DRAFT

NUREG/CR-
BNL-NUREG-

DRAFT COPY

REVIEW OF THE VOGTLE UNITS 1 AND 2 AUXILIARY FEEDWATER SYSTEM RELIABILITY ANALYSIS

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

Department of Nuclear Energy
Brookhaven National Laboratory
Upton, NY 11973

October 1984

Prepared for
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Contract No.DE-AC-02-76CH00016
FIN A-3702

ABSTRACT

DRAFT

This report presents the results of the review of the Auxiliary Feedwater System reliability analysis for the Vogtle Electric Generating Plant (VEGP) Units 1 and 2. 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 125V DC / 120V 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

DRAFT

Page

LIST OF FIGURES

LIST OF TABLES

DRAFT

EXECUTIVE SUMMARY

After the accident at Three Mile Island, a study was performed of 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.(1) At the request of the NRC,(2) Georgia Power Corporation, an operating license applicant, has provided the NRC with a study of the Vogtle Electric Generating Plant (VEGP) Units 1 and 2 AFWS,(3) performed using NREG-0611 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 the reliability of the AFWS is in the High range (unavailability = 2.2E-5/demand).

2. For a loss of offsite power (LOOP) resulting in a concurrent loss of main feedwater (LMFW): The reliability of the AFWS is on the borderline of the High range (unavailability = 1.0E-4/demand).

3. For a loss of all AC power (LOAC), except for the 125V DC / 120V 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 = 3.2E-2/demand).

A comparson of the VEGP AFWS reliability to other AFWS designs in plants using the Westinghouse NSSS is shown in Table 1. The specific quantitative comparison between the applicant's and BNL's results is shown in Table 2. The BNL results are based on the unavailabilites shown in Table 8 of this report, for Case C with "Multiple Errors Assumed."

This evaluation incorporates certain fairly conservative assumptions which were made for lack of information. These are discussed in Section 9.2.3. It is likely that additional information would reduce the unavailability estimates quoted above.

Table 1 VEGP AFWS Conditional Availability Comparison[(a)] To Other Plants Using the Westinghouse NSSS

A. ——| |—— ORDER OF MAGNITUDE IN UNAVAILABILITY REPRESENTED.
——→ INCREASING AVAILABILITY.

B. THE SCALE FOR THIS EVENT IS NOT THE SAME AS THAT FOR THE LMFW AND LMFW/LOOP.

● Applicant's results

◆ BNL assessment

not shown above

Table 2 Unavailabilities of the VEGP AFWS, Comparison of Applicant's Results to BNL Assessment

Transient	Applicant's Results	BNL Assessment
1. LMFW	6.3E-6	2.2E-5
2. LOOP	2.6E-5	1.0E-4
3. LOAC	1.0E-2	3.2E-2

DRAFT

1. INTRODUCTION

This report is a review by Brookhaven National Laboratory (BNL) of the Vogtle Electric Generating Plant (VEGP) Final Safety Analysis Report (FSAR) Appendix 10A, entitled "VEGP Auxiliary Feedwater System Availability Analysis," prepared by Bechtel Corporation for Georgia Power Corporation.(3)

After the accident at Three Mile Island, a study was performed of the Auxiliary Feedwater Systems (AFWS) of all the then-operating plants. The results obtained for operating Westinghouse-designed plants were presented in NUREG-0611.(1) 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(2) 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:(4)

> "...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.(1) 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 to 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, using the above methodology.

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

3. MISSION SUCCESS CRITERIA

According to Ref. 3, the AFWS is composed of three mechanical trains which serve the four steam generators at a given unit. The steam generators have been analyzed to require 510 gal/min of flow under the most severe accident conditions. Each motor-driven pump of trains A and B has a capacity of 630 gal/min and provides more than 100 percent of the required auxiliary feedwater flow. Train A provides feedwater to steam generators 1 and 4, and train B provides feedwater to steam generators 2 and 3. The (steam) turbine-driven pump of train C has a capacity of 1300 gal/min and provides more than 200 percent of the required auxiliary feedwater flow. The turbine-driven pump provides feedwater to all four steam generators. The success criterion for the AFWS is flow to any two steam generators. Furthermore, as outlined by the NRC evaluation of generic AFWSs (NUREG-0611), the AFWS must actuate within the time it takes for the steam generators to boil dry when no flow is provided to the steam generators. At VEGP, the boiloff time (and therefore the limit on the AFWS actuation time) is approximately 30 min, as stated in Reference 3.

In addition, FSAR Subsection 10.4.9.2.1 states that normal flow is from the CST to the auxiliary feedwater pumps. The design of the CST provides for cold shutdown capability for a period of 9 hours: 4 hours at hot standby, followed by a 5 hour cooldown period. Table 3 of this report provides the nuclear steam supply system (NSSS) required makeup rates to the steam generators for the specific transients within the scope of this review. Initially, sensible heat is removed from the RCS to reduce the temperature from a full-power operation average temperature of 588°F to a nominal hot standby temperature of 500°F. Subsequently, to bring the reactor down to 350°F at 50°F/h, an initial makeup rate of 500 gal/min is required.

4. SYSTEM DESCRIPTION

The BNL review of the AFWS reliability is based on the system as described in the VEGP FSAR Sections 10.4.9 and 10A currently on file in BNL's Nuclear Safety Library. The simplified AFWS flow diagrams, fault trees, and other drawings from Section 10A have been included in this report for convenience (see BNL Figures 1 to 7). All figures and tables will be referred to by the present numbering scheme, e.g., Table 1 of this report, which is FSAR Table 10A-5, will be called simply Table 1.

Table 5

NRC-SUPPLIED DATA USED FOR PURPOSES OF CONDUCTING A COMPARATIVE ASSESSMENT OF EXISTING AFWS DESIGNS AND THEIR POTENTIAL RELIABILITIES

	Point Value Estimate of Probability of* Failure on Demand
I. Component (Hardware) Failure Data	
a. Valves:	
Manual Valves (Plugged)	~1 x 10-4
Check Valves	~1 x 10-4
Motor-Operated Valves	
- Mechanical Components	~1 x 10-3
- Plugging Contribution	~1 x 10-4
- Control Circuit (Local to Valve)	
w/Quarterly Tests	~6 x 10-3
w/Monthly Tests	~2 x 10-3
b. Pumps: (1 Pump)	
Mechanical Components	~1 x 10-3
Control Circuit	
- w/Quarterly Tests	~7 x 10-3
- w/Monthly Tests	~4 x 10-3
c. Actuation Logic	~7 x 10-3

---

* Error factors of 3-10 (up and down) about such values are not unexpected for basic data uncertainties.

Table 5 (Cont.)

II. Test and Maintenance Outage Contributions:

a. Calculational Approach

1. Test Outage

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

2. Maintenance Outage

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

b. Data Tables for Test and Maint. Outages*

SUMMARY OF TEST ACT DURATION

Component	Range on Test Act Duration Time, hr	Calculated Mean Test Act Duration Time, t_D, hr
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

Component	Range on Maintenance Act Duration Time, hr	Calculated Mean Maintenance Act Duration Time, t_D, hr
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.

Table 5 (Cont.)

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	5×10^{-4}	20	5×10^{-3}	10	10^{-2}	10
2. More than one valve is affected (coupled errors)	1×10^{-4}	20	1×10^{-3}	10	3×10^{-3}	10
3. Miscalibration of Sensors/Electrical Relays						
(a) One Sensor/Relay Affected	-	-	5×10^{-3}	10	10^{-2}	10
(b) More than one Sensor/Relay Affected	-	-	1×10^{-3}	10	3×10^{-3}	10

Table 5 (Cont.)

	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
b. <u>Acts & 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.	2×10^{-3}		2×10^{-3}	10
	15 min.	1×10^{-3}	0.5 (mod. dep.)	5×10^{-4}	10
	30 min.	5×10^{-4}	.25 (low dep.)	10^{-4}	10
(a) Considering "Non-Dedicated" Operator to Actuate AFW system and Possible Backup Acutation of AFW system	5 min.	5×10^{-2}	-	5×10^{-2}	10
	15 min.	1×10^{-2}	0.5 (mod. dep.)	5×10^{-3}	10
	30 min.	5×10^{-3}	.25 (low dep.)	10^{-3}	10

Table 6 Nomenclature Scheme for Fault Identifiers Added by BNL to the Applicant's Fault Tree

Basic Events

RA = Random Acts (includes pre-accident operator error for manual valves)

MA = Maintenance Acts

TA = Test Acts

OE = Operator Error (includes both pre- and post- accident operator error for motor-operated valves)

CL = Closed

OP = Open

FTO = Fails to Open

ACTRNAF = Random failure of Train A AC power, i.e., Diesel Generator A.

ACTRNBF = Same for Train B.

Components

BYV = Butterfly Valve
CHV = Check Valve
SCV = Stop Check Valve
MGV = Manual Gate Valve
MDP = Motor-Driven Pump
TDP = Turbine-Driven Pump
DG = Diesel Generator
MOV = Motor-Operated Valve

Table 7 Comparison of Data Assumptions

Description	Unavailability/Demand	
	Applicant	BNL
A. Maintenance		
1. Pumps	$5.81x10^{-3}$	$5.8x10^{-3}$
2. Valves		
a. Motor-operated gate and butterfly valves	$2.17x10^{-6}$	$2.1x10^{-3}$
b. Manual butterfly valves on CST discharge lines	$4.0x10^{-7}$	0
c. Manual butterfly valves on pump suction lines	$7.0x10^{-8}$	0
d. Speed governor and trip and throttle valves	$2.17x10^{-6}$	$2.1x10^{-3}$
e. Manual stop check valves at steam generator intakes	0*	0
f. Manual stop check valves on pump discharge lines	$2.17x10^{-6}$	0
g. Manual gate valves on turbine steam intake	0*	0
h. Manual gate valves on pump discharge lines	$7.0x10^{-8}$	0
i. Check valves at steam generator intakes	0*	0
j. Check valves on pump discharge lines	$2.17x10^{-6}$	0
3. Diesel Generators (On Site AC Power)	0	$6.4x10^{-3}$
4. 125V DC Power	$2.4x10^{-6}$	0
B. Testing		
1. Pumps	0	$6.4x10^{-4}$
2. Valves	0≠	0≠
3. Diesel Generators	0	0

---

*It is assumed that no maintenance can be performed on these components due to their proximity to the steam generators.

≠Valve testing does not cause unavailability.

Table 7 (Cont.)

	Unavailability/Demand	
Description	Applicant	BNL
C. Human Errors		
1. Pre-accident nature		
a. Motor-operated valves with Control Room position indication	$5x10^{-4}$	$5x10^{-4}$
b. Manual valves with no Control Room position indication		
i) Post-accident operator recovery not possible within 30 minutes	0	$5x10^{-3}$
ii) Post-accident operator recovery possible within 30 minutes	0	$1x10^{-3}$
2. Post-accident nature		
a. Operator fails to open motor-operated valves (includes transfer to alternate Condensate Storage Tank)	$5x10^{-3}$	$1x10^{-3}$
b. Operator fails to start pumps	$5x10^{-3}$	$1x10^{-3}$
D. Mechanical and Electrical Faults		
1. Plugging of all valves	$1x10^{-4}$	$1x10^{-4}$
2. Failure of mechanical components including pumps and motor-operated valves	$1x10^{-3}$	$1x10^{-3}$
3. Diesel generator fails to start	$3x10^{-2}$	$3x10^{-2}$
4. 125V DC power failure	0	0
5. Failure of actuation logic for pumps and motor-operated valves (per train)	$7x10^{-3}$	$7x10^{-3}$
6. Control circuit failure		
a. Pumps (monthly tests)	$4x10^{-3}$	$4x10^{-3}$
b. Valves (monthly tests)	$2x10^{-3}$	$2x10^{-3}$

Table 7 (Cont.)

Description	Unavailability/Demand	
	Applicant	BNL
E. Summation of Random Failures (Human Errors and Mechanical and Electrical Faults)		
1. Pumps, both motor- and turbine-driven	$5x10^{-3}$	$5x10^{-3}$
2. Valves		
a. Motor-operated, position change required (plugging plus control circuit failure)	$3.1x10^{-3}$	$3.1x10^{-3}$
b. Manual valves (locked open)		
i. No post accident operator recovery possible within 30 minutes (Valve position not verifiable by pump testing)	$1x10^{-4}$	$5.1x10^{-3}$
ii. Post accident operator recovery possible within 30 minutes (Valve position verifiable by pump testing)	$1x10^{-4}$	$1.1x10^{-3}$
c. Check valves	$1x10^{-4}$	$1x10^{-4}$
3. Diesel Generators	$3x10^{-2}$	$3x10^{-2}$

Table 8 VEGP AFWS Unavailability Sensitivity Comparison

Case	A. All Manual Valves 5.1E-3 Random Error	B. All Manual Valves 1.1E-3 Random Error Except SG Intake Valves at 5.1E-3 Random Error	C. All Manual Valves 1.1E-3 Random Error	Applicant's Results
1. LMFW				
a) Independent Failures Only	4.1E-5	1.4E-5	8.8E-6	6.3E-6
b) Multiple Errors Assumed	5.4E-5	2.7E-3	2.2E-5	
2. LOOP				
a) Independent Failures Only	2.0E-4	1.1E-4	8.7E-5	2.6E-5
b) Multiple Errors Assumed	2.1E-4	1.2E-4	1.0E-4	
3. LOAC				
a) Independent Failures Only	3.6E-2	3.2E-2	3.2E-2	1.0E-2
b) Multiple Errors Assumed	3.6E-2	3.2E-2	3.2E-2	

5. EMERGENCY OPERATION

For the discussions below, refer to Figures 1 and 2.

5.1 Loss of Main Feedwater (LMFW)

Offsite power is available and the two motor-driven pumps (MDPs) start automatically upon trip of both Main Feedwater (MFW) pumps or low-low level in any one steam generator. Automatic actuation also occurs upon a Safety Injection signal. The turbine-driven pump starts automatically upon low-low level in any two steam generators by the opening of the DC Train C motor-operated steam admission valve 5106. Unless the normally aligned Condensate Storage Tank 001 contains an inadequate supply of water and pump suction has not already been aligned to the standby CST 002, there are no other closed valves which must be opened either manually or automatically to initiate auxiliary feedwater flow. Transfer to the alternate CST 002 must be done manually, either from the Control Room or locally, by opening the motor-operated valves 5113, 5118 and 5119. The operator can remotely manipulate the position of the AFW flow control valves (5120, 5122, 5125, 5127, 5132, 5134, 5137, and 5139) to control steam generator level. This can also be done locally at the valves. Upon reaching 100 GPM or greater pump flow rate, the motor-operated isolation valves in the recirculation mini-flow lines of each MDP are automatically isolated so that there is no recirculation flow during most of AFWS operation, except for the continuous recirculation flow of the TDP. If the motor-operated valves in the miniflow lines of trains A and B fail to close, there is still sufficient flow to the steam generators because of the presence of a flow-limiting orifice to the miniflow lines.

5.2 Loss of Offsite Power (LOOP)

In this case, with no offsite power available, the MDPs can only be started after receiving an automatic signal from the diesel generators sequencing logic. The TDP is automatically started upon LOOP. The Reactor Coolant Pumps are not powered so that cooldown of the reactor core is by natural circulation. BNL has assumed that the required flow rate is 510 GPM, the same as the LMFW case because of the lack of information concerning this in the applicant's FSAR and reliability analysis. This still results in only one MDP being required.

All valve orientations and manipulations are the same as for the LMFW case, except that the steam admission valve, 5106, is automatically opened to start the TDP directly upon a LOOP signal. Steam generator level control is again either remote from the Control Room or local manual.

5.3 Loss of All AC Power (LOAC)

Since both offsite and onsite power are unavailable, only the steam turbine-driven pump is available to supply AFW flow. All valves in the TDP train, including the flow control valves, are supplied with DC power so that the operator has complete control capability of the single TDP train from the Control Room without requiring local manual actions unless there are component failures. All of the motor-operated valves in the TDP train are powered from a separate DC train designated Train C which derives power from AC Train A with backup power provided by batteries. Therefore, Train C DC power can be assumed to be independent of Train A DC power because it is backed by dedicated batteries which would become the sole power source for the LOAC condition.

Since the LOAC condition includes a blackout sequence signal, the TDP is automatically actuated upon LOOP by opening steam supply valve 5106. For the same reasons explained previously, BNL has assumed that the required flow rate is 510 GPM. Again, the Reactor Coolant Pumps are not powered so that cooldown of the reactor core is by natural circulation. Steam generator level control is performed manually either from the Control Room or locally at the valves.

6. TESTING

The applicant has based his analysis with regard to testing on the following information which has been taken from FSAR Appendix 10A. As of the date of the applicant's evaluation, the Technical Specifications, operating procedures, maintenance procedures, and testing procedures applicable to the VEGP AFWS were not written. Thus, in order to model and analyze the contribution of human error, testing and maintenance to the unreliability of the VEGP AFWS, relevant generic documents were used.

The Technical Specifications used were extracted from the Westinghouse Standard Technical Specifications.(5) The most notable factors of these preliminary Technical Specifications are (with respect to testing):

a. The testing frequency for AFWS pumps is once every 31 days.

b. The testing frequency of pumps and valves with automatic actuation is performed once every 18 months.

c. The testing frequency of each DC train is once every 7 days.

BNL interprets item b. to mean that the automatic actuation signal of pumps and valves is tested every 18 months, not that the pumps and valves themselves are tested every 18 months. BNL also assumes that testing of the automatic actuation signals and the DC trains does not cause those components to be unavailable during the test.

In addition, according to Ref.3, the generic plant testing and maintenance procedures used in the AFWS reliability evaluation were a synthesis of generic procedures. These generic procedures are based on current industry practice, lessons learned from previous human reliability analysis, and the VEGP AFWS design capabilities. Those procedures relevant to testing are:

a. The motor-operated valves in the discharge lines (5120, 5122, 5125, 5127, 5132, 5134, and 5137) are used to manually throttle AFWS flow and pressure during testing to keep AFWS flow from entering a steam generator.

b. The motor-operated valves in the discharge lines receive an automatic actuation signal to go to their full-open position even if they are being used for testing.

c. The only valves requiring manual realignment for testing or flushing are the recirculation bypass valves (81, 82, 83, and 84).

d. If a single recirculation bypass valve has not been closed, there is still sufficient flow to the steam generators due to the presence of a flow-limiting orifice in the recirculation line.

e. The motor-operated valves from CST 002 (5113, 5118, and 5119) are manually controlled with no automatic signals to close (if CST 002 is being used for testing or flushing of an AFWS train).

f. Valve position after a test is checked by a single operation.

The pump testing procedure requires further discussion. According to Ref.3, the design capabilities of the AFWS allow flushing or testing while the plant is operating without affecting main feedwater flow. The alignment of any train of the AFWS for testing or flushing is such that suction is taken from a CST and the flow passes through the pump and discharge lines where the motor-operated valves in the discharge lines are used to throttle the flow and pressure. The flow is then diverted away from the steam generators prior to the stop check valves by the manual opening of the bypass (recirculation) valves and discharged to the condensate system. Each recirculation line is fitted with an orifice that limits the amount of flow diverted away from the steam generators. This allows sufficient flow to the steam generators should the AFWS be required during flushing or testing. When not in use, the recirculation valves (81, 82, 83, and 84) remain closed. Also, upon receipt of any of the AFWS automatic actuation signals, the discharge (control) valves go to the full-open position if not already open. Although the applicant states that failure to close the recirculation valves after a test, or during a test in which the AFWS is required, does not result in excessive flow diversion, it is not clear that this is true when only one MDP is available. In particular, if either MDP has a capacity of 630 GPM at steam generator pressure with the mini-flow recirculation lines closed, a diversion of more than 120 GPM through the test recirculation line would result in a flow rate below the required 510 the GPM LMFW (see Table 3). To see the effect of this, BNL has modeled failure to close the recirculation line valves as independent human errors coupled with testing of a single pump which can cause insufficient flow to the respective steam generator. The net impact on the final results is, however, quite small.

7. SURVEILLANCE REQUIREMENTS

As explained in the previous section, the Technical Specifications were extracted from the preliminary Westinghouse Standard Technical Specifications. The most notable of them with respect to surveillance are:

a. The verification frequency of the CSTs water volume is once every 12 hours.

b. The verification frequency of valves in the flowpath is once every 31 days.

The applicant's failure data is presented in Table 10A-4 of Ref.3 included in this report as Table 4. The above information is used in conjunction with the failure data for human acts and errors given in Table III-2 of NUREG-0611, which is provided as Table 5 of this report. From Table 4, it appears that the applicant has assumed operator errors for motor-operated valves only.

Pre-accident closure was given a $5x10^{-4}$ unavailability/demand which corresponds to the NUREG-0611 value for valves having control room position indication, which is the case for motor-operated valves. However, no pre-accident error was assumed for manual valves, which typically do not have such indication. BNL has assumed a value of $1x10^{-3}$/demand for valves whose position can be verified by the pump testing act and a value of $5x10^{-3}$/demand for valves whose position can not be verified.

Post-accident closure of motor-operated valves is assumed at $5x10^{-3}$/ demand, which is the NUREG-0611 value for a 30 minute allowable actuation time for a "Non-Dedicated" primary operator to actuate the AFWS. This does not consider the probability of the backup control room operator taking the proper action. In this case, the NUREG-0611 value for the overall estimated failure probability is $1x10^{-3}$, i.e., a 0.2 recovery factor, which is what has been assumed in the BNL analysis. No unavailability due to post-accident closure of manual valves is assumed.

DRAFT

8. OUTAGE LIMITATIONS AND MAINTENANCE

8.1 Outage Limitations

From the preliminary Westinghouse Technical Specifications, the limiting conditions of operation are:

a. With one AFWS pump inoperable, the limiting condition of operation action time to hot standby is 78 hours.

b With two AFWS pumps inoperable, the limiting condition of operation action time to hot standby is 6 hours.

c. With one or more steam generators inoperable, the limiting condition of operation action time is 1 hour.

d. With less than 330,000 gal in the CSTs, the limiting condition for operation action time to hot shutdown is 16 hours.

e. With one 125-V dc train inoperable, the limiting condition for operation action time to hot standby is 2 hours.

The above requirement essentially define a maintenance policy which does not allow more than one pump train or steam generator to be unavailable due to maintenance. Any secondary unavailability of a pump train or steam generator is assumed to be due to a failure discovered during testing of the remaining two pump trains. It should be noted that testing by itself does not cause pump unavailability, only the failure to reclose the recirculation bypass valve or reopen the throttled control valve to a steam generator. However, it is assumed that testing of only one pump train at a time is allowed.

8.2 Maintenance

The generic plant procedures contain the following items which pertain to maintenance:

a. The performance of maintenance on a component requires that the component be manually isolated on both the upstream and downstream sides.

b. The motor-operated valves in the miniflow lines of trains A and B (5154 and 5155) are subject to maintenance for calibration of the flow element actuation device in these valves.

The applicant has stated the required actions to perform component maintenance, i.e., the need for both upstream and downstream isolation. Maintenance has been assumed by the applicant for all pumps and valves, including check valves and manually operated check, gate and butterfly valves. However, the applicant did not assume maintenance for the diesel generators.

Although the applicant references both NUREG-0611 and WASH-1400(6) as sources for maintenance unavailabilities, the data values for valves appear to be substantially lower than those given in the referenced sources. In particular, the applicant's data compared to the sources is as follows:

Component in Maintenance	Applicant's Data	NUREG-0611/WASH-1400
Check, stop check motor-operated valves, trip and throttle valve, speed governing valve	2.17×10^{-6}	2.1×10^{-3}
Manual gate valves and manual butterfly valves on pump suction lines	7×10^{-8}	2.1×10^{-3}
Butterfly valves on CST discharge lines	4×10^{-7}	2.1×10^{-3}
Motor and turbine-driven pumps	5.8×10^{-3}	5.8×10^{-3}
Diesel generators	0	6.4×10^{-3}
125V DC electric power	2.4×10^{-6}	*

* out of NUREG-0611 scope

In the BNL analysis, the NUREG-0611/WASH-1400 data were used. However, maintenance was assumed only for motor-operated valves. All other valve maintenance was assumed to be zero.

The modeling of the fault trees and a complete comparison of the data assumptions are discussed in detail in Section 9.2 of this report.

9. RELIABILITY ANALYSIS

9.1 Qualitative Aspects

9.1.1 Mode of System Initiation

1. LMFW - As stated previously in Section 5, both MDPs start automatically upon loss of both MFW pumps or upon low-low level in any one steam generator. 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 both from the Control Room and locally. 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 by the diesel-generator sequencing logic once power is received from the diesel generators. The TDP is also automatically initiated by opening DC-operated valve 5106 by means of 125V DC Train C power provided either by the 120V AC power of the Train A diesel-generator through the inverters or by the dedicated battery backup power. All three pumps can again be manually started by the operator either from the Control Room or locally. Therefore, the applicant still complies with recommendation GL-1 mentioned above.

3. LOAC - In this case, only the TDP is available. Since this case implies LOOP, the TDP is again automatically initiated by opening valve 5106. The pump is normally aligned to CST 001. If the standby CST 002 must be utilized as the suction source, valve 5113 is powered by DC Train C and can be opened manually either from the Control Room or locally, although normally such alignment would have been performed prior to the transient. The TDP can also be manually initiated either from the Control Room or locally in this case. 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

According to Ref.3, the AFWS is aligned to be placed in service automatically in the event of a demand. Following the receipt of a safety injection signal, a two-out-of-four low-low steam generator water level signal from any one steam generator, a trip signal from both main feedwater pumps, or a loss of offsite power signal, the auxiliary feedwater discharge valves go to the full-open position if not already open and the two motor-driven auxiliary feedwater pumps are actuated and begin to deliver flow from the online CST to the steam generators. Once flow has been established, the motor-operated valves in the miniflow lines close automatically. The turbine-driven pump is actuated automatically on two-out-of-four low-low water level in any two steam generators or on a loss of offsite power signal. To actuate the turbine-driven pump, the normally closed dc motor-operated valve (5106) in the steam supply line to the turbine is opened automatically. The speed governing valve and the trip/throttle valve, which are in the same line as the steam inlet valve, are automatically controlled by the speed governor on the turbine-driven pump. Following a transient or accident, the minimum flow is delivered to at least two effective steam generators within 1 min of an automatic auxiliary feedwater actuation signal. Once the system has been actuated, the operator can remotely manipulate the auxiliary feedwater control valves in order to control steam generator water level.

For normal operation, the AFWS is used to fill and/or maintain the water level in the steam generators during startup, shutdown, and hot standby conditions. The AFWS may be actuated and controlled manually during normal operation or abnormal conditions. The motor-operated valves in the miniflow lines of mechanical trains A and B (5155 and 5154) can only be actuated automatically. Although not shown on Figure 1, safety-grade flow meters with both Control Room and remote shutdown panel 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.

For the specific cases covered by this review, system control is as follows:

1. <u>LMFW</u> - Steam generator level control is maintained by the operator manually modulating the motor-operated flow control valves in the pump

discharge lines to each of the four steam generators (MOVs 5120, 5122, 5125, 5127, 5132, 5134, 5137, and 5139). In the event that suction must be transferred from the primary condensate storage tank CST 001 to the standby tank CST 002, the normally closed MOVs 5113, 5118 and 5119 can be manually opened either from the Control Room or locally. There is no automatic pump trip on low suction pressure. The mini-flow lines around the MDPs are automatically isolated when pump flow is above 100 GPM while the mini-flow line around the TDP continuously operates.

There are two normally closed manual gate valves, 055 and 056, on a header which joins the two motor-driven pumps A and B together. Normally MDPA only supplies Steam Generators 1 and 4 while MDPB only supplies Steam Generators 2 and 3. By opening both of these valves, either motor-driven pump alone can supply all four steam generators.

2. <u>LOOP</u> - System control is basically the same as for LMFW. The only significant difference is that AC power is supplied by the diesel generators. Level control can still be accomplished by modulating the flow control valves in the discharge lines to the steam generators. Transfer to the standby condensate storage tank and use of one motor-driven pump to feed all four steam generators are also performed in the same way as for LMFW.

3. <u>LOAC</u> - In this case, only the turbine-driven pump and its flow paths are available. Since all motor-operated valves in its flow paths are DC-operated, the operator can still control steam generator level by modulating the flow control valves either from the Control Room or locally. In effect, the operator can perform all of the same functions as before with the TDP for LMFW and LOOP because the Train C DC power is backed up by its own dedicated batteries which are utilized when Train A 120V AC power is unavailable.

9.1.3 Effects of Test and Maintenance Activities

The effect of testing on this system has been previously discussed in Section 6. As noted in Section 8, the applicant has correctly stated that to perform maintenance on any component, the component must be manually isolated both upstream and downstream. This can quite easily incapacitate an entire pump train. For example (see Figure 1), if maintenance must be performed on one of the manual gate valves on any one of the discharge lines to the four steam generators from the TDP, valves 016, 019, 022, or 025, all four valves must be closed, therby incapacitating the TDP.

9.1.4 Availability of Alternate Water Supplies

There are two redundant condensate storage tanks which are each maintained above a minimum level of 330,000 gallons. The minimum water level of each CST is designed to maintain the reactor in a hot standby condition for 4 hours followed by a 5 hour cooldown period, at which time the residual heat removal system can be used to further cool the reactor coolant system. The combined minimum operating capacity of the CSTs (660,000 gal) is designed to allow a hot standby condition for 31 hours followed by a 5 hour cooldown period until operation of the residual heat removal system is initiated.

Each tank is a Seismic Category 1 structure and has a capacity of 480,000 gal. The minimum safety capacity is ensured by all nozzles of nonsafety systems being located on the storage tanks above the corresponding elevation. The condensate level in each tank is automatically maintained by a level control valve in the line (to the tank) from the demineralized water system, which actuates when the volume in the tank drops to 472,250 gal.

As the water in the online CST is depleted, the operator may manually realign the system so that the standby CST serves all three pumps. A separate line connects each pump to each CST.

Therefore, the applicant has taken substantial measures to ensure an adequate supply of alternate water sources. However, it should be noted that the check valves on the pumps' suction side, valves 013, 033, 051, 058, and 061 have had their flappers removed (see Figure 1). The reason for this is not explained. Such being the case, if and when the operator must transfer to the standby CST 002, it seems that the level in CST 001 will precipitously rise while the level in CST 002 will precipitously fall to equalize the static head. This is because there are effectively no check valves on the pump suction side, so that flow from CST 002 does not isolate CST 001. This might cause some momentary confusion on the operator's part and possible misinterpretation of instrument readings.

The specific emergency procedures for transferring to the standby CST have not been provided in Ref. 3. The procedures should include criteria to inform the operator when the transfer to the standby CST should take place, and should meet all other requirements described in Recommendation GS-4 of NUREG-0611. Ref. 3 does indicate that there are level indicators and alarms both in the Control Room and locally for the CST water level to allow the operator to anticipate the need to makeup water or transfer to the alternate CST to prevent a low pump suction pressure from occurring. It does not indicate whether the indicators and alarms are redundant and 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 Seperation of Power Sources

According to Ref. 3, physical separation between the trains of the AFWS is maintained with regard to the prevention of common cause failures created by fire, flooding, and missiles. The simplified piping layout schematic of the AFWS is provided as Figure 3 of this report. Excluding the containment building, there are only two locations where a portion of all three trains lie in a common area. The first is in the building that houses the CSTs and the second is in a pipe chase in the auxiliary feedwater pumphouse. Both of these locations:

a. are protected from external missiles and have no internal source for missiles,

b. have no components subject to disabling damage due to flooding, and

c. have minimal sources of fire.

Physical separation between electrical components of the AFWS is provided in accordance with Regulatory Guide 1.75 and Institute of Electrical and Electronics Engineers (IEEE) Standard 384.

9.1.6 Common Mode Failures

In BNL's judgement, there are two obvious aspects of the Vogtle AFWS design which yield potentially significant common mode failure contributions to the system unavailability. See Figures 1 and 2. The first aspect involves the manuallly operated stop check valves at the steam generator inlet lines, (113, 114, 115 and 116). If the operator inadvertently closes, any three of the four valves, the mission success criteria is violated. Closure of one of these valves prevents the flow from both of the pumps which normally supply a steam generator. Even if the normally closed inter-connection between the two motor-driven pumps, valves 055 and 056, is open, flow can still not enter the steam generator from the alternate motor-driven pump.

The other aspect is the testing of the turbine-driven pump coupled with common mode failure to close at least two of the recirculation line valves, (81, 82, 83, 84) causing excessive flow diversion form the steam generators. Both of these cases are quantitatively assessed in Section 9.2.3.2. The applicant's own common cause analysis, according to Ref. 3 was performed deterministically and in two parts. The first part was performed explicitly for common cause hardware failure by location, and is discussed in the preceding Section 9.1.5 on physical separation. The second part of the common cause analysis was performed implicitly throughout the evaluation. According to the applicant, the results of the entire common cause analysis revelaed no significant common cause potential within the VEGP AFWS.

9.1.7 Single Point Failures

There were no single point failures discovered during the course of this review.

9.1.8 Adequacy of Emergency Procedures

The applicant has not provided emergency procedures at this time. Such procedures should be provided 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

In Ref. 3, the applicant states that the initial fault tree was developed to the component failure mode level and then expanded to the component failure cause level. The component failure causes considered were:

a. Random failure on demand.
b. Unavailability due to testing.
c. Unavailability due to maintenance.
d. Independent human error during testing or maintenance.
e. Common cause human error during testing or maintnenance.

The fault tree developed for the analysis is shown in FSAR Figure 10A-7, Sheets 1 to 30, included in this report with BNL modifications as Figure 7, Sheets 1 to 33.

Although the applicant states that unavailability due to testing and common cause human error during testing or maintenance were considered in the fault tree, BNL was not able to locate any such aspects in our review of both the fault tree and the applicant's assumptions in Table 3. Neither the fault tree nor the data table contain specific fault identifiers so that the applicant's results can not be unequivocally duplicated. Nevertheless, the fault tree is very comprehensive and great care was evidently taken to correctly model maintenance acts on all pumps and valves. However, the important contribution of diesel-generator maintenance was omitted.

In addition, the fault tree does not model maintenance acts excluded by technical specification requirements in any useful way, particularly considering that the applicant utilized in WAM-CUT(7) computer code. Specifically, in Figure 10A-7, Sheets 2 through 9 (BNL Figure 7, Sheets 3 through 10), show that the inputs to the AND gates :"NOIF TO SG__ FROM TRAIN __ DUE TO MAINTENANCE" and a NOT gate described as "DOES NOT VIOLATE TECHNICAL SPECIFICATIONS".

Obviously the latter gate cannot be utilized as described in any computer code because it does not identify exactly which coincident maintenance events are to be excluded. It is therefore not clear just exactly how the applicant arrived at his numerical results. When utilizing the WAMCUT code, there are basically two approaches to elimination of disallowed coincident test and/or maintenance acts. The first is to make extensive use of NOT gates, while the second is so to define the top event that disallowed maintenance and test acts are inherently excluded.

BNL utilized the SETS code (8) to quantify the results. SETS allows both of the methods mentioned above; additionally, it allows a third method. In the third method, the top event is defined so as to allow unlimited coincident test and maintenance acts; the cutsets are then processed by SETS to eliminate those which are to be disallowed by the Technical Specifications. This is discussed further in Section 9.2.3, BNL Assessment.

9.2.1.2 Failure Data

The applicant's failure data are shown in Table 10A-4, which is included in this report. The data is in substantial agreement with the data prescribed in Table III-2 of NUREG-0611 (see Appendix A), with the very notable exception of valve and diesel generator maintenance unavailabilities. The applicant's data values for valve maintenance are extremely low, ranging from $7x10^{-8}$ to $2.17x10^{-6}$, as compared to the NUREG-0611 value of $2.1x10^{-3}$, while diesel generator maintenance was neglected. The references cited are NUREG-0611 and WASH-1400, but BNL cannot ascertain how the applicant derived his values from those sources.

Reference 3 states: "All data were used to quantify point estimates of unavailability on demand, and uncertainty is not accounted for in the analysis. It should be noted that the data utilized in the reliability analysis is generic, and as such the results are an evaluation of the AFWS design. The implication of the data is that they do not account for the actual characteristics of how the plant is to be operated and maintained", (emphasis by BNL).

The situation of pre-accident operator error with respect to closing manually-operated valves appears to have been omitted from Table 10A-4. This subject is further discussed in Section 9.2.3, BNL Assessment, since it has a significant impact on the quantitative results.

A minor comment: the applicant's data include a maintenance unavailability of $2.4x10^{-6}$ for 125-V DC electric power, while random failure was neglected. It does not appear that maintenance unavailability was included in the fault tree, while random failure was included.

9.2.2 Applicant's Results

9.2.2.1 System Unavailabilities

According to Ref. 3, the quantitative results of the conditional unavailabilities for the three cases designated by the NRC for the AFWS are:

A. Case 1 - LMFW - For the case where there is an assumed loss of main feedwater with a reactor trip occurring and offsite AC power available, the conditional unavailability of the AFWS was calculated to be 6.3×10^{-6}.

B. Case 2 - LMFW/LOOP - For the case where there is an assumed loss of main feedwater with a reactor trip occurring and offsite AC power not available, the conditional unavailability of the AFWS was calculated to be 2.6×10^{-5}.

C. Case 3 - LMFW/LOAC - For the case where there is an assumed loss of main feedwater with a reactor trip occurring and no AC power available, the conditional unavailability of the AFWS was calculated to be 1.0×10^{-2}.

9.2.2.2 Dominant Failure Modes and Conclusions

It is stated in Ref. 3 that the quantitative measure of importance was used as an indication of the dominant contributors to the AFWS conditional unavailability. The value of importance was then taken as the sum of all cut set probabilities containing a category of failure divided by the top event probability. The failure catetories analyzed for each case are: random failure of valves on demand; unavailability of valves due to maintenance; operator error; and pump unavailabilities (random or maintenance).

The applicant's dominant failure modes and conclusions for each case are as follows:

A. Case 1 - LMFW - The most significant contributor to system failure was pump unavailabilities. The importance value to pump unavailabilities was calculated to 86 percent. An examination of the category of pump unavailabilities revealed that pump failures were occurring in combination with electric power system failure. Furthermore, it was determined that the unavailability of the turbine driven pump was not the most significant single component of the AFWS, but this pump did not dominate system unavailability.

and?

B. Case 2 - LMFW/LOOP - The findings for Case 2 revealed pump unavailabilities contribute 80 percent to system unavailability. An examination of this category revealed, as did Case 1, no single component of the AFWS can be thought of as dominating (or controlling) system unavailability. The reduction of the system conditional availability for this case was found to be directly attributable to the assumed loss of redundancy in ac power sources.

C. Case 3 - LMFW/LOAC - The findings for Case 3 revealed (under assumed conditions) that the AFWS is reduced to only the turbine-driven pump. Thus, any single failure along this pump train would be sufficient to fail the AFWS. The dominant contributors to system unavailability were as follows:

1. The turbine-driven pump package (pump, trip throttle valve, and speed governing valve).
2. The steam inlet valve (motor-operated valve 5106).

9.2.3 BNL Assessment

9.2.3.1 Fault Trees

Since the applicant's fault trees, provided in Ref.3, seem to be substantially correct and complete, particularly with respect to the modeling of maintenance acts at the component level, these same fault trees with minor revisions were utilized in the BNL analysis, provided in this report as Figure 7, Sheets 1 to 33. The major revisions which were necessary were the addition of fault identifiers and a finer separation of certain maintenance acts so the top event could be properly identified and the non-functional event "Does Not Violate Technical Specifications" eliminated. The fault identification nomenclature scheme is shown in Table 6. The applicant did not separate the steam generator intake sections in the expanded block diagram, Figure 6, into random and maintenance contributors because no maintenance can be performed on either of the two check valves or the stop check valve in a typical intake section, e.g., check valves 121 and 125 and stop check valve 113 on Steam Generator 1 Intake. However, BNL did so in order to model both maintenance on the stop check valves on the pump discharge lines to a given steam generator and also a possible unavailability due to testing if the operator fails to reclose the recirculation valve in the condensate system return line. See Figure 7, Sheets 12 and 13.

Another significant revision was the inclusion of diesel generator maintenance unavailability on Sheets 14 and 15. There were other minor revisions which are identified on the fault trees. It should also be noted that the top event on Sheet 1 was modified to show the actual gate names and the Boolean expression which was used to replicate the 3 out of 4 combination gate used by the applicant in the WAM-CUT code. The SETS code used by BNL does not utilize combination gates.

The fault trees as shown allow unrestricted coincident test and maintenance acts. Those acts which are not allowed by the Technical Specifications were then deleted from the cutsets by use of the DELETE TERM option of the SETS code. Specifically, the equation establishing the terms to be deleted is based on the Expanded Reliability Block Diagram in Figure 6, and is given below:

DELETE = A*B + B*C + A*C

A = PMPAMAINT + A1MAINT + A4MAINT + TAMDPAC03

B = PMPBMAINT + B2MAINT + B3MAINT + TAMDPB002

C = PMPCMAINT + C1MAINT + C2MAINT + C3MAINT + C4MAINT + TATDPC001

After cutsets are obtained, they are processed to eliminate failure combinations which imply event "DELETE."

This essentially disallows simultaneous maintenance on or testing of two or three pumps, or one pump and one of the discharge flow paths of another pump, or two or more discharge flow paths when each flow path is supplied by a different pump.

9.2.3.2 Failure Data

A general comparison between the applicant's data assumptions and those utilized by BNL is provided in Table 7.

The most important aspects of the applicant's data in terms of sensitivity in the quantitative results are the maintenance unavailabilities assumed for all valves and the pre-accident human error assumed for the operator inadvertently closing a manual valve. The applicant's assumptions for valve maintenance are extremely low compared to the NUREG-0611 data, ranging from 7E-8 to 2.17E-6, while the BNL assumption was 2.1E-3, based on NUREG-0611 data, for all motor-operated valves and 0 for all manually-operated valves and check valves.

Similarly, the applicant appears to have assumed 0 for the pre-accident operator error of inadvertent closure of a manually-operated valve. The BNL assumptions for this case were 5E-3 for locked-open manual valves whose position cannot be verified as a result of the testing of its associated pump and 1E-3 if testing does allow position verification. This has very important implications for the manually-operated stop check valves 113, 114, 115, and 116 at the AFW intake to each steam generator. Since each valve lies in a common discharge path for the two AFW pumps which supply any given steam generator, its inadvertent closure blocks all AFW flow to that steam generator.

It does not appear that pump testing per se can verify the position of those valves because, during the pump test, the discharge pressure is throttled by the motor-operated valves (5120, 5122, 5125, 5127, 5132, 5134, 5137, and 5139) so that flow does not enter the steam generators but is diverted to the Condensate System through the recirculation bypass valves. Thus, no flow passes through the locked-open stop check valves in question. In the NRC Standard Technical Specifications (4), periodic surveillance is generally not required if a valve is locked into its emergency position. Thus, the only way for the position of these valves to be verified appears to be by a voluntary visual inspection during a pump test. However, for independent failures, utilizing the post-accident recovery factor of 0.25 is specified in Table 5 for 30 minutes allowable time, yields (5E-3)*(0.25) Δ 1E-3. The common mode failures described in Section 9.1.6 have been quantified and added to the system unavailabilities for independent failures only, (as shown in Table 8) as follows:

NOFLOSGS1234 = CRVLO*OEFTCCRVS+CMOESCVS*OEFTOSCVS (1)

CRVLO = CMOECRVS + TATDPC001 (2)

where NOFLOSGS1234 = Multiple error contribution to the probability of no flow to steam generators 1, 2, 3, and 4.

CRVLO = probability of the condensate return valves (081, 082, 083, 084) being in the open position.

OEFTCCRVS = probability of the operator failing to close the condensate return valves after automatic AFWS initiation, 5E-3.

CMOESCVS = Common mode probability of pre-accident operator error in leaving the manually-operated stop check valves (113, 114, 115, 116) in the closed position, 1E-3.

OEFTOSCVS = probability of the operator failing to open the stop check valves after automatic AFWS initiation, 5E-3.

CMOECRVS = Common mode probability of pre-accident operator error in leaving the condensate return valves in the open position, 1E-3.

TATDPC001 = probability of the turbine-driven pump undergoing test, which requires that the condensate return valves be open, 6.4E-4.

Substituting (2) into (1)

NOFLOSGS1234 = (CMOECRVS+TATDPC001*.(OEFTCCRVS)
+(CMOESCVS)*(OEFTOSCVS)
=(1E-3+6.4E-4)*(5E-3)+(1E-3)*(5E-3)
= 8.2E-6+5E-6=1.3E-5

Therefore, 1.3E-5 is the multiple error contribution to the top event from either misalignment of multiple stop check valves or misalignment of multiple condensate return valves.

For each of the initiators, and for different error probabiities associated with other valves, Table 8 provides results calculated with and without this contribution. The purpose of this is to display the effect of the assumptions which have been made, which, in the present case, must be regarded as ingredients of a parametric sensitivity study. It is unclear whether opening all of the condensate return valves really fails the system. If not, then the corresponding contribution if 5.E-6 (see above) should be subtracted from the system unavailability quoted in all "Case b" entries in Table 8, and from the results given in the Executive Summary.

9.2.3.3 System Unavailabilities

A sensitivity comparison between the applicibutors because no maintenance can be performed on either of the two check valves or the stop check valve in a typical intake se LOAC in which the following assumptions have been made: ?

1) Case A - All manual valves are assigned a pre-accident operator error rate of 5E-3/demand plus a 1E-4/demand for plugging.

2) Case B - All manual valves are assigned a pre-accident operator error rate of 1E-3/demand plus a 1E-4/demand for plugging except the manually-operated stop check valves at the steam generator intake lines (113, 114, 115, 116) which have a pre-accident operator error rate of 5E-3/demand.

3) Case C - All manual valves are assigned a pre-accident operator error rate of 1E-3/demand plus a 1E-4/demand for plugging. The manually-operated stop check valves 113, 114, 115 and 116 are evaluated with a recovery factor of 0.25, which also equates to a 1E-3/demand failure rate.

The purpose of presenting results in this way is to display more clearly the effects of certain assumptions. In many similar analyses of Westinghouse systems, credit has been taken both implicitly and explicitly for operator action to recover certain errors. Here, choosing lower error probabilities corresponds, in effect, to taking more credit for recovery.

For the purpose of selecting the proper assessment for compliance with the NUREG-0611 guidelines, and correspondence with the applicant's actual design, BNL has chosen Case C with common mode failures included for the final evaluation provided in Tables 1 and 2 in the Executive Summary.

9.2.3.4 Dominant Failure Modes

The results of the BNL analysis are provided in Figures 8, 9 and 10 for Case B of Table 8, assuming independent failures only.

1. Case 1 - LMFW

The dominant failure modes are shown in Figure 8. The leading group is random failure of one pump combined with maintenance outage of a second pump and random failure of one of the manual stop check valves on the steam generator inlet lines supplied by the third pump. The next significant set is random failures of three out of four of the manual stop check valves on the steam generator inlet lines, followed by random failure of two pumps and one of the manual stop check valves supplied by the third pump.

2. Case 2 - LOOP

The dominant failure modes for this case are shown in Figure 9. The leading group is random failure of both diesel generators (ACTRNAF and ACTRNBF) combined with random or maintenance acts on the turbine-driven pump train. The next major group is maintenance acts on one of the pumps combined with random failure of one of the diesel generators and random failure of either one of the manual stop check valves on the steam generator inlet lines supplied by the third pump or random failure of the third pump itself.

3. Case 3 - LOAC

The dominant failure modes are shown in Figure 10 for this case. As expected, single random failures or maintenance acts on the turbine-driven pump itself or one of the several valves on the turbine inlet supply line comprise the predominant group of failure modes. At much lower failure probability rates, the next group consists of double failures pertaining to random failures of the locked-open manually-operated butterfly valves on the condensate storage tank supply lines to the turbine-driven pump suction combined with random failure of or operator failure to open the normally-closed motor-operated valves isolating the turbine-driven pump suction from the standby condensate storage tank.

9.2.3.5 General Comparison to Other Plants

The Vogtle AFWS design is similar to many other plants in that it consists of two motor-driven pumps and a third pump which is steam turbine-driven. It does have several notable features such as two redundant, safety-class, condensate storage tanks each of which has sufficient capacity for an extended cooldown and satisfaction of the design basis requirements. Transfer to the standby tank must be done manually. Another feature is the provision of a third, independent train of DC power for the TDP and its associated motor-operated valves, designated as 125 V DC Train C power. In this manner, failure of either DC Train A or Train B fails only one of the MDPs, not an MDP and the TDP simultaneously.

Also, since the motor-operated throttle valves on the TDP discharge lines to the SGs are DC-powered by Train C, SG level control can be maintained by the operator from the control room even during a LOAC transient.

The location of the test recirculation lines very close to the SG intakes allows the position of all valves on the pumps' discharge lines with the exception of the manually-operated stop check valves on the inlet lines to each SG (113, 114, 115, 116) to be verified by the pump testing.

The MDP headers are joined together by two normally-closed manual valves 055 and 056. By opening both of these valves, either MDP can be utilized to feed all four steam generators. This feature is also provided in several other AFWS designs.

Finally, the provision of the stop check valves 113, 114, 115, and 116 in the SG intake lines is rather unique. Although, as mentioned previously, the potential for human error blocking all AFW flow to an entire steam generator increases, the valves may provide additional safety margin in preventing the back-leakage of steam into the AFW lines.

9.2.3.6 General Comments

The Vogtle AFWS is a generally very well-designed system. The provisions for pump testing allow for nearly complete verification of the valve positions on the pump's discharge, the exception being the steam generator intake lines themselves. The inadvertent closure of the manually-operated stop check valves on the intake lines does, however, have a significant effect on the unavailability analysis. This effect is substantially reduced if the valves have control room position indication or if the operator can credibly recognize the problem and take appropriate actions outside the Control Room within the 30 minutes allowable action time.

The actual procedure for and the sequencing of pump testing was not adequately explained in the applicant's analysis. It is not clear how many of the recirculation bypass line valves to the Condensate System are simultaneously opened during the testing of any one pump. Presumably, the recirculation line valves for the two steam generators supplied by each MDP and the four valves for the four steam generators supplied by the TDP are simultaneously opened.

REFERENCES

1. U.S. NRC, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants," NUREG-0611, 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," dated March 10, 1980.

3. Georgia Power Corporation, "VEGP Auxiliary Feedwater System Reliability Analysis," VEGP FSAR Appendix 10A, current edition.

4. U.S. NRC, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants - LWR Edition - Section 10.4.9, 'Auxiliary Feedwater System'," NUREG-0800, Revision 2, July 1981.

5. U.S. NRC, "Standard Technical Specifications for Westinghouse Pressurized Water Reactors," NUREG-0452, Revision 4, Fall 1981.

6. U.S. NRC, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants - Appendices 3 and 4: Failure Data," WASH-1400 (NUREG75/014), October 1975.

7. Erdmann, R. C., Leverenz, F. L., and Kirch, H., "WAM-CUT: A Computer Code for Fault Tree Evaluation," EPRI-NP-803, Science Applications, Inc., June 1978.

8. Worrell, R. B., Stack, D. W., "A SETS Users Manual for the Fault Tree Analyst," NUREG/CR-0465, Sandia National Laboratory, November 1978.

Table 3 BNL Assumptions of VEGP NSSS Steam Generator Makeup Requirements Based Upon FSAR Information

Power Levels (MWt)	Flow Requirements (GPM) Loss of Main Feedwater (LMFW)	Loss of Offsite Power (LOOP)	Loss of All AC Power (LOAC)
3425	510	510	510

AFW Flow Information

Pump Discharge Flow (gal/min)			Pump Recirculation Flow (gal/min)		
Turbine-Driven Pump	Motor-Driven Pump A	Motor-Driven Pump B	Turbine-Driven Pump	Motor-Driven Pump A	Motor-Driven Pump B
852 at 1235 psia 120°F	552	552	144	0 (a)	0 (a)

(a) The motor-operated valves in the motor-driven pump recirculation lines are intended to close when the pump flow reaches the miniflow, 100 gal/min, within a minute. Thus, the motor-driven pump recirculation flow was not considered.

Table 4 TABLE 10A-4 (SHEET 1 OF 3)

AFWS COMPONENT FAILURE DATA

Fault Event/Tree Description	Component	Failure on Demand	Reference	Repair Time (h)	Unavailability Due to Maintenance	Reference
Check valve (at steam generator intake) fails to open on demand	121, 122, 123, 124, 125, 126, 127, 128	1×10^{-4}	1	NA	NA	NA
Stop check valve (at steam generator intake) fails to open on demand	113, 114, 115, 116	1×10^{-4}	1	NA	NA	NA
Stop check valve (on AFWS discharge) fails to open on demand	017, 020, 023, 026, 037, 040, 043, 046	1×10^{-4}	1	7	2.17×10^{-6}	1, 3
Motor-operated valve (on discharge line) transfers closed	5120, 5122, 5125, 5127, 5132, 5134 5137, 5139	1×10^{-4}	1	7	2.17×10^{-6}	1, 3
Gate valve (on discharge line) transfers closed	015, 016, 019, 022, 025, 035, 036, 039, 042, 045, 060	1×10^{-4}	1	7	7×10^{-8}	1, 3
Check valve (on discharge line) fails to open on demand	001, 002, 014	1×10^{-4}	1	7	2.17×10^{-6}	1, 3
Motor-driven pump fails (includes controls)	003, 002	5×10^{-3}	1	19	5.81×10^{-3}	1
Turbine-driven pump fails (includes controls)	001	5×10^{-3}	1	19	5.81×10^{-3}	1

Table 4 (Cont.) TABLE 10A-4 (SHEET 2 OF 3)

Fault Event/Tree Description	Component	Failure on Demand	Reference	Repair Time (h)	Unavailability Due to Maintenance	Reference
Motor-operated valve (on turbine intake) fails on demand	5106	3.1×10^{-3}	1	7	2.17×10^{-6}	1
Check valves (on turbine steam intake) fail to open on demand	006, 008	1×10^{-4}	1	7	2.17×10^{-6}	1, 3
Motor-operated valves (on turbine steam intake) transfer closed on demand	3009, 3019	1×10^{-4}	1	7	2.17×10^{-6}	1, 3
Gate valve (on turbine steam intake) transfers closed on demand	005, 007	1×10^{-4}	1	NA	NA	NA
Butterfly valve (on suction line) transfers closed	093, 094, 095	1×10^{-4}	1	7	7.0×10^{-8}	1, 3
Motor-operated valve (pump suction line) fails on demand	5113, 5118, 5119	3.1×10^{-3}	1	7	2.17×10^{-6}	1, 3
Butterfly valve (on CST discharge line) transfers closed	090, 091 092, 097, 098, 099	1×10^{-4}	1	40	4×10^{-7}	2, 3
CST fails	001, 002	1×10^{-8}	3	NA	NA	NA
Failure of actuation signal	Train A, train B, speed governor	7×10^{-3}	1	NA	NA	NA
Loss of offsite power	Case 1	0.2	3	NA	NA	NA
Failure of 125-V dc electric power	Train A, train B, train C	NA	NA	2	2.4×10^{-6}	3

Table 4 (Cont.)

TABLE 10A-4 (SHEET 3 OF 3)

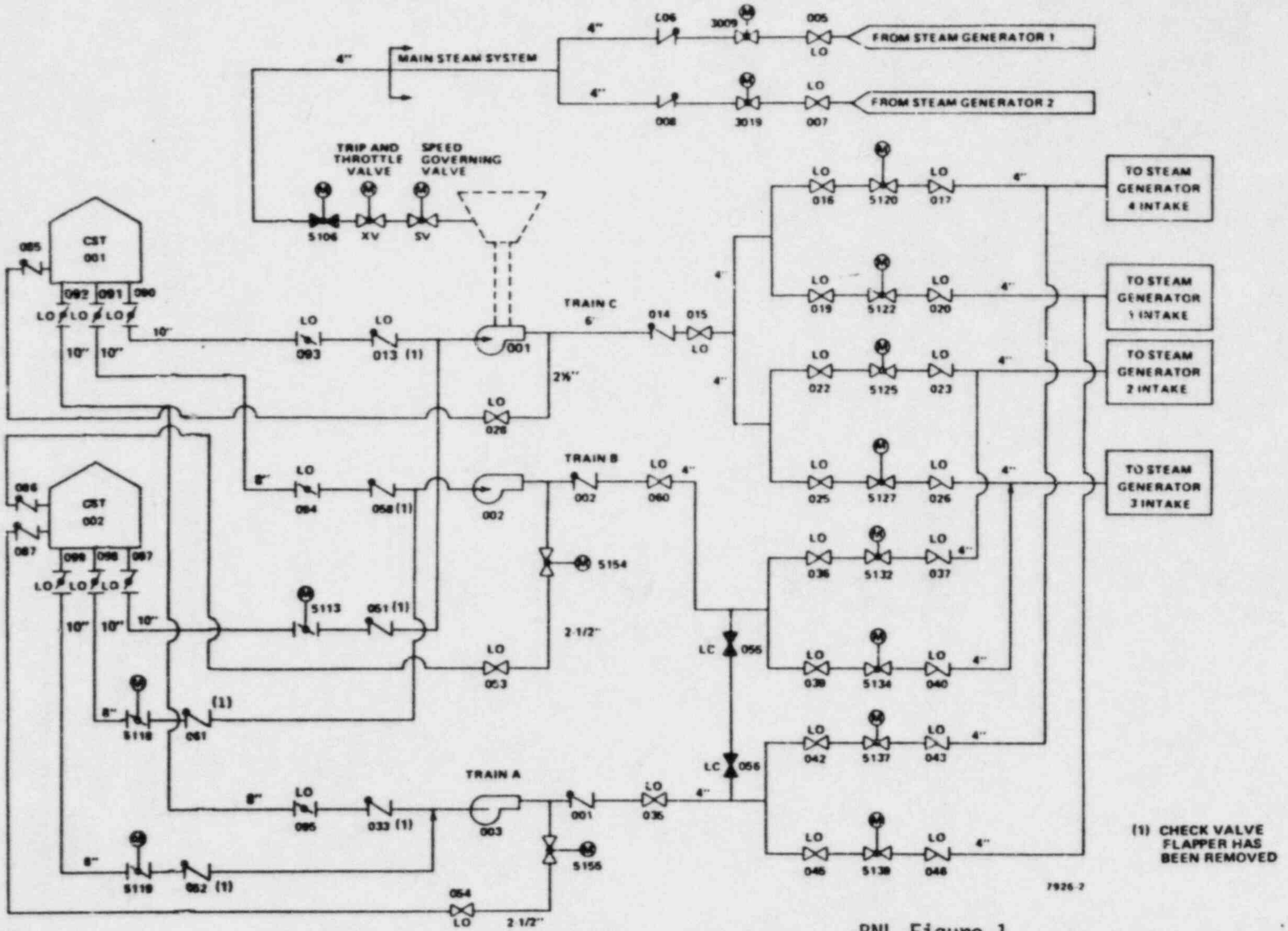
Fault Event/Tree Description	Component	Failure on Demand	Reference	Repair Time (h)	Unavailability Due to Maintenance	Reference
Failure of ac electric power (onsite - case 1 and 2)	Train A, train B	3×10^{-2}	3	NA	NA	NA
Motor-operated valve closed by error	3009, 3019, 5120, 5122, 5125, 5127, 5132, 5134, 5137, 5139	5×10^{-4}	1	NA	NA	NA
No manual open signal to motor-operated valve	3009, 3019, 5106, 5113, 5118, 5119, 5120, 5122, 5125, 5132, 5134, 5137, 5139	5×10^{-3}	1	NA	NA	NA
No manual start signal to pump	001, 002, 003, speed governor	5×10^{-3}	1	NA	NA	NA
Trip and throttle valve or speed governing valve fails to open on demand	Trip and throttle valve, speed governing valve	1.1×10^{-3}	1	7	2.17×10^{-6}	3

---

a. References

1. U.S. Nuclear Regulatory Commission, "Generic Evaluation of Feedwater Transients and Small-Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants," NUREG-0611, Bulletins and Orders Task Force, Office of Nuclear Reactor Regulation, January 1980.
2. Engineering judgment.
3. Rasmussen, N. C., *et al.*, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commerical Nuclear Power Plants," U.S. Nuclear Regulatory Commission, WASH-1400 (NUREG-75/014), October 1975.

b. Maintenance is defined to be maintenance whereby the component is unable to perform its function. Also, unavailability due to maintenance is calculated as the frequency of failure times the repair time.



(1) CHECK VALVE FLAPPER HAS BEEN REMOVED

BNL Figure 1

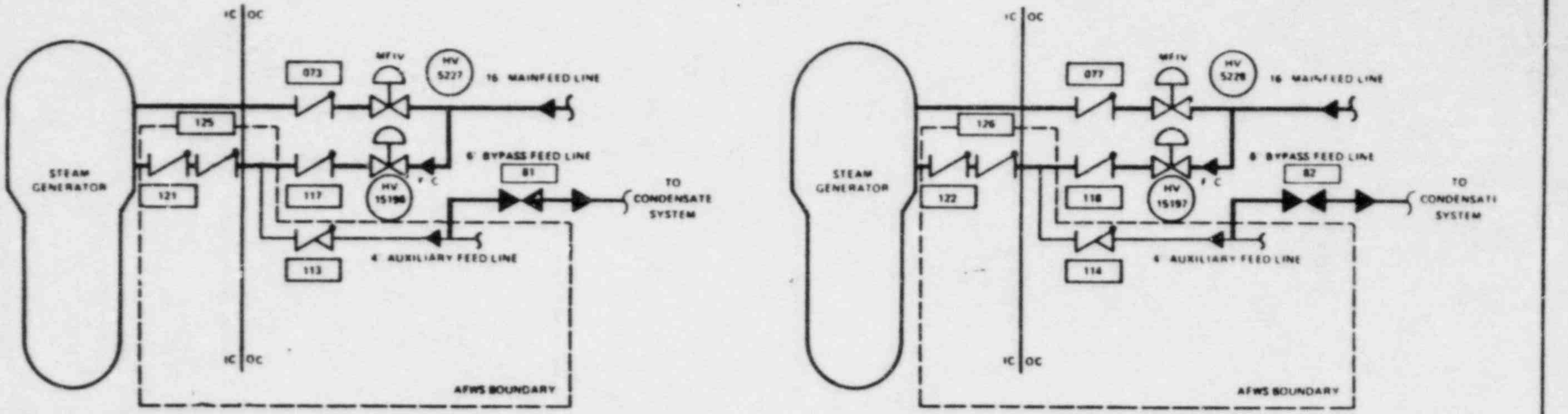
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

AFWS

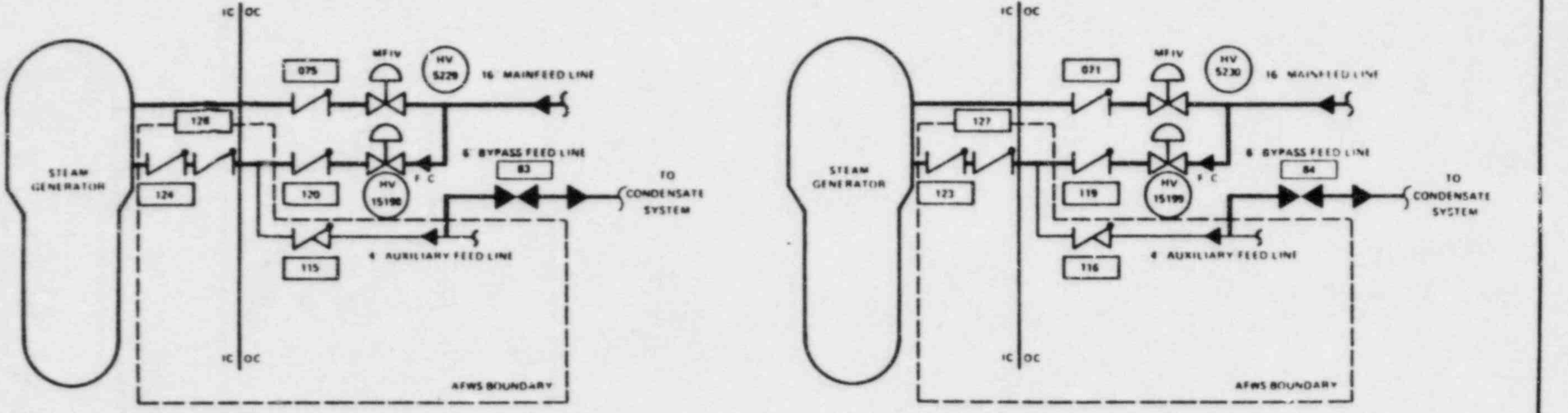
FSAR FIGURE 10A-1

433-9



STEAM GENERATOR 1 INTAKE

STEAM GENERATOR 2 INTAKE



STEAM GENERATOR 3 INTAKE

STEAM GENERATOR 4 INTAKE

BNL Figure 2

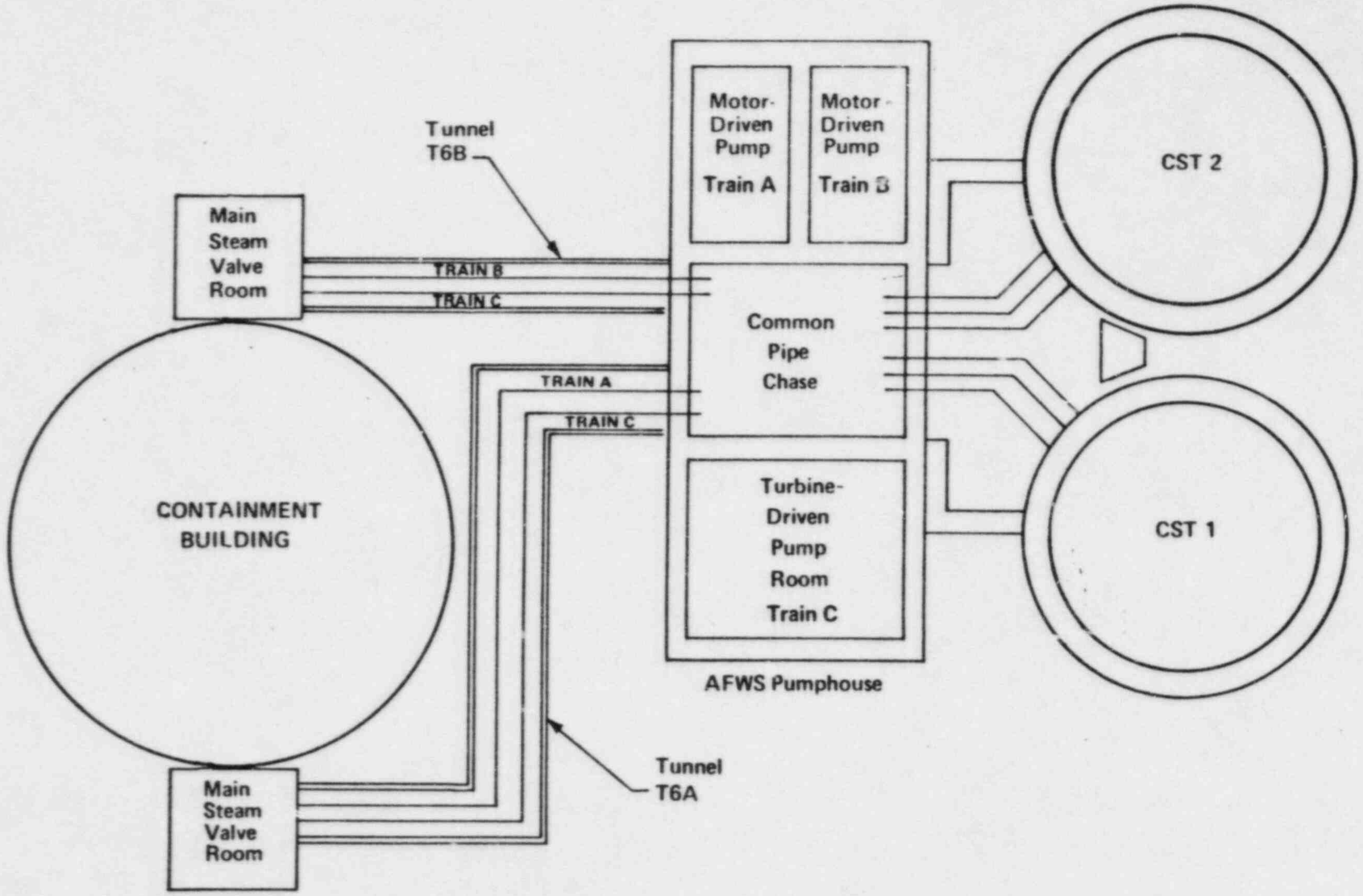
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AUXILIARY FEEDWATER/
STEAM GENERATORS INTAKE

FSAR FIGURE 10A-2

433-9



BNL Figure 3

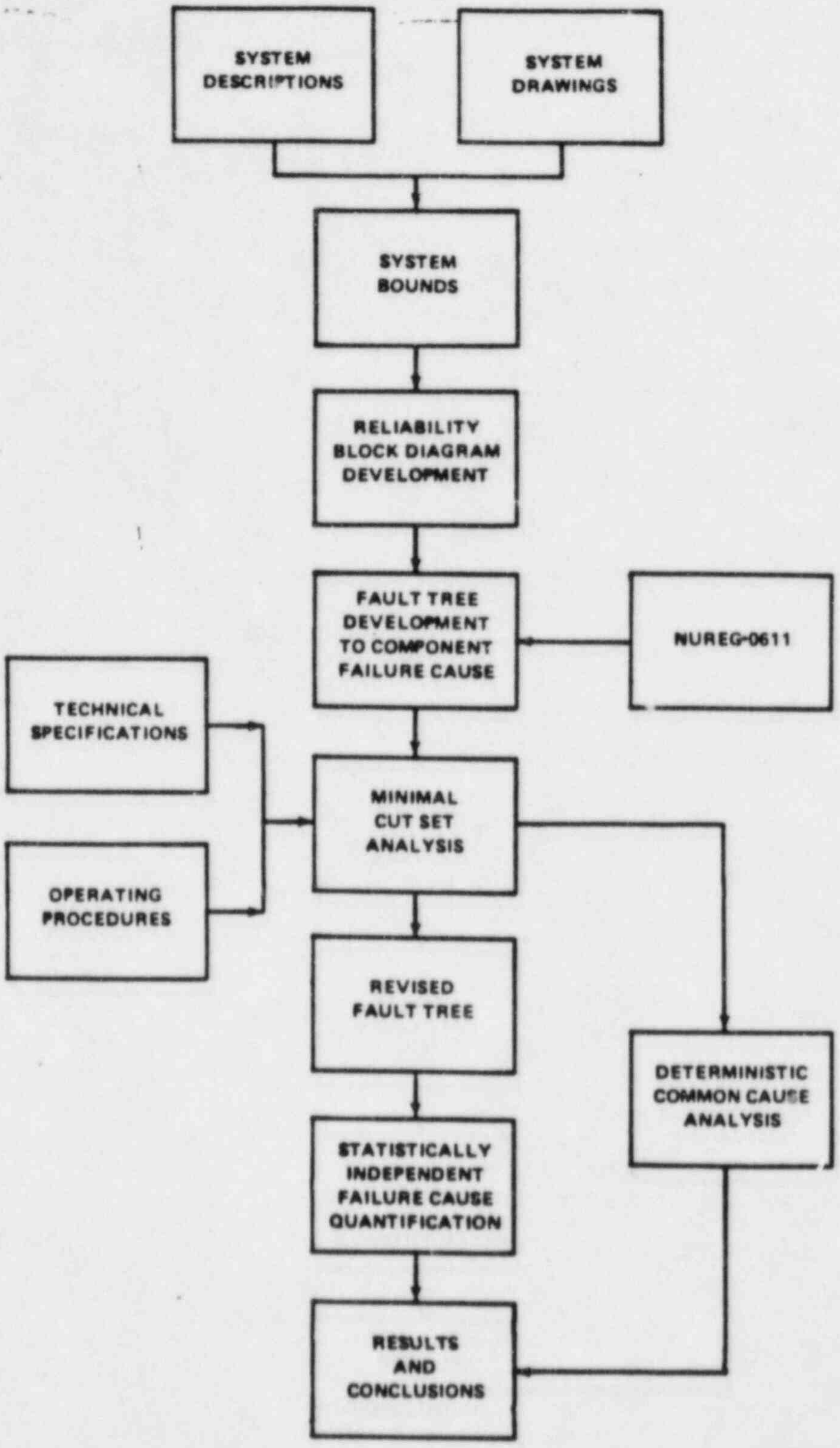
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

AFWS SIMPLIFIED PIPING LAYOUT

FSAR FIGURE 10A-3

433-9



BNL Figure 4

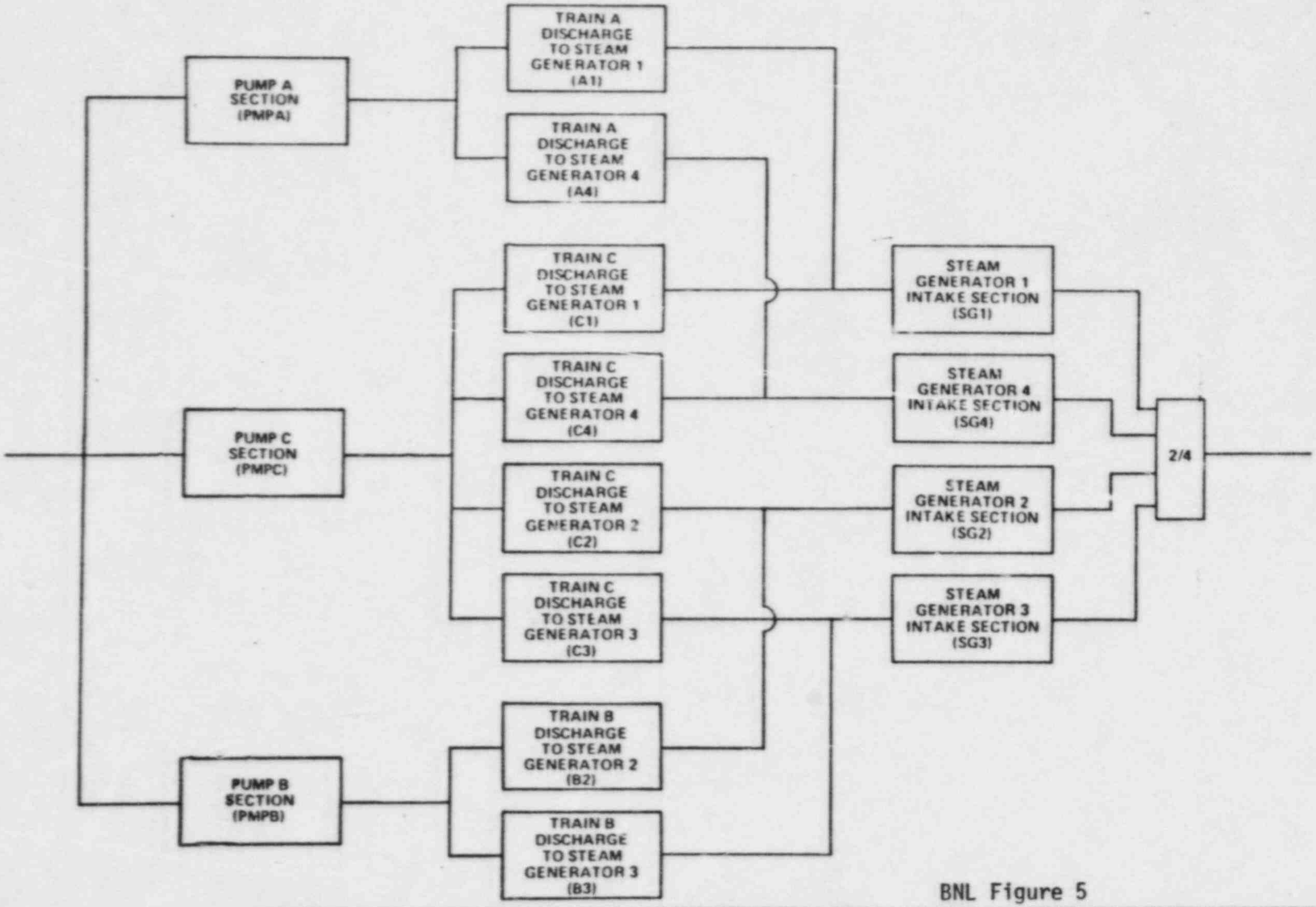
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

AFWS RELIABILITY EVALUATION
METHODOLOGY FLOW CHART

FSAR FIGURE 10A-4

433-9



BNL Figure 5

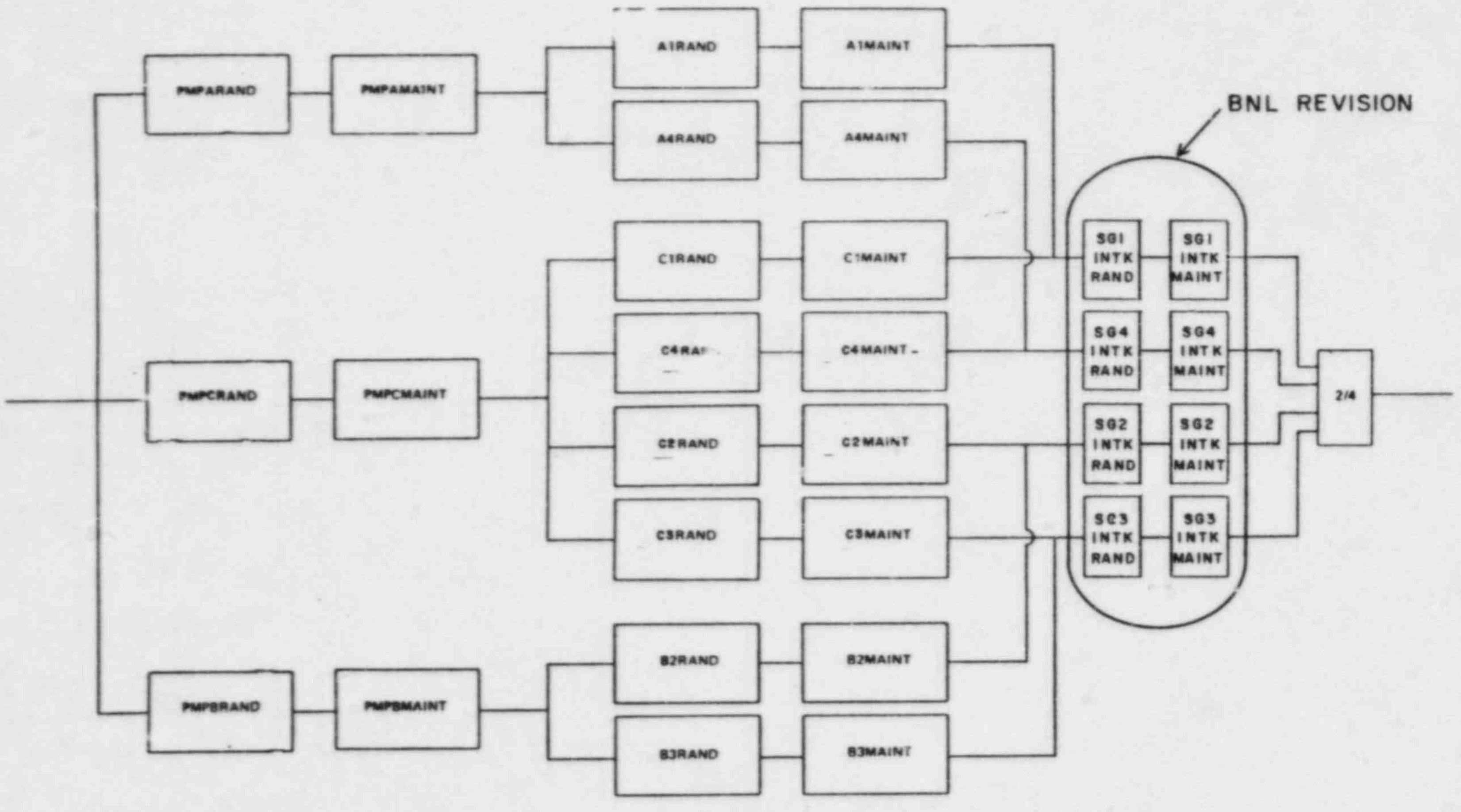
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS BLOCK DIAGRAM

FSAR FIGURE 10A-5

433-9



AFWS BLOCK DIAGRAM

BNL Figure 6

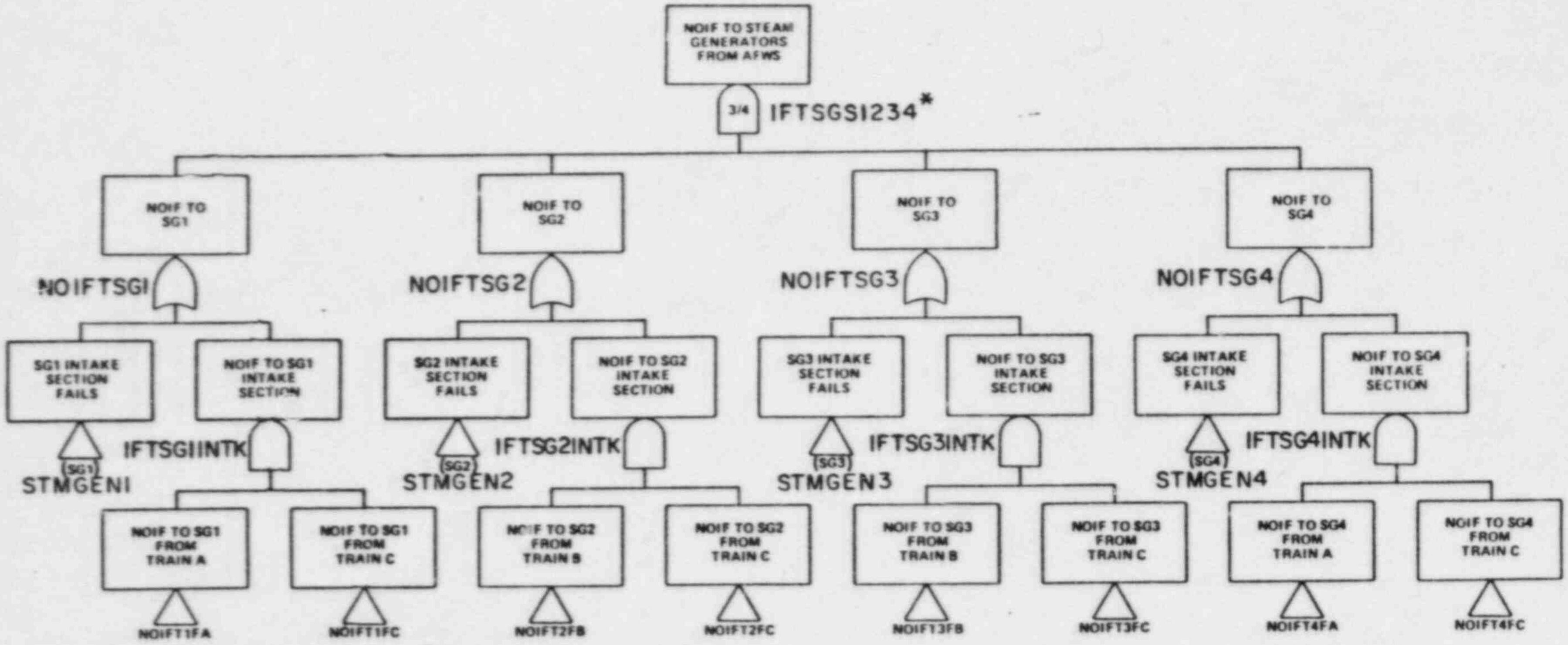
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

AFWS EXPANDED BLOCK DIAGRAM

FSAR FIGURE 10A-6

433-9



NOIF - NO OR INSUFFICIENT FLOW

10967-3

* IFTSGS1234 = STMGENS 123 + STMGENS 124 + STMGENS 134 + STMGENS 234

STMGENS 123 = NOIFTSG1 · NOIFTSG2 · NOIFTSG3

STMGENS 124 = NOIFTSG1 · NOIFTSG2 · NOIFTSG4

STMGENS 134 = NOIFTSG1 · NOIFTSG3 · NOIFTSG4

STMGENS 234 = NOIFTSG2 · NOIFTSG3 · NOIFTSG4

BNL Figure 7 (Sheets 1 of 33)

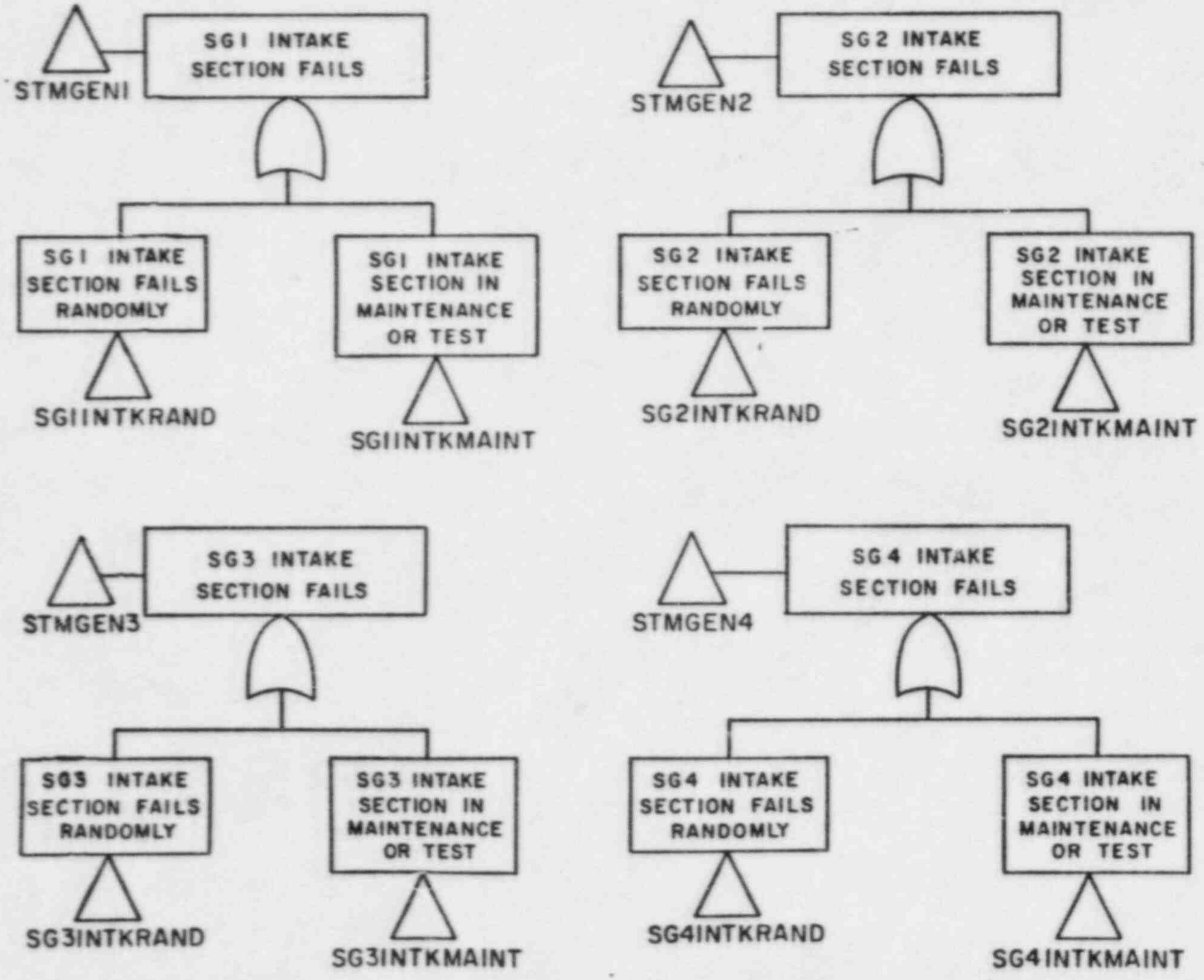
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 1 OF 30)

433-9



BNL Figure 7 (Sheet 2 of 33)

10967-3

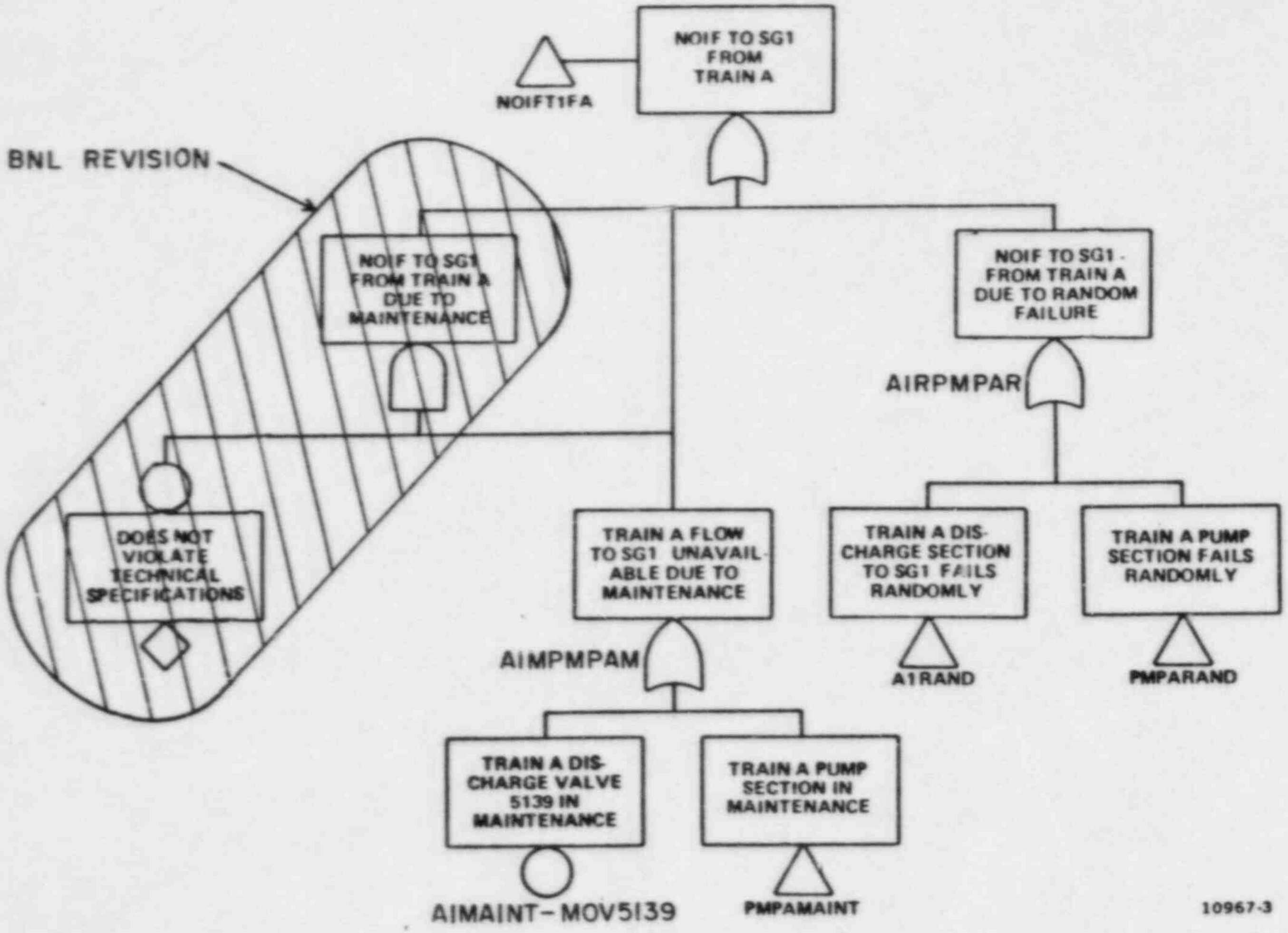
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
BNL ADDITION

FSAR FIG. 10A-7 SHEET 1A OF 30

433-9



BNL Figure 7 (Sheet 3 Of 33)

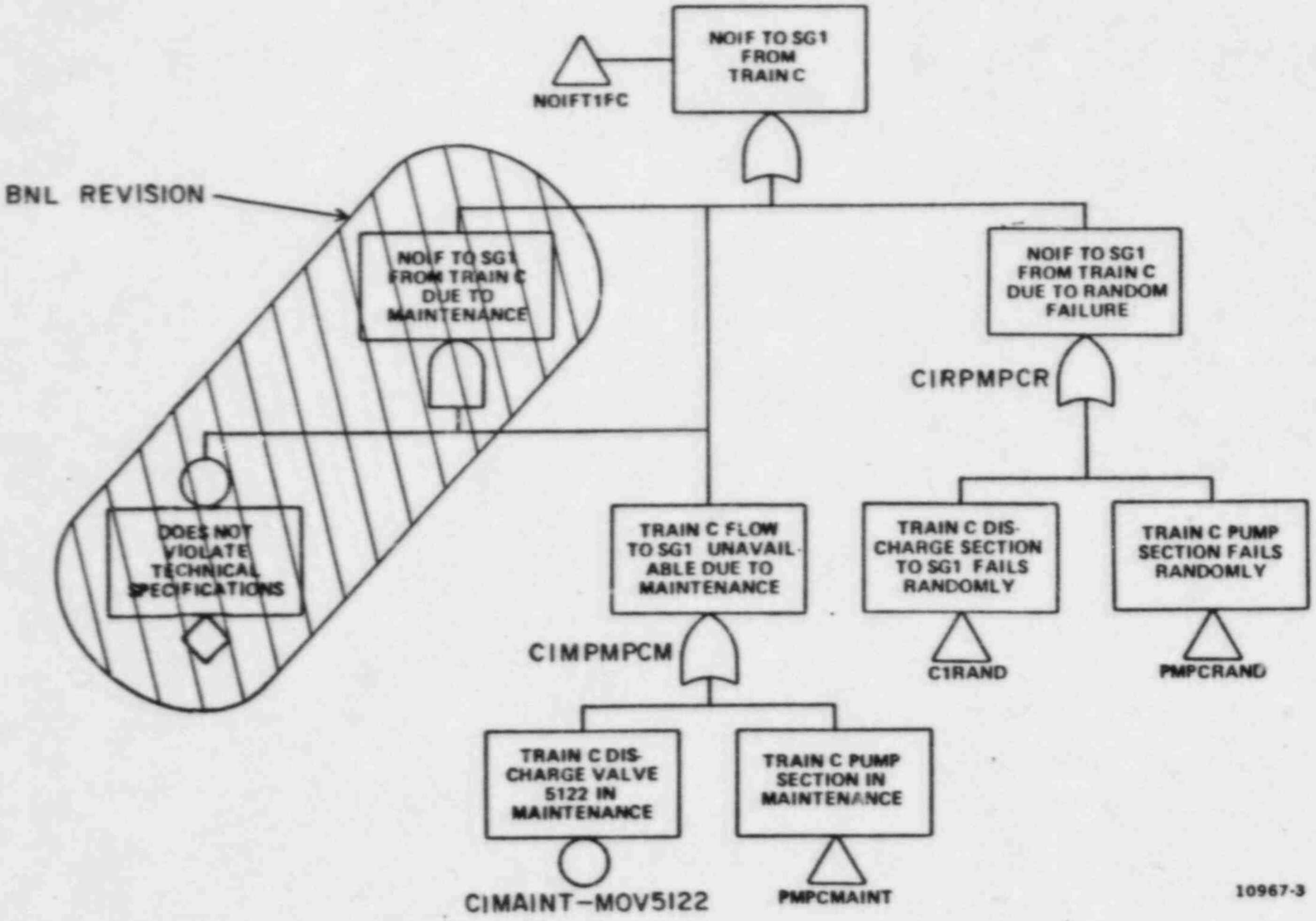
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 2 OF 30)

433-9



BNL Figure 7 (Sheet 4 of 33)

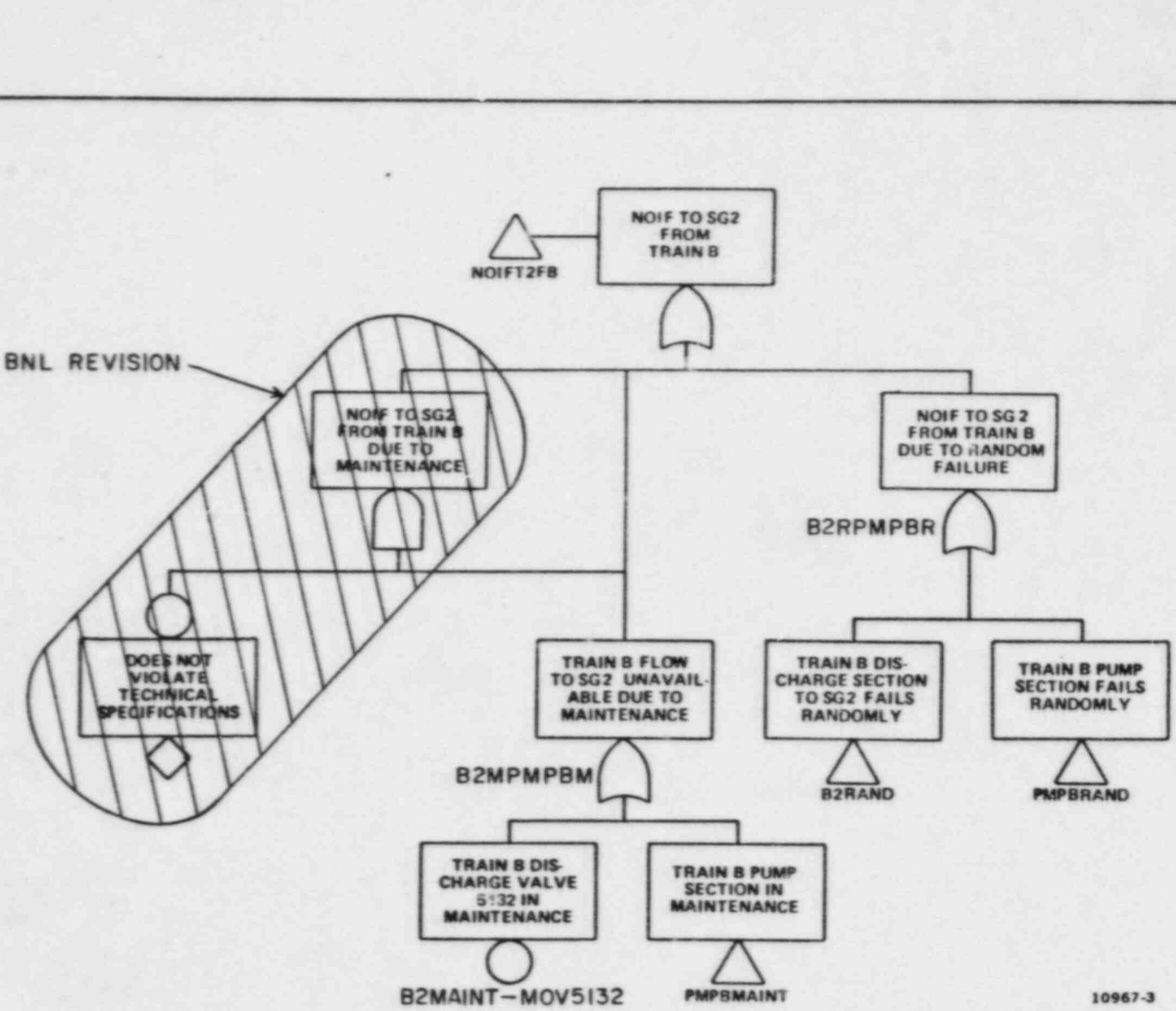
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 3 OF 30)

433-9



BNL Figure 7 (Sheet 5 of 33)

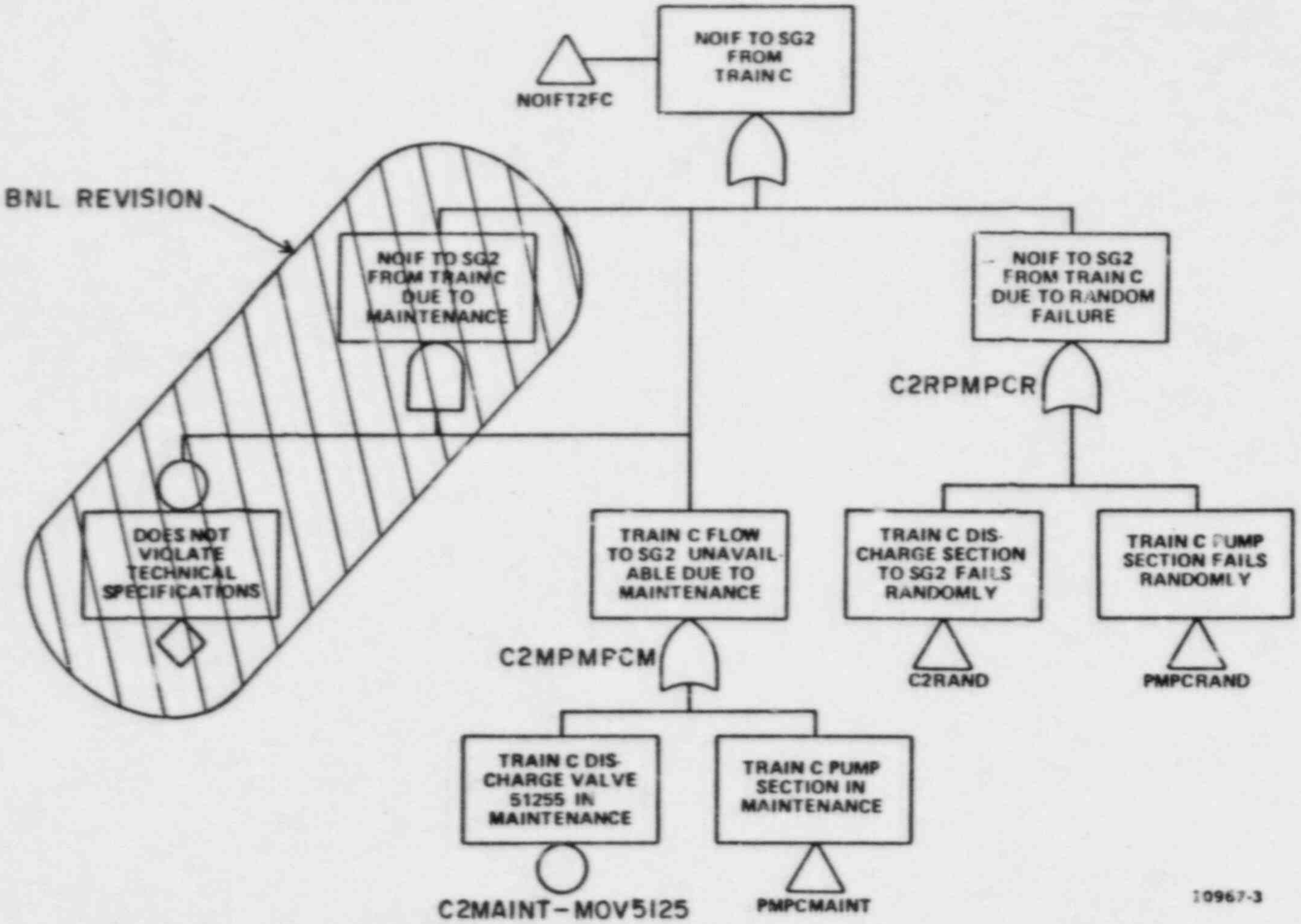
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 4 OF 30)

433-9



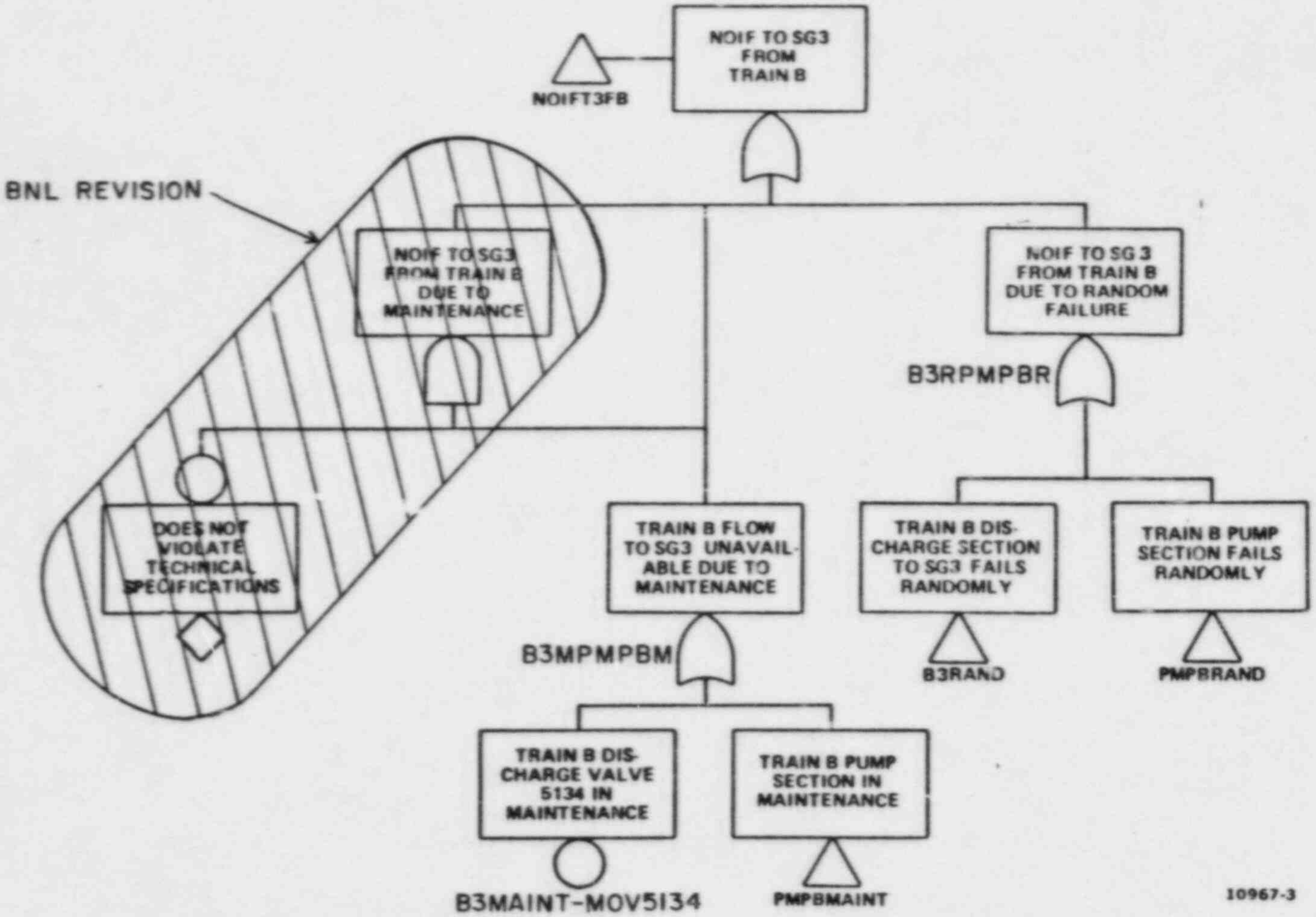
BNL Figure 7 (Sheet 6 of 33)

Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

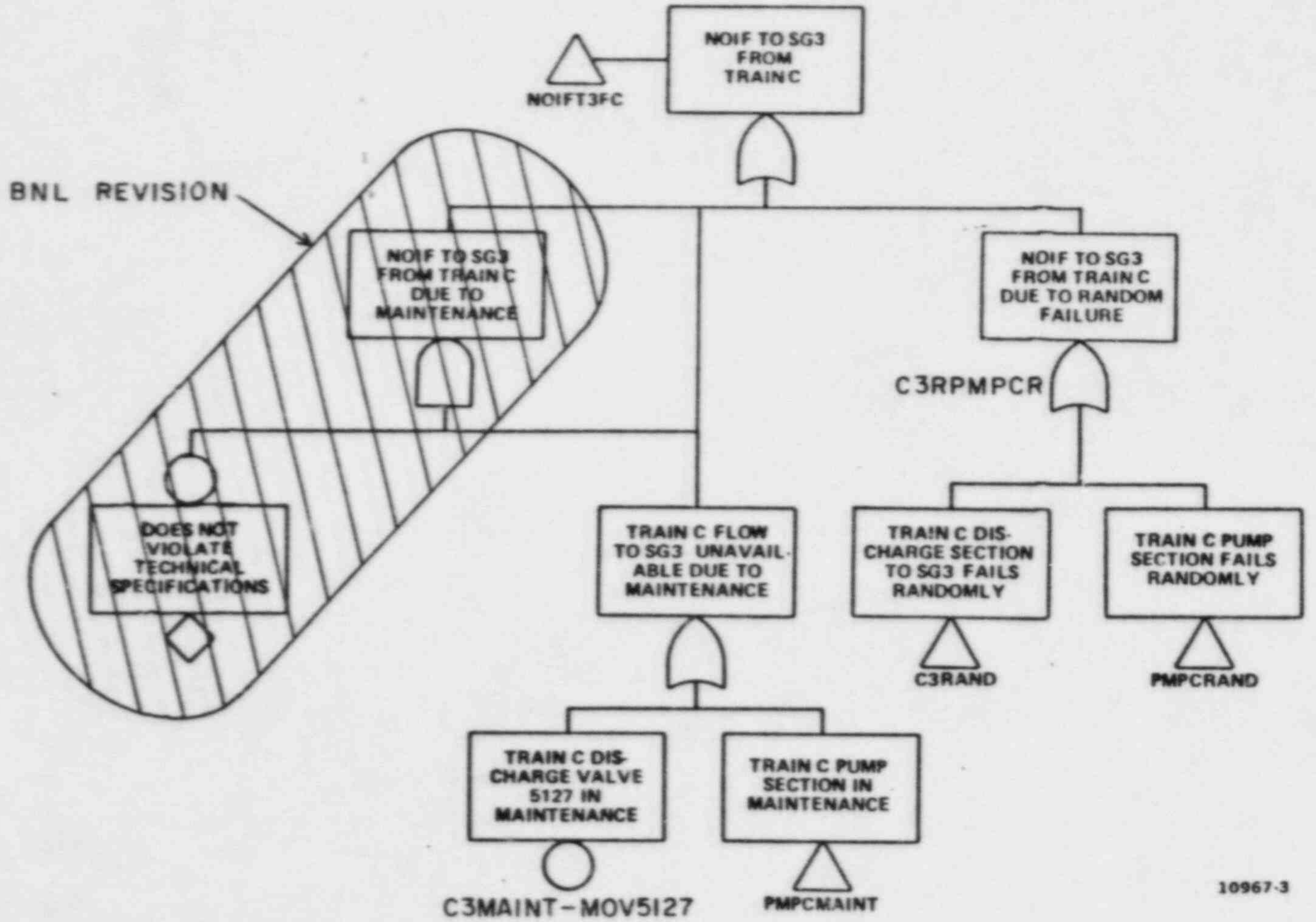
FIGURE 10A-7 (SHEET 5 OF 30)



BNL Figure 7 (Sheet 7 of 33)

Georgia Power VOGTLE ELECTRIC GENERATING PLANT UNIT 1 AND UNIT 2	UNIT 1 AFWS FAULT TREE MODEL FSAR
	FIGURE 10A-7 (SHEET 6 OF 30)

433-9



BNL Figure 7 (Sheet 8 of 33)

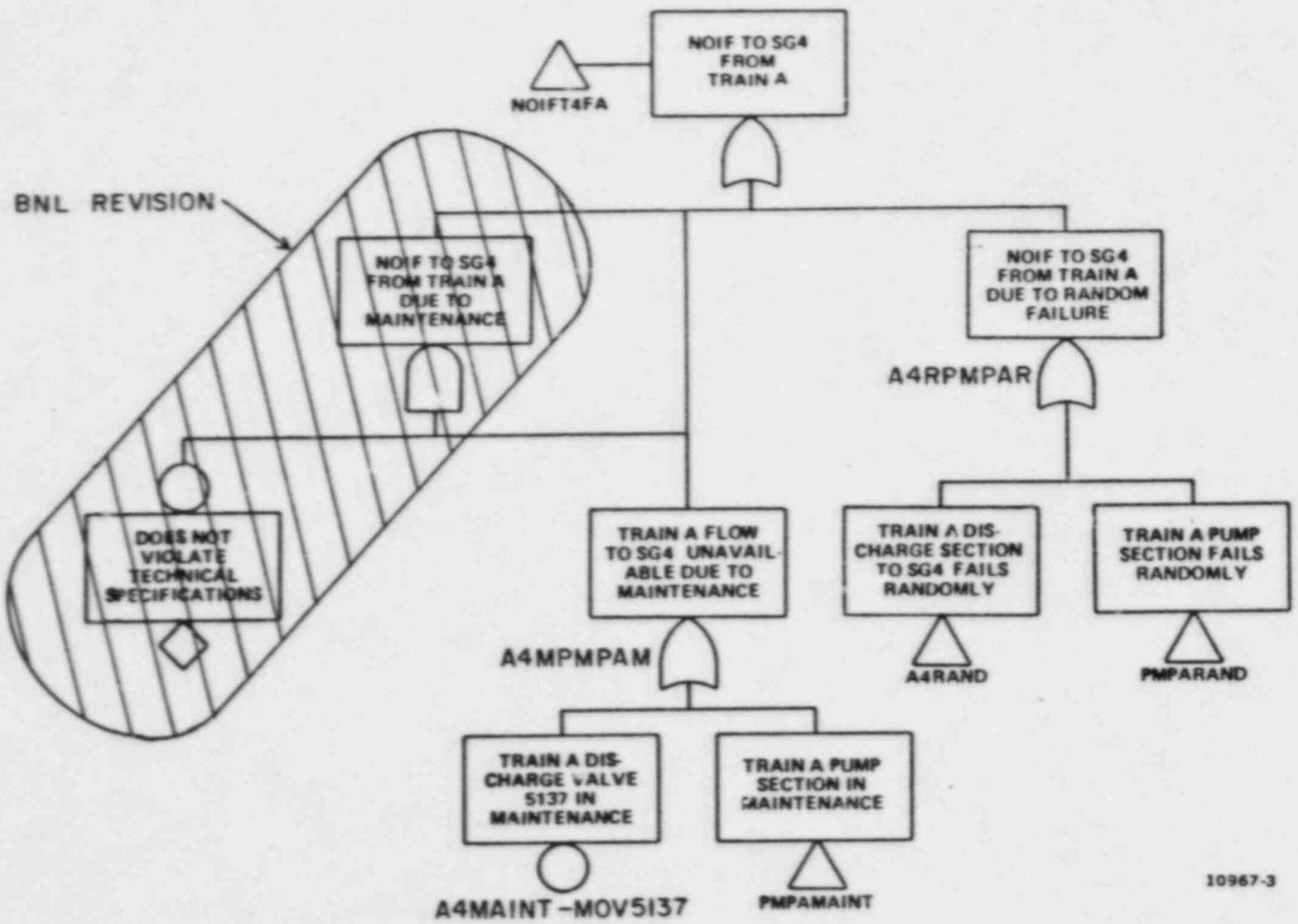
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 7 OF 30)

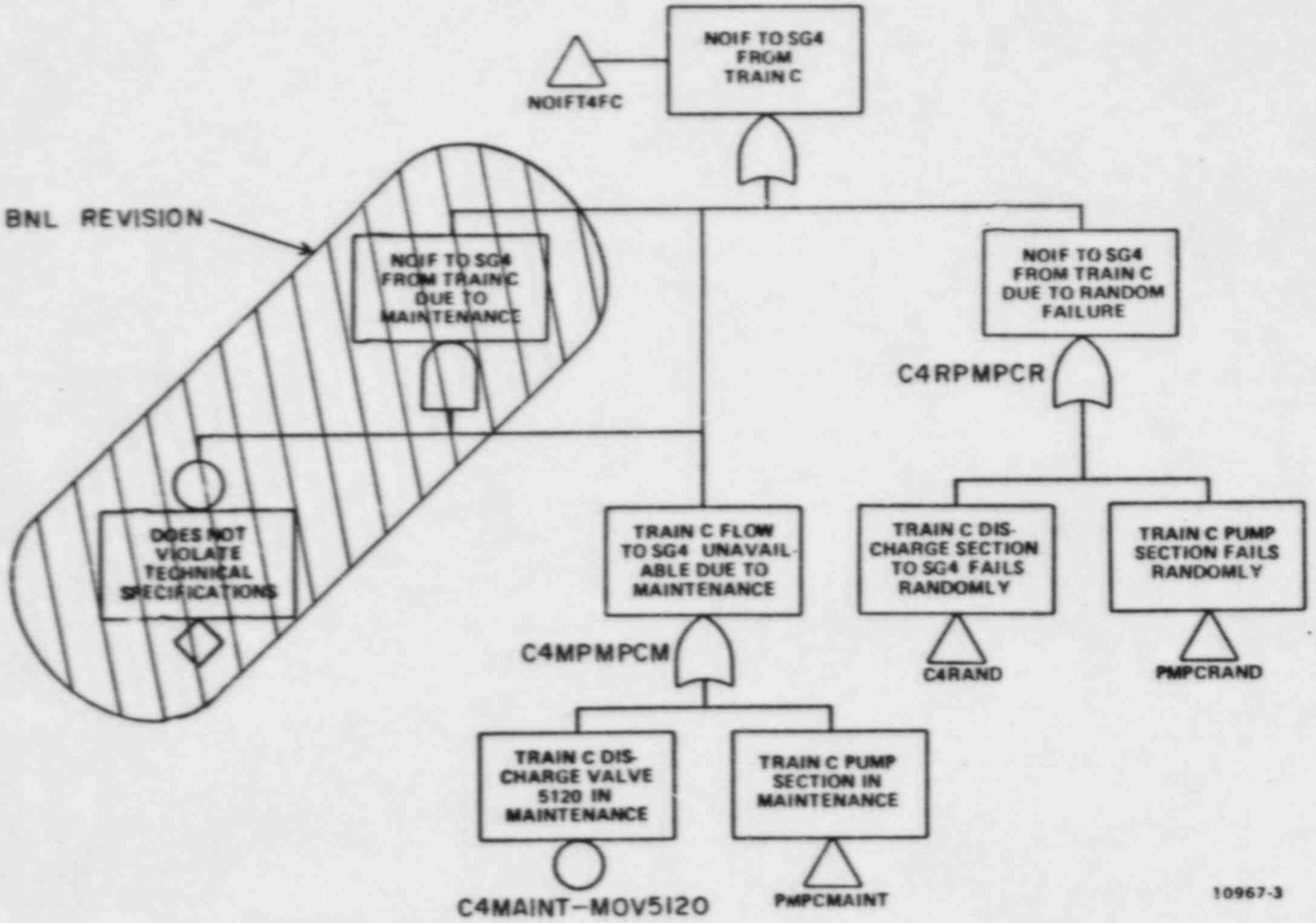
433-9



BNL Figure 7 (Sheet 9 of 33)

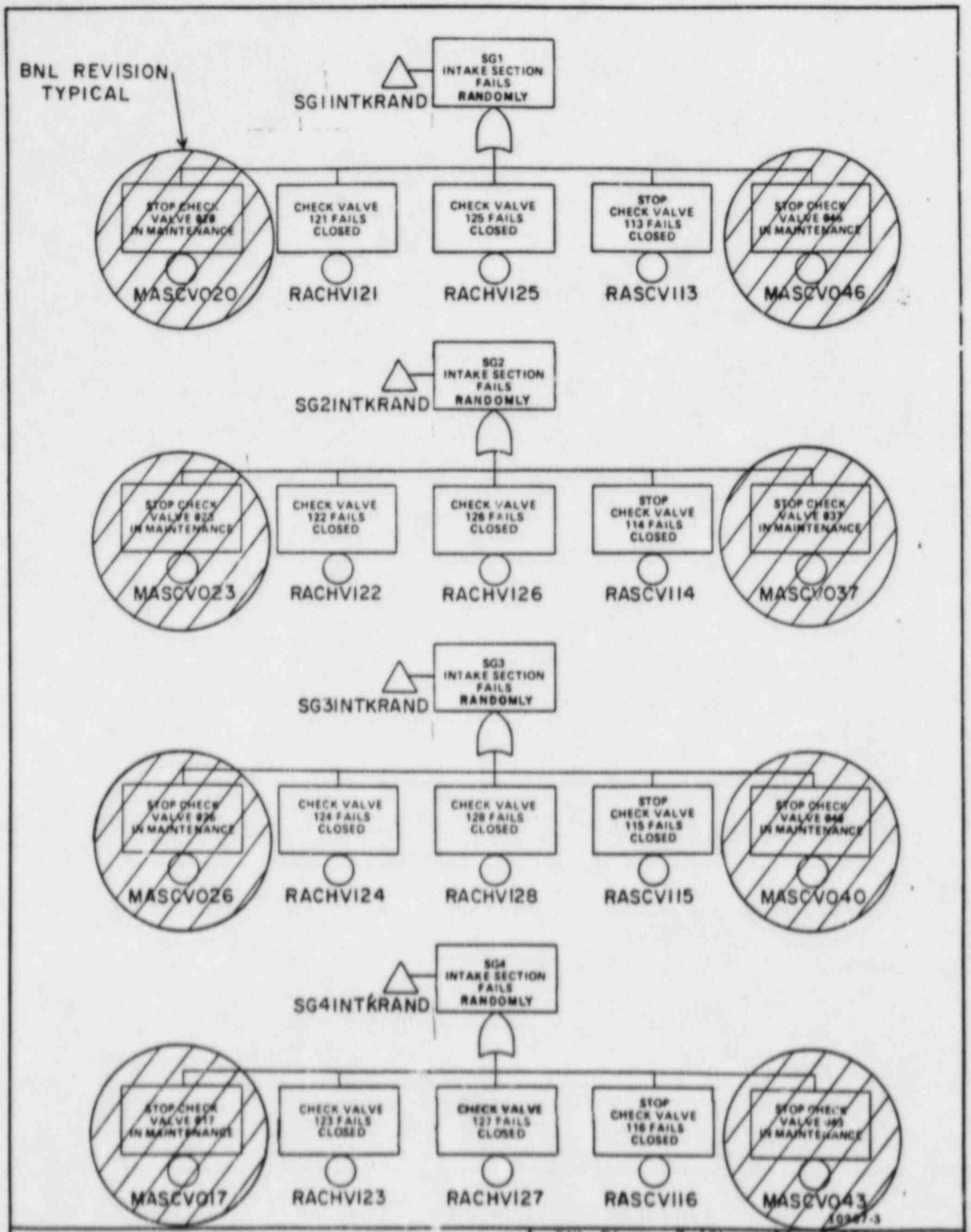
Georgia Power	VOGTLE ELECTRIC GENERATING PLANT UNIT 1 AND UNIT 2	UNIT 1 AFWS FAULT TREE MODEL FSAR
		FIGURE 10A-7 (SHEET 8 OF 30)

433-9



BNL Figure 7 (Sheet 10 of 33)

Georgia Power	VOGTLE ELECTRIC GENERATING PLANT UNIT 1 AND UNIT 2	UNIT 1 AFWS FAULT TREE MODEL FSAR FIGURE 10A-7 (SHEET 9 OF 30)



Georgia Power

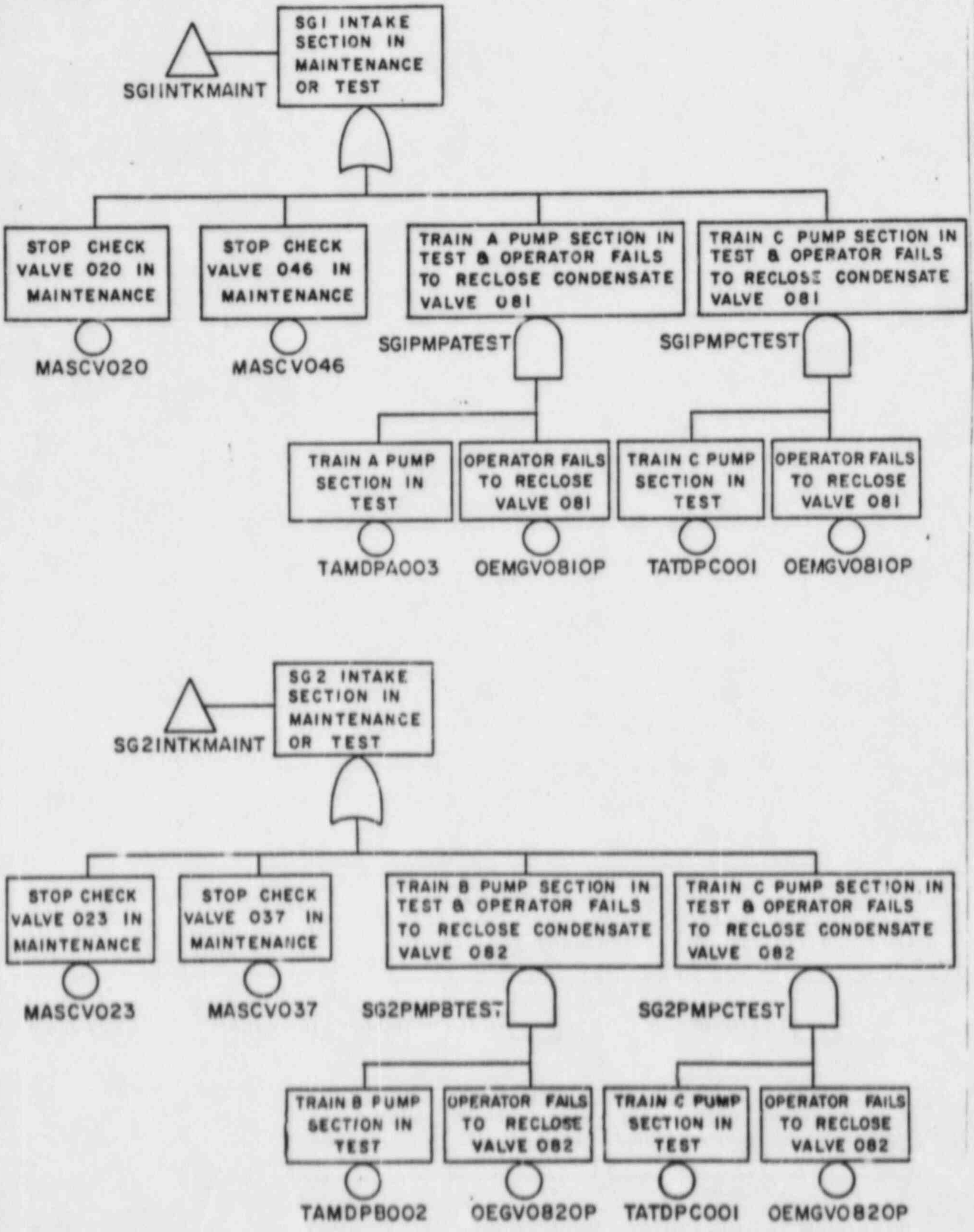
VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 11 of 33)

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 10 OF 30)

433-9



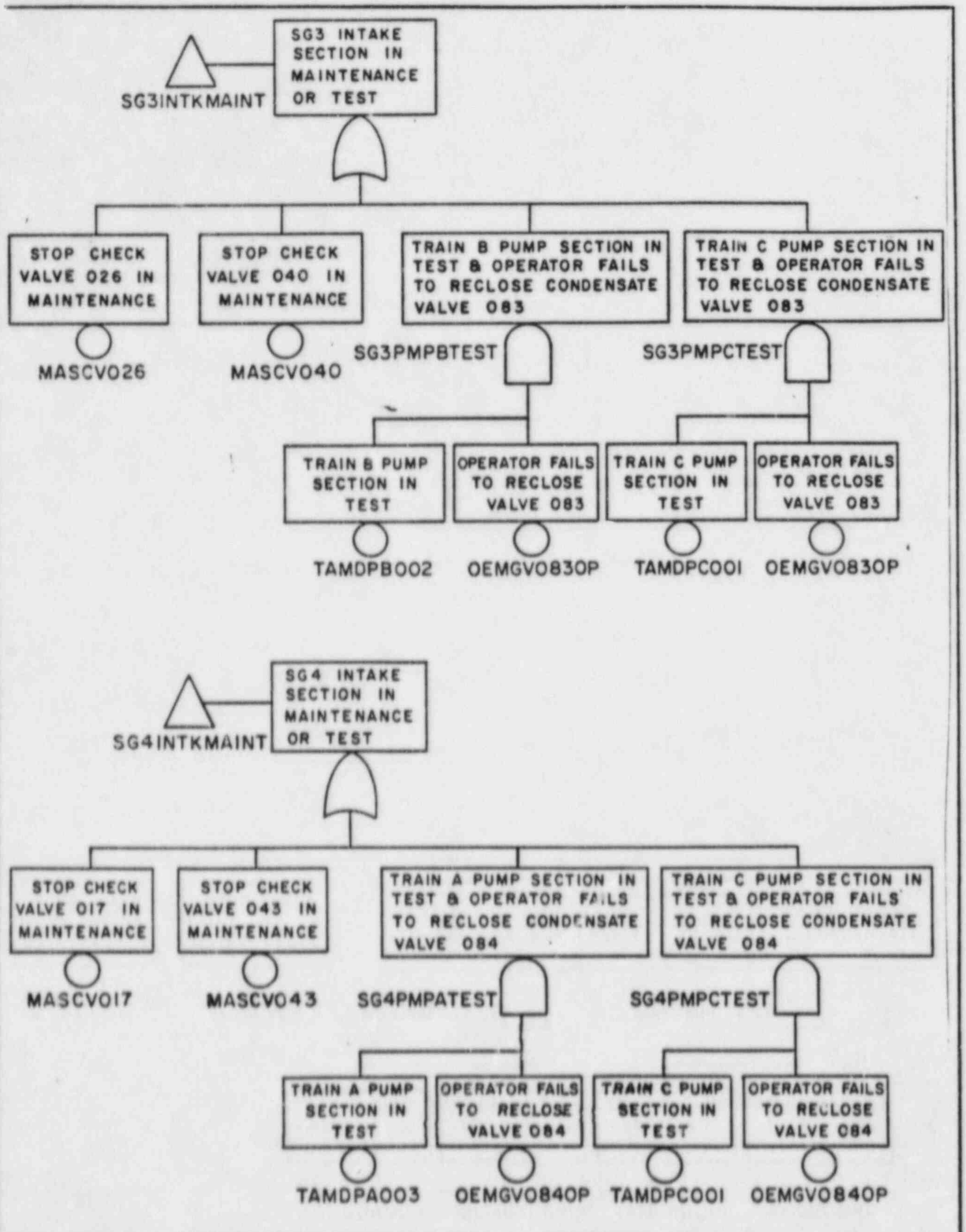
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 12 of 33)
UNIT 1 AFWS FAULT TREE MODEL
BNL ADDITION

FSAR FIG. 10A-7 SHEET 10A OF 30

433-9



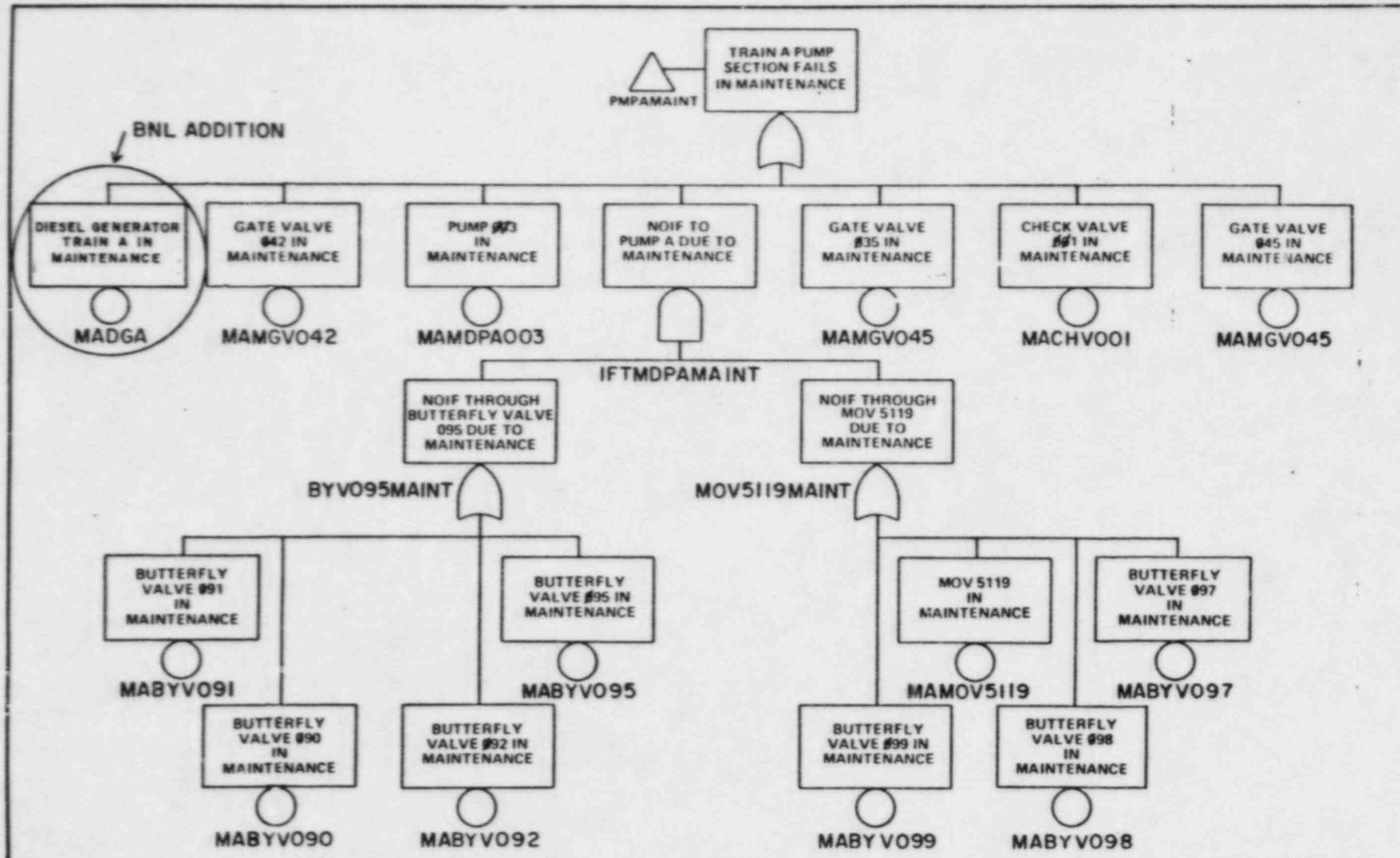
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 13 of 33)
UNIT 1 AFWS FAULT TREE MODEL
BNL ADDITION

FSAR FIG. 10A-7 SHEET 10B OF 30

433-9



NOIF - NO OR INSUFFICIENT FLOW

BNL Figure 7 (Sheet 14 of 33)

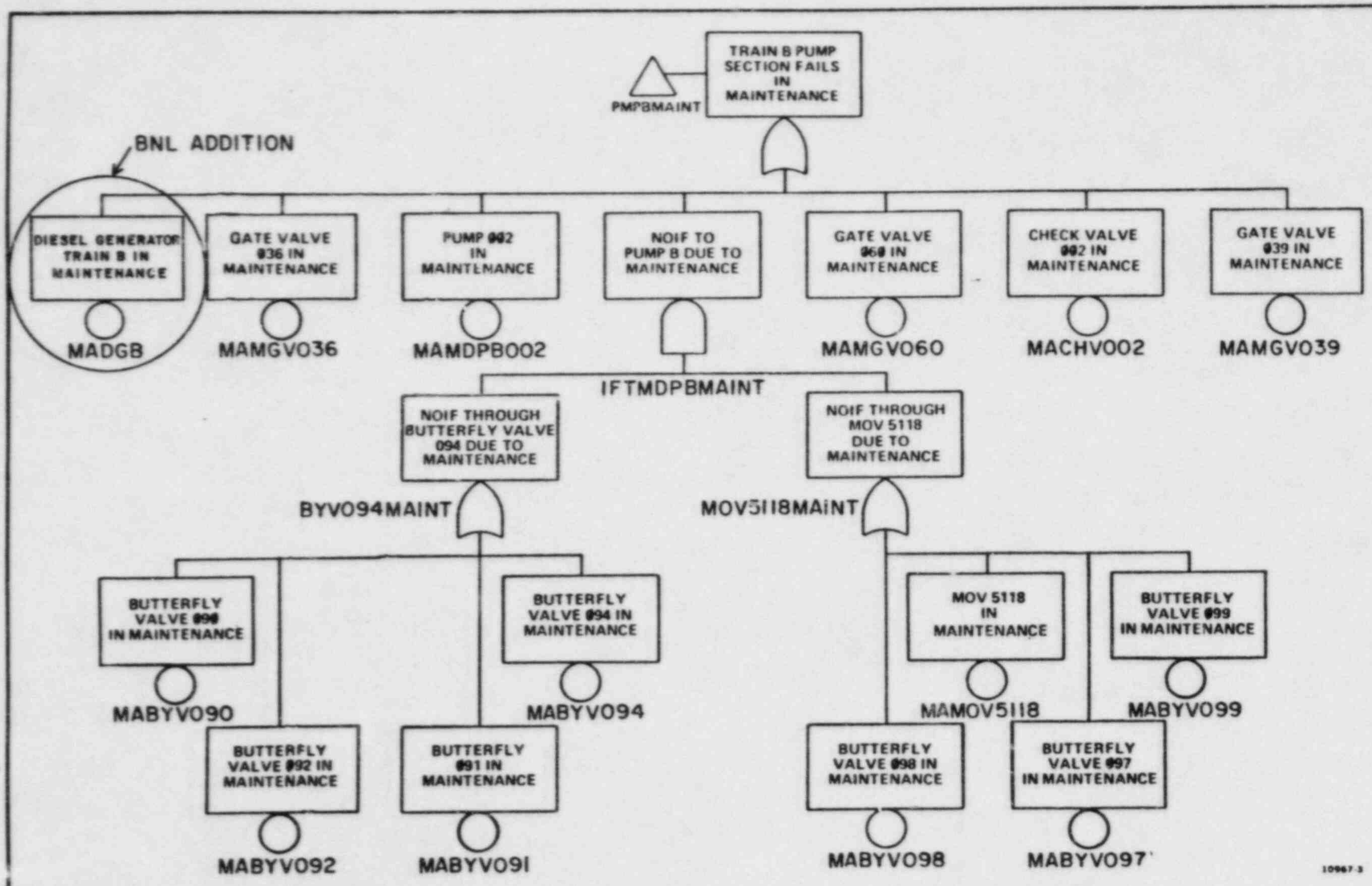
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 11 OF 30)

433-9



NOIF = NO OR INSUFFICIENT FLOW

BNL Figure 7 (Sheet 15 of 33)

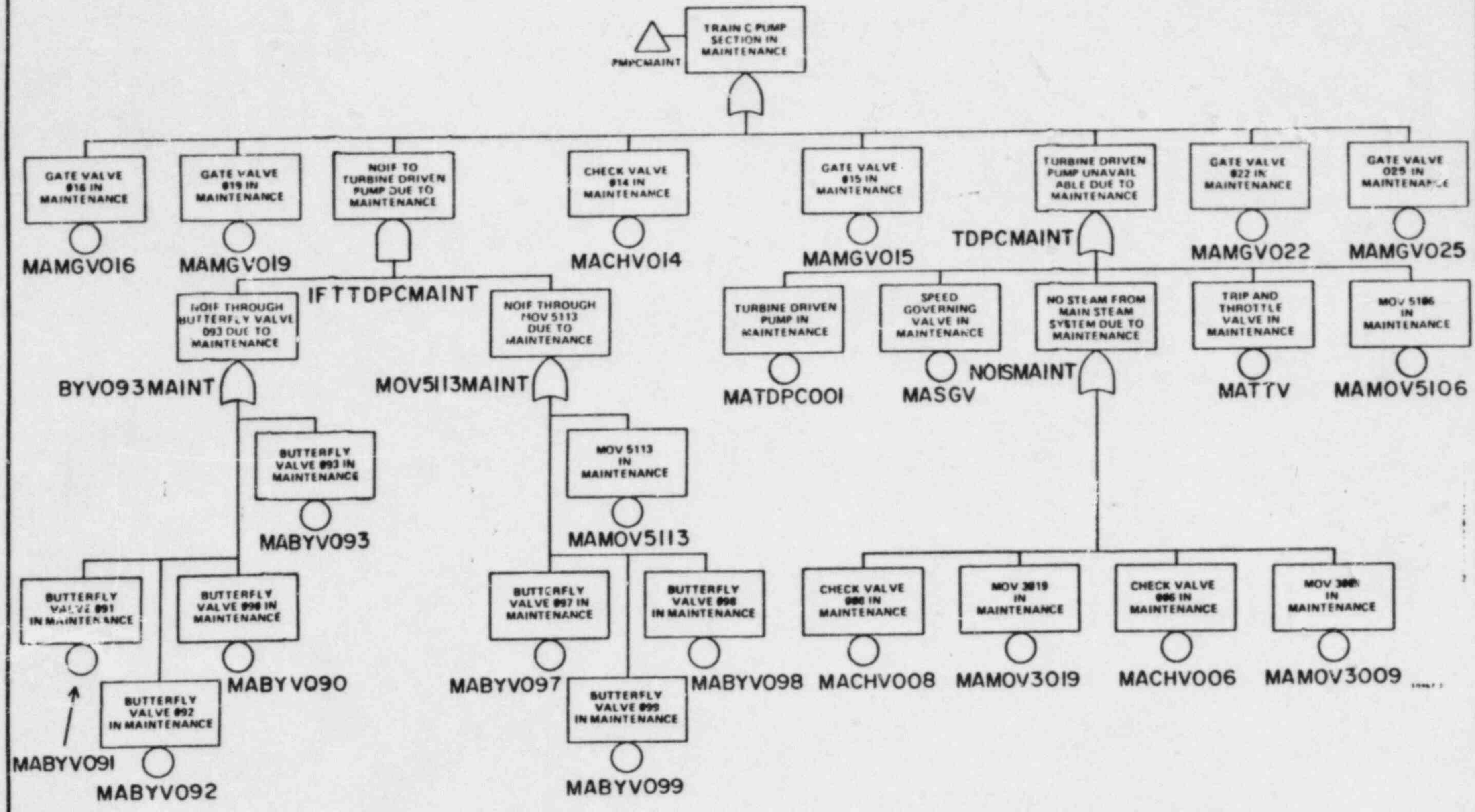
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 12 OF 30)

433-9



BNL Figure 7 (Sheet 16 of 33)

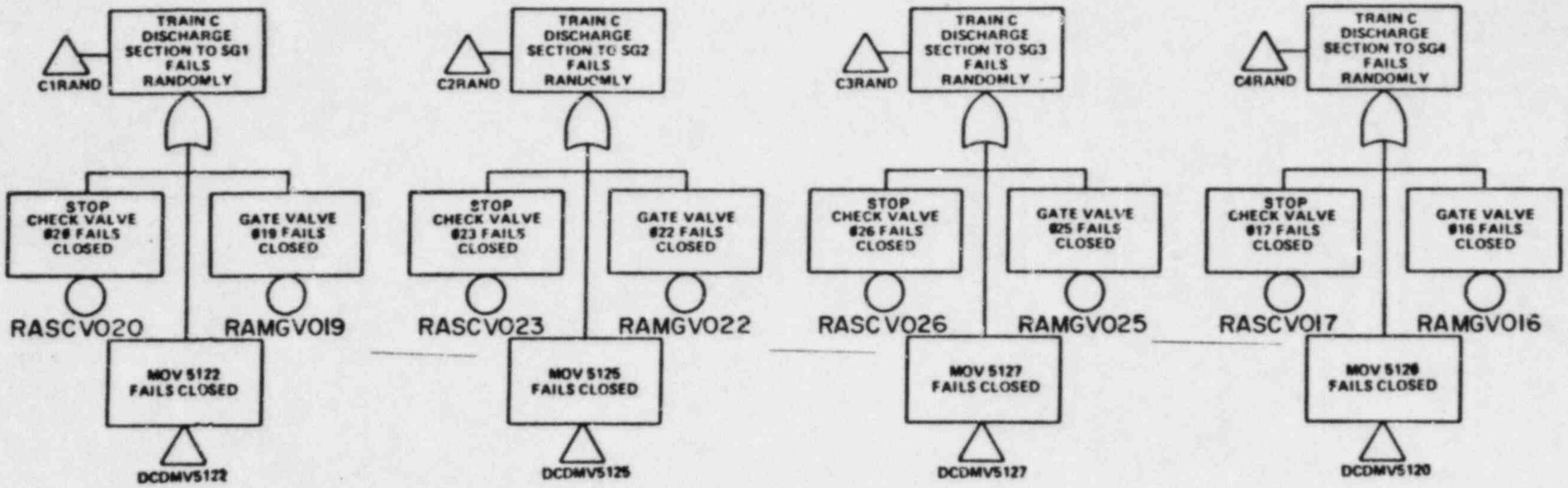
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 13 OF 30)

413-9



10967-3

BNL Figure 7 (Sheet 17 of 33)

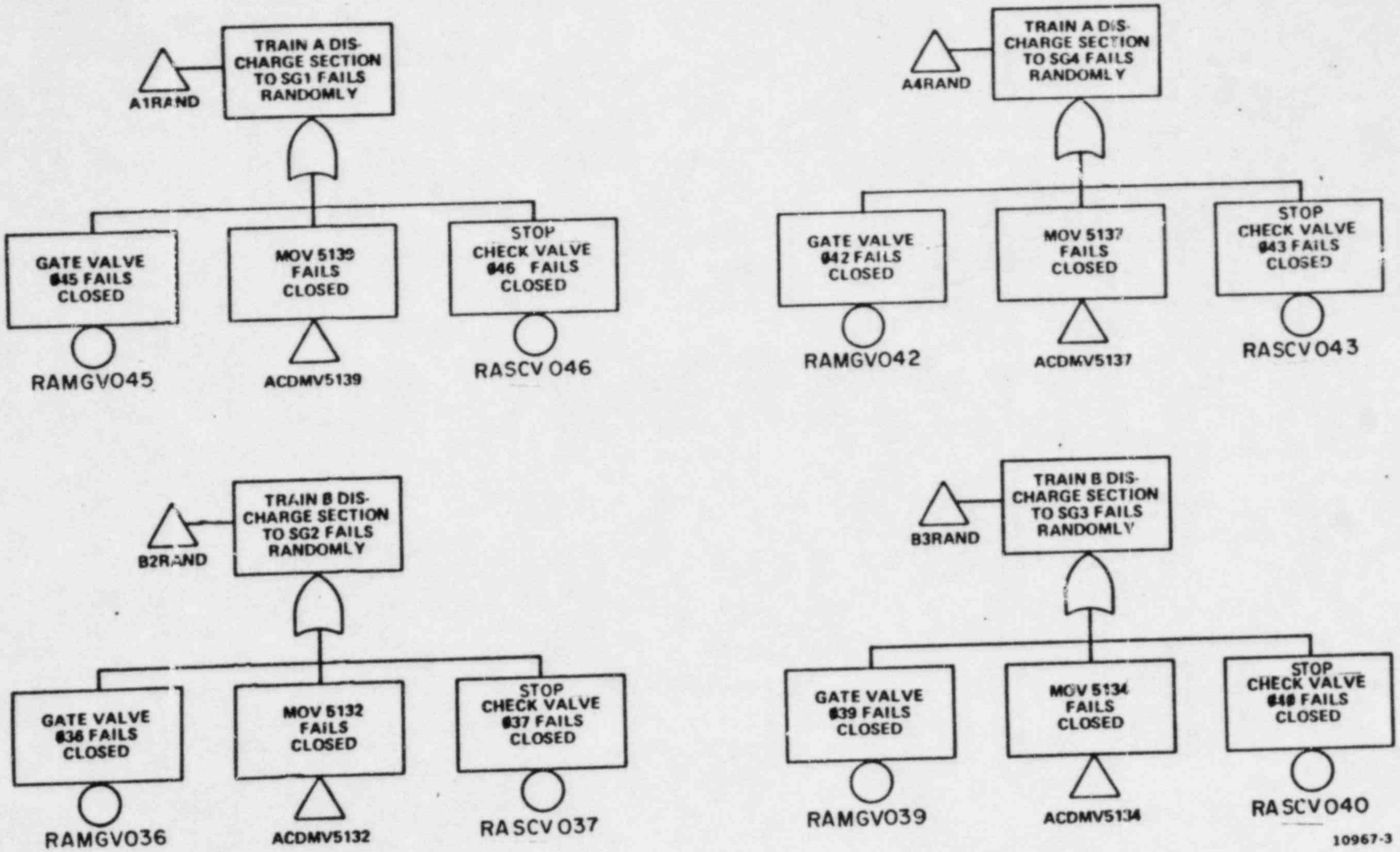
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL, FSAR

FIGURE 10A-7 (SHEET 14 OF 30)

433-9



BNL Figure 7 (Sheet 18 of 33)

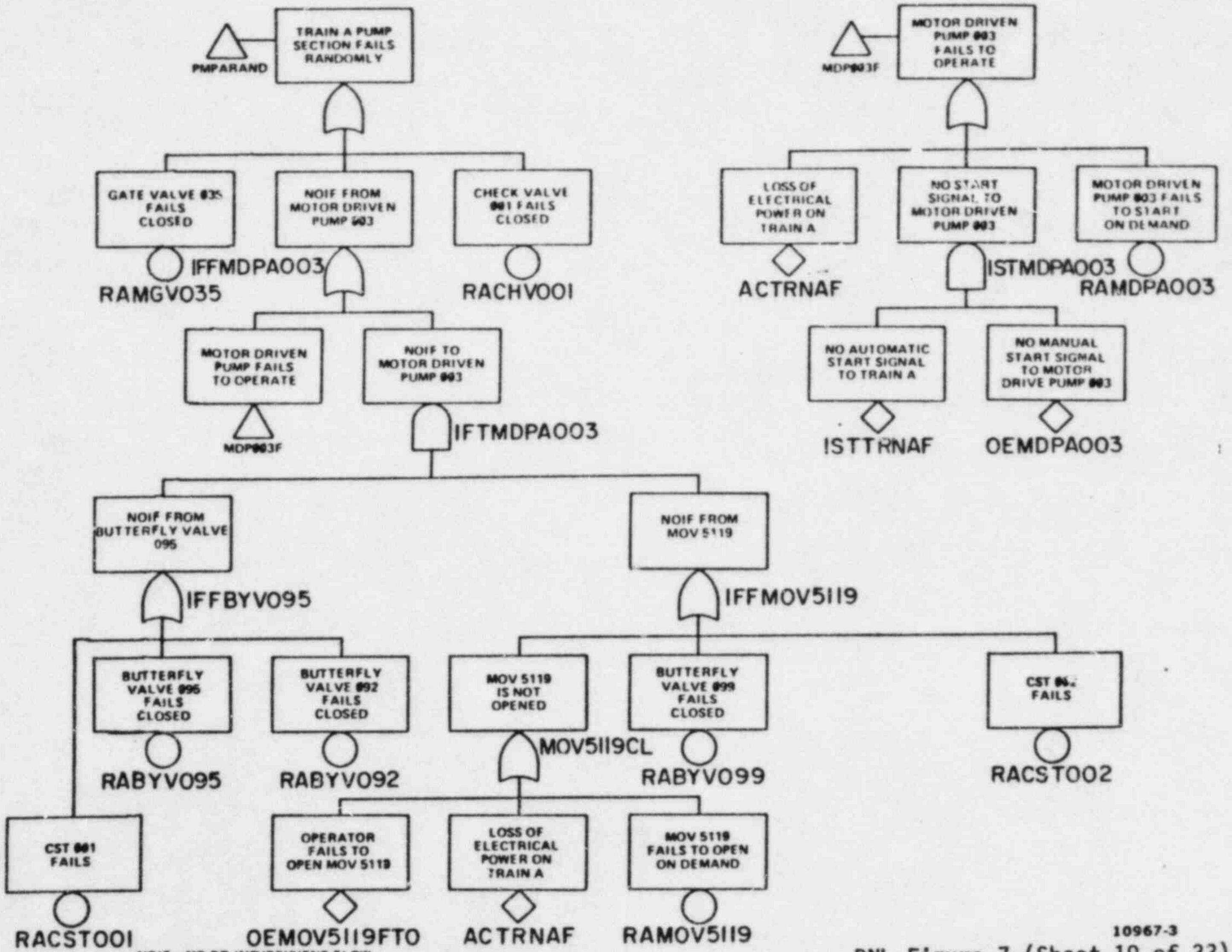
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 15 OF 30)/

433-9



NOIF - NO OR INSUFFICIENT FLOW

10967-3

BNL Figure 7 (Sheet 19 of 33)

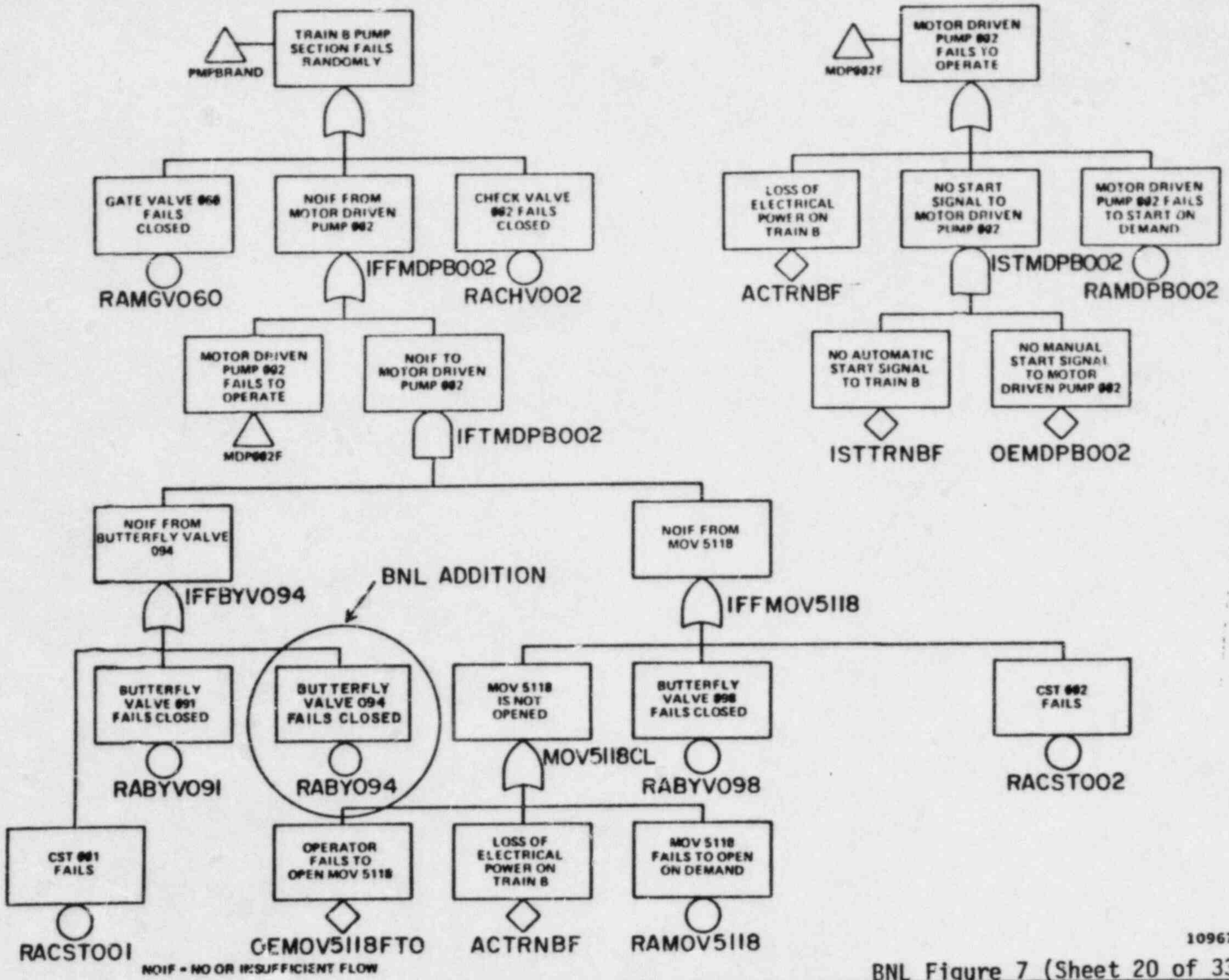
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 16 OF 30)

433-9



10967-3

BNL Figure 7 (Sheet 20 of 33)

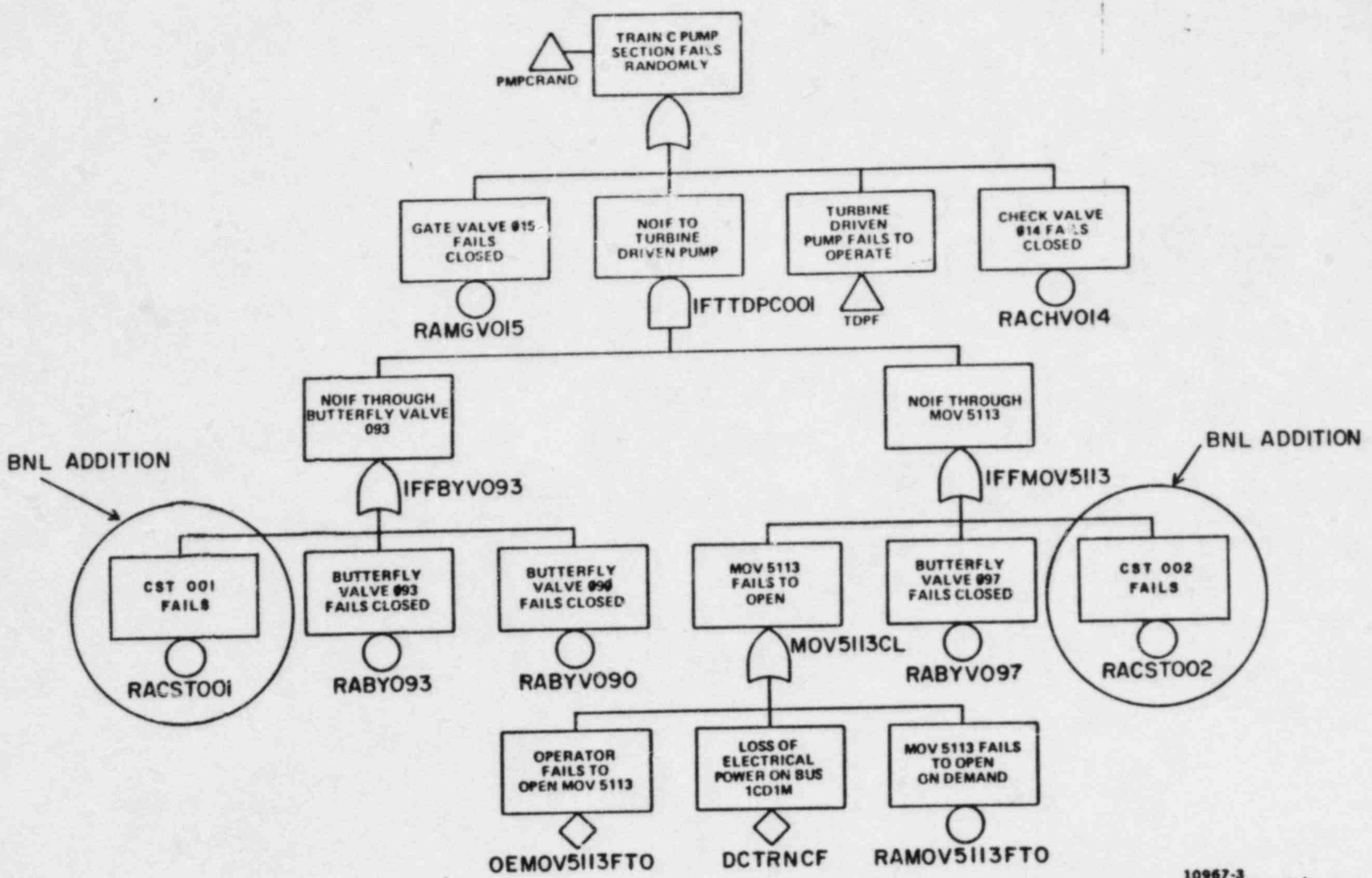
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 17 OF 30)

433-9



10967-3

BNL Figure 7 (Sheet 21 of 33)

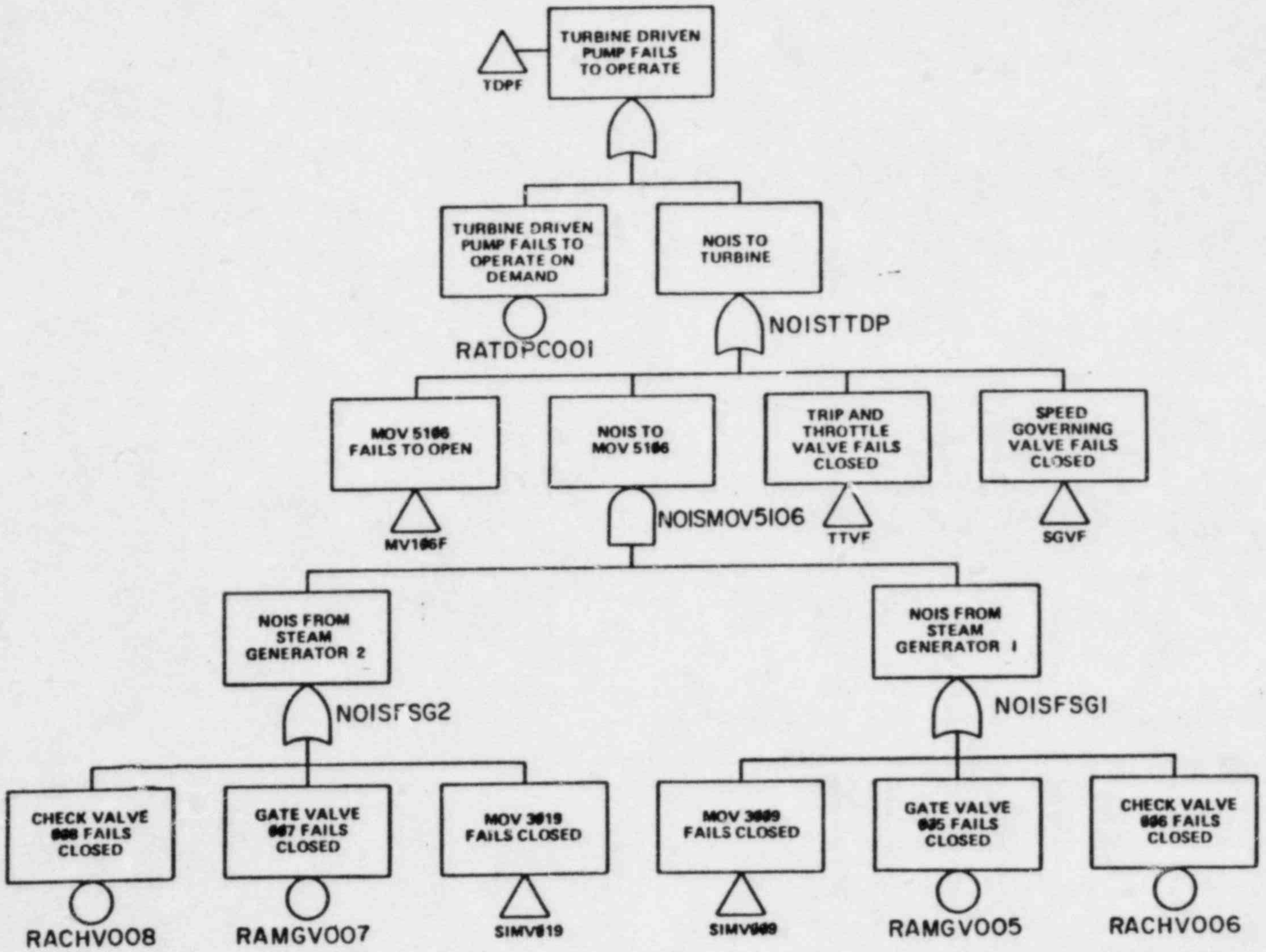
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 18 OF 30)

433-9



NOIS - NO OR INSUFFICIENT STEAM

10967-3

BNL Figure 7 (Sheet 22 of 33)

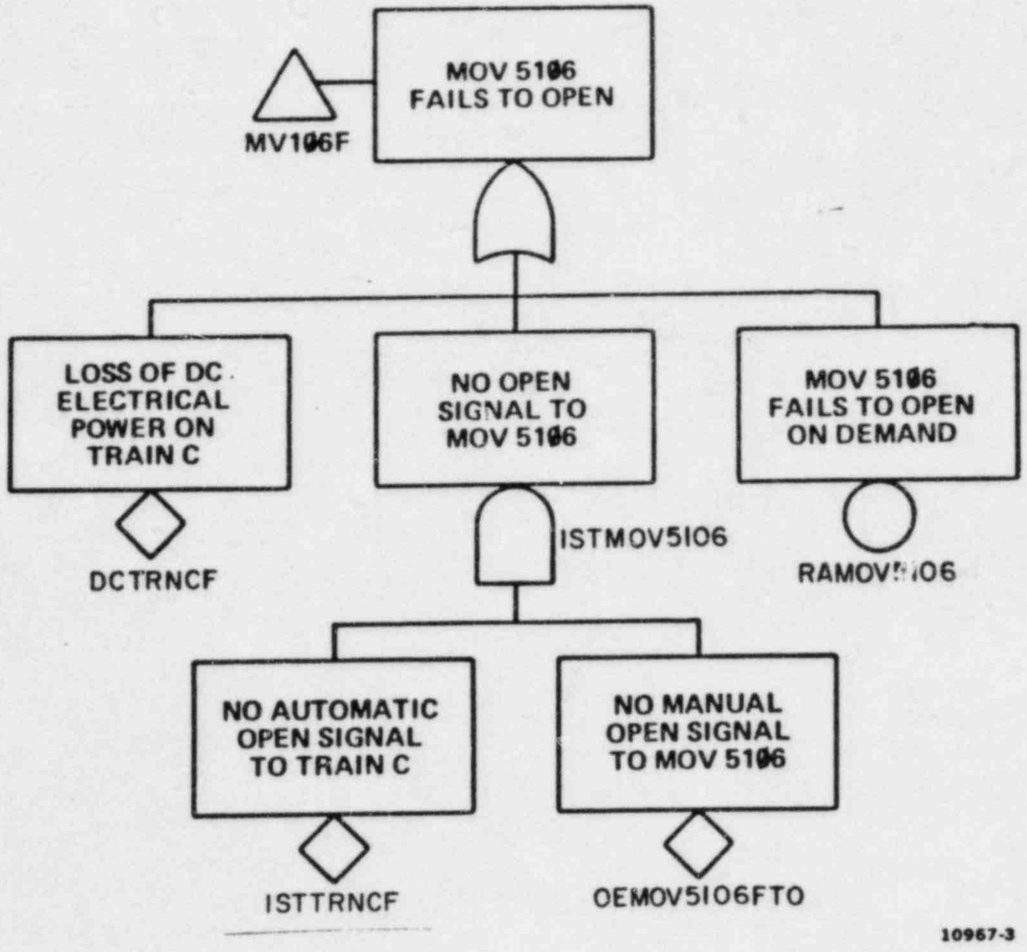
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 19 OF 30)

433-9



BNL Figure 7 (Sheet 23 of 33)

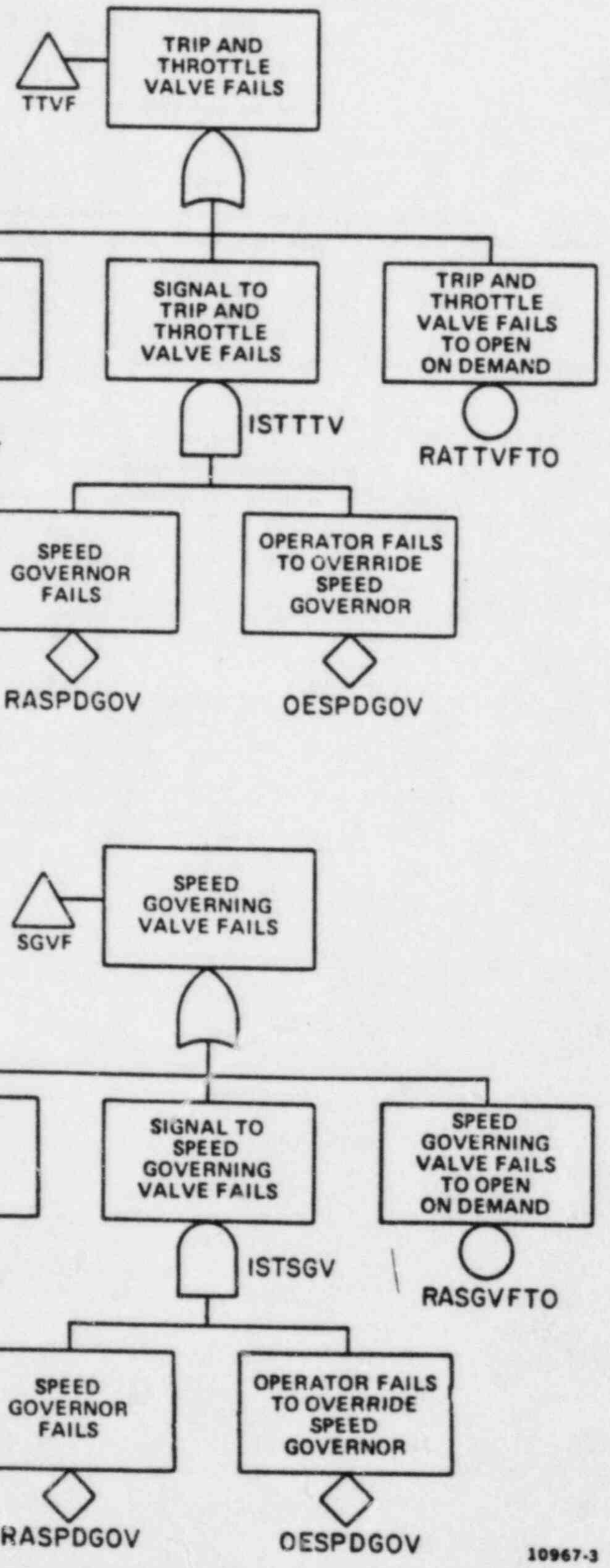
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 20 OF 30)

433-9



10967-3

Georgia Power

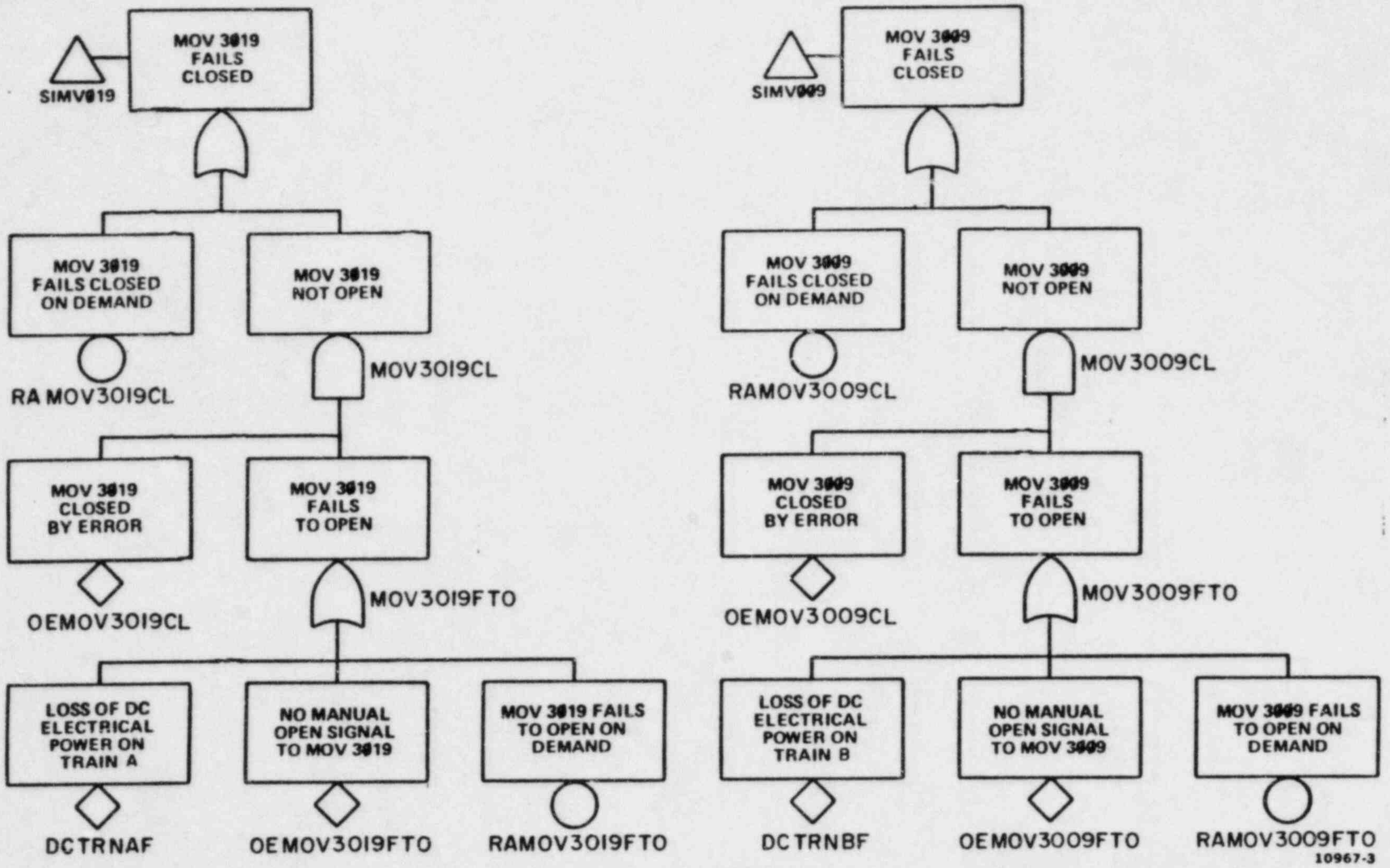
VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 24 of 33)

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 21 OF 30)

433-9



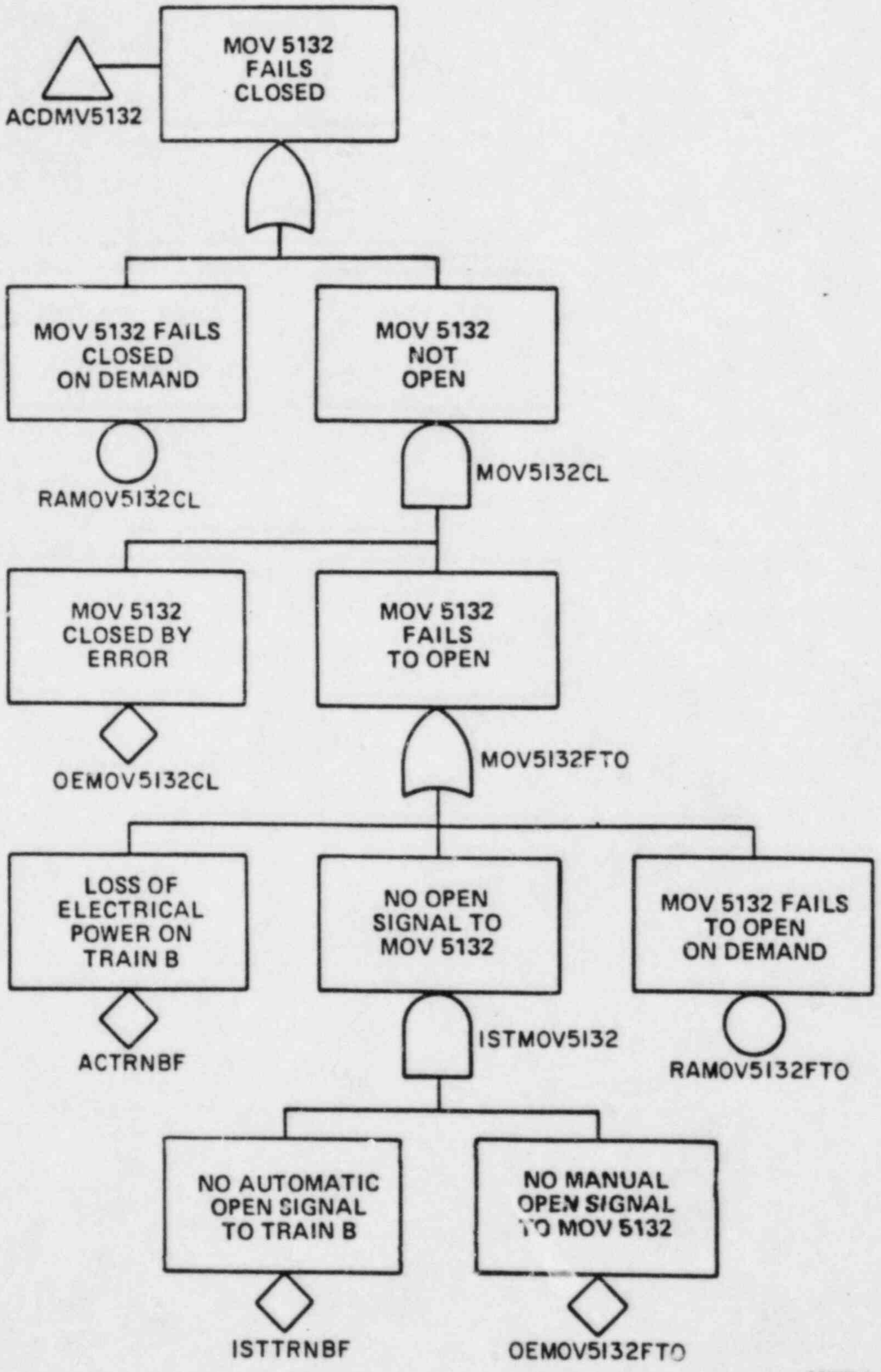
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 25 of 33)
UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 22 OF 30)

433-9



10967-3

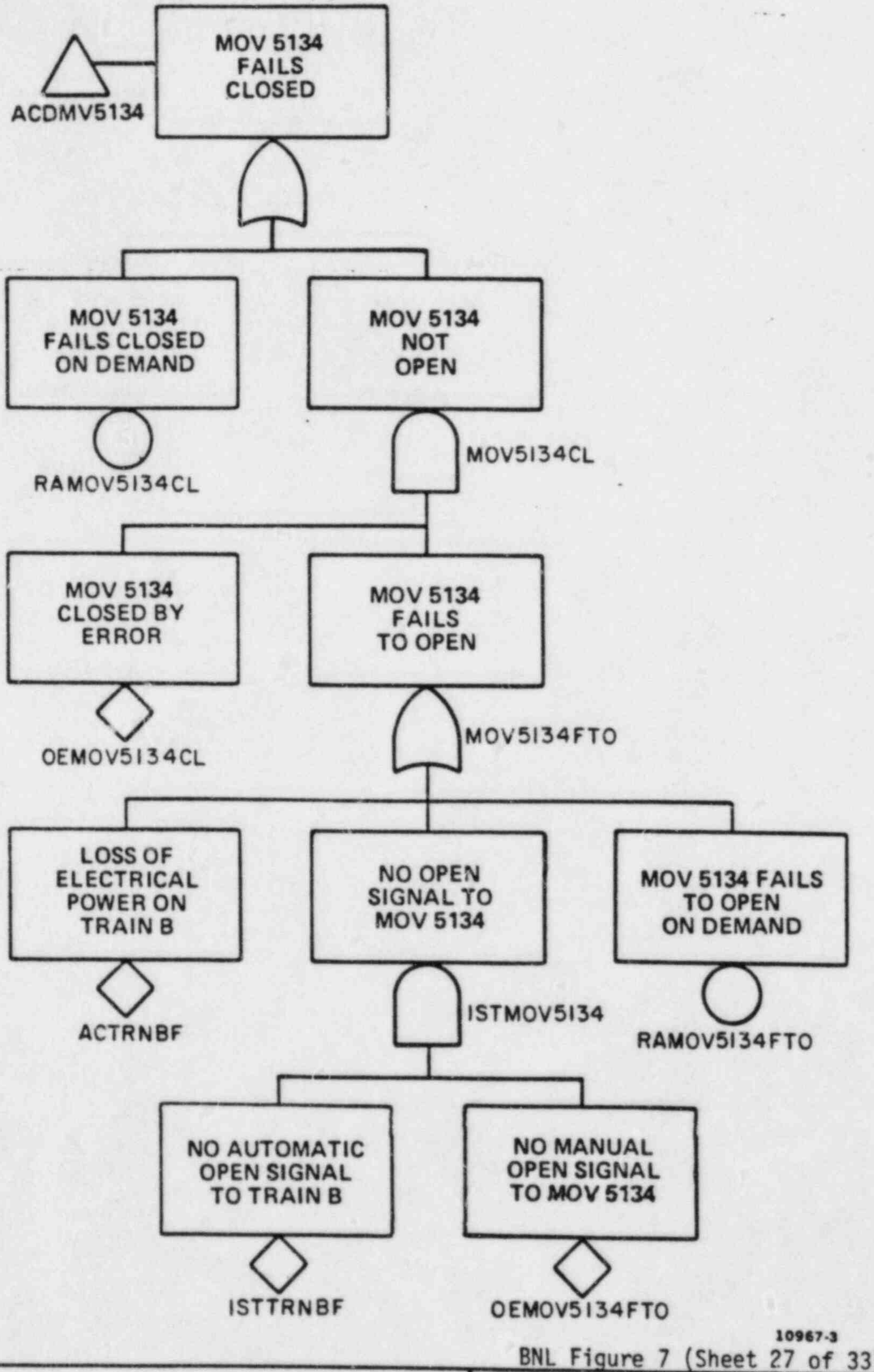
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 26 of 33)
UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 23 OF 30)

433-9



10967-3

BNL Figure 7 (Sheet 27 of 33)

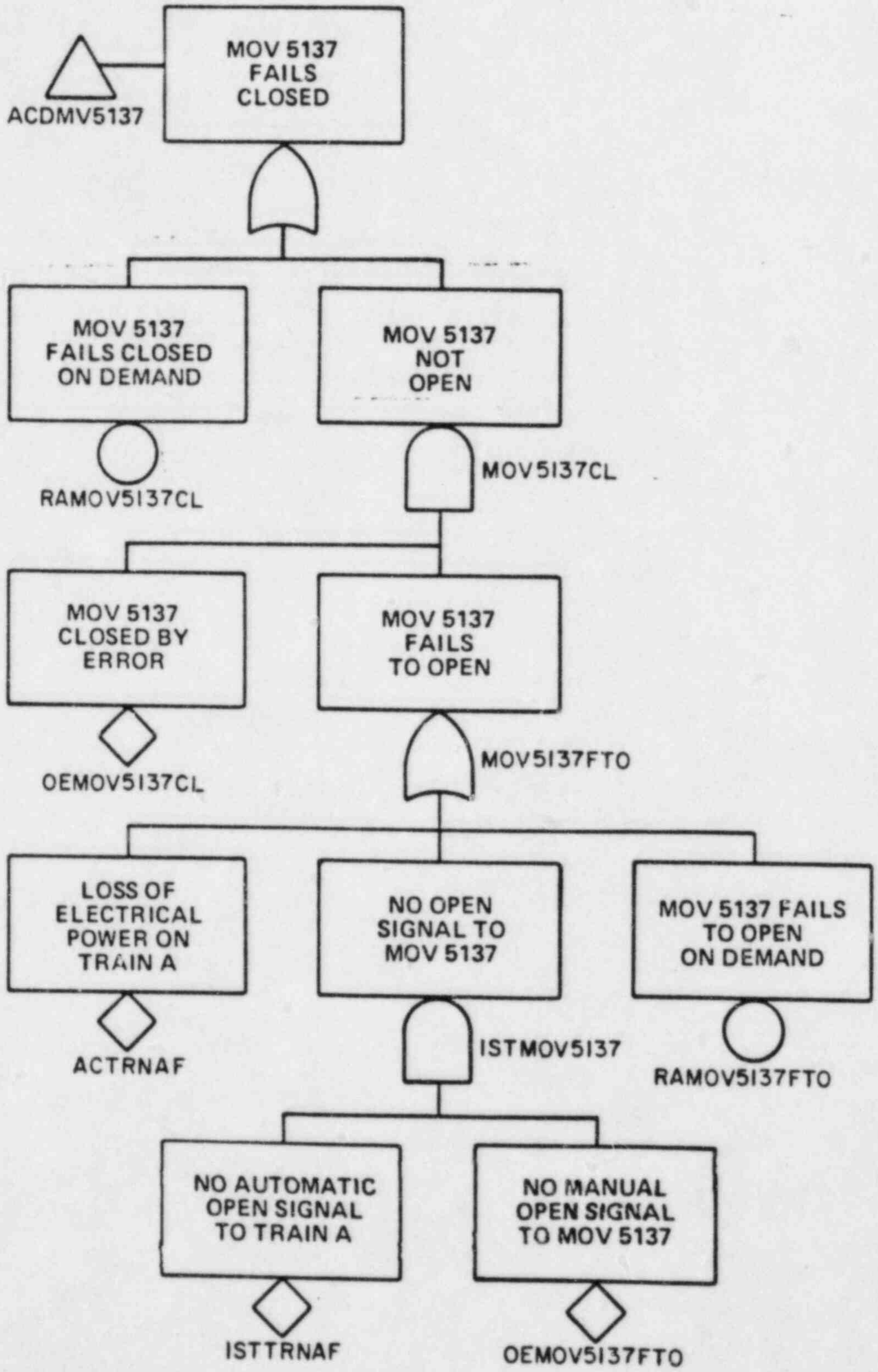
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 24 OF 30)

433-9



10967-3

Georgia Power

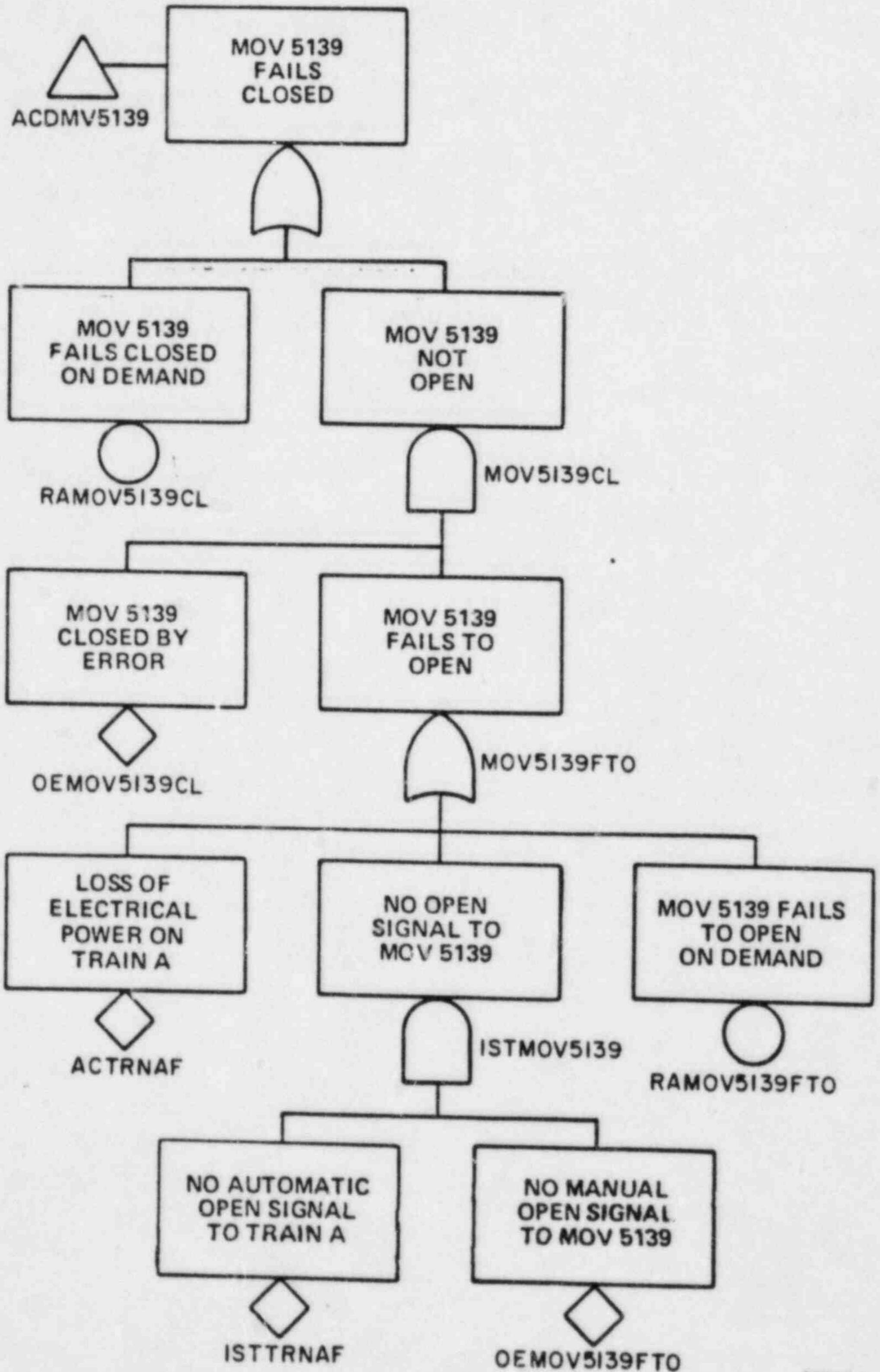
VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 28 of 33)

UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 25 OF 30)

433-9



10967-3

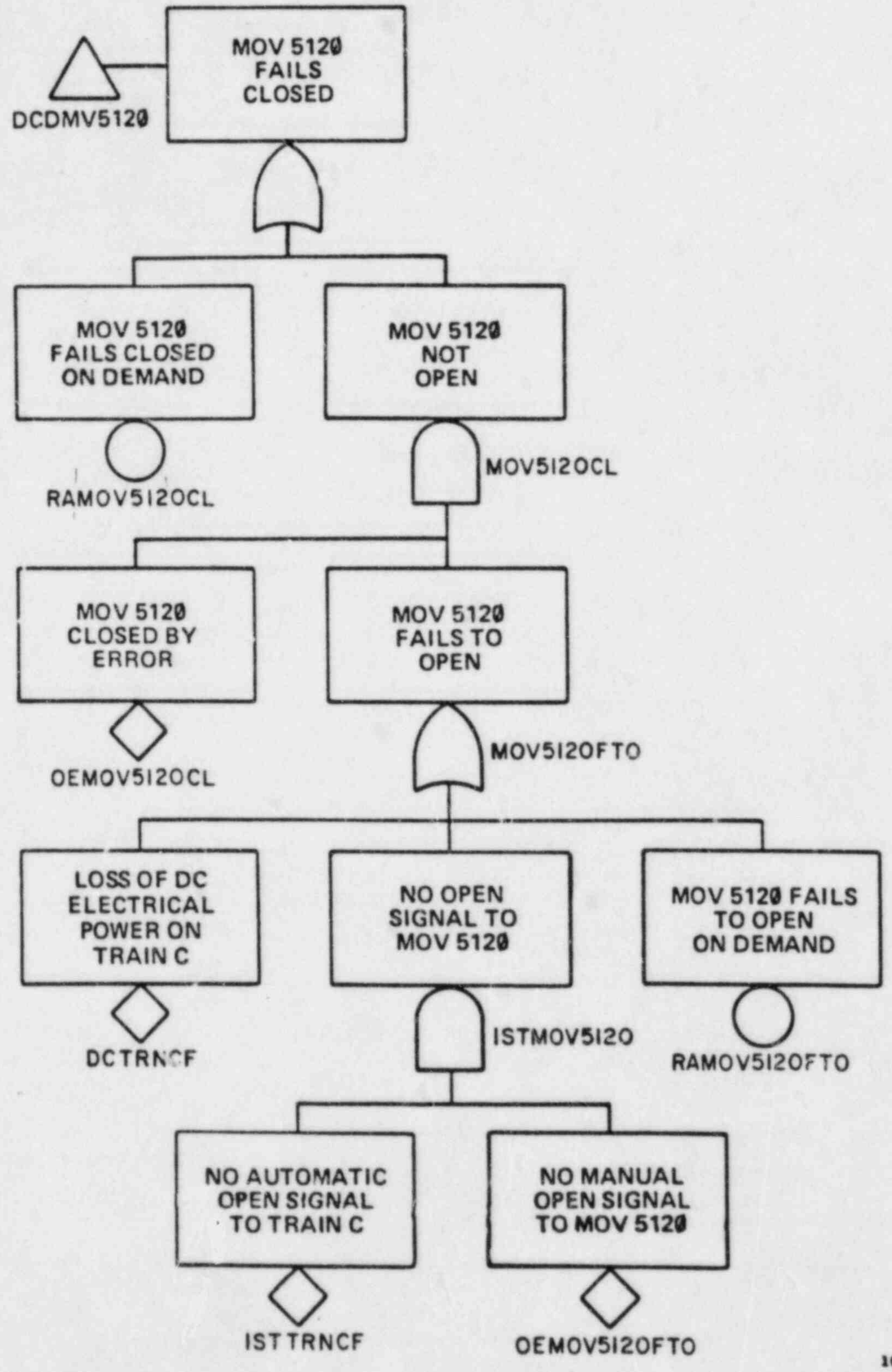
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 29 of 33)
UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 26 OF 30)

433-9



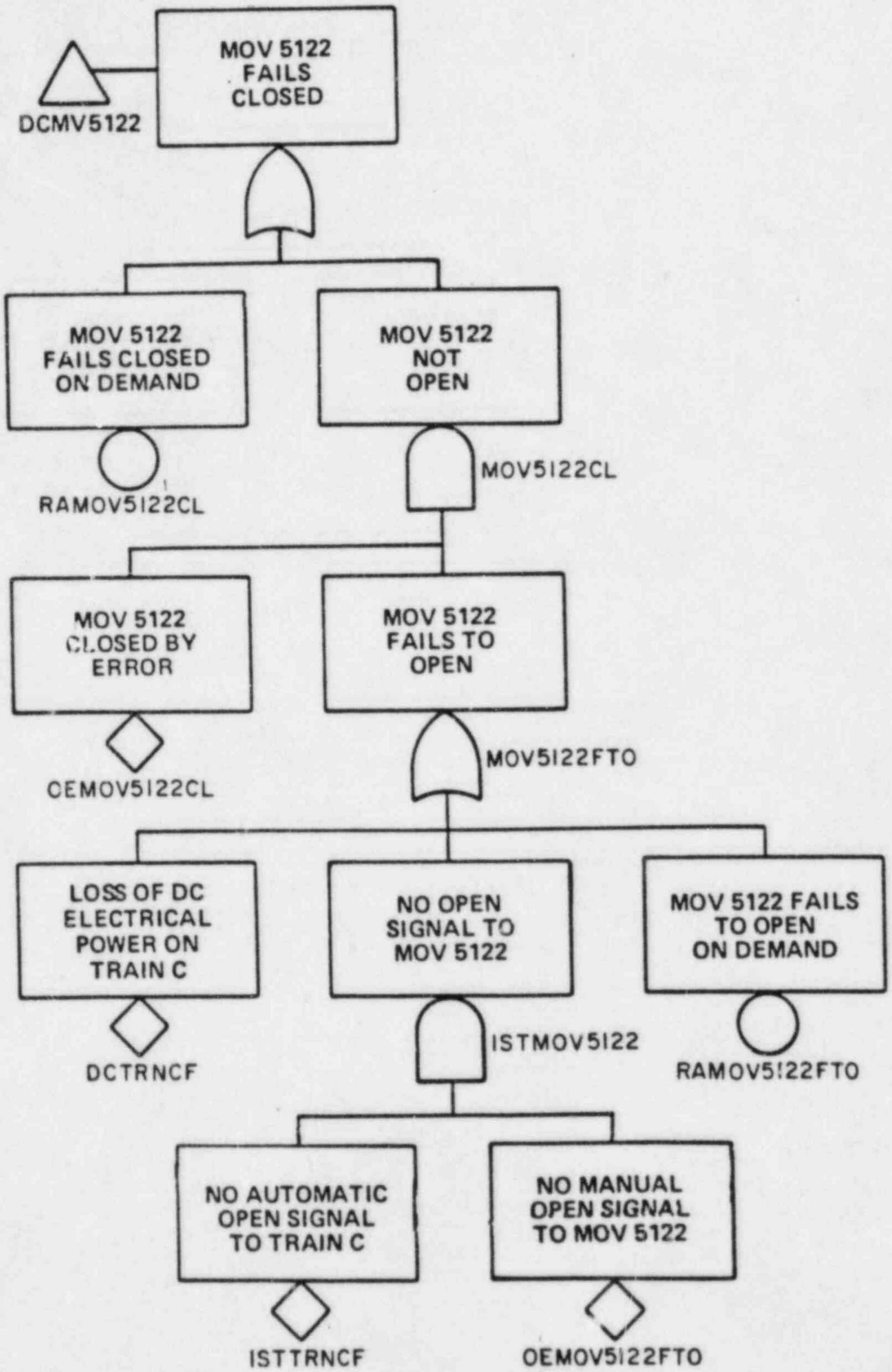
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 30 of 33)
UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 27 OF 30)

433-9



10967-3

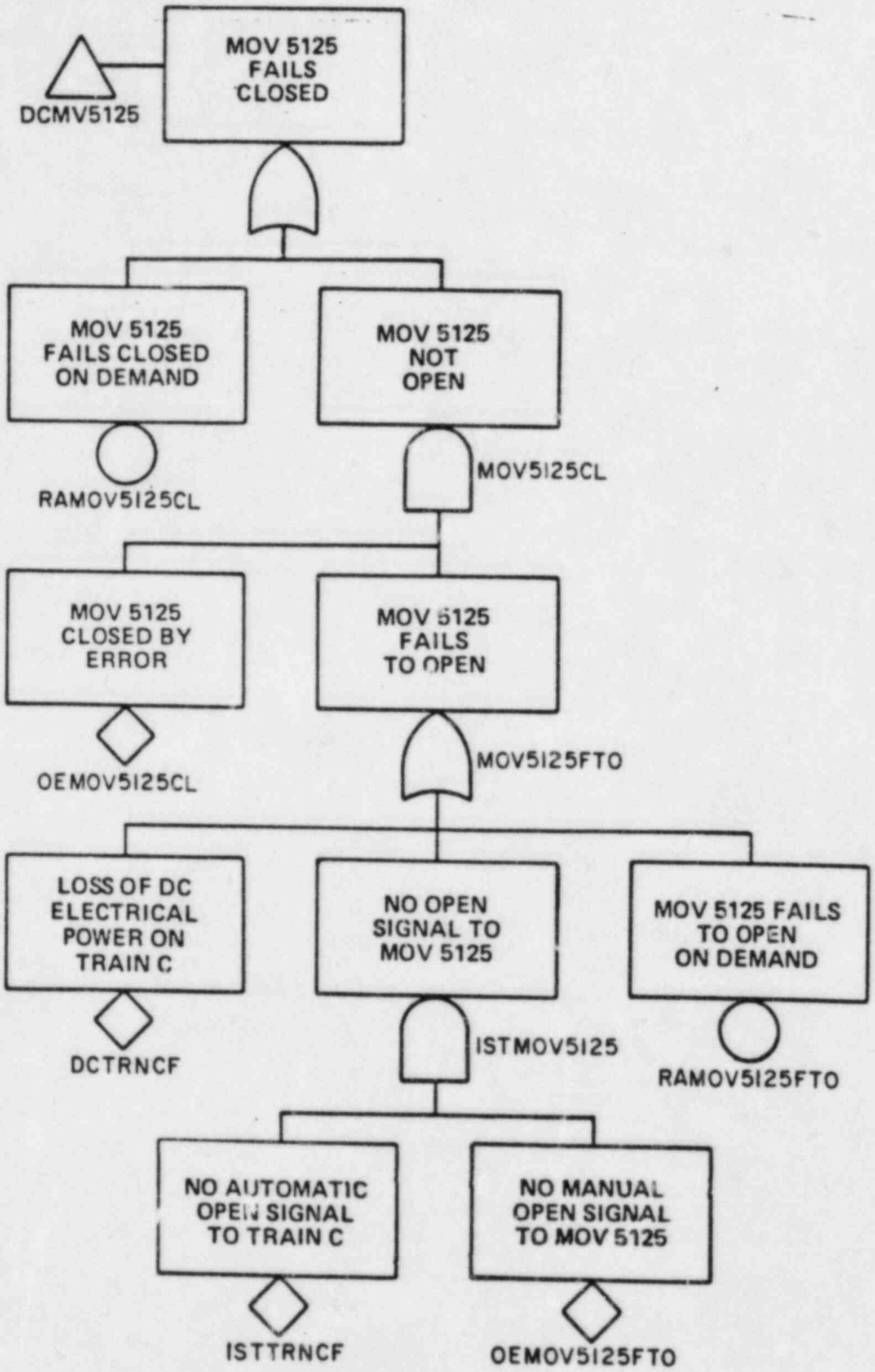
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 31 of 33)
UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 28 OF 30)

433-9



10967-3

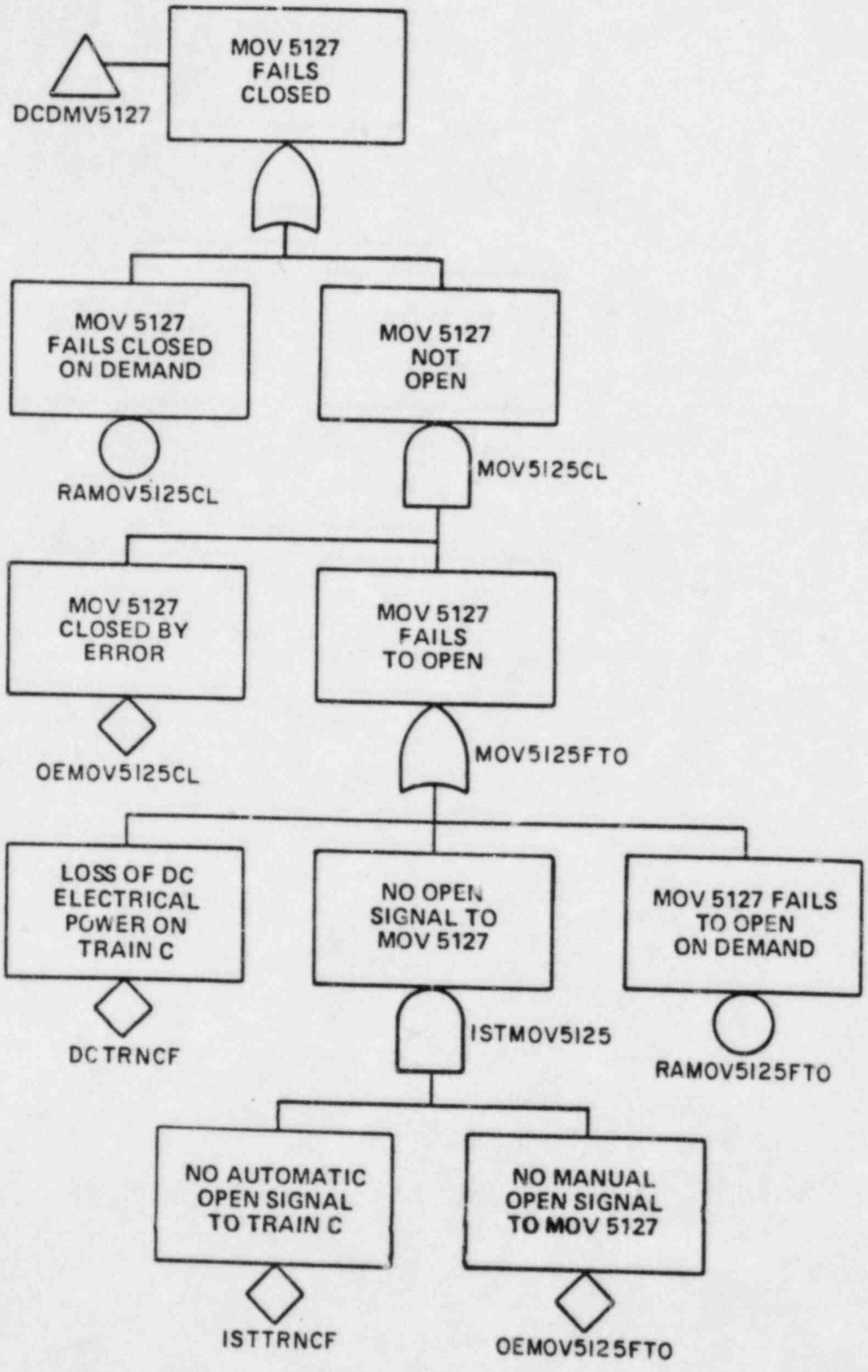
Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 32 of 33)
UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 29 OF 30)

433-9



10967-3

Georgia Power

VOGTLE
ELECTRIC GENERATING PLANT
UNIT 1 AND UNIT 2

BNL Figure 7 (Sheet 33 of 33)
UNIT 1 AFWS FAULT TREE MODEL
FSAR

FIGURE 10A-7 (SHEET 30 OF 30)

433-9

TERM NUMBER	PROB. OF TERM	
		IFTSGS1234-TKDL4 =
1	1.4790E-07	RASCV115 * RAMDPA003 * MATDPC001 +
2	1.4790E-07	RASCV114 * RAMDPA003 * MATDPC001 +
3	1.4790E-07	RASCV116 * RAMDPB002 * MATDPC001 +
4	1.4790E-07	RASCV113 * RAMDPB002 * MATDPC001 +
5	1.4790E-07	RASCV115 * RATDPC001 * MAMDPA003 +
6	1.4790E-07	RASCV114 * RATDPC001 * MAMDPA003 +
7	1.4790E-07	RASCV116 * RATDPC001 * MAMDPB002 +
8	1.4790E-07	RASCV113 * RATDPC001 * MAMDPB002 +
9	1.4500E-07	RAMDPA003 * RAMDPB002 * MATDPC001 +
10	1.4500E-07	RAMDPA003 * RATDPC001 * MAMDPB002 +
11	1.4500E-07	RAMDPB002 * RATDPC001 * MAMDPA003 +
12	1.3265E-07	RASCV113 * RASCV114 * RASCV115 +
13	1.3265E-07	RASCV113 * RASCV114 * RASCV116 +
14	1.3265E-07	RASCV114 * RASCV115 * RASCV116 +
15	1.3265E-07	RASCV113 * RASCV115 * RASCV116 +
16	1.2750E-07	RASCV115 * RAMDPA003 * RATDPC001 +
17	1.2750E-07	RASCV114 * RAMDPA003 * RATDPC001 +
18	1.2750E-07	RASCV116 * RAMDPB002 * RATDPC001 +
19	1.2750E-07	RASCV113 * RAMDPB002 * RATDPC001 +
20	1.2500E-07	RAMDPA003 * RAMDPB002 * RATDPC001 +

BNL Figure 8 VEGP AFWS Unavailability Assessment-Dominant Failure Modes Case No.1-LMFW (Sheet 1 of 2)

```
      TERM     PROB.
------NUMBER---OF TERM------------------------------------------------

----------21---9.1698E-08-----RASCV115-*-RASGVFTO-*-MAMDPA003-+-----
----------22---9.1698E-08-----RASCV114-*-RASGVFTO-*-MAMDPA003-+-----
----------23---9.1698E-08-----RASCV116-*-RASGVFTO-*-MAMDPB002-+-----
----------24---9.1698E-08-----RASCV113-*-RASGVFTO-*-MAMDPB002-+-----
----------25---9.1698E-08-----RASCV115-*-RATTVFTO-*-MAMDPA003-+-----
----------26---9.1698E-08-----RASCV114-*-RATTVFTO-*-MAMDPA003-+-----
----------27---9.1698E-08-----RASCV116-*-RATTVFTO-*-MAMDPB002-+-----
----------28---9.1698E-08-----RASCV113-*-RATTVFTO-*-MAMDPB002-+-----
----------29---9.1698E-08-----RASCV115-*-RAMOV5106-*-MAMDPA003-+-----
----------30---9.1698E-08-----RASCV114-*-RAMOV5106-*-MAMDPA003-+-----
----------31---9.1698E-08-----RASCV116-*-RAMOV5106-*-MAMDPB002-+-----
----------32---9.1698E-08-----RASCV113-*-RAMOV5106-*-MAMDPB002-+-----
----------33---8.9900E-08-----RAMDPA003-*-RASGVFTO-*-MAMDPB002-+-----
----------34---8.9900E-08-----RAMDPB002-*-RASGVFTO-*-MAMDPA003-+-----
----------35---8.9900E-08-----RAMDPA003-*-RATTVFTO-*-MAMDPB002-+-----
----------36---8.9900E-08-----RAMDPB002-*-RATTVFTO-*-MAMDPA003-+-----
----------37---8.9900E-08-----RAMDPA003-*-RAMOV5106-*-MAMDPB002-+-----
----------38---8.9900E-08-----RAMDPB002-*-RAMOV5106-*-MAMDPA003-+-----
----------39---7.9050E-08-----RASCV115-*-RAMDPA003-*-RASGVFTO-+-----
```

BNL Figure 8 (Sheet 2 of 2)

```
 TERM      PROB.
NUMBER    OF TERM

                     IFTSGS1234-TKDL4 =

     1   5.2200E-06   ACTRNAF * ACTRNBF * MATOPC001 +

     2   4.5000E-06   ACTRNAF * ACTRNBF * RATOPC001 +

     3   2.7900E-06   ACTRNAF * ACTRNBF * RASGVFTO +

     4   2.7900E-06   ACTRNAF * ACTRNBF * RATTVFTO +

     5   2.7900E-06   ACTRNAF * ACTRNBF * RAMOV5106 +

     6   1.8900E-06   ACTRNAF * ACTRNBF * MAMOV3009 +

     7   1.8900E-06   ACTRNAF * ACTRNBF * MAMOV3019 +

     8   1.8900E-06   ACTRNAF * ACTRNBF * MAMOV5106 +

     9   1.8900E-06   ACTRNAF * ACTRNBF * MATTV +

    10   1.8900E-06   ACTRNAF * ACTRNBF * MASGV +

    11   9.9000E-07   ACTRNAF * ACTRNBF * RAMGV015 +

    12   9.6000E-07   ACTRNBF * RATOPC001 * MADGA +

    13   9.6000E-07   ACTRNAF * RATOPC001 * MADGB +

    14   8.8740E-07   RASCV116 * ACTRNBF * MATOPC001 +

    15   8.8740E-07   RASCV113 * ACTRNBF * MATOPC001 +

    16   8.8740E-07   RASCV115 * ACTRNAF * MATOPC001 +

    17   8.8740E-07   RASCV114 * ACTRNAF * MATOPC001 +

    18   8.7000E-07   ACTRNBF * RAMDPA003 * MATOPC001 +

    19   8.7000E-07   ACTRNBF * RATOPC001 * MAMDPA003 +
```

BNL Figure 9 VEGP AFWS Unavailability Assessment-Dominant Failure Modes Case No.2-<u>LOOP</u> (Sheet 1 of 2)

```
  TERM      PROB.
  NUMBER   OF TERM

    20   8.7000E-07   ACTRNAF * RAMDPB002 * MATDPC001 +
    21   8.7000E-07   ACTRNAF * RATDPC001 * MAMDPB002 +
    22   7.6500E-07   RASCV116 * ACTRNBF * RATDPC001 +
    23   7.6500E-07   RASCV113 * ACTRNBF * RATDPC001 +
    24   7.6500E-07   RASCV115 * ACTRNAF * RATDPC001 +
    25   7.6500E-07   RASCV114 * ACTRNAF * RATDPC001 +
    26   7.5000E-07   ACTRNBF * RAMDPA003 * RATDPC001 +
    27   7.5000E-07   ACTRNAF * RAMDPB002 * RATDPC001 +
    28   5.9520E-07   ACTRNBF * RASGVFTO * MADGA +
    29   5.9520E-07   ACTRNBF * RATTVFTO * MADGA +
    30   5.9520E-07   ACTRNBF * RAMOV5106 * MADGA +
    31   5.9520E-07   ACTRNAF * RASGVFTO * MADGB +
    32   5.9520E-07   ACTRNAF * RATTVFTO * MADGB +
    33   5.9520E-07   ACTRNAF * RAMOV5106 * MADGB +
    34   5.3940E-07   ACTRNBF * RASGVFTO * MAMDPA003 +
    35   5.3940E-07   ACTRNBF * RATTVFTO * MAMDPA003 +
    36   5.3940E-07   ACTRNBF * RAMOV5106 * MAMDPA003 +
    37   5.3940E-07   ACTRNAF * RASGVFTO * MAMDPB002 +
    38   5.3940E-07   ACTRNAF * RATTVFTO * MAMDPB002 +
```

BNL Figure 9 (Sheet 2 of 2)

TERM NUMBER	PROB. OF TERM	
		IFTSGS1234-TKDL4 =
1	5.8000E-03	MATDPC001 +
2	5.0000E-03	RATDPC001 +
3	3.1000E-03	RASGVFTO +
4	3.1000E-03	RATTVFTO +
5	3.1000E-03	RAMOV5106 +
6	2.1000E-03	MAMOV3009 +
7	2.1000E-03	MAMOV5106 +
8	2.1000E-03	MATTV +
9	2.1000E-03	MASGV +
10	2.1000E-03	MAMOV3019 +
11	1.1000E-03	RAMGV015 +
12	2.2000E-04	DCTRNCF +
13	1.0000E-04	RACHV014 +
14	7.0000E-06	ISTTPNCF * OEMOV5106FTO +
15	3.4100E-06	RABYV090 * RAMOV5113FTO +
16	3.4100E-06	RABYV093 * RAMOV5113FTO +
17	1.2100E-06	RABYV090 * RABYV097 +
18	1.2100E-06	RAMGV005 * RAMGV007 +
19	1.2100E-06	RABYV093 * RABYV097 +
20	1.1000E-06	RABYV093 * OEMOV5113FTO +
21	1.1000E-06	RABYV090 * OEMOV5113FTO +
22	5.0000E-07	RASPDGOV * OESPDGOV +

BNL Figure 10 VEGP AFWS Unavailability Assessment Dominant Failure Modes Case No.3-LOAC