DESCRIPTION
16.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS CHECK VALVE 8730B FAILS TO OPEN
17.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS MOV HV88809B SPURIOUSLY CLOSES
18.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS DISCHARGE CHECK VALVE 8818D FAILS TO OPEN
19.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS DISCHARGE CHECK VALVE 8948D FAILS TO OPEN
20.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS DISCHARGE CHECK VALVE 8818C FAILS TO OPEN

TABLE C-16

CALLAWAY
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.17E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.02E-02	RHR PUMP A FAILS TO RUN FOR SIX WEEKS RHR PUMP B FAILS TO RUN FOR SIX WEEKS
2.	1.02E-03	RHR PUMP A FAILS TO RUN FOR SIX WEEKS RHR PUMP B FAILS TO START
3.	2.81E-04	RHR PUMP A FAILS TO RUN FOR SIX WEEKS RHR PUMP B UNAVAILABLE DUE TO TEST
4.	1.59E-04	RHR PUMP A FAILS TO RUN FOR SIX WEEKS RHR PUMP B UNAVAILABLE DUE TO TEST
5.	2.04E-05	HEAT EXCHANGER A FAILS TO REMOVE HEAT (CCW VALVE SPURIOUSLY) RHR PUMP B FAILS TO RUN FOR SIX WEEKS
6.	2.04E-05	MOV HV8809A SPURIOUSLY CLOSES RHR PUMP B FAILS TO RUN FOR SIX WEEKS
7.	2.04E-05	RHR PUMP A FIALS TO RUN FOR SIX WEEKS HEAT EXCHANGER B FAIL TO REMOVE HEAT (CCW VALVE SPURIOUSLY)
8.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS CHECK VALVE 8730B FAILS TO OPEN
9.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS MOV HV8809B SPURIOUSLY CLOSES
10.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS DISCHARGE CHECK VALVE 8818D FAILS TO OPEN
11.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS DISCHARGE CHECK VALVE 8948D FAILS TO RUN
12.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS DISCHARGE CHECK VALVE 8818C FAILS TO OPEN
13.	2.04E-05	RHR PUMP A FAILS TO RUN FOR SIX WEEKS DISCHARGE CHECK VALVE 8948C FAILS TO OPEN
14.	2.04E-06	HEAT EXCHANGER A FAILS TO REMOVE HEAT (CCW VALVE SPURIOUSLY CLOSE) RHR PUMP B FAILS TO START

TABLE C-16 (Cont)

CALLAWAY
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.17E-02

	PROBABILITY	CUTSET DESCRIPTION
15.	2.04E-06	MOV HV8809A SPURIOUSLY CLOSES RHR PUMP B FAILS TO START
16.	2.04E-06	RHR PUMP A FAILS TO RUN FOR SIX WEEKS CONTACT 42C/A SHORTS HV8701B
17.	2.04E-06	RHR PUMP A FAILS TO RUN FOR SIX WEEKS HIS/CLOSE CONTACT SHORTS HV8701B
18.	2.04E-06	RHR PUMP A FAILS TO R RUN FOR SIX WEEKS CONTACT 42C/A SHORTS PV8702B
19.	2.04E-06	RHR PUMP A FAILS TO RUN FOR SIX WEEKS HIS/CLOSE CONTACT SHORTS PV8702B
20.	2.04E-06	CONTACT 42C/A SHORTS HV8701A RHR PUMP B FAILS TO RUN FOR SIX WEEKS

OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 5

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH

C.3.3 NORTH ANNA

Three fault trees were developed to model the RHR system unavailability for North Anna. These fault trees were developed from the system flow diagrams and control wiring diagrams shown and described in Section 5.3 for North Anna. Each fault tree is discussed below. The RHR suction valves MOV 1700 and MOV 1701 were modeled in detail down to the control circuitry level to explicitly show the change in unavailability due to removal of the autoclosure interlock.

<u>Failure during RHR Initiation</u>

The fault tree developed for this phase of cooldown (Figure C-11) details the failure during initiation of the RHR system. The fault tree was developed based on the RHR system Operating Procedure 1-OP-14.0/14.1, Revision 19, Section 4.1, "Placing RHR System in Operation." The steps for RHR initiation are summarized below:

1. Start Residual Heat Removal pumps 1-RH-P-1A and/or 1B to warm up the RHR System.

2. Unlock and energize the breakers for MOV-1700 and 1701.

3. Open MOV-1700. Open MOV-1701.

4. Open MOV-CC-100A and/or MOV-CC-100B (RHR heat exchangers component cooling water return valves).

5. Place RHR heat exchanger bypass valve (FCV-1605) in "Manual" and close FCV-1605.

6. Close HCV-1758.

7. Energize RHR isolation valves to the Safety Injection System MOV-1720A and MOV-1720B.

8. Open MOV-1720A and MOV-1720B.

9. Open FCV-1605.

10. Open HCV-1758.

Each of these steps was modeled in the fault tree to involve an operator error or a component failure. For example, the fourth step requires the opening of a CCW valve to the RHR heat exchanger. Failure of this step could involve: 1) the operator failing to open the valve or 2) the valve failing to open. This phase of cooldown is not dependent on the autoclosure interlock but on the prevent-open interlock. Thus only one fault tree was developed.

Loss of Short Term Cooling

The fault tree developed for this phase of cooldown (Figure C-12 with ACI and C-13 without ACI) requires that both trains of RHR be in operation. Injection into two of three cold legs for 72 hours is required for success in this phase. The RHR suction valves were modeled in detail to show how the valves could spuriously close.

Loss of Long Term Cooling

For this phase of plant cooldown, only one RHR train (pump and heat exchanger) are required to be operating for a period of six weeks. Injection into two of three cold legs is the success criteria. The fault tree developed for the case with the ACI is shown in Figure C-14, while the fault tree without ACI is shown in Figure C-15.

The fault trees were quantified for the case with and without the autoclosure interlock. The basic event probabilities (component unavailabilities and human error probabilities) are shown in Table C-18. The equation used to calculate the component unavailability is :

$$Q = (\lambda)\ T_M$$

where

Q = component failure probability

(λ) = failure rate for component

T_M = total defined mission time in which the component must operate.

The human error probability calculations for North Anna are shown in Table C-19.

The unavailability of the Train B pump due to test is based on the Technical Specification 3.4.1.3 which states: "All Reactor Coolant pumps and residual heat removal pumps may be de-energized for up to 1 hour ..." Assuming that pump testing occurs on a monthly basis (every 720 hours), the unavailability due to test is calculated by:

$$Q_{test} = (T)/T_T$$

where T = average duration of test (hours)

T_T = interval between tests (hours)

For North Anna, the test unavailability is:

$$\begin{aligned} Q_{test} &= (T)/T_T \\ &= (1 \text{ hours}) / (720 \text{ hours}) \\ &= 1.39E-03 \end{aligned}$$

The unavailability due to maintenance was extracted from Reference 20, "Individual Plant Evaluation Methodology for Pressurized Water Reactors," April 1987, Section 2.4, Table 2.4-2 Generic Maintenance Durations for a standby pump tested monthly or quarterly and a component inoperability time limit of 72 hours. Therefore the unavailability due to maintenance is:

$$\begin{aligned} Q_{main} &= (f_r)\ (T)_R \\ &= (8.42E-05 \text{ events/hour})\ (18.7 \text{ hours/ event}) \\ &= 1.57E-03 \end{aligned}$$

where f_r = frequency of maintenance (events/hour)
$(T)_R$ = mean component repair time (hours/event)

Results

The results of the RHR system unavailability are shown in Table C-17. The dominant cutsets for each phase are shown in Tables C-20 to C-24.

For the failure of initiation fault tree, the dominant failure mode is operator error. The operator failing to energize the circuit breakers to suction valves MOV 1700 and MOV 1701 and the injection isolation valves MOV 1720A and MOV 1720B are the major cutsets. The deletion of the autoclosure interlock has no impact on the failure probability for RHRS initiation.

The failure probability of the short term cooling phase for North Anna is reduced by 12 percent with the deletion of the ACI. The dominant failure mode for each fault tree (with and without the autoclosure interlock) is the failure of either pump to run for 72 hours (both pumps are required for success in this phase). For the case with the autoclosure interlock, failure of components associated with the ACI contribute approximately 2.0E-03 to the failure probability.

In the long term cooling phase for North Anna, the failure of both pumps to run for six weeks is the dominant contributor to the unavailability. For the case with the ACI present, the other cutsets involve the single failure of a component associated with the ACI such as the power supply, signal comparator, bistable switch or pressure transmitter which causes spurious closure of one of the RHR suction valves. The deletion of the ACI for this phase of cooldown reduces the unavailability by 66 percent.

The results of the quantification of the North Anna RHR unavailability fault trees show a trend that the autoclosure interlock becomes more of a determining and detrimental factor as the length of time in which the RHRS is required to operate increases. The deletion of the autoclosure interlock reduces the number of spurious closure of the RHR suction valves and thus increases the availability of the RHRS.

TABLE C-17
NORTH ANNA
RHR UNAVAILABILITY RESULTS

FAULT TREE PHASE	WITH AUTOCLOSURE	WITHOUT AUTOCLOSURE	PERCENT CHANGE
INITIATION	1.90E-02	1.90E-02	0
SHORT TERM COOLING	1.65E-02	1.46E-02	-12
LONG TERM COOLING	4.14E-02	1.39E-02	-66

TABLE C-18

NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
RHR INITIATION					
PM1AA	PM	FAILURE TO START	1.000E-05	2.000E+00	2.00E-05
PM1AX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	2.000E+00	2.00E-04
PM1BA	PM	FAILURE TO START	1.000E-05	2.000E+00	2.00E-05
PM1BX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	2.000E+00	2.00E-04
CVRH15D	CV	FAILURE TO OPEN	2.000E-07	2.000E+00	4.00E-07
CVRH7D	CV	FAILURE TO OPEN	2.000E-07	2.000E+00	4.00E-07
MV1700CBOE	OE	OPERATOR FAILS TO EN	1.600E-03	---	1.60E-03
MV17000E	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
OL49AF	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
OL49CF	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
MSCN520A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
MSCN520B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
MSCN520C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
CT480/120V	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
FU6AMP1	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
FU6AMP2	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
OLCN40U	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
LS4U	LS	LIMIT SWITCH ALL MOD	7.220E-06	2.000E+00	1.44E-05
QSTS18U	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
CN52CU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08

TABLE C-18 (Cont)
NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
RECO520F	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
CN520K	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
SWK	SW	PUSH BUTTON SWITCH A	1.220E-06	2.000E+00	2.44E-06
PT1403F	TP	PRESSURE SENSORS ALL	2.800E-06	2.000E+00	5.60E-06
RSPS1403	RS	RESISTOR STANDARD QU	4.900E-09	2.000E+00	9.80E-09
PSPQ1403	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
CMPC1403	CM	COMPARATOR ALL MODES	2.900E-06	2.000E+00	5.80E-06
BIPS14031	BI	BISTABLE HIGH OUTPUT	2.400E-06	2.000E+00	4.80E-06
RECO14031X	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
RECN14031X	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
MV1701CBOE	OE	OPERATOR FAILS TO EN	1.600E-03	---	1.60E-03
MV1701OE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
1CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
1OL49AF	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1OL49CF	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1MSCN520A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1MSCN520B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1MSCN520C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
1FU6AMP1	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1FU6AMP2	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07

TABLE C-18 (Cont)

NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1OLCN49U	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1LS4U	LS	LIMIT SWITCH ALL MOD	7.220E-06	2.000E+00	1.44E-05
1QSTS18U	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
1CN52CU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1RECO52OF	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
1CN52OK	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1SWK	SW	PUSH BUTTON SWITCH A	1.220E-06	2.000E+00	2.44E-06
PT1402F	TP	PRESSURE SENSORS ALL	2.800E-06	2.000E+00	5.60E-06
RSPS1402	RS	RESISTOR STANDARD QU	4.900E-09	2.000E+00	9.80E-09
PSPQ1402	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
CMPC1402	CM	COMPARATOR ALL MODES	2.900E-06	2.000E+00	5.80E-06
BIPS14021	BI	BISTABLE HIGH OUTPUT	2.400E-06	2.000E+00	4.80E-06
RECO14021X	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
RECN14021X	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
AV1605CLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV1605K	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV1758CLOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV1758K	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
MV1720AOEC	OE	OPERATOR FAILS TO EN	1.600E-03	---	1.60E-03
MV1720AOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MV1720AD	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
MV1720BOEC	OE	OPERATOR FAILS TO EN	1.600E-03	---	1.60E-03

TABLE C-18 (Cont)

NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
MV1720BOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MV1720BD	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
AV1605OPOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV1605D	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AV1758OPOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AV1758D	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
MVCC100AOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVCC100AD	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
MVCC100BOE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVCC100BD	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
SHORT TERM COOLING					
CVX2D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
MV1720AV	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
HXRH1ACCV	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
PM1AX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	7.200E+01	7.20E-03
1MSCN52CAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1MSCN52CBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1MSCN52CCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
1CN52CQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1PBSWF	SW	PUSH BUTTON SWITCH A	1.220E-06	7.200E+01	8.78E-05
CNPC1403Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
RECOPC1403	RE	RELAY ALL FAILURE MO	8.700E-08	7.200E+01	6.26E-06

TABLE C-18 (Cont)
NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
BIPS14032H	BI	BISTABLE HIGH OUTPUT	2.400E-06	7.200E+01	1.73E-04
CMPC1403F	CM	COMPARATOR ALL MODES	2.900E-06	7.200E+01	2.09E-04
PSPQ1403F	PS	LOOP POWER SUPPLY AL	5.800E-06	7.200E+01	4.18E-04
TPPT1403F	TP	PRESSURE SENSORS ALL	2.800E-06	7.200E+01	2.02E-04
2MSCN52CAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2MSCN52CBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2MSCN52CCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
2CN52CQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
2PBSWF	SW	PUSH BUTTON SWITCH A	1.220E-06	7.200E+01	8.78E-05
CNPC1405Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
RECOPC1405	RE	RELAY ALL FAILURE MO	8.700E-08	7.200E+01	6.26E-06
BIPS14052H	BI	BISTABLE HIGH OUTPUT	2.400E-06	7.200E+01	1.73E-04
CMPC1405F	CM	COMPARATOR ALL MODES	2.900E-06	7.200E+01	2.09E-04
PSPQ1405F	PS	LOOP POWER SUPPLY AL	5.800E-06	7.200E+01	4.18E-04
TPPT1405F	TP	PRESSURE SENSORS ALL	2.800E-06	7.200E+01	2.02E-04
PM1BX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	7.200E+01	7.20E-03
HX1BCCV	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CVX3D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
MV1720BQ	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
LONG TERM COOLING					
MV1720AV	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
HX1ACCV	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04

TABLE C-18 (Cont)

NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
PM1AX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	1.008E+03	1.01E-01
1MSCN52CAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1MSCN52CBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1MSCN52CCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
1CN52CQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1PBSWF	SW	PUSH BUTTON SWITCH A	1.220E-06	1.008E+03	1.23E-03
CNPC1403Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
RECOPC1403	RE	RELAY ALL FAILURE MO	8.700E-08	1.008E+03	8.77E-05
BIPS14032H	BI	BISTABLE HIGH OUTPUT	2.400E-06	1.008E+03	2.42E-03
CMPC1403F	CM	COMPARATOR ALL MODES	2.900E-06	1.008E+03	2.92E-03
PSPQ1403F	PS	LOOP POWER SUPPLY AL	5.800E-06	1.008E+03	5.85E-03
TPPT1403F	TP	PRESSURE SENSORS ALL	2.800E-06	1.008E+03	2.82E-03
2MSCN52CAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2MSCN52CBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2MSCN52CCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
2CN52CQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
2PBSWF	SW	PUSH BUTTON SWITCH A	1.220E-06	1.008E+03	1.23E-03
CNPC1405Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
RECOPC1405	RE	RELAY ALL FAILURE MO	8.700E-08	1.008E+03	8.77E-05
BIPS14052H	BI	BISTABLE HIGH OUTPUT	2.400E-06	1.008E+03	2.42E-03
CMPC1405F	CM	COMPARATOR ALL MODES	2.900E-06	1.008E+03	2.92E-03

TABLE C-18 (Cont)
NORTH ANNA BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
PSPQ1405F	PS	LOOP POWER SUPPLY AL	5.800E-06	1.008E+03	5.85E-03
TPPT1405F	TP	PRESSURE SENSORS ALL	2.800E-06	1.008E+03	2.82E-03
CVRH7D	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04
PM1BA	PM	FAILURE TO START	1.000E-05	1.008E+03	1.01E-02
PM1BX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	1.008E+03	1.01E-01
PM1BTEST	TE	PUMP TEST UNAVAILABI	1.390E-03	---	1.39E-03
PM1BMAIN	MA	PUMP MAINTENANCE UNA	1.570E-03	---	1.57E-03
HX1BCCV	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
MV1720BV	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04

TABLE C-19

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Open MOV--CC-100A and/or MOV-CC-100B (RHR heat exchanger component cooling return valves).

REFERENCE: Step 4.1.17 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, "Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open motor operated CCW heat exchanger valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MVCC100AOE and MVCC100BOE

TABLE C-19 (Cont)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Place RHR heat exchanger bypass valve (FCV-1605) in "Manual" and close FCV-1605.

REFERENCE: Step 4.1.19 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, "Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close air operated heat exchanger bypass flow control valve

Median HEP	= 0.003	Table 20-7	Long list > 10 items
Mean HEP	= 3.75E-03		When procedures with checkoff
Error Factor	= 3		provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP	= 0.003	Table 20-12	Select wrong control on a panel
Mean HEP	= 3.75E-03		from an array of similar-
Error Factor	= 3		appearing controls identified
			by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP	= 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP	= 0.16		using written materials
Error Factor	= 5		

$$P_{OE} = (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16)$$
$$= 5.9775E-04 + 6.0E-04$$
$$= 1.198E-03$$
$$= 1.2E-03$$

Fault Tree Identifiers: AV1605CLOE

TABLE C-19 (Cont)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Close HCV-1758 (Heat exchanger outlet flow control valve).

REFERENCE: Step 4.1.20 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, "Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close air operated heat exchanger outlet flow control valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: AV1758CLOE

TABLE C-19 (Cont)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Energize RHR isolation valves to the Safety Injection System MOV-1720A and MOV-1720B.

REFERENCE: Step 4.1.21 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, "Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to energize power supply breaker to motor operated valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator selects wrong circuit breaker

Median HEP = 0.005 Mean HEP = 6.25E-03 Error Factor = 3	Table 20-12	Select wrong circuit breaker in a group of circuit breakers densely grouped and identified by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-3)(0.00625)(0.16) + 0.00375(0.16) \\
&= 9.96E-04 + 6.0E-04 \\
&= 1.596E-03 \\
&= 1.6E-03
\end{aligned}
$$

Fault Tree Identifiers: MV1720AOEC and MV1720BOEC

TABLE C-19 (Cont)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Open RHR isolation valves to the Safety Injection System MOV-1720A and MOV-1720B.

REFERENCE: Step 4.1.22 and 4.1.23 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, 'Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open motor operated Safety Injection isolation valve

Median HEP	= 0.003	Table 20-7	Long list > 10 items
Mean HEP	= 3.75E-03		When procedures with checkoff
Error Factor	= 3		provisions are correctly used

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP	= 0.003	Table 20-12	Select wrong control on a panel
Mean HEP	= 3.75E-03		from an array of similar-
Error Factor	= 3		appearing controls identified
			by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP	= 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP	= 0.16		using written materials
Error Factor	= 5		

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MV1720AOE and MV1720BOE

TABLE C-19 (Cont)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Open heat exchanger bypass valve (FCV-1605).

REFERENCE: Step 4.1.24 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, "Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open air operated heat exchanger bypass flow control valve

Median HEP	= 0.003	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used
Mean HEP	= 3.75E-03		
Error Factor	= 3		

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP	= 0.003	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only
Mean HEP	= 3.75E-03		
Error Factor	= 3		

3. Recovery error - Verifier fails to detect error by others

Median HEP	= 0.1	Table 20-22	Checking routine tasks, checker using written materials
Mean HEP	= 0.16		
Error Factor	= 5		

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: AV1605OPOE

TABLE C-19 (Cont)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Open HCV-1758 (Heat exchanger outlet flow control valve).

REFERENCE: Step 4.1.28 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, "Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open air operated heat exchanger outlet flow control valve

Median HEP	= 0.003	Table 20-7	Long list > 10 items
Mean HEP	= 3.75E-03		When procedures with checkoff
Error Factor	= 3		provisions are correctly used

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP	= 0.003	Table 20-12	Select wrong control on a panel
Mean HEP	= 3.75E-03		from an array of similar-
Error Factor	= 3		appearing controls identified by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP	= 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP	= 0.16		using written materials
Error Factor	= 5		

P_{OE} = (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16)
= 5.9775E-04 + 6.0E-04
= 1.198E-03
= 1.2E-03

Fault Tree Identifiers: AV1758OPOE

TABLE C-19 (Cont)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Open MOV-1700 and MOV-1700.

REFERENCE: Step 4.1.13 and 4.1.14 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, "Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open motor operated suction valve using push-button switch

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to push button to open valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MV1700OE and MV1701OE

TABLE C-19 (Cont)

NORTH ANNA
HUMAN ERROR CALCULATIONS

TASK: Unlock and energize the breakers for MOV-1700 and MOV-1701.

REFERENCE: Step 4.1.11 of 1-OP-14.0/14.1 Revision 19, "Residual Heat Removal System," Section 4.1, "Placing RHR System in Operation."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to energize power supply breaker to motor operated valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator selects wrong circuit breaker

Median HEP = 0.005 Mean HEP = 6.25E-03 Error Factor = 3	Table 20-12	Select wrong circuit breaker in a group of circuit breakers densely grouped and identified by labels only

3. Recovery error - Verifier fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-3)(0.00625)(0.16) + 0.00375(0.16) \\
&= 9.96E-04 + 6.0E-04 \\
&= 1.596E-03 \\
&= 1.6E-03
\end{aligned}
$$

Fault Tree Identifiers: MV1700CBOE and MV1701CBOE

TABLE C-20

NORTH ANNA
DOMINANT CONTRIBUTORS
RHR INITIATION

MEAN PROBABILITY OF FAILURE = 1.90E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.60E-03	OPERATOR FAILS TO ENERGIZE CB TO MOV 1720B
2.	1.60E-03	OPERATOR FAILS TO ENERGIZE CB TO MOV 1720A
3.	1.60E-03	OPERATOR FAILS TO RACK IN CB TO MOV 1701
4.	1.60E-03	OPERATOR FAILS TO RACK IN CB TO MOV 1700
5.	1.20E-03	CCW TO RHR HX MOV-CC-100B FAILS TO OPEN OPERATOR ERROR
6.	1.20E-03	CCW TO RHR HX MOV-CC-100A FAILS TO OPEN OPERATOR ERROR
7.	1.20E-03	HX OUTLET VALVE HCV-1758 FAILS TO OPEN OPERATOR ERROR
8.	1.20E-03	HX BYPASS VALVE FCV-1605 FAILS TO OPEN OPERATOR ERROR
9.	1.20E-03	OPERATOR FAILS TO OPEN MOV 1720B
10.	1.20E-03	OPERATOR FAILS TO OPEN MOV 1720A
11.	1.20E-03	HX OUTLET VALVE HCV-1758 FAILS TO CLOSE OPERATOR ERROR
12.	1.20E-03	HX BYPASS VALVE FCV-1605 FAILS TO CLOSE OEPRATOR ERROR
13.	1.20E-03	OPERATOR FAILS TO OPEN MOV 1701
14.	1.20E-03	OPERATOR FAILS TO OPEN MOV 1700
15.	2.00E-04	RHR PUMP 1-RH-P-1B FAILS TO RUN FOR ONE HOUR
16.	2.00E-04	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR ONE HOUR
17.	2.00E-05	CCW TO RHR HX MOV-CC-100B FAILS TO OPEN
18.	2.00E-05	CCW TO RHR HX MOV-CC-100A FAILS TO OPEN
19.	2.00E-05	HX OUTLET VALVE HCV-1758 FAILS TO OPEN
20.	2.00E-05	HX BYPASS VALVE FCV-1605 FAILS TO OPEN

TABLE C-21

NORTH ANNA
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.65E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	7.20E-03	RHR PUMP 1-RH-P-1B FAILS TO RUN FOR 72 HOURS
2.	7.20E-03	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR 72 HOURS
3.	4.18E-04	LOOP POWER SUPPLY PQ-1405 FAILS
4.	4.18E-04	LOOP POWER SUPPLY PQ-1403 FAILS
5.	2.09E-04	SIGNAL COMPARATOR PC-1405 FAILS
6.	2.09E-04	SIGNAL COMPARATOR PC-1403 FAILS
7.	2.02E-04	PRESSURE TRANSMITTER PT-1405 FAILS
8.	2.02E-04	PRESSURE TRANSMITTER PT-1403 FAILS
9.	1.73E-04	BISTABLE SWITCH PS/1405-2 FAILS
10.	1.73E-04	BISTABLE SWITCH PS/1403-2 FAILS
11.	8.78E-05	PUSHBUTTON SWITCH FAILS MOV1701
12.	8.78E-05	PUSHBUTTON SWITCH FAILS MOV1700
13.	1.44E-05	HEAT EXCHANGER 1-RH-E-1B FAILS TO REMOVE HEAT
14.	1.44E-05	HEAT EXCHANGER 1-RH-E-1A FAILS TO REMOVE HEAT
15.	6.26E-06	RELAY COIL PC-1405-2X FAILS
16.	6.26E-06	RELAY COIL PC-1403-2X FAILS
17.	1.44E-06	CONTACT 52C SHORTS MOV1701
18.	1.44E-06	AUTOCLOSURE INTERLOCK CONTACT PC1405-X SHORTS
19.	1.44E-06	CONTACT 52C SHORTS MOV1700
20.	1.44E-06	AUTOCLOSURE INTERLOCK CONTACT PC1403-X SHORTS

TABLE C-22

NORTH ANNA
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.46E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	7.20E-03	RHR PUMP 1-RH-P-1B FAILS TO RUN FOR 72 HOURS
2.	7.20E-03	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR 72 HOURS
3.	8.78E-05	PUSHBUTTON SWITCH FAILS MOV1701
4.	8.78E-05	PUSHBUTTON SWITCH FAILS MOV1700
5.	1.44E-05	HEAT EXCHANGER 1-RH-E-1B FAILS TO REMOVE HEAT
6.	1.44E-05	HEAT EXCHANGER 1-RH-E-1A FAILS TO REMOVE HEAT
7.	1.44E-06	CONTACT 52C SHORTS MOV1701
8.	1.44E-06	CONTACT 52C SHORTS MOV1700
9.	2.07E-10	MOTOR OPERATED VALVE MOV-1720A SPURIOUSLY CLOSES MOTOR OPERATED VALVE MOV-1720B SPURIOUSLY CLOSES
10.	2.07E-10	MOTOR OPERATED VALVE MOV-1720A SPURIOUSLY CLOSES CHECK VALVE 1SI-161 FAILS TO OPEN
11.	2.07E-10	CHECK VALVE 1SI-144 FAILS TO OPEN MOTOR OPERATED VALVE MOV-1720B SPURIOUSLY CLOSES
12.	2.07E-10	CHECK VALVE 1SI-161 FAILS TO OPEN CHECK VALVE 1SI-144 FAILS TO OPEN

TABLE C-23

NORTH ANNA
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 4.14E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.02E-02	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS RHR PUMP 1-RH-P-1B FAILS TO RUN FOR SIX WEEKS
2.	5.85E-03	LOOP POWER SUPPLY PQ-1405 FAILS
3.	5.85E-03	LOOP POWER SUPPLY PQ-1403 FAILS
4.	2.92E-03	SIGNAL COMPARATOR PC-1405 FAILS
5.	2.92E-03	SINGLE COMPARATOR PC-1403 FAILS
6.	2.82E-03	PRESSURE TRANSMITTER PT-1405 FAILS
7.	2.82E-03	PRESSURE TRANSMITTER PT-1403 FAILS
8.	2.42E-03	BISTABLE SWITCH PS/1405-2 FAILS
9.	2.42E-03	BISTABLE SWITCH PS/1403-2 FAILS
10.	1.23E-03	PUSHBOTTON SWTICH FAILS MOV1701
11.	1.23E-03	PUSHBUTTON SWITCH FAILS MOV1700
12.	1.02E-03	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS RHR PUMP 1-RH-P-1B FAILS TO START
13.	1.59E-04	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS PUMP 1-RH-P-1B UNAVAILABLE DUE TO MAINTENANCE
14.	1.40E-04	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS PUMP 1-RH-P-1B UNAVAILABLE DUE TO TEST
15.	8.77E-05	RELAY COIL PC-1405-2X FAILS
16.	8.77E-05	RELAY COIL PC-1403-2X FAILS
17.	2.04E-05	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS CHECK VALVE 1RH-7 FAILS TO OPEN
18.	2.02E-05	CONTACT 52C SHORTS MOV1701
19.	2.02E-05	AUTOCLOSURE INTERLOCK CONTACT PC1405-X SHORTS
20.	2.02E-05	CONTACT 52C SHORTS MOV1700

TABLE C-24

NORTH ANNA
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.39E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.02E-02	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS RHR PUMP 1-RH-P-1B FAILS TO RUN FOR SIX WEEKS
2.	1.23E-03	PUSHBUTTON SWITCH FAILS MOV1701
3.	1.23E-03	PUSHBUTTON SWITCH FAILS MOV1700
4.	1.02E-03	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS RHR PUMP 1-RH-P-1B FAILS TO START
5.	1.59E-04	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS PUMP 1-RH-P-1B UNAVAILABLE DUE TO MAINTENANCE
6.	1.40E-04	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS PUMP 1-RH-P-1B UNAVAILABLE DUE TO TEST
7.	2.04E-05	RHR PUMP 1-RH-P-1A FAILS TO RUN FOR SIX WEEKS CHECK VALVE 1RH-7 FAILS TO OPEN
8.	2.02E-05	CONTACT 52C SHORTS MOV1701
9.	2.02E-05	CONTACT 52C SHORTS MOV1700
10.	4.08E-08	LOOP 2 HEADER MOV 1720A SPURIOUSLY CLOSES LOOP 3 HEADER MOVE 1720B SPURIOUSLY CLOSES
11.	4.08E-08	HEAT EXCHANGER 1RH-3-1A FAILS TO REMOVE HEAT HEAT EXCHANGER 1-RH-E-1B FAILS TO REMOVE HEAT

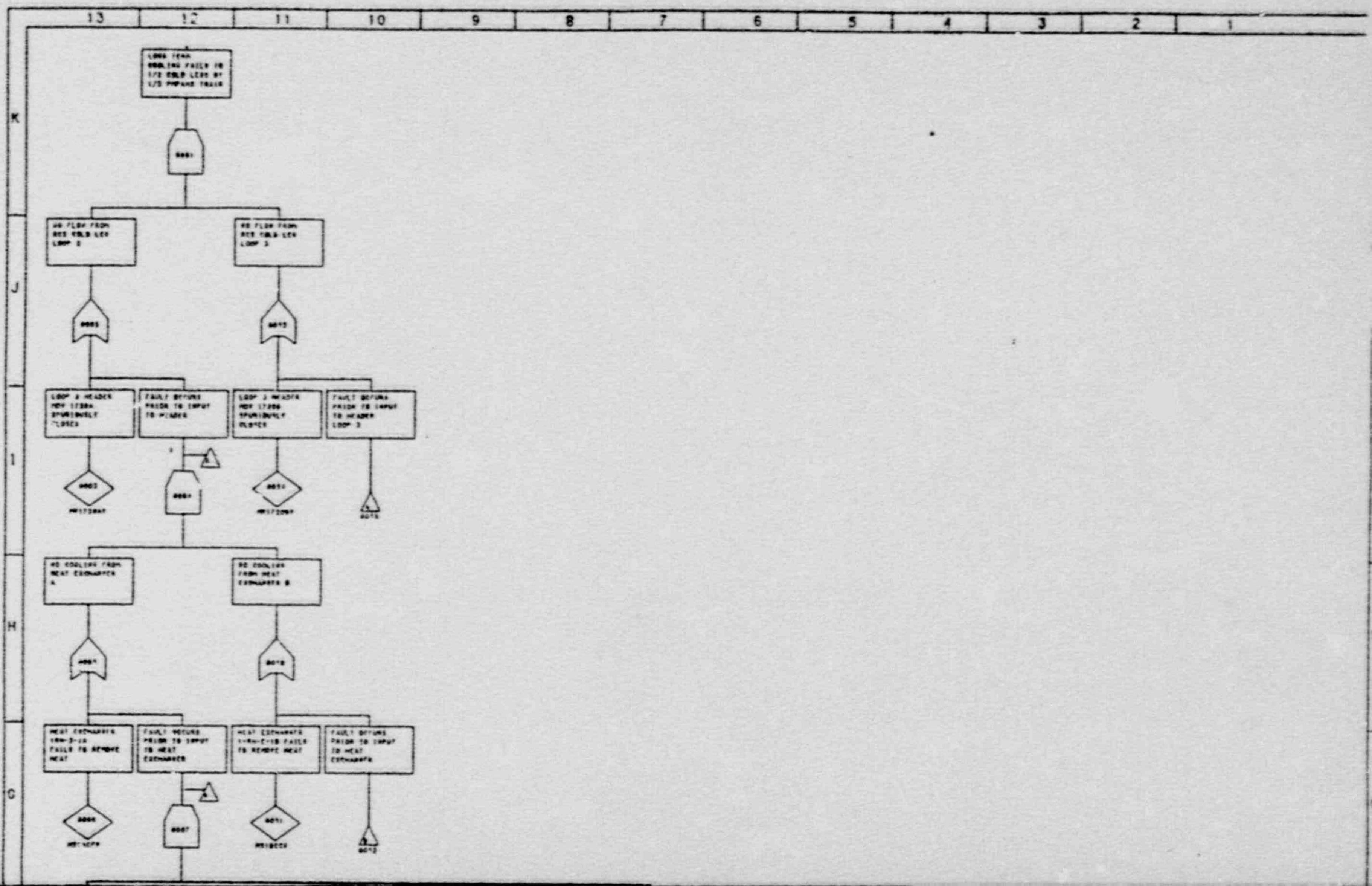
OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 3

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH



13
12
11
10
9
8
7
6
5
4
3
2
1
K
J
I
H
G
LONG TERM COOLING FAILS TO COLD LEGS BY PUMPING TRAIN
NO FLOW FROM RCS COLD LEG
NO FLOW FROM RCS COLD LEG LOOP 3
LOOP HEADER SPURIOUSLY CLOSES
FAULT OCCURS PRIOR TO INPUT TO HEADER
LOOP HEADER SPURIOUSLY CLOSES
FAULT OCCURS PRIOR TO INPUT TO HEADER LOOP 3
NO COOLING FROM HEAT EXCHANGER A
NO COOLING FROM HEAT EXCHANGER B
HEAT EXCHANGER FAILS TO REMOVE HEAT
FAULT OCCURS PRIOR TO INPUT TO HEAT EXCHANGER
HEAT EXCHANGER FAILS TO REMOVE HEAT
FAULT OCCURS PRIOR TO INPUT TO HEAT EXCHANGER

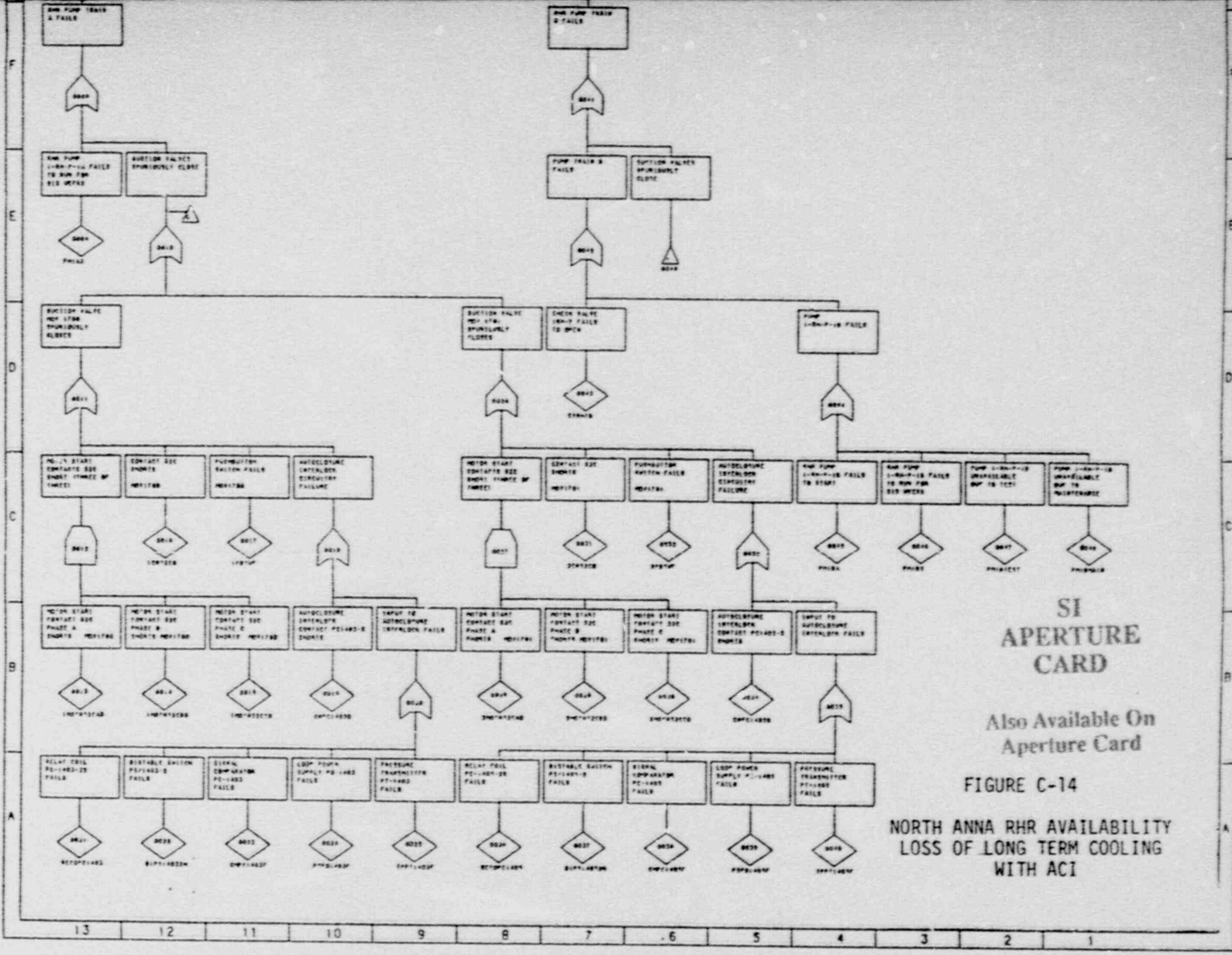
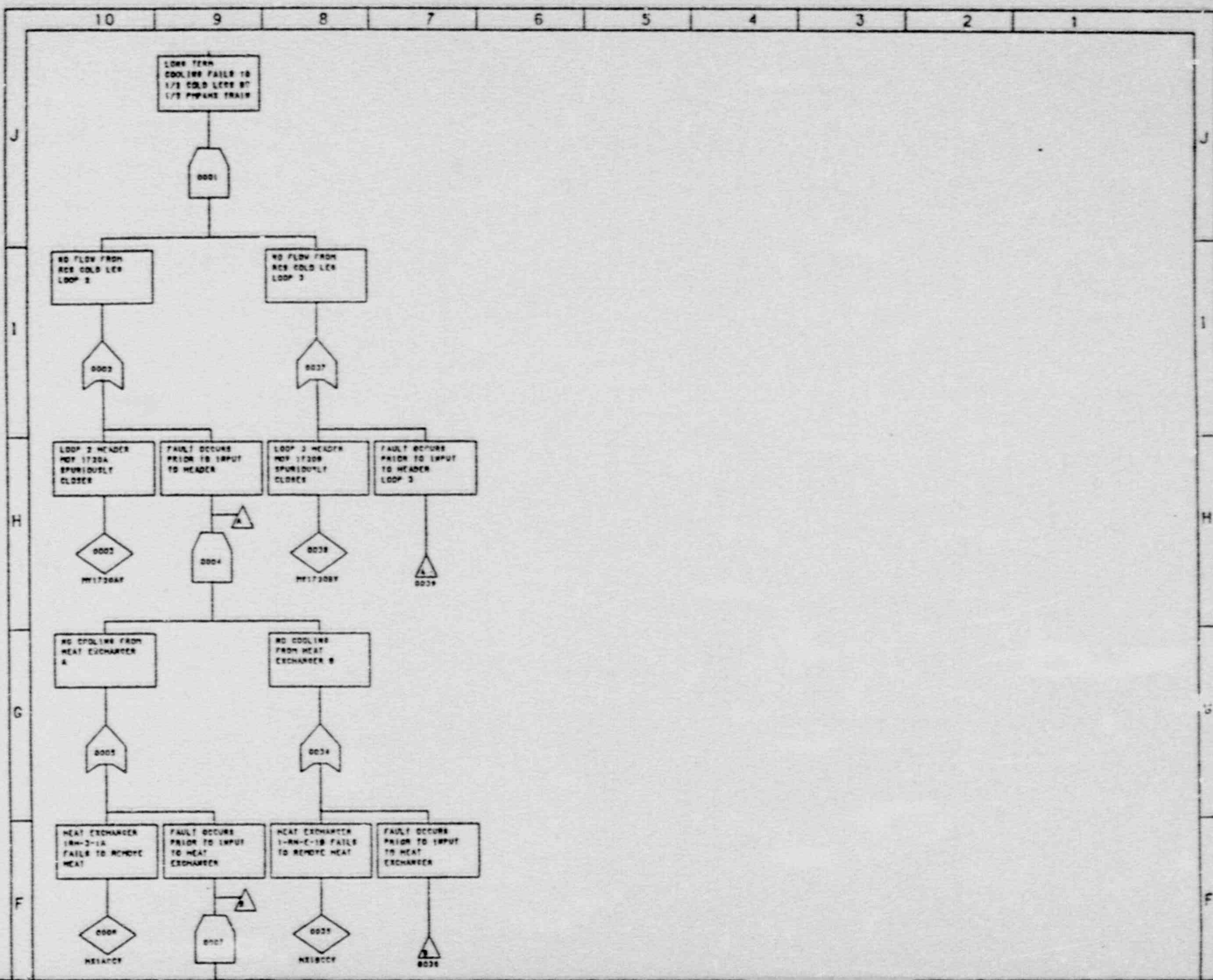


FIGURE C-14

NORTH ANNA RHR AVAILABILITY
LOSS OF LONG TERM COOLING
WITH ACI


LONG TERM COOLING FAILS TO 1/3 COLD LEGS BY 1/2 PUMPING TRAIN
0001
NO FLOW FROM RCS COLD LEG LOOP 2
NO FLOW FROM RCS COLD LEG LOOP 3
0002
0037
LOOP 2 HEADER MOV 1720A SPURIOUSLY CLOSES
FAULT OCCURS PRIOR TO INPUT TO HEADER
LOOP 3 HEADER MOV 1720B SPURIOUSLY CLOSES
FAULT OCCURS PRIOR TO INPUT TO HEADER LOOP 3
0003
0004
0038
0039
NO COOLING FROM HEAT EXCHANGER A
NO COOLING FROM HEAT EXCHANGER B
0005
0034
HEAT EXCHANGER 1RH-3-1A FAILS TO REMOVE HEAT
FAULT OCCURS PRIOR TO INPUT TO HEAT EXCHANGER
HEAT EXCHANGER 1-RH-E-1B FAILS TO REMOVE HEAT
FAULT OCCURS PRIOR TO INPUT TO HEAT EXCHANGER
0006
0007
0035
0036

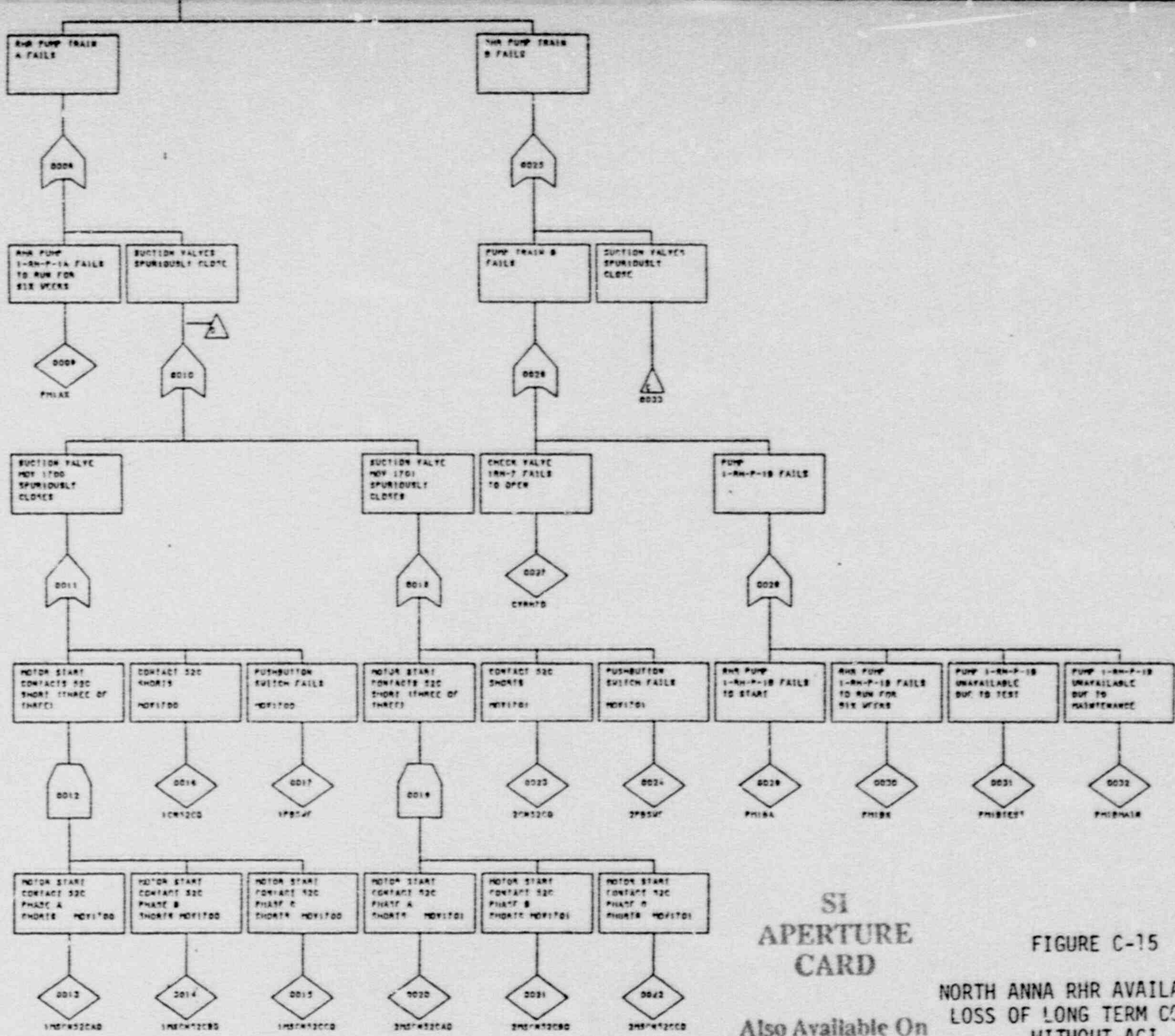


FIGURE C-15

NORTH ANNA RHR AVAILABILITY
LOSS OF LONG TERM COOLING
WITHOUT ACI

C.3.4 SHEARON HARRIS

Three fault trees were developed to model the RHR system unavailability for Shearon Harris. These fault trees were developed from the system flow diagrams and control wiring diagrams shown and described in Section 5.4 for Shearon Harris. Each fault tree is discussed below. The RHR suction valves 1RH1, 1RH2, 1RH39 and 1RH40 were modeled in detail down to the control circuitry level to explicitly show the change in unavailability due to removal of the autoclosure interlock.

Failure during RHR Initiation

The fault tree developed for this phase of cooldown (Figure C-16) details the failure during initiation of the RHR system. The fault tree was developed based on the RHR System Operating Procedure OP-111, Revision 2, Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown." The steps for RHR initiation are summarized below (Train B components are listed in parentheses):

1. Open CCW valves 1CC-147 (1CC-167) from RHR heat exchanger to establish CCW flow through heat exchanger.
2. Close RHR heat exchanger outlet flow control valve 1RH30 (1RH66).
3. Open RHR heat exchanger bypass flow control 1RH20 (1RH58).
4. Close RWST to RHR pump 1SI-322 (1SI-323).
5. Close low head SI train to cold legs, 1SI-340 (1SI-341).
6. Close low head SI to hot leg crossover, 1SI-326 (1SI-327).
7. Open RHR suction valves 1RH1 and 1RH2 (1RH39 and 1RH40).
8. Start RHR pump A-SA (B-SB).
9. Open low head SI train to cold legs, 1SI-340 (1SI-341).

Each of these steps was modeled in the fault tree to involve an operator error or a component failure. For example, the first step requires the opening of a CCW valve to the RHR heat exchanger. Failure of this step could involve: 1) the operator failing to open the valve or 2) the valve failing to open.

This phase of cooldown is not dependent on the autoclosure interlock but on the prevent-open interlock. Thus only one fault tree was developed to determine the unavailablity due to RHR initiation.

Loss of Short Term Cooling

The fault tree developed for this phase of cooldown (Figure C-17 with ACI and C-18 without ACI) requires that both trains of RHR be in operation. Injection into two of three cold legs for 72 hours is required for success in this phase. The RHR suction valves are modeled in detail to show how the valves could spuriously close. With the autoclosure interlock present, a spurious pressure signal could cause the suction valves to spuriously close. With the autoclosure signal removed from the circuit, the valves are less likely to spuriously close.

Loss of Long Term Cooling

For this phase of plant cooldown, only one RHR train (pump and heat exchanger) are required to be operating for a period of six weeks. Injection into two of three cold legs is the success criteria. The fault tree developed for the case with the ACI is shown in Figure C-19, the fault tree without ACI is shown in Figure C-20.

The fault trees were quantified for the case with and without the autoclosure interlock. The basic event probabilities (component unavailabilities and human error probabilities) are shown in Table C-26. The equation used to calculate the component unavailability is :

$$Q = (\lambda)\, T_M$$

where

Q = component failure probability

(λ) = failure rate for component

T_M = total defined mission time in which the component must operate.

The human error probability calculations for Shearon Harris are shown in Table C-27.

The unavailability of the Train B pump due to test is based on the Technical Specification 3.4.1.4.1 which states: "One RHR loop may be inoperable for up to 2 hours for surveillance testing probided the other RHR loop is OPERABLE and in operation." Assuming that pump testing occurs on a monthly basis (every 720 hours), the unavailability due to test is calculated by:

$$Q_{test} = (T)/T_T$$

where T = average duration of test (hours)
T_T = interval between tests (hours)

For Shearon Harris, the test unavailability is:

$$Q_{test} = (T)/T_T$$
$$= (2 \text{ hours}) / (720 \text{ hours})$$
$$= 2.78E\text{-}03$$

The unavailability due to maintenance was extracted from Reference 20, "Individual Plant Evaluation Methodology for Pressurized Water Reactors," April 1987, Section 2.4, Table 2.4-2 Generic Maintenance Durations for a standby pump tested monthly or quarterly and a component inoperability time limit of 72 hours. Therefore the unavailability due to maintenance is:

$$Q_{main} = (f_r)\ (T)_R$$
$$= (8.42E\text{-}05 \text{ events/hour})\ (18.7 \text{ hours/ event})$$
$$= 1.57E\text{-}03$$

where f_r = frequency of maintenance (events/hour)
$(T)_R$ = mean component repair time (hours/event)

RESULTS

The results of the quantification are shown in Table C-25. The major cutsets for each fault tree are shown in Tables C-28 to C-32.

For the failure of initiation fault tree, the dominant failure mode is operator error. The operator failing to open all four suction valves 1RH1, 1RH2, 1RH39, and 1RH40 are the major cutsets. The deletion of the autoclosure interlock has no impact on the failure probability for RHRS initiation.

The failure probability of the short term cooling phase for Shearon Harris is reduced by 10 percent with the delection of the ACI. The dominant failure mode for each fault tree (with and without the autoclosure interlock) is the failure of either pump to run for 72 hours (both pumps are required for success in this phase). For the case with the autoclosure interlock, failure of components associated with the ACI contribute approximately 1.7E-03 to the failure probability.

In the long term cooling phase for Shearon Harris, the failure of both pumps to run for six weeks is the dominant contributor to the unavailability. For the case with the ACI present, the other cutsets involve the failure of a component associated with the ACI such as the power supply, signal comparator or pressure transmitter which causes spurious closure of one of the RHR suction valves. The deletion of the ACI for this phase of cooldown reduces the unavailability by 66 percent.

The results of the quantification of the Shearon Harris RHR unavailability fault trees show a trend that the autoclosure interlock becomes more of a determining and detrimental factor as the length of time in which the RHRS is required to operate increases. The deletion of the autoclosure interlock reduces the number of spurious closures of the RHR suction valves and thus increases the availability of the RHRS.

TABLE C-25
RESULTS OF RHR UNAVAILABILITY
FOR SHEARON HARRIS

FAULT TREE PHASE	WITH AUTOCLOSURE	WITHOUT AUTOCLOSURE	PERCENT CHANGE
INITIATION	3.74E-02	3.74E-02	0
SHORT TERM COOLING	1.61E-02	1.45E-02	-10
LONG TERM COOLING	3.45E-02	1.16E-02	-66

TABLE C-26

SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
RHR INITIATION					
AVRH30OE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AVRH30K	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AVRH66OE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
AVRH66K	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AVRH20OE	OE	OPERATOR FAIL TO PLA	1.800E-03	---	1.80E-03
AVRH20D	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
AVRH58OE	OE	OPERATOR FAIL TO PLA	1.800E-03	---	1.80E-03
AVRH58D	AO	FAILURE TO OPERATE	1.000E-05	2.000E+00	2.00E-05
MVSI322OE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVSI322K	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MVSI323OE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVSI323K	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MVSI340OEK	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVSI340K	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MVSI341OEK	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVSI341K	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MVSI326OE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVSI326K	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
MVSI327OE	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVSI327K	MV	FAILURE TO CLOSE	1.000E-05	2.000E+00	2.00E-05
1RHCBOE	OE	OPERATOR FAILS TO CL	1.500E-03	---	1.60E-03

TABLE C-26 (Cont)

SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1RHOEOPEN	OE	OPERATOR FAILS TO OP	3.200E-03	---	3.20E-03
1CN1A11A2K	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1CN420LOCK	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1CN8706BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1CN8809BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
1CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
1OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
1RECN420A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1RECN420B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1RECN420C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1QSTOU	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
1CN42SU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1RECO420F	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
1CNCR1A	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1FU1	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
1CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1OLCN48MR2	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08

TABLE C-26 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
1CNK734	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
1PS118VAC	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
REPY402A1	RE	RELAY ALL FAILURE MO	8.700E-08	2.000E+00	1.74E-07
CMPB402	CM	COMPARATOR ALL MODES	2.900E-06	2.000E+00	5.80E-06
ISEEPV402C	EE	ISOLATOR E-E CONVERT	4.800E-07	2.000E+00	9.60E-07
PSPGY402	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
RSPS402B	RS	RESISTOR STANDARD QU	4.900E-09	2.000E+00	9.80E-09
TPPT402	TP	PRESSURE SENSORS ALL	2.800E-06	2.000E+00	5.60E-06
2RHCBOE	OE	OPERATOR FAILS TO CL	1.600E-03	---	1.60E-03
2RHOEOPEN	OE	OPERATOR FAILS TO OP	3.200E-03	---	3.20E-03
2CN1A11A2K	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2CN420LOCK	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2CN8706BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2CN8809BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
2CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
2OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
2RECN420A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06

TABLE C-26 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2RECN420B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2RECN420C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
2QSTOU	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
2CN42SU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2RECO420F	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
2CNCR1A	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2FU1	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
2CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2OLCN48MR2	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
2CNK734	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
9RHCBOE	OE	OPERATOR FAILS TO CL	1.600E-03	---	1.60E-03
9RHOEOPEN	OE	OPERATOR FAILS TO OP	3.200E-03	---	3.20E-03
9CN1A11A2K	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
9CN420LOCK	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
9CN8706BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
9CN8809BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
9CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
9CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
9OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07

TABLE C-26 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
9OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
9OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
9RECN420A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
9RECN420B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
9RECN420C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
9QSTOU	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
9CN42SU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
9RECO420F	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
9CNCR1A	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
9FU1	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
9CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
9OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
9OLCN48MR2	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
9OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
9CNK734	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
9PS118VAC	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
REPY405A1	RE	RELAY ALL FAILURE MO	8.700E-08	2.000E+00	1.74E-07
CMPB405	CM	COMPARATOR ALL MODES	2.900E-06	2.000E+00	5.80E-06
ISEEPV405C	EE	ISOLATOR E-E CONVERT	4.800E-07	2.000E+00	9.60E-07
PSPGY405	PS	LOOP POWER SUPPLY AL	5.800E-06	2.000E+00	1.16E-05
RSPS405B	RS	RESISTOR STANDARD QU	4.900E-09	2.000E+00	9.80E-09
TPPT405	TP	PRESSURE SENSORS ALL	2.800E-06	2.000E+00	5.60E-06

TABLE C-26 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
4RHCBOE	OE	OPERATOR FAILS TO CL	1.600E-03	---	1.60E-03
4RHOEOPEN	OE	OPERATOR FAILS TO OP	3.200E-03	---	3.20E-03
4CN1A11A2K	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
4CN420LOCK	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
4CN8706BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
4CN8809BU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
4CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	2.000E+00	2.00E-08
4CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	2.000E+00	7.00E-07
4OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
4OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
4OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	2.000E+00	3.00E-07
4RECN420A	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
4RECN420B	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
4RECN420C	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
4QSTOU	QS	TORQUE SWITCH FAIL T	2.000E-07	2.000E+00	4.00E-07
4CN42SU	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
4RECO420F	CO	RELAY COIL FAILURE	3.000E-06	2.000E+00	6.00E-06
4CNCR1A	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
4FU1	FU	FUSE ALL MODES	1.500E-07	2.000E+00	3.00E-07
4CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
4OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08

TABLE C-26 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
4OLCN48MR2	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
4OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	2.000E+00	4.00E-08
4CNK734	CN	RELAY CONTACTS FAIL	1.000E-06	2.000E+00	2.00E-06
PM1ASAA	PM	FAILURE TO START	1.000E-05	2.000E+00	2.00E-05
PM1ASAX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	2.000E+00	2.00E-04
PM1BSBA	PM	FAILURE TO START	1.000E-05	2.000E+00	2.00E-05
PM1BSBX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	2.000E+00	2.00E-04
MVSI340OED	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVSI340D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
MVSI341OED	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVSI341D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
MVCC147OED	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVCC147D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
MVCC167OED	OE	OPERATOR FAILS TO OP	1.200E-03	---	1.20E-03
MVCC167D	MV	FAILURE TO OPEN	1.000E-05	2.000E+00	2.00E-05
SHORT TERM COOLING					
CVSI83D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CVSI358D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CVSI347D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
MVSI341V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CVRH70D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
HX1BSBF	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05

TABLE C-26 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
PM1BSBX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	7.200E+01	7.20E-03
R39CN42SAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
R39CN42SBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
R39CN42SCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
R39CN42SQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
R39CN2B1Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
R39CNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
9REPY402A2	RE	RELAY ALL FAILURE MO	8.700E-08	7.200E+01	6.26E-06
9CMPB402	CM	COMPARATOR ALL MODES	2.900E-06	7.200E+01	2.09E-04
9PSPGY402	PS	LOOP POWER SUPPLY AL	5.800E-06	7.200E+01	4.18E-04
9TPPT402	TP	PRESSURE SENSORS ALL	2.800E-06	7.200E+01	2.02E-04
R40CN42SAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
R40CN42SBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
R40CN42SCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
R40CN42SQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
R40CN2B1Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
R40CNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
CVSI82D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CVSI357D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CVSI181D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
CVSI356D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05

TABLE C-26 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
CVSI346D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
MVSI340V	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
CVSI34D	CV	FAILURE TO OPEN	2.000E-07	7.200E+01	1.44E-05
HX1ASAF	MV	FAILURE TO REMAIN OP	2.000E-07	7.200E+01	1.44E-05
PM1ASAX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	7.200E+01	7.20E-03
RH1CN42SAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
RH1CN42SBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
RH1CN42SCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
RH1CN42SQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
RH1CN2B1Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
RH1CNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
1REPY402A2	RE	RELAY ALL FAILURE MO	8.700E-08	7.200E+01	6.26E-06
1CMPB402	CM	COMPARATOR ALL MODES	2.900E-06	7.200E+01	2.09E-04
1PSPGY402	PS	LOOP POWER SUPPLY AL	5.800E-06	7.200E+01	4.18E-04
1TPPT402	TP	PRESSURE SENSORS ALL	2.800E-06	7.200E+01	2.02E-04
RH2CN42SAQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
RH2CN42SBQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
RH2CN42SCQ	CN	MOTOR STARTER SPURIO	3.000E-08	7.200E+01	2.16E-06
RH2CN42SQ	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
RH2CN2B1Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06
RH2CNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	7.200E+01	1.44E-06

TABLE C-26 (Cont)

SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
LONG TERM COOLING					
CVRH347D	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04
MVSI341V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
CVRH70D	CV	FAILURE TO OPEN	2.000E-07	1.008E+03	2.02E-04
HX1BSBF	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
PM1BSBA	PM	FAILURE TO START	1.000E-05	1.008E+03	1.01E-02
PM1BSBX	PM	FAIL TO RUN,GIVEN ST	1.000E-04	1.008E+03	1.01E-01
PM1BSBTST	TE	PUMP TEST UNAVAILABI	2.780E-03	---	2.78E-03
PM1BSBMAIN	MA	PUMP MAINTENANCE UNA	1.570E-03	---	1.57E-03
R39CN42SAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
R39CN42SBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
R39CN42SCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
R39CN42SQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
R39CN2B1Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
R39CNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
9REPY402A2	RE	RELAY ALL FAILURE MO	8.700E-08	1.008E+03	8.77E-05
9CMPB402	CM	COMPARATOR ALL MODES	2.900E-06	1.008E+03	2.92E-03
9PSPGY402	PS	LOOP POWER SUPPLY AL	5.800E-06	1.008E+03	5.85E-03
9TPPT402	TP	PRESSURE SENSORS ALL	2.800E-06	1.008E+03	2.82E-03
R40CN42SAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
R40CN42SBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
R40CN42SCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05

TABLE C-26 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
R40CN42SQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
R40CN2B1Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
R40CNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
MVSI340V	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
HX1ASAF	MV	FAILURE TO REMAIN OP	2.000E-07	1.008E+03	2.02E-04
PM1ASA	PM	FAIL TO RUN,GIVEN ST	1.000E-04	1.008E+03	1.01E-01
RH1CN42SAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
RH1CN42SBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
RH1CN42SCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
RH1CN42SQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
RH1CN2B1Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
RH1CNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
1REPY402A2	RE	RELAY ALL FAILURE MO	8.700E-08	1.008E+03	8.77E-05
1CMPB402	CM	COMPARATOR ALL MODES	2.900E-06	1.008E+03	2.92E-03
1PSPGY402	PS	LOOP POWER SUPPLY AL	5.800E-06	1.008E+03	5.85E-03
1TPPT402	TP	PRESSURE SENSORS ALL	2.800E-06	1.008E+03	2.82E-03
RH2CN42SAQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
RH2CN42SBQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
RH2CN42SCQ	CN	MOTOR STARTER SPURIO	3.000E-08	1.008E+03	3.02E-05
RH2CN42SQ	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
RH2CN2B1Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05
RH2CNK735Q	CN	RELAY CONTACTORS SPU	2.000E-08	1.008E+03	2.02E-05

TABLE C-27

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Open CCW from Heat exchanger A-SA (B-SB) 1CC-147 (1CC-167) to establish CCW flow through heat exchanger.

REFERENCE: Step 2 of OP-111 Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open motor operated CCW heat exchanger valve

Median HEP = 0.003	Table 20-7	Long list > 10 items
Mean HEP = 3.75E-03		When procedures with checkoff
Error Factor = 3		provisions are correctly used

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP = 0.003	Table 20-12	Select wrong control on a panel
Mean HEP = 3.75E-03		from an array of similar-
Error Factor = 3		appearing controls identified
		by labels only

3. Recovery error - Shift foreman fails to detect error by others

Median HEP = 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP = 0.16		using written materials
Error Factor = 5		

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MVCC147OE and MVCC167OE

TABLE C-27 (Cont)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Close RHR Heat exchanger A (B) outlet flow control 1RH-30 (1RH-66).

REFERENCE: Step 3 of OP-111 Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close air operated heat exchanger outlet flow control valve

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Shift foreman fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: AVRH30OE and AVRH66OE

TABLE C-27 (Cont)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Place in manual and open RHR Heat exchanger A(B) bypass flow control FCV-605A(B), 1RH-20 (1RH-58).

REFERENCE: Step 4 of OP-111 Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open air operated heat exchanger bypass flow control valve

   Median HEP = 0.003 Table 20-7 Long list > 10 items
   Mean HEP = 3.75E-03 When procedures with checkoff
   Error Factor = 3 provisions are correctly used

2. Commission error - Operator fails to place valve in manual by selecting wrong control

   Median HEP = 0.003 Table 20-12 Select wrong control on a panel
   Mean HEP = 3.75E-03 from an array of similar-
   Error Factor = 3 appearing controls identified by labels only

3. Commission error - Operator fails to open valve by selecting wrong control

   Median HEP = 0.003 Table 20-12 Select wrong control on a panel
   Mean HEP = 3.75E-03 from an array of similar-
   Error Factor = 3 appearing controls identified by labels only

4. Recovery error - Shift foreman fails to detect error by others

   Median HEP = 0.1 Table 20-22 Checking routine tasks, checker
   Mean HEP = 0.16 using written materials
   Error Factor = 5

P_{OE} = 3.75E-03(0.16) + (1-3.75E-03)(3.75E-03)(0.16) + (1-3.75E-03)^2 (3.75E-05)(0.16)
= 6.0E-04 + 5.98E-04 + 5.96E-04
= 1.794E-03
= 1.8E-03

Fault Tree Identifiers: AVRH20OE and AVRH58OE

TABLE C-27 (Cont)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Close RWST to RHR pump A-SA (B-SB), 1SI-322 (1SI-323).

REFERENCE: Step 5 of OP-111 Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated valve from RWST

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Shift foreman fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MVSI322OE and MVSI323OE

TABLE C-27 (Cont)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Close Low Head SI Train A(B) to Cold Legs, 1SI-340 (1SI-341).

REFERENCE: Step 7 of OP-111 Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated valve to cold legs

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error - Shift foreman fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E-04 + 6.0E-04 \\
&= 1.198E-03 \\
&= 1.2E-03
\end{aligned}
$$

Fault Tree Identifiers: MVSI340OEK and MVSI341OEK

TABLE C-27 (Cont)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Close Low Head SI Train A(B) to Hot Leg Crossover, 1SI-326 (1SI-327).

REFERENCE: Step 8 of OP-111 Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to close motor operated valve to hot leg crossover

Median HEP	= 0.003	Table 20-7	Long list > 10 items
Mean HEP	= 3.75E-03		When procedures with checkoff
Error Factor	= 3		provisions are correctly used

2. Commission error - Operator fails to close valve by selecting wrong control

Median HEP	= 0.003	Table 20-12	Select wrong control on a panel
Mean HEP	= 3.75E-03		from an array of similar-appearing controls identified
Error Factor	=3		by labels only

3. Recovery error - Shift foreman fails to detect error by others

Median HEP	= 0.1	Table 20-22	Checking routine tasks, checker
Mean HEP	= 0.16		using written materials
Error Factor	= 5		

$$
\begin{aligned}
P_{OE} &= (1-3.75E\text{-}03)(0.00375)(0.16) + 0.00375(0.16) \\
&= 5.9775E\text{-}04 + 6.0E\text{-}04 \\
&= 1.198E\text{-}03 \\
&= 1.2E\text{-}03
\end{aligned}
$$

Fault Tree Identifiers: MVSI326OE and MVSI327OE

TABLE C-27 (Cont)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Unlock and close the supply breakers to 1RH1 (1RH39) and 1RH2 (1RH40).

REFERENCE: Step 13 of OP-111 Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to unlock and close power supply breaker

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator selects wrong circuit breaker

Median HEP = 0.005 Mean HEP = 6.25E-03 Error Factor = 3	Table 20-12	Select wrong circuit breaker in a group of circuit breakers densely grouped and identified by labels only

3. Recovery error -Foreman fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

P_{OE} = (1-3.75E-3)(0.00625)(0.16) + 0.00375(0.16)
= 9.96E-04 + 6.0E-04
= 1.596E-03
= 1.6E-03

Fault Tree Identifiers: 1RHCBOE

TABLE C-27 (Cont)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Open RCS Loop A(C) to RHR pump A-SA(B-SB) 1RH-1 and 1RH-2 (1RH-39 and 1RH-40). Complete Attachment II checklist.

REFERENCE: Step 14 of OP-111 Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open motor operated suction valve using two-position switch

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to turn control to open valve

Median HEP = 0.01 Mean HEP = 1.61E-02 Error Factor = 5	Table 20-12	Turn two position switch in wrong direction when design violates a strong populational stereotype and operating conditions are normal by labels only

3. Recovery error - Shift foreman fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

$$
\begin{aligned}
P_{OE} &= (1-3.75E-03)(0.016)(0.16) + 0.00375(0.16) \\
&= 2.556E-03 + 6.0E-04 \\
&= 3.166E-03 \\
&= 3.2E-03
\end{aligned}
$$

Fault Tree Identifiers: 1RHOEOPEN and 2RHOEOPEN, 3RHOEOPEN and 4RHOEOPEN

TABLE C-27 (Cont)

SHEARON HARRIS
HUMAN ERROR CALCULATIONS

TASK: Open Low Head SI Train A(B) to Cold Legs, 1SI-340 (1SI-341).

REFERENCE: Step 20a of OP-111, Revision 2, "Residual Heat Removal System," Section 5.1, "Preparing Train A(B) RHR for RCS Cooldown," subsection 5.1, "Procedural Steps."

BREAKDOWN OF TASK:

1. Omission error - Operator fails to open motor operated valve to cold legs

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-7	Long list > 10 items When procedures with checkoff provisions are correctly used

2. Commission error - Operator fails to open valve by selecting wrong control

Median HEP = 0.003 Mean HEP = 3.75E-03 Error Factor = 3	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls identified by labels only

3. Recovery error -Shift foreman fails to detect error by others

Median HEP = 0.1 Mean HEP = 0.16 Error Factor = 5	Table 20-22	Checking routine tasks, checker using written materials

P_{OE} = (1-3.75E-03)(0.00375)(0.16) + 0.00375(0.16)
= 5.9775E-04 + 6.0E-04
= 1.198E-03
= 1.2E-03

Fault Tree Identifiers: MVSI340OED and MVSI341OED

TABLE C-28

SHEARON HARRIS
DOMINANT CONTRIBUTORS
RHR INITIATION

MEAN PROBABILITY OF FAILURE = 3.74E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	3.20E-03	OPERATOR FAILS TO OPEN 1RH40 SUCTION VALVE
2.	3.20E-03	OPERATOR FAILS TO OPEN 1RH40 SUCTION VALVE
3.	3.20E-03	OPERATOR FAILS TO OPEN 1RH2 SUCTION VALVE
4.	3.20E-03	OPERATOR FAILS TO OPEN 1RH1 SUCTION VALVE
5.	1.80E-03	RHR HX BYPASS 1RH58 FAILS TO OPEN OPERATOR ERROR
6.	1.80E-03	RHR HX BYPASS VALVE 1RH20 FAILS TO OPEN OPERATOR ERROR
7.	1.60E-03	OPERATOR FAILS TO RACK IN CIRCUIT BREAKER FOR VALVE 1RH40
8.	1.60E-03	OPERATOR FAILS TO RACK IN CIRCUIT BREAKER FOR VALVE 1RH39
9.	1.60E-03	OPERATOR FAILS TO RACK IN CIRCUIT BREAKER FOR VALVE 1RH2
10.	1.60E-3	OPERATOR FAILS TO RACK IN CIRCUIT BREAKER FOR VALVE
11.	1.20E-03	CCW TO RHR HX OUTLET VALVE 1CC167 FAIL OPEN OPERATOR ERROR
12.	1.20E-03	CCW TO RHR HX OUTLET VALVE 1CC147 FAIL OPEN OPERATOR ERROR
13.	1.20E-03	TRAIN B DISCHARGE VALVE 1SI341 FAIL OPEN OPERATOR ERROR
14.	1.20E-03	TRAIN A DISCHARGE VALVE 1SI340 FAIL OPEN OPERATOR ERROR
15.	1.20E-03	RHR CROSSOVER TO HOT LEG VALVE 1SI327 FAIL CLOS OPERATOR ERROR
16.	1.20E-03	RHR CROSSOVER TO HOT LEG VALVE 1SI326 FAIL CLOS OPERATOR ERROR
17.	1.20E-03	DISCHARGE VALVE 1SI341 FAILS TO CLOSE OPERATOR ERROR
18.	1.20E-03	DISCHARGE VALVE 1SI340 FAILS TO CLOSE OPERATOR ERROR
19.	1.20E-03	RHR SUCTION RWST VALVE 1SI323 FAILS TO CLOSE OPERATOR ERROR
20.	1.20E-03	RHR SUCTION RWST VALVE 1SI322 FAILS TO CLOSE OPERATOR ERROR

TABLE C-29

SHEARON HARRIS
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.61E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	7.20E-03	PUMP 1B-SB FAILS TO RUN FOR 72 HOURS
2.	7.20E-03	PUMP 1A-SA FAILS TO OPERATE FOR 72 HOURS
3.	4.18E-04	LOOP POWER SUPPLY PGY-403 FAILS
4.	4.18E-04	LOOP POWER SUPPLY PGY-402 FAILS
5.	2.09E-04	DUAL COMPARATOR PB-403 FAILS
6.	2.09E-04	DUAL COMPARATOR PB-402 FAILS
7.	2.20E-04	PRESSURE TRANSMITTER PT-403 FAILS
8.	2.02E-04	PRESSURE TRANSMITTER PT-402 FAILS
9.	1.44E-05	RHR HX 1B-SB FAILS TO REMOVE HEAT CCW VALVE SPURIOUSLY CLOSE
10.	1.44E-05	CHECK VALVE 1RH-70 FAILS TO OPEN
11.	1.44E-05	MOTOR OPERATED VALVE 1SI-341 SPURIOUSLY CLOSES
12.	1.44E-05	CHECK VALVE 1SI-347 FAILS TO OPEN
13.	1.44E-05	HEAT EXCHANGER 1A-SA FAILS TO REMOVE HEAT CCW SPUR CLOSE
14.	1.44E-05	CHECK VALVE 1SI-34 FAILS TO OPEN
15.	1.44E-05	MOTOR OPERATED VALVE 1SI340 SPURIOUSLY CLOSES
16.	1.44E-05	CHECK VALVE 1SI-346 FAILS TO OPEN
17.	6.26E-06	AUXILIARY RELAY PY/403A1 FAILS
18.	6.26E-06	AUXILIARY RELAY PY/402A1 FAILS
19.	1.44E-06	CLOSE CONTACT 2B1-2B2 SHORTS
20.	1.44E-06	LOCKIN CIRCUIT FAILURE CONTACT 42S SHORTS

TABLE C-30

SHEARON HARRIS
DOMINANT CONTRIBUTORS
LOSS OF SHORT TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE - 1.45E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	7.20E-03	PUMP 1B-SB FAILS TO RUN FOR 72 HOURS
2.	7.20E-03	PUMP 1A-SA FAILS TO OPERATE FOR 72 HOURS
3.	1.44E-05	RHR HX 1B-SB FAILS TO REMOVE HEAT CCW VALVE SPURIOUSLY CLOSE
4.	1.44E-05	CHECK VALVE 1RH-70 FAILS TO OPEN
5.	1.44E-05	MOTOR OPERATED VALVE 1SI-341 SPURIOUSLY CLOSES
6.	1.44E-05	CHECK VALVE 1SI-347 FAILS TO OPEN
7.	1.44E-05	HEAT EXCHANGER 1A-SA FAILS TO REMOVE HEAT CCW SPUR CLOSE
8.	1.44E-05	CHECK VALVE 1SI-34 FAILS TO OPEN
9.	1.44E-05	MOTOR OPERATED VALVE 1SI340 SPURIOUSLY CLOSES
10.	1.44E-05	CHECK VALVE 1SI-346 FAILS TO OPEN
11.	1.44E-06	CLOSE CONTACT 2B1-2B2 SHORTS
12.	1.44E-06	LOCKING CIRCUIT FAILURE CONTACT 42S SHORTS
13.	1.44E-06	CLOSE CONTACT 2B1-2B2 SHORTS
14.	144E-06	LOCKIN CIRCUIT FAILURE CONTACT 42S SHORTS
15.	1.44E-06	CLOSE CONTACT 2B1-2B2 SHORTS
16.	1.44E-06	LOCKIN CIRCUIT FAILURE CONTACT 42S SHORTS
17.	1.44E-06	CLOSE CONTACT 2B1-2B2 SHORTS
18.	1.44E-06	LOCKING CIRCUIT FAILURE CONTACT 42S SHORTS
19.	2.07E-10	SAFETY INJECTION CHECK VALVE 1SI357 FAILS TO OPEN SAFETY INJECTION CHECK VALVE 1SI356 FAILS TO OPEN
20.	2.07E-10	SAFETY INJECTION CHECK VALVE 1SI357 FAILS TO OPEN SAFETY INJECTION CHECK VALVE 1S181 FAILS TO OPEN

TABLE C-31

SHEARON HARRIS
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 3.45E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.02E-02	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
2.	5.85E-03	LOOP POWER SUPPLY PGY-402 FAILS
3.	5.85E-03	LOOP POWER SUPPLY PGY-403 FAILS
4.	2.92E-03	DUAL COMPARATOR PB-402 FAILS
5.	2.92E-03	DUAL COMPARATOR PB-403 FAILS
6.	2.82E-03	PRESSURE TRANSMITTER PT-402 FAILS
7.	2.82E-03	PRESSURE TRANSMITTER PT-403 FAILS
8.	1.02E-03	RHR PUMP 1B-SB FAILS TO START PUMP 1A-SA FAILS TO RUN FOR SIX WEEKS
9.	2.81E-04	RHR PUMP 1B-SB UNAVAILABLE DUE TO TEST PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
10.	1.59E-04	RHR PUMP 1B-SB UNAVAILABLE DUE TO MAINTENANCE PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
11.	8.77E-05	AUXILIARY RELAY PY/402A1 FAILS
12.	8.77E-05	AUXILIARY RELAY PY/403A1 FAILS
13.	2.04E-05	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS DISCHARGE VALVE 1SI-340 SPURIOUSLY CLOSES
14.	2.04E-05	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS HEAT EXCHANGER 1A-SA FAILS TO REMOVE HEAT CCW VALVE SPUR C
15.	2.04E-05	RHR DISCHARGE VALVE 1SI-341 SPURIOUSLY CLOSES PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
16.	2.04E-05	CHECK VALVE 1RH-347 FAILS TO OPEN PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
17.	2.04E-05	HEAT EXCHANGE 1B-SB FAILS TO REMOVE HEAT CCW VALVE SPUR C PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS

TABLE C-31 (Cont)

SHEARON HARRIS
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITH AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 3.45E-02

	PROBABILITY	CUTSET DESCRIPTION
18.	2.04E-05	CHECK VALVE 1RH70 FAILS TO OPEN PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
19.	2.04E-06	RHR PUMP 1B-SB FAILS TO START DISCHARGE VALVE 1SI-340 SPURIOUSLY CLOSES
20.	2.04E-06	CLOSE CONTACT 2B1-2B2 SHORTS PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS

TABLE C-32

SHEARON HARRIS
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.16E-02

	PROBABILITY	CUTSET DESCRIPTION
1.	1.02E-02	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
2.	1.02E-03	RHR PUMP 1B-SB FAILS TO START PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
3.	2.81E-04	RHR PUMP 1B-SB UNAVAILABLE DUE TO TEST PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
4.	1.59E-04	RHR PUMP 1B-SB UNAVAILABLE DUE TO MAINTENANCE PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
5.	2.04E-05	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS DISCHARGE VALVE 1SI-340 SPURIOUSLY CLOSES
6.	2.04E-05	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS HEAT EXCHANGER 1A-SA FAILS TO REMOVE HEAT CCW VALVE SPUR
7.	2.04E-05	RHR DISCHARGE VALVE 1SI-341 SPURIOUSLY CLOSES PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
8.	2.04E-05	CHECK VALVE 1RH-347 FAILS TO OPEN PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
9.	2.04E-05	HEAT EXCHANGER 1B-SB FAILS TO REMOVE HEAT CCW VALVE SPUR PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
10.	2.04E-05	CHECK VALVE 1RH70 FAILS TO OPEN PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
11.	2.04E-06	RHR PUMP 1B-SB FAILS TO START DISCHARGE VALVE 1SI-340 SPURIOUSLY CLOSES
12.	2.04E-06	CLOSE CONTACT 2B1-2B2 SHORTS PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
13.	2.04E-06	LOCKIN CIRCUIT FAILURE CONTACT 42S SHORTS PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
14.	2.04E-06	CLOSE CONTACT 2B1-2B2 SHORTS PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS
15.	2.04E-06	LOCKIN CIRCUIT FAILURE CONTACT 42S SHORTS PUMP 1A-SA FAILS TO RUN FOR 6 WEEKS

TABLE C-32 (Cont)

SHEARON HARRIS
DOMINANT CONTRIBUTORS
LOSS OF LONG TERM COOLING
WITHOUT AUTOCLOSURE INTERLOCK

MEAN PROBABILITY OF FAILURE = 1.16E-02

	PROBABILITY	CUTSET DESCRIPTION
16.	2.04E-06	RHR PUMP 1B-SB FAILS TO START HEAT EXCHANGER 1A-SA FAILS TO REMOVE HEAT CCW VALVE SPUR
17.	2.04E-06	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS CLOSE CONTACT 2B1-2B2 SHORTS
18.	2.04E-06	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS LOCKIN CIRCUIT FAILURE CONTACT 42S SHORTS
19.	2.04E-06	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS CLOSE CONTACT 2B1-2B2 SHORTS
20.	2.04E-06	RHR PUMP 1B-SB FAILS TO RUN FOR 6 WEEKS LOCKING CIRCUIT FAILURE CONTACT 42S SHORTS

OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 5

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH

APPENDIX D

OVERPRESSURIZATION TRANSIENTS

APPENDIX D
OVERPRESSURIZATION TRANSIENTS

D.1 INTRODUCTION

This appendix details the calculations and analyses involved in the determination of the effect of removal of the RHR autoclosure interlock on overpressurization transients. The first section categorizes the types of initiating events and utilizing operating experience, the frequency of these events is determined. The remaining sections discuss the mass input transients and the consequences from these transients for each of the reference plants.

D.2 INITIATING EVENTS

This section provides the data and calculations used to determine the frequencies of the transient events identified in Section 7.5. Table D-1 lists the transients that have actually occurred at Westinghouse PWRs by the type of transient. This information was collected from various sources, including licensee event reports (LERs). Table D-2 lists the loss of residual heat removal events that have occurred at Westinghouse plants due to the autoclosure interlock.

In order to determine the frequency of these events, a compilation of operating years of experience was performed. This data is provided in Table D-3. This table shows, for each plant, an estimate of the total number of shutdown hours (in which the RHRS would be required to operate) along with the total report period hours. The data was collected from NUREG-0020, Volume 10, No. 12, "Licensed Operating Reactors, Status Summary Report, Data as of 11-30-86," (Reference 25).

To quantify the frequency of overpressurization transients the following formula was used:

$$F\ (\text{Transient}) = \frac{\#\ \text{of transients}}{\#\ \text{of shutdown years}}$$

$$\frac{\#\ \text{of transients}}{\text{Total shutdown years}}$$

$$\frac{\#\ \text{of transients}}{112.4\ \text{shutdown years}}$$

Table D-4 lists the frequencies for each transient using the above formula. For the case of letdown isolation, RHRS isolated, the frequency was calculated utilizing the number of occurrences of the loss of RHR events from Table D-2.

The modification to the autoclosure interlock does not affect the charging/SI pump actuation event frequency or the letdown isolation RHR operable event frequency. However, the letdown isolation - RHR isolated frequency would be significantly reduced due to removal of the autoclosure interlock. This is because many spurious closures of the RHR isolation valves cause the isolation of letdown. In order to account for the reduction in the frequency for the letdown isolation - RHRS isolated case, the frequency for the modification case was assumed to conservatively decrease by one-half. Thus, the frequency for the letdown isolation - RHR isolated case, for the case without the autoclosure interlock, is 2.22E-01/shutdown-year.

Because the heat input transients have no effect on the removal of the autoclosure interlock as discussed in section 7.5, these transients were not examined further. The following sections discuss the mass input transient analysis performed for each of the reference plants.

TABLE D-1

ACTUAL OVERPRESSURIZATION TRANSIENTS WESTINGHOUSE PLANTS ONLY

PLANT	DATE	KEYWORDS	SOURCE	REMARKS
OPENING OF ACCUMULATOR DISCHARGE ISOLATION VALVES				
SURRY 1	1/28/73	VENT TRAPPED AIR	N. SAFETY	FROM 450 TO 590 PSIG
PRAIRIE ISLAND 1	1/16/74	SI SIGNAL INITIATED	N. SAFETY	FROM 395 TO 840 PSIG
INDIAN POINT 2	2/22/74	INADVERTENT SI	N. SAFETY	FROM 150 TO 560 PSIG
NORTH ANNA 1	12/16/85	FALSE PRESSURE SIGNAL	LER	85-023
STARTUP OF INACTIVE LOOP				
INDIAN POINT 2	3/8/72	THERMAL EXPANSION	N. SAFETY	FROM 400 TO 640 PSIG
PRAIRIE ISLAND 1	10/31/73	THERMAL EXPANSION	N. SAFETY	FROM 420 TO 1100 PSIG
INDIAN POINT 2	1/23/74	PRESSURE SURGE	N. SAFETY	FROM 425 TO 525 PSIG
FARLEY 2	10/15/83	PRESSURE SURGE	NPE	TO 480 PSIG RHR RELIEF
TURKEY POINT 4	11/28/81	PRESSURE SURGE	IE 82-17	TO 1100 PSIG
TURKEY POINT 4	11/29/81	PRESSURE SURGE	IE 82-17	TO 750 PSIG
NORTH ANNA 2	5/24/82	FILLING AND VENTING	AEOD	PORV OPENED TWICE
NORTH ANNA 2	5/18/82	PRESSURE SURGE	AEOD	PORV OPENED TWICE
SALEM 2	3/29/85	RCS FILL AND VENT	LER	85-003 PORV OPENED TWICE
SUMMER	5/6/85	DG TESTING	NPE	RHR RELIEF VALVE ACTUATED
NORTH ANNA 1	8/14/85	DURING STARTUP	LER	85-010 BOTH PORVS TWICE
ISOLATION OF LETDOWN WHILE CHARGING CONTINUES - RHR OPERABLE				
GINNA	1969	OPERATOR ERROR	N. SAFETY	TO 2485 PSIG SAFETY VALVE
INDIAN POINT 2	2/17/72	OPERATOR ERROR	N. SAFETY	FROM 420 TO 650 PSIG
INDIAN POINT 2	4/6/72	OPERATOR ERROR	N. SAFETY	FROM 420 TO 680 PSIG
INDIAN POINT 2	5/18/73	FROZEN VALVES	N. SAFETY	FROM 440 TO 575 PSIG
PRAIRIE ISLAND 2	11/27/74	TEST SIGNAL	N. SAFETY	TO 900 PSIG
BEAVER VALLEY 1	2/24/76	ELECTRICAL BUS TRANSFER	N. SAFETY	FROM 400 TO 1000 PSIG
BEAVER VALLEY 1	3/5/76	BUS DEENERGIZED SI SIGNAL	N. SAFETY	FROM 400 TO 1150 PSIG
D.C. COOK 1	4/14/76	RPS TESTING	N. SAFETY	TO 1040 PSIG
INDIAN POINT 2	9/12/76	INSTRUMENT AIR LOST	N. SAFETY	FROM 400 TO 515 PSIG
NORTH ANNA 1	3/78	ELECTRICAL SHORT	NPE	TO 575 PSIG
NORTH ANNA 1	3/80	VALVE FAILED CLOSED	NPE	TO 570 PSIG RHR RELIEF
FARLEY 2	10/15/83	CONTAINMENT ISOLATED	NPE	TO 700 PSIG RHR RELIEF
SUMMER	12/4/84	SHORT CIRCUIT	SPECIALR	84-018 RHR RELIEF
SURRY 1	5/12/85	POSITIONER OUT OF ADJUSTMENT	LER	85-009 PORV CYCLED TWICE

TABLE D-1 (Cont)

ACTUAL OVERPRESSURIZATION TRANSIENTS
WESTINGHOUSE PLANTS ONLY

PLANT	DATE	KEYWORDS	SOURCE	REMARKS
PRESSURIZER HEATERS ACTUATION				
NO WESTINGHOUSE PLANTS				
ISOLATION OF LETDOWN WHILE CHARGING CONTINUES RHR ISOLATED				
TURKEY POINT 3	12/3/74	HIGH PRESSURE AUTOMATIC	N. SAFETY	FROM 50 TO 800 PSIG
ZION 1	6/3/75	OPERATOR ERROR	N. SAFETY	FROM 100 TO 1100 PSIG
TROJAN	7/22/75	UNKNOWN PERSON	N. SAFETY	FROM 400 TO 3326 PSIG
ZION 2	9/18/75	INTERLOCK TEST	N. SAFETY	FROM 95 TO 1300 PSIG
POINT BEACH 2	2/28/76	OPERATIONAL REASONS	NUREG	FROM 400 TO 830 PSIG
INDIAN POINT 3	9/30/76	SPURIOUS CLOSURE	N. SAFETY	FROM 50 TO 2250 PSIG
ZION 2	1/3/86	POWER SUPPLY FLUCTUATION	LER	86-001 PORVS LIFTED
OTHER EVENTS				
BYRON 1	12/28/84	RHR REPRESSURIZATION	LETTER	BYRON-85-0051 RHR RELIEF
BYRON 1	12/30/84	RHR REPRESSURIZATION	LETTER	BYRON-85-0051 RHR RELIEF
NORTH ANNA 1	12/19/85	OP ERROR LETDOWN/CHARGING	LER	85-025 MISMATCH
CALLAWAY	4/5/86	RCP SEAL CONTROL VALVE	SPECIALR	86-03
FARLEY	11/7/86	OPERATOR ERROR	LER	86-020 RHR RELIEF
CHARGING/SAFETY INJECTION ACTUATION				
ZION 1	6/13/73	OP LEFT PUMP RUNNING	N. SAFETY	FROM 110 TO 1290 PSIG
PRAIRIE ISLAND 1	10/74	SI SIGNAL	NPE	
POINT BEACH 2	12/10/74	SI PUMP	NUREG	FROM 345 TO 1400 PSIG
BEAVER VALLEY 1	3/13/76	INADVERTENT SI SIGNAL	N. SAFETY	FROM 425 TO 495 PSIG
ROBINSON 2	1/78	MANUAL SI	NPE	FROM 360 TO 560 PSIG
NORTH ANNA 1	3/29/81	SI SIGNAL	LER	81-018 PORVS LIFTED
NORTH ANNA 2	5/23/83	INADVERTENT SI SIGNAL	NPE	TO 387 PSIG PORV 3 TIMES
SURRY 1	7/7/82	INADVERTENT CHARGING	AEOD	ONE PORV OPENED
GINNA	6/9/83	PERSONNEL ERROR	AEOD	PORV ACTUATED
SALEM 2	6/17/83	PERSONNEL ERROR	AEOD	BOTH PORVS ACTUATED
SURRY 1	6/1/84	PLACE CHARGING IN SERVICE	NPE	PORV CYCLED
TROJAN	6/30/85	I&C TESTING	NPE	350 TO 420 PSIG TWICE
BYRON 1	3/18/85	ACCIDENTAL SI	LER	85034
ZION 2	1/3/86	INVERTER PS FLUCTUATION	LER	86001 RHR ISOLATION

TABLE D-1 (Cont)

ACTUAL OVERPRESSURIZATION TRANSIENTS
WESTINGHOUSE PLANTS ONLY

SOURCES

N. SAFETY	REACTOR VESSEL TRANSIENTS, NUCLEAR SAFETY (ABSTRACTED FROM NUREG-0138)
IE-82-17	IE INFORMATION NOTICE 82-17
AEOD	CASE STUDY REPORT - LOW TEMPERATURE OVERPRESSURE EVENTS AT TURKEY POINT UNIT 4
NPE	NUCLEAR POWER EXPERIENCE
NUREG	NUREG-0224 REACTOR VESSEL PRESSURE TRANSIENT PROTECTION
DHR	AEOD CASE STUDY REPORT- DECAY HEAT REMOVAL PROBLEMS AT U.S. PWRS
LER	LICENSEE EVENT REPORTS
SPECIALR	SPECIAL REPORT

TABLE D-2

LOSS OF RHR EVENTS
DUE TO AUTOCLOSURE INTERLOCK
WESTINGHOUSE PLANTS ONLY

PLANT	DATE	KEYWORDS	SOURCE	REMARKS
KEWAUNEE	9/26/74	LOSS OF INSTRUMENT BUS	LER	74-17 FROM 110 TO 214F
SALEM 1	9/2/76	VOLTAGE TRANSIENT	NSAC52	RHR LOST FOR 19 MINUTES
SALEM 1	9/20/76	ERRATIC PRESSURE INDICATION	NSAC52	RHR LOST FOR 30 MINUTES
INDIAN POINT 3	9/30/76	ROOT CAUSE UNKNOWN	NSAC52	RCS PRESSURE TO 2250 PSIG
FARLEY	7/11/77	CAUSE UNKNOWN	LER	77-8
TROJAN	3/20/78	ESF TESTING	NSAC52	RCS TEMP TO 211°F
FARLEY 1	9/18/78	SSPS DEENERGIZED	NSAC52	RHR LOST FOR 7 MINUTES
FARLEY 1	9/18/78	SSPS DEENERGIZED	NSAC52	RHR LOST FOR 3 MINUTES
NORTH ANNA 1	11/6/79	INSTALLED JUMPER	NSAC52	RHR LOST FOR 5 MINUTES
NORTH ANNA 2	4/23/80	BLOWN POWER SUPPLY FUSE	NSAC52	FALSE HI PRESS SIGNAL
BEAVER VALLEY 1	5/21/80	PERSONNEL ERROR	NSAC52	LOW DECAY HEAT RATE
FARLEY 1	11/28/80	ERRONEOUS HI PRESS SIGNAL	NSAC52	RHR LOST FOR 4 MINUTES
FARLEY 1	12/25/80	INSTRUMENT LEAD SHORT CIRCUIT	NSAC52	RHR LOST FOR 5 MINUTES
MCGUIRE 1	4/27/81	MAINTENANCE ACTIONS	NSAC52	RHR LOST FOR 15 MINUTES
MCGUIRE 1	8/4/81	MAINTENANCE ON PRESS INSTRUM.	NSAC52	RHR LOST FOR 15 MINUTES
MCGUIRE 1	11/18/81	CONSTRUCTION PERSONNEL ERROR	NSAC52	RHR LOST FOR 22 MINUTES
TURKEY POINT 4	11/28/81	STARTUP OF RCP PUMP	NSAC52	PRESS INCREASE TO 1100 PSIG
TURKEY POINT 4	11/29/81	STARTUP OF RCP PUMP	NSAC52	PRESS INCREASE TO 750 PSIG
ZION 1	3/17/82	INADVERTENT OPEN OF INVERTER	AEOD	RHR LOST FOR 3 MINUTES
MCGUIRE 1	6/24/82	INVERTER FAILURE	AEOD	RHR LOST FOR 6 MINUTES
NORTH ANNA 2	7/30/82	PERSONNEL ERROR OPEN BREAKER	AEOD	LESS THAN 1 MINUTE LOSS
SUMMER	8/18/82	MAINTENANCE ERROR	LER	LER 82002
SUMMER	9/15/82	SURVEILLANCE TESTING	LER	LER 82004 MOMENTARY LOSS
SEQUOYAH 1	9/16/82	SSPS POWER REMOVED	AEOD	DURATION UNKNOWN
NORTH ANNA 1	1/22/83	FAILED INVERTER	AEOD	RHR LOST FOR 4 MINUTES
NORTH ANNA 2	4/14/83	OPERATOR ERROR	LER	83-023
NORTH ANNA 2	4/23/83	LOSS OF 120 VAC	NPE	
NORTH ANNA 2	4/29/83	LOSS OF VITAL BUS	AEOD	LESS THAN 1 MINUTE LOSS
GINNA	5/1/83	MCC INSPECTION POWER RESTORED	SOER	SOER 85-4
SALEM 2	5/14/83	DEENERGIZED VITAL INSTR BUS	AEOD	DURATION OF LOSS UNKNOWN
SALEM 2	5/15/83	FAILED COMPARATOR	AEOD	DURATION UNKNOWN
TURKEY POINT 3	10/8/83	PROCEDURAL ERROR DURING TEST	AEOD	RHR LOST FOR 6 MINUTES
DIABLO CANYON 1	10/27/83	SURVEILLANCE TESTING	SOER	85-4 PUMP SEAL/SHAFT DAMAGE
SUMMER 1	11/12/83	120VAC BUS TRANSFER	LER	83-136 RHR LOST FOR 5 MIN
SALEM 2	11/28/83	VITAL BUS TRANSFER	AEOD	DURATION UNKNOWN
SALEM 2	12/20/83	LOSS OF BUS -PERSONNEL ERROR	AEOD	RHR LOST FOR 22 MINUTES

TABLE D-2

LOSS OF RHR EVENTS DUE TO AUTOCLOSURE INTERLOCK WESTINGHOUSE PLANTS ONLY

PLANT	DATE	KEYWORDS	SOURCE	REMARKS
MCGUIRE 2	1/15/84	PERSONNEL ERROR DURING TEST	AEOD	RHR LOST FOR 49 MINUTES
SALEM 2	2/9/84	PROCEDURAL ERROR -POPS TEST	AEOD	RHR LOST FOR 17 MINUTES
SUMMER	10/2/84	SSPS FUSES REMOVED	LER	LER 84044 2 OCCURRENCES
SUMMER	10/18/84	LOSS OF POWER TO 120VAC	LER	LER 84045 RHR LOSS 25 MIN
SUMMER	11/24/84	ESF BUS TRANSFER	AEOD	RHR LOST FOR 5 MINUTES
TURKEY POINT 4	11/30/84	PRESS CONTROLLER MALFUNCTION	LER	LER 84027 PRESS 350 TO 415
DIABLO CANYON 1	1/20/85	PT403 REMOVED FROM SERVICE	LER	85-005
DIABLO CANYON 1	1/25/85	LOSS OF VITAL 4KV BUS	LER	85-006 RHR LOST FOR 2 MIN
FARLEY 1	5/6/85	MAINTENANCE ERROR	NPE	PROCEDURAL AND MAINTENANCE
SEQUOYAH 1	5/14/85	RVLIS SURVEILLANCE TEST	NPE	RHR LOST FOR 16 MINUTES
TURKEY POINT 3	10/25/85	FAILED RELAY IN PRESS COMPAR	LER	LER 85036 RHR LOST 27 MIN
DIABLO CANYON 2	1/17/86	POWER SUPPLY TRANSFER	LER	86-002
TURKEY POINT 4	3/15/86	VITAL BUS BREAKER	LER	86-006 RHR LOST FOR 5 MIN
DIABLO CANYON 1	9/8/86	GROUNDED POWER SUPPLY	LER	86-012

SOURCES

NSAC52	RESIDUAL HEAT REMOVAL EXPERIENCE REVIEW AND SAFETY ANALYSIS - PWRS
AEOD	AEOD/C503 DECAY HEAT REMOVAL PROBLEMS AT US PWRS
LER	LICENSEE EVENT REPORTS
SOER	SIGNIFICANT OPERATING EXPERIENCE REPORT

TABLE D-3
WESTINGHOUSE PLANTS OPERATING HISTORY
AS OF NOVEMBER 30, 1986

PLANT NAME	REPORT PERIOD HRS	GENERATOR HRS	FORCED OUTAGE HRS	SCHEDULED OUTAGE HRS	TOTAL SHUTDOWN HRS	% SHUTDOWN
Beaver Valley 1	92784.0	49587.4	18780.1	24416.5	43196.6	46.6
Beaver Valley 2	0.0	0.0	0.0	0.0	0.0	0.0
Braidwood 1	0.0	0.0	0.0	0.0	0.0	0.0
Braidwood 2	0.0	0.0	0.0	0.0	0.0	0.0
Byron 1	10585.0	8209.7	777.0	1598.3	2375.3	22.4
Byron 2	0.0	0.0	0.0	0.0	0.0	0.0
Callaway	17078.5	14567.9	779.8	1730.8	2510.6	14.7
Catawba 1	12481.0	7926.7	2142.4	2411.9	4554.3	36.5
Catawba 2	2497.0	581.8	1915.2	0.0	0.0	0.0
Comanche Peak 1	0.0	0.0	0.0	0.0	0.0	0.0
Comanche Peak 2	0.0	0.0	0.0	0.0	0.0	0.0
Conn Yankee	165816.0	135953.0	2058.1	28694.9	30753.0	18.5
D.C. Cook 1	104443.0	73574.6	6235.9	24637.5	30873.4	29.6
D.C. Cook 2	78144.0	52499.6	9155.9	16488.5	25644.4	32.8
Diablo Canyon 1	13750.3	10922.2	363.5	2464.6	2828.1	20.6
Diablo Canyon 2	6309.0	5986.5	293.2	29.3	322.5	5.1
Farley 1	78888.0	54910.6	6500.5	17476.9	23977.4	30.4
Farley 2	46801.0	40106.7	1872.3	4822.0	6694.3	14.3
Ginna	149136.0	112909.7	4324.4	31901.9	36226.3	24.3
Indian Point 2	108865.0	71319.3	7134.2	30411.5	37545.7	34.5
Indain Point 3	89881.0	51322.0	12942.5	25616.5	385[illegible].0	42.9
Kewaunee	109225.0	91326.8	2819.9	15078.3	17898.2	16.4
McGuire 1	43824.0	28883.8	5685.9	9254.3	14940.2	34.1
McGuire 2	24120.0	16126.4	3160.0	4833.6	7993.6	33.1
Millstune 3	5328.0	4611.9	716.1	0.0	716.1	13.4
North Anna 1	74401.0	50499.0	7392.2	16509.8	23902.0	32.1
North Anna 2	52272.0	39898.6	4768.9	7604.5	12373.4	23.7
Point Beach 1	140856.0	111950.4	2444.3	23461.3	28905.6	20.5
Point Beach 2	125641.0	108245.0	768.7	16627.3	17396.0	13.8
Prairie Island 1	113592.0	93148.0	3396.8	17047.2	20444.0	18.0
Prairie Island 2	104710.0	89690.8	3359.0	11660.2	15019.2	14.3
Robinson 2	138006.0	96063.5	9581.2	32361.3	41942.5	30.4
Salem 1	82585.0	48684.4	19226.0	14674.6	33900.6	41.0
Salem 2	45001.0	24775.2	14647.4	5578.4	20225.8	44.9
San Onofre 1	170600.0	94422.8	12998.6	63178.6	76177.2	44.7
Seabrook 1	0.0	0.0	0.0	0.0	0.0	0.0
Sequoyah 1	47497.0	23871.0	14387.1	9238.9	23626.0	49.7
Sequoyah 2	39457.0	21494.4	13139.3	4823.3	17962.6	45.5
Shearon Harris 1	0.0	0.0	0.0	0.0	0.0	0.0
South Texas 1	0.0	0.0	0.0	0.0	0.0	0.0
South Texas 2	0.0	0.0	0.0	0.0	0.0	0.0
Summer	25560.0	19283.8	1433.2	4843.0	6276.2	24.6
Surry 1	122208.0	76614.9	13213.4	32379.7	45593.1	37.3
Surry 2	119088.0	76678.6	8437.9	33971.5	42409.4	35.6
Trojan	89832.0	55295.6	9248.4	25288.0	34536.4	38.4
Turkey Point 3	122625.6	84593.8	6401.4	31630.4	38031.8	31.0
Turkey Point 4	116353.0	77190.3	5139.8	34022.9	39162.7	33.7
Vogtle 1	0.0	0.0	0.0	0.0	0.0	0.0
Vogtle 2	0.0	0.0	0.0	0.0	0.0	0.0
Watts Bar 1	0.0	0.0	0.0	0.0	0.0	0.0
Watts Bar 2	0.0	0.0	0.0	0.0	0.0	0.0
Wolfcreek	10895.7	8950.0	377.2	1568.5	1945.7	17.9
Yankee Rowe	228261.0	178236.7	8763.8	41260.5	50024.3	21.9
Zion 1	113232.0	77058.1	11668.2	24505.7	36173.9	31.9
Zion 2	106945.0	76235.8	13662.0	17047.2	30709.2	28.7
TOTAL HOURS	3349579.1	2363317.3	272111.7	714150.1	984346.6	28.8
TOTAL YEARS	382.4	269.8	31.1	81.5	112.4	

TABLE D-4

FREQUENCY OF OVERPRESSURE TRANSIENTS

	TOTAL NUMBER OF OCCURRENCES	FREQUENCY EVENTS/ SHUTDOWN YEAR
OPENING OF ACCUMULATOR DISCHARGE ISOLATION VALVES	4	3.56E-02
STARTUP OF INACTIVE LOOP	11	9.79E-02
ISOLATION OF LETDOWN WHILE CHARGING CONTINUES	14	1.25E-01
CHARGING/SAFETY INJECTION	14	1.25E-01
ISOLATION OF LETDOWN WHILE CHARGING CONTINUES RHR ISOLATED	50	4.45E-01
TOTAL	93	8.27E-01

D.3 MASS INPUT ANALYSIS

The following section describes the assumptions and the calculations involved in the analysis of mass input initiated overpressurization events. The effect of these transients on the RHR System and on the RCS are categorized in order to determine the differences between the events that lead to high overpressure, medium or low pressure conditions.

This analysis utilized event trees to depict the various mitigating actions that can take place after a mass input initiated transient.

The following assumptions and conditions were used in the development of the event trees:

1. The plant is in the cold shutdown mode (mode 5) with a temperature below 160°F and a pressure below 400 psig.

2. One charging pump is in operation and pumping at its maximum flowrate.

3. Letdown via the RHRS is in operation and the flowrate is at its maximum.

4. No Reactor Coolant pumps are in operation.

5. An alarm must actuate before the operat r can intervene and stop the transient. This alarm can come from:

   a) RHR relief valve discharge to PRT (pressurizer relief tank),
   b) PORV discharge,
   c) low temperature overpressure protection system operation,
   or d) RHR pump low flow alarm due to closure of the RHR suction valves.

6. If the flowrate due to the transient is greater than the relief capacity of the operating mitigation systems, another system must operate or the pressure will continue to increase with a rate proportionate to the difference in input/removal rates.

7. When a pump spuriously starts, it runs at its maximum flowrate. Furthermore, the pump is assumed to have an infinite water source.

The event tree sequences were classified into discrete consequence categories. Each consequence category represents a number of individual sequences that all have similar characteristics associated with them. The consequence categories were defined by the parameters listed in Table D-5. The consequence categories define what actions the operator must take by determining the conditions following the transient. A description of the consequence categories is shown in Table D-6.

The event trees were quantified using system/component failure probabilities along with the initiating event frequencies to determine the frequency of the consequence categories for the current configuration and the case without the autoclosure interlock. For each reference plant, the three mass input transients are discussed.

TABLE D-5
CONSEQUENCE CATEGORY PARAMETERS

SYMBOL	DESCRIPTION
L	Low Pressure (Both PORVs, 2 RHR relief valves or 1 RHR and 1 PORV operate)
M	Medium pressure (One PORV or 1 RHR relief valve operate)
H	High pressure (No PORVs or RHR relief valves operate)
LC	Large Continuous Loss of Coolant (both PORVS, Both RHR relief valves or 1 PORV and 1 RHR relief operate and pump continues to run)
SC	Small continuous loss of coolant (1 PORV or 1 RHR relief valve operate and pump continues to run)
LF	Large finite loss of coolant (Both PORVs, both RHR relief valves or 1 RHR relief valve and 1 PORV fail to reseat after pump is stopped)
SF	Small finite loss of coolant (1 RHR relief valve or 1 PORV fail to reseat after pump is stopped)
OP	Overpressure (No RHR relief valves or PORVs operate)
I	RHRS Isolated from RCS
O	RHRS Open to RCS
V	Interfacing system LOCA (RHRS open to RCS at high pressure)

TABLE D-6

TRANSIENT EVENT OUTCOME DESCRIPTIONS

CATEGORY	OUTCOME DESCRIPTION
LSFO	Low pressure with small loss of coolant and the RHRS is open to the RCS. The running pump has been stopped but the one of the relief valves has failed to reseat. The operator must take action to reseat the valve or isolate it and then must add makeup.
LSFI	Low pressure with small loss of coolant and the RHRS is isolated from the RCS. The running pump has been stopped but the one of the relief valves has failed to reseat. The operator must take action to reseat the valve or isolate it and then must add makeup. He must also reinitialize RHR operation.
LSCO	Low pressure with small loss of coolant and the RHRS is open to the RCS. The running pump has not been stopped and coolant is exiting via one relief valve. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely.
LSCI	Low pressure with small loss of coolant and the RHRS is isolated from the RCS. The running pump has not been stopped and coolant is exiting via one relief valve. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely.
LLFO	Low pressure with large loss of coolant and the RHRS is open to the RCS. The running pump has been stopped but two or more of the relief valves has failed to reseat. The operator must take action to reseat valves or isolate them and then must add makeup.
LLFI	Low pressure with large loss of coolant and the RHRS is isolated from the RCS. The running pump has been stopped but two or more of the relief valves has failed to reseat. The operator must take action to reseat the valves or isolate them and then must add makeup. He must also reinitialize RHR operation.
LLCO	Low pressure with large loss of coolant and the RHRS is open to the RCS. The running pump has not been stopped and coolant is exiting via two or more relief valves. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely. The operator must also be aware of possible deadheading or air entrainment of the RHR pumps.

TABLE D-6 (Cont)

TRANSIENT EVENT OUTCOME DESCRIPTIONS

CATEGORY	OUTCOME DESCRIPTION
LLCI	Low pressure with large loss of coolant and the RHRS is isolated from the RCS. The running pump has not been stopped and coolant is exiting via two or more relief valves. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely.
MSFO	Medium pressure with small loss of coolant and the RHRS is open to the RCS. The running pump has been stopped but the one of the relief valves has failed to reseat. The operator must take action to reseat the valve or isolate it and then must add makeup. He must also reduce the RCS pressure and check on the integrity of the RHR System.
MSFI	Medium pressure with small loss of coolant and the RHRS is isolated from the RCS. The running pump has been stopped but the one of the relief valves has failed to reseat. The operator must take action to reseat the valve or isolate it and then must add makeup. He must also reduce the RCS pressure and then reinitialize RHR operation.
MSCO	Medium pressure with small loss of coolant and the RHRS is open to the RCS. The running pump has not been stopped and coolant is exiting via one relief valve. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely. He must also reduce the RCS pressure and check on the integrity of the RHR system.
MSCI	Medium pressure with small loss of coolant and the RHRS is isolated from the RCS. The running pump has not been stopped and coolant is exiting via one relief valve. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely.
MLFO	Medium pressure with large loss of coolant and the RHRS is open to the RCS. The running pump has been stopped but two or more of the relief valves has failed to reseat. The operator must take action to reseat the valves or isolate them and then must add makeup. He must also reduce the RCS pressure and check on the integrity of the RHR System.
MLFI	Medium pressure with large loss of coolant and the RHRS is isolated from the RCS. The running pump has been stopped but two or more of the relief valves has failed to reseat. The operator must take action to reseat the valves or isolate them and then must add makeup. He must also reduce the RCS pressure and then reinitialize RHR operation.

TABLE D-6 (Cont)
TRANSIENT EVENT OUTCOME DESCRIPTIONS

CATEGORY	OUTCOME DESCRIPTION
MLCO	Medium pressure with large loss of coolant and the RHRS is open to the RCS. The running pump has not been stopped and coolant is exiting via two or more relief valves. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely. The operator must also be aware of possible deadheading or air entrainment of the RHR pumps. He must also reduce the RCS pressure and check on the integrity of the RHR System.
MLCI	Medium pressure with large loss of coolant and the RHRS is isolated from the RCS. The running pump has not been stopped and coolant is exiting via two or more relief valves. The operator must take action to stop the running pump or isolate it and then must check that the relief valves have reseated completely. He must also reduce the RCS pressure.
MOPI	Medium overpressure with the RHRS isolated from the RCS. The running pump has been stopped but no relief valves have actuated. The operator must reduce the RCS pressure and then reinitialize RHR operation.
HOPI	High overpressure with the RHRS isolated from the RCS. The running pump has been stopped but no relief valves have actuated. The operator must reduce the RCS pressure, possibly through the RCS vents or pressurizer safety valves.
HOPV	High overpressure with the RHRS open to the RCS. The running pump has not been stopped and no relief valves have actuated. The RHR system integrity has assumed to be lost and an interfacing systems LOCA has occurred. The operator must attempt to isolate the RHR System.

D.3.1 SALEM

The effect of the overpressure transients identified in Section D.2 was evaluated utilizing event trees. Each mitigating system and operator action was modeled as a top node on the event tree for the given transient. The following describe the event tree structure, the success criteria defined for each transient, and the nodal probabilities utilized in the quantification and the results.

The safety functions, i.e. the event tree top events or nodes, for the Salem event trees are defined below:

1. Initiating Event (IE): The mass input initiator that could lead to overpressurization and/or possible RHRS damage, either charging/safety injection pump actuation or letdown isolation.

2. RHRS isolated (RI): The RHRS will be isolated during certain periods of shutdown. This dictates whether or not the RHRS relief valve is available to mitigate the transient and if the possibility exists for damage to the RHRS.

3. RHRS Suction Relief Valve Lifts (RV): If the RHRS is not isolated, the spring loaded relief valves will open at the setpoint pressure.

4. POPS System Operates (POP): The cold overpressure protection system consists of two redundant and independent systems utilizing the pressurizer PORVs. When the system is enabled and reactor coolant temperature is below 368°F, a high pressure signal (above the POPS setpoint) will trip the system automatically and open a PORV until the pressure drops below the reset value. For Salem, the POPS system has a fixed setpoint. The system logic will first annunciate a main control board alarm whenever the measured pressure approaches within a predetermined amount of the allowable pressure. On a further increase in measured pressure, an actuation signal is transmitted to the power-operated relief valve. The cases examined are two PORVs actuate, one PORV actuates or no PORVs actuate.

5a. RHRS Suction/Isolation Valves Automatically Close (RSV): When the pressure increases to the autoclosure setpoint (700 psig), the autoclosure interlock receives a pressure signal that actuates the circuitry and closes the motor-operated valve. This node is addressed in the case with the autoclosure interlock only.

5b. Operator Detects Overpressure Alarm and Isolates the RHRS (OD): For the modification case, an alarm would sound when the pressure reached the high pressure setpoint. Through a revision in operating procedures, it is assumed that the operator will detect the overpressure and isolate the RHRS before the pressure reaches 150% of the RHRS design pressure.

6. Operator Secures Running Pump (OA1): Given an alarm, either by actuation from the RHRS relief valve opening to the pressurizer relief tank (PRT), or from the operation of at least one train of POPS, or from an RHRS pump low flow alarm (on autoclosure of the RHRS suction valves) or from the high pressure alarm on the RHRS suction valves (in the modification case only), the operator will stop the extra running pump (either an SI or charging pump). If the operator stops the running pump, the overpressure event is halted.

7. Operator Opens a PORV (OA2): Given an alarm, if no or one relief valve operates successfully and the pressure still continues to rise, the operator may open a PORV in order to reduce the pressure. The operator may also open a PORV if he fails to stop the running pump in order to increase the time available to mitigate the transient.

8. RHRS Relief Valve Reseats (RVR): Given that the RHRS relief valve successfully operates and the transient was terminated, the relief valve must reseat or coolant would be lost to the PRT. If the transient is not stopped, the relief valve will cycle open and closed and is assumed to eventually fail open.

9. Pressurizer PORVs Reseat (POR): Given that one or more of the PORVs has opened and the transient has been stopped, the valve must close in order to avert a loss of coolant condition. If the transient is not stopped, the valve(s) will cycle until failure occurs.

For each of these nodes, failure probabilities were calculated. These nodal probability calculations are shown in Table D-7 for Salem.

The success criteria for the event trees was determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. For the charging/safety injection pump actuation case, because the charging pump maximum flow rate and the safety injection pump maximum flow rate combined is 1200 gpm (conservative assumption that both pumps operate at maximum flow rates), it was assumed that two PORVs or one PORV and one RHR relief valve are required to mitigate the transient. The following assumptions were also utilized in the analysis of the charging/safety injection mass input transient:

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves (based on the average time for a refueling outage).

Figure D-1 illustrates the event tree for Salem for the charging/safety injection initiating event.

The success criteria for the letdown isolation cases was also determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. Because the charging pump's maximum flow rate is 550 gpm, it was assumed that only RHR relief valve, or one PORV must operate to mitigate the transient. The following assumptions were utilized in the letdown isolation case.

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves.

The event tree for the letdown isolation cases is similar to the charging/safety injection pump actuation event tree. However, the success criteria for the various nodes is changed due to the type of transient. The event tree for the letdown isolation cases are shown in Figures D-2 and D-3.

The results from the quantification of the event trees for Salem are shown in Tables D-9 to D-11. The results show that most of the overpressure consequence categories remain unchanged with deletion of the autoclosure interlock. For the charging/safety injection case, consequence categories MSFO, MSCO, and HOPV increased. However, the increase is in the range of 1E-10 to 1E-11/shutdown year. This is a very insignificant increase in the frequency of these events. For the letdown isolation - RHR operable case, the consequence category MSCI decreased slightly while the HOPV category increased to 1.5E-11/shutdown year. In the letdown isolation - RHR isolated case, the consequence categories affected all decreased due to the reduction in the initiating event frequency. The conclusion to be drawn from the results is that the removal of the autoclosure interlock has a small impact on overpressurization transients for Salem.

TABLE D-7

SALEM NODAL PROBABILITY CALCULATIONS

1. RHR Isolated (RI)

Description: This node divides into two branches. The upper branch indicates that the RHR System is isolated from the RCS while the bottom branch indicates that the RHR System is open to the RCS. For this node, it was assumed that the RHR System may be isolated for a period of time during cold shutdown. The nodal probabilities for the charging/safety injection actuation case are based on assumptions that the one RHR inlet line would be isolated only 10 percent of the time. Thus, the RHR System would be open 90 percent of the time. For the letdown isolation case with the RHR operable, the nodal probability is 1.0 while for the case with the RHR isolated, the nodal probability is 0.0.

Failure probabilities: The probabilities for this node for each case are shown below:

Charging/Safety Injection pump actuation

Both trains isolated	0.10
No trains isolated	0.90

Letdown Isolation

RHR operable	1.0
RHR isolated	0.0

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

2. RHR Relief Valve Operates (RV)

Description: This node divides into two branches. When the RHR inlet line is open to the RCS, the one operable RHR relief valve can open (the top branch) or can fail to open (the bottom branch).

The RHR relief valves are spring-loaded relief valves set to actuate at 375 psig. Each relief valve can relieve 840 gpm at 375 psig.

Failure probabilities: The failure of a relief valve to open is 3E-04 per demand. Thus the probability for this node are:

One (of 1) RHR relief valve fails to open = 3E-04

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

3. POPS system operates at P=375 psig (POP)

Description: The event tree divides into three branches at the POP node. The top branch symbolizes that both trains of POPS operate, the middle branch shows only one train of POPS operates while the bottom branch signifies both trains of POPS have failed to operate.

The POPS (pressurizer overpressure protection system) utilizes two pressurizer relief valves (PORVs). The operator must enable the system when the cold leg RCS temperature is less than 312°F. An alarm is actuated thereby alerting the operator to arm the POPS. The isolation valves for the PORVs are automatically opened when the operator arms the POPS system. The POPS setpoint was 375 psig).

Failure probabilities: The failure probabilities associated with this node were calculated utilizing fault trees. Figure D-6 shows the fault tree developed for two trains of POPS failing to operate while the failure of one train is shown in Figure D-7. The operator error in failing to enable the POPS system is shown below:

Task: Operator fails to arm the POPS via procedures.

1. Ommission error

Median HEP = 0.003 Error factor = 3 Mean HEP = 3.75E-03	Table 20-7	When procedures with checkoff provisions are correctly used-long list, > 10 items

2. Commission error

Median HEP = 0.001 Error factor = 10 Mean HEP = 1.25E-03	Table 20-12	Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups

3. Recovery factor

Median HEP = 0.1 Error factor = 5 Mean HEP = 0.161	Table 20-22	Checker fails to detect error by others - routine tasks

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

3. POPS system operates at P=375 psig (POP) (Cont)

P(operator fails to arm POPS) = 3.75E-03(0.161) + (1-3.75E-03)(1.25E-03)(0.161)
= 6.04E-04 + 2.00E-04
= 8.04E-04

The basic event probabilities utilized in the fault trees are shown in Table D-8. The failure probabilities quantified from the fault trees is:

Two trains of POPS Fail = 3.01E-04
Cne train of POPS Fails = 1.18E-02

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

4a) RHR Suction Valves Close at P-700 psig (')

Description: The node determines whether or not the RHR suction valve autoclosure interlock closes the valves when the RCS pressure reaches 700 psig. For Salem, it was assumed that only one valve of the two isolation valves must close for success. Failure was considered to be the RHRS open to the RCS (i.e. the autoclosure interlock failed to close one of two valves).

Failure probabilities: The failure probability associated with this node was calculated using the fault tree shown in Figure D-4. The basic event probabilities used to quantify the fault tree are shown in Table D-8. The failure probability for this node is:

RHR suction valves fail to isolate = 1.80E-07

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

4b) Operator Isolates RHR System Given Overpressure Alarm (OD)

Description: The proposed modification deletes the autoclosure interlock and adds an alarm to alert the operate when the pressure exceeds the high pressure setpoint and an isolation valve is in the open position. Given an overpressure transient and this alarm the operator will close at least one RHR suction valve on the drop line to isolate the RHR system. The probability of operator failure is conditional on the time he has in which to act. If a mitigating system operates successfully (a PORV or RHR relief valve opens), it was assumed that the operator has 20 minutes in which to act. If no mitigating system operates, the operator has approximately 10 minutes to act.

Failure Probabilities: The failure probability associated with this node was calculated utilizing the fault tree shown in Figure D-5. The operator error probabilities shown in the fault tree are calculated below:

TASK: Operator closes isolation valve given high pressure alarm.

1. Diagnosis within time T by control room personnel of abnormal event annunciated

Median HEP	= 0.1	within 10 minutes	Table 20-3
Error Factor	= 10		
Mean HEP	= 0.266		

Median HEP	= 0.01	within 20 minutes	Table 20-3
Error factor	= 10		
Mean HEP	= 2.66E-02		

2. Operator failure in operating manual controls

Median HEP	= 0.001	Table 2-12	Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups
Error factor	= 10		
Mean HEP	= 1.25E-03		

3. Recovery factor - special short term one-of-a-kind checking

Median HEP = 0.05	Table 20-22
Error factor = 5	
Mean HEP = 8.07E-02	

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

P(Fail in 20 minutes) =
2.66E-02(8.07E-02) +
(1-2.66E-02)(1.25E-03)(8.07E-02)
= 2.15E-03 + 9.82E-05
= 2.25E-03

P(Fail in 10 minutes) =
0.266(8.07E-02) +
(1-0.266)(1.25E-03)(8.07E-02)
= 2.15E-02 + 7.40E-05
= 2.16E-02

The basic event probabilities are shown in Table D-8. The results of the quantification of the fault trees is shown below:

Operator Isolates RHR in 20 minutes = 5.72E-06
Operator Isolates RHR in 10 minutes = 4.73E-04

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

5. Operator Secures Running Pump (OA1)

Description: For any operator action to occur, an alarm must be actuated. This alarm can occur by actuation of a relief valve (PORV or RHR), RHRS pump low flow or high pressure alarm or in the modification case, the high pressure alarm on the RHR suction valves. For the charging/safety injection actuation case, this pump is the safety injection pump. In the letdown isolation case, the charging pump must be stopped.

Failure Probability: The human error probability is calculated below:

1. Failure to diagnose transient in time T

Median HEP = 0.1	within 20 minutes	Table 20-1
Error factor = 10		
Mean HEP = 0.266		

2. Select wrong control

Median HEP = 0.001	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls arranged in well-delineated functional groups
Error factor = 3		
Mean HEP = 1.25E-03		

P(Fail in 20 minutes) = 0.266 + (1-0.266)(1.25E-03)
= 0.267

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

6. Operator Opens PORV (OA2)

Description: If the mass input is greater than the relieving capacity or if no relief valve operates, the operator can open a PORV to reduce the pressure, given an alarm has actuated. If the operator fails to secure the pump, he can open a PORV in order to increase the time he has available in which to act.

Failure Probabilities: This action was modelled as dependent on the operator's success or failure to stop the running pump. The failure probabilities are:

Given failure of previous task

CP = 0.36	Table 20-18	Medium dependence

Given success of previous task

CP = 0.21	Table 20-19	Medium dependence

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

7. RHR Relief Valve Reseats (RVR)

Description: Given that the transient is successfully mitigated, the RHR relief valve must reseat (close) in order to prevent a loss of coolant.

Failure Probability: The probability that the relief valve will not reseat is 3E-2 per demand. Thus the failure probability is:

One relief valve fails to close = 3E-02

TABLE D-7 (Cont)

SALEM NODAL PROBABILITY CALCULATIONS

8. PORVs Reseat (POR)

Description: Given that the transient is successfully mitigated, the PORVs must close in order to prevent a loss of coolant. If the PORVs fail to close, the operator can isolate the open PORV using the associated block valve.

Failure Probability: The failure probability for both PORVs to reseat was calculated utilizing the fault tree shown in Figure D-8. The basic event probabilities are shown in Table D-8. The human error calculation for the operator failing to close the block valve is shown below:

TASK: Operator close block valve

1. Operator Fails to detect leaking PORV

Median HEP = 0.001 Error factor = 3 Mean HEP = 1.25E-03	Table 20-11	Error of commission in check reading display (digital indicators)

2. Operator selects wrong control

Median HEP = 0.001 Error Factor = 3 Mean HEP = 1.25E-03	Table 20-12	Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups

3. Recovery factor - special short term one-of-a-kind checking

Median HEP = 0.05 Error factor = 5 Mean HEP = 8.07E-02	Table 20-22

P(Fail to close block valve) = 1.25E-03(8.07E-02) +
(1-1.25E-03)(1.25E-03)(8.07E-02)
= 1.01E-04 + 1.01E-04
= 2.02E-04

Thus, the failure probabilities for the node are:

Both PORVS fail to close = 5.28E-05
One PORV fails to close = 2.64E-05

TABLE D-8

SALEM BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1RHFU30PHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHFU30PHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHFU30PHC	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHCN9CPHA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHCN9CPHB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHCN9CPHC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHOL49PHA	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1RHOL49PHB	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1RHOL49PHC	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1RHCB8	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
1RHCT230	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
1RHFU15A1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHFU15A2	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1RHOLCN49	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHRECO9C	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
1RHRECN90	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RHQS17	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
1RHCN9XC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHCN9C	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RHRECO9XC	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
IVPC403R	IV	I-E CONVERTER ALL FA	2.000E-07	1.200E+01	2.40E-06
IVPM403R	IV	I-E CONVERTER ALL FA	2.000E-07	1.200E+01	2.40E-06

TABLE D-8 (Cont)
SALEM BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
TPRS403	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
PSPQ403	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
STCT403	ST	TOGGLE SWITCH ALL MO	2.330E-07	1.200E+01	2.80E-06
TP403	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
1RECO63Y	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
1RECN63Y	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
BI403B	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
1PS118VAC	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
CM403AB	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
2RHFU30PHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2RHFU30PHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2RHFU30PHC	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2RHCN9CPHA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2RHCN9CPHB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2RHCN9CPHC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2RHOL49PHA	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2RHOL49PHB	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2RHOL49PHC	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2RHCB8	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
2RHCT230	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
2RHFU15A1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06

TABLE D-8 (Cont)

SALEM BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2RHFU15A2	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2RHOLCN49	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2RHRECO9C	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2RHRECN90	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2RHQS17	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
2RHCN9XC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2RHCN9C	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2RHRECO9XC	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
IVPC405R	IV	I-E CONVERTER ALL FA	2.000E-07	1.200E+01	2.40E-06
IVPM405R	IV	I-E CONVERTER ALL FA	2.000E-07	1.200E+01	2.40E-06
TPRS405	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
PSPQ405	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
STCT405	ST	TOGGLE SWITCH ALL MO	2.330E-07	1.200E+01	2.80E-06
TP405	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
2RECO63Y	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
2RECN63Y	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
BI405B	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
2PS118VAC	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
CM405AB	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
OPARMPOPS	OE	OPERATOR FAILS TO AR	8.040E-04	---	8.04E-04
AV1PR1F	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03

TABLE D-8 (Cont)

SALEM BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
AV1PR1SIG	TP	P TRANSMITTER ALL MO	1.730E-06	5.040E+02	8.72E-04
AV1PR2F	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
AV1PR2SIG	TP	P TRANSMITTER ALL MO	1.730E-06	5.040E+02	8.72E-04
AV1PR1K	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
MV1PR6K	MV	FAILURE TO CLOSE	1.000E-05	5.040E+02	5.04E-03
OPMV1PR6	OE	OPERATOR FAIL BLOCK	2.020E-04	---	2.02E-04
AV1PR2K	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
MV1PR7K	MV	FAILURE TO CLOSE	1.000E-05	5.040E+02	5.04E-03
OP1PR7	OE	OPERATOR FAIL BLOCK	2.020E-04	---	2.02E-04

TABLE D-9

SALEM
CHARGING/SAFETY INJECTION ACTUATION
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	8.91E-02	8.91E-02	-
LSFO	2.47E-03	2.47E-03	-
LSCI	0	0	-
LSCO	0	0	-
LLFO	4.30E-06	4.30E-06	-
LLCO	3.00E-02	3.00E-02	-
LLCI	3.30E-03	3.30E-03	-
LSFI	3.95E-13	9.38E-12	+9E-12
LLFI	4.82E-07	4.82E-07	-
MSFO	2.63E-12	8.34E-11	+8.1E-11
MLFO	0	0	-
MSFI	7.74E-05	7.74E-05	-
MLFI	0	0	-
MSCO	4.54E-12	1.44E-10	+1.4E-10
MSCI	5.56E-05	5.56E-05	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	1.45E-05	1.45E-05	-
HOPI	1.96E-05	1.96E-05	-
HOPV	5.10E-15	1.34E-11	+1.3E-11
TOTAL	1.25E-01	1.25E-01	

TABLE D-10

SALEM
LETDOWN ISOLATION RHR OPERABLE
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	8.89E-02	8.89E-02	-
LSFO	2.75E-03	2.75E-03	-
LSCI	0	0	-
LSCO	3.34E-02	3.34E-02	-
LLFO	1.43E-09	1.43E-09	-
LLCO	9.89E-06	9.89E-06	-
LLCI	0	0	-
LSFI	4.81E-13	4.81E-13	-
LLFI	0	0	-
MSFO	0	0	-
MLFO	0	0	-
MSFI	0	0	-
MLFI	0	0	-
MSCO	0	0	-
MSCI	5.38E-09	5.37E-09	-1E-11
MLCO	0	0	-
MLCI	0	0	-
MOPI	4.84E-09	4.84E-09	-
HOPI	3.02E-09	3.02E-09	-
HOPV	5.66E-15	1.49E-11	+1.5E-11
TOTAL	1.25E-01	1.25E-01	

TABLE D-11

SALEM
LETDOWN ISOLATION RHR ISOLATED
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	3.26E-01	1.63E-01	-1.63E-01
LSFO	0	0	-
LSCI	1.40E-03	6.99E-04	-7E-04
LSCO	0	0	-
LLFO	0	0	-
LLCO	0	0	-
LLCI	1.17E-01	5.85E-02	-5.8E-02
LSFI	1.02E-07	5.07E-08	-5.1E-08
LLFI	1.70E-05	8.48E-06	-8.5E-06
MSFO	0	0	-
MLFO	0	0	-
MSFI	0	0	-
MLFI	0	0	-
MSCO	0	0	-
MSCI	0	0	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	0	0	-
HOPI	3.73E-04	1.86E-04	-1.9E-04
HOPV	0	0	-
TOTAL	4.45E-01	2.22E-01	

FIGURE D-1
SALEM CHARGING/SAFETY INJECTION EVENT TREE

FIGURE D-2
SALEM LETDOWN ISOLATION RHR OPERABLE EVENT TREE

FIGURE D-3
SALEM LETDOWN ISOLATION RHR ISOLATED EVENT TREE

OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 2

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH

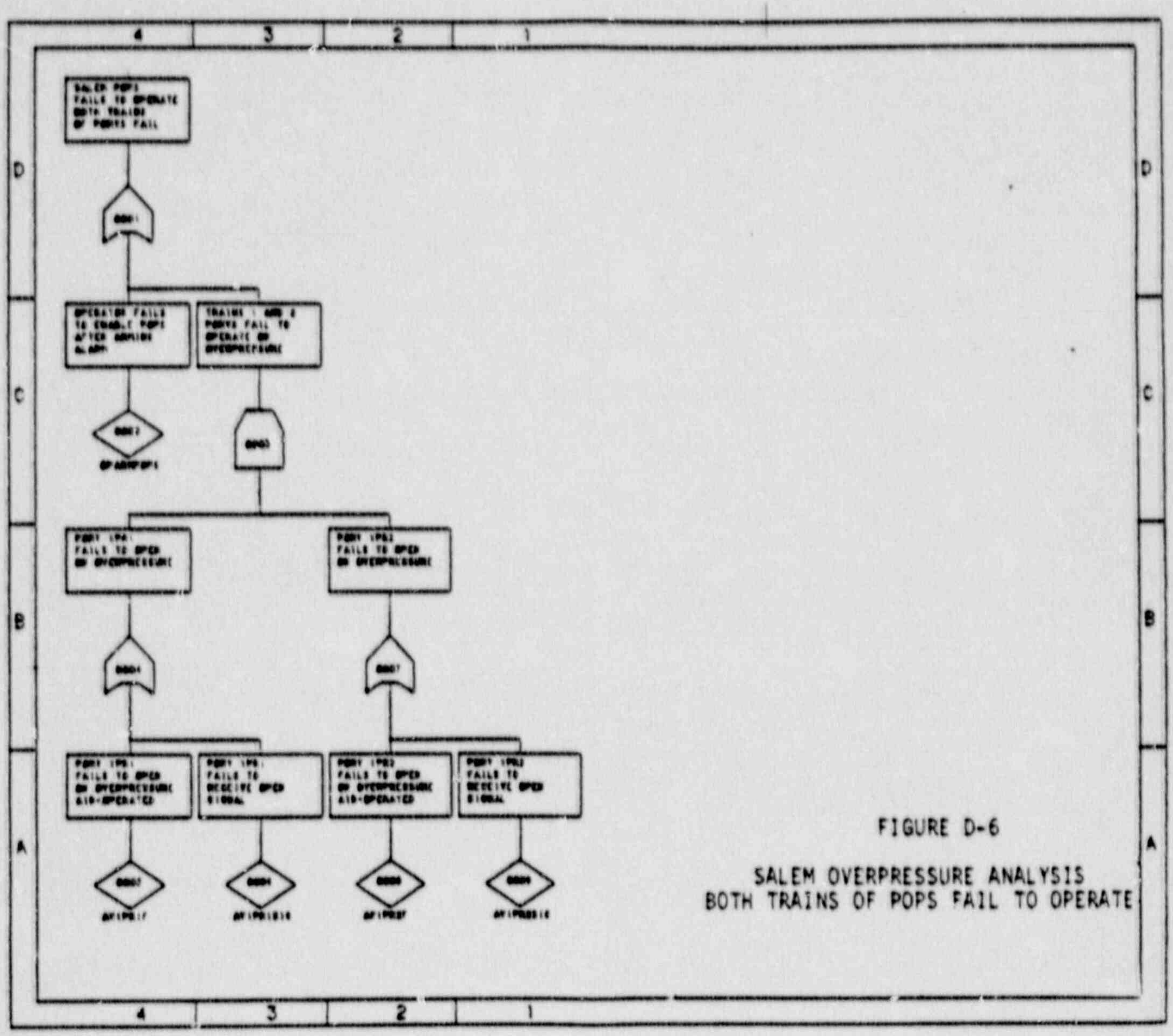


FIGURE D-6

SALEM OVERPRESSURE ANALYSIS
BOTH TRAINS OF POPS FAIL TO OPERATE

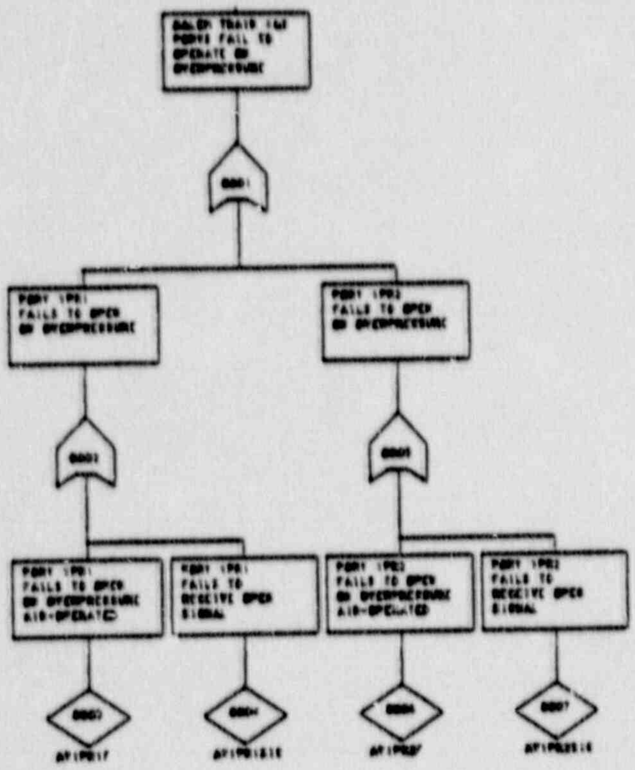


FIGURE D-7

SALEM OVERPRESSURE ANALYSIS
ONE OF TWO TRAINS OF POPS FAILS

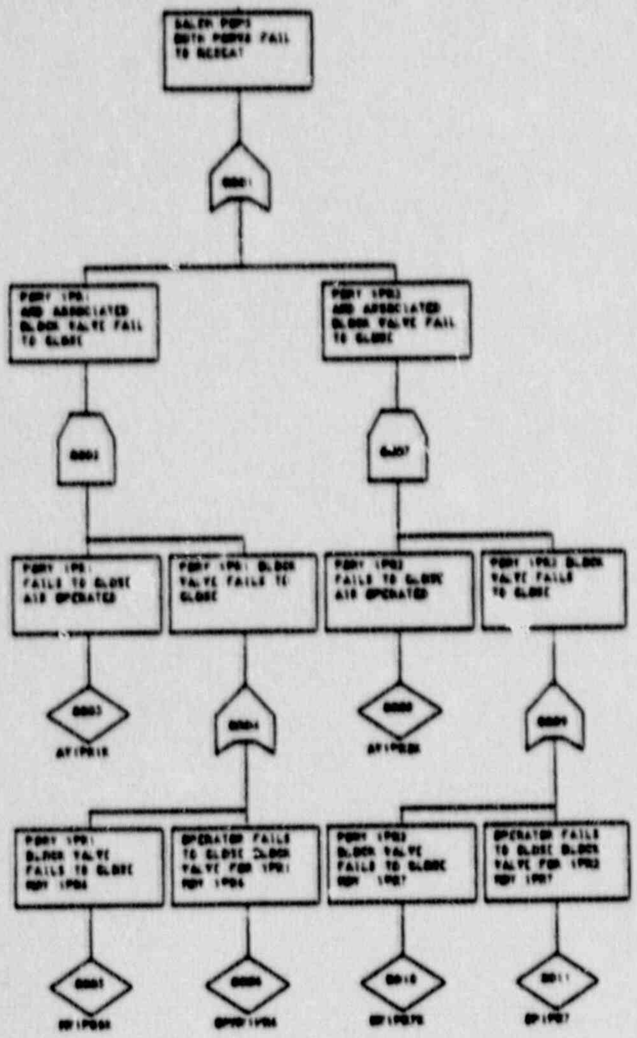


FIGURE D-8

SALEM OVERPRESSURE ANALYSIS
BOTH PORVS FAIL TO RESEAT

D.3.2 CALLAWAY

The effect of the overpressure transients identified in Section D.2 for Callaway was evaluated utilizing event trees. Each mitigating system and operator action was modeled as a top node on the event tree for the given transient. The following describe the event tree structure, the success criteria definod for each transient, and the nodal probabilities utilized in the quantification and the results.

The safety functions, i.e. the event tree top events or nodes, for the Callaway event trees are defined below:

1. Initiating Event (IE): The mass input initiator that could lead to overpressurization and/or possible RHRS damage, either charging/safety injection pump actuation or letdown isolation.

2. RHRS isolated (RI): The RHRS will be isolated during certain periods of shutdown. This dictates whether or not the RHRS relief valve is available to mitigate the transient and if the possibility exists for damage to the RHRS. For Callaway, the event tree allows for both trains of RHRS to be isolated, one train or no trains.

3. RHRS Suction Relief Valve Lifts (RV): If the RHRS is not isolated, the spring loaded relief valves will open at the setpoint pressure. If one trair of RHRS is isolated, only one RHR relief valve is available and if both trains are isolated, there are no RHR relief valves available to mitigate the transient.

4. COPS System Operates (COP): The cold overpressure protection system consists of two redundant and independent systems utilizing the pressurizer PORVs. When the system is enabled and reactor coolant temperature is below 368°F, a high pressure signal (above the COPS setpoint) will trip the system automatically and open a PORV until the pressure drops below the reset value. For Callaway, the COPS system has a variable setpoint. An auctioneered system temperature is

continuously converted to an allowable pressure and then compared to the actual RCS pressure. The system logic will first annunciate a main control board alarm whenever the measured pressure approaches within a predetermined amount of the allowable pressure. On a further increase in measured pressure, an actuation signal is transmitted to the power-operated relief valve. For this analysis, it was assumed that the COPS would actuate at its lowest setpoint (530 psig). The cases examined are two PORVs actuate, one PORV actuates or no PORVs actuate.

5a. RHRS Suction/Isolation Valves Automatically Close (RSV): When the pressure increases to the autoclosure setpoint (682 psig), the autoclosure interlock receives a pressure signal that actuates the circuitry and closes the motor-operated valve. This node is addressed in the case with the autoclosure interlock only.

5b. Operator Detects Overpressure Alarm and Isolates the RHRS (OD): For the modification case, an alarm would sound when the pressure reached the high pressure setpoint. Through a revision in operating procedures, it is assumed that the operator will detect the overpressure and isolate the RHRS before the pressure reaches 150% of the RHRS design pressure.

6. Operator Secures Running Pump (OA1): Given an alarm, either by actuation from the RHRS relief valve opening to the pressurizer relief tank (PRT), or from the operation of at least one train of COPS, or from an RHRS pump low flow alarm (on autoclosure of the RHRS suction valves) or from the high pressure alarm on the RHRS suction valves (in the modification case only), the operator will stop the extra running pump (either an SI or charging pump). If the operator stops the running pump, the overpressure event is halted.

7. Operator Opens a PORV (OA2): Given an alarm, if no or one relief valve operates successfully and the pressure still continues to rise, the operator may open a PORV in order to reduce the pressure. The operator may also open a PORV if he fails to stop the running pump in order to increase the time available to mitigate the transient.

8. RHRS Relief Valve Reseats (RVR): Given that the RHRS relief valves successfully operate and the transient was terminated, the relief valve must reseat or coolant would be lost to the PRT. If the transient is not stopped, the relief valve will cycle open and closed and is assumed to eventually fail open.

9. Pressurizer PORVs Reseat (POR): Given that one or more of the PORVs has opened and the transient has been stopped, the valve must close in order to avert a loss of coolant condition. If the transient is not stopped, the valve(s) will cycle until failure occurs.

For each of these nodes, failure probabilities were calculated. These nodal probability calculations are shown in Table D-12 for Callaway.

The success criteria for the event trees was determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. For the charging/safety injection pump actuation case, because the charging pump maximum flow rate and the safety injection pump maximum flow rate combined is 1200 gpm (conservative assumption that both pumps operate at maximum flow rates), it was assumed that two PORVs or two RHR relief valves or one PORV and one RHR relief valve are required to mitigate the transient. The following assumptions were also utilized in the analysis of the charging/safety injection mass input transient:

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves.

Figure D-9 illustrates the event tree for Callaway for the charging/safety injection initiating event.

The success criteria for the letdown isolation cases was also determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. Because the charging pump's maximum flow rate is 550 gpm, it was assumed that only RHR relief valve, or one PORV must operate to mitigate the transient. The following assumptions were utilized in the letdown isolation case.

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves.

The event tree for the letdown isolation cases is similar to the charging/safety injection pump actuation event tree. However, the success criteria for the various nodes is changed due to the type of transient. The event trees for the letdown isolation cases are shown in Figures D-10 and D-11.

The results from the quantification of the event trees for Callaway are shown in Tables D-14 to D-16. The results show that most of the overpressure consequence categories remain unchanged with deletion of the autoclosure interlock. For the charging/safety injection case, consequence categories MSFO, MSCO, and HOPV increased. However, the increase is in the range of 1E-11 to 1E-12/shutdown year. This is a very insignificant increase in the frequency of these events. For the letdown isolation - RHR operable case, the consequence category LSCI decreased slightly while the HOPV category increased to 3E-15/shutdown year. In the letdown isolation - RHR isolated case, the consequence categories affected all decreased due to the reduction in the initiating event frequency. The conclusion to be drawn from the results is that the removal of the autoclosure interlock has a small impact on overpressurization transients.

Several factors that were not taken into account in the analysis but are worth mentioning are presented below. The following precautions are noted in the Callaway FSAR which are designed to reduce the chances of an overpressurization event.

1. If all reactor coolant pumps have stopped for more than five minutes during plant heatup and the reactor coolant temperature is greater than the charging and seal injection water temperature, a steam bubble will be formed in the pressurizer prior to restarting a reactor coolant pump. This precaution minimizes the pressure transient when the pump is started and the cold water previously injected by the charging pumps is circulated through the warmer reactor coolant components. The steam bubble will accommodate the resultant expansion as the cold water is rapidly warmed.

2. To preclude inadvertent emergency core cooling system actuation during heatup and cooldown, procedures requiring blocking the pressurizer pressure and low steam line pressure signal actuation logic at 1,900 psig.

3. During further cooldown, closure and power lockout of the accumulator isolation valves and power lockout of the nonoperating charging pumps and safety injection pumps will be performed at 1,000 psig, approximately 425°F RCS conditions.

4. The recommended procedure for periodic emergency core cooling system pump performance testing will be to test the pumps during normal power operation or at hot shutdown conditions. This precludes any potential for developing a cold overpressurization transient. Should cold shutdown testing of the pumps be desired, the test will be done when the vessel is open to the atmosphere.

5. SIS circuitry testing, if done during cold shutdown, requires RHRS alignment and nonoperating charging pump and safety injection pumps power lockout to preclude developing cold overpressurization transients.

TABLE D-12

CALLAWAY NODAL PROBABILITY CALCULATIONS

1. RHR Isolated (RI)

Description: This node divides into two branches. The upper branch indicates that the RHR system is isolated from the RCS while the bottom branch indicates that the RHR system is open to the RCS. For this node, it was assumed that the RHR system may be isolated for a period of time during cold shutdown. The nodal probabilities for the charging/safety injection actuation case are based on assumptions that both trains of RHR would be isolated only five percent of the time and one train would be isolated 10 percent of the time. Thus, both trains of RHR would not be isolated from the RCS 85 percent of the time. For the letdown isolation case with the RHR operable, the nodal probability is 1.0 while for the case with the RHR isolated, the nodal probability is 0.0.

Failure probabilities: The probabilities for this node for each case are shown below:

Charging/Safety Injection pump actuation

Both trains isolated	0.05
One train isolated	0.10
No trains isolated	0.85

Letdown Isolation

RHR operable	1.0
RHR isolated	0.0

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

2. RHR Relief Valve Operates (RV)

Description: This node divides into three branches if both trains of RHR are open to the RCS and into two branches if only one train of RHR is not isolated from the RCS. If both trains of RHR are open to the RCS, two RHR relief valves can operate (indicated by the top branch), one RHR relief valve can operate (indicated by the middle branch), or both relief valves can fail to open (indicated by the bottom branch). When only one train of RHR is open to the RCS, the one operable RHR relief valve can open (the top branch) or can fail to open (the bottom branch).

The RHR relief valves are spring-loaded relief valves set to actuate at 450 psig. Each relief valve can relieve 770 gpm at 450 psig and ≤200°F.

Failure probabilities: The failure of a relief valve to open is 3E-04 per demand. Thus the probabilities for this node are:

2 (of 2) RHR relief valves fail to open = (3E-04)(3E-04)=9E-08
One (of 2) RHR relief valve fails to open = 3E-04 +3E-04=6E-04
One (of 1) RHR relief valve fails to open = 3E-04

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

3. PORV COPS system operates at P=530 psig (COP)

Description: The event tree divides into three branches at the COP node. The top branch symbolizes that both trains of COPS operate, the middle branch shows only one train of COPS operates while the bottom branch signifies both trains of COPS have failed to operate.

The COPS (cold overpressure system) utilizes two pressurizer relief valves (PORVs). The operator must enable the system when the cold leg RCS temperature is less than 368°F. An alarm is actuated thereby alerting the operator to arm the COPS. The COPS has a variable pressure setpoint determined by the measured RTD temperature. For this analysis, the setpoint was assumed to be constant at 530 psig (the lowest setpoint allowed).

Failure probabilities: The failure probabilities associated with this node were calculated utilizing fault trees. Figure D-14 shows the fault tree developed for two trains of COPS failing to operate while the failure of one train is shown in Figure D-15. The operator error in failing to enable the COPS system is shown below:

Task: Operator fails to arm the COPS following alarm.

Median HEP	=0.0001	Table 20-23	Failure to initiate some kind of intended corrective action as required
Error Factor	= 10		
Mean HEP	= 2.66E-04		

The basic event probabilities utilized in the fault trees are shown in Table D-13. The failure probabilities quantified from the fault trees is:

Two trains of COPS Fail = 3.01E-04
One train of COPS Fails = 1.18E-02

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

4a) RHR Suction Valves Close at P=682 psig (RSV)

Description: The node determines whether or not the RHR suction valve autoclosure interlock closes the valves when the RCS pressure reaches 682 psig. For Callaway, it was assumed that only one valve on each train must close for success. Failure was considered to be both trains of RHR open to the RCS (i.e. the autoclosure interlock failed to close one valve on each train).

Failure probabilities: The failure probability associated with this node was calculated using the fault tree shown in Figure D-12. The basic event probabilities used to quantify the fault tree are shown in Table D-13. The failure probability for this node is:

Both trains of RHR fail to isolate = 2.23E-07
One train of RHR fails to isolate = 1.24E-07

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

4b) Operator Isolates RHR System Given Overpressure Alarm (OD)

Description: The proposed modification deletes the autoclosure interlock and adds an alarm to alert the operate when the pressure exceeds the high pressure setpoint and an isolation valve is in the open position. Given an overpressure transient and this alarm the operator will close at least one RHR suction valve on each drop line to isolate the RHR System. The probability of operator failure is conditional on the time he has in which to act. If a mitigating system operates successfully (a PORV or RHR relief valve opens), it was assumed that the operator has 20 minutes in which to act. If no mitigating system operates, the operator has approximately 10 minutes to act.

Failure Probabilities: The failure probabilities associated with this node were calculated utilizing the fault tree shown in Figure D-13. The operator error probabilities shown in the fault tree are calculated below:

TASK: Operator closes isolation valve given high pressure alarm.

1. Diagnosis within time T by control room personnel of abnormal event annunciated

Median HEP = 0.1 within 10 minutes Table 20-3
Error Factor = 10
Mean HEP = 0.266

Median HEP = 0.01 within 20 minutes Table 20-3
Error factor = 10
Mean HEP = 2.66E-02

2. Operator failure in operating manual controls

Median HEP = 0.001 Table 20-12 Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups
Error factor = 10
Mean HEP = 1.25E-03

3. Recovery factor - special short term one-of-a-kind checking

Median HEP = 0.05 Table 20-22
Error factor = 5
Mean HEP = 8.07E-02

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

4b) Operator Isolates RHR System Given Overpressure Alarm (OD)(Cont)

P(Fail in 20 minutes) =
2.66E-02(8.07E-02) +
(1-2.66E-02)(1.25E-03)(8.07E-02)
= 2.15E-03 + 9.82E-05
= 2.25E-03

P(Fail in 10 minutes) =
0.266(8.07E-02) +
(1-0.266)(1.25E-03)(8.07E-02)
= 2.15E-02 + 7.40E-05
= 2.16E-02

The basic event probabilities are shown in Table D-13. The results of the quantification of the fault trees is shown below:

Operator Isolates RHR in 20 minutes = 1.11E-05
Operator Isolates RHR in 10 minutes = 9.42E-04

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

5. Operator Secures Running Pump (OA1)

Description: For any operator action to occur, an alarm must be actuated. This alarm can occur by actuation of a relief valve (PORV or RHR), RHRS pump low flow or high pressure alarm or in the modification case, the high pressure alarm on the RHR suction valves. For the charging/safety injection actuation case, this pump is the safety injection pump. In the letdown isolation case, the charging pump must be stopped.

Failure Probability: The human error probability is calculated below:

1. Failure to diagnose transient in time T

Median HEP	= 0.1	within 20 minutes	Table 20-1
Error factor	= 10		
Mean HEP	= 0.266		

2. Select wrong control

Median HEP	= 0.001	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls arranged in well-delineated functional groups
Error factor	= 3		
Mean HEP	= 1.25E-03		

P(Fail in 20 minutes) = 0.266 + (1-0.266)(1.25E-03)
= 0.267

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

6. Operator Opens PORV (OA2)

Description: If the mass input is greater than the relieving capacity or if no relief valve operates, the operator can open a PORV to reduce the pressure, given an alarm has actuated. If the operator fails to secure the pump, he can open a PORV in order to increase the time he has available in which to act.

Failure Probabilities: This action was modelled as dependent on the operator's success or failure to stop the running pump. The failure probabilities are:

Given failure of previous task

CP = 0.36	Table 20-18	Medium dependence

Given success of previous task

CP = 0.21	Table 20-19	Medium dependence

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

7. RHR Relief Valve Reseats (RVR)

Description: Given that the transient is successfully mitigated, the RHR relief valve must reseat (close) in order to prevent a loss of coolant.

Failure Probability: The proba[illegible] that the relief valve will not reseat is 3E-2 per demand. If bo[illegible] relief valves actuated, both relief valves must close. Thus the failure probabilities are:

Both relief valves fail to close = 3E-02 +3E-02 = 6E-02
One relief valve fails to close = 3E-02

TABLE D-12 (Cont)

CALLAWAY NODAL PROBABILITY CALCULATIONS

8. PORV's Reseat (POR)

Description: Given that the transient is successfully mitigated, the PORVs must close in order to prevent a loss of coolant. If the PORVs fail to close, the associated block valves receive a signal to automatically close if the PORV fails to completely close, thus eliminating the need for operator action.

Failure Probability: The failure probability for both PORVs to reseat was calculated utilizing the fault tree shown in Figure D-16. The basic event probabilities are shown in Table D-13. The failure probabilities are:

Both PORVS fail to close = 5.08E-05
One PORV fails to close = 2.54E-05

TABLE D-13

CALLAWAY BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2ACN42C/A	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2ACB52	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
2AFU40APHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2AFU40APHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2AFU40APHC	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2AOL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2AOL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2AOL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2AMSCN42CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2AMSCN42CB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2AMSCN42CC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2AFU1APHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2AFU1APHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2ACT480120	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
2AFU2AMP	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2AOLCN49AB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2AOLCN49BB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2AOLCN49CC	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2AQSWS17	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
2ACN42OB	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
2AMSRECO42	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05

TABLE D-13 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2ALSZS8	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
2ACNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
RSPS403	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
CMPB403B	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
PSPQY403	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
BIPS403B	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
TPPT403	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
1ACN42C/A	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1ACB52	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
1AFU40APHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1AFU40APHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1AFU40APHC	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1AOL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1AOL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1AOL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1AMSCN42CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1AMSCN42CB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1AMSCN42CC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1AFU1APHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1AFU1APHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1ACT480120	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06

TABLE D-13 (Cont)

CALLAWAY BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1AFU2AMP	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1AOLCN49AB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1AOLCN49BB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1AOLCN49CB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1AQSWS17	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
1ACN420B	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
1AMSRECO42	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
1ALSZS8	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
1ACNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
RSPS405	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
CMPB405B	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
PSPQY405	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
BIPS405B	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
TPPT405	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
2BCN42CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2BCB52	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
2BFU40APHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2BFU40APHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2BFU40APHC	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2BOL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2BOL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06

TABLE D-13 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2BOL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2BMSCN42CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2BMSCN42CB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2BMSCN42CC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2BFU1APHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2BFU1APHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2BCT480120	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
2BFU2AMP	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2BOLCN49AB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2BOLCN49BB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2BOLCN49CB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2BQSWS17	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
2BCN420B	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
2BMSRECO42	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
2BLSZS8	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
2BCNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1BCN42CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1BCB52	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
1BFU40APHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1BFU40APHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1BFU40APHC	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06

TABLE D-13 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1BOL49A	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1BOL49B	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1BOL49C	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1BMSCN42CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1BMSCN42CB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1BMSCN42CC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1BFU1APHA	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1BFU1APHB	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1BCT480120	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
1BFU2AMP	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1BOLCN49AB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1BOLCN49BB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1BOLCN49CB	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1BQSWS17	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
1BCN420B	CN	MOTOR STARTER SPURIC	3.000E-08	1.200E+01	3.60E-07
1BMSREC042	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
1BLSZS8	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
1BCNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
OPARMCOPS	OE	OPERATOR FAILS TO AR	2.660E-04	---	2.66E-04
AVPCV455AF	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
AV455ASIG	TP	P TRANSMITTER ALL MO	1.730E-06	5.040E+02	8.72E-04

TABLE D-13 (Cont)
CALLAWAY BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
AVPCV456AF	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
AV456ASIG	TP	P TRANSMITTER ALL MO	1.730E-06	5.040E+02	8.72E-04
AVPCV455AK	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
MV455AK	MV	FAILURE TO CLOSE	1.000E-05	5.040E+02	5.04E-03
AVPCV456AK	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
MV456AK	MV	FAILURE TO CLOSE	1.000E-05	5.040E+02	5.04E-03

TABLE D-14

CALLAWAY
CHARGING/SAFETY INJECTION ACTUATION
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	8.67E-02	8.67E-02	-
LSFO	2.76E-04	2.76E-04	-
LSCI	0	0	-
LSCO	0	0	-
LLFO	4.67E-03	4.67E-03	-
LLCO	3.17E-02	3.17E-02	-
LLCI	1.66E-03	1.66E-03	-
LSFI	0	0	-
LLFI	2.32E-07	2.32E-07	-
MSFO	7.33E-14	6.54E-12	+6.5E-12
MLFO	0	0	-
MSFI	1.36E-05	1.35E-05	-1E-07
MLFI	0	0	-
MSCO	4.58E-14	4.08E-12	+4E-12
MSCI	7.74E-06	7.74E-06	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	5.82E-07	5.82E-07	-
HOPI	2.24E-06	2.24E-06	-
HOPV	1.41E-16	1.07E-12	+1.1E-12
TOTAL	1.25E-01	1.25E-01	

TABLE D-15

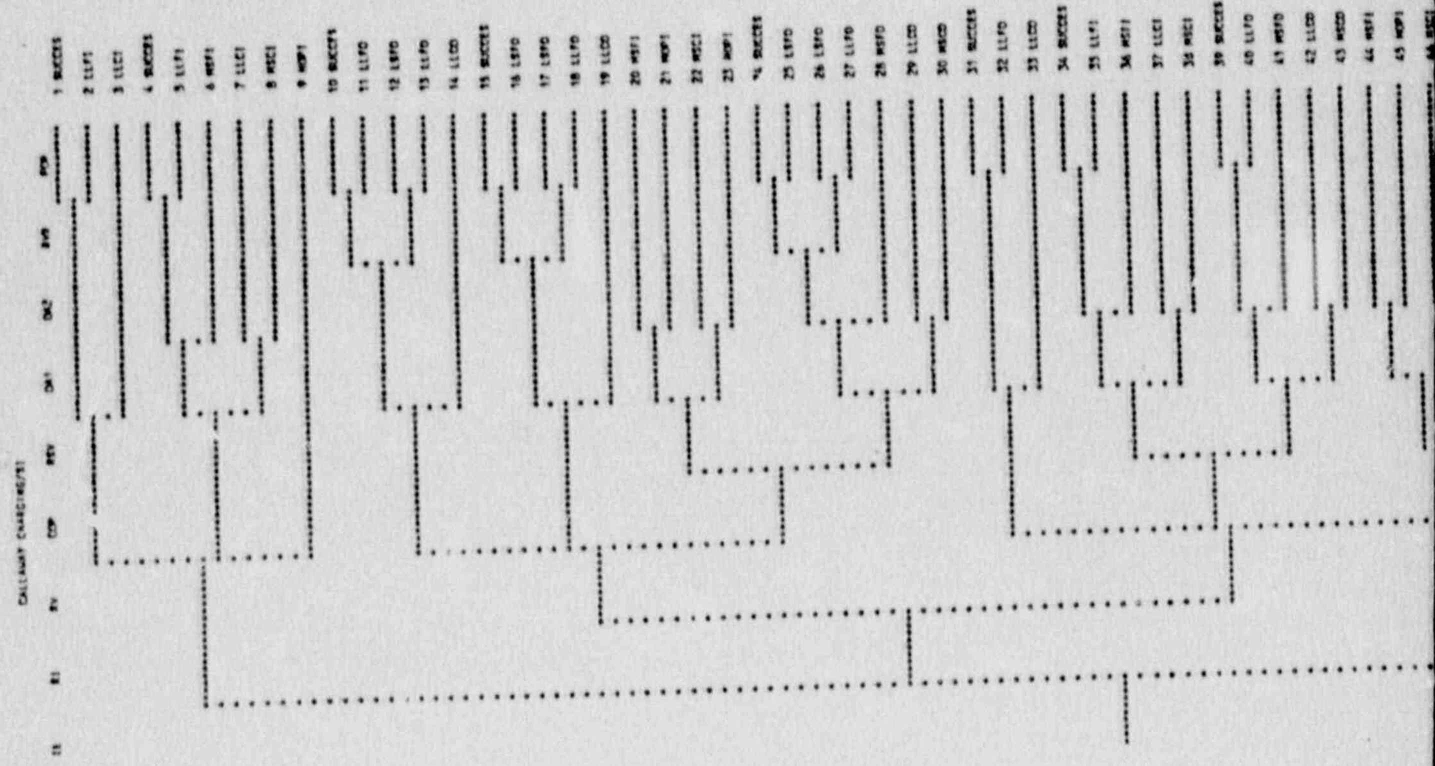
CALLAWAY
LETDOWN ISOLATION RHR OPERABLE
RESULTS

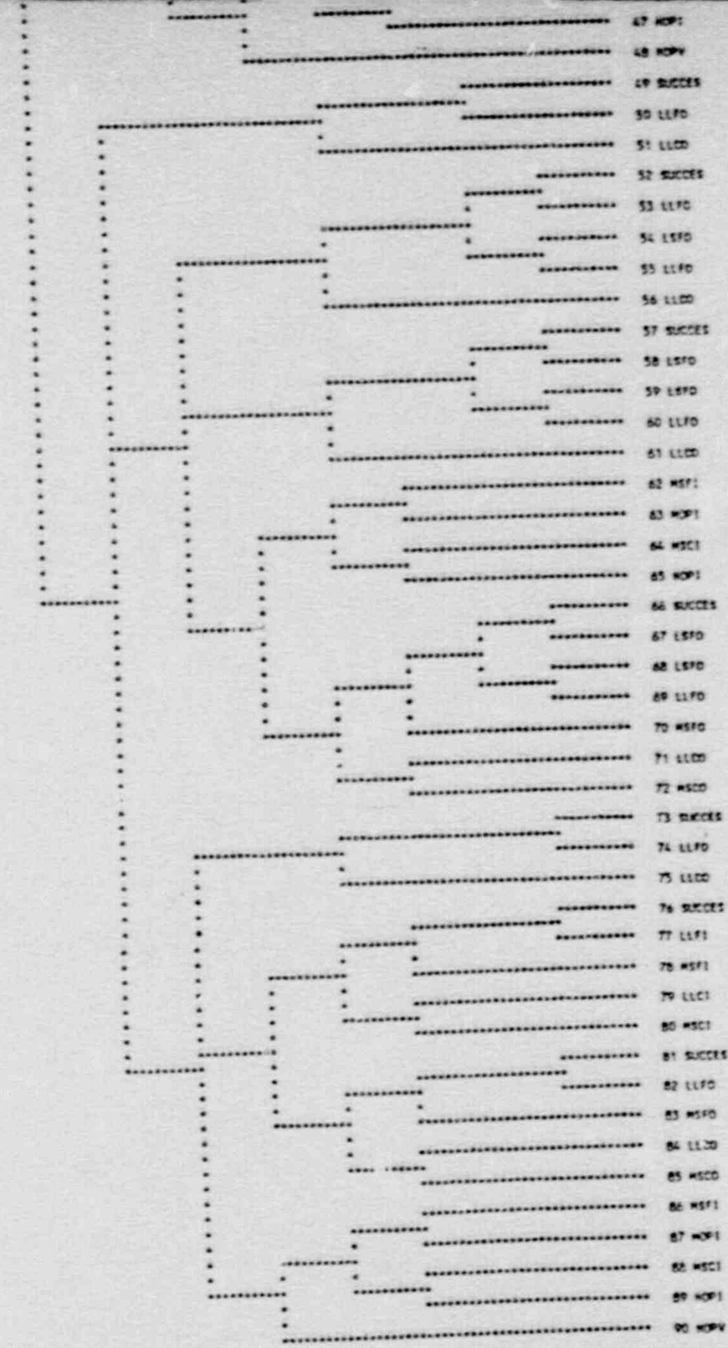
CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	8.61E-02	8.61E-02	-
LSFO	2.75E-06	2.75E-06	-
LSCI	5.79E-13	5.78E-13	-1E-15
LSCO	2.00E-05	2.00E-05	-
LLFO	5.49E-03	5.49E-03	-
LLCO	3.34E-02	3.34E-02	-
LLCI	0	0	-
LSFI	4.98E-17	4.98E-17	-
LLFI	0	0	-
MSFO	0	0	-
MLFO	0	0	-
MSFI	0	0	-
MLFI	0	0	-
MSCO	0	0	-
MSCI	0	0	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	5.21E-13	5.21E-13	-
HOPI	3.25E-13	3.25E-13	-
HOPV	7.55E-19	3.19E-15	+3.2E-15
TOTAL	1.25E-01	1.25E-01	

TABLE D-16

CALLAWAY
LETDOWN ISOLATION RHR ISOLATED
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	3.26E-01	1.63E-01	-1.63E-01
LSFO	0	0	-
LSCI	1.40E-03	6.99E-04	-7E-04
LSCO	0	0	-
LLFO	0	0	-
LLCO	0	0	-
LLCI	1.17E-01	5.86E-02	-5.8E-02
LSFI	9.76E-08	4.88E-08	-4.9E-08
LLFI	1.64E-05	8.17E-06	-8.2E-06
MSFO	0	0	-
MLFO	0	0	-
MSFI	0	0	-
MLFI	0	0	-
MSCO	0	0	-
MSCI	0	0	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	0	0	-
HOPI	1.34E-04	6.68E-05	-6.7E-05
HOPV	0	0	-
TOTAL	4.45E-01	2.22E-01	

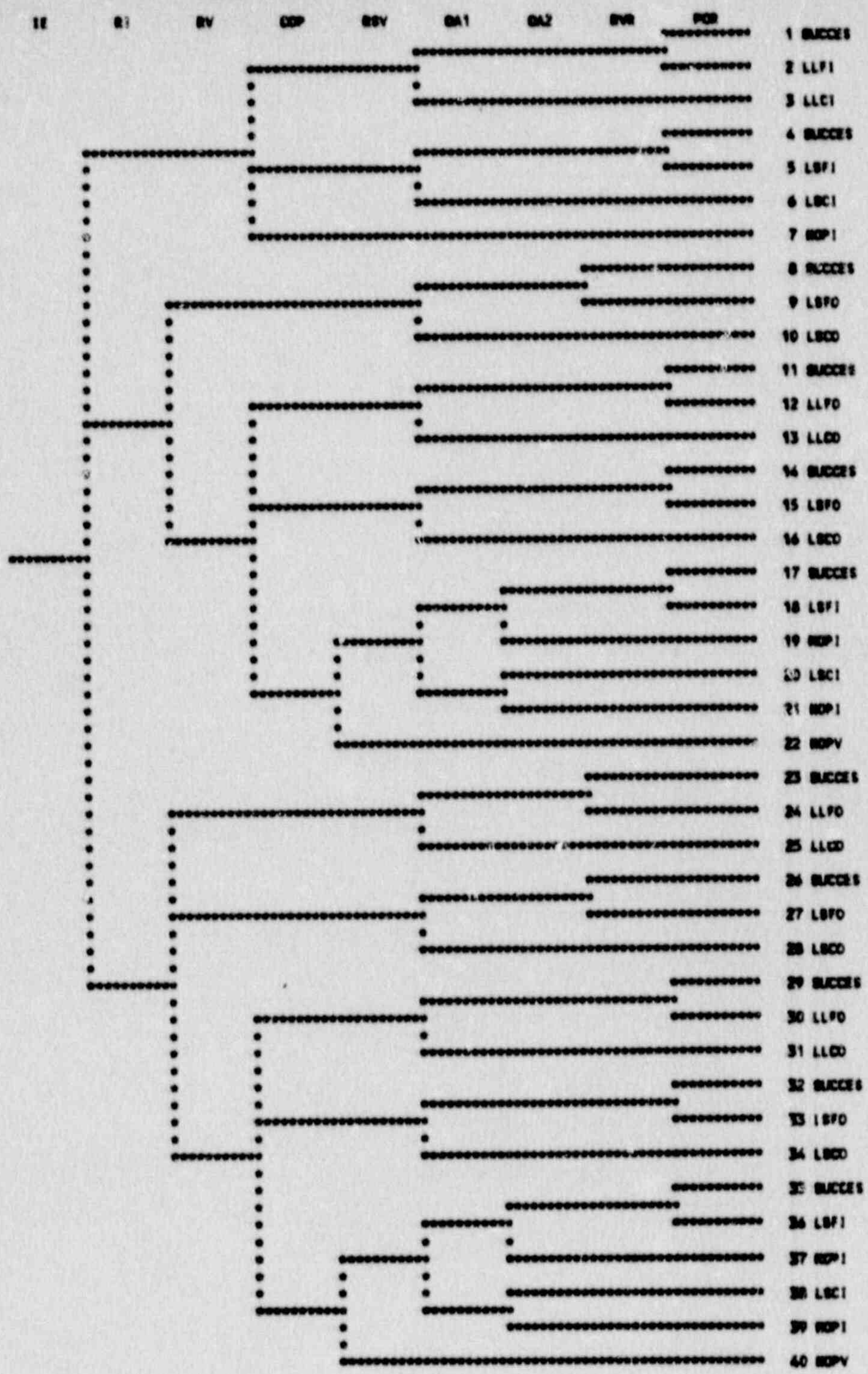




EVENT	EVENT NAME
IE	CHARGING/SI INJECTION
RI	RHRS ISOLATED
RV	RHR RELIEF VALVES LIFT
COP	OPS PORVS OPEN
RSV	RHR SUCTION VALVES CLOSE
OA1	OPERATOR STOPS PUMP
OA2	OPERATOR OPENS PORV
RVR	RHR RELIEF RESEATS
[illegible]	[illegible]

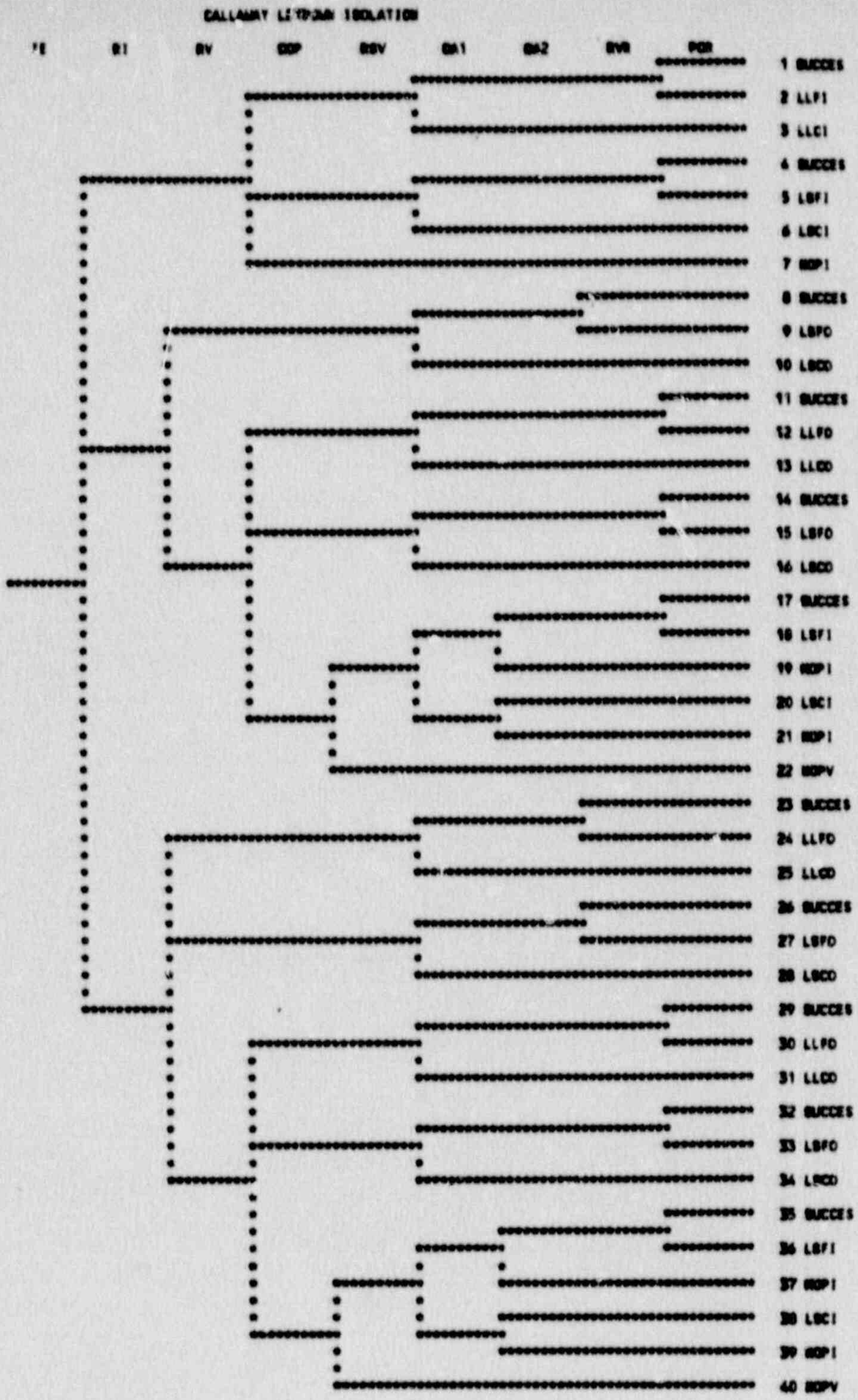
FIGURE D-9
CALLAWAY CHARGING/
SAFETY INJECTION EVENT TREE

CALLAWAY LETDOWN ISOLATION



EVENT	EVENT NAME
IE	LETDOWN ISOLATION
RI	RHRS ISOLATED
RV	RHR RELIEF VALVES LIFT
COP	OPS PORVS OPEN
RSV	RHR SUCTION VALVES CLOSE
OA1	OPERATOR STOPS PUMP
OA2	OPERATOR OPENS PORV
RVR	RHR RELIEF RESEATS
POR	PORVS RESEAT

FIGURE D-10
CALLAWAY LETDOWN ISOLATION
RHR OPERABLE EVENT TREE



EVENT EVENT NAME
IE LETDOWN ISOLATION
RI RHRS ISOLATED
RV RHR RELIEF VALVES LIFT
OOP OPS PORVS OPEN
RSV RHR SUCTION VALVES CLOSE
OA1 OPERATOR STOPS PUMP
OA2 OPERATOR OPENS PORV
RVR RHR RELIEF RESEATS
POR PORVS RESEAT

FIGURE D-11
CALLAWAY LETDOWN ISOLATION
RHR ISOLATED EVENT TREE

OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 2

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH

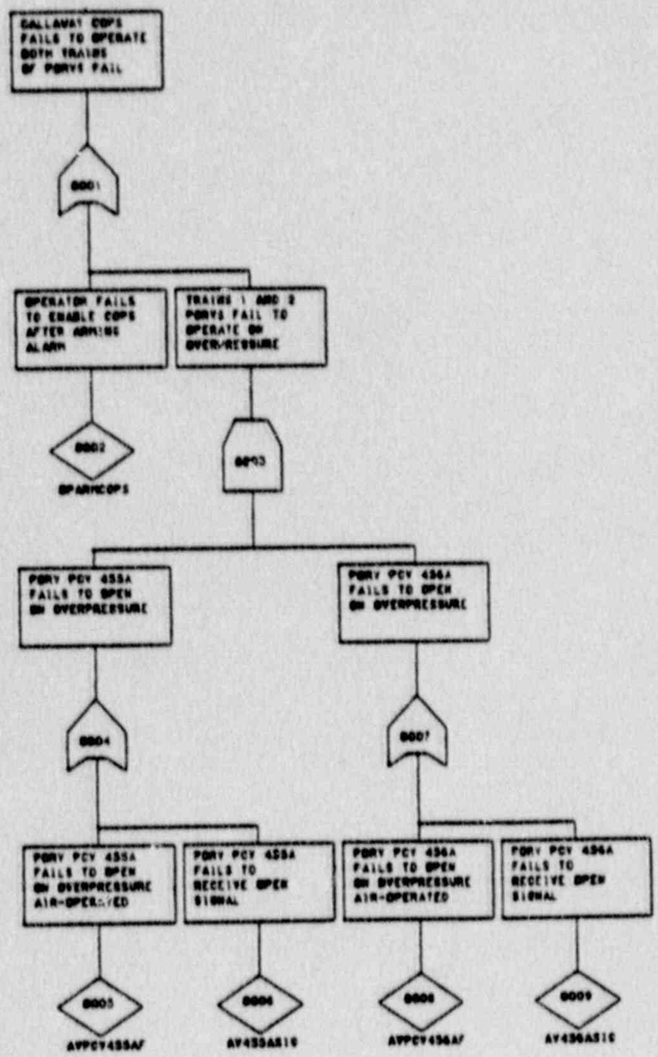


FIGURE D-14

CALLAWAY OVERPRESSURE ANALYSIS
BOTH TRAINS OF PORVS FAIL TO OPEN

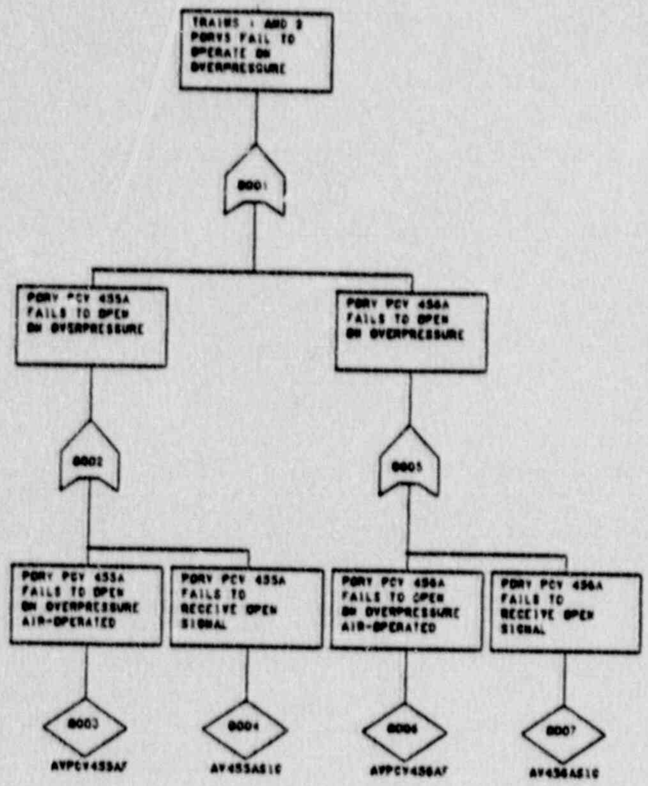


FIGURE D-15

CALLAWAY OVERPRESSURE ANALYSIS
ONE OF TWO PORVS FAIL TO OPEN

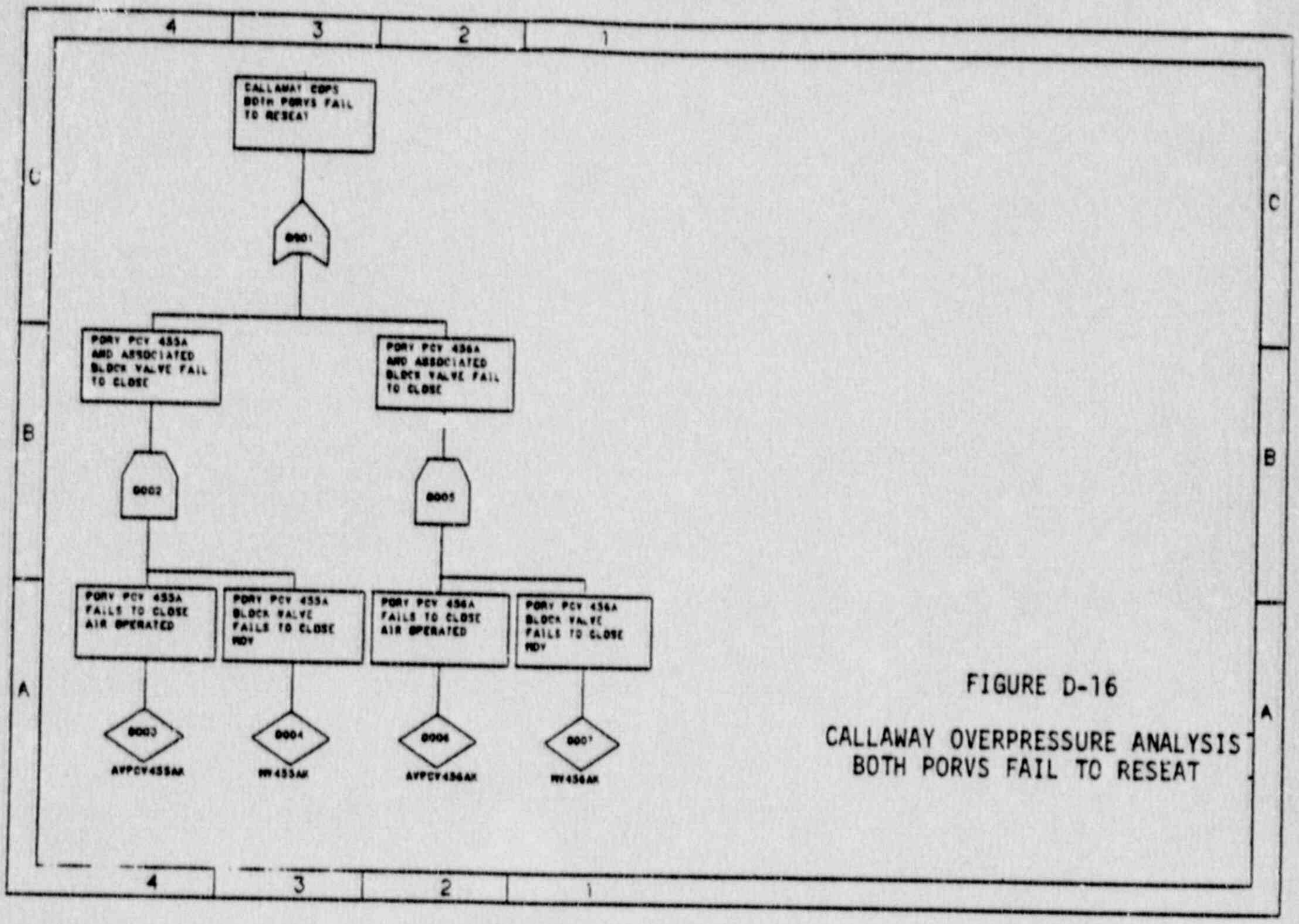


FIGURE D-16

CALLAWAY OVERPRESSURE ANALYSIS
BOTH PORVS FAIL TO RESEAT

D.3.3 NORTH ANNA

The effect of the overpressure transients identified in Section D.2 was evaluated utilizing event trees. Each mitigating system and operator action was modeled as a top node on the event tree for the given transient. The following describe the event tree structure, the success criteria defined for each transient, and the nodal probabilities utilized in the quantification and the results.

The safety functions, i.e. the event tree top events or nodes, for the North Anna event trees are defined below:

1. Initiating Event (IE): The mass input initiator that could lead to overpressurization and/or possible RHRS damage, either charging/safety injection pump actuation or letdown isolation.

2. RHRS isolated (RI): The RHRS will be isolated during certain periods of shutdown. This dictates whether or not the RHRS relief valve is available to mitigate the transient and if the possibility exists for damage to the RHRS.

3. OPS System Operates (OPS): The cold overpressure protection system consists of two redundant and independent systems utilizing the pressurizer PORVs. When the system is enabled and reactor coolant temperature is below 375°F, a high pressure signal (above the OPS setpoint) will trip the system automatically and open a PORV until the pressure drops below the reset value. For North Anna, the OPS system has two fixed setpoints. The system logic will first annunciate a main control board alarm whenever the measured pressure approaches within a predetermined amount of the allowable pressure. On a further increase in measured pressure, an actuation signal is transmitted to the power-operated relief valve. The cases examined are two PORVs actuate, one PORV actuates or no PORVs actuate.

4. RHRS Suction Relief Valve Lifts (RV): If the RHRS is not isolated, the spring loaded relief valves will open at the setpoint pressure.

5a. RHRS Suction/Isolation Valves Automatically Close (RSV): When the pressure increases to the autoclosure setpoint (582 psig), the autoclosure interlock receives a pressure signal that actuates the circuitry and closes the motor-operated valve. This node is addressed in the case with the autoclosure interlock only.

5b. Operator Detects Overpressure Alarm and Isolates the RHRS (OD): For the modification case, an alarm would sound when the pressure reached the high pressure setpoint. Through a revision in operating procedures, it is assumed that the operator will detect the overpressure and isolate the RHRS before the pressure reaches 150% of the RHRS design pressure.

6. Operator Secures Running Pump (OA1): Given an alarm, either by actuation from the RHRS relief valve opening to the pressurizer relief tank (PRT), or from the operation of at least one train of OPS, or from an RHRS pump low flow alarm (on autoclosure of the RHRS suction valves) or from the high pressure alarm on the RHRS suction valves (in the modification case only), the operator will stop the extra running pump (either an SI or charging pump). If the operator stops the running pump, the overpressure event is halted.

7. Operator Opens a PORV (OA2): Given an alarm, if no or one relief valve operates successfully and the pressure still continues to rise, the operator may open a POR' in order to reduce the pressure. The operator may also open a PORV if he fails to stop the running pump in order to increase the time available to mitigate the transient.

8. Pressurizer PORVs Reseat (POR): Given that one or more of the PORVs has opened and the transient has been stopped, the valve must close in order to avert a loss of coolant condition. If the transient is not stopped, the valve(s) will cycle until failure occurs.

9. RHRS Relief Valve Reseats (RVR): Given that the RHRS relief valve successfully operates and the transient was terminated, the relief valve must reseat or coolant would be lost to the PRT. If the transient is not stopped, the relief valve will cycle open and closed and is assumed to eventually fail open.

For each of these nodes, failure probabilities were calculated. These nodal probability calculations are shown in Table D-17 for North Anna.

The success criteria for the event trees was determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. For the charging/safety injection pump actuation case, because the maximum flow rate of two charging pumps is 1300 gpm (conservative assumption that both pumps operate at maximum flow rates), it was assumed that two PORVs or two RHR relief valves or one PORV and one RHR relief valve are required to mitigate the transient. The following assumptions were also utilized in the analysis of the charging/safety injection mass input transient:

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves.

Figure D-17 illustrates the event tree for North Anna for the charging/safety injection initiating event.

The success criteria for the letdown isolation cases was also determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. Because the charging pump's maximum flow rate is 650 gpm, it was assumed that only RHR relief valve, or one PORV must operate to mitigate the transient. The following assumptions were utilized in the letdown isolation case.

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves.

The event tree for the letdown isolation cases is similar to the charging/safety injection pump actuation event tree. However, the success criteria for the various nodes is changed due to the type of transient. The event trees for the letdown isolation cases are shown in Figures D-18 and D-19.

The results from the quantification of the event trees for North Anna are shown in Tables D-19 to D-21. The results show that most of the overpressure consequence categories remain unchanged with deletion of the autoclosure interlock. For the charging/safety injection case, consequence categories MSFO, MSCO, and HOPV increased. However, the increase is in the range of 1E-14 to 1E-15/shutdown year. This is a very insignificant increase in the frequency of these events. For the letdown isolation - RHR operable case, the HOPV consequence category increased to 4.5E-15/shutdown year. In the letdown isolation - RHR isolated case, the consequence categories affected all decreased due to the reduction in the initiating event frequency. The conclusion to be drawn from the results is that the removal of the autoclosure interlock has a small impact on overpressurization transients for North Anna.

Several factors that were not taken into account in the analysis but are worth mentioning are presented below. The following precautions are noted in the North Anna FSAR which are designed to reduce the chances of an overpressurization event.

1. The pressurizer pressure safety injection signal actuations are blocked when the reactor coolant system pressure decreases to less than 1990 psig.

2. The accumulator discharge motor-operated valves are closed when the pressure is below 1000 psig (approximately 950 psig). The breakers are de-energized and locked open.

3. When the RCS cold leg temperature is at 320°F, all but one (two pumps) charging pump is placed in pull-to-lock and one LHSI pump is placed in pull-to-lock.

4. When the RCS temperature is less than 200°F and the pressure is between 300-325 psig, the remaining low head injection pump is placed in the pull-to-lock position.

5. To start a reactor coolant pump while the reactor coolant system in in a water-solid condition, the operating procedures require: 1) special permission from the operating supervisor and 2) that the associated steam generator secondary-side bulk water temperature is not greater that 50°F above the reactor coolant system pressure.

TABLE D-17
NORTH ANNA NODAL PROBABILITY CALCULATIONS

1. RHR Isolated (RI)

Description: This node divides into two branches. The upper branch indicates that the RHR system is isolated from the RCS while the bottom branch indicates that the RHR system is open to the RCS. For this node, it was assumed that the RHR system may be isolated for a period of time during cold shutdown. The nodal probabilities for the charging/safety injection actuation case are based on assumptions that the one RHR inlet line would be isolated only 10 percent of the time. Thus, the RHR system would be open 90 percent of the time. For the letdown isolation case with the RHR operable, the nodal probability is 1.0 while for the case with the RHR isolated, the nodal probability is 0.0.

Failure probabilities: The probabilities for this node for each case are shown below.

Charging/Safety Injection pump actuation

Both trains isolated	0.10
No trains isolated	0.90

Letdown Isolation

RHR operable	1.0
RHR isolated	0.0

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

2. OPS system operates at P=345 psig (OPS)

Description: The event tree divides into three branches at the OPS node. The top branch symbolizes that both trains of OPS operate, the middle branch shows only one train of OPS operates while the bottom branch signifies both trains of OPS have failed to operate.

The OPS (overpressure protection system) utilizes two pressurizer relief valves (PORVs). The operator must enable the system when the RCS temperature is less than 375°F. For North Anna, the PORV setpoints are variable for each PORV. The setpoints are:

	$185°F<T_c<375°F$	$T_c<185°F$
PCV-1455C	415 psig	345 psig
PCV-1456	420 psig	350 psig

For this analysis, the OPS setpoint was assumed to be 345 psig for both PORVs.

Failure probabilities: The failure probabilities associated with this node were calculated utilizing fault trees. Figure D-22 shows the fault tree developed for two trains of OPS failing to operate while the failure of one train is shown in Figure D-23. The operator error in failing to enable the OPS system is shown below:

Task: Operator fails to arm the OPS via procedures.

1. Omission error

Median HEP = 0.003 Error factor = 3 Mean HEP = 3.75E-03	Table 20-7	When procedures with checkoff provisions are correctly used-long list, > 10 items

2. Commission error

Median HEP = 0.001 Error factor = 10 Mean HEP = 1.25E-03	Table 20-12	Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups

3. Recovery factor

Median HEP = 0.1 Error factor = 5 Mean HEP = 0.161	Table 20-22	Checker fails to detect error by others - routine tasks

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

2. OPS system operates at P=345 psig (OPS) (Cont)

P(operator fails to arm OPS) = 3.75E-03(0.161) +
(1-3.75E-03)(1.25E-03)(0.161)
= 6.04E-04 + 2.00E-04
= 8.04E-04

The basic event probabilities utilized in the fault trees are shown in Table D-18. The failure probabilities quantified from the fault trees is:

Two trains of OPS Fail = 8.39E-04
One train of OPS Fails = 1.18E-02

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

3. RHR Relief Valve Operates (RV)

Description: This node divides into three branches when the RHR is open to the RCS. Two RHR relief valves can operate (indicated by the top branch), one RHR relief valve can operate (indicated by the middle branch), or both relief valves can fail to open (indicated by the bottom branch).

The RHR relief valves are spring-loaded relief valves set to actuate at 467 psig. Each relief valve can relieve 900 gpm at 467 psig.

Failure probabilities: The failure of a relief valve to open is 3E-04 per demand. Thus the probability for this node are:

2 (of 2) RHR relief valves fail to open =(3E-04)(3E-04)=9E-08
One (of 2) RHR relief valve fails to open = 3E-04 +3E-04=6E-04

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

4a) RHR Suction Valves Close at P=582 psig (RSV)

Description: The node determines whether or not the RHR suction valve autoclosure interlock closes the valves when the RCS pressure reaches 582 psig. For North Anna, it was assumed that only one valve of the two isolation valves must close for success. Failure was considered to be the RHRS open to the RCS (i.e. the autoclosure interlock failed to close one of two valves).

Failure probabilities: The failure probability associated with this node was calculated using the fault tree shown in Figure D-20. The basic event probabilities used to quantify the fault tree are shown in Table D-18. The failure probability for this node is:

RHR suction valves fail to isolate = 1.43E-07

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

4b) Operator Isolates RHR System Given Overpressure Alarm (OD)

Description: The proposed modification deletes the autoclosure interlock and adds an alarm to alert the operate when the pressure exceeds the high pressure setpoint and an isolation valve is in the open position. Given an overpressure transient and this alarm the operator will close at least one RHR suction valve on the drop line to isolate the RHR system. The probability of operator failure is conditional on the time he has in which to act. If a mitigating system operates successfully (a PORV or RHR relief valve opens), it was assumed that the operator has 20 minutes in which to act. If no mitigating system operates, the operator has approximately 10 minutes to act.

Failure Probabilities: The failure probability associated with this node was calculated utilizing the fault tree shown in Figure D-21. The operator error probabilities shown in the fault tree are calculated below:

TASK: Operator closes isolation valve given high pressure alarm.

1. Diagnosis within time T by control room personnel of abnormal event annunciated

   Median HEP = 0.1 within 10 minutes Table 20-3
   Error Factor = 10
   Mean HEP = 0.266

   Median HEP = 0.01 within 20 minutes Table 20-3
   Error factor = 10
   Mean HEP = 2.66E-02

2. Operator failure in operating manual controls

   Median HEP = 0.001 Table 20-12 Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups
   Error factor = 10
   Mean HEP = 1.25E-03

3. Recovery factor - special short term one-of-a-kind checking

   Median HEP = 0.05 Table 20-22
   Error factor = 5
   Mean HEP = 8.07E-02

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

4b) Operator Isolates RHR System Given Overpressure Alarm (OD) (Cont)

P(Fail in 20 minutes) =
2.66E-02(8.07E-02) +
(1-2.66E-02)(1.25E-03)(8.07E-02)
= 2.15E-03 + 9.82E-05
= 2.25E-03

P(Fail in 10 minutes)=
0.266(8.07E-02) +
(1-0.266)(1.25E-03)(8.07E-02)
= 2.15E-02 + 7.40E-05
= 2.16E-02

The basic event probabilities are shown in Table D-18. The results of the quantification of the fault trees is shown below:

Operator Isolates RHR in 20 minutes = 5.87E-06
Operator Isolates RHR in 10 minutes = 4.74E-04

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

5. Operator Secures Running Pump (OA1)

Description: For any operator action to occur, an alarm must be actuated. This alarm can occur by actuation of a relief valve (PORV or RHR), RHRS pump low flow or high pressure alarm or in the modification case, the high pressure alarm on the RHR suction valves. For the charging pump actuation case and the letdown isolation case, the charging pump must be stopped.

Failure Probability: The human error probability is calculated below:

1. Failure to diagnose transient in time T

Median HEP	= 0.1	within 20 minutes	Table 20-1
Error factor	= 10		
Mean HEP	= 0.266		

2. Select wrong control

Median HEP	= 0.001	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls arranged in well-delineated functional groups
Error factor	= 3		
Mean HEP	= 1.25E-03		

P(Fail in 20 minutes) = 0.266 + (1-0.266)(1.25E-03)
= 0.267

0040D:1D/101189

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

6. Operator Opens PORV (OA2)

Description: If the mass input is greater than the relieving capacity or if no relief valve operates, the operator can open a PORV to reduce the pressure, given an alarm has actuated. If the operator fails to secure the pump, he can open a PORV in order to increase the time he has available in which to act.

Failure Probabilities: This action was modelled as dependent on the operator's success or failure to stop the running pump. The failure probabilities are:

Given failure of previous task

CP = 0.36	Table 20-18	Medium dependence

Given success of previous task

CP = 0.21	Table 20-19	Medium dependence

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

7. PORVs Reseat (POR)

Description: Given that the transient is successfully mitigated, the PORVs must close in order to prevent a loss of coolant. If the PORVs fail to close, the operator can isolate the open PORV using the associated block valve.

Failure Probability: The failure probability for both PORVs to reseat was calculated utilizing the fault tree shown in Figure D-24. The basic event probabilities are shown in Table D-18. The human error calculation for the operator failing to close the block valve is shown below:

TASK: Operator closes block valve

1. Operator fails to detect leaking PORV

Median HEP	= 0.001	Table 20-11	Error of commission in check reading display (digital indicators)
Error factor	= 3		
Mean HEP	= 1.25E-03		

2. Operator selects wrong control

Median HEP	= 0.001	Table 20-12	Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups
Error Factor	= 3		
Mean HEP	= 1.25E-03		

3. Recovery factor - special short term one-of-a-kind checking

Median HEP	= 0.05	Table 20-22
Error factor	= 5	
Mean HEP	= 8.07E-02	

P(Fail to close block valve) = 1.25E-03(8.07E-02) + (1-1.25E-03)(1.25E-03)(8.07E-02)
= 1.01E-04 + 1.01E-04
= 2.02E-04

Thus, the failure probabilities for the node are:

Both PORVS fail to close = 5.28E-05
One PORV fails to close = 2.64E-05

TABLE D-17 (Cont)

NORTH ANNA NODAL PROBABILITY CALCULATIONS

8. RHR Relief Valve Reseats (RVR)

Description: Given that the transient is successfully mitigated, the RHR relief valve must reseat (close) in order to prevent a loss of coolant.

Failure Probability: The probability that the relief valve will not reseat is 3E-2 per demand. If both RHR relief valves actuated, both relief valves must close. If only one RHR relief valve actuates, it must close. Thus the failure probabilities are:

Both relief valves fail to close = 3E-02 +3E-02 = 6E-02
One relief valve fails to close = 3E-02

TABLE D-18
NORTH ANNA BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
PT1402F	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
RSPS1402	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
PSPQ1402	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
CMPC1402	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
BIPS14022	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
RECO14022X	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
RECN14022X	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1700CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
OL49AF	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
OL49CF	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
MSCN52CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
MSCN52CB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
MSCN52CC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
CT480/120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
FU6AMP1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
FU6AMP2	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
OLCN40U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
LS8U	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
QSTS17U	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
CN520U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
RECO52CF	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05

TABLE D-18 (Cont)
NORTH ANNA BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
PT1403F	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
RSPS1403	RS	RESISTOR STANDARD OU	4.900E-09	1.200E+01	5.88E-08
PSPQ1403	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
CMPC1403	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
BIPS14032	BI	BISTABLE LOW OUTPUT	1.650E-06	1.200E+01	1.98E-05
RECO14032X	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
RECN14032X	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1701CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
1OL49AF	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1OL49CF	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1MSCN52CA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1MSCN52CB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1MSCN52CC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
1FU6AMP1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1FU6AMP2	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1OLCN49U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1LS8U	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
1QSTS17U	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
1CN520U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1RECO52CF	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05

TABLE D-18 (Cont)
NORTH ANNA BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
OPARMOPS	OE	OPERATOR FAILS TO AR	8.040E-04	---	8.04E-04
AVPCV1455C	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
AV1455CSIG	TP	P TRANSMITTER ALL MO	1.730E-06	5.040E+02	8.72E-04
AVPCV1456F	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
AV1456SIG	TP	P TRANSMITTER ALL MO	1.730E-06	5.040E+02	8.72E-04
AVPCV1455C	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
MV1455C	MV	FAILURE TO CLOSE	1.000E-05	5.040E+02	5.04E-03
OPMV1455C	OE	OPERATOR FAIL BLOCK	2.020E-04	---	2.02E-04
AVPCV1456K	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
MV1456K	MV	FAILURE TO CLOSE	1.000E-05	5.040E+02	5.04E-03
OPMV1456	OE	OPERATOR FAIL BLOCK	2.020E-04	---	2.02E-04

TABLE D-19

NORTH ANNA
CHARGING/SAFETY INJECTION ACTUATION
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	9.15E-02	9.15E-02	-
LSFO	4.17E-08	4.17E-08	-
LSCI	1.42E-05	1.42E-05	-
LSCO	0	0	-
LLFO	6.68E-05	6.68E-05	-
LLCO	3.00E-02	3.00E-02	-
LLCI	3.32E-03	3.32E-03	-
LSFI	0	0	-
LLFI	4.82E-07	4.82E-07	-
MSFO	1.25E-15	5.13E-14	+5.0E-14
MLFO	[illegible]	0	-
MSFI	2.27E-05	2.27E-05	-
MLFI	0	0	-
MSCO	7.80E-16	3.20E-40	+3.1E-14
MSCI	9.69E-09	9.69E-09	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	8.72E-09	8.72E-09	-
HOPI	1.05E-05	1.05E-05	-
HOPV	1.21E-18	4.03E-15	+4.0E-15
TOTAL	1.25E-01	1.25E-01	

0040D:1D/101189

TABLE D-20

NORTH ANNA
LETDOWN ISOLATION RHR OPERABLE
RESULTS

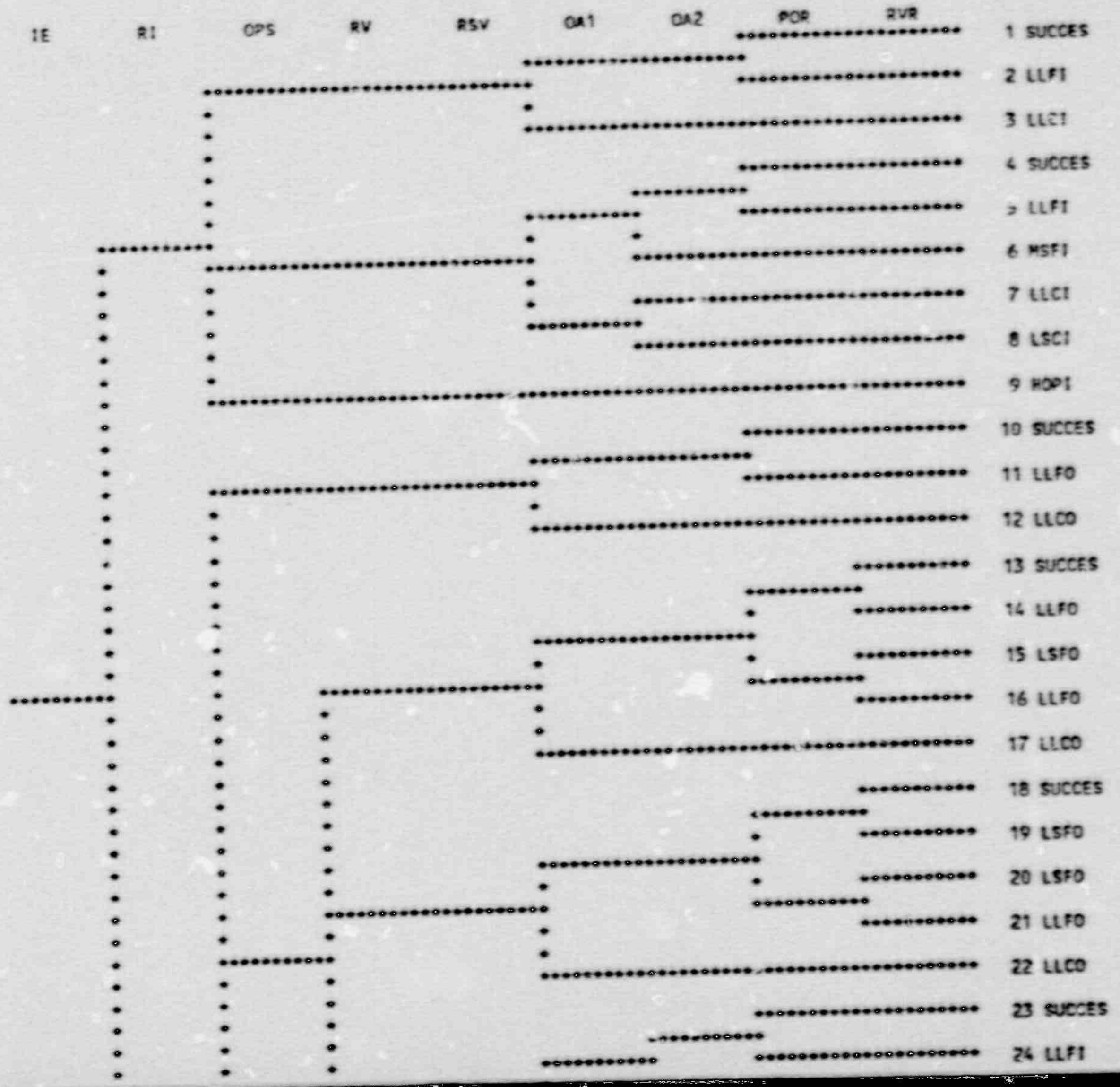
CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	9.16E-02	9.16E-02	-
LSFO	2.99E-08	2.99E-08	-
LSCI	0	0	-
LSCO	3.94E-04	3.94E-04	-
LLFO	9.39E-06	9.39E-06	-
LLCO	3.30E-02	3.30E-02	-
LLCI	0	0	-
LSFI	0	0	-
LLFI	0	0	-
MSFO	0	0	-
MLFO	0	0	-
MSFI	1.44E-16	1.44E-16	-
MLFI	0	0	-
MSCO	0	0	-
MSCI	1.61E-12	1.61E-12	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	1.45E-12	1.45E-12	-
HOPI	9.07E-13	9.07E-13	-
HOPV	1.35E-18	4.47E-15	+4.5E-15
TOTAL	1.25E-01	1.25E-01	

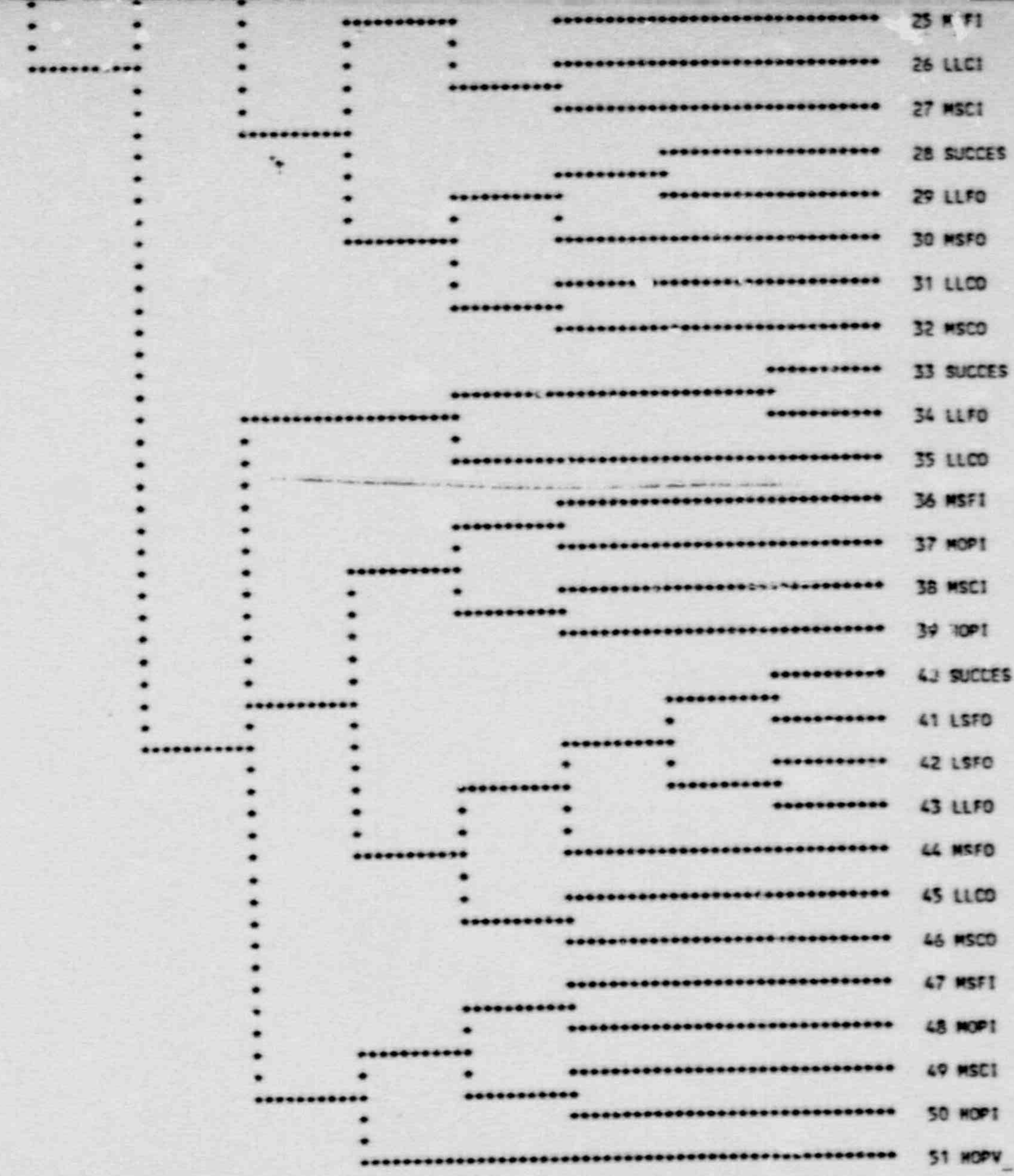
TABLE D-21

NORTH ANNA
LETDOWN ISOLATION RHR ISOLATED
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	3.26E-01	1.63E-01	-1.63E-01
LSFO	0	0	-
LSCI	1.40E-03	6.99E-04	-7E-04
LSCO	0	0	-
LLFO	0	0	-
LLCO	0	0	-
LLCI	1.17E-01	5.85E-02	-5.8E-02
LSFI	1.02E-07	5.07E-08	-5.1E-08
LLFI	1.70E-05	8.48E-06	-8.5E-06
MSFO	0	0	-
MLFO	0	0	-
MSFI	0	0	-
MLFI	0	0	-
MSCO	0	0	-
MSCI	0	0	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	0	0	-
HOPI	3.73E-04	1.86E-04	-1.9E-04
HOPV	0	0	-
TOTAL	4.45E-0[illegible]	2.22E-01	

NORTH ANNA CHARGING/SI





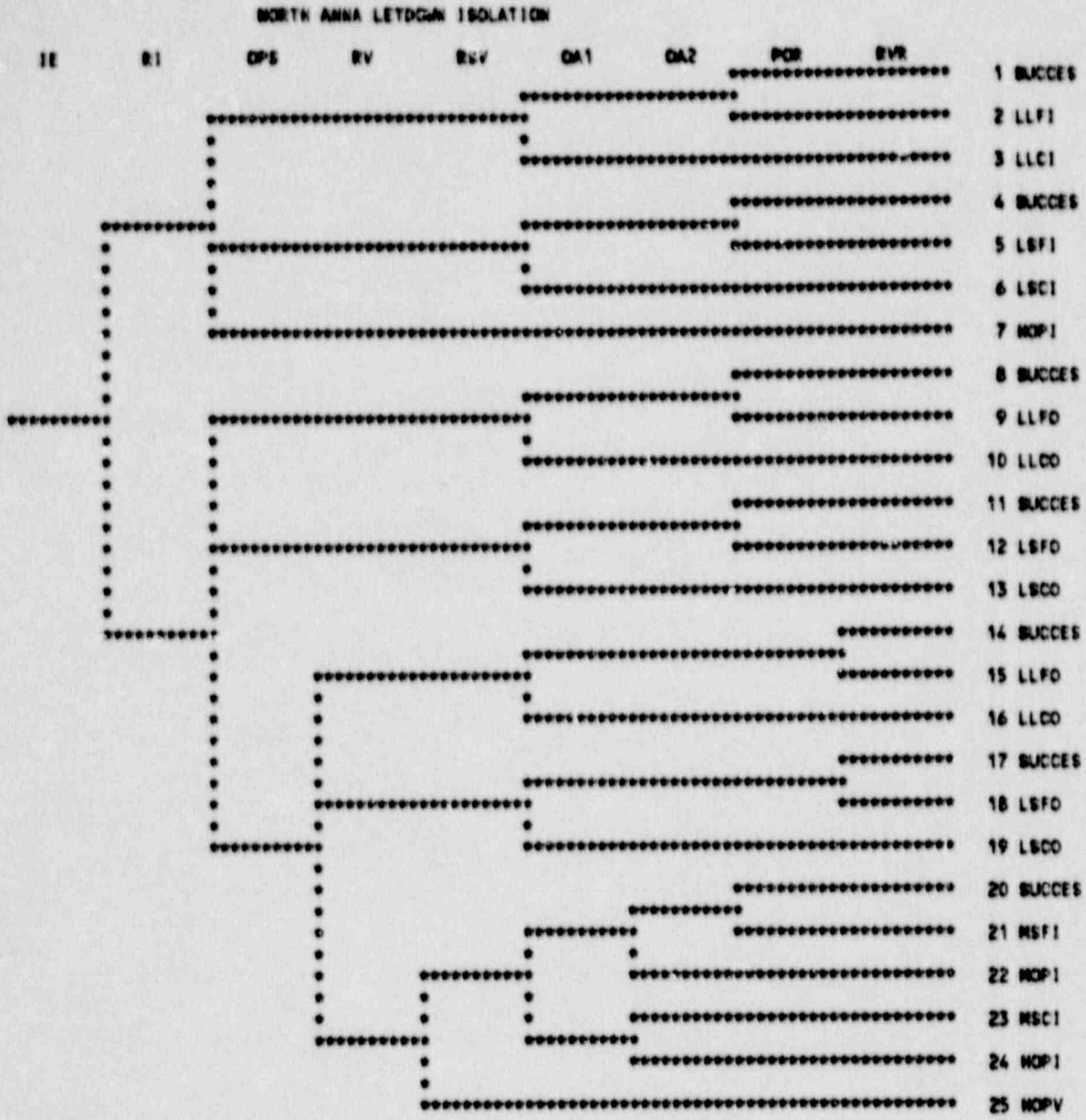
SI
APERTURE
CARD

Also Available On
Aperture Card

IE	CHARGING/SI
RI	RHRS ISOLATED
OPS	OPS PORVS OPEN
RV	RHR RELIEF VALVES LIFT
RSV	RHR SUCTION VALVES CLOSE
OA1	OPERATOR STOPS PUMP
OA2	OPERATOR OPENS PORV
POR	PORVS RESEAT
RVR	RHR RELIEF RESEATS

8911150026-79

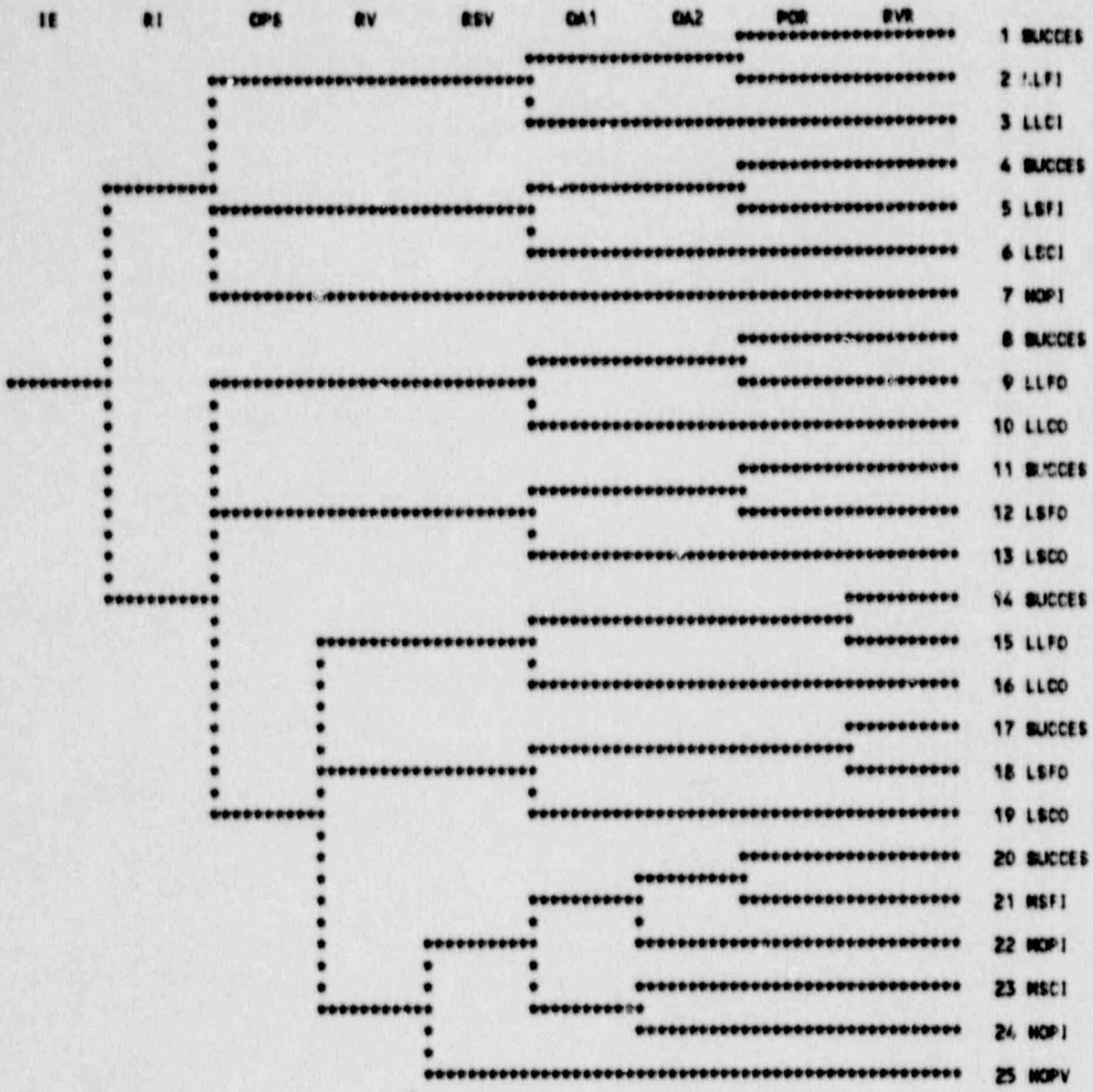
FIGURE D-17
NORTH ANNA CHARGING/
SAFETY INJECTION EVENT TREE



EVENT	EVENT NAME
IE	LETDOWN ISOLATION
RI	RHRS ISOLATED
OPS	OPS PORVS OPEN
RV	RHR RELIEF VALVES LIFT
RSV	RHR SUCTION VALVES CLOSE
OA1	OPERATOR STOPS PUMP
OA2	OPERATOR OPENS PORV
POR	PORVS RESEAT
RVR	RHR RELIEF RESEATS

FIGURE D-18
NORTH ANNA LETDOWN ISOLATION
RHR OPERABLE EVENT TREE

NORTH ANNA LETDOWN ISOLATION



EVENT	EVENT NAME
IE	LETDOWN ISOLATION
RI	RHRS ISOLATED
OPS	OPS PORVS OPEN
RV	RHR RELIEF VALVES LIFT
RSV	RHR SUCTION VALVES CLOSE
OA1	OPERATOR STOPS PUMP
OA2	OPERATOR OPENS PORV
POR	PORVS RESEAT
RVR	RHR RELIEF RESEATS

FIGURE D-19

NORTH ANNA LETDOWN ISOLATION
RHR ISOLATED EVENT TREE

OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 2

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH

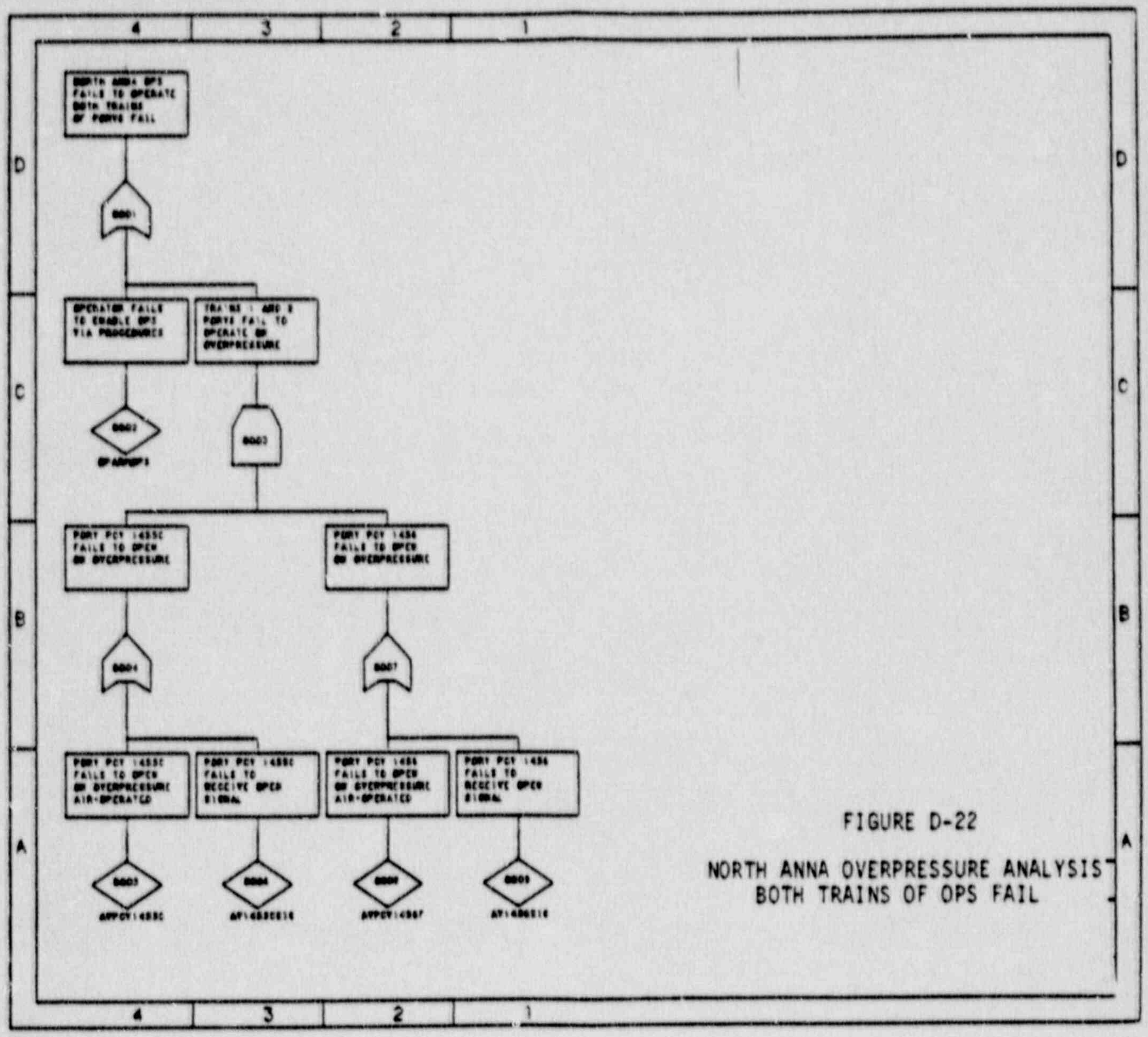


FIGURE D-22

NORTH ANNA OVERPRESSURE ANALYSIS
BOTH TRAINS OF OPS FAIL

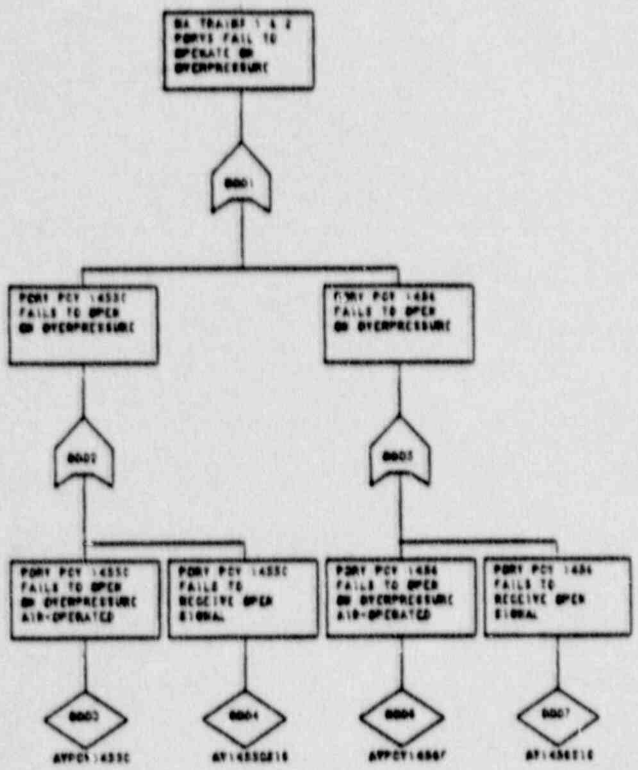


FIGURE D-23

NORTH ANNA OVERPRESSURE ANALYSIS
ONE OF TWO TRAINS OF OPS FAIL

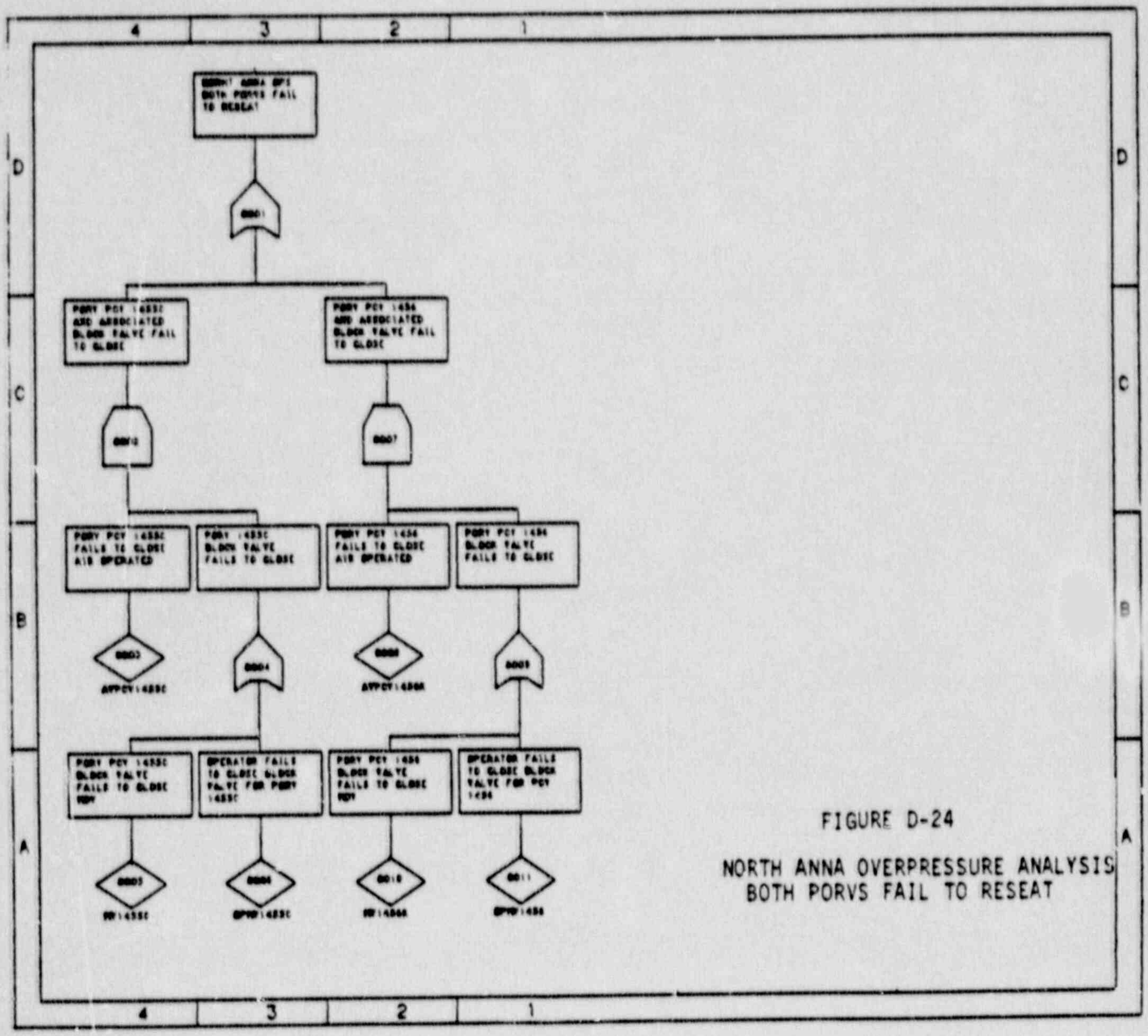


FIGURE D-24

NORTH ANNA OVERPRESSURE ANALYSIS
BOTH PORVS FAIL TO RESEAT

D.3.4 SHEARON HARRIS

The effect of the overpressure transients identified in Section D.2 was evaluated utilizing event trees. Each mitigating system and operator action was modeled as a top node on the event tree for the given transient. The following describe the event tree structure, the success criteria defined for each transient, and the nodal probabilities utilized in the quantification and the results.

The safety functions, i.e. the event tree top events or nodes, for the Shearon Harris event trees are defined below:

1. Initiating Event (IE): The mass input initiator that could lead to overpressurization and/or possible RHRS damage, either charging/safety injection pump actuation or letdown isolation.

2. RHRS isolated (RI): The RHRS will be isolated during certain periods of shutdown. This dictates whether or not the RHRS relief valve is available to mitigate the transient and if the possibility exists for damage to the RHRS. For Shearon Harris, the event tree allows for both trains of RHRS to be isolated, one train or no trains.

3. COPS System Operates (COP): The cold overpressure protection system consists of two redundant and independent systems utilizing the pressurizer PORVs. When the system is enabled and reactor coolant temperature is below 335°F, a high pressure signal (above the COPS setpoint) will trip the system automatically and open a PORV until the pressure drops below the reset value. For Shearon Harris, the COPS system has a variable setpoint. An auctioneered system temperature is continuously converted to an allowable pressure and then compared to the actual RCS pressure. The system logic will first annunciate a main control board alarm whenever the measured pressure approaches within a predetermined amount of the allowable pressure. On a further increase in measured pressure, an actuation signal is transmitted to

the power-operated relief valve. For this analysis, it was assumed that the COPS would actuate at its lowest setpoint (390 psig). The cases examined are two PORVs actuate, one PORV actuates or no PORVs actuate.

4. RHRS Suction Relief Valve Lifts (RV): If the RHRS is not isolated, the spring loaded relief valves will open at the setpoint pressure. If one train of RHRS is isolated, only one RHR relief valve is available and if both trains are isolated, there are no RHR relief valves available to mitigate the transient.

5a. RHRS Suction/Isolation Valves Automatically Close (RSV): When the pressure increases to the autoclosure setpoint (700 psig), the autoclosure interlock receives a pressure signal that actuates the circuitry and closes the motor-operated valve. This node is addressed in the case with the autoclosure interlock only.

5b. Operator Detects Overpressure Alarm and Isolates the RHRS (OD): For the modification case, an alarm would sound when the pressure reached the high pressure setpoint. Through a revision in operating procedures, it is assumed that the operator will detect the overpressure and isolate the RHRS before the pressure reaches 150% of the RHRS design pressure.

6. Operator Secures Running Pump (OA1): Given an alarm, either by actuation from the RHRS relief valve opening to the pressurizer relief tank (PRT), or from the operation of at least one train of COPS, or from an RHRS pump low flow alarm (on autoclosure of the RHRS suction valves) or from the high pressure alarm on the RHRS suction valves (in the modification case only), the operator will stop the extra running pump (either an SI or charging pump). If the operator stops the running pump, the overpressure event is halted.

7. Operator Opens a PORV (OA2): Given an alarm, if no or one relief valve operates successfully and the pressure still continues to rise, the operator may open a PORV in order to reduce the pressure. The operator may also open a PORV if he fails to stop the running pump in order to increase the time available to mitigate the transient.

8. Pressurizer PORVs Reseat (POR): Given that one or more of the PORVs has opened and the transient has been stopped, the valve must close in order to avert a loss of coolant condition. If the transient is not stopped, the valve(s) will cycle until failure occurs.

9. RHRS Relief Valve Reseats (RVR): Given that the RHRS relief valves successfully operate and the transient was terminated, the relief valve must reseat or coolant would be lost to the PRT. If the transient is not stopped, the relief valve will cycle open and closed and is assumed to eventually fail open.

For each of these nodes, failure probabilities were calculated. These nodal probability calculations are shown in Table D-22 for Shearon Harris.

The success criteria for the event trees was determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. For the charging/safety injection pump actuation case, because the charging pump maximum flow rate and the safety injection pump maximum flow rate combined is 1300 gpm (conservative assumption that both pumps operate at maximum flow rates), it was assumed that two PORVs or two RHR relief valves or one PORV and one RHR relief valve are required to mitigate the transient. The following assumptions were also utilized in the analysis of the charging/safety injection mass input transient:

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction [illegible] components while 6 weeks (1008 hours) was assumed for the PORVs and block valves.

Figure D-25 illustrates the event tree for Shearon Harris for the charging/safety injection initiating event.

The success criteria for the letdown isolation cases was also determined based on conservative estimates of the flow rates and relieving capacities of the relief valves. Because the charging pump's maximum flow rate is 650 gpm, it was assumed that only RHR relief valve, or one PORV must operate to mitigate the transient. The following assumptions were utilized in the letdown isolation case.

1. No credit is taken for the RCS vents.

2. The detection time for failure was assumed to be 24 hours for the suction valve components while 6 weeks (1008 hours) was assumed for the PORVs and block valves.

The event tree for the letdown isolation cases is similar to the charging/safety injection pump actuation event tree. However, the success criteria for the various nodes is changed due to the type of transient. The event trees for the letdown isolation cases are shown in Figures D-26 and D-27.

The results from the quantification of the event trees for Shearon Harris are shown in Tables D-24 to D-26. The results show that most of the overpressure consequence categories remain unchanged with deletion of the autoclosure interlock. For the charging/safety injection case, consequence categories MSFO, MSCO, and HOPV increased. However, the increase is in the range of 1E-11 to 1E-12/shutdown year. This is a very insignificant increase in the frequency of these events. For the letdown isolation - RHR operable case, the consequence categories LSCI and MSCI decreased slightly while the HOPV category increased to 3E-15/shutdown year. In the letdown isolation - RHR isolated case, the consequence categories affected all decreased due to the reduction in the initiating event frequency. The conclusion to be drawn from the results is that the removal of the autoclosure interlock has a small impact on overpressurization transients.

TABLE D-22

SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

1. RHR Isolated (RI)

Description: This node divides into two branches. The upper branch indicates that the RHR system is isolated from the RCS while the bottom branch indicates that the RHR system is open to the RCS. For this node, it was assumed that the RHR system may be isolated for a period of time during cold shutdown. The nodal probabilities for the charging/safety injection actuation case are based on assumptions that both trains of RHR would be isolated only five percent of the time and one train would be isolated 10 percent of the time. Thus, both trains of RHR would not be isolated from the RCS 85 percent of the time. For the letdown isolation case with the RHR operable, the nodal probability is 1.0 while for the case with the RHR isolated, the nodal probability is 0.0.

Failure probabilities: The probabilities for this node for each case are shown below:

Charging/Safety Injection pump actuation

Both trains isolated	0.05
One train isolated	0.10
No trains isolated	0.85

Letdown Isolation

RHR operable	1.0
RHR isolated	0.0

TABLE D-22 (Cont)
SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

2. COP system operates at P=390 psig (COP)

Description: The event tree divides into three branches at the COP node. The top branch symbolizes that both trains of COPS operate, the middle branch shows only one train of COPS operates while the bottom branch signifies both trains of COPS have failed to operate.

The COPS (cold overpressure protection system) utilizes two pressurizer relief valves (PORVs). The operator must enable the system when the cold leg RCS temperature is less than 335°F. An alarm is actuated thereby alerting the operator to arm the COPS. If the isolation valves for the PORVs are closed when the RCS auctioned temperature is below a set value, alarms will sound to indicate that the COP is unavailable. The COPS has a variable pressure setpoint determined by the measured RTD temperature. For this analysis, the setpoint was assumed to be constant at 390 psig (the lowest setpoint allowed).

Failure probabilities: The failure probabilities associated with this node were calculated utilizing fault trees. Figure D-30 shows the fault tree developed for two trains of COPS failing to operate while the failure of one train is shown in Figure D-31. The operator error in failing to enable the COPS system is shown below:

Task: Operator fails to arm the COPS following alarm.

Median HEP	=0.0001	Table 20-23	Failure to initiate some kind of intended corrective action as required
Error Factor	= 10		
Mean HEP	= 2.66E-04		

The basic event probabilities utilized in the fault trees are shown in Table D-23. The failure probabilities quantified from the fault trees is:

Two trains of COPS Fail = 3.01E-04
One train of COPS Fails = 1.18E-02

TABLE D-22 (Cont)

SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

3. RHR Relief Valve Operates (RV)

Description: This node divides into three branches if both trains of RHR are open to the RCS and into two branches if only one train of RHR is not isolated from the RCS. If both trains of RHR are open to the RCS, two RHR relief valves can operate (indicated by the top branch), one RHR relief valve can operate (indicated by the middle branch), or both relief valves can fail to open (indicated by the bottom branch). When only one train of RHR is open to the RCS, the one operable RHR relief valve can open (the top branch) or can fail to open (the bottom branch).

The RHR relief valves are spring-loaded relief valves set to actuate at 450 psig. Each relief valve can relieve 900 gpm at 450 psig.

Failure probabilities: The failure of a relief valve to open is 3E-04 per demand. Thus the probabilities for this node are:

Two (of 2) RHR relief valves fail to open = (3E-04)(3E-04)=9E-08
One (of 2) RHR relief valve fails to open = 3E-04 +3E-04=6E-04
One (of 1) RHR relief valve fails to open = 3E-04

TABLE D-22 (Cont)

SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

4a) RHR Suction Valves Close at P=700 psig (RSV)

Description: The node determines whether or not the RHR suction valve autoclosure interlock closes the valves when the RCS pressure reaches 700 psig. For Shearon Harris, it was assumed that only one valve on each train must close for success. Failure was considered to be both trains of RHR open to the RCS (i.e. the autoclosure interlock failed to close one valve on each train).

Failure probabilities: The failure probability associated with this node was calculated using the fault tree shown in Figure D-28. The basic event probabilities used to quantify the fault tree are shown in Table D-23. The failure probability for this node is:

Both trains of RHR fail to isolated = 2.62E-07
One train of RHR fails to isolate = 1.54E-07

TABLE D-22 (Cont)

SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

4b) Operator Isolates RHR System Given Overpressure Alarm (OD)

Description: The proposed modification deletes the autoclosure interlock and adds an alarm to alert the operate when the pressure exceeds the high pressure setpoint and an isolation valve is in the open position. Given an overpressure transient and this alarm the operator will close at least one RHR suction valve on each drop line to isolate the RHR system. The probability of operator failure is conditional on the time he has in which to act. If a mitigating system operates successfully (a PORV or RHR relief valve opens), it was assumed that the operator has 20 minutes in which to act. If no mitigating system operates, the operator has approximately 10 minutes to act.

Failure Probabilities: The failure probabilities associated with this node were calculated utilizing the fault tree shown in Figure D-29. The operator error probabilities shown in the fault tree are calculated below:

TASK: Operator closes isolation valve given high pressure alarm.

1. Diagnosis within time T by control room personnel of abnormal event annunciated

   Median HEP = 0.1 within 10 minutes Table 20-3
   Error Factor = 10
   Mean HEP = 0.266

   Median HEP = 0.01 within 20 minutes Table 20-3
   Error factor = 10
   Mean HEP = 2.66E-02

2. Operator failure in operating manual controls

   Median HEP = 0.001 Table 20-12 Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups
   Error factor = 10
   Mean HEP = 1.25E-03

3. Recovery factor - special short term one-of-a-kind checking

   Median HEP = 0.05 Table 20-22
   Error factor = 5
   Mean HEP = 8.07E-02

TABLE D-22 (Cont)
SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

4b) Operator Isolates RHR System Given Overpressure Alarm (OD) (Cont)

P(Fail in 20 minutes) =
2.66E-02(8.07E-02) +
(1-2.66E-02)(1.25E-03)(8.07E-02)
= 2.15E-03 + 9.82E-05
= 2.25E-03

P(Fail in 10 minutes)=
0.266(8.07E-02) +
(1-0.266)(1.25E-03)(8.07E-02)
= 2.15E-02 + 7.40E-05
= 2.16E-02

The basic event probabilities are shown in Table D-23. The results of the quantification of the fault trees is shown below:

Operator Isolates RHR in 20 minutes = 1.09E-05
Operator Isolates RHR in 10 minutes = 9.40E-04

TABLE D-22 (Cont)

SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

5. Operator Secures Running Pump (OA1)

Description: For any operator action to occur, an alarm must be actuated. This alarm can occur by actuation of a relief valve (PORV or RHR), RHRS pump low flow or high pressure alarm or in the modification case, the high pressure alarm on the RHR suction valves. For the charging/safety injection actuation case, this pump is the safety injection pump. In the letdown isolation case, the charging pump must be stopped.

Failure Probability: The human error probability is calculated below:

1. Failure to diagnose transient in time T

Median HEP	= 0.1	within 20 minutes	Table 20-1
Error factor	= 10		
Mean HEP	= 0.266		

2. Select wrong control

Median HEP	= 0.001	Table 20-12	Select wrong control on a panel from an array of similar-appearing controls arranged in well-delineated functional groups
Error factor	= 3		
Mean HEP	= 1.25E-03		

P(Fail in 20 minutes) = 0.266 + (1-0.266)(1.25E-03)
= 0.267

TABLE D-22 (Cont)

SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

6. Operator Opens PORV (OA2)

Description: If the mass input is greater than the relieving capacity or if no relief valve operates, the operator can open a PORV to reduce the pressure, given an alarm has actuated. If the operator fails to secure the pump, he can open a PORV in order to increase the time he has available in which to act.

Failure Probabilities: This action was modelled as dependent on the operator's success or failure to stop the running pump. The failure probabilities are:

Given failure of previous task

CP = 0.36	Table 20-18	Medium dependence

Given success of previous task

CP = 0.21	Table 20-19	Medium dependence

TABLE D-22 (Cont)

SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

7. PORVs Reseat (POR)

Description: Given that the transient is successfully mitigated, the PORVs must close in order to prevent a loss of coolant. If the PORVs fail to close, the operator can isolate the open PORV using the associated block valve.

Failure Probability: The failure probability for both PORVs to reseat was calculated utilizing the fault tree shown in Figure D-32. The basic event probabilities are shown in Table D-23. The human error calculation for the operator failing to close the block valve is shown below:

TASK: Operator close block valve

1. Operator Fails to detect leaking PORV

Median HEP	= 0.001	Table 20-11	Error of commission in check reading display (digital indicators)
Error Factor	= 3		
Mean HEP	= 1.25E-03		

2. Operator selects wrong control

Median HEP	= 0.001	Table 20-12	Select wrong control from an array of similar-appearing controls arranged in well-delineated functional groups
Error Factor	= 3		
Mean HEP	= 1.25E-03		

3. Recovery factor - special short term one-of-a-kind checking

Median HEP	= 0.05	Table 20-22
Error Factor	= 5	
Mean HEP	= 8.07E-02	

P(Fail to close block valve) = 1.25E-03(8.07E-02) + (1-1.25E-03)(1.25E-03)(8.07E-02)
= 1.01E-04 + 1.01E-04
= 2.02E-04

Thus, the failure probabilities for the node are:

Both PORVS fail to close = 5.28E-05
One PORV fails to close = 2.64E-05

TABLE D-22 (Cont)

SHEARON HARRIS NODAL PROBABILITY CALCULATIONS

6. RHR Relief Valve Reseats (RVR)

Description: Given that the transient is successfully mitigated, the RHR relief valve must reseat (close) in order to prevent a loss of coolant.

Failure Probability: The probability that the relief valve will not reseat is 3E-2 per demand. If both RHR relief valves actuated, both relief valves must close. Thus the failure probabilities are:

Both relief valves fail to close = 3E-02 +3E-02 = 6E-02
One relief valve fails to close = 3E-02

TABLE D-23

SHEARON HARRIS BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1LSACU	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
1PS118VAC	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
REPY403A2	RE	RELAY ALL FAILURE MO	8.700E-08	1.200E+01	1.04E-06
CMPB403	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
ISEEPV403C	EE	ISOLATOR E-E CONVERT	4.800E-07	1.200E+01	5.76E-06
PSPGY403	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
RSPS403B	RS	RESISTOR STANDARD OU	4.900E-09	1.200E+01	5.88E-08
TPPT403	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
1CN2A12A2U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1CNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
1CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
1OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
1RECN42SA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RECN42SB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1RECB42SC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
1QSTCU	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
1CN42OU	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
1RECO42S	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05

TABLE D-23 (Cont.)

SHEARON HARRIS BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
1C[illegible]789	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1FU1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
1CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1OLCN49MR2	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
1OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2LSACU	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
2PS118VAC	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
REPY402A2	RE	RELAY ALL FAILURE MO	8.700E-08	1.200E+01	1.04E-06
CMPB402	CM	COMPARATOR ALL MODES	2.900E-06	1.200E+01	3.48E-05
ISEEPV402C	EE	ISOLATOR E-E CONVERT	4.800E-07	1.200E+01	5.76E-06
PSPGY402	PS	LOOP POWER SUPPLY AL	5.800E-06	1.200E+01	6.96E-05
RSPS402B	RS	RESISTOR STANDARD QU	4.900E-09	1.200E+01	5.88E-08
TPPT402	TP	PRESSURE SENSORS ALL	2.800E-06	1.200E+01	3.36E-05
2CN2A12A2U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2CNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
2CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
2OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
2OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06

TABLE D-23 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
2RECN42SA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2RECN42SB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2RECB42SC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
2QSTCU	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
2CN42OU	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
2RECO42S	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
2CNCR1789	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2FU1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
2CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2OLCN49MR2	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
2OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
9LSACU	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
9CN2A12A2U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
9CNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
9CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
9CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
9OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
9OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
9OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
9RECN42SA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05

TABLE D-23 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
9RECN42SB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
9RECB42SC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
9QSTCU	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
9CN42OU	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
9RECO42S	CO	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
9CNCR1789	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
9FU1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
9CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
9OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
9OLCN49MR2	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
9OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
4LSACU	LS	LIMIT SWITCH ALL MOD	7.220E-06	1.200E+01	8.66E-05
4CN2A12A2U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
4CNK735	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
4CBU	CB	CIRCUIT BREAKER OPEN	1.000E-08	1.200E+01	1.20E-07
4CT480120V	CT	CURRENT TRANSFORMER	3.500E-07	1.200E+01	4.20E-06
4OL49MRA	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
4OL49MRB	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
4OL49MRC	OL	THERMAL OVERLOAD PRE	1.500E-07	1.200E+01	1.80E-06
4RECN42SA	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
4RECN42SB	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05

TABLE D-23 (Cont)
SHEARON HARRIS BASIC EVENT PROBABILITIES FOR FAULT TREES

FAULT TREE IDENTIFIER	COMP	FAILURE MODE	FAILURE RATE (/HR OR /D)	DETECTION TIME (HR)	FAILURE PROBABILITY
4RECB42SC	CN	RELAY CONTACTS FAIL	1.000E-06	1.200E+01	1.20E-05
4QSTCU	QS	TORQUE SWITCH FAIL T	2.000E-07	1.200E+01	2.40E-06
4CN42OU	CN	MOTOR STARTER SPURIO	3.000E-08	1.200E+01	3.60E-07
4RECO42S	CC	RELAY COIL FAILURE	3.000E-06	1.200E+01	3.60E-05
4CNCR1789	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
4FU1	FU	FUSE ALL MODES	1.500E-07	1.200E+01	1.80E-06
4CN5557U	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
4OLCN49MR1	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
4OLCN49MR2	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
4OLCN49MR3	CN	RELAY CONTACTORS SPU	2.000E-08	1.200E+01	2.40E-07
OPARMCOPS	OE	OPERATOR FAILS TO AR	2.660E-04	---	2.66E-04
AV1RC116F	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
AV116SIG	TP	P TRANSMITTER ALL MO	1.730E-06	5.040E+02	8.72E-04
AV1RC118F	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
AV118SIG	TP	P TRANSMITTER ALL MO	1.730E-06	5.040E+02	8.72E-04
AV1RC116K	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
MV115K	MV	FAILURE TO CLOSE	1.000E-05	5.040E+02	5.04E-03
OPMV115	OE	OPERATOR FAIL BLOCK	2.020E-04	---	2.02E-04
AV1RC118K	AO	FAILURE TO OPERATE	1.000E-05	5.040E+02	5.04E-03
MV117K	MV	FAILURE TO CLOSE	1.000E-05	5.040E+02	5.04E-03
OPMV117	OE	OPERATOR FAIL BLOCK	2.020E-04	---	2.02E-04

TABLE D-24

SHEARON HARRIS
CHARGING/SAFETY INJECTION ACTUATION
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	9.15E-02	9.15E-02	-
LSFO	3.28E-06	3.28E-06	-
LSCI	0	0	-
LSCO	0	0	-
LLFO	6.11E-05	6.11E-05	-
LLCO	3.17E-02	3.17E-02	-
LLCI	1.66E-03	1.66E-03	-
LSFI	0	0	-
LLFI	2.41E-07	2.41E-07	-
MSFO	9.1[illegible]E-14	6.42E-12	+6.3E-12
MLFO	0	0	-
MSFI	1.35E-05	1.35E-05	-
MLFI	0	0	-
MSCO	5.68E-14	4.01E-12	+4E-12
MSCI	7.74E-06	7.74E-06	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	5.82E-07	5.82E-07	-
HOPI	2.24E-06	2.24E-06	-
HOPW	1.75E-16	1.06E-12	+1.1E-12
TOTAL	1.25E-01	1.25E-01	

0040D:1D/101189

TABLE D-25

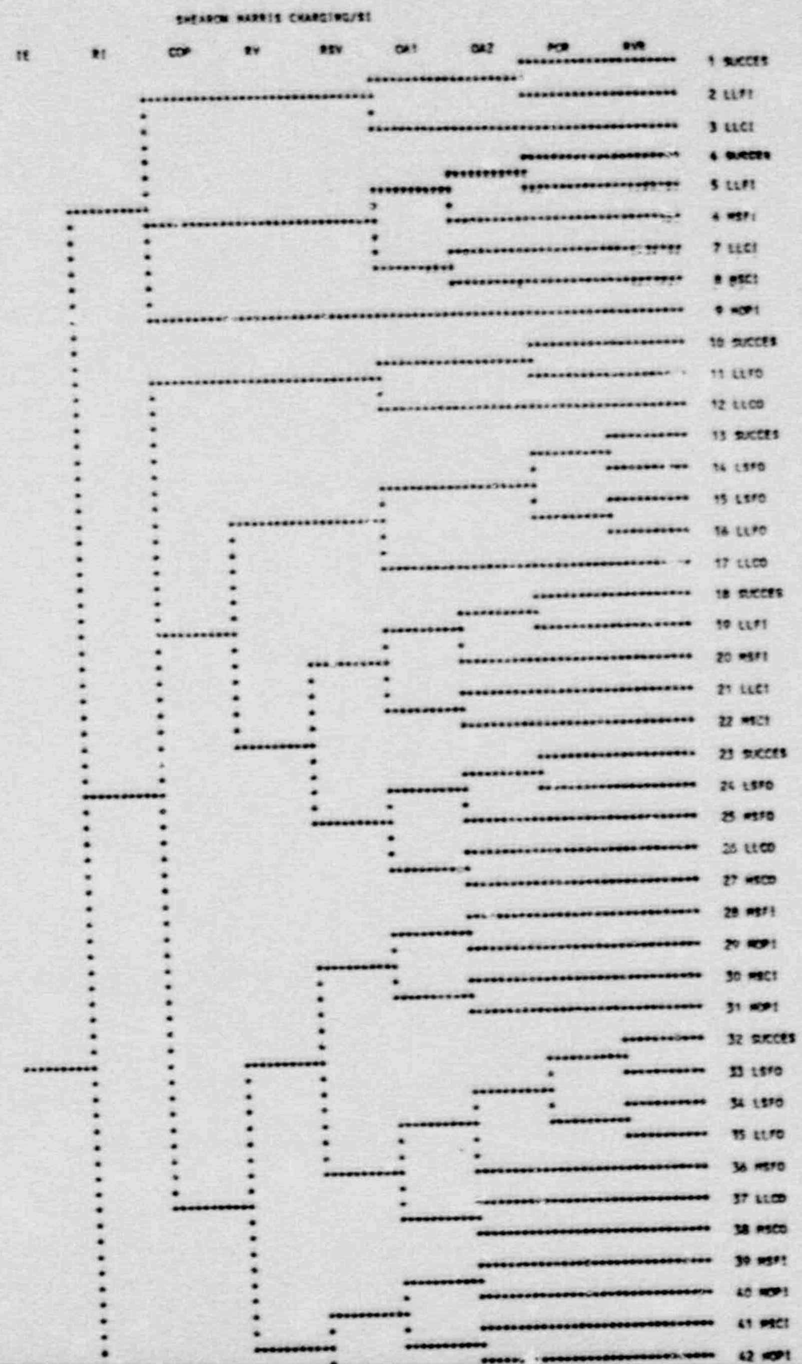
SHEARON HARRIS
LETDOWN ISOLATION RHR OPERABLE
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	9.16E-02	9.16E-02	-
LSFO	2.90E-08	2.90E-08	-
LSCI	0	0	-
LSCO	3.94E-04	3.94E-04	-
LLFO	6.43E-06	6.43E-06	-
LLCO	3.30E-02	3.30E-02	-
LLCI	0	0	-
LSFI	5.13E-17	5.17E-17	-1E-19
LLFI	0	0	-
MSFO	0	0	-
MLFO	0	0	-
MSFI	0	0	-
MLFI	0	0	-
MSCO	0	0	-
MSCI	5.79E-13	5.78E-13	-1E-15
MLCO	0	0	-
MLCI	0	0	-
MOPI	5.21E-13	5.21E-13	-
HOPI	3.25E-13	3.25E-13	-
HOPV	8.87E-19	3.18E-15	+3.2E-15
TOTAL	1.25E-01	1.25E-01	

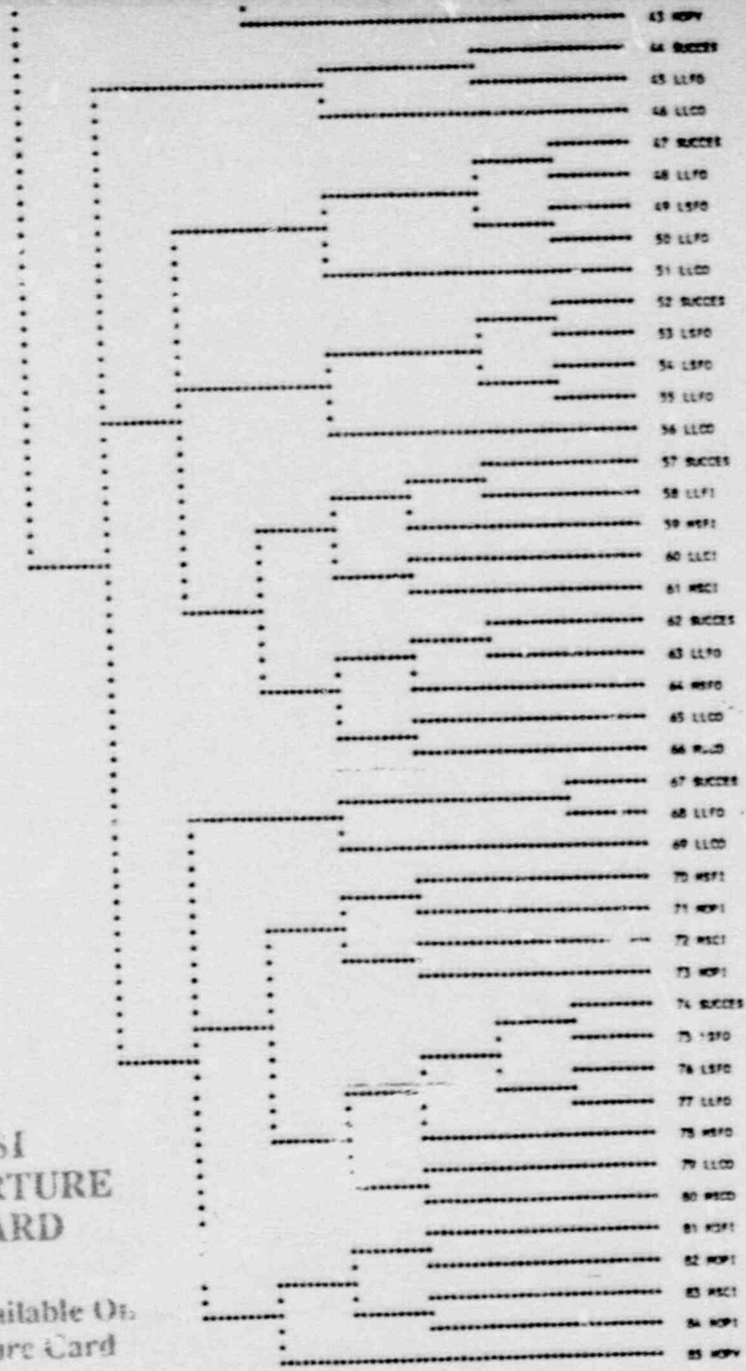
TABLE D-26

SHEARON HARRIS
LETDOWN ISOLATION RHR ISOLATED
RESULTS

CONSEQUENCE CATEGORY	FREQUENCY WITH ACI	FREQUENCY WITHOUT ACI	FREQUENCY CHANGE
SUCCESS	3.26E-01	1.63E-01	-1.63E-01
LSFO	0	0	-
LSCI	1.40E-03	6.99E-04	-7E-04
LSCO	0	0	-
LLFO	0	0	-
LLCO	0	0	-
LLCI	1.17E-01	5.86E-02	-5.[illegible]
LSFI	1.02E-07	5.07E-08	-5.1[illegible]
LLFI	1.70E-05	8.49E-06	-8.5E-06
MSFO	0	0	-
MLFO	0	0	-
MSFI	0	0	-
MLFI	0	0	-
MSCO	0	0	-
MSCI	0	0	-
MLCO	0	0	-
MLCI	0	0	-
MOPI	0	0	-
HOPI	1.34E-04	6.68E-05	-6.7E-05
HOPV	0	0	-
TOTAL	4.45E-01	2.22E-01	



SHEARON HARRIS CHARGING/SI
IE
RI
CCP
RV
RSV
CA1
CA2
PCR
RVR
1 SUCCES
2 LLFI
3 LLCI
4 SUCCES
5 LLFI
6 MSFI
7 LLCI
8 MSCI
9 MCPI
10 SUCCES
11 LLFO
12 LLCO
13 SUCCES
14 LSFO
15 LSFO
16 LLFO
17 LLCO
18 SUCCES
19 LLFI
20 MSFI
21 LLCI
22 MSCI
23 SUCCES
24 LSFO
25 MSFO
26 LLCO
27 MSCO
28 MSFI
29 MCPI
30 MSCI
31 MCPI
32 SUCCES
33 LSFO
34 LSFO
35 LLFO
36 MSFO
37 LLCO
38 MSCO
39 MSFI
40 MCPI
41 MSCI
42 MCPI



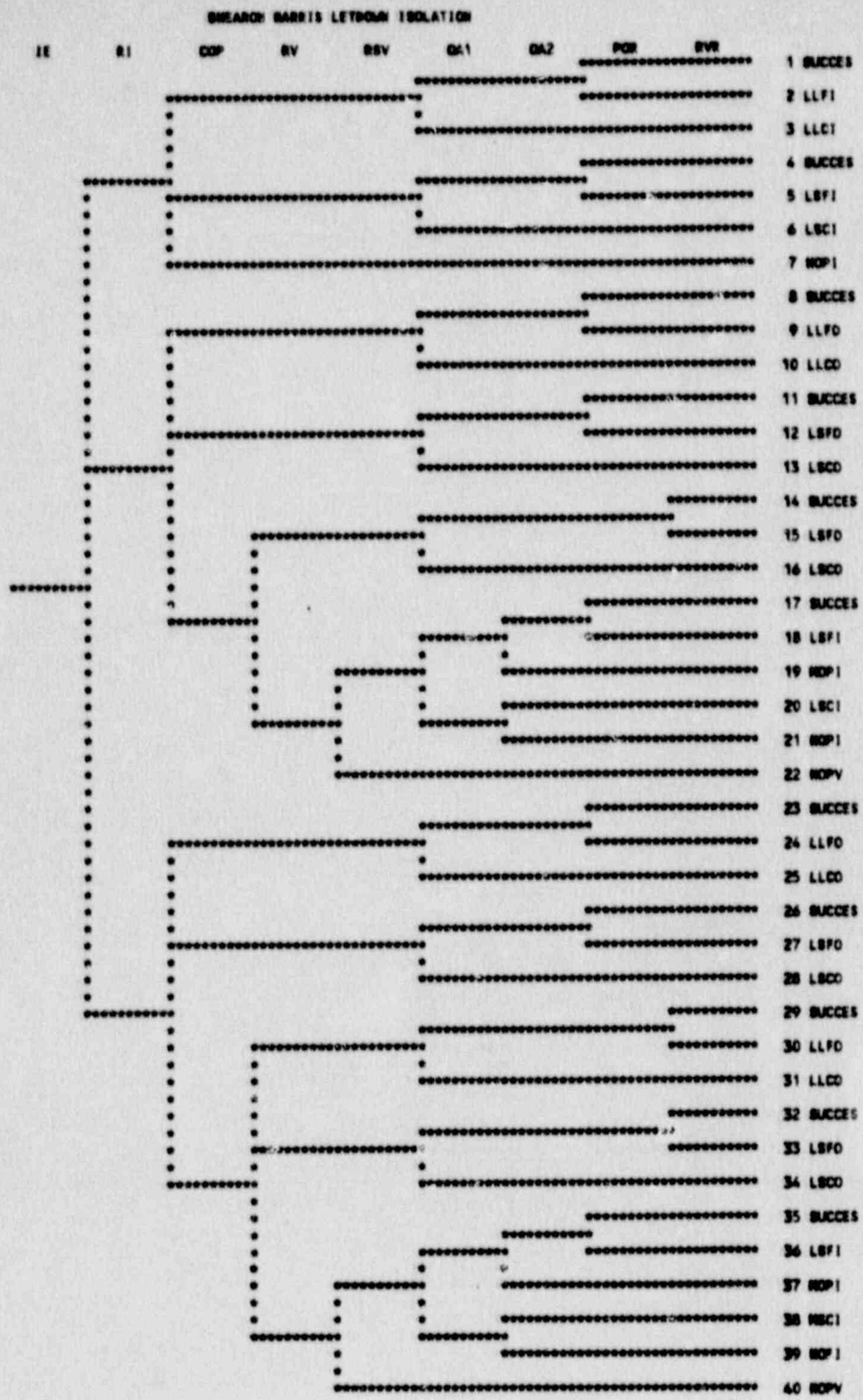
SI
APERTURE
CARD

Also Available On
Aperture Card

EVENT	EVENT NAME
IE	CHARGING/SI
RI	RHRS ISOLATED
COP	COPS PORVS OPEN
RV	RHR RELIEF VALVES LIFT
RSV	RHR SUCTION VALVES CLOSE
OA1	OPERATOR STOPS PUMP
OA2	OPERATOR OPENS PORV
POR	PORVS RESEAT
RVR	RHR RELIEF RESEAT

FIGURE D-25
SHEARON HARRIS CHARGING/
SAFETY INJECTION EVENT TREE

8911150026-82

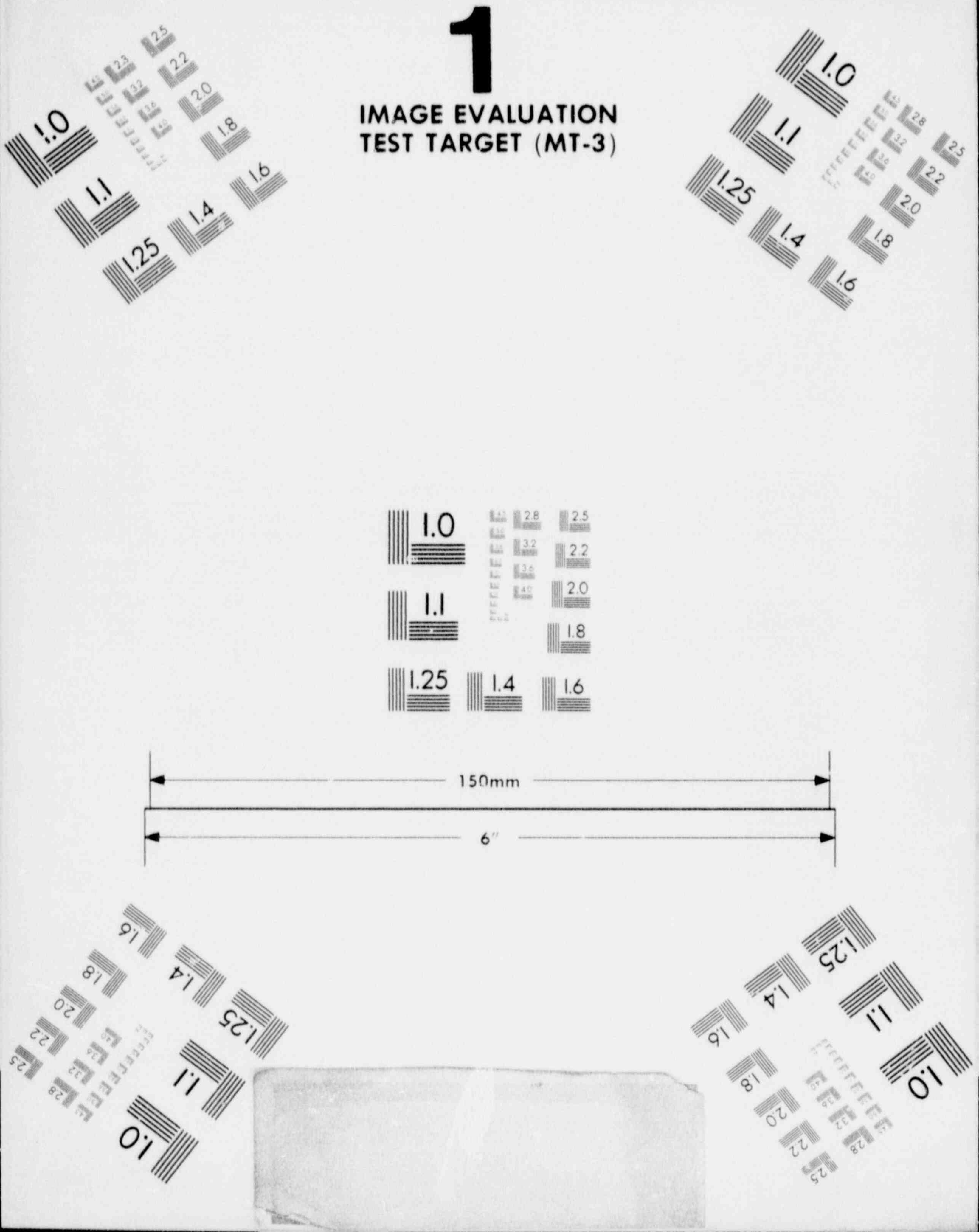


EVENT	EVENT NAME
IE	LETDOWN ISOLATION
RI	RHRS ISOLATED
COP	OPS PORVS OPEN
RV	RHR RELIEF VALVES LIFT
RSV	RHR SUCTION VALVES CLOSE
OA1	OPERATOR STOPS PUMP
OA2	OPERATOR OPENS PORV
POR	PORVS RESEAT
RVR	RHR RELIEF RESEATS

FIGURE D-26
SHEARON HARRIS LETDOWN ISOLATION
RHR OPERABLE EVENT TREE

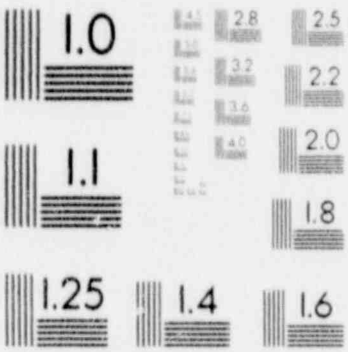
1

IMAGE EVALUATION TEST TARGET (MT-3)



1

IMAGE EVALUATION TEST TARGET (MT-3)



150mm

6"

1

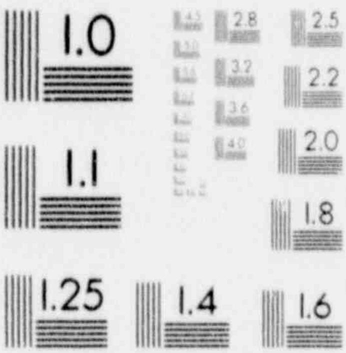
IMAGE EVALUATION TEST TARGET (MT-3)

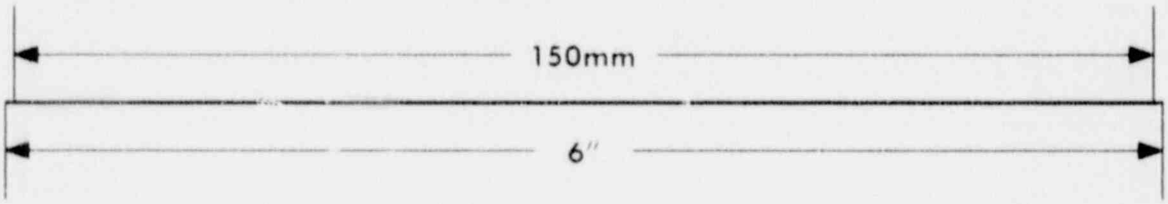
150mm

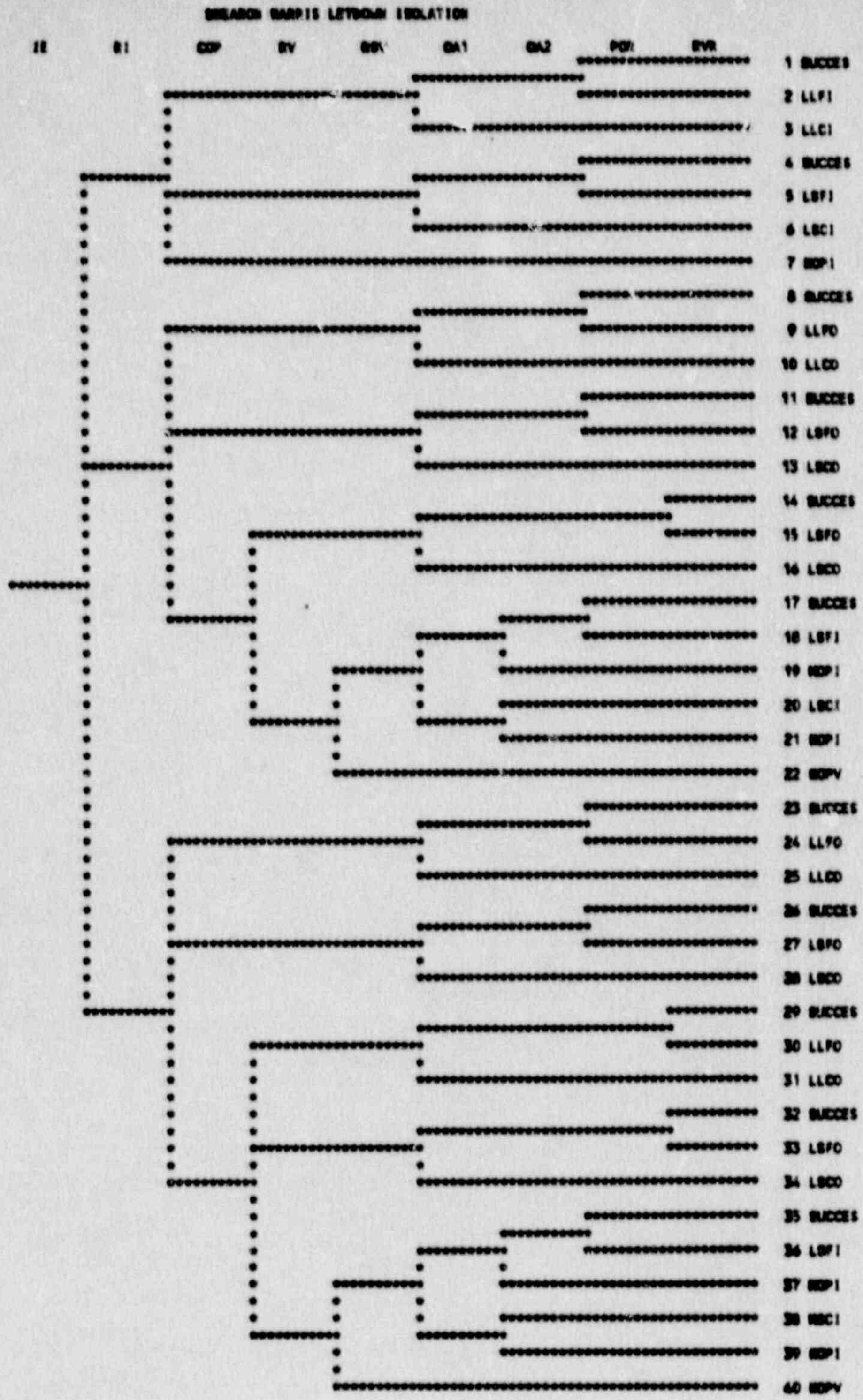
6″

1

IMAGE EVALUATION TEST TARGET (MT-3)







EVENT	EVENT NAME
IE	LETDOWN ISOLATION
RI	RHRS ISOLATED
OOP	OPS PORVS OPEN
RV	RHR RELIEF VALVES LIFT
RSV	RHR SUCTION VALVES CLOSE
OA1	OPERATOR STOPS PUMP
OA2	OPERATOR OPENS PORV
POR	PORVS RESEAT
RVR	RHR RELIEF RESEATS

FIGURE D-27
SHEARON HARRIS LETDOWN ISOLATION
RHR ISOLATED EVENT TREE

OVERSIZE DOCUMENT PAGE PULLED

SEE APERTURE CARDS

NUMBER OF OVERSIZE PAGES FILMED ON APERTURE CARDS 2

APERTURE CARD/HARD COPY AVAILABLE FROM

RECORDS AND REPORTS MANAGEMENT BRANCH

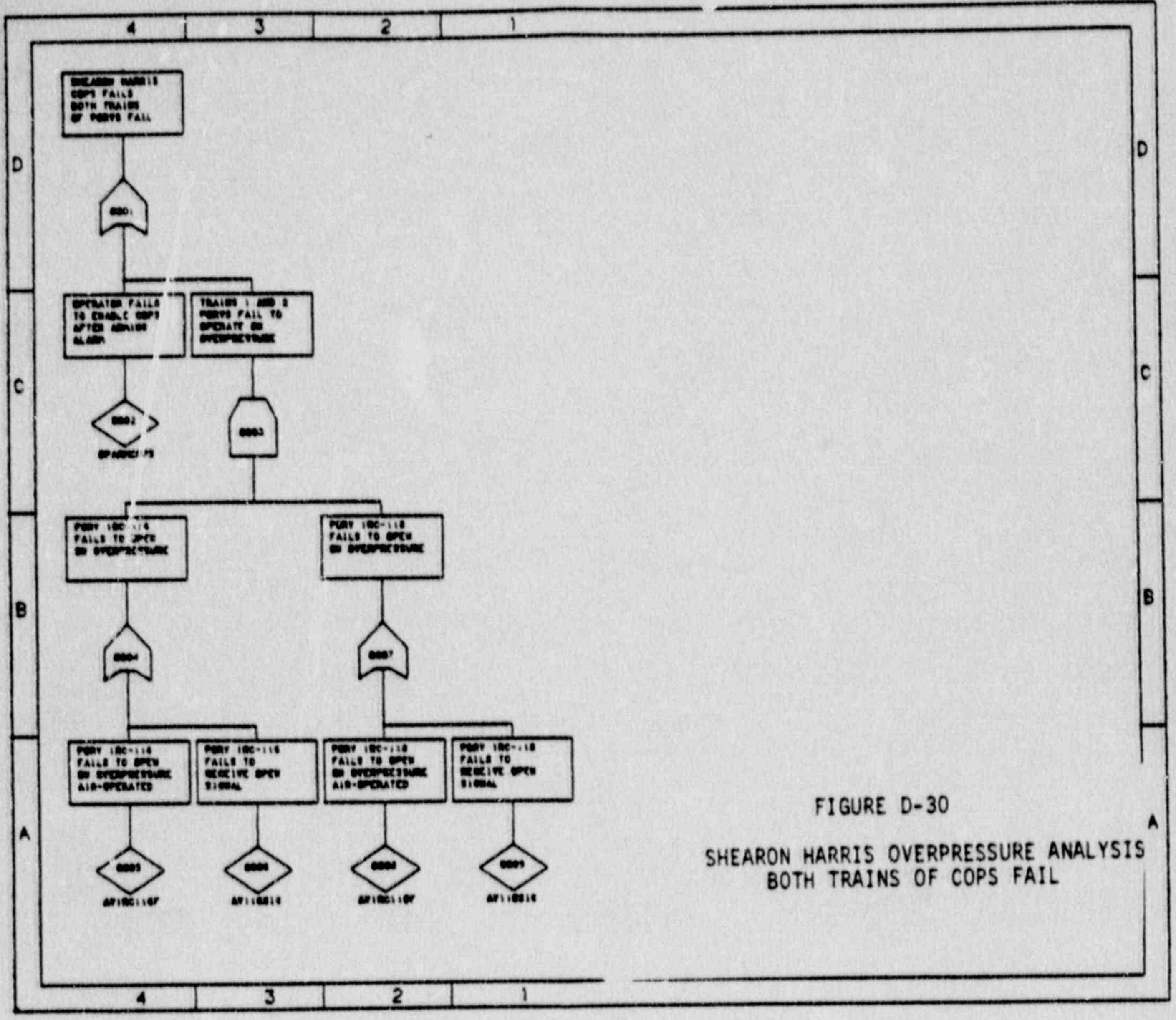


FIGURE D-30

SHEARON HARRIS OVERPRESSURE ANALYSIS
BOTH TRAINS OF COPS FAIL

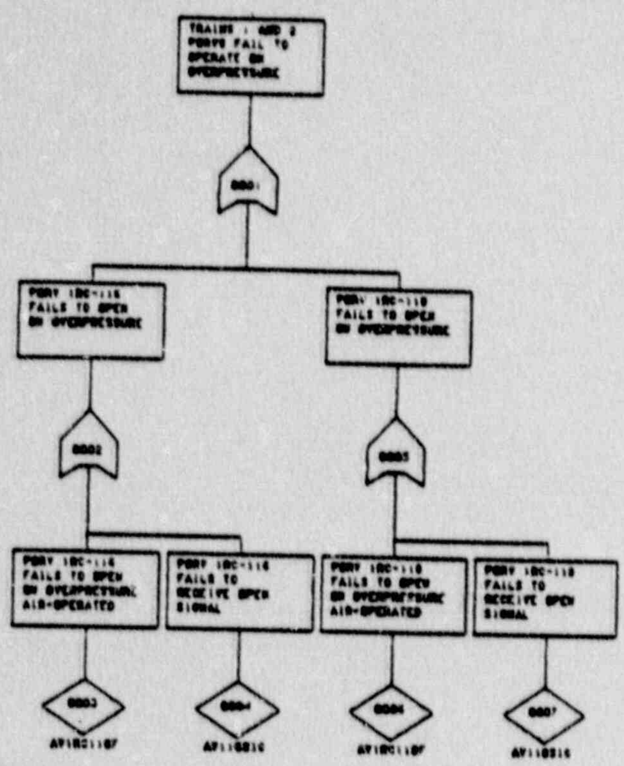


FIGURE D-31

SHEARON HARRIS OVERPRESSURE ANALYSIS
ONE OF TWO COPS TRAINS FAIL TO OPERATE

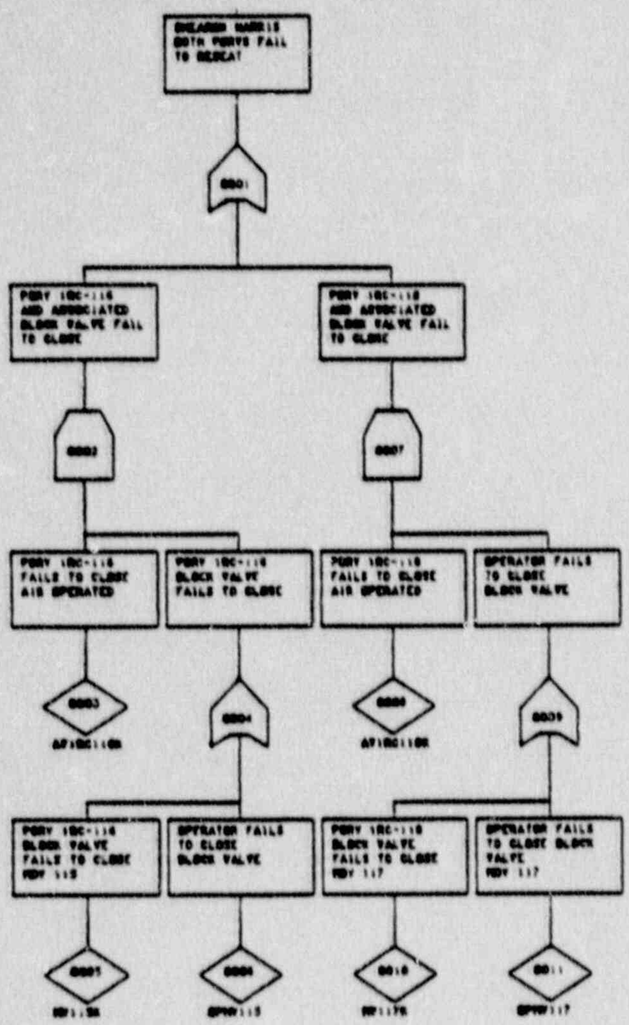


FIGURE D-32

SHEARON HARRIS OVERPRESSURE ANALYSIS
COPS PORVS FAIL TO RESEAT