To the Graduate Council:

I am submitting herewith a thesis written by Vernon Hart Guthrie entitled "A Reliability Analysis of the Clinch River Breeder Reactor Plant Containment/Confinement Annulus Filtration System." I recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Nuclear Engineering.

J. B. Fussell, Major Professor

We have read this thesis
and recommend its acceptance:

Accepted for the Council:

Vice Chancellor
Graduate Studies and Research

Thesis
79
.G883
cop. 2

A RELIABILITY ANALYSIS OF THE CLINCH RIVER BREEDER REACTOR PLANT CONTAINMENT/CONFINEMENT ANNULUS FILTRATION SYSTEM

A Thesis

Presented for the

Master of Science

Degree

The University of Tennessee, Knoxville

Vernon Hart Guthrie

June 1979

1389786

ACKNOWLEDGEMENTS

The author wishes to express his sincere appreciation to his advisor Dr. J. B. Fussell whose support, advice, and availability were vital to the completion of this thesis.

The author also wishes to thank Dr. P. F. Pasqua for supporting this thesis through a research assistantship and for his support in the completion of this thesis.

Sincere thanks is given to Mr. D. P. Wagner and Mr. J. J. Rooney for their aid and advice throughout the development of this thesis. Mr. D. K. Goeser, Mr. W. H. Hamilton, and other personnel of Westinghouse Electric Corporation are thanked for their contributions during our many discussions.

Special appreciation is given to Miss L. S. Baker for her help with computer work and to Mr. W. M. Simpkins and Mr. H. A. Stiles for their assistance in the preparation of figures. Special appreciation is also given to Mrs. B. G. Colson for her speed in the typing of this thesis. The author would also like to thank Dr. H. L. Dodds and Dr. L. F. Miller for their support in the completion of this thesis.

The work reported herein was performed under contract between the Nuclear Engineering Department, The University of Tennessee, and Westinghouse Electric Corporation.

ABSTRACT

This thesis presents a reliability analysis of the Containment/Confinement Annulus Filtration System of the proposed Clinch River Breeder Reactor Plant. This analysis does not investigate the capability of the system; but rather the undependability of the system is estimated, and those components most important to the system undependability are identified. A new technique for performing a common cause failure analysis is used in this analysis to reduce the cost of analysis.

For the assumptions made in this analysis, the expected value of the system undependability, that is, the probability the system does not start or (logical or) does not complete the mission, is 0.675 for a thirty day mission. Based on the uncertainty in the input data, there is roughly a 95 percent likelihood that the undependability lies between 0.14 and 0.999. These bounds reflect no uncertainty in the system modeling.

TABLE OF CONTENTS

CHAPTER		PAGE
1.	INTRODUCTION	1
	1.1 Background	1
	1.2 Objectives	2
2.	RELIABILITY ANALYSIS METHODOLOGY	3
	2.1 System Reliability Analysis Procedure	3
	2.2 Qualitative Methodology	4
	2.3 Quantitative Methodology	6
3.	NEW TECHNIQUE FOR DETERMINING COMMON CAUSE FAILURE POTENTIAL	7
	3.1 Introduction	7
	3.2 Reconstruction of the Fault Tree	7
	3.3 Identification of Common Cause Events	15
	3.4 Identification of Common Cause Candidates	17
	3.5 Conclusions Regarding the New Procedure Used for Computer-Aided Common Cause Failure Analysis	18
4.	ANALYSIS OF THE CLINCH RIVER BREEDER REACTOR PLANT CONTAINMENT/CONFINEMENT ANNULUS FILTRATION SYSTEM	20
	4.1 System Description and Operation	20
	4.2 Modeling Approach	24
	4.3 Assumptions for the Qualitative Analysis	25
	4.3.1 Assumptions in Obtaining the Minimal Cut Sets	25
	4.3.2 Assumptions in Obtaining the Common Cause Events	26
	4.4 Assumptions for the Quantitative Analysis	26
	4.5 Analysis Procedure	27
5.	RESULTS OF THE ANALYSIS OF THE CLINCH RIVER BREEDER REACTOR PLANT CONTAINMENT/CONFINEMENT ANNULUS FILTRATION SYSTEM	29
6.	CONCLUSIONS AND RECOMMENDATIONS	35
LIST OF REFERENCES		38
APPENDICES		41
A.	CRBRP Annulus Filtration System Logic Model	42

PAGE

B. Minimal Cut Set Information 104

C. Common Cause Failure Analysis Information 129

D. Quantitative Data 143

E. Lists of Important Cut Sets 152

F. Important Details of the Quantitative Analysis 157

G. Glossary of Terms 162

LIST OF REFERENCES 164

VITA 166

LIST OF TABLES

TABLE		PAGE
5.1	The Best Estimate of the Probability of Failure For CRBRP Systems as Analyzed at The University of Tennessee	32
6.1	List of Components Most Important to System Undependability	37
A.1	Abbreviations Used in Point Descriptions in the Fault Tree	44
A.2	Abbreviations Used in the Fault Tree	52
B.1	System Identification Codes	106
B.2	Component Description Codes	107
B.3	Failure Mode Codes	110
B.4	Operator Identification Codes	112
B.5	List of One and Two Event Cut Sets	113
C.1	Special Conditions Resulting in Dependence Between Components	130
C.2	Generic Cause Susceptibilities	131
C.3	Generic Cause Susceptibility and Special Condition Description Codes	132
C.4	List of Common Cause Events	136
D.1	Quantitative Event Data	144
E.1	List of Important Cut Sets at the Occurrence of a DBA	153
E.2	List of Important Cut Sets at the End of the Analysis Period	155

LIST OF FIGURES

FIGURE		PAGE
3.1	Example Problem Fault Tree	8
3.2	Location Map for the Example Problem	10
3.3	IMPACT Map for the Example Problem	11
3.4	HIGH TEMPERATURE Map for the Example Problem	11
3.5	GRIT Map for the Example Problem	12
3.6	Map Showing Component Groupings Designated in the "Policies"	14
3.7	Reconstructed Fault Tree for the Example Problem	16
4.1	A Schematic of the CRBRP Annulus Filtration and Cooling Systems	21
5.1	Schematic Indicating Components Included in One Event Cut Sets	30
5.2	The Undependability of the CRBRP Annulus Filtration System After the Occurrence of a DBA Versus Time	34
A.1	Schematic Showing Points Used in Development of the System Fault Tree	43
A.2	Schematic Showing the Location of Loops in the Annulus Filtration System	45
A.3	Schematic Showing the Direction of Flow in Loop A1	46
A.4	Schematic Showing the Direction of Flow in Loop B1	47
A.5	Schematic Showing the Direction of Flow in Loop A2	48
A.6	Schematic Showing the Direction of Flow in Loop B2	49
A.7	Schematic Showing the Direction of Flow in Loop A3	50

FIGURE		PAGE
A.8	Schematic Showing the Direction of Flow in Loop B3	51
A.9	CRBRP Annulus Filtration System Fault Tree	53
B.1	Identification Code Format	105
C.1	Domain Map for Generic Cause Susceptibilities Impact, Corrosion (Acid), and Stress	133
C.2	Domain Map for Generic Cause Susceptibilities Vibration and Temperature (High)	134
C.3	Domain Map for Generic Cause Susceptibility Pressure	135
C.4	Domain Map for Generic Cause Susceptibilities Grit, Moisture, and Corrosion (Oxidation)	136
C.5	Domain Map for Generic Cause Susceptibility Temperature (Low)	137
C.6	Map Showing Domains Identified for "Pressure" in the CCFA	140
C.7	Map Showing the Groups of Components Identified for Special Conditions in the CCFA	142

CHAPTER 1

INTRODUCTION

1.1 Background

The Clinch River Breeder Reactor Plant (CRBRP) is the United States' first large scale demonstration breeder reactor power plant. The CRBRP design contains several safety related systems. One safety related system is the containment/confinement Annulus Filtration System which is designed to aid in meeting the allowable dose at the boundary of the plant in the event of a design basis accident. In the event of an accident involving radiation release into the containment building, the Annulus Filtration System (AFS) must start and continue to function properly for an extended period of time. Otherwise, the public could be subjected to radiation doses above regulated limits. Therefore, a complete reliability evaluation of the AFS failure is essential. A description of the AFS is given in the Preliminary Safety Analysis Report (PSAR). Specifically, the PSAR states, "two 100% redundant filter fan units . . . with associated ductwork and accessories are provided for the annulus exhaust, recirculation, and filtering. This insures that no single active failure will prevent 100% operation of the annulus filtration system."[1]

In a meeting with CRBRP project personnel[2] a decision was made to perform a qualitative and quantitative reliability analysis of the AFS using fault tree analysis techniques.[3,4,5,6,7,8,9] The methods used in this thesis are similar to those used in the Reactor Safety Study (WASH-1400)[10]; however, a new methodology is used in the qualitative analysis to evaluate possible common cause failures of the system.

This new methodology was used because the high computer cost of other methods.[11,12,13,14,15] The overall methodology used in this thesis is discussed in Chapter 2. The new methodology for common cause failure evaluation is presented in Chapter 3. Appendix G contains a glossary of terms used in this thesis.

1.2 Objectives

A major objective of this thesis is to identify those events or combination of events whose occurrence will result in the failure of the CRBRP Annulus Filtration System. This objective includes the identification of the minimal cut sets and the common cause events of the system. A new methodology for determining the common cause events is demonstrated.

Another objective of this thesis is to use the results of the qualitative analysis to perform a quantitative analysis. The minimal cut sets are to be ranked by importance, and those with the highest rank are identified. Also, the probability the system will not work upon demand or will fail to work during the mission, the system undependability, is determined. Since the AFS is still in the design process, the results of the analysis presented here can be input to that design effort.

CHAPTER 2

RELIABILITY ANALYSIS METHODOLOGY

2.1 System Reliability Analysis Procedure

A system reliability analysis can consist of nine steps. These are:

1. System definition
2. System fault tree construction
3. Determination of the minimal cut sets
4. Common cause failure analysis
5. Updating the qualitative analysis to reflect the common cause failure analysis results
6. Quantitative analysis
7. Uncertainty analysis
8. Formulation of conclusions and recommendations
9. Final documentation.

The first step, system definition, includes determining the physical system bounds and defining the main or TOP event of interest. The TOP event of the fault tree describes the problem being addressed by the analysis. Also, all conditions and assumptions about the system that might effect the analysis are listed.

A fault tree is constructed to graphically represent the failure logic of a system associated with a particular TOP event. The fault tree enumerates and develops, to the basic event level, those events which will cause the TOP event to occur.

The minimal cut sets of the fault tree describe the combination of hardware failures or operator errors, that is the basic events,

that will cause the TOP event. A common cause failure analysis is performed to identify sources of basic event statistical dependence.

A quantitative analysis is performed to determine system failure characteristics. The quantitative analysis reflects system failures due to independent basic event failures (minimal cut sets) and causes of dependent basic event failure (common cause events). This quantitative analysis shows the characteristics of the system for a specified mission and those basic events or sets of basic events most important to system failure.

2.2 Qualitative Methodology

There are two parts to a qualitative analysis. The first is to determine the minimal cut sets from the system fault tree. Two computer programs used to determine the minimal cut sets from a fault tree of a system are PREP[8] and MOCUS[7]. PREP deterministically tests all possible combinations of basic events to see which combinations will cause the TOP event to occur. Those combinations that cause the TOP event to occur are listed, and a search is made to delete all super sets.

The second part of a qualitative analysis is to perform a common cause failure analysis. An existing common cause failure analysis technique[11,13,14,15] requires that each minimal cut set, of the fault tree being analyzed, be searched to determine if the criteria for a common cause candidate is met. This is accomplished by first creating a list of secondary failures for each basic event of the fault tree. The secondary failures of a basic event are described by either

generic cause susceptibilities and the respective domains for the basic events, or special conditions.* Then, for each basic event in a minimal cut set, these lists are searched and any causes of secondary failure common to all the basic events in the minimal cut set are determined. Those causes of secondary failure found to be common to all the basic events of a minimal cut set are called common cause events and the minimal cut set is called a common cause candidate. This procedure is repeated for all minimal cut sets to find all the common cause events, and common cause candidates of the system being analyzed. This common cause failure analysis step requires many searches to be made and for large systems an analysis can be expensive. Even using newly developed methodologies[10,13] which reduce the time required and increase the size of the system that may be analyzed for this approach, the analysis time may become prohibitive for large systems. In an effort to reduce the time and cost of a computer aided search to find the common cause events of a system, a new approach to identifying the common cause events is taken in this thesis. This new approach uses the computer programs PREP and MOCUS. This new methodology is discussed in detail in Chapter 3.

Once the common cause candidates and common cause events have been determined, possible mechanisms for the common cause events are identified. For example, high temperature, a common cause event, may be caused by a fire, or vibration may be caused by machinery in motion. Identification of the mechanisms by which the common cause

*A glossary of terms is given in Appendix G.

events occur, is needed if the analyst is to design against the common cause events and in quantifying the common cause events for the system's quantitative analysis.

2.3 Quantitative Methodology

A quantitative analysis may be used to determine the probability of system failure on demand (system unavailability on demand), the probability the system does not fail during a mission (system reliability), or the expected number of times the system will fail during a mission. The system dependability may be obtained by multiplying the system availability on demand by the system reliability given that the system was working initially. Computer programs available to aid in the calculation of these characteristics include SUPERPOCUS[7], KITT-1[8], and KITT-2[8]. Each of these computer programs has the capability to rank the basic events or cut sets according to their relative importances. This option is useful in identifying those events or sets of events that are most likely to cause a system failure. The SUPERPOCUS program allows for the determination of both unavailability and unreliability importances, while the KITT computer programs determine only the unavailability importances.

The input to these computer programs consists of basic event data and common cause event data. Data for a basic event is its failure rate, repair rate, initial failed probability, or probability of failure during the mission. The uncertainty in this data may be expressed as input to the SAMPLE program. Uncertainty bounds can then be determined for system characteristics.

CHAPTER 3

NEW TECHNIQUE FOR DETERMINING COMMON CAUSE FAILURE POTENTIAL

3.1 Introduction

The new procedure for common cause failure analysis given in this chapter is illustrated by an example problem. The logic model for this example problem is given in Figure 3.1. The three major steps in the new methodology are reconstruction of the fault tree, identification of common cause events, and identification of common cause candidates. These steps are described in detail in Sections 3.2 through 3.4 respectively. The common cause candidates are then input to the next common cause failure analysis step - identification of specific credible mechanisms for common cause failure.

3.2 Reconstruction of the Fault Tree

Each basic event in the logic model of the system being analyzed is replaced by an OR logic gate. In this system the basic events are given by the letters E, F, G, H, I, and J, which represent the failure modes of the components G', H', I', J', E', and F' respectively. The new OR gates are labeled with their former basic event labels.

Into each OR gate are input eight character alphanumeric events describing all domain and generic cause susceptibilities, or special conditions relative to that basic event.* Basic events that are one event cut sets are turned off and, therefore, receive no input since they do not satisfy the definition of common cause failure.

---

*A glossary of terms is given in Appendix G.

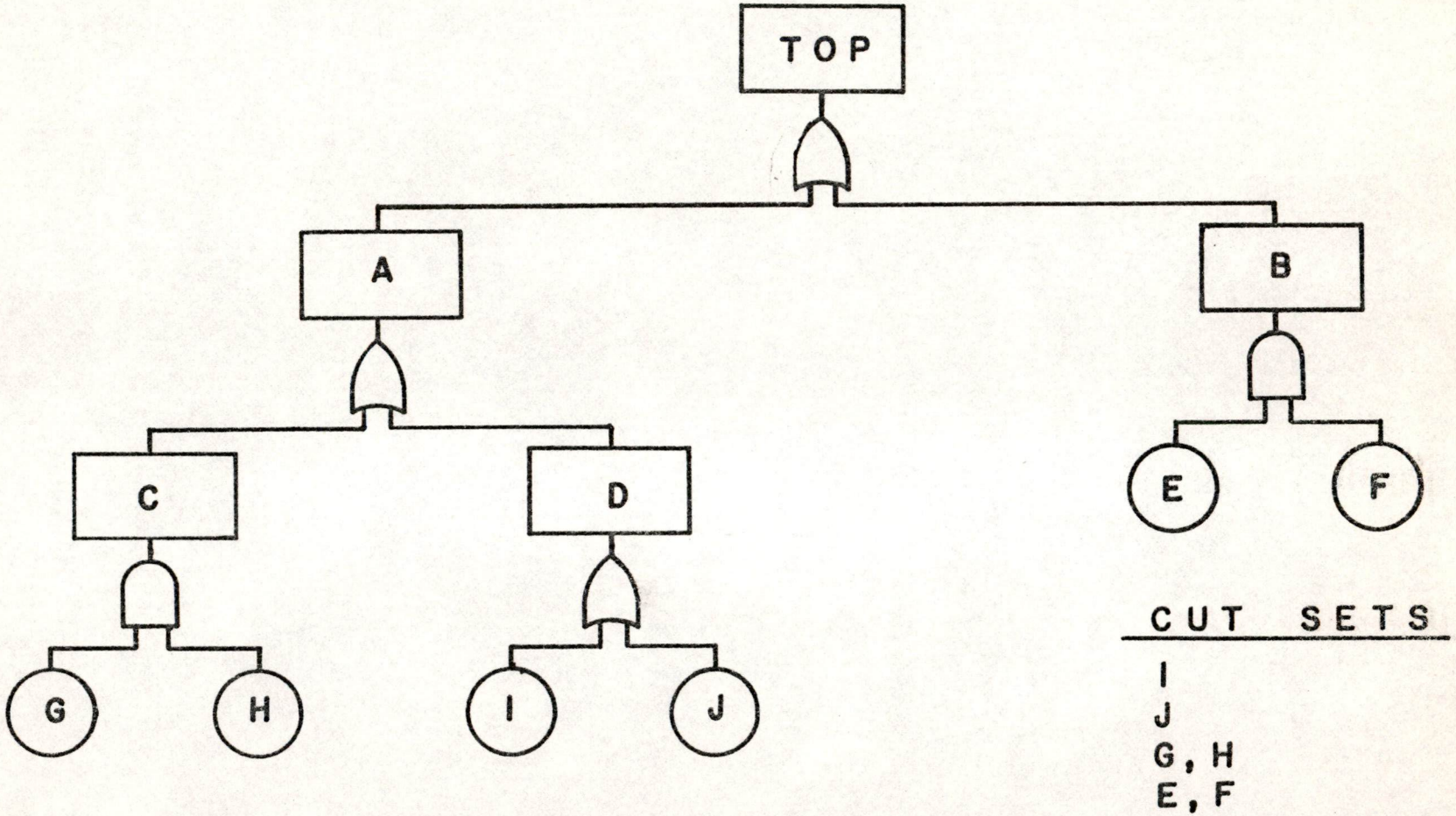


Figure 3.1. Example Problem Fault Tree

A physical location map[11] of the system given in Figure 3.1 is drawn in Figure 3.2. This map displays only the general location of the components within the physical bounds of the system. This location map is necessary in order to meet the criteria for secondary failures given in section 2.2. Using this map, the system is divided to indicate barriers against generic cause susceptibilities. A map must be drawn for each generic cause susceptibility. There are usually many natural barriers in a system, for example, walls and component housings. However, a barrier for one generic cause susceptibility may not be a barrier for another generic cause susceptibility. A missile's impact may be confined to one room, while the high temperature of a fire may affect several rooms in the system. Considering all walls to be barriers against impact, a map showing lines between components separated by walls can be drawn as shown in Figure 3.3. Each section of the map is called a domain. For example, domain 1 contains components G', H', and E'. If the generic cause susceptibilities considered for this system are impact, high temperature, and grit then two more domain maps must be drawn. Maps for high temperature and grit are given in Figures 3.4 and 3.5 respectively.

Using the domain maps, a list of generic cause susceptibilities and domains is obtained for each component. This list is compiled in the form of eight character alphanumeric descriptors. The first four characters indicate the generic cause susceptibility. The characters IMPT, TEMH, and GRIT represent impact, high temperature, and grit respectively. The last four characters of the eight character alphanumeric descriptors describe which domain the component

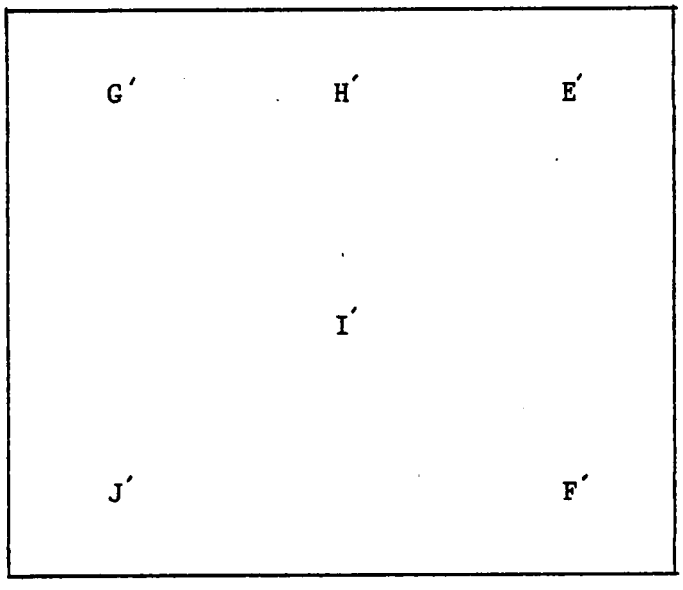


Figure 3.2. Location Map for the Example Problem.

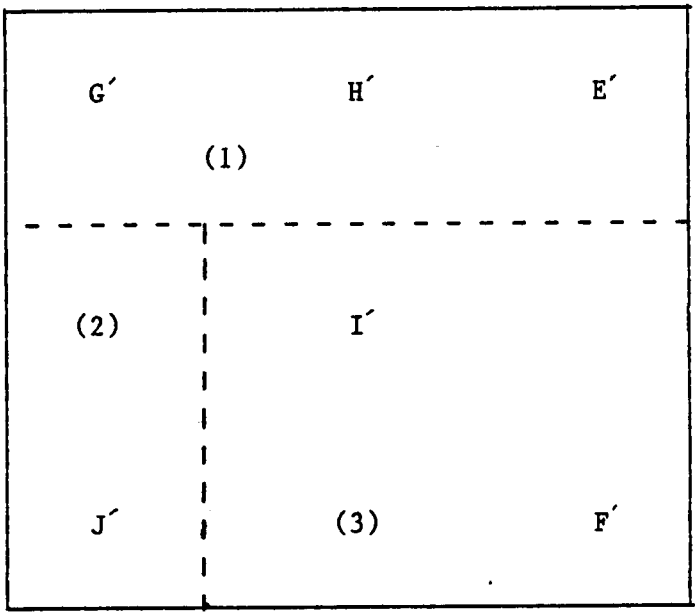


Figure 3.3. IMPACT Map for the Example Problem.

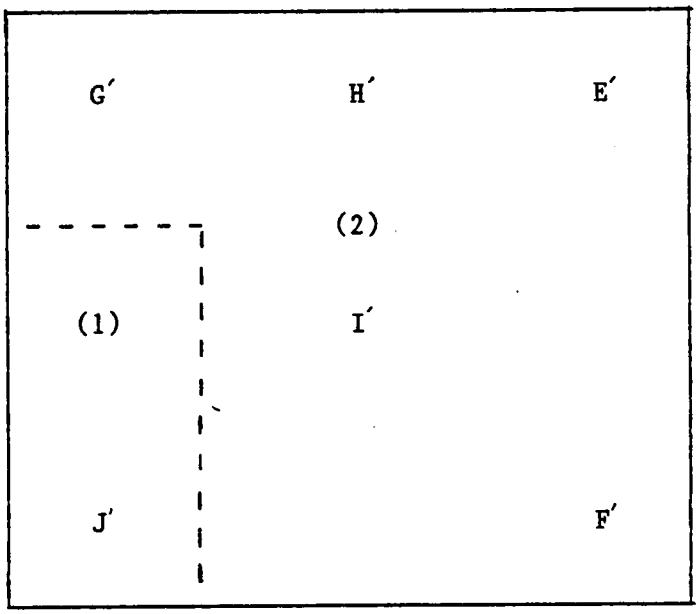


Figure 3.4. HIGH TEMPERATURE Map for the Example Problem.

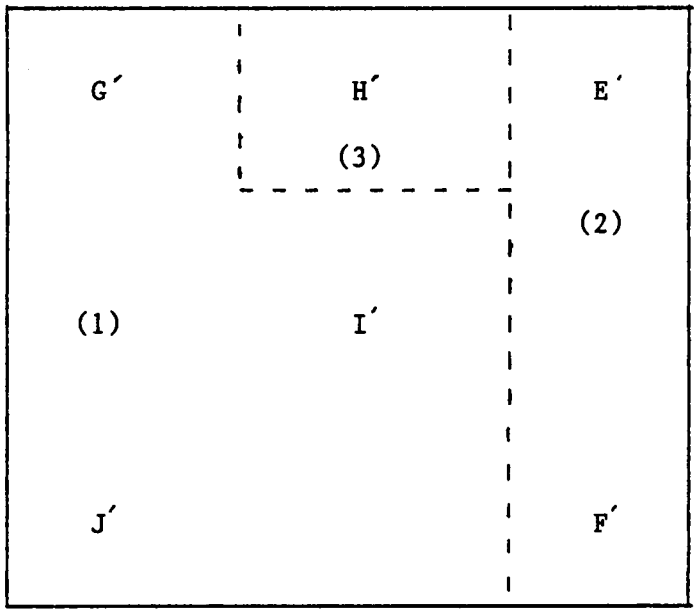


Figure 3.5. GRIT Map for the Example Problem.

is in for a particular generic cause susceptibility. For example, the component G' is in domain 1 on the impact map and so for the generic cause susceptibility impact the last four descriptor characters are L001. This indicates LOCATION 01.

The special conditions or common links for each basic event are also compiled in the form of eight character alphanumeric descriptors. The first four characters of an eight character alphanumeric descriptor indicate the special condition. For this example system the special conditions manufacturer, maintenance, and operator or operation are considered; and are described by the characters MANU, MAIN, and OPOP respectively. The last four characters of the eight character alphanumeric descriptors are determined by policies set up for each of the special conditions. These policies can be written to minimize the number of common cause events determined by requiring, when practical, that components in the same minimal cut sets be "separated." For example, since E' and F' in the previous example are in the same minimal cut set, the analyst could recommend that different maintenance crews work on these components. For this example problem the policy for manufacturer is: company 1 manufactures components G', H', and F'; company 2 manufactures component J'; and company 3 manufactures components I' and F'. Figure 3.6 shows a map with dotted lines separating the groups of components given above with the groups being numbered according to the company numbers. The policies for maintenance and operator crews for this example also require assignment by the groups of the map in Figure 3.6. For component I' which is in group 3, the last four descriptor characters for the special condition manufacturer are CS03. This indicates COMMON SOURCE 03. For this

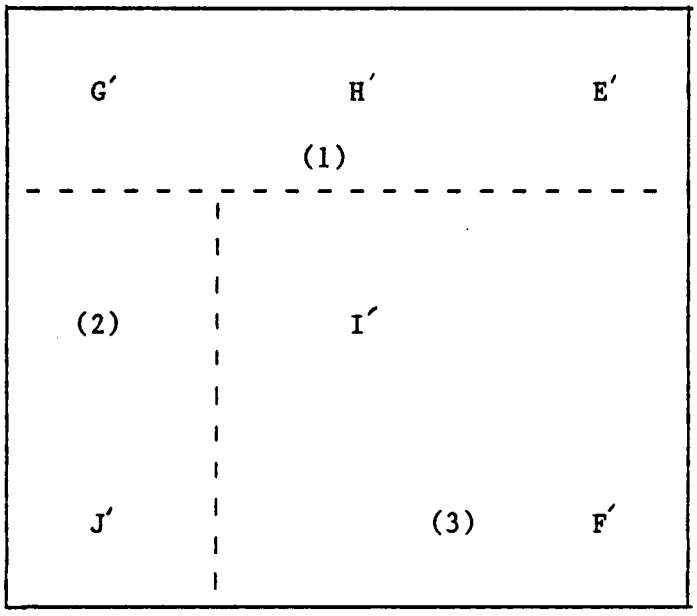


Figure 3.6. Map Showing Component Groupings Designated in the "Policies."

example system, three descriptors for special conditions are input for each basic event.

Below are compiled the list of secondary failure descriptors for each basic event of the system, except those that represent one event cut sets.

G	H	E	F
IMPTL001	IMPTL001	IMPTL001	IMPTL003
TEMPL002	TEMPL002	TEMPL002	TEMPL002
GRITL001	GRITL003	GRITL002	GRITL002
MANUCS01	MANUCS01	MANUCS01	MANUCS03
MAINCS01	MAINCS01	MAINCS01	MAINCS03
OPOPCS01	OPOPCS01	OPOPCS01	OPOPCS03

Figure 3.7 shows the reconstructed tree with the secondary failure descriptors listed above input into the appropriate gates.

3.3 Identification of Common Cause Events

The TREE given in Figure 3.7 must now be solved to find the one event cut sets. The one event cut sets are those secondary failure descriptors which by themselves can cause the TOP event to occur, and are, therefore common cause events for the system being analyzed. The One Event cut sets of this TREE can be easily found by inspection. If either event B or event C occur, the TOP event will occur. Therefore, a one event cut set for this system is a descriptor that is input to gates G and H or to gates E and F. Checking the input to gates G and H one can see that the descriptor IMPTL001 is in each list and is, therefore, a one event cut set. Checking the complete list of descriptors for the new OR gates G and H and the complete list of descriptors for the new OR gates E and F, the following list of one event cut sets, common cause events, is found.

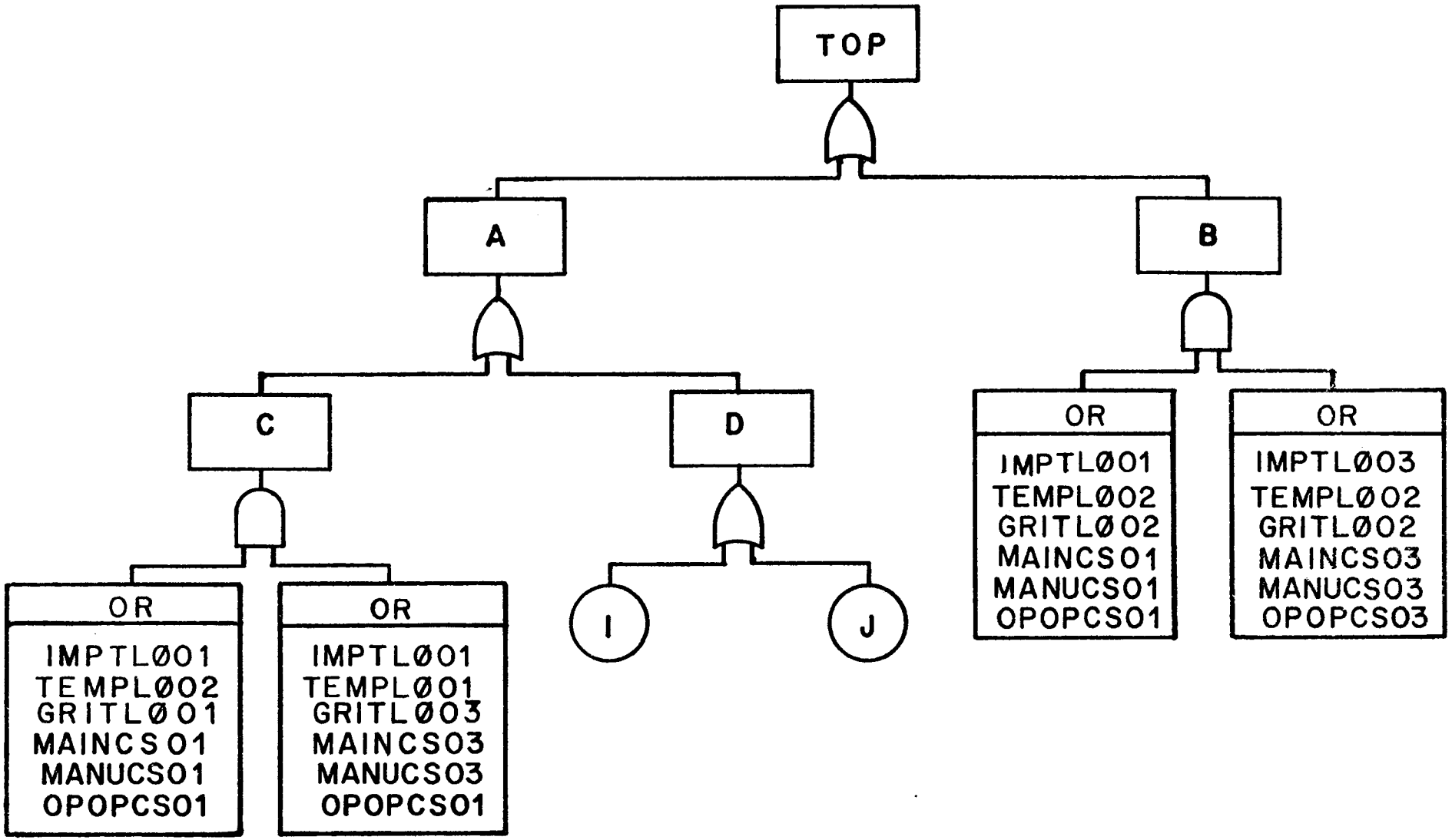


Figure 3.7. Reconstructed Fault Tree for the Example Problem.

IMPTL001
TEMPL002
GRITL002
MANUCS01
MAINCS01
OPOPCS01

For large systems the list of one event cut sets, common cause events, can be found using the computer program PREP. Each basic event in the TREE is replaced by an OR gate, and eight character alphanumeric events describing possible secondary failures of the basic event are input to the OR gate. The option allowing only the one event cut sets to be determined is used. The list obtained will be the common cause events of the system.

3.4 Identification of Common Cause Candidates

For a more complete common cause failure analysis, one may wish to know the common cause candidates. The minimal cut sets identified as common cause candidates can be used to make design corrections. For example, if all the basic events in a minimal cut set are susceptible to impact, a wall can be placed so that the entire cut set can not be failed by the same missile, thus eliminating a possible common cause failure of the system. Also, the the number of minimal cut sets failed by a common cause event affects the quantitative analysis.

The common cause candidates in Figure 3.7 can be found easily by inspection. The minimal cut sets, excluding One Event cut sets, of Figure 3.1 (page 8) are G,H and E,F . The descriptor IMPTL001 is in the lists of basic events G, H, and E but does not occur in the list of basic event F. Therefore the common cause event TEMPL002 can potentially fail only the minimal cut set G,H . On the other hand, one can see by inspection that the common cause event IMPTL001 can

potentially fail both G,H and E,F . Inspecting each common cause event, the following list of common cause events and their respective common cause candidates is determined.

IMPTL001	G,H
TEMPL002	G,H; E,F
GRITL002	E,F
MANUCS01	G,H
MAINCS01	G,H
OPOPSC01	G,H

For large systems the list of common cause candidates associated with a common cause event can be found using the computer program MOCUS. A description of the original fault tree (i.e. Figure 3.1., page 8) is input into MOCUS. Then, all basic events in the fault tree not containing a particular common cause event are turned off. The minimal cut sets obtained are the common cause candidates associated with a common cause event. A separate MOCUS run must be made for each common cause event of interest.

3.5 Conclusions Regarding the New Procedure Used for Computer-Aided Common Cause Failure Analysis

Previously existing methods for common cause failure analysis require that either a complete list of minimal cut sets of the system being analyzed be obtained[15] or that a partial list of system cut sets be obtained.[11,14] Obtaining these lists of cut sets is often the most expensive step in a common cause failure analysis. The list of cut sets, once obtained, is then searched to identify the common cause events and common cause candidates of the system. This search can require long run times on any computer and consequently are generally expensive. Using the new procedure for common cause failure analysis presented in this chapter, the common cause events of the CRBRP

Containment/Confinement Annulus Filtration System were determined with a run time of 1.17 minutes on The University of Tennessee IBM 360/65 computer. While the common cause events of the system were determined, because of the requirements of the analysis presented in this thesis the common cause candidates were not determined. However, the cost of determining the common cause candidates as described in this chapter should be less than the cost of obtaining a list of cut sets for a fault tree as required by other techniques. The step in the new procedure for determining the common cause events requires the same input as previously existing methods except that no list of cut sets is required. The input to the step in the new procedure for determining the common cause candidates is given in section 3.4. A study to compare the procedure used in this analysis to previously existing procedures is recommended.

CHAPTER 4

ANALYSIS OF THE CLINCH RIVER BREEDER REACTOR PLANT CONTAINMENT/CONFINEMENT ANNULUS FILTRATION SYSTEM

4.1 System Description and Operation

The system analyzed in this thesis is the Containment/Confinement Annulus Filtration System (AFS) of the proposed Clinch River Breeder Reactor Plant. The system is designed so that, if the system functions properly, an acceptable upper limit of leakage of radioactive materials from the containment/confinement annulus is not exceeded under design basis accident conditions. The system is also required to maintain 0.25 inch of H_2O negative pressure with respect to the outside atmosphere in the Containment/Confinement Annulus in order to collect all leakage from the containment vessel. Another system that can affect the AFS is the Annulus Cooling System (ACS), and it is, therefore, included in the analysis.

The AFS, as shown schematically in Figure 4.1, consists of two identical filter units with each unit having an associated Annulus Pressure Maintenance Fan that can exhaust 3,000 cubic feet per minute of filtered air and an Annulus Filter Fan that can recirculate 11,000 cubic feet per minute of filtered air. These two filter trains are labeled A and B.

Figure 4.1 also shows that the ducts of the two filter trains are interconnected. Ducts from the Annulus Pressure Maintenance Fans A and B are connected and lead to the exhaust ducts. Ducts from the Annulus Filter Fans A and B are connected and lead to the recirculation ducts. Air Operated Damper (AOD) 17 and the Gravity Damper

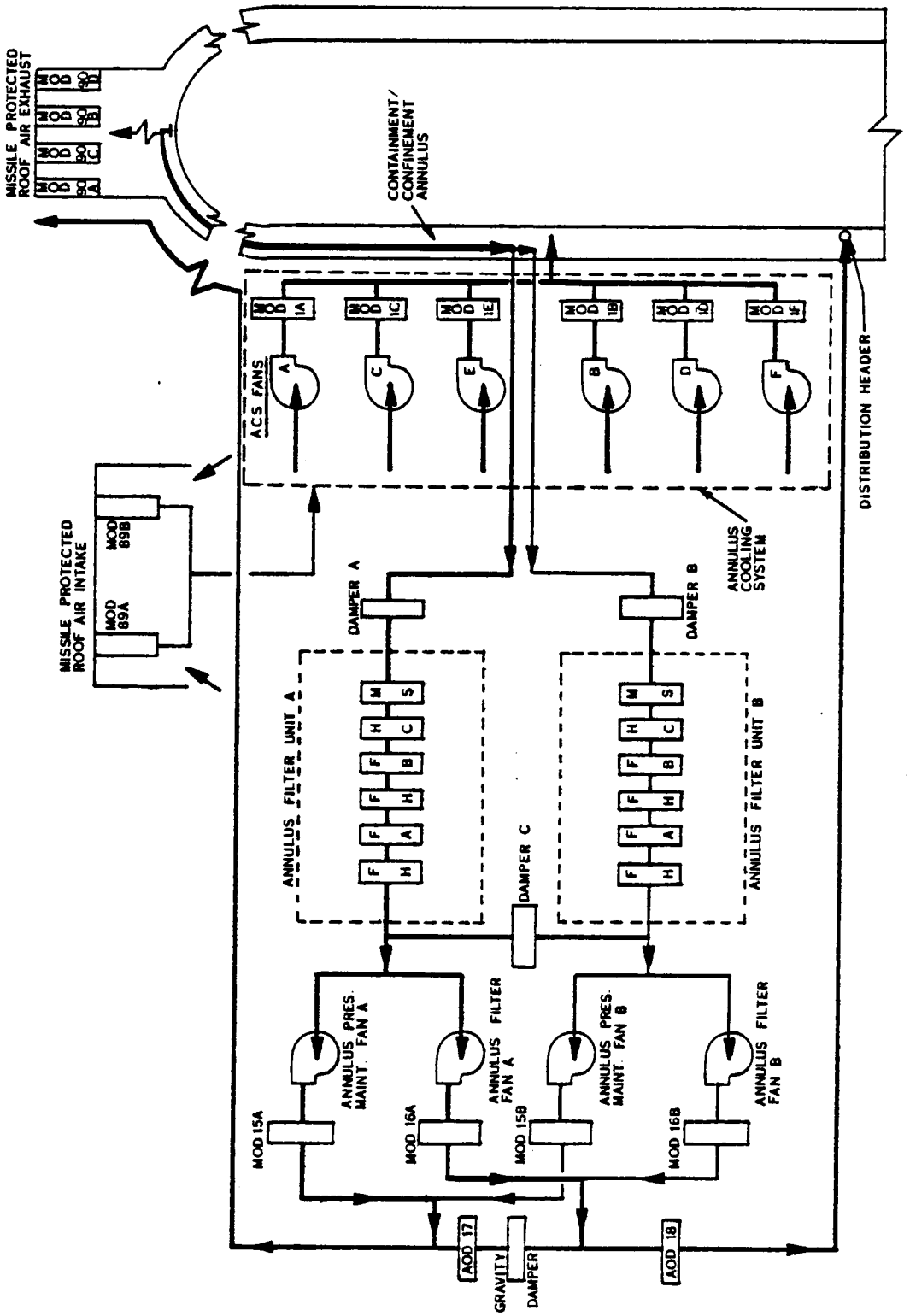


Figure 4.1. A Schematic of the CRBRP Annulus Filtration and Cooling Systems.

are positioned so that the exhaust flow necessary to maintain 0.25 inch of H_2O negative pressure in the annulus can be maintained by bleeding flow from the recirculation air. That is, if both Annulus Pressure Maintenance Fans fail (which will cause loss of capability to provide the required 0.25 inch H_2O negative pressure in the annulus), then both of the Annulus Filter Fans will be started. In this case some of the flow that normally passes through AOD 18 will pass through the gravity damper and the partially opened AOD 17 providing the exhaust flow necessary to maintain 0.25 inch H_2O negative pressure in the annulus.

Several other Annulus Filtration System components may be seen in Figure 4.1. AOD 18 is positioned to block flow in the recirculation ducts. Each of the four fans of the AFS has an associated motor operated damper that may be used to block the duct or to regulate flow from the respective fan. Each annulus filter unit[19,20] consists of a moisture separator, heating coil, high efficiency bag filter, high efficiency particulate air (HEPA) filter, adsorber filter, and a high efficiency particulate air (HEPA) filter. Manually Operated Dampers A and B are placed before their respective filter units to block flow in the event of a filter failure. The filter units are connected and the Manually Operated Damper C allows a small flow to be drawn through the filter system not being used. This small flow is needed to cool the filters heated by radioactive particles, and is needed for the entire period that the unit is not in use. Damper C can be opened to allow flow through filter unit B(A) that is drawn by A(B) train fans. However, the position of damper C cannot be changed after the occurrence of a DBA. Also included in the AFS are the four motor

operated dampers MOD 90A, 90B, 90C, and 90D at the top of the confinement structure. These dampers are scheduled to be opened only if cooling of the containment becomes necessary and are not scheduled to be opened during operation of the AFS.

The Annulus Cooling System is also shown in Figure 4.1. This system has six fans and each fan can provide 133,000 cubic feet per minute of flow. This flow circulates through the annulus, cooling the containment, and is then exhausted through the MODs 90A, 90B, 90C, and 90D. Each fan has an associated damper to restrict or block flow as needed. Air for the system is drawn in through MOD 89A and 89B of the Missile Protected Fresh Air Intake. This system is not scheduled to be activated during a design basis accident. If the system is inadvertently activated the AFS can no longer function since all of the air in the annulus will be exhausted out the top of the containment.

During normal operation, one of the annulus pressure maintenance fans will exhaust air from the annulus through its associated filter unit and discharges to the outside atmosphere to maintain the required .25 inch negative pressure. No recirculation of the filtered air is performed. The filter trains alternate on one month schedules.[1]

Upon the occurrence of a design basis accident, containment isolation (which seals leak paths to the atmosphere) is activated, and is assumed to work for this analysis. Also, all four of the AFS fans are tested. If all four fans operate correctly, one annulus pressure maintenance fan and its associated annulus filter fan will continue to operate with its associated filter unit. If one complete train is not

found to be operating correctly, both units will be run in an effort to maintain the required filtered exhaust and recirculation air flows.

4.2 Modeling Approach

The fault tree developed for the CRBRP annulus filtration system, with an explanation of the terms and abbreviations used, is contained in Appendix A. The TOP event is "Loss of Capability to Provide Adequate Filtered Ventilation of the Containment/Confinement Annulus During a Design Basis Accident Given Containment Isolation is Adequate." Information required for the fault tree construction was obtained from personnel of Westinghouse - Advanced Reactors Division in Oak Ridge, Tennessee, and Burns and Roe Inc., in Oradell, New Jersey. Assumptions made for the construction of the fault tree are:

1. A loss of capability to provide adequate filtration of the containment/confinement annulus is assumed to occur upon (1) loss of capability to exhaust filtered air, (2) loss of capability to recirculate filtered air, (3) loss of capability to maintain 0.25 inch H_2O negative pressure in the annulus, or (4) loss of filtration capability.
2. A component is considered failed if it cannot fully perform its task.
3. At the occurrence of a design basis accident, the filter train A is assumed to be the system assigned to maintain the required 0.25 inch H_2O negative pressure, while all other components are assumed to be cold standby, that is installed but turned off.

4. Secondary failures are not considered in the fault tree. Secondary failures are treated in the common cause failure analysis.
5. The fault tree is coherent[21] in failure and repair.
6. The annulus filtration system is assumed to be needed at all times during a DBA.

4.3 Assumptions for the Qualitative Analysis

4.3.1 Assumptions in Obtaining the Minimal Cut Sets

A list of minimal cut sets determined for the fault tree of Appendix A is given in Appendix B. A description of the eight character alphanumeric descriptors used to define the basic events of the fault tree of Appendix A is also contained in Appendix B. Assumptions made in obtaining the minimal cut sets are:

1. The fault tree of Appendix A is assumed to identify all important modes of system failure. That is, all important events that can cause a failure of the AFS can be determined from the fault tree.
2. The one and two event cut sets adequately represent the TOP event for the purposes of the analysis.
3. The assumption was inadvertantly made that damper C is designed so that a flow larger than needed for cooling the standby filter system cannot occur. This assumption eliminates some cut sets. While a small change would occur in the quantitative results, the undependability would be slightly higher, the author does not feel this assumption will change the conclusions.

4.3.2 Assumptions in Obtaining the Common Cause Events

A list of common cause events determined for the fault tree of Appendix A is given in Appendix C. A description of the eight character alphanumeric descriptors used to define possible common cause events is also contained in Appendix C. Assumptions made in obtaining the common cause events are:

1. The fault tree of Appendix A adequately models the TOP event so that important causes of system faulure due to dependent component failure or operator actions can be identified.
2. Table C.2 adequately lists the generic cause susceptibilities for this analysis.
3. The barriers to the generic cause susceptibilities of this analysis are correctly defined by the domain maps given in Appendix C.
4. Table C.1 adequately lists the special conditions for this analysis.
5. The policies given in Appendix C adequately describe procedures or criteria for each of the special conditions of Table C.1. These policies were developed for this thesis because no such policies have been set elsewhere.

4.4 Assumptions for the Quantitative Analysis

There is no data bank containing all the quantitative failure and repair data needed for this thesis work. However, data for similar components does exist. Also, a large variation in data for a particular component often exists. The available data was considered and a value that seems to best model the components' anticipated behavior

was then assigned. Failure information for this analysis was obtained from several sources. These include WASH-1400[10]; Reliability Technology[22]; and IEEE Nuclear Reliability Data Manual (IEEE std 500-1977)[23]. A list of the basic event failure information is given in Appendix D.

No source of data on the repair times of components in this analysis exists. Therefore, the repair time assigned to a particular failure mode of a component in this analysis was assigned subjectively. All components contained in the same cells as the filter units after the occurrence of a DBA are assumed to be nonrepairable because of the high concentration of radionuclides in the filters. The repair time of other components before a DBA is assumed to be four times as long as the same component's repair time after a DBA. This is done since the repair crews before a DBA will probably not see the urgency for repair that will be stressed after the occurrence of a DBA. A list of basic events and their assigned repair times for both before and after a DBA is given in Appendix D.

4.5 Analysis Procedure

The completed fault tree was used to perform a qualitative analysis of the system. The first step in the qualitative analysis was to obtain the minimal cut sets from the fault tree using the PREP computer program as discussed in section 2.2. The second step was to identify common cause events. This was accomplished using the new procedure for common cause failure analysis described in detail in Chapter 3.

A quantitative analysis to determine the dependability of the system was performed using the minimal cut sets and the common cause events determined in the qualitative analysis. The analysis is performed for a 30 day mission. A detailed description of the procedure is given in Appendix F. Basic event and common cause event data was obtained as described in section 4.4. Using this data and the SUPERPOCUS computer program the system availability at the occurrence of a DBA was determined. The KITT-2 computer program was used to determine the system reliability given the system is initially working. Multiplying the system availability by the system reliability, given the system is initially working, the system dependability was obtained at the end of the 30 day mission. Once this dependability value was determined an uncertainty analysis of the result was performed using the SAMPLE computer program.

Using the SUPERPOCUS computer program, those cut sets and their respective components that are most likely to be unavailable at the beginning of a DBA were determined. Then, using the KITT-2 computer program, those cut sets and their respective components that are most likely to be unreliable at the end of the one month mission were determined. Lists of the most important cut sets for each case are given in Appendix E.

CHAPTER 5

RESULTS OF THE ANALYSIS OF THE CLINCH RIVER BREEDER REACTOR PLANT CONTAINMENT/CONFINEMENT ANNULUS FILTRATION SYSTEM

The TOP event for this analysis is "Loss of Capability to Provide Adequate Filtered Ventilation of the Containment/Confinement Annulus During a Design Basis Accident Given Containment Isolation is Adequate." In the qualitative analysis 29 one event minimal cut sets and 298 two event minimal cut sets were determined. A list of one and two event minimal cut sets is given in Appendix B. The 29 one event minimal cut sets are not interpreted as 29 individual hardware failures that will fail the system since these 29 events include operator actions. Nevertheless, there are 12 components that individually can fail the system. These components are shown in Figure 5.1. Of these 12, the most important components are Air Operated Damper (AOD) 18, AOD 17, and the four dampers over the containment/confinement annulus (MOD 90A, 90B, 90C, and 90D). These six components account for approximately 65 percent of the probability the system will be failed on demand (the initial system unavailability), and they account for approximately 75 percent of the probability the system will have failed during the mission. A system failure occurs if AOD 18 is in the closed state during a DBA since no recirculation would be possible. AOD 17 is positioned so that the exhaust flow necessary to maintain 0.25 inch water gauge negative pressure in the annulus can be maintained by bleeding flow from the recirculation air if both Annulus Pressure Maintenance Fans fail to operate. The proper air flow is

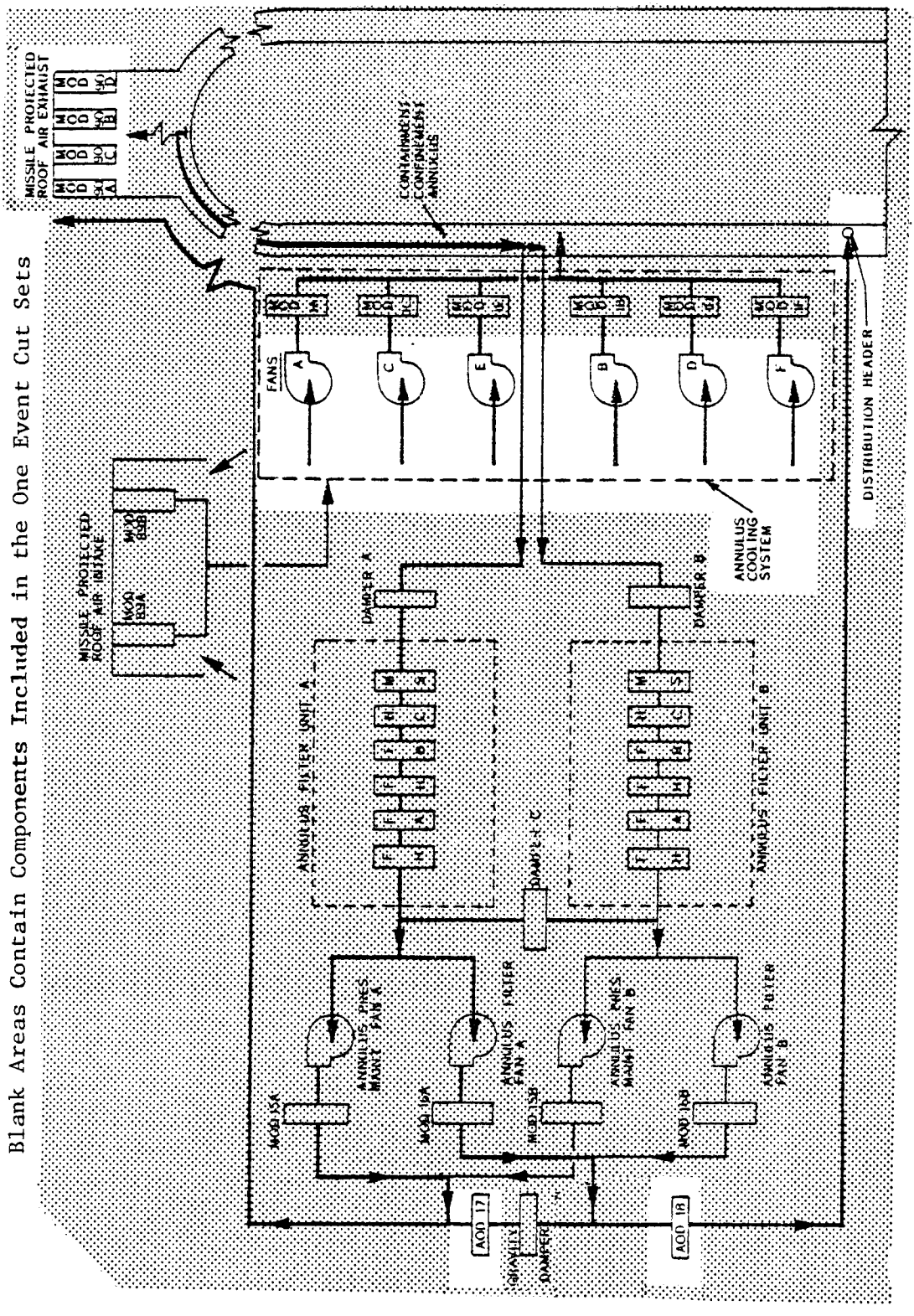


Figure 5.1. Schematic Indicating Components Included in One Event Cut Sets

controlled by the partial opening of the damper. However, if the Annulus Pressure Maintenance Fans are working and AOD 17 is open then air necessary for recirculation will be vented to the atmosphere and a system failure will occur. If either MOD 90A, 90B, 90C or 90D is open, negative pressure could be lost in sections of the annulus, and a possible leak path from the annulus to the atmosphere would be established.

Seven common cause events (generic level) were identified and are listed in Appendix C. Due to the large number of one event minimal cut sets, identifying specific mechanisms for the common cause events and other detailed common cause failure information adds no significant information to the analysis, therefore these details were not determined.

For the assumptions made in this analysis, the expected value of the system undependability, that is, the probability the system does not start or (logical or) does not complete the mission, is 0.675 for a thirty day mission. Based on the uncertainty in the input data, there is roughly a 95 percent likelihood that the undependability lies between 0.14 and 0.999. These bounds reflect no uncertainty in the system modeling. A comparison of this result with other analysis results as have been obtained at The University of Tennessee for the CRBRP are given in Table 5.1.

The system dependability over the mission reflects contributions from two parts. The probability the system works on demand (0.979), the initial system availability, was multiplied by the probability the system will not have failed during the mission given that it was initially working (.332). From this product a system dependability of

TABLE 5.1

THE BEST ESTIMATE OF THE PROBABILITY OF FAILURE
FOR CRBRP SYSTEMS AS ANALYZED AT
THE UNIVERSITY OF TENNESSEE

System	Best Estimate of Probability of Failure
Annulus Filtration	0.675
Onsite Electrical Power Supply[24]	0.00069
Shutdown Heat Removal[25]	0.00021
Shutdown[12]	0.000015

0.325 is obtained. The system undependability, the complement of the dependability, is therefore 0.675. From the SAMPLE computer program and hand calculations the 95 percent confidence bounds on the mission undependability are 0.14 to .999. Details of the calculation of these quantitative results are described in Appendix F. The results given above are shown graphically in Figure 5.2.

In the quantitative analysis the important minimal cut sets at the beginning of a DBA and at the end of the one month analysis period were determined and are listed in Appendix E. Also given in Appendix E are the unavailabilities or unreliabilities of these minimal cut sets.

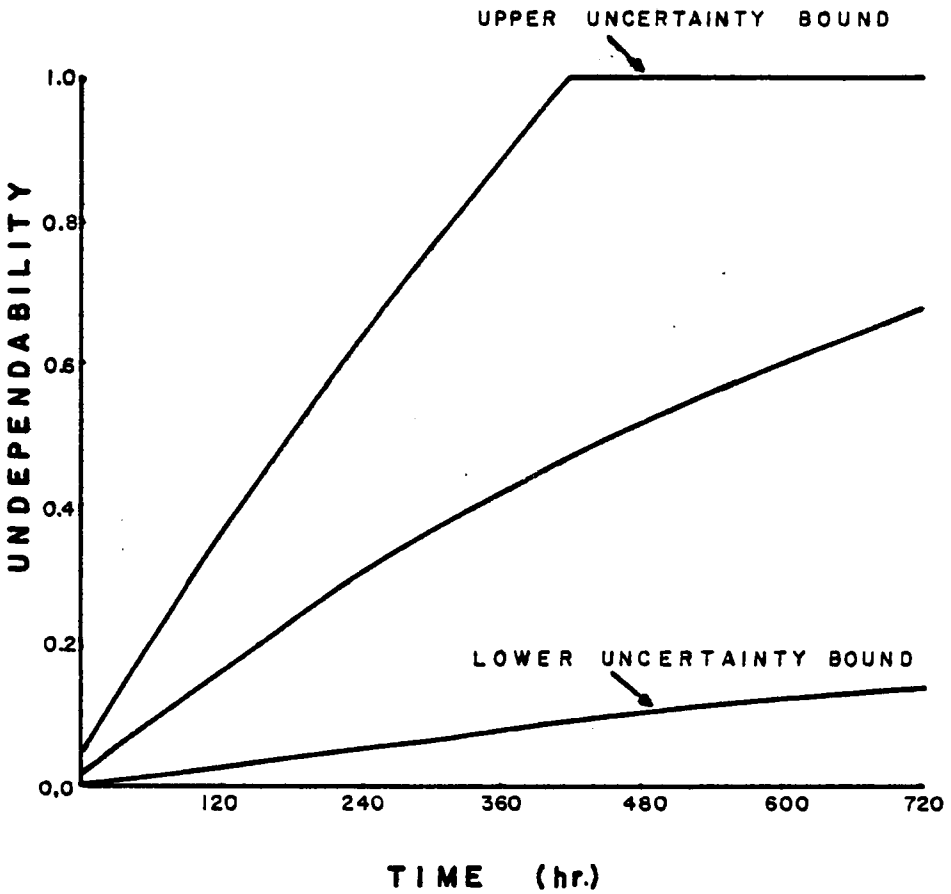


Figure 5.2. The Undependability of the CRBRP Annulus Filtration System After the Occurrence of a DBA Versus Time.

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

The methodology used in this analysis provides a systematic and thorough procedure that may be used to evaluate a system's design. In developing a fault tree for a system the analyst is required to understand a system's design, the functions and capabilities of the components, and to examine the possible system failure modes using a systematic procedure. The minimal cut sets and the common cause events determined identify the credible modes of system failure. The most important system components are determined from the quantitative analysis. System characteristics such as dependability or reliability are also obtained from the quantitative analysis.

The annulus filtration system as described in Section 4.1 is assumed to have the capability to filter the containment/confinement annulus given a sufficient number of components function. In this analysis the undependability of the system is estimated, and those components most important to the system undependability are identified. The results of the analysis of the annulus filtration system show that the expected value of the system undependability, that is, the probability the system does not start or (logical or) does not complete the mission, is 0.675 for a thirty day mission. Based on the uncertainty in the input data, there is roughly a 95 percent likelihood that the undependability lies between 0.14 and 0.999. These bounds reflect no uncertainty in the system modeling.

A design criterion for the annulus filtration system is set to insure that no single active failure will prevent 100 percent

operation of the system. However, the results of this analysis show that this criterion has not been met since several important possible single active failures are identified that can result in system failure. The six most important single failures are listed in Table 6.1. Six other one event hardware minimal cut sets are the inadvertent operation of any one of the six annulus cooling fans. These are of less importance, however, than the failures listed in Table 6.1 because of the lower probabilities of occurrence.

Since much of the component data used in this analysis was inferred from data for similar components, there is a large uncertainty in the undependability value. It is recommended that the system designers, during decision-making efforts, consider that the lower bound (the best system that can be achieved) on the mission undependability is 0.14.

TABLE 6.1

LIST OF COMPONENTS MOST IMPORTANT
TO SYSTEM UNDEPENDABILITY

(A failure of any of these components can cause the
TOP event to occur.)

Component	Failure Mode
Air Operated Damper 17	Open
Air Operated Damper 18	Closed
Motor Operated Damper 90A	Open
Motor Operated Damper 90B	Open
Motor Operated Damper 90C	Open
Motor Operated Damper 90D	Open

LIST OF REFERENCES

LIST OF REFERENCES

1. "CRBRP Preliminary Safety Analysis Report," Project Management Corporation, April 1975.

2. Goeser, D. K., and Fussell, J. B., personal communication, January 10, 1978.

3. Vesely, W. E., Analysis of Fault Trees by Kinetic Tree Theory, Idaho Nuclear, IN-13303, October 1967.

4. Haasl, D. F., "Advanced Concepts in Fault Tree Analysis," System Safety Symposium, Seattle, The Boeing Company, June 1965.

5. Lambert, H. E., System Safety Analysis and Fault Tree Analysis, University of California, UCID-16238, May 1973.

6. Fussell, J. B., "Fault Tree Analysis - Concepts and Techniques," Generic Techniques in System Reliability Analysis, Noordhoff, Leyden, 1976, pp. 133-162.

7. Fussell, J. B. et al., SUPERPOCUS - A Computer Program for Calculating System Probabilistic Reliability and Safety Characteristics, The University of Tennessee, NERS 77-01, February 1977.

8. Vesely, W. E., and Narum, R. E., PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree, Idaho Nuclear, IN-1349, August 1970.

9. Fussell, J. B., Henry, E. B., and Marshall, N. H., MOCUS - A Computer Program to Obtain Minimal Sets from Fault Trees, Aerojet Nuclear Company, ANCR-1156, August 1974.

10. Nuclear Regulatory Commission, REACTOR Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG 75/014), Washington, Government Printing Office, October 1975.

11. Wagner, D. P., "A Procedure for Qualitative Common Cause Failure Analysis of Complex Systems," Master's Thesis, The University of Tennessee, Knoxville, August 1977.

12. Cate, C. L., "A Method for Quantitative Evaluation of Common Cause Failures in System Reliability Analyses," Master's Thesis, The University of Tennessee, Knoxville, August 1977.

13. Cate, C. L., and Fussell, J. B., BACFIRE - A Computer Program for Common-Cause Analysis, NERS-77-02, Nuclear Engineering Department, The University of Tennessee, Knoxville, May 1977.

14. Rooney, J. J., and Fussell, J. B., BACFIRE II - A Computer Program to Aid in Common Cause Failure Analysis of Complex Systems, NERS-78-03, The University of Tennessee, Knoxville, August 1978.

15. Burdick, G. R., Marshall, N. H., and Wilson, J. R., COMCAN - A Computer Program for Common Cause Analysis, Aerojet Nuclear Company, ANCR-1156, August 1974.

16. Wagner, D. P., Cate, C. L., and Fussell, J. B., "Reliability and Safety Methodology for an Analysis of the Clinch River Breeder Reactor Plant," Proceedings of the Seventh Annual Modeling and Simulation Conference, Volume 7, Pittsburgh, April 26-27, 1976, pp. 1066-1070.

17. Cate, C. L., Wagner, D. P., and Fussell, J. B., "A Computer Aided Approach to Qualitative and Quantitative Common Cause Failure Analysis," Proceedings of the Eighth Annual Modeling and Simulation Conference, Volume 8, Part 1, Pittsburgh, April 21-22, 1977, pp. 25-30.

18. Wagner, D. P., Cate, C. L., and Fussell, J. B., "Common Cause Failure Analysis Methodology for Complex Systems," Nuclear Systems Reliability Engineering and Risk Assessment, SIAM, Philadelphia, 1977, pp. 289-313.

19. Nuclear Regulatory Commission, Regulatory Guide 1.52, Washington, Government Printing Office, March 1978.

20. ERDA 76-21, "Nuclear Air Cleaning Handbook," Oak Ridge National Laboratory, C. A. Burchstead, J. E. Kahn, and A. B. Fuller, March 31, 1976.

21. Esary, J. C., and Proschan, F., "Coherent Structures of Nonidentical Components," Technometrics, Vol. 5, 1963, pp. 191-209.

22. Green, A. E., and Bourne, A. J., Reliability Technology, John Wiley and Sons Ltd., London, 1972.

23. "IEEE Nuclear Reliability Data Manual," (IEEE Std 500-1977), The Institute of Electrical and Electronics Engineers, Inc., 1977.

24. Campbell, D. J., Linn, M. A., Rooney, J. J., and Fussell, J. B., A Reliability Assessment of the Clinch River Breeder Reactor Plant Safety Related Electrical Power Supply System, NERS-78-01, The University of Tennessee, January 1978.

25. Campbell, D. J., An Analysis of the Importance of Shutdown Heat Removal Components to the Overall System Availability, NERS-78-07, Masters Thesis, The University of Tennessee, December 1978.

APPENDICES

APPENDIX A

CRBRP ANNULUS FILTRATION SYSTEM LOGIC MODEL

The CRBRP annulus filtration system logic model was developed in fault tree format. The assumptions used in development of the fault tree are given in Section 4.2.

The position of the reference points used in the development of the fault tree are shown in Figure A.1. A description of the abbreviations used to identify the points is given in Table A.1. A description of the loops identified in the fault tree is given in Figures A.2 through A.8. Abbreviations used in event descriptions are given in Table A.2.

The logic model for the CRBRP annulus filtration system is presented in Figure A.9.

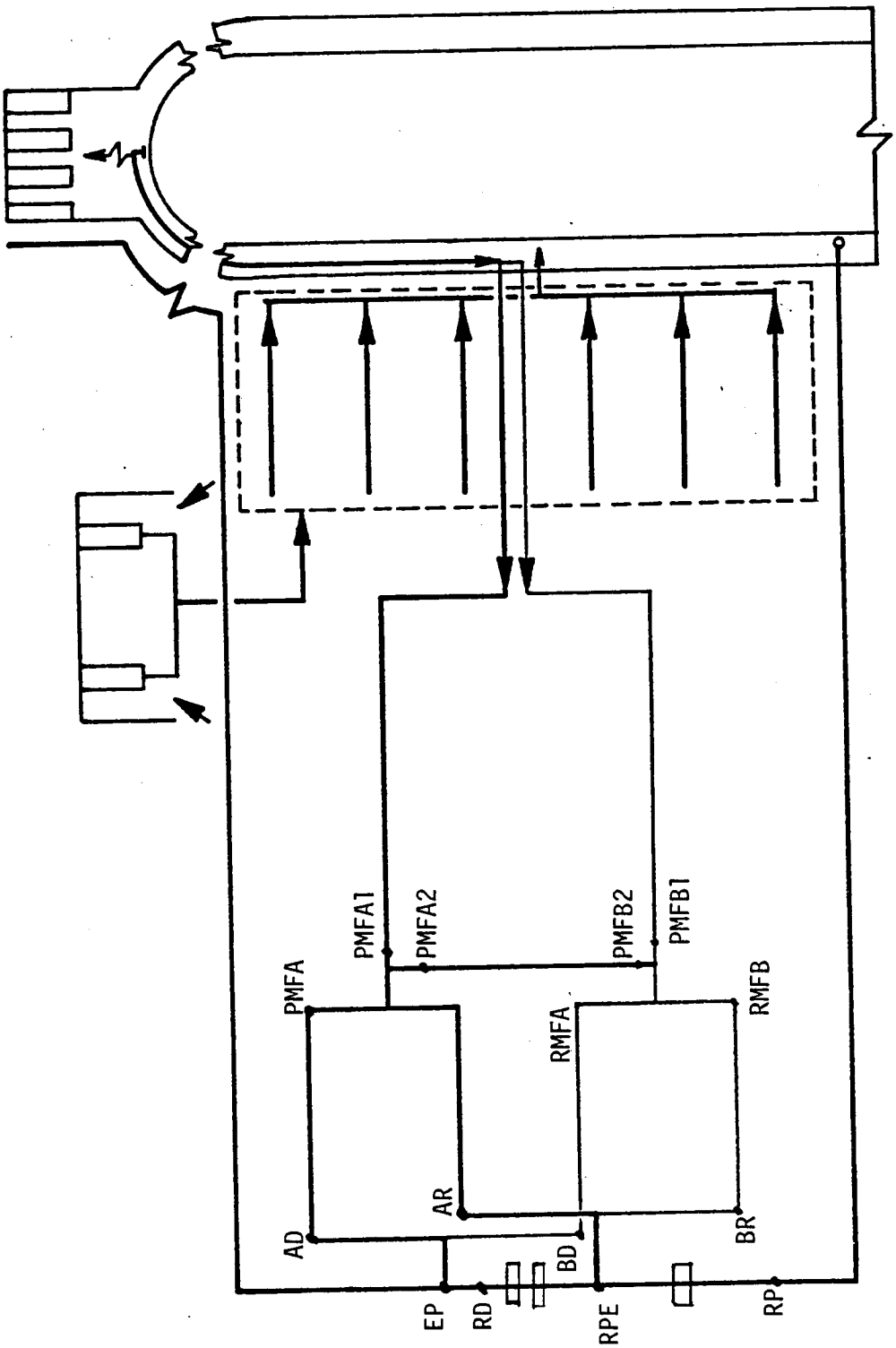


Figure A.1. Schematic Showing Points Used in Development of the System Fault Tree.

TABLE A.1

ABBREVIATIONS USED IN POINT DESCRIPTIONS IN THE FAULT TREE

Abbreviation	Description
EP	Exhaust Point
RP	Recirculation Point
RD	Recirculation Direct
RPE	Recirculation Point Exhaust
AD	System A Direct Vent
BD	System B Direct Vent
AR	System A Recirculation
BR	System B Recirculation
PMFA	Pressure Maintenance Fan A
PMFA1	Pressure Maintenance Fan A Flow Path 1
PMFA2	Pressure Maintenance Fan A Flow Path 2
RMFA	Recirculation Fan A
RMFB	Recirculation Fan B

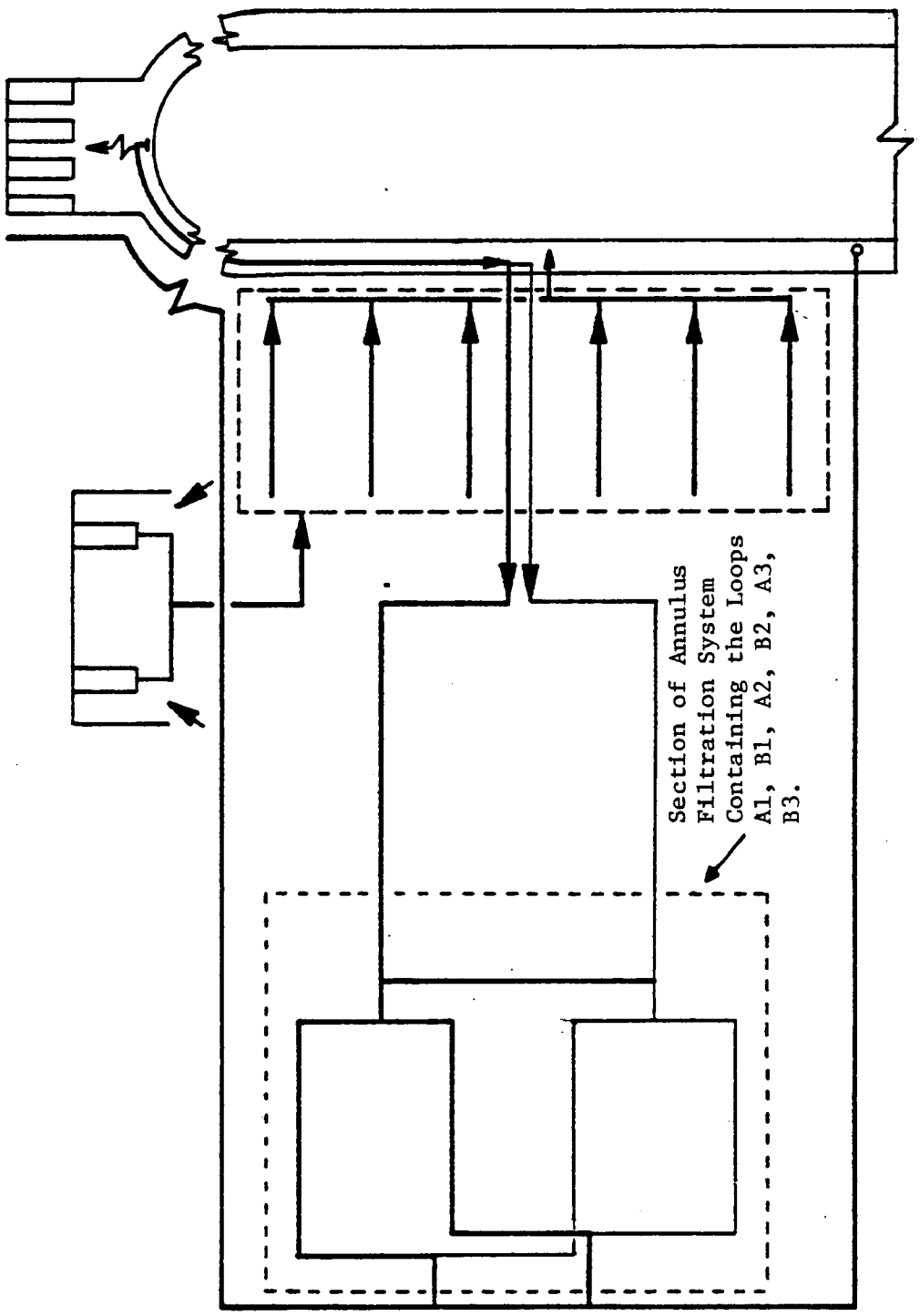


Figure A.2. Schematic Showing the Location of Loops in the Annulus Filtration System.

LOOP A1

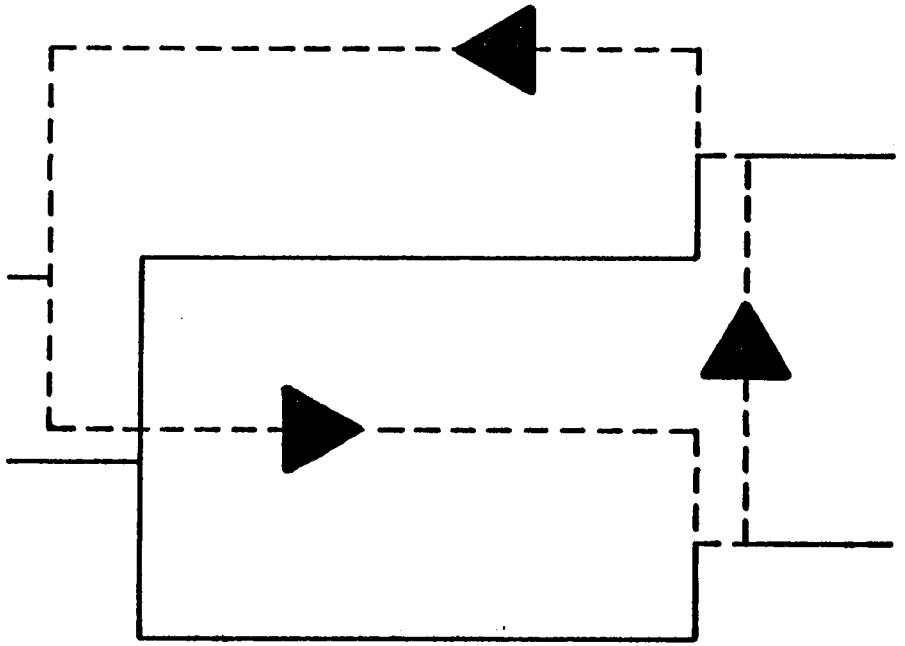


Figure A.3. Schematic Showing the Direction of Flow in Loop A1.

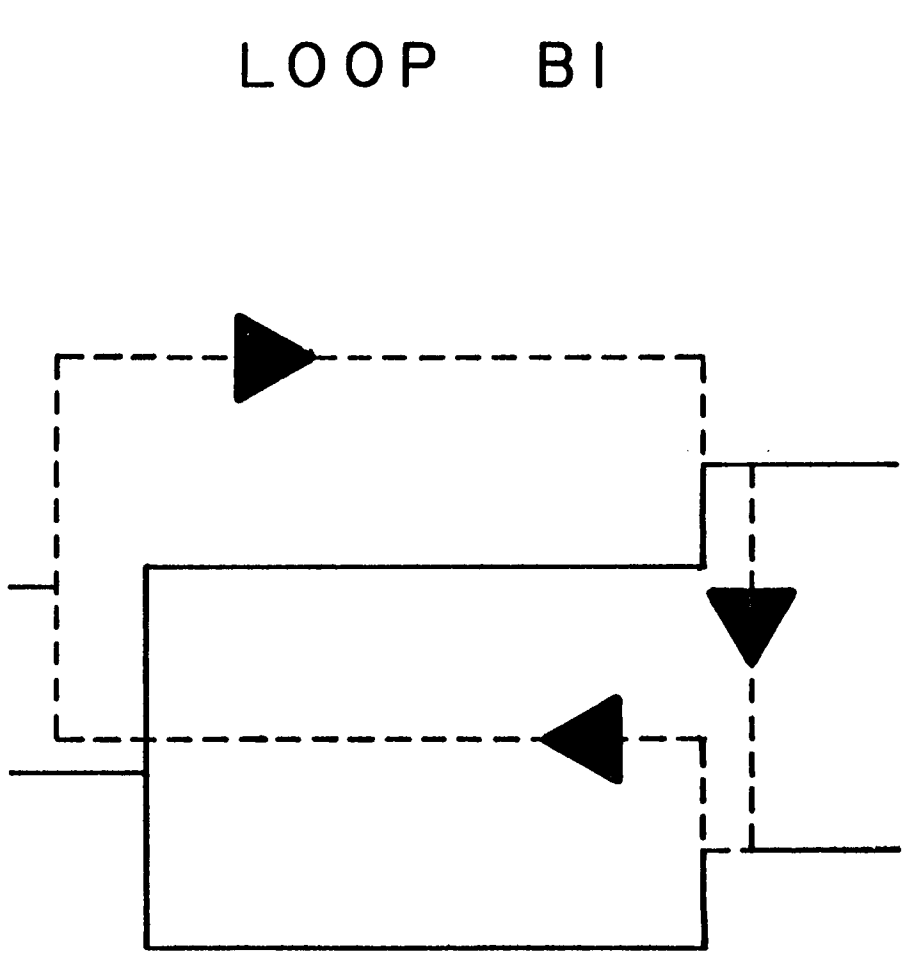


Figure A.4. Schematic Showing the Direction of Flow in Loop B1.

LOOP A2

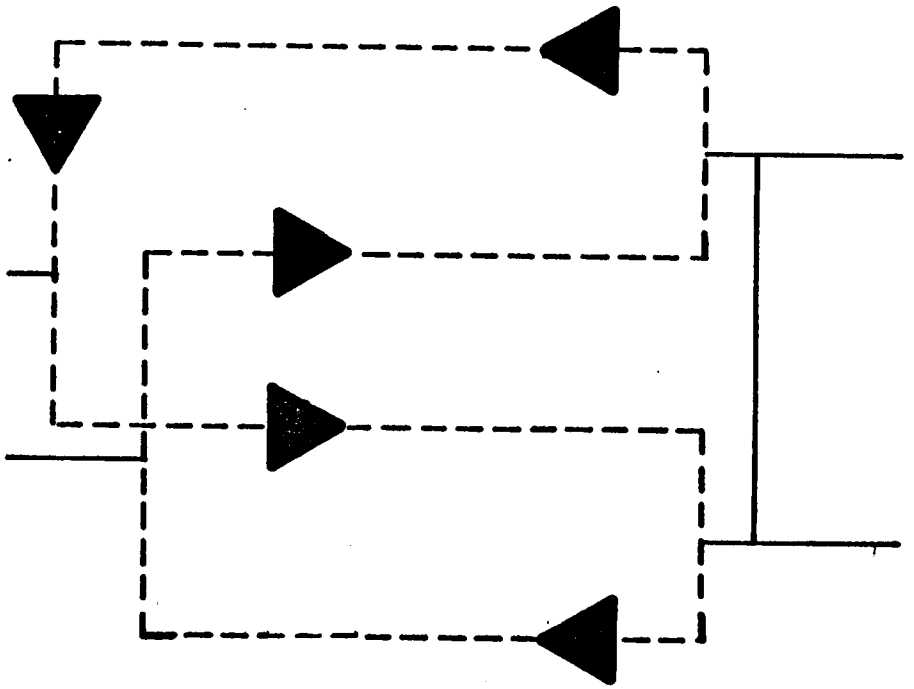


Figure A.5. Schematic Showing the Direction of Flow in Loop A2.

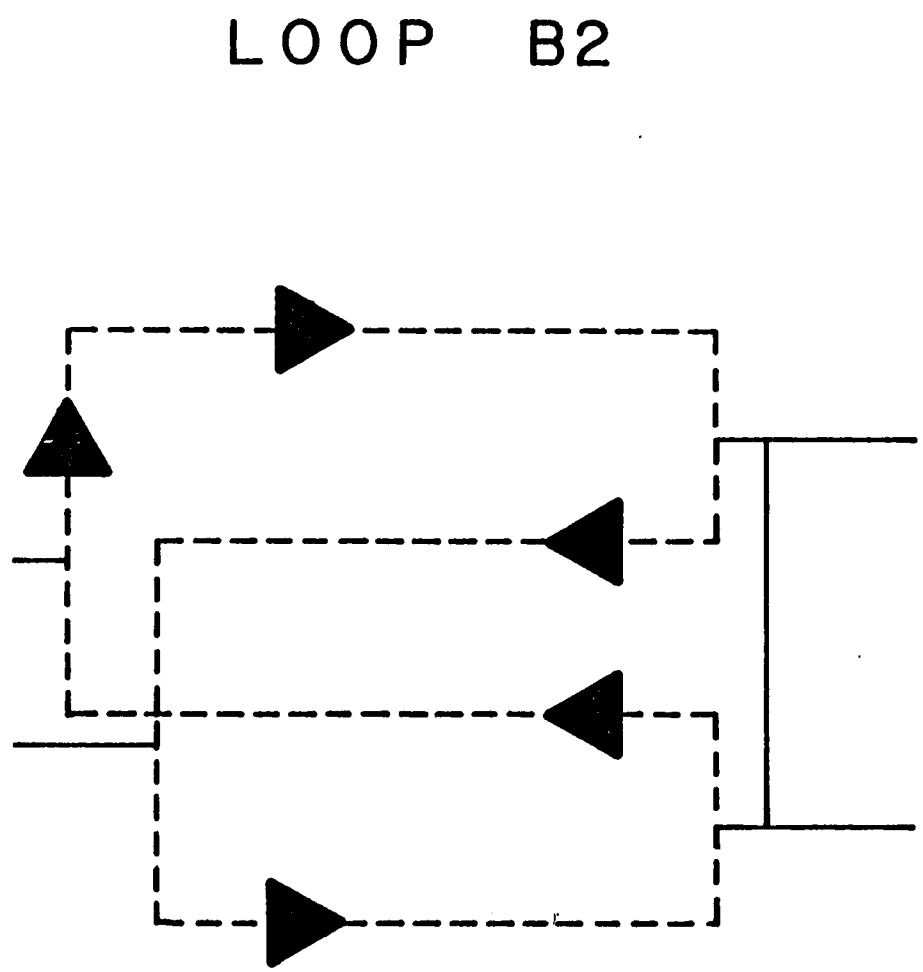


Figure A.6. Schematic Showing the Direction of Flow in Loop B2.

LOOP A3

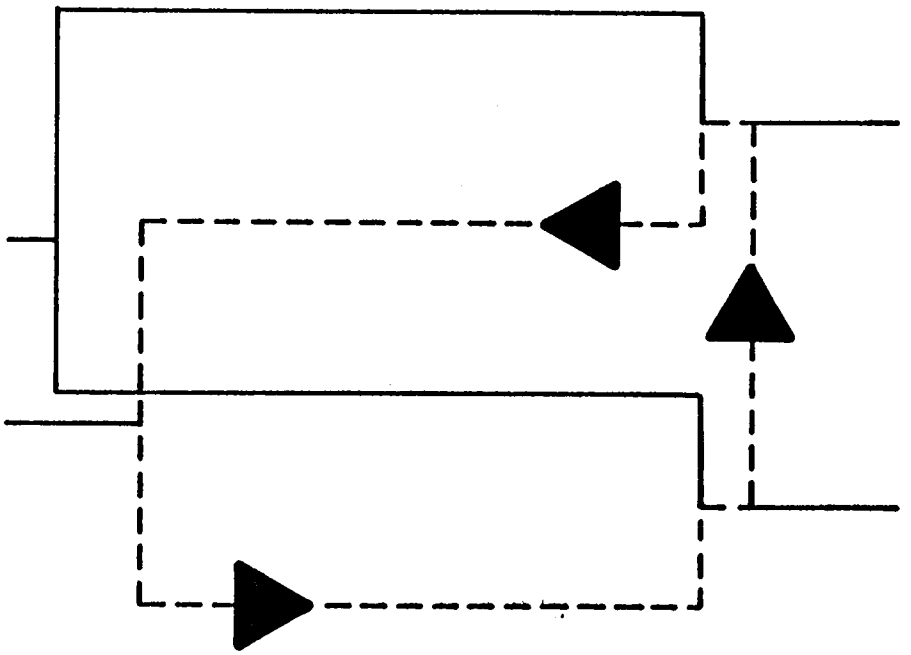


Figure A.7. Schematic Showing the Direction of Flow in Loop A3.

LOOP B3

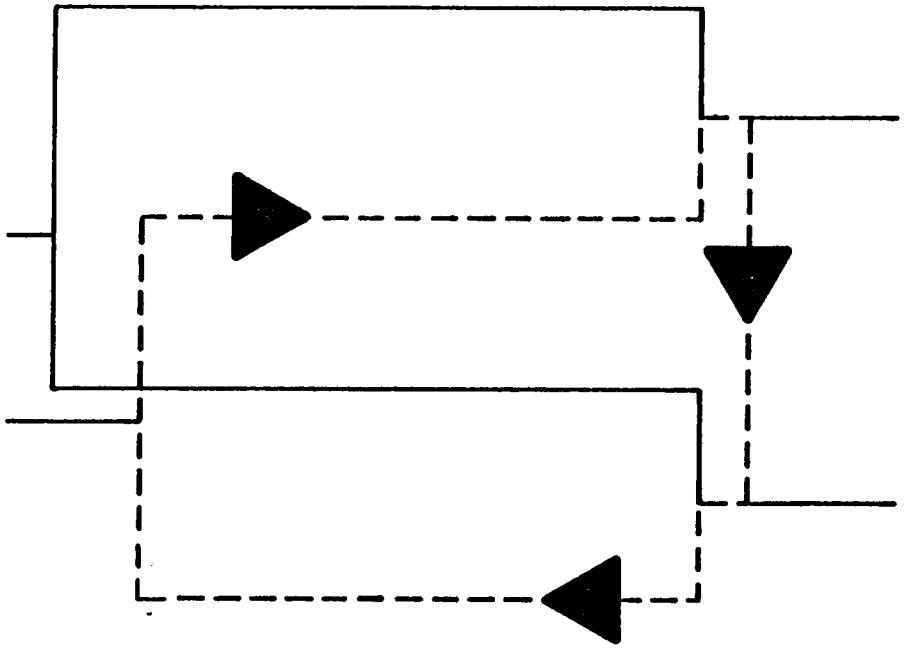


Figure A.8. Schematic Showing the Direction of Flow in Loop B3.

TABLE A.2

ABBREVIATIONS USED IN THE FAULT TREE

Abbreviation	Description
AFS	Annulus Filtration System
ACS	Annulus Cooling System
LOC	Loss of Capability
LTA	Less than Adequate

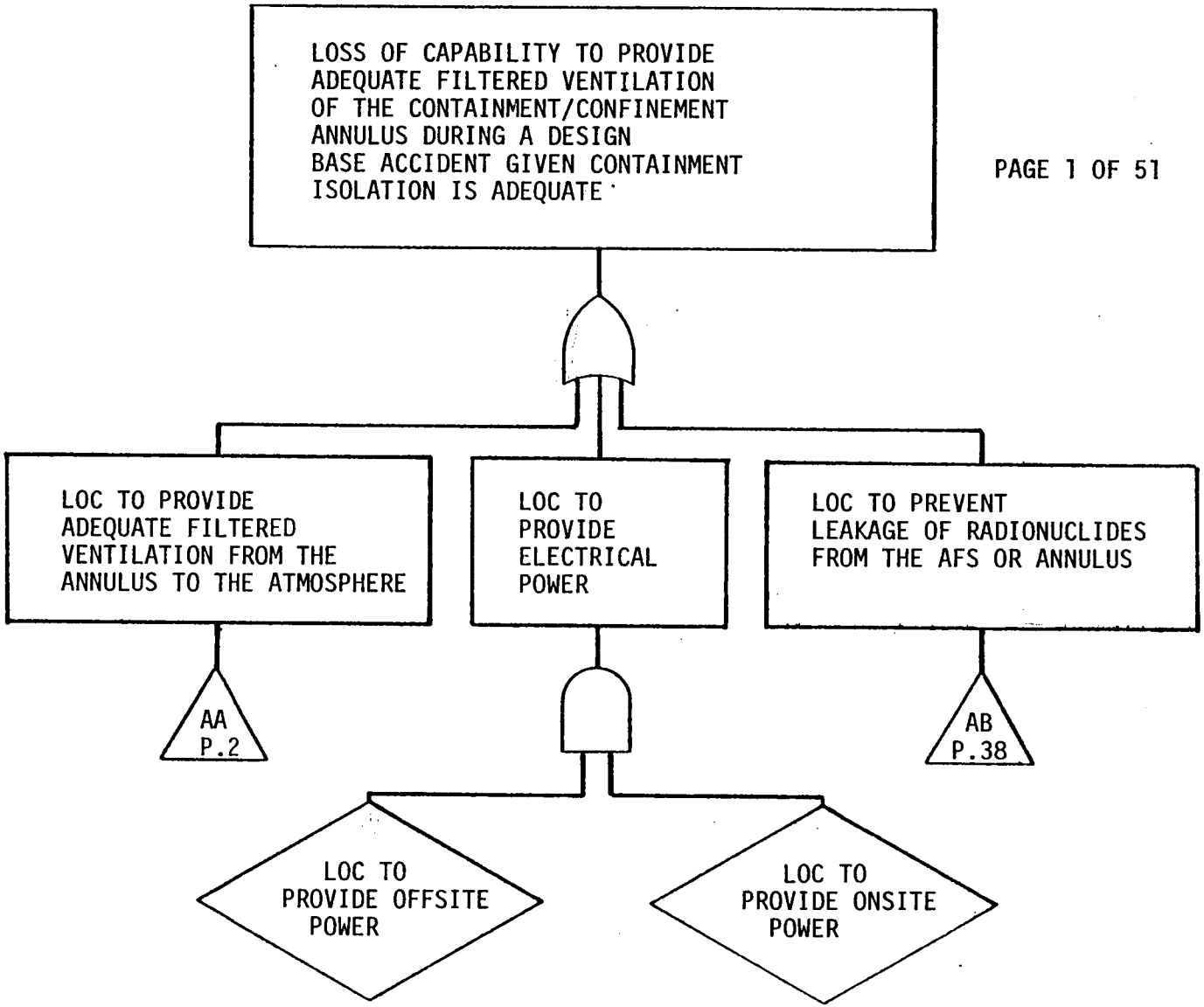
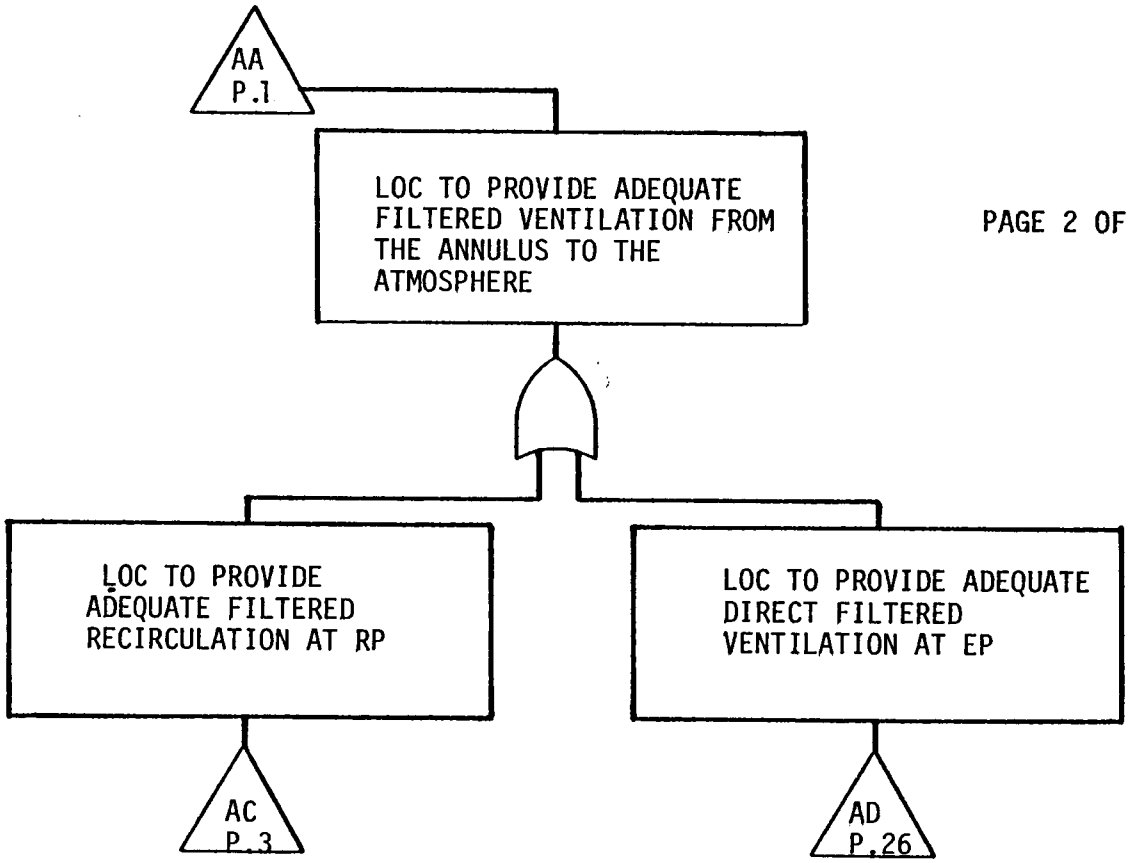


Figure A.9. CRBRP Annulus Filtration System Fault Tree



PAGE 2 OF 51

Figure A.9. (continued)

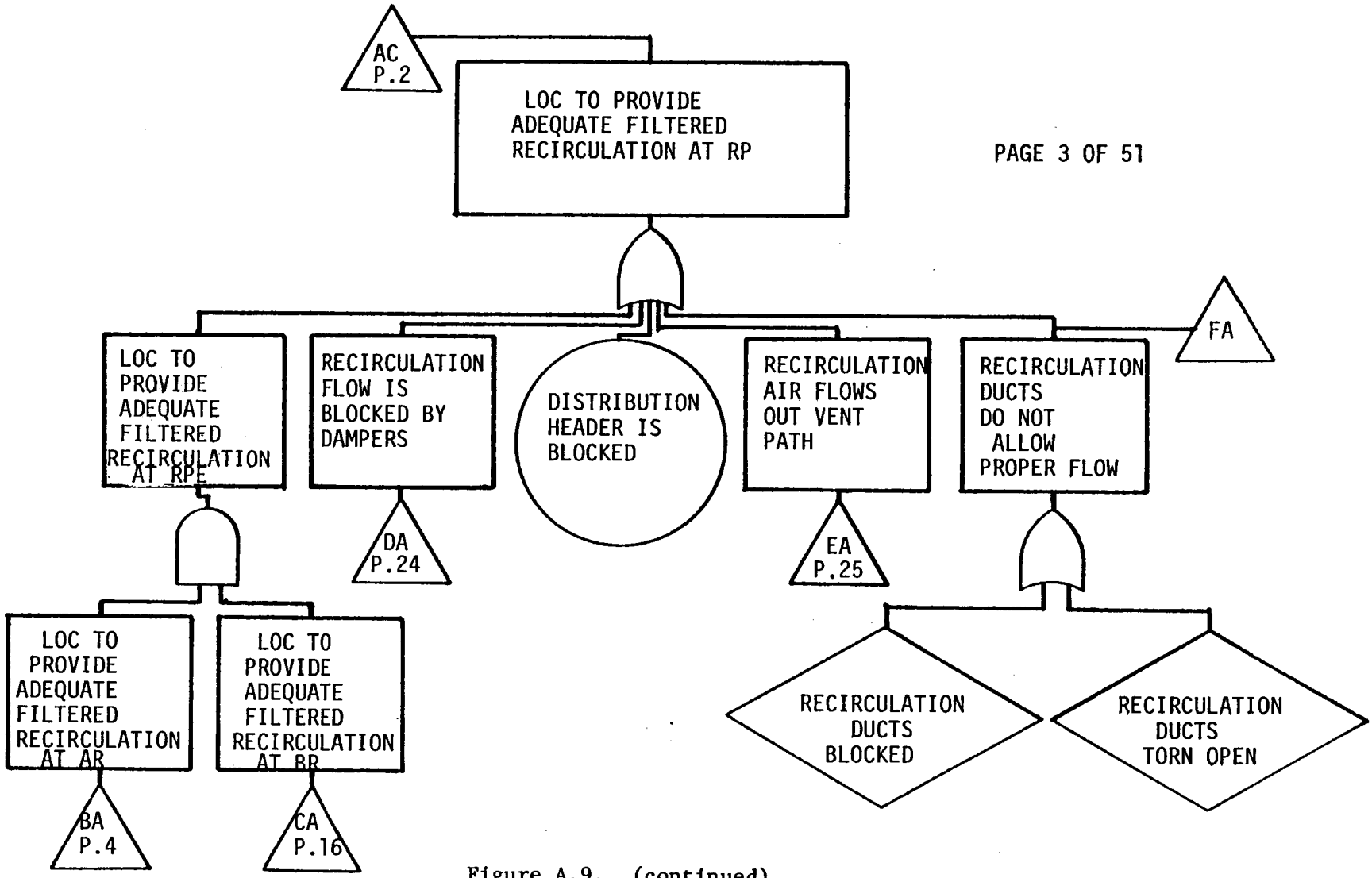


Figure A.9. (continued)

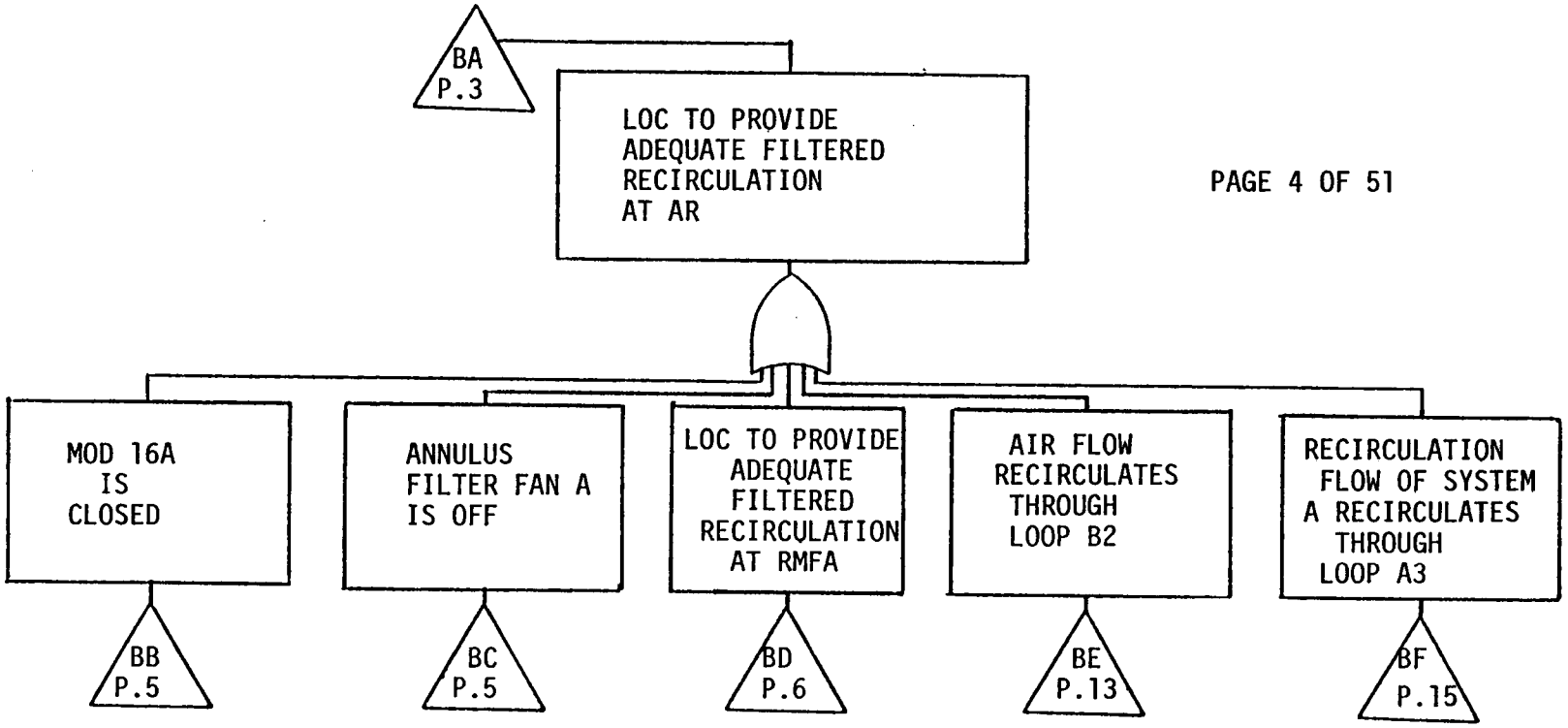
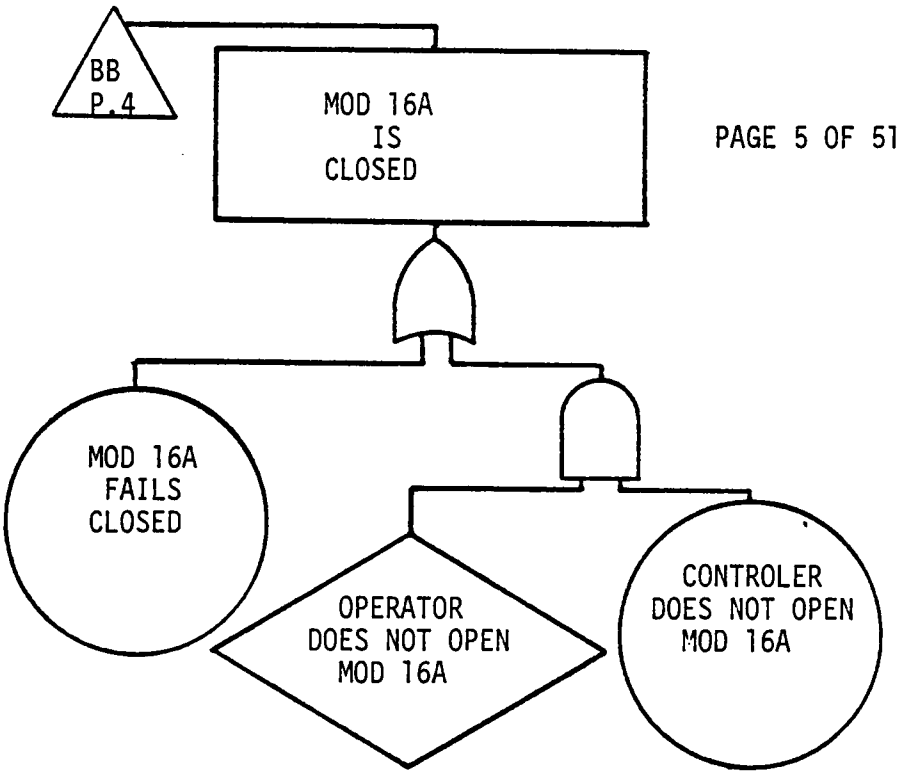


Figure A.9. (continued)



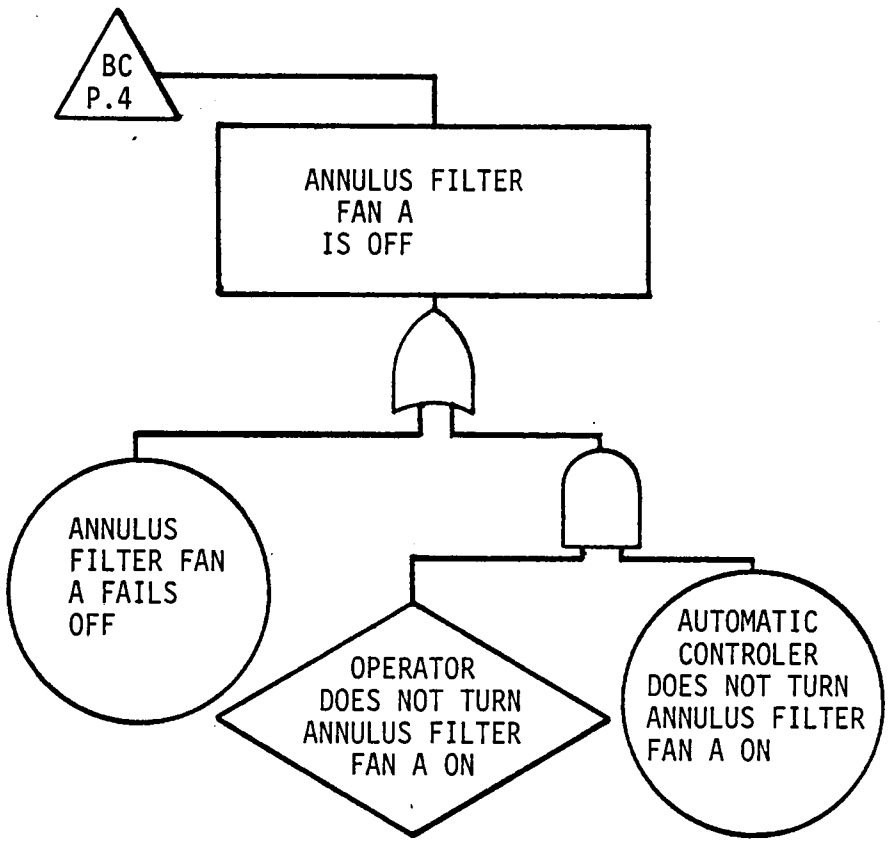


Figure A.9. (continued)

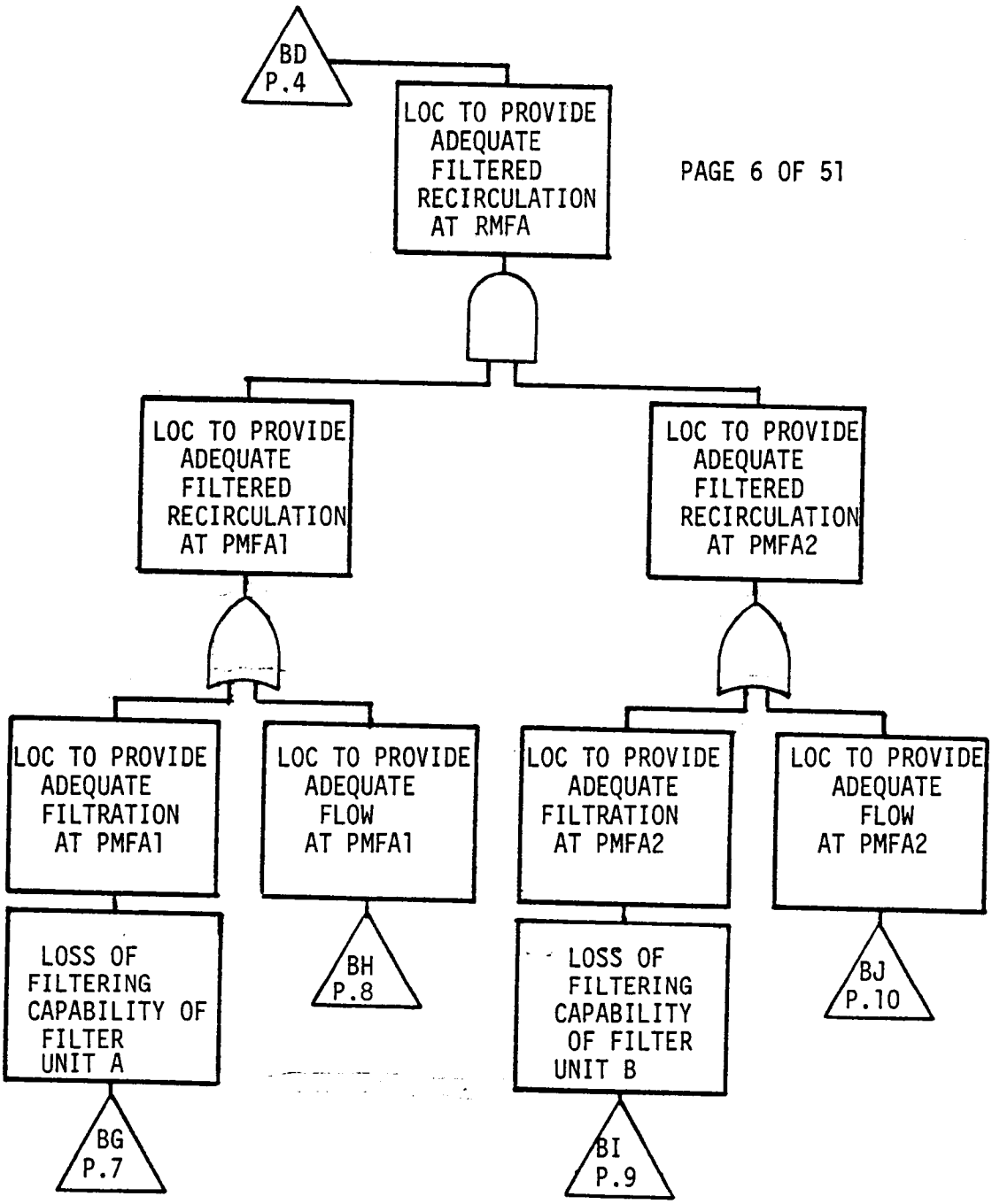


Figure A.9. (continued)

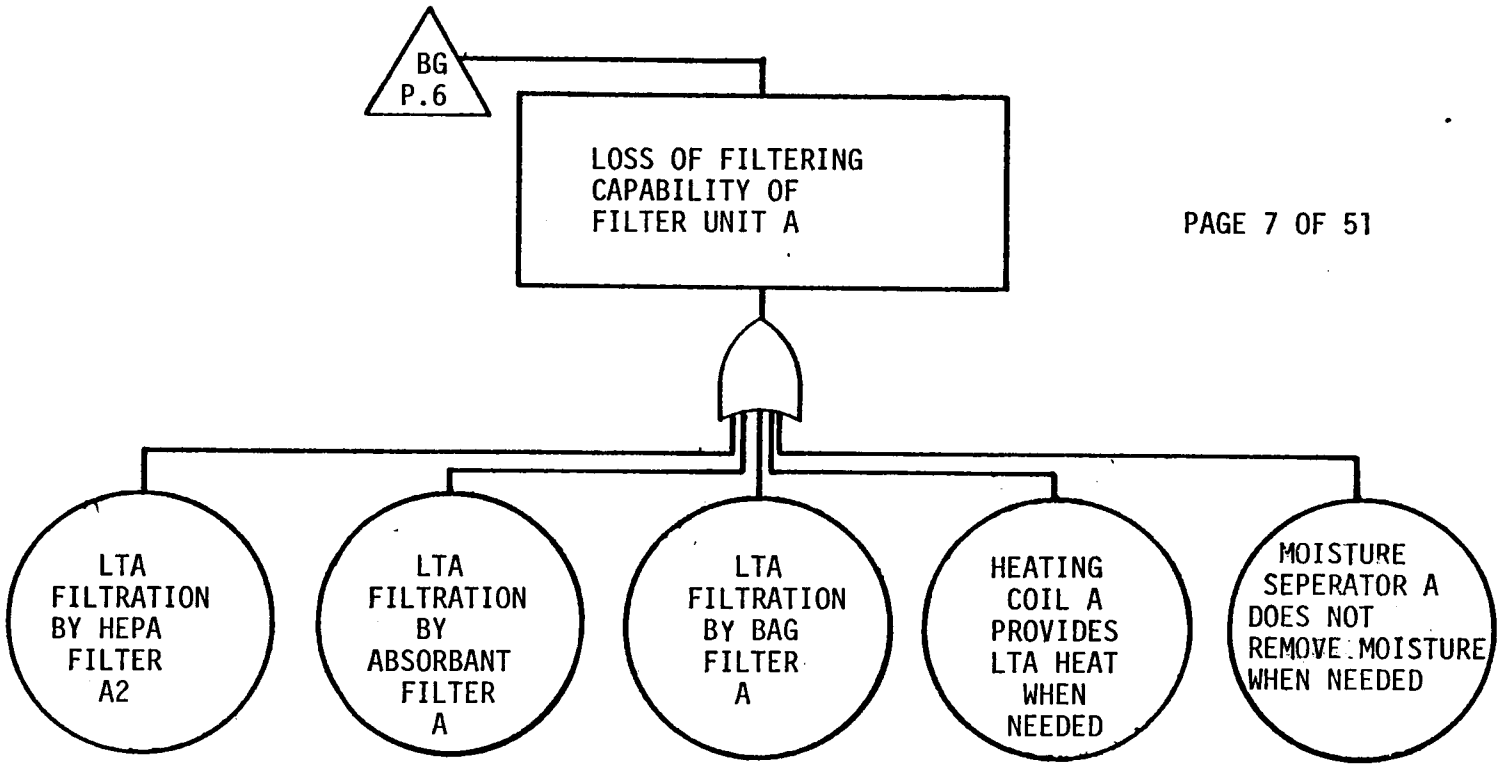


Figure A.9. (continued)

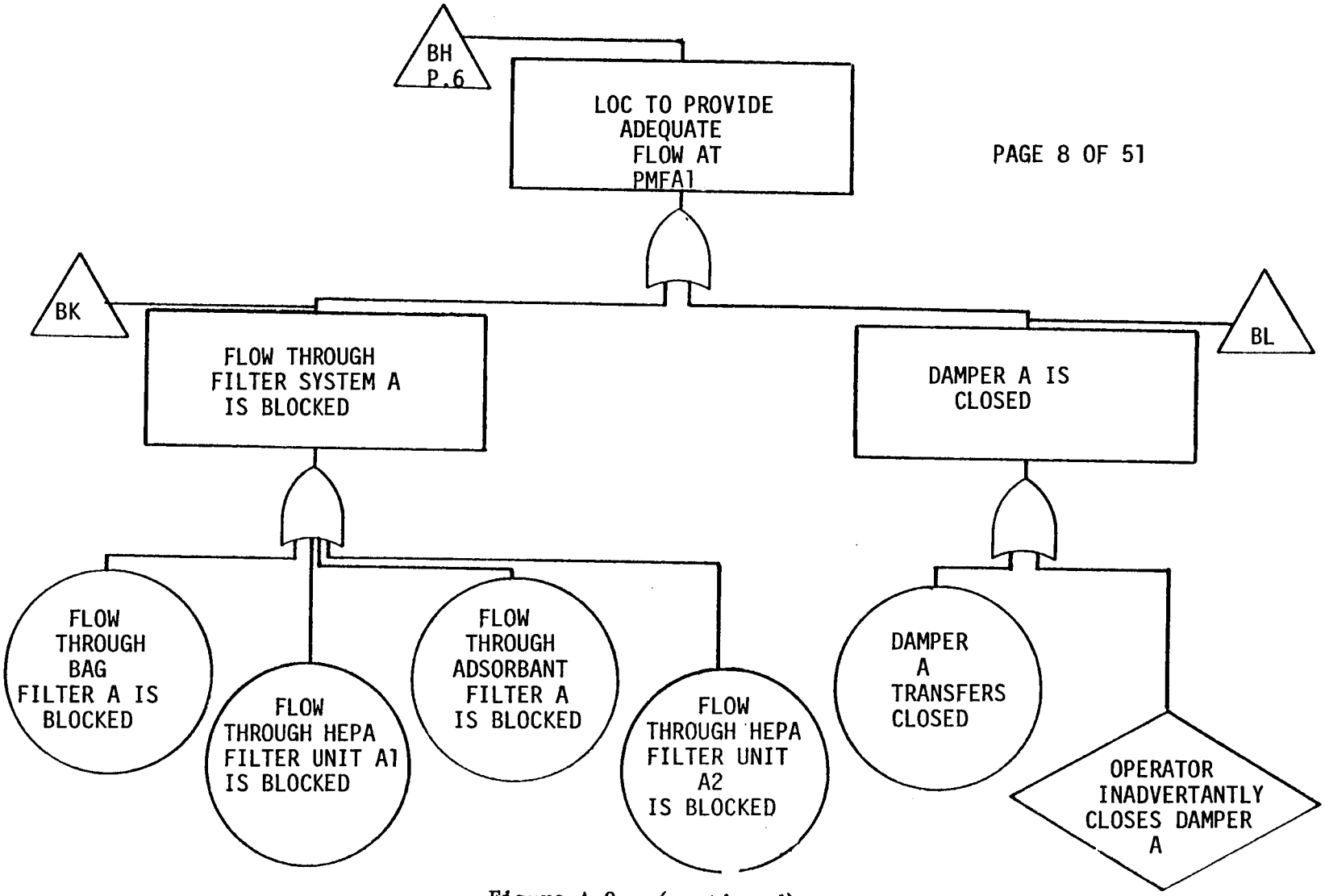


Figure A.9. (continued)

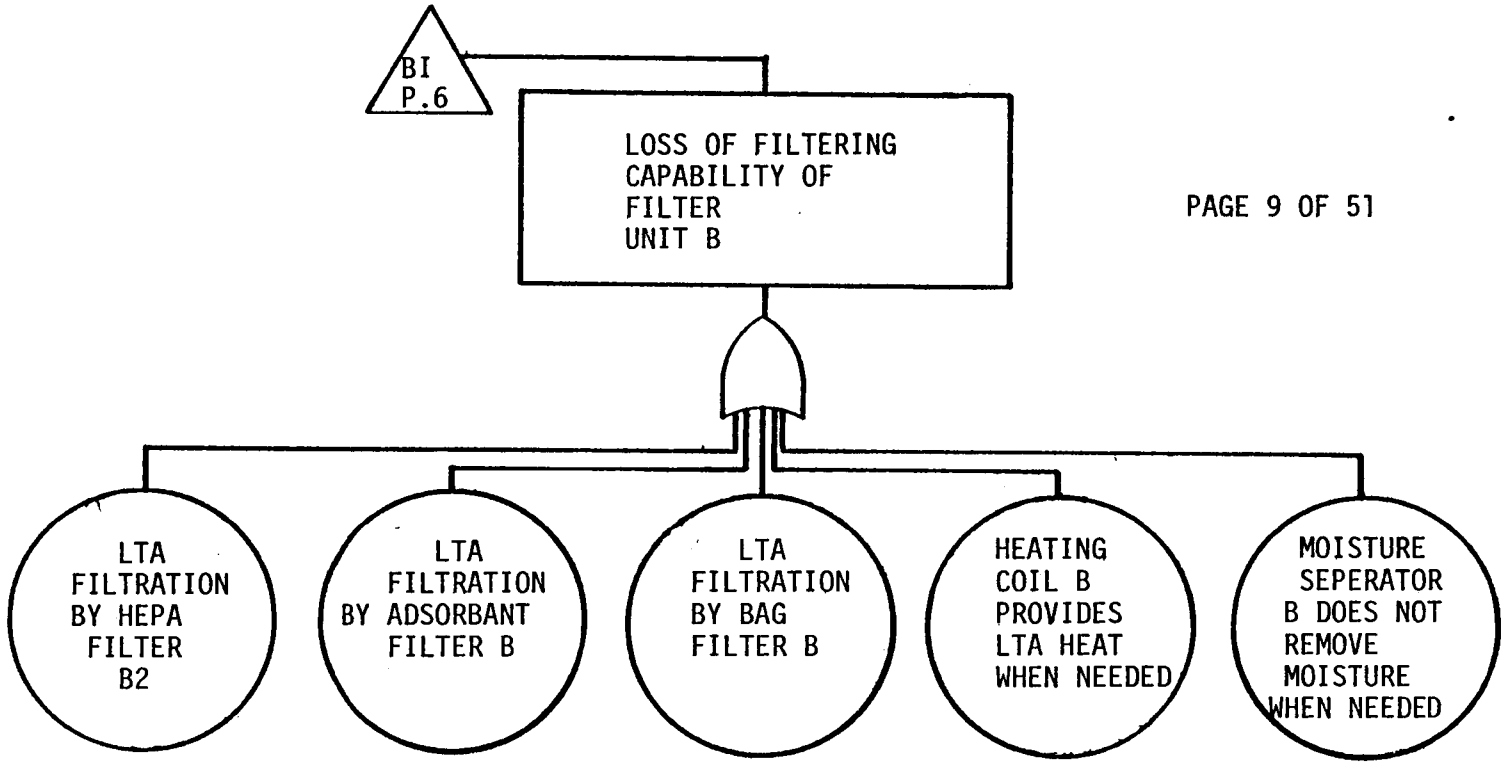


Figure A.9. (continued)

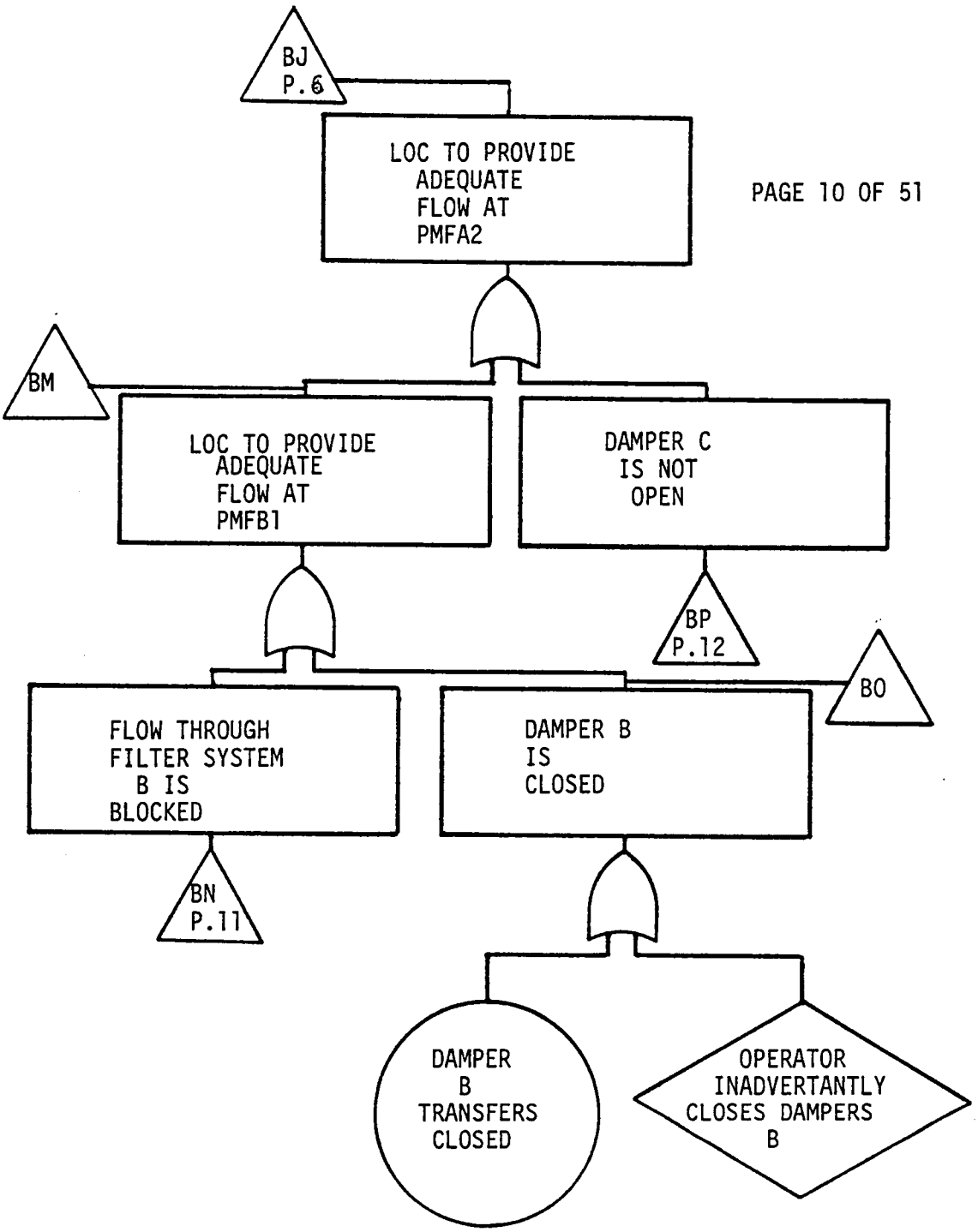


Figure A.9. (continued)

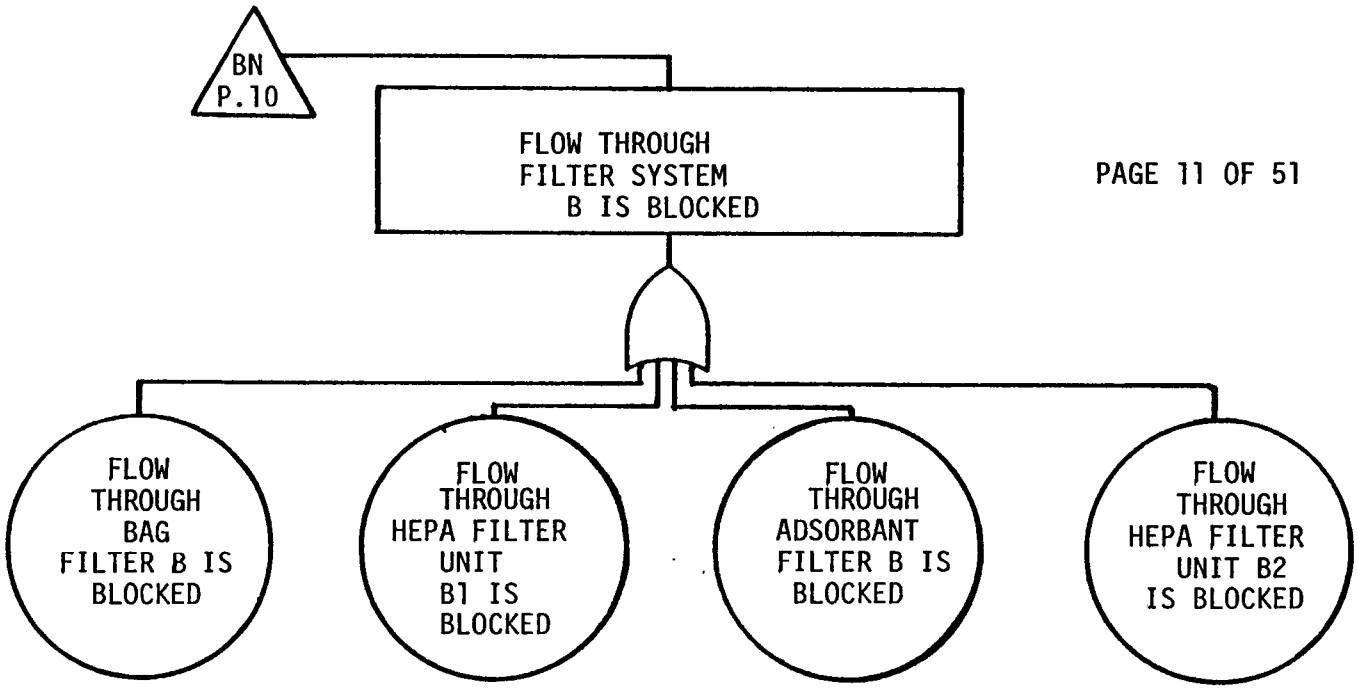


Figure A.9. (continued)

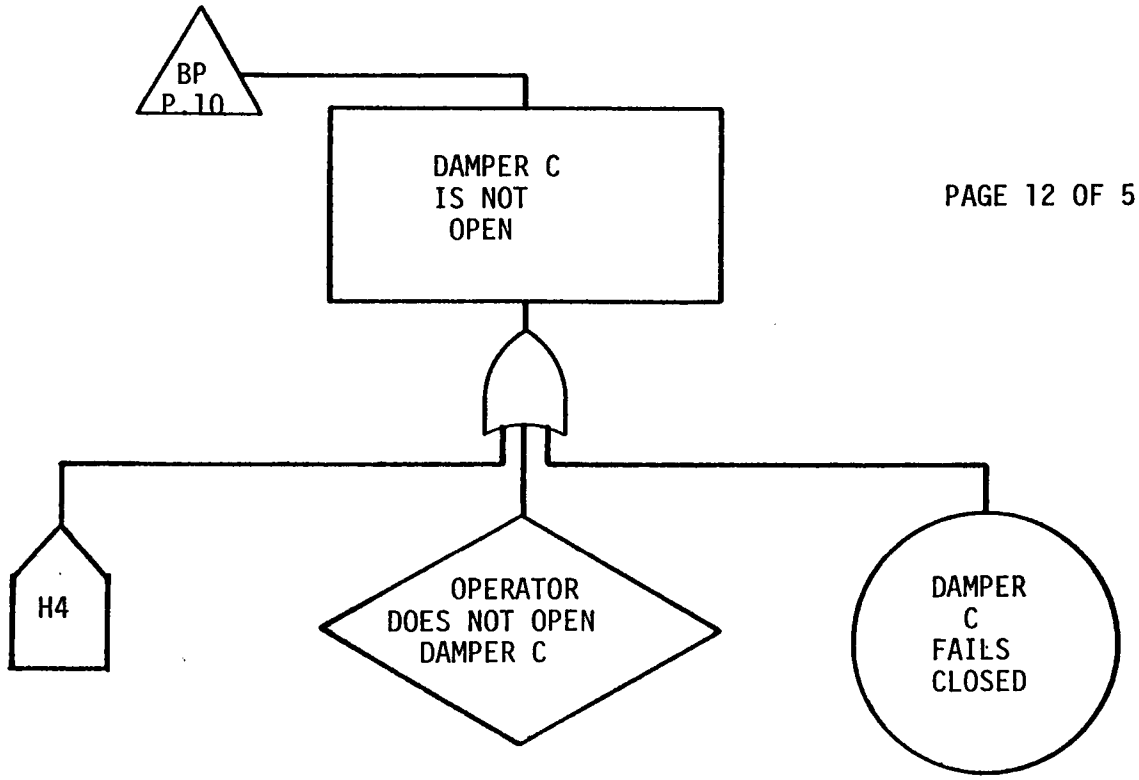


Figure A.9. (continued)

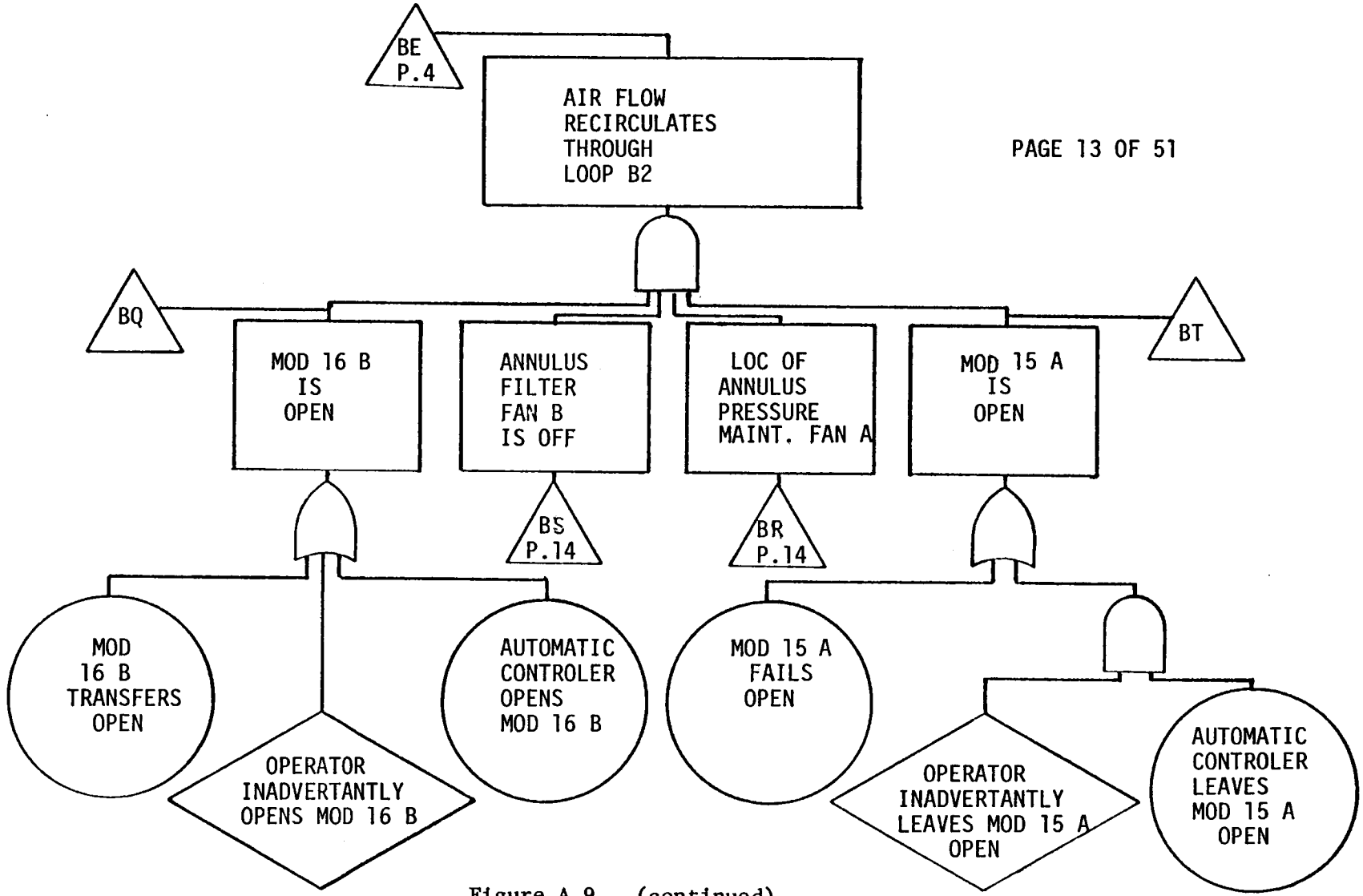


Figure A.9. (continued)

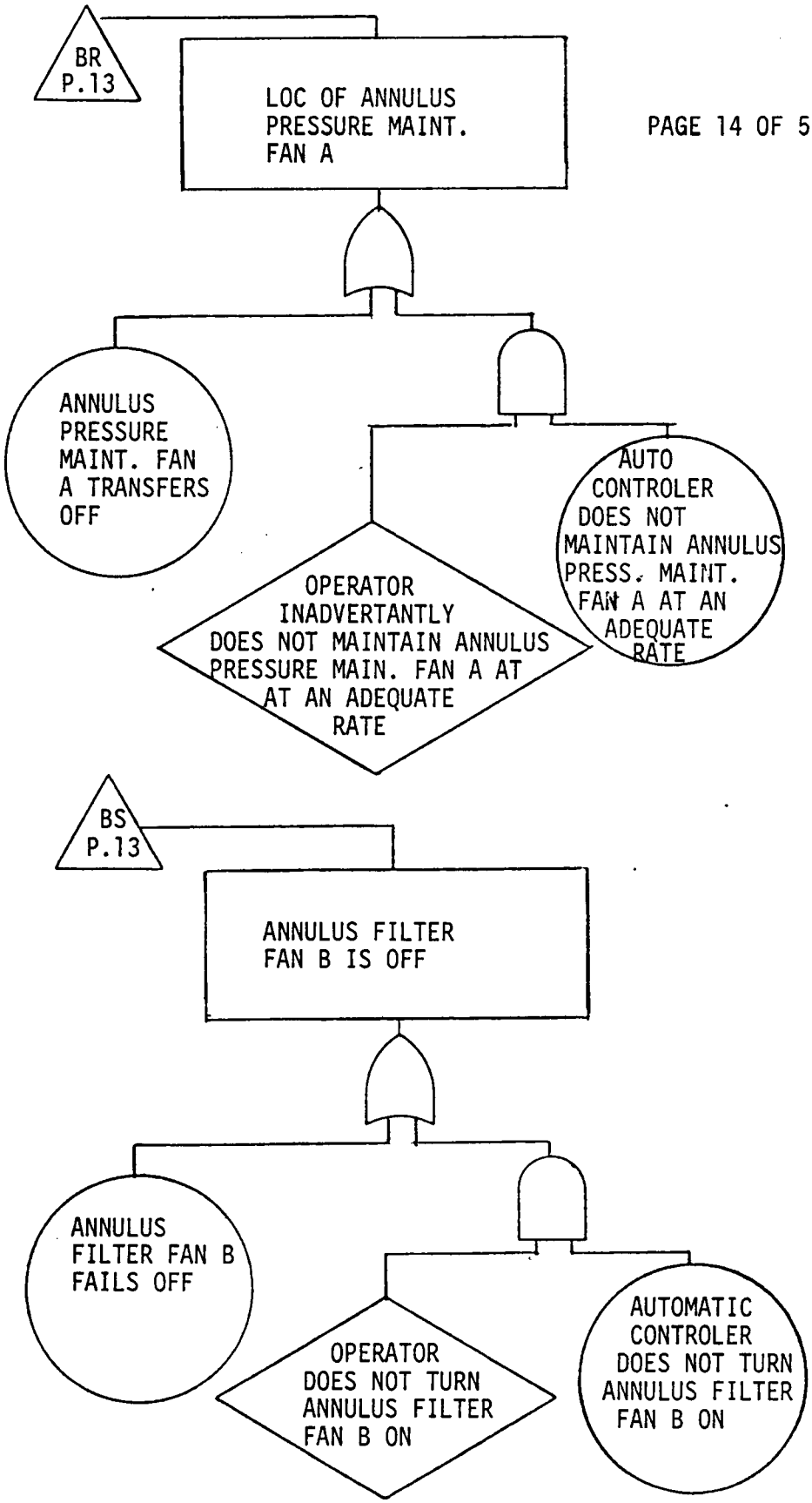


Figure A.9. (continued)

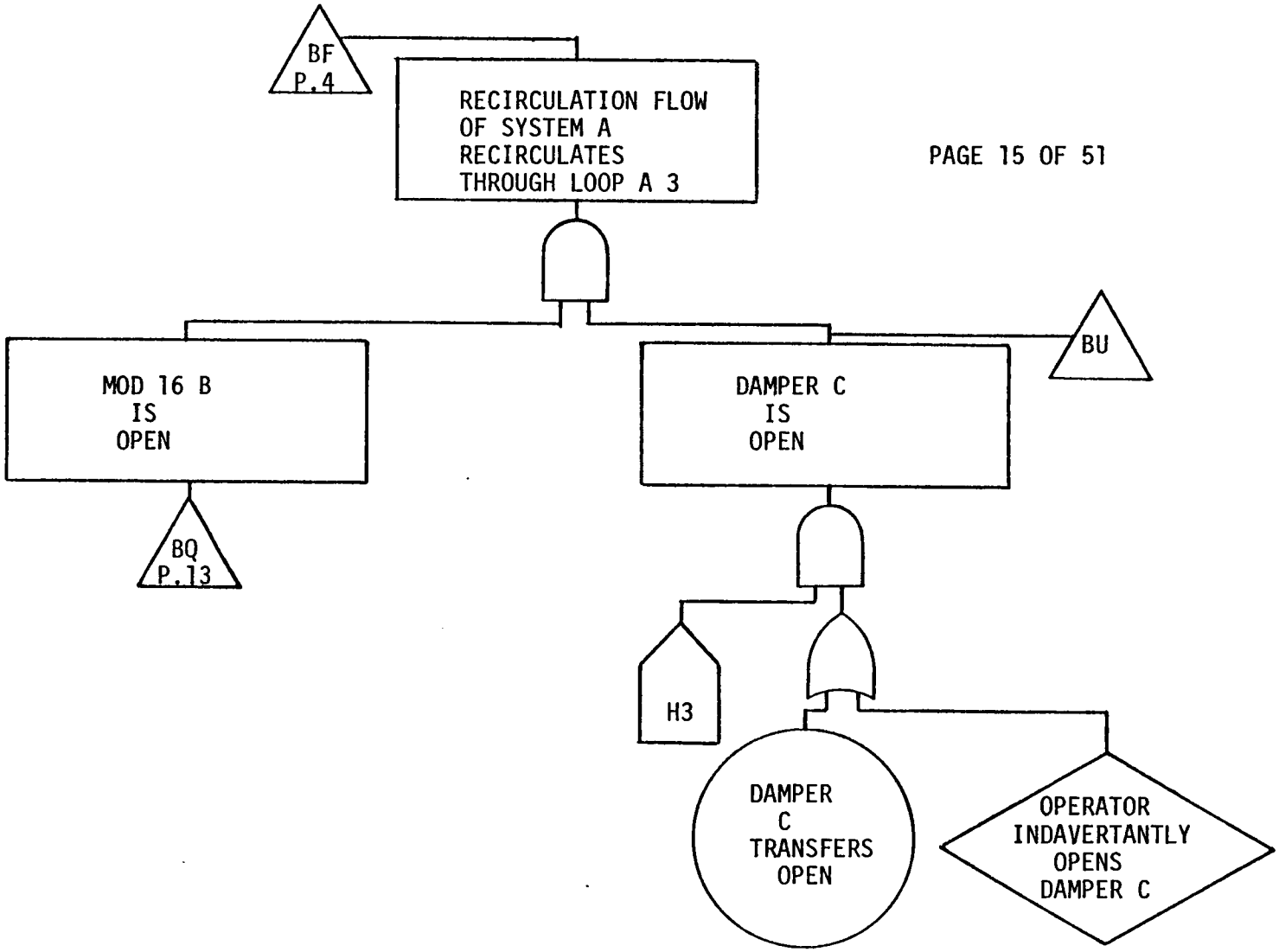


Figure A.9. (continued)

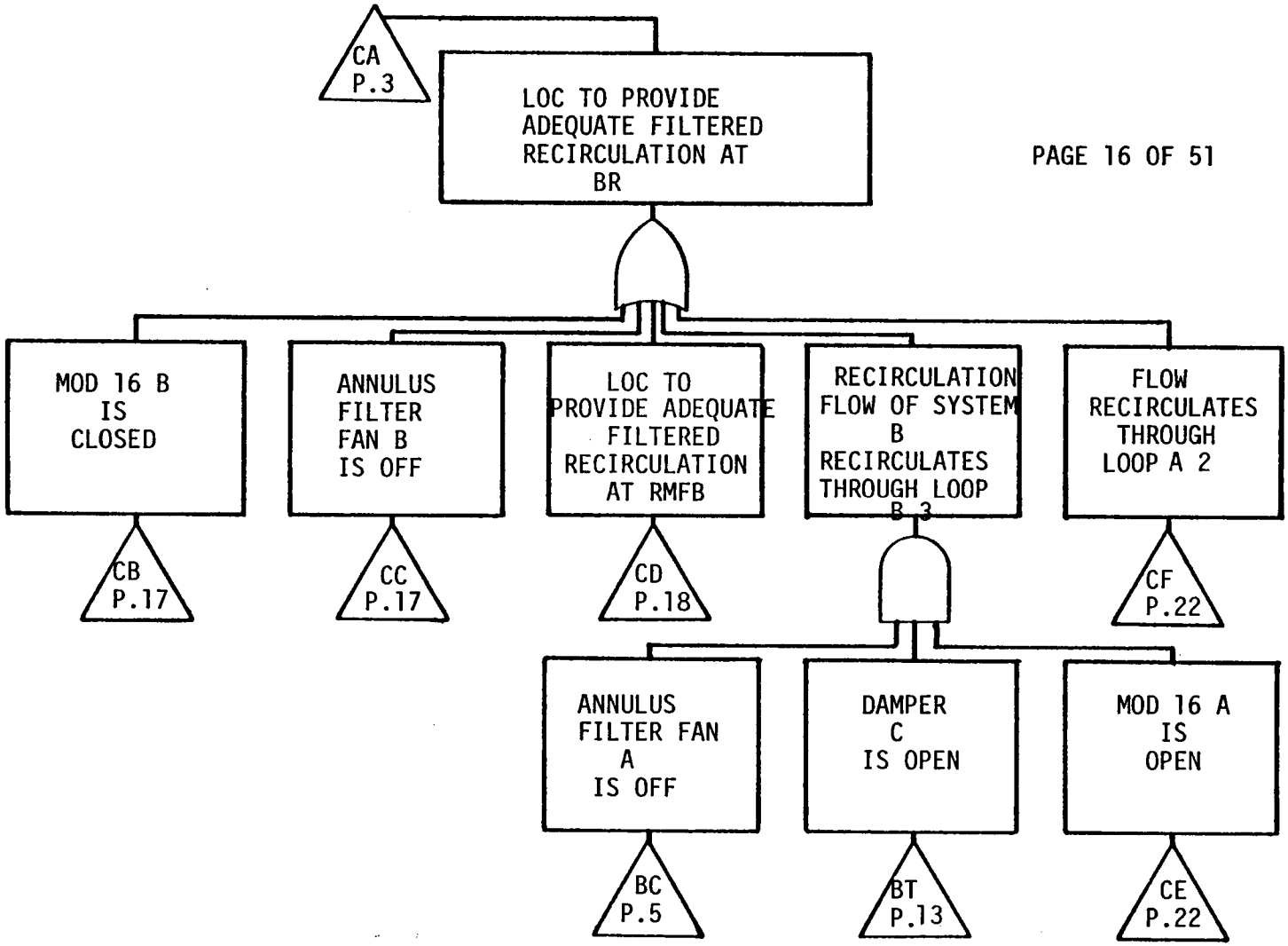


Figure A.9. (continued)

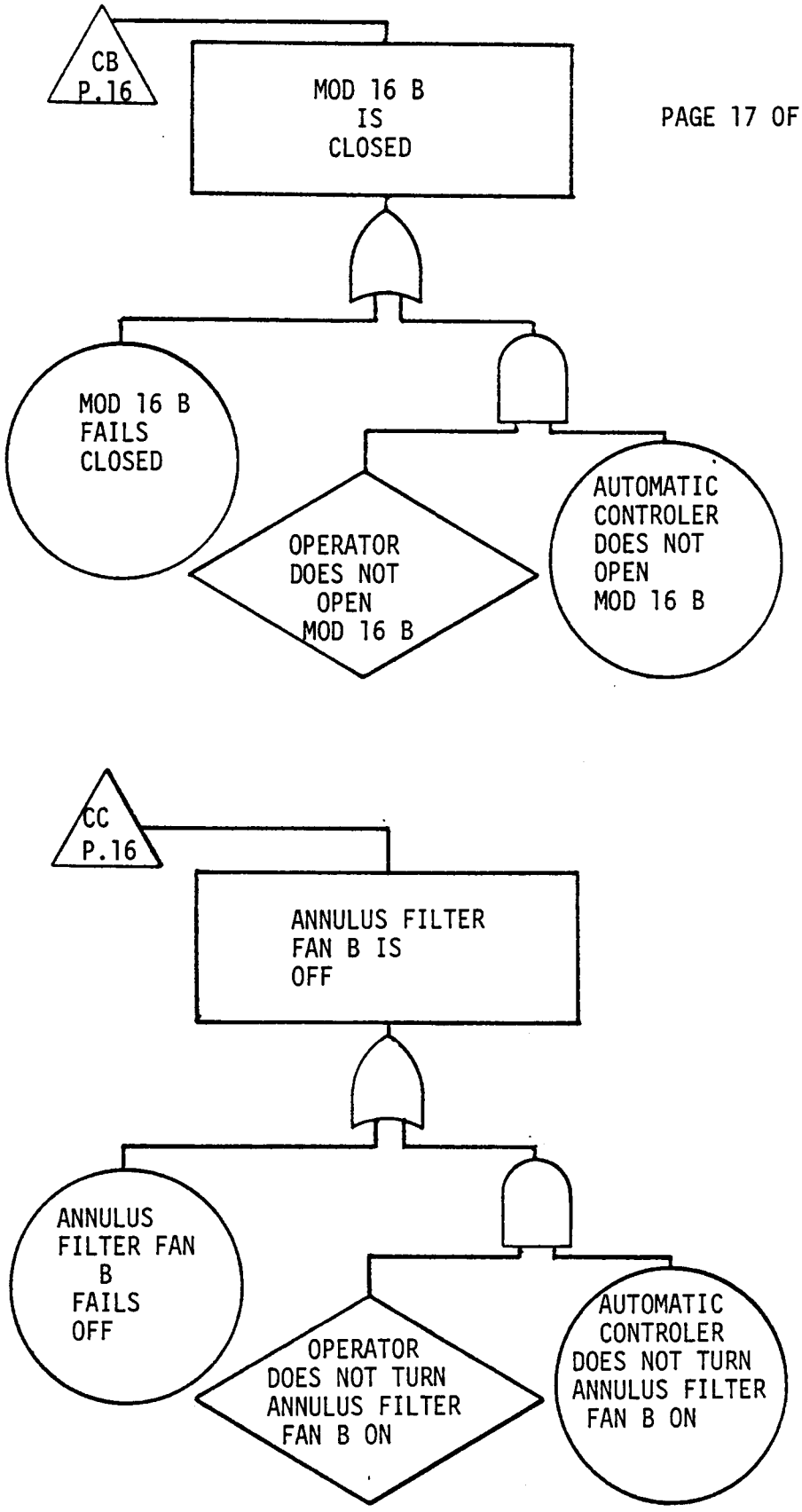


Figure A.9. (continued)

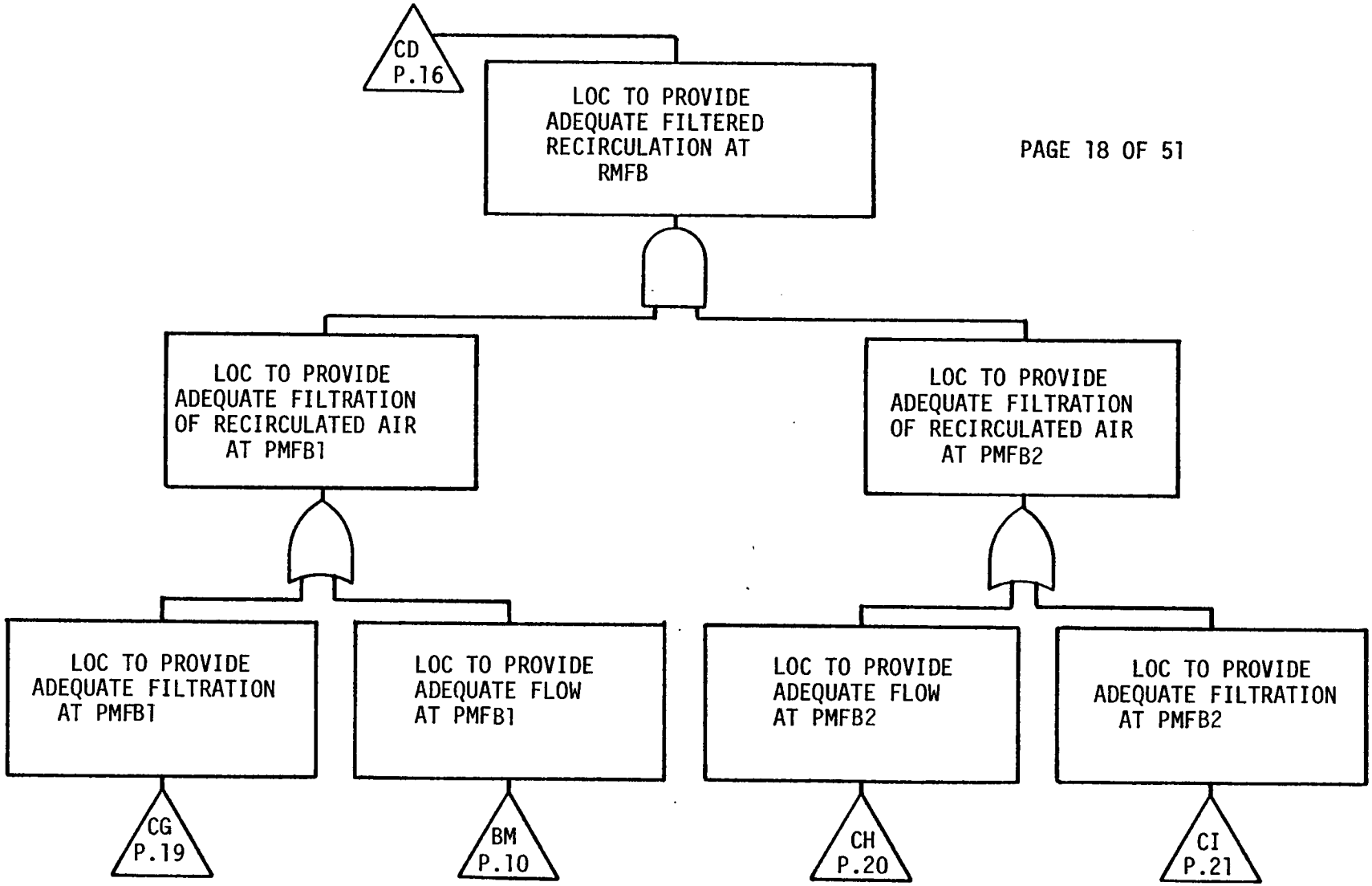


Figure A.9. (continued)

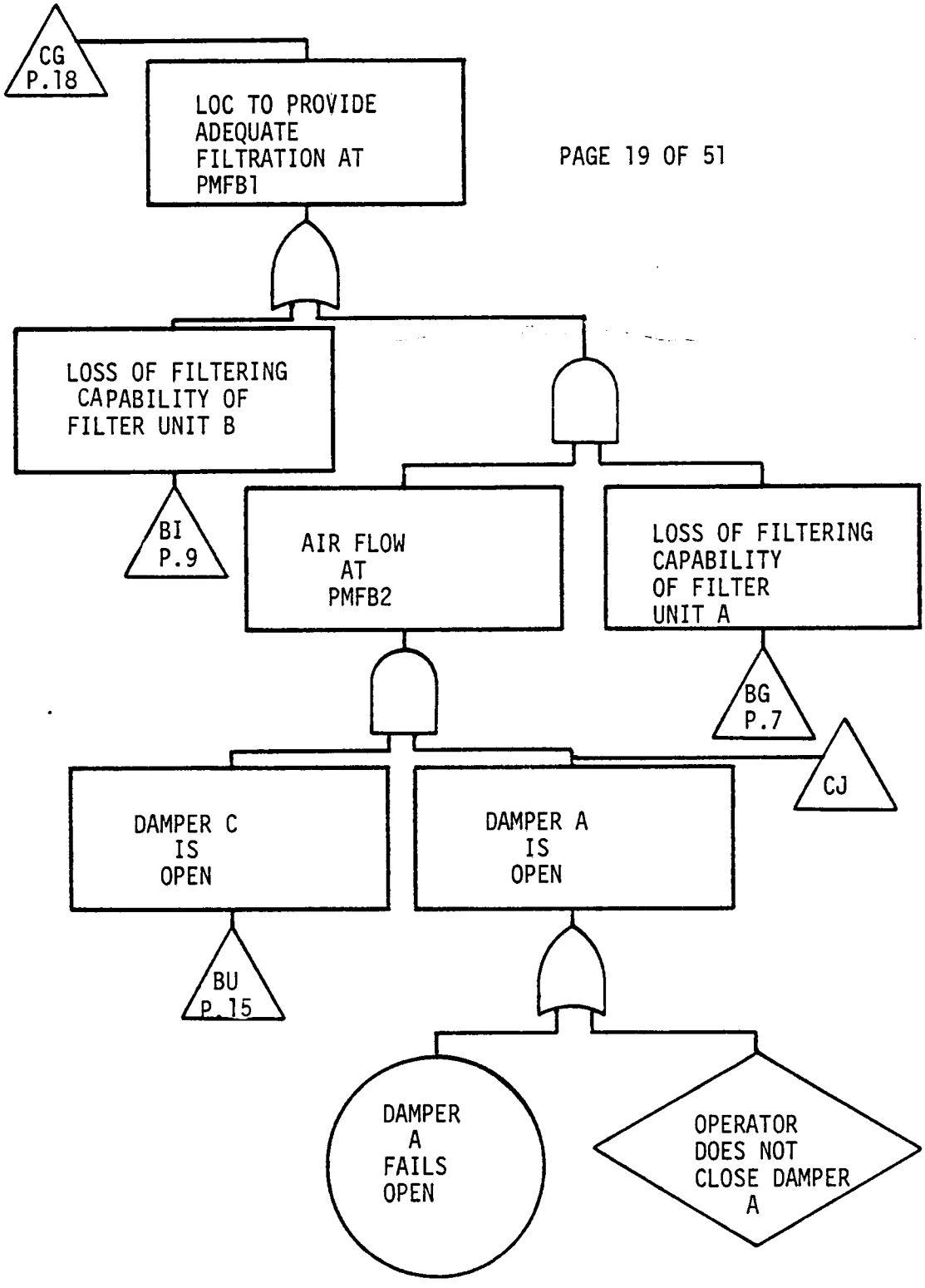


Figure A.9. (continued)

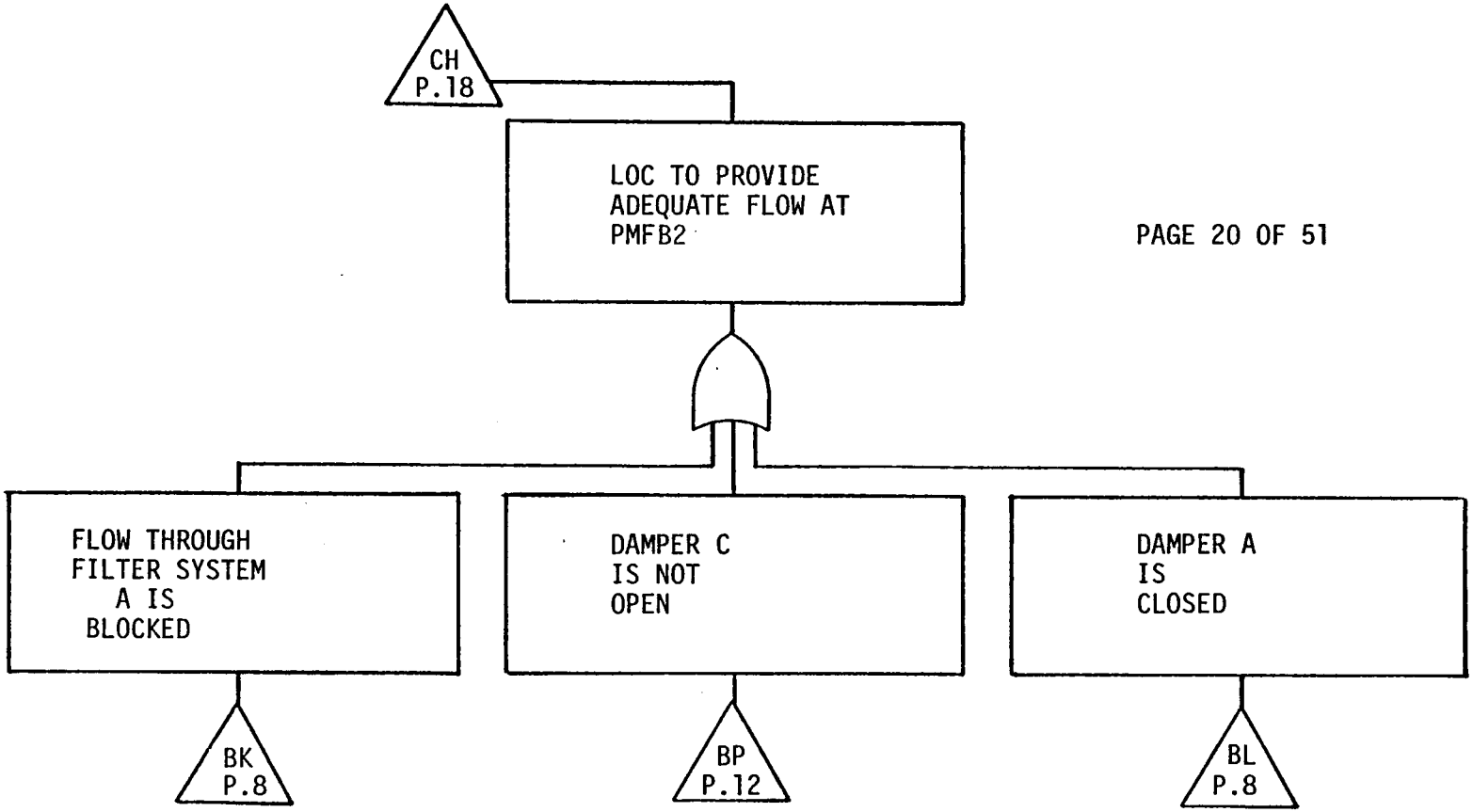


Figure A.9. (continued)

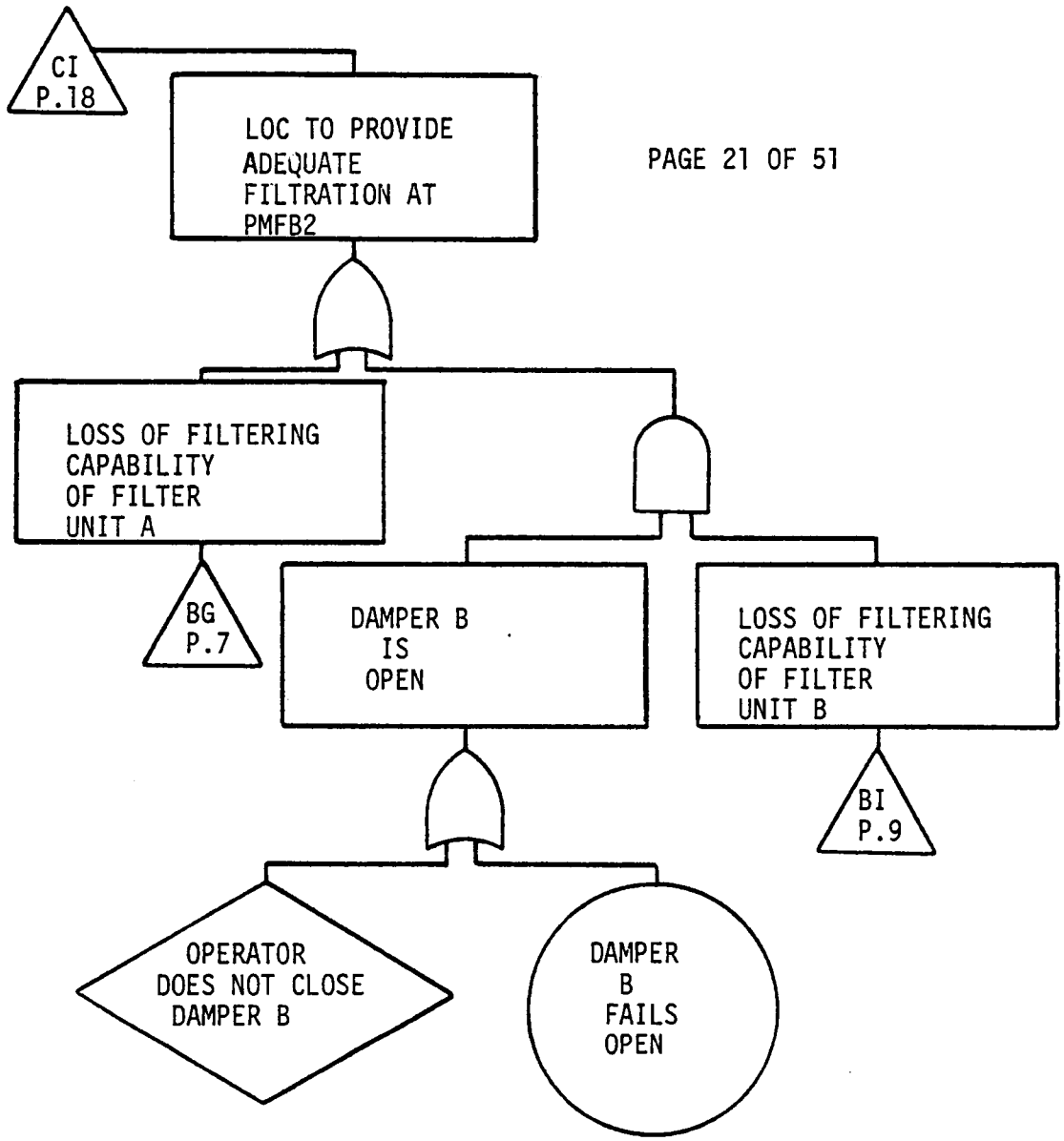


Figure A.9. (continued)

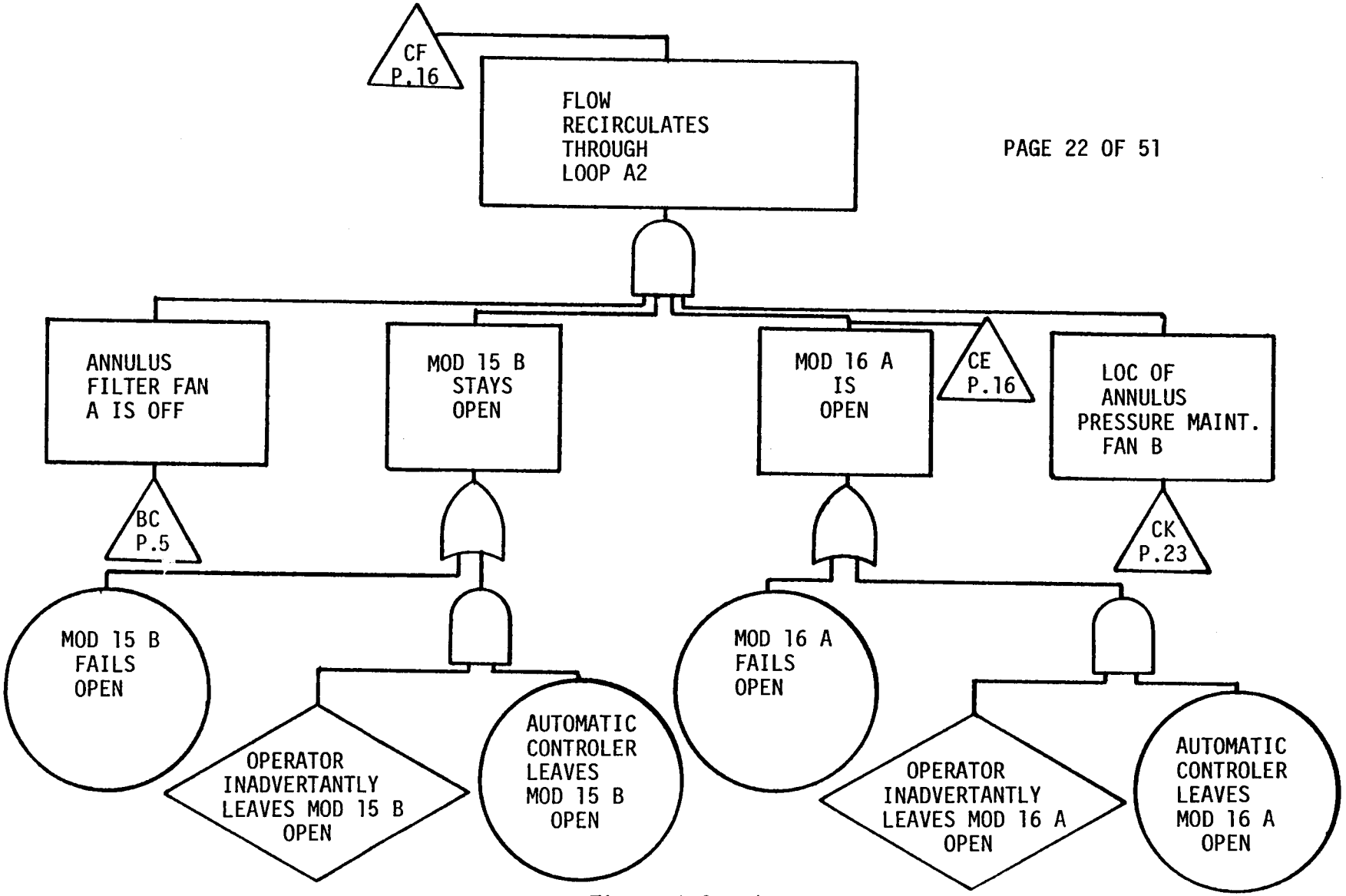


Figure A.9. (continued)

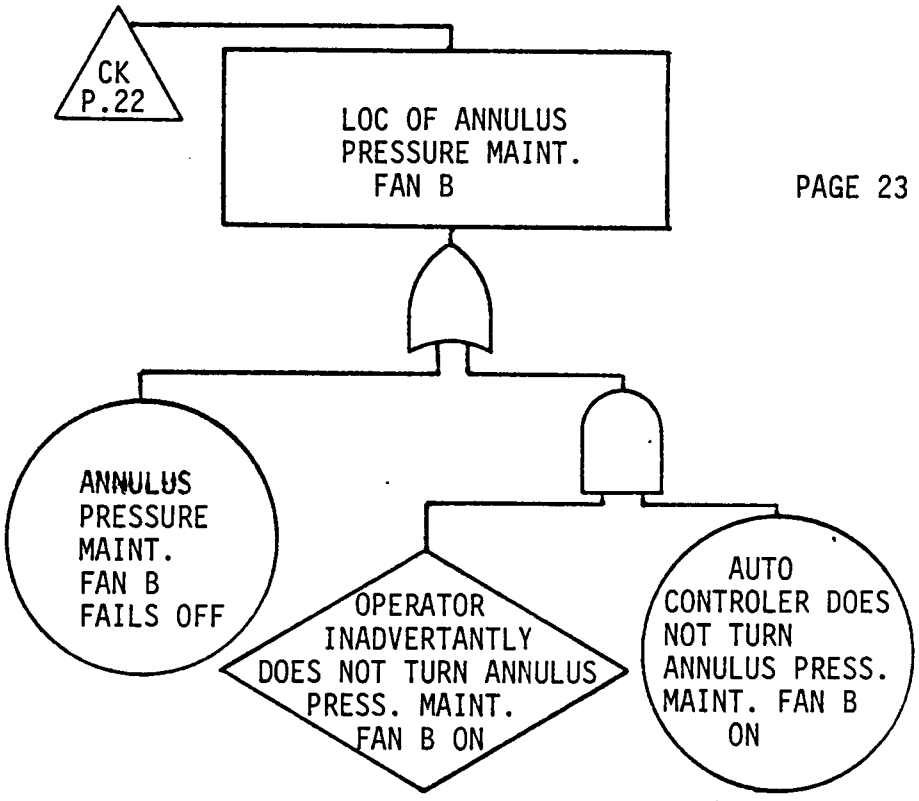


Figure A.9. (continued)

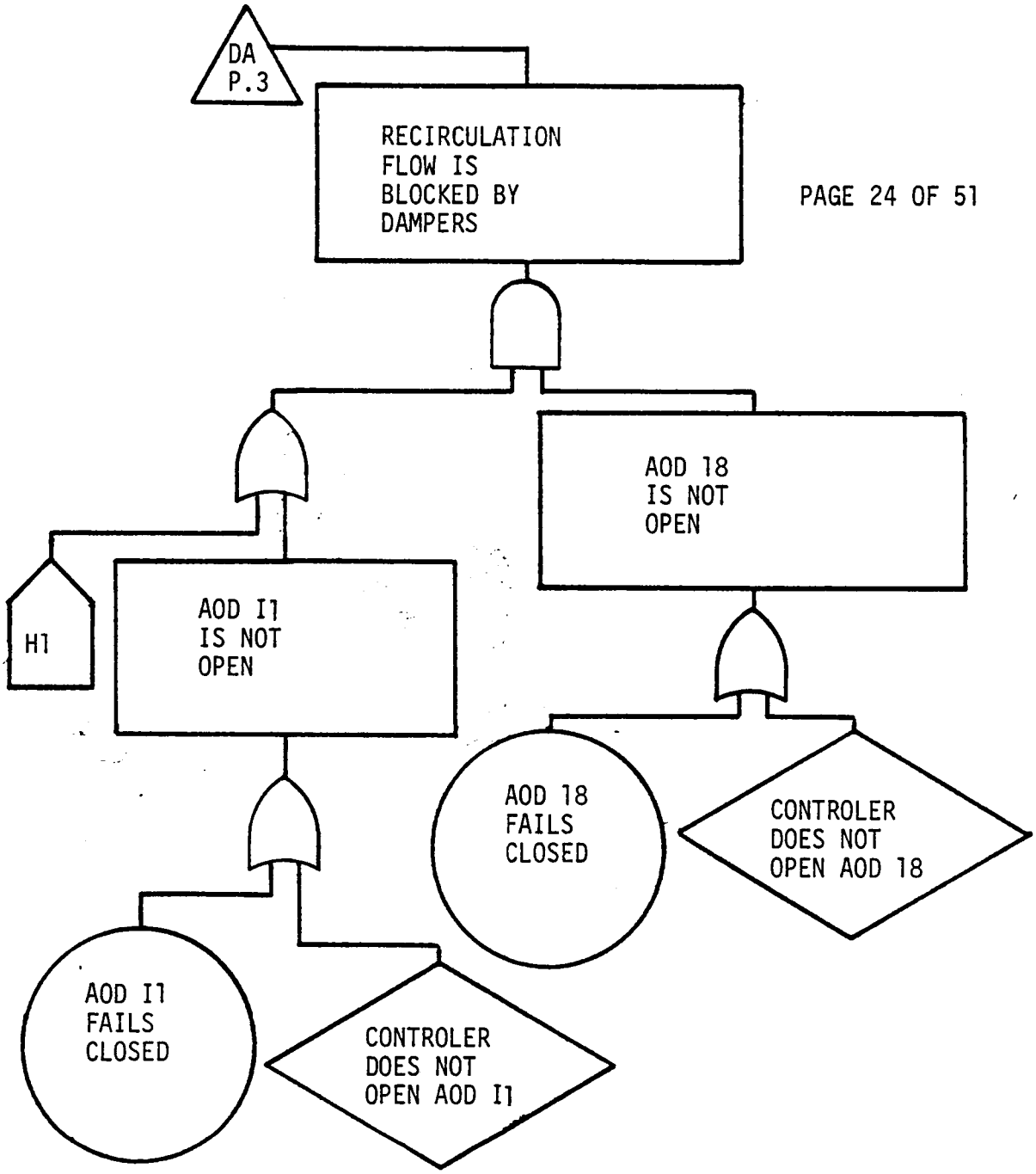


Figure A.9. (continued)

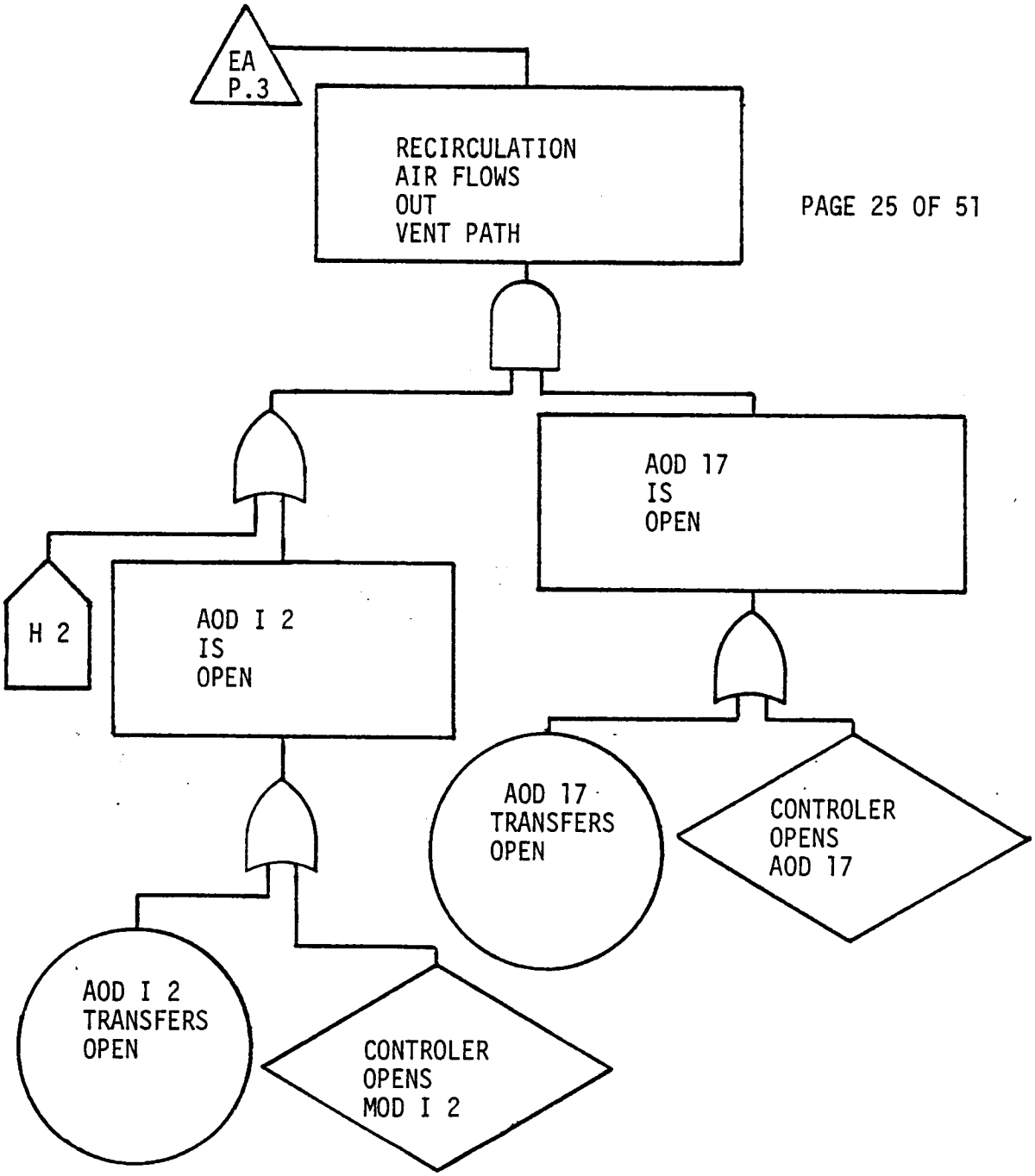


Figure A.9. (continued)

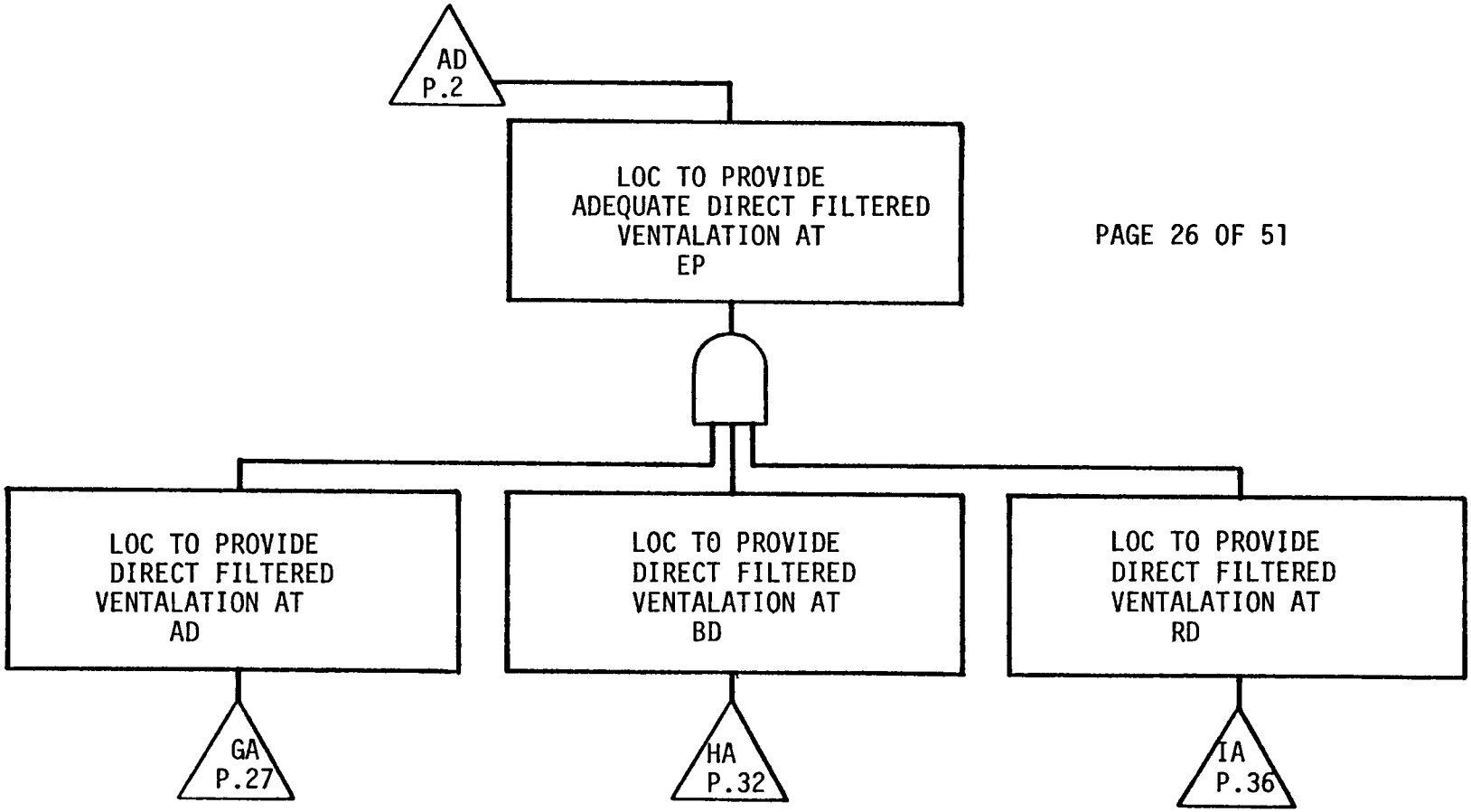


Figure A.9. (continued)

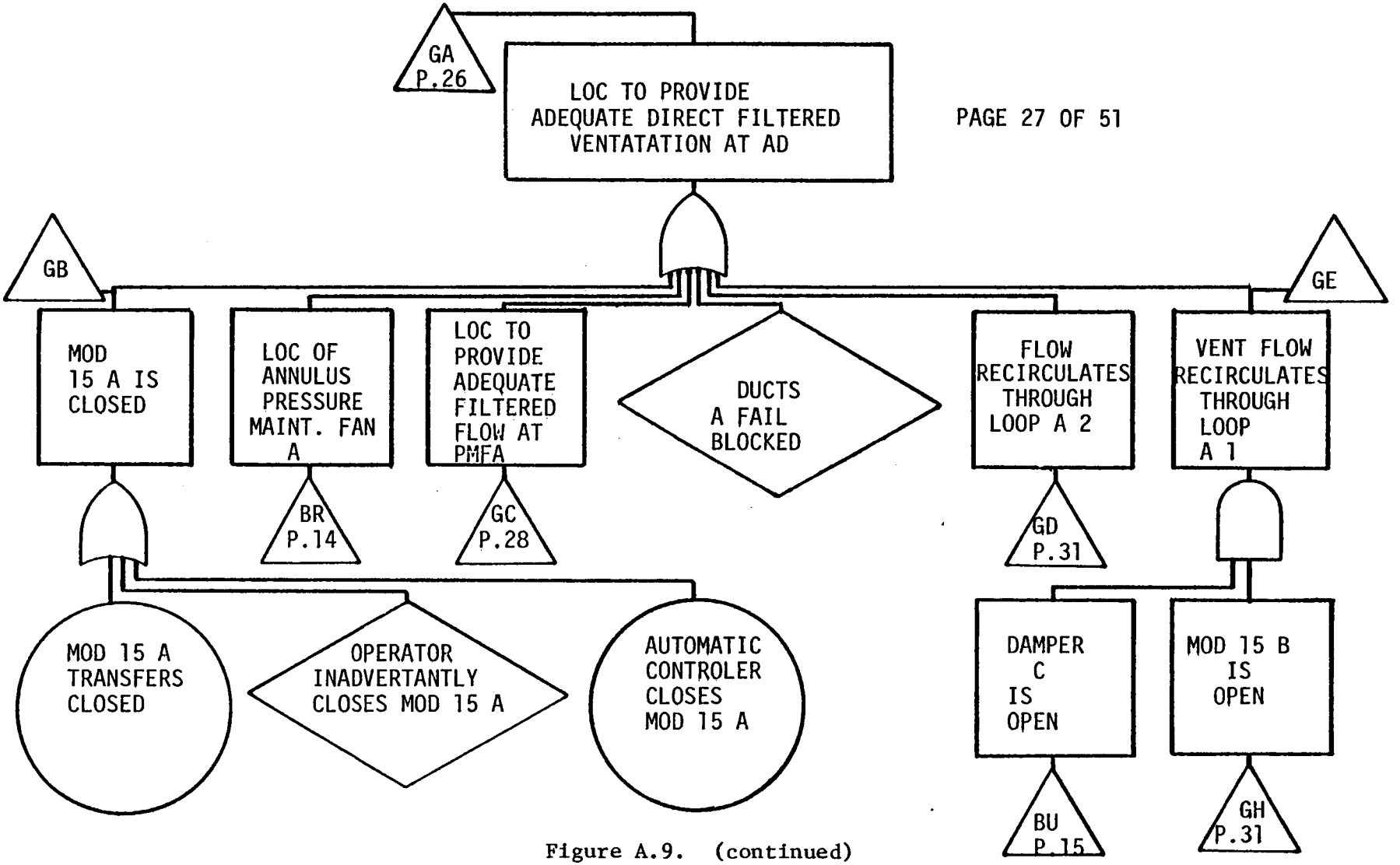


Figure A.9. (continued)

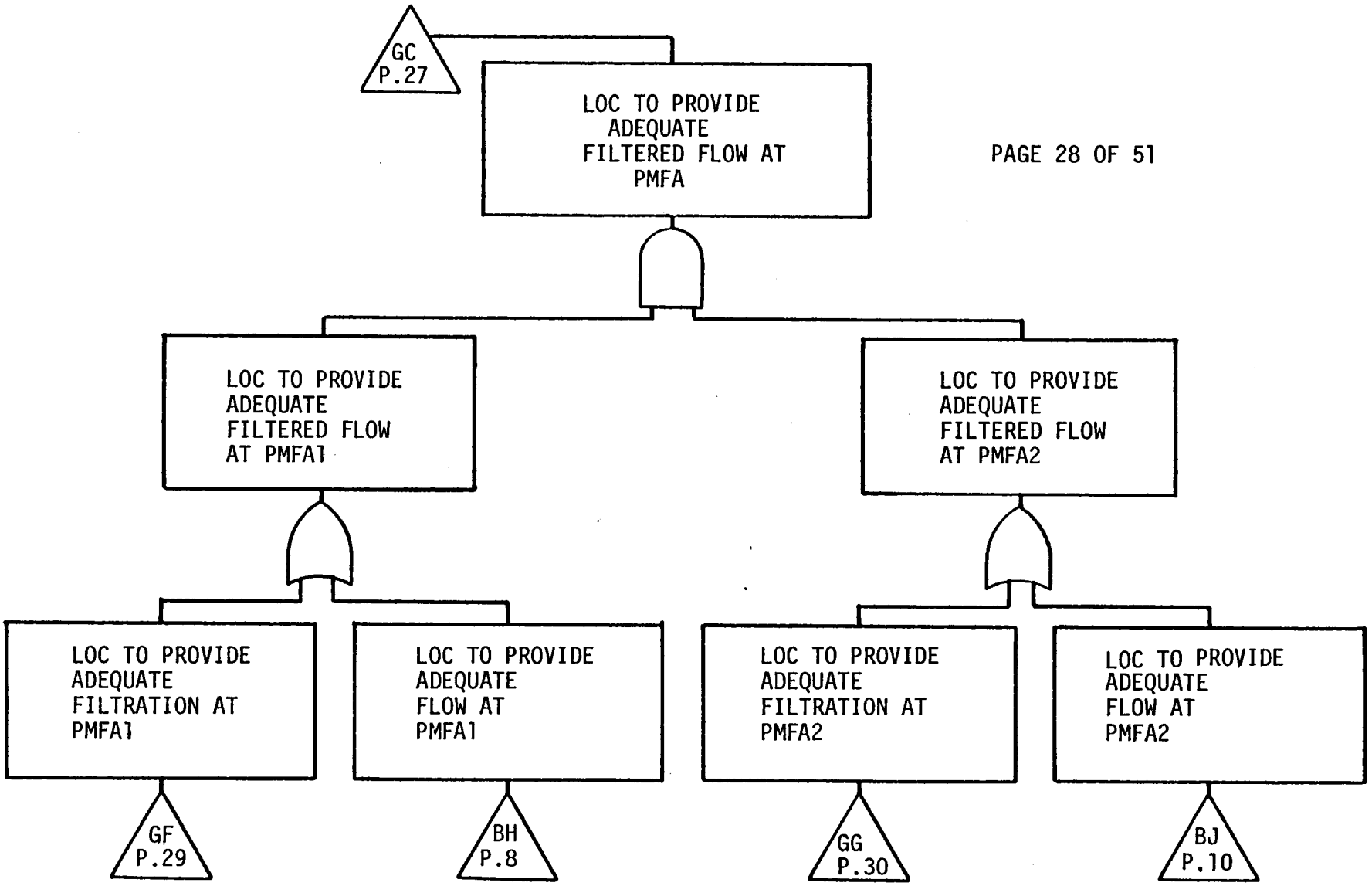


Figure A.9. (continued)

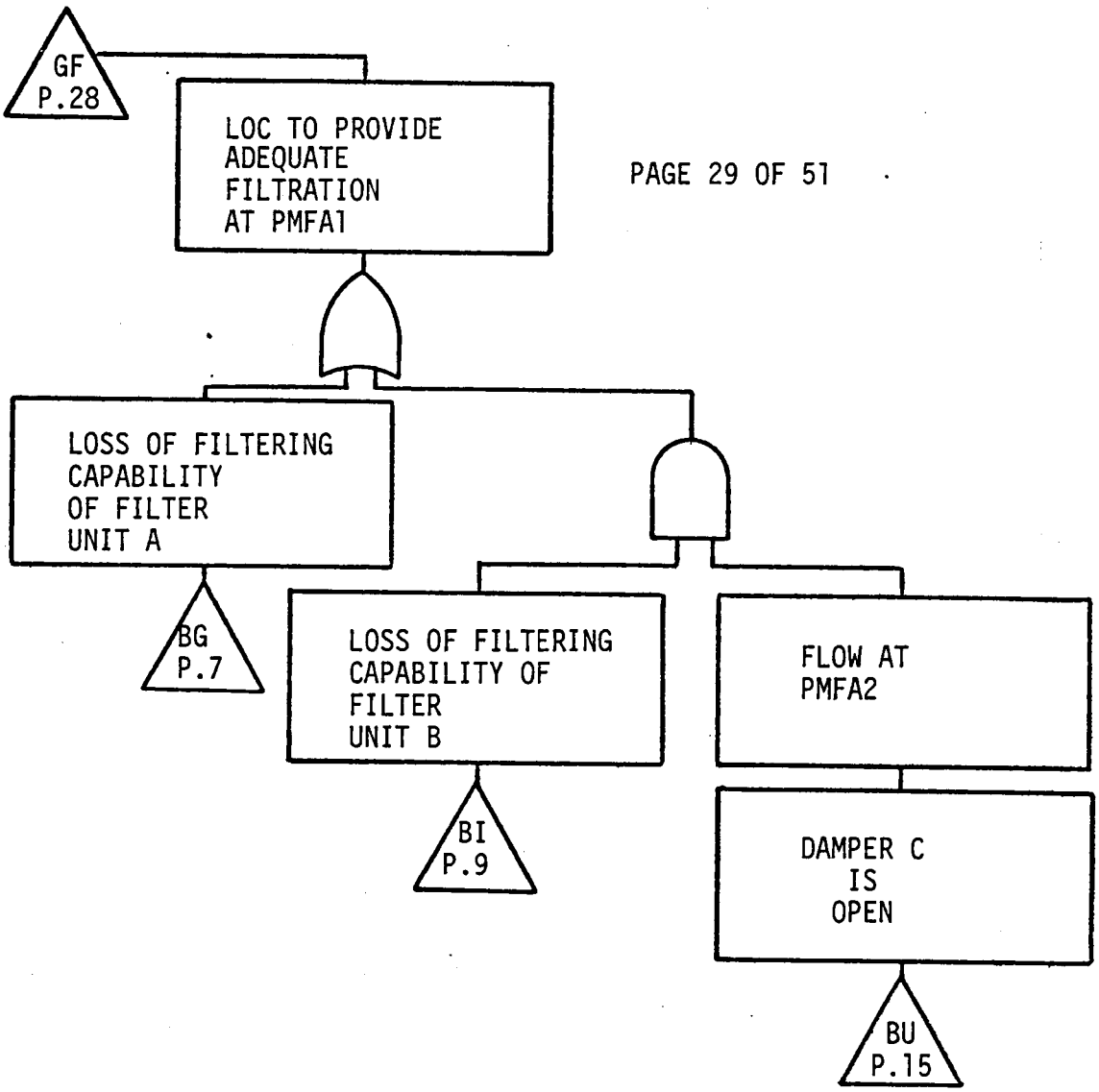


Figure A.9. (continued)

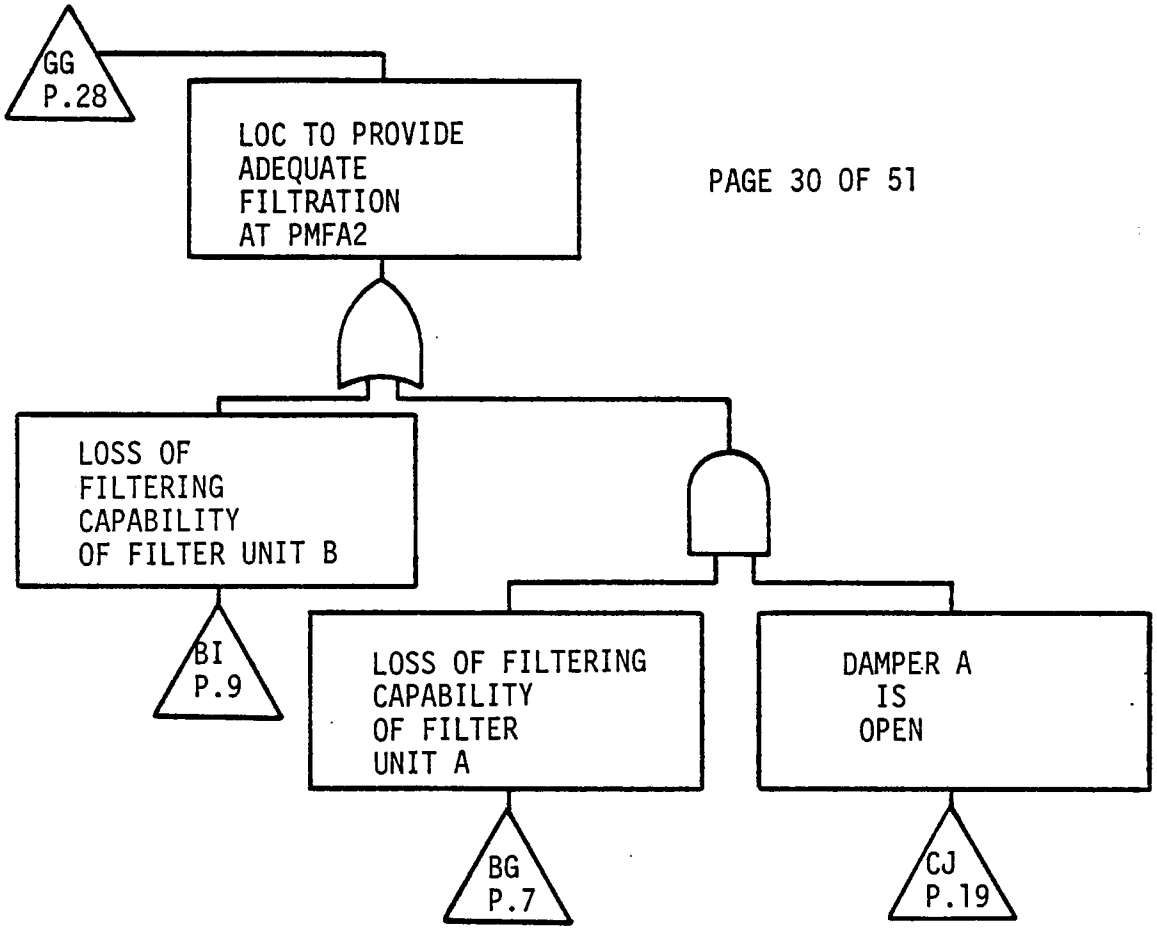


Figure A.9. (continued)

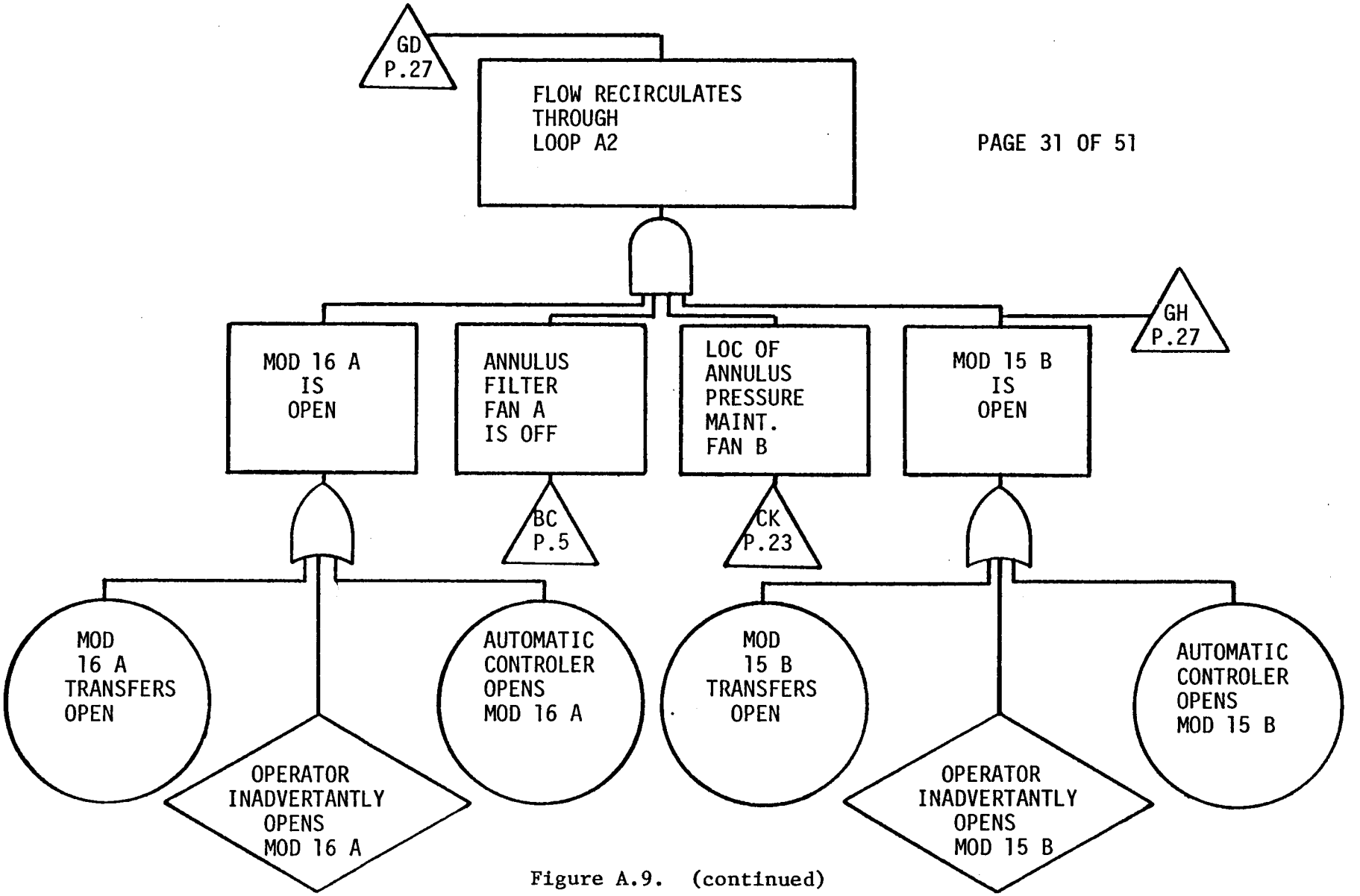


Figure A.9. (continued)

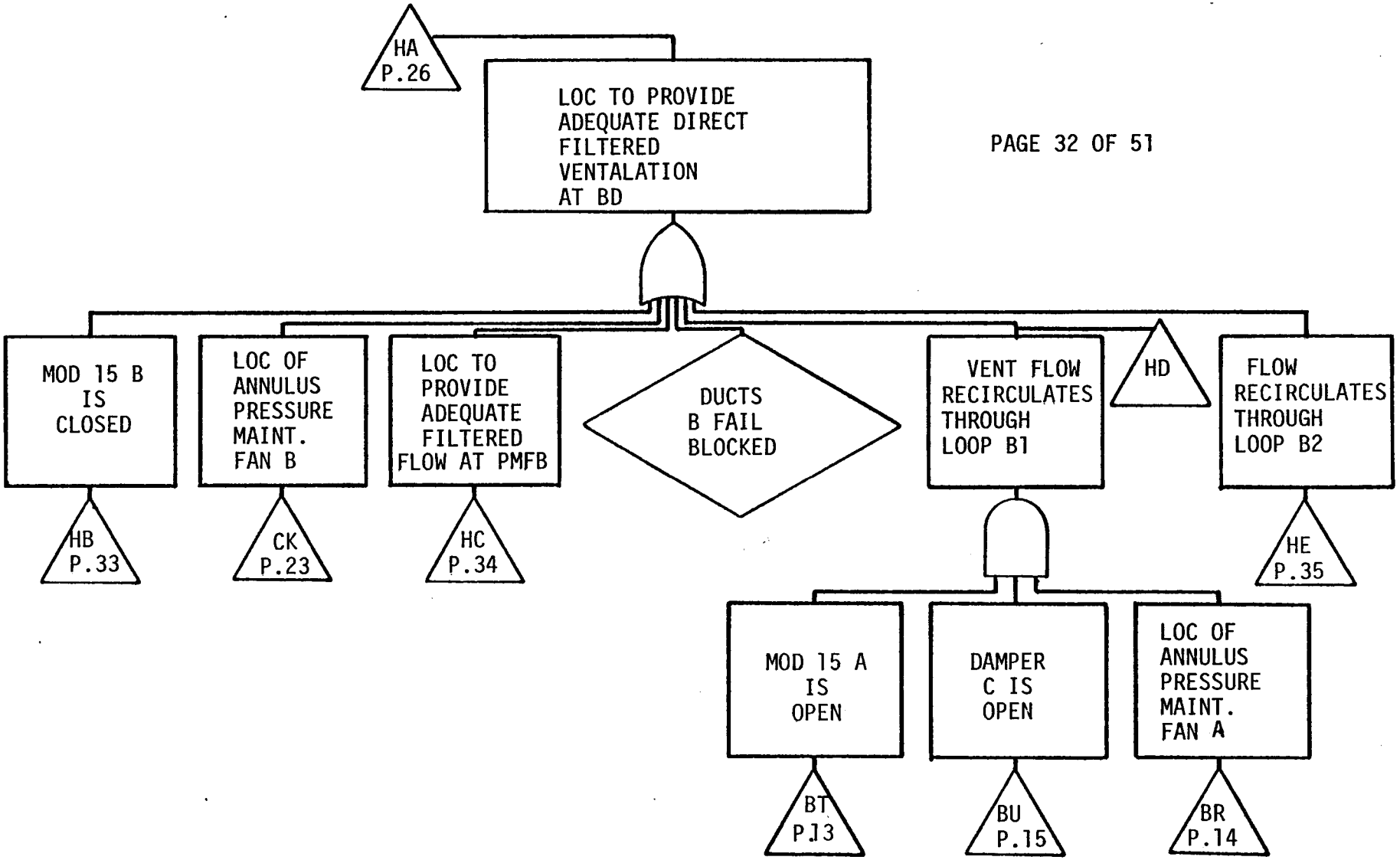


Figure A.9. (continued)

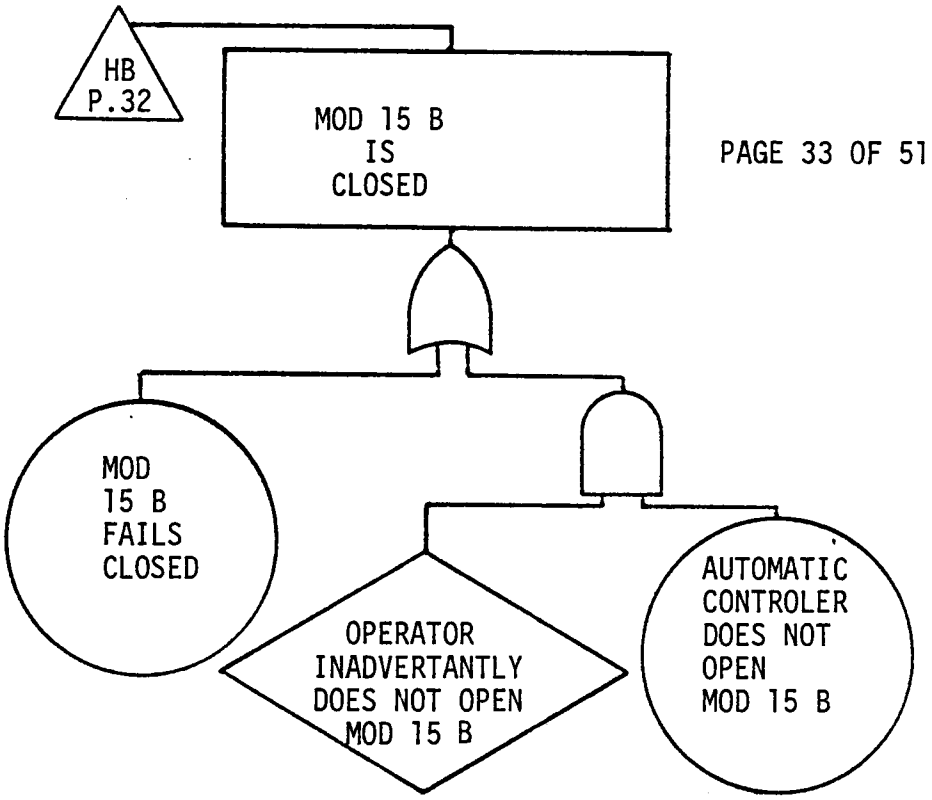


Figure A.9. (continued)

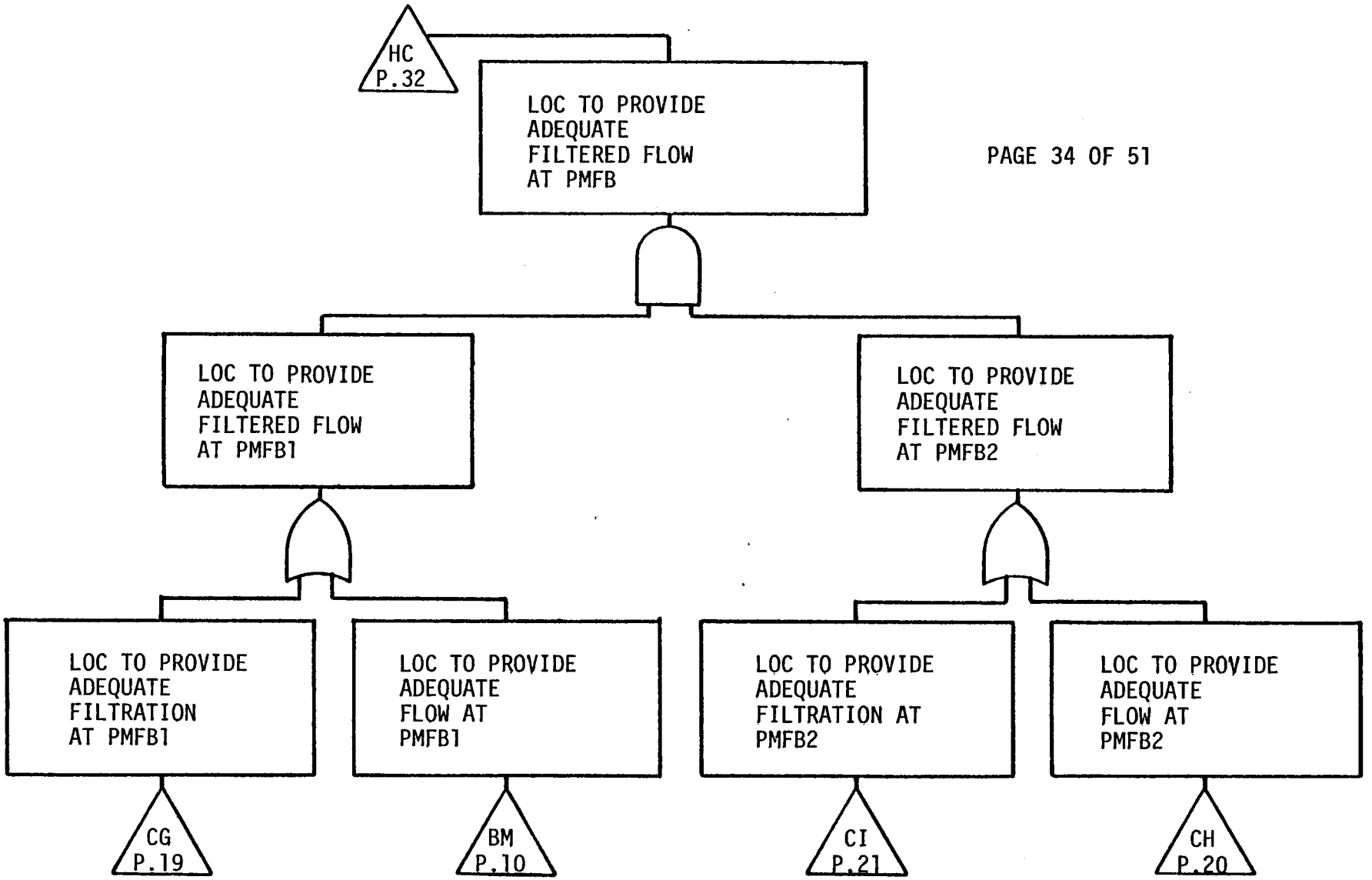


Figure A.9. (continued)

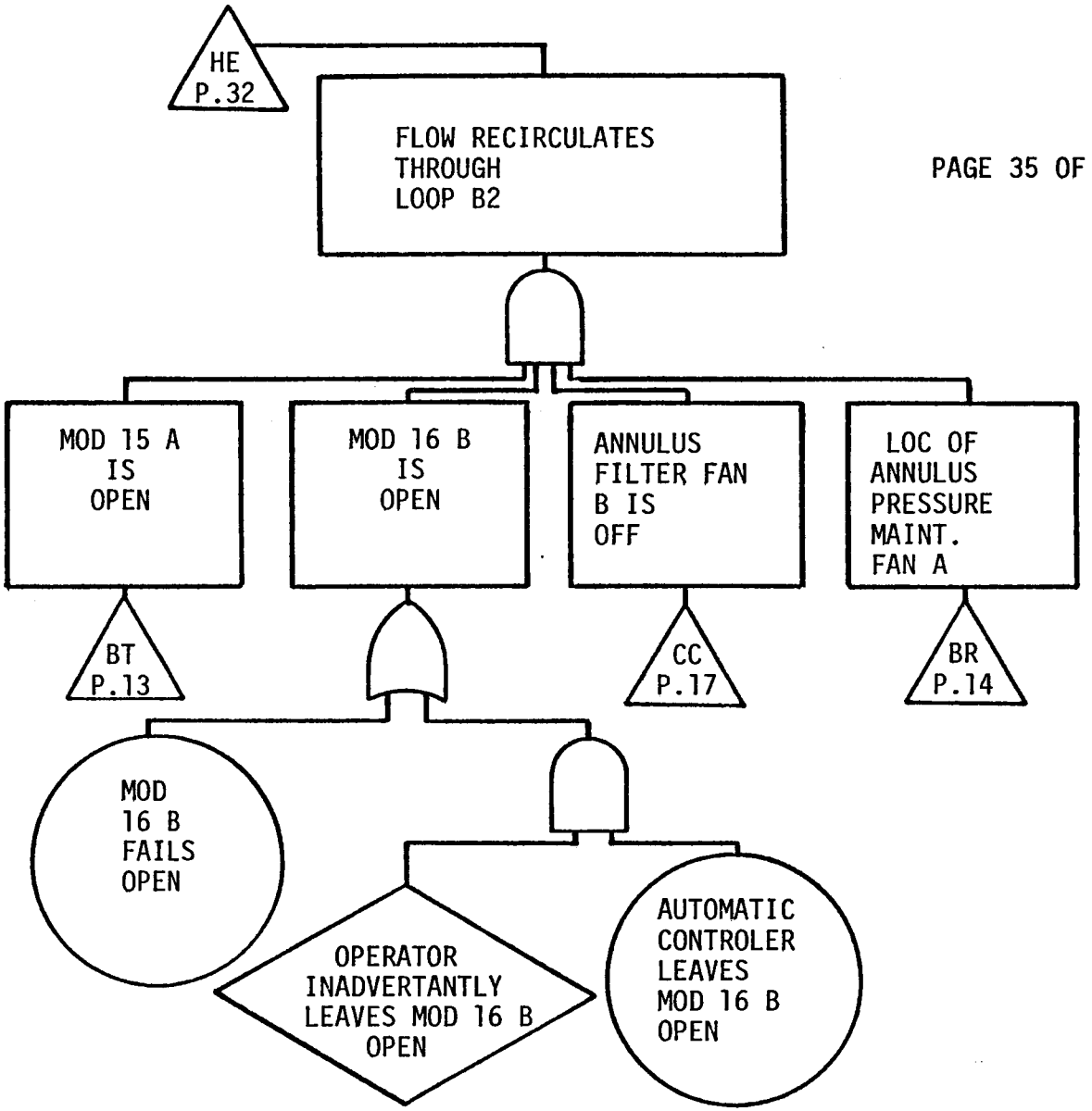


Figure A.9. (continued)

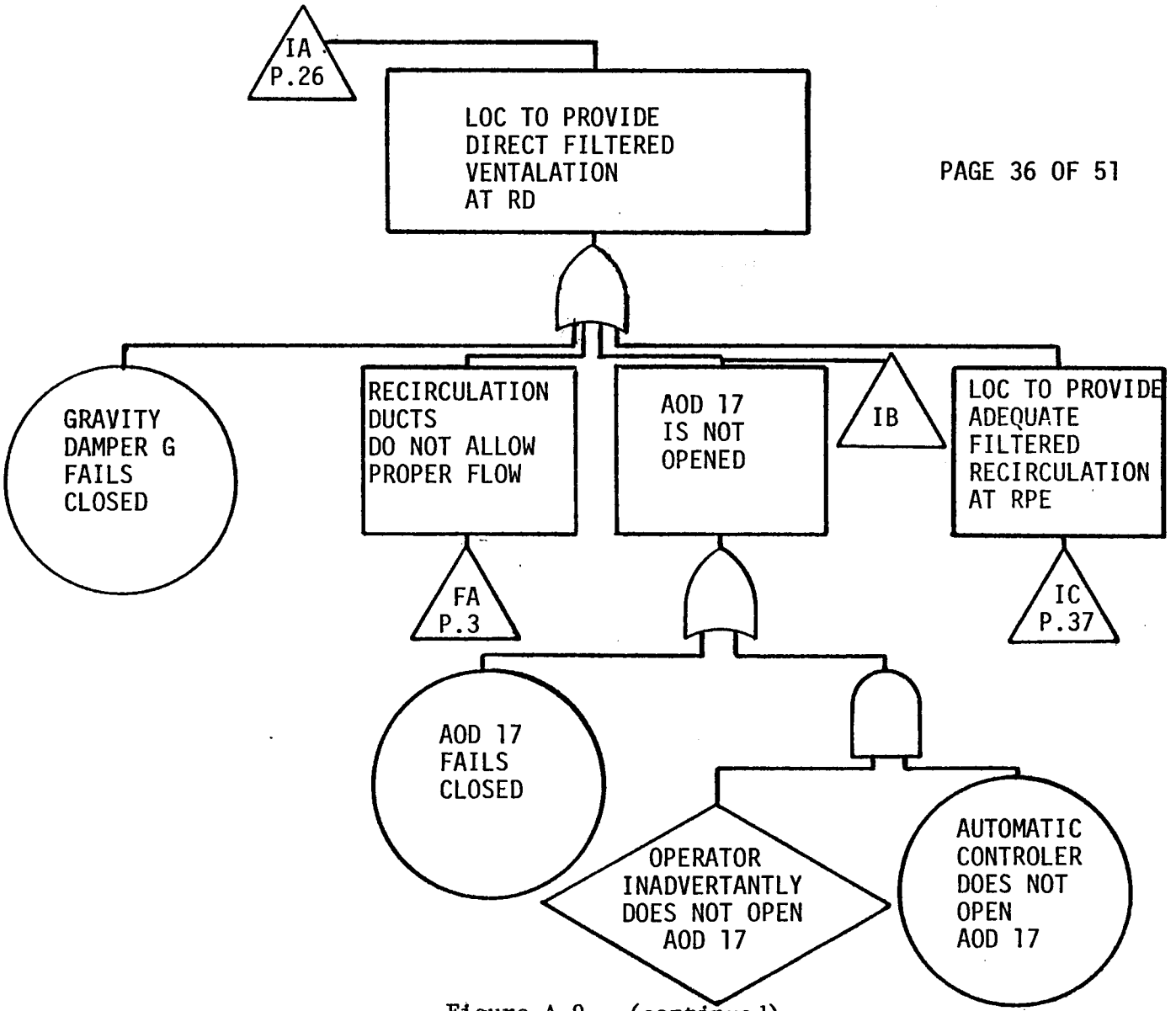


Figure A.9. (continued)

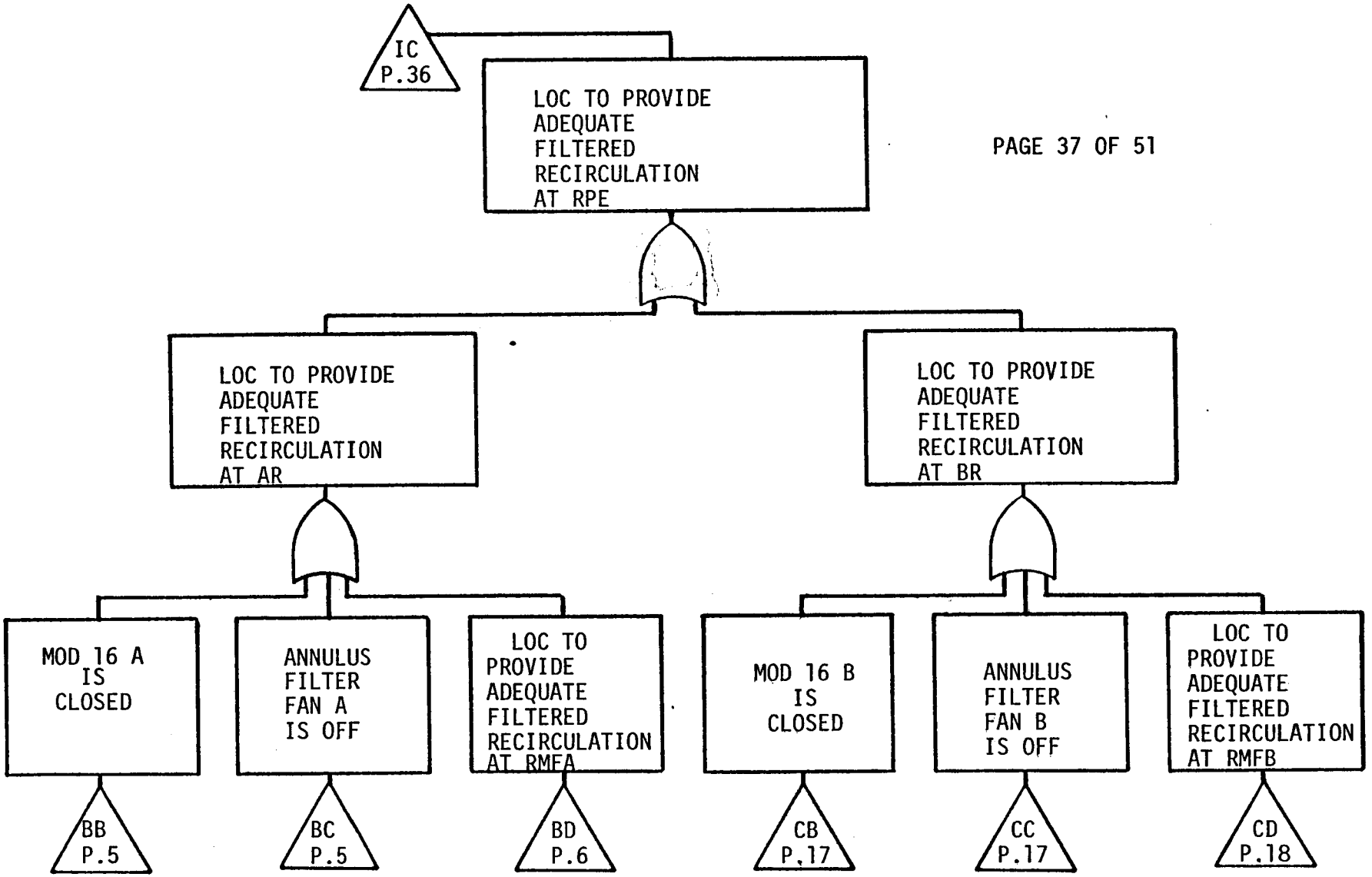


Figure A.9. (continued)

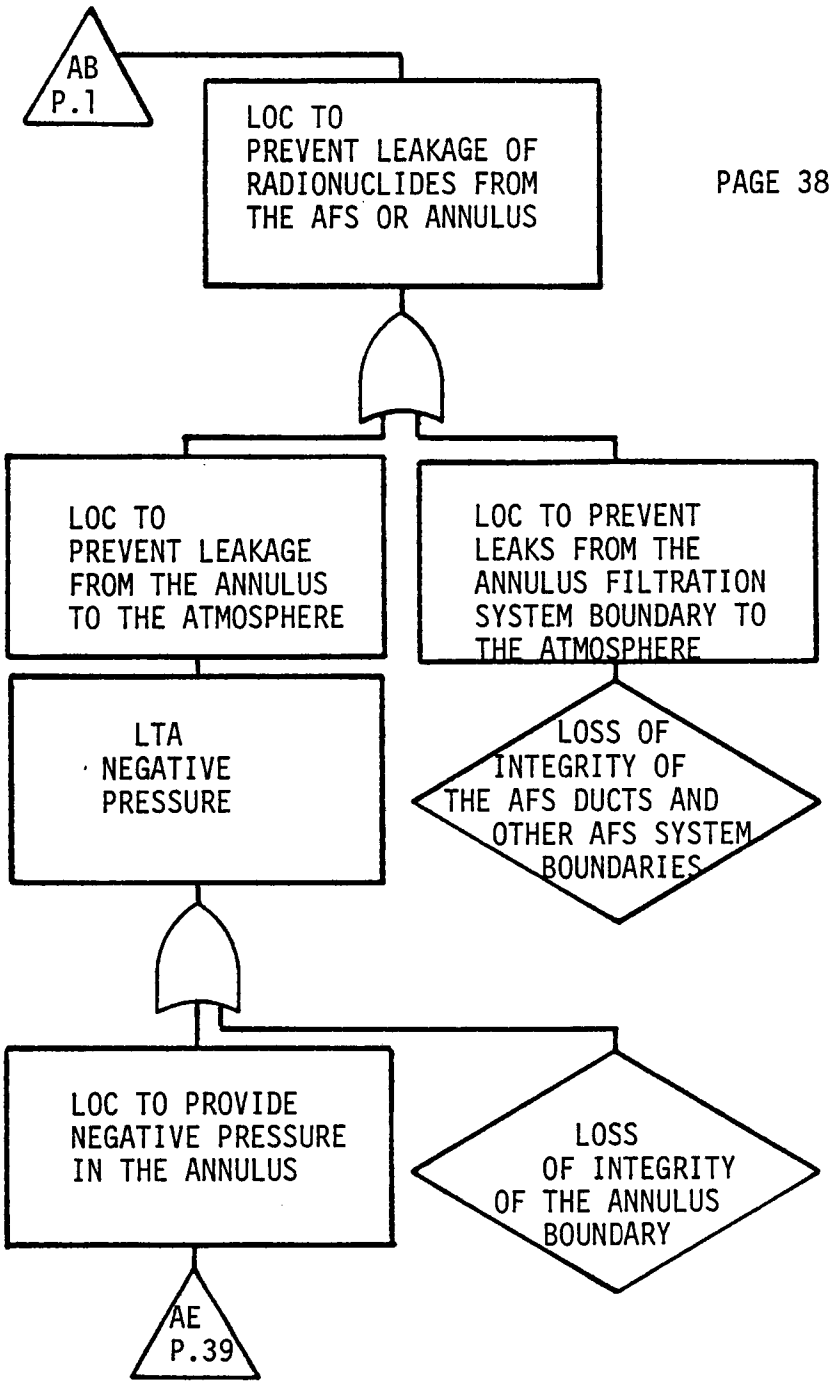


Figure A.9. (continued)

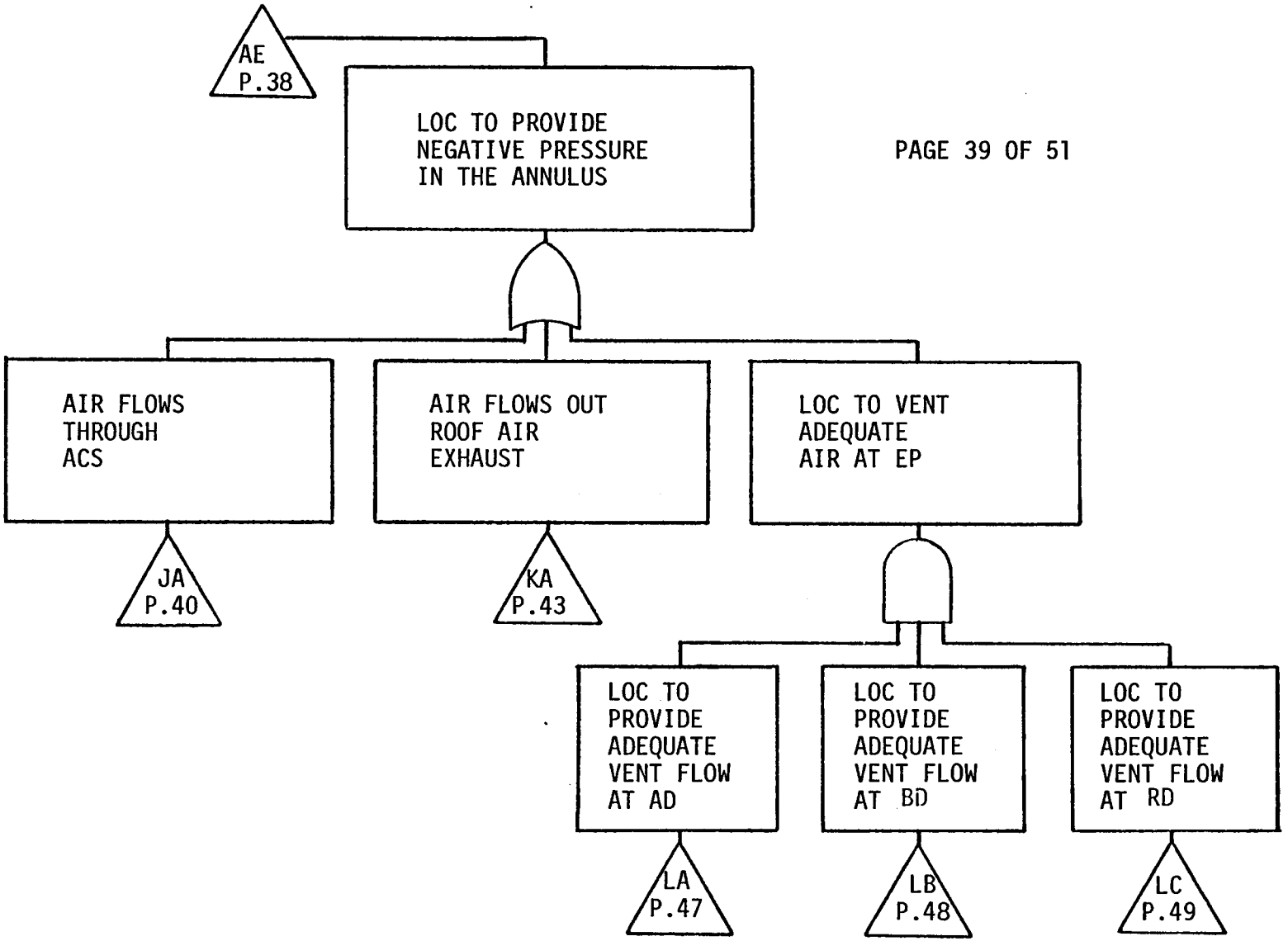


Figure A.9. (continued)

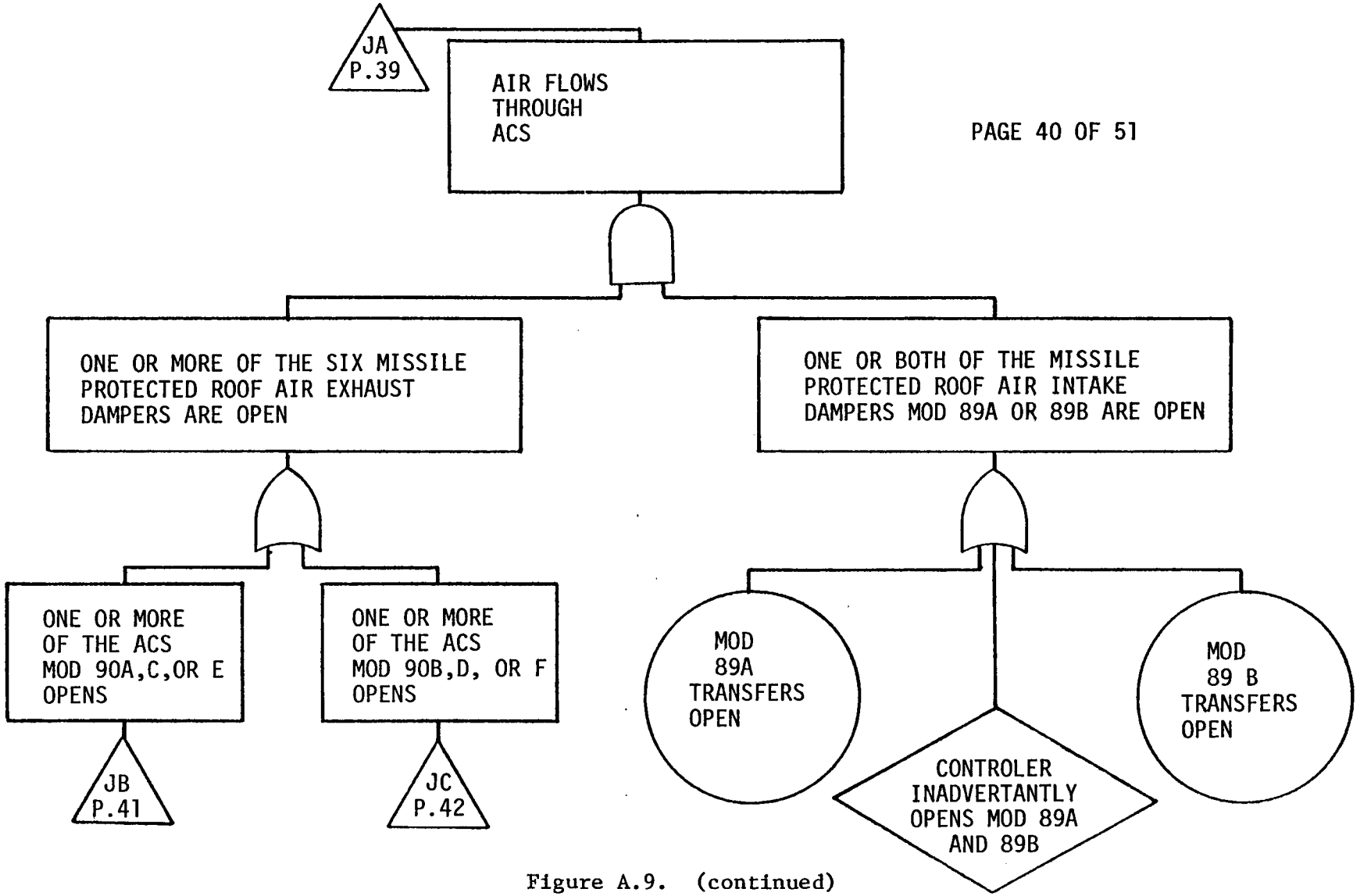


Figure A.9. (continued)

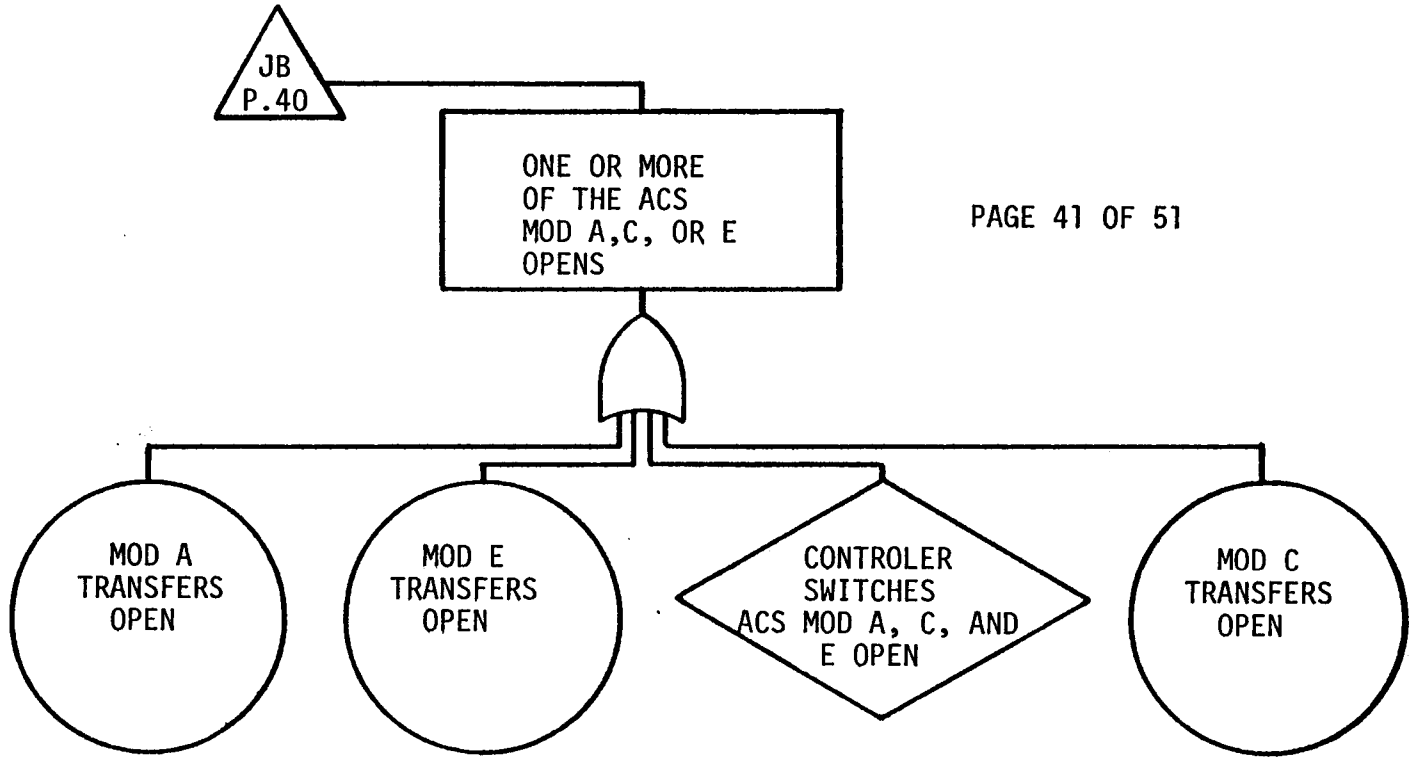


Figure A.9. (continued)

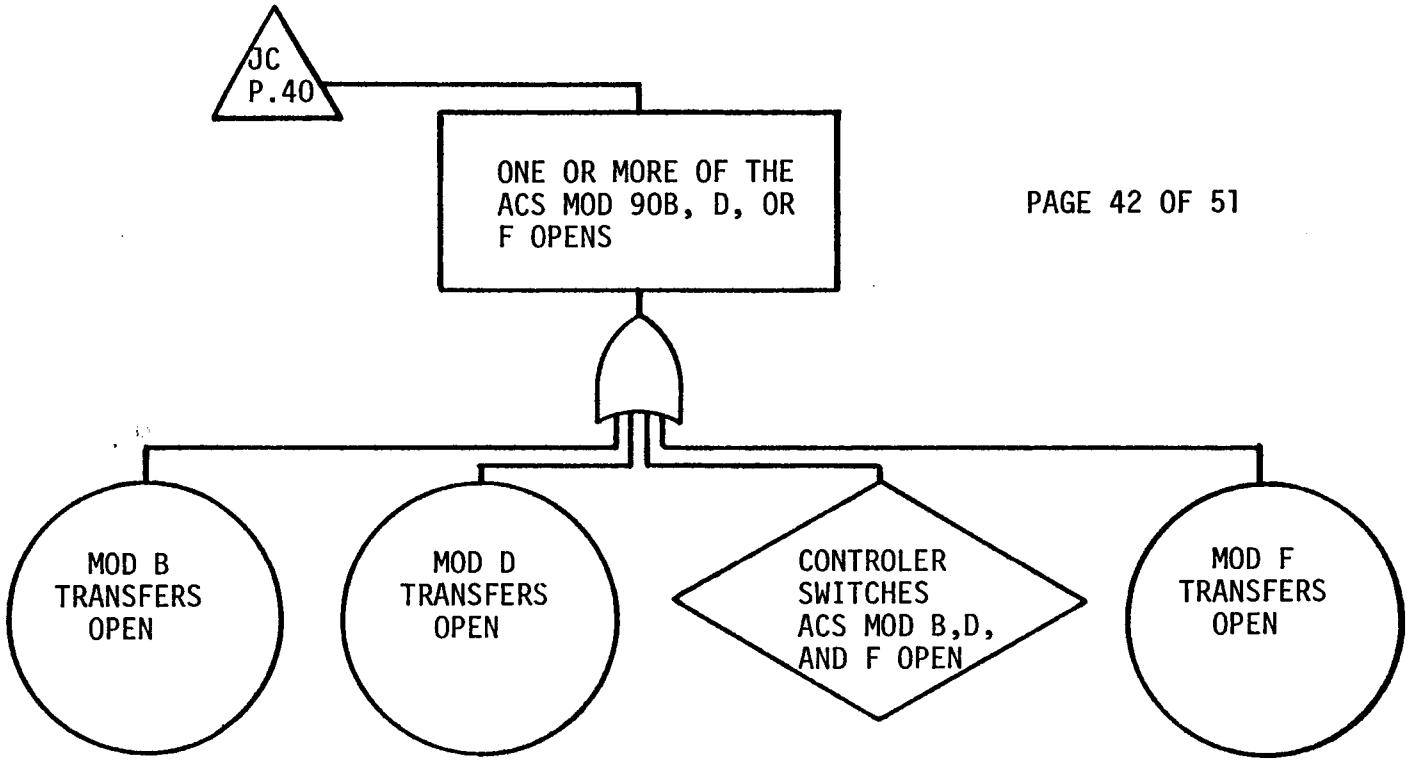


Figure A.9. (continued)

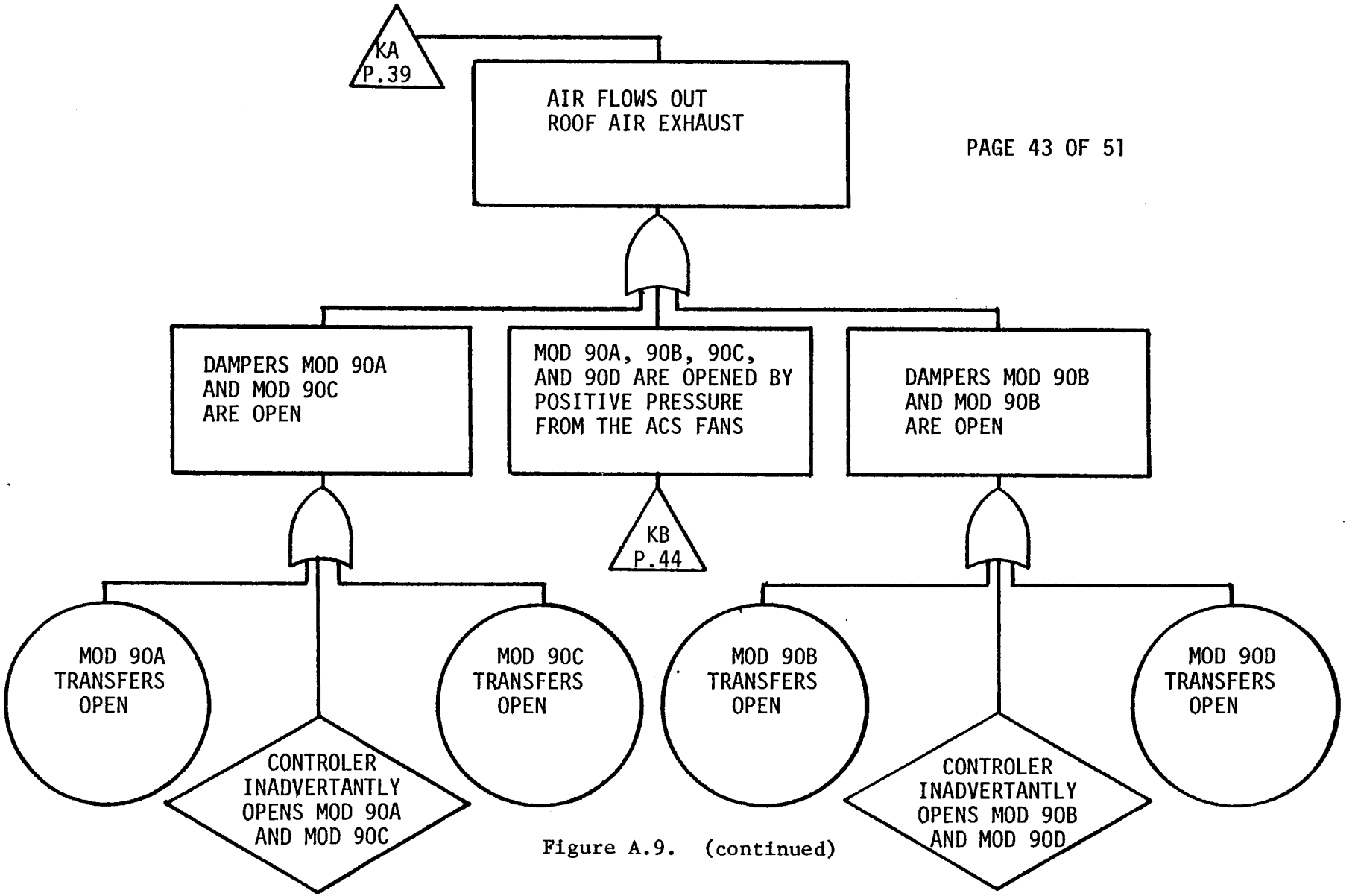


Figure A.9. (continued)

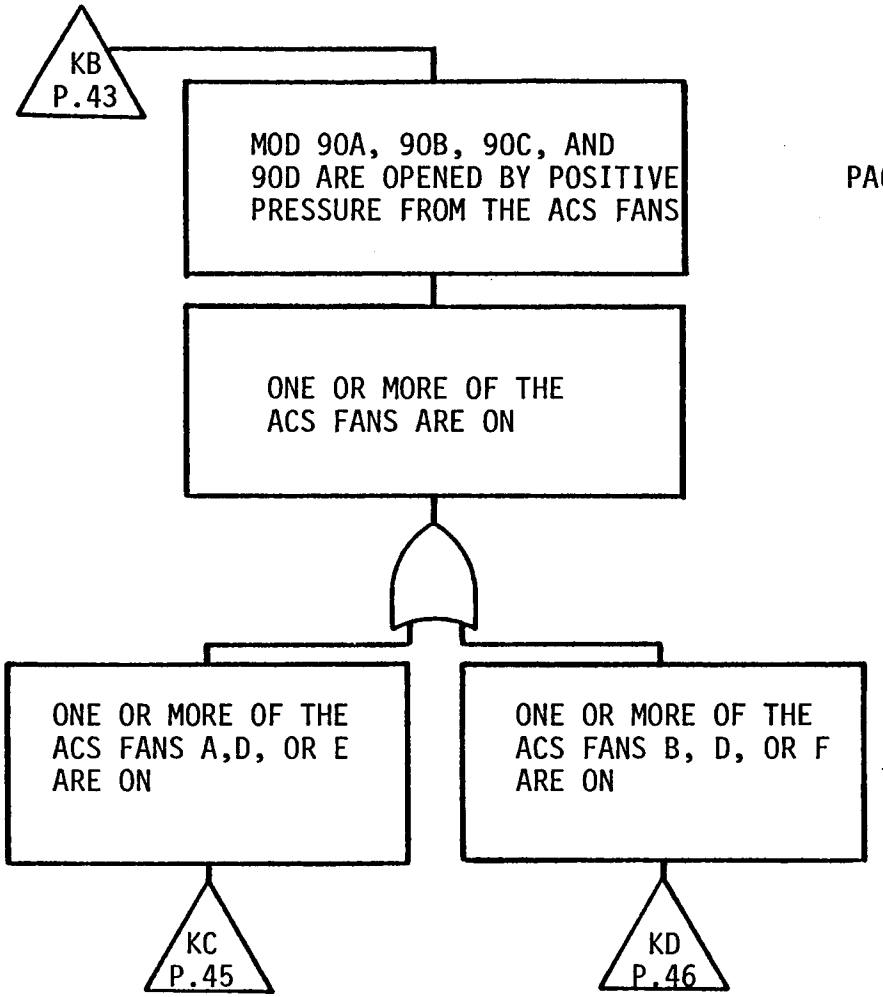


Figure A.9. (continued)

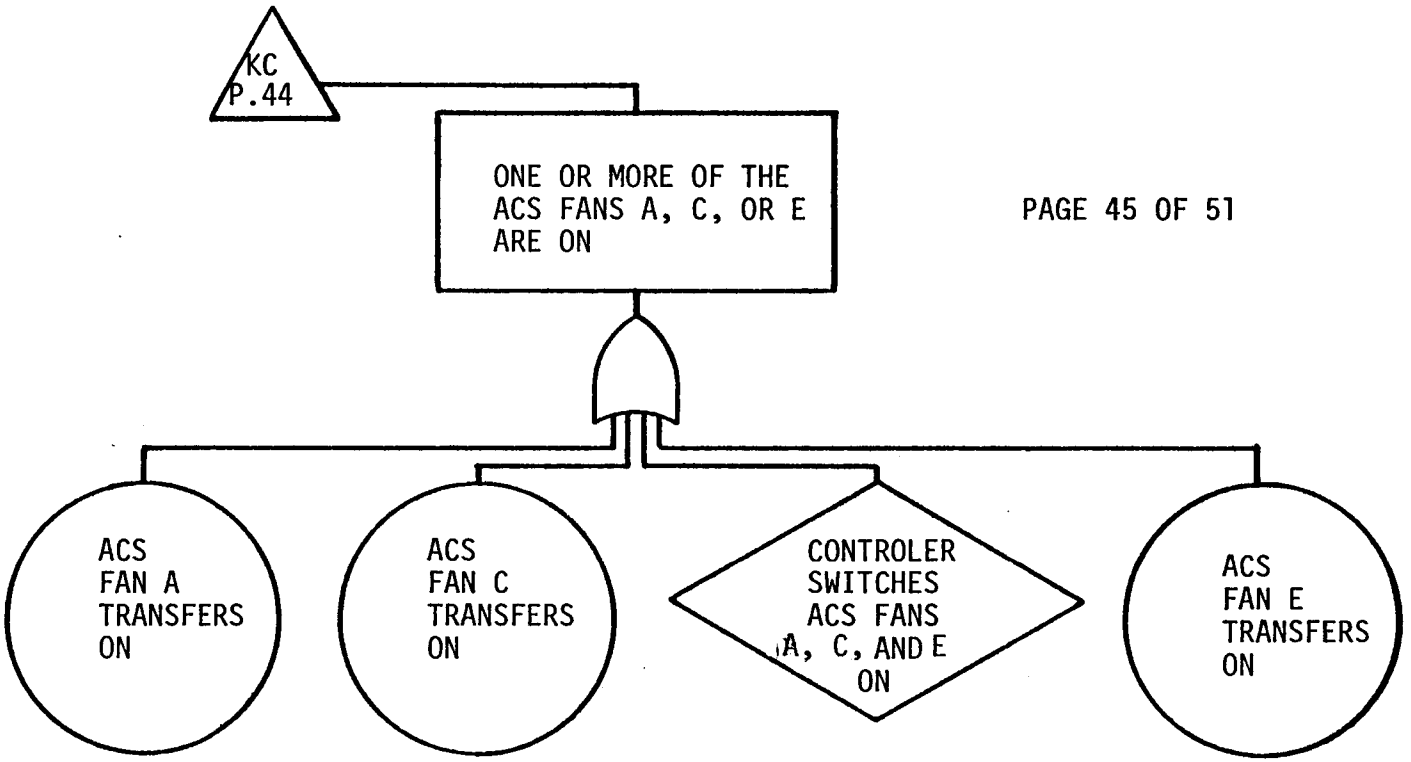


Figure A.9. (continued)

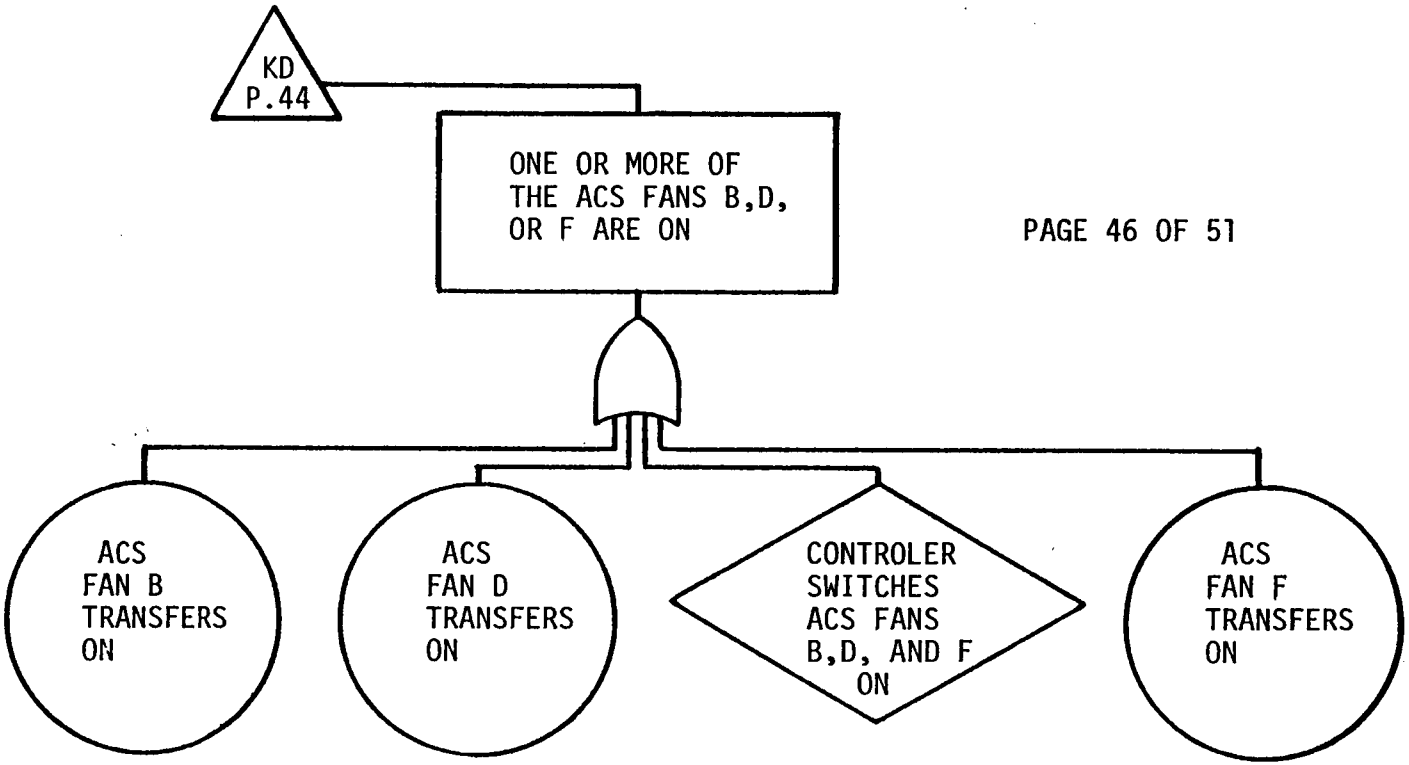


Figure A.9. (continued)

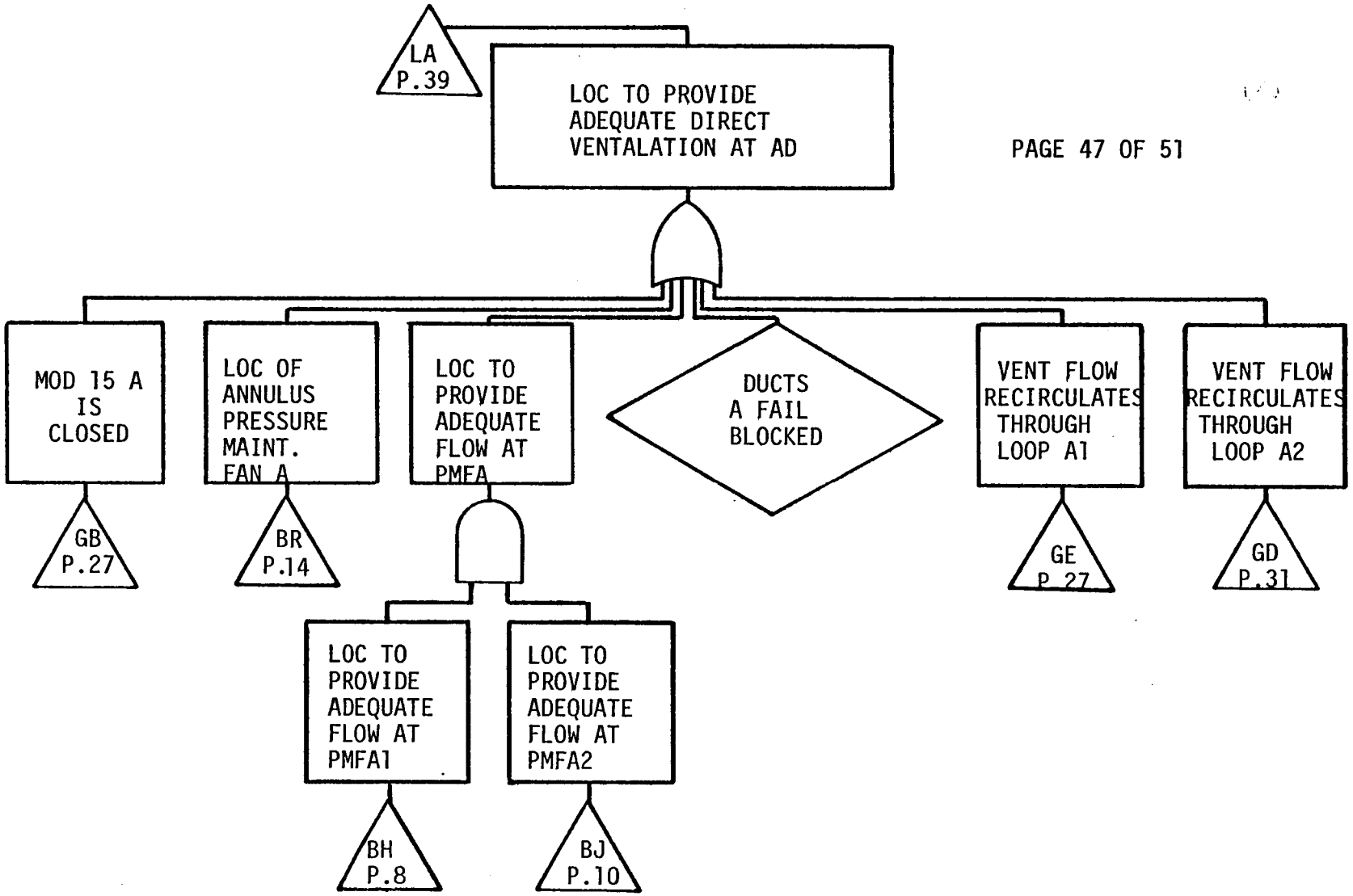


Figure A.9. (continued)

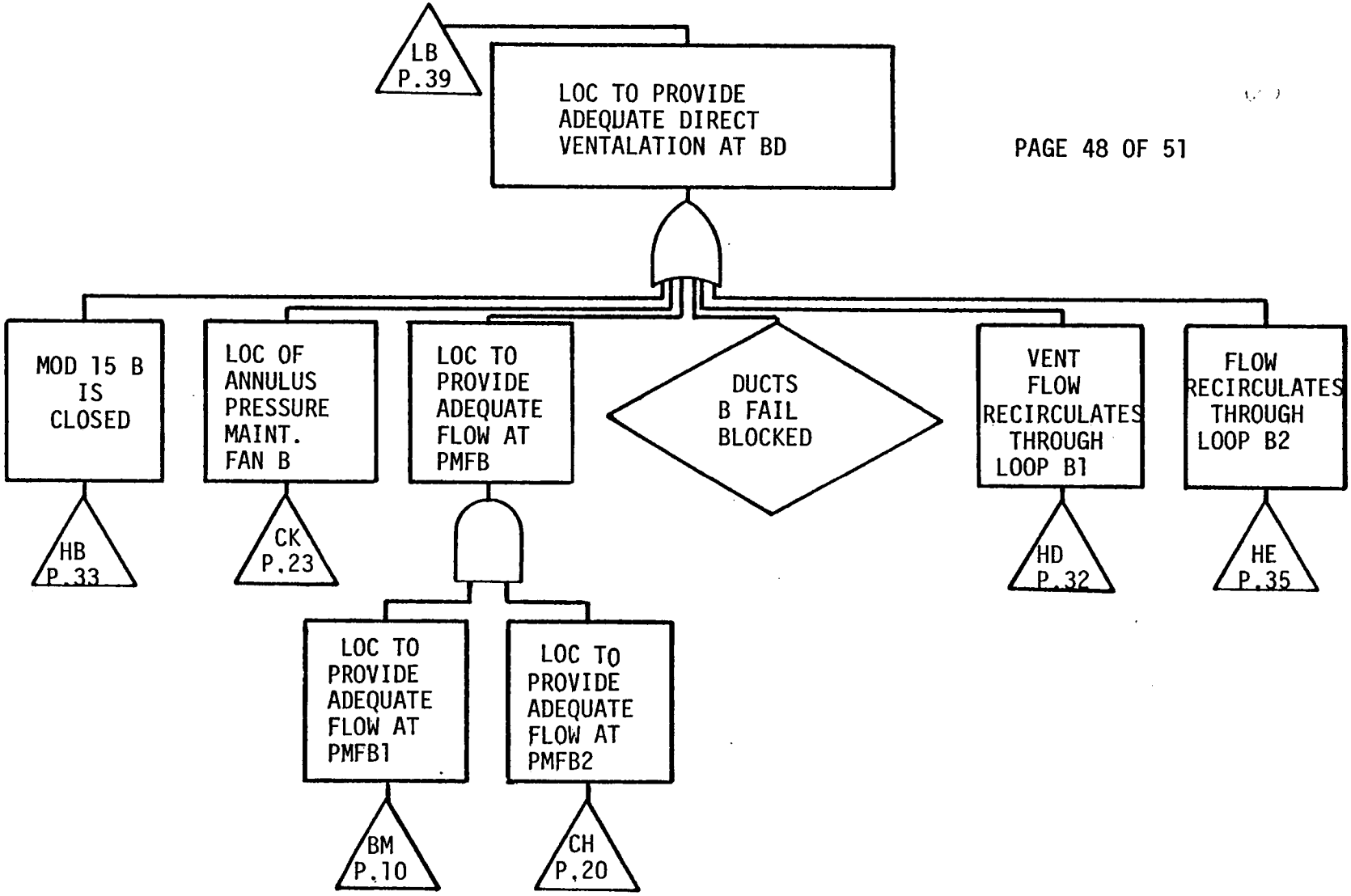


Figure A.9. (continued)

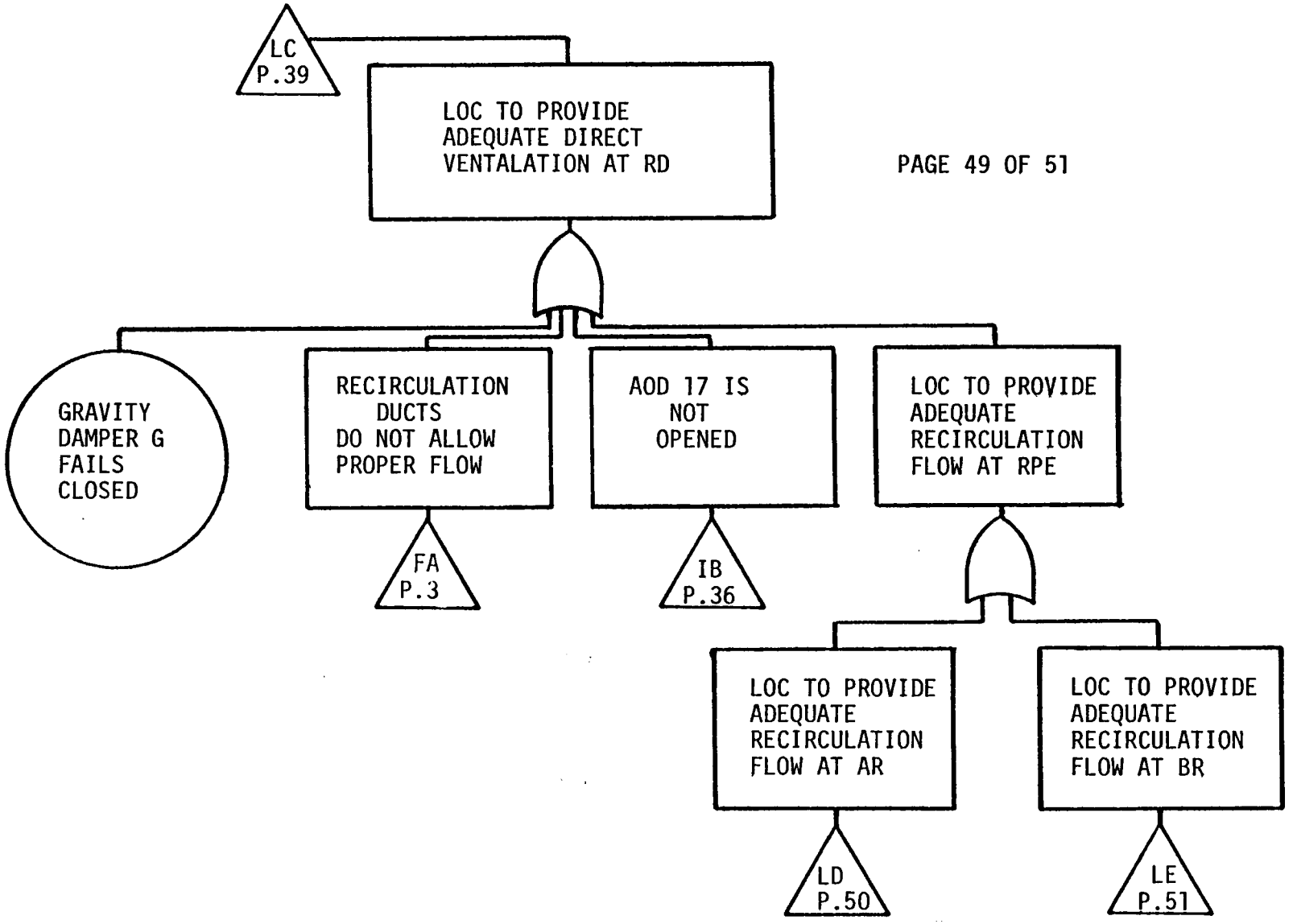


Figure A.9. (continued)

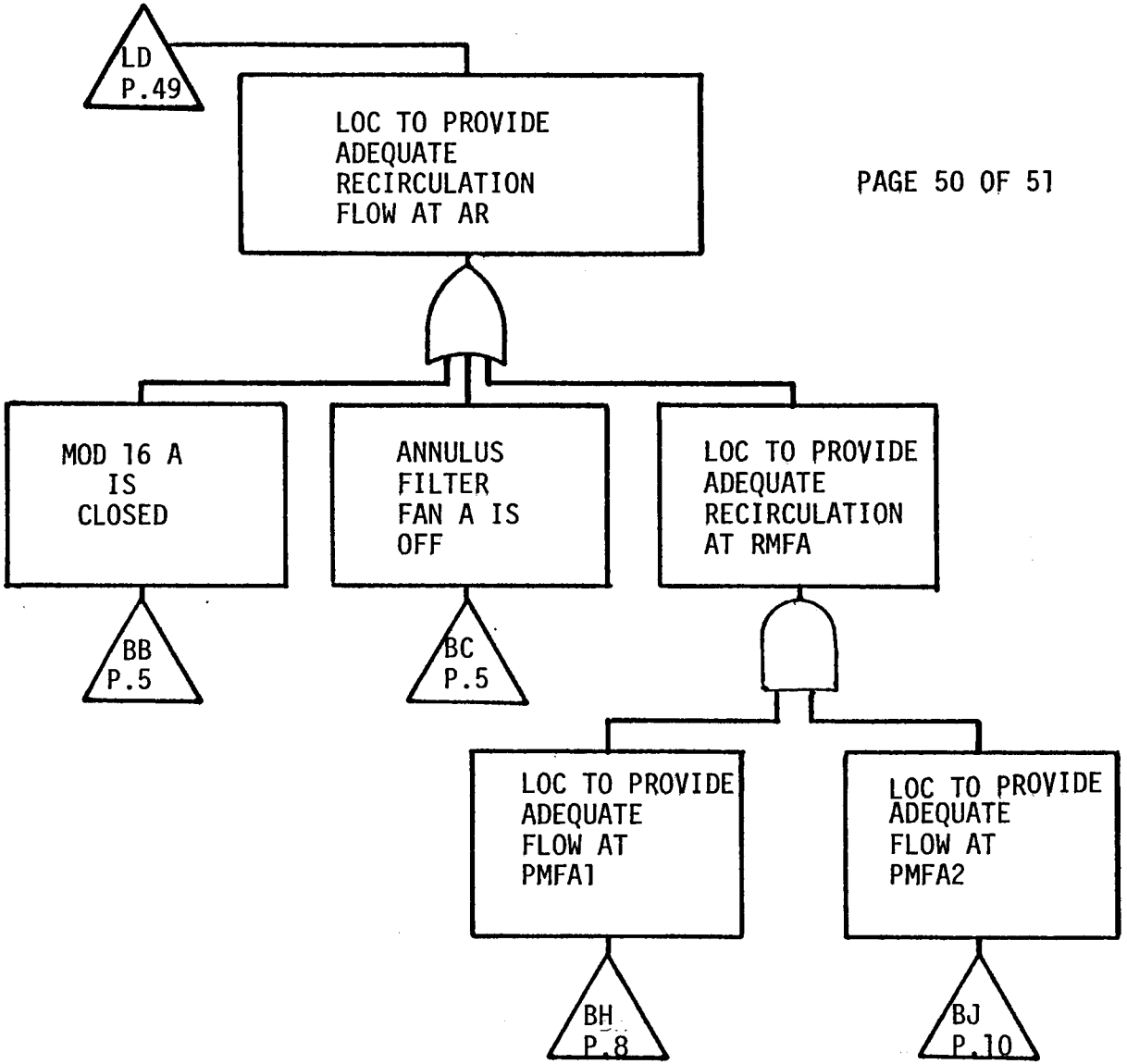


Figure A.9. (continued)

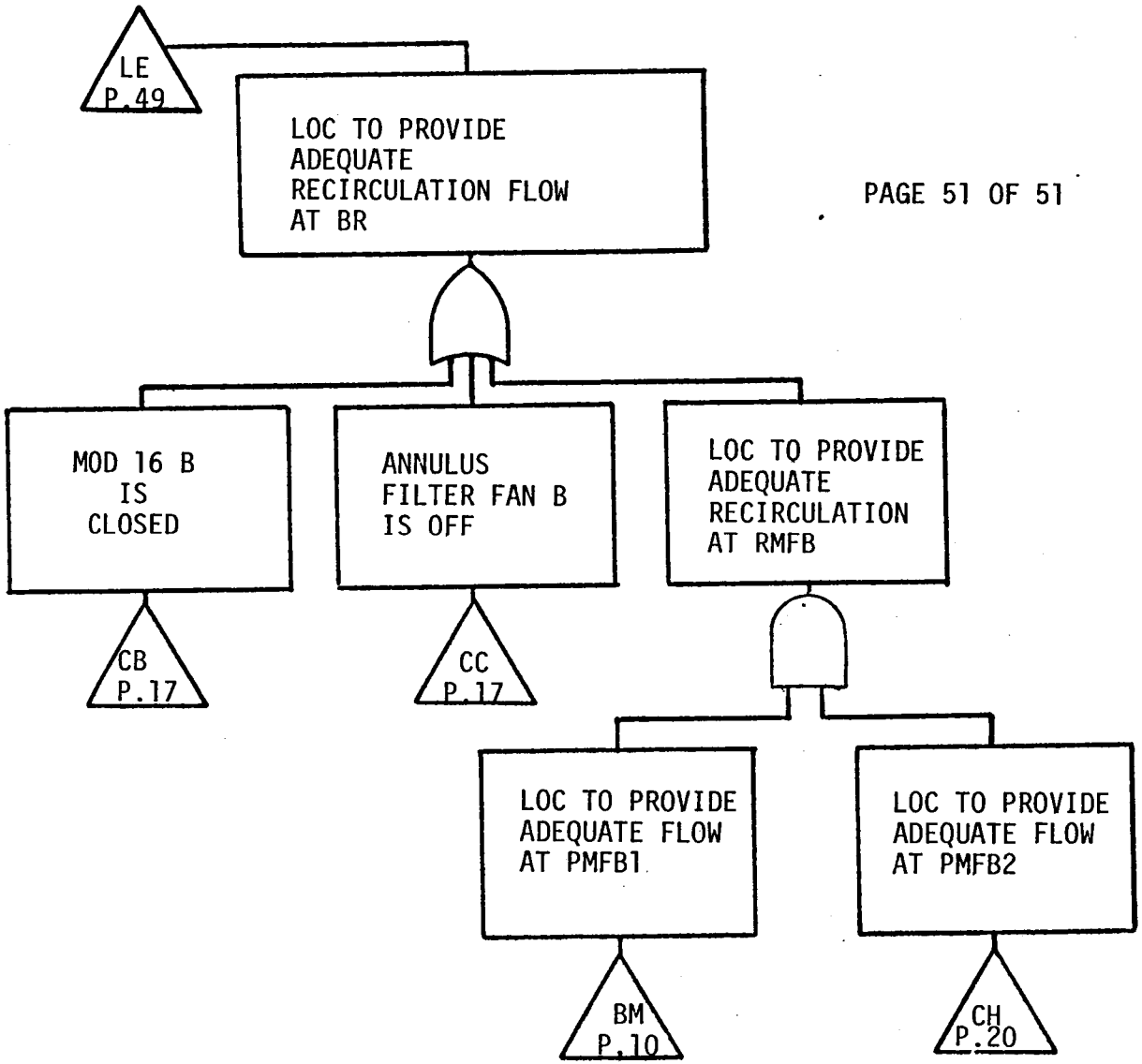


Figure A.9. (continued)

APPENDIX B

MINIMAL CUT SET INFORMATION

An eight character identification code is used to describe the basic events of the fault tree. The format of the code is shown in Figure B.1. The code may be deciphered by referring to Tables B.1 through B.3. Some operator events describing operator errors are described by a two letter code which is deciphered in Table B.4. Using these codes and the PREP computer program, a list of the one and two-event cut sets was determined and appears in Table B.5.

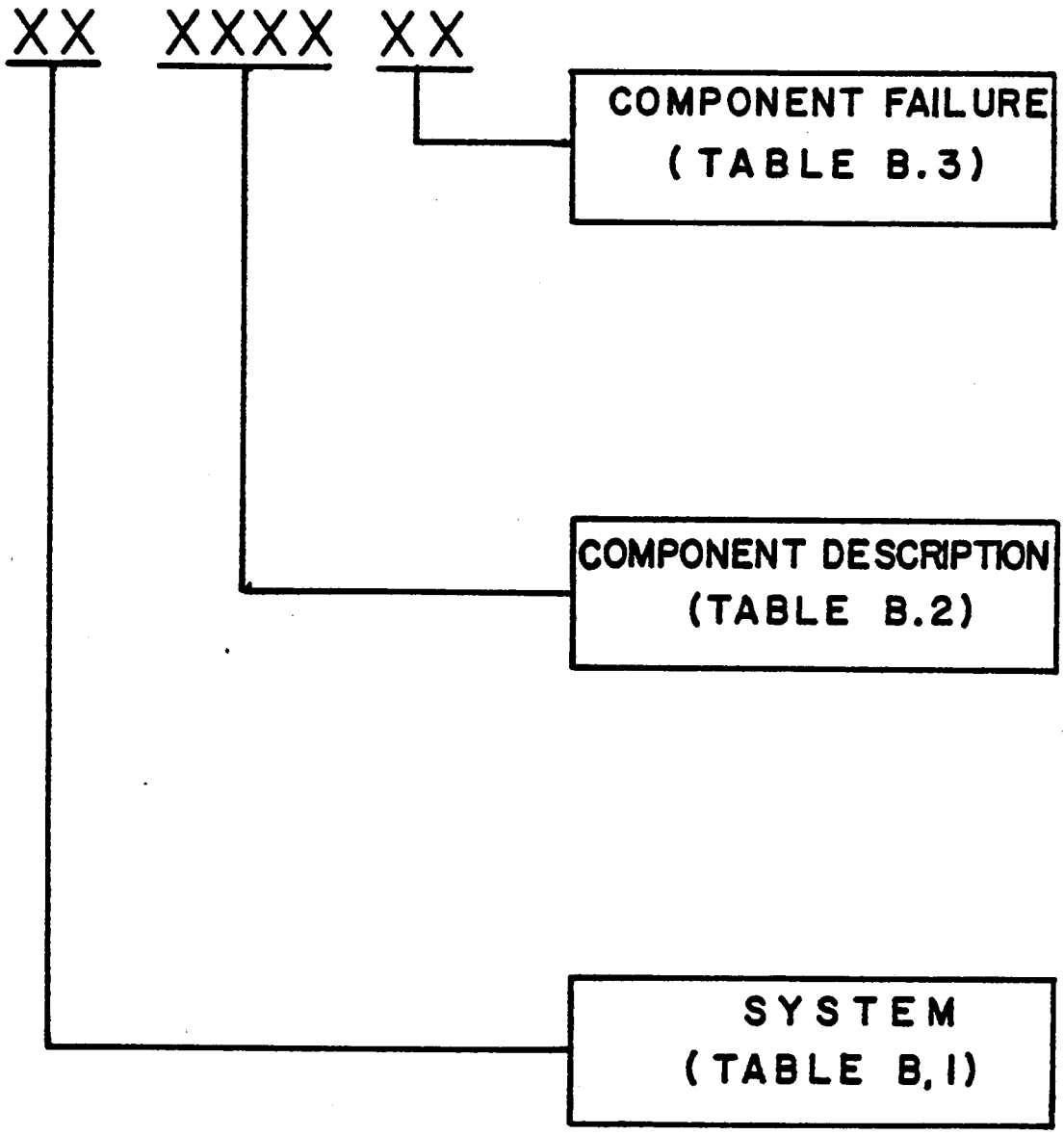


Figure B.1. Identification Code Format.

TABLE B.1

SYSTEM IDENTIFICATION CODES

Code	Description
AF	Annulus Filtration System
AC	Annulus Cooling System

TABLE B.2

COMPONENT DESCRIPTION CODES

Code	Description
ADFA	Adsorbant Filter A
ADFB	Adsorbant Filter B
ADI1	Air Operated Damper I1
ADI2	Air Operated Damper I2
AD17	Air Operated Damper 17
AD18	Air Operated Damper 18
AFFA	Annulus Filter Fan A
AFFB	Annulus Filter Fan B
ANNB	The Annulus Boundary
APFA	Annulus Pressure Maint. Fan A
APFB	Annulus Pressure Maint. Fan B
BGFA	Bag Filter A
BGFB	Bag Filter B
CSFA	Annulus Cooling System Fan A
CSFB	Annulus Cooling System Fan B
CSFC	Annulus Cooling System Fan C
CSFD	Annulus Cooling System Fan D
CSFE	Annulus Cooling System Fan E
CSFF	Annulus Cooling System Fan F
DCTA	Ducts A

TABLE B.2 (continued)

Code	Description
DCTB	Ducts B
DHED	Distribuion Header
DMPA	Damper A
DMPB	Damper B
DMPC	Damper C
DUSB	AFS Ducts and System Boundaries
FACE	ACS Fans A, C, and E
FBDF	ACS Fans B, D, and F
GDPG	Gravity Damper G
HCOA	Heating Coil A
HCOB	Heating Coil B
HFA1	HEPA Filter A1
HFA2	HEPA Filter A2
HFB1	HEPA Filter B1
HFB2	HEPA Filter B2
M15A	Motor Operated Damper 15A
M15B	Motor Operated Damper 15B
M16A	Motor Operated Damper 16A
M16B	Motor Operated Damper 16B
M89A	Motor Operated Damper 89A
M89B	Motor Operated Damper 89B

TABLE B.2 (continued)

Code	Description
M90A	Motor Operated Damper 90A
M90B	Motor Operated Damper 90B
M90C	Motor Operated Damper 90C
M90D	Motor Operated Damper 90D
MACE	Motor Operated Damper A, C, and E
MODA	Motor Operated Damper A
MODB	Motor Operated Damper B
MODC	Motor Operated Damper C
MODD	Motor Operated Damper D
MODE	Motor Operated Damper E
MODF	Motor Operated Damper F
MSPA	Moisture Separator A
MSPB	Moisture Separator B
POFS	Power Offsite
PONS	Power Onsite
89AB	Motor Operated Dampers 89A & 89B
90AC	Motor Operated Dampers 90A & 90C
90BD	Motor Operated Dampers 90B & 90D

TABLE B.3

FAILURE MODE CODES

Code	Description
AC	Automatic Controller Closes
AO	Automatic Controller Does Not Open
AP	Automatic Controller Opens
AR	Operator Does Not Maintain at an Adequate Rate
BL	Blocked
CN	Automatic Controller Switches ON
CO	Automatic Controller Leaves Open
CR	Automatic Controller Does Not Maintain at an Adequate Rate
CS	Automatic Controller Switches Open
FC	Fails Closed
FO	Fails Off
FP	Fails Open
LC	Loss of Capability to Provide
LF	Less than Adequate Filtration
LH	Less than Adequate Heat When Needed
LI	Loss of Integrity
LO	Operator Inadvertently Leaves Open
NM	Does Not Remove Moisture When Needed
NO	Automatic Controller Does Not Open

TABLE B.3 (continued)

Code	Description
OC	Operator Inadvertantly Closes
OD	Operator Does Not Close
OO	Operator Does Not Open
OP	Operator Opens
OT	Operator Does Not Turn ON
TC	Transfers Closed
TF	Transfer Off
TN	Transfers ON
TO	Torn Open
TP	Transfers Open

TABLE B.4

OPERATOR IDENTIFICATION CODES

Code	Description
01	Operator Does Not Open AODI1
02	Operator Does Not Open AOD18
03	Operator Does Not Open MODI2
04	Operator Opens AOD17
05	Operator Inadvertently Opens MOD 89A and 89B
06	Operator Switches ACS MOD A, C, and E Open
07	Operator Switches ACS MOD B, D, and F Open
08	Operator Inadvertently Opens MOD 90A and 90C
09	Operator Inadvertently Opens MOD 90B and 90D
010	Operator Switches ACS Fans A, C, and E ON
011	Operator Switches ACS Fans B, D, and F ON

TABLE B.5

LIST OF ONE AND TWO EVENT CUT SETS

Identification Number	Cut Set
1	AFDHEDBL
2	AFAD18FC
3	AFAD17TP
4	AFDUSBLI
5	AFANNBLI
6	ACM90ATP
7	ACM90CTP
8	ACCSFATN
9	ACCSFCTN
10	ACCSFETN
11	ACCSFBTN
12	ACCSFDTN
13	ACCSFFTN
14	AFRDUCBL
15	AFRDUCTO
16	ACM90DTP
17	ACM90BTP
18	AC90BDOP
19	ACFBDFCN
20	ACFACECN

TABLE B.5 (continued)

Identification Number	Cut Set
21	AC90ACOP
22	AFAO17OP
23	AFAD18NO
24	02
25	04
26	08
27	09
28	010
29	011
30	ACMODBTP ACM89ATP
31	ACMOCBTF AC89ABOP
32	ACMCDBTF ACM89BTF
33	ACMODBTP 05
34	ACMODDTF ACM89ATP
35	ACMODDTP AC89ABOP
36	ACMODDTP ACM89BTP
37	ACMODDTP 05
38	ACMBDFCS ACM89ATP
39	ACMBDFCS AC89ABOP
40	ACMBDFCS ACM89BTP
41	ACMBDFCS 05

TABLE B.5 (continued)

Identification Number	Cut Set	
42	ACMODFTP	ACM89ATP
43	ACMODFTP	AC89ABOP
44	ACMODFTP	ACM89BTP
45	ACMODFTP	05
46	07	ACM89ATP
47	07	AC89ABOP
48	07	ACM89BTP
49	07	05
50	ACMODATP	ACM89ATP
51	ACMODATP	AC89ABOP
52	ACMODATP	ACM89BTP
53	ACMODATP	05
54	ACMODATP	ACM89ATP
55	ACMODETP	AC89ABOP
56	ACMODETP	ACM89BTP
57	ACMODETP	05
58	ACMACECS	ACM89ATP
59	ACMACECS	AC89ABOP
60	ACMACECS	ACM89BTP
61	ACMACECS	05
62	ACMODCTP	ACM89ATP

TABLE B.5 (continued)

Identification Number	Cut Set	
63	ACMODCTP	AC89ABOP
64	ACMODCTP	ACM89BTP
65	ACMODCTP	05
66	06	ACM89ATP
67	06	AC89ABOP
68	06	ACM89BTP
69	06	05
70	AFPONSLC	AFPOFSLC
71	AFDMPBTC	AFM15ATC
72	AFDMPBTC	AFM15AOC
73	AFDMPBTC	AFM15AAC
74	AFDMPBOC	AFM15ATC
75	AFDMPBOC	AFM15AOC
76	AFDMPBOC	AFM15AAC
77	AFBGFBBL	AFM15ATC
78	AFBGFBBL	AFM15AOC
79	AFBGFBBL	AFM15AAC
80	AFHFB1BL	AFM15ATC
81	AFHFB1BL	AFM15AOC
82	AFHFB1BL	AFM15AAC
83	AFADFBBL	AFM15ATC

TABLE B.5 (continued)

Identification Number	Cut Set
84	AFADFBBL AFM15AOC
85	AFADFBBL AFM15AAC
86	AFHFB2BL AFM15ATC
87	AFHFB2BL AFM15AOC
88	AFHFB2BL AFM15AAC
89	AFHPB2LF AFM15ATC
90	AFHFB2LF AFM15AOC
91	AFHFB2LF AFM15AAC
92	AFADFBLF AFM15ATC
93	AFADFBLF AFM15AOC
94	AFADFBLF AFM15AAC
95	AFBGFBLF AFM15ATC
96	AFBGFBLF AFM15AOC
97	AFBGFBLF AFM15AAC
98	AFHCOBLF AFM15ATC
99	AFHCOBLF AFM15AOC
100	AFHCOBLF AFM15AAC
101	AFMSPBNM AFM15ATC
102	AFMSPBNM AFM15AOC
103	AFMSPBNM AFM15AAC
104	AFDMPATC AFDMPBTC

TABLE B.5 (continued)

Identification Number	Cut Set
105	AFDMPATC AFDMPBOC
106	AFDMPATC AFBGFBBL
107	AFDMPATC AFHFB1BL
108	AFDMPATC AFACFBBL
109	AFDMPATC AFHFB2BL
110	AFDMPATC AFHFB2LF
111	AFDMPATC AFACFBLF
112	AFDMPATC AFBGFBLF
113	AFDMPATC AFHCOBLH
114	AFDMPATC AFMSPBNM
115	AFDMPAOC AFDMPBTC
116	AFDMPAOC AFDMPBOC
117	AFDMPAOC AFBGFBBL
118	AFDMPAOC AFHFB1BL
119	AFDMPAOC AFADFBBL
120	AFDMPAOC AFHFB2BL
121	AFDMPAOC AFHFB2LF
122	AFDMPAOC AFADFBLF
123	AFDMPAOC AFBGFBLF
124	AFDMPAOC AFHCOBLF
125	AFDMPAOC AFMSPBNM

TABLE B.5 (continued)

Identification Number	Cut Set
126	AFBGFABL AFDMPBTC
127	AFBGFABL AFDMPBOC
128	AFBGFABL AFBGFBBL
129	AFBGFABL AFHFB1BL
130	AFBGFABL AFADFBBL
131	AFBGFABL AFHFB2BL
132	AFBGFABL AFHFB2LF
133	AFBGFABL AFADFBLF
134	AFBGFABL AFBGFBLF
135	AFBGFABL AFHCOBLF
136	AFBGFABL AFMSPBNM
137	AFHFA1BL AFDMPBTC
138	AFHFA1BL AFDMPBOC
139	AFHFA1BL AFBGFBBL
140	AFHFA1BL AFHFB1BL
141	AFHFA1BL AFADFBBL
142	AFHFA1BL AFHFB2BL
143	AFHFA1BL AFHFB2LF
144	AFHFA1BL AFADFBLF
145	AFHFA1BL AFBGFBLF
146	AFHFA1BL AFHCOBLH

TABLE B.5 (continued)

Identification Number	Cut Set
147	AFHFA1BL AFMSPBNM
148	AFADFABL AFDMPBTC
149	AFADFABL AFDMPBOC
150	AFADFABL AFBGFBBL
151	AFADFABL AFHFB1BL
152	AFADFABL AFADFBBL
153	AFADFABL AFHFB2BL
154	AFADFABL AFHFB2LF
155	AFADFABL AFADFBLF
156	AFADFABL AFBGFBLF
157	AFADFABL AFHCOBLH
158	AFADFABL AFMSPBNM
159	AFHFA2BL AFDMPBTC
160	AFHFA2BL AFDMPBOC
161	AFHFA2BL AFBGFBBL
162	AFHFA2BL AFHFB1BL
163	AFHFA2BL AFADFBBL
164	AFHFA2BL AFHFB2BL
165	AFHFA2BL AFHFB2LF
166	AFHFA2BL AFADFBLF
167	AFHFA2BL AFBGFBLF

TABLE B.5 (continued)

Identification Number	Cut Set
168	AFHFA2BL AFHCOBLH
169	AFHFA2BL AFMSPBNM
170	AFHFA2LF AFDMPBTC
171	AFHFA2LF AFDMPBOC
172	AFHFA2LF AFBGFBBL
173	AFHFA2LF AFHFB1BL
174	AFHFA2LF AFADFBBL
175	AFHFA2LF AFHFB2BL
176	AFHFA2LF AFHFB2LF
177	AFHFA2LF AFADFBLF
178	AFHFA2LF AFBGFBLF
179	AFHFA2LF AFHCOBLF
180	AFHFA2LF AFMSPBNM
181	AFADFALF AFDMPBTC
182	AFADFALF AFDMPEOC
183	AFADFALF AFBGFBBL
184	AFADFALF AFHFB1BL
185	AFADFALF AFADFBBL
186	AFACFALF AFHFB2BL
187	AFADFALF AFHFB2LF
188	AFADFALF AFADFBLF

TABLE B.5 (continued)

Identification Number	Cut Set
189	AFACFALF AFBGFBLF
190	AFADFALF AFHCOBLH
191	AFADFALF AFMSPBNM
192	AFBGFALF AFDMPBTC
193	AFBGFALF AFDMPBOC
194	AFBGFALF AFBGFBBL
195	AFBGFALF AFHFB1BL
196	AFBGFALF AFADFBBL
197	AFBGFALF AFHFB2BL
198	AFBGFALF AFHFB2LF
199	AFBGFLAF AFADFBLF
200	AFBGFALF AFBGFBLF
201	AFBGFALF AFHCOBLH
202	AFBGFALF AFMSPBNM
203	AFHCOALH AFDMPETC
204	AFHCOALH AFDMPBOC
205	AFHCOALH AFBGFBBL
206	AFHCOALH AFHFB1BL
207	AFHCOALH AFADFBBL
208	AFHCOALH AFHFB2BL
209	AFHCOALH AFHFB2LF

TABLE B.5 (continued)

Identification Number	Cut Set
210	AFHCOALH AFADFBLF
211	AFHCOALH AFBGFBLF
212	AFHCOALH AFHCOBLH
213	AFHCOALH AFMSPBNM
214	AFMSPANM AFDMPETC
215	AFMSPANM AFDMPBOC
216	AFMSPANM AFBGFBBL
217	AFMSPANM AFHFB1BL
218	AFMSPANM AFADFBBL
219	AFMSPANM AFHFB2BL
220	AFMSPANM AFHFB2LF
221	AFMSPANM AFADFBLF
222	AFMSPANM AFBGFBLF
223	AFMSPANM AFHCOBLH
224	AFMSPANM AFMSPBNM
225	AFM15BFP AFDMPATC
226	AFM15BFP AFDMPAOC
227	AFM15BFP AFBGFABL
228	AFM15BFP AFHFA1BL
229	AFM15BFP AFADFABL
230	AFM15BFP AFHFA2BL

TABLE B.5 (continued)

Identification Number	Cut Set
231	AFM15BFP AFHFA2LF
232	AFM15BFP AFADFALF
233	AFM15BFP AFBGFALF
234	AFM15BFP AFHCOALH
235	AFM15BFP AFMSPANM
236	AFAPFBFO AFDMPATC
237	AFAPFBFO AFDMPAOC
238	AFAPFBFO AFBGFABL
239	AFAPFBFO AFHFA1BL
240	AFAPFBFO AFADFABL
241	AFAPFBFO AFHFA2BL
242	AFAPFBFO AFHFA2LF
243	AFAPFBFO AFADFALF
244	AFAPFBFO AFBGFALF
245	AFAPFBFO AFHCOALH
246	AFAPFBFO AFMSPANM
247	AFAFFBFO AFDMPATC
248	AFAFFBFO AFDMPAOC
249	AFAFFBFO AFBGFABL
250	AFAFFBFO AFHFA1BL
251	AFAFFBFO AFADFABL

TABLE B.5 (continued)

Identification Number	Cut Set
252	AFAFFBFO AFHFA2BL
253	AFAFFBFO AFHFA2LF
254	AFAFFBFO AFADFALF
255	AFAFFBFO AFBGFALF
256	AFAFFBFO AFHCOALH
257	AFAFFBFO AFMSPANM
258	AFM16BFO AFDMPATC
259	AFM16BFC AFDMPAOC
260	AFM16BFC AFBGFABL
261	AFM16BFC AFHFA1BL
262	AFM16BFC AFADFABL
263	AFM16BFC AFHFA2BL
264	AFM16BFC AFHFA2LF
265	AFM16BFC AFADFALF
266	AFM16BFC AFBGFALF
267	AFM16BFC AFHCDALH
268	AFM16BFC AFMSPANM
269	AFAPFATF AFDMPBTC
270	AFAPFATF AFDMPBOC
271	AFAPFATF AFBGFBBL
272	AFAPFATF AFHFB1BL

TABLE B.5 (continued)

Identification Number	Cut Set
273	AFAPFATF AFADFBBL
274	AFAPFATF AFHFB2BL
275	AFAPFATF AFHFB2LF
276	AFAPFATF AFADFBLF
277	AFAPFTAF AFBGFBLF
278	AFAPFATF AFHCOBLH
279	AFAPFATF AFMSPBNM
280	AFAFFAFO AFDMPBTC
281	AFAFFAFO AFDMPBOC
282	AFAFFAFO AFBGFBBL
283	AFAFFAFO AFHFB1BL
284	AFAFFAFO AFADFBBL
285	AFAFFAFO AFHFB2BL
286	AFAFFAFO AFHFB2LF
287	AFAFFAFO AFADFBLF
288	AFAFFAFO AFBGFBLF
289	AFAFFAFO AFHCOBLH
290	AFAFFAFO AFMSPBNM
291	AFAFFAFO AFAFFBFO
292	AFAFFAFO AFM16BFC
293	AFM16AFC AFDMPBTC

TABLE B.5 (continued)

Identification Number	Cut Set
294	AFM16AFC AFDMPBOC
295	AFM16AFC AFBGFBBL
296	AFM16AFC AFHFB1BL
297	AFM16AFC AFADFBBL
298	AFM16AFC AFHFB2BL
299	AFM16AFC AFHFB2LF
300	AFM16AFC AFADFBLF
301	AFM16AFC AFBGFBLF
302	AFM16AFC AFHCOBLH
303	AFM16AFC AFMSPBNM
304	AFM16AFC AFAFFBFO
305	AFM16AFC AFM16BFC
306	AFDUTABL AFDMPBTC
307	AFDUTABL AFDMPBOC
308	AFDUTABL AFBGFBBL
309	AFDUTABL AFHFB1BL
310	AFDUTABL AFADFBBL
311	AFDUTABL AFHFB2BL
312	AFDUTABL AFHFB2LF
313	AFDUTABL AFADFBLF
314	AFDUTABL AFBGFBLF

TABLE B.5 (continued)

Identification Number	Cut Set
315	AFDUTABL AFHCOBLH
316	AFDUTABL AFMSPBNM
317	AFDUTBBL AFDMPATC
318	AFDUTBBL AFDMPAOC
319	AFDUTBBL AFBGFABL
320	AFDUTBBL AFHFA1BL
321	AFDUTBBL AFADFABL
322	AFDUTBBL AFHFA2BL
323	AFDUTBBL AFHFA2LF
324	AFDUTBBL AFADFALF
325	AFDUTBBL AFBGFALF
326	AFDUTBBL AFHCOALH
327	AFDUTBBL AFMSPANM

APPENDIX C

COMMON CAUSE FAILURE ANALYSIS INFORMATION

Table C.1 lists the special conditions and Table C.2 lists the generic cause susceptibilities used in this thesis.

An eight character identification code was used to describe the possible common cause events. A detailed description of the code is given in Chapter 3. The code for the generic cause susceptibilities or special conditions may be deciphered by referring to Table C.3. The domains for the generic cause susceptibilities are shown in Figures C.1 through C.5. The groups for special conditions are determined by policies set up for each special condition. These policies are as follows:

1. Energy Source

   Each of the domains in Map IV is supplied by separate energy sources. Therefore the Common Link will be referred to by the letter J and the appropriate domain number of the component from Map IV.

2. Manufacturer

   No attempt is made at this stage of the design to identify manufacturers. Because of this, the Common Link, Manufacturer, will be omitted from the common cause analysis.

3. Installation Contractor

   Each of the domains in Map IV will be installed by an independent installation crew. The quality assurance program should ensure that this procedure is followed. Therefore,

TABLE C.1

SPECIAL CONDITIONS RESULTING IN DEPENDENCE BETWEEN COMPONENTS

Symbol	Special Condition	Example
J	Energy Source	Same power supply
U	Installation Contractor	Same contractor
M	Maintenance	Incorrect procedure Inadequately trained personnel
X	Manufacturer	Inadequate quality control
K	Operator or operation	Disabled or overstressed Faulty operating procedures

TABLE C.2

GENERIC CAUSE SUSCEPTIBILITIES

Symbol	Generic Cause	Example Sources
G	Grit	Airborne dust, smoke from a sodium fire
I	Impace	Severe pressure change, missiles, structural failure, earthquake
P	Pressure	Out-of-tolerance system changes (fan overspeed, flow blockage), explosion
S	Stress	Mechanical stress at weld region of metals
T	Temperature (High)	Fire, collection of radioactive isotopes
V	Vibration	Machinery in motion, earthquake
A	Corrosion (Acid)	Acid used in maintenance for removing rust and cleaning
O	Corrosion (Oxidation)	Moist atmosphere
X	Temperature (Low)	Heating system failure

TABLE C.3

GENERIC CAUSE SUSCEPTIBILITY AND
SPECIAL CONDITION DESCRIPTION CODES

Code	Description
CORA	CORROSION (ACID)
CORO	CORROSION (OXIDATION)
ENSO	ENERGY SOURCE
GRIT	GRIT
IMPT	IMPACT
INCO	INSTALLATION CONTRACTOR
MAIN	MAINTENANCE
MANU	MANUFACTURER
MOIS	MOISTURE
OPOP	OPERATOR OR OPERATION
PRES	PRESSURE
STRS	STRESS
TEMH	TEMPERATURE (HIGH)
TEML	TEMPERATURE (LOW)
VIBR	VIBRATION

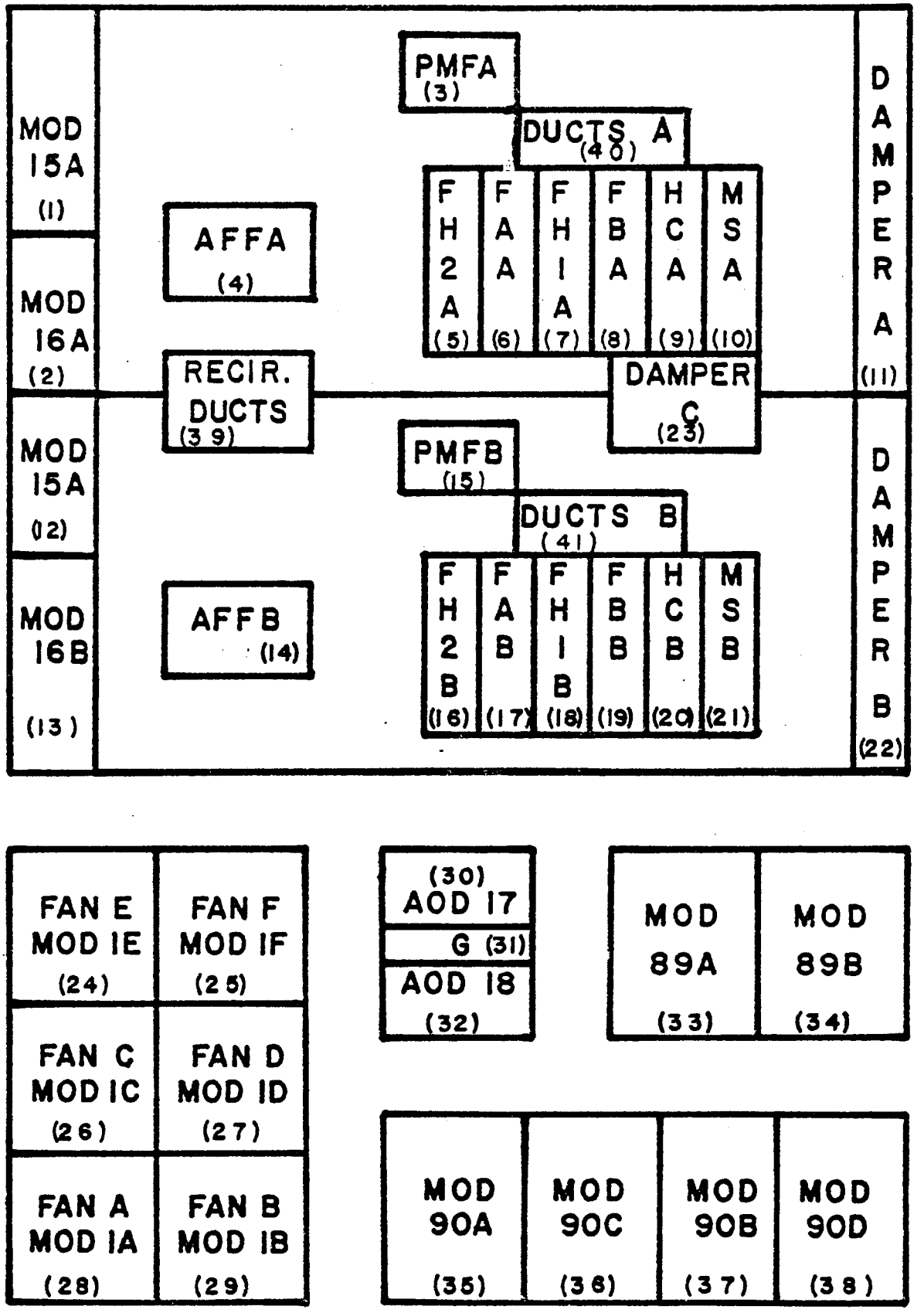


Figure C.1. Domain Map for Generic Cause Susceptibilities Impact, Corrosion (Acid), and Stress.

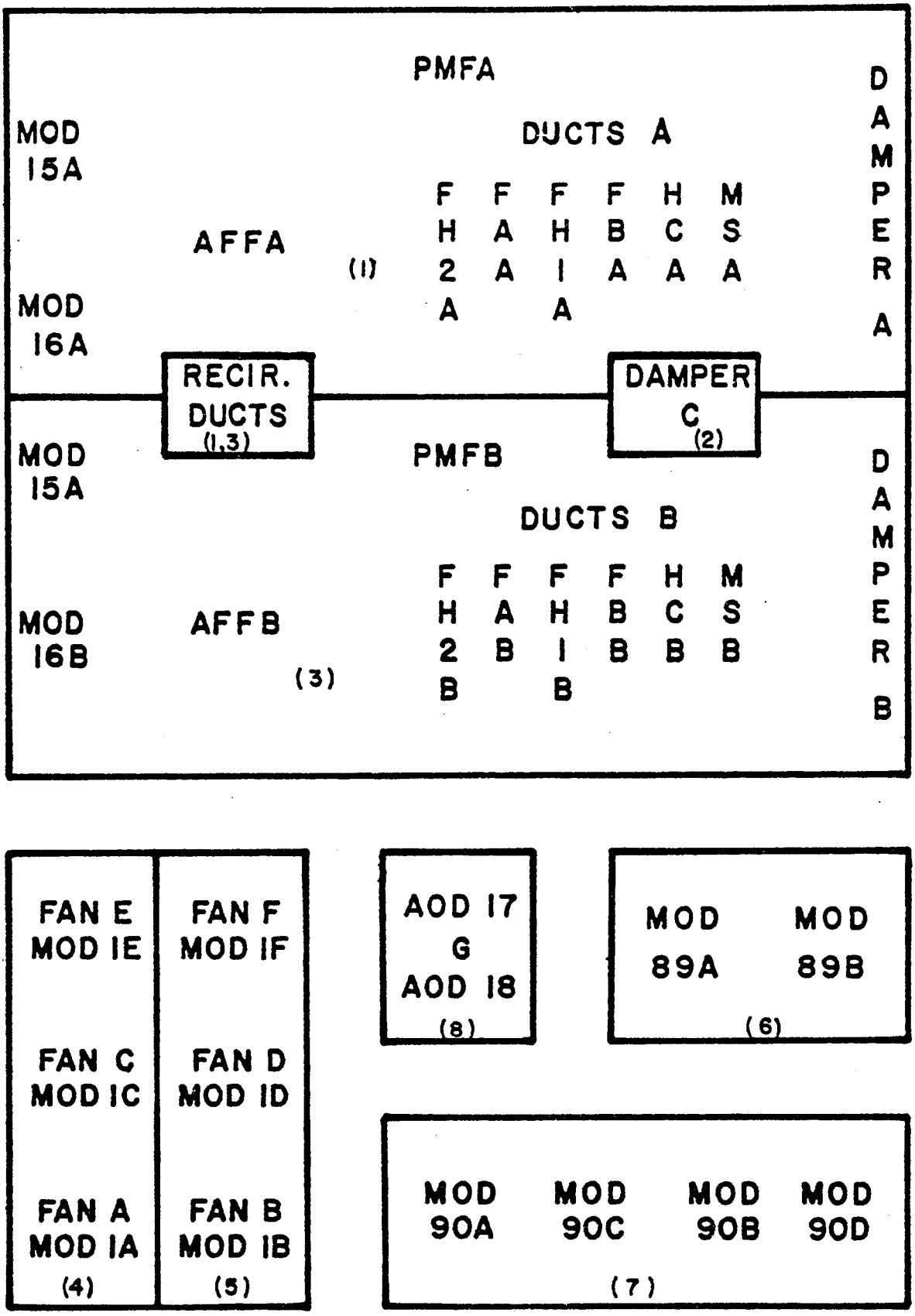


Figure C.2. Domain Map for Generic Cause Susceptibilities Vibration and Temperature (High).

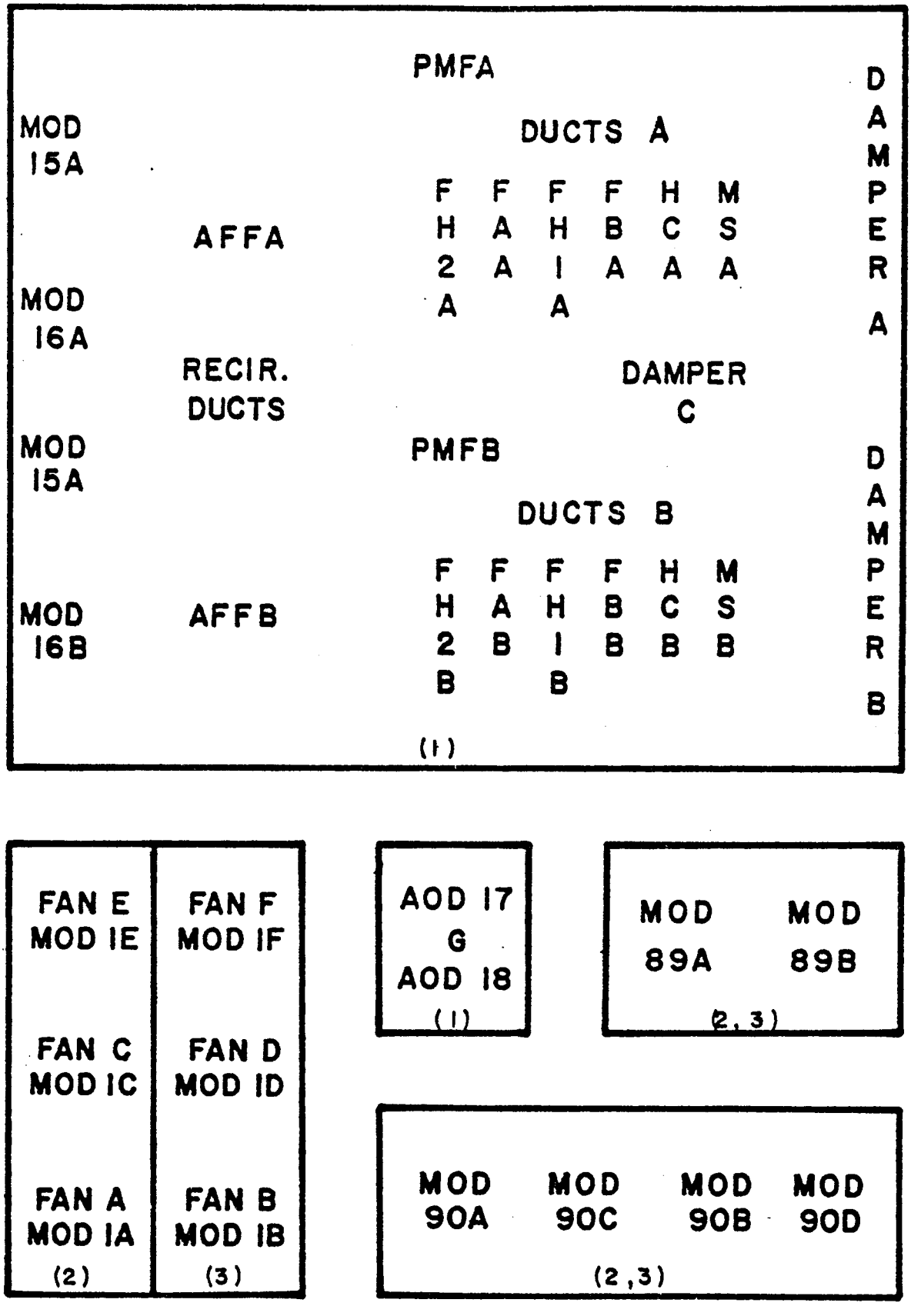


Figure C.3. Domain Map for Generic Cause Susceptibility Pressure.

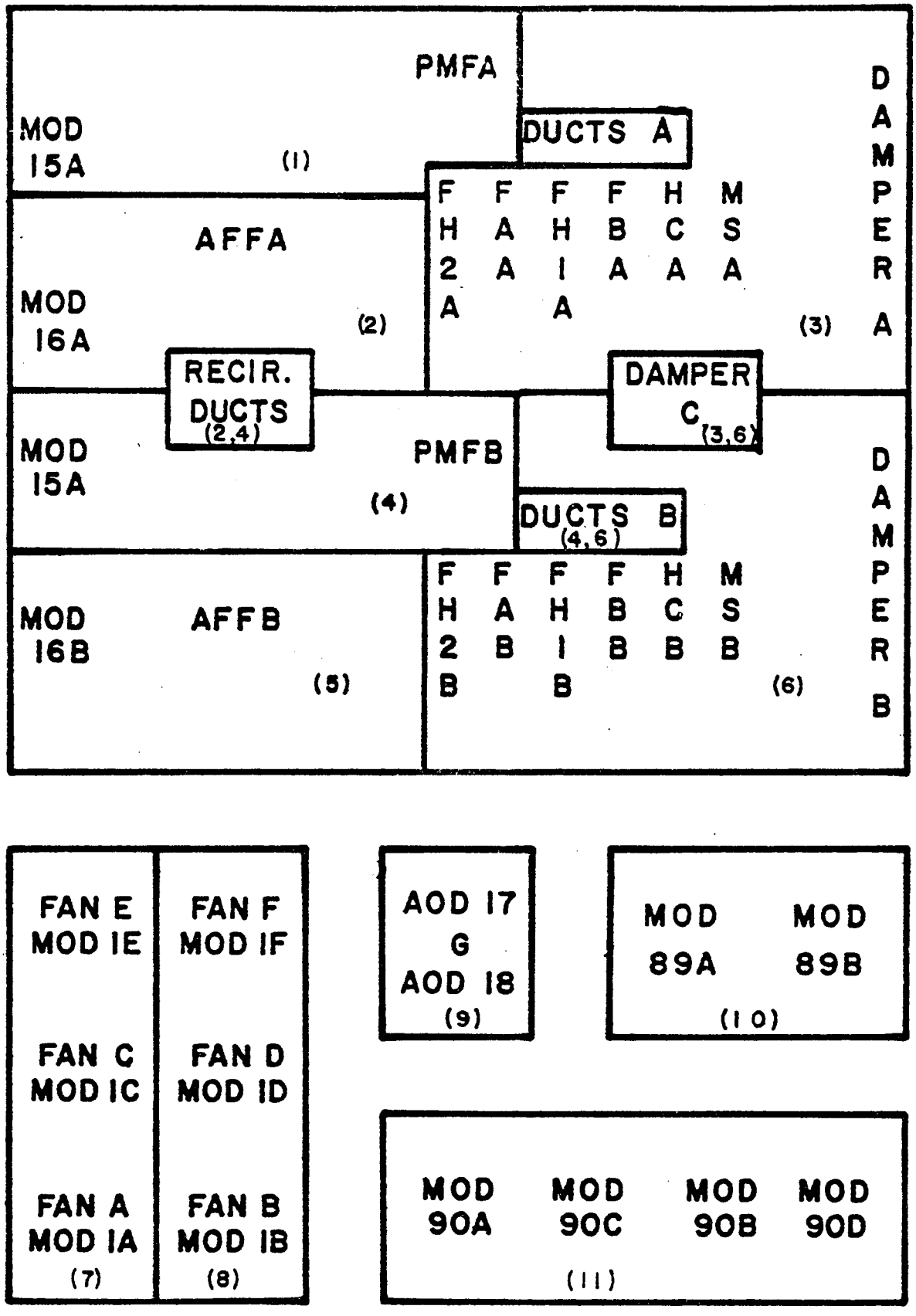


Figure C.4. Domain Map for Generic Cause Susceptibilities Grit, Moisture, and Corrosion (Oxidation).

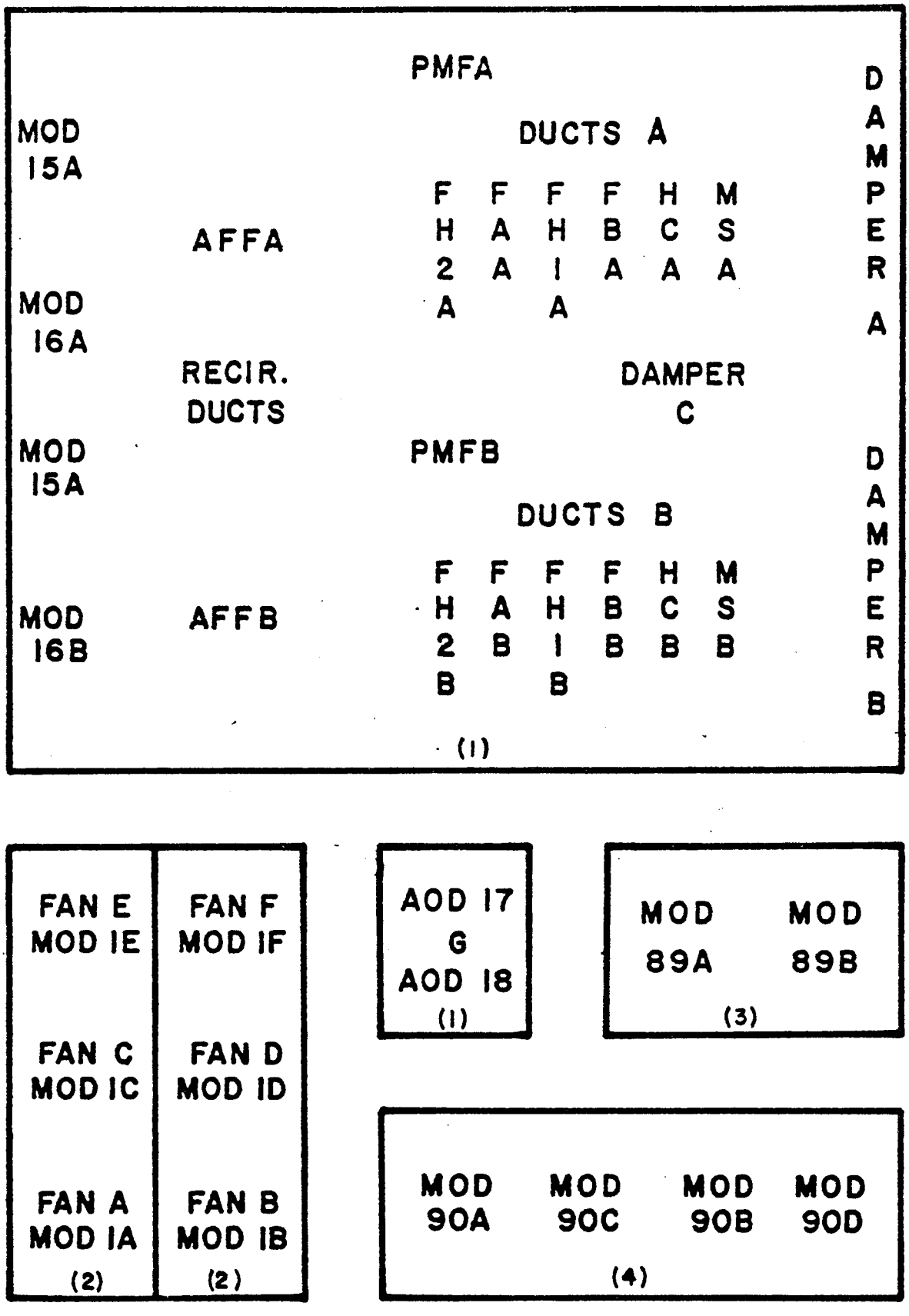


Figure C.5. Domain Map for Generic Cause Susceptibility Temperature (Low).

the Common Link will be referred to by the letter U and the appropriate domain number of the component from Map IV.

4. Maintenance

The Annulus Filtration System components in Train A and Train B will be maintenanced by crews (1) and (2) respectively. Crew (1) will also maintenance dampers AOD 17, Gravity damper, and AOD 18. Annulus Cooling System (ACS) Fans 1A, 1C, and 1E will be maintenanced by crew (3); and Fans 1B, 1D, and 1F will be maintenanced by crew (4). ACS dampers MOD 90A, MOD 90C, and MOD 89A will be maintenanced by crew (3); and MOD 90B, MOD 90D, and MOD 89B will be maintenanced by crew (4). Therefore, the Common Link will be referred to by the letter M and the appropriate number of the crew assigned to the component.

5. Operator or Operation

Four sets of operators will be assigned components corresponding to those assigned to the four maintenance crews. Therefore, the Common Link will be referred to by the letter K and the appropriate number of the crew assigned to the component.

The common cause events identified are listed in Table C.4. Three of these are due to the generic cause susceptibility "pressure." Figure C.6 shows the three domains identified for "pressure." Possible mechanisms for "pressure" are fan overspeed, flow blockage, or tornado.

Two special conditions were identified in the common cause failure analysis. They are "maintenance" and "operator or operation."

TABLE C.4

LIST OF COMMON CAUSE EVENTS

Identification Number	Event
328	MAINCS03
329	MAINCS04
330	OPOPCS03
331	OPOPCS04
332	PRESL001
334	PRESL002
335	PRESL003

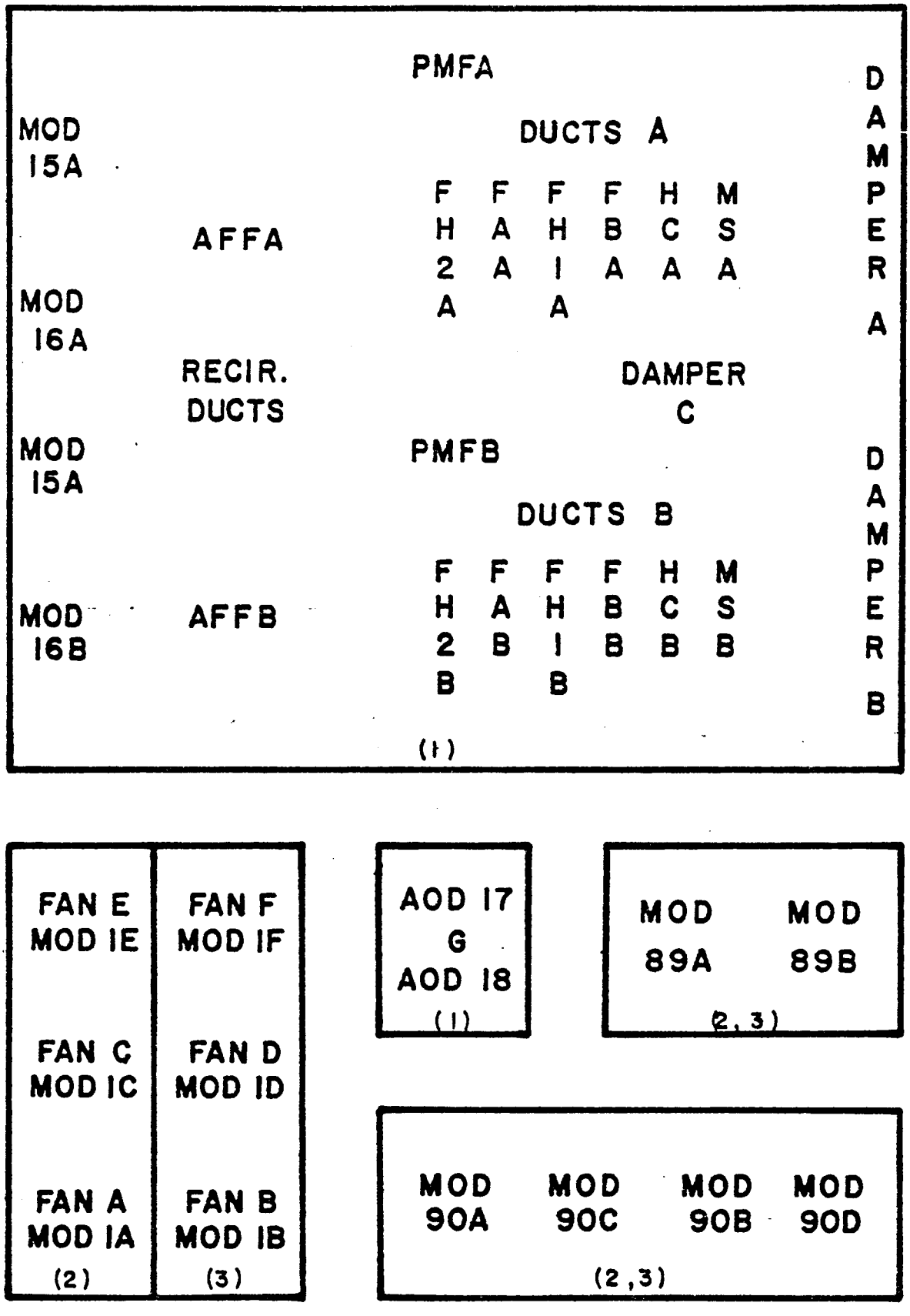


Figure C.6. Map Showing Domains Identified for "Pressure" in the CCFA.

Each of these was identified in two common cause events. Figure C.7 shows the groups of components affected by the special conditions. The lines in the figure reflect the policies given above. Possible mechanisms are use of incorrect procedure or inadequately trained personnel. Possible mechanisms for "operator or operation" are faulty operating procedures, inadequately trained personnel, or fatigue.

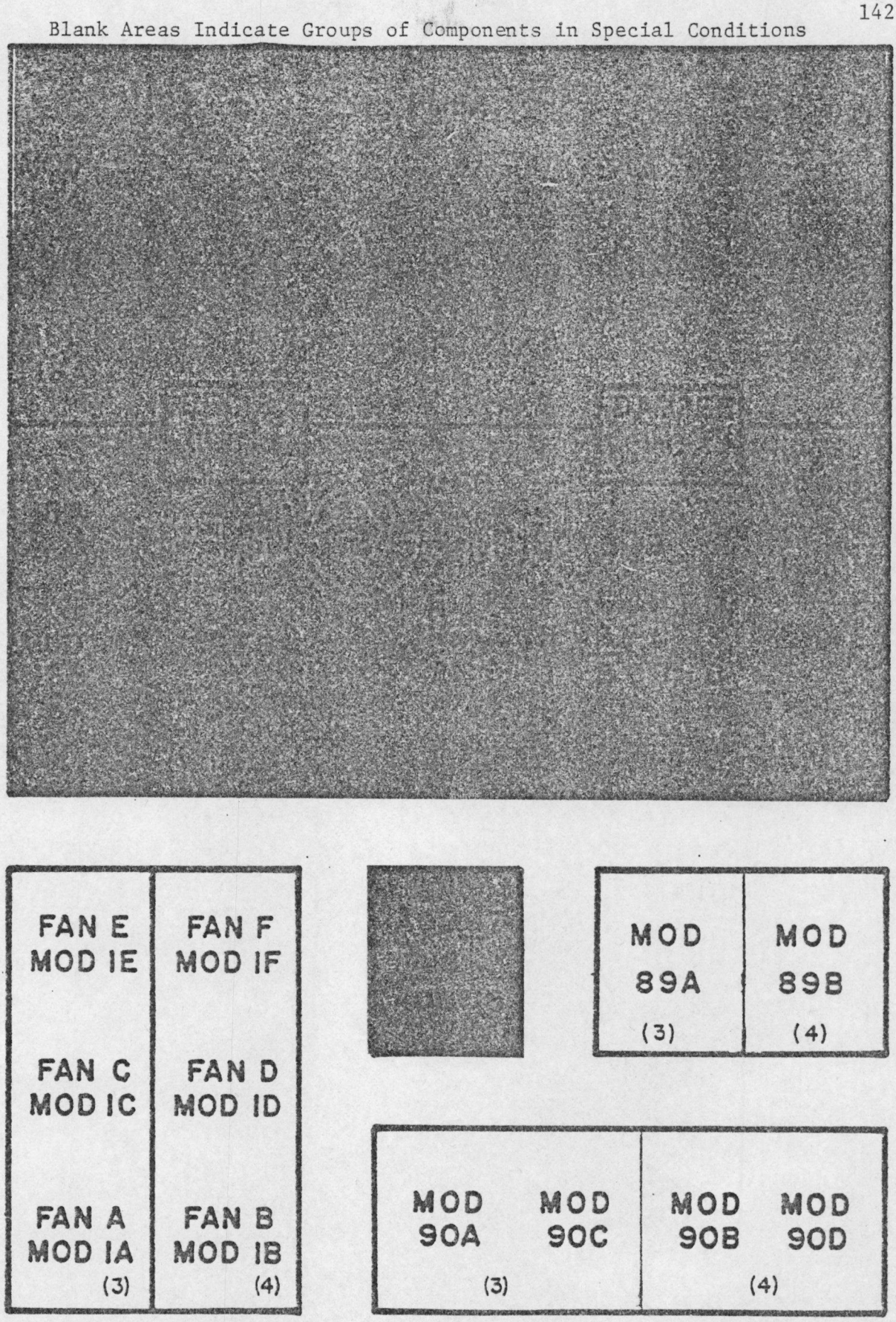


Figure C.7. Map Showing the Groups of Components Identified for Special Conditions in the CCFA.

APPENDIX D

QUANTITATIVE DATA

The input data for the annulus filtration system analysis is given in Table D.1. This data includes all event names used in the analysis, the initial failed probability of the events, the failure rate of each event before a DBA, the failure rate of each event after a DBA, and the repair time of each event.

TABLE D.1

QUANTITATIVE EVENT DATA

Event Descriptor	Initial Failed Probability	Failure Rate (1/hr)	Repair Time Before DBA (hr)	Repair Time After DBA (hr)
ACCSFATN	0.0	1×10^{-6}	96	24
ACCSFBTN	0.0	1×10^{-6}	96	24
ACCSFCTN	0.0	1×10^{-6}	96	24
ACCSFDTN	0.0	1×10^{-6}	96	24
ACCSFETN	0.0	1×10^{-6}	96	24
ACCSFFTN	0.0	1×10^{-6}	96	24
ACFACECN	0.0	1×10^{-4}	4	2
ACFBDFCN	0.0	1×10^{-4}	4	2
ACM89ATP	1.94×10^{-2}	1×10^{-4}	20	5
ACM89BTP	1.94×10^{-3}	1×10^{-4}	20	5
ACM90ATP	0.0	1×10^{-4}	20	5
ACM90BTP	0.0	1×10^{-4}	20	5
ACM90CTP	0.0	1×10^{-4}	20	5
ACM90DTP	0.0	1×10^{-4}	20	5
ACMACECS	3.98×10^{-4}	1×10^{-4}	4	2
ACMBDFCS	3.98×10^{-4}	1×10^{-4}	4	2
ACMODATP	1.94×10^{-4}	1×10^{-4}	20	5
ACMODBTP	1.94×10^{-4}	1×10^{-4}	20	5

TABLE D.1 (continued)

Event Descriptor	Initial Failed Probability	Failure Rate (1/hr)	Repair Time Before DBA (hr)	Repair Time After DBA (hr)
ACMODCTP	1.94×10^{-4}	1×10^{-4}	20	5
ACMODDTP	1.94×10^{-4}	1×10^{-4}	20	5
ACMODETP	1.94×10^{-4}	1×10^{-4}	20	5
ACMODFTP	1.94×10^{-4}	1×10^{-4}	20	5
AC89ACOP	3.78×10^{-4}	1×10^{-4}	4	2
AC89BDOP	3.78×10^{-4}	1×10^{-4}	4	2
AC90ACOP	3.98×10^{-4}	1×10^{-4}	4	2
AC90BDOP	3.98×10^{-4}	1×10^{-4}	4	2
AFADFABL	3.59×10^{-4}	1×10^{-5}	0.0	0.0
AFADFALF	3.59×10^{-4}	1×10^{-5}	0.0	0.0
AFADFBBL	3.59×10^{-4}	1×10^{-5}	0.0	0.0
AFADFBLF	3.59×10^{-4}	1×10^{-5}	0.0	0.0
AFADI1FC	1.94×10^{-4}	1×10^{-4}	20	5
AFADI1NO	3.98×10^{-4}	1×10^{-4}	4	2
AFADI2OP	3.98×10^{-4}	1×10^{-4}	4	2
AFADI2TP	1.94×10^{-4}	1×10^{-4}	20	5
AFAD17A0	3.98×10^{-4}	1×10^{-4}	4	2
AFAD17FC	1.94×10^{-4}	1×10^{-4}	20	5
AFAD1700	0.0	0.0	0.0	.0001
AFAD17OP	3.98×10^{-4}	1×10^{-4}	4	2

TABLE D.1 (continued)

Event Descriptor	Initial Failed Probability	Failure Rate (1/hr)	Repair Time Before DBA (hr)	Repair Time After DBA (hr)
AFAD17TP	0	1×10^{-4}	20	5
AFAD18FC	0	1×10^{-4}	20	5
AFAD18NO	0	1×10^{-4}	4	2
AFADFABL	1.94×10^{-4}	1×10^{-5}	20	0
AFADFALF	9.86×10^{-5}	1×10^{-5}	20	0
AFAFFAAT	3.98×10^{-4}	1×10^{-4}	4	0
AFAFFAFO	8.54×10^{-2}	1×10^{-4}	100	0
AFAFFAOT	0	0	0	0
AFAFFBAO	3.52×10^{-2}	1×10^{-4}	0	0
AFAFFBFO	3.52×10^{-2}	1×10^{-4}	0	0
AFAFFBOT	0	0	0	0
AFANNBLI	0	0	0	.00001
AFAPFAAR	0	0	0	.01
AFAPFACR	3.98×10^{-4}	1×10^{-4}	4	0
AFAPFATF	8.31×10^{-4}	1×10^{-5}	96	0
AFAPFBAO	3.52×10^{-2}	1×10^{-4}	0	0
AFAPFBFO	3.52×10^{-2}	1×10^{-4}	0	0
AFAPFBOT	0	0	0	.01
AFAPFBTF	8.31×10^{-4}	1×10^{-5}	96	0
AFBGFABL	1.94×10^{-4}	1×10^{-5}	20	0

TABLE D.1 (continued)

Event Descriptor	Initial Failed Probability	Failure Rate (1/hr)	Repair Time Before DBA (hr)	Repair Time After DBA (hr)
AFBGFALF	9.86×10^{-5}	1×10^{-5}	10	0
AFBGFBBL	3.59×10^{-3}	1×10^{-5}	0	0
AFBGFBLF	3.59×10^{-3}	1×10^{-5}	0	0
AFDHEDBL	0	0	0	0
AFDMPAFP	1.94×10^{-3}	1×10^{-4}	20	0
AFDMPAOC	0	0	0	.01
AFDMPAOD	0	0	0	.01
AFDMPATC	3.98×10^{-5}	1×10^{-5}	4	0
AFDMPBFP	1.94×10^{-4}	1×10^{-4}	20	0
AFDMPBOC	0	0	0	.01
AFDMPBOD	0	0	0	.01
AFDMPBOT	0	0	0	.01
AFDMPBTC	3.59×10^{-2}	1×10^{-5}	0	0
AFDMPCFC	1.94×10^{-4}	1×10^{-5}	20	0
AFDMPCOO	0	0	0	.01
AFDMPCOP	0	0	0	.01
AFDMPCTP	1.94×10^{-4}	1×10^{-5}	20	0
AFDUSBLI	0	0	0	.00001
AFDUTABL	1.94×10^{-5}	1×10^{-6}	20	0
AFDUTBBL	3.6×10^{-4}	1×10^{-6}	0	0

TABLE D.1 (continued)

Event Descriptor	Initial Failed Probability	Failure Rate (1/hr)	Repair Time Before DBA (hr)	Repair Time After DBA (hr)
AFGDPGFC	1.94×10^{-3}	1×10^{-4}	20	5
AFHCOALH	1.94×10^{-4}	1×10^{-5}	20	0
AFHCOBLH	3.59×10^{-2}	1×10^{-5}	0	0
AFHFA1BL	1.94×10^{-4}	1×10^{-5}	20	0
AFHFA2BL	1.94×10^{-4}	1×10^{-5}	20	0
AFHFA2LF	3.59×10^{-3}	1×10^{-5}	40	0
AFHFB1BL	3.59×10^{-3}	1×10^{-5}	0	0
AFHFB2BL	3.59×10^{-3}	1×10^{-5}	0	0
AFHFB2LF	3.59×10^{-3}	1×10^{-5}	0	0
AFMSPANM	1.94×10^{-4}	1×10^{-5}	20	0
AFMSPBNM	3.59×10^{-3}	1×10^{-5}	0	0
AFM15AAC	3.98×10^{-4}	1×10^{-4}	4	0
AFM15ACO	3.98×10^{-4}	1×10^{-4}	4	0
AFM15AFP	1.94×10^{-4}	1×10^{-4}	20	0
AFM15ALO	0	0	0	.01
AFM15AOC	0	0	0	.01
AFM15ATC	1.94×10^{-3}	1×10^{-4}	20	0
AFM15BAO	3.52×10^{-2}	1×10^{-4}	0	0
AFM15BAP	3.52×10^{-2}	1×10^{-4}	0	0
AFM15BCO	3.98×10^{-4}	1×10^{-4}	4	0

TABLE D.1 (continued)

Event Descriptor	Initial Failed Probability	Failure Rate (1/hr)	Repair Time Before DBA (hr)	Repair Time After DBA (hr)
AFM15BFP	3.52×10^{-2}	1×10^{-4}	0	0
AFM15BL0	0	0	0	.01
AFM15B00	0	0	0	.01
AFM15B0P	0	0	0	.01
AFM15BTP	3.52×10^{-2}	1×10^{-4}	0	0
AFM16AAN	3.98×10^{-4}	1×10^{-4}	4	0
AFM16AAP	3.98×10^{-4}	1×10^{-4}	4	0
AFM16AC0	3.98×10^{-4}	1×10^{-4}	4	0
AFM16AFC	1.94×10^{-3}	1×10^{-4}	20	0
AFM16AFP	1.94×10^{-3}	1×10^{-4}	20	0
AFM16AL0	0	0	0	.01
AFM16A0P	0	0	0	.01
AFM16A00	0	0	0	.01
AFM16ATP	1.94×10^{-4}	1×10^{-4}	20	0
AFM16BAP	3.52×10^{-2}	1×10^{-4}	0	0
AFM16BA0	3.52×10^{-2}	1×10^{-4}	0	0
AFM16BC0	3.52×10^{-2}	1×10^{-6}	0	0
AFM16BFC	3.52×10^{-2}	1×10^{-4}	0	0
AFM16BFP	3.52×10^{-2}	1×10^{-4}	0	0
AFM16BL0	0	0	0	.01

TABLE D.1 (continued)

Event Descriptor	Initial Failed Probability	Failure Rate (1/hr)	Repair Time Before DBA (hr)	Repair Time After DBA (hr)
AFM16B0P	0	0	0	.01
AFM16B00	0	0	0	.01
AFM16BTP	3.52×10^{-2}	1×10^{-4}	0	0
AFP0FSLC	0	0	0	.000001
AFP0NSLC	0	0	0	.000001
AFRDUCBL	1.94×10^{-5}	1×10^{-6}	20	5
AFRDUCT0	1.94×10^{-4}	1×10^{-5}	20	5
01	0	0	0	.0001
02	0	0	0	.0001
03	0	0	0	.0001
04	0	0	0	.0001
05	0	0	0	.0001
06	0	0	0	.0001
07	0	0	0	.0001
08	0	0	0	.0001
09	0	0	0	.0001
010	0	0	0	.0001
011	0	0	0	.0001
MAINCS03	0	1.39×10^{-9}	0	0
MAINCS04	0	1.39×10^{-9}	0	0

TABLE D.1 (continued)

Event Descriptor	Initial Failed Probability	Failure Rate (1/hr)	Repair Time Before DBA (hr)	Repair Time After DBA (hr)
0P0PCS03	0	1.39×11^{-9}	0	0
0P0PCS04	0	1.39×10^{-9}	0	0
PRESL001	0	1×10^{-8}	0	0
PRESL002	0	1×10^{-8}	0	0
PRESL003	0	1×10^{-8}	0	0

APPENDIX E

LISTS OF IMPORTANT CUT SETS

Using the SUPERPOCUS computer program, those cut sets that are most likely to be unavailable at the beginning of a DBA were determined. A list of these cut sets and their respective unavailabilities are given in Table E.1.

Using the KITT-2 computer program those cut sets that are most likely to be unreliable at the end of the analysis period were determined. A list of these cut sets and their respective unreliabilities are given in Table E.2.

TABLE E.1

LIST OF IMPORTANT CUT SETS AT
THE OCCURRENCE OF A DBA

Identification Number (same as Table B.5)	Cut Set	Unreliability	Percent of System Unavailability Accounted for by the Cut Sets Listed
2	AFAD18FC	.00200	
3	AFAD17TP	.00200	
6	ACM90ATP	.00200	
7	ACM90DTP	.00200	
16	ACM90DTP	.00200	
17	ACM90BTP	.00200	
259	AFM16BFC AFDMPAOC	.00070	
248	AFAFFBFO AFDMPAOC	.00070	
237	AFAPFBFO AFDMPAOC	.00070	90%
226	AFM15BFP AFDMPAOC	.00070	
292	AFAFFAFO AFM16BC	.00069	
291	AFAFFAFO AFAFFBFO	.00069	
23	AFAD18NO	.00040	
22	AFAD17OP	.00040	
21	AC90ACOP	.00040	
20	ACFACECN	.00040	
19	ACFBDFCN	.00040	
18	AC90BDOP	.00040	

TABLE E.1 (continued)

Identification Number (same as Table B.5)	Cut Set	Unreliability	Percent of System Unavailability Accounted for by the Cut Sets Listed
15	AFRDUCT0	.00020	
305	AFM16AFC AFM16BFC	.00015	
304	AFM16AFC AFAFFBF0	.00015	

TABLE E.2

LIST OF IMPORTANT CUT SETS AT
END OF THE ANALYSIS PERIOD

Identification Number (same as Table B.5)	Cut Set	Unreliability	Percent of System Unreliability Accounted for by the Cut Sets Listed
2	AFAD18FC	.0695	
3	AFAD17TP	.0695	
6	ACM90ATP	.0695	
7	ACM90CTP	.0695	
16	ACM90DTP	.0695	
17	ACM90BTP	.0695	
18	AC90BD0P	.0695	
19	ACFBDFCN	.0695	
20	ACFACECN	.0695	
21	AC90AC0P	.0695	
22	AFAD170P	.0695	
23	AFAD18N0	.0695	90%
291	AFAFFAF0 AFAFFBF0	.0092	
292	AFAFFAF0 AFM16BFC	.0092	
304	AFM16AFC AFAFFBF0	.0092	
305	AFM16AFC AFM16BFC	.0092	
15	AFRDUCT0	.0071	
226	AFM15BFP AFDMPA0C	.0010	

TABLE E.2 (continued)

Identification Number (same as Table B.5)	Cut Set	Unreliability	Percent of System Unreliability Accounted for by the Cut Sets Listed
237	AFAPFBF0 AFDMPA0C	.0010	
248	AFAFFBF0 AFDMPA0C	.0010	
281	AFAFFAF0 AFDMPB0C	.0010	
294	AFM16AFC AFDMPB0C	.0010	

APPENDIX F

IMPORTANT DETAILS OF THE QUANTITATIVE ANALYSIS

The sytem characteristic of interest in this analysis is the dependability of the system over the mission. The dependability of a system is the probability the system works upon demand and then does not fail during the mission. This quantity is calculated by multiplying the system availability upon demand by the system reliability over the mission given the system is working initially.

The system characteristics mentioned above are determined using the computer programs SUPERPOCUS and KITT-2. The input to these programs consists of a list of minimal cut sets, and a list of common cause events represented as one event cut sets. The minimal cut sets are made up on independent component failures due to either a hardware failure or an operator error. Hardware failures of components are described by an initial failed probability, a failure rate, and if the component is repairable, a repair time. Three methods are used to handle those independent component failures caused by operators. If the operator introduces failures to the component then a failure rate and a repair time are assigned to the event. For example, an operator may close a damper when it is supposed to remain open. On the other hand, if the operator fails to perform an assigned task, then a probability of occurrence is assigned to the event. For example, an operator may fail to manually close a motor operated damper after its automatic controller has failed to close it. Finally, failure rates are

assigned to those independent component failures caused by operators that are also one event cut sets.

Dependent failures of components found in the common cause failure analysis are identified by either a special condition or a generic cause susceptibility in a particular domain. The quantitative reliability characteristic of a special condition is the probability of the TOP event occurring by that special condition. Since the common cause events are input as one event cut sets, their probability of occurrence must be approximated in KITT-2 by inputting an appropriate failure rate and making the event nonrepairable. This is required to obtain the correct effect on the system reliability. The generic cause susceptibilities must be input into KITT-2 as a failure rate and assumed to be nonrepairable. The common cause failures identified have no effect on the outcome of the quantitative analysis due to the large number of one and two event minimal cut sets that are relatively far more probable. Many systems have no one or two event minimal cut sets and few three event minimal cut sets.[1,2] In that case the results of a common cause failure analysis could dominate the system's quantitative results. The common cause candidates for this analysis were not identified since no useful information would have been obtained and their determination could have been quite expensive.

Since a DBA is equally likely to occur at any time during a period of normal operation, the probability of system failure upon demand is determined by finding the average unavailability of the system for a 30 day period during normal operation. A 30 day mission is chosen because the two filter fan units alternate on a 30 day cycle. The assumption is made that filter-fan unit B has just shut

down and that unit A has just begun working. Using the SUPERPOCUS computer program the system unavailability at different tims during a 30 day cycle was obtained, and from these values an integral average unavailability of the system of 0.021 (or availability of .979) was determined.

The Nuclear Regulatory Commission requires that the AFS be designed to operate for a 30 day period after the occurrence of a DBA.[3] The probability the AFS will fail during this 30 day mission given the system is initially working is determined by finding the system unreliability over the mission given the system is initially working. This system unreliability is determined using the KITT-2 computer program, and the system reliability is determined by subtracting the unreliability value from one. Input to the KITT-2 computer program for each basic event consist of the probability the event is failed given the system is initially working, and the appropriate failure rates and mean down times. The probability an event is failed given the system is initially working is described by the probability the system is initially working given the event is failed times the probability the event is unavailable divided by the probability the system is initially working. Since the probability the system is initially working given the event is failed divided by the probability the system is initially working is less than one but usually close to one, the probability the event is failed given the system is initially working can be conservatively approximated by the probability the event is unavailable. The probability the event is unavailable, except for events of one event cut sets, is approximated by using the integral average unavailabilities of each basic event

during a 30 day normal operating period since a DBA is equally likely to occur at any time during a period of normal operation. The probability a one event cut set is failed given the system is working is zero. A system unreliability of .668 (or reliability of .332) was obtained from the KITT-2 computer run.

Multiplying the system reliability over the mission obtained from KITT-2 by the system availability upon demand obtained from SUPERPOCUS, a system dependability of .325 is determined. Therefore, the undependability of the system is .675.

The uncertainty in the undependability value is determined using the SAMPLE computer program and hand calculations. The undependability can be approximated by the addition of the unavailability of the system at the beginning of a DBA plus the unreliability of the system over the mission given the system is initially working. Therefore, the uncertainty in the undependability is found by combining the uncertainty of the unavailability and unreliability values. This combination is accomplished by adding the variances of the two values determined from the SAMPLE runs, and then taking the square root of this sum to obtain the standard deviation of the undependability. The assumption is made here that the unavailability and the unreliability distributions determined by SAMPLE are normal distributions.[4] Also, the assumption is made that the unavailability is adequately approximated by the minimal cut sets listed in Table E.1 and that the unreliability is adequately approximated by the minimal cut sets listed in Table E.2. A standard deviation of 0.0225 was obtained for the unavailability value and a standard deviation of 0.266 was obtained for the unreliability value. Taking the square root of the

sum of the variances of these two values a standard deviation of 0.267 is obtained for the undependability value. A 95 percent bound is then obtained by adding and subtracting two standard deviations to the undependability value of 0.675 giving a bound from 0.141 to 1.0. Since the upper bound obtained is 1.0 the confidence bound includes all the upper portion of the system undependability distribution. Therefore, the percent chance that the system will have an actual undependability greater than 0.141 over a 30 day mission after the occurrence of a DBA is 97.5.

APPENDIX G

GLOSSARY OF TERMS

Fault Tree. A graphical representation of the failure logic of a system associated with a particular TOP event.

TOP Event. Describes the problem being addressed by an analysis.

System Component. The smallest unit of the system as developed in the system logic model. A component may be a single item, such as a relay or a fuse, or a complex entity, such as the flux monitoring system of a nuclear reactor scram system. Specific action of a human operator may be treated as a component. The system component defines the level of resolution of the analysis.

Basic Event. A malfunction (failure mode) of a system component, for example, "damper fails closed." A basic event is a constituent of a specific failure logic model, such as a fault tree.

Minimal Cut Set. A group of basic events that are collectively sufficient to cause system failure. The occurrence of each basic event in the minimal cut set is necessary if the system failure is the result of the failure of the minimal cut set in question. A minimal cut set is failed if and only if all the basic event in that minimal cut set exist at the same time.

Common Cause Failure. Multiple failure of system components that results in a specified system failure due to one specific condition or cause of failure.

Common Cause Event. A secondary failure cause that is common to all the basic events in one or more component minimal cut sets.

Common Cause Candidate. A minimal cut set which has a potential for failure by a single generic cause of failure. The identification of common cause candidates is restricted to two-basic event or larger component minimal cut sets. One-basic event minimal cut sets, also termed single failures, do not satisfy this definition of a common candidate.

Special Condition. A characteristic of a basic event such that if all the basic events in a minimal cut set share this special condition (regardless of the location of the basic events in the system), the minimal cut is a common cause candidate.

Generic Cause Susceptibilities. A characteristic of a basic event such that if all the basic events in a minimal cut set share this generic cause susceptibility and have a common location, the minimal cut set is a common cause candidate.

Common Location. An area of a building, etc., where a single occurrence of a given generic cause could affect all components within.

Susceptibility. Capability of a generic cause of failure to result in the occurrence of a basic event.

LIST OF REFERENCES

LIST OF REFERENCES

1. Wagner, D. P., "A Procedure for Qualitative Common Cause Failure Analysis of Complex Systems," Master's Thesis, The University of Tennessee, Knoxville, August 1977.

2. Rooney, J. J., "An Automated Procedure for Qualitative Common Cause Failure Analysis of Complex Systems," Master's Thesis, The University of Tennessee, Knoxville, August 1978.

3. Nuclear Regulatory Commission, Regulatory Guide 1.52, Washington, Government Printing Office, March 1978.

4. Walpole, R. E., and Myers, R. H., Probability and Statistics for Engineers and Scientists, New York, Macmillan Publishing Co., Inc., 1972.

VITA

Vernon Hart Guthrie was born in Vicksburg, Mississippi, on November 10, 1954. He is the son of Mr. and Mrs. William Shreve Guthrie, Jr. He was raised in Port Gibson, Mississippi. After graduating from Chamberlain-Hunt Academy in May 1973, he entered Louisiana State University. After two years at Louisiana State University he transferred into the undergraduate program in Nuclear Engineering at Mississippi State University, Starkville, where he received the Bachelor of Science degree in May 1977.

Vernon entered the graduate program in Nuclear Engineering at The University of Tennessee, Knoxville, in June 1977. After receiving the Master of Science degree in June 1979, he will begin work for Union Carbide Corporation in Oak Ridge, Tennessee.