The Light company Houston Lighting & Power P.O. Box 1700 Houston, Texas 77001 (713) 228-9211

October 21, 1985
ST-HL-AE-1413
File No.: G9.17

Mr. George W. Knighton, Chief
Licensing Branch No. 3
Division of Licensing
U. S. Nuclear Regulatory Commission
Washington, DC 20555

South Texas Project
Units 1 and 2
Docket Nos. STN 50-498, STN 50-499
Responses to DSER/FSAR Items
AFWS Reliability, Appendix 10A

Dear Mr. Knighton:

The attachment enclosed provides STP's response to Draft Safety Evaluation Report (DSER) or Final Safety Analysis Report (FSAR) items.

The item number listed below corresponds to those assigned on STP's internal list of items for completion which includes open and confirmatory DSER items, STP FSAR open items and open NRC questions. This list was given to your Mr. N. Prasad Kadambi on October 8, 1985 by our Mr. M. E. Powell.

The attachment includes pages which will be incorporated in a future FSAR amendment.

The items which are attached to this letter are:

Attachment	Item No.*	Subject
1	F 10.0-1	AFWS Reliability, App. 10A

B001
1/1

* Legend
D - DSER Open Item
F - FSAR Open Item
C - DSER Confirmatory Item
Q - FSAR Question Response Item

L1/DSER/z

If you should have any questions concerning this matter, please contact Mr. Powell at (713) 993-1328.

Very truly yours,

M. R. Wisenburg
Manager, Nuclear Licensing

JSP/bl

Attachments: See above

L1/DSER/z

cc:

Hugh L. Thompson, Jr., Director
Division of Licensing
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Robert D. Martin
Regional Administrator, Region IV
Nuclear Regulatory Commission
611 Ryan Plaza Drive, Suite 1000
Arlington, TX 76011

N. Prasad Kadambi, Project Manager
U.S. Nuclear Regulatory Commission
7920 Norfolk Avenue
Bethesda, MD 20814

Claude E. Johnson
Senior Resident Inspector/STP
c/o U.S. Nuclear Regulatory
Commission
P.O. Box 910
Bay City, TX 77414

M.D. Schwarz, Jr., Esquire
Baker & Botts
One Shell Plaza
Houston, TX 77002

J.R. Newman, Esquire
Newman & Holtzinger, P.C.
1615 L Street, N.W.
Washington, DC 20036

Director, Office of Inspection
and Enforcement
U.S. Nuclear Regulatory Commission
Washington, DC 20555

E.R. Brooks/R.L. Range
Central Power & Light Company
P.O. Box 2121
Corpus Christi, TX 78403

H.L. Peterson/G. Pokorny
City of Austin
P.O. Box 1088
Austin, TX 78767

J.B. Poston/A. vonRosenberg
City Public Service Board
P.O. Box 1771
San Antonio, TX 78296

Brian E. Berwick, Esquire
Assistant Attorney General for
the State of Texas
P.O. Box 12548, Capitol Station
Austin, TX 78711

Lanny A. Sinkin
3022 Porter Street, N.W. #304
Washington, DC 20008

Oreste R. Pirfo, Esquire
Hearing Attorney
Office of the Executive Legal Director
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Charles Bechhoefer, Esquire
Chairman, Atomic Safety &
Licensing Board
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Dr. James C. Lamb, III
313 Woodhaven Road
Chapel Hill, NC 27514

Judge Frederick J. Shon
Atomic Safety and Licensing Board
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Mr. Ray Goldstein, Esquire
1001 Vaughn Building
807 Brazos
Austin, TX 78701

Citizens for Equitable Utilities, Inc.
c/o Ms. Peggy Buchorn
Route 1, Box 1684
Brazoria, TX 77422

Docketing & Service Section
Office of the Secretary
U.S. Nuclear Regulatory Commission
Washington, DC 20555
(3 Copies)

Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
1717 H Street
Washington, DC 20555

Revised 9/25/85

SOUTH TEXAS PROJECT
14926-001

APPENDIX 10A

AUXILIARY FEEDWATER SYSTEM

RELIABILITY EVALUATION

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES (Cont'd)

10A.1 INTRODUCTION

10A.1.1 Purpose

This Appendix describes the reliability evaluation of the STP auxiliary feedwater system. The evaluation was performed in a manner consistent with NUREG-0611 to allow a comparison to other plants of the reliability of the STP system for specific initiating events. The results of the evaluation show the system compares favorably with other designs and has a high reliability for the initiating events considered.

This reliability evaluation reflects the auxiliary feedwater system design at the time it was performed. Subsequent modifications will not result in revision of this appendix unless they could have a significant impact on the results presented.

10A.1.2 Objectives

The objectives of the evaluation are:

- To perform an analysis to evaluate the reliability of the AFWS in accordance with the guidelines contained in NUREG 0611.
- To provide indication of the contributors of the auxiliary feedwater system unavailability for the initiating events described in NUREG-0611.

10A.1.3 Scope

Three initiating events are analyzed:

Case I: Loss of main feedwater (LMFW)

Case II: Loss of main feedwater coincident with loss of offsite power (LMFW/LOOP)

Case III: Loss of main feedwater coincident with loss of all AC power (LMFW/LOAC)

10A.1.4 General Approach

The principal technique used in the quantitative evaluation is the construction and analysis of fault trees which represent the AFWS' failure logic. A summary of the basic tasks in the evaluation is presented in Figure 10A-1.

AUXILIARY FEEDWATER SYSTEM RELIABILITY EVALUATION

Fault trees representing the AFWS failure logic are presented in Section 10A.3.2. AFWS unavailability is based on the Boolean logic associated with the system fault trees. The fault trees are reduced to a list of cut-sets to identify the failure modes. Failure rate data (see Section 10A.3.4) are inserted to evaluate system unavailability. Although the failure data are derived primarily from NUREG-0611, secondary sources of failure data are WASH-1400 (Ref. 2), NUREG/CR-1362 (Ref. 3), and the Zion Probabilistic Safety Assessment (Ref. 6).

Fault tree development is consistent with the procedures and data available in NUREG-0611, and is limited to AFWS unavailability per demand. STP technical specifications allow continued operation of the plant with AFWS Train A out-of-service for an indefinite period of time. Therefore, this evaluation assumes that Train A would not be available at the time of AFW initiation. In reality, it is expected that Train A would have an availability similar to the other three trains of AFW. This assumption results in system unavailability being conservative by at least 33% for Cases 1 and 2. In this appendix, unavailability is synonymous with unreliability, and the terms are used interchangeably. The importance of specific failure modes is examined, as are the interrelationships between and significance of hardware failure, test and maintenance outages, and human errors.

In addition to the quantitative evaluation described above, a qualitative evaluation is performed in a manner consistent with NUREG-0611. This evaluation rates system reliability based on design features such as equipment redundancy, manual versus auto actuation, single-point failure vulnerability, and technical specification limits on train outage time. The rating is done to compare the South Texas design with other U.S. plants using a Westinghouse nuclear steam supply system.

The success criteria used for LMFW, LMFW/LOOP, and LMFW/LOAC require that there be a minimum flow of 515 GPM delivered to at least one steam generator.

There are four AFW trains, each of which is dedicated to a single steam generator. Three of the AFW trains (Trains A, B, and C) are motor driven; the fourth (Train D) is turbine driven. Each AFW train is designed to deliver 550 GPM within one minute of actuation. Only the 'D' Train is operable under LOAC. Translating the success criteria in the preceding paragraph into failure criteria for fault tree development, "failure" reduces to "no flow to any SG" in the case of LMFW and LMFW/LOOP, and "no flow to SG D" in the case of LMFW/LOAC.

10A.1.5 Assumptions

Assumptions used in this evaluation are consistent with those specified in NUREG-0611. Specific assumptions used in the evaluation are:

1. Hardware and Human Error Failure Data

   The hardware and human error failure data, taken primarily from NUREG-0611, are used in the evaluation of basic events in this study. These data are presented in Section 10A.3.4.

2. Test and Maintenance Outage Contribution

The study uses the calculational approach and the outage duration data presented in Table III-2 of NUREG-0611. These data are presented in Section 10A.3.4.

3. Power Availability

Consistent with NUREG-0611, the following assumptions are used to model power availability.

- Offsite power is assumed to have availability equal to 1.0 for Case I and zero for Cases II and III.

- Diesel generator availability for Case I is not relevant, since offsite power availability is 1.0. For Case II, the availability of one diesel generator (Train C) is assumed equal to 1.0 (Ref. 1) and the other one (Train B) equal to 0.95 (Table 10A-2). For Cases II and III, offsite and/or emergency onsite AC power is assumed to be restored within a period of 2 hours.

- DC and battery-backed AC are assumed to have availability equal to 1.0 (Ref. 1) for all three cases.

4. Sample and Test Lines

The only sample or test line providing a significant flow diversion and/or leakage path is the pump test return line, which was considered in the human errors analysis. Since this 3-inch return line discharges to the AFWST at atmospheric pressure, significant flow may be diverted if this normally locked-closed valve is inadvertently left open after testing the pump.

5. Passive Piping Components

All piping components (e.g., pipe sections, flanges, reducers, etc.) are assumed available with a probability of 1.0. They are not considered in the fault tree development.

6. Degraded Component Failures

Degraded component failures are not considered in this evaluation; that is, components are assumed to operate properly or are treated as total failures. Component failures are assumed to occur instantaneously and completely.

7. Uncoupling of Human Errors

This study assumes that test and maintenance activities are staggered. That is, redundant AFWS components are not tested by the same personnel on the same shift, but in general, tests and/or maintenance of redundant components involve time and/or personnel changes (e.g., different personnel and shifts, or the same personnel on a different day, etc.) In addition, a double-check procedure is assumed to assure the correct status of locked open valves after test and maintenance. This significantly reduces the probability of human error in two or more trains simultaneously. Given that test and maintenance activities are staggered and the use of a double check procedure, it is reasonable to assume that human errors for test and maintenance are uncoupled.

For the above reasons, the evaluation does not consider concurrent disabling of multiple trains because of human error in conjunction with test or maintenance to be a credible failure scenario.

8. Technical Specification

The auxiliary feedwater system design is evaluated in accordance with the STP Technical Specifications (Ref. 7).

Train A - Out of Service,
Trains B, C, and D - Operable except for the scenarios illustrated in the fault trees in Section 10A.3.4.

9. HVAC Support

The motor driven auxiliary feedwater pump rooms are cooled by safety-related HVAC units powered by their respective trains. The turbine driven pump room is cooled by a Train A HVAC unit, however, the turbine driven pump is qualified for operation following the loss of all HVAC. Consistent with NUREG-0611 methodology, HVAC support to the pumps is not considered in this evaluation.

10. Auxiliary Feedwater Storage Tank

Water from the AFWST is assumed to be available at all times. The AFWST capacity is sufficient allow the RCS to remain at hot standby for 4 hours followed by a 10 hour cooldown at which point further RCS cooldown is performed by the residual heat removal system. If additional quantities are needed, water can be provided to the AFWST from the demineralized water storage tank, the condenser hot well, or an alternate

onsite source. The AFWST has level instrumentation with control room indication and annunciation to warn operators of low AFWST water inventory.

10A.2 SYSTEM DESCRIPTION

10A.2.1 Introduction

This AFWS description summarizes the more extensive description given in Section 10.4.9. Emphasis is placed on operation following the three loss of normal feedwater extents covered by this reliability evaluation. The water for the AFWS is supplied from the auxiliary feedwater storage tank (AFWST). Water is supplied to the AFW inlet nozzles on the secondary side of the steam generators following a loss of normal feedwater flow as described in Section 10A.2.3. The AFWS serves as a backup to the main feedwater system during normal startup and shutdown operations.

The AFWS maintains the steam generators' water inventory during periods when the main feedwater system is unavailable. The system is a safety-related system. The AFWS is activated by an auto-start and is designed to deliver flow water to the steam generators within one minute. A minimum flow of 515 gal/min must be supplied to any one steam generator on a loss of feedwater transient.

Four pump trains are utilized, each taking suction from the AFWST by separate suction lines. A P&ID for the AFWS is shown on Figure 10A-2. Figure 10A-3 is a simplified reliability block diagram of this system. Figure 10A-4 is the detailed reliability block diagram from which the simplified reliability block diagram (Figure 10A-3) was derived. As mentioned earlier, this analysis conservatively assumes that Train A is out of service at the onset of the transient for Cases I & II. Subsequent discussions with respect to the quantitative analysis contained in this evaluation do not include of AFWS Train A.

Trains B and C of the AFWS have motor-driven pumps. Train D has a steam turbine pump. Initiation of the system is automatic upon actuation of two out of four low-low water level instrument channels in any steam generator. Crossover lines are provided downstream of the pumps to interconnect the trains and are operable from the control room for Case I. The valves connecting the crossover lines to the AFW pump discharge lines are normally closed, fail closed upon loss of instrument air and close on AFWS actuation. The crossover line valves can be opened manually from outside the control room. The air operated crossover valves are expected to remain operable from the control room after loss of offsite power for a period of time due to stored air in the instrument air receiver tanks. Thus, loss of offsite power does not result in instantaneous loss of crossover valve operation from the control room. However, since the instrument air system is a non safety-related system which is not immediately operable following LOOP, no credit for remote manual operation of the crossover valves is taken in the Case II evaluation. The valves are assumed to be opened locally in the analysis. For

Case III (LMFW/LOAC), no crossover capability is assumed since there are three valves required to be opened locally to establish a flow path to a second steam generator.

Each AFW train provides feedwater to a single dedicated steam generator following an actuation signal. No hardware components are common between trains other than the aforementioned crossover lines. Each train, which consists of suction piping, pump/driver combination, discharge piping, cross-connect piping between trains and test and recirculation piping, is housed in a separate Seismic Category I compartment.

Pump pressure and flow testing is accomplished through a 3-inch diameter recirculation line connected to the 4-inch diameter main flow line downstream of the flow element. Flow through this line is regulated by a normally locked-closed globe valve downstream of the recirculation connection to the main line. Opening this valve allows recirculation to the AFWST for pump testing.

10A.2.2 Component Description

1. Motor-Driven Pumps:

   The motor driven pumps are driven by AC-powered electric motors. Each motor receives power from an independent Class 1E power supply bus and its corresponding standby diesel generator. The pumps are horizontal, centrifugal, multistage units.

2. Turbine-Driven Pump:

   The turbine pump is a horizontal, centrifugal, multistage, noncondensing steam turbine-driven unit. A steam line connection is taken from the Safety Class 2 section of the Steam Generator D main steam line upstream of the main steam isolation valve. The turbine steam inlet line is provided with remote manual isolation and throttle valves. The turbine discharge steam exhausts directly to atmosphere. Overspeed of the AFW pump turbine automatically trips the turbine. Once this occurs, the mechanical overspeed trip latching mechanism must be manually reset in order to restore the turbine to an operable status. Power for all controls, valve operators, trip solenoid and other support systems is from the Train D Class 1E DC System. The major support system is the lube oil pump and cooling system. The lube oil pump is direct driven off the turbine shaft. The cooling water supply for the turbine lube oil cooler comes from a first stage bleedoff point on the turbine driven pump, passes through the lube oil heat exchanger, and returns to the suction of the same pump.

3. Piping and Valves

The safety-related AFWS piping is manufactured and installed in accordance with the ASME Code. Motor operated valves AF0019, AF0065, MS0143, AF0085 and solenoid valve FV0143 are normally closed. Motor operated valve XMS0514 is normally open. Valves AF0065 and AF0085 are AC powered. Valves MS0143, FV0143, AF0019, and XMS0514 are DC powered.

4. Auxiliary Feedwater Storage Tank (AFWST)

The Seismic Category I auxiliary feedwater storage tank provides water to the AFW pumps. It is a concrete, stainless steel lined, 497,000 gallon tank which has sufficient capacity to allow the RCS to remain at hot standby for 4 hours followed by a 10 hour cooldown at which point further RCS cooldown is performed by the residual heat removal system.

The AFWST is designed to withstand environmental design conditions, including floods, earthquakes, hurricanes, tornado loadings, and tornado missiles. The AFWST is designed so that no single active failure will preclude the ability to provide water to the AFW system. Each train has a dedicated suction line from the AFWST to the AFW pumps. The water level in the AFWST is indicated in the control room as well as at the auxiliary shutdown panel. A low level alarm is also provided in the control room.

10A.2.3 Emergency Operation

The AFWS is designed for automatic actuation in an emergency. Any of the following conditions automatically starts the three Class 1E motor-driven pumps:

1. Two out of four channels showing low-low water level in any steam generator

2. Safety injection signal

3. 4.16 kV bus undervoltage. The AFW pump is started in conjunction with diesel generator starting and load sequencing. Water is not automatically fed to the steam generator until condition 1 or 2 above exists.

The turbine-driven auxiliary feedwater pump starts automatically on any of the following signals:

1. Two out of four channels showing low-low water level in any steam generator

2. Safety injection signal

A one-inch bypass line with a normally closed solenoid operated valve (FV0143) and crifice is provided around the steam inlet valve (MS0143). This bypass valve (FV0143) opens upon receipt of either of the above signals to supply steam to the turbine and allow the turbine to reach governor control speed. After a time delay to allow governor control speed to be reached, the steam inlet valve is opened which allows rated steam flow to the turbine. This arrangement precludes an overspeed trip due to excessive steam flow prior to governor warmup. This bypass line is not dependent upon AC power to operate.

Automatic jog control of the auxiliary feedwater flow control valves operates to initially limit the maximum and minimum flow to any SG when the system is started by an automatic signal. The operator may assume manual flow control after resetting the system.

10A.2.4 Power Sources

The onsite AC Power Systems of Units 1 and 2 each consist of four major subsystems as follows.

1. 13.8 kV Auxiliary Power System (non-Class 1E)
2. 13.8 kV Standby Power System (non-Class 1E)
3. 138 kV Emergency Transformer Systems (non-Class 1E)
4. Onsite Standby Power System (Class 1E)

The arrangement of the AC Power Distribution Systems provides sufficient switching flexibility and equipment redundancy to ensure reliable power supply to the Class 1E and non-Class 1E plant loads during startup, normal operation, and shutdown following a design basis event.

The Onsite Standby Power Supply Systems of Units 1 and 2 each consist of three independent, physically separated, standby DGs supplying power to three associated load groups designated Train A, Train B, and Train C. Each load group consists of a 4.16 kV ESF bus and the electrical loads connected to that bus. The Onsite Standby Power Supply Systems of Units 1 and 2 operate independently of each other. Each standby DG and load group of a particular unit is also physically separated and electrically independent from the other two standby DGs and their load groups.

Each 4.16 kV ESF bus is provided with switching that permits energization of the bus by five alternate sources:

1. The respective unit auxiliary transformer
2. No. 1 standby transformer
3. No. 2 standby transformer

4. Standby DG

5. 138 kV emergency transformer

When neither standby transformer nor the respective unit auxiliary transformer is available, the standby DGs supply the power required by the ESF loads to safely shut down the reactor. The 138 kV emergency transformer provides an additional means for supplying power to these systems if for any reason the above power sources are unavailable. The 138 kV emergency transformer is immediately available; however, its use is operator controlled.

Each standby DG is automatically started in the event of loss of offsite power or safety injection (SI) signal, and the required Class 1E loads connected to that ESF bus are automatically connected in a predetermined time sequence. Each standby DG is ready to accept load within 10 seconds after the start signal.

The Class 1E 125V DC battery systems of each unit consist of four independent, physically separated buses, each energized by two battery chargers and one battery. Emergency power required for plant protection and control is supplied without interruption by the batteries when the power from the Class 1E essential AC source is interrupted.

Each battery system also supplies power to inverters, two each for channels I and IV and one each for channels II and III. The inverters convert DC power to AC power at 118V AC, 60 Hz single phase for the vital instrumentation and protection system. The six vital AC busses supply power to instrumentation channels I, II, III, and IV which are associated with electrical trains A, D, B and C respectively. The two battery chargers associated with each of the four 125V DC busses are connected to separate Class 1E busses of the same train to enhance the reliability of each DC bus in the event that offsite power is lost. Following a loss of offsite power, AC power to the battery chargers is supplied by the standby DGs. Components in the turbine-driven train are powered from the Train D Class 1E DC system. Consistent with NUREG 0611, it is assumed that offsite and/or onsite AC power are restored within two hours to supply power to the battery chargers to restore the Train D battery to full capacity.

In the motor driven trains, the pump motors and valve actuators in each train are powered by the corresponding Class 1E train. Instrumentation and controls in each train are provided by DC or AC power from its associated Class 1E train.

10A.2.5 Testing

The AFWS inservice testing and inspection frequencies assumed in this analysis are described below. The frequencies are in agreement with Reference 7 with the exception of automatic valve position verification which is indicated as at least once every 31 days in the Technical Specifications. This increase in

test frequency serves to decrease the auxiliary feedwater system hardware related unavailability (Table 10A-6) without affecting human error and test and maintenance related unavailability. The calculated total auxiliary feedwater system unavailabilities are therefore conservative.

Component Test	Test Frequency
o Motor Driven Pumps Operability	Recirculate to AFWST at least once every 92 days
o Turbine Driven Pump Operability	Recirculate to AFWST at least once every 92 days
o Automatic Valve Position	Verify position at least once every 92 days
o Non-Automatic Valve Position	Verify position at least every 31 days
o Automatic Valve Actuation	Verify actuation to correct position during each refueling shutdown
o Motor and Turbine Driven Pump Actuation	Verify pumps start on actuation signal during each refueling shutdown
o Train Operability	Verify ability to establish flow path to each steam generator following cold shutdowns greater than 30 days

10A.3 METHODOLOGY

This section presents the step-by-step procedure followed in performing the AFWS quantitative reliability evaluation.

10A.3.1 System Review

In the first step, the various drawings, P&IDs, and schematics representing the AFWS were examined. Special attention was given to identifying:

1. Instrumentation systems required for system actuation
2. Fluid systems connected directly or indirectly to the AFWS
3. Power sources for each component
4. Any obvious single-point vulnerabilities.

The reliability information described in Appendix III of NUREG-0611 was then appraised, and AFWS studies of other facilities were reviewed. With this information, the evaluation boundaries were established.

10A.3.2 Fault Tree Development and Quantification

The reliability block diagram for the AFWS (Figure 10A-4) was constructed. A simplified version of the reliability block diagram is provided in Figure 10A-3. Fault trees (Figures 10A-5 through 10) are constructed from the reliability block diagram and the P&IDs. These trees include the occurrence of individual component failures. Fault trees for test and maintenance, and human error after test and maintenance are also constructed (Figures 10A-11 and 12). From these detailed fault trees, simplified trees were constructed. The simplified trees contain the same system information, but basic events that are under a single OR-gate or AND-gate are combined into a composite event (hereafter referred to as a supercomponent). By using simplified fault trees, a tree containing a manageable number of events is constructed, yet the fault propagation within and between systems is preserved. When consolidating basic events into composite events, care is taken to assure that no basic event appearing in a composite event appears elsewhere in the tree. Definitions of composite events are given in Section 10A.3.4. Reduced fault trees (Figures 10A-13 and 14) are constructed to provide a simple illustration of the overall logic configuration for each case, but are not used in the quantification process.

Quantification of the AFWS fault trees is done by two computer programs, FTAP and IMPORTANCE. Refer to Section 10A.3.5 for a description of these computer programs.

Three distinct contributions to AFWS unavailability are quantified in the evaluations. Unavailability due to random hardware failures is quantified using the AFWS hardware-related fault tree (Figures 10A-5 through 10). AFWS unavailability resulting from system downtime for test and maintenance is also quantified. In addition, system unavailability resulting from human errors associated with test and maintenance activities is quantified. The total AFWS unavailability (per demand) is the sum of the unavailabilities due to random hardware failure, test and maintenance, and human error.

10A.3.3 Common Cause Failure Evaluation

The evaluation and design provisions of common cause factors such as floods (Section 3.4), fires (Section 9.5.1), earthquakes (Section 3.2), sabotage and high energy pipe breaks (Section 3.6) are outside the scope of this AFWS unavailability study. The only common cause factor considered is that resulting from human errors during test and maintenance.

This evaluation assumes that human errors are statistically independent. Tests and maintenance of redundant components will involve time and/or personnel changes (e.g., different personnel and shifts or the same personnel on a different day, etc.). This assumption is also supported by Technical

Specification limitations on plant operation associated with coincident test and maintenance activities that reduce train availability to an unacceptable level.

10A.3.4 Failure Data

10A.3.4.1 Description of Supercomponents

The detailed reliability block diagram illustrated on Figure 10A-4 shows groupings of equipment within each train of the AFWS that function as an identifiable unit, and whose failure logic can be represented in a fault tree as basic events connected under a single OR-gate or AND-gate. These equipment groupings, referred to as supercomponents, can be used to generate simplified fault trees in which the supercomponents are used to represent basic events rather than each individual piece of equipment.

The following symbols represent supercomponent abbreviations used in Figure 10A-4.

MB1, MC1, MD1 = hardware-related failure of motor-driven and turbine-driven AFW pumps and associated valves in Trains B, C, and D, respectively upstream of the crossover valves.

MB2, MC2, MD2 = hardware-related failure of flow elements and associated valves on the steam generator side of AFW Trains B, C, and D, respectively downstream of the crossover valves.

MD3 = hardware-related failure of valves controlling steam supply to turbine-driven AFW pump for Train D.

DG12, DG13 = hardware-related failures and test or maintenance unavailabilities causing inability of diesel generators for Trains B and C (respectively) to start.

SB = Failure of both automatic and manual backup actuation signals for Train B (ASB, MSB on Figure 10A-4).

SC = failure of both automatic and manual backup actuation signals for Train C (ASC, MSC on Figure 10A-4).

SD = failure of both automatic and manual backup actuation signals for Train D (ASA, MSD on Figure 10A-4).

BVLC = CVLC = DVLC = Human error related unavailability due to operator's failure to restore the block valves on the pump suction or discharge lines following maintenance.

Table 10A-1 enumerates the individual pieces of equipment included within each of the above-listed supercomponent groupings. Equipment numbers shown in the table correspond to those shown on Figure 10A-4.

10A.3.4.2 Failure Rate Data

10A.3.4.2.1 Hardware

Hardware-related failure data used in this evaluation are presented in Table 10A-2. Unless otherwise indicated, all failure data are taken directly from NUREG-0611.

10A.3.4.2.2 Human Error

Since the AFWS is automatically actuated, the treatment of human error is limited to mispositioning manual valves based on the human error probabilities given in NUREG-0611. Valves considered are AF0024, AF0053, AF0073, AF0012, AF0059, and AF0078 and manual valves in the recirculation lines to the AFST which are not shown on the detailed reliability block diagram (Figure 10A-4).

During maintenance, valves AF0024, AF0053, AF0073, AF0012, AF0059, and AF0078 must be closed in order to drain the water from pumps. They may inadvertently be left closed. A failure rate of 5×10^{-3} per demand is used in this calculation. During the testing of a pump, the manual valve in the recirculation line must be open. The manual valve may inadvertently be left open. A failure rate of 5×10^{-3} per demand is used in this calculation. For Train D, the trip and throttle valve overspeed trip mechanism must be manually reset after maintenance or a previous overspeed trip. A failure rate of 5×10^{-3} per demand is used for this calculation.

10A.3.4.2.3 Test and Maintenance

The approach presented in NUREG-0611 is used. Testing and maintenance (T&M) activities that remove components and/or the system from service can be significant contributors to overall AFWS unavailability. The most common forms of valve maintenance performed during power operation are packing adjustments and repairs to the MOV and AOV control circuits and operators. Nearly all of these activities are performed with the valve in the safe position during the maintenance interval. Therefore, maintenance of MOVs and AOVs is not considered to contribute to valve unavailability, except for the stop check isolation valves. Since the valves are normally closed, maintenance would disable any local control circuit, effectively failing that portion of the train. Check valves and manual valves are expected to require very little maintenance. The low test and maintenance impact on this part of the AFWS is the basis for not including a human error contributor to unavailability for the manual valves in the individual steam generator flow paths. Although testing and maintenance contributions are not treated for the valves associated with the branch flowpaths to a specific steam generator, unavailability from testing and maintenance of the pump subsystem is treated.

In the subsystem part of the fault tree, testing and maintenance are treated as a distinct composite basic event. Unavailability due to T&M is calculated using outage durations from NUREG-0611 and the test frequencies as presented in Section 10A.2.5. T&M unavailabilities for each train are comprised of contributions due to testing of the train, maintenance of the pump, and maintenance of the stop check isolation valve. The sum of these contributions constitute the total test and maintenance unavailability of a particular train. T&M unavailabilities are provided in Table 10A-3.

STP Technical Specifications (Reference 7) do not allow coincident test or maintenance of components of more than one AFW pump train. Therefore, the analysis explicitly accounts for maintenance in one train and coincident hardware related failures in the remaining two trains.

10A.3.4.3 Computed Unavailabilities for Composite Events

The unavailability per demand of each of the supercomponents described in Section 10A.3.4.1 is calculated by substituting the failure rate data in Tables 10A-2 and 10A-3 into the supercomponent expressions given in Table 10A-1. Unavailability per demand for each supercomponent grouping is summarized in Table 10A-4.

10A.3.5 Computer Programs

The following Bechtel Power Corporation computer programs are used in performing the evaluation of auxiliary feedwater system unavailability.

10A.3.5.1 FTAP

This program is used to generate fault tree cut sets. Minimal cut set families are generated by one of three processing methods: (1) top-down, (2) bottom up, or (3) "Nelson" method. FTAP results have been verified by comparison with hand calculations.

10A.3.5.2 IMPORTANCE

This program uses the minimum cut sets generated by FTAP and basic event data, failure rates and fault duration times to determine system and subsystem unavailability. This program has been verified by comparison with hand calculations.

10A.4 RESULTS OF THE RELIABILITY EVALUATION

The results of the AFWS reliability evaluation are provided in two forms. The first is a general qualitative evaluation based on system design features. The second part is a quantitative evaluation based on the fault tree representation of the AFWS design.

AUXILIARY FEEDWATER SYSTEM RELIABILITY EVALUATION

10A.4.1 Qualitative Evaluation

In the qualitative characterization of the reliability of AFW systems, NUREG-0611 assumes that the traits identified in Table 10A-5 exist for specific reliability ratings. These characterizations are reviewed for each of the three initiating events considered in NUREG-0611.

10A.4.1.1 Loss of Main Feedwater

In NUREG-0611, some of the plants whose AFWS are found to have low reliability have single-point vulnerabilities. This is due to a single manual valve through which all AFW flow passes, where a human error of failing to reopen the valve after maintenance is found to be the dominant failure contributor. The South Texas design has four lines supplying water to the four pump trains. Thus, no single human error could disable the system. The only single failure that could disable the system is rupture of the auxiliary feedwater storage tank. The unavailability due to this failure is extremely small and this event would be readily detected by tank level indication and low level alarms in the main control room.

The NUREG-0611 plants classified in the high-reliability range for this transient generally have three AFW pumps (two motor and one steam turbine driven) which are actuated automatically, with manual backup signal.

Since the South Texas AFWS design includes all these features and control room actuated crossover capability, it receives a high reliability rating for this transient even though Train A is assumed out of service.

10A.4.1.2 Loss of Main Feedwater with Loss of Offsite Power

The major difference between this and the previous LMFW event is that offsite power sources are not available and the system must rely on onsite power sources (i.e., diesel generators, batteries and steam).

The reliability of various AFWS designs for this event are generally found to be quite similar to those for the previous initiating event (LMFW). The major difference is that onsite AC power sources are required and the potential impact of degrading these power sources (e.g., the loss of one or more emergency diesel-generators) on the AFWS reliability is evaluated.

Compared to other Westinghouse NSSS plants evaluated in NUREG-0611, the South Texas AFWS contains a greater number of motor driven pump trains (3 versus the typical 2); however, this analysis conservatively assumes that one train is out of service. This redundancy reduces the likelihood of AFWS unavailability during a LMFW/LOOP event.

For this reason and the local manual crossover capability, the qualitative reliability rating given the South Texas AFWS is comparable to that of other high reliability Westinghouse NSSS plants as reported in NUREG-0611.

10A.4.1.3 Loss of Main Feedwater with Loss of All AC Power

The major feature of this initiating event is the total dependency of the AFWS on steam power. Low and medium reliability classifications under this event are generally due to systems having AC power dependencies in the steam turbine-driven pump train. Such dependencies may include lube oil cooling, AC power to steam turbine admission valves, or air-operated valves which fail closed on loss of air. Those systems characterized as having a relatively high reliability are usually automatically actuated and have no potentially degrading AC power dependencies (except HVAC).

When comparing the STP AFWS to the NUREG-0611 plants which have a high reliability characterization, the STP design has a comparably high reliability because the turbine pump train has no AC dependency in order to function. However, since no credit is taken for the steam turbine driven pump to serve other than SG-D (due to absence of control room activated crossover capability and the requisite manual actuation of the stop check isolation valves in the other trains), the South Texas AFWS is rated slightly lower than some of the highest rated other Westinghouse NSSS plants as reported in NUREG-0611 (refer to Figure 10A-15). As noted earlier, it is possible to manually initiate crossover from outside the control room if the need should ever arise. The turbine driven pump is qualified for operation in the environment resulting from a loss of HVAC.

10A.4.1.4 Qualitative Comparison with Other Designs

Figure 10A-15 is a reproduction of the reliability characteristic chart presented in NUREG-0611 for AFWS designs in plants using the Westinghouse NSSS. An added row presents the results of a qualitative evaluation of South Texas AFWS reliability. The figure shows the relative reliability ranking of South Texas AFWS for each of the three cases studied and compares these results to those obtained by the NRC. This qualitative evaluation is included to complement the results of the quantitative analysis.

10A.4.2 Quantitative Evaluation

The quantitative characterization of the South Texas AFWS reliability is developed using the methods and data provided in NUREG-0611. The system's conditional unavailability is quantified for three initiating events: LMFW, LMFW/LOOP and LMFW/LOAC. System unavailability is associated with hardware failure, human error, and test and maintenance downtime.

10A.4.2.1 Quantitative Results

The results of the quantitative evaluation are presented in Table 10A-6. Table 10A-6 identifies the individual contributions of hardware failure, human

error, and test and maintenance to the AFWS unavailability for three initiating events (LMFW, LMFW/LOOP and LMFW/LOAC). System unavailability for the LMFW and LMFW/LOOP events is approximately 2 x 10^{-5} and 4 x 10^{-5} per demand, respectively. Even for the LMFW/LOAC event, where all AC power is lost and the system is totally dependent on the steam turbine driven pump to supply water to the steam generators, the system unavailability of approximately 6 x 10^{-2} per demand is good. These results demonstrate that the South Texas AFWS design is reliable when compared with other designs and the USNRC acceptance criteria of 10^{-5} to 10^{-4} per demand for the LMFW transient (Ref. 5) particularly when one considers that the South Texas AFWS analysis excludes one train from consideration.

10A.4.2.2 Failure Modes

There are many possible combinations of random hardware failures, component unavailabilities due to test or maintenance, and human error which can result in the unavailability of the AFWS. Since each system component (e.g., pump, valve) generally has a different failure rate, there are certain combinations of failure modes that contribute significantly more to the total unavailability of the AFWS than others. These are the most significant failure modes. Unavailability per demand of each of the possible combinations of failure modes is computed by quantifying each of the minimal cut-sets generated by the computer code "FTAP". Once the unavailabilities associated with each minimal cut set have been computed, their percentage contribution to total AFWS unavailability can be determined, and significant failure modes identified.

The AFWS reliability evaluation uses the computer code FTAP to generate minimal cut-sets based on Boolean expressions for the random hardware failure, test and maintenance, and human error fault trees shown in Section 10A.3.2. In general, higher-order cut-sets contribute less to the top event than do lower order cut-sets if the failure rates of the basic events are similar. With three separate pump trains, the aggregate of third-order cut-sets (representing various combinations of pump and valve failures affecting different trains) contribute significantly to the failure of the entire AFWS. Higher order cut-sets (e.g., fourth-order) involve other basic events with much smaller failure rates, and their aggregate contribution to total AFWS unavailabilty is numerically small.

The following sections present a summary of failure modes associated with the LMFW, LMFW/LOOP, and LMFW/LOAC failure scenarios.

10A.4.2.2.1 Loss of Main Feedwater (Case I)

For the LMFW scenario (Case I), the "FTAP" code produces 1 first-order cut-set, 0 second-order cut-sets and 10 third-order cut-sets for the hardware failure fault tree shown on Figures 10A-6 through 10A-10. The "FTAP" run for the test and maintenance fault tree shown on Figure 10A-11 results in no first-order cut-set and 34 third-order cut-sets. The human error fault trees

(Figure 10A-12) produce no first or second-order cut-sets, and 23 third-order cut-sets. From Table 10A-6, it can be seen that the hardware failure cut-sets (in aggregate) contributes about 25 percent to total AFWS unavailability; human error cut-sets about 51 percent; and test and maintenance cut-sets about 24 percent. Within each group of cut-sets, no one particular failure mode could be characterized as a true dominant contributor. The single first-order cut-set for the hardware failure fault tree represents unavailability of the AFWST which is numerically small (approximately 3.6×10^{-8} per demand). To simplify the discussion, AFWST unavailability (here and in the following two sections) will be treated as a hardware-related failure. Third-order cut-sets for the hardware failure fault tree represent various combinations of failures of pumps and valves in different AFW trains. Because failure rates assigned to pumps and valves are numerically similar, the numerical values of the 10 third-order cut-sets are close to one another, with no single contributor being dominant. Human error is the largest contributor to AFWS unavailability for Case I (LMFW).

10A.4.2.2.2 Loss of Main Feedwater Coincident with Loss of Offsite Power (Case II)

For the LMFW/LOOP scenario (Case II), the "FTAP" code produces 1 first-order cut-set, 0 second-order cut-sets, and 14 third-order cut-sets for the hardware failure fault tree shown on Figures 10A-6 through 10A-10. The greater number of hardware failure cut-sets for Case II versus Case I is attributable to combinations of pump and valve failures in addition to failure of the diesel generator to start (diesel generator operation is required for Case II but not Case I). From the test and maintenance and human error fault trees (Figures 10A-11 and 12), a combined total of 0 first-order cut-sets, 0 second-order cut-sets, and 65 third-order cut-sets are generated by "FTAP". Considering the aggregate contribution of hardware failure, test and maintenance, and human error to total AFWS unavailability for Case II, hardware failure cut-sets contributes 40 percent to the total unavailability, test and maintenance contributes about 15 percent, and human error contributes 45 percent (refer to Table 10A-6). As for Case I, no cut-sets belonging to the test and maintenance group are dominant contributors. In the category of hardware failure, various combinations of failures of one diesel generator affecting one train and valve failures disabling a second and third train are responsible for 66 percent of the total unavailability attributable to hardware-related failures. For the human error contribution to total AFWS unavailability, human error affecting one train, plus failure of one diesel generator disabling a second train, and a valve failure disabling a third train represent 39 percent of the total human error contribution to AFWS unavailability.

From the quantitative analysis of Case II, it is concluded that failure of diesel generators to start, hardware failures associated with valves in the pump discharge lines, and human error are the most important factors affecting AFWS unavailability.

10A.4.2.2.3 Loss of Main Feedwater Coincident with Loss of All AC Power (Case III)

AFWS unavailability for the LMFW/LOAC scenario (Case III) is attributable to any hardware-related failure, test or maintenance unavailability, or human error that could disable Train D, since this is the only AFW train which can operate independently of AC power. The percentage contribution of each to total AFWS unavailability for Case III is as follows (see Table 10A-6): hardware-related failure, 52 percent; test and maintenance, 14 percent; and human error, 34 percent.

10A.4.2.3 Conclusions

The quantitative evaluation of auxiliary feedwater system reliability concludes the system reliability is high and in accordance with the guidelines contained in Standard Review Plan 10.4.9, Rev. 2. The qualitative evaluation also shows the system reliability to compare favorably with that of other plants described in NUREG 0611. With the exception of the loss of the AFWST (an extremely low probability event), no single point vulnerabilities were identified in the system. Furthermore, no second order cut-sets were identified and no AC dependencies were found in Train D.

10A.5 REFERENCES

1. NUREG-0611 "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants" by USNRC January, 1980.

2. WASH-1400 "Nuclear Reactor Safety Study" Appendix III, Failure Data, by USNRC October, 1975.

3. NUREG/CR-1362, "Data Summaries of Licensee Event Reports on Diesel Generators at U.S. Commercial Nuclear Power Plants; January 1, 1976 to December 31, 1978", March 1980, by E.G.&G. Idaho, Inc.

4. NUREG-0452, Revision 4, Standard Technical Specifications for Westinghouse Pressurized Water Reactors, USNRC, Fall 1981.

5. NUREG-0800, USNRC Standard Review Plan, Section 10.4.9, July 1981.

6. Zion Probabilistic Safety Assessment; Pickard, Lowe, & Garrick; Newport Beach, CA. September, 1981.

7. Dewease, J. G. (Houston Lighting and Power) to Thompson, H. L. (USNRC), "South Texas Project Electric Generating Station Technical Specifications, Offsite Dose Calculation Manual, Process Control Program," ST-HL-AE-1271, June 17, 1985

TABLE 10A-1

CONSTITUENTS OF SUPERCOMPONENTS[(a)]

MB1 = AF0095 + AF0053 + MPA02 + AF0058 + AF0059

MC1 = AF0096 + AF0073 + MPA03 + AF0091 + AF0078

MD1 = AF0093 + AF0024 + MPA04 + AF0011 + AF0012

MB2 = FV7524 + AF0061 + FE7524 + AF0065 + AF0120

MC2 = FV7523 + AF0080 + FE7523 + AF0085 + AF0121

MD2 = FV7526 + AF0014 + FE7526 + AF0019 + AF0122

MD3 = Governor Valve + XMS0514 + MS0143

SB = ASB x MSB

SC = ASC x MSC

SD = ASA x MSD

(a) For general description of supercomponents, refer to Section 10A.3.4.1 and Figure 10A-4.

Table 10A-2

Component Basic Event Failure Probabilities*

1. Check valve. Failure to open. AF0122, AF0120, AF0121, AF0011, AF0058, AF0091	1×10^{-4}/d(a)
2. Automatic actuation signal. ASA, ASB, ASC	7×10^{-3}/d
3. Manual backup signal. (Conditional probability given automatic signal fails) MSB, MSC, MSD	1×10^{-2}/d
4. Flow element plugging. FE7526, FE7524, FE7523 (This failure rate was taken from WASH-1400 for plugging of the flow orifice Table III 4-1).	3×10^{-4}/d
5. Gate valve. Plugging contribution. AF0014, AF0012, AF0024, AF0093, AF0061, AF0059, AF0053, AF0095, AF0080, AF0078, AF0073, AF0096	1×10^{-4}/d
6. Air operated valve (crossover valves) FV7515, FV7516, FV7518	
Case I: (Control room operation)	
Mechanical components	3×10^{-4}/d
Plugging contribution	1×10^{-4}/d
Operator failure (Manual backup signal)	1×10^{-2}/d
Local control circuit	6×10^{-3}/d
Total	1.64×10^{-2}/d
Case II: (Local Manual Operation)	
Plugging contribution	1×10^{-4}/d
Local manual actuation	2.34×10^{-2}/d** (Ref. 6)
Total	2.35×10^{-2}/d
7. Solenoid valve failure FV0143	
Mechanical components	1×10^{-3}d
Plugging contribution	1×10^{-4}/d (WASH-1400)
Local control circuit	6×10^{-3}/d
Total	7.1×10^{-3}/d

* Data Source, NUREG-0611 except as noted.
** The median value presented here was calculated from the mean value and the variance contained in Reference 6.

Table 10A-2 (Continued)

Component Basic Event Failure Probabilities

8. Motor-operated valve, failure to open.	
AF0019, AF0065, AF0085, MS0143,	
FV7523, FV7524, FV7526	
Mechanical components	1×10^{-3}/d
Plugging contribution	1×10^{-4}/d
Control circuit (local)	6×10^{-3}/d
Total	7.1×10^{-3}d
9. Motor-driven pump.	
MPA02, MPA03	
Mechanical components	1×10^{-3}/d
Control circuit (local)	7×10^{-3}/d
Total	8×10^{-3}/d
10. Turbine-driven pump.	
MPA04	
Mechanical Components	1×10^{-3}/d
Overspeed Trip:	
Solenoid Valve Failure (See Item 7)	7.1×10^{-3}/d
Orifice Plugged	3×10^{-4}/d
Total	8.4×10^{-3}/d
11. Motor-operated valve.	
XMSØ514 Plugging contribution.	1×10^{-4}/d
12. Auxiliary feedwater storage tank (unavailability per demand estimated from that given for condensate storage tank in WASH 1400)	3.6×10^{-8}/d
13. Diesel generator.	
DG13	0
DG12	4.8×10^{-2}/d

The hardware failure rate of diesel-generators (4×10^{-2}/demand) is taken from Ref. 3. Total diesel generator 12 unavailability is the sum of unavailabilities due to hardware failure, test, and maintenance; i.e., total unavailability = $4 \times 10^{-2} + 1.9 \times 10^{-3} + 6.4 \times 10^{-3} = 4.8 \times 10^{-2}$ (Refer to Table 10A-3).

14. Governor Valve	
Plugging Contribution	1×10^{-4}/d

(a) d = demand

4759c/0181c

Table 10A-3

Unavailability of Components Due to Testing or Maintenance

Component	Hrs/ Test	Test/ Yr	Hrs/ Maint.	Q_{test}(a)	Q_{maint}(b)
Pump	1.4	4	19	6.39×10^{-4}/d(c)	5.8×10^{-3}/d
Valve			7	---	2.1×10^{-3}/d
Diesel Generator	1.4	12	21	1.9 x 10-3/d	6.4×10^{-3}/d

(a) $Q_{test} = \frac{(\#\text{ hrs/test})(\#\text{tests/year})}{(\#\text{hrs/year})}$ [See NUREG-0611, Table III-2]

(b) $Q_{maint.} = \frac{(0.22)(\#\text{hrs/maintenance activity})}{720}$ [See NUREG-0611, Table III-2]

(c) d = demand

Table 10A-4

Composite Event Unavailability (per Demand)

	Supercomponent	Probability of Failure
Hardware:	MB1	8.4×10^{-3}
	MC1	8.4×10^{-3}
	MD1	8.8×10^{-3}
	MB2	1.47×10^{-3}
	MC2	1.47×10^{-3}
	MD2	1.47×10^{-3}
	MD3	7.3×10^{-3}
	SB	7×10^{-5}
	SC	7×10^{-5}
	SD	7×10^{-5}
Human Error:	BVLC	1×10^{-2}
	CVLC	1×10^{-2}
	DVLC	1×10^{-2}

Table 10A-5

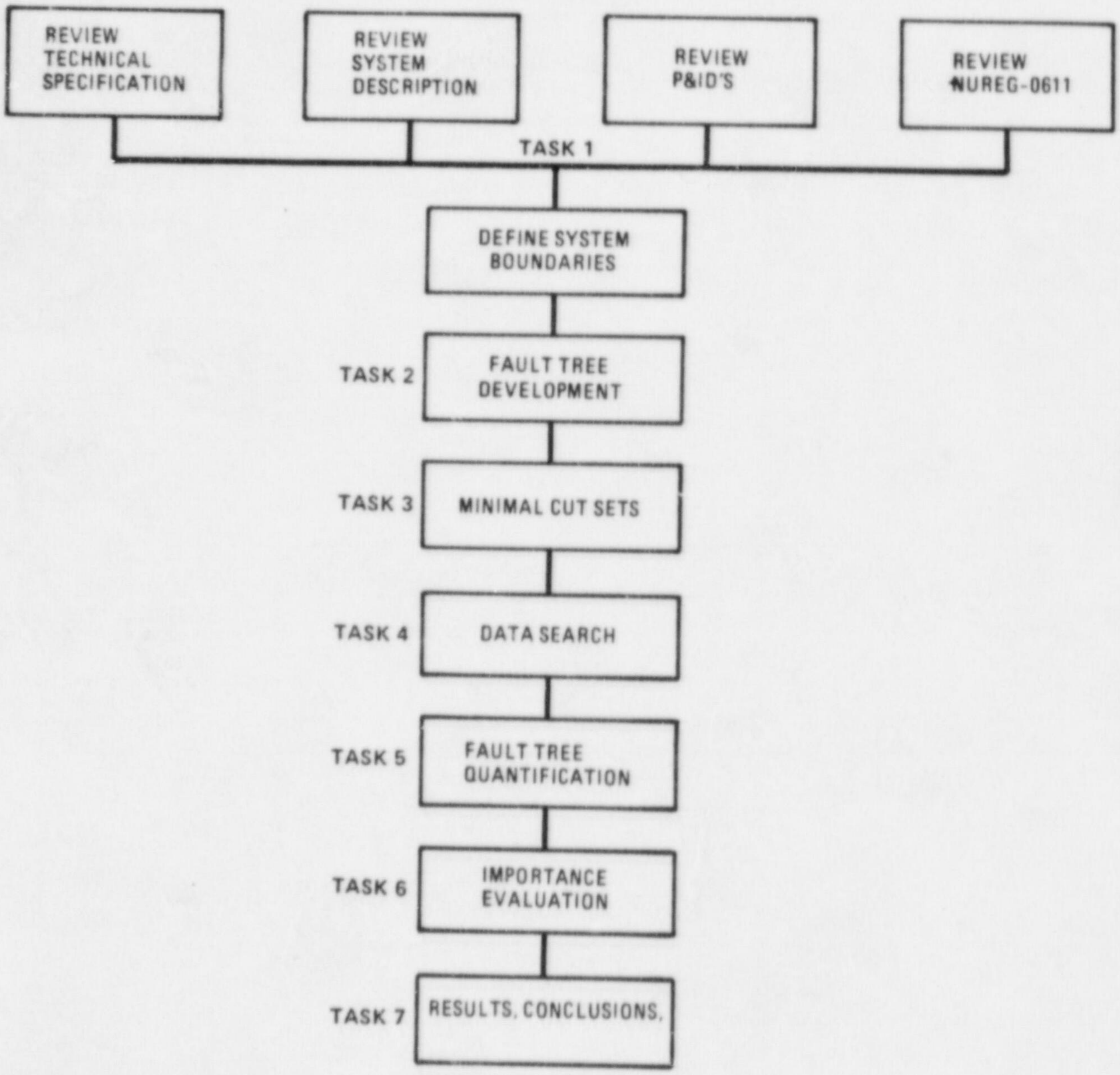
AFWS Qualitative Reliability Characterization Traits

Low-Reliability	Medium-Reliability	High-Reliability
a. Manual system actuation	a. Auto actuation with manual backup	a. Auto actuation with manual backup
b. Two-pump system	b. System with more than two pumps	b. System with more than two pumps and reduced AC dependence
c. Single-point vulnerabilities present	c. Single-point vulnerabilities may be present	c. No single-point vulnerabilities present
d. Technical Specifications permit unlimited outage time for system maintenance, tests, etc.	d. Technical Specifications permit unlimited outage time	d. Technical Specifications do not allow unlimited outage time

Table 10A-6

AFWS Unavailability (per Demand)

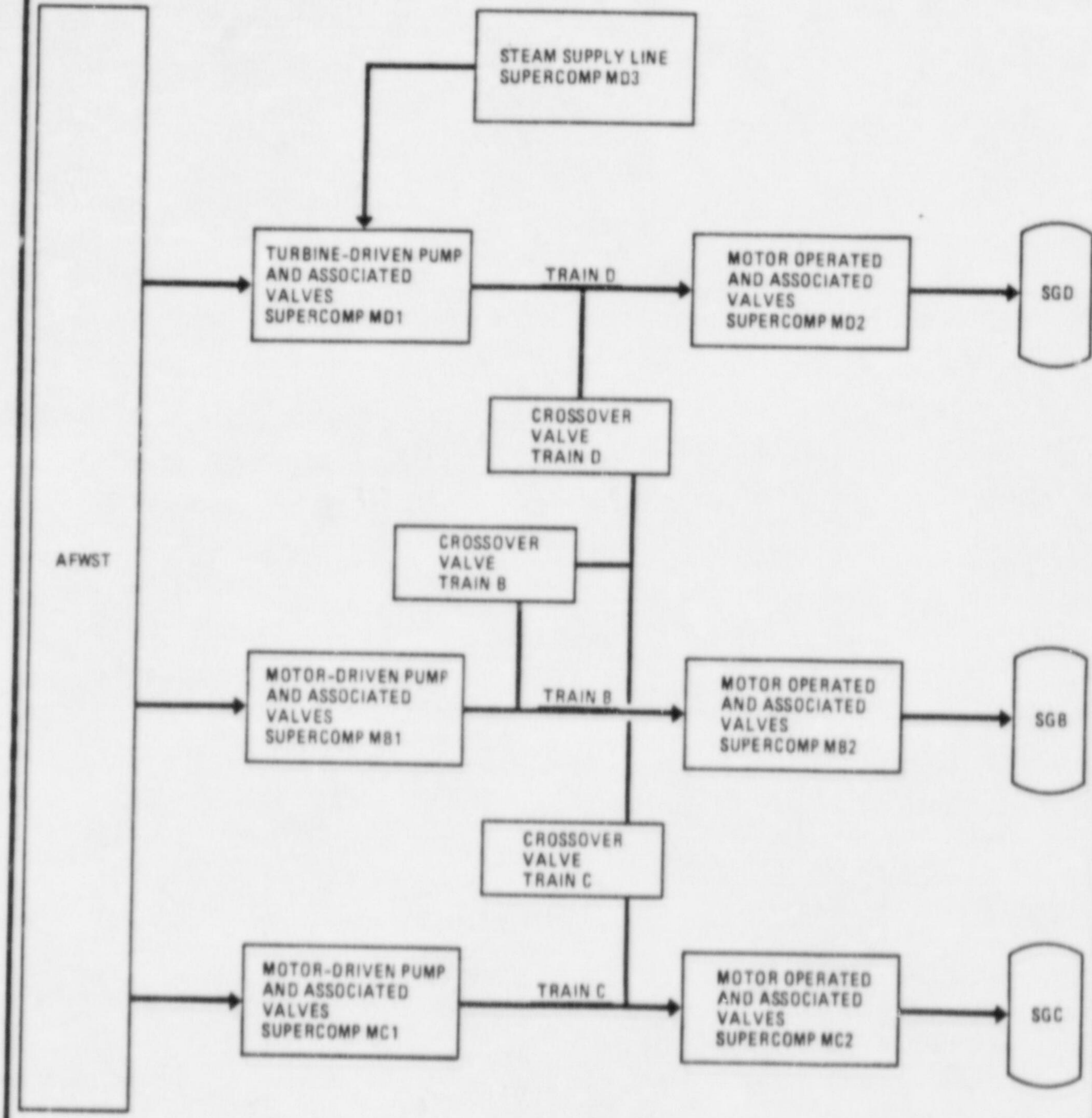
	LMFW	LMFW/LOOP	LMFW/LOAC
Hardware Failure	4.60×10^{-6}	1.57×10^{-5}	3.06×10^{-2}
Human Error	9.33×10^{-6}	1.80×10^{-5}	1.99×10^{-2}
Test and Maintenance	4.28×10^{-6}	5.87×10^{-6}	8.52×10^{-3}
Total	1.82×10^{-5}	3.96×10^{-5}	5.90×10^{-2}



SOUTH TEXAS PROJECT UNITS 1 & 2

BASIC TASKS OF THE SOUTH TEXAS PROJECT AFWS RELIABILITY EVALUATION

Figure 10 A-1

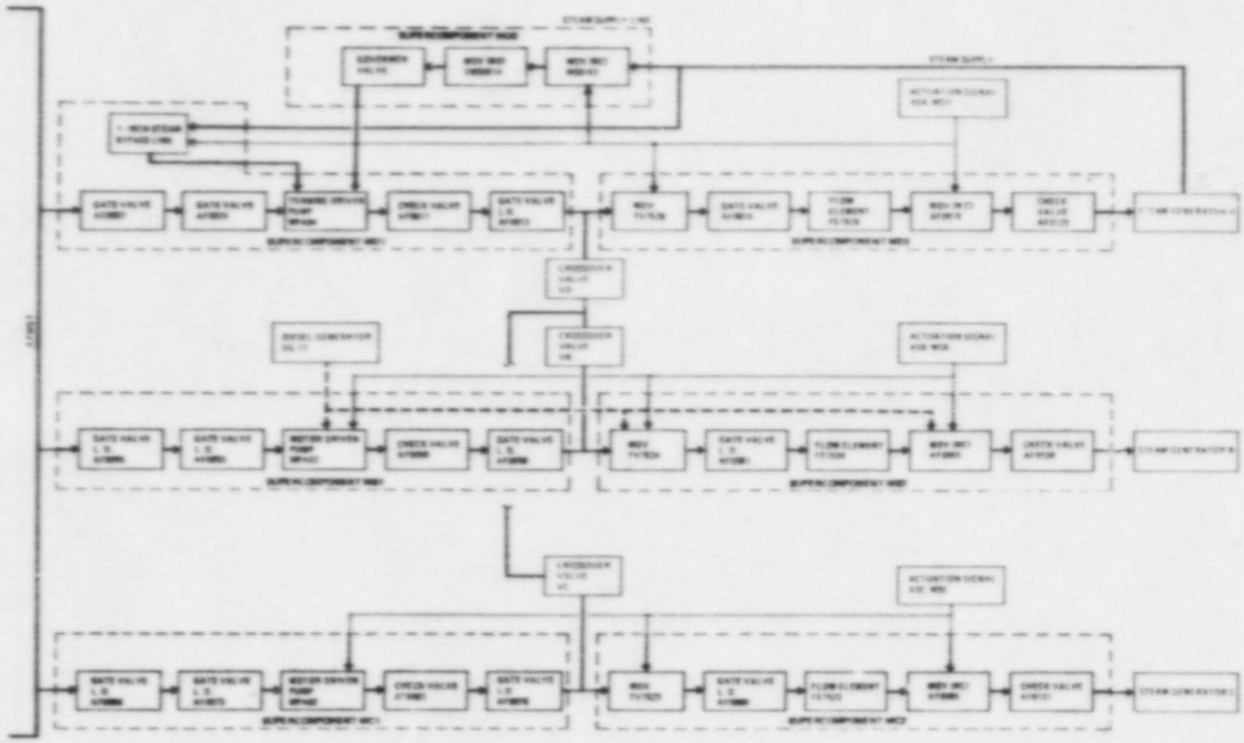


TRAIN A IS NOT SHOWN SINCE IT IS ASSUMED TO BE UNAVAILABLE IN THIS ANALYSIS.

SOUTH TEXAS PROJECT UNITS 1 & 2

SOUTH TEXAS AFWS RELIABILITY BLOCK DIAGRAM (Simplified)

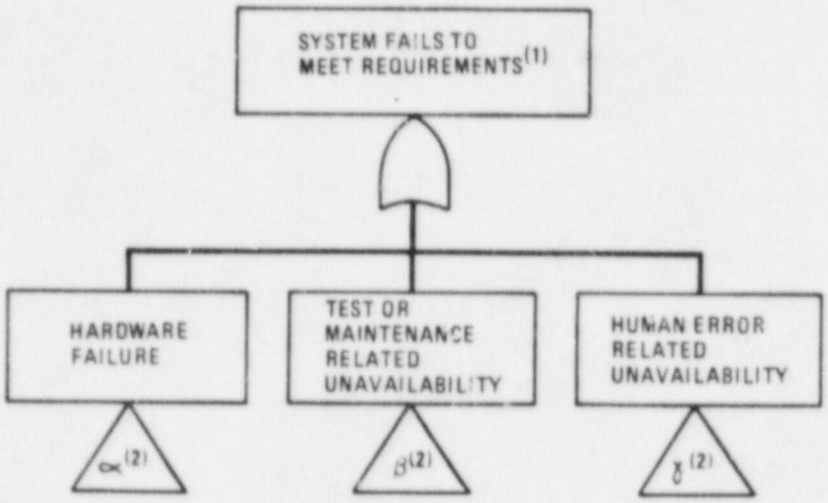
Figure 10 A-3



SOUTH TEXAS PROJECT
UNITS 1 & 2

DETAILED RELIABILITY BLOCK DIAGRAM SHOWING CONSTITUENTS OF SUPERCOMPONENTS

Figure 10 A-4



NOTES:

(1) FAILURE CRITERIA:

CASE I: NO FLOW TO ANY STEAM GENERATOR FOR T ≥ 20 MIN
CASE II: NO FLOW TO ANY STEAM GENERATOR FOR T ≥ 20 MIN
CASE III: NO FLOW TO STEAM GENERATOR D FOR T ≥ 20 MIN

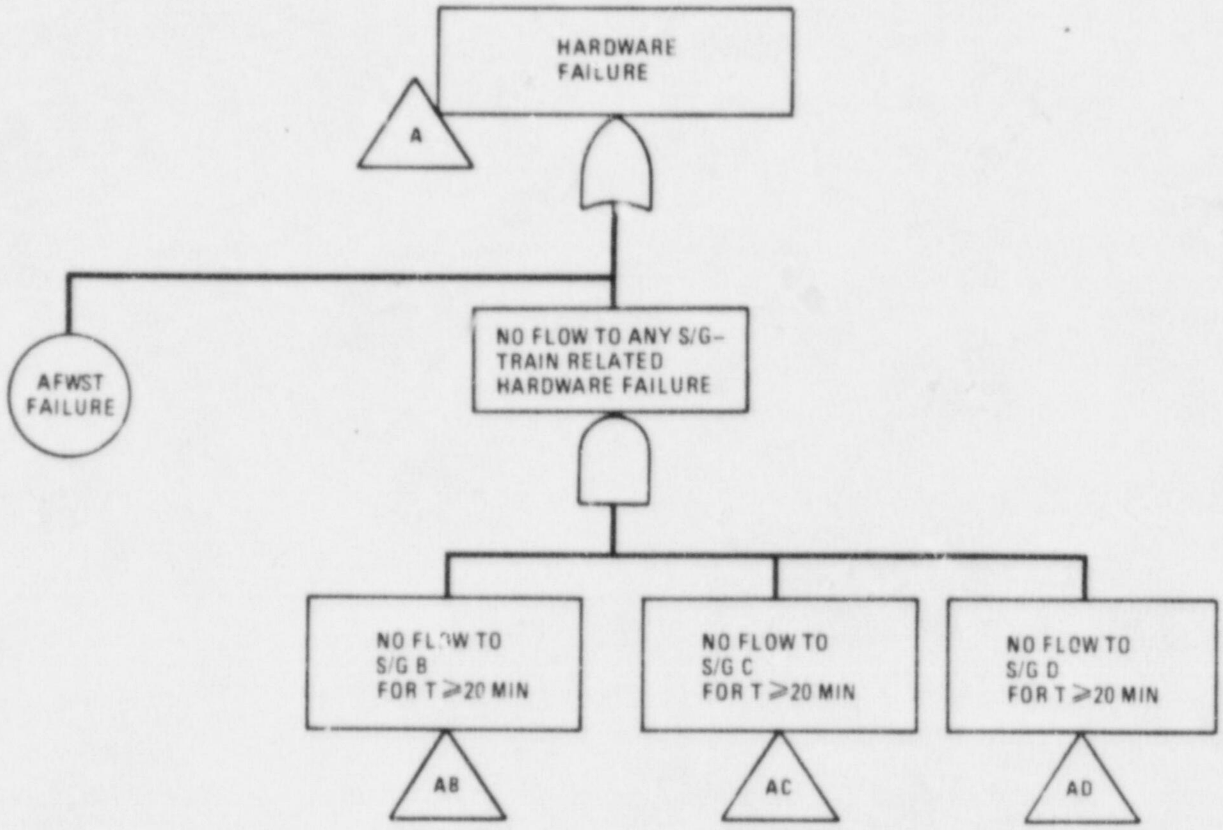
(2)

SUBTREE	LMFW (CASE I)	LMFW/LOOP (CASE II)	LMFW/LOAC (CASE III)
α	A	A	AD
β	B	B	D
γ	C	C	E

SOUTH TEXAS PROJECT UNITS 1 & 2

MASTER FAULT TREE

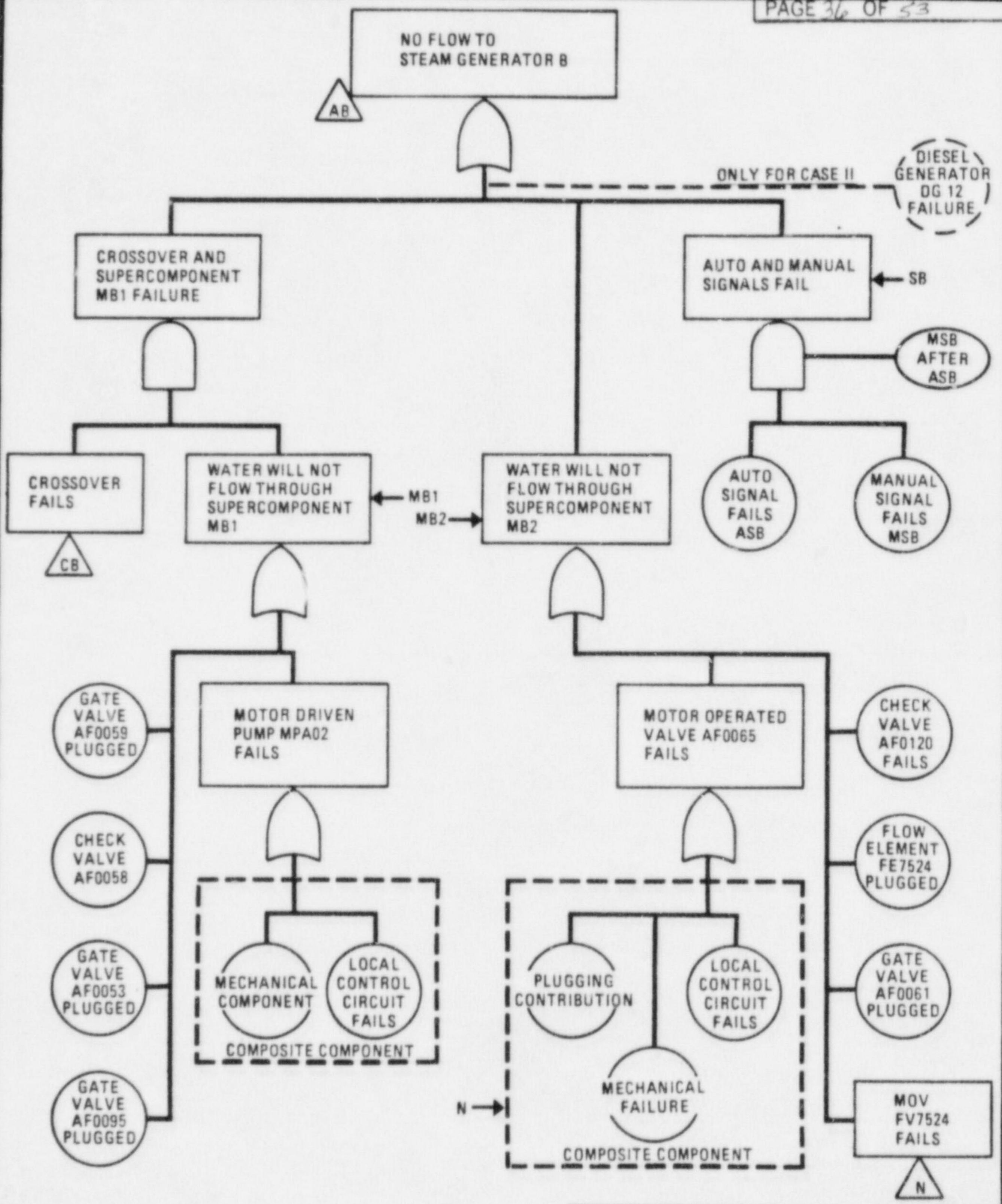
Figure 10 A-5



SOUTH TEXAS PROJECT UNITS 1 & 2

HARDWARE FAULT TREE, CASES I & II

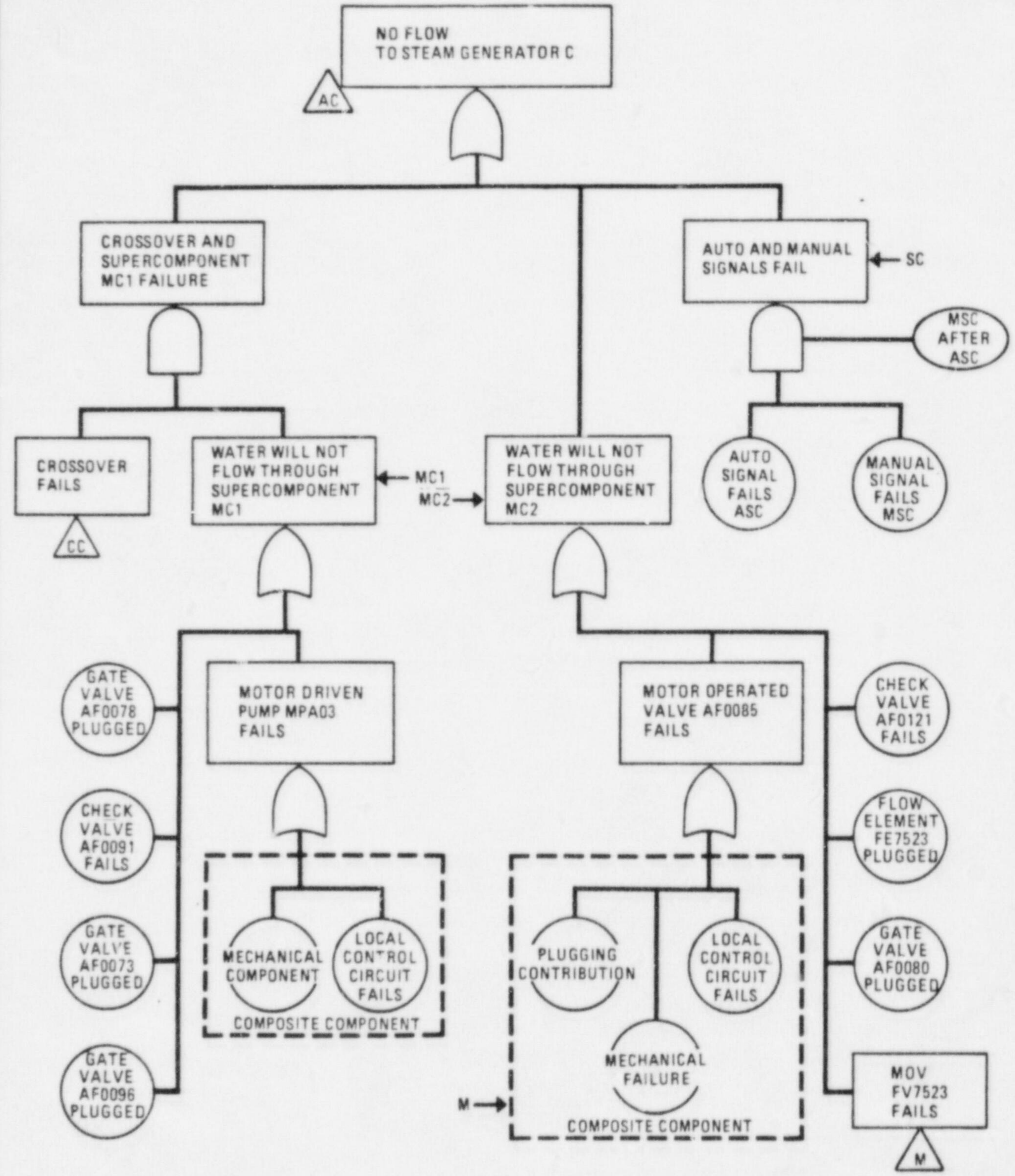
Figure 10 A-6



SOUTH TEXAS PROJECT UNITS 1 & 2

TRAIN B HARDWARE FAULT TREE

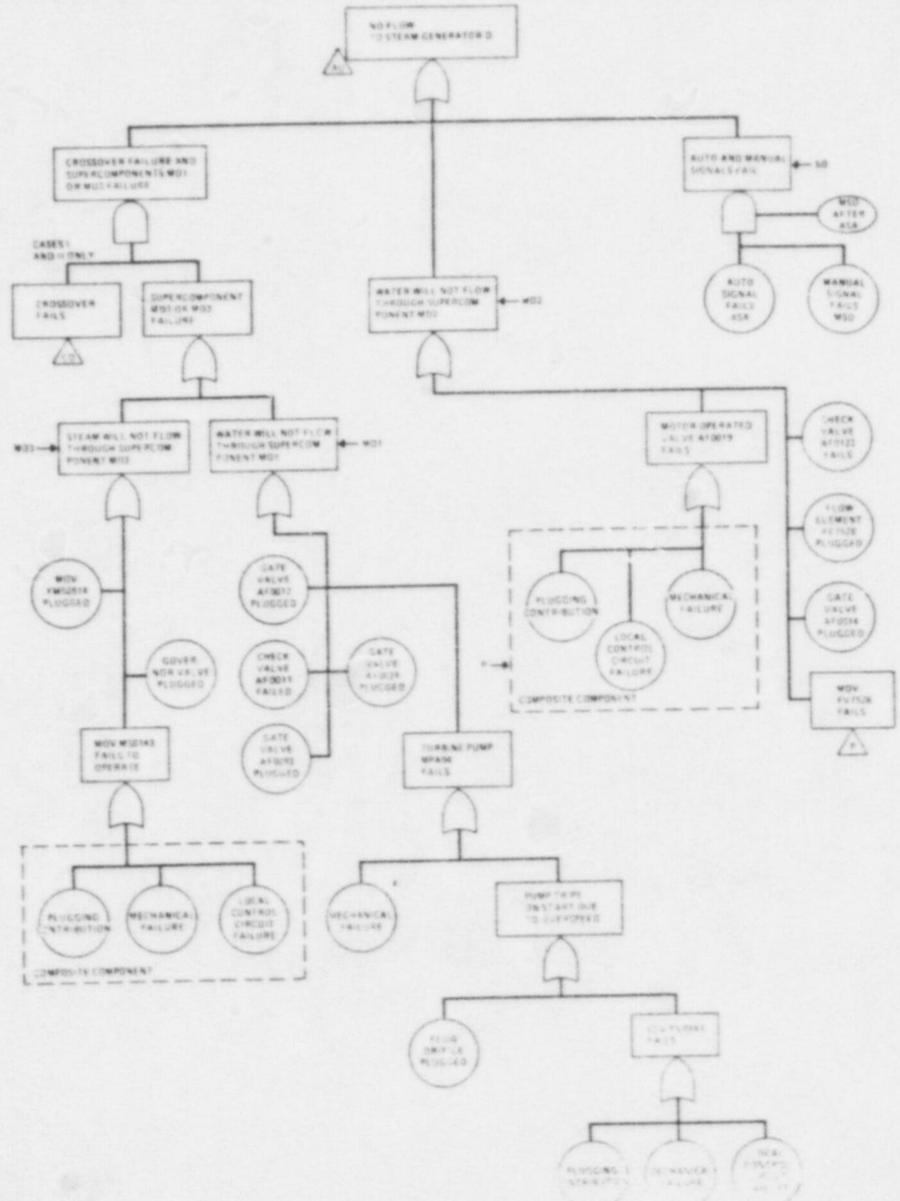
Figure 10 A-7



SOUTH TEXAS PROJECT UNITS 1 & 2

TRAIN C HARDWARE FAULT TREE

Figure 10 A-8



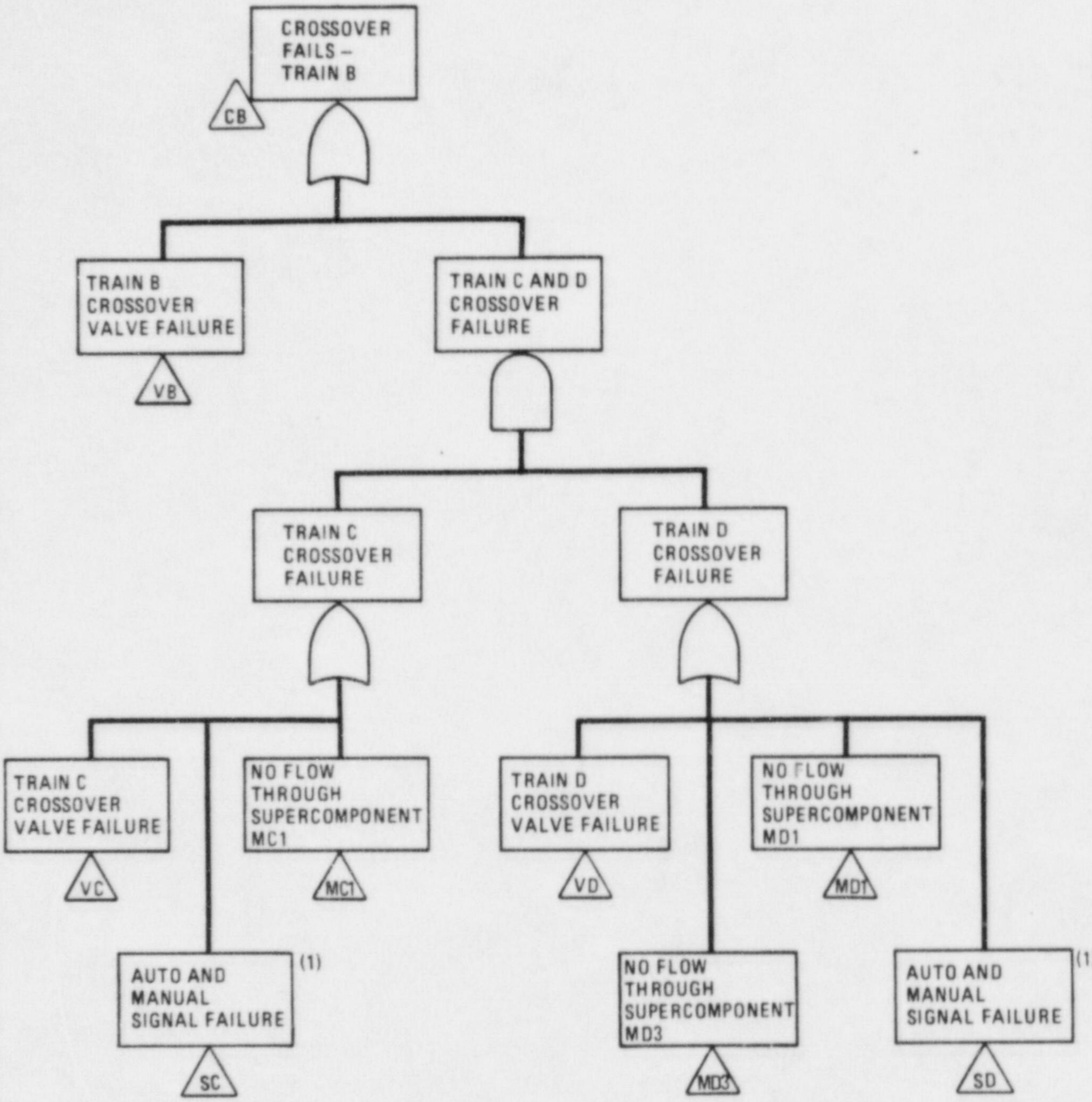
SOUTH TEXAS PROJECT
UNITS 1 & 2

TRAIN D HARDWARE
FAULT TREE

Figure 10 A 9

ATTACHMENT 1
ST-HL-AE- 1413
PAGE 38 OF 53

TRAIN B CROSSOVER FAILURE



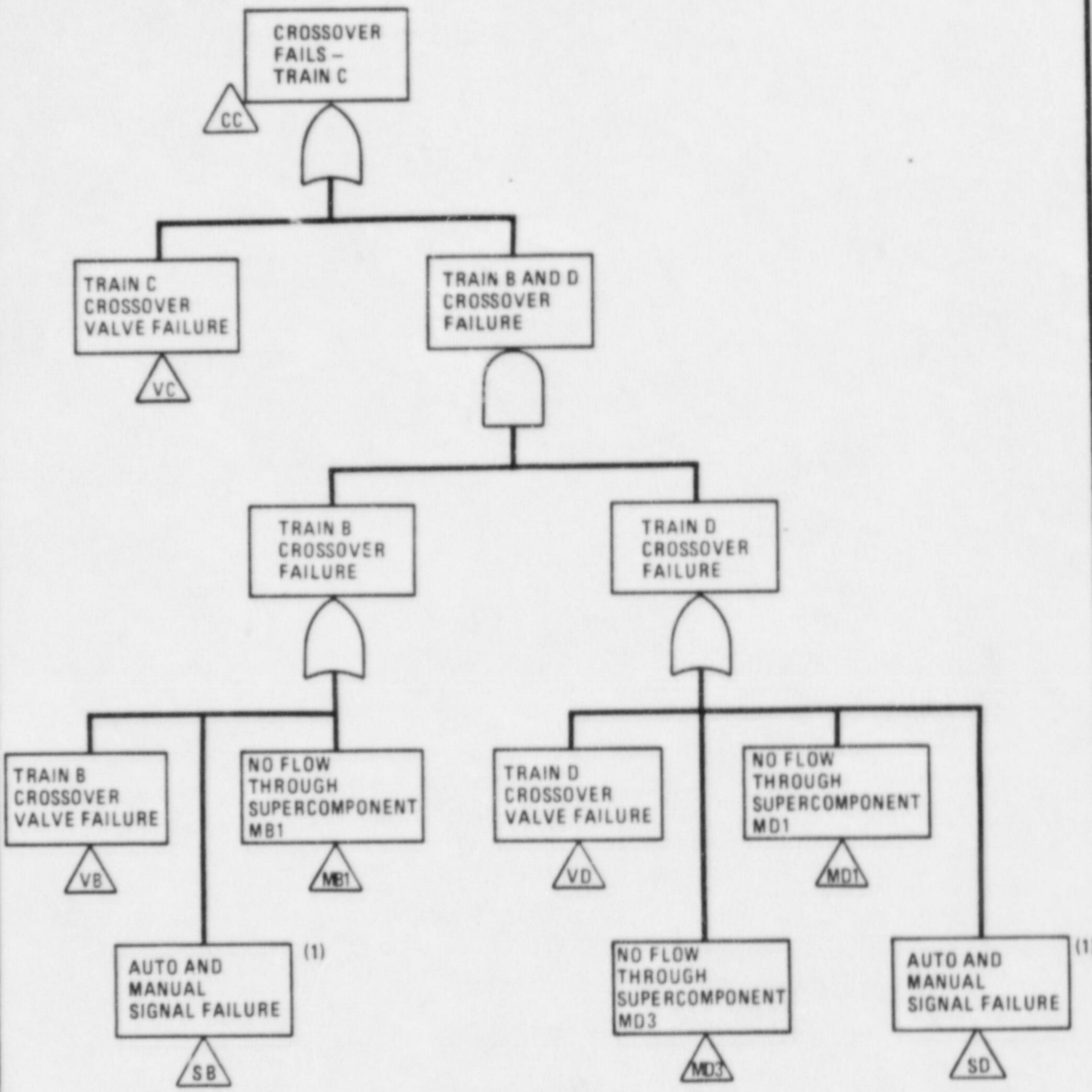
(1) THIS TERM IS NEGLIGIBLE COMPARED TO OTHER HARDWARE FAILURES AND IS NOT INCLUDED IN THE FAULT TREE QUANTIFICATION.

SOUTH TEXAS PROJECT UNITS 1 & 2

SUPPORTING HARDWARE FAULT TREES (Sheet 1 of 4)

Figure 10 A-10

TRAIN C CROSSOVER FAILURE

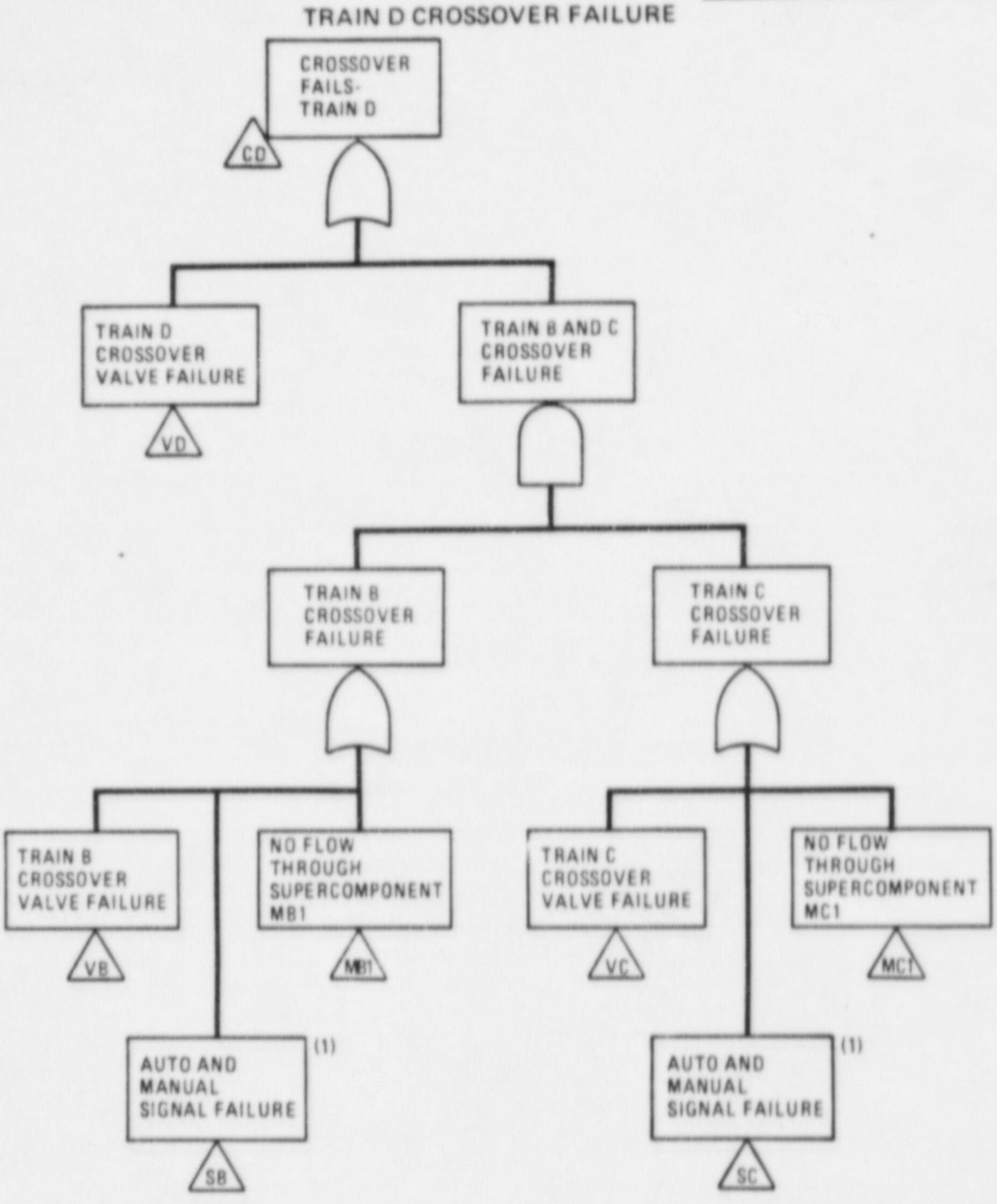


(1) THIS TERM IS NEGLIGIBLE COMPARED TO OTHER HARDWARE FAILURES AND IS NOT INCLUDED IN THE FAULT TREE QUANTIFICATION.

SOUTH TEXAS PROJECT UNITS 1 & 2

SUPPORTING HARDWARE FAULT TREES
(Sheet 2 of 4)

Figure 10 A-10



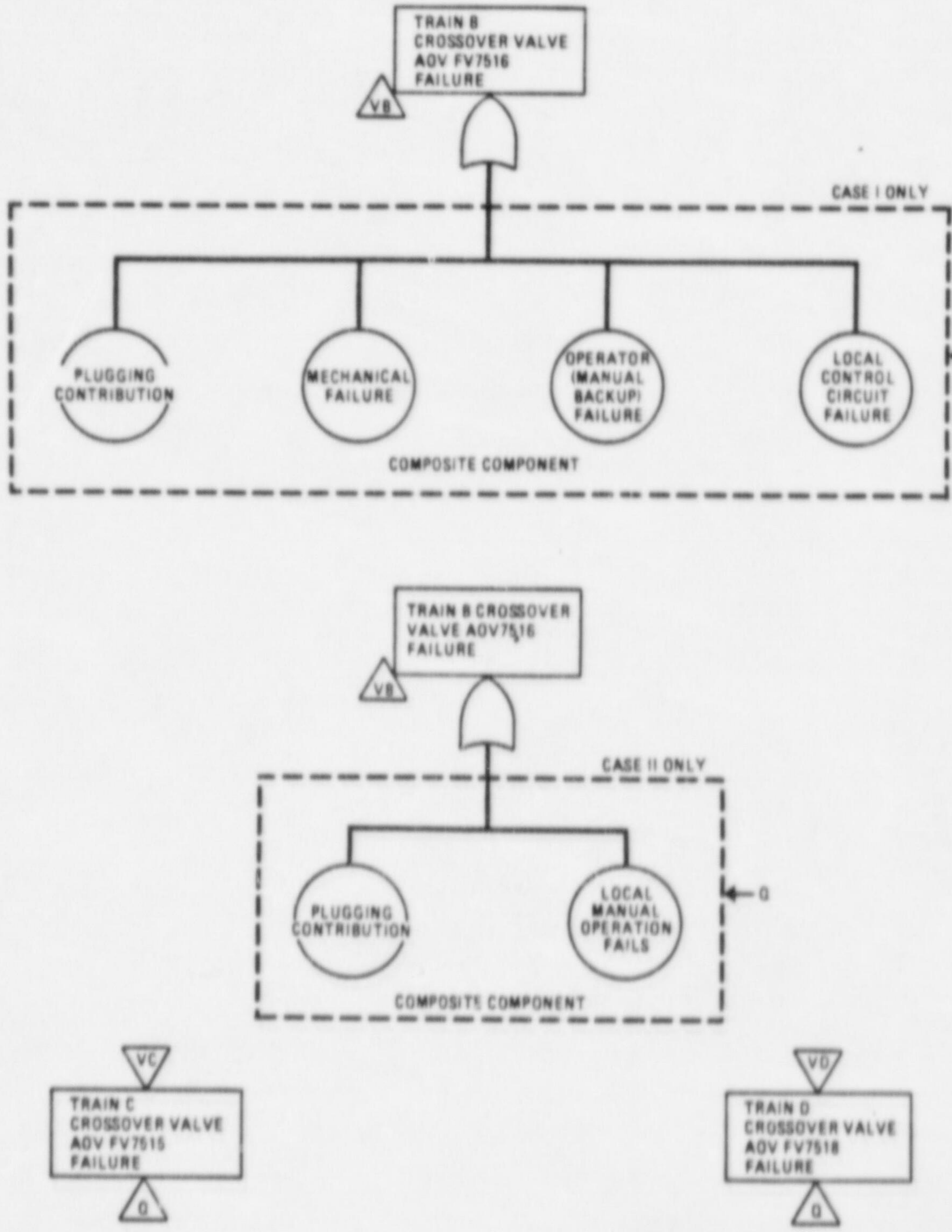
(1) THIS TERM IS NEGLIGIBLE COMPARED TO OTHER HARDWARE FAILURES AND IS NOT INCLUDED IN THE FAULT TREE QUANTIFICATION.

SOUTH TEXAS PROJECT UNITS 1 & 2

SUPPORTING HARDWARE FAULT TREES (Sheet 3 of 4)

Figure 10 A-10

CROSSOVER VALVE FAILURE

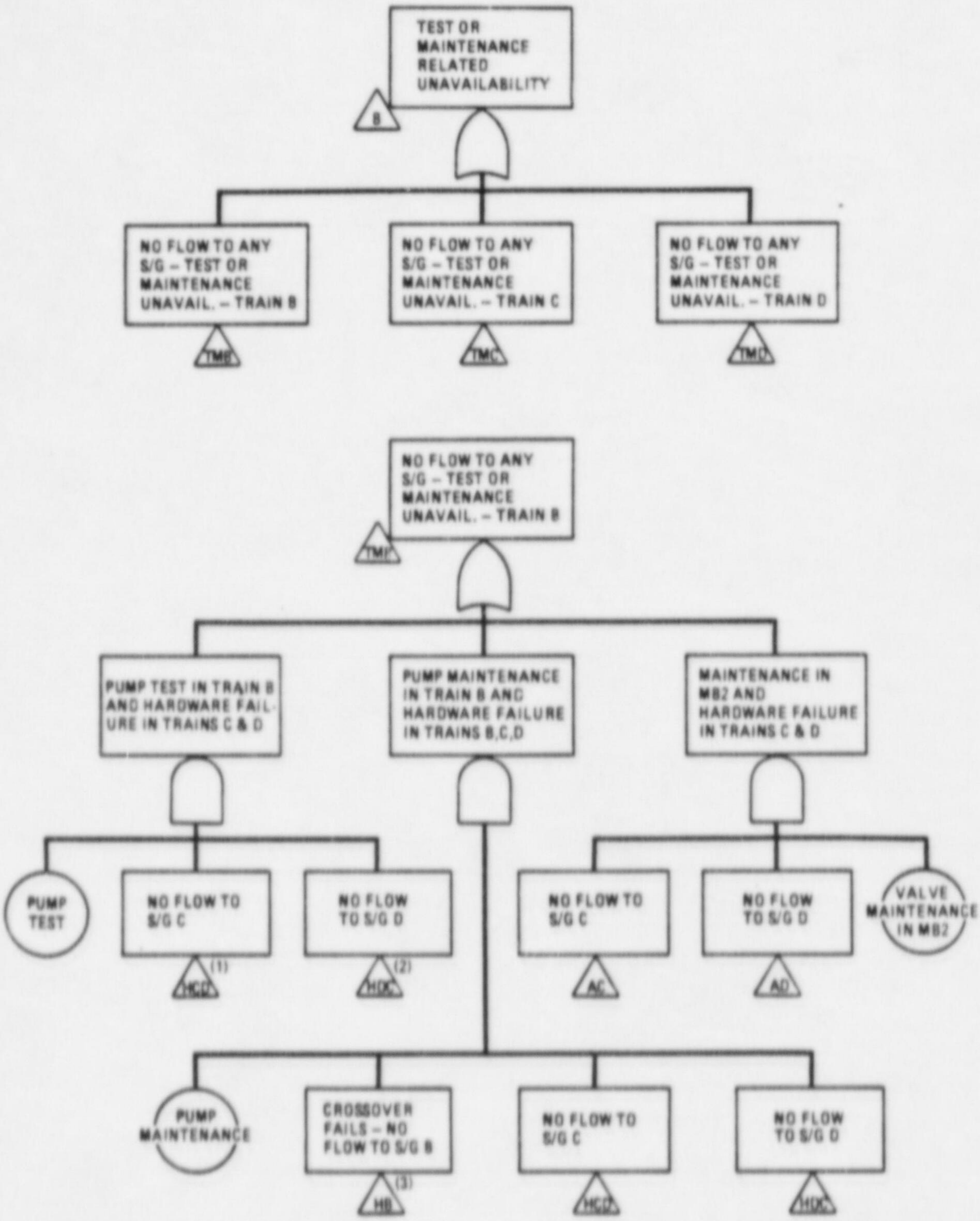


SOUTH TEXAS PROJECT UNITS 1 & 2

SUPPORTING HARDWARE FAULT TREES (Sheet 4 of 4)

Figure 10 A-10

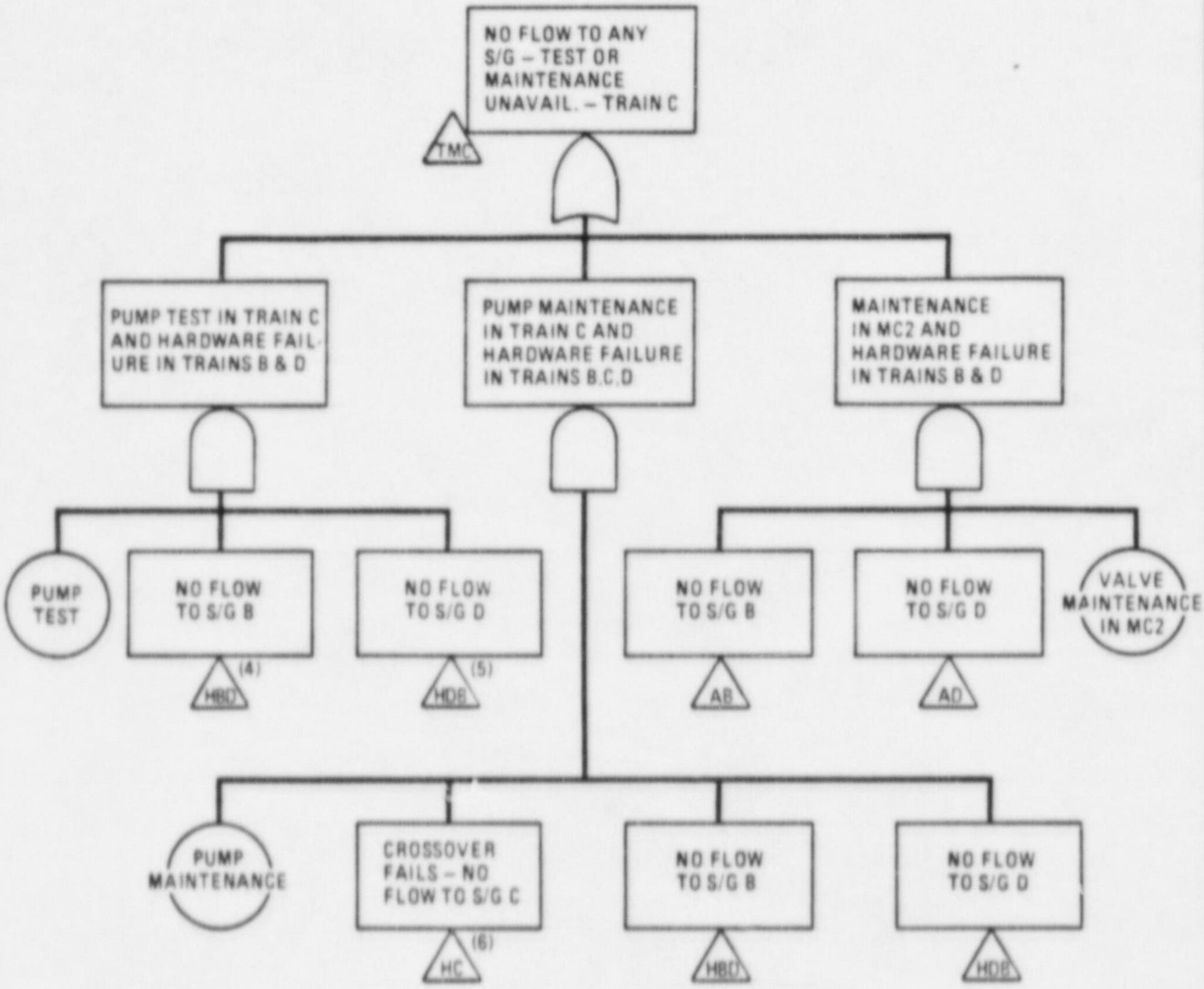
ATTACHMENT 7
ST-HL-AE- 1413
PAGE 43 OF 53



SOUTH TEXAS PROJECT UNITS 1 & 2

TEST AND MAINTENANCE FAULT TREES (Sheet 1 of 4)

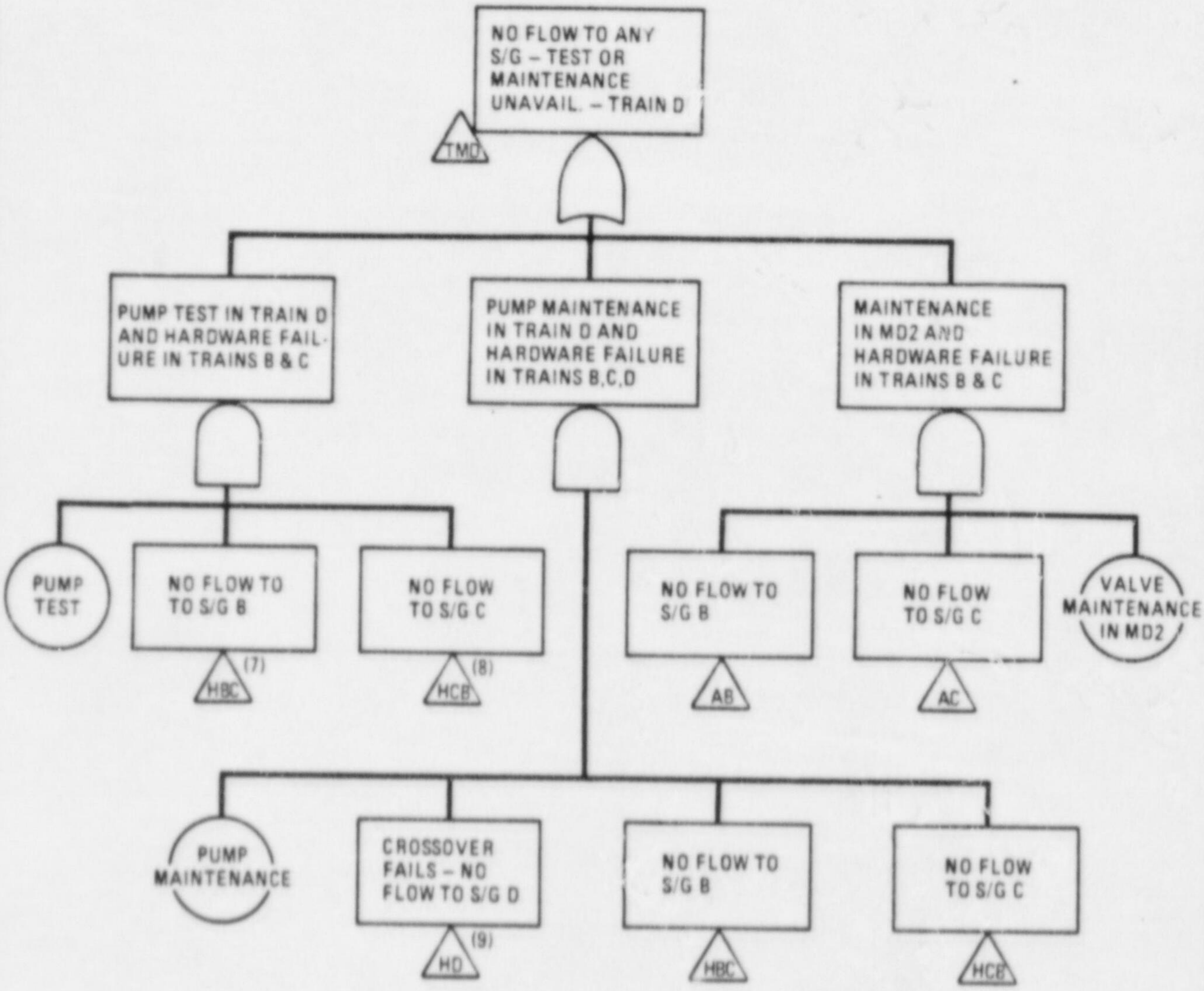
Figure 10 A-11



SOUTH TEXAS PROJECT UNITS 1 & 2

TEST AND MAINTENANCE FAULT TREES (Sheet 2 of 4)

Figure 10 A-11

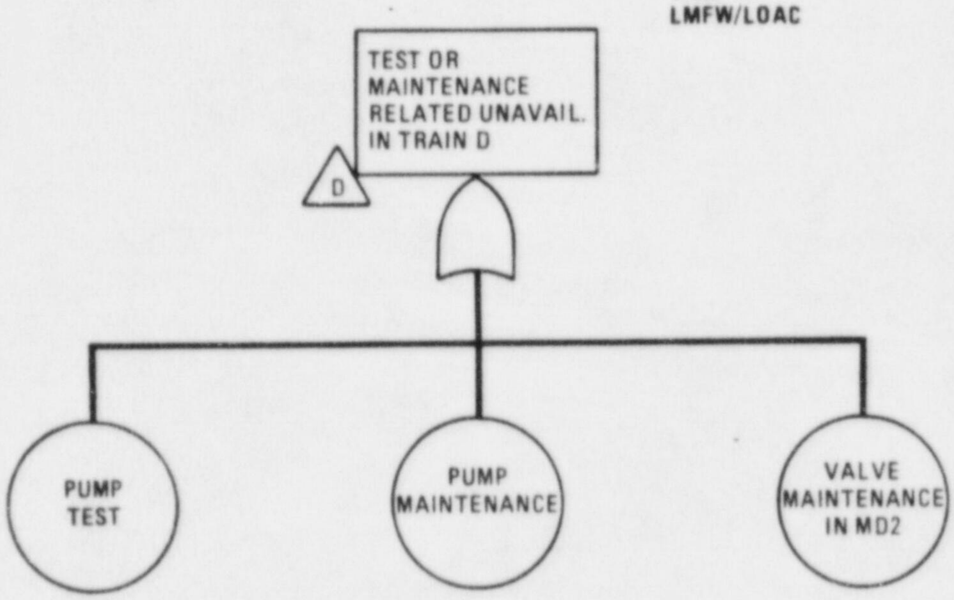


SOUTH TEXAS PROJECT
UNITS 1 & 2

TEST AND MAINTENANCE FAULT TREES
(Sheet 3 of 4)

Figure 10 A-11

CASE III
LMFW/LOAC



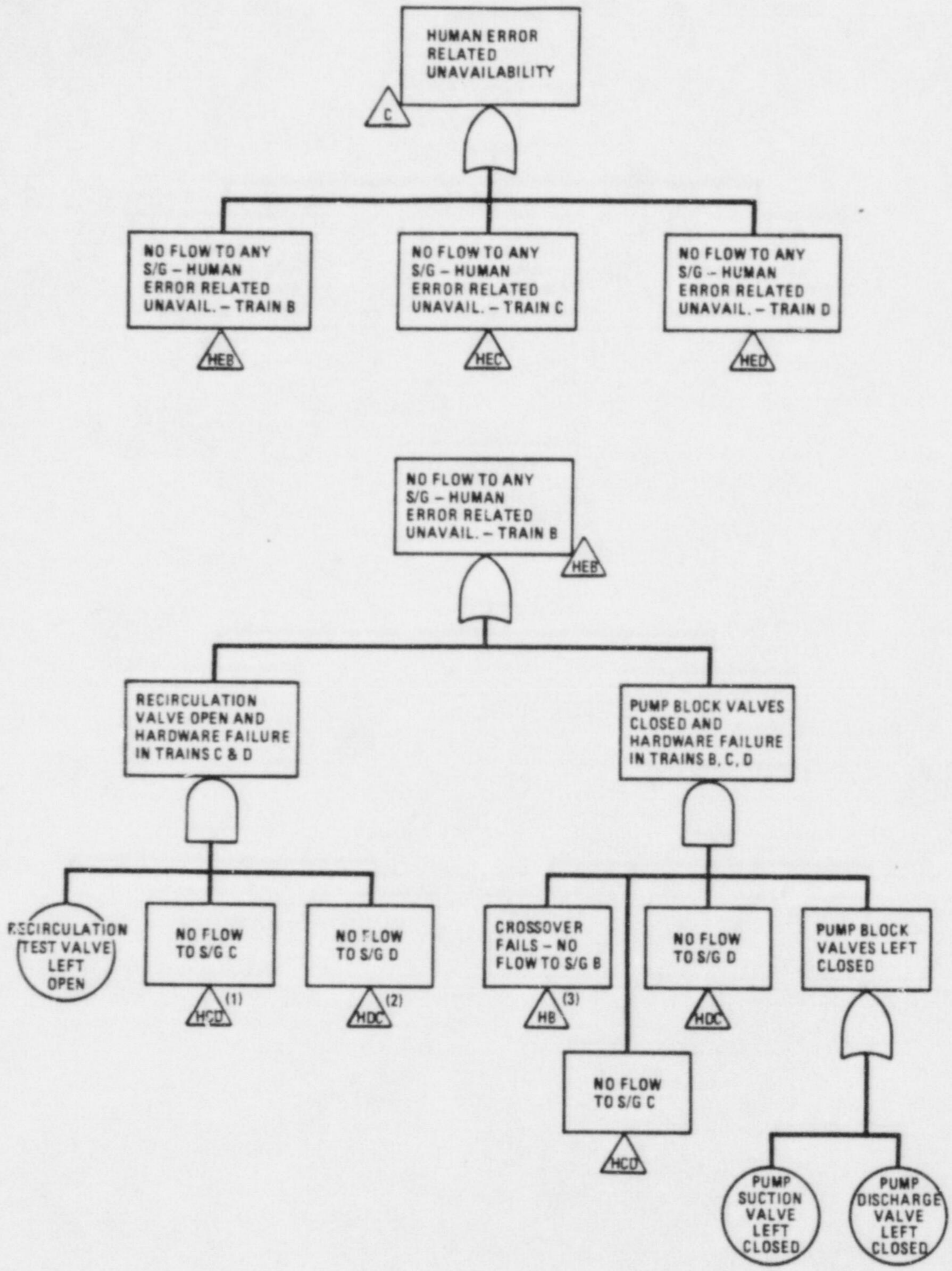
FOOTNOTES: (1) – (9)

SEE FOOTNOTES ON FIGURE 10A-12 FOR EXPLANATION OF THE BOTTOM COMPONENTS IN THESE TREES.

SOUTH TEXAS PROJECT UNITS 1 & 2

TEST AND MAINTENANCE FAULT TREES (Sheet 4 of 4)

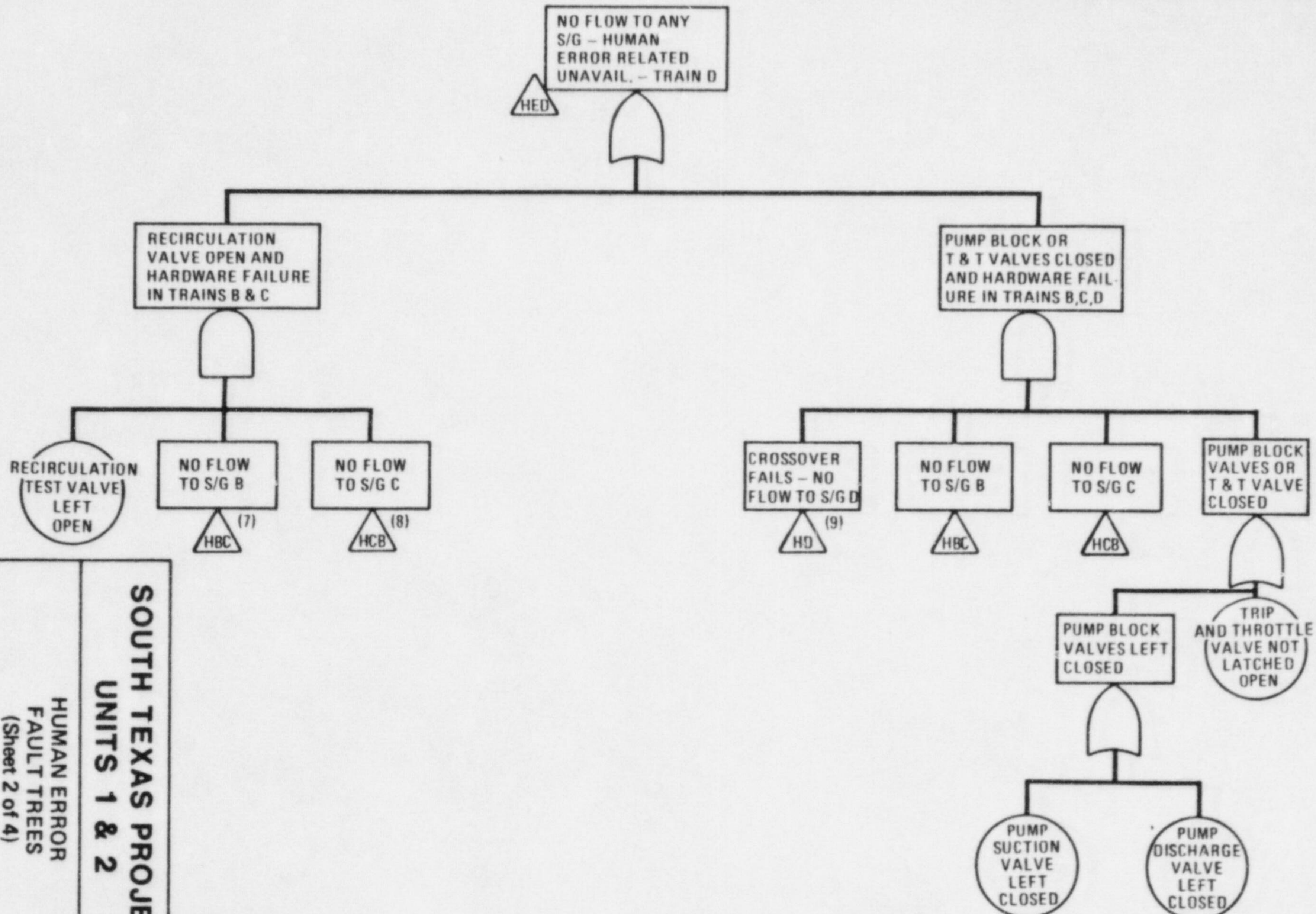
Figure 10 A-11



SOUTH TEXAS PROJECT UNITS 1 & 2

HUMAN ERROR FAULT TREES (Sheet 1 of 4)

Figure 10 A-12

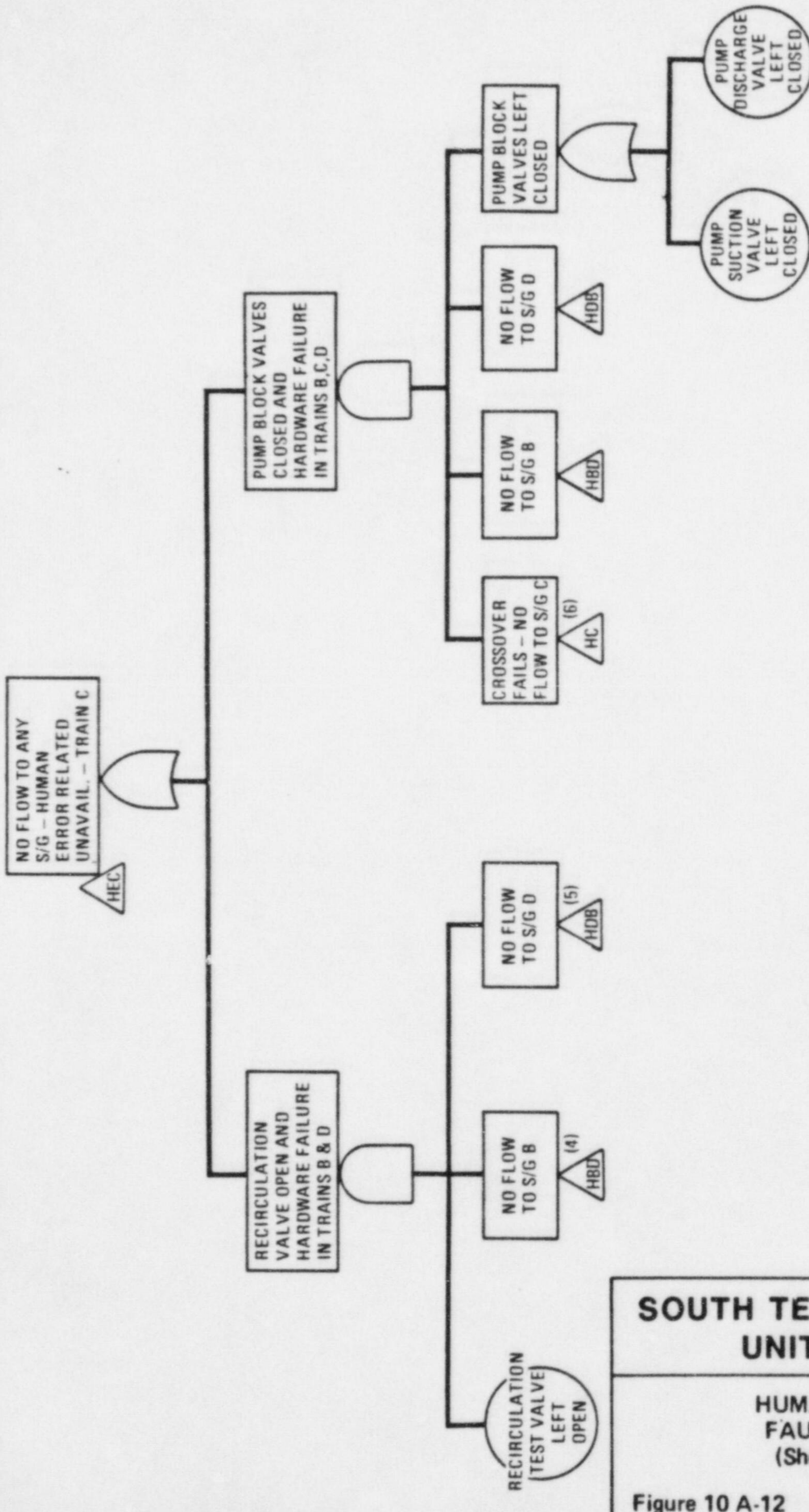


SOUTH TEXAS PROJECT UNITS 1 & 2

Figure 10 A-12

HUMAN ERROR FAULT TREES (Sheet 2 of 4)

ATTACHMENT 1
ST-HL-AE-1413
PAGE 48 OF 53

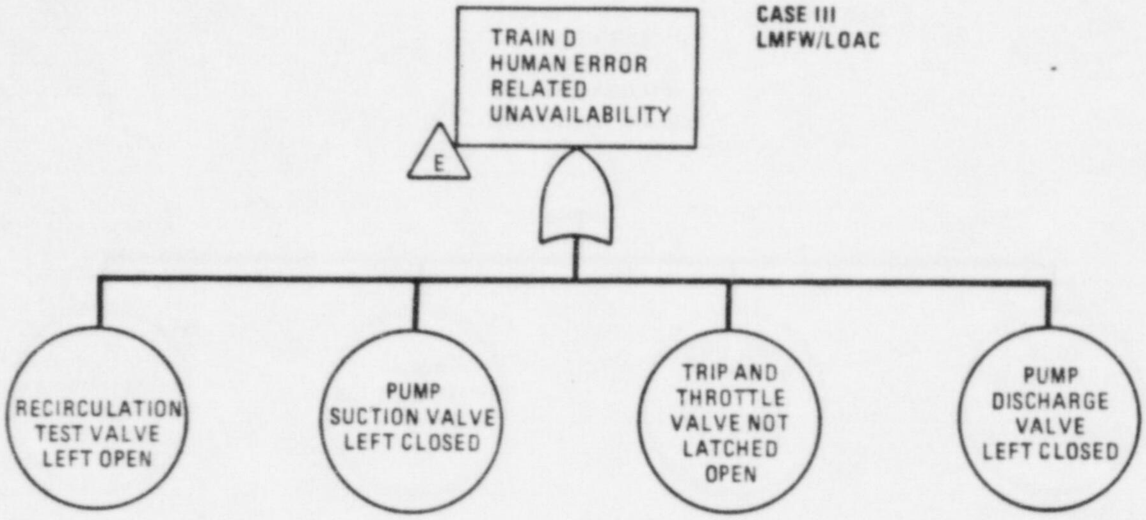


SOUTH TEXAS PROJECT
UNITS 1 & 2

HUMAN ERROR
FAULT TREES
(Sheet 3 of 4)

Figure 10 A-12

CASE III
LMFW/LOAC



FOOTNOTES:

(1) HCD IS IDENTICAL TO AC EXCEPT THAT MB1, VB, AND THE IMMEDIATELY CONNECTING "AND" AND "OR" GATES ARE REMOVED.

(2) HDC IS IDENTICAL TO AD EXCEPT THAT MB1, VB, AND THE IMMEDIATELY CONNECTING "AND" AND "OR" GATES ARE REMOVED.

(3) HB IS IDENTICAL TO AB EXCEPT THAT MB1, AND THE IMMEDIATELY CONNECTING "AND" GATES ARE REMOVED.

(4) HBD IS IDENTICAL TO AB EXCEPT THAT MC1, VC, AND THE IMMEDIATELY CONNECTING "AND" AND "OR" GATES ARE REMOVED.

(5) HDB IS IDENTICAL TO AD EXCEPT THAT MC1, VC, AND THE IMMEDIATELY CONNECTING "AND" AND "OR" GATES ARE REMOVED.

(6) HC IS IDENTICAL TO AC EXCEPT THAT MC1, AND THE IMMEDIATELY CONNECTING "AND" GATES ARE REMOVED.

(7) HBC IS IDENTICAL TO AB EXCEPT THAT MD1, MD3, VD, AND THE IMMEDIATELY CONNECTING "AND" AND "OR" GATES ARE REMOVED.

(8) HCB IS IDENTICAL TO AC EXCEPT THAT MD1, MD3, VD, AND THE IMMEDIATELY CONNECTING "AND" AND "OR" GATES ARE REMOVED.

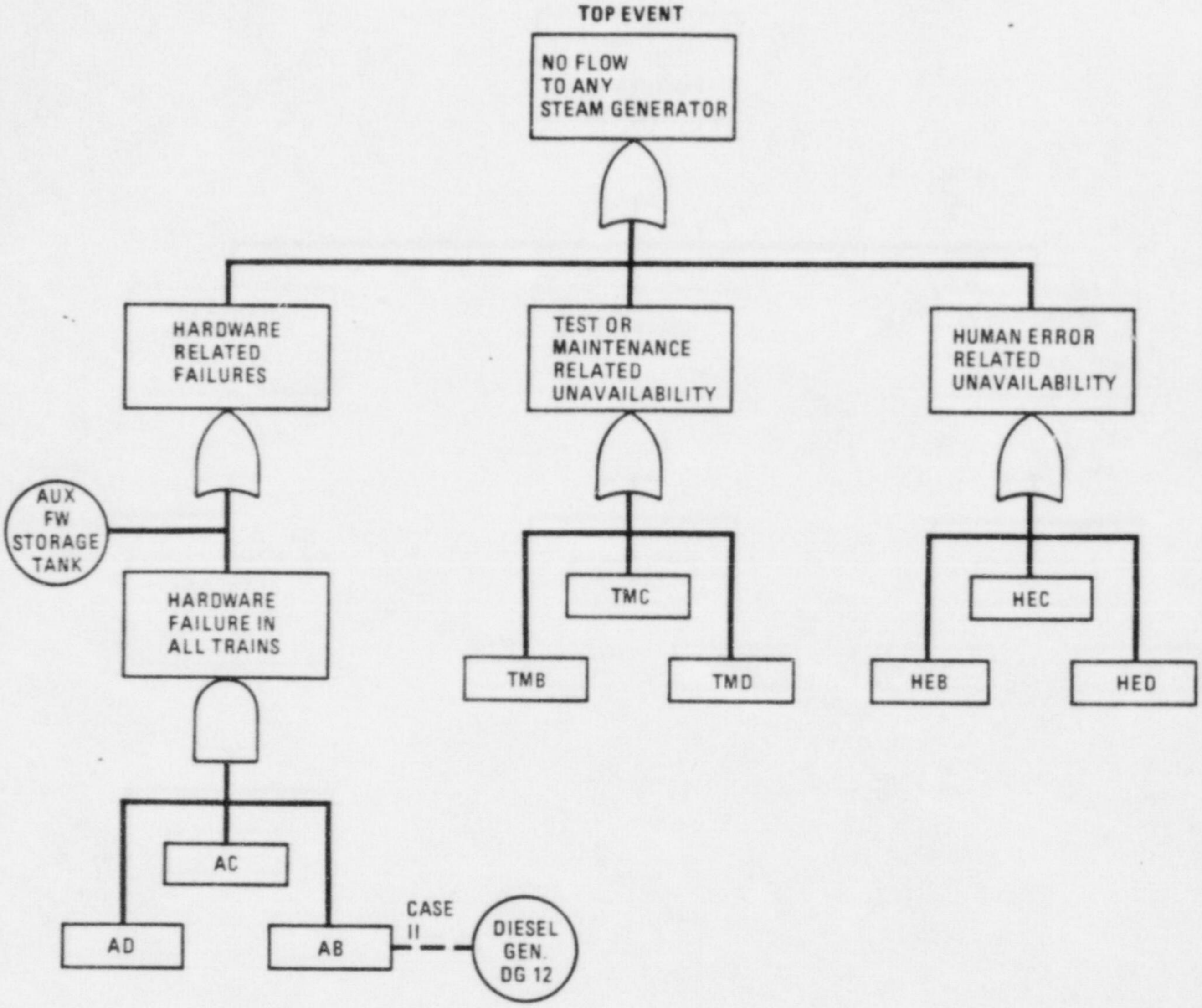
(9) HD IS IDENTICAL TO AD EXCEPT THAT MD1, MD3, AND THE IMMEDIATELY CONNECTING "AND" AND "OR" GATES ARE REMOVED.

COMPONENTS AB,AC, AND AD ARE SHOWN ON FIGURES 10A-7, 10A-8 AND 10A-9. THE CONTINUATION OF THESE TREES WHICH SHOW COMPONENTS MB1, VB, MC1, VC, MD1, MD3, AND VD ARE SHOWN ON FIGURE 10A-10. THE SIGNAL FAILURE TERMS ARE NEGLIGIBLE. AND ARE NOT INCLUDED IN THE QUANTITATIVE ANALYSIS.

SOUTH TEXAS PROJECT
UNITS 1 & 2

HUMAN ERROR
FAULT TREES
(Sheet 4 of 4)

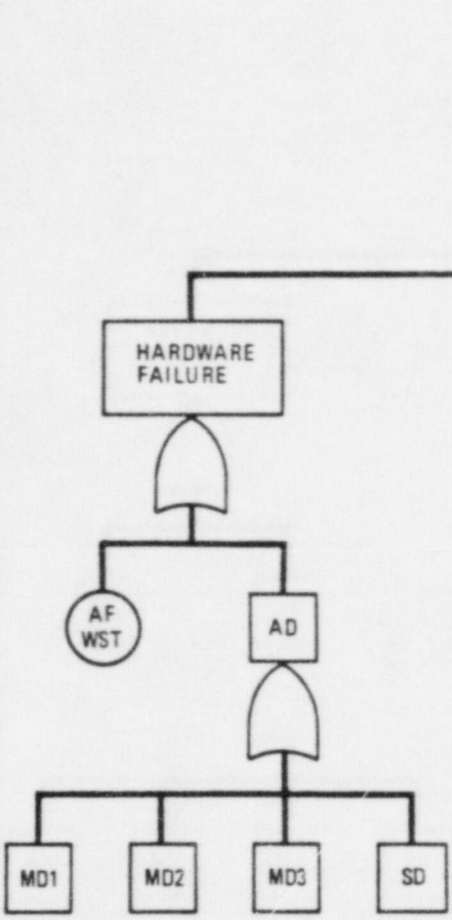
Figure 10 A-12



SOUTH TEXAS PROJECT UNITS 1 & 2

REDUCED FAULT TREE FOR CASES I AND II

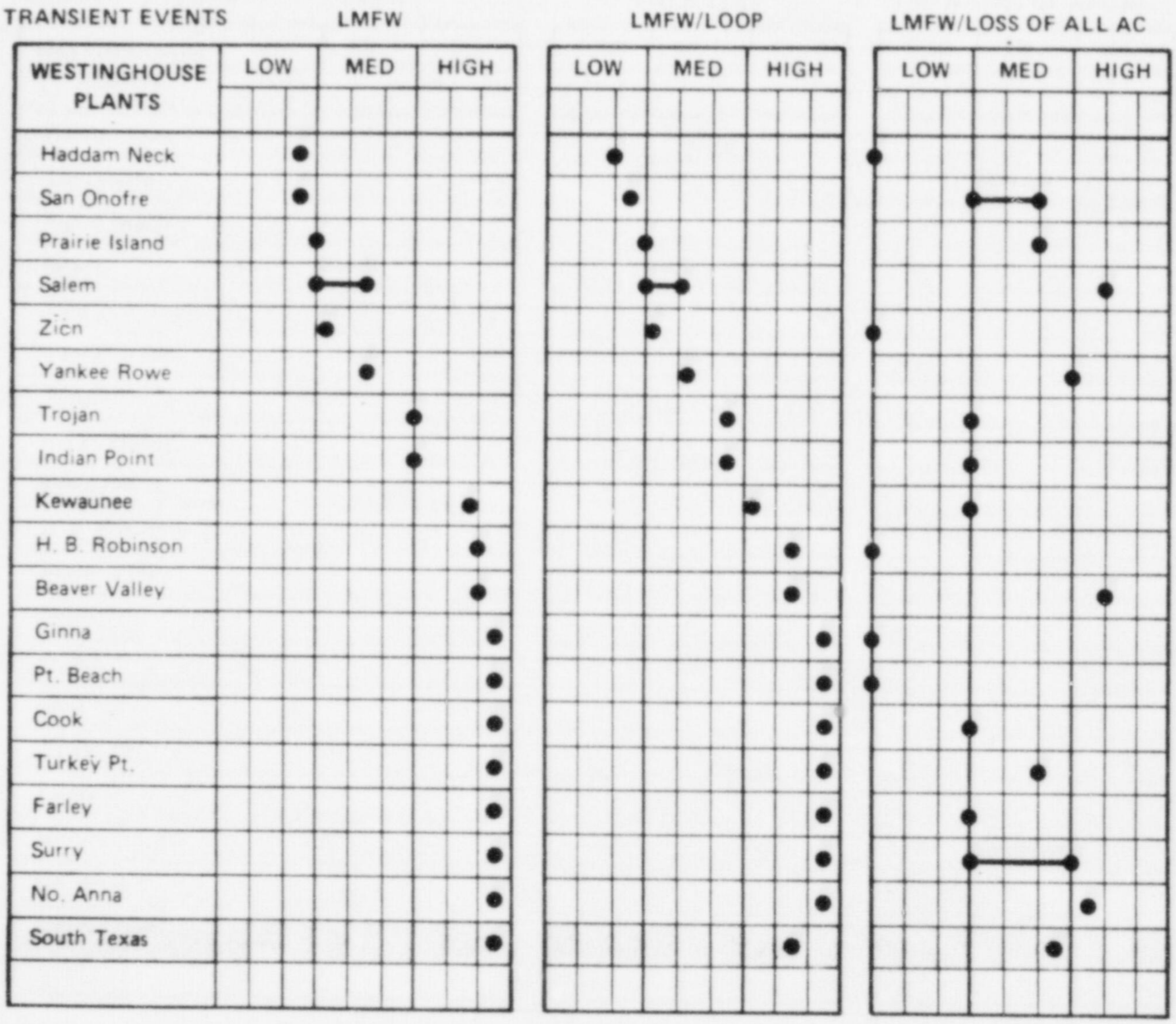
Figure 10 A-13



SOUTH TEXAS PROJECT UNITS 1 & 2

REDUCED FAULT TREE FOR CASE III

Figure 10 A-14



SOUTH TEXAS PROJECT
UNITS 1 & 2

QUALITATIVE COMPARISON OF RELIABILITY CHARACTERISTICS OF STP AFWS, AND AFWS DESIGNS FOR OTHER PLANTS USING WESTINGHOUSE NSSS

Figure 10 A-15