

---

---

# Review of the Shearon Harris Unit 1 Auxiliary Feedwater System Reliability Analysis

---

---

Prepared by  
A. Fresco, R. Youngblood, I.A. Papazoglou

Brookhaven National Laboratory

Prepared for  
U.S. Nuclear Regulatory  
Commission

8603100084 860228  
PDR ADOCK 05000400  
A PDR

## NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability of responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

## NOTICE

### Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.  
Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,  
Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda, NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices, Licensee Event Reports; vendor reports and correspondence; Commission papers, and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

# Review of the Shearon Harris Unit 1 Auxiliary Feedwater System Reliability Analysis

---

Manuscript Completed: August 1985  
Date Published: February 1986

Prepared by  
A. Fresco, R. Youngblood, I. A. Papazoglou

Brookhaven National Laboratory  
Department of Nuclear Energy  
Upton, NY 11973

Prepared for  
Division of Systems Integration  
Office of Nuclear Reactor Regulation  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555  
NRC FIN A3702

## ABSTRACT

This report presents the results of a review of the Auxiliary Feedwater System Reliability Analysis for the Shearon Harris Nuclear Power Plant (SHNPP) Unit 1. The objective of this report is to estimate the probability that the Auxiliary Feedwater System will fail to perform its mission for each of three different initiators: (1) loss of main feedwater with offsite power available, (2) loss of offsite power, (3) loss of all ac power except vital instrumentation and control 125-V dc/120-V ac power. The scope, methodology, and failure data are prescribed by NUREG-0611, Appendix III. The results are compared with those obtained in NUREG-0611 for other Westinghouse plants.

## TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT.....	iii
LIST OF FIGURES.....	vii
LIST OF TABLES.....	viii
EXECUTIVE SUMMARY.....	ix
1. INTRODUCTION.....	1
2. SCOPE OF BNL REVIEW.....	1
3. MISSION SUCCESS CRITERIA.....	2
4. SYSTEM DESCRIPTION.....	3
5. EMERGENCY OPERATION.....	3
5.1 Loss of Main Feedwater (LMFW).....	3
5.2 Loss of Offsite Power (LOOP).....	4
5.3 Loss of All ac (LOAC).....	4
6. TESTING.....	4
7. TECHNICAL SPECIFICATIONS.....	6
8. ASSUMPTIONS.....	6
8.1 Maintenance.....	6
8.2 Operator Errors.....	8
9. RELIABILITY ANALYSIS.....	8
9.1 Qualitative Aspects.....	8
9.1.1 Mode of System Initiation.....	8
9.1.2 System Control Following Initiation.....	9
9.1.3 Effects of Test and Maintenance Activities.....	10
9.1.4 Availability of Alternative Water Supplies.....	10
9.1.5 Adequacy and Separation of Power Sources.....	10
9.1.6 Single-Point Failures.....	11
9.1.7 Adequacy of Emergency Procedures.....	11
9.2 Quantitative Aspects.....	11
9.2.1 Applicant's Use of NRC-Suggested Methodology and Data..	11
9.2.1.1 Fault Tree Construction and Evaluation.....	11
9.2.1.2 Failure Data.....	13
9.2.2 Applicant's Results.....	13
9.2.2.1 System Unavailabilities.....	13
9.2.2.2 Dominant Failure Modes and Conclusions.....	13
9.2.3 BNL Assessment.....	14
9.2.3.1 Fault Trees.....	14
9.2.3.2 Failure Data.....	14
9.2.3.3 System Unavailabilities.....	15

## TABLE OF CONTENTS (Cont.)

	<u>Page</u>
9.2.3.4 Dominant Failure Modes.....	15
9.2.3.5 General Comparison with Other Plants.....	16
9.2.3.6 General Comments.....	16
REFERENCES.....	17
APPENDIX A: SHNPP FSAR Section 10.4.9 "Auxiliary Feedwater System".....	A-1
APPENDIX B: SHNPP FSAR Technical Specifications "Auxiliary Feedwater System and Condensate Storage Tank".....	B-1
APPENDIX C: "NRC-Supplied Data for Purposes of Conduction a Comparative Assessment of Existing AFWS Designs and Their Potential Reliabilities".....	C-1

## LIST OF FIGURES

<u>Figure</u>	<u>Title</u>	<u>Page</u>
1	Comparison of Reliability of the SHNPP AFWS with that of Other AFWS Designs in Plants using the Westinghouse NSSS.....	xi
FSAR 10.4.9A-1	Shearon Harris Nuclear Power Plant-Unit 1 Auxiliary Feedwater System Availability Study Simplified Flow Diagram.....	xii
2A	SHNPP Auxiliary Feedwater System BNL Results - Dominant Cut Sets - LMFW Case 1A - Applicant's Assumption: One Motor- Driven Pump Required.....	19
2B	SHNPP Auxiliary Feedwater System BNL Results - Dominant Cut Sets - LMFW Case 1B - BNL Assessment: Two Motor-Driven Pumps Required.....	21
3	SHNPP Auxiliary Feedwater System BNL Results - Dominant Cut Sets - LOOP Case 2.....	23
4	SHNPP Auxiliary Feedwater System BNL Results - Dominant Cut Sets - LOAC Case 3.....	25
FSAR 10.4.9A-1	Shearon Harris Nuclear Power Plant-Unit 1 Auxiliary Feedwater System Availability Study Simplified Flow Diagram.....	27
FSAR 10.4.9A-2	Shearon Harris Nuclear Power Plant-Unit 1 Auxiliary Feedwater System Availability Study Fault Tree-Loss of Main Feedwater (LMFW) and Loss of Offsite Power (LOOP) Cases.....	28

## LIST OF TABLES

<u>Table</u>	<u>Title</u>	<u>Page</u>
1	Unavailabilities of the SHNPP AFWS-Comparison of Applicant's Results with BNL Assessment.....	xiii
2	Comparison of Data Assumptions.....	33
3	Summary of Applicant's Dominant Failure Modes.....	36
4	Definition of Disallowed Test and Maintenance Acts...	37
5	Definition of Top Event for LMFW.....	38
6	Comparison of Results.....	40



## EXECUTIVE SUMMARY

After the accident at Three Mile Island, a study was done on the reliability of the Auxiliary Feedwater System (AFWS) of each then-operating plant with NSSS designed by Westinghouse. The results of that study were presented in NUREG-0611<sup>(1)</sup>. At the request of the NRC<sup>(2)</sup>, Carolina Power and Light Company, an operating license applicant, provided the NRC with a study of the Shearon Harris (SHNPP) Units 1 and 2 AFWS<sup>(3)</sup> that was done with NUREG-0611 used as a guideline. BNL has reviewed this study. The BNL conclusions are as follows ("High", "Medium", and "Low" refer to the NUREG-0611 reliability scale).

1. For an accident resulting in a loss of main feedwater (LMFW) with offsite power available:
  - a. Applicant's Case - Only one motor-driven pump (or the turbine driven pump) is required. The reliability of the AFWS is in the High range (Unavailability =  $9.2E-6$ /demand).
  - b. BNL Assessment - Both motor-driven pumps (or the turbine-driven pump) are required. The reliability of the AFWS is in the Medium range. (Unavailability =  $4.6E-4$ /demand).
2. For a loss of offsite power (LOOP) resulting in a concurrent loss of main feedwater (LMFW): The reliability of the AFWS is in the High range. (Unavailability =  $4.9E-5$  /demand). Only one motor-driven pump is required.
3. For a loss of all ac power (LOAC), except for the 125-V dc/120-V ac vital instrumentation and control power systems, resulting in a concurrent loss of main feedwater (LMFW): The reliability of the AFWS is in the Medium range. (Unavailability =  $2.5E-2$ /demand).

Results are summarized in Table 1. The SHNPP AFWS reliability is compared with that of other AFWS designs in Westinghouse plants in Figure 1.

#### General Comments

The following aspects of the AFWS should be highlighted:

##### 1. Pump Discharge Isolation Valves

Although there will be monthly verification that the manual suction isolation valves are open by virtue of the pump testing, it is stated in the SHNPP study<sup>(3)</sup> that the manual valves on the pumps' discharge headers will be closed to by-pass flow to the Condensate Storage Tank through the mini-flow circulation lines. Since no position indication for either the suction or the discharge valves appears in the Control Room, if one or more of the valves were left closed after a test, this situation would remain undetected until the next pump test. However, given 30 minutes before steam generator boil-dry, the operator should be able to determine by steam generator level indication

that the valves are closed and restore the valves to the open position, should this be necessary.

## 2. Turbine-Driven Pump (TDP) Dependence on Train B 125-V dc Power

The TDP is dependent upon Train B 125-V dc power, does not appear to be in conflict with any of the short-term or long-term recommendations of NUREG-0611, as discussed in Subsection 9.2.2.2. Loss of Train B 125-V dc power also incapacitates Motor Driven Pump B. Although consideration of loss of dc power does not appear to be within the scope of NUREG-0611, dc power is a significant shared support system, and, depending on the top event definition for LMFW, loss of Train B dc power may be a single failure.

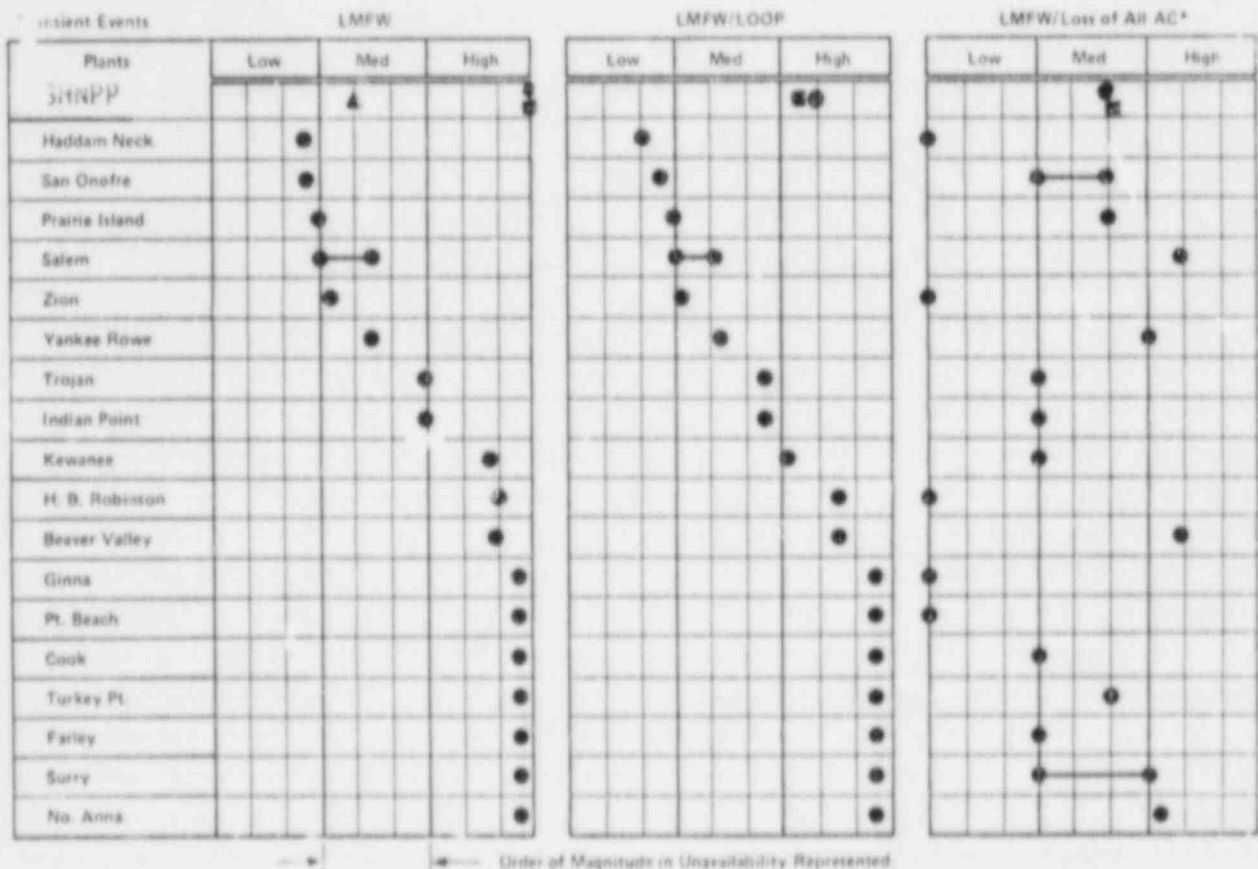
## 3. Flow Control With LOOP and Only One Diesel-Generator Available

As discussed in Subsection 9.1.2, upon LOOP, if Diesel-Generator A is unavailable, flow control of both motor-driven pumps cannot be directly accomplished because the corresponding flow control valves are dependent upon Train A ac power. Similarly, if Diesel Generator B is unavailable, flow control of the TDP cannot be directly accomplished because its flow control valves are dependent upon Train B ac power.

## 4. Test and Maintenance Policies

Because of the mixture of Train A and Train B power-operated valves on the pumps' discharge headers, confusion may result on the part of the plant operating personnel concerning which valves may or may not be tested or maintained concurrently with any one pump without a detailed statement of the correct policy. Such a policy has not been provided in this report.

There appears to be a contradiction concerning the test interval of the pumps. Ref. 3 states that pumps are to be tested quarterly but the Technical Specifications in Appendix B state that the testing is to be performed at least once every 31 days.



\*Note: The scale for this event is not the same as that for the LMFW and LMFW/LOOP

- Applicant's Results
- ▲ BNL Assessment - Case 1A
- BNL Assessment - Case 1B, 2, and 3

Figure 1 Comparison of reliability of the SHNPP AFWS with that of other AFWS designs in plants using the Westinghouse NSS5.

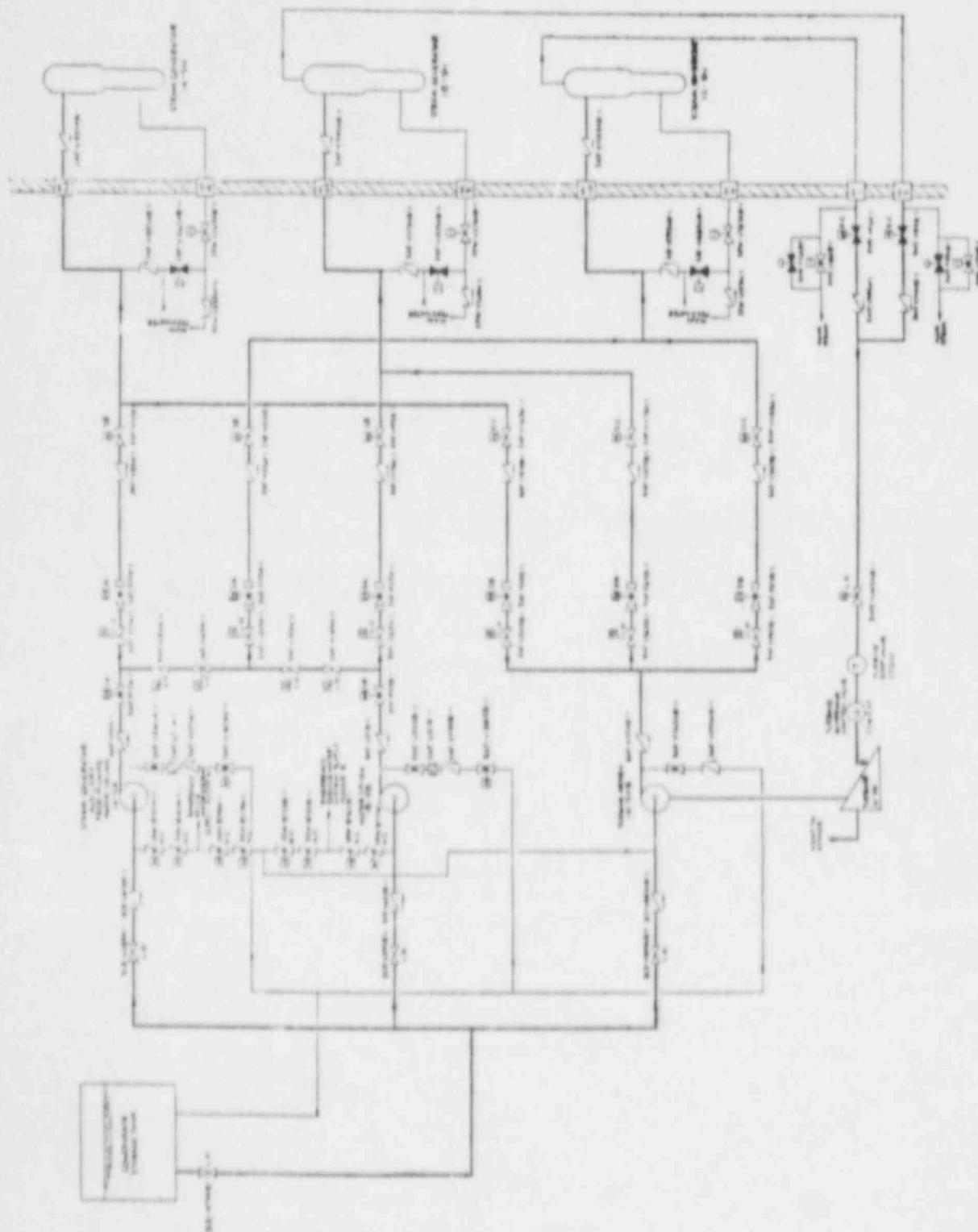


FIGURE 10-418-1. JACKSON HARRIS NUCLEAR POWER PLANT UNIT 1 SECONDARY FEEDWATER SYSTEM. AVAILABILITY STUDY SIMPLIFIED FLOW DIAGRAM

Table 1 Unavailabilities of the SHNPP AFWS -  
Comparison of Applicant's Results with  
BNL Assessment

Transient	APPLICANT'S RESULTS	BROOKHAVEN NATIONAL LABORATORY ASSESSMENT	
	Mission Success A	Mission Success A	Mission Success B
1. LMFW	6.6E-6	9.2E-6	4.6E-4
2. LOOP	6.1E-5	4.9E-5	--
3. LOAC	1.9E-2	2.5E-2	--

NOTE: Mission Success A refers to LMFW only, wherein a flow of 450 GPM from the turbine-driven pump or one of the motor-driven pumps is adequate (possible only if the mini-flow recirculation line is isolated).

Mission Success B refers also to LMFW only, wherein flow from both of the motor-driven pumps (or the turbine-driven pump) is required.

## 1. INTRODUCTION

This report is a review by Brookhaven National Laboratory (BNL) of the Shearon Harris Nuclear Power Plant (SHNPP) Final Safety Analysis Report (FSAR) Appendix 10.4.9A, entitled "Auxiliary Feedwater System Availability Analysis," prepared by Ebasco Services for Carolina Power and Light Company<sup>(3)</sup>.

After the accident at Three Mile Island, a study was done on the Auxiliary Feedwater Systems (AFWS) of all the then-operating plants. The results obtained for operating Westinghouse-designed plants were presented in NUREG-0611<sup>(1)</sup>. At that time, the objective was to compare AFWS designs; accordingly, generic failure probabilities were used in the analysis, rather than plant-specific data. Some of these generic data were presented in NUREG-0611. The probability that the AFWS would fail to perform its mission on demand was estimated for three initiating events:

- (a) loss of main feedwater (LMFW) without loss of offsite power;
- (b) loss of main feedwater associated with loss of offsite power (LOOP);
- (c) loss of main feedwater associated with loss of offsite and onsite ac (LOAC).

Since then, each applicant for an operating license has been required<sup>(2)</sup> to submit a reliability analysis of the plant's AFWS, carried out in a manner similar to that employed in the NUREG-0611 study. A quantitative criterion for AFWS reliability has been defined by the NRC in the current Standard Review Plan (SRP) for Auxiliary Feedwater Systems<sup>(4)</sup>:

"...An acceptable AFWS should have an unreliability in the range of  $10^{-4}$  to  $10^{-5}$  per demand based on an analysis using methods and data presented in NUREG-0611 and NUREG-0635. Compensating factors such as other methods of accomplishing the safety functions of the AFWS or other reliable methods for cooling the reactor core during abnormal conditions may be considered to justify a larger unavailability of the AFWS."

## 2. SCOPE OF BNL REVIEW

The BNL review has been conducted in accordance with the methodology, data, and scope of NUREG-0611, Appendix III<sup>(1)</sup>. It has two major objectives:

- (a) To evaluate the applicant's reliability analysis of the AFWS.

- (b) To provide an independent assessment, to the extent practical, of the AFWS unavailability.

Unavailability as used in this report has been defined as the "probability that the AFWS will not perform its mission on demand." The term unavailability is used interchangeably with unreliability. Specific goals of this review are then:

- (a) To compare the applicant's AFWS with that of the operating plants studied in NUREG-0611 by following the methodology of the latter as closely as possible.
- (b) To evaluate the applicant's AFWS with respect to the reliability goal set forth in SRP 10.4.9, i.e., that the AFWS has unreliability in the range of  $10^{-4}$  to  $10^{-5}$  per demand, by using the above methodology.

The NUREG-0611 methodology and the BNL review specifically exclude externally caused common-mode failures such as those due to earthquakes, tornados, floods, etc., and internal failures caused by pipe ruptures.

### 3. MISSION SUCCESS CRITERIA

The mission success criteria are described in Ref. 3. Portions are extracted below.

"The total flow rates required for at least two of three steam generators to provide adequate protection for the core have been established by Westinghouse and are as follows: (1) 475 GPM for LMFW, (2) 400 GPM for LMFW/LOOP, and (3) 380 GPM for LMFW/SB (Station Blackout equivalent to loss of all ac power).

The postulated top events are the failure of the AFWS to provide sufficient flow to at least two of the three steam generators (SGs) or less than 475, 400, 380 GPM total AFWS flow to less than two SGs for LMFW, LMFW/LOOP, or LMFW/SB, respectively.....

Consistent with the NRC request..., the scope of the top event spans only the availability of the system to start on demand for the three transients under consideration and does not include the reliability of the system to carry out this mission through the required duration (several hours)."

According to Table 10.4.9-1 of the FSAR (see Appendix A of this report), the capacity of each of the two motor-driven pumps is 450 GPM including 50 GPM for recirculation. Thus, the net capacity is only 400 GPM, so that two

motor-driven pumps appear to be required for LMFW. However, it is also stated in Appendix A that 380 GPM are required for:

- (a) LMFW with no offsite power available (LOOP),
- (b) Feedline rupture,
- (c) Steamline rupture,
- (d) Control room evacuation,
- (e) Loss of all ac power,
- (f) Loss of coolant accident (LOCA),

and that 500 GPM are required for loss of normal feedwater (LMFW). The reason for the difference is the application of more stringent and conservative acceptance criteria for Condition II events (e.g., loss of normal feedwater) than for Condition IV events (feedline rupture).

In addition, the applicant's fault trees shown in Figure 10.4.9A-2 of Ref. 3 appear to indicate that only one of the two motor-driven pumps (MDPs) is required for LMFW and LOOP. BNL has assumed that both of the MDPs are required for the LMFW case but only one for the LOOP case.

The time to boil the steam generators dry was not given in Appendix A. For purposes of calculating time available for operator action, BNL assumed this to be 30 minutes, based on NUREG-0611 information for other Westinghouse NSSS plants.

#### 4. SYSTEM DESCRIPTION

The BNL review of the AFWS reliability is based on the system as described in the SHNPP FSAR Section 10.4.9 currently on file in BNL's Nuclear Safety Library. This is provided as Appendix A of this report. The referenced flow diagrams have not been included in this report since the applicant has provided a simplified AFWS Flow Diagram (Figure 10.4.9A-1) in Ref. 3.

#### 5. EMERGENCY OPERATION

##### 5.1 Loss of Main Feedwater (LMFW)

Since offsite power is available, the two MDPs are started automatically upon loss of both Main Feedwater pumps. The pumps' flow is normally directed to the steam generators without any valve position changes required. The pumps' suction is supplied from the Condensate Storage Tank (CST) through a



single locked-open manual isolation valve 3CE-V27SAB-1. The alternative suction sources from the Emergency Service Water System (ESWS) Supply Headers are isolated from the AFWS pumps by several normally closed motor-operated valves. The transfer to these sources is manual and involves clearing the low suction pressure pump trips and opening the motor-operated isolation valves. In the event that one of the MDPs is unavailable, the applicant assumed that the net capacity of 400 GPM from the other MDP is inadequate to meet the stated flow requirements of 475 GPM. Therefore, it was assumed that the recirculation line to the CST must be isolated to increase the pump capacity to 450 GPM. However, this is still below the 475 GPM requirements stated in Ref. 3 (and the 500 GPM requirement stated in Appendix A). The apparent discrepancy between the modeling and the stated success requirements remains to be clarified.

The turbine-driven pump 1X-SB (TDP) must be manually started from the Control Room by opening the two normally closed, dc motor-operated Main Steam supply valves, 2MS-V9SA-1 and 2MS-V8SB-1. The Turbine Stop Valve and the Turbine Governing Control Valve are normally open.

## 5.2 Loss of Offsite Power (LOOP)

This case is identical to LMFW with the following exceptions:

- (a) The TDP is automatically started via dc power.
- (b) The MDPs are automatically started only after ac power becomes available, i.e., after startup and load sequencing of the two Emergency Diesel Generators.
- (c) The net capacity (400 GPM) of one MDP is assumed by the applicant to be sufficient to meet the flow requirements.

## 5.3 Loss of All ac (LOAC)

This case differs substantially from LMFW and LOOP in that only the TDP is available and it must be started manually from the Main Control Board (MCB) or the Auxiliary Control Panel (ACP) by opening the Main Steam Supply valves, 2MS-V9SA-1 or 2MS-V8SB-1. Also, only the CST is available as a suction source since the motor-operated isolation valves from the ESWS are ac powered.

## 6. TESTING

Although Ref. 3 states that system testing has no potential for causing common-mode system failures since there are no system tests which would simultaneously disable both system trains, the detailed application of this policy is not clearly identified for the valves on both the MDPs' common discharge header and the discharge header of the TDP. For example, if testing of the TDP or the Train B flow control valves on the discharge header is performed concurrently with testing of pressure control valve 3AF-P2SB-1 at

the outlet of MDPB, there would be no ostensible violation of the Technical Specifications (see Section 7.0) because all components, including the TDP, are on Train B only. Yet flow from both the TDP and MDPB would be blocked.

Therefore, BNL has assumed that no test (and/or maintenance) acts will be performed which will simultaneously block all flow to any one steam generator or block flow from more than one pump.

Ref. 3 states that final technical specifications and operating procedures are not yet available so that typical technical specifications and system operating procedures were used. As per Ref. 3, particular component information is as follows:

#### Pumps

The pumps are tested quarterly as per ASME Section XI, Subsection IWP. To perform the tests, the manual isolation valves downstream of the pumps are closed to allow flow back to the CST through the minimum flow recirculation line. Each pump is manually started from the control room. Although the pumps are operating during the test, they are unavailable to provide flow to the SGS. BNL has assumed that the test unavailability is all represented in the pumps although the manual isolation valves technically are all closed simultaneously. Also, the applicant's assumption of quarterly testing is in conflict with the SHNPP Technical Specifications provided in the FSAR which state that the tests are to be performed monthly (see Section 7). Therefore, BNL has assumed monthly testing.

In addition, Appendix A states that the pumps will be verified to start upon an Auxiliary Feedwater Actuation Signal (AFAS) at least once every 18 months (i.e., during refueling shutdown). This agrees with the technical specifications. Since this test is performed during shutdown, there is no contribution to AFWS unavailability.

#### Valves

Ref. 3 states that all motor or hydro-motor operated valves will be tested quarterly to the position required to fulfill their function, in accordance with ASME Section XI, Subsection IWV. However, because the test is brief, lasting only for the stroke time of the valve, valve unavailability due to test outage is very small, and was not included in the applicant's study. Although there is merit to the applicant's contention, BNL considers this to be in conflict with the NUREG-0611 requirements that 0.86 hours be assumed for valve testing. That value has been assumed in the BNL analysis.

Ref. 3 also states that each check valve subject to testing in accordance with ASME Section XI, Subsection IWV, can be tested during the testing of the pumps and power operated valves, and that if a system demand were to occur either during or after testing, the check valve would be returned to its proper position by the fluid forces of the system operation. Thus, it has been assumed that testing of the check valves does not contribute

to the system unavailability either by outage or by errors. BNL agrees with this assumption.

According to Ref. 3, monthly inspections are performed to verify that those valves in the flow path for the monthly pump tests are in the open position and, where applicable, are locked. Each manual valve is locked open, except the recirculation mini-flow lines. It should be noted that inspection of locked-open valves appears to exceed the requirements of the Standard Technical Specifications.

#### Control Circuits

Ref. 3 states that the quarterly ASME Section XI tests for pumps and power operated valves is also a control circuit test. Thus, BNL finds that there is no additional unavailability caused by control circuit testing.

#### Actuating Logic

It is beyond the scope of this review to verify the statement in Ref. 3 that, as demonstrated in FSAR Section 7.3, testing of the AFAS logic does not affect generation of the AFAS on demand and thus does not contribute to AFWS unavailability.

#### Diesel Generators

It is beyond the scope of this review to verify the statement in Ref. 3 that, as demonstrated in FSAR Section 8.3, testing of the diesel generators does not affect their ability to respond on demand, and thus does not contribute to AFWS unavailability.

### 7. TECHNICAL SPECIFICATIONS

The SHNPP technical specifications currently on file in BNL's Nuclear Safety Library are provided in Appendix B and have been used by BNL as reference material.

### 8. ASSUMPTIONS

#### 8.1 Maintenance

Although Ref. 3 states that system maintenance has no potential for causing common mode failures because plant procedures will prohibit maintenance which would simultaneously disable both system trains, the detailed application of this policy is not clearly identified. It is particularly obscure for the SHNPP system as evidenced by the location of both Train A and Train B valves on both the MDPs' common discharge header and the discharge header of the TDP (see Figure 10.4.9A-1). If maintenance of, for

example, MOV 2AF-V10SB-1 on the MDP line to SGA is required, there is no obvious reason not to allow maintenance on flow control valve 3AF-F1SA-1, even though each valve is on a different emergency bus.

Therefore, as stated previously in Section 6, BNL has assumed that no test or maintenance acts will be performed which will simultaneously block all flow to any one steam generator or block flow from more than one pump.

The applicant has made the following assumptions regarding maintenance in Ref. 3:

General

There is little or no incapacitating maintenance planned during plant operation unless a component fails to function during a periodic test. Some components cannot be repaired while the plant is in operation.

Specific

A. Pumps

$$Q_{\text{MAINT}} = \frac{0.22(\text{maint. acts/month}) \times 7(\text{hr/maint. act})}{720(\text{hr/month})} = 2.1 \times 10^{-3}/\text{demand}$$

However, BNL finds that since the SHNPP technical specifications (Appendix B) allow one of the pumps to be down for 72 hours, the proper maintenance outage time to assume according to NUREG-0611 is 19 hours, not 7 hours. This results in a pump maintenance unavailability of  $5.8 \times 10^{-3}/\text{demand}$ , which was used in the BNL analysis.

B. Valves

Maintenance unavailability was assumed for power-operated valves only, as follows:

$$Q_{\text{MAINT}} = \frac{0.22(\text{maint. acts/month}) \times 7(\text{hr/maint. act})}{720(\text{hr/month})} = 2.1 \times 10^{-3}/\text{demand}$$

Maintenance on valves requires isolation (by closing adjacent valves) of the valve being worked on, introducing the possibility that the valves used for isolation could be left in the closed position. This is accounted for in the (applicant's) analysis by assigning a probability that the affected valves are left in the closed position.

BNL finds that  $2.1 \times 10^{-3}/\text{demand}$  is the correct value for valve maintenance according to the analysis in NUREG-0611. With regard to the statement concerning isolation of other valves to allow maintenance on a particular power-operated valve, this is indeed true, but often the number and location of other valves that must be closed will severely restrict the flowpaths to the steam generators. To be correct, these simultaneous closures should be

modeled into the fault tree. However, since maintenance is assumed for power-operated valves only, it is assumed that all maintenance is such that closure of any other valve besides the affected valve is not required, i.e., maintenance is performed on the valve actuator and its associated components only, and not on the valve body or internal mechanism.

### C. Diesel Generators

The following maintenance unavailability for the diesel generators was assumed in Ref. 3:

$$Q_{\text{MAINT}} = \frac{0.22(\text{maint. acts/month}) \times 21(\text{hr/maint. act})}{720 (\text{hr/month})} = 6.4 \times 10^{-3} / \text{demand}$$

This is the correct value from NUREG-0611.

## 8.2 Operator Errors

According to Ref. 3, it was assumed that the operator did not correct component failures, except the following:

1. The operator is assumed to be available to back up the automatic actuation of the AFWS. Failure of the operator to back up system automatic level actuation signals has been factored into the fault tree as event HE1, and assigned an unavailability of  $5 \times 10^{-4}$ /demand.
2. The operator is assumed to be available to change the AFWS pumps' suction source, from the Main Control Board, to the backup ESWS source if the primary source (the CST) is unavailable. Failure of the operator to manually initiate backup ESWS has been factored into the fault tree as event HE2, and also assigned an unavailability of  $5 \times 10^{-4}$ /demand. This is the correct value from Table III-2 of NUREG-0611 for manual actuation of the AFWS from the Control Room considering a "dedicated" operator with 30 minutes available time to act (before steam generator boil-dry). This corresponds closely to the system under consideration.

## 9. RELIABILITY ANALYSIS

### 9.1 Qualitative Aspects

#### 9.1.1 Mode of System Initiation

1. LMFW. As stated in Section 5, both MDPs start automatically upon loss of both MFW pumps. Should the MDPs fail to start, the TDP will start automatically upon low-low level in any two steam generators. All three pumps can be manually started by the operator from the Control Room. Therefore, the applicant complies with Recommendation

GL-1 of NUREG-0611 that AFWS flow be automatically initiated using safety grade equipment and that manual start serve as a backup to automatic AFWS initiation.

2. LOOP. Both MDPs are automatically initiated once power is received from the diesel generators. The TDP is also automatically initiated. Should the LOOP signal fail to start the pumps, the MDPs will start upon low-low level in any one of the SGs and the TDP will start upon low-low level in any two of the SGs. All three pumps can again be manually started by the operator from the Control Room. Therefore, the applicant still complies with recommendation GL-1 mentioned above.
3. LOAC. In this case, only the TDP is available. It is automatically started upon the concurrent LOOP signal, as in the other two cases, by opening either or both of the dc-operated Main Steam Supply MOVs, 2MS-V9SA-1 and 2MS-V8SB-1.

The TDP is aligned to the CST, which is the sole suction source because the normally closed MOVs isolating the ESWS, the alternative suction source, are ac powered. Therefore, the applicant complies with Recommendation GL-3 of NUREG-0611 which states that at least one AFW pump and its associated flow path and essential instrumentation should automatically initiate AFW system flow and be capable of being operated independently of any ac power source for at least two hours.

#### 9.1.2 System Control Following Initiation

1. LMFW. SG level control is maintained by the operator manually modulating the appropriate flow control valves in the TDP and MDPs' supply lines. If for some reason the pump suction pressure decreases to the level which causes the pumps to trip, the operator would have to clear the pump trips on low suction pressure and open the motor-operated isolation valves on the connections to the ESWS.
2. LOOP. System control is basically the same as for LMFW. However, if Diesel Generator A is unavailable, the flow control valves on the common discharge header from both MDPA and MDPB (i.e., 3AF-F1SA-1, 3AF-F2SA-1, and 3AF-F3SA-1), would also become unavailable. This effectively prevents flow control on the MDP header even though MDPB itself is still available. One alternative possibility is to use the motor-operated isolation valves, 2AF-V10SB-1, 2AF-V23SB-1, and 2AF-V19SB-1 also on the MDP common discharge header. However, these valves may not have a means of partial opening or closing; if they are of fully open/fully closed design, it may be difficult to use them for flow control.

If Diesel Generator B is unavailable, flow from the TDP could not be modulated because the flow control valves 3AF-F5SB-1, 3AF-F5SB-1,

and 3AF-F6SB-1 also become unavailable. The situation is similar for the motor-operated isolation valves 2AF-V116SA-1, 2AF-V117SA-1, and 2AF-V118SA-1 as mentioned above.

Level control in such situations can still be roughly accomplished by alternately starting and stopping the appropriate pumps.

3. LOAC. Only the TDP is available and it is supplied from the CST. The alternative suction sources from the ESWS cannot be used because they are ac dependent. Under the conditions cited above, i.e., Diesel Generator B is unavailable, flow control via the flow control valves is difficult if not impossible. Level control can still be roughly accomplished by alternately starting and stopping the pump.

Although not shown on the Simplified Flow Diagram, Figure 10.4.9A-1, safety-grade flowmeters with Control Room indication and instrument channels powered from emergency busses have been provided to indicate flow to each steam generator. This appears to satisfy the requirements of Additional Short-Term Recommendation 5.3.3 of NUREG-0611.

#### 9.1.3 Effects of Test and Maintenance Activities

This subject was discussed in Sections 6 and 8.

#### 9.1.4 Availability of Alternative Water Supplies

The CST contains a minimum of 240,000 gallons dedicated for use in the AFWS. Transfer to the alternative ESWS supplies is performed manually from the Control Room as discussed previously. Specific emergency procedures for transferring to the ESWS supplies have not been provided in Ref. 3. The procedures should include criteria to inform the operators when, and in what order, the transfer to alternative water sources should take place, and should meet all other requirements described in Recommendation GS-4 of NUREG-0611. Ref. 3 does state that redundant level indicators in the Control Room for the AFWS primary water supply (the CST) allow the operator to anticipate the need to make up water or transfer to the alternative water supplies to prevent the occurrence of low pump suction pressure. It does not state whether redundant low level alarms are provided in the Control Room, or whether the low-low level of such alarms allows at least 20 minutes for operator action, as described in Additional Short-Term Recommendation 5.3.1 of NUREG-0611.

#### 9.1.5 Adequacy and Separation of Power Sources

Table 10.4.9A-2 of Ref. 3 states that the AFWS provides two independent and diverse sources of feedwater, a motor-driven train and a turbine-driven train. The two motor-driven pumps are powered from the ESF (Engineered Safeguard Features) electrical ac power distribution system. The turbine steam supply valves are dc motor-operated valves, one powered from the safety-related 125-V dc bus on Train A and the other on Train B. The Turbine Stop Valve (called the Trip and Throttle Valve in Appendix B) and the Turbine

Governing Control Valve can be operated only by Train B 125-V dc Power. See Table 10.4.9A-1 "Power Supplies."

#### 9.1.6 Single-Point Failures

Under the applicant's assumptions for mission success discussed in Section 3, BNL has not found any single-point failures, the closest situation being inadvertent closure of the manual isolation valve, 3CE-V27SAB-1, at the CST, causing all three pumps to trip upon low pressure. However, the ESWS alternative sources could be utilized unless the pump trips failed to actuate and the operator failed to act within the time available before pump damage could occur.

In contrast, in the BNL assessment, if two MDPs are required for LMFW, loss of Train B 125-V dc power becomes a single-point failure. This is further discussed in Subsections 9.2.3.4 and 9.2.3.6.

#### 9.1.7 Adequacy of Emergency Procedures

The applicant has not yet provided emergency procedures but should do so in the future.

### 9.2 Quantitative Aspects

#### 9.2.1 Applicant's Use of NRC-Suggested Methodology and Data

##### 9.2.1.1 Fault Tree Construction and Evaluation

The applicant describes the construction of his fault trees, Figure 10.4.9A-2, Sheets 1 to 5, in Ref. 3 as follows:

The fault trees were constructed from the FMEA (independent failure analysis) and the common cause failure analysis. The failures and combinations of failures that could defeat operation of the subsystem (including failures from other subsystems) were combined using conventional AND and OR gates. Then the subsystems were arranged through a logic which related them to the "top event" specified in Subsection 10.4.9A.2.1. This step was particularly complex for the AFS due to its extensive interconnection of redundant trains and the multiple ways in which it can successfully perform its function.

To simplify the fault tree, only the failure contributing component states (or events) from the FMEA, and not all possible causes of the state were incorporated into the fault tree. For example, if a valve being closed (unable to pass fluid) was a contributor in the fault tree, "VALVE XX CLOSED" was included as the event in the fault tree rather than placing an OR gate in the tree with event inputs such as "VALVE XX CLOSED DUE TO



MAINT", "VALVE XX CLOSED DUE TO ERROR", "VALVE XX PLUGGED WITH DEBRIS", etc. The latter would generate an unmanageable number of cut sets, and would produce a computer analysis output which focused on causes of concern as opposed to component of concern, which is more useful. The causes and probabilities of each event along with the rationale for their selection is listed in Subsection 10.4.9A.5.1.

A single fault tree including all components considered in the study was first generated. This fault tree represented the system under Case 2 and is given on Figure 10.4.9A-2. The Case 1 fault tree was then developed by applying the SETS FRMNEWFT procedure to the Case 2 fault tree with the PHI option to delete ac power failures (since offsite power is given to be present for this case) and by manually adding as a system failure the inability of the MDP recirculation lines to isolate when the only AFS pump available is a single MDP. The Case 3 fault tree was also developed by applying the FRMNEWFT procedure to the Case 2 fault tree, but using the OMEGA option to assure ac power failure.

Although the applicant states that the Form New Fault Tree procedure of SETS<sup>(5)</sup>, FRMNEWFT, was used to represent Case 1-LMFW, it seems clear from the results that still only one MDP was assumed to be required for this case. BNL has calculated the system unavailability for this assumption and also for the case in which two MDPs are required. The methodology and results are given in Section 9.2.3.

Also, although separation of all possible causes of a component failure into maintenance, human error, hardware failure, etc., produces a larger number of cut sets, we do not agree that focusing on the component of concern, rather than on the cause of concern, is more useful. To be able to identify what percentage of the total unavailability is caused by maintenance or testing seems to be more useful since the capability of focusing on which component is involved in the bulk of the cut sets is also retained. For comparison purposes, it is also important not to assess double and triple maintenance cut sets, which the applicant's method implicitly does.

Figure III-2 of NUREG-0611, "Simplified Fault Tree Logic Structure-LOFW Transient," shows independent failures separately from test and maintenance cut sets. Thus, the applicant's method differs substantially from the NUREG-0611 guidelines. In the BNL analysis, test and maintenance have been identified separately, as explained in Subsection 9.2.3.1 of this report.

The applicant's statement that the inability of the MDP recirculation lines to isolate when the only AFS pump available is a single MDP was manually added to the cut sets generated by the fault tree refers to the discussion of Mission Success Criteria in Section 3. If 475 GPM are assumed

to be required for LMFW and the net capacity of one MDP is 400 GPM, then isolation of the 50 GPM recirculation flow can increase the pump capacity only to 450 GPM. For this reason and the reasons discussed in Section 3, BNL has assumed that both MDPs are required for LMFW.

This matter is related to the definition of the top event, as explained in Table 10.4.9A-2 of Ref. 3, and the segment of the tree which defines "134 GPM to Each SG from MDPs" and "Exactly One MDP Available." If the applicant has assumed in effect that the flow from two MDPs, or one MDP with its recirculation flow line isolated, is required for mission success in the LMFW case, then the top event required differs from that shown in Figure 10.4.9A-2. The new top event can be created by adding "Failure of the Recirculation Line to be Isolated" as an AND gate with "Exactly One MDP Available."

#### 9.2.1.2 Failure Data

The applicant's failure data are shown in Table 10.4.9A-3 of Ref. 3. The data are in substantial agreement with the data prescribed in Table III-2 of NUREG-0611 (see Appendix C). The data assumptions by the applicant and by BNL are compared in Table 2. Note that many NUREG-0611 data correspond to values used in WASH-1400.<sup>(5)</sup>

#### 9.2.2 Applicant's Results

##### 9.2.2.1 System Unavailabilities

The applicant's results, which are described in Ref. 3, are the following:

The overall system failure probability was determined from the minimal cut sets using the SETS COMTRMVAL procedure. This uses the rare event approximation which neglects the intersection corrections of independent events. Since the probabilities of the basic event in the fault tree are small, the rare event approximation is valid for this study. The results are as follows:

TRANSIENT	$\bar{a}$
Case 1	$6.6 \times 10^{-6}$
Case 2	$6.1 \times 10^{-5}$
Case 3	$1.9 \times 10^{-2}$

BNL agrees that the rare event approximation is valid for this analysis.

##### 9.2.2.2 Dominant Failure Modes and Conclusions

The applicant's dominant cut sets are listed in Tables 10.4.9A-6, 10.4.9A-7, and 10.4.9A-8 of Ref. 3 for LMFW, LOOP, and LOAC respectively. The conclusions are summarized in Table 3.

In the case of LOOP, the reason for the large contribution, 13.1%, of the 2-element cut set, (6900-V ac "A") • (125-V dc "B"), is that the TDP is dependent upon 125-V dc power from Train "B". This is indicated in Table 10.4.9A-1 under "Power Supplies" where 125-V dc "B" is listed as the only source of power to valves 2MS-V8SB-1, TSV, and TGCV. According to Figure 10.4.9A-2, Sheet 4, the Turbine Stop Valve closes if, as a secondary failure, pump speed control is lost. This in turn is shown occurring if Train B 125-V dc power is lost. MDPB is also incapacitated upon loss of Train B 125-V dc power.

### 9.2.3 BNL Assessment

#### 9.2.3.1 Fault Trees

Since the applicant has not identified test or maintenance outages as separate inputs on the fault tree, BNL has approached the problem in the following manner.

First, each component which is subject to test or maintenance unavailability was identified on the fault tree. Then each of these components' basic failure events was converted to an OR gate consisting of the basic failure event, and the test and/or maintenance outages as inputs. The DELETE TERM option of the SETS program was then utilized to eliminate disallowed terms.

The underlying assumption in the test and maintenance policy is that any combination of simultaneous maintenance and/or test acts which shuts off all flow to any one steam generator or flow from more than one pump should be disallowed. The corresponding definition of DELETE TERM is shown in Table 4. It should be noted that the above definition does not preclude all simultaneous test and/or maintenance on Train A and Train B components. For example, maintenance on both the motor-operated isolation valve and the electrohydraulic motor-operated flow control valve in any one of the flow paths to the steam generators could be performed simultaneously even though one is a Train A component and the other is a Train B component.

As previously discussed in the LMFV case, BNL has checked the system unavailability for the case in which 400 GPM, which is the net flow rate from either MDP when mini-flow recirculation is accounted for, is sufficient for mission success. In effect, this means that one MDP is sufficient without isolation of the mini-flow recirculation line. This corresponds to the applicant's fault trees as presented in Ref. 3, using the PHI option of SETS to zero out ac power failures. The case where 500 GPM is required for LMFV as per FSAR 10.4.9 (see Appendix A), or effectively the flow from both MDPs, was also calculated. The comparative definitions of the two top events are shown in Table 5.

#### 9.2.3.2 Failure Data

A general comparison between the applicant's data and BNL's has already been shown in Table 2.

### 9.2.3.3 System Unavailabilities

The applicant's results and BNL's are compared in Table 6. Note that for LMFV, the system unavailability is much less than  $1 \times 10^{-4}$  / demand for the case of one MDP required but significantly exceeds  $1 \times 10^{-4}$  if two MDPs are required. This is to be expected because the cumulative unavailability of a two-train system, one of whose trains consists of two pumps, should be higher than that of not only the pure three-train system but also a two-train system in which each train consists of a single pump.

The probable reason why BNL's results for LOOP are slightly lower than the applicant's is that the effects of deleting disallowed test and maintenance acts for the LOOP case are magnified because of the large contribution from maintenance on the diesel-generators.

### 9.2.3.4 Dominant Failure Modes

#### 1. Case 1-LMFV.

A. One MDP Required. For this situation the dominant cut sets are failure of both suction sources by closure of valve 3CE-V27SAB-1 at the CST combined with human error in failing to transfer to the alternative ESWS supplies followed by failure of Train B 125-V dc power, incapacitating both the TDP and MDPB, in conjunction with various component failures which incapacitate MDPA. The next significant block of cut sets is spurious actuation of the steam generator line break isolation signals. Cut sets that involve maintenance of one of the pumps combined with component failures incapacitating both of the remaining two pumps are next in order (see Figure 2A).

B. Two MDPs Required. For this case, loss of Train B 125-V dc power is a single element cut set which eliminates both the TDP and MDPB. The next block of cut sets comprises the dual component type consisting of maintenance or test acts on the TDP or its associated valves combined with failures of MDPA or MDPB or conversely maintenance or test acts on MDPA or MDPB combined with failures of the TDP (see Figure 2B).

#### 2. Case 2 - LOOP.

The predominant cut sets are both double and triple type consisting of such failures as loss of Train B 125-V dc power combined with failure of DGA or test or maintenance acts on MDPA, maintenance on the TDP or its associated valves, and component failures of either diesel generator combined with failure of the opposite train pump. Also included is closure of valve 3CE-V27SAB-1 at the CST combined with human error in failing to transfer to the alternative ESWS supplies (see Figure 3).

#### 3. LOAC.

As expected, single-element cut sets predominate with the largest being maintenance on the TDP, followed by inadvertent closure of the manual

isolation valves in the pump suction line, maintenance on or component failures of the turbine stop valve or governing control valve, etc. (see Figure 4).

#### 9.2.3.5 General Comparison with Other Plants

The SHNPP AFWS design is similar to that of many other plants in that it consists of two motor-driven pumps and a third pump which is steam turbine driven. It appears to be fairly unusual in that both of its suction sources are safety-class design, i.e., the CST and the ESWS. The volume of water in the CST is sufficient to eliminate the need for any further operator actions to maintain suction supply subsequent to AFWS initiation. The ESWS serves merely as a backup source which should be required only in a rare event. It is also somewhat unusual in that low suction pressure trips are provided for all three pumps.

The two MDPs feed into a common discharge header which allows either pump to supply all three steam generators. The TDP has a separate header which supplies all three steam generators. The scheme for limiting AFWS flow to a steam generator undergoing depressurization does not restrict the flow of any pump to all three steam generators.

Depending upon what additional events accompany a LMFV transient, the flow from one MDP may not be sufficient. Therefore, in the SHNPP design, the motor-operated recirculation line isolation valve of each MDP is automatically isolated when the other MDP fails to start or run, as indicated by under voltage in the 6900-V ac emergency bus. This increases the flow of one MDP from 400 GPM to 450 GPM. The adequacy of this increased flow rate was discussed above in Section 3.

According to Ref. 3, the applicant will inspect locked-open manual valves during the monthly pump tests. This appears to exceed the requirements of the Standard Technical Specifications.

#### 9.2.3.6 General Comments

The following aspects of the AFWS should be highlighted:

##### 1. Pump Discharge Isolation Valves

Although there will be monthly verification that the manual suction isolation valves are open by virtue of the pump testing, it is stated in Ref. 3 that the manual valves on the pumps' discharge headers will be closed to by-pass flow to the CST through the mini-flow recirculation lines. Since no position indication for either the suction or the discharge valves appears in the Control Room, if one or more of the valves were left closed after a test, this situation would remain undetected until the next pump test. However, given 30 minutes before steam generator boil-dry, the operator should be able to determine by steam generator level indication that the valves are closed and restore the valves to the open position, should this be necessary.

## 2. Turbine-Driven Pump Dependence on Train B 125-V dc Power

The TDP is dependent upon Train B 125-V dc power, but this does not appear to be in conflict with any of the short-term or long-term recommendations of NUREG-0611, as discussed in Subsection 9.2.2.2. Loss of Train B 125-V dc power also incapacitates MDPB. Although consideration of loss of dc power does not appear to be within the scope of NUREG-0611, dc power is a significant shared support system, and depending on the top event definition for LMFWR, loss of Train B dc power may be a single failure.

## 3. Flow Control With LOOP and Only One Diesel-Generator Available

As discussed in Subsection 9.1.2, upon LOOP, if Diesel Generator A is unavailable, flow control of both MDPs cannot be directly accomplished because the corresponding flow control valves are dependent upon Train A ac power. Similarly, if Diesel Generator B is unavailable, flow control of the TDP cannot be directly accomplished because its flow control valves are dependent upon Train B ac power.

## 4. Test and Maintenance Policies

Because of the mixture of Train A and Train B power-operated valves on the pumps' discharge headers, confusion may result on the part of the plant operating personnel concerning which valves may or may not be tested or maintained concurrently with any one pump without a detailed statement of the correct policy. Such a policy has not been provided in this report.

There appears to be a contradiction concerning the test interval of the pumps. Ref. 3 states that pumps are to be tested quarterly but the Technical Specifications in Appendix B state that the testing is to be performed at least once every 31 days.

## REFERENCES

1. "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse Designed Operating Plants," NUREG-0611, U.S. NRC (January, 1980).
2. Letter from D.F. Ross, Jr., U.S. NRC, to All Pending Operating License Applicants of Nuclear Steam Supply Systems Designed by Westinghouse and Combustion Engineering (March 10, 1980).
3. "Auxiliary Feedwater System Availability Analysis," SHNPP FSAR Appendix 10.4.9A (April 18, 1983).
4. "Auxiliary Feedwater System (PWR)," U.S. NRC Standard Review Plan 10.4.9, Rev.-2, NUREG-0800 (July, 1981).

5. Worrell, Richard B. and Stack, Desmond W., "A SETS Users Manual for the Fault Tree Analyst," NUREG/CR-0465 (November, 1978).
6. "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants - Appendices 3 and 4: Failure Data," U.S. NRC, WASH-1400 (NUREG 75/014) (October, 1975).

~~LMFW =~~

<del>1</del>	<del>2.5900E-06</del>	<del>HE2 * MIV37SAGC +</del>
<del>2</del>	<del>1.2760E-06</del>	<del>MOPAMO * 125VDCBF +</del>
<del>3</del>	<del>1.1220E-06</del>	<del>125VDCBF * MOPSAF +</del>
<del>4</del>	<del>4.6900E-07</del>	<del>MPOVPISA * 125VDCBF +</del>
5	4.4000E-07	TAMCPA * 125VDCSF +
6	2.4200E-07	MIV5SAG * 125VDCBF +
7	2.4200E-07	MIV6SAG * 125VDCBF +
8	1.5086E-07	TOPMO * MCPSAF * MOPBSF +
9	1.3200E-07	POVPISA * 125VDCBF +
10	5.4621E-08	MATSV * MCPSAF * MOPBSF +
11	5.4621E-08	MATGCV * MOPSAF * MOPBSF +
12	5.2900E-08	LBIS1AAF * LBIS1CAF +
13	5.2900E-08	LBIS1ABF * LBIS1CAF +
14	5.2900E-08	LBIS1BAF * LBIS1CBF +
15	5.2900E-08	LEIS1BBF * LBIS1CBF +
16	5.2900E-08	LBIS1AAF * LBIS1CBF +
17	5.2900E-08	LEIS1ABF * LBIS1CBF +
18	5.2900E-08	LBIS1AAF * LBIS1BAF +
19	5.2900E-08	LBIS1AAF * LBIS1BBF +
20	5.2900E-08	LBIS1ABF * LBIS1BAF +
21	5.2900E-08	LEIS1ABF * LBIS1BBF +
22	5.2900E-08	LBIS1BAF * LBIS1CAF +
23	5.2900E-08	LEIS1BBF * LBIS1CAF +
24	5.2020E-08	TATOP * MOPSAF * MOPBSF +

Figure 2A SHNPP Auxiliary Feedwater System BNL Results - Dominant Cut sets -  
LMFW Case 1A - Applicant's Assumption: One Motor-Driven Pump Required  
(Sheet 1 of 2)



25	4.8400E-08	125VDCBF * 125VDCAF +
26	3.2538E-08	MOPBMO * MIV14SABC * MOPSAF +
27	3.2538E-08	MOPAMO * MIV14SABC * MOPBSF +
28	3.2538E-08	TDFMO * MIV14SAC * MOPSAF +
29	3.2538E-08	TDFMO * MIV15SAC * MOPSAF +
30	3.2538E-08	TDFMO * MIV6SAC * MOPBSF +
31	3.2538E-08	TDFMO * MIV5SAC * MOPBSF +
32	2.9580E-08	MOPBMO * TDPSABF * MOPSAF +
33	2.9580E-08	MOPAMO * TDPSABF * MOPBSF +
34	2.8611E-08	MIV14SABC * MOPSAF * MOPBSF +
35	2.6010E-08	TDPSABF * MOPSAF * MOPBSF +
36	2.3000E-08	LEIS1ABF * CV155SABFC +
37	2.3000E-08	CV153SABFC * LBIS1BAF +
38	2.3000E-08	CV153SABFC * LBIS1CBF +
39	2.3000E-08	CV153SABFC * LBIS1BBF +
40	2.3000E-08	LBIS1ABF * CV154SABFC +
41	2.3000E-08	CV154SABFC * LBIS1CBF +
42	2.3000E-08	CV154SABFC * LBIS1CAF +
43	2.3000E-08	LBIS1AAF * CV155SABFC +
44	2.3000E-08	LBIS1AAF * CV154SABFC +
45	2.3000E-08	CV153SABFC * LBIS1CAF +
46	2.3000E-08	LBIS1BAF * CV155SABFC +
47	2.3000E-08	LEIS1BBF * CV155SABFC +
48	2.2000E-08	CV1SAFC * 125VDCBF +

Figure 2A (Cont.) (Sheet 2 of 2)

TRUNKDEL =		
1	2.2000E-04	125VDCBF +
2	2.9580E-05	TOPMO * MDP3SF +
3	2.9580E-05	TOPMO * MDP3AF +
4	1.0710E-05	MATSV * MDP3SF +
5	1.0710E-05	MATGCV * MDP3SF +
6	1.0710E-05	MATSV * MDP3AF +
7	1.0710E-05	MATGCV * MDP3AF +
8	1.0200E-05	TATDP * MDP3SF +
9	1.0200E-05	TATDP * MDP3AF +
10	6.3800E-06	MDP3MO * MIV14SA3C +
11	6.3800E-06	MDP3MO * MIV14SA3C +
12	5.8000E-06	MDP3MO * TOP3AF +
13	5.3000E-06	MDP3MO * TOP3AF +
14	5.6100E-06	MDP3SF * MIV14SA3C +
15	5.6100E-06	MDP3AF * MIV14SA3C +
16	5.1000E-06	MDP3SF * TOP3AF +
17	5.1000E-06	MDP3AF * TOP3AF +
18	3.4800E-06	TOPMO * PCVP1SAC +
19	3.4800E-06	TOPMO * PCVP2SBC +
20	2.5500E-06	HE2 * MIV27SABC +
21	2.3100E-06	MAPCV2S3 * MIV14SA3C +
22	2.3100E-06	MAPCV1SA * MIV14SABC +
23	2.2000E-06	TAMDPB * MIV14SA3C +
24	2.2000E-06	TAMOPA * MIV14SA3C +

Figure 2B SHNPP Auxiliary Feedwater System BNL Results Dominant Cut sets - LMFV Case 1B - BNL Assessment: Two Motor-Driven Pumps Required (Sheet 1 of 2)

23	2.2000E-06	TAMOPB * MIV14SA3C +
24	2.2000E-06	TAMOPA * MIV14SA3C +
25	2.1000E-06	MAPCVP2S3 * TOPSA3F +
26	2.1000E-06	MAPCVP1SA * TOPSA3F +
27	2.0000E-06	TAMOPB * TOPSA3F +
28	2.0000E-06	TAMOPA * TOPSA3F +
29	1.3340E-06	MOPB40 * TSVS3C +
30	1.3340E-06	MOPA40 * TSVS3C +
31	1.2760E-06	TOP40 * 125V0CAF +
32	1.2600E-06	MATSV * PCVP1SAC +
33	1.2600E-06	MATGV * PCVP1SAC +
34	1.2600E-06	MATSV * PCVP2S3C +
35	1.2600E-06	MATGV * PCVP2S3C +
36	1.2000E-06	TATOP * PCVP1SAC +
37	1.2000E-06	TATOP * PCVP2S3C +
38	1.1730E-06	MOPBSF * TSVS3C +
39	1.1730E-06	MOPSAF * TSVS3C +
40	1.1220E-06	125V0CAF * M540V3S3C +

LOOP =

1	6.6000E-06	DGAF * 125VDCBF *
2	5.2200E-06	TOPMO * DGAF * DGBF *
3	4.5900E-06	DGAF * DGBF * MIV27SABC *
4	4.5900E-06	DGAF * DGBF * MIV30SABC *
5	2.5500E-06	HEZ * MIV27SABC *
6	1.8900E-06	MATSV * DGAF * DGBF *
7	1.8900E-06	MATGCV * DGAF * DGBF *
8	1.8000E-06	TATDP * DGAF * DGBF *
9	1.2760E-06	MDPAMO * 125VDCBF *
10	1.1220E-06	125VDCBF * MDPSAF *
11	9.9000E-07	DGAF * DGBF * MIV14SABC *
12	9.0000E-07	DGAF * DGBF * TDPSABF *
13	8.8740E-07	TDPMO * DGAF * MDPBSF *
14	8.8740E-07	TDPMO * DGBF * MDPSAF *
15	4.6200E-07	MAPCVPIA * 125VDCBF *
16	4.4000E-07	TAMOPA * 125VDCBF *
17	3.2130E-07	MATSV * DGAF * MDPBSF *
18	3.2130E-07	MATGCV * DGAF * MDPBSF *
19	3.2130E-07	MATSV * DGBF * MDPSAF *
20	3.2130E-07	MATGCV * DGBF * MDPSAF *
21	3.0600E-07	TATDP * DGAF * MDPBSF *
22	3.0600E-07	TATDP * DGBF * MDPSAF *

Figure 3 SHNPP Auxiliary Feedwater System BNL Results - Dominant Cut sets - LOOP - Case 2 (Sheet 1 of 2)

23	2.4200E-07	MIV6SAC * 125VDCBF *
24	2.4200E-07	MIV5SAC * 125VDCBF *
25	2.0700E-07	DGAF * DGRF * TSVSRC *
26	1.9140E-07	MDPBM0 * DGAF * MIV14SABC *
27	1.9140E-07	TDPMO * MIV14SAC * DGAF *
28	1.9140E-07	TDPMO * MIV15SAC * DGAF *
29	1.9140E-07	TDPMO * MIV6SAC * DGRF *
30	1.9140E-07	TDPMO * MIV5SAC * DGRF *
31	1.9140E-07	MDPAMO * DGRF * MIV14SABC *
32	1.7400E-07	MDPRMO * DGAF * TDPSABF *
33	1.7400E-07	MDPAMO * DGBF * TDPSABF *
34	1.6830E-07	DGAF * MIV14SABC * MDPRSF *
35	1.6830E-07	DGBF * MIV14SABC * MDPSAF *
36	1.5300E-07	DGAF * TDPSABF * MDPRSF *
37	1.5300E-07	DGBF * TDPSABF * MDPSAF *
38	1.5300E-07	DGAF * DGBF * TGCVSRC *
39	1.5086E-07	TDPMO * MDPSAF * MDPBSF *
40	1.4080E-07	MADGA * 125VDCBF *
41	1.3200E-07	PCVP1SAC * 125VDCBF *
42	1.1016E-07	DGAF * 480VACTBF * MIV27SABC *
43	1.1016E-07	480VACTAF * DGBF * MIV27SABC *
44	1.0440E-07	TDPMO * PCVP2S9C * DGAF *
45	1.0440E-07	TDPMO * PCVP1SAC * DGBF *

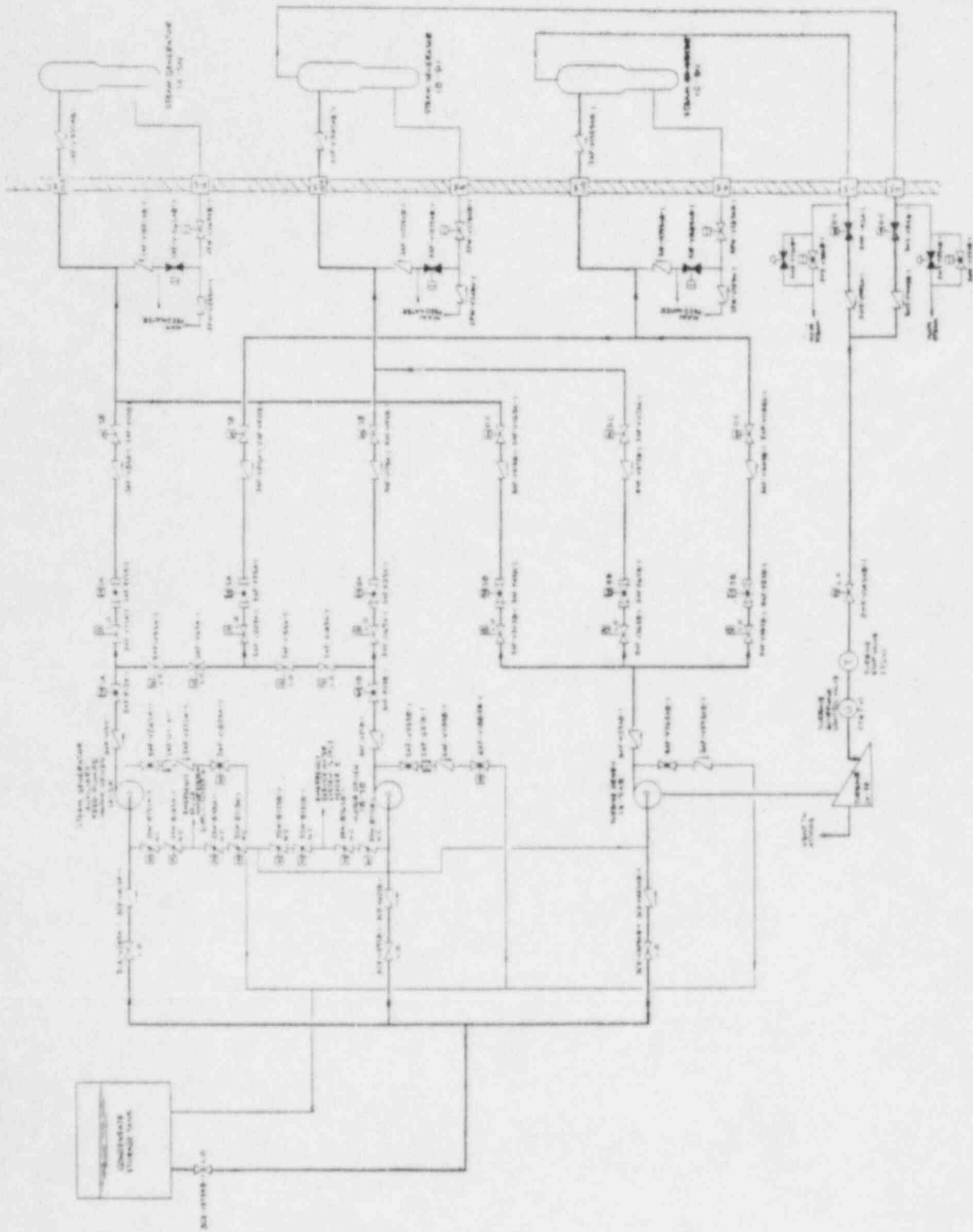
Figure 3 (Cont.) (Sheet 2 of 2)

LOAD =		
1	5.8000E-03	TOPMO +
2	5.1000E-03	MIV27SA3C +
3	5.1000E-03	MIV30SA3C +
4	2.1000E-03	MATSV +
5	2.1000E-03	MATGCV +
6	2.0000E-03	TATDP +
7	1.1000E-03	MIV14SA3C +
8	1.0000E-03	TOPSA3F +
9	2.3000E-04	TSV33C +
10	2.2000E-04	125V03BF +
11	1.7000E-04	TGCVS3C +
12	1.0000E-04	CV43SA3FC +
13	1.0000E-04	CV3SA3FC +
14	2.6010E-05	MSM0V9SAC * MSM0V3S3C +
15	1.0710E-05	MAHSM0V9SA * MSM0V8S3C +
16	1.0710E-05	MAHSM0V9S3 * MSM0V9SAC +
17	4.4100E-06	MAHSM0V9SA * MAHSM0V8S3 +
18	4.4100E-06	MAFCVF5S3 * MAFCVF5S3 +
19	4.4100E-06	MAH0V117SA * MAFCVF5S3 +

Figure 4 SHNPP Auxiliary Feedwater System BNL Results - Dominant Cut sets - LOAC - Case 3 (Sheet 1 of 2)

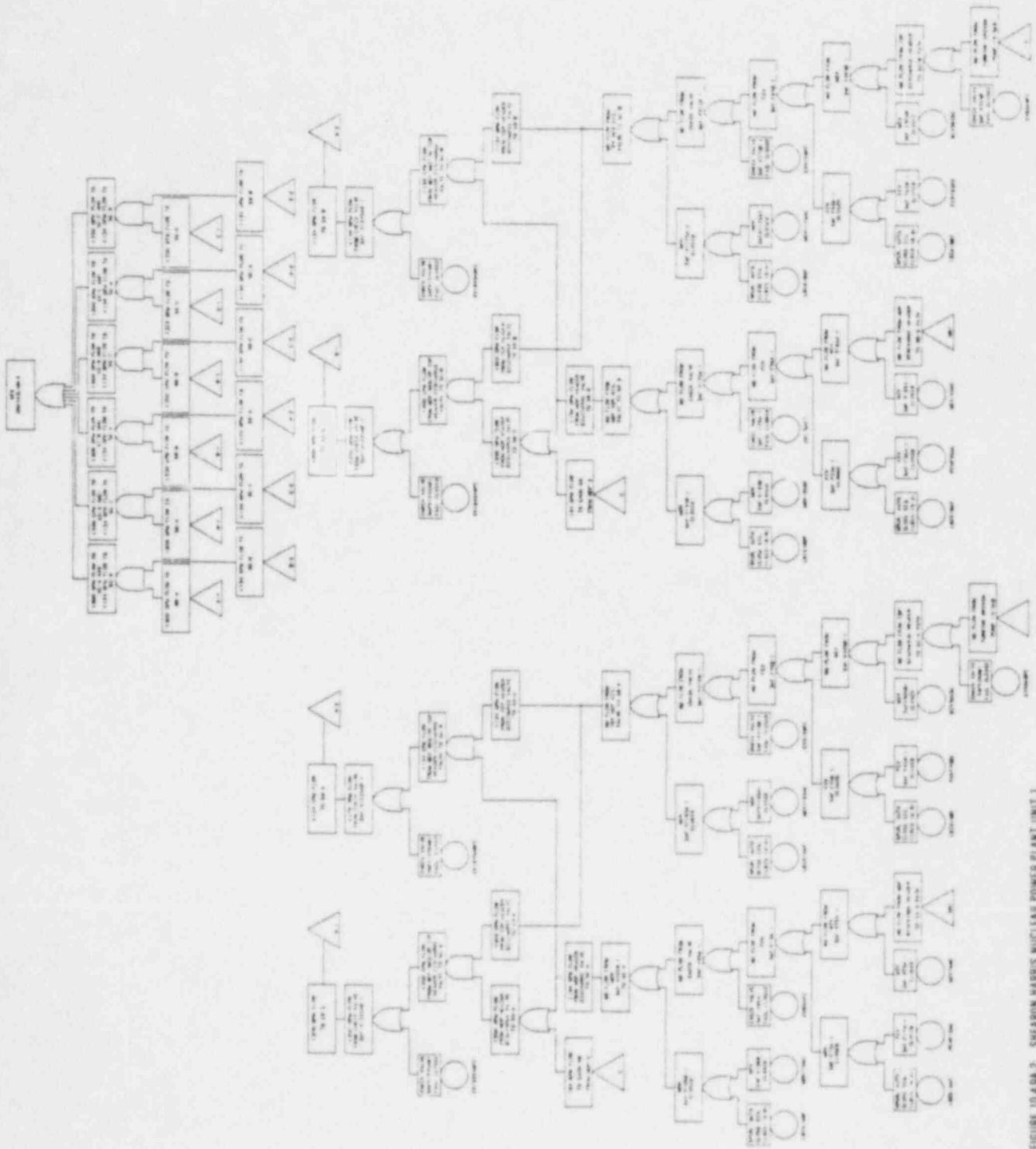
20	4.4100E-06	MAFCVF4S3 * MAFCVF5S3 +
21	4.4100E-06	MAMQV116SA * MAFCVF5S3 +
22	4.4100E-06	MAFCVF6S3 * MAMQV118SA +
23	4.4100E-06	MAMQV117SA * MAMQV118SA +
24	4.4100E-06	MAFCVF4S3 * MAMQV118SA +
25	4.4100E-06	MAMQV116SA * MAMQV118SA +
26	4.4100E-06	MAFCVF4S3 * MAFCVF6S3 +
27	4.4100E-06	MAFCVF4S3 * MAMQV117SA +
28	4.4100E-06	MAMQV116SA * MAFCVF6S3 +
29	4.4100E-06	MAMQV116SA * MAMQV117SA +
30	2.3100E-06	MAFCVF6S3 * MIV33S3C +
31	2.3100E-06	MAMQV117SA * MIV33S3C +
32	2.3100E-06	MAFCVF4S3 * MIV33S3C +
33	2.3100E-06	MAMQV116SA * MIV33S3C +
34	2.3100E-06	MAFCVF5S3 * MIV35S3C +
35	2.3100E-06	MAFCVF5S3 * MIV30S3C +
36	2.3100E-06	MAMQV118SA * MIV36S3C +
37	2.3100E-06	MAMQV118SA * MIV30S3C +
38	2.3100E-06	MAFCVF6S3 * MIV30S3C +
39	2.3100E-06	MAMQV117SA * MIV30S3C +
40	2.3100E-06	MAFCVF4S3 * MIV35S3C +
41	2.3100E-06	MAMQV116SA * MIV36S3C +

Figure 4 (Cont.) (Sheet 2 of 2)

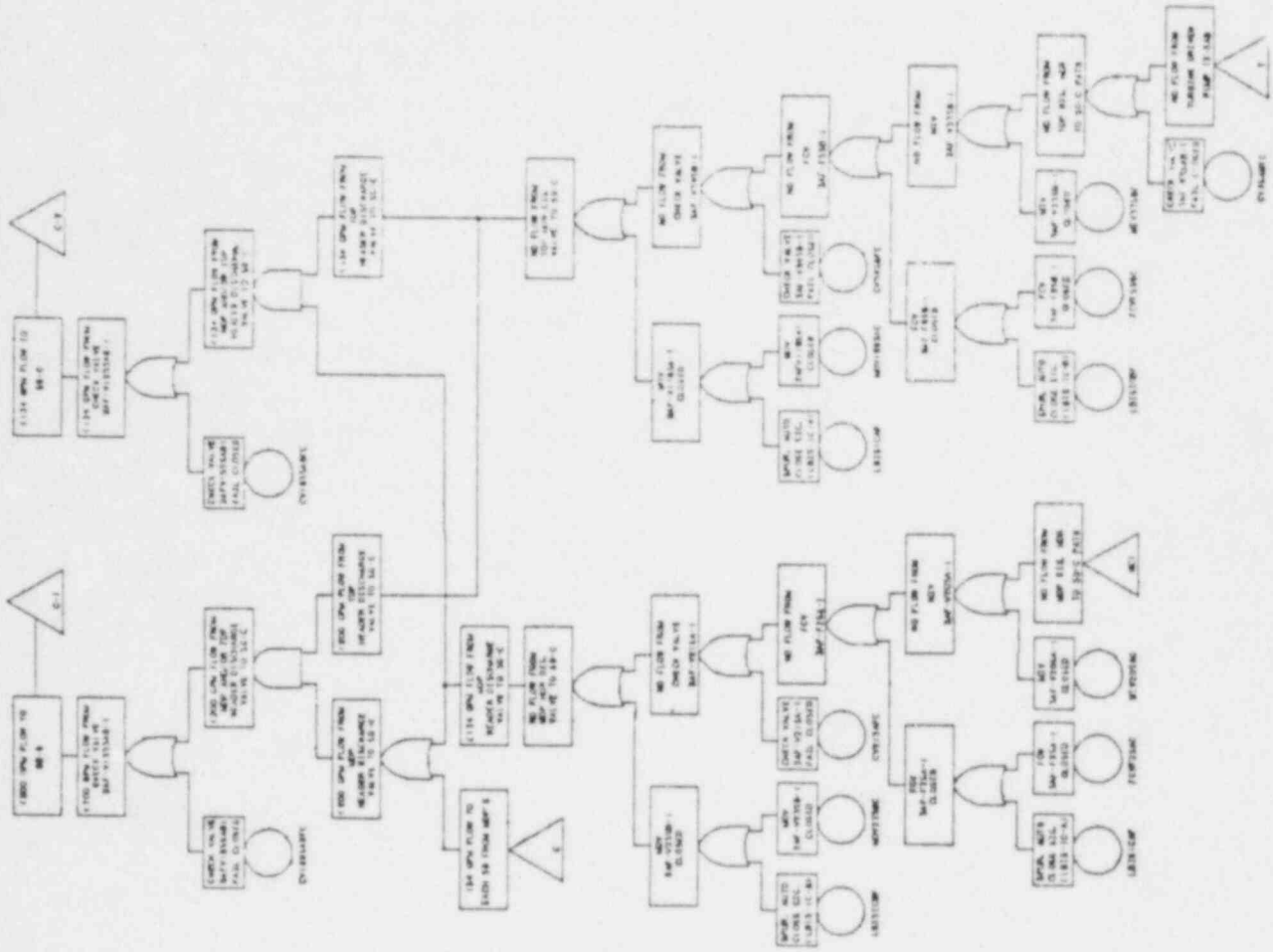


FSAR FIGURE 10.4.9A-1: SHEARON HARRIS NUCLEAR POWER PLANT UNIT 1 AUXILIARY FEEDWATER SYSTEM AVAILABILITY STUDY SIMPLIFIED FLOW DIAGRAM

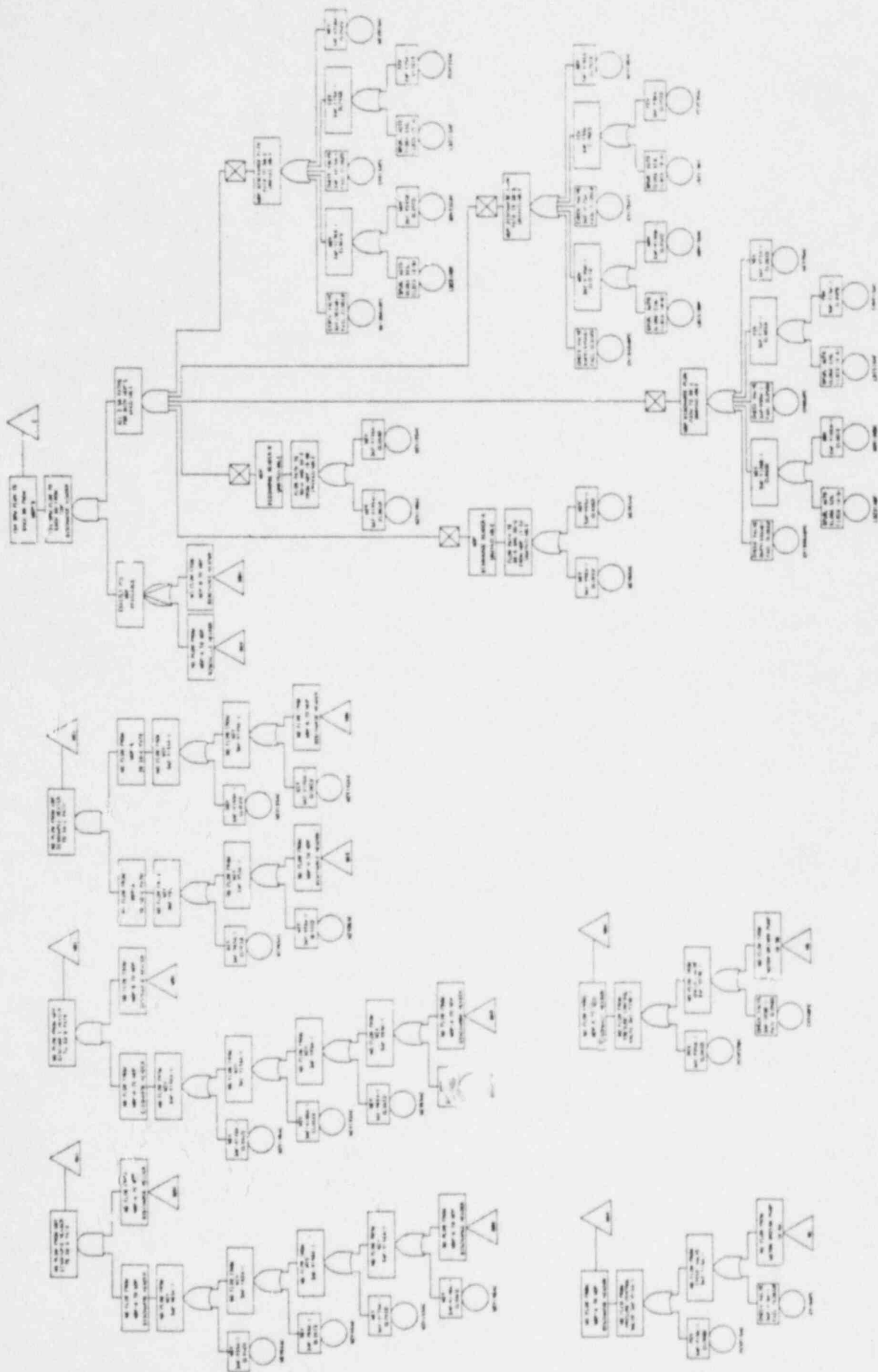




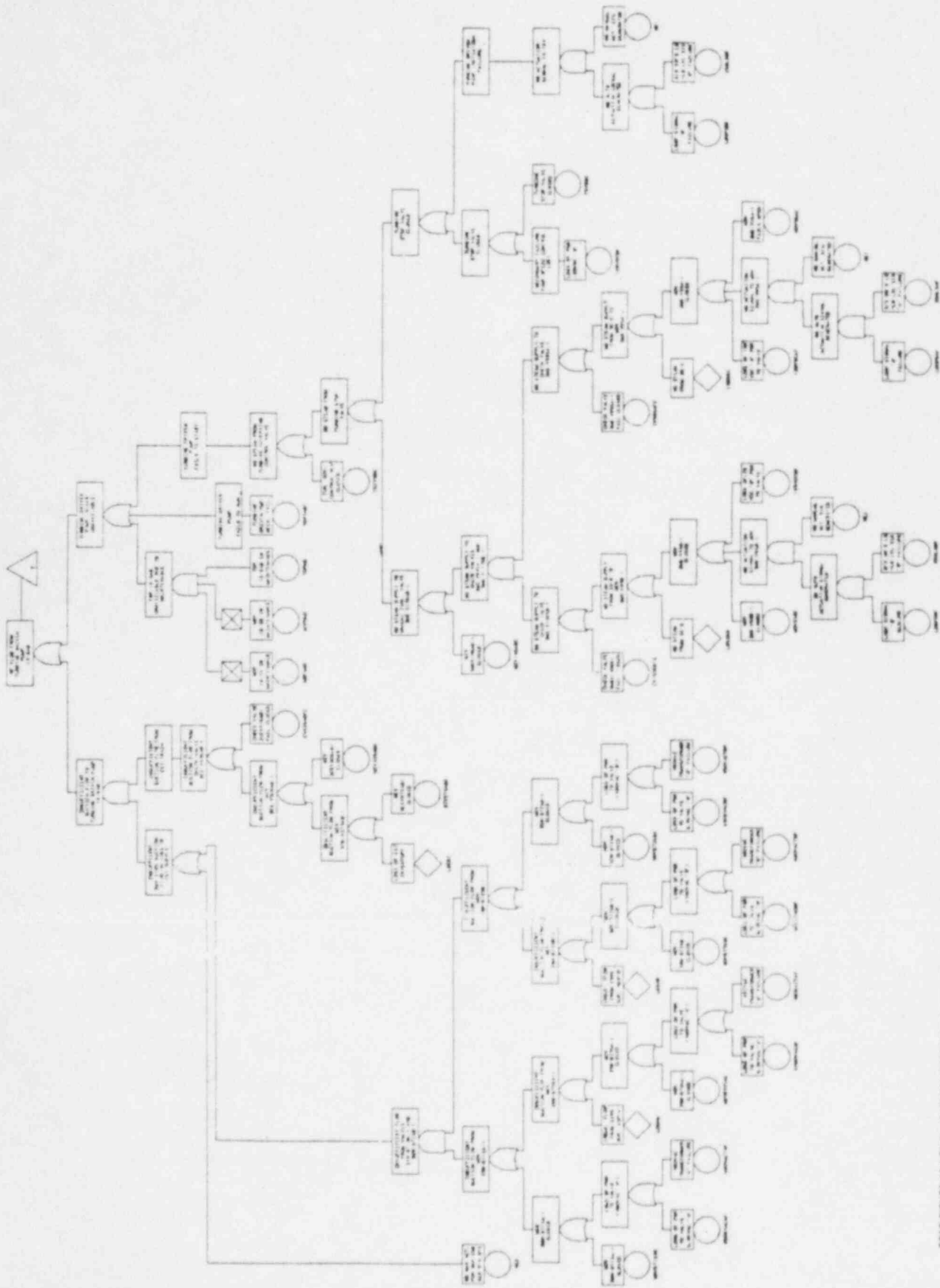
FSAB FIGURE 10.4 DA-2. SHEARON HARRIS NUCLEAR POWER PLANT UNIT 1  
AUXILIARY FEEDWATER SYSTEM AVAILABILITY STUDY FAULT TREE - LOSS OF  
MAIN FEEDWATER (LWFI) AND LOSS OF OFF-SITE POWER (LOOP) CASES  
(SHEET 1 OF 5)



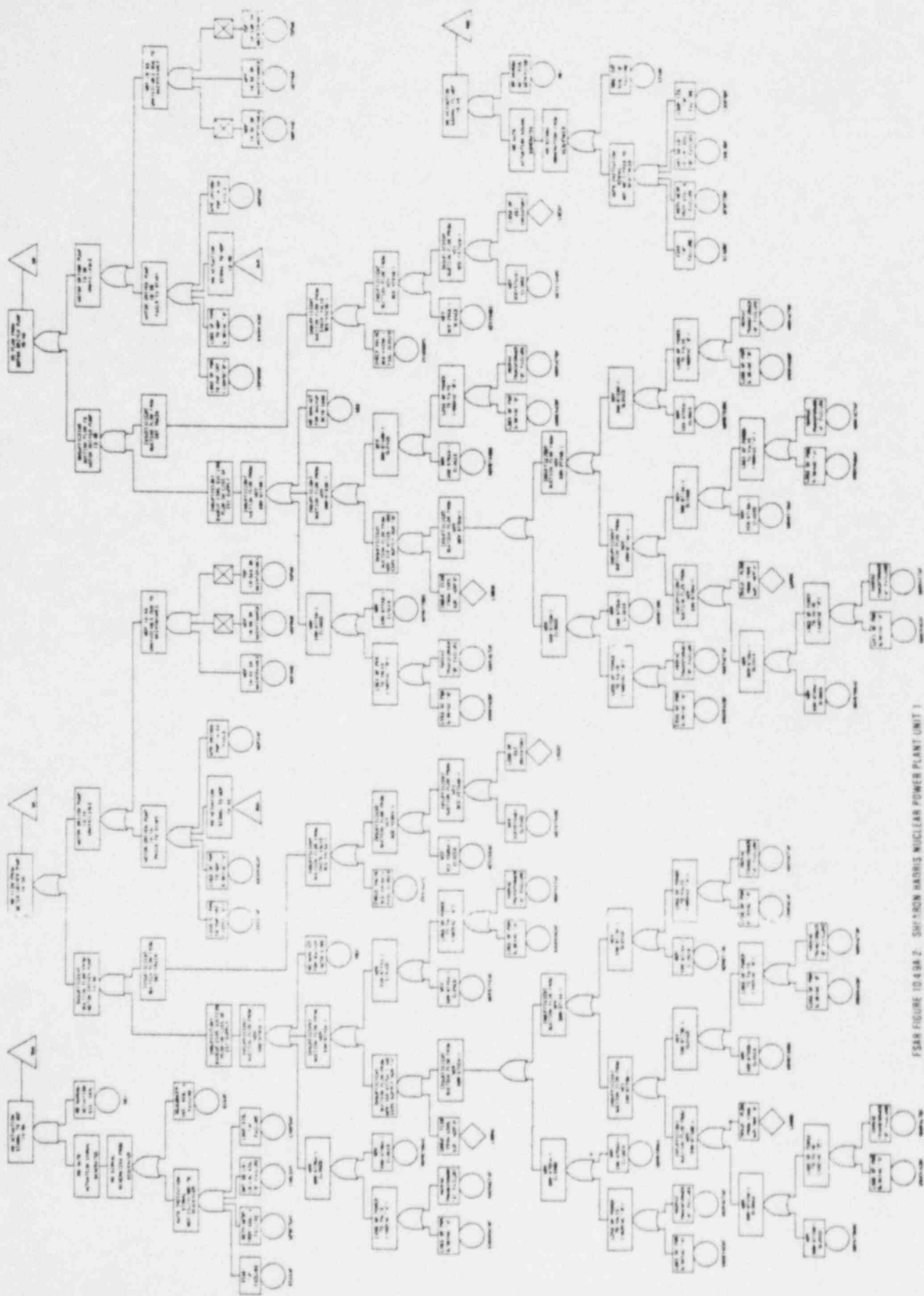
FSAR FIGURE 10.4.9A.2 SHEARON HARRIS NUCLEAR POWER PLANT UNIT 1 AUXILIARY FEEDWATER SYSTEM AVAILABILITY STUDY FAULT TREE - LOSS OF MAIN FEED, WATER (LMPW) AND LOSS OF OFFSITE POWER (LOOP) CASES. (SHEET 2 OF 5)



FSAR FIGURE 10.4.2. SHEARON HARRIS NUCLEAR POWER PLANT UNIT 1  
AUXILIARY FEEDWATER SYSTEM AVAILABILITY STUDY FAULT TREE - LOSS OF  
MAIN FEEDWATER (LWFW) AND LOSS OF OFF-SITE POWER (LOOSP) CASE  
(SHEET 3 OF 5)



FSAR FIGURE 10.4.5A.2. SHEARON HARRIS NUCLEAR POWER PLANT UNIT 1  
AUXILIARY FEEDWATER SYSTEM AVAILABILITY STUDY FAULT TREE - LOSS OF  
MAIN FEEDWATER (LMFR) AND LOSS OF OFFSITE POWER LOOP/CCTSES  
(SMF-140P.5)



FSAR FIGURE 10.4.9A-2 SHIPSON HARRIS NUCLEAR POWER PLANT (UNIT 1)  
AUXILIARY FEEDWATER SYSTEM AVAILABILITY STUDY FAULT TREE - LOSS OF  
MAIN FEEDWATER (LFW) AND LOSS OF OFF-SITE POWER (LOOP) CASE  
(SHEET 3 OF 5)

Table 2 Comparison of Data Assumptions

DESCRIPTION	UNAVAILABILITY/DEMAND	
	APPLICANT	BNL
1. <u>Maintenance</u>		
a. Pumps	$2.1 \times 10^{-3}$	$5.8 \times 10^{-3}$
b. Valves		
i. Motor-operated	$2.1 \times 10^{-3}$	$2.1 \times 10^{-3}$
ii. Electro-hydraulic motor-operated	$2.1 \times 10^{-3}$	$2.1 \times 10^{-3}$
iii. Manual	0	0
iv. Check	0	0
c. Diesel Generators	$6.4 \times 10^{-3}$	$6.4 \times 10^{-3}$
2. <u>Testing</u>		
a. Pumps	0	$2.0 \times 10^{-3}$
b. Valves (only for valves which are to be tested, not all valves)		
i. Motor-operated	0	$3.9 \times 10^{-4}$
ii. Electro-hydraulic motor-operated	0	$3.9 \times 10^{-4}$
iii. Manual	0	0
iv. Check	0	0
c. Diesel Generators	0	0
3. <u>Random Failures</u>		
a. <u>Human Errors</u>		
<u>Pre-Accident Nature</u>		
i. Valve inadvertently closed or open due to maintenance error		
1. Motor-operated electro-hydraulic motor-operated	$5 \times 10^{-4}$	$5 \times 10^{-4}$
2. Manual		
No operator recovery (Post-Acc.)	$5 \times 10^{-3}$	$5 \times 10^{-3}$
With operator recov. (Post-Acc.)	$5 \times 10^{-3}$	$1 \times 10^{-3}$

Table 2 (Cont.)

DESCRIPTION	UNAVAILABILITY/DEMAND	
	APPLICANT	BNL
<u>Post Accident Nature</u>		
i. Valve inadvertently closed or due to control room error	0	0
ii. Operator fails to manually initiate the AFSW pumps	$5 \times 10^{-4}$	$5 \times 10^{-4}$
iii. Operator fails to transfer to the backup ESWS suction sources	$5 \times 10^{-4}$	$5 \times 10^{-4}$
<u>b. Mechanical or Electrical Faults</u>		
i. Plugging of all valves	$1 \times 10^{-4}$	$1 \times 10^{-4}$
ii. Failure of mechanical components Pumps, motor-operated valves (including electro-hydraulic)	$1 \times 10^{-3}$	$1 \times 10^{-3}$
iii. Loss of pump motor cooling	N/A	N/A
iv. Control circuit failure:		
<u>Active</u>		
Pumps (Monthly tests)	$4 \times 10^{-3}$	$4 \times 10^{-3}$
Valves (Quarterly tests)	$6 \times 10^{-3}$	$6 \times 10^{-3}$
<u>Passive (Spurious)</u>		
Pumps (Monthly tests)	$1.3 \times 10^{-4}$	$1.3 \times 10^{-4}$
Valves (Quarterly tests)	$6.7 \times 10^{-4}$	$6.7 \times 10^{-4}$
Line Break Isolation Signals	$2.3 \times 10^{-4}$	$2.3 \times 10^{-4}$
v. Failure of actuation logic to pumps and power-operated valves	$7 \times 10^{-3}$	$7 \times 10^{-3}$
vi. Diesel-generator fails to start	$3 \times 10^{-2}$	$3 \times 10^{-2}$
vii. 480V AC station service transformer failure	$7.2 \times 10^{-4}$	$7.2 \times 10^{-4}$
viii. 125V DC power supply fails	$2.2 \times 10^{-4}$	$2.2 \times 10^{-4}$
ix. Auto 6900V under-voltage signal failure (for MDP recirculation isolation valves)	$2.1 \times 10^{-3}$	0
<u>c. Summation of Random Failures</u>		
<u>i. Pumps</u>		
1. Motor-driven	$5.1 \times 10^{-3}$	$5.1 \times 10^{-3}$
2. Turbine-driven	$1.0 \times 10^{-3}$	$1.0 \times 10^{-3}$

Table 2 (Cont.)

DESCRIPTION	UNAVAILABILITY/DEMAND	
	APPLICANT	BNL
c. <u>Summation of Random Failures</u> (Cont'd)		
ii. Valves: (Flow Blockage Probability)		
1. Motor-operated		
a. Position change required	$7.6 \times 10^{-3}$	$7.6 \times 10^{-3}$
b. No position change req.	$6.0 \times 10^{-4}$	$6.0 \times 10^{-4}$
2. Electro-hydraulic motor-operated		
a. Pressure control	$2.0 \times 10^{-4}$	$7.0 \times 10^{-4}$
b. Flow control	$1.0 \times 10^{-4}$	$6.0 \times 10^{-4}$
3. Manual (locked open)		
a. No post-accident recovery possible	$5.1 \times 10^{-3}$	$5.1 \times 10^{-3}$
b. Post-accident recovery possible	$5.1 \times 10^{-3}$	$1.1 \times 10^{-3}$
4. Check	$1.0 \times 10^{-4}$	$1.0 \times 10^{-4}$
iii. Diesel Generators	$3.0 \times 10^{-2}$	$3.0 \times 10^{-2}$



Table 3 Summary of Applicant's Dominant Failure Modes

FAILURE DESCRIPTION	% OF TOTAL UNAVAILABILITY
1. <u>LMFW</u>	
a. (TDP steam supply valves or TDP)•(MDPA)•(MDPB) + (TDP steam supply supply valves or TDP)• [MDPA + MDPB]•(one MIV in common MDP discharge header) + (TDP steam supply valves or TDP)• (two MIVs in common MDP discharge header)	39.3
b. Spurious signal generation of any two combined line break isolation signals	9.6
c. (One PCV)•(TDP steam supply valves or TDP)• [(MDP opposite to PCV)+(one MIV in common MDP discharge header)]	11.0
d. (One FCV)•(TDP steam supply valves or TDP)• (one MIV in common MDP discharge header)	5.4
2. <u>LOOP</u>	
a. (6900V AC "A")•(6900V AC "B")•(TDP or steam supply valves)	27.6
b. (6900V AC "A")•(125V DC "B")	13.1
c. (6900V AC "A")•(6900V AC "B")•(TDP manual suction isolation valve)	11.1
d. (6900V AC "A")•(6900V AC "B")•(two other various basic events)	30.2
3. <u>LOAC</u>	
a. (TDP manual steam isolation valve)	26.8
b. (TDP manual suction isolation valve)	26.8
c. (TDP)	16.3
d. (TDP governing control valve)	12.1
e. (TDP stop valve)	12.1

Table 4 Definition of Disallowed Test and Maintenance Acts

Let:

1. MDPA = MAPCVP1SA + TAPCVP1SA + MDPAMO + TAMDPA + MADGA
2. MDPB = MAPCVP2SB + TAPCVP2SB + MDPBMO + TAMDPB + MADGB
3. TDP = TDPMO + TATDP + MATGCV + MATSV + MAMSMOV9SA • MAMSMOV8SB
4. MDPSGA = MAMOV10SB + TAMOV10SB + MAFCVF1SA + TAFCVF1SA
5. MDPSGB = MAMOV19SB + TAMOV19SB + MAFCVF3SA + TAFCVF3SA
6. MDPSGC = MAMOV23SB + TAMOV23SB + MAFCVF2SA + TAFCVF2SA
7. TDPSGA = MAMOV116SA + TAMOV116SA + MAFCVF4SB + TAFCVF4SB
8. TDPSGB = MAMOV117SA + TAMOV117SA + MAFCVF6SB + TAFCVF6SB
9. TDPSGC = MAMOV118SA + TAMOV118SA + MAFCVF5SB + TAFCVF5SB

Defining DELETE as any combination which shuts off all flow to any one steam generator or flow from more than one pump, we obtain:

$$\begin{aligned} \text{DELETE} = & \text{MDPSGA} \cdot (\text{TDP} + \text{TDPSGA}) + \\ & \text{MDPSGB} \cdot (\text{TDP} + \text{TDPSGB}) + \\ & \text{MDPSGC} \cdot (\text{TDP} + \text{TDPSGC}) + \\ & \text{MDPA} \cdot \text{MDPB} + \text{TDP} \cdot (\text{MDPA} + \text{MDPB}) \end{aligned}$$

Note: MA \_\_\_\_\_ = Maintenance Act on Component ID, except for MDPAMO, MDPBMO and TDPMO which are the applicant's terms for maintenance outage on MDPA, MDPB and the TDP, respectively.

TA \_\_\_\_\_ = Test Act on Component ID

Table 5 Definition of Top Event for LMFW

Case 1A - One MDP is Required

This case is defined in Table 10.4.9A-2 of Ref.3. Auxiliary Feedwater System function is not fulfilled if:

1. LT200SGA134SGB = (<200 GPM is delivered to SGA) \*  
(<134 GPM is delivered to SGB)  
or
2. LT200SGA134SGC = (<200 GPM is delivered to SGA) \*  
(<134 GPM is delivered to SGC)  
or
3. LT200SGB134SGA = (<200 GPM is delivered to SGB) \*  
(<134 GPM is delivered to SGA)  
or
4. LT200SGB134SGC = (<200 GPM is delivered to SGB) \*  
(<134 GPM is delivered to SGC)  
or
5. LT200SGC134SGA = (<200 GPM is delivered to SGC) \*  
(<134 GPM is delivered to SGA)  
or
6. LT200SGC134SGB = (<200 GPM is delivered to SGC) \*  
(<134 GPM is delivered to SGB)

Therefore:

$$\begin{aligned} \text{TOP} = & \text{LT200SGA134SGB} + \text{LT200SGA134SGC} + \\ & \text{LT200SGB134SGA} + \text{LT200SGB134SGC} + \\ & \text{LT200SGC134SGA} + \text{LT200SGC134SGB} \end{aligned}$$

Case 1B - Two MDPs are Required

In this case, mission success occurs if  $\geq 250$  GPM is delivered to each of any two steam generators. Mission failure is then:

$$\text{TOP} = \text{LT250SGA250SGB} + \text{LT250SGA250SGC} + \text{LT250SGB250SGC}, \text{ where}$$

$$\text{LT250SGA250SGB} = (<250 \text{ GPM is delivered to SGA}) \cdot (<250 \text{ GPM is delivered to SGB})$$

$$\text{LT250SGA250SGC} = (<250 \text{ GPM is delivered to SGA}) \cdot (<250 \text{ GPM is delivered to SGC})$$

$$\text{LT250SGB250SGA} = (<250 \text{ GPM is delivered to SGB}) \cdot (<250 \text{ GPM is delivered to SGA})$$

Table 5 (Cont.)

Since partial failures are not considered in this analysis, less than 250 GPM to a steam generator is functionally the same as less than 200 GPM to a steam generator. In the fault trees, these cases are represented by transfer symbols A-1, B-1, and C-1.

The top event can be re-defined as

$$\text{TOP} = (\text{LT200CV153}) \cdot (\text{LT200CV154}) + (\text{LT200CV153}) \cdot (\text{LT200CV155}) \\ + (\text{LT200CV154}) \cdot (\text{LT200CV155})$$

where

$$(\text{LT200CV153}) \cdot (\text{LT200CV154}) = \\ \{ <200 \text{ GPM from check valve } 2\text{AF-V153SAB-1 to SGA} \} \cdot \\ \{ <200 \text{ GPM from check valve } 2\text{AF-V154SAB-1 to SGB} \}$$

$$(\text{LT200CV153}) \cdot (\text{LT200CV155}) = \\ \{ <200 \text{ GPM from check valve } 2\text{AF-V153SAB-1 to SGA} \} \cdot \\ \{ <200 \text{ GPM from check valve } 2\text{AF-V155SAB-1 to SGC} \}$$

$$(\text{LT200CV154}) \cdot (\text{LT200CV155}) = \\ \{ <200 \text{ GPM from check valve } 2\text{AF-V154SAB-1 to SGB} \} \cdot \\ \{ <200 \text{ GPM from check valve } 2\text{AF-V155SAB-1 to SGC} \}$$

---

Table 6 Comparison of Results

CASE	APPLICANT	BNL
1. <u>LMFW</u>		
A. One MDP Required	6.6 E-6	9.2 E-6
B. Two MDPs Required	-----	4.6 E-4
2. <u>LOOP</u>	6.1 E-5	4.9 E-5
3. <u>LOAC</u>	1.9 E-2	2.5 E-2

## APPENDIX A: SHNPP FSAR Section 10.4.9 "Auxiliary Feedwater System"

## 10.4.9 AUXILIARY FEEDWATER SYSTEM\*

The Auxiliary Feedwater System serves as a backup system for supplying feedwater to the secondary side of the steam generators at times when the normal feedwater system is not available, thereby maintaining the heat sink capabilities of the steam generator. The system provides an alternate to the Feedwater System during start-up, hot standby and cooldown and also functions as an engineered safeguards system. In the latter function, the Auxiliary Feedwater System is directly relied upon to prevent core damage in the event of transients such as loss of normal feedwater or a secondary system pipe rupture.

10.4.9.1 Design Bases

The Auxiliary Feedwater System (AFS) is designed to supply sufficient quantities of feedwater to the secondary side of the steam generators to achieve stable hot standby conditions and plant cooldown if necessary.

Plant conditions which may be accompanied by the unavailability or a loss of normal feedwater and therefore require operation of the AFS are:

- a) Loss of main feedwater with offsite power available
- b) Loss of main feedwater without offsite power available (station blackout)
- c) Feedline rupture
- d) Steamline rupture
- e) Control Room evacuation
- f) Loss of all AC power
- g) Loss of coolant accident (LOCA)

The causes and analyses of the above events are discussed in Chapter 15. The flow requirements for the Auxiliary Feedwater System were established based on these analyses, as well as upon the cooldown operations following these events. The auxiliary feedwater flow rates required to provide adequate protection for the core and to assure an emergency cooldown have been established by Westinghouse and are as follows: 1) 380 gpm for all of the above events except, 2) 500 gpm for loss of normal feedwater. The reason for this difference is the application of more stringent and conservative acceptance criteria for Condition II events (e.g. loss of normal feedwater) than for Condition IV events (feedline rupture). The auxiliary feed pumps are capable of supplying to the steam generators 400 gpm each from the two motor driven pumps and 800 gpm from the turbine driven pump. Thus for Condition IV events, the AFS has the capability of supplying 200% of the required flow even with a failure of the largest pump.

\* Further information contained in the TMI appendix.

For a transient or accident condition, the minimum flow is delivered to at least two effective steam generators within one minute of the automatic auxiliary feedwater actuation signal. After any transient or accident, the system is capable of maintaining the required flow for a period of time (at least two hours) sufficient to attain stable zero load hot standby conditions.

In addition, the Auxiliary Feedwater System provides sufficient flow (380 gpm minimum) to cool the plant from zero load hot standby conditions down to a reactor coolant hot leg temperature of 350F, where the Residual Heat Removal System is operated. The 350F RHR initiation temperature corresponds to a steam generator pressure of 125 psia with a reactor coolant pump operating or 100 psia if only natural circulation exists in the Reactor Coolant System.

Although the Auxiliary Feedwater System functions as an emergency system, it also serves as an alternate feedwater system during hot standby and cooldown operations whenever conditions are such that shutting down the Feedwater System is advantageous. The Auxiliary Feedwater System will also be used to adjust steam generator water levels prior to and during plant start-up and to establish and maintain wet layup conditions in the steam generators.

Components and piping of the AFS from and including the containment isolation valves to the steam generator nozzle are designed and fabricated in accordance with the requirements of ASME III, Class 2. Other AFS components and piping are designed and fabricated in accordance with ASME III, Class 3 requirements. Section 10.4.9.3 contains additional information on safety-related design bases.

#### 10.4.9.2 System Description

##### 10.4.9.2.1 General Information

The Auxiliary Feedwater System flow diagram is shown on Figure 10.1.0-3, 10.1.0-4, and 9.2.1-1 and the performance characteristics of its principal components are summarized in Table 10.4.9-1.

The Auxiliary Feedwater System (AFS) consists of two motor driven pumps and one turbine driven pump with associated valves, piping, controls, and instrumentation. The system components are located in the Reactor Auxiliary Building in the engineered safety feature systems area with the exception of the condensate storage tank (CST), which is located in the Tank Building, and the supply piping to the steam generator which is located in the Containment Building.

##### 10.4.9.2.2 Flow Path

The motor driven and turbine driven auxiliary feedwater pumps normally take suction from the condensate storage tank (CST) via a common supply line. The CST is sized to maintain a minimum inventory of 240,000 gallons plus sufficient margin for normal condensate system makeup and surges. The design basis for sizing the condensate storage tank is described in Section 9.2.6. Tank makeup water is supplied from the demineralized water storage tank through the demineralized water transfer pumps.

The auxiliary feedwater pumps can also be remote manually aligned to take suction from the Emergency Service Water System, in the event of a loss of the CST. (See Sections 9.2.1 and 9.2.5). There are two isolation valves for each connection between the AFS and service water. This prevents inadvertent leakage contamination of the auxiliary feedwater by impurities in the service water.

The motor driven pumps discharge into a common header which supplies three independent lines, one for each steam generator. Each of these supply lines contain check valves, motor operated isolation valves, and flow control valves as described below. The turbine driven pump supplies three additional lines, one for each steam generator. Each of these supply lines also contains check valves, motor operated isolation valves, and flow control valves. This arrangement thus provides two independent and diverse sources of feedwater, a motor driven train, and a turbine driven train. A single failure in either train will not affect the other.

The motor driven supply and the turbine driven supply for each steam generator are connected together, and a common line with flow element carries the water through the steam and feedwater pipe tunnel into Containment and connects to the auxiliary feedwater nozzle on the steam generator. Blockage of one of these common supply lines will not affect flow in the lines to the other two steam generators since these lines are independent. A ruptured supply line will be automatically isolated as a feedline rupture casualty described below.

#### 10.4.9.2.3 Component Description

The motor driven auxiliary feedwater pumps are powered from the redundant emergency busses A and B. In the event of loss of the normal power source, power is supplied by the emergency diesel generators associated with these power busses.

The motor driven auxiliary feedwater pumps are protected against excessive runout at low steam generator pressure by a electro-hydraulically operated pressure control valve in the discharge line from each pump. These valves maintain pump discharge pressure above a pre-set minimum value.

The steam turbine driven auxiliary feedwater pump is powered by a single stage, solid wheel, non-condensing, horizontal split casing steam turbine which discharges to the atmosphere. It is designed for start-up from a cold condition, and will operate with steam generator pressures ranging from 1200 psig to 105 psig.

Steam for the auxiliary feedwater pump turbine is supplied from two steam generators and taken from the main steam lines upstream of the main steam isolation valves. The turbine steam supply valves are DC motor operated valves powered from the redundant vital DC busses. A check valve located downstream of each steam supply valve will prevent loss of steam to the turbine drive in the event of a steam line break.

The steam supply valves are normally closed and will receive a signal to open at the same time the turbine actuation signal is initiated. The turbine trip



and throttle (T and T) valve is normally open. The turbine T and T valve requires solenoid actuation to allow a spring to close it. The solenoid is actuated by redundant overspeed trips; one mechanical and one electrical. The power supply for the trip solenoid is 125V DC, thereby maintaining only DC powered control for the steam driven pump. To allow remote opening of the turbine T and T valve, a DC motor operator is provided. The auxiliary feed pump turbine is equipped with an electronic speed controller powered from a safety grade DC supply. This controller adjusts pump speed and therefore discharge pressure by opening or closing the turbine governor valve.

Each steam generator auxiliary feedwater supply line from the motor driven auxiliary feedwater pump discharge header contains a Safety Class 2 motor operated auxiliary feedwater isolation valve in series with a Safety Class 3 electro-hydraulic operated flow control valve. Each valve on each steam generator auxiliary feedwater supply line is powered from redundant vital AC power trains. Each turbine driven pump steam generator supply line contains a Safety Class 2 normally open DC powered motor operated auxiliary feedwater isolation valve in series with a Safety Class 3 electro-hydraulic DC operated flow control valve. Thus, loss of all AC power will not affect the capability of the turbine driven pump to supply water to the steam generators.

#### 10.4.9.2.4 System Operations

The AFS is not normally operating except during cooldown, hot standby, or testing as described previously. It is lined up for automatic starting on any of the following signals:

- (a) Motor driven pumps:
  - 1) Safety injection
  - 2) Lo-Lo level in one steam generator
  - 3) Loss of both main feedwater pumps
  - 4) Loss of off-site power
- (b) Turbine driven pump:
  - 1) Lo-Lo level in two steam generators
  - 2) Loss of off-site power

The AFS can also be started manually from the main control board (MCB) and from the auxiliary control panel (ACP). It is shut down manually.

The flow rate to each steam generator may be controlled manually from the MCB or ACP by modulating the appropriate flow control valves in the turbine and motor driven supply lines.

#### 10.4.9.3 Safety Evaluation

The AFS is capable of withstanding the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, and floods (see Chapter 3). In addition, all components of the AFS except the CST, are located within the Reactor Auxiliary Building and the Containment Building which provide protection against the effects of externally generated missiles. The CST is classified

Safety Class 3, Seismic Category I. A concrete enclosure protects the tank from tornado, hurricane and missile damage. Components of the AFS located within the Reactor Auxiliary Building and Containment Building are protected against the effects of internally generated missiles by separation and enclosures, see Section 3.5.1. All components of the AFS are protected against the dynamic effects associated with high and moderate energy piping failures as described in Sections 3.6.1 and 3.6.2. The AFS has been designed to operate in the environment resulting during normal and accident plant conditions as described in Section 3.11.

The Auxiliary Feedwater System is capable of performing its intended safety function despite the single failure of any component. See Table 10.4.9-2 for a summary of the failure mode and effects analysis for the AFS.

The system is designed with adequate provisions to manually initiate the protective actions of the system from the auxiliary control panel in the event the Control Room must be evacuated.

During normal power operation, pipe rupture in the main feedwater, high pressure portion of auxiliary feedwater (the high pressure portion of the AFS during normal power operation starts with the check valves adjacent to the auxiliary feed isolation valves and goes to the steam generator nozzle), or Main Steam Supply System would be the most severe piping failure with respect to AFS performance requirements. These failures would result in a turbine and reactor trip; therefore, off-site power is assumed unavailable in accordance with Branch Technical Position APCS 3-1. Even with an assumed single active failure, the AFS would have more than adequate capacity to supply the required 380 gpm flow.

In the event of a steam line or main feedwater pipe break, the system will automatically terminate auxiliary feedwater flow to the affected steam generator and is designed to assure that the minimum required flow rate is directed to the unaffected steam generators. Each supply line from the AFS motor driven pump discharge header is provided with a normally open, motor operated, AC powered, isolation valve connected to the B-train ESF bus. In addition, an AC powered electro-hydraulic operated flow control valve connected to the A-train ESF bus is provided in series with the isolation valve. This arrangement provides adequate redundancy for isolation of a faulted SG in the event of a single active failure of either valve. Similarly, each supply line from the AFS turbine driven pump header is provided with a normally open motor operated AC powered isolation valve connected to the A-train ESF bus. A DC powered electro-hydraulic operated flow control valve is provided in series with the isolation valve and is powered through the B-train DC battery system. Thus, sufficient redundancy and power supply diversity is afforded in order to assure isolation of a faulted steam generator.

Physical and electrical separation are maintained throughout the pump control, control signals, electrical power supplies, steam supplies and instrumentation essential for operation of each auxiliary feedwater pump. The motor driven AFS pumps are powered from the ESF electrical AC power distribution system, (Section 8.3.1). The controls associated with the turbine driven AFS pump are powered by the safety related 125 volt DC bus. The DC bus receives power

from both its own batteries and battery charger associated with the corresponding ESF electrical AC distribution division. See Section 8.3.2 for a description of the design basis for the on-site DC power system.

Water hammer in the AFS is minimized by designing the system to remain full of water. The suction piping to the AFW pumps and part of the discharge piping are always under a positive head of water due to the higher elevation of the CST. The remainder of the discharge piping is pressurized to steam generator pressure. Void formation in the vicinity of the steam generator auxiliary feed nozzle during power operation is prevented by the tempering flow from the Feedwater System (Section 10.4.7). In addition, the AFS will be monitored for water hammer during the initial test program as described in Section 3.9.2.1.

#### 10.4.9.4 Inspection and Testing Requirements

The Auxiliary Feedwater System will undergo preoperational and start-up tests as described in Section 14.2.12. It will be verified that the system is not susceptible to hydraulic instabilities as part of the dynamic effects testing described in Section 3.9.2.1. Periodic tests as required by the Technical Specifications, Section 16.2, will be performed. In-service inspection will be carried out in accordance with Section 6.6, and the pump and valve testing requirements of Section 3.9.6 will apply.

#### 10.4.9.5 Instrumentation Requirements

The following parameters will be displayed on the auxiliary control panel and on the main control board to provide the operator with sufficient information to monitor and operate the system.

- a) Condensate storage tank level
- b) Motor driven auxiliary feedwater pump discharge pressure
- c) Turbine driven auxiliary feedwater pump discharge pressure
- d) Auxiliary feedwater flow to each steam generator
- e) Auxiliary feedwater pump status
- f) Auxiliary feedwater pump turbine speed and steam inlet pressure
- g) Auxiliary feedwater regulating valve position
- n) Auxiliary feedwater isolation valve position
- i) DC motor operated steam isolation valve position
- j) Service water supply to AFS valve position.

A detailed discussion of ESF instrumentation and controls is given in Section 7.3.

TABLE 10.4.9-1

AUXILIARY FEEDWATER  
DESIGN PARAMETERS

1)	Auxiliary Feedwater Pumps	
	Quantity	3
	Driver	1 Turbine, 2 Motor
	Capacity (gpm each)	900 (turbine driven pump) <sup>(1)</sup> 450 (motor driven pumps) <sup>(2)</sup>
	TDH, psig	1265
	SG Pressure, psig	1205 <sup>(3)</sup>
	Pumping Temperature, °F	32-125
	Code	ASME Section III Class 3
	Seismic Category	I
2)	Piping and Valves	
	Code	ASME Section III Class 2 & 3
	Seismic Category	I
3)	Condensate Storage Tank	
	Capacity, gal.	415,000
	Minimum Capacity, gal.	240,000
	Design Pressure	Atmospheric
	Code	ASME Section III Class 3
	Seismic	I
4)	Time to deliver full flow to at least two steam generators upon receipt of an actuation signal without normal offsite and onsite power available (in Sec)	60

## NOTES:

- (1) Includes 100 gpm recirculation flow.  
 (2) Includes 50 gpm recirculation.  
 (3) Lowest safety valve setting plus 3% accumulation.

TABLE 10.4.9-2  
FAILURE MODE AND EFFECTS ANALYSIS AUXILIARY FEEDWATER SYSTEM

No.	Name	Failure Mode	Cause	Effects	Method of Detection	Inherent Compensating Provision
1	Motor-driven AFS pump	Fails to start	Diesel Generator fails to start	Loss of flow from this pump	Low pressure indication from AFS pump discharge	Redundant turbine driven AFS pump
2	Turbine-driven AFS pump	Fails to start	DC Power System Failure	Loss of flow from this pump	Low pressure indication from AFS pump discharge	Redundant motor driven AFS pumps
3a	AFS isolation valves	Fails to close to faulted SG	Control failure or loss of power	None	Valve position	Automatic closure of AFS flow control valve
3b	AFS isolation valves	Fails closed to intact SG	Control failure	Temporary loss of flow from corresponding pump	Low flow indication and valve position	Redundant flow provided from other pumps-valve may be manually opened to reestablish flow
4a	AFS flow control valve	Fails to close to Faulted SG	Control failure or loss of power	None	Valve position	Automatic closure of AFS isolation valve
4b	AFS flow control valve	Fails closed to intact SG	Control failure	Temporary loss of flow from corresponding pump	Low flow indication and valve position	Redundant flow provided from other pumps-valve may be manually opened to reestablish flow
5a	AFS pressure control valve	Fails open	Control failure or mechanical binding	Excessive pump runoff when system is shutting down causing trip of motor.	Valve position low discharge pressure.	Redundant pumps
5b	AFS pressure control valve	Fails closed	Control failure or mechanical binding	Loss of flow	Valve position high discharge pressure.	Redundant pumps

10.4.9-8

APPENDIX B: SHNPP FSAR Technical Specifications "Auxiliary Feedwater System and Condensate Storage Tank"

PLANT SYSTEMS

AUXILIARY FEEDWATER SYSTEM

LIMITING CONDITION FOR OPERATION

---

3.7.1.2 At least three independent steam generator auxiliary feedwater pumps and associated flow paths shall be OPERABLE with:

- a. Two feedwater pumps, each capable of being powered from separate emergency busses, and
- b. One feedwater pump capable of being powered from an OPERABLE steam supply system.

APPLICABILITY: MODES 1, 2 and 3.

ACTION:

With one auxiliary feedwater pump inoperable, restore at least three auxiliary feedwater pumps (two capable of being powered from separate emergency busses and one capable of being powered by an OPERABLE steam supply system) to OPERABLE status within 72 hours or be in at least HOT STANDBY within the next 6 hours and in HOT SHUTDOWN within the following 6 hours.

SURVEILLANCE REQUIREMENTS

---

4.7.1.2 Each auxiliary feedwater pump shall be demonstrated OPERABLE:

- a. At least once per 31 days by:
  1. Verifying that each motor driven pump develops a discharge pressure of greater than or equal to Later psig at a flow of greater than or equal to Later gpm.
  2. Verifying that the steam turbine driven pump develops a discharge pressure of greater than or equal to Later psig at a flow of greater than or equal to Later gpm when the secondary steam supply pressure is greater than Later psig. The provisions of Specification 4.0.4 are not applicable for entry into MODE 3.
  3. Verifying that each non-automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, is in its correct position.

PLANT SYSTEMSSURVEILLANCE REQUIREMENTS (Continued)

---

4. Verifying that each automatic valve in the flow path is in the fully open position whenever the auxiliary feedwater system is placed in automatic control or when above 10 percent RATED THERMAL POWER.
  - b. At least once per 18 months during shutdown by:
    1. Verifying that each automatic valve in the flow path actuates to its correct position on a faulted steam generator isolation test signal.
    2. Verifying that each auxiliary feedwater pump starts automatically upon receipt of the following simulated test signals.
      - a. Motor driven pumps
        - 1) Steam Generator Water Level-low, low, or
        - 2) Safety Injection
      - b. Turbine Driven Pump
        - 1) Steam Generator Water Level-low, low  
(2 Steam Generators)

PLANT SYSTEMSCONDENSATE STORAGE TANKLIMITING CONDITION FOR OPERATION

---

3.7.1.3 The condensate storage tank (CST) shall be OPERABLE with a minimum contained volume of 240,000 gallons of water.

APPLICABILITY: MODES 1, 2 and 3.

ACTION:

With the condensate storage tank inoperable, within 4 hours either:

- a. Restore the CST to OPERABLE status or be in at least HOT STANDBY within the next 6 hours and in HOT SHUTDOWN within the following 6 hours, or
- b. Demonstrate the OPERABILITY of the ultimate heat sink via the Essential Service Water System as a backup supply to the auxiliary feedwater pumps and restore the condensate storage tank to OPERABLE status within 7 days or be in at least HOT STANDBY within the next 6 hours and in HOT SHUTDOWN within the following 6 hours.

SURVEILLANCE REQUIREMENTS

---

4.7.1.3.1 The condensate storage tank shall be demonstrated OPERABLE at least once per 12 hours by verifying the contained water volume is within its limits when the tank is the supply source for the auxiliary feedwater pumps.

4.7.1.3.2 The ultimate heat sink via the Essential Service Water System shall be demonstrated OPERABLE at least once per 12 hours by opening the valves that supply service water to the auxiliary feedwater pump suction and verifying Essential Service Water header pressure whenever the service water system is the supply source for the auxiliary feedwater pumps.



PLANT SYSTEMS

ACTIVITY

LIMITING CONDITION FOR OPERATION

---

3.7.1.4 The specific activity of the secondary coolant system shall be less than or equal to 0.10 microcuries/gram DOSE EQUIVALENT I-131.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTION:

With the specific activity of the secondary coolant system greater than 0.10 microcuries/gram DOSE EQUIVALENT I-131, be in at least HOT STANDBY within 6 hours and in COLD SHUTDOWN within the following 30 hours.

SURVEILLANCE REQUIREMENTS

---

4.7.1.4 The specific activity of the secondary coolant system shall be determined to be within the limit by performance of the sampling and analysis program of Table 4.7-1.

APPENDIX C: "NRC-Supplied Data for Purposes of Conducting A Comparative Assessment of Existing APWS Designs and Their Potential Reliabilities"

Point Value Estimate  
of Probability of\*  
Failure on Demand

I. Component (Hardware) Failure Data

a. Valves:

Manual Valves (Plugged)	$\sim 1 \times 10^{-4}$
Check Valves	$\sim 1 \times 10^{-4}$
Motor-Operated Valves	
- Mechanical Components	$\sim 1 \times 10^{-3}$
- Plugging Contribution	$\sim 1 \times 10^{-4}$
- Control Circuit (Local to Valve)	
w/Quarterly Tests	$\sim 6 \times 10^{-3}$
w/Monthly Tests	$\sim 2 \times 10^{-3}$

b. Pumps: (1 Pump)

Mechanical Components	$\sim 1 \times 10^{-3}$
Control Circuit	
- w/Quarterly Tests	$\sim 7 \times 10^{-3}$
- w/Monthly Tests	$\sim 4 \times 10^{-3}$

c. Actuation Logic  $\sim 7 \times 10^{-3}$

\* Error factors of 2-10 (up and down) about such values are not unexpected for basic data uncertainties.

## II. Test and Maintenance Outage Contributions:

### a. Calculational Approach Test Outage

$$Q_{\text{TEST}} = \frac{(\text{hrs/test}) (\text{tests/year})}{\text{hrs/year}}$$

### 2. Maintenance Outage

$$Q_{\text{MAINT.}} = \frac{(0.22) (\text{hrs/maint. act})}{720}$$

### b. Data Tables for Test and Maint. Outages\*

#### SUMMARY OF TEST ACT DURATION

<u>Component</u>	<u>Range on Test Act Duration Time, hr</u>	<u>Calculated Mean Test Act Duration Time, t<sub>g</sub>, hr</u>
Pumps	0.25 - 4	1.4
Valves	0.25 - 2	0.86
Diesels	0.25 - 4	1.4
Instrumentation	0.25 - 4	1.4

#### LOG-NORMAL MODELED MAINTENANCE ACT DURATION

<u>Component</u>	<u>Range on Maintenance Act Duration Time, hr</u>	<u>Calculated Mean Maintenance Act Duration Time, t<sub>g</sub>, hr</u>
Pumps	1/2 - 24	7
	1/2 - 72	19
Valves	1/2 - 24	7
Diesels	2 - 72	21
Instrumentation	1/4 - 24	6

\* Note: These data tables were taken from the Reactor Safety Study (WASH-1400) for purposes of this AFW system assessment. Where the plant technical specifications placed limits on the outage duration(s) allowed for AFW system trains, this tech spec limit was used to estimate the mean duration times for maintenance. In general, it was found that the outages allowed for maintenance dominated those contributions to AFW system unavailability from outages due to testing.

III. Human Acts & Errors - Failure Data:

Estimated Human Error/Failure Probabilities  
Modifying Factors & Situations\*

	With Valve Position Indication in Control Room		With Local Walk-Around & Double Check Procedures		W/O Either	
	Point Value Est	Est. on Error Factor	Point Value Est	Est. on Error Factor	Point Value Estimate	Est On Error Factor
a. Acts & Errors of A Pre-Accident Nature						
1. Valves Mispositioned During Test/Maint						
(a) Specific Single Valve Wrongly Selected out of A Population of Valves During Conduct of a Test or Maintenance Act (X No. of Valves in Population at Choice)	$\frac{1}{20} \times 10^{-2} \times \frac{1}{X}$	20	$\frac{1}{2} \times 10^{-2} \times \frac{1}{X}$	10	$10^{-2} \times \frac{1}{X}$	10
(b) Inadvertently Leaves Correct Valve in Wrong Position	$5 \times 10^{-4}$	20	$5 \times 10^{-3}$	10	$10^{-2}$	10
2. More than one valve is affected (coupled errors)	$1 \times 10^{-4}$	20	$1 \times 10^{-3}$	10	$3 \times 10^{-3}$	10
3. Miscalibration of Sensors/Electrical Relays						
(a) One Sensor/Relay Affected	-	-	$5 \times 10^{-3}$	10	$10^{-2}$	10
(b) More than one Sensor/Relay Affected	-	-	$1 \times 10^{-3}$	10	$3 \times 10^{-3}$	10

	Time Actuation Needed	Estimated Failure Prob. for Primary Operator to Actuate AFWS	Estimated Failure Prob. of other (Backup) Control Rm. Operator to Actuate AFWS	Overall Estimate of Failure Probability	Estimated Error Factor on Overall Probability
d. <u>Acts &amp; Errors of a Post-Accident Nature</u>					
1. Manual Actuation of AFW system from Control Room					
(a) Considering "Dedicated" Operator to Actuate AFW system and Possible Backup Actuation of AFWS	5 min.	$2 \times 10^{-3}$	-	$2 \times 10^{-3}$	10
	15 min.	$1 \times 10^{-3}$	0.5 (mod. dep.)	$5 \times 10^{-4}$	10
	30 min.	$5 \times 10^{-4}$	.25 (low dep.)	$10^{-4}$	10
(a) Considering "Non-Dedicated" Operator to Actuate AFW system and Possible Backup Actuation of AFW system	5 min.	$5 \times 10^{-2}$	-	$5 \times 10^{-2}$	10
	15 min.	$1 \times 10^{-2}$	0.5 (mod. dep.)	$5 \times 10^{-3}$	10
	30 min.	$5 \times 10^{-3}$	.25 (low dep.)	$10^{-3}$	10

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by T/DC add Vol. No. if any)

NUREG/CR-4311  
BNL-NUREG-51902

2. TITLE AND SUBTITLE

Review of the Shearon Harris Unit 1 Auxiliary Feedwater System Reliability Analysis

3. LEAVE BLANK

4. DATE REPORT COMPLETED

MONTH

YEAR

August

1985

5. DATE REPORT ISSUED

MONTH

YEAR

February

1986

5. AUTHOR(S)

A. Fresco, R. Youngblood, and I. A. Papazoglou

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Brookhaven National Laboratory  
Upton, New York 11973

8. PROJECT/TASK/WORK UNIT NUMBER

FIN OR GRANT NUMBER

A-3702

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Division of Safety Technology  
Office of Nuclear Reactor Regulation  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555

11. TYPE OF REPORT

Final

6. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)

This report presents the results of a review of the Auxiliary Feedwater System Reliability Analysis for the Shearon Harris Nuclear Power Plant (SHNPP) Unit 1. The objective of this report is to estimate the probability that the Auxiliary Feedwater System will fail to perform its mission for each of three different initiators: (1) loss of main feedwater with offsite power available, (2) loss of offsite power, (3) loss of all ac power except vital instrumentation and control 125-V dc/120-V ac power. The scope, methodology, and failure data are prescribed by NUREG-0611, Appendix III. The results are compared with those obtained in NUREG-0611 for other Westinghouse plants.

14. DOCUMENT ANALYSIS - KEYWORDS/DESCRIPTORS

Reliability Analysis  
Auxiliary Feedwater Systems  
Pump and Valve Failure Rates  
Shearon Harris Nuclear Power Plant Unit 1

NUREG-0611

15. IDENTIFIERS OPEN ENDED TERMS

15. AVAILABILITY STATEMENT

Unlimited

16. SECURITY CLASSIFICATION

(This page)  
Unclassified

(This report)  
Unclassified

17. NUMBER OF PAGES

18. PRICE

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

OFFICIAL BUSINESS  
PENALTY FOR PRIVATE USE, \$300

SPECIAL FOURTH CLASS RATE  
POSTAGE & FEES PAID  
USNRC  
WASH D.C.  
PERMIT No. G-67

120555078877 1 1AM  
US NRC  
ADM-DIV OF TIDC  
POLICY & PUB MGT BR-PDR NUREG  
W-501 DC 20555  
WASHINGTON

REVIEW OF THE SHEARCO HARRIS UNIT 1  
AUXILIARY FEEDWATER SYSTEM RELIABILITY ANALYSIS

NUREG/CR-4311

FEBRUARY 1986