WCAP-11117
Rev. 2.0

WESTINGHOUSE CLASS 3

RESIDUAL HEAT REMOVAL SYSTEM AUTOCLOSURE INTERLOCK REMOVAL REPORT FOR DIABLO CANYON NUCLEAR POWER PLANT

Revision 2.0

Pacific Gas and Electric Company
Contract No. Z12-5-238-85

JULY 1987

N. L. Burns
T. J. Gerlowski
R. M. Malinchak

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

0057v:1D/070187

TABLE OF CONTENTS

LIST OF TABLES

LIST OF TABLES (Cont)

LIST OF FIGURES

LIST OF FIGURES (Cont)

ABSTRACT

A review and analysis has been performed which justifies the deletion of the autoclosure interlock of the Residual Heat Removal System suction isolation valves (MOV-8701, MOV-8702). The open permissive circuitry remains intact. An alarm is added to notify the operator of an incorrectly positioned valve (MOV-8701, MOV-8702). A probabilistic analysis was used to determine that deletion of the autoclosure interlock is acceptable from a safety standpoint.

1.0 INTRODUCTION

Recently, the Nuclear Regulatory Commission (NRC) has expressed interest in the acceptability of removing the autoclosure interlock (ACI) on the Residual Heat Removal System (RHRS) suction isolation valves. This interest arises from a concern 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 autoclosure interlock circuitry. Isolation of the RHRS while operating could result in a loss of decay heat removal capability, overpressurization of the Reactor Coolant System (RCS) with possible power-operated relief valve (PORV) challenge, and/or RHRS pump damage.

This report provides an evaluation of the removal of the Residual Heat Removal System autoclosure interlock at the Diablo Canyon Nuclear Power Plant. The report reviews the basis for the interlock in terms of regulations and justifies removal of the autoclosure interlock based on a safety evaluation of the effect of autoclosure interlock removal on low temperature overpressure protection, RHRS availability and interfacing system LOCA potential.

1.1 Background

A U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of Operational Data, report (Reference 1) analyzed U.S. pressurized water reactor (PWR) experiences involving loss of an operating Decay Heat Removal (DHR) system. This report indicated that 130 loss of decay heat removal events were reported between 1976 and 1983. The consequences of a total loss of DHR system under certain conditions could lead to core uncovery, and resultant fuel damage. In addition, analysis of operating data revealed that an underlying or root cause of most loss of DHR system 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 DHR system (or RHRS) is operational.

Reference 1 lists summaries of loss of RHRS events that occurred during 1982 and 1983. A Nuclear Safety Analysis Center/Electric Power Research Institute report (Reference 2) identified loss of RHRS events for the period 1976 through 1981. Table 1-1 from Reference 1 is reproduced and provides a tabulation of these 130 DHR system losses for 33 plants during the period of 1976 through 1983. The leading category of loss of DHR system events (37 of 130) was an inadvertent automatic closure of the suction isolation valves in the RHRS. Most of these events were caused by human error. Table 1-2 is also reproduced from Reference 1 and tabulates the number of events for five categories of failure that cause a loss of RHRS operation and illustrates that 28.5% of the events were caused by inadvertent automatic closure of suction isolation valves.

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.

As stated in Reference 1, plant "operating data has shown that for RHRS operation, removal of power or removal of the autoclosure interlocks to the RHRS suction isolation valve can be a safe, effective method for preventing spurious suction isolation".

Also, 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 as part of Task A-45 evaluating the competing risks associated with RHRS suction isolation valve closures and Event V. The Sandia report (Reference 3), "Potential Benefits Obtained by Requiring Safety-Grade Cold Shutdown Systems," was done for the Calvert Cliffs plants' configuration. Subsequent to their quantification of risks, Sandia concluded that:

"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.

...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 melt 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 4, 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.

It is also important to note that Westinghouse has evaluated Kewaunee's proposal for removing the autoclosure interlocks on the RHRS suction valves. Reference 5 notes that Westinghouse's analysis concluded that for Kewaunee, the proposed modification would be a safety improvement. NRR has subsequently approved the modification. 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.

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	

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)

2.0 SUMMARY OF RESULTS

The analysis presented in this report supports removal of the autoclosure interlock. Based on prior operating experience, the autoclosure interlock has been a dominant contributor to the loss of decay heat removal. Spurious closure of the RHRS isolation valves due to false signals, deenergization of power buses and various testing errors has occurred steadily since the implementation of the ACI in the 1970s. Recently the effects of the spurious closure of these valves are being realized. An NRC report has determined that spurious closure of the RHRS isolation valves account for approximately 29 percent of the total RHR system failures. This report has raised a concern that the autoclosure interlock has become detrimental to overall safety. Most recent reports on the subject favor removal of the autoclosure interlock or some type of modification to the interlock.

However, before a change can be implemented, the NRC has requested that the effects of removal of the interlock be examined. Through examination of the interfacing systems LOCA frequency, the RHRS availability, and the effects on overpressurization transients, the results of this report show that there would be no net increase in risk consequences from removal of the interlock.

Two modifications to the autoclosure interlock were addressed in this report. The first modification considered was the addition of an alarm which would actuate if the RCS pressure increased above a given setpoint and either of the RHRS isolation valves is open. The other modification, a single switch to close both valves (based on NRC suggestions), will not provide adequate assurance that the valves are closed. An alarm would have to be installed to alert the operator of a high RCS pressure and that the RHR suction valves are open. Based on the analyses presented in this report, a single switch and alarm configuration does not result in an appreciable change in safety as compared to the modification that includes an alarm only. Furthermore, during leak rate testing of the valves, the single switch would have to be overridden or bypassed in order to singularly test each isolation valve. Therefore, the design change that is recommended for Diablo Canyon is the deletion of the autoclosure interlock and the addition of an alarm.

3.0 LICENSING BASIS

3.1 History

During the 1960's, typical RHR systems for a pressurized water reactor plant consisted of twin (auxiliary) coolant trains connected to the RCS via a single suction line. Two closed valves in series isolated the RHRS from the RCS while the RCS was in operation. A "prevent-open" interlock was added to one of the valves to prevent its opening while RCS pressure was above RHRS design pressure. The second valve had its power disconnected via administrative procedures. As an additional design feature, the valve motor operator was sized with insufficient torque to move the disc with a pressure differential greater than 600 psi. Finally, a relief valve set at RHRS design pressure was located just downstream of the suction valves.

The early 1970's saw the Atomic Energy Commission (AEC) pressing for a pressure interlock on both valves. (Reference 6). As two suction lines were also starting to make their appearance, the AEC position was extended to four suction isolation valves. Other AEC positions that evolved at that time (1971) were 1) interlocks for automatic closure on pressure, 2) diverse principles for interlocks, and 3) commitment to IEEE-279. Table 3-1 provides a brief impact of these requirements and some of the plants affected.

The introduction of the autoclose interlock re-emphasized a previous concern, i.e. RCS pressure control during RHRS operation. Spurious closure of the suction valves isolates the suction line relief valves and the low pressure letdown line from the RHRS 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, subsequently aggravating the transient. (Reference 7 & 8)

A joint meeting between industry (W, B&W, and CE) and AEC in March 1974 attempted to clarify the AEC's requirement for the interlocks. (Reference 9)

This discussion brought about two acceptable methods of overpressure protection while the RHRS is in operation or when returning the RCS to operation (Reference 10):

- o automatic closure interlocks, or
- o sufficient capacity of the RHRS suction line relief valves, or
- o a combination of the above

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 RCPB) 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. (Reference 11)

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 a Branch Technical Position in the summer of 1975. (Reference 12)

Faced with the requirement for retaining the autoclosure interlock, discussion with the NRC centered on raising the setpoint such that the autoclosure feature did not prematurely isolate the RHRS. This was in conjunction with lowered setpoints for the RHRS suction line relief valves (to 450 from 500 psig), to allow the relief valves to perform. The raised autoclosure setpoint, however, did not preclude transients initiated by a spurious closure of the valves. (Reference 13)

The Safety Evaluation Report (SER) for the RESAR-41 application provided the final NRC position on the issue (Reference 14). While Branch Technical Position ICSB-3 required that "the valve operators should 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 will be equipped with autoclosure and prevent-open interlocks to prevent possible exposure of the residual heat removal system to excessive pressures. The interlocks will 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."

The situation of a possible loss-of-coolant accident would exist should an operator neglect to close one of the series isolation valves when the plant is returned to normal pressure. Passive failure of the closed valve disc would expose the RHRS to full RCS pressure, resulting in a possible rupture of the RHRS outside containment. Then the NRC recognized an autoclosure setpoint above the RHRS design pressure separated the autoclosure feature from pressure transient mitigation. The requirement, then, was to demonstrate the adequacy of the relief valves.

The industry experienced problem of loss of RHRS capability and possible pump damage following a failure of the autoclosure interlock was reviewed in conjunction with the RESAR-3S application (Reference 15). Actions taken by several utilities were to remove power from one or more of the suction valves during the timeframe when the RHRS pumps are most susceptible to damage due to loss of suction (i.e. refueling). Westinghouse recommended this via a technical bulletin in mid-1977 (Reference 16). Various other publications also dealt with the issue (References 17 & 18).

Use of the pressurizer power-operated relief valves in conjunction with the RHRS relief valves was reviewed and found acceptable by the NRC. While the NRC did recognize the higher (above RHRS design pressure) setpoint, they stopped short of permitting the removal of the autoclosure feature from the plant (Reference 19).

In 1977, Working Group ANS-56.3 (previously ANS-32.4 and ANS-55.4) finished work on ANSI/ANS-56.3-1977 (Reference 20). This standard permitted the designer a choice between a suction valve automatic closure feature and relief valves having adequate relieving capacity. The standard also stated that:

> "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 was published by Oak Ridge National Laboratory detailing the review and evaluation of events placed in the NSIC file involving the removal of decay heat in US BWRs and PWRs from June 1979 through June 1981 (Reference 21). The Oak Ridge study reported that during the two-year period "the most frequent event involving a significant problem with DHR system was the cavitation of RHRS pumps". Five events were traced to spurious closure of the suction valves due to signals from their autoclosure interlocks.

Shortly thereafter, an EPRI report also detailed events where RHRS operation was curtailed due to inadvertant suction valve closure (Reference 2). 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 feature has been reviewed against applicable regulatory and industry safety standard criteria.

3.2.1 ANSI/ANS 56.3-1977

"Overpressure Protection of Low Pressure Systems Connected to the Reactor Coolant Pressure Boundary".

Section 3 of this standard 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 plan operating condition when the two valves are open. Figure 1 of the standard depicts these methods.

Following removal, the method of overpressure protection provided is that depicted in Figure 1 as 1(b).

3.2.2 Standard Review Plan

"Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plant," NUREG-0800, July 1981.

The NRC position is stated in two branch technical position papers: RSB 5-1 and ICSB 3. ICSB 3, 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."

Position B.1. of RSB 5-1 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 RSB position is clear in that an autoclosure interlock must be utilized and its setpoint must be tied to the RHRS design pressure. The ICSB position however does not emphatically require an autoclosure interlock.

While the ICSB position makes no mention of relief valves, 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. <u>Pump Protection Requirements</u>

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 regards it as optional) is compounded by the NRC's acceptance of the autoclosure setpoint above RHRS design pressure. As events from the past few years have shown loss of RHRS cooling to be a more serious and more frequent transient than overpressure transients, emphasis should be placed on the recognized pump protection requirements of RSB 5-1.

An April 17, 1984 NRC memorandum (Reference 22) discussed a clarification of the design basis of RHRS interlocks and a concern centered on the safety implications of the failure mode of interlocks due to a loss of an instrument bus. Reference 22 concludes that:

"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 W plants such that a loss of an instrument bus will not result in a loss of RHRS cooling. Also, it is recommended that action be taken to clarify the purpose of the RHRS interlocks for the Diablo Canyon record as well as any required changes."

A January 1985 RSB position states that (Reference 5):

"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."

3.2.3 10CFR50.59

This section 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 technical specifications or an unreviewed safety question.

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 the Diablo Canyon Nuclear Power Plant, Units 1 and 2", NUREG-1151 does not contain a similar surveillance requirement.

Thus 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 that needs to be addressed is (i) as defined above: 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?

Section 6.6 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 overpressurization event does increase, the increase is from E-14 to E-12 and is considered to be insignificant and offset by the reduction in frequency of Event V and the slight 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.

Addressing the second question (ii) as defined above: is the possibility of an accident or malfunction of a different type than any evaluated previously in the safety analysis report created?

Chapter 15.0 of the Diablo Canyon Final Safety Analysis Report states that the analysis of an RHRS overpressurization accident, requested in Reg. Guide 1.70, rev. 1, is not necessary because the RHRS interlocks makes the overpressurization of the RHRS extremely unlikely.

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 RHRS 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 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. The interlock function is to preclude conditions that could lead to a LOCA outside of containment due to operator error. The interlock function is not to isolate the RHRS from the RCS when the RHRS is operating in the decay heat mode.

There are several levels of defense which would assure 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 alarms that sound a "valve not full closed" signal in conjunction with a "RCS pressure - high" signal. The intent of these alarms is to alert the operator that either of the RCS-RHRS isolation valves is not fully closed, and the 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 at a higher pressure.

Thus, removal of the RHR ACI does not create the possibility of an accident different than that described in the DCPP FSAR Update. RHR overpressurization in shutdown modes is prevented because of the addition of alarms to warn the operator of "valve not full closed" and the relief capacity of the RHR safety valves. In operating modes, the open permissive interlocks function to prevent the opening of the RHRS suction/isolation valves when the RCS is at high pressure. The open permissive interlocks are not affected by the proposed ACI removal.

Item (iii) does not apply as the autoclosure interlock is not used as a basis for any technical specifications.

3.2.4 10CFR50, Appendix R

Appendix R governs the Fire Protection Program to be applied to all nuclear power plants, and states that "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." Given that the result of the PRA portion of this report justifies the deletion of the autoclose interlock based on a criterion of availability and reliability the RHR system is made in effect, more available, this change does not adversely impact the current Diablo Canyon Appendix R Fire Protection Safety Analysis Report. Of course, changes made as a part of the autoclose deletion must be reviewed by the customer and made in accord with Appendix R requirements that apply to Diablo Canyon, such as train separation, fire barriers, fire hazards analyses, etc. as defined in section III.G. of Appendix R to 10CFR50.

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
(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	4 Loop Plants 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.	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.	Shearon Harris, 1,2,3,4 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.		

0205x:1b-040886

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.

0205x:1b-040386

4.0 RESIDUAL HEAT REMOVAL SYSTEM

4.1 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. To effect this, the RHRS transfers heat from the RCS to the Component Cooling Water System (CCWS) to reduce reactor coolant temperature to the cold shutdown temperature at a controlled rate during the latter part of normal plant cooldown and maintains this temperature until the plant is started up again.

As a secondary function, the RHRS also serves as part of the Emergency Core Cooling System (ECCS) during the injection and recirculation phases of a LOCA. The RHRS is also used to transfer refueling water between the refueling water storage tank and the refueling cavity before and after the refueling operations.

4.2 System Description

A schematic diagram of the RHRS is present in Figure 4-1. The RHRS consists of two heat exchangers, two motor-driven pumps and the associated piping, valves and instrumentation necessary for operational control. The inlet line to the RHRS is connected to the hot leg of reactor coolant loop 4, while the return lines are connected to the cold legs of each of the reactor coolant loops.

The RHRS suction line is isolated from the RCS by two motor-operated valves in series while the discharge lines are isolated by two check valves in each line. The RHRS isolation valves and the inlet line pressure relief valve are located inside containment while the remainder of the system is located outside containment.

During system operation, reactor coolant flows from the RCS to the RHRS pumps, through the tube side of the RHRS exchangers and back to the RCS. The heat is transferred in the RHRS exchangers to the component cooling water circulating through the shell side of the heat exchangers.

Coincident with RHRS operations, a portion of the reactor coolant flow may be diverted from downstream of the RHRS heat exchangers to the 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. Pressure regulation is necessary to maintain the pressure range dictated by the fracture prevention criteria requirements of the reactor vessel and by the No. 1 seal differential pressure and NPSH requirements of the RCPs.

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

4.3 System Operation

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

Reactor Startup

Generally, during cold shutdown, residual heat from the reactor core is being removed by the RHRS. The number of pumps and heat exchangers in service depends on the RHRS load at the time.

At initiation of 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 via a line that is connected to the common header downstream of the RHRS heat exchanger. Indication of steam bubble formations is provided in the control room by the damping out of the RCS pressure fluctuations and by pressurizer level indication. The RHRS is then isolated from the RCS and the system pressure is controlled by normal letdown and the pressurizer spray and pressurizer heaters.

Power Generation and Hot Standby Operation

During power generation and hot standby operation, the RHRS is not in service but is aligned for operation as part of the ECCS.

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 steam generators.

When the reactor coolant nominal temperature and pressure are reduced to < 350°F and less than 425 psig, respectively, 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 RHRS heat exchangers is increased.

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 pressure is reduced and the temperature is 140°F or lower, the RCS may be opened for refueling or maintenance.

Refueling

Both RHRS pumps are utilized during refueling to pump borated water from the refueling water storage tank 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 inlet isolation valves are opened, the Refueling Water Storage Tank (RWST) supply valves are closed, and RHRS operation resumes.

During refueling, the RHRS is maintained in service with the number of pumps and heat exchangers in operation as required by the heat load.

Following refueling, the RHRS pumps are used to drain the refueling cavity to the top of the reactor vessel flange by pumping water from the RCS to the Refueling Water Storage Tank.

4.4 Component Description

This section describes the major components of the RHRS.

RHRS Pumps

Two pumps are installed in the RHRS. The pumps are sized to deliver sufficient reactor coolant flow through the RHRS 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 RHRS pumps are protected from overheating and loss of suction flow by miniflow bypass lines that provide flow to the pump suction at all times. 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 when the RHRS pump discharge flow is less than 500 gpm and close when the flow exceeds 1000 gpm.

A pressure sensor in each pump discharge header provides a signal for an indicator in the control room. A high-pressure alarm is also actuated by the pressure sensor.

The two 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.

RHRS Heat Exchangers

Two 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

8701, 8702, Inlet Isolation Valves
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 8701 and 8702 are interlocked with RCS pressure transmitters PT-405 and PT-403, respectively. These interlocks prevent the inadvertent opening of the valves, 8701 and 8702, when the RCS pressure is above approximately 390 psig. Both valves also close automatically when the RCS pressure is higher than approximately 700 psig.

Also, valve 8702 is interlocked such that it cannot be opened if the temperature in the pressurizer vapor space (T-454) is above a temperature corresponding to a saturation pressure which would cause overpressurization of the RHRS.

A more detailed description of the interlocks is provided in Section 5.0.

8700A, 8700B, Pump Suction Isolation Valves

These valves are motor-operated gate valves which are normally open except when the RHRS is used as part of the Safety Injection System (SIS) during the recirculation phase. An interlock is provided between valve 8700A (8700B) and valves 8982A (8982B), 9003A (9003B) and 8804A (8804B) to prevent the opening of the suction valve without closing the others.

HCV-637, HCV-638, Heat Exchanger Flow Control Valves

These valves are air-operated butterfly valves which may be positioned from the main control room. By manually adjusting these valves, the flow through the heat exchangers may be controlled.

HCV-670, Bypass Flow Control Valves

This valve, located in the heat exchanger bypass line, is an air operated butterfly valve which may be positioned from the main control room. By adjusting the valve the bypass flow around the heat exchangers may be changed to regulate the residual return flow temperature, and in conjunction with HCV-637 and 638 the total return flow. The line containing the valve is isolated from the RHRS pumps and heat exchangers by two manual gate valves in the piping cross-tie between the RHRS pumps and heat exchangers. These valves are opened prior to initiation of residual heat removal operations.

FCV-641A, FCV-641B, Miniflow Stop Valves

These normally closed valves are motor-operated globe valves which are located in the residual heat removal pump miniflow line. The valves are controlled by flow transmitters FIC-641A and FIC-641B, respectively, which are located in the discharge line of the RHRS pump. 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.

8716A, 8716B, Crosstie Valves

These motor operated valves, located in the piping crosstie downstream of the residual heat exchangers, are normally open during normal plant operating and

RHRS operation. These valves are controlled from the main control board and fail "as is". These valves are used to align the RHRS for the recirculation phases following a loss of coolant accident.

8948A, 8948B, 8948C, 8948D, RHRS Injection Line Check Valves

There is one check valve in each branch of the cold leg injection line to prevent backflow from the RCS.

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

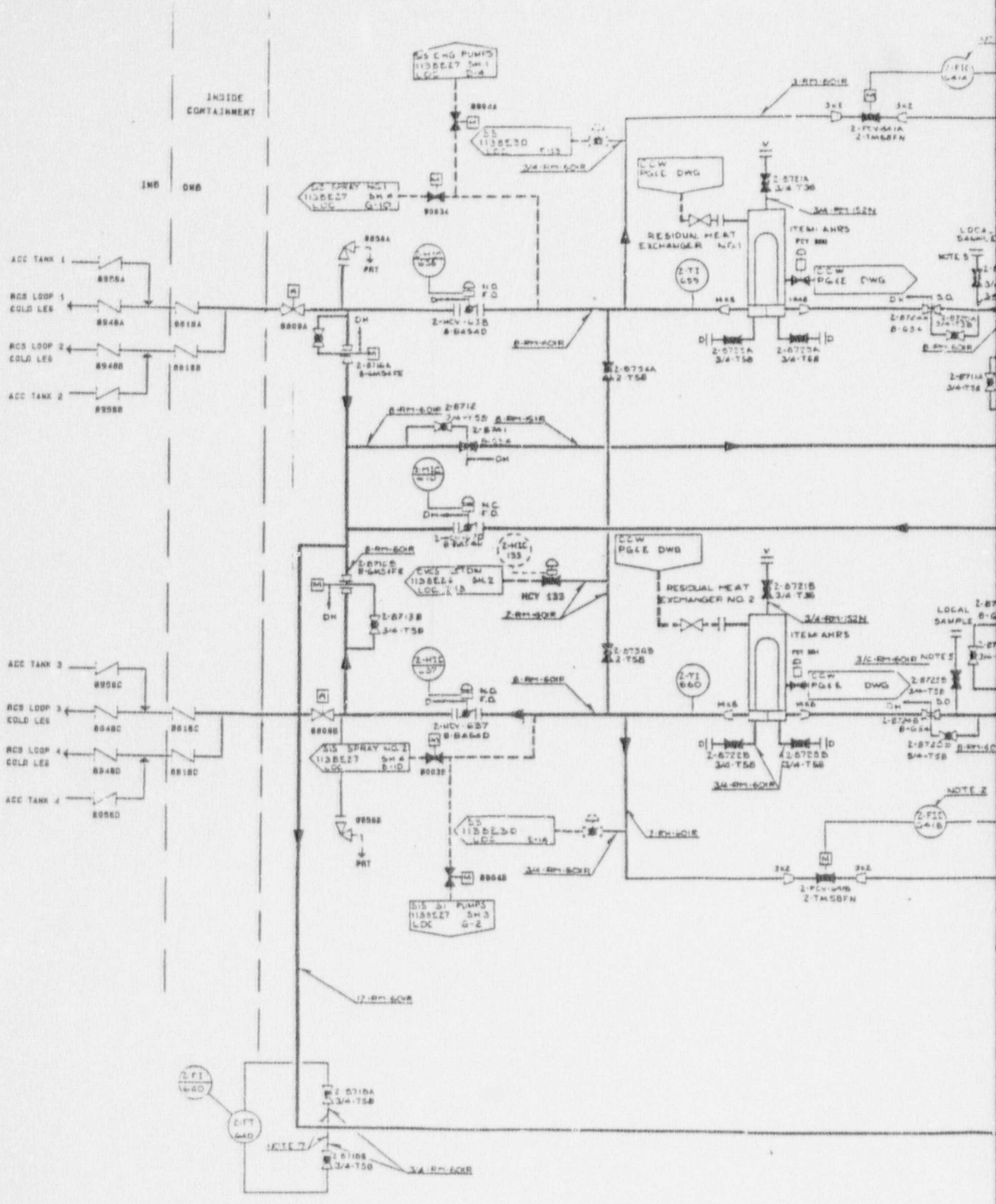
One check valve is located in each branch of the RHRS return line to serve as a backup in the event of leakage of the check valves on the cold leg injection line.

8809A, 8809B Gate Valve

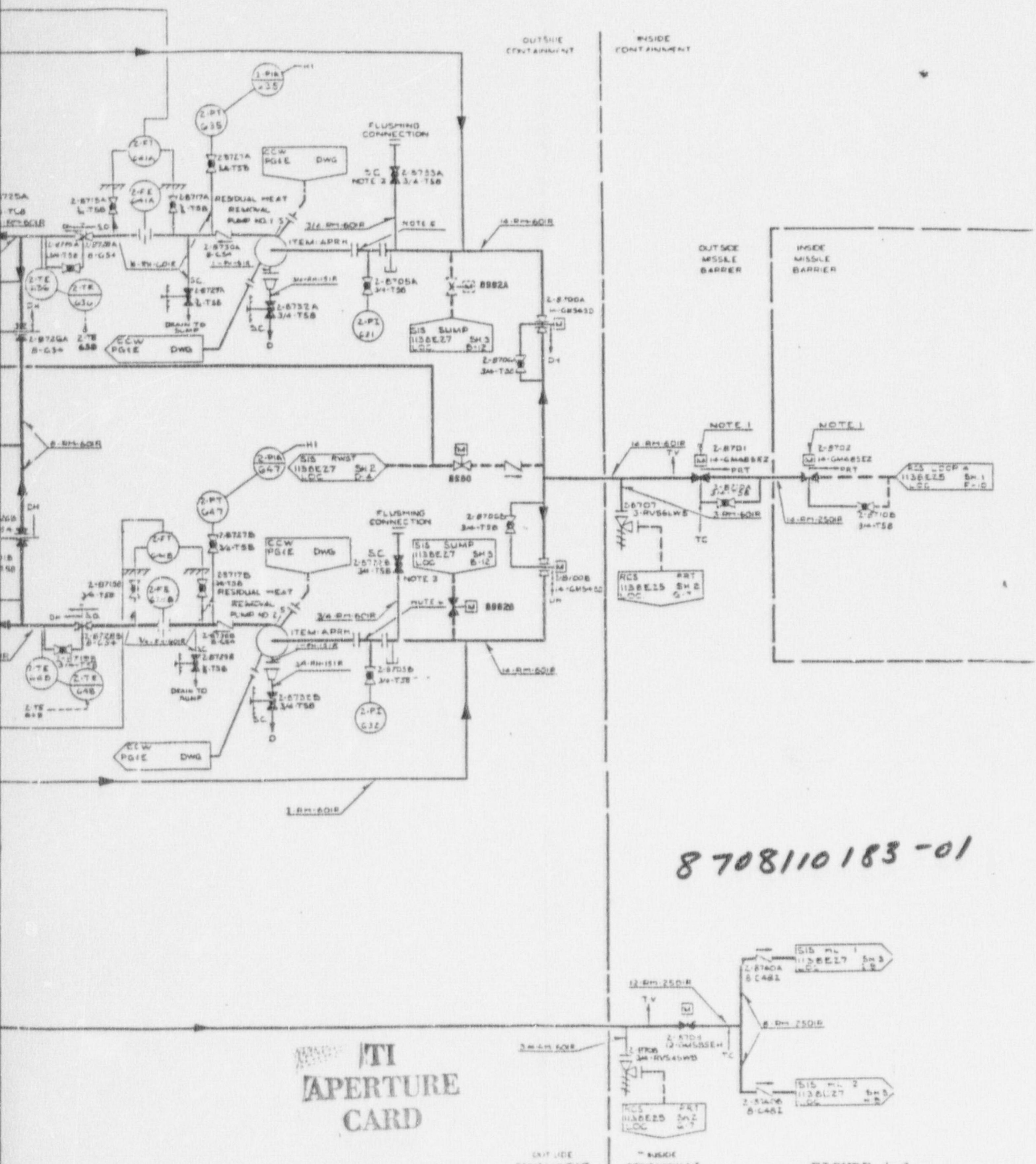
There is an eight-inch normally open, motor-operated gate valve in each parallel discharge line from the residual heat removal pump, downstream of the heat exchanger and discharge crosstie header.

8726A, 8726B Crosstie Valves

These two manual gate valves isolate the heat exchanger bypass line. During startup of the RHRS, these valves must be opened.



INSIDE CONTAINMENT
INB
DWB
ACC TANK 1
RCS LOOP 1 COLD LEG
RCS LOOP 2 COLD LEG
ACC TANK 2
ACC TANK 3
RCS LOOP 3 COLD LEG
RCS LOOP 4 COLD LEG
ACC TANK 4
SIS CHG PUMPS 113BE27 SH 1 LOC D-4
SIS SPRAY NO 1 113BE27 SH 4 LOC G-10
SIS SPRAY NO 2 113BE27 SH 4 LOC D-10
SIS SI PUMPS 113BE27 SH 3 LOC G-2
RESIDUAL HEAT EXCHANGER NO 1
RESIDUAL HEAT EXCHANGER NO 2
CCW PG&E DWG
ITEM AHRS
CVCS LETDN
HCV 133
2-TI 659
2-TI 660
2-FT 640
2-FI 640
2-HCV-638
2-HCV-637
NOTE 2
NOTE 5
NOTE 7
LOCAL SAMPLE
PRT
12-RM-60IR
8-RM-60IR
3/4-RM-60IR
3/4-RM-152N
2-TM58FN



8708110183-01

APERTURE CARD

Also Available On Aperture Card

FIGURE 4-1
RHRS FLOW DIAGRAM

5.0 PROPOSED MODIFICATION

To effect the removal of the autoclosure interlock (ACI), certain modifications must be made to the Diablo Canyon Plant. These changes fall into two categories: modifications to the electrical design, and modifications to the operating procedures. The following text defines the functional requirements for these changes, and actual implementation of the changes will be by Pacific Gas & Electric. The model used in the analysis for this report is based on an assumed method of implementation; this method was chosen based on inputs from both Pacific Gas & Electric and Westinghouse. The final modifications made to Diablo Canyon, both electrically and procedurally, must meet the given functional requirements to ensure validity of this report.

5.0.1 Current Interlocks

There are two normally closed motor operated series isolation valves in the RHR pump suction line from the RCS loop 4 hot leg. Valve 8702 is the first valve from the RCS and 8701 is second. The interlock feature provided for both valves is essentially identical in function. Each valve is interlocked against opening unless the RCS pressure as measured by appropriate channels is less than approximately 390 psig; in addition, valve 8701 is also interlocked with RCS temperature and will not be permitted to open unless the RCS temperature is less than 475°F. Each valve is also interlocked to automatically close on increasing RCS pressure greater than 700 psig; for valve 8701, both RCS pressure and temperature are required for the valve to automatically close. These interlocks are shown functionally on Figures 5-6 and 5-7, and also are shown on elementary wiring diagrams in Figures 5-8 and 5-9. Currently, the valve control via the interlocks is shown in the center of the elementary diagrams as a single line circuit comprised of contacts that close when the appropriate conditions are met; i.e., auto-close for valve 8701 functionally receives inputs from PC-405BX and TC454, and valve 8702 receives inputs from PC403BX. The open permissive is similarly shown. As can also be seen on Figures 5-8 and 5-9, marked revisions which implement the deletion of the auto-close interlock are shown. These are encircled by clouds and are explained in section 5.1.1 through 5.1.3.

5.1 Functional Requirements

The items included in the functional requirements are discussed below.

5.1.1 Alarms are to be provided (for each valve in the RHRS suction line) that sound given a "valve not full closed" signal in conjunction with a "RCS pressure-high" signal. See Figures 5-1 and 5-2. The intent of these alarms is to alert the operator that either of the RCS-RHRS isolation valves in series is not fully closed, and the double valve isolation from the RCS to the RHRS is not intact. Valve position indication input to this alarm must be from the valve Stem Mounted Limit Switches (SMLS) and power to that 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 power lockout. (See Figure 5-3) The elementary wiring diagrams also show the alarm circuits for the valves. These were added to the upper right position of the diagrams, and indicate a monitor light, an annunciator, a power source, a pressure input, and a valve position input. Also note 3 has been added which specifies that the valve position must be input whenever the valve is not fully closed. This alarm must be verified safety grade just as other safety-related alarms would be, such as those occurring for Refueling Water Storage Tank Level.

5.1.2 The autoclosure portion of the current interlock will be removed, shown functionally on Figures 5-4 and 5-5. The only change is removing the autoclose portion, as the open permissive circuit will not be altered. The original interlocks are shown on Figures 5-6 and 5-7, for comparison. The elementary wiring diagrams also show the auto-closure portion deletion simply by disconnecting the autoclose input line from contact 5 on each valve. This will effect the minimal plant required changes, and will also provide positive invalidation of the autoclose interlock. These changes are marked in the lower central portion of the diagram. Note that inputs will still be made to the interlock; however the contact(s) will never be closed by the autoclose signal, and thus the valve will never close from an "autoclose" signal.

5.1.3 The plant specific operating procedures for heatup from cold shutdown to hot standby must be modified to reflect the appropriate (new) alarm recognition and responses for the added alarms. These new procedure sections will verify that the operator takes steps to close the open valve, or if this is not possible, to return to the shutdown mode of operation.

Overall, the functional requirements reflect the deletion of the ACI, while retaining the open permissive portion of the interlock.

5.2 Alternative Modification

In the determination of the modification which would be proposed, considerations were given to many factors including regulatory requirements, systems design, and minimizing plant changes. The set of changes which best meet all of the considerations was chosen as the proposed modification as defined in Section 5.1. Other modifications were considered, but did not meet all the criteria as well as the proposed modification. For example, a single switch capable of closing both valves in series (instead of separate switches for each valve) was also considered. However, from a reliability standpoint, the single switch and alarm versus an alarm only, provides no significant advantage. Furthermore, in order to test the isolation valves for leakage, pursuant to Technical Specification Surveillance Requirement 4.4.6.2.2, the single switch circuitry would have to be bypassed or overridden so that each valve could be "demonstrated operable by verifying leakage to be within its limit ..." (Reference 29). Thus, the alarm modification supports the "minimum-change" concept with respect to plant design changes and operations.

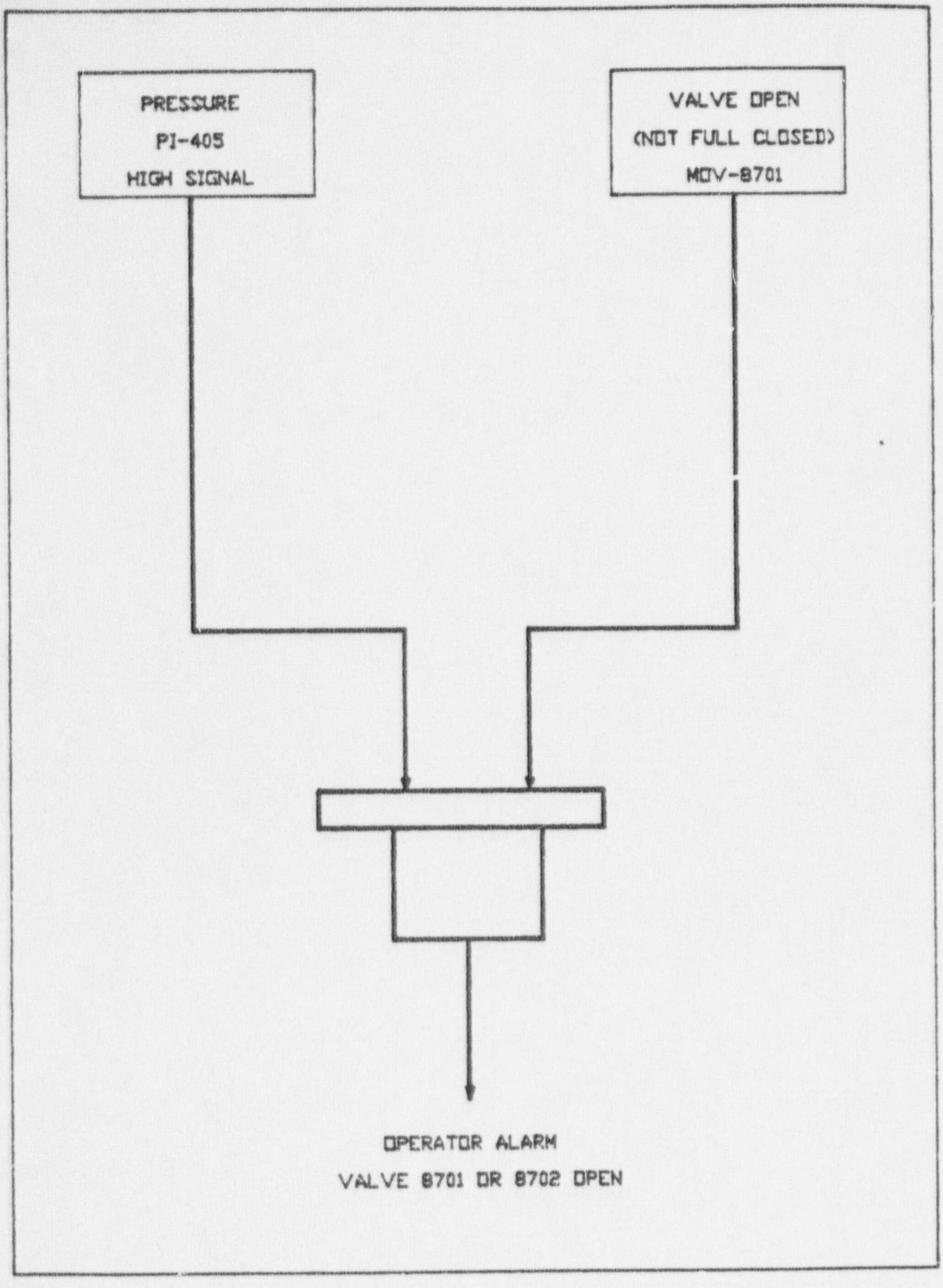


FIGURE 5-1

VALVE ALARM - MOV-8701

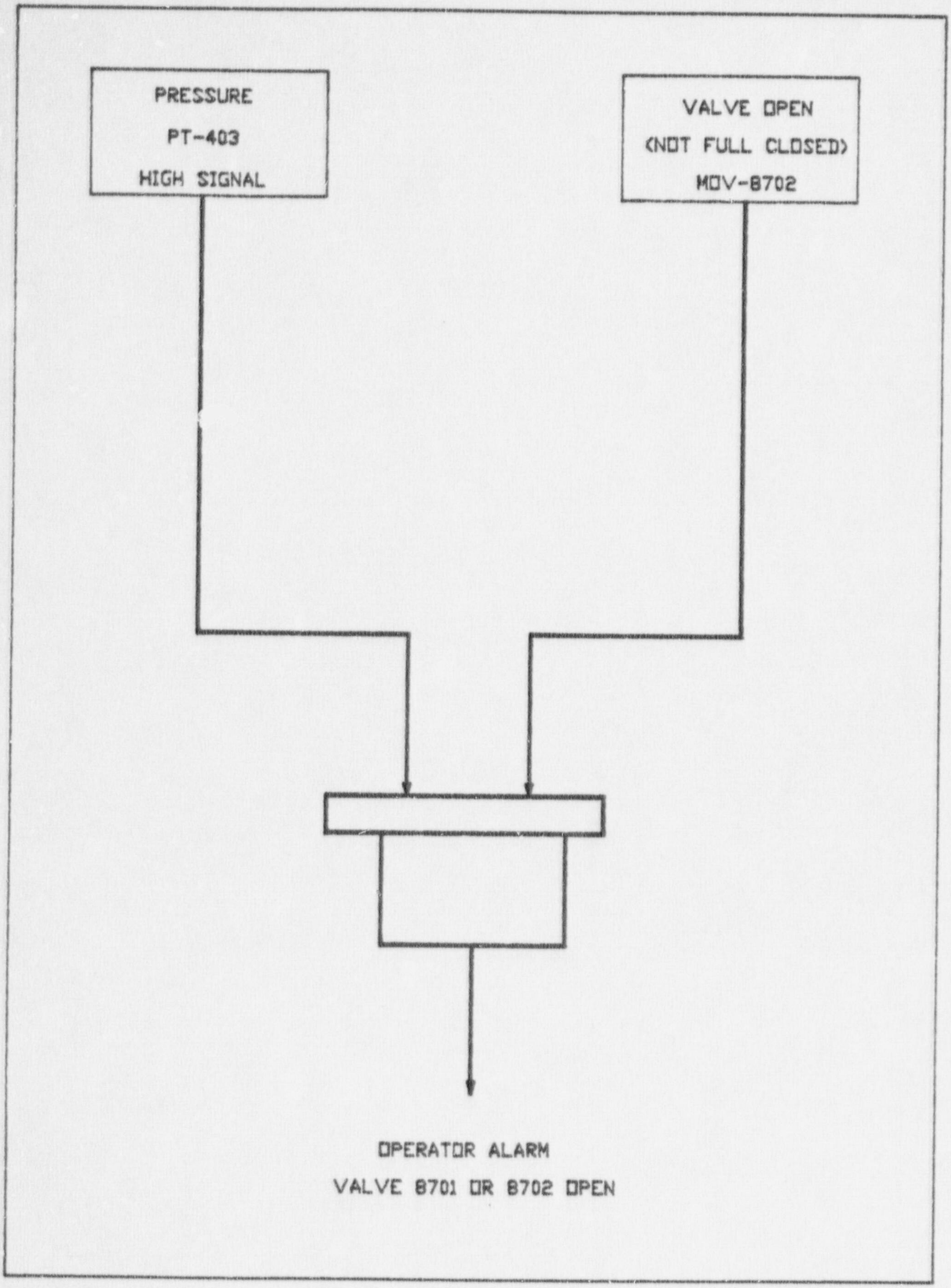


FIGURE 5-2

VALVE ALARM - MOV-8702

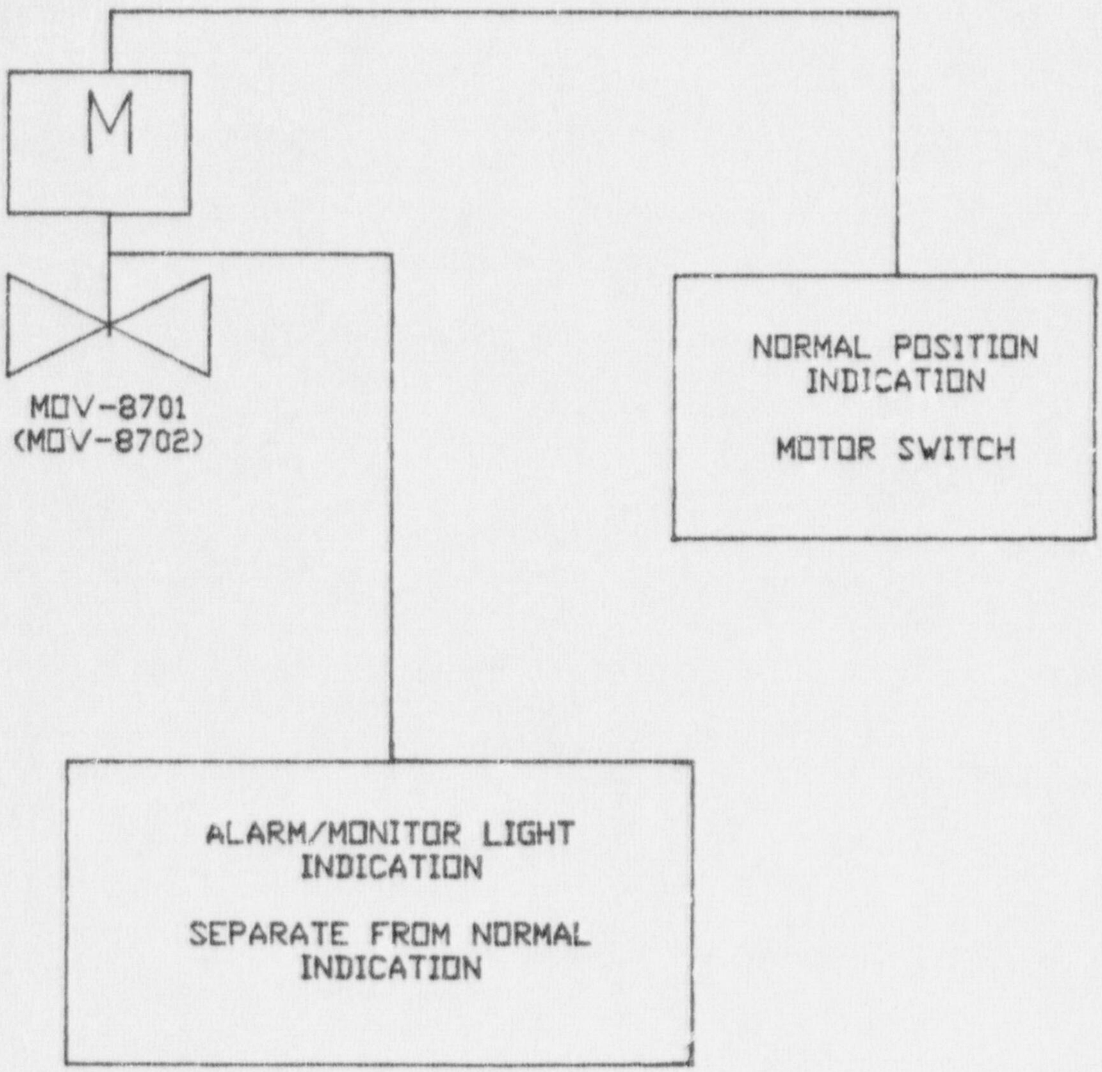


FIGURE 5-3

POSITION INDICATION

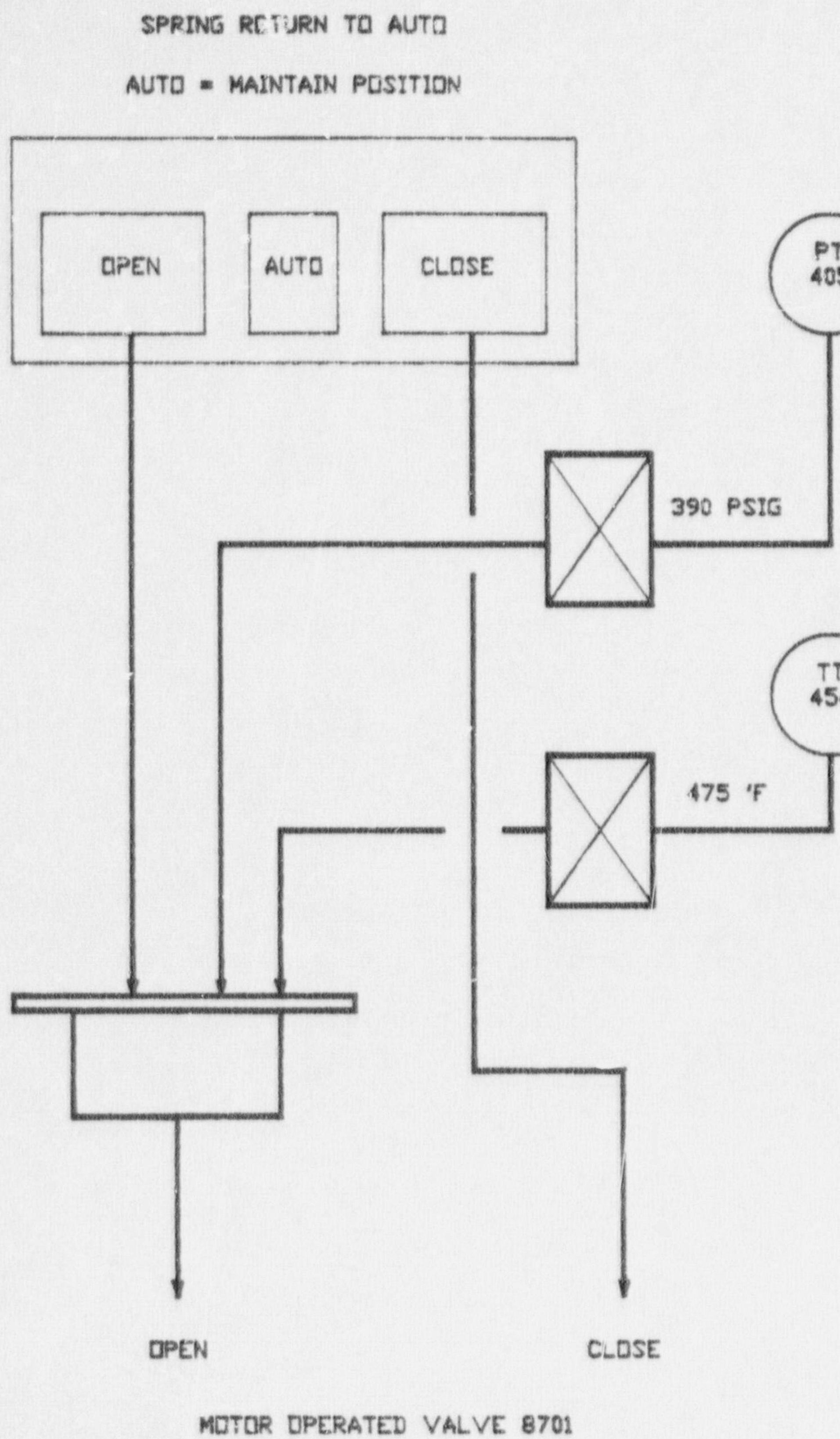


FIGURE 5-4

PROPOSED INTERLOCK - MOV-8701

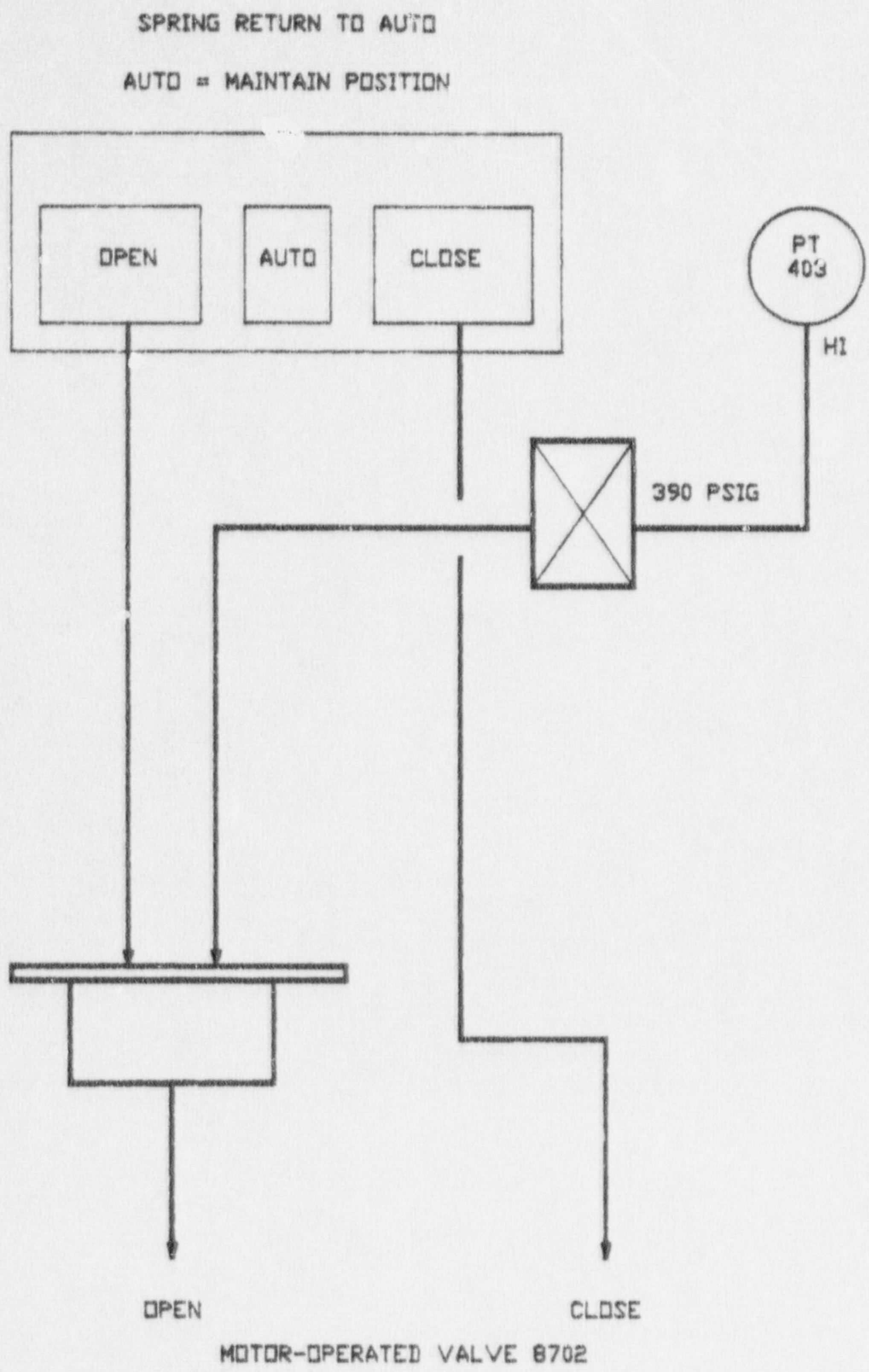


FIGURE 5-5

PROPOSED INTERLOCK - MOV-8702

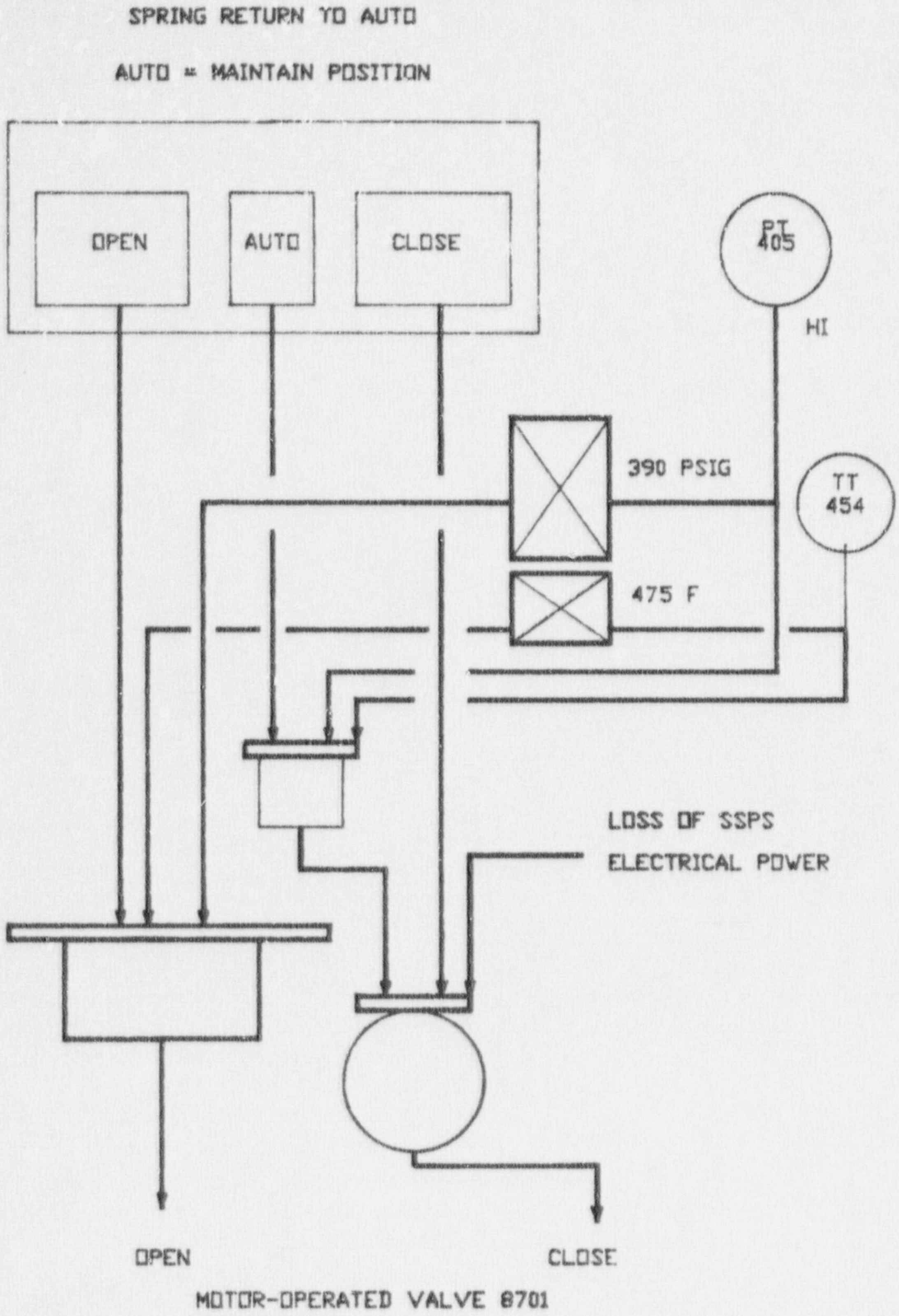


FIGURE 5-6

CURRENT INTERLOCK - MOV-8701

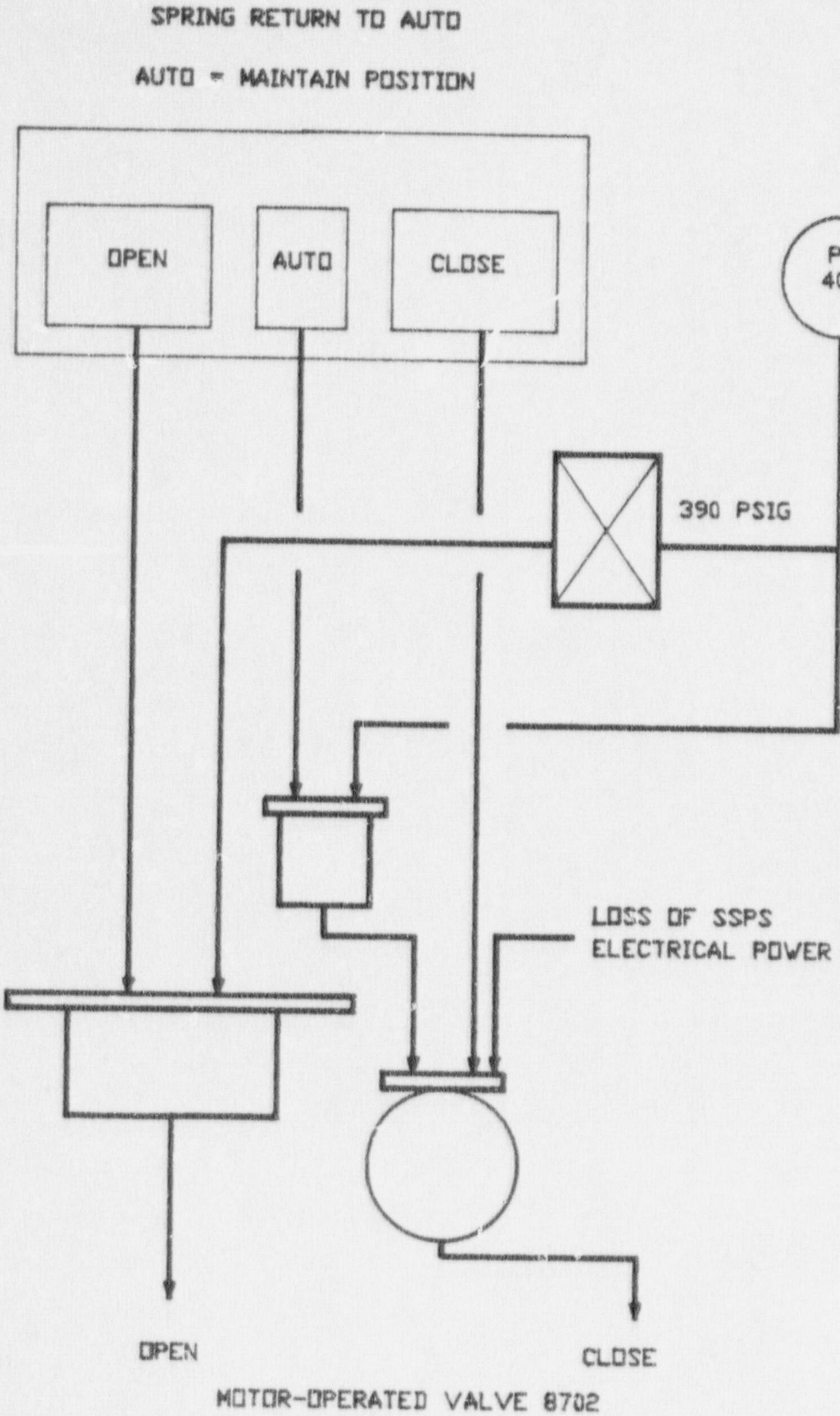
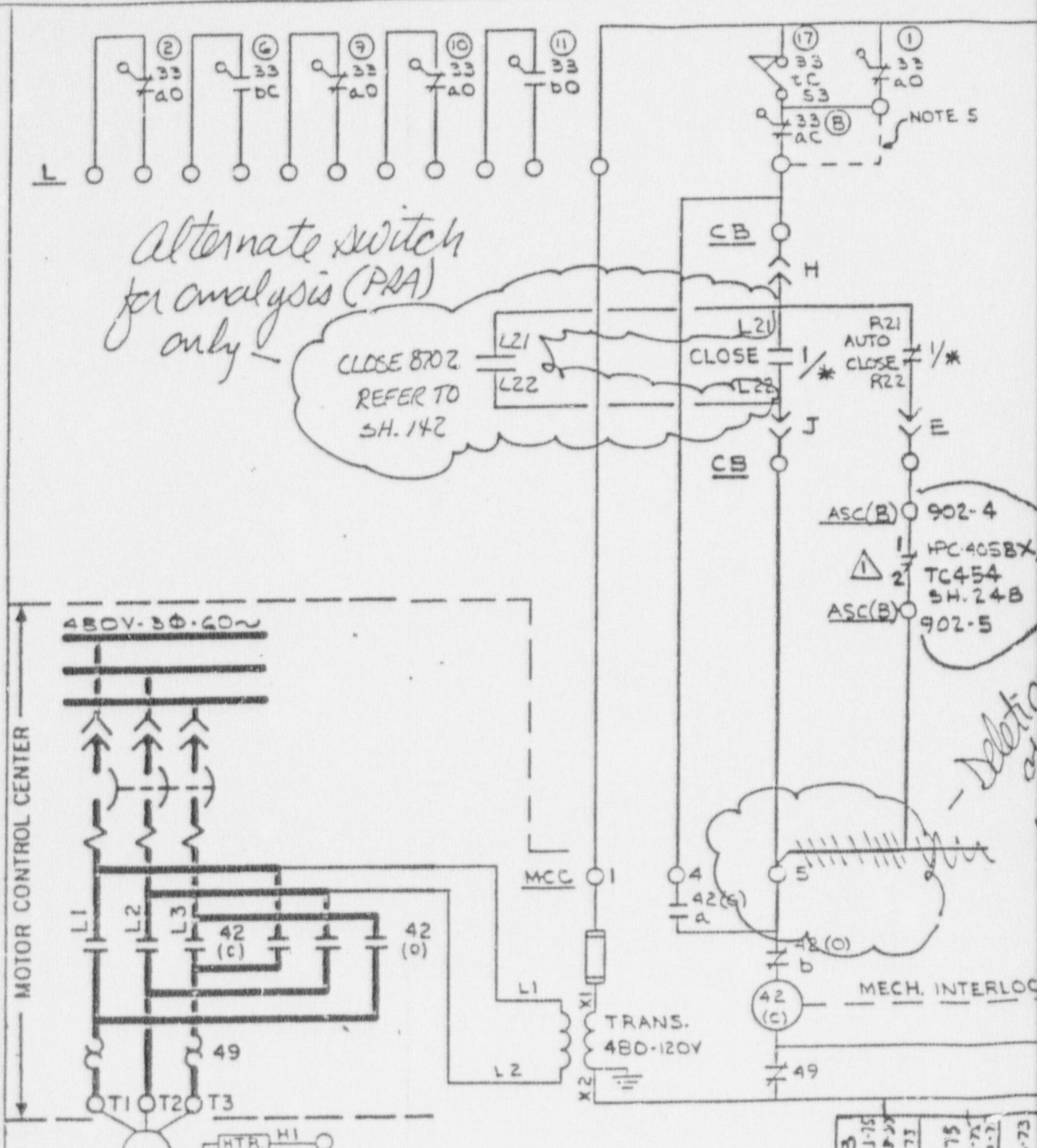


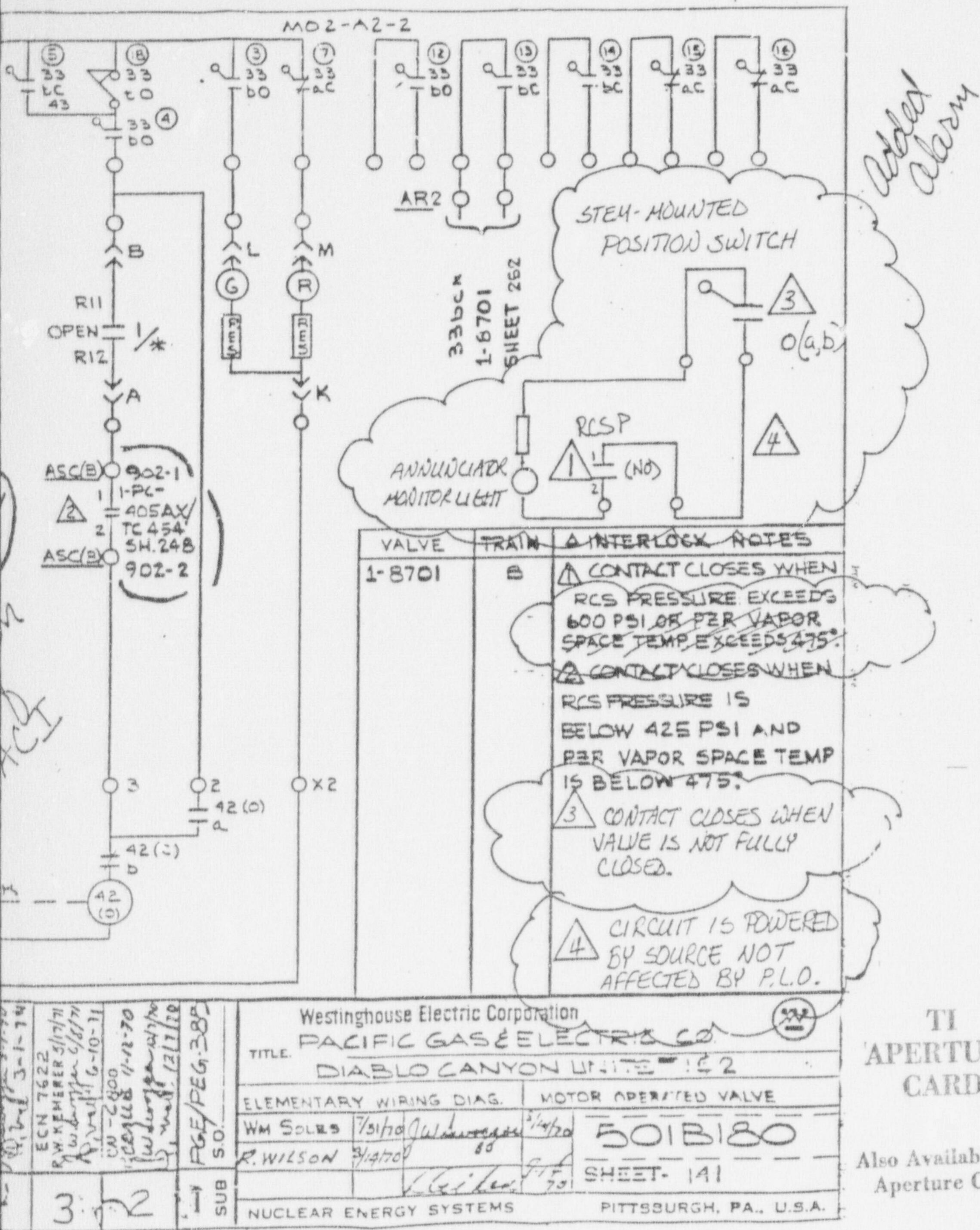
FIGURE 5-7

CURRENT INTERLOCK - MOV-8702



NOTES:
1. * - VALVE NO.
2. 1/* - DEV. 1 SH.20 N.P.C. SH.21
3. CONTROL SHOWN FOR W TYPE W MOTOR CONTROL CENTER.
4. REF. "LIMITORQUE" DWG. 15-477-2785-3 & 2786-3
5. ADD JUMPER IF TORQUE SEATING IS REQD.

ECN-30613 W.m. Soles 6-23-75 6-25-75	ECN-30552 W. DEAN 5-5-75	ECN-5733 W.M.CAMP 4-26-73
6	5	[illegible]

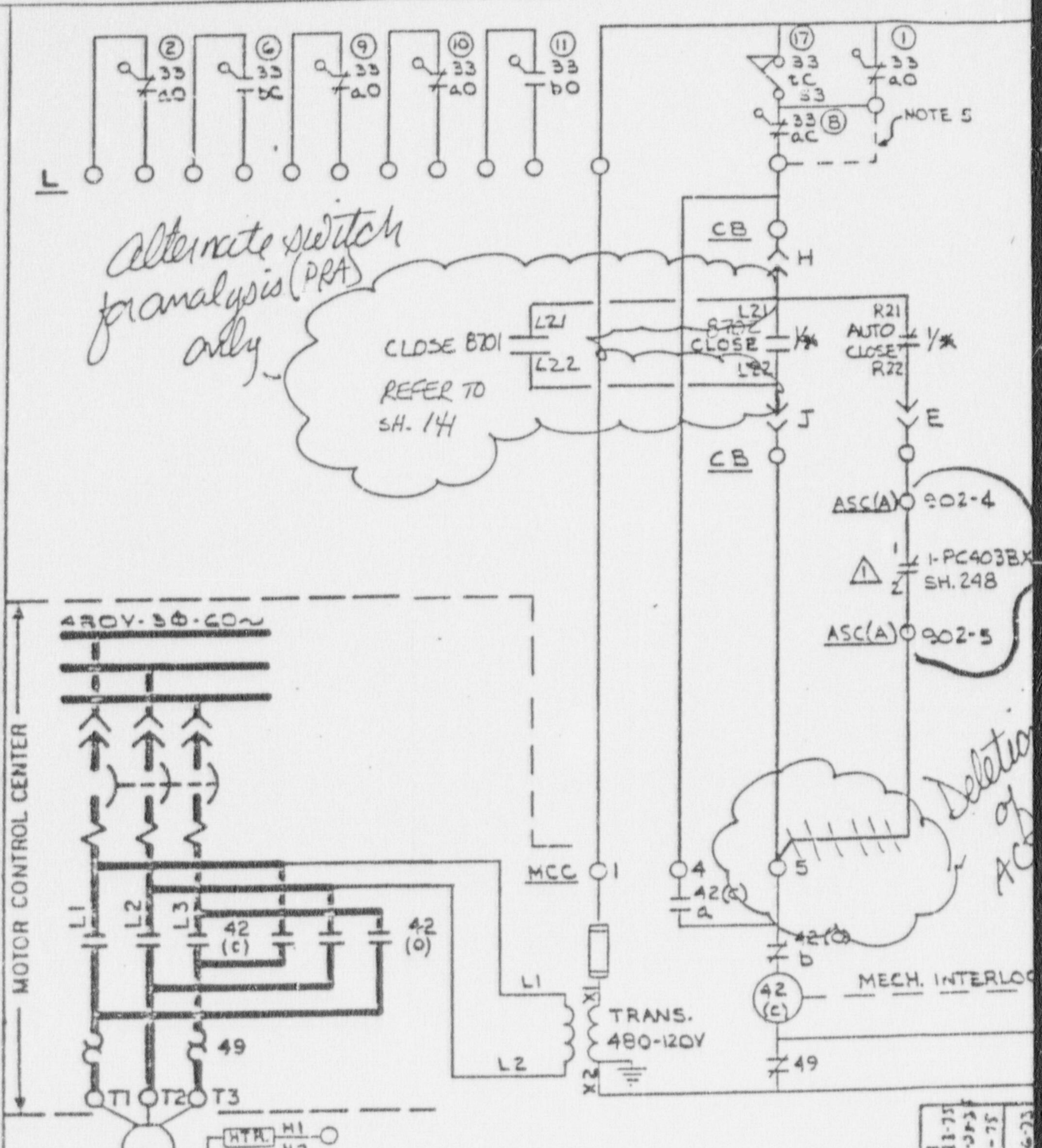


TI
APERTURE
CARD

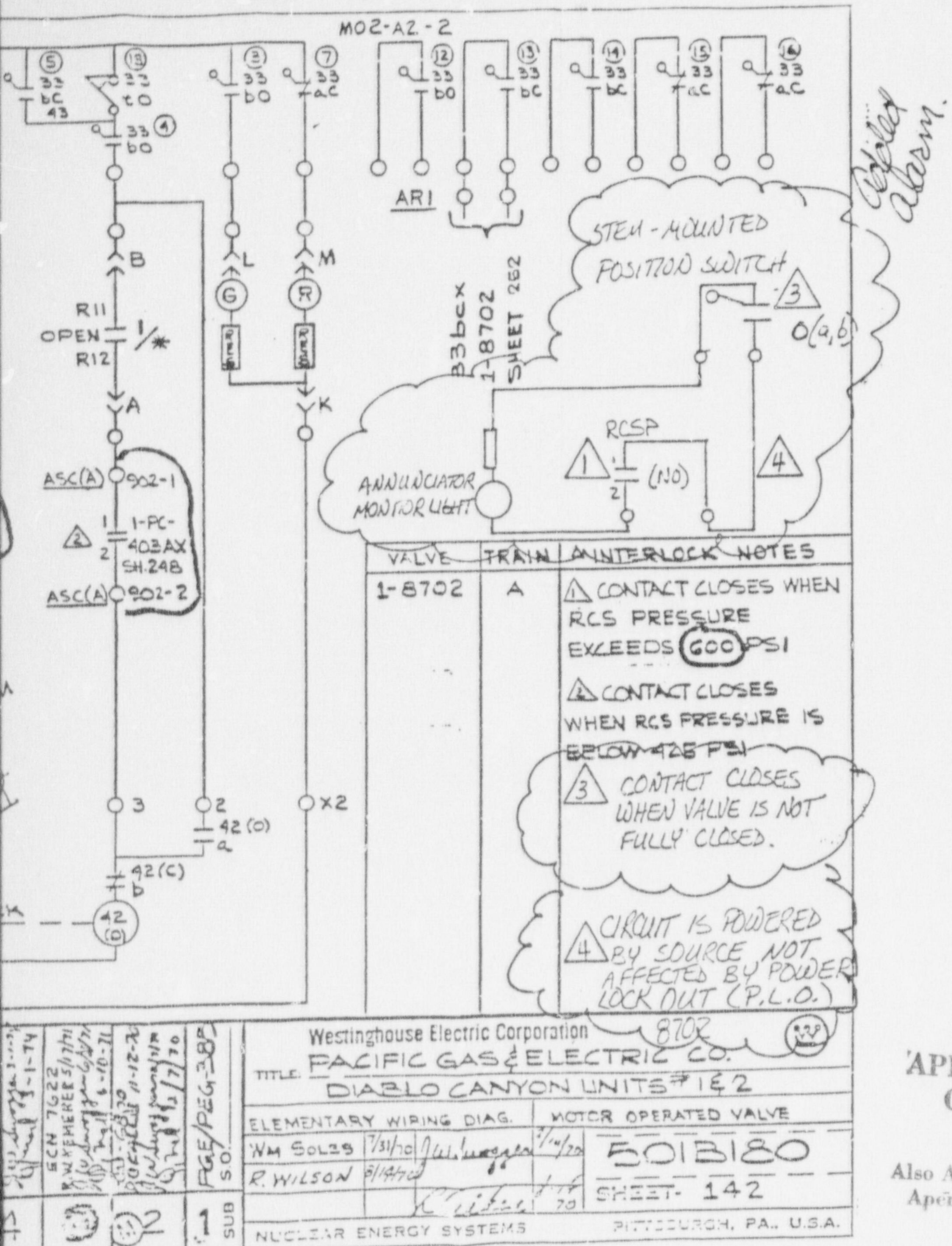
Also Available On
Aperture Card

FIGURE 5-8
ELEMENTARY WIRING DIAGRAM - 8701

8708110183 -02



NOTES:
1. ✱-VALVE NO.
2. V✱-DEV.1 SH.20 N.P. "C" SH.21
3. CONTROL SHOWN FOR W TYPE W MOTOR CONTROL CENTER.
4. REF.-"LIMITORQUE" DWG. 15-477-2785-3 & 2786-3
5. ADD JUMPER IF TORQUE SEATING IS REQD.



TI
APERTURE
CARD

Also Available On
Aperture Card

FIGURE 5-9
ELEMENTARY WIRING DIAGRAM - 8702

8708110183-03

6.0 PROBABILISTIC ANALYSIS

6.1 Introduction

This section describes the probabilistic analyses performed to justify removal of the autoclosure interlock. Three different areas were examined in this analysis: 1) the likelihood of an interfacing system LOCA; 2) the potential increase in RHRS availability and 3) low temperature overpressurization concerns. Each of the three areas were analyzed utilizing the current configuration and then the proposed modification. The NRC-proposed single switch to close both isolation valves was also analyzed. 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.

6.2 Data

The data used in this analysis was derived primarily from the Interim Reliability Evaluation Program (IREP). When data was unavailable for electrical components, other sources were chosen, particularly IEEE 500 and WASH-1400. The component failure data is presented in Table 6.2-1.

Testing information was obtained from the Technical Specifications while maintenance information was extracted from the Zion Probabilistic Safety Study (assumed to be representative of PWRs).

Human error probabilities were obtained from Swain and Guttman (Ref. 27) and are explained in the individual analyses.

6.3 Event V Analysis

An interfacing systems LOCA, referred to as an Event V in WASH-1400, is a breach of the high pressure reactor coolant system 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.

In this section, the frequency of an interfacing systems LOCA is calculated for the RHRS-RCS system interface for three cases: 1) with the present interlock configuration, 2) with the proposed modification logic, and 3) with the NRC proposed modification.

Analysis

Typically, RHRS suction paths are the dominant V-sequence source. Figure 6.3-1 depicts the RHRS suction valve arrangement. As shown in the figure, one suction line contains two series motor-operated valves. Failure of these normally closed valves would expose the low pressure piping upstream of the valves to the existing RCS pressure.

Failure combinations involving rupture of two series motor-operated valves are included in the analysis. Also included are the combinations of one valve failing open and subsequent rupture of the other valve. Failure of both valves to close during startup operations is not included because this condition would become apparent during startup testing and corrective action would be taken.

Based on the above information, the following expression is developed for the frequency of an Event V via the RHRS suction path:

$$F(VSEQ) = \lambda_2\, Q(V_1) + \lambda_1\, Q(V_2) + \lambda_2\, Q(V_1R)$$

where

λ_1 = failure rate of MOV 8701 (rupture)
λ_2 = failure rate of MOV 8702 (rupture)
$Q(V_1)$ = probability that MOV 8701 is open
$Q(V_2)$ = probability that MOV 8702 is open
$Q(V_1R)$ = probability of rupture of MOV 8701.

The following assumptions were applied in the development of this equation:

1) The frequency of valve rupture is that of catastrophic internal leakage. The failure rate λ_i is the same for either valve given that the valve is exposed to RCS pressure.

2) Valve 8702 is at RCS pressure and valve 8701 is at RCS pressure only if valve 8702 fails open.

3) No common cause rupture of the two valves is considered. This is based on the fact that no common cause ruptures of valves have actually occurred.

4) The calculation is based on an occurrence when the plant is not in the shutdown mode.

Assuming that the total defined mission time is the time between refueling outages (i.e., every 18 months), the quantity $Q(V_1R) = 6.57E-4$. The values for λ_1, and λ_2 are equal and are taken to be 1E-7/hr. The probabilities for $Q(V_1)$ and $Q(V_2)$ were quantified through the use of the detailed fault trees (see Appendix B). The probabilities were calculated to be:

	With Present Configuration	With Modification	With NRC Modification
MOV 8701 $Q(V_1)$	2.39E-5	1.27E-8	1.19E-8
MOV 8702 $Q(V_2)$	2.39E-5	1.27E-8	1.19E-8

Using these values and substituting into the V-sequence equation yields the following results:

	With Present Configuration	With Proposed Modification	With NRC Modification
$F(V_{seq})$	6.17E-7/yr	5.76E-7/yr	5.76E-7/yr

The frequency of an Event V decreases by approximately seven percent with removal of the ACI. The main contributor to the frequencies in each case is a double rupture of MOV 8702 then 8701. The deletion of the ACI has no impact on this contributor. The other contributor (the rupture of one valve while the other valve has failed open) decreases from 4.19E-8/year for the present configuration to 1.11E-11/year for the modification case and to 1.04E-11/year for the NRC modification case. This is a significant decrease in the occurrence of an Event V by this failure mode. The deletion of the autoclosure interlock and the inclusion of an alarm is beneficial in reducing this contribution.

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

1) Both suction valves have AC power removed from the operators during Modes 1, 2, and 3. This prevents opening of the valves during these modes.

2) Both suction valves have open permissive interlocks that prevent the valves from being opened whenever the RCS pressure is greater than approximately 390 psig. The second isolation valve also has an open-permissive interlock that prevents it from being opened if the pressurizer temperature exceeds 475°F.

3) It is highly unlikely that the valve could move against the high ΔP across the valve when the plant is in Modes 1, 2, or 3 (i.e., valve motor size is inadequate to open the valve given the high ΔP).

4) If a RHRS pump seal should fail during an Event V, water would spill onto the floor of the pump compartment. Each RHRS pump is in a separate, shielded compartment that drains to a sump containing two 30-gpm pumps that can pump the spillage to the waste disposal system. Gross leakage from the RHRS can be accommodated in the pump compartments, each of which has a capacity of 9450 gallons.

5) 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.

Based on the analysis, a modification is beneficial in reducing the frequency of an interfacing system LOCA.

6.4 RHRS Availability

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 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 decay heat 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.

Removal of the autoclosure interlock will reduce the number of spurious closure events and thus increase the availability of the RHRS system.

Analysis

Three different scenarios were postulated to evaluate the unavailability of the RHRS: 1) failure during startup of the RHRS, 2) failure during the first 72 hours after initiation (in which two trains of RHRS are required), and 3) failure during long term cooling (a 6 week time period was assumed in which only one train of RHRS is required).

The models used for the analysis are fault trees. The major components in the RHR system were modeled including valves, heat exchangers and pumps. The two suction valves are modeled in detail to explicitly show the changes in the unavailability due to removal of the autoclosure interlock. Detailed descriptions of the analysis are shown in Appendix C.

The results of the analysis are shown in Table 6.4-1. As can be seen from the table, the unavailability of the RHRS slightly decreases with removal of the autoclosure interlock. A trend appears to be occurring in which the change in unavailability (with and without the interlock) decreases more rapidly as the time period required for RHRS operation increases. Thus, removal of the interlock increases the availability of the RHRS.

6.5 Overpressurization Transients

A number of occurrences in the past have happened in which the temperature - pressure limits have exceeded a plant's Technical Specifications. A majority of these events have occurred during startup or shutdown conditions. These pressure transients are of concern because the vessel material is more brittle at relatively low temperatures than at operating temperatures.

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 will also be subject to overpressure for which it may not be designed to handle. However, the RHRS relief valve will be available to help mitigate the transient. The tradeoffs 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.

INITIATING EVENTS

Many past reports have characterized the different types of transients possible at cold shutdown. These events have been grouped into two general categories: 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 each transient event and attempts to quantify the frequency of these events.

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

Rod withdrawal during shutdown would have only a minor effect on the RCS. The neutron flux would increase to the source range trip setpoint prior to core generation.

A Westinghouse analysis of this event for the RESAR-3 and -41 designs 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 transient 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 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. The RHRS is then isolated from the RCS.

If the RHRS is not isolated by the operator, RCS pressure would increase to that of the suction relief valve. Discharge through the relief valve would prevent the operator from increasing the pressure further.

If only one of the suction valves is closed, 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 scenario is addressed in Section 6.3.

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 scenario results. 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).

Startup of an Inactive Loop

The startup of an inactive reactor coolant pump is another heat input transient. This transient occurs when charging flow is continued for a period of time without having all of the reactor coolant pumps in operation. This cold water collects in the low areas of the loop piping. When the inactive reactor coolant pump is started, the cold water mixes in the warm steam generators, and the cold water expands as its density decreases. This expansion results in an increase in RCS pressure.

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 RHRS relief valve will protect the RHRS from overpressurization as long as the RCS does not boil. A loss of cooling would cause a slow rise in the coolant temperature and pressure.

Opening of Accumulator Discharge Isolation Valve

The opening of an accumulator discharge valve will input water into the RCS which is already water solid. The peak pressure reached during this event will be between the initial RCS pressure and the accumulator nitrogen pressure.

Letdown Isolation

For this event, two scenarios are considered: isolation of letdown while the RHRS remains functional and isolation of the RHRS itself. Of these, the pressure transient associated with the second event is greater in that the mass addition transient is coupled with a heatup transient. Additionally, isolation of the RHRS precludes the use of the RHRS relief valve in mitigating the pressure rise and places this action on the LTOP system.

Charging/Safety Injection Pump Actuation

Under stable pressure conditions, the inadvertent actuation of a charging pump or safety injection pump that results in coolant addition without an increase in letdown will cause a pressure transient.

These transients were researched in order to determine the frequency of these events. Appendix D details the events that have occurred and the quantification of the frequencies of these transients. Table 6.5-1 lists the transients and the frequencies calculated based on operating experience.

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,

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. Figure 6.5-1 was generated from these analyses. Note that the above transients are applicable to Diablo Canyon Power Plant, see Reference 25.

This figure shows that heat input transients occur quickly in time. The figure also shows that given that 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 700 psig). Furthermore, the LTOP system and the RHRS suction relief valve are capable of mitigating these transients. The probability of the failure of the RHRS relief valve coupled with failure of two trains of the LTOP system is extremely small (on the order of 3E-09). Given that the initiating event frequency for pressurizer heaters actuation is 6.32E-3/yr, the frequency of RHRS damage from this event is roughly 1.9E-11/yr. For the decay heat addition case (loss of an RHRS cooling train) the initiator frequency (5.37E-1/yr) coupled with failure of the RHRS relief valve and the LTOP system (3E-09) yields a frequency of RHRS damage of 1.6E-9/year.

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 LTOP system must both fail in order for this event to occur. Given that the frequency for startup of an inactive loop transient is 6.95E-2/yr, the frequency of an interfacing systems LOCA would be approximately 2.1E-10/yr.

From this analysis, a modification to 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 Valve Lifts at P=450 psig (RV): If the RHRS is not isolated, the spring loaded relief valve will open at a pressure of approximately 450 psig. The valve is sized to relieve the combined flow of both charging pumps into the RCS at cold conditions and this prevents exceeding the RHRS design pressure.

4. LTOP System Operates at P=450 psig (LTP): 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 330°F, a high pressure signal (above 450 psig) will trip the system automatically and open a PORV until the pressure drops below the reset value.

5a. RHRS Suction/Isolation Valves Automatically Close at P=700 psig (RS): When the pressure increases to 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 present configuration case only.

5b. Operator Detects Overpressure Alarm and Isolates the RHRS (OD): For the modification case, an alarm would sound when the pressure reached approximately 700 psig. 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 LTOP, 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 Safety Relief Valve Opens at P=2485 psig (PZR): If the charging SI pump has sufficient suction head, the RCS pressure could be increased to the safety relief valve setpoint (P=2485 psig). If the charging pump is not secured then the valve will cycle open and closed.

9. RHRS Relief Valve Reseats (VR): 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.

10. Pressurizer PORVs Reseat (PRV): 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. The calculation of these probabilities is detailed in Appendix D. The results of these calculations (i.e., the failure probabilities) for each of the nodes is shown in Table 6.5-2.

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 were defined by the parameters listed in Table 6.5-3.

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.

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 450 psig. The accumulator design pressure is 700 psig and the normal operating pressure is 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 LTOP system failed to operate. Therefore, the interlock has no effect on this transient.

Letdown Isolation/RHRS Operable

The quantification of the event tree for this case is shown in Appendix D. The consequence frequencies for most of the categories decrease or do not change. However, the frequency of a high overpressure interfacing systems LOCA increases from 6.54E-15/Yr to 2.28E-12/Yr. These frequencies are conservative because it was assumed that the operator must act within 10 minutes of the onset of the event, and that if he fails no other operator action would take place. Furthermore, with a mismatch between the charging flowrate with no letdown (maximum flowrate of 550 gpm) the pressure would not increase as quickly as some of the other transients. Another important assumption is made that the RHRS could not withstand great pressure. This is also discussed in Section 6.3. The final assumption that is conservative is that the charging pump will continue to run at its maximum flowrate against the large ΔP that would exist.

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 RHRS 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 2.34E-1/Yr to 1.17E-1/Yr). (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 to be reduced by one half. See additional explanation in Appendix D.) The result of the reduction in initiator frequency decreases the challenges to the mitigating systems in the RHRS and reduces the frequencies of the consequences.

Charging/Safety Injection Pump Actuation

The analysis of this transient (assuming maximum flowrates from the pumps and no letdown) in regard to removal of the autoclosure interlock showed an increase in the frequency of high overpressure interfacing systems LOCA from 5.89E-15/Yr to 2.05E-12/Yr. Most of the other consequence category frequencies decreased.

The conservative assumptions discussed in the letdown isolation - RHRS operable case also apply in this analysis. Specifically it is doubtful that both pumps will continue to run at maximum flowrate as the pressure increases. Thus more time would be available in which the operator can mitigate the transient because the pressure would increase more slowly.

A summary of the overpressurization analysis is shown in Table 6.5-4.

6.6 Conclusions

Based on the three areas of probabilistic analysis - the frequency of an Event V, the availability of the RHRS, and the effect on overpressure transients, the overall increase in safety due to removal of the autoclosure interlock can be seen.

The frequency of an interfacing systems LOCA decreased from 6.17E-7/yr to 5.76E-7/yr at power while the frequency increased from approximately 1.24E-14/yr to 4.33E-12/yr in the overpressurization analysis. Compared to the "at-power" case, the overpressurization case frequency is not as significant as the decreased frequency at power conditions.

Furthermore, the availability of the RHRS increases slightly with removal of the autoclosure interlock (from 2.28E-2 to 2.21E-2 for the long term cooling analysis). The trend in this analysis shows that the longer the RHRS is required, the more of a detriment to decay heat removal is the autoclosure interlock. Also, the loss of one power bus (due to failure or testing) will cause closure of the RHRS suction valves and failure of an inverter supplying power will cause the suction valves to fail closed in the present configuration. With removal of the interlock, these types of concerns will not be as significant.

From a probabilistic point of view, the removal of the autoclosure interlock indicates an increase in safety.

TABLE 6.2-1
DATA

COMPONENT	FAILURE MODE	FAILURE RATE	DATA BASE	REMARKS
AIR OPERATED VALVE	FAILURE TO OPERATE	3E-03/D	IREP	
ALARM	FAILURE TO OPERATE	6E-07/H	IEEE-500	
BUSES	ALL MODES	1.0E-08/H	IREP	
CHECK VALVE	FAILURE TO OPEN	1E-04/D	IREP	
CIRCUIT BREAKERS	SPURIOUS OPEN	1.0E-08/H	IEEE-500	
CIRCUIT BREAKERS	FAILURE TO OPEN	2.0E-08/H	IEEE-500	
CIRCUIT BREAKERS	FAILURE TO CLOSE	3.0E-08/H	IEEE-500	
CODE SAFETY VALVES	FAILURE TO OPEN	1E-05/D	IREP	
CODE SAFETY VALVES	FAILURE TO CLOSE	1E-02/D	IREP	
FUSES	PREMATURE OPEN	3.0E-06/H	IREP	
LIMIT SWITCH	CONTACTS SHORT	2.70E-08/H	WASH 1400	
LIMIT SWITCH	FAILURE TO OPERATE	1.0E-04/D	IREP	
MANUAL SWITCH	FAILURE TO TRANSFER	3E-05/D	IREP	
MANUAL VALVE	FAILURE TO OPERATE	3E-07/H	IREP	1 ACTUATION/MON
MANUAL VALVE	FAILURE TO OPERATE	1E-04/D	IREP	
MOTOR DRIVEN PUMP	FAILURE TO START	3E-03/D	IREP	
MOTOR DRIVEN PUMP	FAIL TO RUN,GIVEN START	3E-05/H	IREP	
MOTOR OPERATED VALVE	FAILURE TO CLOSE	3E-03/D	IREP	
MOTOR OPERATED VALVE	FAILURE TO OPEN	3E-03/D	IREP	
MOTOR OPERATED VALVE	FAIL TO REMAIN OPEN/CLOSE	1E-07/H	IREP	
MOTOR OPERATED VALVE	CATASTROPHIC	1E-07/H	IREP	
OVERLOAD BREAKER	PREMATURE OPEN	3.0E-06/H	RATE FOR A FUSE	
PRESSURE TRANSMITTER	LOW OUTPUT	6.0E-08/H	IEEE-500	
PRESSURE TRANSMITTER	ALL MODES	1.73E-06/H	IEEE-500	
PRESSURE TRANSMITTER	HIGH OUTPUT	1.3E-07/H	IEEE-500	
RELAYS	CONTACTS FAIL TO TRANSFER	1.0E-06/H	NREP	
RELAYS	CONTACTS FAIL TO TRANSFER	3E-04/D	IREP	
RELAYS	NORM OPEN CONTACTS SHORT	2.7E-08/H	WNTD	
RELAYS	NORM CLOSED CONTACTS OPEN	1.2E-07/H	WNTD	
RELAYS	COIL FAILURE	3.0E-06/H	NREP	
RELAYS	COIL FAILURE	3E-06/H	IREP	
RELIEF VALVES	FAILURE TO CLOSE	3E-02/D	IREP	
RELIEF VALVES	FAILURE TO OPEN	3E-04/D	IREP	
ROTARY MANUAL SWITCH	CONTACTS FAIL OPEN	1.70E-06/H	WNTD	
ROTARY MANUAL SWITCH	SHORT ACROSS CONTACTS	1.70E-06/H	WNTD	
TEMPERATURE TRANSMITTER	HIGH OUTPUT	1.5E-07/H	IEEE-500	
TEMPERATURE TRANSMITTER	ALL MODES	1.71E-06/H	IEEE-500	
TEMPERATURE TRANSMITTER	LOW OUTPUT	6.0E-08/H	IEEE-500	
TORQUE SWITCH	FAILURE TO OPERATE	1.0E-04/D	IREP	
TORQUE SWITCH	CONTACTS SHORT	2.7E-08/H	WASH 1400	
TRANSFORMERS	ALL MODES	3.5E-07/H	IEEE-500	
WIRES	OPEN CIRCUIT	3E-06/H	IREP	
WIRES	SHORT TO GROUND	3E-07/H	IREP	
WIRES	SHORT TO POWERED	3E-08/H	IREP	

TABLE 6.4-1

RHRS UNAVAILABILITIES

	Present Configuration	Modification	NRC Modification
MOV 8701 Fails to Open	5.02E-3	5.02E-3	5.02E-3
MOV 8702 Fails to Open	5.02E-3	5.02E-3	5.02E-3
MOVs 8701 and 8702 Spuriously Close (T=72 hrs)	6.64E-5	2.22E-5	2.22E-5
MOVs 8701 and 8702 Spuriously Close (T=1008 hrs)	9.29E-4	3.11E-4	3.11E-4
RHRS Failure During Startup	2.07E-2	2.07E-2	2.07E-2
RHRS Failure Over Short Term (T=72 hrs)	7.11E-5	2.69E-5	2.69E-5
RHRS Failure Over Long Term (T=1008 hrs)	2.01E-3	1.39E-3	1.39E-3
Total RHRS Unavailability Over Short Term	2.08E-2	2.07E-2	2.07E-2
Total RHRS Unavailability Over Long Term	2.28E-2	2.21E-2	2.21E-2

TABLE 6.5-1
OVERPRESSURIZATION INITIATOR FREQUENCIES

Initiating Event	Frequency (Per Reactor Year)
1.0 PREMATURE OPENING OF RHRS	Not Analyzed
2.0 ROD WITHDRAWAL	Not Analyzed
3.0 HEAT INPUT/REMOVAL	
3.1 Failure to Isolate RHR During Startup	Not Analyzed
3.2 Pressurizer Heaters Actuation	6.32E-3
3.3 Startup of Inactive RCS Loop	6.95E-2
3.4 Loss of RHRS Cooling Train	5.37E-1
4.0 MASS INPUT/LETDOWN	
4.1 Opening of Accumulator Discharge Isolation Valve	1.89E-2
4.2 Letdown Isolation	
4.2.1 RHRS Operable	1.01E-1
4.2.2 RHRS Isolated (Present)	2.34E-1
(Modification)	1.17E-1
4.3 Charging/Safety Injection Pump Actuation	9.72E-3

TABLE 6.5-2

NODAL SYSTEM/COMPONENT FAILURE PROBABILITIES

Node	Conditions	Failure Probability
RI	Charging Pump Tree	0.9
	Letdown-RHRS Operable Tree	1.0
	Letdown-RHRS Isolated Tree	0.0
RV		3.0E-4
LTP	One Train Fails	7.71E-3
	Two Trains Fail	1.50E-5
RS	Present Configuration Only	1.44E-5
OD	Modification Cases Only	
	20 minutes action time	5.25E-4
	10 minutes action time	5.02E-3
OA1		0.217
OA2	Given Success of Previous Task	0.21
	Given Failure of Previous Task	0.36
PZR		1.0E-15
VR		3.0E-2
PRV	Given One PORV Opens	3E-3
	Given Two PORVS Open	6E-3

TABLE 6.5-3

DESCRIPTION OF CONSEQUENCE CATEGORIES

Identifier	Description
H	High Pressure Transient (P>2485 psig)
M	Medium Pressure Transient (450<P<2485)
L	Low Pressure Transient (P<450 psig)
SF	Small finite loss of coolant (<1000 gpm)
LF	Large finite loss of coolant (>1000 gpm)
SC	Small continuous loss of coolant (<1000 gpm)
LC	Large continuous loss of coolant (>1000 gpm)
OP	Overpressure
I	RHRS Isolated
O	RHRS Open
V	Interfacing Systems LOCA

TABLE 6.5-4
SUMMARY OF OVERPRESSURIZATION ANALYSIS

Initiating Event	Initiating Event Frequency (Per Yr)	Effect of Removal of Autoclosure Interlock
1. Premature Opening of RHRS	(None to Date)	No effect. The prevent-open interlock is of importance in this case, not the autoclose interlock.
2. Rod Withdrawal	(None to Date)	No effect. A small increase in temperature is expected but this increase would not affect the RHRS.
3. Failure to Isolate RHRS During Startup	Not Analyzed	This transient is described in Section 6.3. However, the RHRS relief valve's operation would stop further increases in pressure.
4. Pressurizer Heaters Actuation	6.32E-3	This transient causes a slow rise in pressure. The relief valves are available to mitigate the transient. Pressurizer heaters would automatically shutoff. No effect.
5. Startup of an Inactive Loop	6.95E-2	No effect. The rise in pressure is too quick for the slow closing isolation valves.
6. Loss of RHR Cooling Train	5.37E-1	No effect. The rise in pressure from decay heat is slow which would give the operator more time to react.
7. Opening of Accumulator Discharge Isolation Valves	1.89E-2	No effect. Mass would be input from the accumulator until the RCS and accumulator pressure equal. Accumulator pressure would not exceed 700 psig.

TABLE 6.5-4 (Cont)
SUMMARY OF OVERPRESSURIZATION ANALYSIS

Initiating Event	Initiating Event Frequency (Per Yr)	Effect of Removal of Autoclosure Interlock
8. Letdown Isolation RHRS Operable	1.01E-1	Increases frequency of high overpressure interfacing systems LOCA from 6.5E-15/Yr to 2.28E-12/Yr. Decreases other types of consequences.
9. Letdown Isolation RHRS Isolated	2.34E-1 (Present) 1.17E-1 (Modification)	Decreases frequency of all consequences due to decrease in letdown isolation from inadvertent closure of isolation valves.
10. Charging/Safety Injection Pump Actuation	1.01E-1	Increases frequency of high overpressure interfacing systems LOCA from 5.89E-15/Yr to 2.05E-12/Yr. Decreases other types of consequences.

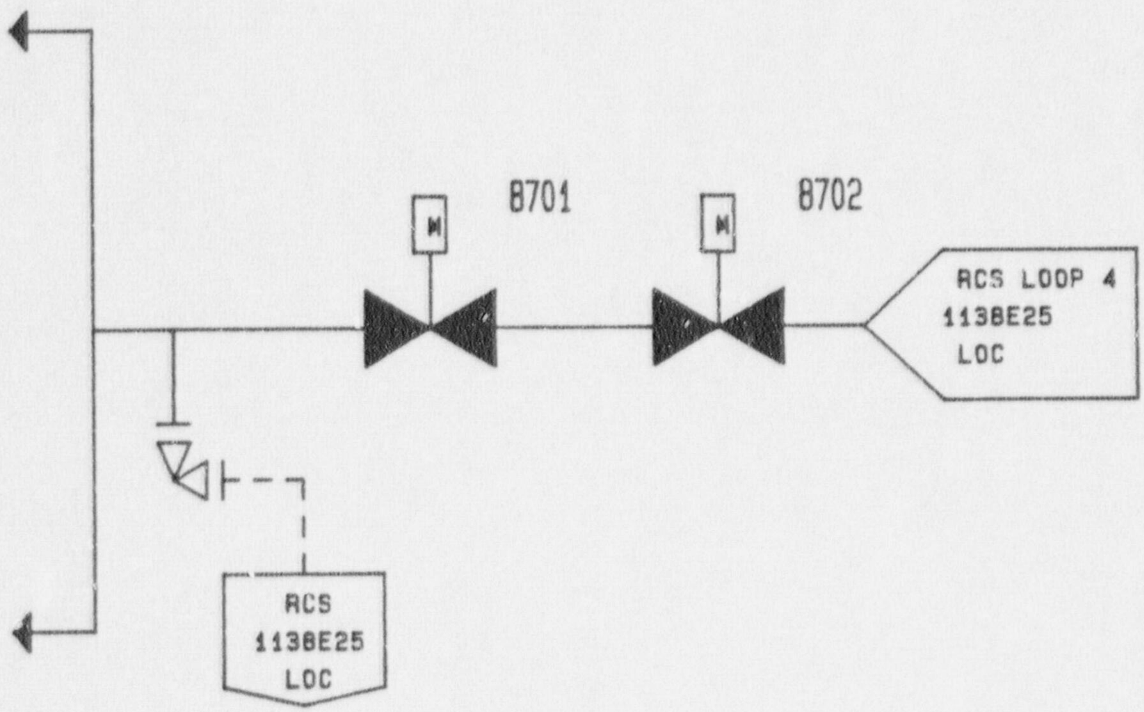


FIGURE 6.3-1

RHR Suction Valve Arrangement

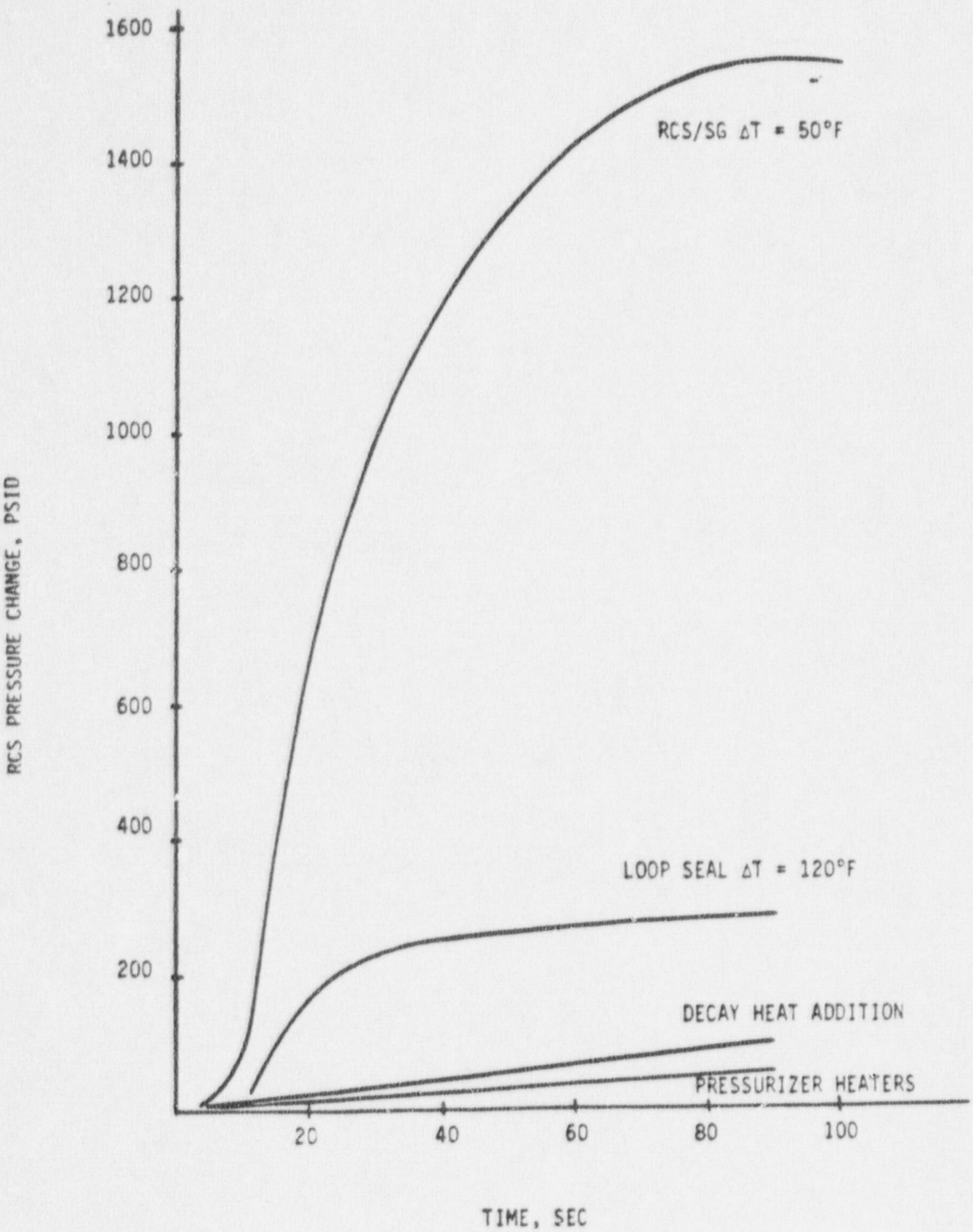


Figure 6.5-1
Typical Heat Input Transients
No Relief Valve Actuation

7.0 CONCLUSIONS

This section outlines the conclusions reached from the analysis. The conclusions address the NRC concerns expressed in Reference 5.

1. MEANS AVAILABLE TO MINIMIZE A LOCA OUTSIDE THE CONTAINMENT

The two motor operated valves serve as the primary Reactor Coolant System pressure boundary. They are remote operated, and are powered by separate electrical sources. Therefore, the capability of this set of valves to isolate the Residual Heat Removal System is very reliable. Plant operating procedures instruct the operator to isolate the RHRS during plant heatup, so the likelihood of these valves being left open is remote. Therefore, during normal heatup and cooldown operations, redundant valves and operator action are adequate to insure RHRS isolation.

Should a pressure peak occur in the RCS, the pressure would not be imparted to the low pressure portion of the RHRS, since a relief valve (900 gpm/450 psig) protects the low pressure system. This relief valve discharges inside containment to the pressurizer relief tank (PRT). A discharge would be detected by high temperature, level, and pressure alarms in the PRT.

It would be noted that there are Technical Specification surveillance requirements applicable to these valves.

The frequency of an interfacing systems LOCA is reduced from 6.17E-7/yr for the case with the autoclosure interlock to 5.76E-7/yr for the case with removal of the ACI and addition of an alarm.

2. ALARMS TO ALERT THE OPERATOR OF AN IMPROPERLY POSITIONED RHRS ISOLATION VALVE

Each isolation valve has its position indicated on the main control board at its control switch. In addition, should both valves not be closed when RCS pressure is above RHRS pressure, the relief valve would actuate, resulting in

PRT pressure, level and temperature alarms. Also the RHRS contains pressure alarms which actuate as the pressure approaches the RHRS design pressure. Additional alarms will be implemented to provide indication of an isolation valve being open when RCS pressure exceeds a pre-determined value. The proposed Westinghouse design change incorporates additional alarms in the control room to alert the operator of valve position when the RCS pressure reaches a given pressure.

3. VERIFICATION OF THE ADEQUACY OF RHRS RELIEF VALVE CAPACITY

In support of RESAR-3 and RESAR-41 applications, Westinghouse performed several analyses that demonstrated that the relief valve does protect the RHRS from overpressure. These analyses were reviewed, and their applicability to the Diablo Canyon Power Plant was verified as a part of this program.

4. MEANS OTHER THAN AUTO-CLOSE INTERLOCKS TO ENSURE BOTH ISOLATION VALVES ARE CLOSED (E.G. SINGLE SWITCH ACTUATING BOTH VALVES)

Operating instructions, along with redundant position indication and alarms, are sufficient to insure isolation.

Furthermore the alarm which would actuate given a high pressure signal and either isolation valve open would indicate the position of the valves along with the indicating lights.

A single switch to close both valves alone would not provide adequate assurance that the valves would be closed. An alarm would also have to be installed. However it is believed that the location of the hand switches (for both valves) near each other on the MCB is sufficient to ensure timely operator actions.

5. ASSURANCE THAT THE OPEN PERMISSIVE CIRCUITRY IS NEITHER REMOVED OR AFFECTED BY THE PROPOSED CHANGE

The Westinghouse design leaves the open permissive circuit intact.

6. ASSURANCE THAT ISOLATION VALVE POSITION INDICATION WILL REMAIN AVAILABLE IN THE CONTROL ROOM REGARDLESS OF THE PROPOSED CHANGE

The Westinghouse design leaves the valve position indication at the main control board intact. This indication will be by two means

(i) continuous valve position indication (MCB status lights)
(ii) absence of the alarms provided with the autoclose interlock removal.

7. ASSESSMENT OF THE EFFECT OF THE PROPOSED CHANGE ON RHRS AVAILABILITY, AS WELL AS LOW TEMPERATURE OVERPRESSURE PROTECTION

This change will increase the availability of the RHRS relief valve to mitigate low temperature overpressure occurrences, thereby reducing challenges to the power operated relief valves, and keeping RCS pressure at cold temperatures in an acceptable range with respect to Appendix G limits.

The probabilistic analysis of the reliability of the RHRS showed that the availability slightly increased with the deletion of the autoclosure interlock.

Several overpressure transients were modeled to show system and operator response to these transients. An increase in the frequency of a LOCA at shutdown conditions was found. However the relative magnitude of the resulting frequency is insignificant compared to the frequency at power conditions.

Based on the answers provided to the above concerns, removal of the autoclosure interlock along with implementation of the recommended modification results in a net improvement in safety.

8.0 REFERENCES

1. 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," 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. 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.

4. 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.

5. Memorandum from B. W. Sheron, NRC to RSB members, "Auto Closure Interlocks for PWR Residual Heat Removal (RHR) Systems," January 28, 1985.

6. Westinghouse letter, R. I. Hayford to J. D. McAdoo, Subject: AEC Concerns for Administrative Positioning for Critical Valves, E-EPS-596, August 24, 1971.

7. Northern States Power Company letter, L. O. Mayer to J. F. O'Leary (AEC), Subject: Exceeding Allowed Pressure-Temperature Limit During Startup Testing, Docket 50-282, November 9, 1973.

8. Westinghouse letter, R. W. Fleming, Subject: Reactor Coolant Pressure Control, F11H2-SO-76, March 7, 1974.

9. Westinghouse Trip Report, D. W. Williams, Subject: Meeting with AEC on Residual Heat Removal (RHR) System Valve Interlocks - March 21, 1974, NS-RPE-81, March 25, 1974.

10. Atomic Energy Commission staff memorandum, G. R. Mazetis, to T. M. Novak, Subject: Summary of Meeting with PWR Vendors, April 9, 1974.

11. Atomic Energy Commission letter, T. M. Novak to Reactor Systems Branch Personnel, Subject: Shutdown Cooling System Requirements, November 27, 1974.

This letter imposed the AEC position identified in an AEC meeting of February 13, 1974 and documented in:

Atomic Energy Commission staff memorandum, J. Angelo, Subject: RP-TR Staff Meeting of February 13, 1974 Regarding the Requirements on Shutdown Cooling System Designs, February 28, 1974.

12. "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-75/087, Branch Technical Position ICSB-3, September 1975.

13. Wisconsin Public Service Corporation letter, E. W. James to J. F. O'Leary (AEC), Subject: Abnormal Occurrence Report, Docket 50-305, October 4, 1974.

14. "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.

15. 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.

16. Westinghouse Nuclear Service Division Technical Bulletin, Subject: Residual Heat Removal Pump, NSD-TB-77-7, Pittsburgh, Pennsylvania, July 15, 1977.

17. "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.

18. Casto, William R., "Reactor-Vessel Pressure Transients," Nuclear Safety, Vol. 18, No. 4, July-August 1977, pp 513-519.

19. Nuclear Regulatory Commission letter, R. W. Reid to R. H. Grace (Yankee Atomic Electric Company), Docket 50-309, August 22, 1977.

20. 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.

21. 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.

22. Nuclear Regulatory Commission Memorandum, to R. Mattson, "RHRS Interlocks for Westinghouse Plants," April 17, 1984.

23. AEOD Case Study Report, Low Temperature Overpressure Events at Turkey Point Unit 4, March 1984.

24. NSAC/84, Zion Nuclear Plant Residual Heat Removal PRA, Pickard, Lowe and Garrick, Inc., July 1985.

25. WCAP-10529, COMS - Cold Overpressure Mitigating System, R. W. Fleming, February, 1984.

26. WCAP-9540, Results of Analysis for Pressure Mitigation of RCS Cold Overpressurization Transients in 412 and 312 Plants, A. M. Sklencar, July 1979.

27. NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, A. D. Swain, H. E. Guttmann, August 1983.

28. Diablo Canyon Updated FSAR.

29. Diablo Canyon Technical Specifications.

30. Diablo Canyon Operating Procedures.
OP L-5 REV. 6 9/03/84.
OP B-2:V REV. 2 8/31/84.
OP B-2:IV REV. 2 8/31/84.

APPENDIX A

OVERVIEW OF FAULT TREE AND EVENT TREE

QUANTIFICATION

APPENDIX A

OVERVIEW OF FAULT TREE AND EVENT TREE QUANTIFICATION

This appendix provides an overview of how fault trees and event trees are quantified. The first section explains fault trees while the middle section describes event trees and the final section summarizes the computer codes used in the analysis.

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 thus depicts the logical interrelationships of basic events that lead to the undesired event--which is the top event of the fault tree.

It is important to understand that 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 thus 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.

It is also important to point out that a fault tree is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively and often is. This qualitative aspect, of course, is true of virtually all varieties of system models. The fact that a fault tree is a particularly convenient model to quantify does not change the qualitative nature of the model itself.

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. Thus, 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:

$$q_c = 1/2\ \lambda s\ T_T \tag{1}$$

where q_c is the component average unavailability, λs 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:

$$q_c = q_d \tag{2}$$

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:

$$q_c = q_d + 1/2\ \lambda s\ T_T \tag{3}$$

with the parameters q_c, q_d, λs and T_T are as previously defined. Data is usually not 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 operating system is given by the expression:

$$q_c = \lambda_o T_M \tag{4}$$

with q_c as previously defined, λ_o 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 $\lambda_c T_M \leq 0.1$

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:

$$q_c = q_d + \lambda_o T_M \tag{5}$$

or

$$q_c = 1/2 \lambda s T_T + \lambda_o T_M \tag{6}$$

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 as 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.

The scheduled preventative maintenance outage contribution to component unavailability for point value computation is estimated by:

$$q_{SM} = f_M \, (\tau_M/T_T) \qquad (8)$$

where q_{SM} is the component unavailability due to scheduled maintenance, f_M is the frequency (per test period) with which scheduled maintenance occurs, τ_M is the mean component outage time for scheduled maintenance, and T_T is the test period.

In both of the above expressions (i.e. 7 and 8) since q_{RM} and q_{SM} are probability values all of the parameters on the right hand side of the expressions must be compatible and cancel out so that respective "q" values obtained are dimensionless. For instance, for monthly testing, if the test period (T_T) is expressed in hours per month, the repair duration (τ_R) is in hours, and f_R is the reciprocal of the number of months between repair acts, then q_{RM} is dimensionless.

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.

The frequency (f_R) per test period with which repair is expected to occur is abstracted from the Zion PRA Study and is assumed typical for PWR plants. Test period related with the data covers monthly and quarterly testing and the data presented is given as events per hour. Therefore Q_{RM} can be directly calculated using the data by the expression:

$$q_{R} \quad (\text{Events/Hr}) \; (\tau_R) \tag{9}$$

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 compc nt 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:

$$q_t = \tau_t/T_T \tag{10}$$

where q_t is the average unavailability from the test outage, τ_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". This document will be used to establish the methodology for the quantification of human errors as required for event and fault tree quantification. Brief summaries of selected task of human reliability analysis are given in the paragraphs that follow.

A task analysis of each task operator contributing to an event tree sequence and/or system unavailability quantification using fault trees is to be performed. This forms the basis for the development of human reliability analysis probability trees. Tasks given by emergency operating procedures, test procedures, and maintenance procedures are formally broken down into smaller units (steps) of human behavior. These individual units of performance constitute elements of behavior for which potential errors can be identified. A task analysis table is prepared based on analysis of tasks. The format of the table is not important, however, the table should contain all information pertinent to required task (i.e. equipment on which action is performed, the required action by operator, limits of his performance, location of controls, etc.). The details in task analysis and the amount of information recorded are used to obtain human error probability (HEP) estimates used at a later time in the analysis quantification of human errors.

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 chronologically 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. Extreme care should be exercised in deciding which errors, if any, are to be discounted. Rather than discounting a "questionable" error the analyst thinks unlikely, it should be included in the analysis.

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 limb' 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 as is in knowing that the difference between the scenario being analyzed from that of Chapter 20 will not materially affect anal sis results. In other cases, the actual situation and the one described in Chapter 20 may reflect tasks that are basically the same but are performed under different circumstances (e.g., operator stress level, available operators etc.). For such cases the human error probability must then be modified to reflect the conditions under which the task is actually being performed. This is usually done during the assessment of the performance shaping factors acting on the task as detailed in NUREG/CR-1278.

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 technique.

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, although sometimes the fault states are located above the success states.

The accident sequences that results 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. The codes used in fault tree analysis (WESCUT, SIMON2 and GRAFTER2) are presented followed by the event tree codes (SUPER3).

A.3.1 GRAFTER2

GRAFTER2 is a computer code written in FORTRAN and ASSEMBLER languages to construct fault trees interactivity on an IBM-XT or an IBM-AT computer. It is used in conjunction with the SIMON2 and WESCUT codes to carry out fault tree analysis from construction stage, to data base management, then to quantification.

The GRAFTER2 code can be used to construct, store, update and print fault trees interactively. 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. Computer keyboard is used to move to different locations of the fault tree.

A.3.2 WESCUT

WESCUT is a computer code written in FORTRAN77 to run on an IBM-PC model AT or XT. It identifies the 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 gate specified in the input for cutset identification, the code identifies and prints out the cutsets. The cutsets are listed in order of decreasing probability. The mean probability and variance for the gate is also calculated and is printed.

A.3.3 SIMON 2

SIMON2 is a computer code written in FORTRAN to be run on IBM-XT or an IBM-AT computer to support the fault tree analysis done by the GRAFTER2 code. Three major objectives are defined for the implementation of the code:

1. To minimize hand calculations and data entry that go into fault tree analysis.

2. Provide tables for documentation.

3. Improve quality assurance by providing a master data file for all the fault trees needed for a given project.

SIMON2 calculates and tabulates basic event failure probabilities and variances. If requested, these probabilities and variances can also be placed in a GRAFTER2 fault tree (to be referred to as a "GRAFTER2 database") generated by GRAFTER2.

A.3.4 SUPER3

SUPER3 is a code for event tree analysis using an IBM-XT or AT computer. The code will draw an event tree or draw and quantify an event tree. In addition, the code will run a series of quantifications of a single event tree using alternate event probabilities if required for sensitivity or other studies.

The code can be used to construct and quantify an event tree with a maximum of 25 nodes and with up to 10 branches for each event node. The event tree is further limited to a total of 650 branches. The event tree may be repeatedly recalculated with multiple set of probability values for the purpose of conducting sensitivity or other studies.

Output includes or may include the event tree picture, accident sequence number, number of failures, sequence pathname, sequence probability, sequence frequency and sequence category, consequence category, consequence probability and consequence frequency and, finally, the event tree frequency (sum of the consequence frequencies).

The code can present the output information in any of several formats selected to suit user needs.

TABLE A.1-1

FAULT TREE COMPONENT IDENTIFICATION CODES

Nine or ten character codes identify component failures in the fault trees. The format of component failures in the fault trees is STCCCXXXXF where:

* S is the system identification code.
* T is the identification of the train to which the component belongs.
* CCC is the component type identification code.
* XXXX is the number designating the single component in the P&IDs.
* F is the specific component failure.

The following lists the codes used in this evaluation.

COMPONENT IDENTIFICATION CODE

Code Letters	Component Identification
	System
R	Residual Heat Removal System
	Train
1	Train #1
2	Train #2
	Mechanical Components
HE	Heat Exchanger
PV	Pressure Vessel
PM	Motor Driven Pump

TABLE A.1-1 (Cont)

COMPONENT IDENTIFICATION CODE

Code Letters	Component Identification
CV	Valve, Check
HV	Valve, Hydraulic Operated
AV	Valve, Air (Pneumatic) Operated
LS	Limit Switch
LO	Lockout Relay or Switch
SW	Manual Switch (Pushbutton)
SR	Manual Switch (Rotary)
MO	Motor
MS	Motor Starter
RE	Relay
RL	Relay (Latching Type)
CN	Relay or Switch Contact
QS	Switch, Torque
OL	Thermal Overload Element
XY	Valve, Manual
MV	Valve, Motor Operated
AV	Valve, Relief Pneumatic or Hydraulic Operated
AS	Valve, Relief Solenoid Operated
SV	Valve, Solenoid Operated

Electrical Components

CB	Circuit Breaker
CS	Control Switch
CO	Coil
FU	Fuse
CT	Transformer, Current
TP	Transmitter, Pressure
TT	Transmitter, Temperature
TE	RTD Temperature Element

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)
I	Interference
J	Degraded
K	Does Not Close
M	Maintenance
N	No Input
O	Open
P	Plugged
Q	Short Circuit
R	Rupture
S	Short to Ground
T	Test
U	Spurious Opening
V	Spurious Closing
X	Does Not Run
H	Fails High
L	Fails Low
VS	Visual Detection
ST	Status Light
OE	Operator Error
TST	Test
MAIN	Maintenance

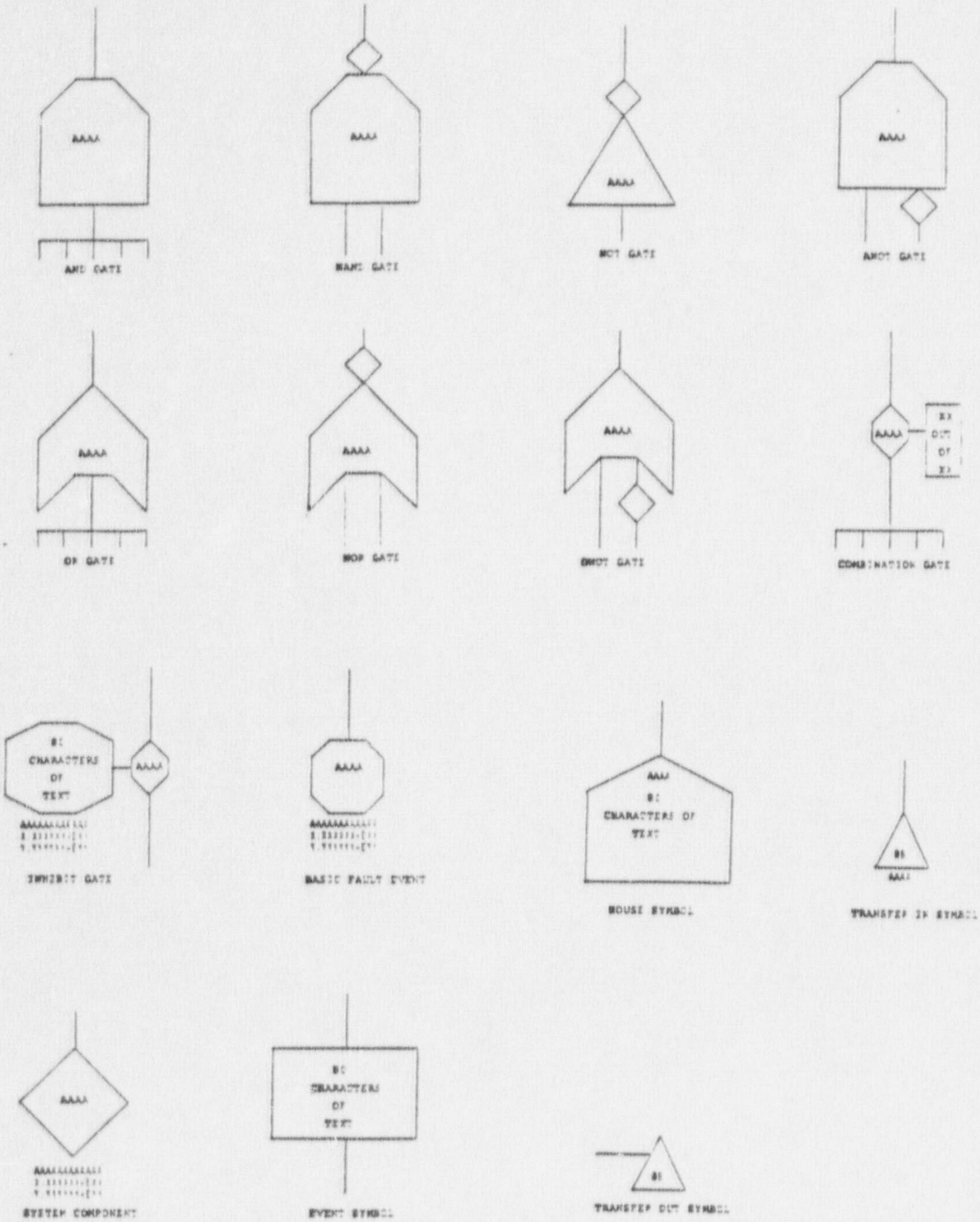


Figure A-1
Basic Fault Tree Symbols

APPENDIX B

EVENT V ANALYSIS

APPENDIX B
EVENT V ANALYSIS

The frequency of an interfacing systems LOCA is an important safety concern because a direct release of radionuclides to the atmosphere may occur. In this appendix, the frequency of an event via the RHR suction path is calculated for three cases: 1) with the present interlock configuration, 2) with the proposed modification, and 3) with the NRC proposed modification.

The failure combinations considered in the analysis involve: 1) rupture of two series motor-operated valves and 2) one valve failing open and subsequent rupture of the other valve.

The following conditions were applied in the analysis:

1. The frequency of valve rupture is that of catastrophic internal leakage. The failure rate λ is the same for either valve given that the valve is exposed to RCS pressure.

2. Valve 8702 is at RCS pressure and valve 8701 is at RCS pressure only if valve 8702 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 calculation is based on an occurrence when the plant is at power, not in the shutdown mode.

5. All electrical power is assumed to be available with a probability 1.0.

The frequency of an event V is calculated using the following expression:

$$F(VSEQ) = \lambda_2\ Q(V_1) + \lambda_1\ Q(V_2) + \lambda_2\ Q(V_1R)$$

where

λ_2 = failure rate of MOV 8702 (rupture)
λ_1 = failure rate of MOV 8701 (rupture)
$Q(V_1)$ = probability that MOV 8701 is open
$Q(V_2)$ = probability that MOV 8702 is open
$Q(V_1R)$ = probability of rupture of MOV 8701.

The failure rate due to rupture of a motor-operated valve is 1.0E-7 per hr (λ_1 and λ_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 8701 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 MOV 8701 rupturing is:

$$Q(V_1R) = \lambda \frac{T_M}{2} = \frac{1.0E-7}{hr} \times \frac{13140 \text{ hrs}}{2}$$

$$Q(V_1R) = 6.57E-4$$

In order to determine the probabilities of motor-operated valves 8701 or 8702 being open while at power, detailed fault trees of these valves were used.

Figure B-1 and B-2 shows the elementary wiring diagrams for MOV 8702 and 8701 respectively for the present interlock configuration. Figures B-3 and B-4 show the NRC-proposed modification to these diagrams in which the autoclose portion is deleted and an alarm and a single switch to close both valves is added. The other modification considers the alarm only.

The fault trees developed from these elementary wiring diagrams are shown in Figures B-5 to B-10.

The scenarios examined in the fault trees are: 1) the valve is not closed after previous use (either by operator error or failure of the autoclosure interlock) 2) the valve fails to close when the operator turns a switch and 3) the valve spuriously opens. Each of these scenarios is described below.

For the present interlock configuration motor-operated valve 8701 or 8702 can be left open after previous use by the operator failing to close the valve during startup, an operator failing to detect the wrong valve position via the status light during mode transition and the autoclosure interlock failing to close the valve. For the modification case with the alarm only, another error is added in which the operator fails to detect the wrong position via the alarm and the autoclose portion is deleted.

With the modification of a single switch in place, if the operator fails to close a valve, neither valve would be closed. If the plant was beginning startup operations, the position of the valves would be detected and corrective action taken. Thus, with a single switch to close both valves, the operator failing to close one valve is not a credible event and not included in the analysis.

Spuriously opening of the valves for both cases involves an operator failing to rack power out to the valves in combination with a failure in the "OPEN" valve circuitry.

The valve failing to close when the operator turns the switch is another failure mode. In this scenario, the valve's circuitry or mechanical components cause the motor-operated valve to not close on demand. The operator must detect this failure either by the status light in the present configuration case or by the status light and alarm in the modification case.

Table B-1 show the failure probabilities used in the fault trees based on a 12 hour detection interval.

This interval is based on the fact that the valve's position will be detected within one shift. To calculate the basic event probabilities, the following formula was used:

$$Q = \lambda \frac{T\ detect}{2}$$

where:

Q = basic event probability

λ = failure rate for component

T detect = detection interval

Also presented in Table B-2 are the human error probabilities calculated in the analysis. The probabilities were obtained from Swain, et.al and the detailed calculations and the values used are documented for each human error scenario.

Results

The probabilities obtained from the fault tree quantification for the isolation valves being open are:

		With Present Configuration	With Modification	With NRC Modification
$Q_{(V1)}$	MOV 8701 is open	2.39E-5	1.27E-8	1.19E-8
$Q_{(V2)}$	MOV 8702 is open	2.39E-5	1.27E-8	1.19E-8

The major cutsets (failure combinations) obtained from the quantification are shown in Tables B-3 and B-4 for the present configuration. The dominant cutsets for MOVs 8701 and 8702 are failure of the valve to close when the operator turns the switch in combination with the failure of the operator to detect that the valve is still open by use of the status light.

For the modification case, the dominant contributors are listed in tables B-5 and B-6. For the NRC modification case, Tables B-7 and B-8 show the cutsets obtained in the quantification. The dominant failure combination in both cases is the operator fails to detect that the valve is still open after he turns the switch. However, now the valve position will be detected by the status light and the alarm. Both devices would have to fail or the operator would have to fail to recognize these two indicators in order for the possibility of an Event V to occur.

The frequency of an Interfacing Systems LOCA is calculated for each scenario. The results are shown below:

	With Present Configuration	With Modification	With NRC Modification
F(VSEQ)	6.17E-7/yr	5.76E-7/yr	5.76E-7/yr

The frequency of an Event V decreases by approximately seven percent with removal of the ACI. The main contributor to the frequencies in each case is a double rupture of MOV 8702 then 8701. The deletion of the ACI has no impact on this contributor. The other contributor (the rupture of one valve while the other valve has failed open) decreases from 4.19E-8/year for the present configuration to 1.11E-11/year for the modification case and to 1.04E-11/yer for the NRC modification case. This is a significant decrease in the occurrence of an Event V by this failure mode. The deletion of the auto closure interlock and the inclusion of an alarm is beneficial in reducing this contribution.

From this analysis, it can be concluded that a modification is beneficial in reducing the frequency of an interfacing systems LOCA by reducing the frequency of contributions other than a double valve rupture event.

TABLE B-1

COMPONENT RANDOM FAILURE UNAVAILABILITIES

SYSTEM: MOV 8701 and 8702 - V-SEQUENCE

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R1TP405AXL	Fails Low	6.0E-8/hr	12 hrs	-	3.6E-7	Combined into
R1TT454AXL	Fails Low	6.0E-8/hr	12 hrs	-	3.6E-7	R1405ACTV 7.2E-7
R1SRCNQ	Short	1.7E-6/hr	12 hrs	-	1.02E-5	
R1CN420AQ	Short	2.7E-8/hr	12 hrs	-	1.62E-7	
R1CBU	Spurious Open	1.0E-8/hr	12 hrs	-	6.0E-8	
R1CTF	Fails	3.5E-7/hr	12 hrs	-	2.10E-6	
R1FUU	Premature Open	3.0E-6/hr	12 hrs	-	1.8E-5	
R1OL49U	Premature Open	3.0E-6/hr	12 hrs	-	1.8E-5	Rate for a fuse
R1QS33TCU	Fails to Operate	1E-4/d	1 demand	-	1E-4	
R1LS33AOU	Fails to Operate	1E-4/d	1 demand		1E-4	
R1LS33ACU	Fails to Operate	1E-4/d	1 demand		1E-4	
R1SRCNU	Spurious Open	1.7E-6/hr	12 hrs		1.02E-5	
R1TP405BXL	Fails Low	6.0E-8/hr	12 hrs		3.6E-7	Combined into
R1TT454BXL	Fails Low	6.0E-8/hr	12 hrs		3.6E-7	R1405ACTF 7.2E-7
R1MSCOF	Coil Failure	3E-6/hr	12 hrs		1.8E-5	
R1CN42CAK	Fail to Transfer	3E-4/d	1 demand	-	3E-4	
R1MV8701K	Fail to Close	3E-3/d	1 demand	-	3E-3	
R2TP403ACTV	Fails Low	6.0E-8/hr	12 hrs	-	3.6E-7	

0207x 6-040886

TABLE B-1 (Cont)

COMPONENT RANDOM FAILURE UNAVAILABILITIES (cont)

SYSTEM: MOV 8701 and 8702 - V-SEQUENCE

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R2SRCNQ	Short	1.7E-6/hr	12 hrs	-	1.02E-5	
R2CN420AQ	Short	2.7E-8/hr	12 hrs	-	1.62E-7	
R2CBU	Spurious Open	1.0E-8/hr	12 hrs	-	6.0E-8	
R2CTF	Fails	3.5E-7/hr	12 hrs	-	2.10E-6	
R2FUU	Premature Open	3.0E-6/hr	12 hrs	-	1.8E-5	
R2OL49U	Premature Open	3.0E-6/hr	12 hrs	-	1.8E-5	Rate for a fuse
R2QS33TCU	Fails to Operate	1E-4/d	1 demand	-	1E-4	
RITP405CNQ	Shorts	2.7E-8/hr	12 hrs	-	1.62E-7	
RITP405CNK	Failure to Transfer	3E-4/d	1 demand	-	3E-4	
RI405COF	Coil Failure	3E-6/hr	12 hrs	-	1.8E-5	
R2TP403CNQ	Shorts	2.7E-8/hr	12 hrs	-	1.62E-7	
R2TP403CNK	Failure to Transfer	3.0E-4d	1 demand	-	3E-4	
R2403COF	Coil Failure	3E-6/hr	12 hrs	-	1.8E-5	

0207x:6-040886

TABLE B-1 (Cont)

COMPONENT RANDOM FAILURE UNAVAILABILITIES

SYSTEM: MOV 8701 and 8702 - V-SEQUENCE

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R2LS33AOU	Fails to Operate	1E-4/d	1 demand		1E-4	
R2LS33ACU	Fails to Operate	1E-4/d	1 demand		1E-4	
R2SRCNU	Spurious Open	1.7E-6/hr	12 hrs		1.02E-5	
R2TP403ACTF	Fails Low	6.0E-8/hr	12 hrs		3.6E-7	
R2MSCOF	Coil Failure	3E-6/hr	12 hrs		1.8E-5	
R2CN42CAK	Fail to Transfer	3E-4/d	1 demand	-	3E-4	
R2MV8702K	Fail to Close	3E-3/d	1 demand	-	3E-3	
R1ALARM	Fails to Operate	6E-7/hr	12 hrs	-	3.6E-6	
R1SRCNK	Fails to Transfer	3E-5/D	1 demand	-	3E-5	
R1ALLSK	Fail to Transfer	1E-4/D	1 demand	-	1E-4	
R1TP405ACTF	Low Output	6.0E-8/hr	12 hrs	-	3.6E-7	Modification Cases
R2ALARM	Fails to Operate	6E-7/hr	12 hrs	-	3.6E-6	
R2SRCNK	Fails to Transfer	3E-5/D	1 demand	-	3E-5	
R2TP403ACTF	Low Output	6.0E-8/hr	12 hrs	-	3.6E-7	Modification Cases

0207x-6-040886

TABLE B-2

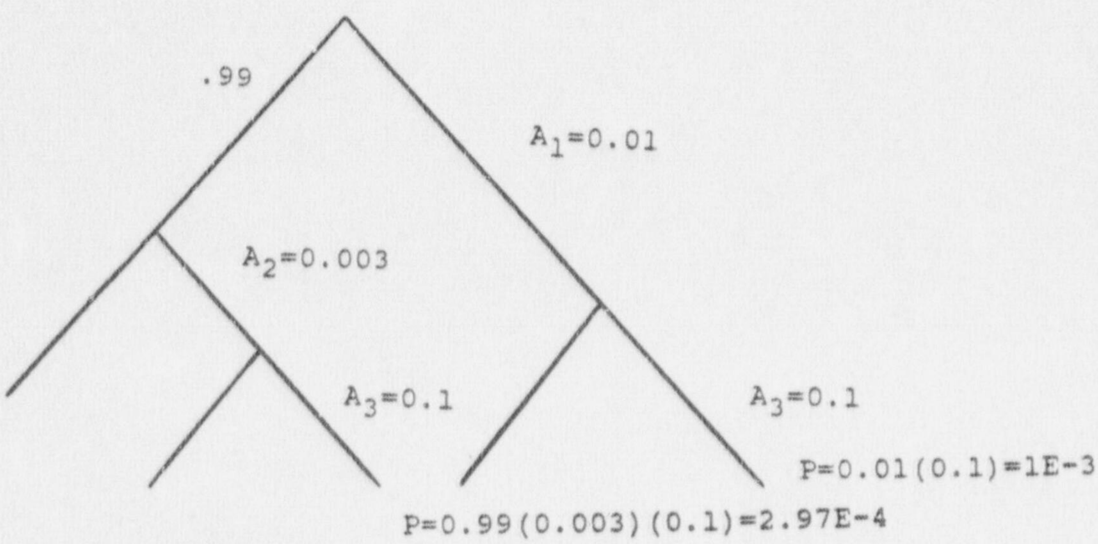
HUMAN ERROR CALCULATIONS

1. Operator prematurely racks power out by opening the breakers for MOV's 8701 and 8702 using operating procedure OP B-2:IV.

   1. Omission error - operator fails to close MOV
      HEP = 0.01 Table 20-7 no checkoff provisions, long list, ≥ 10 items

   2. Commission error - operator selects wrong circuit breaker
      HEP = 0.003 Table 20-12

   3. Recovery error - checker fails to detect errors by others
      HEP = 0.1 Table 20-22



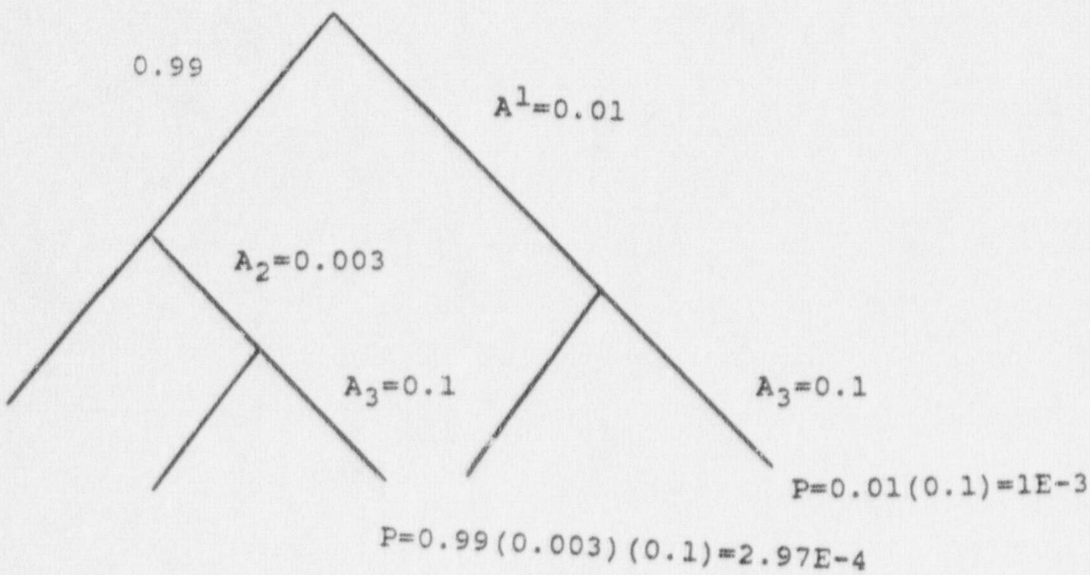
P_{OE} = 1E-3 + 2.97E-4
= 1.297E-3
= 1.3E-3

Fault Tree Identifiers: R1CBOEB and R2CBOEB

TABLE B-2 (Cont)

2. Operator fails to remove power from valve at circuit breaker for MOV's 8701 and 8702 using operating procedure OP B-2:IV

1.	Omission error HEP = 0.01	-	operator fails to open circuit break Table 20-7 no checkoff provisions, long list, ≥ 10 items
2.	Commission error HEP = 0.003	-	operator selects wrong circuit breaker Table 20-12
3.	Recovery error HEP = 0.1	-	checker fails to detect errors by others Table 20-22



P_{OE} = 1E-3 + 2.97E-4
= 1.3E-3

Fault Tree Identifiers: R1CBREMOE and R2CBREMOE

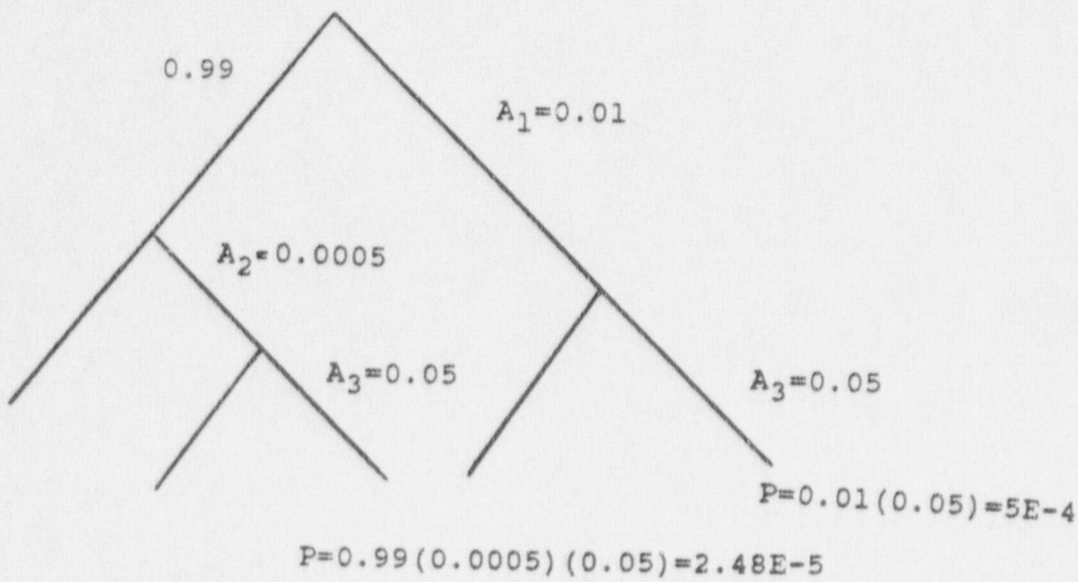
TABLE B-2 (Cont)

3. Operator fails to close MOV after previous use using operating procedure OP B-2:IV

1. Omission error - operator fails to close MOV
   HEP = 0.01 Table 20-7 no checkoff provisions
   long list, ≥ 10 items

2. Commission error - operator turns rotary control in wrong direction
   HEP = 0.0005 Table 20-12

3. Recovery error - checker fails to detect errors by others
   HEP = 0.05 Table 20-22



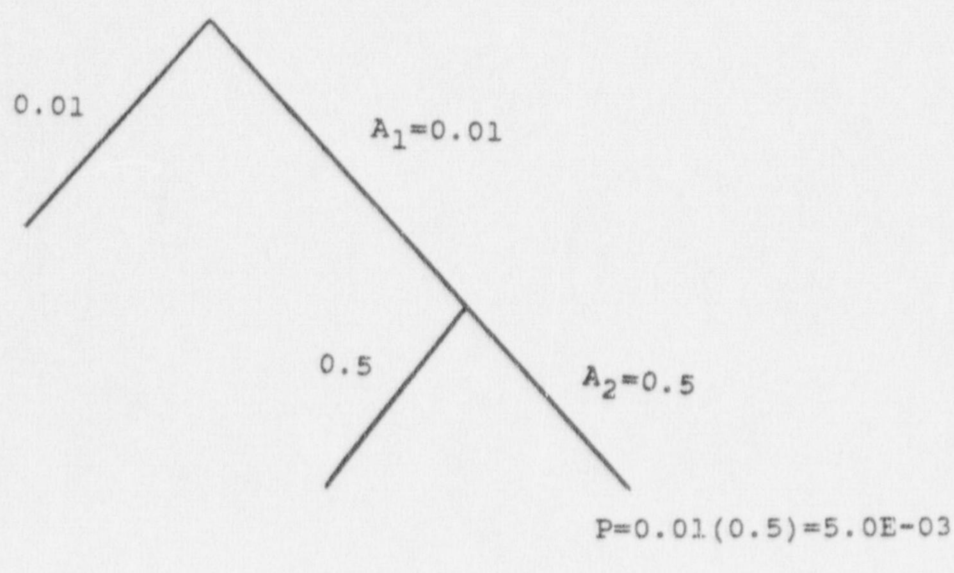
P_{OE} = 5E-4 + 2.48E-5
= 5.25E-4

Fault Tree Identifiers: R187010EO and R287020EO

TABLE B-2 (Cont)

4. Operator fails to detect wrong position via status light

   1. Omission error - operator fails to detect
      HEP = 0.01 Table 20-27 long list > 10 items
   2. Commission error - checker fails to detect
      HEP = 0.5 Table 20-22 second checker

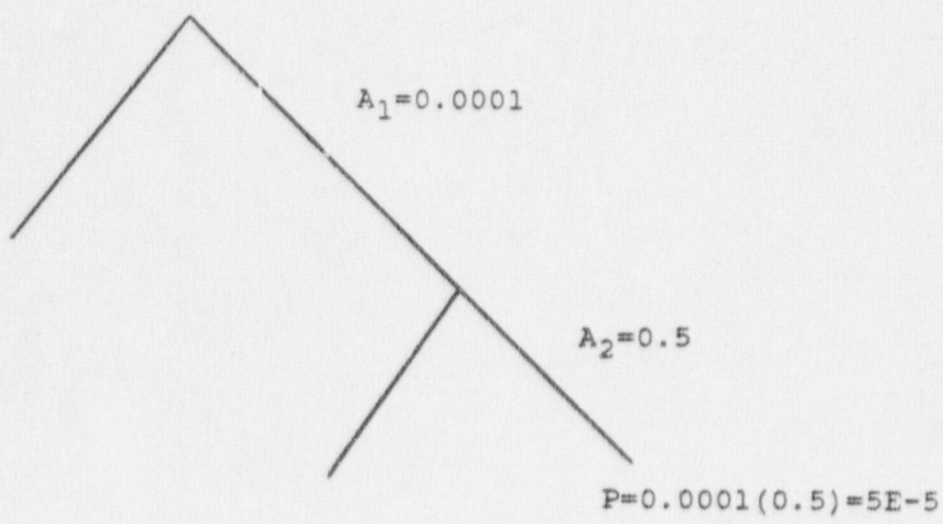


P_{OE} = 5E-3
Fault Tree Identifiers: R187010EST and R287020EST

5. Operator fails to detect wrong position via alarm

    1. Omission error - operator fails to detect
       HEP = 0.0001 Table 20-23 one annunciator

    2. Recovery error - checker fails to detect
       HEP = 0.5 Table 20-22 second checker



P_{OE} = 5E-5
Fault Tree Identifiers: R2B702ALOE, R1B201ALOE

TABLE B-3

MOV 8701 IS OPEN-PRESENT CONFIGURATION

DOMINANT CONTRIBUTORS

Cut Set Probability	Percent Contribution to Unavailability	Cut set	Description
1. 1.50E-5	62.8	R1MV8701K, R187010EST	8701 Fails to Close and Operator Fails to Detect via Status Light
2. 6.50E-6	27.2	R1CBOEB, R187010EST	Operator Prematurely Racks Power Out and Fails to Detect via Status Light
3. 1.50E-6	6.3	R1CN42CAK, R187010EST	Contact 42(c)A Fails to Transfer and Operator Fails to Detect via Status Light
4. 5.00E-7	2.1	R1L533ACU, R187010EST	Limit Switch 33AC Fails Open and Operator Fails to Detect via Status Light
5. 1.50E-7	0.6	R187010EST, R15RCNK	Close Contact on Switch Fails to Transfer and Operator Fails to Detect via Status Light

Mean Unavailability = 2.39E-5

TABLE B-4
MOV 8702 IS OPEN-PRESENT CONFIGURATION
DOMINANT CONTRIBUTORS

Cut Set Probability	Percent Contribution to Unavailability	Cut set	Description
1. 1.50E-5	62.8	R2MV8702K, R287020EST	8702 Fails to Close and Operator Fails to Detect via Status Light
2. 6.50E-6	27.2	R2CBOEB, R287020EST	Operator Prematurely Racks Power Out and Fails to Detect via Status Light
3. 1.50E-6	6.3	R2CN42CAK, R287020EST	Contact 42(c)A Fails to transfer and Operator Fails to Detect via Status Light
4. 5.00E-7	2.1	R2LS33ACU, R287020EST	Limit Switch 33AC Fails Open and Operator Fails to Detect via Status Light
5. 1.50E-7	0.6	R287020EST, R25RCNK	Close Contact on Switch Fails to Transfer and Operator Fails to Detect via Status Light

Mean Unavailability = 2.39E-5

TABLE B-5
MOV 8701 IS OPEN-MODIFICATION
DOMINANT CONTRIBUTORS

Cut Set Probability	Percent Contribution to Unavailability	Cut set	Description
1. 4.50E-9	35.4	R18701EST, R1TP405CNK, R18701K	Alarm Pressure Transmitter Relay Contact Fails to Transfer, Valve Fails to Close, Operator Fails to Detect via Status Light
2. 1.95E-9	15.4	R18701EST, R1TP405CNK, R1CBOEB	Alarm Pressure Relay Contact Fails to Transfer, Operator Prematurely Racks Power Out and Fails to Detect via Status Light.
3. 1.50E-9	11.8	R18701EST, R1ALLSK, R18701K	Alarm Limit Switch Fails to Operate, Valve Fails to Close and Operator Fails to Detect
4. 7.87E-10	6.2	R18701OE, R18701EST, R1TP405CNK	Operator Fails to Close Valve, Fails to Detect via Status Light and Alarm Pressure Relay Contact Fails
5. 7.50E-10	5.9	R18701EST, R18701ALO, R18701K	Operator Fails to Detect via Status Light and Alarm, Valve Fails to Close

Mean Unavailability = 1.27E-8

TABLE B-6

MOV 8702 IS OPEN-MODIFICATION

DOMINANT CONTRIBUTORS

Cut Set Probability	Percent Contribution to Unavailability	Cut set	Description
1. 4.50E-9	35.4	R28702EST, R2TP403CNK, R28702K	Alarm Pressure Transmitter Relay Contact Fails to Transfer, Valve Fails to Close, Operator Fails to Detect via Status Light
2. 1.95E-9	15.4	R28702EST, R2TP403CNK, R2CBOEB	Alarm Pressure Relay Contact Fails to Transfer, Operator Prematurely Racks Power Out and Fails to Detect via Status Light.
3. 1.50E-9	11.8	R28702EST, R2ALLSK, R28702K	Alarm Limit Switch Fails to Operate, Valve Fails to Close and Operator Fails to Detect
4. 7.87E-10	6.2	R287020E, R28702EST, R2TP403CNK	Operator Fails to Close Valve, Fails to Detect via Status Light and Alarm Pressure Relay Contact Fails
5. 7.50E-9	5.9	R28702EST, R28702ALO, R28702K	Operator Fails to Detect via Status Light and Alarm, Valve Fails to Close

Mean Unavailability = 1.27E-8

TABLE B-7
MOV 8701 IS OPEN-NRC MODIFICATION
DOMINANT CONTRIBUTORS

Cut Set Probability	Percent Contribution to Unavailability	Cut set	Description
1. 4.50E-9	37.8	R18701EST, R18701K, R1TP405CNK	Valve Fails to Close, Alarm Pressure Relay Contact Fails to Transfer and Operator Fails to Detect
2. 1.95E-9	16.4	R1CBOEB, R18701EST, R1TP405CNK	Alarm Pressure Relay Contact Fails to Transfer, Operator Prematurely Racks Power Out and Fails to Detect via Status Light.
3. 1.50E-9	12.6	R18701K, R18701EST, R28702K	Valve Fails to Close, Alarm Limit Switch Fails to Transfer, Operator Fails to Detect
4. 7.50E-10	6.3	R18701K, R18701EST, R18701ALOE	Valve Fails to Close, Operator Fails to Detect via Alarm and Status Light
5. 6.50E-10	5.5	R1CBOEB, R18701EST, R1ALLSK	Operator Prematurely Racks Power Out, Fails to Detect and Alarm Limit Switch Fails to Transfer

Mean Unavailability = 1.19E-8

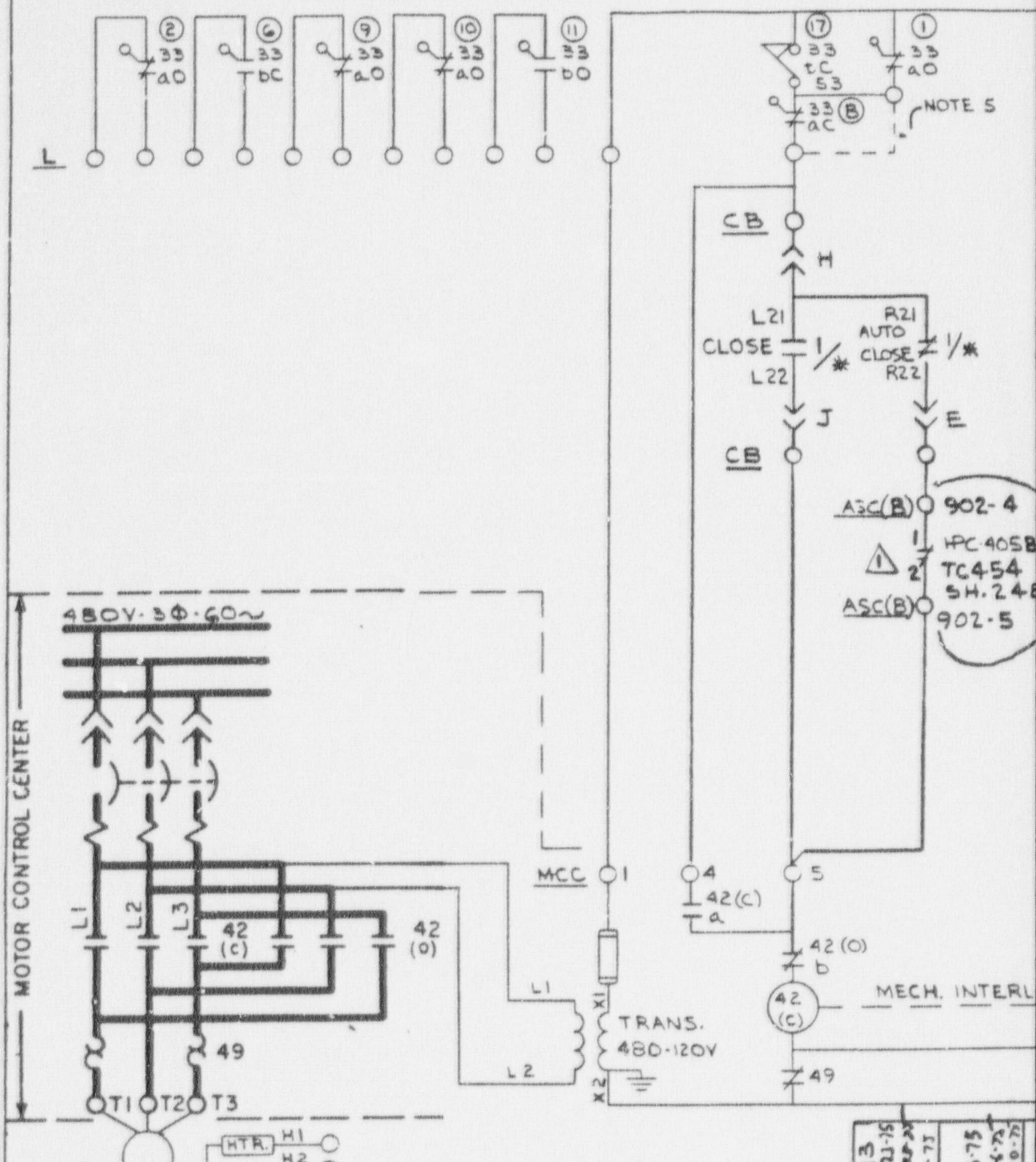
TABLE B-8

MOV 8702 IS OPEN-NRC Modification

DOMINANT CONTRIBUTORS

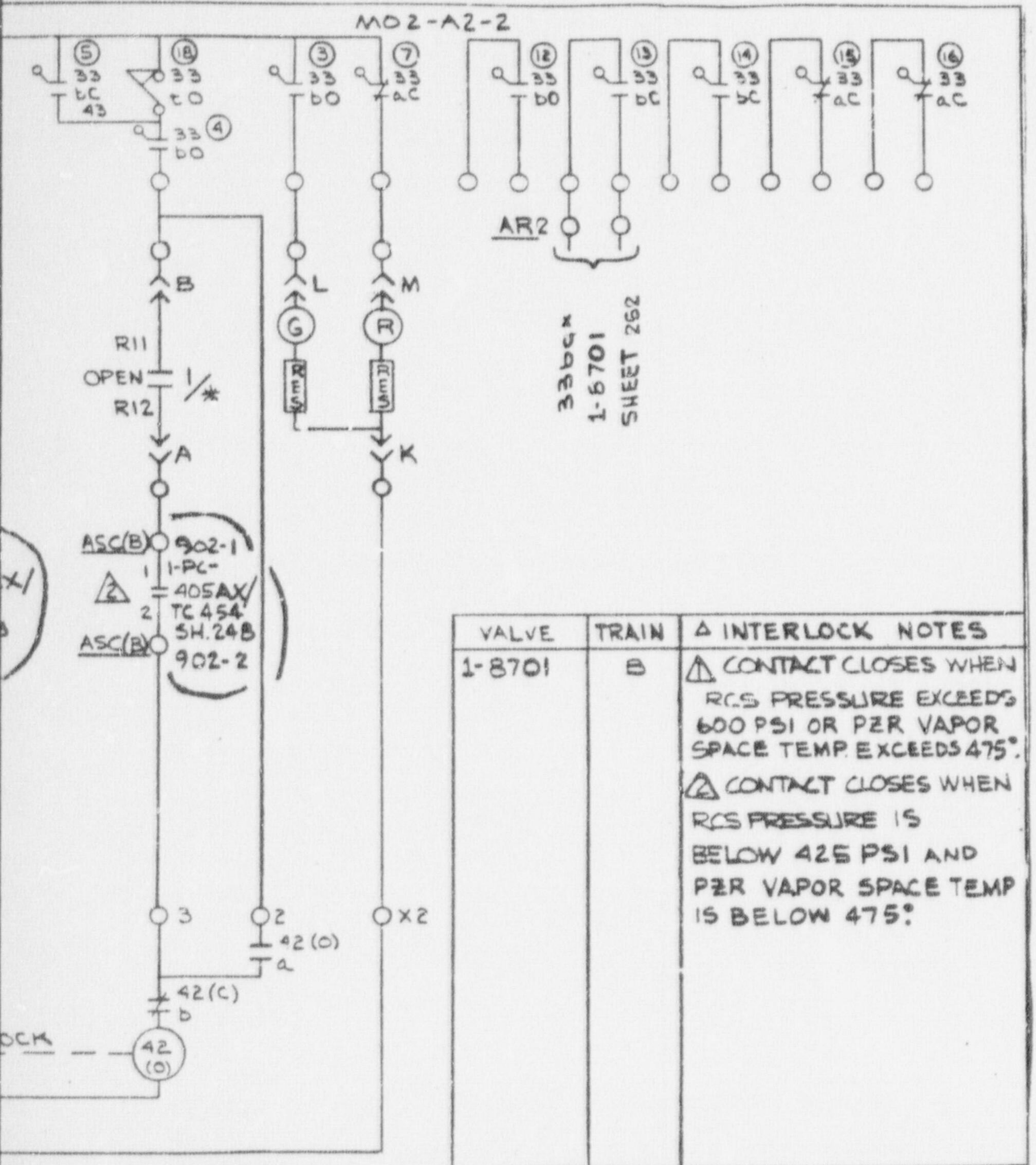
Cut Set Probability	Percent Contribution to Unavailability	Cut set	Description
1. 4.50E-9	37.8	R28702K, R28702EST, R2TP403CNK	Valve Fails to Close, Alarm Pressure Relay Contact Fails to Transfer and Operator Fails to Detect
2. 1.95E-9	16.4	R2CBOEB, R28702EST, R2TP403CNK	Alarm Pressure Relay Contact Fails to Transfer, Operator Prematurely Racks Power Out, Fails to Detect via Status Light
3. 1.50E-9	12.6	R28702K, R28702EST, R2ALLSK	Valve Fails to Close, Alarm Limit Switch Fails to Transfer, Operator Fails to Detect
4. 7.50E-10	6.3	R28702K, R28702EST, R28702ALOE	Valve Fails to Close, Operator Fails to Detect via Alarm and Status Light
5. 6.50E-10	5.5	R2CBOEB, R28702EST, R2ALLSK	Operator Prematurely Racks Power Out, Fails to Detect and Alarm Limit Switch Fails to Transfer

Mean Unavailability = 1.19E-8



NOTES:
1. * - VALVE NO.
2. 1/* - DEV. | SH.20 N.P.C. SH.21
3. CONTROL SHOWN FOR W TYPE W MOTOR CONTROL CENTER.
4. REF. "LIMITORQUE" DWG. 15-477-2785-3 & 2786-3
5. ADD JUMPER IF TORQUE SEATING IS REQD.

ECN-30613 Wm. Soles 6-23-75	6
ECN-30552 W. DEAN 3-5-75	5



VALVE	TRAIN	△ INTERLOCK NOTES
1-8701	B	△1 CONTACT CLOSES WHEN RCS PRESSURE EXCEEDS 600 PSI OR PZR VAPOR SPACE TEMP. EXCEEDS 475°. △2 CONTACT CLOSES WHEN RCS PRESSURE IS BELOW 425 PSI AND PZR VAPOR SPACE TEMP IS BELOW 475°.

4	W.M.CAMP 4-26-73		3-1-74
3	ECN 7622 R.W.KEMERER 5/17/71	6/8/71	6-10-71
2	ECW-C800	11-12-70	12/17/70
1	PGE/PEG-385		
SUB	S.O.		

Westinghouse Electric Corporation

TITLE PACIFIC GAS & ELECTRIC CO.
DIABLO CANYON UNITS #1 & 2

ELEMENTARY WIRING DIAG.		MOTOR OPERATED VALVE	
WM SOLES	7/31/70	8/14/70	501B180
R. WILSON	8/14/70	9-16-70	SHEET- 141

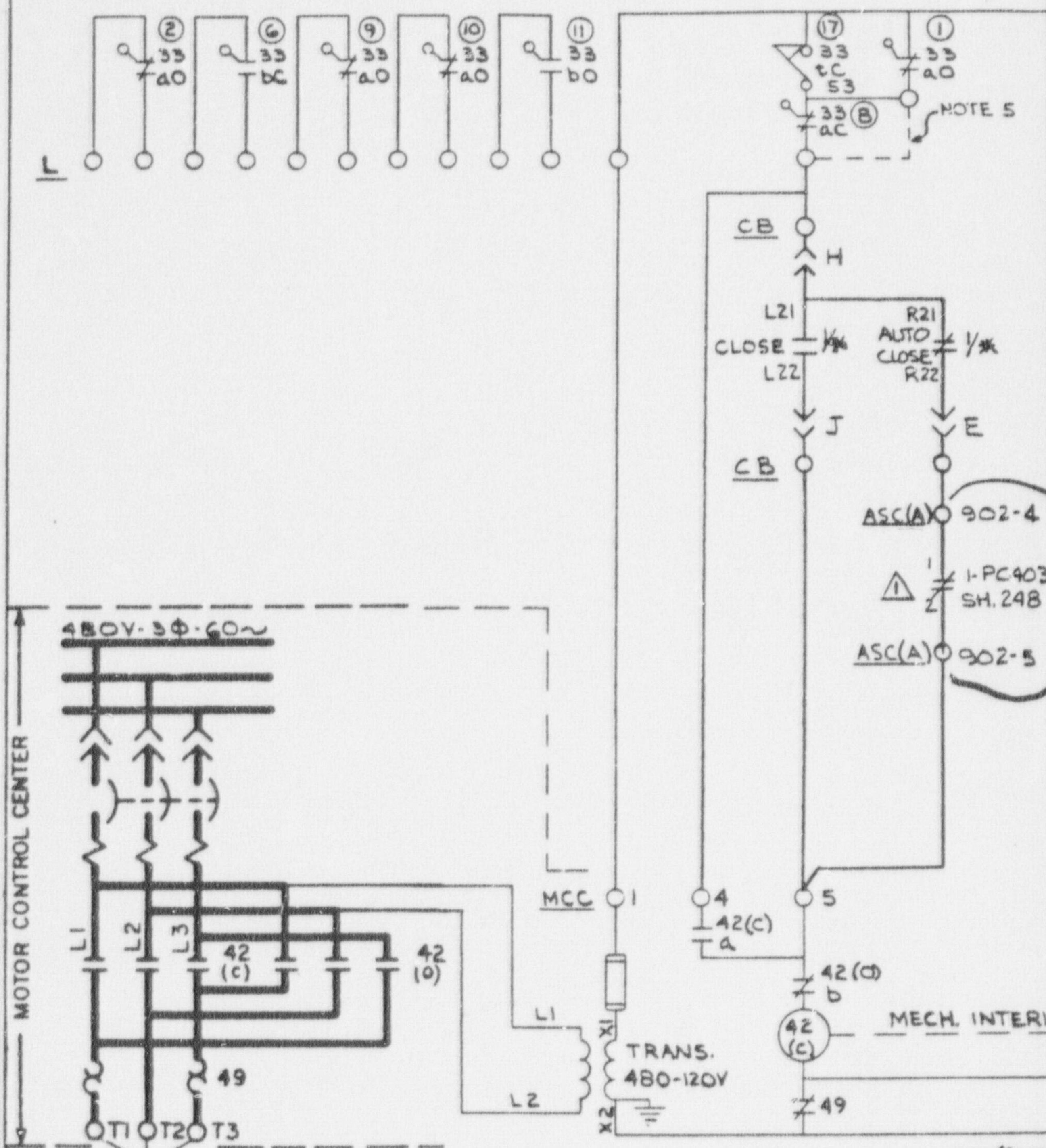
NUCLEAR ENERGY SYSTEMS PITTSBURGH, PA., U.S.A.

TI APERTURE CARD

Also Available On Aperture Card

FIGURE B-1
PRESENT INTERLOCK CONFIGURATION 8701

8708110183-04



NOTES:
1. * - VALVE NO.
2. 1/* - DEV. 1 SH. 20 N.P. "C" SH. 21
3. CONTROL SHOWN FOR W TYPE W MOTOR CONTROL CENTER.
4. REF. "LIMITORQUE" DWG. 15-477-2785-3 & 2786-3
5. ADD JUMPER IF TORQUE SEATING IS REQD.

ECN-30613

5

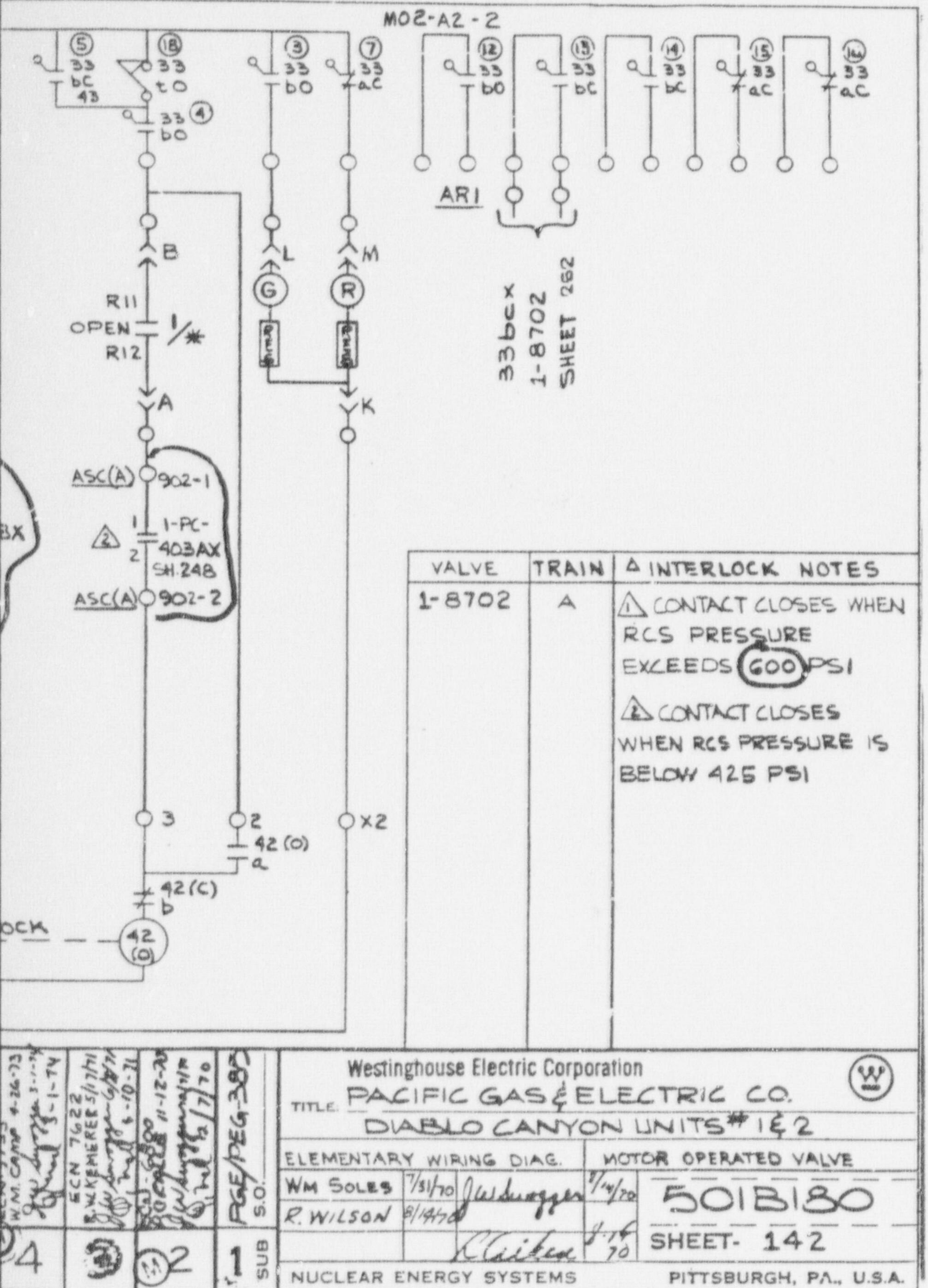
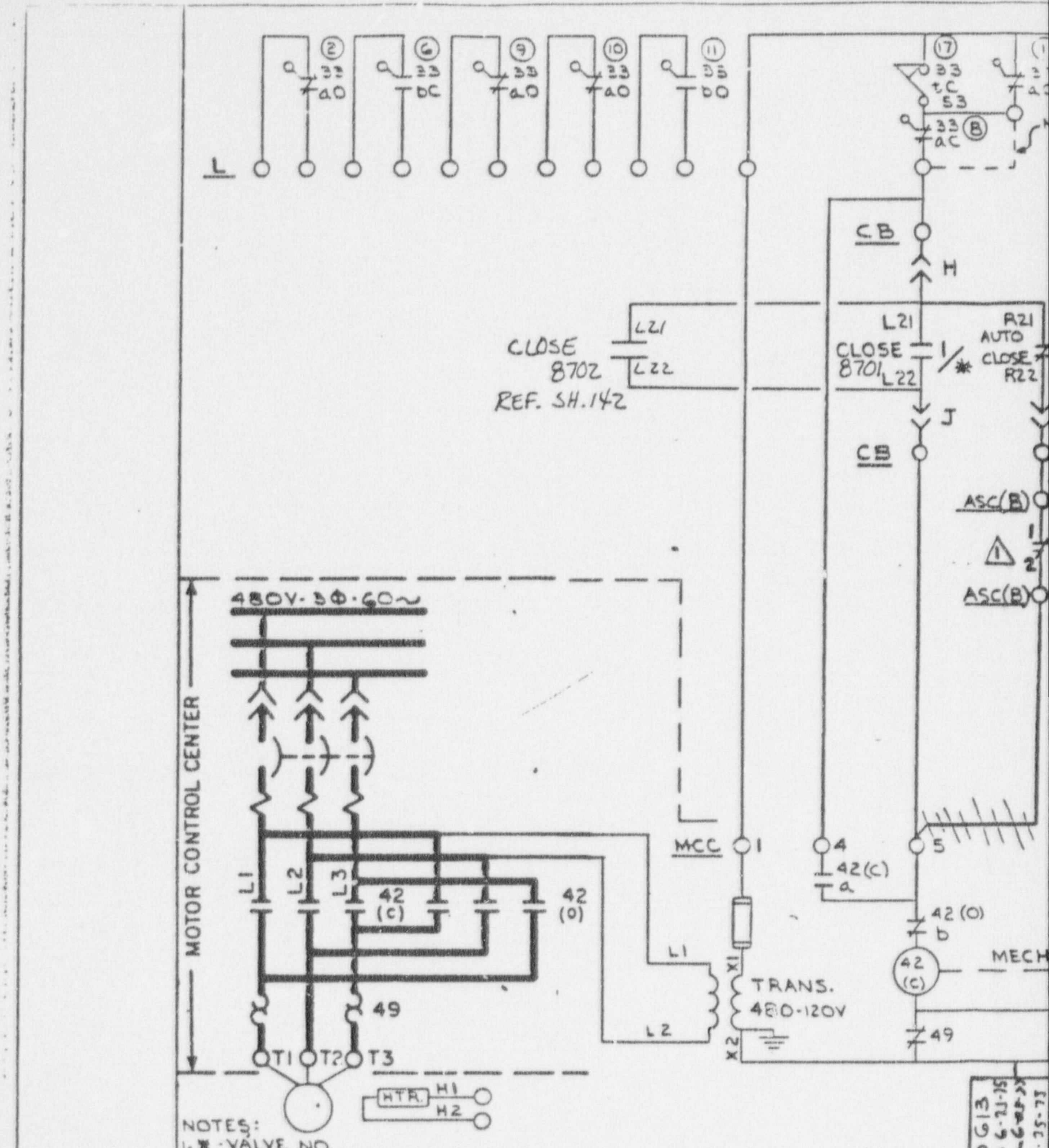
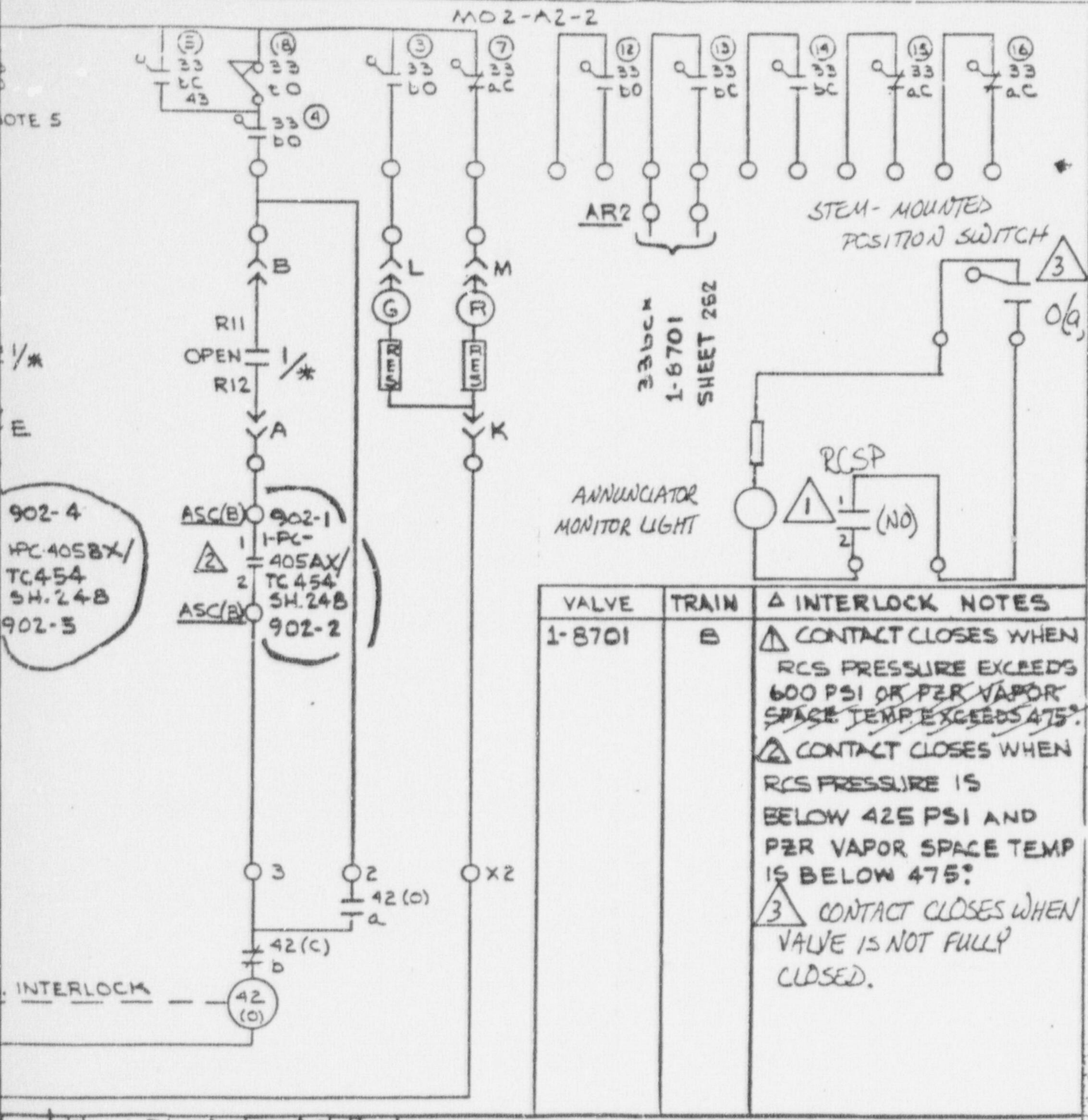


FIGURE B-2
PRESENT INTERLOCK CONFIGURATION 8702

8708110183-05



NOTES:
1. * - VALVE NO.
2. 1/* - DEV. 1 SH.20 N.P.C. SH.21
3. CONTROL SHOWN FOR W TYPE W MOTOR CONTROL CENTER.
4. REF. "LIMITORQUE" DWG. 15-477-2785-3 & 2786-3
5. ADD JUMPER IF TORQUE SEATING IS REQD.



VALVE	TRAIN	△ INTERLOCK NOTES
1-8701	B	△1 CONTACT CLOSES WHEN RCS PRESSURE EXCEEDS 600 PSI ~~OR PZR VAPOR SPACE TEMP EXCEEDS 475°.~~ △2 CONTACT CLOSES WHEN RCS PRESSURE IS BELOW 425 PSI AND PZR VAPOR SPACE TEMP IS BELOW 475°. △3 CONTACT CLOSES WHEN VALVE IS NOT FULLY CLOSED.

5	4	3	2	1	SUB
ECN-30552 W. DEAN 3-5-73	ECN 3733 W.N. CAMP 4-26-73	ECN 7622 R.W. KEMERER 5/17/71	CW-6800 11-12-70	PGE/PEG 385	S.O.

Westinghouse Electric Corporation

TITLE PACIFIC GAS & ELECTRIC CO.
DIABLO CANYON UNITS 1 & 2

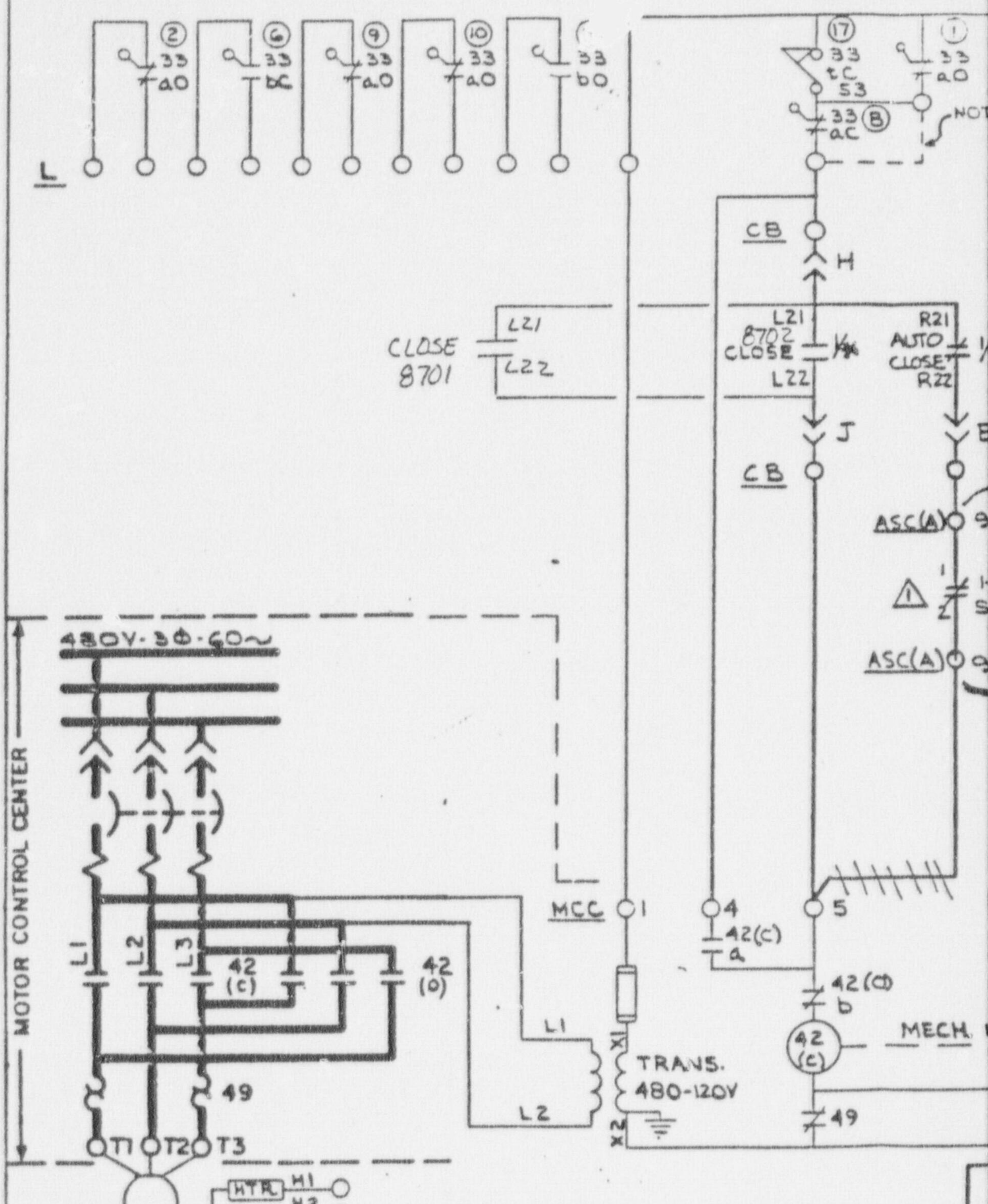
ELEMENTARY WIRING DIAG. MOTOR OPERATED VALVE

WM SOLES	7/31/70	
R. WILSON	8/14/70	501B180
		SHEET- 141

NUCLEAR ENERGY SYSTEMS PITTSBURGH, PA., U.S.A.

FIGURE B-3
NRC-PROPOSED MODIFICATION 8701

8708110183-06



NOTES:
1. ⊗ - VALVE NO.
2. V⊗ - DEV. 1 SH.20 N.P. "C" SH.21
3. CONTROL SHOWN FOR W TYPE W MOTOR CONTROL CENTER.
4. REF. - "LIMITORQUE" DWG. 15-477-2785-3 & 2786-3
5. ADD JUMPER IF TORQUE SEATING IS REQD.

ECN-30613

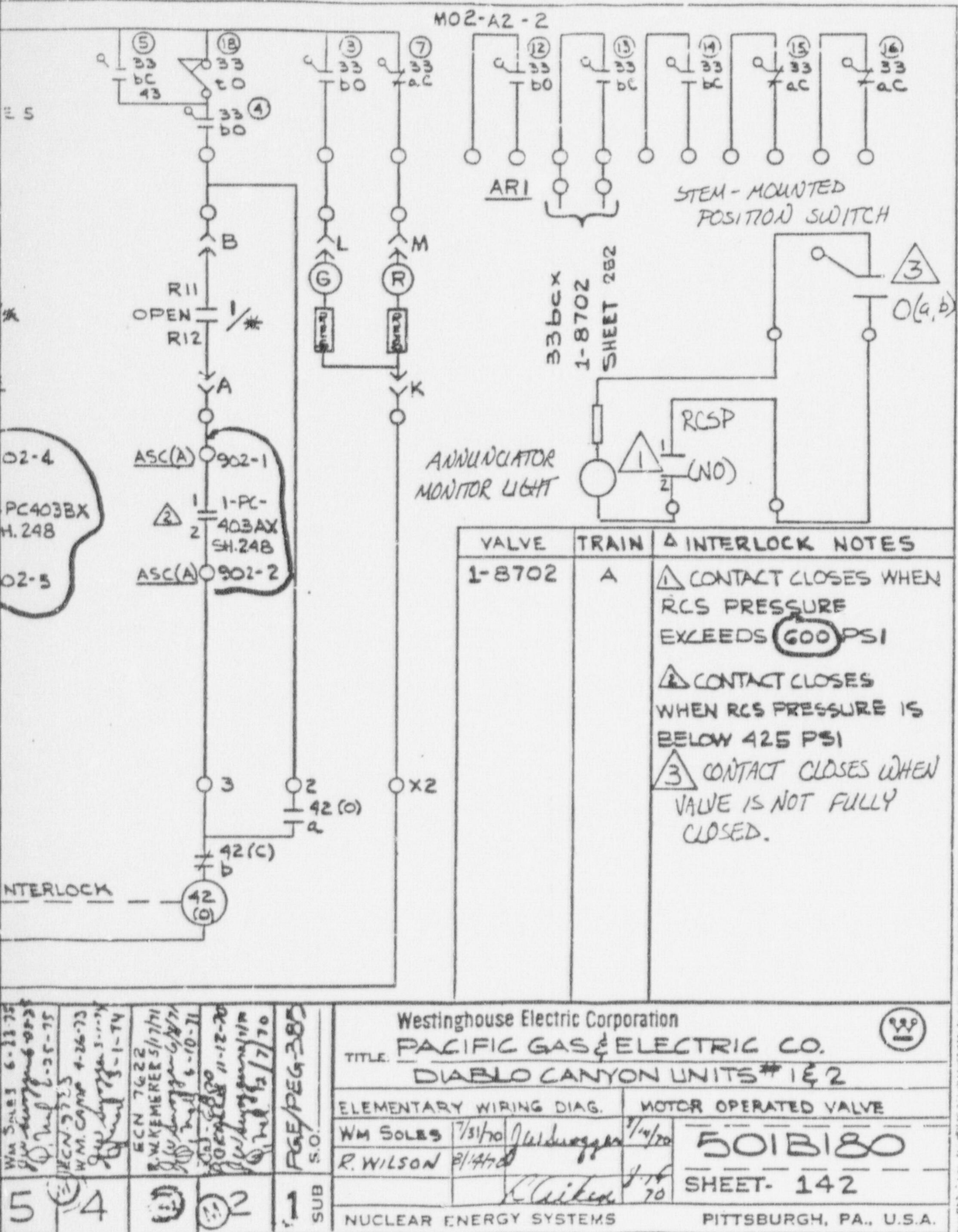
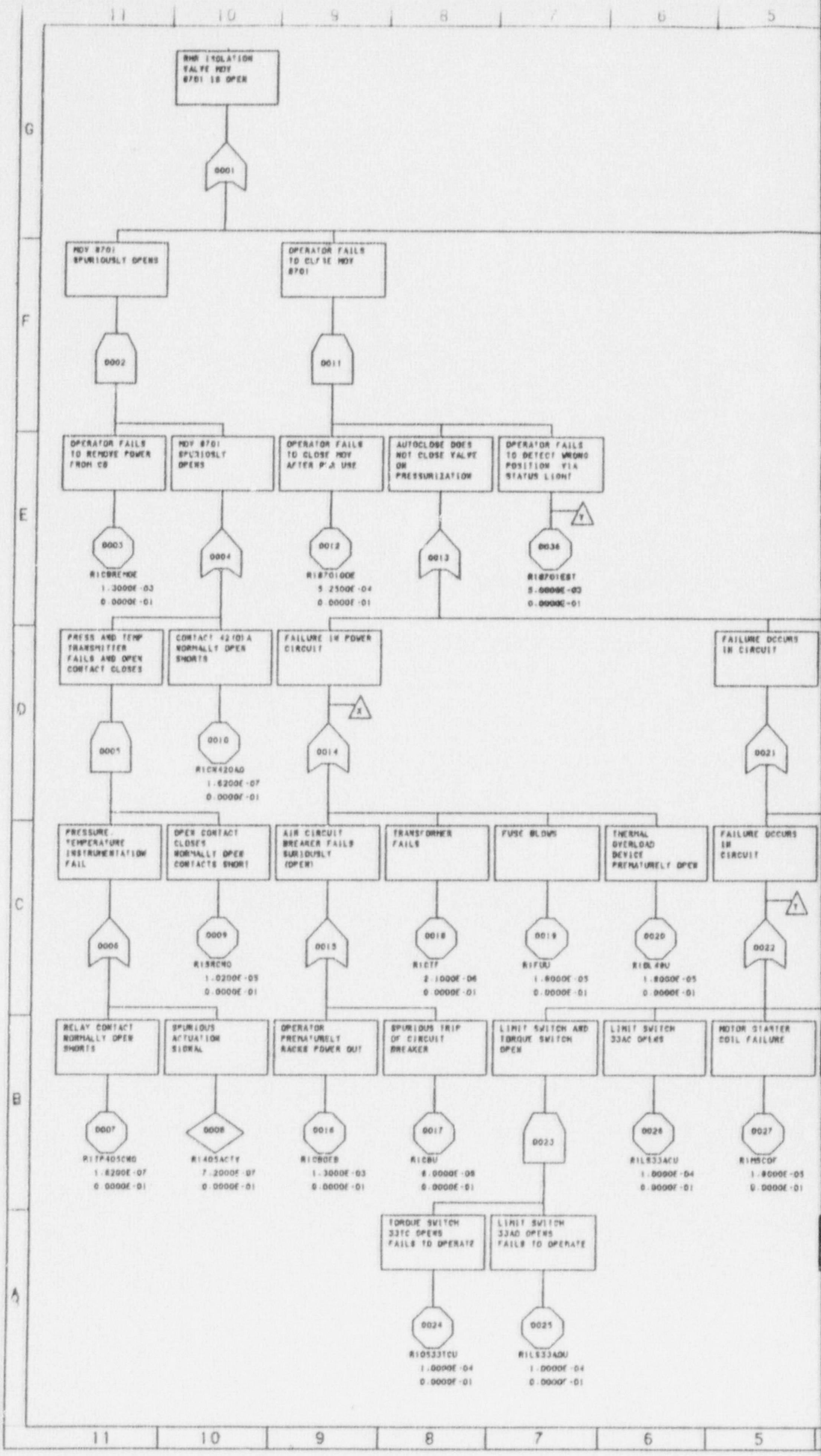
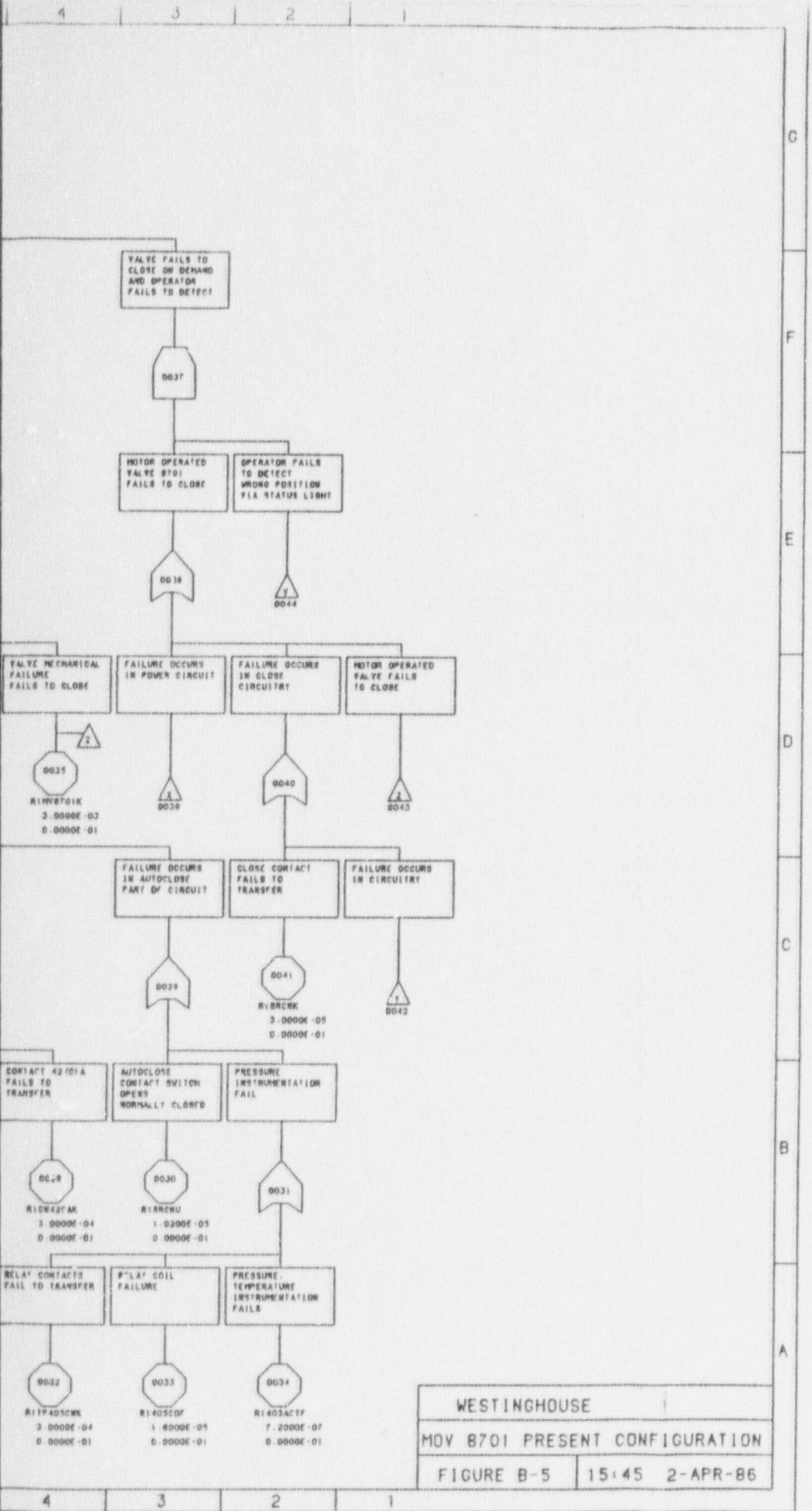


FIGURE B-4
NRC-PROPOSED MODIFICATION 8702

8708110183 -07



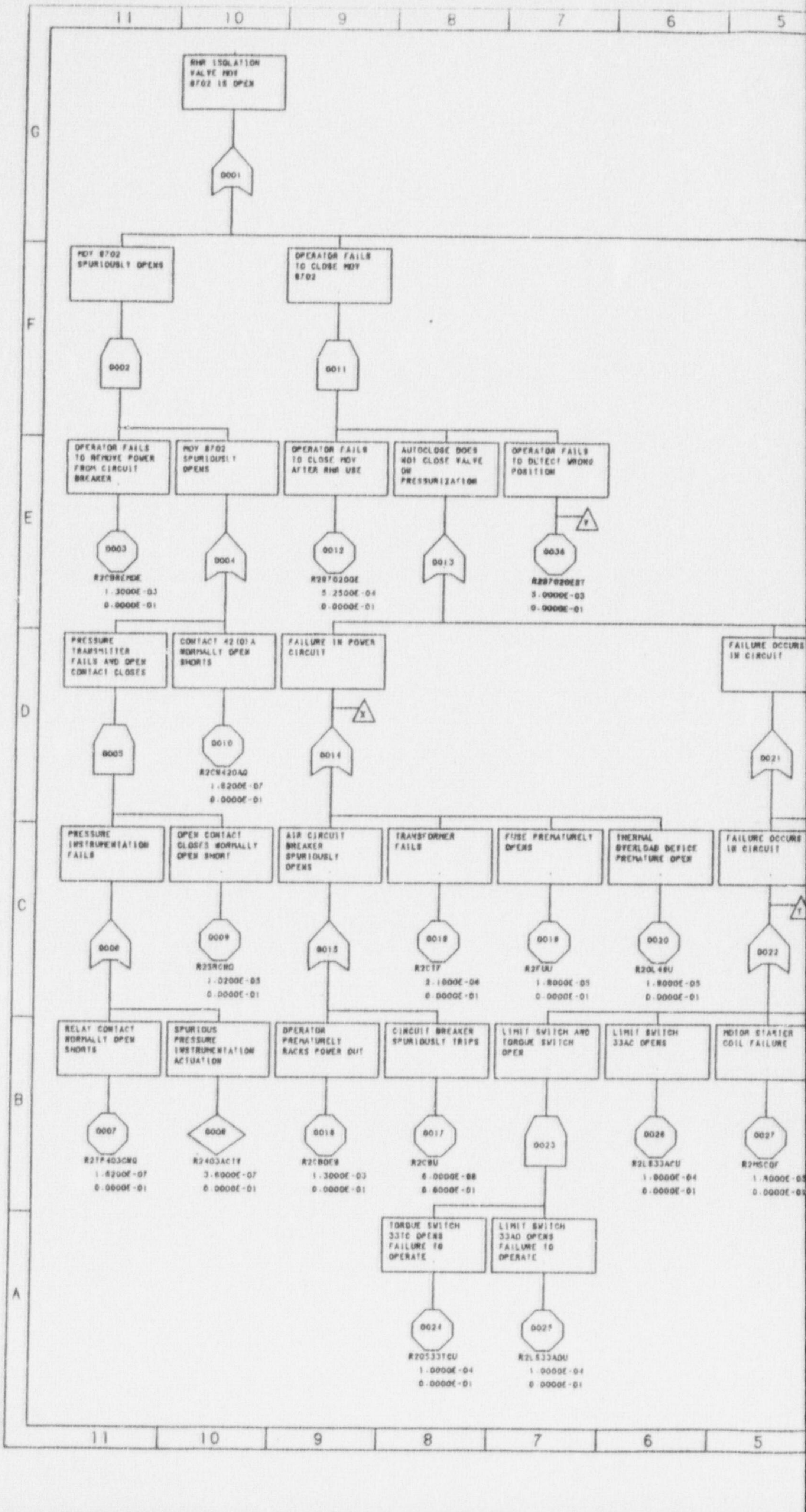
RHR ISOLATION VALVE MOV 8701 IS OPEN
0001
MOV 8701 SPURIOUSLY OPENS
OPERATOR FAILS TO CLOSE MOV 8701
0002
0011
OPERATOR FAILS TO REMOVE POWER FROM CB
MOV 8701 SPURIOUSLY OPENS
OPERATOR FAILS TO CLOSE MOV AFTER P/J USE
AUTOCLOSE DOES NOT CLOSE VALVE ON PRESSURIZATION
OPERATOR FAILS TO DETECT WRONG POSITION VIA STATUS LIGHT
0003
0004
0012
0013
0036
PRESS AND TEMP TRANSMITTER FAILS AND OPEN CONTACT CLOSES
CONTACT 42101A NORMALLY OPEN SHORTS
FAILURE IN POWER CIRCUIT
FAILURE OCCURS IN CIRCUIT
0005
0010
0014
0021
PRESSURE, TEMPERATURE INSTRUMENTATION FAIL
OPEN CONTACT CLOSES NORMALLY OPEN CONTACTS SHORT
AIR CIRCUIT BREAKER FAILS SURIOUSLY (OPEN)
TRANSFORMER FAILS
FUSE BLOWS
THERMAL OVERLOAD DEVICE PREMATURELY OPEN
FAILURE OCCURS IN CIRCUIT
0006
0009
0015
0018
0019
0020
0022
RELAY CONTACT NORMALLY OPEN SHORTS
SPURIOUS ACTUATION SIGNAL
OPERATOR PREMATURELY RACKS POWER OUT
SPURIOUS TRIP OF CIRCUIT BREAKER
LIMIT SWITCH AND TORQUE SWITCH OPEN
LIMIT SWITCH 33AC OPENS
MOTOR STARTER COIL FAILURE
0007
0008
0016
0017
0023
0026
0027
TORQUE SWITCH 33TC OPENS FAILS TO OPERATE
LIMIT SWITCH 33AO OPENS FAILS TO OPERATE
0024
0025
11
10
9
8
7
6
5
G
F
E
D
C
B
A



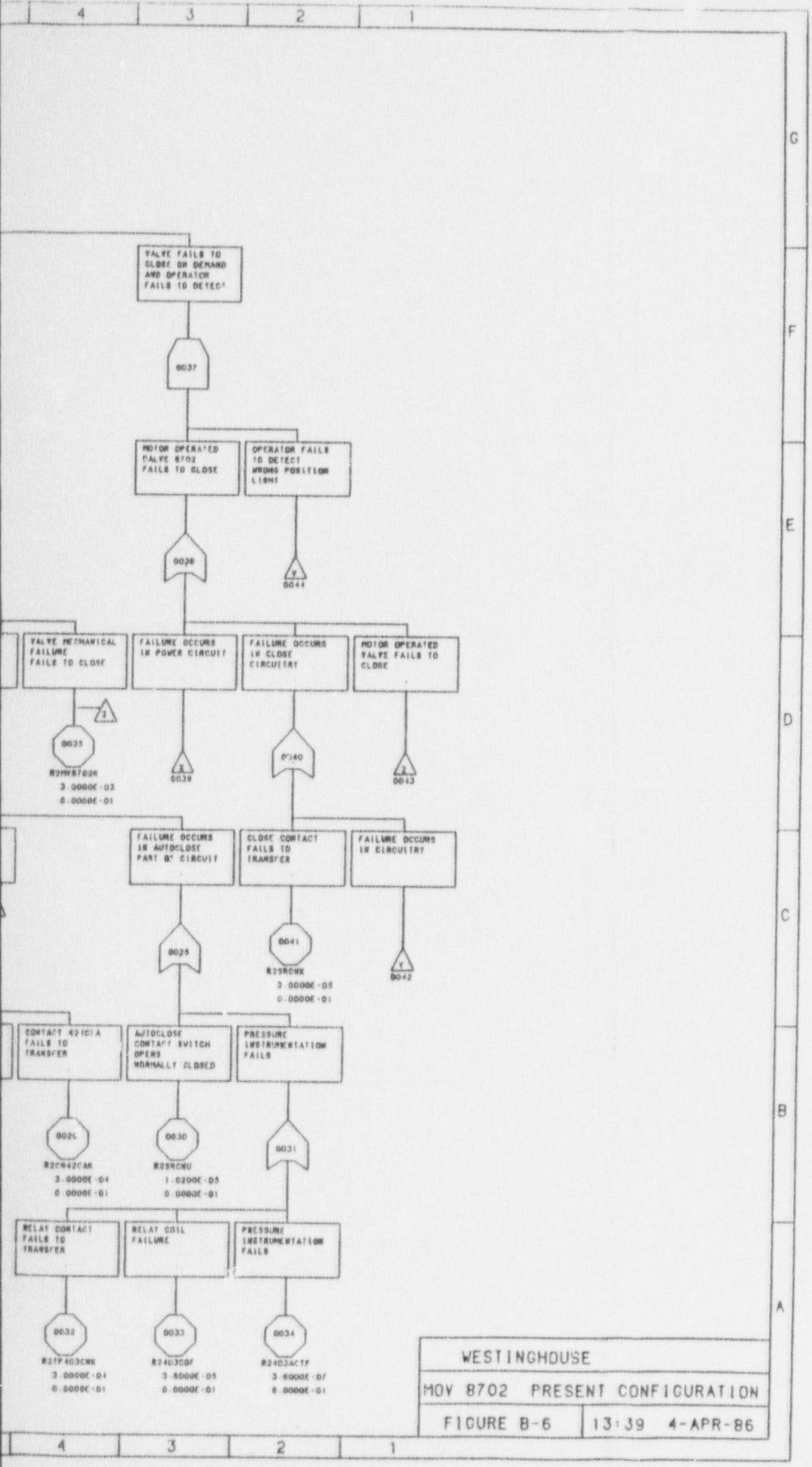
TI APERTURE CARD

Also Available On Aperture Card

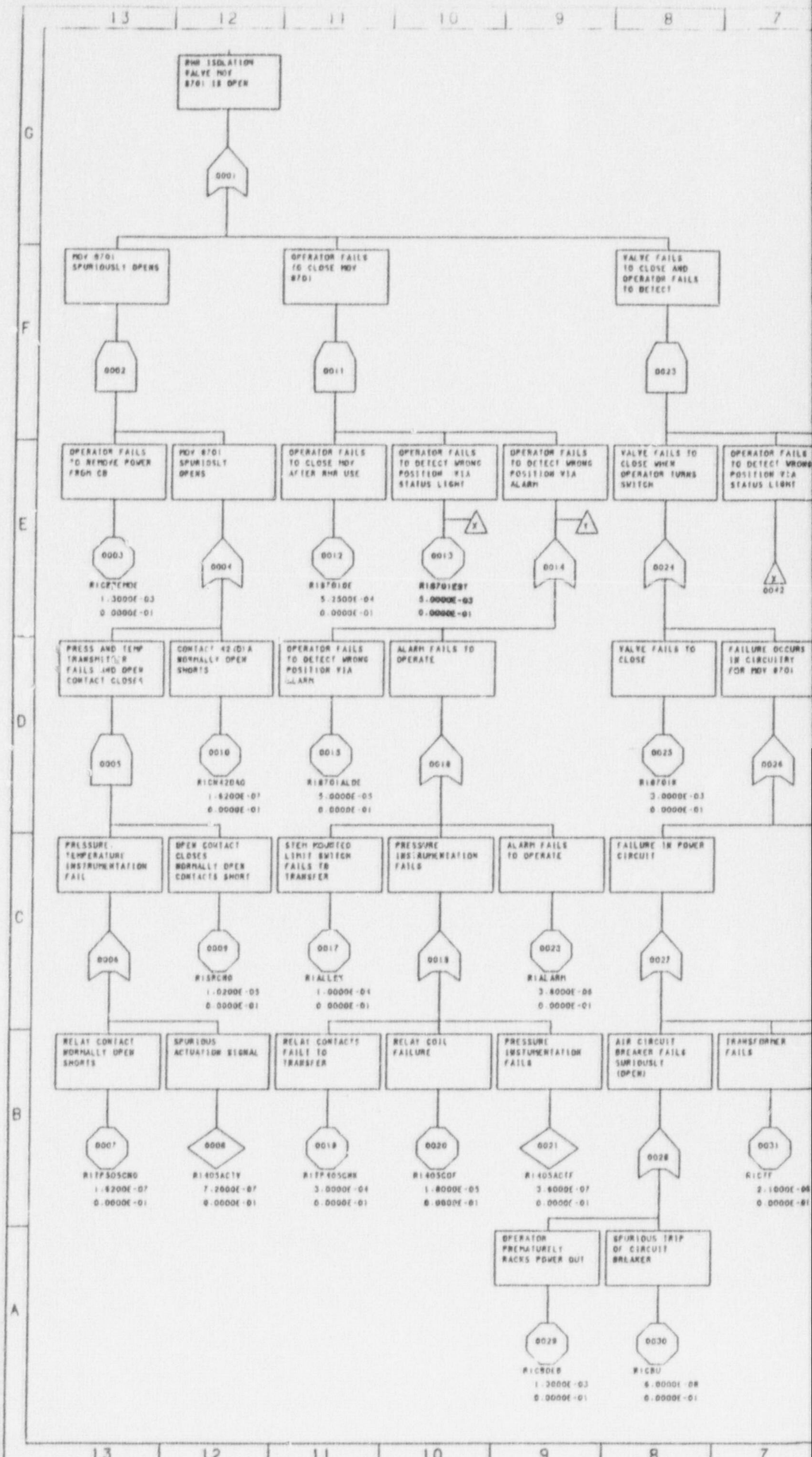
8708110185-08



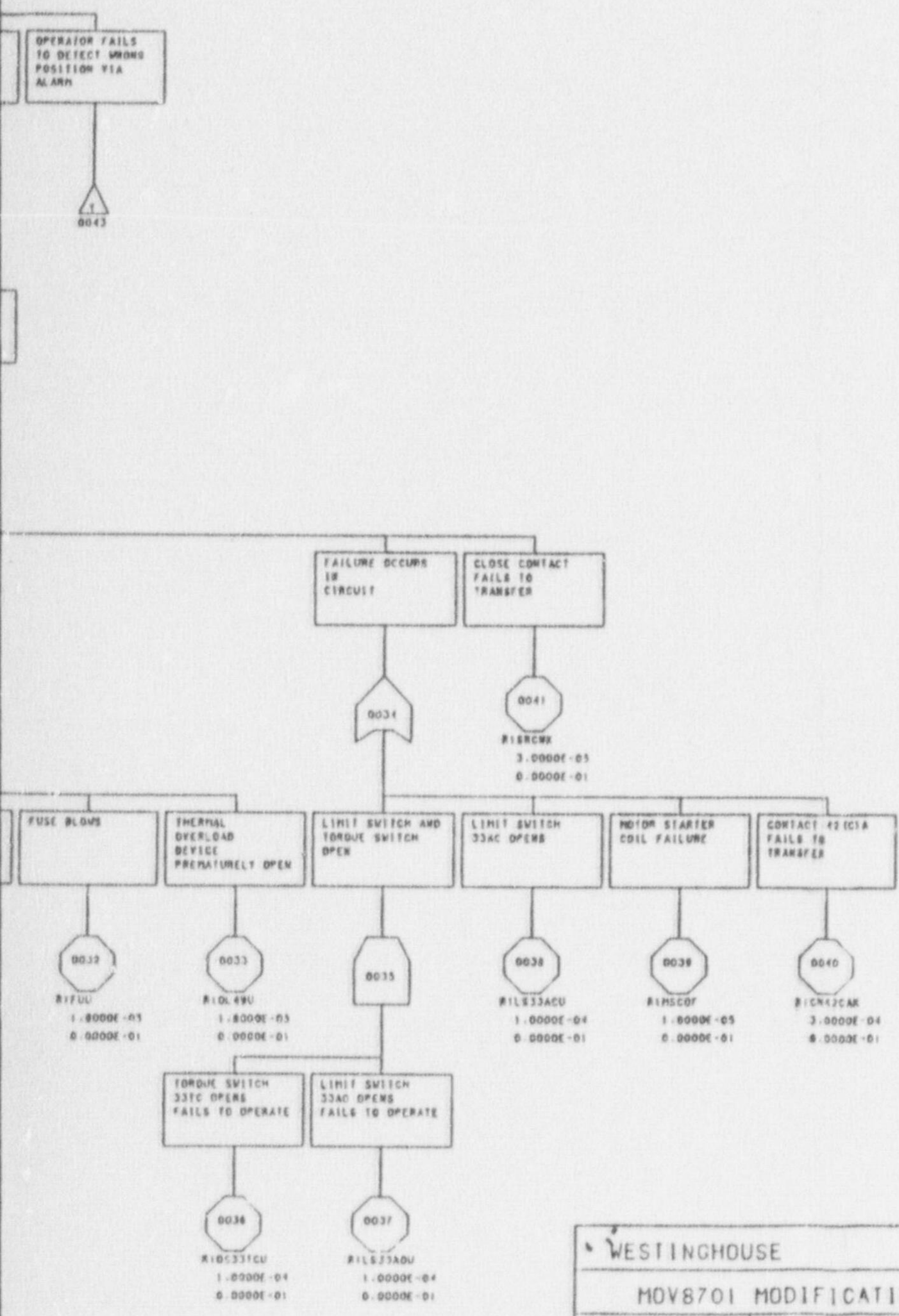
RHR ISOLATION VALVE MOV 8702 IS OPEN
0001
MOV 8702 SPURIOUSLY OPENS
OPERATOR FAILS TO CLOSE MOV 8702
0002
0011
OPERATOR FAILS TO REMOVE POWER FROM CIRCUIT BREAKER
MOV 8702 SPURIOUSLY OPENS
OPERATOR FAILS TO CLOSE MOV AFTER RHR USE
AUTOCLOSE DOES NOT CLOSE VALVE ON PRESSURIZATION
OPERATOR FAILS TO DETECT WRONG POSITION
Y
0003
R2CBREMDE
1.3000E-03
0.0000E-01
0004
0012
R2870200E
5.2500E-04
0.0000E-01
0013
0036
R287020EST
5.0000E-03
0.0000E-01
PRESSURE TRANSMITTER FAILS AND OPEN CONTACT CLOSES
CONTACT 42(O)A NORMALLY OPEN SHORTS
FAILURE IN POWER CIRCUIT
FAILURE OCCURS IN CIRCUIT
X
0005
0010
R2CN420AO
1.8200E-07
0.0000E-01
0014
0021
PRESSURE INSTRUMENTATION FAILS
OPEN CONTACT CLOSES NORMALLY OPEN SHORT
AIR CIRCUIT BREAKER SPURIOUSLY OPENS
TRANSFORMER FAILS
FUSE PREMATURELY OPENS
THERMAL OVERLOAD DEVICE PREMATURE OPEN
FAILURE OCCURS IN CIRCUIT
Y
0006
0009
R2SRCNO
1.0200E-03
0.0000E-01
0015
0018
R2CTF
2.1000E-06
0.0000E-01
0019
R2FUU
1.8000E-05
0.0000E-01
0020
R2OL48U
1.8000E-05
0.0000E-01
0022
RELAY CONTACT NORMALLY OPEN SHORTS
SPURIOUS PRESSURE INSTRUMENTATION ACTUATION
OPERATOR PREMATURELY RACKS POWER OUT
CIRCUIT BREAKER SPURIOUSLY TRIPS
LIMIT SWITCH AND TORQUE SWITCH OPEN
LIMIT SWITCH 33AC OPENS
MOTOR STARTER COIL FAILURE
0007
R2TP403CNO
1.8200E-07
0.0000E-01
0008
R2403ACTY
3.6000E-07
0.0000E-01
0016
R2CBOEB
1.3000E-03
0.0000E-01
0017
R2CBU
6.0000E-08
0.0000E-01
0023
0026
R2LS33ACU
1.0000E-04
0.0000E-01
0027
R2MSCOF
TORQUE SWITCH 33TC OPENS FAILURE TO OPERATE
LIMIT SWITCH 33AO OPENS FAILURE TO OPERATE
0024
R2OS33TCU
1.0000E-04
0.0000E-01
0025
R2LS33AOU
1.0000E-04
0.0000E-01



8708110183-09



RHR ISOLATION VALVE MOV 8701 IS OPEN
0001
MOV 8701 SPURIOUSLY OPENS
OPERATOR FAILS TO CLOSE MOV 8701
VALVE FAILS TO CLOSE AND OPERATOR FAILS TO DETECT
0002
0011
0023
OPERATOR FAILS TO REMOVE POWER FROM CB
MOV 8701 SPURIOUSLY OPENS
OPERATOR FAILS TO CLOSE MOV AFTER RHR USE
OPERATOR FAILS TO DETECT WRONG POSITION VIA STATUS LIGHT
OPERATOR FAILS TO DETECT WRONG POSITION VIA ALARM
VALVE FAILS TO CLOSE WHEN OPERATOR TURNS SWITCH
OPERATOR FAILS TO DETECT WRONG POSITION VIA STATUS LIGHT
0003
0004
0012
0013
0014
0024
0042
1.3000E-03
0.0000E-01
5.2500E-04
0.0000E-01
5.0000E-03
0.0000E-01
PRESS AND TEMP TRANSMITTER FAILS AND OPEN CONTACT CLOSES
CONTACT 42/D1A NORMALLY OPEN SHORTS
OPERATOR FAILS TO DETECT WRONG POSITION VIA ALARM
ALARM FAILS TO OPERATE
VALVE FAILS TO CLOSE
FAILURE OCCURS IN CIRCUITRY FOR MOV 8701
0005
0010
0015
0016
0025
0026
1.6200E-07
0.0000E-01
5.0000E-05
0.0000E-01
3.0000E-03
0.0000E-01
PRESSURE-TEMPERATURE INSTRUMENTATION FAIL
OPEN CONTACT CLOSES NORMALLY OPEN CONTACTS SHORT
STEM MOUNTED LIMIT SWITCH FAILS TO TRANSFER
PRESSURE INSTRUMENTATION FAILS
ALARM FAILS TO OPERATE
FAILURE IN POWER CIRCUIT
0006
0009
0017
0018
0022
0027
1.0200E-05
0.0000E-01
1.0000E-04
0.0000E-01
3.8000E-06
0.0000E-01
RELAY CONTACT NORMALLY OPEN SHORTS
SPURIOUS ACTUATION SIGNAL
RELAY CONTACTS FAIL TO TRANSFER
RELAY COIL FAILURE
PRESSURE INSTUMENTATION FAILS
AIR CIRCUIT BREAKER FAILS SPURIOUSLY (OPEN)
TRANSFORMER FAILS
0007
0008
0019
0020
0021
0028
0031
1.6200E-07
0.0000E-01
7.2600E-07
0.0000E-01
3.0000E-04
0.0000E-01
1.8000E-05
0.0000E-01
3.6000E-07
0.0000E-01
2.1000E-06
0.0000E-01
OPERATOR PREMATURELY RACKS POWER OUT
SPURIOUS TRIP OF CIRCUIT BREAKER
0029
0030
1.3000E-03
0.0000E-01
6.0000E-08
0.0000E-01
13
12
11
10
9
8
7
G
F
E
D
C
B
A



WESTINGHOUSE

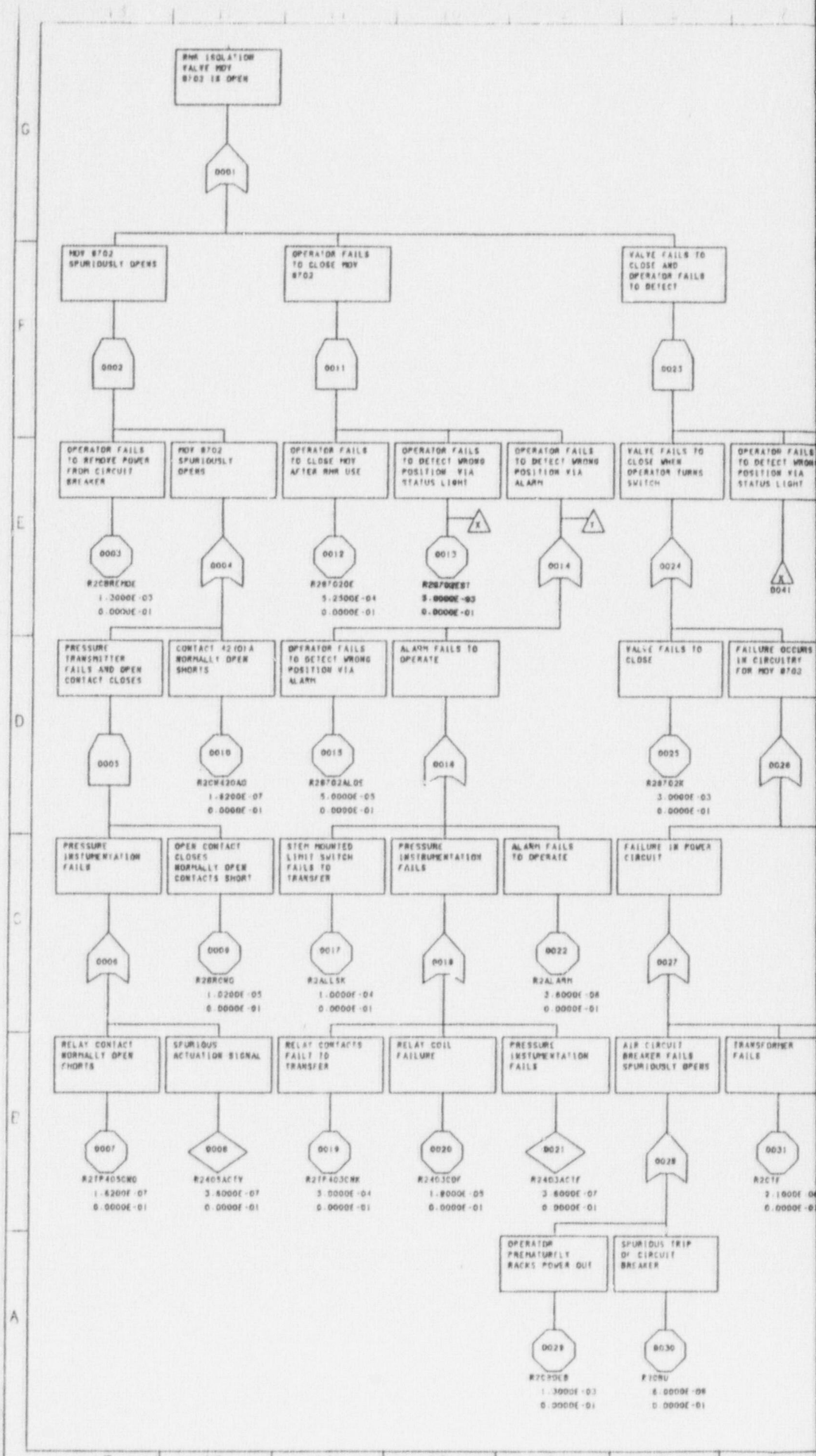
MOV8701 MODIFICATION

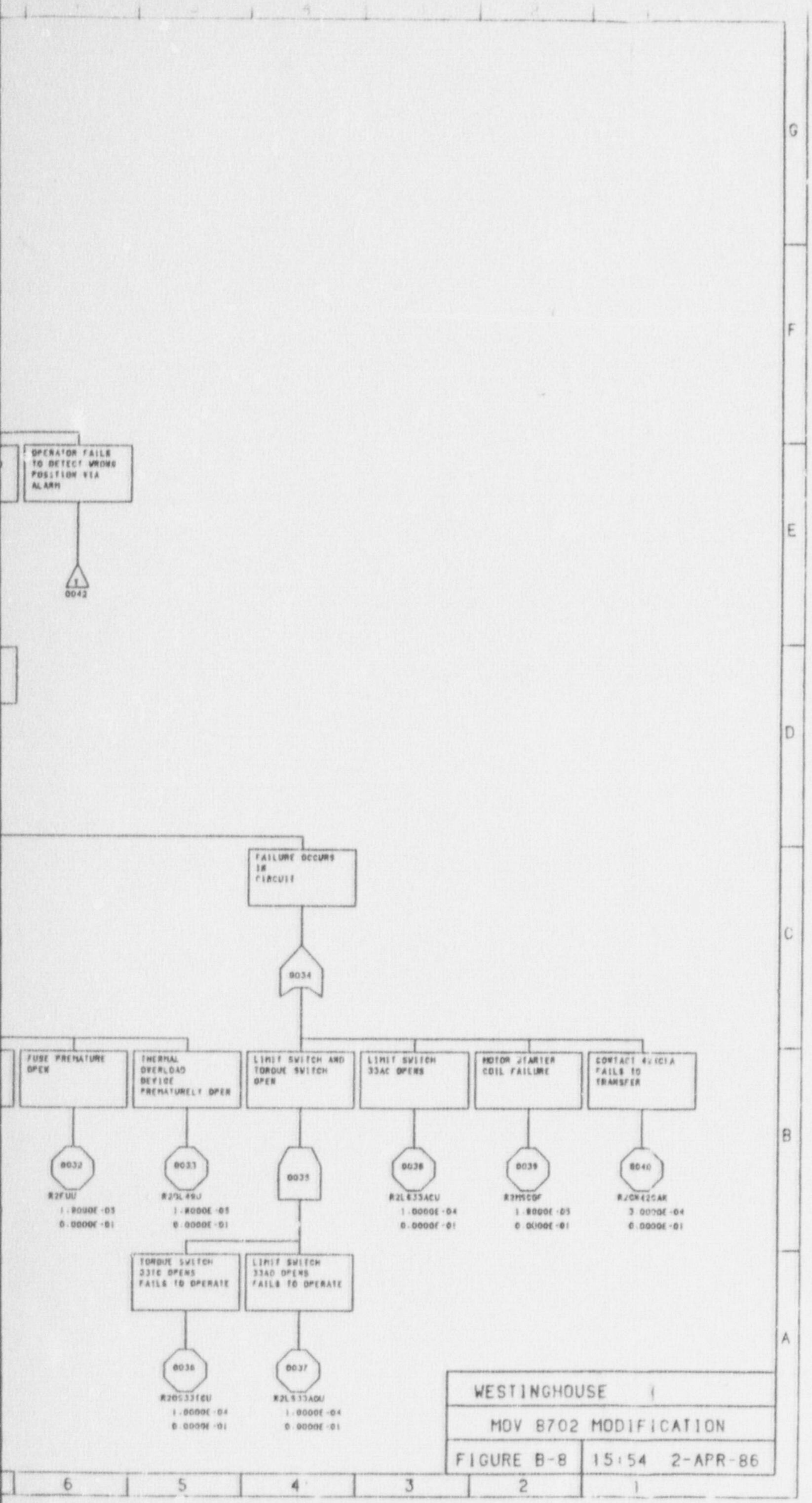
FIGURE B-7 15:53 2-APR-86

TI APERTURE CARD

Also Available On Aperture Card

8708110183-10

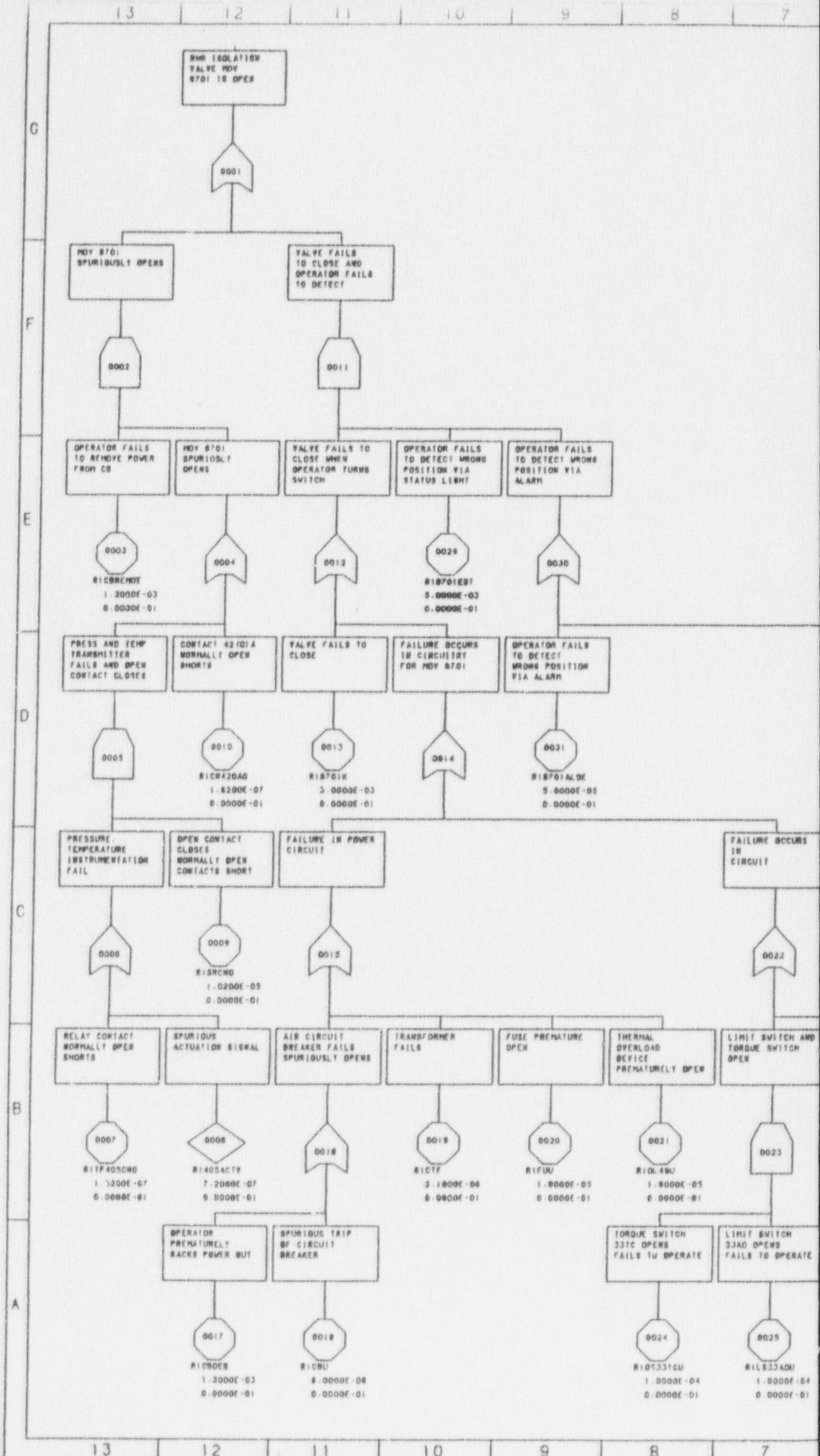

RHR ISOLATION VALVE MOV 8702 IS OPEN
0001
MOV 8702 SPURIOUSLY OPENS
OPERATOR FAILS TO CLOSE MOV 8702
VALVE FAILS TO CLOSE AND OPERATOR FAILS TO DETECT
0002
0011
0023
OPERATOR FAILS TO REMOVE POWER FROM CIRCUIT BREAKER
MOV 8702 SPURIOUSLY OPENS
OPERATOR FAILS TO CLOSE MOV AFTER RHR USE
OPERATOR FAILS TO DETECT WRONG POSITION VIA STATUS LIGHT
OPERATOR FAILS TO DETECT WRONG POSITION VIA ALARM
VALVE FAILS TO CLOSE WHEN OPERATOR TURNS SWITCH
OPERATOR FAILS TO DETECT WRONG POSITION VIA STATUS LIGHT
X
Y
0003
R2CBREMOE
1.3000E-03
0.0000E-01
0004
0012
R28702OE
5.2500E-04
0.0000E-01
0013
R28702EST
5.0000E-03
0.0000E-01
0014
0024
X
0041
PRESSURE TRANSMITTER FAILS AND OPEN CONTACT CLOSES
CONTACT 421DIA NORMALLY OPEN SHORTS
OPERATOR FAILS TO DETECT WRONG POSITION VIA ALARM
ALARM FAILS TO OPERATE
VALVE FAILS TO CLOSE
FAILURE OCCURS IN CIRCULTRY FOR MOV 8702
0005
0010
R2CM420AO
1.8200E-07
0.0000E-01
0015
R28702ALOE
5.0000E-05
0.0000E-01
0016
0025
R28702K
3.0000E-03
0.0000E-01
0026
PRESSURE INSTUMENTATION FAILS
OPEN CONTACT CLOSES NORMALLY OPEN CONTACTS SHORT
STEM MOUNTED LIMIT SWITCH FAILS TO TRANSFER
PRESSURE INSTRUMENTATION FAILS
ALARM FAILS TO OPERATE
FAILURE IN POWER CIRCUIT
0006
0009
R2BRCNO
1.0200E-05
0.0000E-01
0017
R2ALLSK
1.0000E-04
0.0000E-01
0018
0022
R2ALARM
2.6000E-08
0.0000E-01
0027
RELAY CONTACT NORMALLY OPEN SHORTS
SPURIOUS ACTUATION SIGNAL
RELAY CONTACTS FAILT TO TRANSFER
RELAY COIL FAILURE
PRESSURE INSTUMENTATION FAILS
AIR CIRCUIT BREAKER FAILS SPURIOUSLY OPENS
TRANSFORMER FAILS
0007
R2TP405CNO
1.6200E-07
0.0000E-01
0008
R2405ACTY
3.6000E-07
0.0000E-01
0019
R2TP403CNK
3.0000E-04
0.0000E-01
0020
R2403COF
1.8000E-05
0.0000E-01
0021
R2403ACTF
3.6000E-07
0.0000E-01
0028
0031
R2CTF
OPERATOR PREMATURELY RACKS POWER OUT
SPURIOUS TRIP OF CIRCUIT BREAKER
0029
R2CROEB
1.3000E-03
0.0000E-01
0030
R2CBU
6.0000E-08
0.0000E-01
G
F
E
D
C
B
A
13
12
11
10
9
8
7

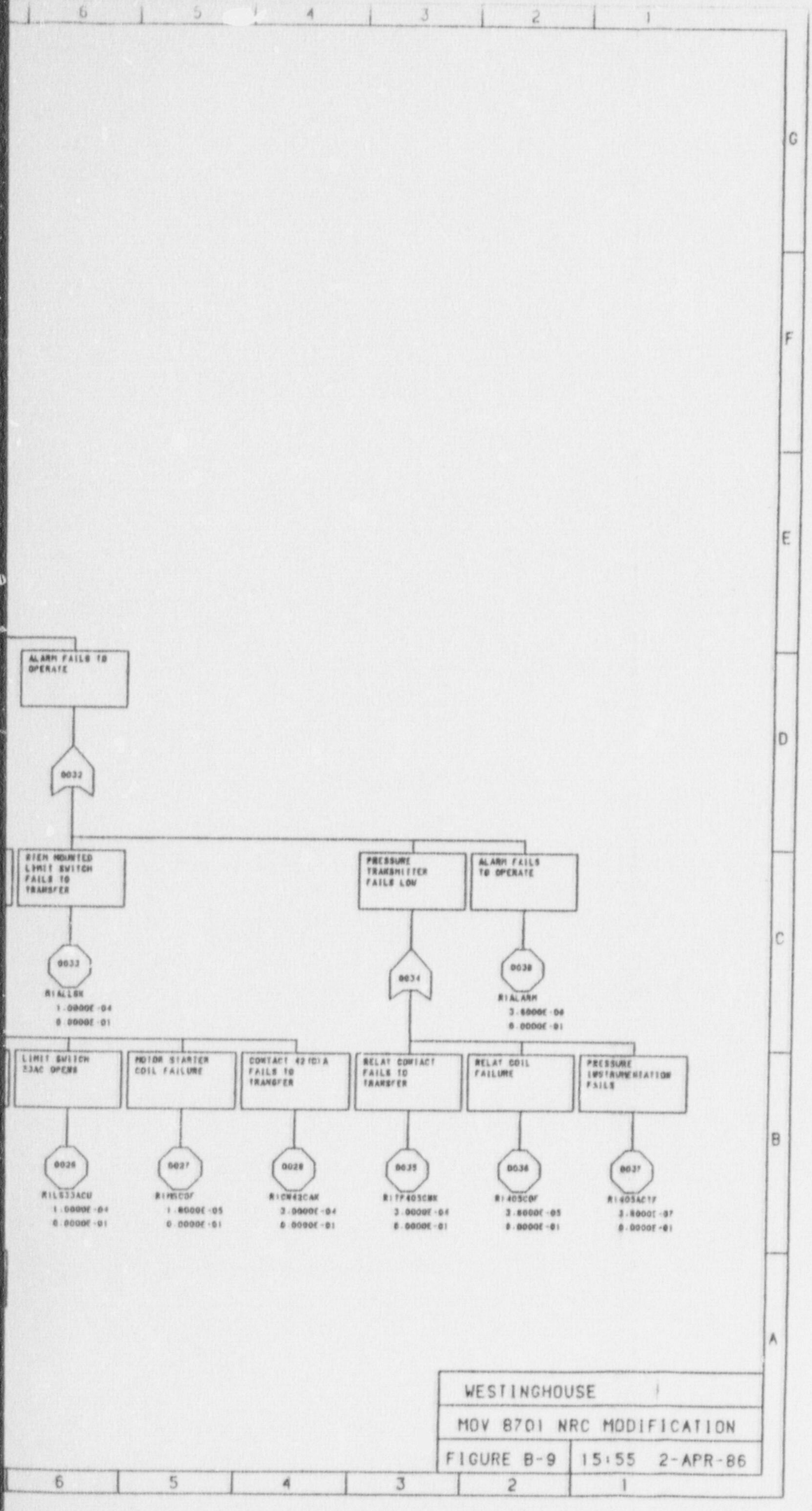


TI
APERTURE
CARD

Also Available On
Aperture Card

8708110183-11

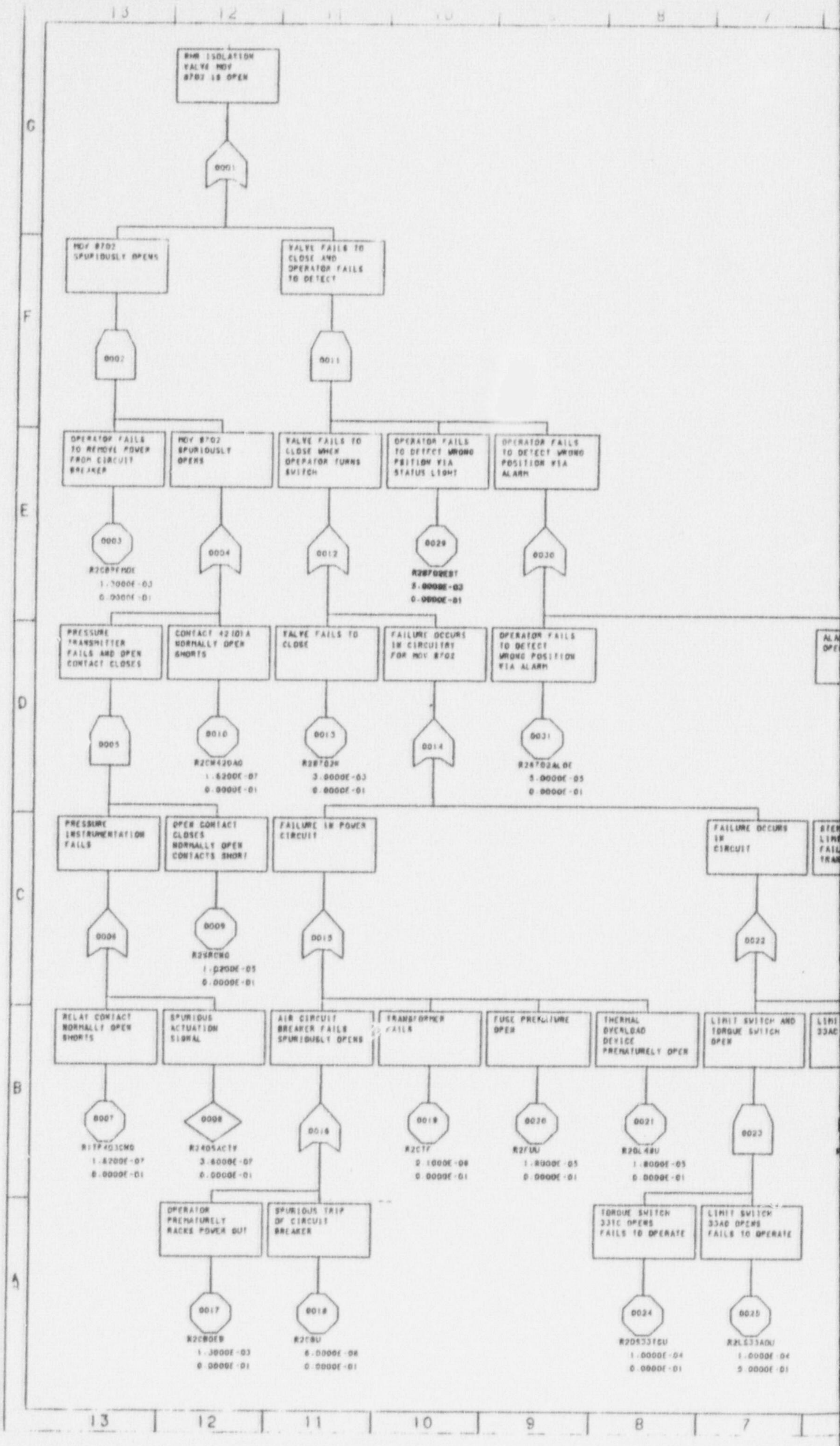

RHR ISOLATION VALVE MOV 8701 IS OPEN
0001
MOV 8701 SPURIOUSLY OPENS
VALVE FAILS TO CLOSE AND OPERATOR FAILS TO DETECT
0002
0011
OPERATOR FAILS TO REMOVE POWER FROM CS
MOV 8701 SPURIOUSLY OPENS
VALVE FAILS TO CLOSE WHEN OPERATOR TURNS SWITCH
OPERATOR FAILS TO DETECT WRONG POSITION VIA STATUS LIGHT
OPERATOR FAILS TO DETECT WRONG POSITION VIA ALARM
0003 R1CBREMOT 1.3000E-03 0.0000E-01
0004
0012
0029 R18701EST 5.0000E-03 0.0000E-01
0030
PRESS AND TEMP TRANSMITTER FAILS AND OPEN CONTACT CLOSES
CONTACT 42(03)A NORMALLY OPEN SHORTS
VALVE FAILS TO CLOSE
FAILURE OCCURS IN CIRCUITRY FOR MOV 8701
OPERATOR FAILS TO DETECT WRONG POSITION VIA ALARM
0005
0010 R1CR420A0 1.8200E-07 0.0000E-01
0013 R18701K 3.0000E-03 0.0000E-01
0014
0031 R18701ALOE 5.0000E-05 0.0000E-01
PRESSURE-TEMPERATURE INSTRUMENTATION FAIL
OPEN CONTACT CLOSES NORMALLY OPEN CONTACTS SHORT
FAILURE IN POWER CIRCUIT
FAILURE OCCURS IN CIRCUIT
0006
0009 R1SRCMO 1.0200E-05 0.0000E-01
0015
0022
RELAY CONTACT NORMALLY OPEN SHORTS
SPURIOUS ACTUATION SIGNAL
AIR CIRCUIT BREAKER FAILS SPURIOUSLY OPENS
TRANSFORMER FAILS
FUSE PREMATURE OPEN
THERMAL OVERLOAD DEVICE PREMATURELY OPEN
LIMIT SWITCH AND TORQUE SWITCH OPEN
0007 R1TP405CMO 1.5200E-07 0.0000E-01
0008 R1405ACTY 7.2000E-07 5.0000E-01
0016
0019 R1CTF 3.1000E-06 0.0000E-01
0020 R1FUU 1.8000E-05 0.0000E-01
0021 R1OL49U 1.8000E-05 0.0000E-01
0023
OPERATOR PREMATURELY RACKS POWER OUT
SPURIOUS TRIP OF CIRCUIT BREAKER
TORQUE SWITCH 33TC OPENS FAILS TO OPERATE
LIMIT SWITCH 33AO OPENS FAILS TO OPERATE
0017 R1CBOES 1.3000E-03 0.0000E-01
0018 R1CBU 6.0000E-08 0.0000E-01
0024 R1OS33TCU 1.0000E-04 0.0000E-01
0025 R1LS33AOU 1.0000E-04 0.0000E-01
13 12 11 10 9 8 7
G F E D C B A



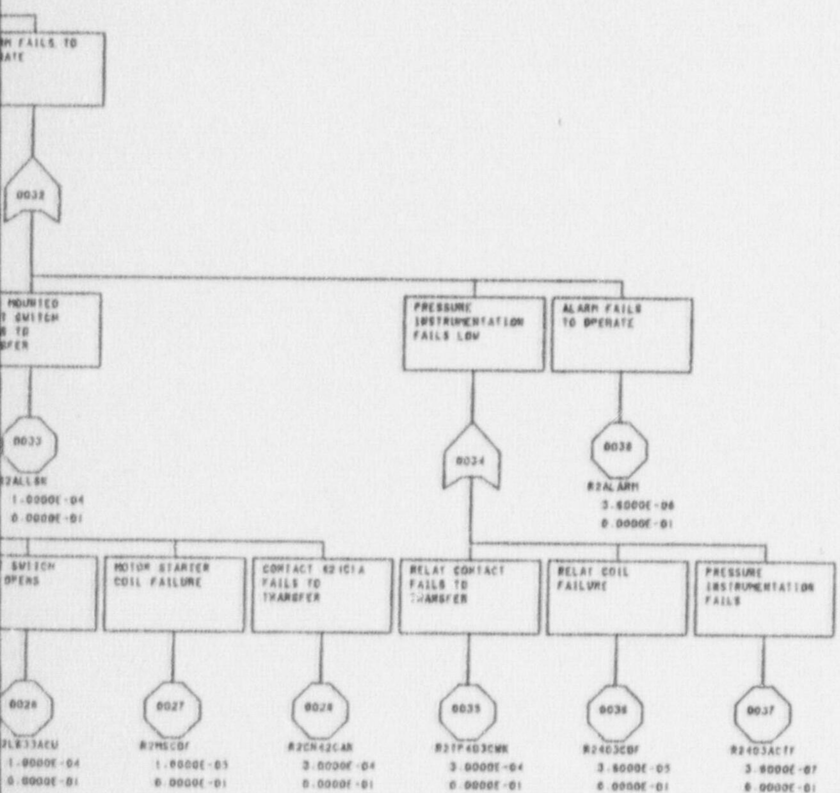
TI
APERTURE
CARD

Also Available On
Aperture Card

8708110183-12



RHR ISOLATION VALVE MOV 8702 IS OPEN
0001
MOV 8702 SPURIOUSLY OPENS
VALVE FAILS TO CLOSE AND OPERATOR FAILS TO DETECT
0002
0011
OPERATOR FAILS TO REMOVE POWER FROM CIRCUIT BREAKER
MOV 8702 SPURIOUSLY OPENS
VALVE FAILS TO CLOSE WHEN OPERATOR TURNS SWITCH
OPERATOR FAILS TO DETECT WRONG PSITION VIA STATUS LIGHT
OPERATOR FAILS TO DETECT WRONG POSITION VIA ALARM
0003
0004
0012
0029
0030
1.2000E-03
0.0000E-01
3.0000E-03
0.0000E-01
PRESSURE TRANSMITTER FAILS AND OPEN CONTACT CLOSES
CONTACT 42101A NORMALLY OPEN SHORTS
VALVE FAILS TO CLOSE
FAILURE OCCURS IN CIRCUITRY FOR MOV 8702
OPERATOR FAILS TO DETECT WRONG POSITION VIA ALARM
0005
0010
0013
0014
0031
1.6200E-07
0.0000E-01
3.0000E-03
0.0000E-01
5.0000E-05
0.0000E-01
PRESSURE INSTRUMENTATION FAILS
OPEN CONTACT CLOSES NORMALLY OPEN CONTACTS SHORT
FAILURE IN POWER CIRCUIT
FAILURE OCCURS IN CIRCUIT
0006
0009
0015
0022
1.0200E-05
0.0000E-01
RELAY CONTACT NORMALLY OPEN SHORTS
SPURIOUS ACTUATION SIGNAL
AIR CIRCUIT BREAKER FAILS SPURIOUSLY OPENS
TRANSFORMER FAILS
FUSE PREMATURE OPEN
THERMAL OVERLOAD DEVICE PREMATURELY OPEN
LIMIT SWITCH AND TORQUE SWITCH OPEN
0007
0008
0016
0019
0020
0021
0023
1.6200E-07
0.0000E-01
3.6000E-07
0.0000E-01
2.1000E-08
0.0000E-01
1.8000E-05
0.0000E-01
1.8000E-05
0.0000E-01
OPERATOR PREMATURELY RACKS POWER OUT
SPURIOUS TRIP OF CIRCUIT BREAKER
TORQUE SWITCH 33TC OPENS FAILS TO OPERATE
LIMIT SWITCH 33AO OPENS FAILS TO OPERATE
0017
0018
0024
0025
1.3000E-03
0.0000E-01
6.0000E-08
0.0000E-01
1.0000E-04
0.0000E-01
1.0000E-04
5.0000E-01



WESTINGHOUSE

MOV 8702 NRC MODIFICATION

FIGURE B-10 | 15:56 2-APR-86

TI APERTURE CARD

Also Available On Aperture Card

8708110183-13

APPENDIX C

RESIDUAL HEAT REMOVAL SYSTEM
(RHRS)

AVAILABILITY ANALYSIS

APPENDIX C

RHRS AVAILABILITY ANALYSIS

The residual heat removal system shown in Figure 4.1 was analyzed to determine the unavailability of the system to remove decay heat. 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).

C.1 Fault Tree Development

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 guidelines are described and the system components affected by the guidelines is discussed.

Random Fault Postulation and Consideration

Guideline a. The "local faults of piping" in a fluid system segment are not to be 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. Pipe faults such as pipe plugging, orifice plugging and plugging from chemical crystallization due to loss of pipe heat tracing system are to be considered as credible faults.

AFFECTED COMPONENTS: Piping faults will not be considered.

Guideline b. Random mechanical failure of locally locked open manual valves are not to be 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 will be 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.

AFFECTED COMPONENTS: Valves 8728A, 8728B, 8720A and 8720B are sealed open and thus closure of these valves is not considered a credible fault.

Guideline c. Normally open manual, air and motor-operated valves that are not required to change state during operation will be 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 will be considered as a credible event if applicable (see treatment of test and maintenance faults to follow).

AFFECTED COMPONENTS: MOV's 8809A, 8809B, 8700A, 8700B, 8716A and 8716B are normally open valves that do not change state during RHR operation. Spurious closure of these valves during long term cooling with be considered.

Guideline d. Potential flow diversion paths of fluid system that are isolated from the main flow path by one or more locally locked closed valves will not be considered as faults of the system.

AFFECTED COMPONENTS: Manual Valve 8741 is a normally locked closed valve on the return line to the refueling water storage tank and thus is not a credible event.

Guideline e. Potential flow diversion paths isolated from the main flow path by normally closed manual, air, and motor-operated, and check valves will not be treated as faults of the system. However, valve misposition prior to operation due to human error and/or spurious control signal will be considered a system fault, if credible.

AFFECTED COMPONENTS: Motor-operated valves 8804A and 8804B are normally closed valves in the lines loading from the discharge side of the RHR heat exchanger to the suction side of the centrifugal charging pumps and safety injection pumps respectively. Motor operated valves 9003A and 9003B are normally closed valves in the lines from the RHR heat exchanger to the containment spray system. These valves are not considered.

Guideline f. Check valves failing closed to flow in the forward direction and failing open to flow in the reverse direction will be 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 need not be included in fault tree development since their combined probability of failure to isolate flow would be of low probability relative to other system faults.

AFFECTED COMPONENTS: The check valves on the cold leg injection lines are two check valves in series and are not considered to fail open in the reverse direction.

Guideline g. Tank failures are to be included in fault tree development, but failure of heat exchangers (coolers) to transfer heat due to plugging of the tube side and leakage (primary to secondary) are not. An exception is made for the case of heat exchangers plugging when the tube side flow of coolant transfer medium is untreated. Plugging is to be considered as a credible event for such cases if the coolant medium is untreated.

AFFECTED COMPONENTS: Failure of the heat exchangers due to plugging or leakage is not considered a credible fault.

C.2 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 warmup 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 are required for 72 hours. (Note: some plants can operate with only one train during this phase but the cooldown time is increased). 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 fault trees developed for these scenarios are shown in Figures C-1 to C-3. Figure C-1 shows the fault tree for the startup of the RHR system. The fault tree in Figure C-2 depicts the initial phase of cooldown in which both trains of RHR are required. The long term cooling fault tree is shown in Figure C-3 (only one train of RHR is required).

Figure C-4 to C-8 show the detailed fault trees for motor-operated isolation valves 8701 and 8702. These trees are developed using the present interlock configuration and the two modification configurations. The unavailabilities calculated from these trees are input into the cooling and startup trees to calculate the system unavailability.

Assumptions

The assumptions used to develop the fault trees are presented below.

1. Injection into two cold legs by two pump trains is required for success for the startup and short term cooling scenarios. Injection into two cold legs by one pump train is required for long term cooling.

2. The startup fault tree was derived using the operating procedures OP B-2:V.

3. The initial phases of startup and initial cooldown fault tree require two trains of operation. Therefore, no testing or maintenance operations are assumed to occur during these phases.

4. In the long term cooling fault tree, test and maintenance can occur. Therefore, spurious closure of valves and operator error in mispositioning of valves is considered credible.

5. During the warmup period, it is assumed that pump No. 1 is started first and must run for 2 hours. Pump No. 2 is started after 1 hour of warmup and must run for 1 hour.

6. For long term cooling, it is assumed that pump No. 1 is operating and pump No. 2 is on standby and thus must start and run.

7. All electrical power (AC and DC) is assumed to be available.

C.2 Data

Table C.2-1 shows the basic event probabilities used to calculate the unavailability of the RHR system. The formula used to calculate the basic event probability is:

$$Q = \lambda \ Tm$$

where

Q = basic event probability

λ = failure rate for component

Tm = total defined mission time in which the component must operate

The unavailability of RHR pump 2 due to test is based on the technical specifications which allow for a two hour unavailability limit. Maintenance unavailabilities were extracted from the Zion PSS for standby systems tested monthly or quarterly assuming a 72 hour component inoperability time limit.

The human error probabilities (HEPs) are calculated for each operator action required during RHR operation and are presented in Table C.2-2. The HEPs are extracted from Swain, et.al.

C.3 Results

The results from the quantification of the fault trees is shown in Table C.3-1. The dominant cutsets for each case shown in Table C.3-2.

TABLE C.2-1

COMPONENT RANDOM FAILURE UNAVAILABILITIES

SYSTEM: RESIDUAL HEAT REMOVAL

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R1CV8948AD	Failure to Open	1E-4/d	1 demand	-	1E-4	
R1CV8818AD	Failure to Open	1E-4/d	1 demand	-	1E-4	
R1CV8948BD	Failure to Open	1E-4/d	1 demand	-	1E-4	
R1CV8818BD	Failure to Open	1E-4/d	1 demand	-	1E-4	
R2CV8948CD	Failure to Open	1E-4/d	1 demand	-	1E-4	
R2CV8818CD	Failure to Open	1E/4/d	1 demand	-	1E-4	
R2CV8948DD	Failure to Open	1E/4/d	1 demand	-	1E-4	
R2CV8818DD	Failure to Open	1E-4/d	1 demand	-	1E-4	
R2CV8730BD	Failure to Open	1E-4/d	1 demand	-	1E-4	
R1CV8730AD	Failure to Open	1E-4/d	1 demand	-	1E-4	
R1PM1A	Failure to Start	3E-3/d	1 demand	-	1E-4	
R2PM2A	Failure to Start	3E-3/d	1 demand	-	1E-4	
R1PM1XS	Failure to Run	3E-5/hr	-	72 hours	2.16E-3	for short term
R2PM2XS	Failure to Run	3E-5/hr	-	72 hours	2.16E-3	for short term
R1PMIX	Failure to Run	3E-5/hr	-	2 hrs	6E-5	for startup
R1PMIX	Failure to Run	3E-5/hr	-	1 hr	3E-5	for startup

0207x:6-040886

TABLE C.2-1 (Cont)

COMPONENT RANDOM FAILURE UNAVAILABILITIES

SYSTEM: RESIDUAL HEAT REMOVAL

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R1AV638D	Failure to Open	3E-3/d	1 demand	-	3E-3	
R2AV6337D	Failure to Open	3E-3/d	1 demand	-	3E-3	
R2HXCCW364	Failure to Operate	3E-3/d	1 demand	-	3E-3	
R1HXCCW365	Failure to Operate	3E-3/d	1 demand	-	3E-3	
R1PMIX	Failure to Run	3E-5/hr	-	1008 hrs	3.02E-2	for long term
R2PM2X	Failure to Run	3E-5/hr	-	1008 hrs	3.02E-2	for long term
R1MV641AD	Failure to Open	3E-3/d	1 demand	-	3E-3	
R2MV641BD	Failure to Open	3E-3/d	1 demand	-	3E-3	
R1AV670D	Failure to Open	3E-3/d	1 demand	-	3E-3	
R2AV670D	Failure to Open	3E-3/d	1 demand	-	3E-3	
R1XV8726AD	Failure to Operate	1E-4/d	1 demand	-	1E-4	
R2AV638K	Failure to Close	3E-3/d	1 demand	-	3E-3	
R1AV638K	Failure to Close	3E-3/d	1 demand	-	3E-3	
R2XV8726BD	Failure to Operate	1E-4/d	1 demand	-	1E-4	
R1AV670K	Failure to Close	3E-3/d	1 demand	-	3E-3	
R1MV8809AV	Spuriously Closes	1E-7/hr	-	1008 hrs	1.01E-4	

0207x:6-040886

TABLE C.2-1 (Cont)

COMPONENT RANDOM FAILURE UNAVAILABILITIES

SYSTEM: RESIDUAL HEAT REMOVAL

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R2MV8809BV	Spuriously Closes	1E-7/hr	-	1008 hrs	1.01E-4	
R1MV8716Av	Spuriously Closes	1E-7/hr	-	1008 hrs	1.01E-4	
R1MV8716BV	Spuriously Closes	1E-7/hr	-	1008 hrs	1.01E-4	
R1MV8700AV	Spuriously Closes	1E-7/hr	-	1008 hrs	1.01E-4	
R2MV8700BV	Spuriously Closes	1E-7/hr	-	1008 hrs	1.01E-4	

TABLE C.2-1 (Cont)

COMPONENT RANDOM FAILURE UNAVAILABILITIES

SYSTEM: RESIDUAL HEAT REMOVAL - MOV 8701 - FAIL TO OPEN SPURIOUSLY CLOSE

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R1ACBU	Spuriously Opens	1.0E-8/hr	-	2 hrs	2.00-8	
R1CTF	Fails	3.5E-7/hr	-	2 hrs	7.0E-7	
R1FUU	Premature Open	3.0E-6/hr	-	2 hrs	6E-6	
R1OL49U	Spuriously Opens	3.0E-6/hr	-	2 hrs	6E-6	Rate for a fuse
R1LS33BCK	Fails to Transfer	1E-4/d	1 demand	-	1E-4	
R1QS33TOK	Fails to Transfer	1E-4/d	1 demand	-	1E-4	
R1LS33BOK	Fails to Transfer	1E-4/d	1 demand	-	1E-4	
R1SRCNK	Fails to Close	3E-5/d	1 demand	-	3E-5	
R1MSCOF	Coil Failure	3E-6/hr	-	2 hrs	6E-6	
R1CN420AK	Fail to Transfer	3E-4/d	1 demand	-	3E-4	
R1TP405AXH	Fails High	1.3E-7/hr	-	2 hrs	2.6E-7	
R1TT454H	Fails High	1.5E-7	-	2 hrs	3.0E-7	
R1MV8701D	Fail to Open	3E-3/d	1 demand		3E-3	
R1MV8701V	Fails to Remain Open	1E-7/hr	72 hrs	-	7.2E-6	
			1008 hrs		7.01E-4	
R1TP405BXV	Fails High	1.3E-7/hr	72 hrs	-	9.36E-6	
			1008 hrs		1.31E-4	

TABLE C.2-1 (Cont)

COMPONENT RANDOM FAILURE UNAVAILABILITIES (continued)

SYSTEM: RESIDUAL HEAT REMOVAL - MOV 8701 - FAIL TO OPEN SPURIOUSLY CLOSE

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R1SRCNQ	Shorts	2.7E-8/hr	72 hrs	-	1.94E-6	
			1008 hrs		2.72E-5	
R1CN42ACQ	Shorts	2.7E-8/hr	72 hrs	-	1.94E-6	
			1008 hrs		2.72E-5	
R1TT454HV	Fails High	1.5E-7/hr	72 hrs	-	1.08E-5	
			1008 hrs		1.51E-4	

TABLE C.2-1 (Cont)

COMPONENT RANDOM FAILURE UNAVAILABILITIES

SYSTEM: RESIDUAL HEAT REMOVAL - MOV 8701 - FAIL TO OPEN SPURIOUSLY CLOSE

Fault Tree Identifier	Failure Mode	Failure Rate	Fault Detection Interval	Mission Time	Fault Event Probability	Analysis Comments
R2ACBU	Spuriously Opens	1.0E-8/hr		2 hrs	2.0E-8	
R2CTF	Fails	3.5E-7/hr		2 hrs	7.0E-7	
R2FUU	Premature Open	3.0E-6/hr	-	2 hrs	6.0E-6	
R2OL49U	Spuriously Opens	3.0E-6/hr	-	2 hrs	6.0E-6	Rate for a fuse
R2LS33BCK	Fails to Transfer	1E-4/d	1 demand	-	1E-4	
R2QS33TOK	Fails to Transfer	1E-4/d	1 demand	-	1E-4	
R2LS33BOK	Fails to Transfer	1E-4/d	1 demand	-	1E-4	
R2SRCNK	Fails to Close	3E-5/d	1 demand	-	3E-5	
R2MSCOF	Coil Failure	3E-6/hr	-	2 hrs	60E-6	
R2CN420AK	Fail to Transfer	3E-4/d	1 demand	-	3E-4	
R2TP405AXH	Fails High	1.3E-7/hr	-	2 hrs	2.6E-7	
R2MV8702D	Fail to Open	3E-3/d	1 demand		3E-3	
R2MV8702V	Fails to Remain Open	1E-7/hr	72 hrs	-	7.2E-6	
			1008 hrs		7.01E-4	
R2TP405BXV	Fails High	1.3E-7/hr	72 hrs	-	9.36E-6	
			1008 hrs		1.31E-4	
R2SRCNQ	Shorts	2.7E-8/hr	72 hrs	-	1.94E-6	
			1008 hrs		2.72E-5	
R2CN42ACQ	Shorts	2.7E-8/hr	72 hrs	-	1.94E-6	
			1008 hrs		2.72E-5	

0207x:6-040886

TABLE C.2-1 (Cont)

COMPONENT MAINTENANCE UNAVAILABILITIES

SYSTEM: RESIDUAL HEAT REMOVAL

Fault Tree Identifier	Description	Mean Time to Repair	Mean Maintenance Acts Per Hour	Unavailability Due to Maintenance	Analysis Comments
R2PM2MAIN	Pump No. 2	18.7 hours/event	8.42E-Events/hour	1.57E-3	From Zion PSS Prior Distribution Standby Systems tested monthly or quarterly 72 hour component inoperability time limit

TABLE C.2-1 (Cont)

COMPONENT UNAVAILABILITIES DUE TO TEST

SYSTEM: RESIDUAL HEAT REMOVAL

Fault Tree Identifier	Average Duration of Test	Interval Between Tests	Unavailability From Test Outage	Analysis Comments
R2PM2T3T	2 hours	92 days	9.06E-4	2 hour test duration per Tech Spec 3.4.1.4.1 92 day (Quarterly) functional test for pumps

TABLE C.2-2

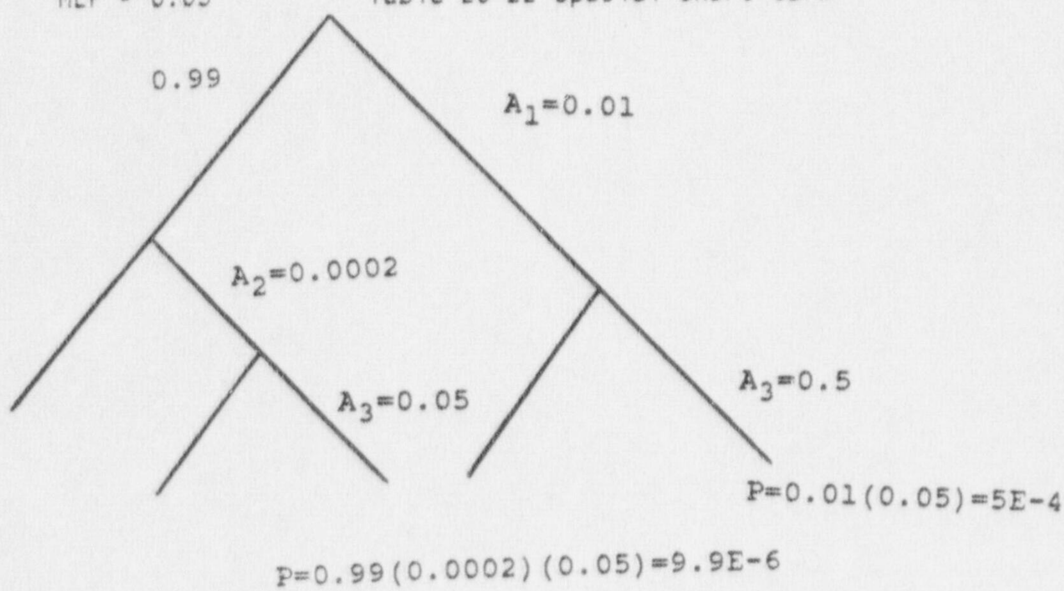
HUMAN ERROR CALCULATIONS

1. Operator fails to close air operated valve 638 or 637 or 670.

1. Omission error - operator fails to close MOV
   HEP = 0.01 Table 20-7 no checkoff provisions, long list, > 10 items

5. Commission error - turn switch in wrong direction
   HEP = $\frac{0.001}{5}$ = 0.0002 Table 20-12

3. Recovery error - checker fails to detect errors by others
   HEP = 0.05 Table 20-22 special short-term



P_{OE} = 9.9E-6 + 5E-4
= 5.10E-4

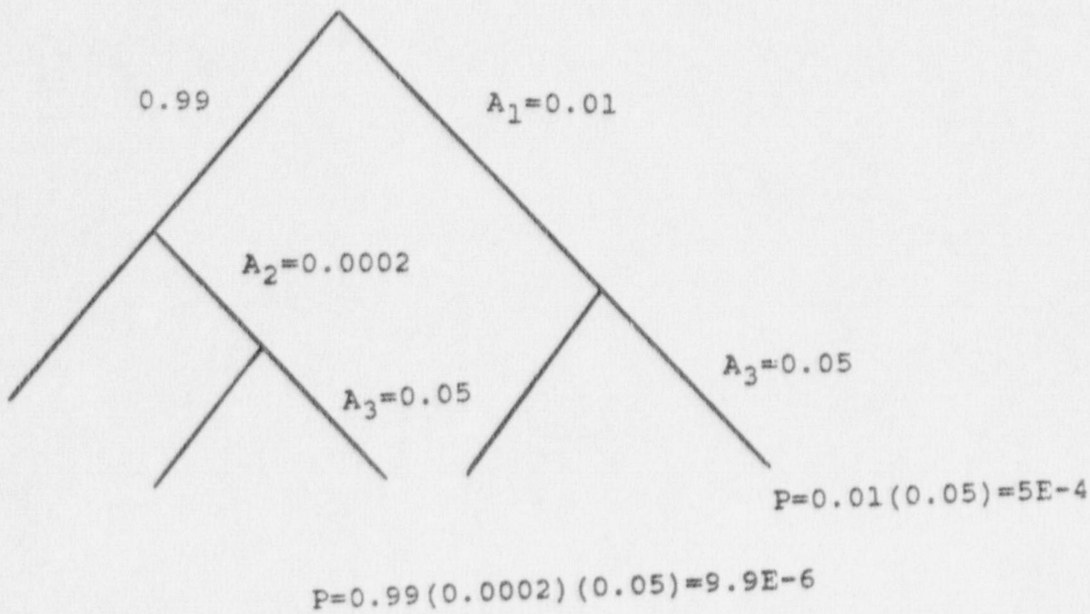
Fault Tree Identifiers: R2AV637OE R1AV638OE R1AV670KOE

TABLE C.2-2 (Cont)

HUMAN ERROR CALCULATIONS

2. Operator fails to open air operated valve 637, 638, 670, CCW valves

1. Omission error	-	operator fails to open MOV
HEP = 0.01		Table 20-7 no checkoff provisions, long list, > 10 items
2. Commission error	-	turn switch in wrong direction
HEP = 0.001/5 = 0.0002		Table 20-12
3. Recovery error	-	checker fails to detect errors by others
HEP = 0.05		Table 20-22 special short term



P_{OE} = 9.9E-6 + 5E-4

= 5.10E-4

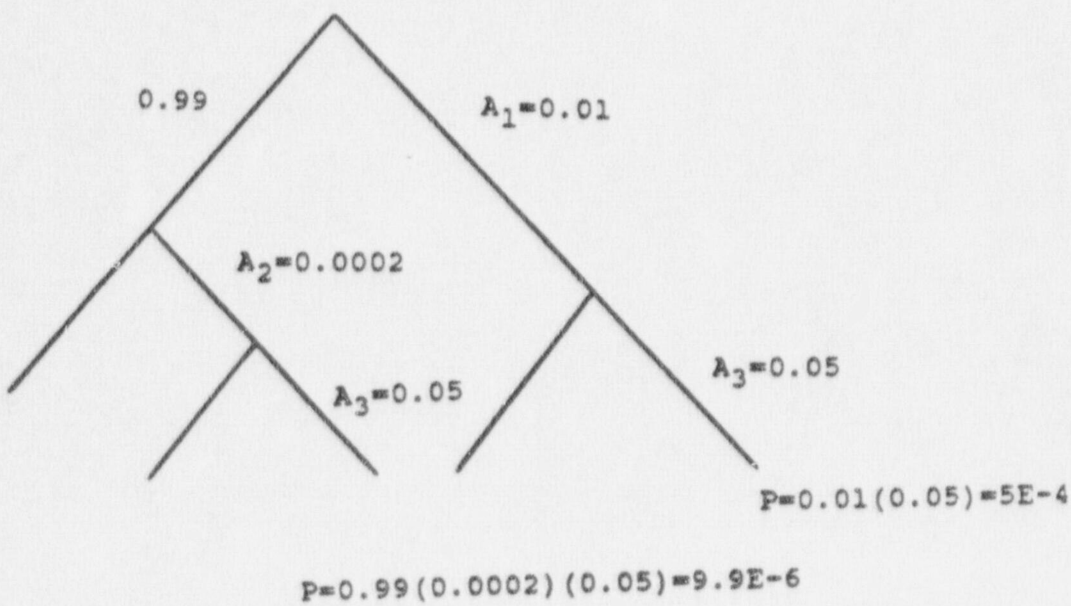
Fault Tree Identifiers:		
	R1AV638DOE	R2AV637OOE
	R1AV670OE	R2ASV670OE
	R2HXCCWOE	R1HXCCWOE

TABLE C.2-2 (Cont)

HUMAN ERROR CALCULATIONS

2. Operator fails to open air operated valve 637, 638, 670, CCW valves

1.	Omission error HEP = 0.01	-	operator fails to open MOV Table 20-7 no checkoff provisions, long list, > 10 items
2.	Commission error HEP = 0.001/5 = 0.0002	-	turn switch in wrong direction Table 20-12
3.	Recovery error HEP = 0.05	-	checker fails to detect errors by others Table 20-22 special short term



P_{OE} = 9.9E-6 + 5E-4

= 5.10E-4

Fault Tree Identifiers:		
	R1AV638DOE	R2AV637OE
	R1AV670OE	R2ASV670OE
	R2HXCCWOE	R1HXCCWOE

TABLE C.2-2
HUMAN ERROR CALCULATIONS

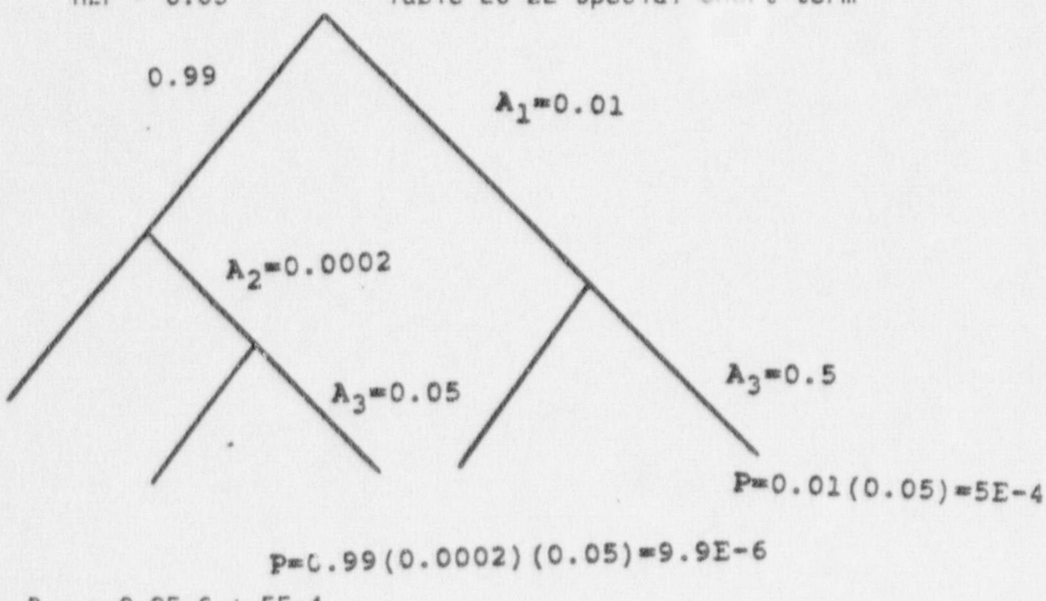
1. Operator fails to close air operated valve 638 or 637 or 670.

   1. Omission error - operator fails to close MOV
      HEP = 0.01 Table 20-7 no checkoff provisions, long list, > 10 items

   5. Commission error - turn switch in wrong direction

      $$HEP = \frac{0.001}{5} = 0.0002$$ Table 20-12

   3. Recovery error - checker fails to detect errors by others
      HEP = 0.05 Table 20-22 special short-term

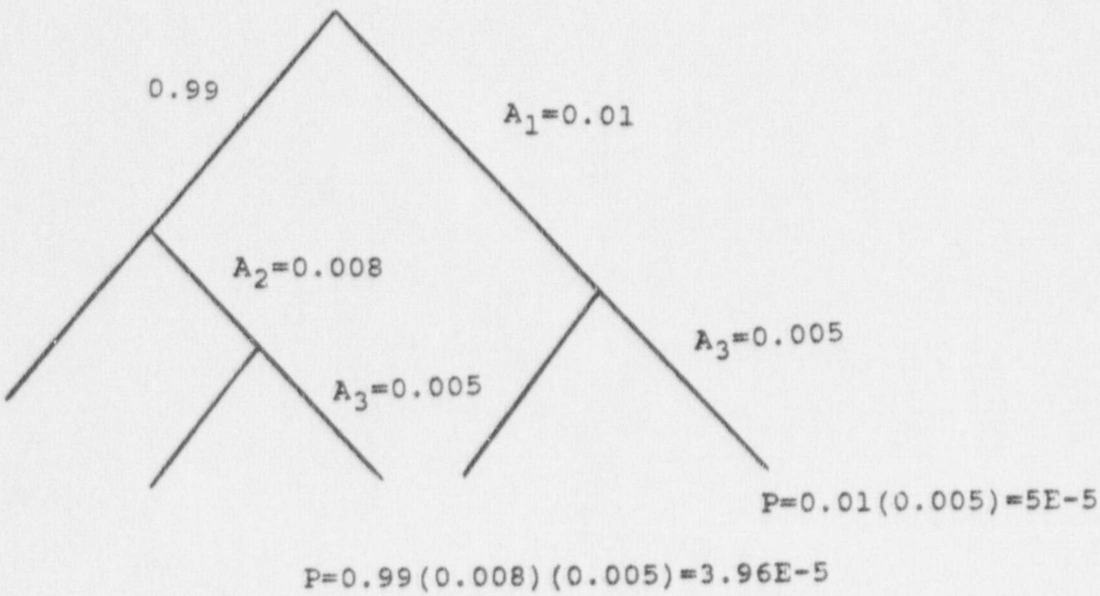


P_{OE} = 9.9E-6 + 5E-4
= 5.10E-4

Fault Tree Identifiers: R2AV637OE R1AV638OE R1AV670KOE

3. Operator fails to open manual valve 8726A, 8726B

1. Omission error	-	operator fails to open XV
HEP = 0.01		Table 20-7 no checkoff provisions long list, > 10 items
2. Commission error	-	making an error of selection
HEP = 0.008		Table 20-13 ambiguously labeled part of a group of valves
3. Recovery error	-	detecting locally operated valves
HEP = 0.005		Table 20-14 rising stem only



P_{OE} = 3.96E-5 + 5E-5
= 8.96E-5

Fault Tree Identifiers: R1XV8726A0 R2XV8726B0

TABLE C.2-2 (Cont)

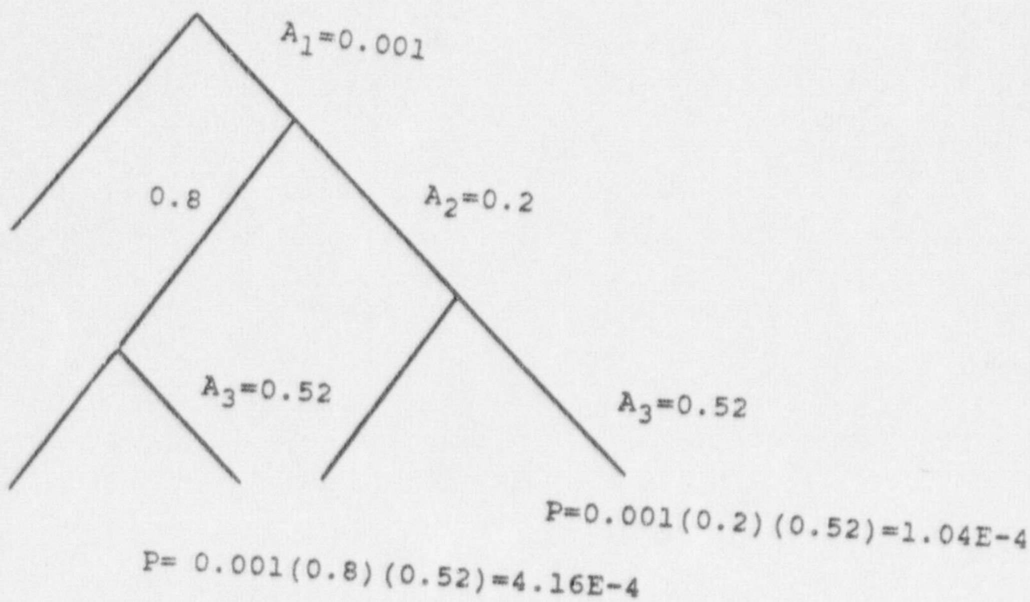
HUMAN ERROR CALCULATIONS

4. Operator inadvertently closes valve (motor-operated or air operated)

   1. Commission error - select wrong control
      HEP = 0.001 Table 20-12 well-delineated

   2. Recovery error - detect closed valve
      HEP = 0.2 Tabl- 20-22 routine tasks

   3. Recovery error - basic walk around detection
      HEP = 0.52 Table 20-27 daily walk around



P_{OE} = 4.16E-4 + 1.04E-4

= 5.2E-4

Fault Tree Identifiers: R1HCV638OE, R2HCV637OE

TABLE C.2-2 (Cont)

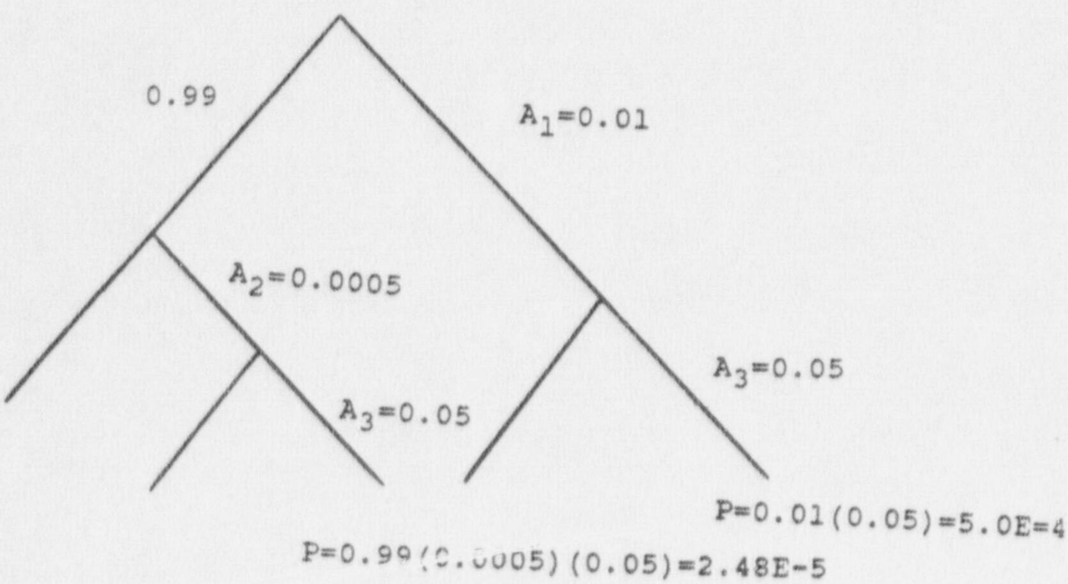
HUMAN ERROR CALCULATIONS

5. Operator fails to open MOV 8701 or 8702

   1. Omission error - operator fails to open MOV
      HEP = 0.01 Table 20-7 no checkoff provisions, long list > 10 items

   2. Commission error - turn switch in wrong direction
      HEP = 0.0005 Table 20-12

   3. Recovery error - checker fails to detect
      HEP = 0.05 Table 20-22 special short term



P_{OE} = 5E-4 + 2.48E-5
= 5.25E-4

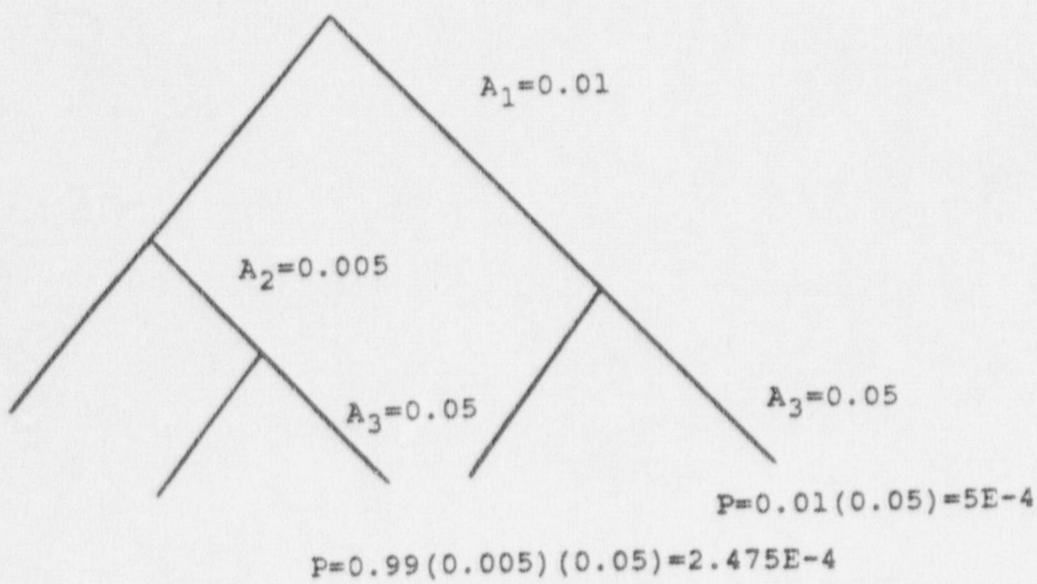
Fault Tree Identifiers: R1MV8701OE, R2MV8702OE

6. Operator fails to close breakers for MOV's 8701 or 8702

   1. Omission error - operator fails to close breakers
      HEP = 0.01 Table 20-7 no checkoff provisions, long list, > 10 items

   2. Commission error - select wrong circuit breaker
      HEP = 0.005 Table 20-12 densely grouped

   3. Recovery error - checker fails to detect error
      HEP = 0.05 Table 20-22



P_{OE} = 5E-4 + 2.47E-4
= 7.47E-4

Fault Tree Identifiers: R1ACBVOE, R2ACBVOE

TABLE C.3-1

RHRS UNAVAILABILITIES

	With Present Configuration	With Modification	With NRC Modification
MOV 8701 fails to open	5.02E-3	5.02E-3	5.02E-3
MOV 8702 fails to open	5.02E-3	5.02E-3	5.02E-3
MOV 8701 or 8702 Spuriously over T = 72 hours	6.64E-5	2.22E-5	2.22E-5
MOV 8701 or 8702 Spuriously Close over T = 1008 hours	9.29E-4	3.11E-4	3.11E-4
RHRS fails during warmup	2.07E-2	2.07E-2	2.07E-2
RHRS fails over short term	7.11E-5	2.69E-5	2.69E-5
RHRS fails over long term	2.01E-3	1.39E-3	1.39E-3
Total RHRS Unavailability over short term	2.08E-2	2.07E-2	2.07E-2
Total RHRS Unavailability over long term	2.28E-2	2.21E-2	2.21E-2

TABLE C.3-2

MOV 8701 Fails to Open

DOMINANT CONTRIBUTORS

Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 3.00E-3	59.8	R1MV8701D	Valve Mechanical Failure
2. 7.47E-4	14.9	R1ACBVDE	Operator Fails to Close Circuit Breaker
3. 5.25E-4	10.5	R1MV87010E	Operator Fails to Open MOV
4. 3.00E-4	6.0	R1CN420AK	Relay Contact Fails to Close
5. 3.00E-4	6.0	R1TP405CNK	Pressure Relay Contact Fails to Transfer
6. 1.00E-4	2.0	R1LS33BOK	Limit Switch Fails to Close
7. 3.00E-5	0.6	R1SRCNK	Rotary Switch Contact Fails to Close

MEAN UNAVAILABILITY = 5.02E-3

0058v:1D/112486

TABLE C.3-2 (Cont)

MOV 8702 Fails to Open

DOMINANT CONTRIBUTORS

Cutset Probability	Percent Contribution to Unavailability	Cutset	Description
1. 3.00E-3	59.8	R2MV8702D	Valve Mechanical Failure
2. 7.47E-4	14.9	R2ACBVDE	Operator Fails to Close Circuit Breaker
3. 5.25E-4	10.5	R2MV8702DE	Operator Fails to Open MOV
4. 3.00E-4	6.0	R2CN420AK	Relay Contact Fails to Close
5. 3.00E-4	6.0	R2TP403CNK	Pressure Relay Contact Fails to Transfer
6. 1.00E-4	2.0	R2LS33BOK	Limit Switch Fails to Close
7. 3.00E-5	0.6	R2SRCNK	Rotary Switch Contact Fails to Close

MEAN UNAVAILABILITY = 5.02E-3

0207x:6-050586

TABLE C.3-2 (Cont)

Present Configuration

MOV 8701 or 8702 Spuriously Close (T=72 hrs)

DOMINANT CONTRIBUTORS

Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 2.02E-5	30.4	R2403ACT	Pressure Transmitter 403 Actuation Fails
2. 2.02E-5	30.4	R1405ACT	Pressure Transmitter 405 Actuation Fails
3. 7.20E-6	10.8	R2MV8702V	Valve Spuriously Closes
4. 7.20E-6	10.8	R1MV8701V	Valve Spuriously Closes
5. 1.94E-6	2.9	R2CN42ACQ	Relay Contact 42AC Shorts in MOV 8702
6. 1.94E-6	2.9	R2SRCNQ	Rotary Switch Contact Shorts in MOV 8702
7. 1.94E.6	2.9	R1CN42ACQ	Relay Contact 42AC Shorts in MOV 8701
8. 1.94E-6	2.9	R1SRCNQ	Rotary Switch Contact Shorts in MOV 8702

MEAN UNAVAILABILITY = 6.64E-5

0058v:1D/112486

TABLE C.3-2 (Cont)

Present Configuration

MOV 8701 or 8702 Spuriously Closes (T=1008 hrs)

DOMINANT CONTRIBUTORS

Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 2.82E-4	30.4	R2403ACT	Pressure Transmitter 403 Actuation Fails
2. 2.82E-4	30.4	R1405ACT	Pressure Transmitter 405 Actuation Fails
3. 1.01E-4	10.9	R2MV8702V	Valve Spuriously Closes
4. 1.01E-4	10.9	R1MV8701V	Valve Spuriously Closes
5. 2.72E-5	2.9	R2CN42ACQ	Relay Contact 42AC Shorts in MOV 8702
6. 2.72E-5	2.9	R2SRCNQ	Rotary Switch Contact Shorts in MOV 8702
7. 2.72E.5	2.9	R1CN42ACQ	Relay Contact 42AC Shorts in MOV 8701
8. 2.72E-5	2.9	R1SRCNQ	Rotary Switch Contact Shorts in MOV 8701

MEAN PROBABILITY = 9.29E-4

0207x:6-050586

TABLE C.3-2 (Cont)

NRC Modification and Modification

MOV 8701 or 8702 Spuriously Close (T=72 hrs)

DOMINANT CONTRIBUTORS

Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 7.20E-6	32.4	R2MV8702V	Valve Spuriously closes
2. 7.20E-6	32.4	R1MV8701V	Valve Spuriously Closes
3. 1.94E-6	8.7	R1SRCNQ	Rotary Switch Contact Shorts in MOV 8701
4. 1.94E-6	8.7	R2CN42ACQ	Relay Circuit 42AC Shorts in MOV 8702
5. 1.94E-6	8.7	R2SRCNQ	Rotary Switch Contact Shorts in MOV 8702
6. 1.94E-6	8.7	R1CN42ACQ	Relay Contact 42AC Shorts in MOV 8701

MEAN PROBABILITY = 2.22E-5

0207x:6-050588

TABLE C.3-2 (Cont)

NRC Modification and Modification

MOV 8701 or 8702 Spuriously Close (T=1008 hrs)

DOMINANT CONTRIBUTORS

	Cutset Probability	Contribution to Unavailability	Cutset	Description
1.	1.01E-4	32.5	R2MV8702V	Valve Spuriously closes
2.	1.01E-4	32.5	R1MV8701V	Valve Spuriously Closes
3.	2.72E-5	8.7	R1SRCNQ	Rotary Switch Contact Shorts in MOV 8701
4.	2.72E-5	[illegible].7	R2CN42ACQ	Relay Circuit 42AC Shorts in MOV 8702
5.	2.72E-5	8.7	R2SRCNQ	Rotary Switch Contact Shorts in MOV 8702
6.	2.72E-5	8.7	R1CN42ACQ	Relay Contact 42AC Shorts in MOV 8701

MEAN PROBABILITY = 3.11E-4

TABLE C.3-2 (Cont)

RHR Fails During Warmup

DOMINANT CONTRIBUTORS

Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 5.02E-3	24.2	R1MV8702	MOV 8702 Fails to Open
2. 5.02E-3	24.2	R1MV8701	MOV 8701 Fails to Open
3. 3.00E-3	14.5	R1AV670K	AV 670 Fails to Close
4. 3.00E-3	14.5	R2AV637D	AV 637 Fails to Open
5. 3.00E-3	14.5	R1AV638D	AV 638 Fails to Open
6. 5.10E-4	2.5	R1AV670KOE	Operator Fails to Close AV 670
7. 5.10E-4	2.5	R2AV637DOE	Operator Fails to Open AV 637
8. 5.10E-4	2.5	R1AV638DOE	Operator Fails to Open AV 638

MEAN PROBABILITY = 2.07E-2

TABLE C.3-2 (Cont)

Present Configuration — Short Term Cooling

MOV 8701 or 8702 Spuriously Close (T=72 hrs)

DOMINANT CONTRIBUTORS

Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 6.64E-5	93.4	R1MV1SOL	MOV 8701 or 8702 Spuriously Close
2. 4.67E-6	6.6	R1PMIXS R2PM2XS	RHR Pumps Fail to Continue Running

MEAN PROBABILITY = 7.11E-5

0058v:1D/112486

TABLE C.3-2 (Cont)

Modification and NRC Modification Short Term Cooling

DOMINANT CONTRIBUTORS

Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 2.22E-5	82.5	R1MV1SOL	MOV 8701 or 8702 Spuriously Close
2. 4.67E-6	17.4	R1PMIXS R2PM2XS	RHR Pumps Fail to Continue Running

MEAN PROBABILITY = 2.69E-5

TABLE C.3-2 (Cont)

Present Configuration Long Term Cooling

DOMINANT CONTRIBUTORS

Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 9.29E-4	46.2	R1MV2SOL	MOV 8701 or 8702 Spuriously Close
2. 9.12E-4	45.4	R1PM1X R2PM2X	RHR Pumps Fail to Continue Running
3. 9.06E-5	4.5	R1PM1X R2PM2A	Pump #1 Fails to Run and Pump #2 Fails to Start
4. 4.74E-5	2.4	R1PM1X R2PM2MAIN	Pump #1 Fails to Run and Pump #2 Unavailable Due to Maintenance
5. 2.74E-5	1.4	R1PM1X R2PM2TST	Pump #1 Fails to Run and Pump #2 Unavailability Due to Test
6. 3.05E-6	0.2	R1PM1X R2MV8700BV	Pump #1 Fails to Run and MOV 8700B Spuriously Closes
7. 3.05E-6	0.2	R1MV8700AV R2PM2X	Pump #2 Fails to Run and MOV 8700A Spuriously Closes
8. 3.02E-6	0.2	R1PM1X R2CV8730BD	Pump #1 Fails to Run and CV8730B Fails to Open

MEAN PROBABILITY = 2.01E-3

0207x:6-050586

TABLE C.3-2 (Cont)

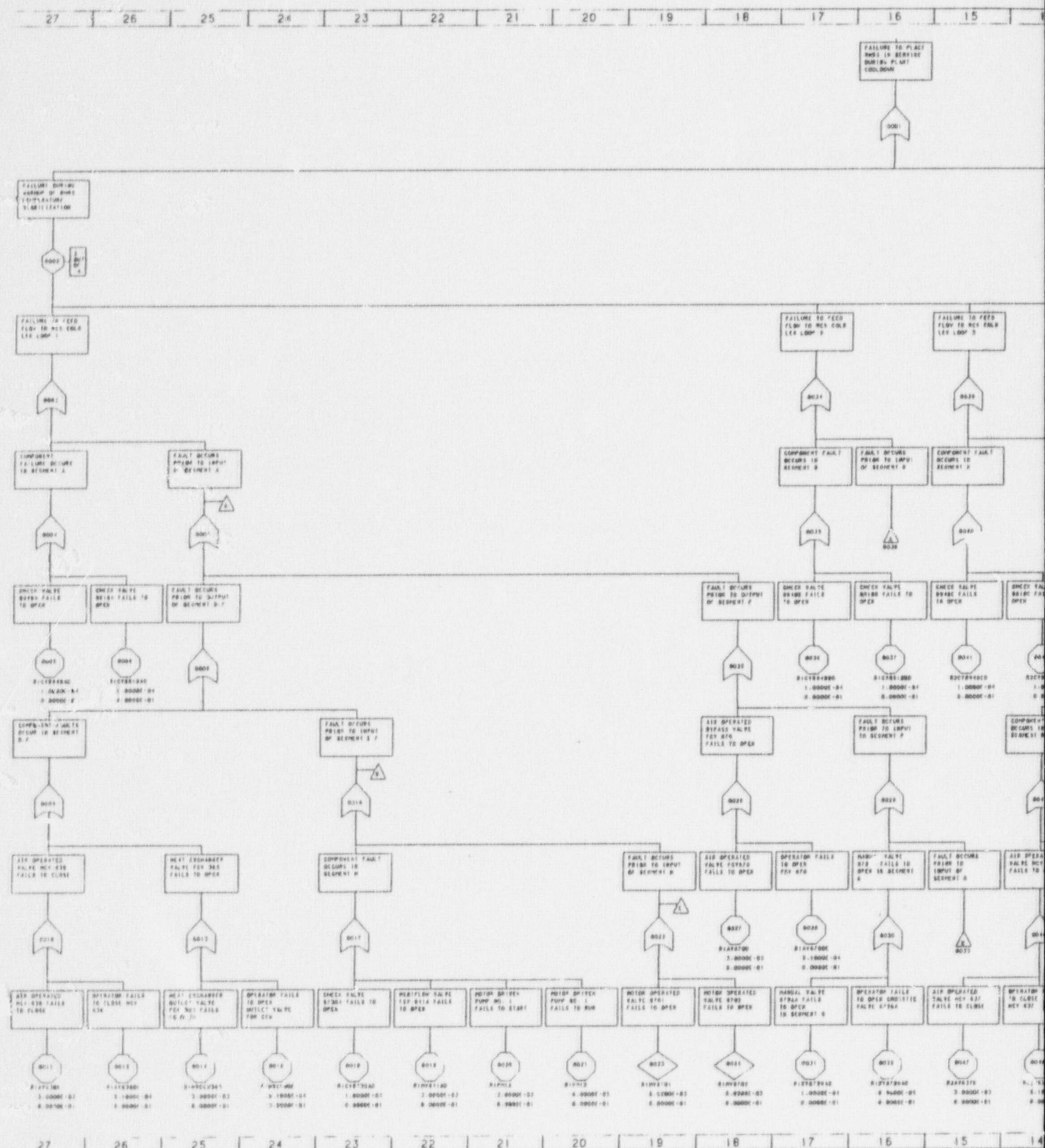
Modification and NRC Modification Long Term Cooling

DOMINANT CONTRIBUTORS

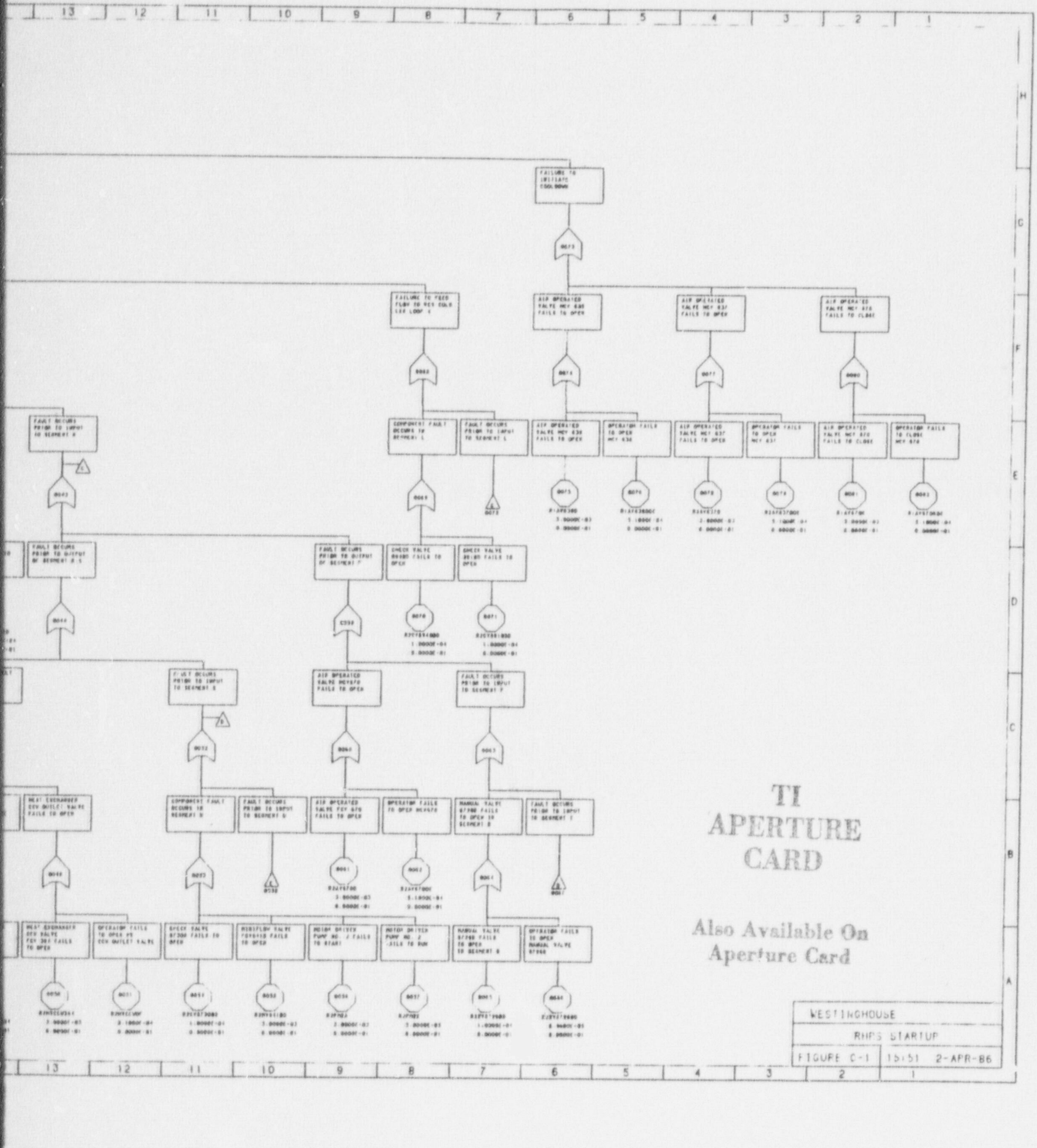
Cutset Probability	Contribution to Unavailability	Cutset	Description
1. 9.12E-4	65.6	R1PM1X R2PM2X	RHR Pumps Fails to Continue Running
2. 3.11E-4	22.4	R1MV1SOL	MOV 8701 or 8702 Spuriously Close
3. 9.06E-5	6.5	R1PM1X R2PM2A	RHR Pump #1 Fails to Run and Pump #2 Fails to Start
4. 4.74E-5	3.4	R1PM1X R2PM2MAIN	Pump #1 Fails to Run and Pump #2 Unavailable due to Maintenance
5. 2.74E-5	2.0	R1PM1X R2PM2TST	Pump #1 Fails to Run and PUmp #2 Unavailable Due to Test
6. 3.05E-6	0.2	R1PM1X R2MV8700BV	Pump #1 Fails to Run and MOV 8700B Spuriously Closes
7. 3.05E-6	0.2	R1MV8700AV R2PM2X	Pump #2 Fails to Run and MOV 8700A Spuriously Closes
8. 3.02E-6	0.2	R1PM1X R2CV8730BD	Pump #1 Fails to Run and CV 8730B Fail to Open

MEAN PROBABILITY = 1.39E-3

0207x:6-050586



27
26
25
24
23
22
21
20
19
18
17
16
15

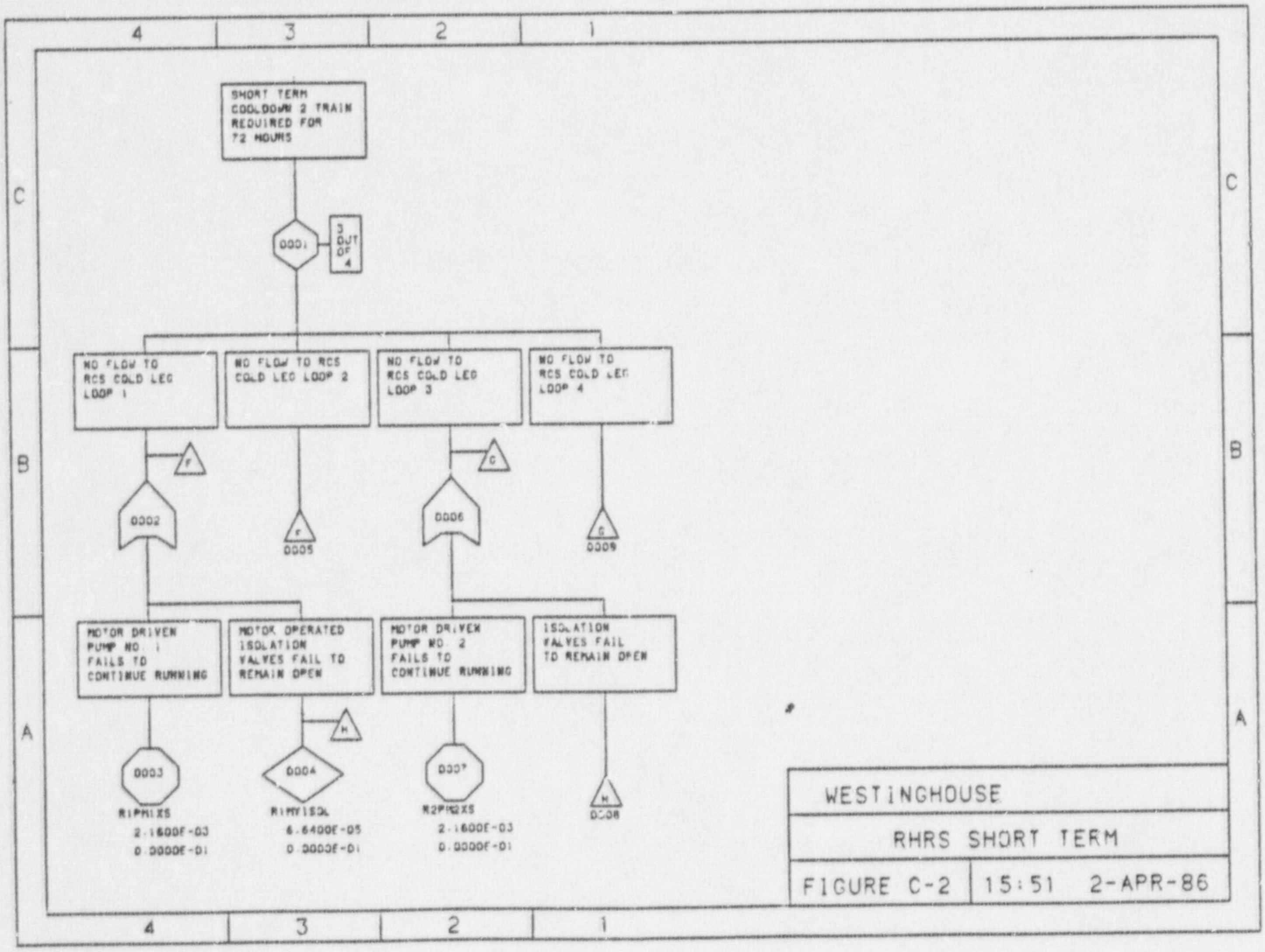


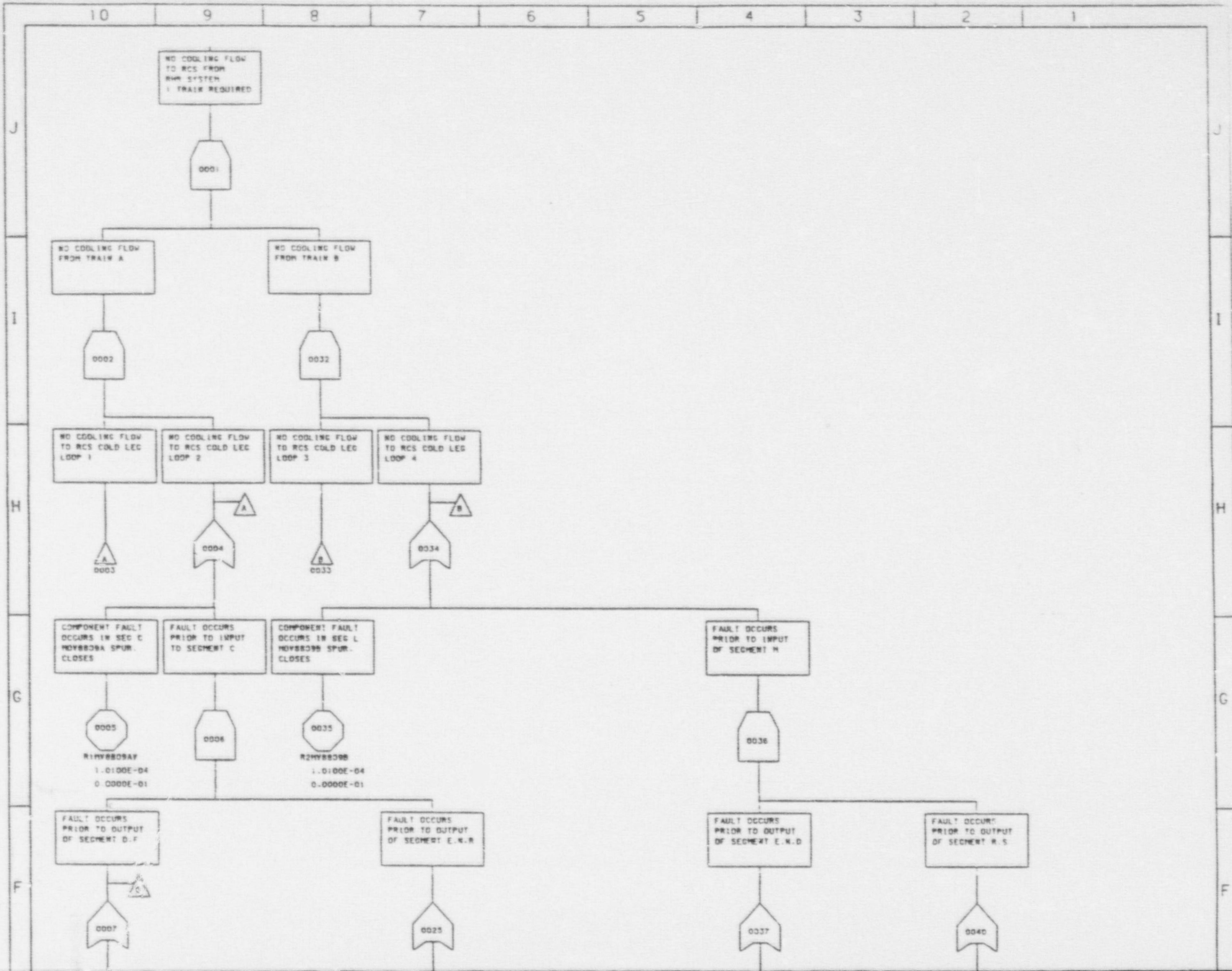
TI
APERTURE
CARD

Also Available On
Aperture Card

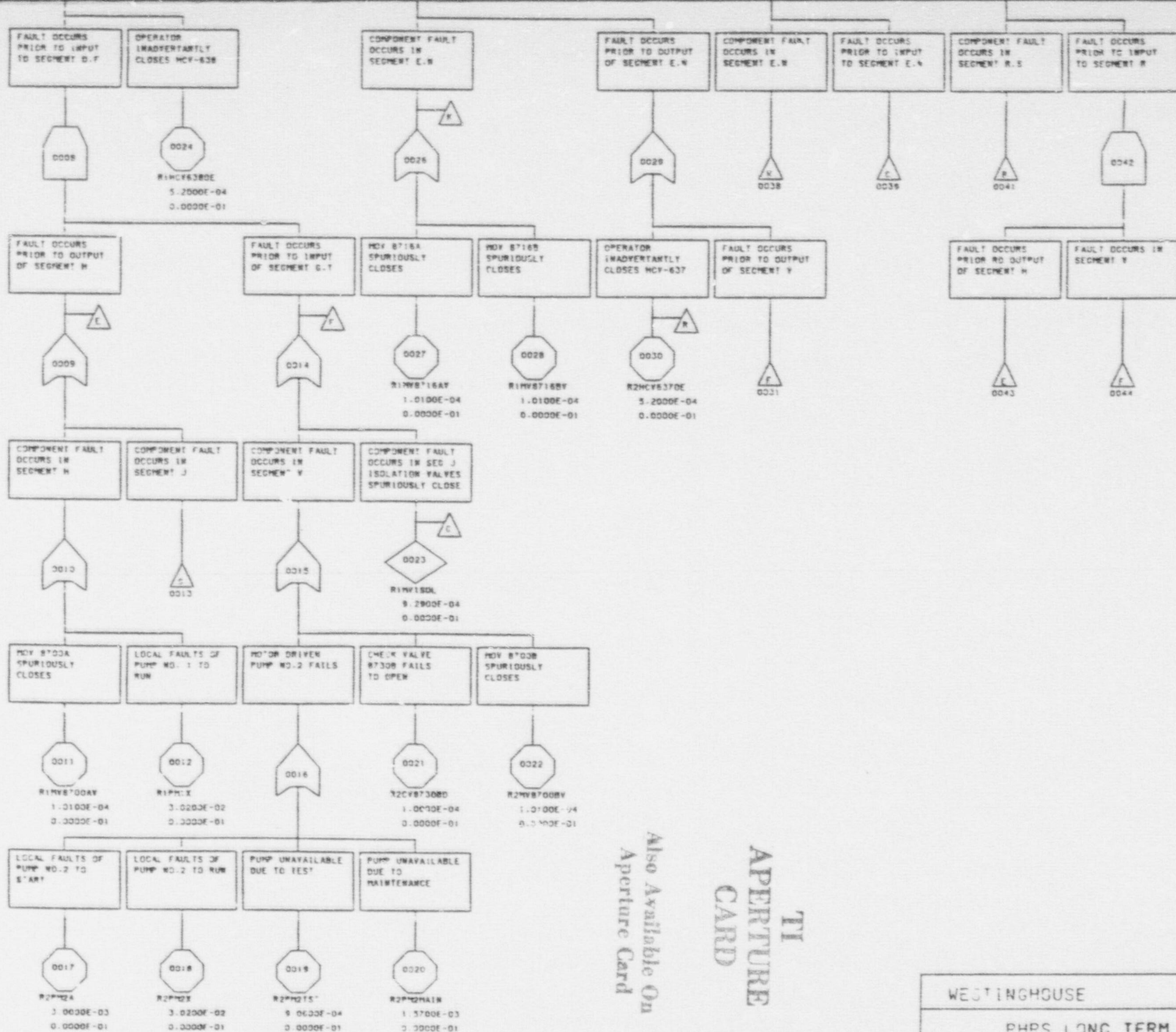
WESTINGHOUSE	
RHPS STARTUP	
FIGURE C-1	15:51 2-APR-86

8708110183-14


SHORT TERM COOLDOWN 2 TRAIN REQUIRED FOR 72 HOURS
0001
3 OUT OF 4
NO FLOW TO RCS COLD LEG LOOP 1
NO FLOW TO RCS COLD LEG LOOP 2
NO FLOW TO RCS COLD LEG LOOP 3
NO FLOW TO RCS COLD LEG LOOP 4
F
0002
F
0005
G
0006
G
0009
MOTOR DRIVEN PUMP NO. 1 FAILS TO CONTINUE RUNNING
MOTOR OPERATED ISOLATION VALVES FAIL TO REMAIN OPEN
MOTOR DRIVEN PUMP NO. 2 FAILS TO CONTINUE RUNNING
ISOLATION VALVES FAIL TO REMAIN OPEN
H
0003
R1PM1XS
2.1600E-03
0.0000E-01
0004
R1MV1SOL
6.6400E-05
0.0000E-01
0007
R2PM2XS
2.1600E-03
0.0000E-01
H
0008
WESTINGHOUSE
RHRS SHORT TERM
FIGURE C-2
15:51 2-APR-86



10
9
8
7
6
5
4
3
2
1
J
I
H
G
F
NO COOLING FLOW TO RCS FROM RHR SYSTEM 1 TRAIN REQUIRED
0001
NO COOLING FLOW FROM TRAIN A
NO COOLING FLOW FROM TRAIN B
0002
0032
NO COOLING FLOW TO RCS COLD LEG LOOP 1
NO COOLING FLOW TO RCS COLD LEG LOOP 2
NO COOLING FLOW TO RCS COLD LEG LOOP 3
NO COOLING FLOW TO RCS COLD LEG LOOP 4
A
0003
A
0004
B
0033
B
0034
COMPONENT FAULT OCCURS IN SEC C MOV8809A SPUR. CLOSES
FAULT OCCURS PRIOR TO INPUT TO SEGMENT C
COMPONENT FAULT OCCURS IN SEG L MOV8809B SPUR. CLOSES
FAULT OCCURS PRIOR TO INPUT OF SEGMENT M
0005
R1MV8809AF
1.0100E-04
0.0000E-01
0006
0035
R2MV8809B
1.0100E-04
0.0000E-01
0036
FAULT OCCURS PRIOR TO OUTPUT OF SEGMENT D.F
FAULT OCCURS PRIOR TO OUTPUT OF SEGMENT E.K.R
FAULT OCCURS PRIOR TO OUTPUT OF SEGMENT E.K.D
FAULT OCCURS PRIOR TO OUTPUT OF SEGMENT R.S
0007
0025
0037
0040

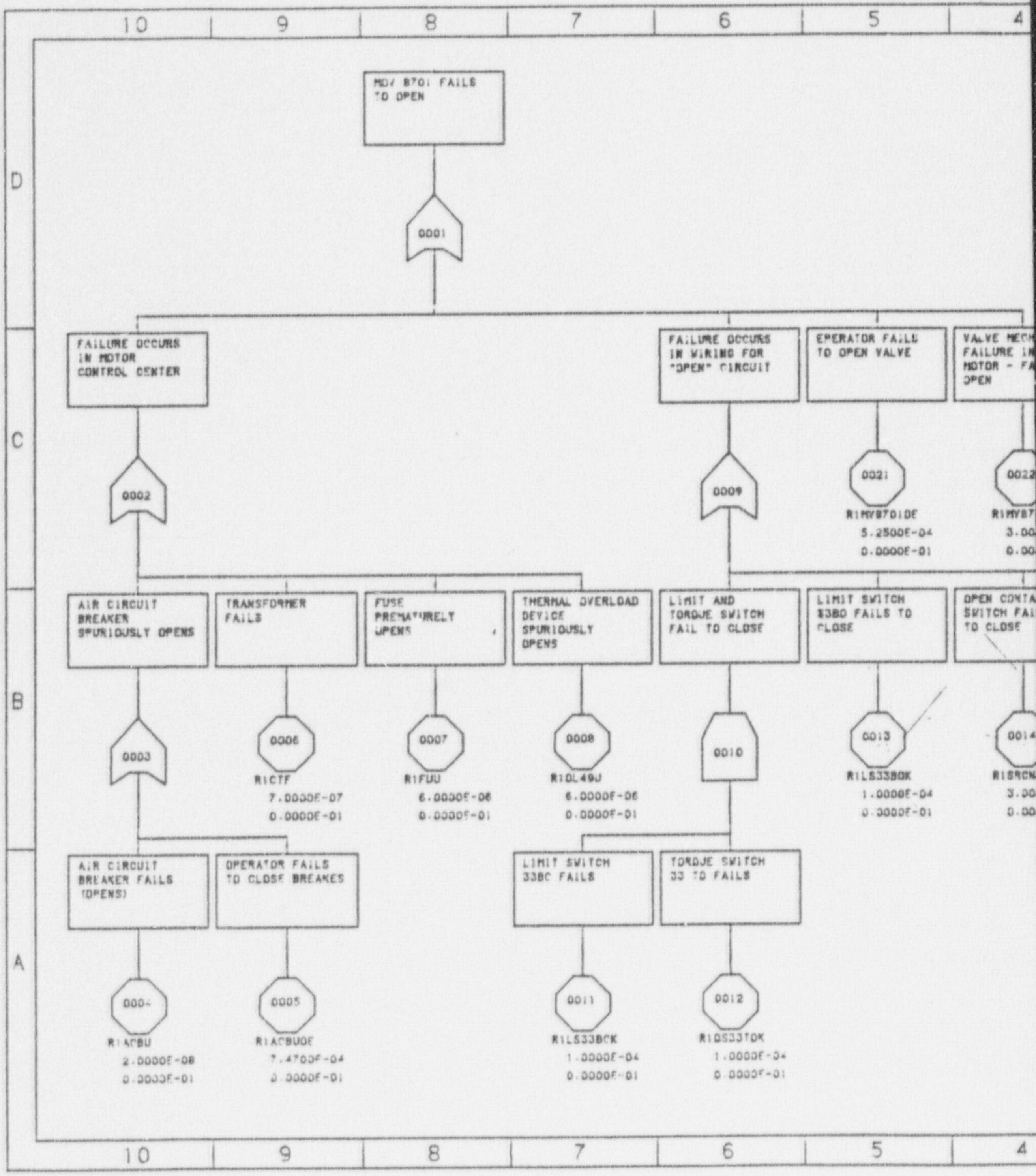


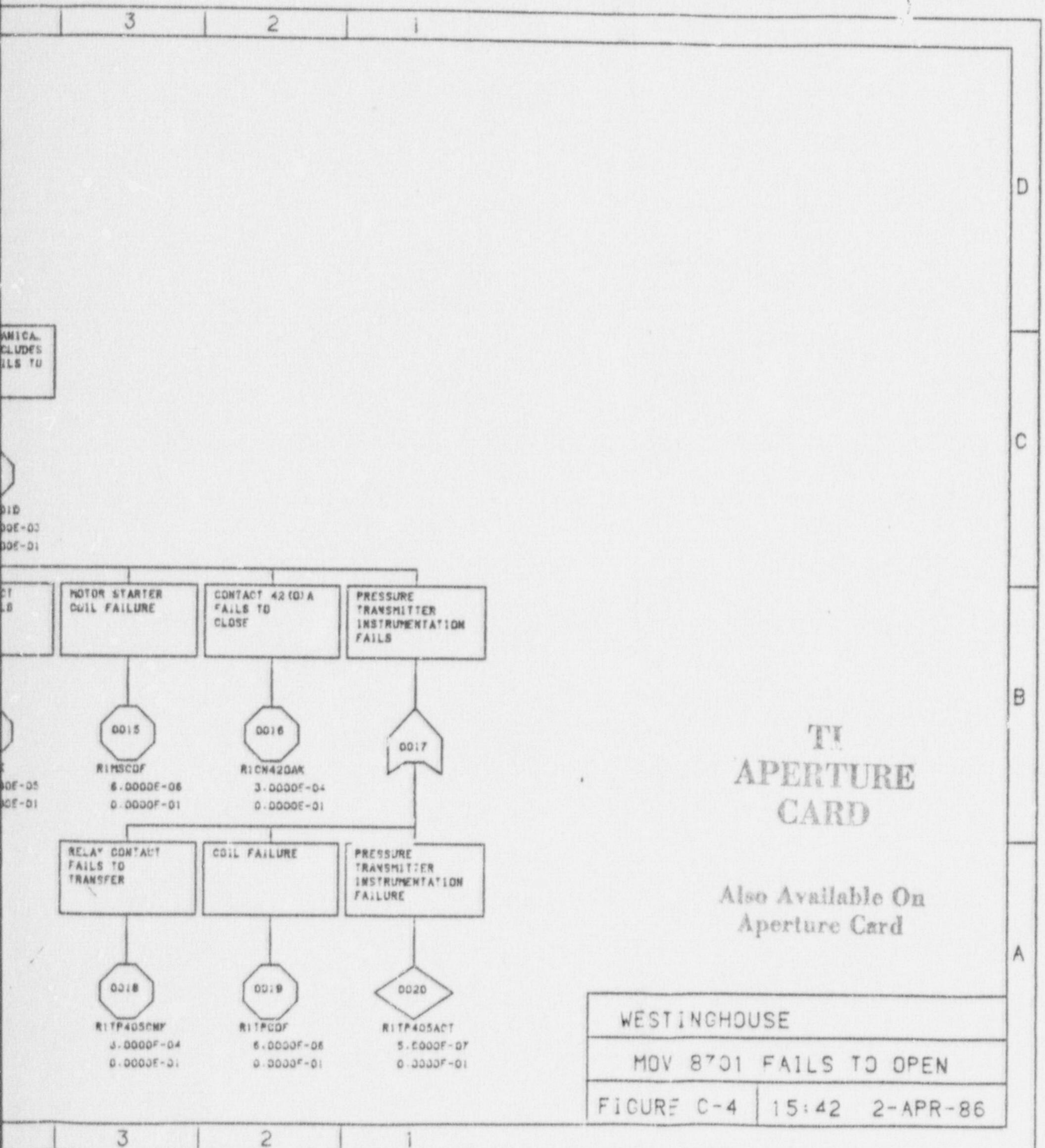
TI
APERTURE
CARD

Also Available On
Aperture Card

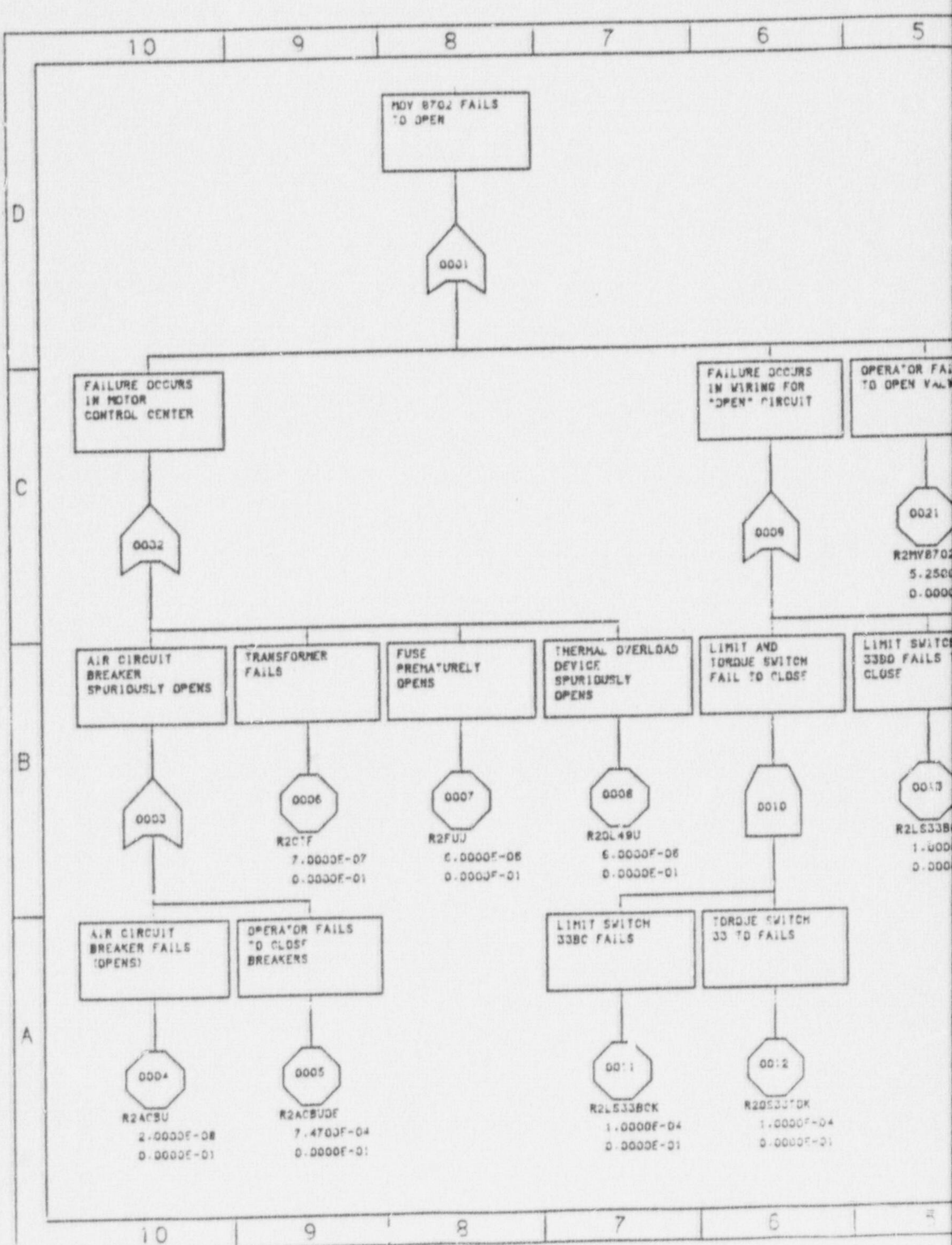
WESTINGHOUSE		
RHRS LONG TERM		
FIGURE C-3	15:43	2-APR-86

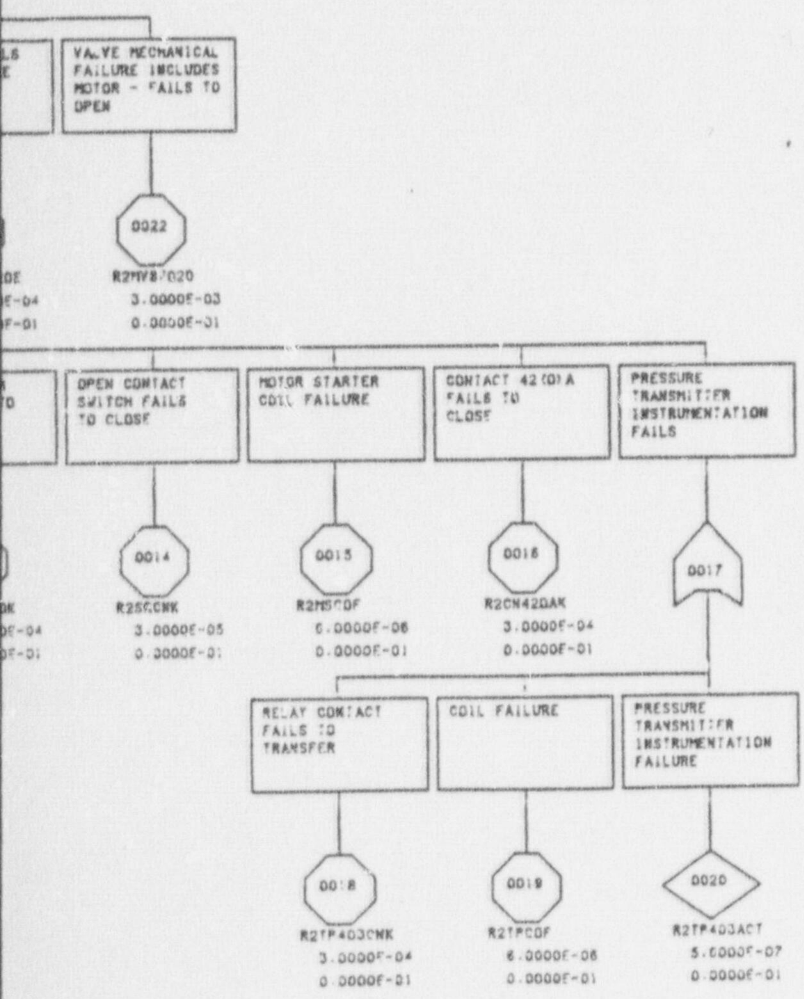
8708110183-15


10
9
8
7
6
5
4
D
C
B
A
MOV 8701 FAILS TO OPEN
0001
FAILURE OCCURS IN MOTOR CONTROL CENTER
0002
FAILURE OCCURS IN WIRING FOR "OPEN" CIRCUIT
0009
EPERATOR FAILS TO OPEN VALVE
0021
R1MV8701DE
5.2500E-04
0.0000E-01
VALVE MECH
FAILURE IN
MOTOR - FA
OPEN
0022
AIR CIRCUIT BREAKER SPURIOUSLY OPENS
0003
TRANSFORMER FAILS
0006
R1CTF
7.0000E-07
0.0000E-01
FUSE PREMATURELY OPENS
0007
R1FUU
6.0000E-08
0.0000E-01
THERMAL OVERLOAD DEVICE SPURIOUSLY OPENS
0008
R1OL49J
6.0000E-06
0.0000E-01
LIMIT AND TORQUE SWITCH FAIL TO CLOSE
0010
LIMIT SWITCH 33BO FAILS TO CLOSE
0013
R1LS33BOK
1.0000E-04
0.0000E-01
OPEN CONTA
SWITCH FAI
TO CLOSE
0014
AIR CIRCUIT BREAKER FAILS (OPENS)
0004
R1ACBU
2.0000E-08
0.0000E-01
OPERATOR FAILS TO CLOSE BREAKER
0005
R1ACBUOE
7.4700E-04
0.0000E-01
LIMIT SWITCH 33BC FAILS
0011
R1LS33BCK
1.0000E-04
0.0000E-01
TORQUE SWITCH 33 TO FAILS
0012
R1QS33TOK
1.0000E-04
0.0000E-01



870811 0183-16


MOV 8702 FAILS TO OPEN
0001
FAILURE OCCURS IN MOTOR CONTROL CENTER
0032
FAILURE OCCURS IN WIRING FOR "OPEN" CIRCUIT
0009
OPERATOR FA
TO OPEN VAL
0021
R2MV8702
AIR CIRCUIT BREAKER SPURIOUSLY OPENS
0003
TRANSFORMER FAILS
0006
R2CTF
7.0000E-07
0.0000E-01
FUSE PREMATURELY OPENS
0007
R2FUJ
6.0000F-06
0.0000F-01
THERMAL OVERLOAD DEVICE SPURIOUSLY OPENS
0008
R2OL49U
6.0000F-06
0.0000E-01
LIMIT AND TORQUE SWITCH FAIL TO CLOSE
0010
LIMIT SWITC
33BO FAILS
CLOSE
AIR CIRCUIT BREAKER FAILS (OPENS)
0004
R2ACBU
2.0000E-08
0.0000E-01
OPERATOR FAILS TO CLOSE BREAKERS
0005
R2ACBUDE
7.4700F-04
0.0000F-01
LIMIT SWITCH 33BC FAILS
0011
R2LS33BCK
1.0000E-04
0.0000E-01
TORQUE SWITCH 33 TO FAILS
0012
1.0000F-04
0.0000F-01
10
9
8
7
6
5
D
C
B
A



TI APERTURE CARD

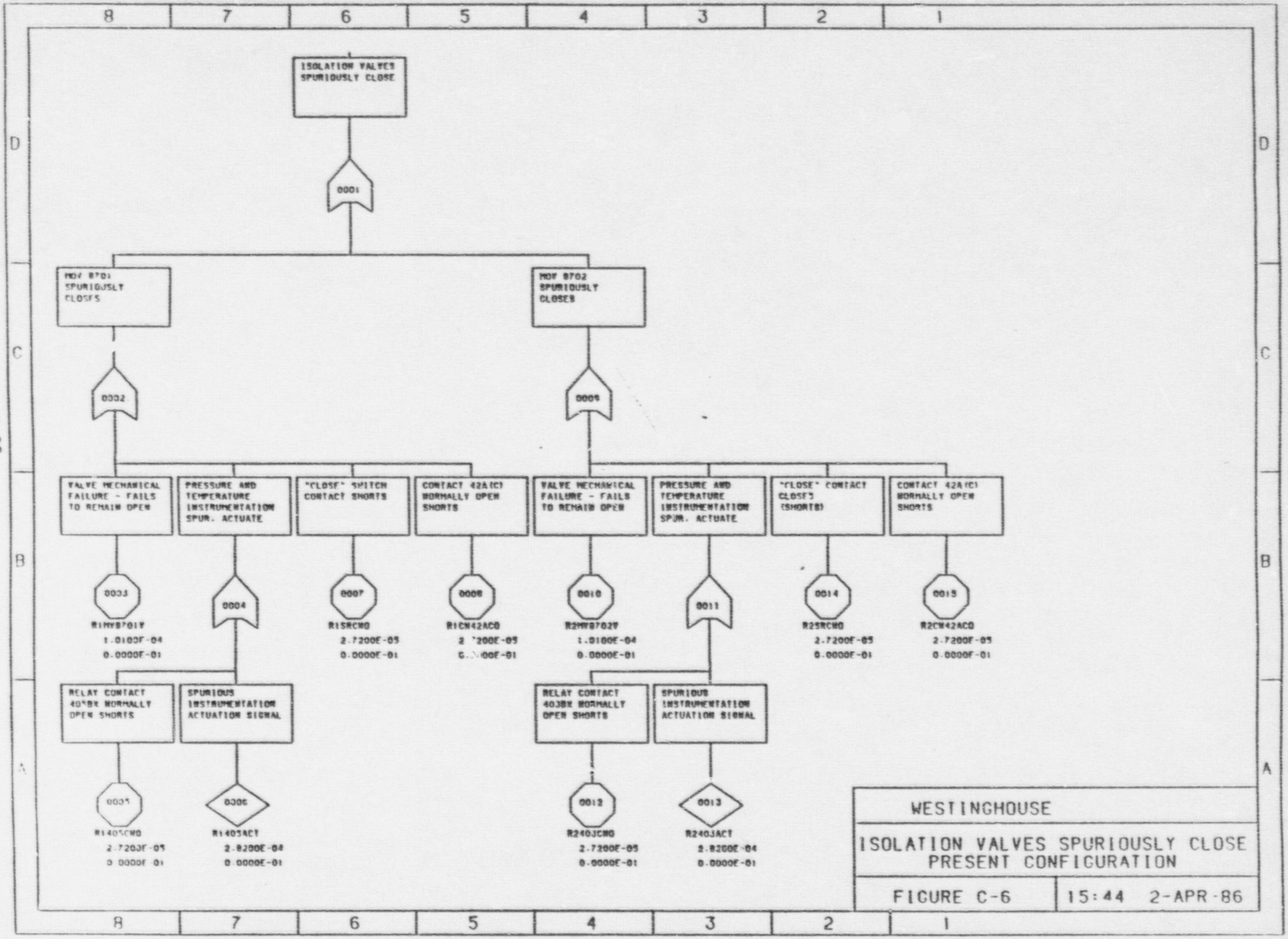
Also Available On Aperture Card

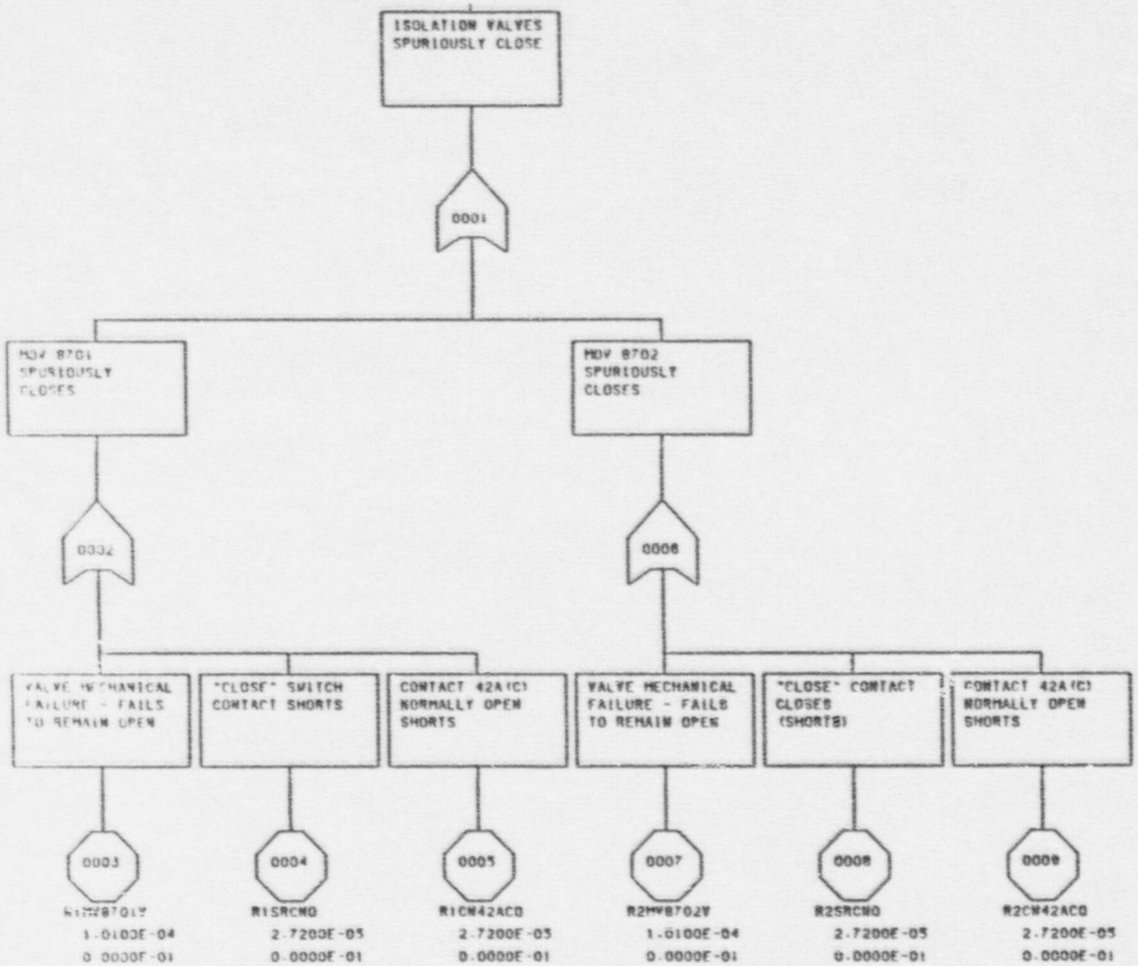
WESTINGHOUSE

MOV 8702 FAILS TO OPEN

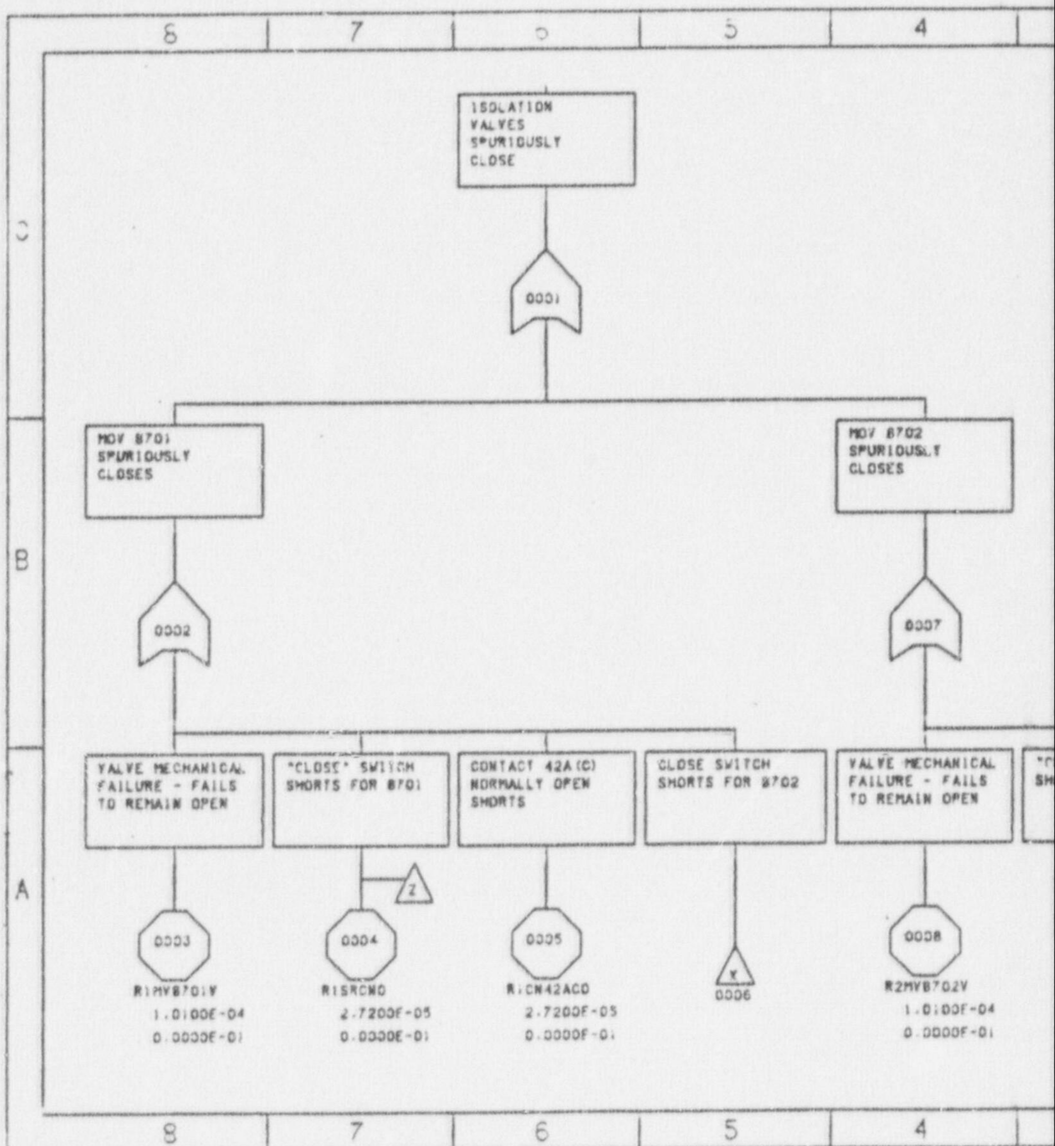
FIGURE C-5 15:41 2-APR-86

8708110183-17

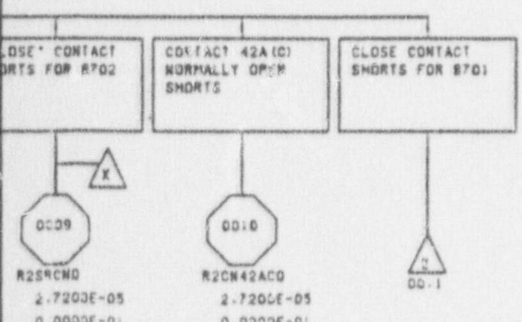

ISOLATION VALVES SPURIOUSLY CLOSE
0001
MOV 8701 SPURIOUSLY CLOSES
MOV 8702 SPURIOUSLY CLOSES
0002
0009
VALVE MECHANICAL FAILURE - FAILS TO REMAIN OPEN
PRESSURE AND TEMPERATURE INSTRUMENTATION SPUR. ACTUATE
"CLOSE" SWITCH CONTACT SHORTS
CONTACT 42A(C) NORMALLY OPEN SHORTS
VALVE MECHANICAL FAILURE - FAILS TO REMAIN OPEN
PRESSURE AND TEMPERATURE INSTRUMENTATION SPUR. ACTUATE
"CLOSE" CONTACT CLOSES (SHORTS)
CONTACT 42A(C) NORMALLY OPEN SHORTS
0003
R1MV8701V
1.0100E-04
0.0000E-01
0004
0007
R1SRCMO
2.7200E-05
0.0000E-01
0008
R1CN42ACO
2.7200E-05
0.0000E-01
0010
R2MV8702V
1.0100E-04
0.0000E-01
0011
0014
R2SRCMO
2.7200E-05
0.0000E-01
0015
R2CN42ACO
2.7200E-05
0.0000E-01
RELAY CONTACT 40ʼBX NORMALLY OPEN SHORTS
SPURIOUS INSTRUMENTATION ACTUATION SIGNAL
RELAY CONTACT 403BX NORMALLY OPEN SHORTS
SPURIOUS INSTRUMENTATION ACTUATION SIGNAL
0005
R1405CMO
2.7200E-05
0.0000E-01
0006
R1403ACT
2.8200E-04
0.0000E-01
0012
R2403CMO
2.7200E-05
0.0000E-01
0013
R2403ACT
2.8200E-04
0.0000E-01
WESTINGHOUSE
ISOLATION VALVES SPURIOUSLY CLOSE
PRESENT CONFIGURATION
FIGURE C-6
15:44 2-APR-86



WESTINGHOUSE	
ISOLATION VALVES SPURIOUSLY CLOSE MODIFICATION	
FIGURE C-7	15:46 2-APR-86



8
7
6
5
4
ISOLATION VALVES SPURIOUSLY CLOSE
0001
MOV 8701 SPURIOUSLY CLOSES
MOV 8702 SPURIOUSLY CLOSES
0002
0007
VALVE MECHANICAL FAILURE - FAILS TO REMAIN OPEN
"CLOSE" SWITCH SHORTS FOR 8701
CONTACT 42A(C) NORMALLY OPEN SHORTS
CLOSE SWITCH SHORTS FOR 8702
VALVE MECHANICAL FAILURE - FAILS TO REMAIN OPEN
Z
0003
R1MV8701V
1.0100E-04
0.0000E-01
0004
R1SRCNO
2.7200E-05
0.0000E-01
0005
R1CN42ACO
2.7200E-05
0.0000E-01
X
0006
0008
R2MV8702V
1.0100E-04
0.0000E-01
C
B
A



WESTINGHOUSE

ISOLATION VALVES SPURIOUSLY CLOSE
NRC MODIFICATION

FIGURE C-8 | 15:52 2-APR-86

TI
APERTURE
CARD

Also Available On
Aperture Card

8708110183-18

APPENDIX D

OVERPRESSURIZATION

ANALYSIS

APPENDIX D

OVERPRESSURIZATION TRANSIENTS

D.1 INTRODUCTION

This appendix details the calculations and qualitative analyses involved in the determination of the effect of removal of the RHR autoclosure interlock. The first section categorizes the types of initiating events and using operating experience determines the frequency of these events. The remaining section discusses the mass input transients and the consequences from these transients.

D.2 INITIATING EVENTS

This section provides the data and calculations used to determine the frequencies of the transient events identified in Section 6.5. Table D.2-1 lists the transients that have actually occurred at U.S. PWRs by the type of transient.

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.2-2. This table shows, for each plant, a rough estimate of the total number of shutdown hours (in which the RHRS would be required to operate) along with the total report period hours. This data shows that roughly 31 percent of the time that a plant has been operating, it is in the shutdown modes.

Therefore to quantify the frequency of overpressurization transients the following formula was used:

$$F\ (\text{Transient}) = \frac{\#\ \text{of transients}}{\#\ \text{of shutdown years}}$$

$$\frac{\#\ \text{of transients}}{\text{Total report period years} \times \%\ \text{in shutdown}}$$

$$\frac{\#\ \text{of transients}}{510.30\ \text{years} \times 31\%}$$

Table D.2-3 lists the frequencies for each transient using the above formula.

For the loss of RHR cooling train initiating event and for the letdown isolation/RHRS isolated event, an estimate of the number of events was made utilizing the AEOD Case Study Report "Decay Heat Removal Problems at U.S. Pressurized Water Reactors." The Letdown isolation, RHRS isolated event was assumed to be synonymous with the automatic closure of Suction/Isolation valves events reported in Table 1-2 (37 events). The number of loss of RHR cooling train events was determined by subtracting the number of autoclosure events and the number of inability to open suction/isolation valve events from the total number of events (130-37-8=85 events).

For the modification case in which the autoclosure interlock is removed, the number of letdown isolation events due to isolation of the RHRS via autoclosure of the suction valves would essentially decrease to zero. However to account for some unknown causes of closure of the suction valves, the number of events was conservatively assumed to only decrease by one-half.

If the failure rate for a motor-operated valve to spuriously close is taken from Table 6.2-1 as 1E-7/hr, the frequency for a letdown isolation event due to spurious closure of one of the motor operated suction valves would be:

$$\text{Frequency} = 2 \text{ valves} \times \frac{1E\text{-}7}{\text{hr}} \times \frac{8760 \text{ hrs}}{\text{year}} \times 31\%$$

$$= 5.43E\text{-}4/\text{year}$$

Thus the reduction of the frequency by one-half is a conservative assumption.

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 overpressure conditions.

This analysis utilized event trees to depict the various mitigating actions that 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 390 psig.

2. One charging pump is in operation and pumping at its maximum flowrate of 550 gpm.

3. Letdown via the RHRS is in operation and the flowrate is 120 gpm.

4. No RCPs are in operation.

5. An alarm must actuate before the operator can intervene and stop the transient. This alarm can come from:

   a) RHR relief valve discharge to PRT (pressurizer relief tank),
   b) PORV discharge to PRT,
   c) LTOP 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 (charging pump flowrate = 550 gpm and safety injection pump flowrate = 650 gpm). Furthermore, these pumps are assumed to have an infinite water source.

The event trees derived in this analysis are shown in Figure D.3-1, D.3-2, and D.3-3. Figure D.3-1 depicts the mitigating actions given the initiator - Charging/Safety Injection Pump Actuation, while letdown isolation with the RHR operable and inoperable are shown in Figure D.3-2 and D.3-3 respectively.

The node that is affected by removal of the autoclosure interlock is the RS node (RHRS Suction Valve Close). This node changes from an automatic system (the autoclosure interlock) to an operator action (given an alarm). No distinction between the modification and the NRC proposed modification is made for this node.

The probability calculations for each node are shown in Table D.3-1. The success criteria for each node is also shown on the tables.

The results of the quantification of the event trees is shown in Tables D.3-2 to D.3-4. These tables also detail the change in frequencies of the consequence categories due to the removal of the autoclosure interlock.

TABLE D.2-1
ACTUAL OVERPRESSURIZATION TRANSIENTS

PLANT	DATE	KEYWORDS	SOURCE	REMARKS
OPENING OF ACCUMULATOR ISOLATION DISCHARGE VALVES				
SURRY 1	JAN 28,1973	VENT TRAPPED AIR	N. SAFETY	FROM 450 TO 590 PSIG
PRAIRIE ISLAND 1	JAN 16, 1974	SI SIGNAL INITIATED	N. SAFETY	FROM 395 TO 840 PSIG
INDIAN POINT 2	FEB 22,1974	INADVERTENT SI	N.SAFETY	FROM 150 TO 560 PSIG
STARTUP OF INACTIVE LOOP				
INDIAN POINT 2	MARCH 8,1972	THERMAL EXPANSION	N. SAFETY	FROM 400 TO 640 PSIG
PRAIRIE ISLAND 1	OCT 31, 1973	THERMAL EXPANSION	N. SAFETY	FROM 420 TO 1100 PSIG
INDIAN POINT 2	JAN 23, 1974	PRESSURE SURGE	N. SAFETY	FROM 425 TO 525 PSIG
ST. LUCIE 1	JUNE 17, 1976	THERMAL EXPANSION	N. SAFETY	FROM 435 TO 815 PSIG
FARLEY 2	OCT 1983	PRESSURE SURGE	NPE	TO 480 PSIG RHR RELIEF
TURKEY POINT 4	NOV 28,1981	PRESSURE SURGE	IE 82-17	TO 1100 PSIG
TURKEY POINT 4	NOV 29,1981	PRESSURE SURGE	IE 82-17	TO 750 PSIG
NORTH ANNA 2	MAY 24, 1982	FILLING AND VENTING	AEOD	PORV OPENED TWICE
NORTH ANNA 2	MAY 18,1982	PRESSURE SURGE	AEOD	PORV OPENED TWICE
SALEM 2	MARCH 1985	RCS FILL AND VENT	NPE	PORV OPENED TWICE 400P
SUMMER	MAY 1985	DG TESTING	NPE	RHR RELIEF VALVE
ISOLATION OF LETDOWN WHILE CHARGING CONTINUES		RHR OPERABLE		
GINNA	1969	OPERATOR ERROR	N. SAFETY	TO 2485 PSIG SAFETY VA
INDIAN POINT 2	FEB 17, 1972	OPERATOR ERROR	N. SAFETY	FROM 420 TO 650 PSIG
INDIAN POINT 2	APRIL 6, 1972	OPERATOR ERROR	N. SAFETY	FROM 420 TO 680 PSIG
INDIAN POINT 2	MAY 18,1973	FROZEN VALVES	N. SAFETY	FROM 440 TO 575 PSIG
PRAIRIE ISLAND 2	NOV 27, 1974	TEST SIGNAL	N. SAFETY	TO 900 PSIG
ST. LUCIE 1	AUG 12, 1975	BROKEN WIRES ON RELAY	N. SAFETY	FROM 210 TO 600 PSIG
BEAVER VALLEY 1	FEB 24,1976	ELECTRICAL BUS TRANSFER	N. SAFETY	FROM 400 TO 1000 PSIG
BEAVER VALLEY 1	MARCH 5, 1976	BUS DEENERGIZED SI SIGNAL	N. SAFETY	FROM 400 TO 1150 PSIG
D.C. COOK 1	APRIL 14, 1976	RPS TESTING	N. SAFETY	TO 1040 PSIG
INDIAN POINT 2	SEPT 12, 1976	INSTRUMENT AIR LOST	N. SAFETY	FROM 400 TO 515 PSIG
NORTH ANNA 1	MARCH 1978	ELECTRICAL SHORT	NPE	TO 575 PSIG
NORTH ANNA 1	MARCH 1980	VALVE FAILED CLOSED	NPE	TO 570 PSIG RHR RELIEF
FARLEY 2	OCT 1983	CONTAINMENT ISOLATED	NPE	TO 700 PSIG RHR RELIEF
SAN ONOFRE	MAY 7, 1982	INADVERTENT DECREASE	AEOD	RELIEF VALVE IN SDC
SURRY 1	MAY 1985	POSITIONER OUT OF ADJUSTMENT	NPE	PORV CYCLED TWICE 410P
PRESSURIZER HEATERS ACTUATION				
RANCHO SECO	SEPT 1981	EMERGENCY OPERATION INTERMITTE	NPE	

TABLE D.2-1 (CONT.)

ISOLATION OF LETDOWN WHILE CHARGING CONTINUES RHR ISOLATED

INDIAN POINT 2	FEB-APRIL 1972	OPERATOR ERROR	NPE	TO 670 PSIG
INDIAN POINT 2	FEB -APRIL 1972	OPERATOR ERROR	NPE	TO 650 PSIG
TURKEY POINT 3	DEC 3, 1974	HIGH PRESSURE AUTOMATIC	N. SAFETY	FROM 50 TO 800 PSIG
ZION 1	JUNE 3, 1975	OPERATOR ERROR	N. SAFETY	FROM 100 TO 1100 PSIG
TROJAN	JULY 22, 1975	UNKNOWN PERSON	N. SAFETY	FROM 490 TO 3326 PSIG
ZION 2	SEPT 18, 1975	INTERLOCK TEST	N. SAFETY	FROM 95 TO 1300 PSIG
POINT BEACH 2	FEB 28, 1976	OPERATIONAL REASONS	NNC	FROM 400 TO 830 PSIG
INDIAN POINT 3	SEPT 30, 1976	SPURIOUS CLOSURE	N. SAFETY	FROM 50 TO 2250 PSIG
DAVIS BESSE	APRIL 19,1980	LOSS OF BUS	DHR	TEMP FROM 80 TO 170

CHARGING/SAFETY INJECTION PUMP ACTUATION

ZION 1	JUNE 13, 1973	OP. LEFT PUMP RUNNING	N. SAFETY	FROM 110 TO 1290 PSIG
PALISADES	DEC 1981	TESTING DG	NPE	PORV OPENED
PRAIRIE ISLAND 1	OCT 1974	SI SIGNAL	NPE	
POINT BEACH 2	DEC 10, 1974	SI PUMP	NNC	FROM 345 TO 1400 PSIG
BEAVER VALLEY 1	MARCH 13, 1976	INADVERTENT SI SIGNAL	N. SAFETY	FROM 425 TO 495 PSIG
ROBINSON 2	JAN 1978	SI SIGNAL	NPE	FROM 360 TO 560 PSIG
NORTH ANNA 1	MARCH 1981	SI SIGNAL	NPE	RCS PORVS LIFTED
PALISADES	DEC 1981	BUS TRANSFER SI SIGNAL	NPE	OPPS OPERATED
NORTH ANNA 2	MAY 1983	INADVERTENT SI SIGNAL	NPE	TO 381 PSIG PORV 3 TIM
SURRY 1	JULY 7,1982	INADVERTENT CHARGING	AEOD	ONE PORV OPENED
PALISADES	DECEMBER 4, 1982	INADVERTENT SI	AEOD	PORV OPENED
GINNA	JUNE 9,1983	PERSONNEL ERROR	AEOD	PORV ACTUATED
SALEM 2	JUNE 17,1983	PERSONNEL ERROR	AEOD	BOTH PORVS ACTUATED
SURRY 1	JUNE 1984	PLACE CHARGING IN SERVICE	NPE	PORV CYCLED
TROJAN	JUNE 1985	I&C TESTING	NPE	FROM 350 TO 420 PSIG
PALO VERDE 1	APRIL 1985	BATTERY TESTING	NPE	1350 GAL INJECTED

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
NNC	WESTINGHOUSE SEARCH OF LERS
DHR	AEOD CASE STUDY REPORT- DECAY HEAT REMOVAL PROBLEMS AT U.S. PWRs

TABLE D.2-2
PLANT OPERATING EXPERIENCE

PLANT	REPORT PERIOD HRS	GENERATOR HRS	FORCED OUTAGE HRS	SCHEDULED OUTAGE HRS	TOTAL SHUTDOWN HRS	SHUTDOWN %
ARKANSAS 1	95,275.00	62,794.10	11,560.50	20,920.40	32,480.90	0.34
ARKANSAS 2	49,104.00	33,174.20	6,754.70	9,175.10	15,929.80	0.32
BEAVER VALLEY 1	83,304.00	42,718.70	18,442.40	22,142.90	40,585.30	0.49
BYRON	1,105.00	878.70	86.50	139.80	226.30	0.20
CALLAWAY 1	7,598.50	6,906.10	354.10	338.30	692.40	0.09
CALVERT CLIFFS 1	91,909.00	69,895.50	6,295.10	15,718.40	22,013.50	0.24
CALVERT CLIFFS 2	75,264.00	61,921.90	3,981.30	9,360.80	13,342.10	0.18
CATAWBA 1	3,001.00	2,537.80	463.20	(0.00)	463.20	0.15
COOK 1	94,968.00	66,217.70	4,499.40	24,250.90	28,750.30	0.30
COOK 2	68,664.00	46,588.00	8,767.40	13,308.60	22,076.00	0.32
CRYSTAL RIVER 3	75,720.00	47,819.70	11,968.00	15,932.30	27,900.30	0.37
DAVIS-BESSE 1	63,601.00	34,371.80	10,827.80	18,401.40	29,229.20	0.46
DIABLO CANYON 1	4,270.30	4,134.50	96.90	38.90	135.80	0.03
FARLEY 1	69,408.00	46,941.60	6,382.90	16,083.50	22,466.40	0.32
FARLEY 2	37,321.00	31,928.40	1,686.80	3,705.80	5,392.60	0.14
FORT CALHOUN 1	106,081.00	81,073.00	1,750.30	23,257.70	25,008.00	0.24
GINNA	139,656.00	104,552.80	4,220.80	30,882.40	35,103.20	0.25
HADDAM NECK	156,336.00	129,395.40	1,292.10	25,648.50	26,940.60	0.17
INDIAN POINT 2	99,385.00	65,707.60	6,438.70	27,238.70	33,677.40	0.34
INDIAN POINT 3	80,401.00	44,194.10	11,168.50	25,038.40	36,206.90	0.45
KEWAUNEE	99,745.00	83,122.90	2,760.10	13,862.00	16,622.10	0.17
MAINE YANKEE	113,772.60	88,128.50	5,728.70	19,915.40	25,644.10	0.23
MCGUIRE 1	34,344.00	23,501.00	3,858.30	6,984.70	10,843.00	0.32
MCGUIRE 2	14,640.00	10,141.50	2,127.80	2,370.70	4,498.50	0.31
MILLSTONE 2	86,352.00	57,428.50	10,887.70	18,035.80	28,923.50	0.33
NORTH ANNA 1	64,921.00	43,731.50	5,919.70	15,269.80	21,189.50	0.33
NORTH ANNA 2	42,792.00	31,968.10	4,279.80	6,544.10	10,823.90	0.25
OCONEE 1	107,785.00	75,690.10	12,515.50	19,579.40	32,094.90	0.30
OCONEE 2	97,705.00	70,162.30	10,649.30	16,893.40	27,542.70	0.28
OCONEE 3	95,352.00	67,367.80	11,066.80	16,917.40	27,984.20	0.29
PALISADES	121,575.00	64,253.70	15,556.10	41,765.20	57,321.30	0.47
POINT BEACH 1	131,376.00	103,442.80	2,413.40	25,519.80	27,933.20	0.21
POINT BEACH 2	116,161.00	100,959.40	697.20	14,504.40	15,201.60	0.13
PRAIRIE ISLAND 1	104,112.00	84,538.50	3,390.70	16,182.80	19,573.50	0.19
PRAIRIE ISLAND 2	95,230.00	81,075.40	3,315.50	10,839.10	14,154.60	0.15
RANCHO SECO 1	92,401.00	49,336.30	20,949.00	22,115.70	43,064.70	0.47
ROBINSON 2	128,526.00	88,303.90	9,045.00	31,177.10	40,222.10	0.31
SALEM 1	73,105.00	41,040.60	18,488.80	13,575.60	32,064.40	0.44
SALEM 2	35,521.00	18,579.00	12,789.40	4,152.60	16,942.00	0.48
SAN ONOFRE 1	161,120.00	91,890.70	11,930.50	57,298.80	69,229.30	0.43
SAN ONOFRE 2	19,585.00	12,034.50	713.90	6,836.60	7,550.50	0.39
SAN ONOFRE 3	13,896.00	8,815.30	1,448.90	3,631.80	5,080.70	0.37
SEQUOYAH 1	38,017.00	23,871.00	5,339.10	8,806.90	14,146.00	0.37
SEQUOYAH 2	29,977.00	21,494.40	3,659.30	4,823.30	8,482.60	0.28
ST. LUCIE 1	77,688.00	55,736.00	2,459.90	19,492.10	21,952.00	0.28
ST. LUCIE 2	19,585.00	16,190.80	2,044.00	1,350.20	3,394.20	0.17
SUMMER 1	16,080.00	11,320.20	1,033.30	3,726.50	4,759.80	0.30
SURRY 1	112,728.00	69,374.10	12,981.30	30,372.60	43,353.90	0.38
SURRY 2	109,608.00	69,451.40	7,925.90	32,230.70	40,156.60	0.37
TMI 1	97,873.00	31,589.90	58,748.50	7,534.60	66,283.10	0.68
TROJAN	80,352.00	47,590.30	9,010.40	23,751.30	32,761.70	0.41
TURKEY PT. 4	106,873.00	73,834.60	4,628.50	28,409.90	33,038.40	0.31
TURKEY PT.3	113,145.60	77,211.20	4,766.60	31,167.80	35,934.40	0.32
YANKEE ROWE 1	218,781.00	170,173.80	8,326.10	40,281.10	48,607.20	0.22
ZION 1	103,752.00	70,245.40	11,113.00	22,393.60	33,506.60	0.32
ZION 2	97,465.00	69,607.80	13,138.10	14,719.10	27,857.20	0.29
TOTAL HOURS	4,474,313.00	3,086,954.80	432,743.50	954,614.70	1,387,358.20	0.31
TOTAL YEARS	510.77	352.39	49.40	108.97	158.37	

TABLE D.2-3
OVERPRESSURIZATION FREQUENCIES

Transient	Number of Transients	Frequency
1. Premature Opening of the RHR System	0	0
2. Rod Withdrawal	Not Analyzed	Not Analyzed
3. Heat Input/Removal		
3.1 Failure to Isolate RHR during Startup	Not Analyzed	Not Analyzed
3.2 Pressurizer Heaters Actuation	1	6.32E-3/yr
3.3 Startup of Inactive RCS Loop	11	6.95E-2/yr
3.4 Loss of RHR Cooling Train	85*	5.37E-1/yr
4. Mass Input/Letdown		
4.1 Opening of Accumulator Discharge Isolation Valve	3	1.89E-2/yr
4.2 Letdown Isolation		
4.2.1 RHRS Operable	16	1.01E-1/yr
4.2.2 RHRS Isolated (Present)	37*	2.34E-1/yr
(Modification)	19**	1.17E-1/yr
4.3 Charging/Safety Injection Pump Actuation	16	1.01E-1/yr

* From AEOD Decay Heat Removal Case Study Report.

**Assumed to be one half of present configuration case.

TABLE D.3-1

NODAL PROBABILITY CALCULATIONS

1. RHR Isolated (RI)

Description: For the charging/safety injection pump initiating event, it was assumed that the RHR is not isolated approximately 90% of the time during cold shutdown. For the letdown isolation RHR operable, the RHR is not isolated while for the letdown isolation, RHR isolated the transient has no effect on the RHRS.

Case	RI Failure Probability
Charging/Safety Injection Pump	0.9
Letdown Isolation - RHR Operable	1.0
Letdown Isolation - RHR Isolated	0.0

TABLE D.3-1 (Cont)

NODAL PROBABILITY CALCULATIONS

2. RHR Relief Valve Operates (RV)

Success: RHR Relief Valve Opens at P=450 psig

Failure: Relief Valve Fails to Open

Description: The RHR relief valve is a spring-loaded relief valve set to actuate at a pressure of 450 psig. It can relieve 900 gpm at 450 psig.

Probability (RV Fails to Open) = 3E-4

TABLE D.3-1 (Cont)

NODAL PROBABILITY CALCULATIONS

3. LTOP System Operates at P=450 psig (LTP)

Success: One or Two Trains of LTOP operate

Failure: Both trains fail to operate

Description: The LTOP system consists of two trains that utilize the PORVs. The operator must enable the system at P=475 psig or an alarm sounds. The LTOP system is set at P=450 psig and T=323°F. A PORV can relieve 700 gpm at P=450 psig.

Failure Probabilities: The failure probabilities were calculated through the use of fault trees. Figure D.3-4 shows the fault tree developed for two trains of LTOP while the failure of one train of LTOP is shown in Figure D.3-5.

LTP Failure Probabilities

Two Trains Fail	1.50E-5
One Train Fails	7.71E-3

TABLE D.3-1 (Cont)

NODAL PROBABILITY CALCULATIONS

4a) RHR Suction Valves Close at P=700 psig (RS)

Success: Autoclose Feature Closes
One of Two RHR Isolation
Valves at P=700 psig

Failure: Both isolation valves do not close.

Description: The autoclose feature utilizes a pressure signal to actuate the valve operator which closes the valve.

Failure Probabilities: The failure probability was calculated using a fault tree. Figure D.3-6 depicts the autoclose failing to close one of two isolation valves (MOV 8701 or 8702).

RS Failure Probability = 1.44E-5

4b) Operator Isolates RHR System Given Overpressure Alarm (OD)

Success: Operator closes one of two isolation valves when alarm sounds at P=700 psig.

Failure: Operator fails to close either isolation valve.

Description: The modification cases assume an alarm operates when the pressure exceeds 700 psig and an isolation valve is in the open position. Given this alarm, the operator (through training and operating procedures) will close one of the isolation valves.

Failure Probability: The probability of failure is conditional on a time factor. If an mitigating system operates successfully, it is assumed that the operator has 20 minutes in which to act. If no mitigating system operates, the operator has approximately 10 minutes in which to act. The calculations are shown below:

HUMAN ERROR CALCULATIONS

1. Diagnosis within time T by control room personnel of abnormal event

HEP = 0.01	within 20 minutes	Table 20-3
HEP = 0.1	within 10 minutes	

2. Estimated HEP in operating manual controls

HEP = 0.0005	Turn rotary control in wrong direction (Table 20-12)

TABLE D.3-1 (Cont)

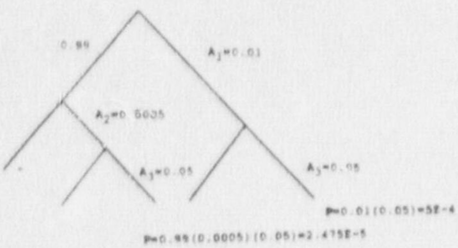
NODAL PROBABILITY CALCULATIONS

4b) (Continued)

3. Recovery factor - special short term one of a kind checking

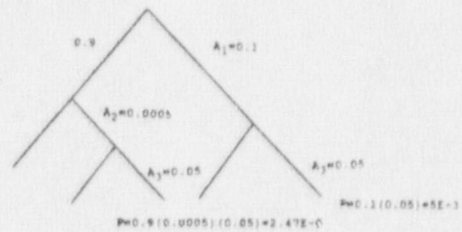
HEP = 0.05 Table 20-22

20 minutes



P(20 minutes) = 5.25E-4

10 minutes



P(10 minutes) = 5.02E-3

TABLE D.3-1 (Cont)

NODAL PROBABILITY CALCULATIONS

5. Operator Secures Running Pump (OA1)

Success: Operator Stops Pump

Failure: Pump Continues to Run

Description: For any operator action to occur, an alarm must sound. The probability that the operator secures the pump also considers that the operator neglects the alarm.

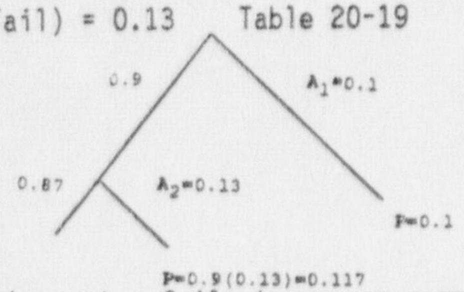
Failure Probability: The human error probability is calculated below:

1. Initial screening model for diagnosis in time T

   HEP = 0.1 within 20 minutes Table 20-1

2. Conditional probability of failure for task N given success of preceding task (N-1)

   CP (Fail) = 0.13 Table 20-19 High Dependence



P(operator fails to secure pump) = 0.217

TABLE D.3-1 (Cont)
NODAL PROBABILITY CALCULATIONS

6. Operator Opens PORV (OA2)

Success: Operator opens a PORV to reduce pressure

Failure: Operator fails to open PORV

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. 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:

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.3-1 (Cont)
NODAL PROBABILITY CALCULATIONS

7. Pressurizer Safety Valve Lifts at P=2485 psig (PZR)

Success: One of three safety valve operate.

Failure: All three safety valves fail.

Description: The safety valves can relieve approximately 875 gpm at P = 2485 psig and T = 100°F.

Failure Probability: The failure of one valve to open is 1E-5/D. Thus the failure of all three valves is:

P(valves fail to open) = (1E-5) (1E-5) (1E-5) = 1E=15

TABLE D.3-1 (Cont)
NODAL PROBABILITY CALCULATIONS

8. RHR Relief Valve Reseats (VR)

Success: Relief Valve Closes

Failure: Relief Valve Fails to Close

Description: Given that the transient is successfully mitigated, the RHR relief valve must close in order to prevent a loss of coolant.

Failure Probability: The probability that the relief valve will not reseat is 3E-2.

TABLE D.3-1 (Cont)

NODAL PROBABILITY CALCULATIONS

9. PORVs Reseat (PRV)

Success: The PORVS that opened close.

Failure: None of the actuated PORVs close.

Description: Given that the transient is mitigated, the PORVs must close in order to prevent a loss of coolant.

Failure Probability: The failure to reseat for a PORV is 3E-3.

If two PORVs operated, two must close P(2 PORVs fail to close) = 6E-3

TABLE D.3-2

CONSEQUENCE CATEGORY FREQUENCIES (PER YEAR)

FOR LETDOWN ISOLATION RHR OPERABLE TREE

(INITIATING EVENT FREQUENCY = 1.01E-1)

Consequence Cateogry	Frequency Present Configuration	Frequency Modification Case	Net Change (+ or -)
SUCCESS	7.6253E-2	7.6253E-2	0
HLCI	3.5505E-11	3.5327E-11	-1.78E-13
LLFO	4.7266E-4	4.7266E-4	0
LSFO	2.3576E-3	2.3576E-3	0
LLCO	2.1917E-2	2.1917E-2	0
LSCO	3.7935E-7	3.7935E-7	0
MSFI	8.4341E-13	8.3919E-13	-4.22E-15
MOPI	7.4732E-11	7.4358E-11	-3.74E-13
MSCI	6.3120E-11	6.2804E-11	-3.16E-13
HOVI	3.5505E-26	3.5327E-26	-1.78E-28
HOPOV	6.5448E-15	2.2816E-12	+2.275E-12
		Total Change	0

TABLE D.3-3

CONSEQUENCE CATEGORY FREQUENCIES (PER YEAR)

FOR LETDOWN ISOLATION RHR ISOLATED TREE

(INITIATING EVENT FREQUENCY

PRESENT CASE: 2.34E-1/yr

MODIFICATION CASE: 1.17E-1/yr)

Consequence Cateogry	Frequency Present Configuration	Frequency Modification Case	Net Change (+ or -)
SUCCESS	1.8212E-1	9.1062E-2	-9.1058E-2
LLFI	1.0908E-3	5.4542E-4	-5.4538E-4
LLCI	5.0386E-2	2.5193E-2	-2.5193E-2
LSFI	4.2379E-6	2.1190E-6	-2.1189E-6
LSCI	3.915E-4	1.9575E-4	-1.9575E-4
HLCI	3.510E-6	1.7550E-6	-1.7550E-6
HOPI	3.510E-21	1.7550E-21	-1.735E-21
		Total Change	-1.17E-1

TABLE D.3-4
CONSEQUENCE CATEGORY FREQUENCIES (PER YEAR)
FOR CHARGING/SI PUMP TREE
(INITIATING EVENT FREQUENCY = 1.01E-1/yr)

Consequence Cateogry	Frequency Present Configuration	Frequency Modification Case	Net Change (+ or -)
SUCCESS	7.6488E-2	7.6488E-2	0
LSFI	4.7269E-5	4.7269E-5	0
LLCI	2.1748E-3	2.1748E-3	0
MSCI	1.7133E-5	1.7133E-5	0
HLCI	2.5802E-7	2.5976E-7	-6E-11
HOPI	2.5802E-22	2.5796E-22	-6E-26
LSFO	2.5343E-3	2.5343E-3	0
LLFO	1.2885E-5	1.2885E-5	0
LLCO	1.9725E-2	1.9725E-2	0
MOPI	2.2420E-7	2.2408E-7	-1.20E-10
MSFO	4.6819E-13	1.7069E-11	1.66E-11
MSCO	4.4959E-12	1.6391E-10	1.594E-10
MSFI	4.9463E-10	4.9438E-10	-2.50E-13
HOPOV	5.8903E-15	2.0534E-12	2.048E-12
		Total Change	0

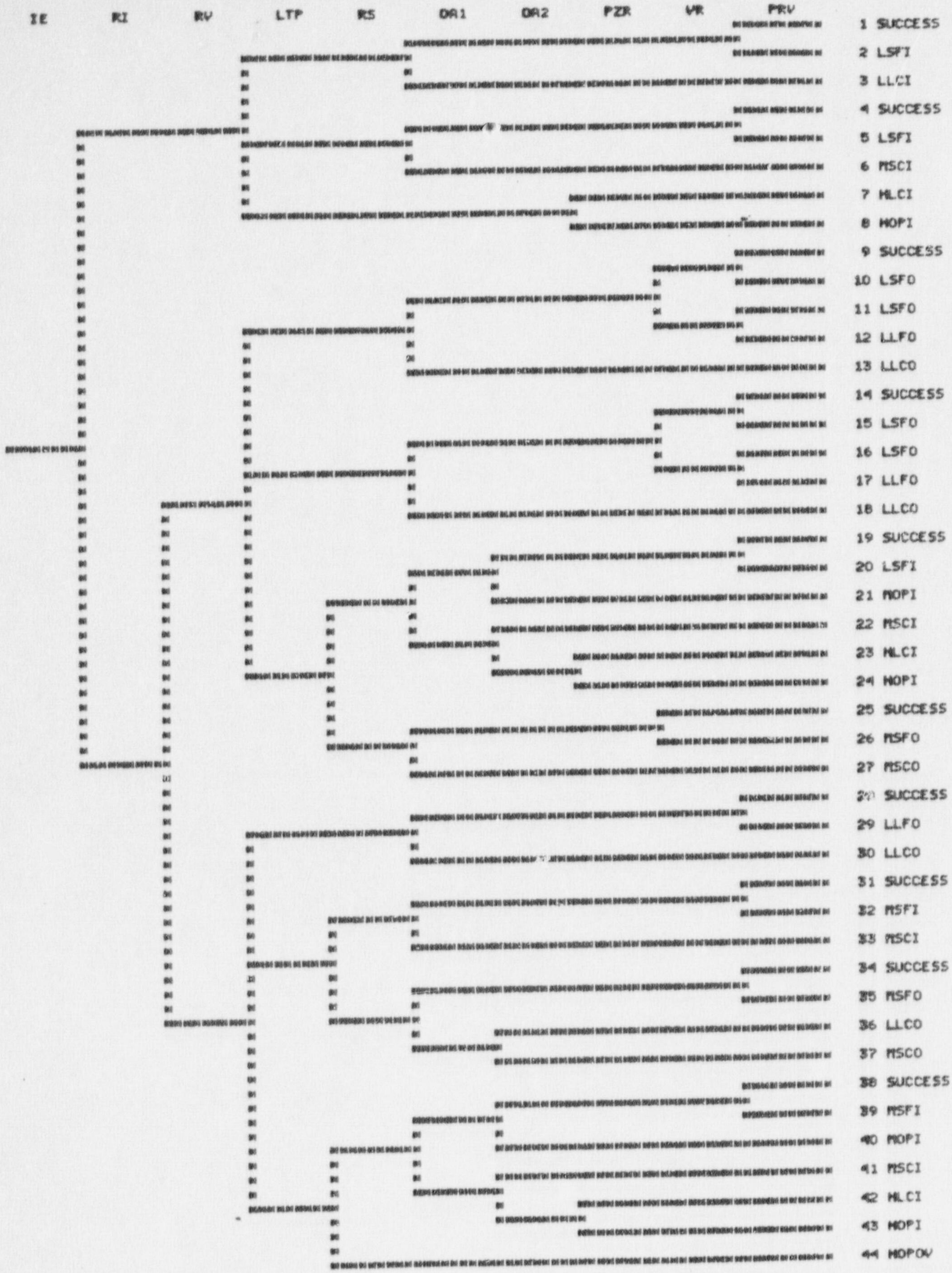


Figure D.3-1
Charging/Safety Injection Pump Actuation

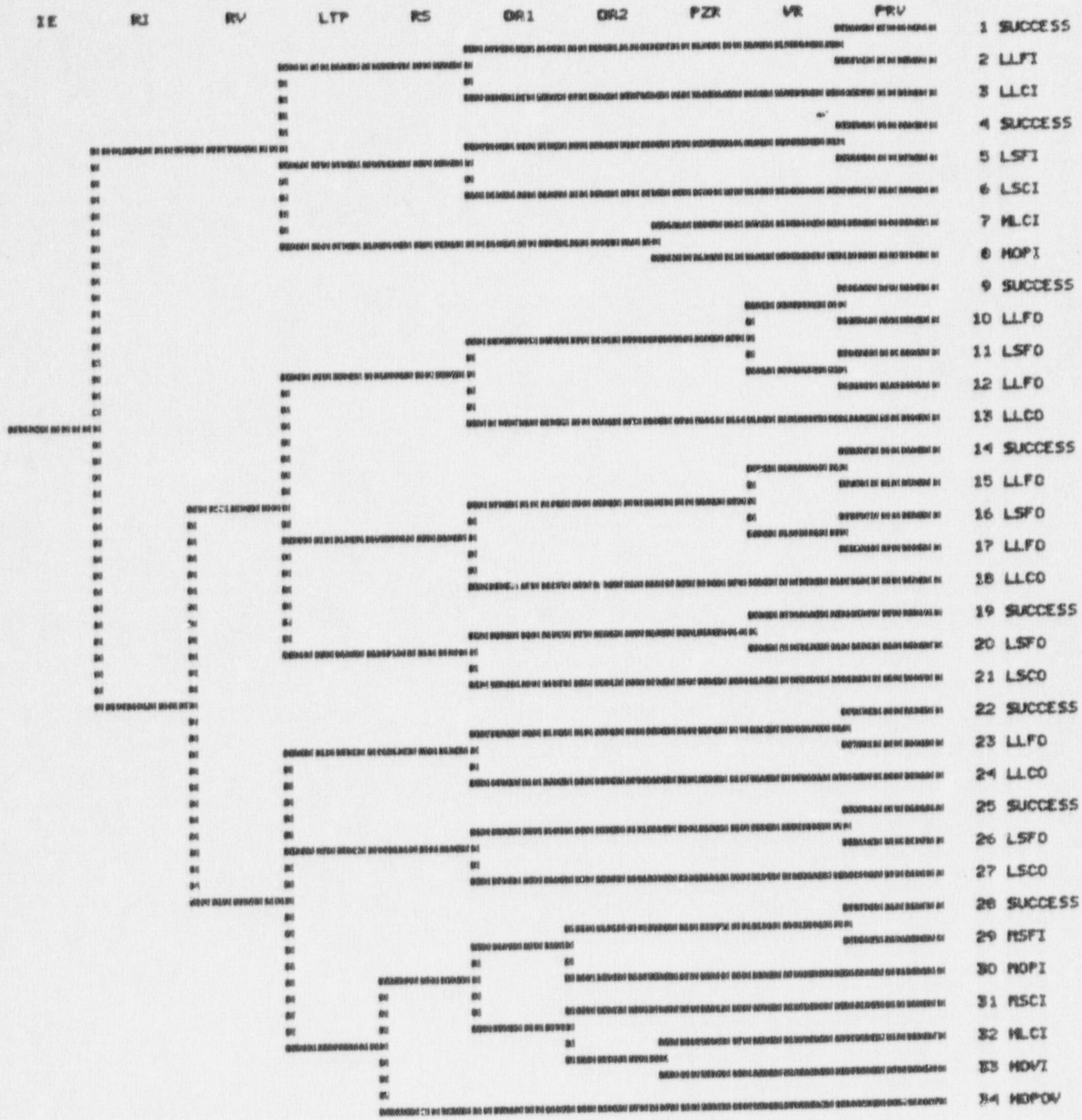


Figure D.3-2
Letdown Isolation - RHR Operable

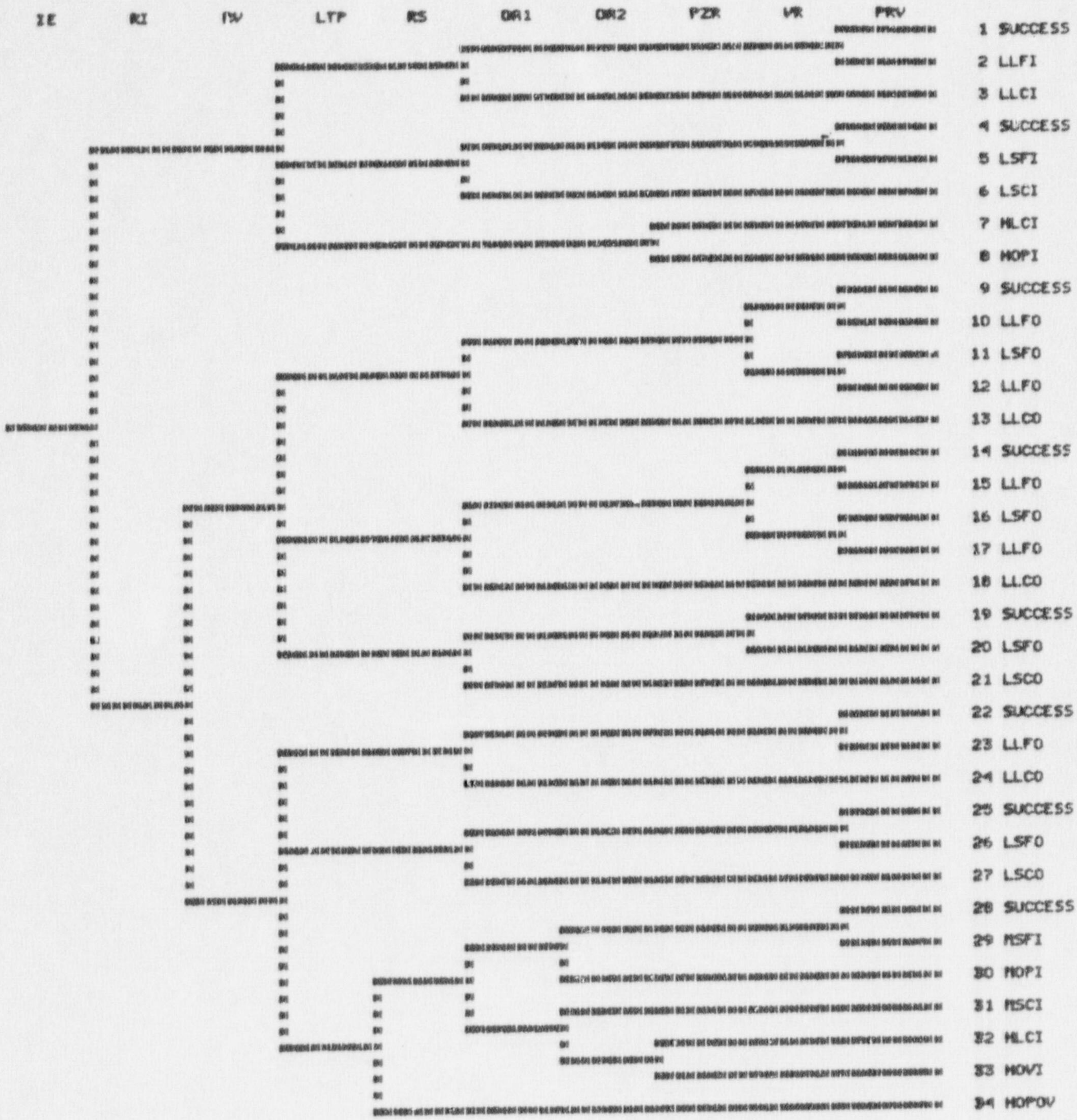
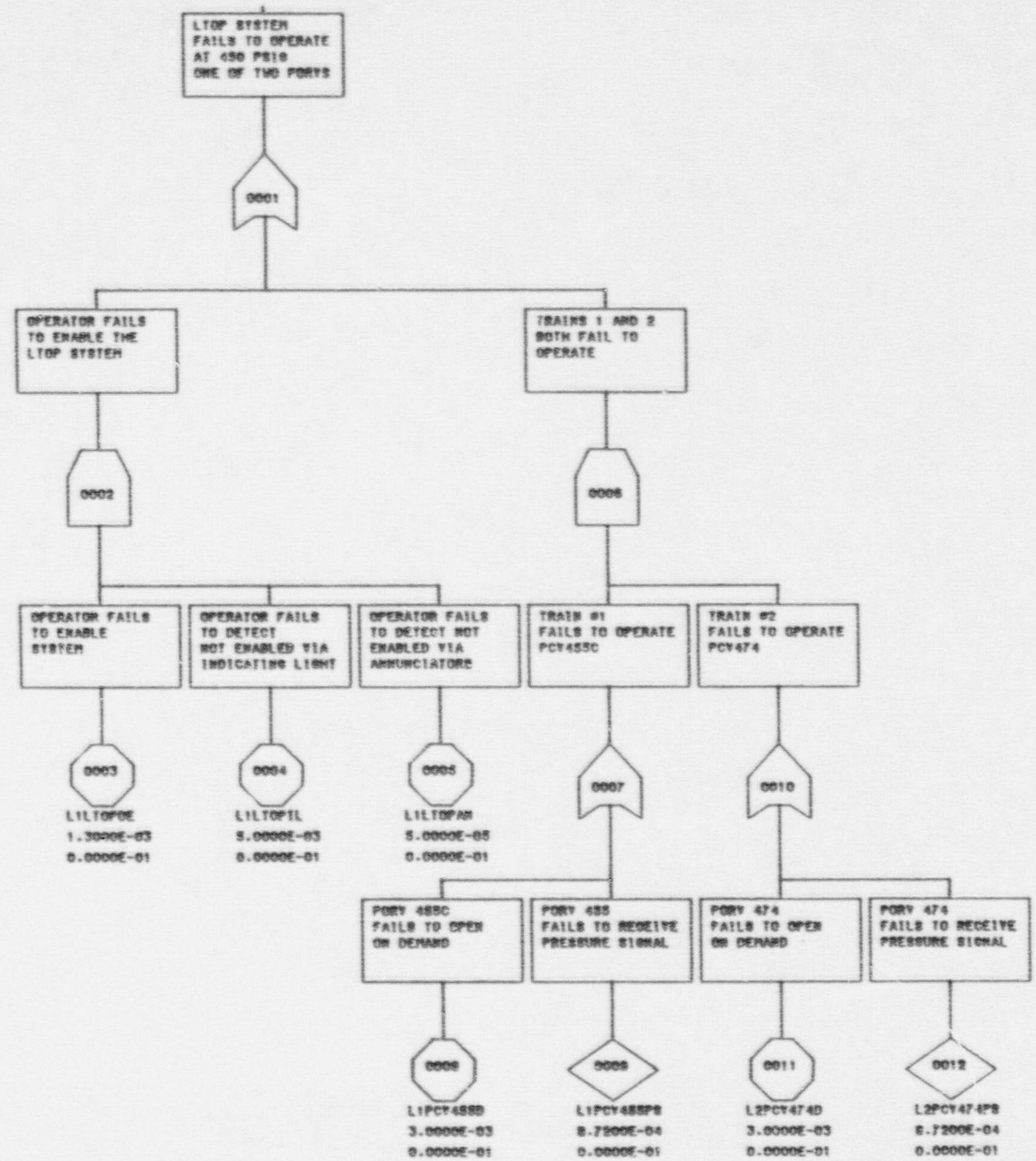


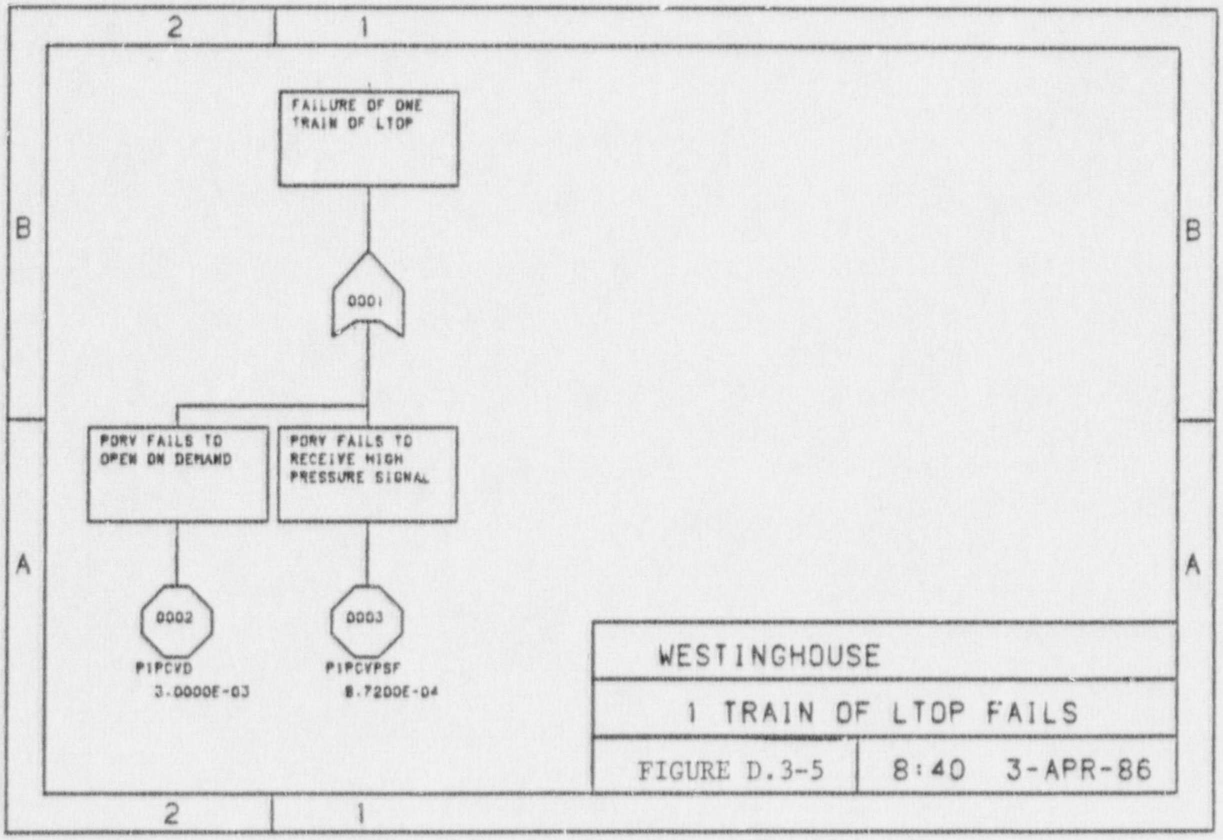
Figure D.3-3
Letdown Isolation - RHR Inoperable (Isolated)

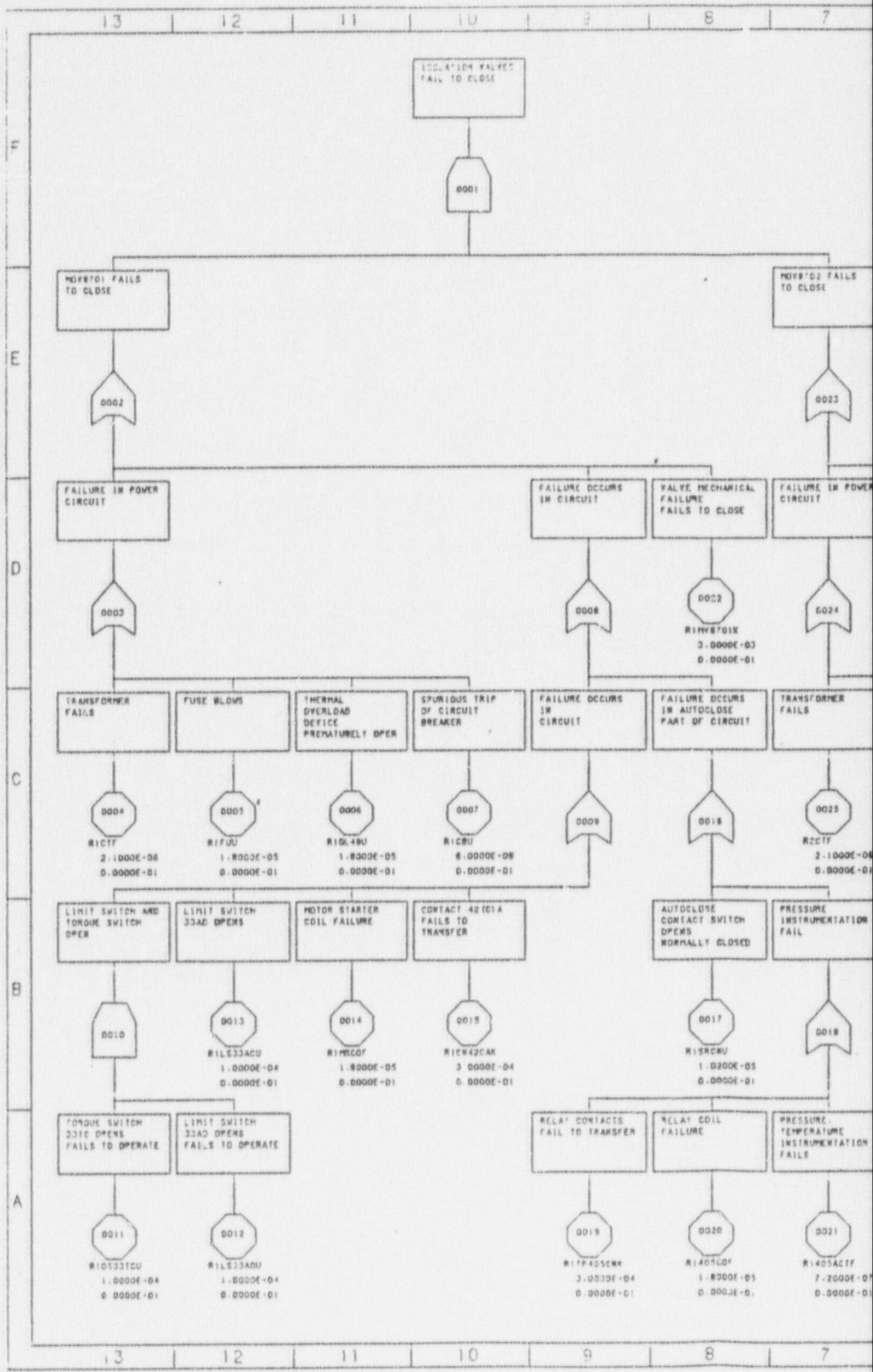


WESTINGHOUSE

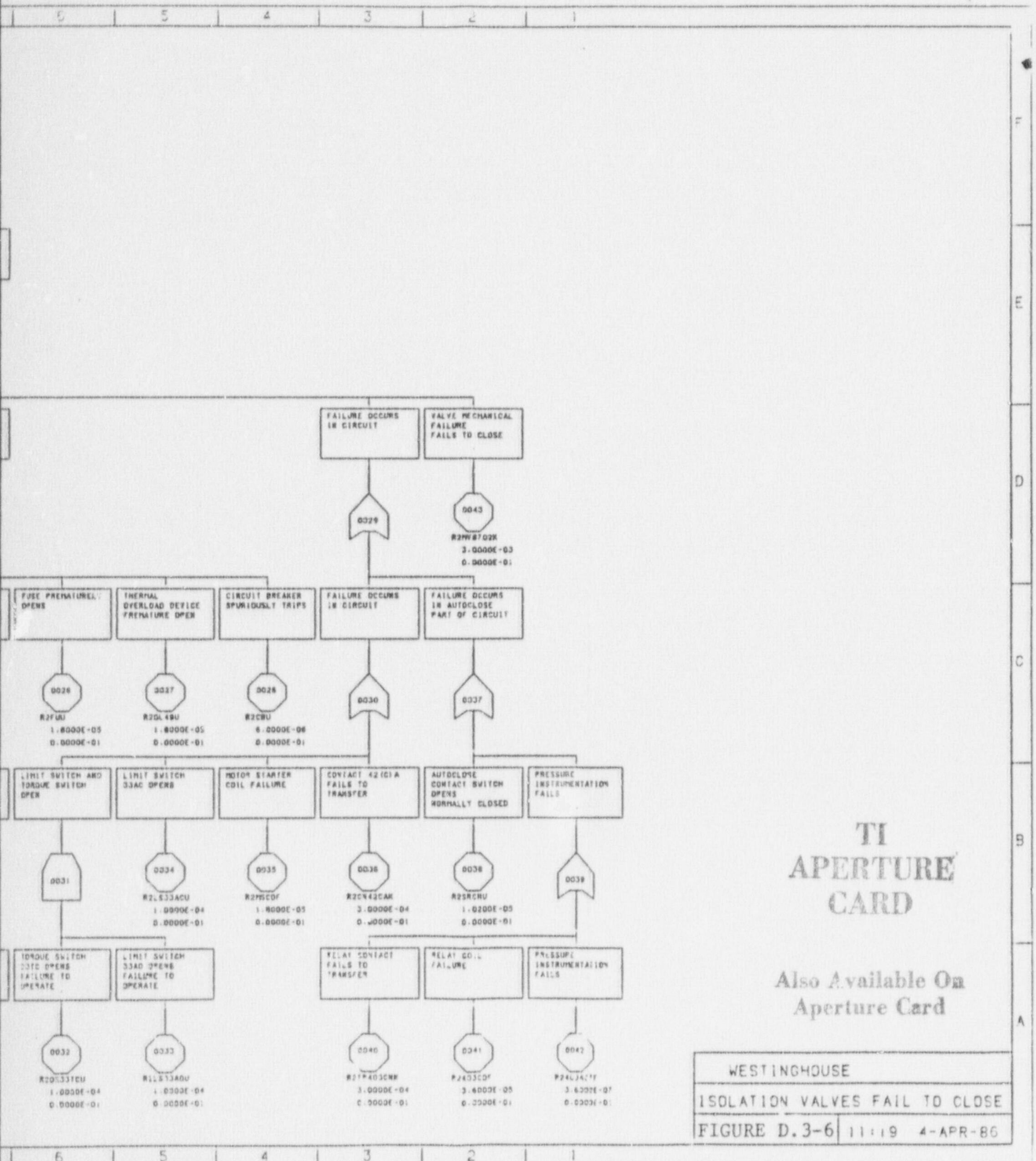
2 TRAINS OF LTOP FAIL

FIGURE D.3-4 | 9:36:19 86-11-20


2
1
B
A
FAILURE OF ONE TRAIN OF LTOP
0001
PORV FAILS TO OPEN ON DEMAND
PORV FAILS TO RECEIVE HIGH PRESSURE SIGNAL
0002
P1PCVD
3.0000E-03
0003
P1PCVPSF
8.7200E-04
WESTINGHOUSE
1 TRAIN OF LTOP FAILS
FIGURE D.3-5
8:40 3-APR-86



ISOLATION VALVES FAIL TO CLOSE
0001
MOV8701 FAILS TO CLOSE
MOV8702 FAILS TO CLOSE
0002
0023
FAILURE IN POWER CIRCUIT
FAILURE OCCURS IN CIRCUIT
VALVE MECHANICAL FAILURE FAILS TO CLOSE
FAILURE IN POWER CIRCUIT
0003
0008
0022
R1MV8701X
3.0000E-03
0.0000E-01
0024
TRANSFORMER FAILS
FUSE BLOWS
THERMAL OVERLOAD DEVICE PREMATURELY OPEN
SPURIOUS TRIP OF CIRCUIT BREAKER
FAILURE OCCURS IN CIRCUIT
FAILURE OCCURS IN AUTOCLOSE PART OF CIRCUIT
TRANSFORMER FAILS
0004
R1CTF
2.1000E-08
0.0000E-01
0005
R1FUU
1.8000E-05
0.0000E-01
0006
R1OL49U
1.8000E-05
0.0000E-01
0007
R1CBU
6.0000E-08
0.0000E-01
0009
0016
0025
R2CTF
2.1000E-08
0.0000E-01
LIMIT SWITCH AND TORQUE SWITCH OPEN
LIMIT SWITCH 33AD OPENS
MOTOR STARTER COIL FAILURE
CONTACT 42(O)A FAILS TO TRANSFER
AUTOCLOSE CONTACT SWITCH OPENS NORMALLY CLOSED
PRESSURE INSTRUMENTATION FAIL
0010
0013
R1LS33ACU
1.0000E-04
0.0000E-01
0014
R1MSCOF
1.8000E-05
0.0000E-01
0015
R1CN42CAK
3.0000E-04
0.0000E-01
0017
R1SRCNU
1.0200E-05
0.0000E-01
0018
TORQUE SWITCH 33TC OPENS FAILS TO OPERATE
LIMIT SWITCH 33AD OPENS FAILS TO OPERATE
RELAY CONTACTS FAIL TO TRANSFER
RELAY COIL FAILURE
PRESSURE-TEMPERATURE INSTRUMENTATION FAILS
0011
R1OS33TCU
1.0000E-04
0.0000E-01
0012
R1LS33ADU
1.0000E-04
0.0000E-01
0019
R1TP405CNK
3.0000E-04
0.0000E-01
0020
R1405COF
1.8000E-05
0.0000E-01
0021
R1405ACTF
7.2000E-07
0.0000E-01



WESTINGHOUSE

ISOLATION VALVES FAIL TO CLOSE

FIGURE D.3-6 11:19 4-APR-86

TI APERTURE CARD

Also Available On Aperture Card

8708110183-19