3.0 PLANT SYSTEMS ANALYSIS

In this section, plant systems and operator action failure probabilities are quantified. For this purpose, fault tree analysis is used whenever applicable.

3.1 ON-SITE EMERGENCY POWER

3.1.1 SYSTEM DESCRIPTION

The On-site Emergency Power System is a major support system which supplies power to most front-line systems. It is required to ensure safe plant shutdown or to mitigate the effects of some postulated accidents. The on-site emergency power distribution system supplies power to all critical loads whether or not offsite power is available.

Normally, power is supplied by the plant generator. In the event of a unit trip (i.e., turbine, reactor or generator trip), offsite power becomes the power supply. Upon loss of all offsite power sources, the on-site emergency diesel generators supply power directly to both emergency buses.

The on-site emergency power supply is a self-contained system located within the plant. The emergency supply is comprised of two totally independent, diesel-driven generators. Each emergency generator is dedicated to one of the two emergency buses and provides power to all emergency safety feature equipment and essential loads on that bus. Both diesels are fast started automatically and can accept loads within ten seconds of a loss of offsite power or receipt of an accident signal. The accident signal starts the diesel generators in anticipation of a possible loss of offsite power during or after the accident, but the diesels are not connected to the buses unless the preferred offsite source is lost.

3.1.2 FAULT TREE ANALYSIS

The fault tree for this analysis of the on-site emergency power system is shown in Figure 3.1-1. This section addresses the methods and calculations utilized in the analysis.

8507110476 850628
PDR ADOCK 05000601
K PDR

3.1.2.1 SUCCESS CRITERIA

The On-site Emergency Power System was modeled to determine the unavailability of power at the two emergency buses A and B. The system was modeled in terms of its response to a complete loss of offsite power. Success is the availability of one of the two buses.

3.1.2.2 DEPENDENCE ON SUPPORT STATES

Loss of on-site emergency power, both the loss of both buses and the loss of one bus cases, is modeled within the support states, since AC power is a support system.

3.1.2.3 FAILURE MODEL

Loss of power on an emergency bus is dominated by failure of the diesel generator to start, load or run for the mission time following loss of offsite power. The diesel generators to be used in this design will have at least 97% availability upon demand and during the mission time. Thus the failure
(a,c) probability for loss of power on one emergency bus is [ ]. Of this value,
(a,c) [ ] is attributed to diesel generator unavailability due to maintenance. This unavailability implies that each diesel generator will be in maintenance
(a,c) for [ ] hours a year. The random failures due to all causes are assumed to
(a,c) sum to [ ].

The fault tree for this analysis appears in Figure 3.1-1. The tree is quantified as presented in Section 3.1.3.1. Although no attempt was made to quantify the lower branches that appear on the fault tree, they were included for the purpose of illustration.

3.1.2.3.1 RANDOM FAILURE MODEL

(a,c) As discussed, the portion of the [ ] unavailability of one emergency bus
(a,c) attributed primarily to the random failure of the bus is [ ].

3.1.2.3.2 COMMON CAUSE MODEL

The common cause analysis was developed by using the Beta Factor method described in the guidelines, Appendix 3B.

The common cause calculation for failure of two diesel generators to start and run is as follows:

CCF DG start and run = B_2Q_T = [ ] (a,c)

3.1.2.3.3 TEST MODEL

Each diesel generator is tested monthly on a staggered basis so that one of the two diesel generators is tested every two weeks.

Operational tests are performed during plant refueling shutdowns These tests consist of diesel generator fast start and sequential loading in response to simulated accident and loss of offsite power signals. All protective relays, circuit breakers, load shedding devices and associated equipment are tested.

The diesel generators are not unavailable during these tests.

3.1.2.3.4 MAINTENANCE MODEL

No maintenance is scheduled for the on-site emergency power system during normal reactor operation. Most preventative maintenance is performed during plant refueling outages. Unscheduled maintenance on the diesel generators may take place when problems are discovered during periodic testing. Minor preventative maintenance may be performed when the diesels are taken out of service, but it is assumed that the duration of the maintenance event will not be extended due to preventative activities.

As discussed, the portion of the [ ] unavailability of one emergency bus attributed to unscheduled maintenance of one diesel generator is [ ]. (a,c) (a,c)

3.1.2.3.5 HUMAN ERROR MODEL

Due to the high degree of protective instrumentation and operator awareness of diesel importance, it has been assumed that there are no human errors which could lead to component unavailability in the on-site emergency power system. As mentioned previously, there is no scheduled maintenance. Most preventative maintenance is performed during the scheduled plant refueling outages and unscheduled maintenance is performed only when periodic testing reveals component failure. It is further felt that the failure data for system components implicitly includes contributions from operation errors, and explicit treatment is therefore not necessary.

All diesel generator testing is performed from the control room. Upon completion of the start and run test, the operator secures the diesel generator. The control switch, when released, returns to the normal auto-start position, allowing the diesel to be fast started automatically in the event of an emergency. Any switch failure would be alarmed immediately, as would any other condition adversely affecting diesel generator operation.

Unscheduled maintenance may be required if the results of monthly testing of the diesel generators are unsatisfactory. Upon completion of the repair, the diesel generator would be run for one hour at full load. This test is also performed from the control room as described previously.

3.1.2.3.6 INPUT DATA

The data used in this analysis was taken from the discussion presented in Section 3.1.2.3.1.

3.1.3 FAULT TREE QUANTIFICATION

The following sections describe the results of the quantification of the on-site emergency power system unavailability.

3.1.3.1 SYSTEM UNAVAILABILITY CALCULATIONS

For the loss of both buses case, the system was quantified by hand as follows:

$$Q_{system} = Q_{busA} \times Q_{busB} + Q_{ccf} = [\quad] \qquad \text{(a,c)}$$

For the loss of one bus case, the system unavailability is simply [ ]. (a,c)

In both calculations the value obtained (mean) was squared to obtain an estimate of variance.

3.1.3.2 DOMINANT CUTSETS

For the loss of both buses case, the system failure is dominated by common cause failure of both emergency buses; approximately [ ] percent. (a,c)

For the loss of one of one bus case, the system is dominated by loss of power of the emergency bus due to random faults; approximately [ ] percent. (a,c)

FIGURE 3.1-2

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
ONSITE EMERGENCY POWER SYSTEM
(PROPRIETARY)

3.2 INTEGRATED PROTECTION SYSTEM

3.2.1 SYSTEM DESCRIPTION

3.2.1.1 INTEGRATED PROTECTION SYSTEM

The Integrated Protection System (IPS) is structured of four divisions consisting of cabinets, electronics and other equipment that provide for protection of the plant. The IPS includes the equipment from processor input circuitry and manual actuation switch input circuitry through to the power switching devices that actuate the various component actuation devices controlled by the IPS. A supply of power from the 120 VAC vital bus is required for the IPS to function.

3.2.1.2 VITAL BUS SYSTEM

The 120 VAC Bus System is a safety related, regulated 120 VAC support system. It supplies control and instrument power to the plant protection systems.

The 120 VAC vital bus system normally uses offsite and on-site AC power from the main electric power system but can function independently upon loss of these normal power supplies via the battery and associated inverter.

The 120 VAC vital bus system is divided into four separate channels. The 120 VAC vital bus of each channel receives power from its own solid state inverter through a high speed static transfer switch. The primary source of power to each inverter is from a separate 480 VAC emergency bus through a rectifier. Upon loss of rectifier output, a secondary DC supply to the inverter is immediately available. This supply is from the associated 125 VDC static battery charger and/or battery. Additionally, on loss of inverter output power, the high speed static switch automatically transfers a tertiary source of regulated 120 VAC power to the vital bus. This alternate source is provided from a second 480 VAC emergency bus through a 480 V to 120 V stepdown and regulating transformer.

Each vital bus or channel provides a unique source of power to its corresponding Engineered Safeguards Features (ESF) cabinet or Emergency Generator Loading Sequencer (EGLS) cabinet. Thus, total failure of the vital bus system is defined as loss of 120 VAC power to both trains in the ESF actuation and EGLS systems.

The loss of 125 VDC does not cause a direct loss of IPS divisions, but is equivalent to such a loss because it prevents actuation of components.

The voltage of each 120 VAC vital bus is continuously monitored and displayed in the control room. An alarm is sounded in the control room upon a change of state in the static transfer switch due to loss of inverter output.

3.2.2 ANALYSIS AND RESULTS

These systems were not analyzed specifically for this study, however Westinghouse in-house studies provide information useful in this instance.

These in-house studies indicate the Integrated Protection System/Vital Bus System unavailability value for failure of four IPS Divisions to be [ ]. (a,c)

The dominant contributor to unavailability of the Integrated Protection System/Vital Bus System is the unavailability of 120 VAC vital bus power, contributing approximately 97%.

3.3 SERVICE WATER-COMPONENT COOLING WATER SYSTEM

3.3.1 SYSTEM DESCRIPTION

The Service Water-Component Cooling Water (SW-CCW) system analyzed in this study utilizes a body of water such as a river, lake, or ocean as the ultimate heat sink. There are no cooling towers, fans, basins, etc. in the system. The SW-CCW system consists of four service water pumps and four component cooling water pumps connected in two trains, i.e., A and B pumps feed one set of heat loads and C and D pumps feed a second set of heat loads. The service water trains feed separate headers, therefore service water pumps A or B can feed either component cooling water HX A or B or both. The same situation applies to SW and CCW pumps C and D. The service water trains draw water from and return it to the body of water which is the ultimate heat sink for the system.

Service water pumps A and B feed through a single strainer as do trains C and D through their own single strainer. A standby strainer is provided for each pair of pumps. Differential pressure gauges are provided across each of the four strainers to indicate the degree of cleanliness of the strainers during operation. In the event the differential pressure indication approaches the specified limit, the standby strainer may be manually valved into service. The operating strainer may be manually valved out and back flushed for cleaning.

During normal reactor operation, with all AC power available, one CCW pump, CCW heat exchanger, one SW pump and associated equipment and one SW strainer will be operating for each train, i.e., two of four CCW pumps, two of four heat exchangers, two of four service water pumps and two of four service water strainers. An equal number of components are in standby. For purposes of discussion, as well as the construction of the fault trees, CCW pumps A and C, heat exchangers A and C, service water pumps A and C and service water strainers A and C are assumed to be operating with components B and D in standby. Standby components are modeled to start and operate.

Under conditions of loss of offsite power and diesel generator(s) startup, the operating pumps stop and must restart. Under conditions of loss of one bus, the operating pumps stop and must restart when the diesel generator starts.

SW-CCW system emergency operation requires the isolation of certain normal operation heat loads and the assumption of others (See Table 3.3-1). The heat loads are redundant and are divided between the two SW-CCW subsystems. Group 1 heat loads correspond to components A and B and Group 2 loads correspond to components C and D.

A simplified flow diagram of the Service Water-Component Cooling Water system appears in Figure 3.3-1.

3.3.2 FAULT TREE ANALYSIS

The fault tree analysis of the SW-CCW was performed in accordance with the guidelines of Section 3.10. The fault tree developed for the unavailability of both trains with offsite power available is presented in Figure 3.3-2 (SW-CCW). The system components are listed in Table 3.3-2.

The unavailability of both trains in conjunction with the loss of offsite power which requires running pumps to stop and restart is also studied.

To simplify the fault trees, subtree transfer techniques have been used which have created cutsets that are physically impossible. This is conservative since these cutsets do not exist in reality. These cutsets have been removed from the lists of dominant contributors although the values of these cutsets have not been removed from the unavailability values obtained from the quantifications.

The remainder of this section addresses the methods and calculations utilized in the analysis.

3.3.2.1 Success Criteria

The success criteria of the Service Water-Component Cooling Water system is affected by whether or not the non-emergency heat loads are isolated. In the event all non-emergency heat loads are isolated, the following success criteria apply:

Either the Group 1 or Group 2 heat loads must receive adequate flow. Either one of the two component cooling water pumps with its associated heat exchanger can provide adequate flow. One service water pump and one service water strainer are adequate.

In the event all non-emergency heat loads are not removed, the following success criteria apply:

Either the Group 1 or Group 2 heat loads must receive adequate flow. If only one group is receiving flow and one of the heat loads in that group fails to isolate, then two CCW pumps and their associated heat exchangers must provide adequate, cooled flow. One SW pump and strainer supplying these two CCW heat exchangers are adequate for this case.

Further information about the heat and flow loads to be isolated and those to be valved in is detailed in Table 3.3-1.

3.3.2.2 Dependence on Support States

The Service Water-Component Cooling Water system depends only on AC power for system operation. The offsite AC power available, loss of offsite power with on-site AC power, loss of one bus and no power available cases have been analyzed. The SW-CCW is modeled and used as a support system itself. Refer to Sections 4.1.2 and 4.2.2 for calculations of support state split fractions.

3.3.2.3 Random Failure Model

The following assumptions were utilized in the development of the fault tree for this analysis:

1. During normal reactor operation, with all AC power available, at least two pumps will be operating. It is assumed for the analysis that SW-CCW trains A and C are running and B and D are in standby. The SW-CCW mission time is assumed to be 24 hours.

2. During reactor operation with loss of offsite power, the operating pumps are assumed to stop and to require restart.

3. During reactor operation with loss of one bus, the operating pumps are assumed to stop and to require restart.

4. The heat exchangers and block valves that interface with dependent emergency systems, such as motor cooling, are not included in this analysis, but are included in the analyses of these dependent systems.

5. The heat exchangers and block valves for non-emergency systems are included in this analysis since their failure to isolate adversely impacts the SW-CCW system. This is very conservative since it takes no credit for operator isolation of non-essential loads.

6. Manual switchover from an operating SW strainer to a standby strainer in the event the operating strainer becomes clogged is modeled on the basis that the clogging will be relatively gradual, detectable and that action will be feasible within the twenty-four hour mission time.

7. No credit is taken for the fact that the Residual Heat Removal system does not need SW-CCW cooling flow for long term cooling for at least the first one-half hour into the emergency and possibly much longer.

3.3.2.4 Common Cause Analysis

The common cause analysis of the SW-CCW system addresses potential common cause failures between the a) standby SW pumps; b) normally running SW pumps; c) standby CCW heat exchanger motor-operated valves; d) standby CW pumps;

e) operating CCW pumps; f) standby SW strainers; g) operating SW strainers; h) each pair motor-operated valves for non-essential heat loads. In those cases where the normally running pumps stop and must restart, the common cause calculations assume that all 8 CCW and SW pumps are standby pumps and need to be started. (Human error common cause failure is discussed in Section 3.3.2.6.)

Calculations:

The random failure unavailability and beta factors are the same for both the service water pumps and component cooling water pumps, so a single calculation will serve for both component types.

1. CCF calculations for standby SW and CCW pumps:

   CCF SW-CWW start and run = B_2Q_T = 0.1 X 2.81E-03 = 2.81E-04

2. CCF calculations for operating SW and CCW pumps:

   CCF SW-CCW run = B_2Q_T = 0.1 X 1.40E-03 = 1.40E-04

3. CCF calculation for motor-operated valves:

   CCF MOV open = B_2Q_T = 0.1 X 5.77E-03 = 5.77E-04

4. CCF calculation for operating SW strainers:

   CCF strainer operating = B_2Q_T = 0.1 X 7.20E-04 = 7.20E-05

5. CCF calculation for standby SW strainers:

   CCF strainer standby = B2QT = 0.1 X 7.20E-04 = 2.95E-05

6. CCF calculation for operating and standby SW and CCW pumps restart and start and run (one of four success criteria):

   CCF all SW-CCW start and run $6B_2Q_T^3 + 4B_3Q_T^2 + B_4Q_T$

   $= 6(.1)(2.81E\text{-}03)^3 + 4(.1/5)(2.81E\text{-}03)^2 + (.1/10)(2.81E\text{-}03)$

   $= 2.87E\text{-}05$

   The values were entered at the appropriate points in the fault tree. The methodology used and the beta factors and their development are described in Appendix 3B.

7. The common cause failure of the isolation of the non-essential heat loads is estimated separately below. The contribution of the dominant cutsets resulting from this failure is added to unavailability calculated by the fault tree analysis. Note that this failure has not been modeled in the fault tree.

   For each set of motor-operated valves used in isolation of the heat loads a common cause failure of $q = \beta_2 q_{MOV} + 0.1\ (5.77 \times 10^{-3}) = 5.8 \times 10^{-4}$. For two such sets of valves, the total failure of isolating any of the non-essential loads is $q = 2 \times 5.8 \times 10^{-4} = 1.2 \times 10^{-3}$. Note that isolation of the heat loads to RCP motors is not included since there are two sets of two valves for isolation of that non-essential load.

3.3.2.5 Test and Maintenance Model

Testing of components is not modeled because any test would not render the system inoperative. In addition, two of the four SW-CCW trains are running, on an alternating basis, during normal reactor operation.

Unavailability due to maintenance is included for the standby SW-CCW trains. The methodology used and the quantification is contained in Appendix 3B.

3.3.2.6 Human Error Model

The Service Water-Component Cooling Water system has two of the four trains operating on an alternating basis during normal reactor operation and the isolation of various loads as well as the startup of the standby trains during an emergency is automatic. The system is generally not subject to human errors of omission or commission.

The possibility of the clogging of an operating strainer is modeled along with those operations necessary to switchover to the standby strainer. The switchover operations modeling includes unavailability due to human errors.

The human error unavailability values were entered at the appropriate points in the fault tree. The methodology used and the unavailability values development are described in Appendix 3B.

3.3.2.7 INPUT DATA

The component failure rate data used in these analyses was taken from the WAPWR master databank (SIMON.DATA, Appendix 3B). This master data was supplemented by the common cause failure calculations specific to these analyses.

The following assumptions were made regarding data:

Service water pump failure rates are based upon clear fluid service and may or may not apply to seawater service,

Strainer failure rates are also based upon freshwater service and again may or may not apply to seawater.

Three different sets of input data were utilized for quantification, assuming system symmetry on the two power buses. The variables were the availability of 4160 VAC buses as follows: 1) offsite power available; 2) loss of offsite power; 3) loss of one (either) power bus; and 4) loss of all AC electric power (both buses).

An input listing of component identifiers and associated probabilities for analysis of the SW-CCW with all power available is presented in Table 3.3-3.

The input listings of component identifiers and associated probabilities for analysis of the SW-CCW with loss of offsite power and the SW-CCW with loss of one (either) power bus are not presented.

The loss of all electric power (both buses) is not necessary to model due to the unavailability of power to the pumps.

3.3.3 FAULT TREE QUANTIFICATION

The following sections describe the results of the quantification of the SW-CCW unavailability.

3.3.3.1 System Unavailability Calculations

The quantification of the SW-CCW fault tree was accomplished using the WAMCUT code to obtain the system and subsystem unavailability values. The WAMCUT code was used to identify the dominant cutsets and their contributions to system unavailability. The results are presented in Table 3.3-4.

The major cutsets derived for system failure and the relative probabilities are presented in Tables 3.3-5 and 3.3-6. The contributions of these cutsets to system unavailability are presented in the tables as relative percentages.

TABLE 3.3-1

HEAT LOADS TABLE FOR SW-CCW

	Heat Load Name	Group 1 (Train AB)	Group 2 (Train CD)	Normal Reactor Operation		Emergency Reactor Operation	
				ON	OFF	ON	OFF
1.	Instrument Air Compressor	X	X	X		X	
2.	RHR/CS pump miniflow	X	X		X	X	
3.	RHR/CS pump miniflow	X	X		X	X	
4.	HHSI,RHR/CS pump oil and motor	X	X	X		X	
5.	HHSI,RHR/CS pump oil and motor	X	X	X		X	
6.	Charging pump oil & water	X	X	X		X	
7a.	Waste disposal building	X		X			X
b.	Sampling	X		X			X
c.	Miscellaneous	X		X			X
8a.	BRS evaporator		X	X			X
b.	Seal Injection HX		X	X			X
c.	Miscellaneous		X	X			X
9.	Spent fuel pit HX	X	X	X			X
10.	CCW pump motor	X	X	X		X	
11.	CCW pump motor	X	X	X		X	
12.	RCP thermal barrier and oil	X	X	X		X	
13.	RCP thermal barrier and oil	X	X	X		X	

TABLE 3.3-1 (cont.)
HEAT LOADS TABLE

Heat Load Name	Group 1 (Train AB)	Group 2 (Train CD)	Normal Reactor Operation		Emergency Reactor Operation	
			ON	OFF	ON	OFF
14. RHR HX	X	X		X	X	
15. RHR HX	X	X		X	X	
16. Letdown HX		X	X			X
17a. Fan cooler (running)	X	X	X		X	
b. Fan cooler (running or standby)	X	X	(X)	(X)		X
18a. RCP motor	X	X	X			X
b. RCP motor	X	X	X			X
c. RCDT HX	X		X			X
Excess Letdown HX	X		X			X

TABLE 3.3-2

LIST OF COMPONENTS FOR SW-CCW

System Component	Bus A Dependent	Bus B Dependent	Tested (Note 1)	Maintained (Note 2)	Human Error (Note 3)
[					] (a,c)

TABLE 3.3-2 (cont.)

LIST OF COMPONENTS

System Component	Bus A Dependent	Bus B Dependent	Tested (Note 1)	Maintained (Note 2)	Human Error (Note 3)
[					] (a,c)

TABLE 3.3-2 (cont.)

LIST OF COMPONENTS

System Component	Bus A Dependent	Bus B Dependent	Tested (Note 1)	Maintained (Note 2)	Human Error (Note 3)
[					] (a,c)

NOTES:

1. Testing does not render portions of the system inoperative. In addition, two of four SW-CCW trains are running, on an alternate basis, during all normal reactor operation.

2. Service Water trains B and D, Component Cooling Water trains B and D and Service Water strainers B and D are assumed to be in standby and their components can therefore be maintained.

3. Human Error Symbols

   FR = Failure to restore after test or maintenance
   FO = Failure to open
   FC = Failure to close

TABLE 3.3-3

SW-CCW COMPONENT FAILURE PROBABILITIES

(a,c)

TABLE 3.3-3 (cont.)

SW-CCW COMPONENT FAILURE PROBABILITIES

(a,c)

TABLE 3.3-3 (cont.)

SW-CCW COMPONENT FAILURE PROBABILITIES

(a,c)

TABLE 3.3-3 (cont.)

SW-CCW COMPONENT FAILURE PROBABILITIES

(a,c)

TABLE 3.3-3 (cont.)

SW-CCW COMPONENT FAILURE PROBABILITIES

(a,c)

TABLE 3.3-3 (cont.)

SW-CCW COMPONENT FAILURE PROBABILITIES

(a,c)

TABLE 3.3-4

SUMMARY OF RESULTS FOR SW-CCW

Description	SW-CCW System Unavailability	
	Mean	Variance
[		] (a,c)

TABLE 3.3-5

DOMINANT CUTSETS FOR SW-CCW

Unavailability of both SW-CCW trains
(all power available to both buses)

[ ] (a,c)

TABLE 3.3-6

DOMINANT CUTSETS FOR SW-CCW, LOSS OF ONE BUS

Unavailability of one particular train
(all power available to the bus)

Dominant Cutsets	Relative Contribution (%)
[	(a,c)]

(a,c)

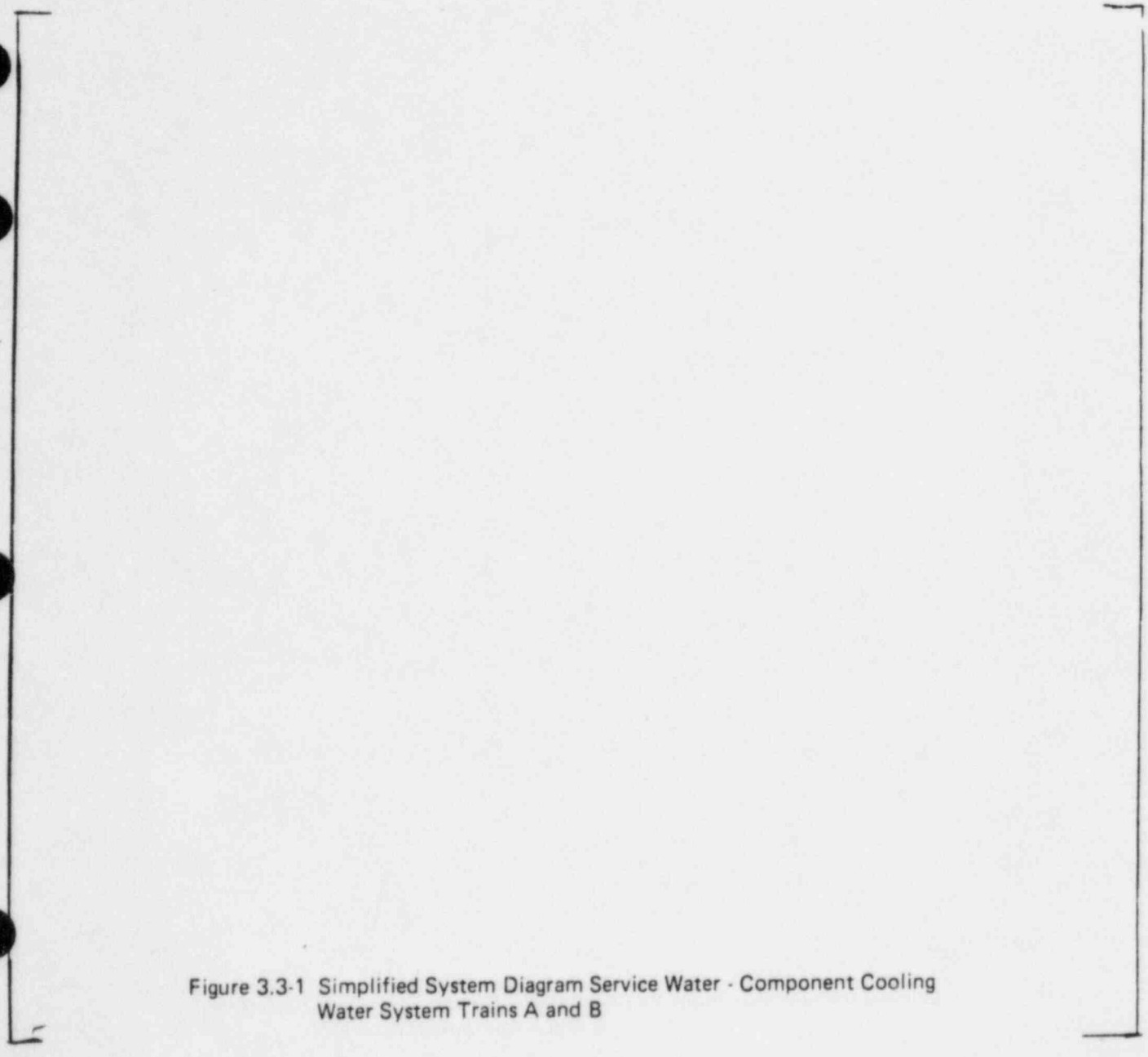


Figure 3.3-1 Simplified System Diagram Service Water - Component Cooling Water System Trains A and B

FIGURE 3.3-2

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
COMPONENT COOLING WATER SYSTEM
(PROPRIETARY)

3.4 INTEGRATED SAFEGUARDS SYSTEM

3.4.1 SYSTEM DESCRIPTION

The Integrated Safeguards System (ISS) consists of four identical and separate mechanical subsystems. The ISS is powered by two separate and redundant emergency electrical power trains and receives actuation signals from two separate and redundant actuation cabinets. One subsystem is shown schematically in Figure 3.4-1 in its normal valve alignment.

The basic configuration consists of:

- o Four pumping subsystems each containing one high-head and one low-head pump.
- o An emergency water storage tank located inside the containment building.
- o Four accumulators
- o Four core reflood tanks
- o Four residual heat removal heat exchangers
- o Two spray additive tanks

The accumulators, core reflood tanks and residual heat removal heat exchangers are located inside the containment building. The pumping subsystems are located in the auxiliary building and are kept physically separate from each other. Since only the pumps and their associated piping and valves are located outside containment, the ISS minimizes the components associated with any post-accident recirculation of highly radioactive fluid outside containment. It is proposed that each of the four ISS pumping subsystems be housed in separate containment pressure pump enclosures (CPPE). This total containment encapsulation concept for the ISS eliminates the potential for post-accident releases of highly radioactive liquid or gases into the auxiliary building and subsequently into the environment.

With the CPPE concept or with the more traditional filtered, vented pump compartment design, the four pumping subsystems, or modules, can be physically independent and are identical to each other. Each pumping module contains one

low-head pump, one low-head pump miniflow heat exchanger, one high-head pump and the associated piping and valves necessary for these pumps to perform their intended safety functions.

The high-head pumps, which perform the safety injection function, are aligned to take suction from an Emergency Water Storage Tank (EWST) and to deliver coolant to the reactor coolant system via the Residual Heat Removal (RHR) heat exchangers and the four separate reactor vessel injection nozzles. The EWST is located at a low elevation inside the containment building.

The low-head pumps are primarily residual heat removal pumps, which are used for plant cooldown and during refueling operations to remove decay heat. During residual heat removal operation they take suction from the Reactor Coolant System hot legs and recirculate coolant through the core via the RHR heat exchangers and the four reactor vessel injection nozzles. However, during a LOCA or steam break accident, these pumps function as containment spray pumps. They are aligned to take suction from the EWST and deliver water to the containment spray ring headers on receipt of a high containment pressure actuation signal.

The four core reflood tanks provide a supplemental injection flow to the Reactor Coolant System (RCS) during the post accident reflood phase following an intermediate to large LOCA. The core reflood tanks represent a passive injection subsystem which delivers coolant to the RCS via the four reactor vessel injection nozzles. This passive subsystem is a low pressure, high resistance, low flow system.

The four accumulators provide a rapid reflood of the reactor vessel lower plenum and downcomer volumes following an intermediate to large LOCA. The accumulators represent a passive injection subsystem which delivers coolant to the RCS via the four RCS cold legs. The accumulators are a higher pressure, low res tance, high flow system.

In the event that the normal CVCS letdown/boration capability was not available, feed and bleed emergency letdown/boration operation would be utilized to achieve a cold shutdown boration of the RCS prior to emergency

plant cooldown operations. Two emergency letdown lines are routed directly from the RCS hot legs to the EWST. The high-head pumps would be used during this operation to provide the borated makeup to the RCS from the EWST.

Safety Injection

The four high-head pumps are the safety injection pumps. In the event that a safety injection ("S") signal were initiated, these pumps would start automatically and inject coolant directly into the reactor vessel downcomer. Each high-head pump is aligned to take suction from the EWST located inside the containment and to deliver directly to the reactor vessel. All valves in this flow path are normally open. Therefore, the only action required to establish emergency core cooling is the automatic starting of the high-head pumps. There are no piping interconnections between these four separate high-head subsystems. The four high-head pumps are sized such that one high-head pump would be sufficient to prevent core uncovery for small LOCAs up to at least a break equivalent to a break of a 6 inch diameter pipe. Each high-head pumping system is provided with a normally closed flow path to a corresponding RCS hot leg. Several hours after a LOCA, all ISS pumping systems could be temporarily realigned for hot leg recirculation to ensure termination of boiling within the core.

In the event of a steam break accident, the high-head pumps inject borated water into the RCS with sufficient shutdown reactivity to compensate for the change in the RCS volume and counteract the reactivity increase caused by the resulting system cooldown. The high-head pumps would continue injecting borated water following a steam break until the initial RCS volume had been reestablished with borated water to prevent the possibility of an uncontrolled return to criticality.

The EWST provides a continuous suction source for the high-head pumps thus eliminating the conventional realignment from the Refueling Water Storage Tank (RWST) to the containment sump. In the event of any LOCA, the coolant floods the containment low spots and then spills to the EWST thus establishing a continuous recirculation path between the EWST, the high-head pumps, and the

RCS. Since the EWST is located inside the containment, the initial EWST water (a,c) temperature is approximately [ ] compared to the minimum 32°F RWST temperature, thereby reducing the potential for thermal shock to the RCS. The conventional realignment from the 32°F RWST water temperature to a maximum 300°F containment sump water temperature imposes a thermal transient on the safety injection equipment, which has been essentially eliminated by the EWST arrangement.

The four accumulators are primarily responsible for rapidly refilling the reactor vessel lower plenum and downcomer following a major blowdown of the RCS that would occur with a large or intermediate LOCA. The four core reflood tanks provide a diverse, passive means to reflood or supplement the reflooding of the core thus eliminating the need for large capacity low-head safety injection pumps.

Since the core reflooding phase occurs over a finite time period and imposes the largest flow requirement on the safeguards pumps, the core reflood tanks provide a means to reduce the flow requirement on the pumping system as well as provide a diverse and passive means to meet the large break LOCA functional requirement.

One RHR heat exchanger is installed in each of four high pressure injection headers that are routed from the four high-head pumps to the four reactor vessel ISS injection nozzles. These high pressure heat exchangers are located inside the containment building. In the event of a LOCA, these heat exchangers are available to remove heat from the EWST recirculation water regardless of the break size since they are located in the high-head pump to the reactor vessel flow path.

The RHR/CS pumps can be manually realigned to provide back-up safety injection flow. For smaller LOCAs the operator would also have to depressurize the RCS by opening the pressurizer PORVs or hot leg vents.

3.4.2 FAULT TREE MODEL

ISS reliabilities for small LOCA (< 6") and large LOCA (> 6") events are calculated for the Direct Vessel Injection design. Common cause and EWST failures are modeled, and are included in the fault tree quantification.

For both small and large LOCA events, three system failure probabilities are calculated. These are:

1. Failure probability for the injection phase.

2. Failure probability for the recirculation phase.

3. Failure probability for the total mission time.

The failure probabilities calculated for small LOCA events are displayed in Table 3.4-1. The failure probabilities calculated for large LOCA are displayed in Table 3.4-2. Examples of fault trees used for small and large LOCAs are given by Figures 3.4-2 and 3.4-3, respectively.

3.4.2.1 SUCCESS CRITERIA

For a small LOCA equivalent to a break of a 6 inch diameter pipe or smaller, any one of four HHSI subsystems delivering flow to the RCS can prevent core melt. For a large LOCA, the four core reflood tanks and the four high-head pumps provide eight separate means for injecting coolant directly into the reactor vessel. Any combination of five of these eight components is sufficient to keep the peak clad temperature below 2200°F using Appendix K assumptions. Best estimate analysis was not assumed but it would show that one HHSI plus one or two CRT would prevent core melt.

Another success mode for both small and large LOCA is the operator realigning one RHR/CS pump to the RCS and, if necessary, opening the pressurizer PORV.

3.4.2.2 DEPENDENCE ON SUPPORT STATES

The electrical load associated with two of the four ISS subsystems is assigned to one of the two separate and redundant load groups or emergency electrical power trains while the electrical loads associated with the other two ISS subsystems are assigned to the second emergency electrical power train. Two safeguards vital buses and two emergency diesel generators would be associated with the two emergency electrical trains.

3.4.2.3 RANDOM FAILURE MODEL

The following assumptions were made in the development of the ISS fault tree:

1. Heat exchanger-related failures are not modeled for 1 and 3 hour injection phase small LOCA.

2. The component cooling water valving for the RHR heat exchanger includes a normally open manual valve on the heat exchanger inlet and a motor-operated valve on the heat exchanger outlet that automatically opens at a set coolant temperature. No actuation failures are modeled for this MOV, since even if actuation fails, operators have ample time to respond.

3. The component cooling water valving for each of the high-head safety injection pumps includes a normally open block valve on the component cooling water inlet and outlet flow lines.

3.4.2.4 COMMON CAUSE MODEL

Common cause was calculated according to WAPWR Fault Tree Guidelines. Components which may fail due to common cause include HHSI motor-driven pumps and the motor-operated valves on the outlet of the four RHR heat exchangers. The common cause calculations are shown on Tables 3.4-3, 3.4-4 and 3.4-5.

3.4.2.5 TEST AND MAINTENANCE MODEL

The HHSI pumps are periodically tested on miniflow without realigning any valves. Therefore, the HHSI pumps are not made unavailable due to testing.

3.4.2.6 MAINTENANCE MODEL

Unavailability of a pump train due to maintenance activities is modeled in accordance with the fault tree guidelines.

3.4.2.7 HUMAN ERROR MODEL

No operator actions are included in the modeling of the ISS system. Operator actions are assumed to open HX cooling valves if automatic actuation fails.

3.4.2.8 INPUT DATA

The input data for the one hour ISS and one hour large LOCA responses is shown by Tables 3.4-6 and 3.4-7.

3.4.3 FAULT TREE QUANTIFICATION

The fault trees for small and large LOCA cases are quantified and the results are summarized below. Note that the tank unavailabilities for accumulators and CRTs are separately quantified as shown in Table 3.4-8. The system unavailability calculations for large LOCA, when only one division (two pumps) is supported is given by Table 3.4-9.

3.4.3.1 SYSTEM UNAVAILABILITY CALCULATIONS

The system unavailability calculations by fault trees and hand calculations are summarized in Tables 3.4-1 and 3.4-2.

3.4.3.2 DOMINANT CUTSETS

The dominant cutsets for selected cases are given by Table 3.4-10.

TABLE 3.4-1

ISS FAILURE PROBABILITIES FOR SMALL LOCA

Case	1 Train	1 Division	System
[			] (a,c)

Case Descriptions:

1 Hour: 1 hour mission time to be used in large LOCA fault tree

3 Hour: 3 hour mission time to be used for "injection phase" or short-term cooling

24 Hour: with HX: 24 hour mission time to be used for failure of long-term cooling when containment fan coolers fail so that RHR HX cooling is needed

24 Hour: no HX: 24 hour mission time to be used for failure of long-term cooling when containment fan coolers are available so that no HX cooling is needed

TABLE 3.4-2

ISS FAILURE PROBABILITIES FOR LARGE LOCA

Case	1 Train	1 Division	System
[			] (a,c)

* Includes 1.65×10^{-5} CCF of 4/4 HX.

Case Descriptions:

1 Hour: 1 hour mission time for short-term cooling.

24 Hour: with HX: 24 hour mission time for long-term cooling when containment fan coolers fail so that RHR heat exchanger cooling is needed.

24 Hour: no HX: 24 hour mission time for long-term cooling when containment fan coolers are available so that RHR heat exchanger cooling is not needed.

TABLE 3.4-3

COMMON CAUSE CALCULATION FOR 1-HOUR MISSION TIME

Random Pump Failures:

Fail to Start	:	1.34×10^{-3}
Fail to Run	:	4.86×10^{-5}
Circuit Breaker Faults		
Trip Circuit	:	2.34×10^{-4}
Actuation Circuit	:	5.57×10^{-6}
Control Power	:	1.16×10^{-4}
Cooling Faults	:	N/A
Total (Q_T)	=	1.74×10^{-3}

Common Cause Calculations:

2/2 Pumps Fail: $q = (0.1)\ (1.74 \times 10^{-3}) = 1.74 \times 10^{-4}$

4/4 Pumps Fail: $q \cong \beta_4\ Q_T = 1.7 \times 10^{-5}$

$V = 3.0 \times 10^{-10}$

3/4 Pumps Fail: $q \cong 4\beta_3\ Q_T = 8.4 \times 10^{-5}$

(4 combinations)

$V = 7.1 \times 10^{-9}$

2/4 Pumps Fail: $q \cong 6\beta_2\ Q_T = 1.04 \times 10^{-3}$

$V = 1.1 \times 10^{-6}$

TABLE 3.4-4

COMMON CAUSE CALCULATIONS FOR 3-HOUR MISSION TIME

Random Pump Failures:

Fail to Start	:	1.34×10^{-3}
Fail to Run	:	1.46×10^{-4}
Circuit Breaker Faults		
Trip Circuit	:	2.34×10^{-4}
Actuation Circuit	:	5.57×10^{-6}
Control Power	:	1.16×10^{-4}
Cooling Faults	:	N/A
Total (Q_T)	=	1.84×10^{-3}

Common Cause Calculations:

2/2 Pumps Fail:	$q = (0.1)\ (1.84 \times 10^{-3})$	$= 1.84 \times 10^{-4}$
	$V =$	3.4×10^{-8}
4/4 Pumps Fail:	$q \cong (0.01)\ (1.84 \times 10^{-3})$	$= 1.84 \times 10^{-5}$
	$V =$	$= 3.4 \times 10^{-10}$

TABLE 3.4-5

COMMON CAUSE CALCULATONS FOR 24-HOUR MISSION TIME

Random Pump Failures:

Fail to Start	:	1.34×10^{-3}
Fail to Run	:	1.17×10^{-3}
Circuit Breaker Faults		
Trip Circuit	:	2.34×10^{-4}
Actuation Circuit	:	5.57×10^{-6}
Control Power	:	1.16×10^{-4}
Cooling Faults	:	N/A
Total (Q_T)	=	2.86×10^{-3}

Common Cause Calculations:

2/2 Pumps Fail:	$q = 0.1 \times (2.86 \times 10^{-3})$	=	2.86×10^{-4}
	V =	=	8.2×10^{-8}
4/4 Pumps Fail:	$q \cong (0.01)\ (2.86 \times 10^{-3})$	=	2.86×10^{-5}
	V =	=	8.2×10^{-10}
3/4 Pumps Fail:	$q \cong 4(0.02)\ (2.86 \times 10^{-3})$	=	2.29×10^{-4}
(4 combinations)	V =	=	5.2×10^{-8}
2/4 Pumps Fail:	$q \cong 6(0.1)\ (2.86 \times 10^{-3})$	=	1.7×10^{-3}
(6 combinations)	V =	=	2.9×10^{-6}

CCF of 2/2 HX cooling is estimated as $q = 1.65 \times 10^{-4}$. For this purpose, an estimate of MOV failure is used.

For 4/4 HX, a β_4 value of 0.01 is used to get 1.65×10^{-5}. Note that these estimates are for order of magnitude determination and do not reflect any detailed analysis.

TABLE 3.4-6

INPUT DATA FOR 1-HOUR MISSION TIME FOR SMALL LOCA (a,c)

TABLE 3.4-6 (cont.)

INPUT DATA FOR 1-HOUR MISSION TIME FOR SMALL LOCA

(a,c)

TABLE 3.4-6 (cont.)

INPUT DATA FOR 1-HOUR MISSION TIME FOR SMALL LOCA

(a,c)

TABLE 3.4-7

INPUT DATA FOR 1-HOUR MISSION TIME FOR LARGE LOCA (a,c)

TABLE 3.4-8

QUANTIFICATION OF ACCUMULATOR AND CRT UNAVAILABILITIES

Random Failures of 1 Tank Train:

Check Valve fails to open	:	3.2×10^{-4}
Check Valve fails to open	:	3.2×10^{-4}
MOV Transfers closed; local faults	:	2.6×10^{-3}
Total (Q_T)	=	3.2×10^{-3}

Common Cause Failure:

(Low tank pressure) $q = 1 \times 10^{-6}$

2/3 Accumulators fail: $q = 3 (3.2 \times 10^{-3})^2 + 1.0 \times 10^{-6} = 3.2 \times 10^{-5}$

(3 combinations)

$V = \qquad = 1.0 \times 10^{-9}$

4/4 CRTs Fail: $q = 1.0 \times 10^{-6}$

$V = 1.0 \times 10^{-12}$

* It is modeled that MOV local faults can be detected during refueling shutdown (18 months). Thus, the mean time interval for failure calculation is $\frac{8760 \times 1.5}{2} = 6570$ hrs.

TABLE 3.4-9

CALCULATION OF ISS FAILURE PROBABILITIES FOR LARGE LOCA

WHEN ONLY ONE DIVISION (2 PUMPS) ARE SUPPORTED

Dominant Cutsets (by inspection)	Mission Time 1-HR	24-HR with HX	24 HR no HX
[			] (a,c)

* See note on Table 3.4-5 for comments.

TABLE 3.4-10

DOMINANT CUTSETS FOR SELECTED CASES FOR ISS

Cutsets	Probability
Small LOCA 3-HR Mission Time	
[	(a,c)]

FIGURE 3.4-2

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
INTEGRATED SAFEGUARDS SYSTEM
SMALL LOCA
(PROPRIETARY)

FIGURE 3.4-3

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
INTEGRATED SAFEGUARDS SYSTEM
LARGE LOCA
(PROPRIETARY)

(a,c)

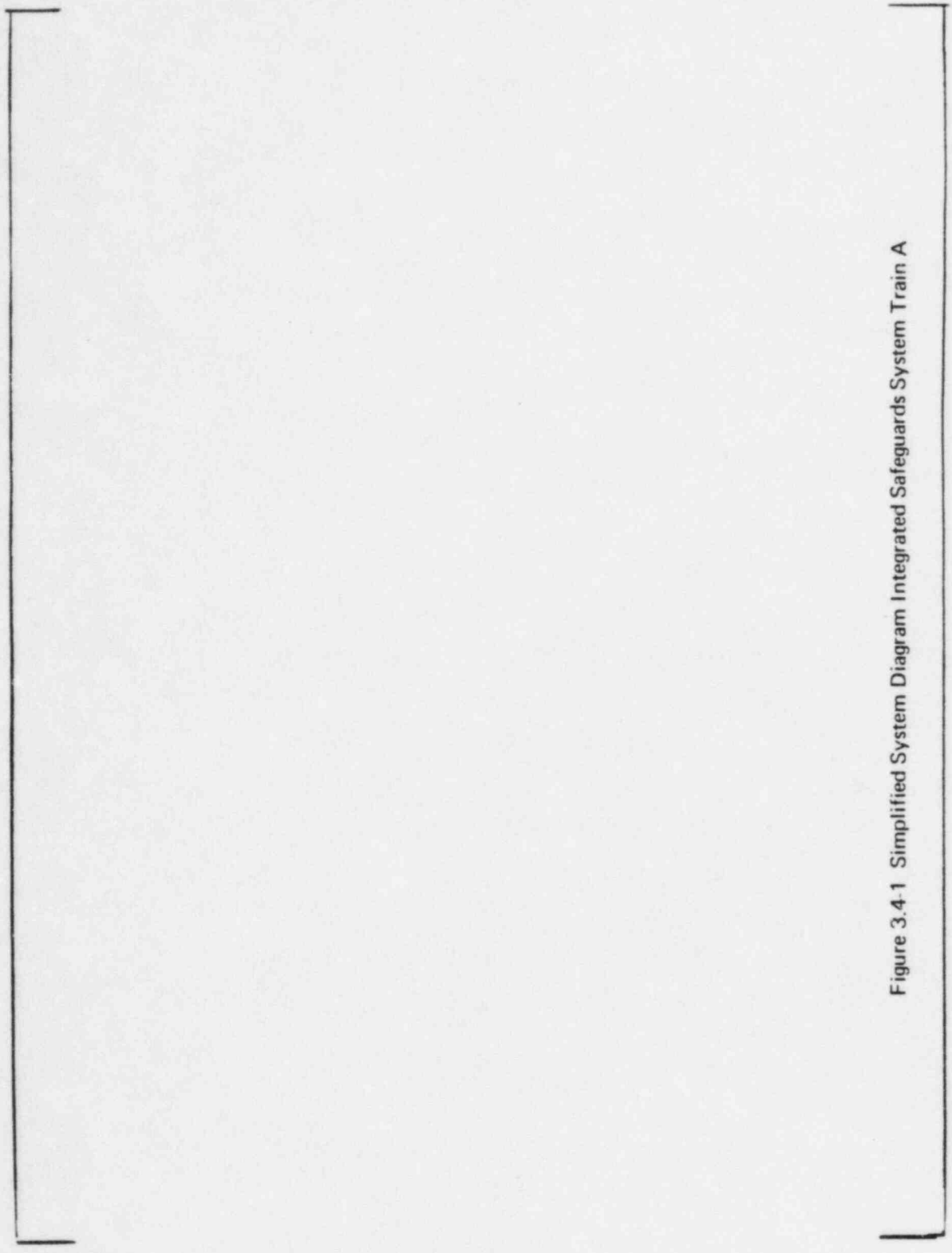
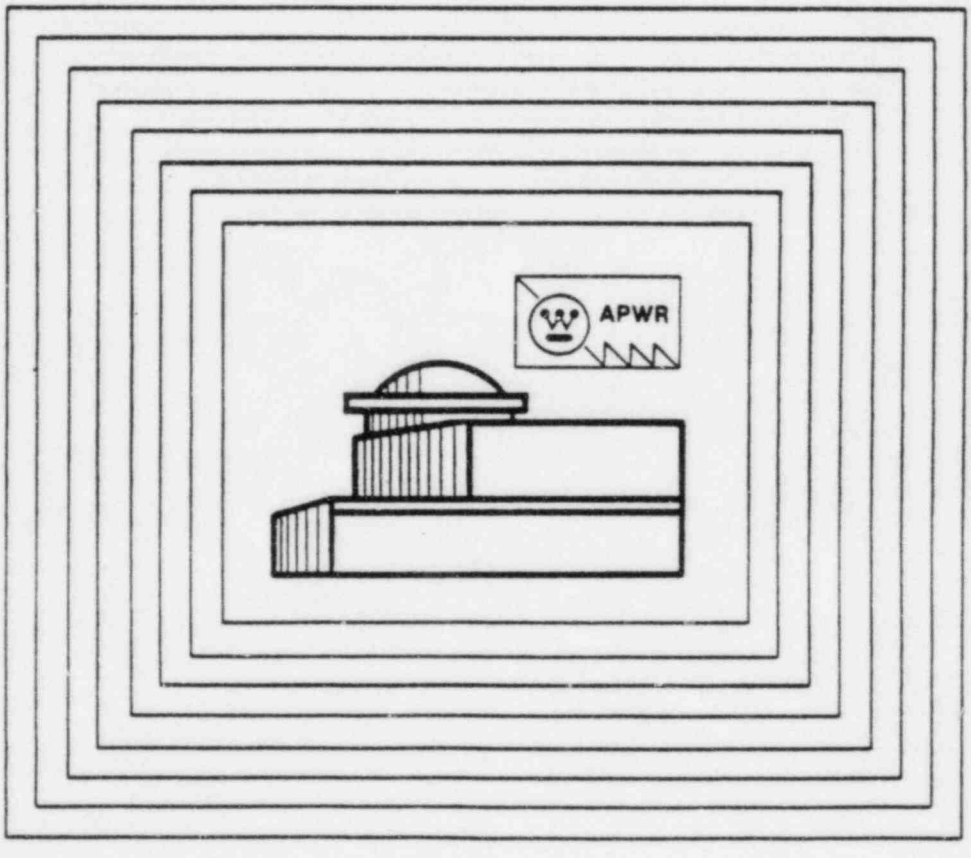


Figure 3.4-1 Simplified System Diagram Integrated Safeguards System Train A

RESAR-SP/90
PROBABILISTIC SAFETY STUDY

WESTINGHOUSE
ADVANCED PRESSURIZED
WATER REACTOR



STANDARD PLANT DESIGN

3.5 CONTAINMENT SPRAY SYSTEM

3.5.1 SYSTEM DESCRIPTION

The Integrated Safety System (ISS) containment spray system is designed to automatically provide sufficient flow to the containment spray ring headers to ensure that the following criteria are satisfied:

- In conjunction with the containment fan cooling system, rapidly reduce the containment pressure and temperature following any loss of coolant accident (and steam break accident) and maintain them at acceptably low levels.

- Reduce the concentration and quantity of fission products released to the environment following postulated accidents, using accepted N.R.C. calculational methods such that the offsite radiation exposures are within the guideline values of 10 CFR 100.

- Suitable redundancy shall be provided to assure that the ISS containment spray safety function can be accomplished assuming a loss of either on-site or offsite power and the most limiting single failure.

- Complete coverage of the containment cross-sectional area shall be achieved with minimum safeguards operation. The containment spray ring header layout and nozzle orientation and spacing shall ensure that the maximum containment volume coverage is obtained.

- The spray header design shall permit the operation of only one of the four ISS low-head pumping subsystems without exceeding the runout of the spray pump. The operation of one ISS spray system shall provide 50 percent containment coverage with 50 percent of the required flow. For an ISS powered by two emergency electrical power trains, spray subsystems assigned to the same electrical train shall deliver to a matched set of ring headers to obtain 100 percent coverage with a single failure of an electrical train.

- To ensure the retention of the iodine in the EWST solution during long-term recirculation, the pH of the recirculation water should be maintained between [ ]. (a,c) All sources of borated water, such as the reactor coolant system, accumulators, core reflood tanks, and emergency water storage tank (EWST) shall be considered.

The four low-head pumps are primarily Residual Heat Removal (RHR) pumps which would be used for normal plant cooldown and during normal refueling operations to remove the core decay heat. However, in case of a loss of coolant or steam break accident these low-head pumps would function as containment spray pumps.

The ISS containment spray system has a dual function of fission product removal and pressure suppression/heat removal following a major mass/energy release within the containment. However, a safeguard containment fan cooling system is provided as an integral part of the post-accident containment heat removal system, therefore the performance requirements for the ISS containment spray subsystem are based on providing sufficient flow to the containment spray ring headers to ensure coverage of the containment cross-sectional area with minimum safeguards operation.

In the event of a high containment pressure signal ("P" signal) during reactor power operation, the four low-head pumps would receive an automatic signal to start. Also, the valves in the pump discharge headers would receive an automatic signal to open. The low-head pumps would function as containment spray pumps and would take suction from the EWST and deliver to the containment spray headers which are located in the top of the containment building.

(a,c) A design flow of approximately [ ] gpm has been established for a [ ] foot diameter spherical containment. This design flow rate is based on an assumed spray ring header layout and nozzle type, orientation and spacing that would ensure that the maximum containment volume coverage was obtained. A SPRACO 1713A spray nozzle has been assumed with a pressure drop of 40 psig at a spray nozzle design flow rate of 15.2 gpm.

Each low-head pump is capable of providing one-half of the design flow. Therefore two of the four low-head pumps are required to meet the [ ] gpm spray design flow rate. (a,c)

Note that when spray recirculation is no longer required, the low-head pumps may be aligned for long-term safety injection recirculation, thereby providing 4 additional pumps for long-term core cooling when only one is needed. A system diagram is included as Figure 3.5-1.

The low-head pumps are single-stage, horizontal centrifugal pumps driven by a water-cooled induction motor. The primary function of these pumps is to recirculate coolant through the core and through residual heat removal (RHR) heat exchangers during plant cooldown and shutdown operations. During these operations the low-head pumps are aligned to take suction from the RCS hot legs and to deliver to the reactor vessel injection nozzles. In the event of a large LOCA or steam break these pumps function as containment spray pumps and take suction from the EWST and deliver coolant to the containment ring headers to perform the spray recirculation function. If spray recirculation is not required during a long-term post-accident core cooling phase, these low-head pumps can be aligned for direct vessel injection and can perform a long-term ECCS recirculation function. The low-head pumps are also used to return the refueling water from the refueling canal back to the EWST prior to plant start-up operations.

These pumps must be protected against extremely low flow or no flow operation. This requirement is satisfied by a miniflow heat exchanger in parallel with each pump. A flow path from the discharge header of each low-head pump is routed to the miniflow heat exchanger and from the miniflow heat exchanger to the pump suction. The shell side of the miniflow heat exchangers is connected to the component cooling water system. This heat exchanger is provided to protect the pumps from potential damage in the event they are started with all discharge flow paths blocked. It also eliminates the need for routing these mini-flows outside the shielded and vented safeguards pump area.

Component cooling water is recirculated through the shell of each heat exchanger to transfer the heat from the coolant to the ultimate sink.

3.5.2 FAULT TREE ANALYSIS

The fault tree was developed according to the WAPWR Guide to Fault Tree Development in Section 3.10. All of the assumptions specific to this fault tree model are stated in Section 3.5.2.3. The containment spray fault tree is presented in Figure 3.5-2.

3.5.2.1 SUCCESS CRITERIA

The success criteria for the ISS containment spray function fault tree is at least one of four containment spray subsystems delivering flow to the spray header. This criteria ensures that even without containment fan coolers the containment will not fail due to overpressurization.

3.5.2.2 DEPENDENCE ON SUPPORT STATES

Trains A and D of the Containment Spray System are dependent on 4160V Bus 1A and trains C and D on 4160V Bus 1B. Each train of the Containment Spray System has a motor-driven containment spray/RHR pump and one motor-operated valve which depends on electric power.

3.5.2.3 FAILURE MODEL

3.5.2.3.1 RANDOM FAILURE MODEL

The random failure fault tree model was developed according to the APWR Guide to Fault Tree Development in Section 3.10. The assumptions used in the fault tree model for the containment spray system are as follows:

Full flow pump test is done only during refueling.

Pump test during operation is performed by ensuring that proper discharge head is developed when the pump is started and run on miniflow. During normal operation, the trains are never unavailable for test. Flow tests are performed following pump maintenance.

Component cooling valve CCWCD is not considered because misposition of the valve would not constitute a failure.

Parallel sets of valves are considered to have one valve on each MCC. MCC failures are approximated by circuit breaker failure to transfer closed.

3.5.2.4 COMMON CAUSE MODEL

The common cause modeling of the system is done in accordance with the common cause guidelines in Section 3.10.3. All common cause calculations are the product of a β and a random failure probability. Common cause failure to run and common cause failure to start are modeled for the motor-driven pumps. Common cause failure of various motor-operated valves which require position changes is also modeled in the fault tree. These include common cause failure of valves 9011 A, B, C, and D. Table 3.5-1 contains the common cause calculations for this system.

3.5.2.5 TEST MODEL

The ISS provides a means for performing a total system and pump performance test during reactor power or shutdown operations. Each low-head and high-head pump can be aligned to take suction from the EWST and to discharge back into the EWST via a system performance test flow path located downstream of each RHR heat exchanger. It is recommended that a full flow system and pump performance test be performed during each major refueling operation. The entire pump performance curve can be verified from miniflow to pump runout during these tests. Quarterly miniflow tests (which would require no valve repositioning) are recommended for ISS pumps. In the event that the miniflow tests produce unacceptable pump characteristics, additional pump performance

data can be obtained during reactor power operations. This system performance test capability may also be utilized should major pump maintenance or replacement be required during reactor power operations. Train test is not modeled in the fault tree because the trains are never unavailable due to test during normal operation.

3.5.2.6 MAINTENANCE MODEL

Maintenance of the containment spray system is modeled for complete trains, not individual components.

3.5.2.7 HUMAN ERROR MODEL

There are no operator actions required to initiate the containment spray system, therefore human error does not affect the availability of the containment spray system.

3.5.2.8 INPUT DATA

Table 3.5.2 lists all event identifiers, brief descriptions of the failure mode they represent, and the numbers used as input to the fault tree quantification. All numbers in this table are drawn from the data bank in Section 3.10.7.

3.5.3 FAULT TREE QUANTIFICATION

3.5.3.1 SYSTEM UNAVAILABILITY CALCULATIONS

The fault tree was analyzed using the WAMBAM computer code. For support state 3, the unavailability is 1.0 because of the dependencies of the system on electrical power. The unavailability value for one bus of electric power available is [2.67E-03] and for both buses of electric power available is [3.01E-05].

(a,c)

(a,c)

3.5.3.2 DOMINANT CUTSETS

The WAMCUT computer code was used to obtain cutsets for the containment spray system fault tree model for all support states. The dominant cutsets for the containment spray system are listed in Table 3.5-3 along with the percent of the unavailability which they contribute.

TABLE 3.5-1

CONTAINMENT SPRAY SYSTEM COMMON CAUSE CALCULATIONS

Failure Mode	Data Bank Source ID	β	Random Failure Mode	Random Failure Probability	Result
[					] (a,c)

TABLE 3.5-2

CONTAINMENT SPRAY SYSTEM COMPONENT FAILURE PROBABILITIES

(a,c)

TABLE 3.5-2 (cont.)

CONTAINMENT SPRAY SYSTEM COMPONENT FAILURE PROBABILITIES (a,c)

TABLE 3.5-2 (cont.)

CONTAINMENT SPRAY SYSTEM COMPONENT FAILURE PROBABILITIES (a,c)

TABLE 3.5-3

CONTAINMENT SPRAY SYSTEM

DOMINANT CUTSETS

Description	Contribution
[	] (a,c)

(a,c)

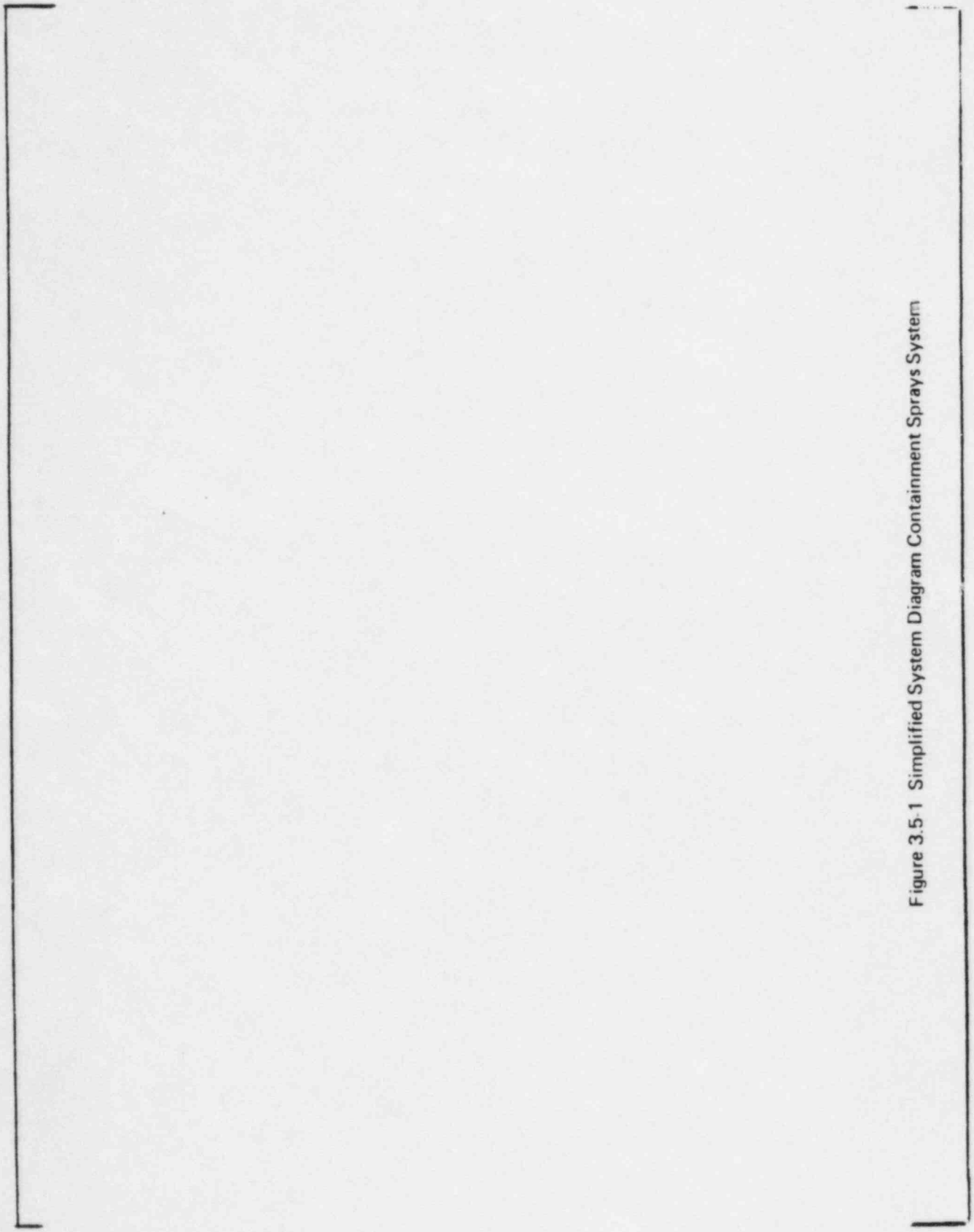


Figure 3.5-1 Simplified System Diagram Containment Sprays System

(a,c)

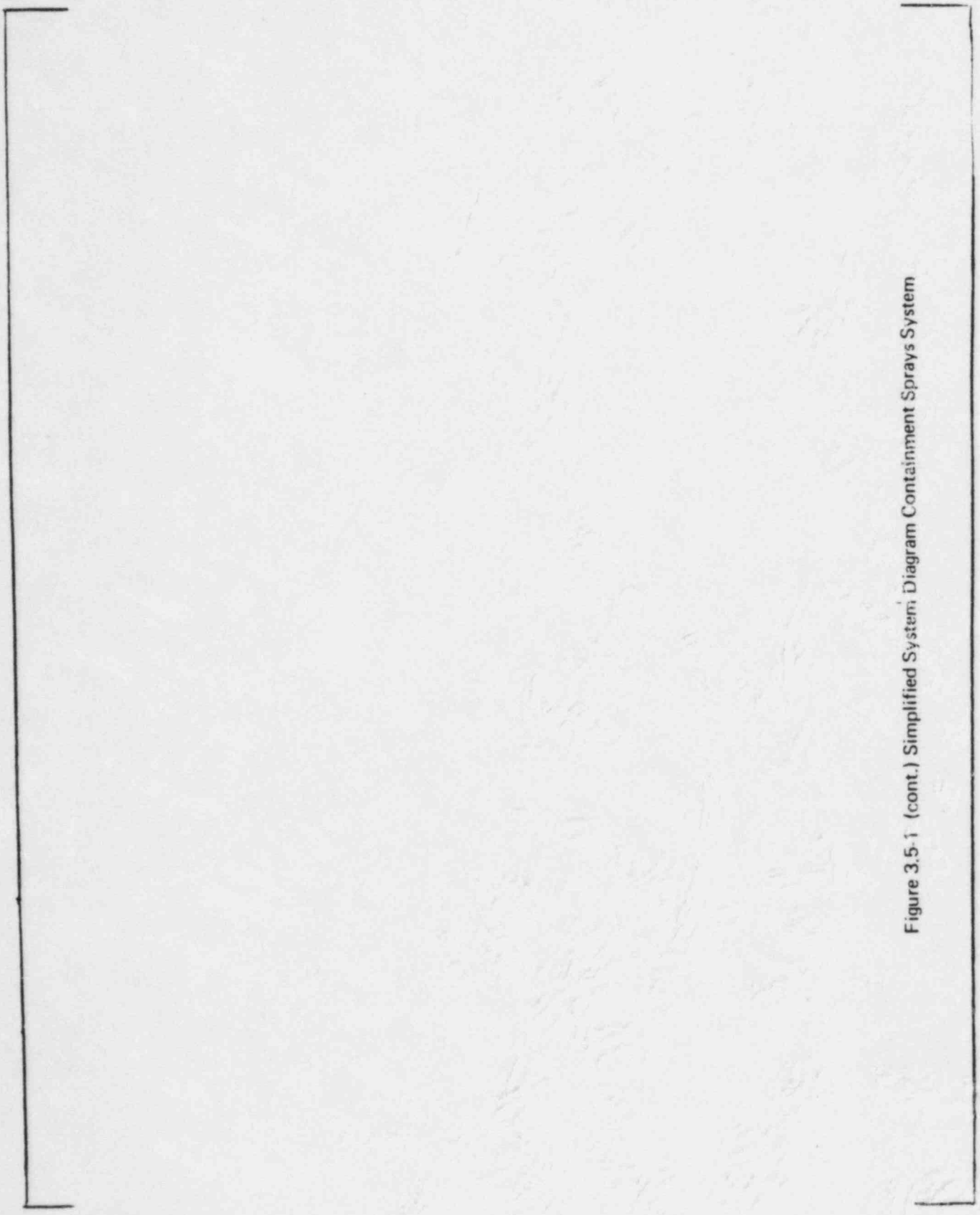


Figure 3.5-1 (cont.) Simplified System Diagram Containment Sprays System

FIGURE 3.5-2

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
CONTAINMENT SPRAYS SYSTEM
(PROPRIETARY)

3.6 CONTAINMENT FAN COOLER SYSTEM

3.6.1 SYSTEM DESCRIPTION

The reactor containment fan cooler system is designed to meet the following requirements:

A. During normal operation the system cools and dehumidifies the containment.

B. Following a postulated loss-of-coolant accident (LOCA), the reactor containment fan coolers provide the design heat removal capacity for the containment, assuming that the core residual heat is released to the containment as steam and water.

C. The reactor containment fan cooler system and the integrated safeguards system (Section 3.4) share in removing heat from the containment building following a LOCA.

D. One fan cooler in each of two cooling water trains operates during a LOCA. This prevents the possibility of local boiling in the fan cooling coils which might occur if two fans per train were operated, and assures that the resultant temperature of the cooling water does not exceed the safe maximum temperature.

E. The fan coolers operate in low speed with a lower than normal airflow during LOCA to prevent motor overload.

F. The containment coolers, including the fan and motor combination, are designed to remain operable in the accident environment.

G. The fan cooler housing is designed to withstand the maximum transient pressure rise associated with accident conditions.

H. The fan cooler housing is designed to drain the condensate which forms on the cooling coil surface under normal and accident conditions.

J. If the two running fan coolers fail, the operator must start the standby fan coolers.

The fan cooler system recirculates the containment air (or air-steam mixture in the event of a LOCA) through cooling coils to transfer heat from the containment atmosphere to the component cooling water (CCW) system. The fan cooler system consists of four identical fan cooler units, each having a vertical axial flow fan, a two-speed 480 VAC electric motor, a mist separator, and a CCW cooling coil. Each fan cooler has its own air distribution duct. The air distribution duct routes the cooled air to various levels of the containment building and contains no dampers.

The fan cooler system is made up of two trains, each having two fan cooler units. Each train receives electric power from a separate redundant essential bus and is cooled by a separate redundant CCW train. A simplified diagram of the fan cooler system is shown in Figure 3.6-1. Fans associated with Train A receive power from essential bus A. Fans associated with Train B receive power from essential bus B.

Bypass lines are provided for each fan cooler and are designed to carry the full cooling water flow when the fan cooler is in maintenance. Only one fan cooler is out for maintenance at a time.

During normal operation a maximum of three fan coolers will operate at high speed. The minimum number of fan coolers which will normally operate is assumed to be two; one cooler per train. Upon receipt of the safety injection signal the automatic control system for the fan coolers will switch the fan speed of one cooler in each train to low and will shut off the third fan cooler, if operating. The deenergized coolers are standbys for the operating coolers in their respective trains. While the safety injection signal is in effect, a standby cooler can be started manually if desired but the fans cannot be manually switched to high speed. None of the valves associated with the fan coolers are required to move for post-LOCA containment cooling.

3.6.2 FAULT TREE MODEL

3.6.2.1 FAULT TREE MODEL

The containment fan cooler fault tree analysis is shown in Figure 3.6-2.

3.6.2.1 SUCCESS CRITERIA

Any one of the four fan coolers will provide sufficient heat removal following a LOCA to maintain the containment pressure below the design value. Following a LOCA, the fan coolers work in conjunction with the containment spray system to reduce the containment pressure and temperature. However, one fan cooler can maintain the containment pressure below the design value without the assistance of the sprays. Therefore, the success criteria for the fan cooler system is one fan cooler unit available.

3.6.2.2 DEPENDENCE OF FAN COOLERS ON SUPPORT STATES

Fan cooler train A depends on electric power and component cooling water from ESF bus A and CCW train A. Fan cooler train B depends on electric power and component cooling water from ESF bus B and CCW train B.

3.6.2.3 RANDOM FAILURE MODEL

Random failure of a fan cooler to run was obtained from the Zion Probabilistic Safety Study. The random failure of a normally running fan cooler to switch to low speed and the random failure of a standby cooler to start were included in one data value so that it was not necessary, in the random model, to treat two fan coolers as standby and two as running. However, the common cause model required some distinction between running and standby, as discussed in the common cause section. As the control and actuation circuits for the fan coolers have not yet been designed, the best available random failure data for control and actuation was selected from the master data file in Section 3.10. Since the fan motors are 480 volt, the control and actuation failure probability for motor-operated valves (also 480 volt) were selected. The

non-standard control features associated with the stopping of only one of two operating fans in a train was lumped in the common cause model.

3.6.2.4 COMMON CAUSE MODEL

Common cause modeling of the system was done in accordance with the common cause guidelines in Appendix 3B. Common cause calculations were the product of the β value and a random failure probability. Table 3.6-1 gives a summary of the common cause calculations. As indicated, a β value of 0.1 was used for all common cause calculations except for the common cause failure of control and actuation circuits. A conservative β value of 0.4 was selected to account for additional common cause effects associated with the activation of only one fan cooler per train with the S signal. Whereas with most fan cooler systems the activation of all four coolers would be considered success, the activation of four coolers in the APWR system (or three coolers, or two on the same train) does not constitute success. The conservative β value of 0.4 accounts for the additional complexity of control and actuation.

Failure of standby fan cooler units and running units are treated as separate common cause failures. One common cause failure causes two coolers in the same operating mode to fail. Since the two coolers on a single train operate in the same mode, these two are linked by using a transfer in the fault tree.

The random failure modes and β's used apply to alternating pumps, with no distinction between running and standby at the time of the LOCA. Therefore, the common cause probabilities are equal for both sets of fan cooler units.

3.6.2.5 TEST MODEL

It was assumed that the unavailability of the fan coolers would not be affected by testing since they do not have to be isolated.

3.6.2.6 MAINTENANCE MODEL

Only one fan cooler will be in maintenance at a time. When one fan cooler is in maintenance, the other three fan coolers are modeled as not being in maintenance.

3.6.2.7 HUMAN ERROR MODEL

The only human error considered in the model was the failure to restore the manual cooling water bypass valve on the cooler following maintenance. Random failure to restore one or both of the manual cooling water block valves was not considered because this error would result in blockage of cooling flow to the normally-operating fan cooler and would be corrected immediately by plant operators. The common cause failure to restore the bypass and block valve following maintenance was considered as this combination of failures would not result in a blockage of flow in the train.

3.6.2.8 INPUT DATA

Table 3.6-2 lists the failure probabilities and variances for each event identifier. The data taken from Section 3.10.

3.6.3 FAULT TREE QUANTIFICATION

In this section, the results of the fault tree quantification and the dominant cutsets are presented.

3.6.3.1 SYSTEM UNAVAILABILITY CALCULATION

Computed failure probabilities and variances for the fault tree top event titled, "Failure of Containment Fan Cooling System" are given in Table 3.6-3. The calculated failure probability of the fan cooling system in the event of a LOCA in conjunction with a loss of offsite power is also given in Table 3.6-3. Loss of offsite power affects the common cause failure of fan coolers to start. Since two fan coolers are assumed to be in normal operation prior

to LOCA, only the standby coolers in each train are linked in the common cause modeling of failure to start when offsite power is available. However, the loss of offsite power results in the stopping of all four fans. Therefore, common cause failure to start is linked to all four fan coolers, even though only one cooler per train is started.

3.6.3.2 DOMINANT CUTSETS

Dominant cutsets are listed in Table 3.6-4.

TABLE 3.6-1

FAN COOLER COMMON CAUSE CALCULATIONS

Description of Random Failure	Random Failure Probability	β	Failure Probability for Two Coolers Due to Common Cause
[			] (a,c)

Note 1: This common cause failure was modeled on a single cooler basis for the standby coolers. Common cause failure to restore the bypass and block valves consists of three possible combinations: Failure to close the bypass valve and open the inlet block valve, failure to close the bypass valve and open the outlet block valve, and failure to close the bypass valve and open both block valves. Therefore, the common cause failure probability was multiplied by a factor of 3.

TABLE 3.6-2

INPUT DATA FOR FAN COOLER SYSTEM FAULT TREE

(a,c)

[redacted]

TABLE 3.6-3

CONTAINMENT FAN COOLER SYSTEM FAILURE PROBABILITY

Probability of Failure and Variance for Fan Cooler System

Case Number	Support State 2 Prob.	Var.	Support State 1 Prob.	Var.	Support State 0 Prob.	Var.
(See Note 2)						
[						](a,c)

Note 1: Support State 2 = All support systems available

Support State 1 = Power on ESF Bus A unavailable, or CCW Train A unavailable

Support State 0 = ESF Power or CCW unavailable

Note 2: Case No. 1 is calculated assuming no loss of offsite power. Case No. 2 is calculated assuming a loss of offsite power.

TABLE 3.6-4

DOMINANT CUTSETS FOR CONTAINMENT FAN COOLER SYSTEM

(OFFSITE POWER AVAILABLE)

Cutset Description	Percent of Unavailability
[	[

(a,c)

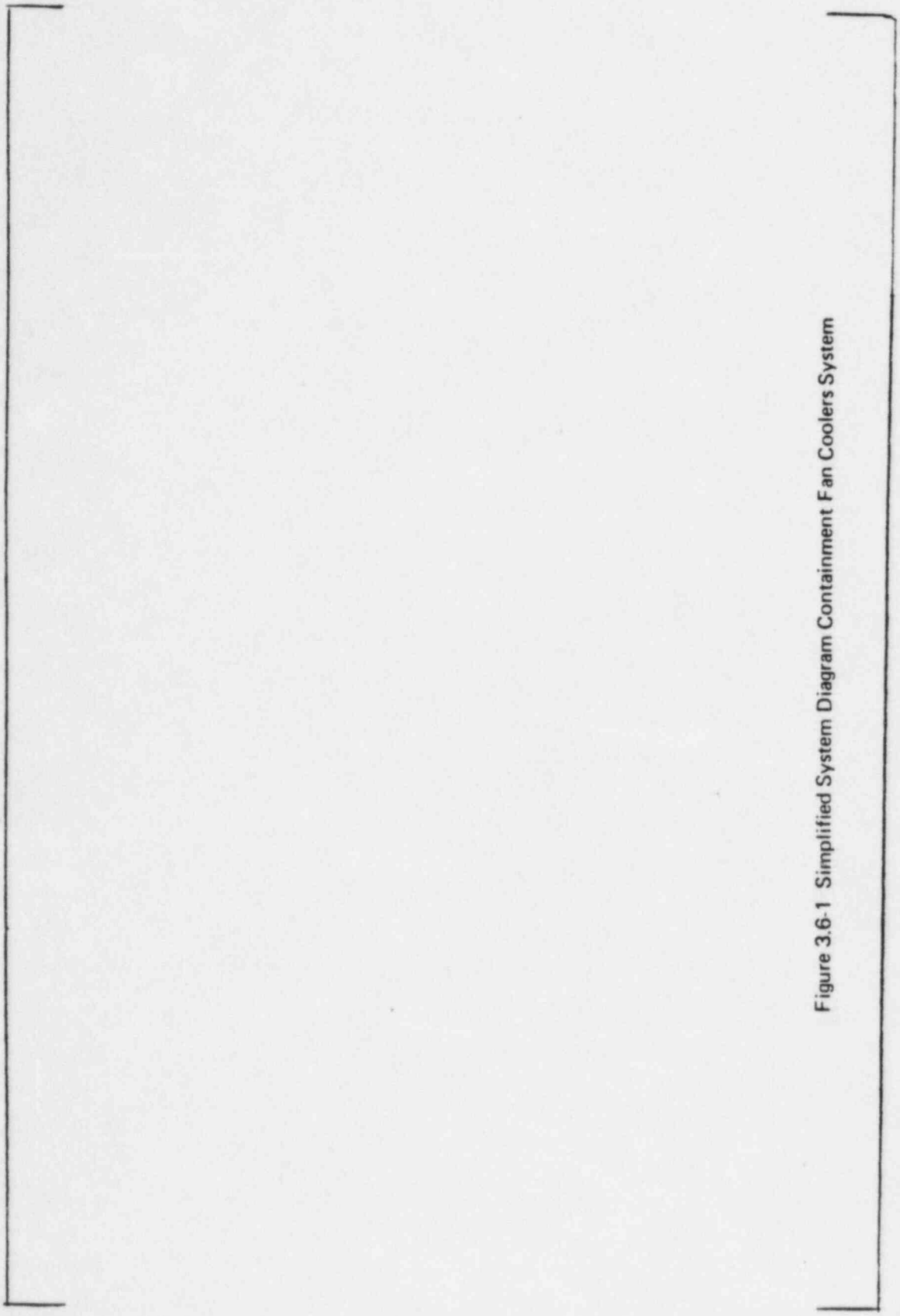


Figure 3.6-1 Simplified System Diagram Containment Fan Coolers System

FIGURE 3.6-2

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
CONTAINMENT FAN COOLERS SYSTEM
(PROPRIETARY)

3.7 SECONDARY COOLING

3.7.1 START-UP FEEDWATER SYSTEM

3.7.1.1 SYSTEM DESCRIPTION

Whenever the main feedwater system is unavailable during startup/shutdowns and standby, the start-up feedwater system (SUFW) provides feedwater flow to the steam generators. The SUFW is actuated automatically following a reactor trip. A motor-driven pump on normal AC supplies water to all four steam generators from the deaerator storage tank or the condensate storage tank. The lines to each steam generator are identical in terms of valve location and type. The start-up feedwater system will be automatically isolated if any one of the four parallel sections receives low or no water supply. Please refer to the system schematic in Figure 3.7.1-1.

3.7.1.2 FAULT TREE MODEL FOR THE SUFW

The SUFW is modeled in the fault tree shown in Figure 3.7.1-2. Table 3.7.1-1 lists all the components used in the fault tree model, their identifiers, failure modes, and the probability and variance used for the quantification. The data for the failure probabilities is drawn from the data bank described in Section 3.10.5.

3.7.1.2.1 SUCCESS CRITERIA FOR SUFW

The success criteria for the SUFW is for the one pump to provide sufficient flow to all four steam generators.

3.7.1.2.2 DEPENDENCE OF SUFW ON SUPPORT STATES

The SUFW is powered by offsite AC power and not by the emergency buses. Therefore, there is a dependence on offsite AC power for the SUFW. The system is considered to be available for transients and other events which don't include either a loss of offsite power, loss of cooling water flow, or an actuation of the IPS.

3.7.1.2.3 RANDOM FAILURE MODEL FOR THE SUFW

The random failure fault tree models were developed and applied according to the APWR Fault Tree Guide Lines in Section 3.10. The following assumptions are not addressed in Section 3.10, but apply to the SUFW fault tree analysis.

1. Common cause was not treated as an independent failure mechanism for the components in this system since it consists of a single train of equipment. Common cause failure of all air-operated control valves has a probability of 7×10^{-5}, which is insignificant with respect to other system failures.

2. The system is a control grade system and is not tested. However, the system is used for every start-up and shutdown operation. The analysis assumes that the system is used at least once upon reactor trip and is therefore operated ten times per year.

3. The mission time for the system is 24 hours.

4. The pump suction piping was assumed to include a manual block valve and a normally closed MOV to the deaerator storage tank.

3.7.1.2.4 MAINTENANCE MODEL OF SUFW

Maintenance of the system is modeled as a train. Table 3.7.1-1 lists all of the components in the model and if they are maintained. The table also indicates which valves have failure to restore as a failure mode. It is assumed that train maintenance outages will be dominated by the pump, and that any required valve repairs will occur when the pump is taken out of service.

3.7.1.3 FAULT TREE QUANTIFICATION FOR SUFW

3.7.1.3.1 SYSTEM UNAVAILABILITY CALCULATIONS FOR SUFW

The fault trees were analyzed using the WAMCUT computer codes. The dominant cutsets are presented in Table 3.7.1-2. The system has an unreliability of [ ] with a variance of [ ].

TABLE 3.7.1-1

INPUT DATA FOR START-UP FEED WATER SYSTEM

[ ] (a,c)

TABLE 3.7.1-1 (Continued)

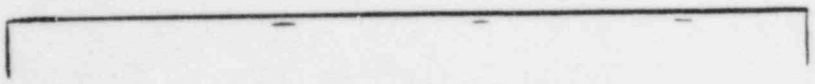
INPUT DATA FOR START-UP FEED WATER SYSTEM

[ ] (a,c)

TABLE 3.7.1-2

DOMINANT CUTSETS FOR START-UP FEED WATER SYSTEM

Description	Percent Contribution
[	] (a,c)



(a,c)

Figure 3.7.1-1 Simplified System Diagram Start-up Feedwater System

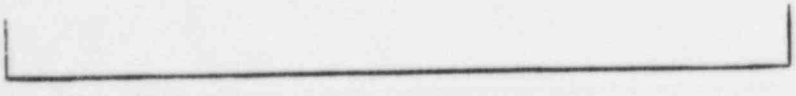


FIGURE 3.7.1-2

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
STARTUP FEEDWATER SYSTEM
(PROPRIETARY)

3.7.2 EMERGENCY FEEDWATER SYSTEM

3.7.2.1 SYSTEM DESCRIPTION

The Emergency Feedwater System (EFWS) functions as a heat removal system with the steam generator and steam generator relief valves and safety valves. It can operate independently from the main or startup feedwater system for emergencies or as required in startup, shutdown, or hot standby conditions. However, the system is not normally used for this purpose.

The EFWS consists of two identical subsystems. Each subsystem contains a motor driven and turbine driven pump which supply feedwater to two steam generators. Each subsystem is tied in to separate emergency buses. The EFWS is initiated by a signal from the reactor protection system or by low-low steam generator water level. The system is designed to deliver adequate flow to each of the four steam generators following a transient without the need for operator action for at least 30 minutes. A cavitating venturi is provided at the inlet of each steam generator to limit the flow to [ ] gpm. This serves to prevent pump runout, prevent steam generator overfill, and prevent excessive core cooldown. A single line diagram of the system is shown in Figure 3.7.2-1. (a,c)

Either of the four emergency feedwater pumps supplying one of the four steam generators will provide enough feedwater to remove decay heat and prevent a core melt.

3.7.2.2 FAULT TREE ANALYSIS

The EFWS fault tree is shown in Figure 3.7.2-2. The success criteria for ATWS is later implemented at the top level logic.

3.7.2.2.1 SUCCESS CRITERIA FOR EMERGENCY FEEDWATER SYSTEM

The success criteria for the EFWS is full pump flow from a single pump to a single steam generator for all initiating events except ATWS. The success criteria for an ATWS event is full pump flow from two pumps to four steam generators.

3.7.2.2.2 DEPENDENCE ON SUPPORT STATES

One train of each subsystem depends on electric power. The other train in each subsystem has no support state dependencies since it is a steam turbine driven pump with fail-open valves.

3.7.2.2.3 FAILURE MODEL

3.7.2.2.3.1 RANDOM FAILURE MODEL

The random failure fault tree models were developed according to the APWR Guide to Fault Tree Development in Section 3.10. The following assumptions are not addressed in Section 3.10 but apply to the EFWS fault tree:

1) Pump cooling is supplied by minimum flow lube oil cooler lines.

2) Success time for the EFW system is 24 hours.

3) System testing is performed on a monthly basis.

3.7.2.2.3.2 COMMON CAUSE MODEL

The only common cause failure considered is that of the pumps to start and to run, and air operated valves which must stroke. The β factor represents those common elements between two components which could cause their failure. The βs for motor driven and turbine driven pumps both include failures pertaining to the pump and the driver. A β of 0.1 was used for all common cause contributions.

3.7.2.2.3.3 TEST AND MAINTENANCE MODEL

The test and maintenance of the system is modeled by segments. Table 3.7.2-1 lists all of the components and failure rates for a 24 hour mission time in the model and if they are tested or maintained. The table also indicates which valves have failure to restore as a failure mode.

3.7.2.2.3.4 HUMAN ERROR MODEL

The only human errors modeled consist of failure to restore valves to their proper position following test or maintenance.

3.7.2.2.3.5 INPUT DATA

The data for component failure values is taken from the WAPWR master databank (Section 3.10). An input listing of component identifiers and associated probabilities is presented in Table 3.7.2-1.

3.7.2.2.4 FAULT TREE QUANTIFICATION

3.7.2.2.4.1 SYSTEM UNAVAILABILITY CALCULATIONS

The fault trees were analyzed using the WAMCUT computer code. A total of nine cases were analyzed to provide input for the various support states. The three cases of full AC power available, 1 AC power bus available, no AC power available were analyzed for the three situations of four intact steam generators, one faulted (three intact) steam generators, and ATWS. The failure probabilities and variance for each of the cases are shown in Table 3.7.2-2.

3.7.2.2.4.2 DOMINANT CUTSETS

The dominant cutsets are presented in Table 3.7.2-3.

TABLE 3.7.2-1
INPUT DATA FOR EFWS

(a,c)

TABLE 3.7.2-1 (Cont)
INPUT DATA FOR EFWS

(a,c)

TABLE 3.7.2-1 (Cont)

INPUT DATA FOR EFWS

(a,c)

TABLE 3.7.2-1 (Cont)
INPUT DATA FOR EFWS

[ ] (a,c)

TABLE 3.7.2-2

EFWS UNAVAILABILITY
(24 Hours)

FULL AC POWER	ONE AC POWER BUS	NO AC POWER
[		]

(a,c)

*Variance

TABLE 3.7.2-3

EMERGENCY FEEDWATER SYSTEM

DOMINANT CUTSETS

I. Four Intact Steam Generators (Full AC Power)

Description	Contribution
[	] (a,c)

TABLE 3.7.2-3 (Cont.)

II. Three Intact Steam Generators
If steam generator A is faulted:

Description	Contribution
[	] (a,c)

If Steam Generator D is faulted: (Full AC Power)

Description	Contribution
[	] (a,c)

TABLE 3.7.2-3 (Cont.)

III. ATWS (Full AC Power)

Description	Contribution
[	] (a,c)

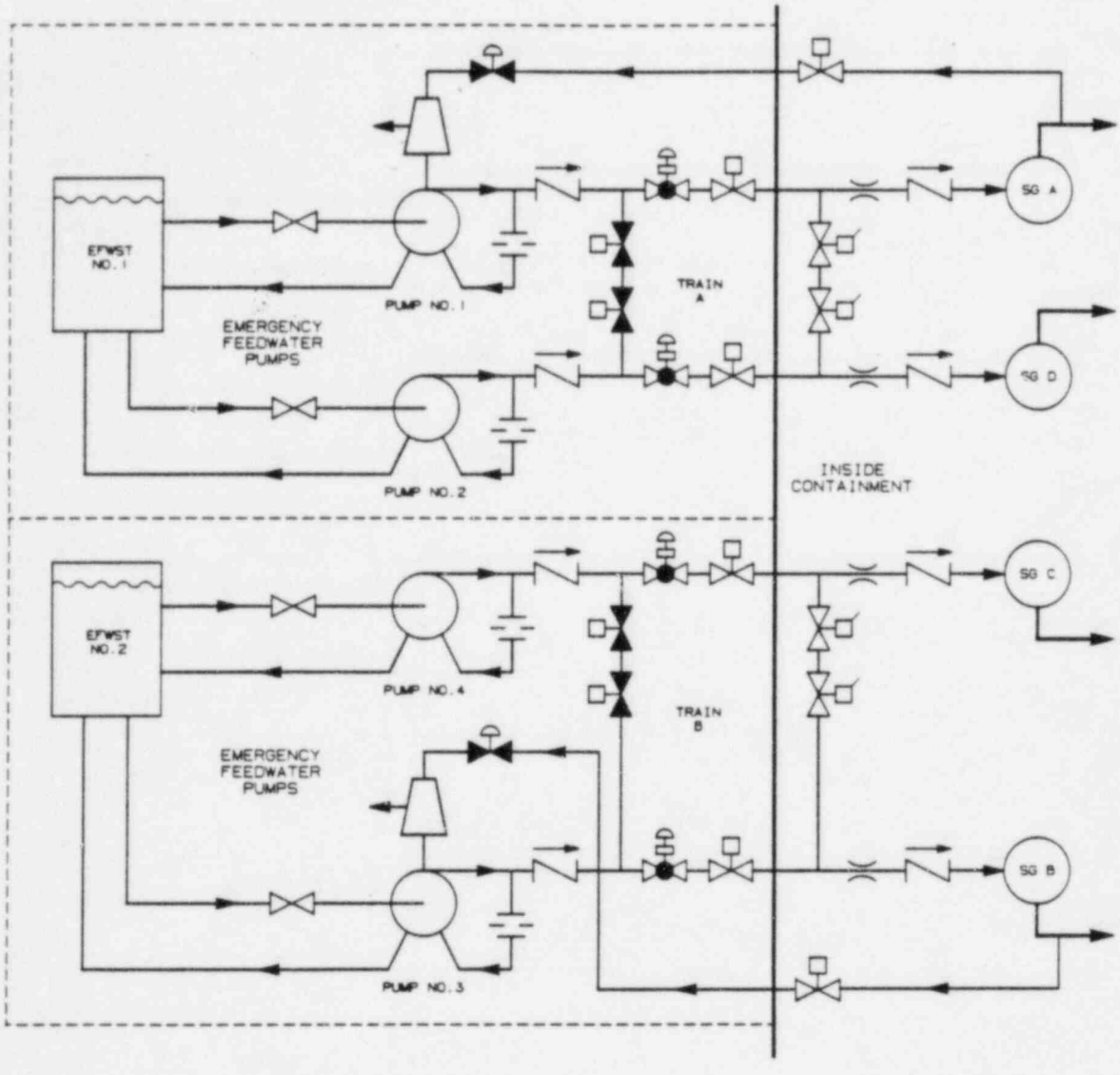


Figure 3.7.2-1 Emergency Feedwater Simplified System Diagram

FIGURE 3.7.2-2

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
EMERGENCY FEEDWATER SYSTEM
(PROPRIETARY)

3.8 BACK-UP SEAL INJECTION SYSTEM

3.8.1 SYSTEM DESCRIPTION

The Back-up Seal Injection Pump in the CVCS is designed to deliver the required flow of seal injection water to all four Reactor Coolant Pumps (RCPs) in the event that the normal seal injection flow is lost. The BSI consists of a positive displacement pump driven by a DC motor. The DC motor receives power from a DC generator driven by a small diesel motor. DC power is also available from AC sources if they are available. The system is a control grade system.

A simple schematic of the system is shown in Figure 3.8-1.

3.8.2 FAULT TREE ANALYSIS

The BSI is modeled in the fault tree shown in Figure 3.8-2.

3.8.2.1 SUCCESS CRITERIA

The success criteria for the BSI is to provide sufficient flow to all four RCPs.

3.8.2.2 DEPENDENCE ON SUPPORT STATES

Since the BSI has its own dedicated diesel generator power system, there is no dependence on support states.

3.8.2.3 RANDOM FAILURE MODEL

The random failure fault tree models were developed and applied according to the APWR Fault Tree Guidelines in Section 3.10. The mission time is 6 hours.

3.8.2.4 COMMON CAUSE MODEL

Common cause was not treated as a failure mechanism for the components in this system since there are no commonalities between this system and any other.

3.8.2.5 TEST MODEL

The system is a control grade system and is not tested. However, the system is used to keep the accumulators full and for back-up CVCS seal injection. The analysis assumes that the system is used at least once every three weeks and is therefore "tested" routinely.

3.8.2.6 MAINTENANCE MODEL

Maintenance of the system is modeled by segments. Table 3.8-1 lists all of the components in the model and if they are maintained. The table also indicates which valves have failure to restore as a failure mode.

3.8.2.7 HUMAN ERROR MODEL

Human error modeling consisted of failure to restore valves to the proper position following test or maintenance.

3.8.2.8 INPUT DATA

Table 3.8-1 lists all the components used in the fault tree model, their identifiers, failure modes, and the probability and variance used for the quantification. The data for the failure probabilities is drawn from the data bank described in Section 3.10.5.

3.8.3 FAULT TREE QUANTIFICATION

3.8.3.1 SYSTEM UNAVAILABILITY CALCULATIONS

The fault trees were analyzed using the WAMCUT computer code. Table 3.8-2 provides the results of this analysis.

3.8.3.2 DOMINANT CUTSETS

The dominant cutsets are also indicated in Table 3.8-2.

TABLE 3.8-1
INPUT DATA FOR BSI

(a,c)

TABLE 3.8-1
INPUT DATA FOR BSI (Cont)

[ ] (a,c)

TABLE 3.8-2

BACK-UP SEAL INJECTION UNAVAILABILITY AND DOMINANT CUTSETS

System Unavailability [ ] (a,c)

Variance

Dominant Cutsets

Description	Contribution
[	] (a,c)

(a,c)

Figure 3.8-1 Simplified System Diagram Emergency Seal Cooling System

FIGURE 3.8-2

ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
EMERGENCY SEAL COOLING SYSTEM
(PROPRIETARY)

3.9 STEAM GENERATOR OVERFILL PROTECTION SYSTEM

3.9.1 SYSTEM DESCRIPTION

A Steam Generator overfill protection system has been provided to prevent water flow through downstream steam pipes and valves following, for example, a steam generator tube rupture accident. Preventing such flow increases the integrity of the steam generators isolation function by reducing the probability of both pipe failure and valve failure.

The system consists of a four inch line and normally open motor operated valve that branches into two three inch lines with normally closed solenoid operated globe valves. These valves provide a safety grade steam generator blowdown to the Emergency Water Storage Tank (EWST). Valve actuation open occurs on high-high steam generator water level, and closure occurs on some lower level. The opening of either valve will prevent an overfill condition in the affected steam generator following a tube rupture. A simplified flow diagram of the system is presented in Figure 3.9-1.

3.9.2 FAULT TREE ANALYSIS

3.9.2.1 FAILURE TO PREVENT OVERFILL

The fault tree of the system failing to operate upon the occurrence of increasing steam generator water level is presented in Figure 3.9-2.

3.9.2.2 SUCCESS CRITERIA

Either one of two parallel solenoid valves must open upon demand to prevent steam generator overfill.

3.9.2.3 DEPENDENCE ON SUPPORT STATES

It is assumed that the solenoid operators are powered by 125 V DC power, and thus available independent of plant support state. If power supply is

120 V AC, which is battery backed through an inverter, it also is assumed to be available in all plant states.

3.9.2.4 RANDOM FAILURE MODEL

Random component failures include those that could cause the motor operated block valve to be closed when a demand is put on the system. Also, those failures which could cause the solenoid operated valves to fail to transfer to the open position are modeled.

3.9.2.5 COMMON CAUSE MODEL

Common cause failure of the redundant solenoid valves is modeled, utilizing a beta factor of 0.1. No common cause failures between steam generators is modeled, since the demand on the system may be caused by a steam generator tube rupture, which affects a single SG.

3.9.2.6 TEST MODEL

It is assumed for this analysis that a flow test, with verification of flow through both valves, will be performed at each refueling (18 month intervals).

3.9.2.7 MAINTENANCE MODEL

If a system failure occurs during test, maintenance is assumed to restore the system to operability before power operation is resumed.

3.9.2.8 HUMAN ERROR MODEL

Operator error in failing to open and electrically lock out motor operated valve 9780 is not considered a credible failure mode in this analysis, since closure of the valve is only anticipated for either isolation of a failed-open solenoid of valve, or following solenoid valve maintenance, which is a very low frequency event. Also, a system flow test following solenoid valve maintenance will assure that the MOV has been restored to its open position.

3.9.2.9 INPUT DATA

The input data the quantification of the fault tree is presented in Table 3.9-1.

3.9.3 FAULT TREE QUANTIFICATION

3.9.3.1 SYSTEM UNAVAILABILITY CAICULATION

Quantification of the fault tree shows an unreliability of [ ] (a,c) with a variance of [ ] (a,c) of the system on demand. Due to the long period of time between test, the local failure of the single MOV dominates the system unreliability. It is felt that this is a very conservative representation of system failure, since an actual failure mode of the subject valve consistent with failures that comprise the data base is incredible. Most valve failures to the closed position, except for operator errors, are comprised of switch and control failures (power is locked out to this MOV), and valve stem failure due to corrosion, which generally isn't applicable to the main steam or feedwater systems (failures have usually manifested themselves in non-filtered or purified water systems, such as service water). Therefore, this result is considered to be conservative, and is used to maintain consistency throughout the systems analysis.

3.9.3.2 DOMINANT CUTSETS

The dominant cutsets and their relative contribution to system unreliability are presented in Table 3.9-2.

Table 3.9-1

Input Data For Steam Generator Overfill Protection System

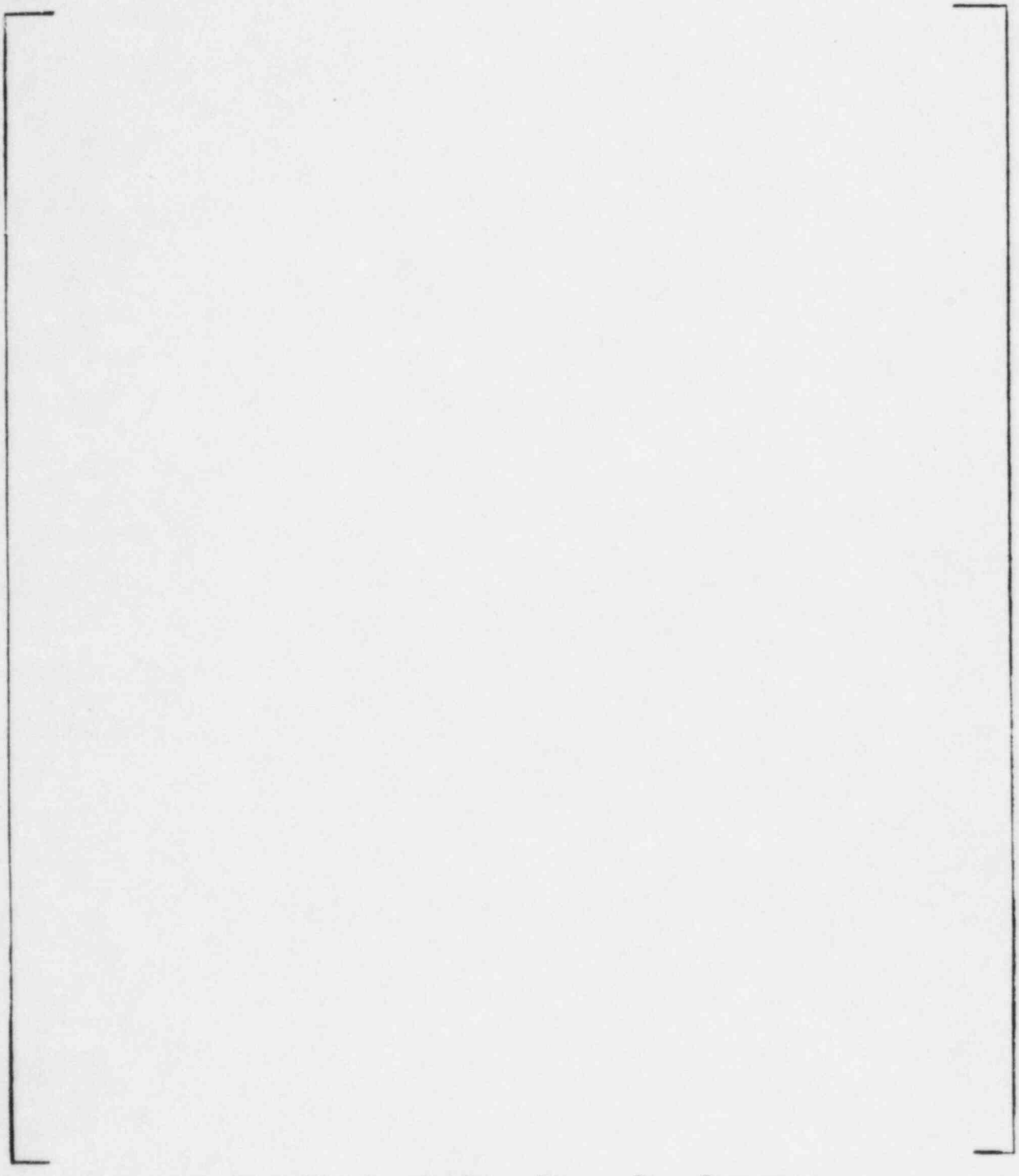
[ ] (a,c)

Table 3.9-2

Dominant Failure Cutsets of the Steam Generator
Overfill Protection System

Failure Description	Contribution (%)
Local failure of MOV 9780 (Fails closed)	94
Common cause failure of both Solenoid Valves, 9783, 9784 Fail to OPEN ON DEMAND	6

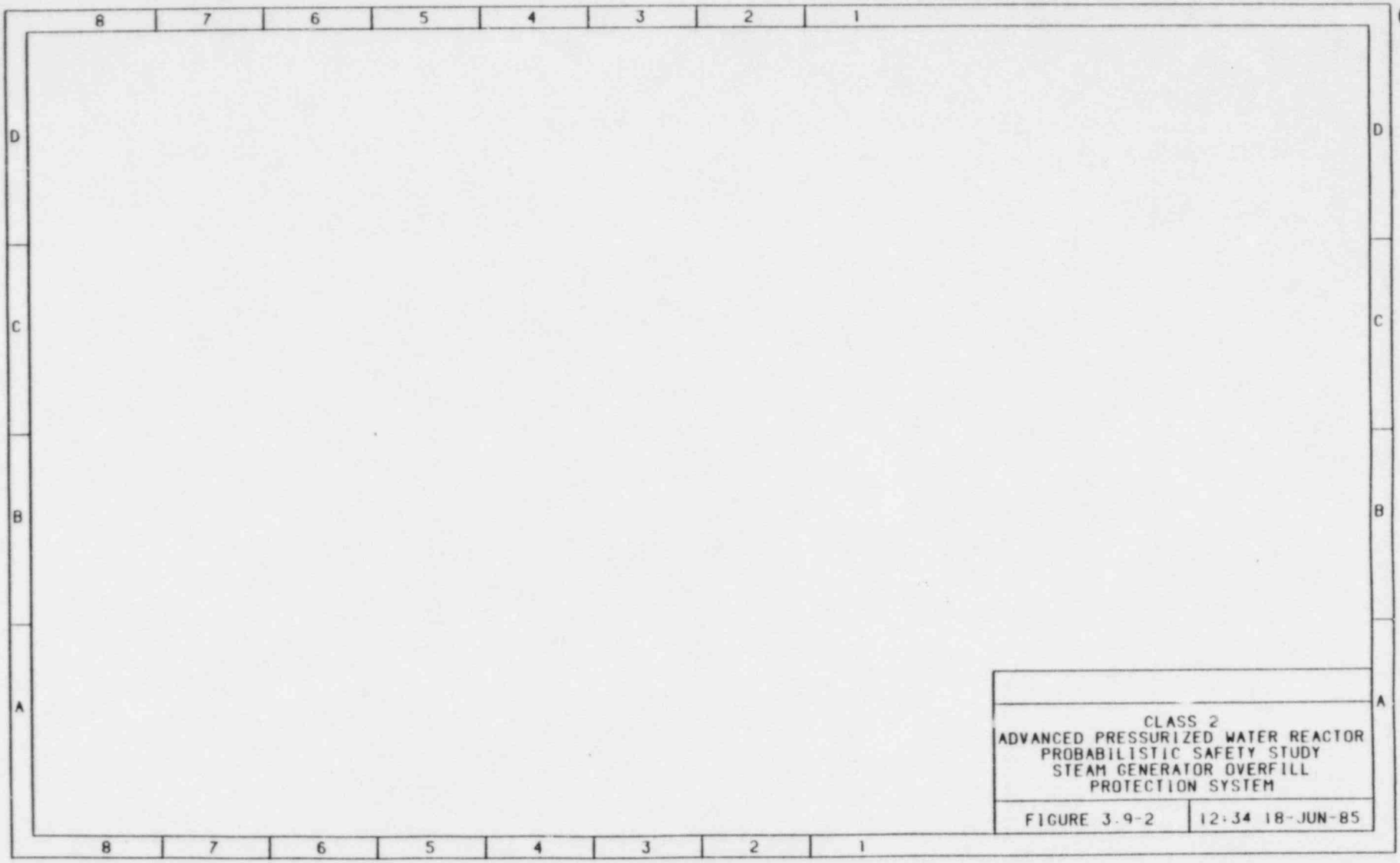
13804-9



(a,c)

Figure 3.9-1 Simplified System Diagram - Steam Generator Overfill Protection System

(a,c)


8
7
6
5
4
3
2
1
D
C
B
A
CLASS 2
ADVANCED PRESSURIZED WATER REACTOR
PROBABILISTIC SAFETY STUDY
STEAM GENERATOR OVERFILL
PROTECTION SYSTEM
FIGURE 3.9-2
12:34 18-JUN-85

3.10 GUIDE TO FAULT TREE DEVELOPMENT

3.10.1 FAULT TREE GUIDELINES

3.10.1.1 GENERAL

In order to assure consistency in the system fault trees for the APWR Program, Westinghouse will follow a set of basic guidelines for their systems analyses. The guidelines have been developed with the intent of following the principal methods now used in PRAs and as described in the "PRA Procedures Guide" (NUREG/CR-2300, Revision 1) and also outlined in "Probabilistic Safety Analysis Procedures Guide" (NUREG/CR-2815, Jan, 1984). Engineering judgement will be the final arbiter in taking exception to these guidelines and should be noted by the analyst in his/her tree documentation.

3.10.1.2 RANDOM FAULT POSTULATION AND CONSIDERATION

a) Pipe ruptures and orifice plugging are not considered as credible faults since their contribution to system fault, compared to that of other components, is insignificant.

   Although a system may be in standby for long periods of time prior to the accident, other system faults such as valves being mispositioned, valves not opening/closing on demand, or pumps not starting and running on demand will dominate.

b) Misposition of normally open manual, air, and motor-operated valves prior to the accident due to human error and/or spurious control signal will remain as a system fault, if credible (see test and maintenance Section 1.3).

c) Misposition faults of valves prior to an accident will not be included in the fault trees if the valve receives an automatic signal to return

to its operable state under accident conditions. When opening time is critical for the accident condition, it should be evaluated on a case-by-case basis.

d) Potential flow diversion paths will be included as system faults if these paths contribute a flow diversion area that is greater than 5 percent of the desired flow path area. However, if the pressure differential between the desired path and the potential diversion path is extremely high, a flow area less than 5 percent in the diversion path may prove to be significant.

e) Potential flow diversion paths isolated from the main flow path by normally closed valves will be treated as faults of the system. Valve misposition prior to the accident due to human error and/or spurious control signal will be considered a system fault, if credible.

f) No credit is taken in the first cut of the fault trees for alternate sources of cooling water or electric power even in the cases where the source can be remotely lined up from the control room.

g) Control circuit faults of components after successful initial operation will be considered only in those cases where the component is expected to receive an additional signal during the course of the accident to readjust or change its operating state.

h) Tank failures are included in the fault trees, but mechanistic failure of heat exchangers (coolers) to transfer heat due to plugging of the primary side and leakage (primary to secondary) are not.

i) Check valves failing closed to flow in the forward direction and failing open to flow in the reverse direction will be included as credible events.

3.10.1.3 FAULTS DUE TO TEST AND MAINTENANCE

a) Maintenance unavailabilities will be treated at a train level; namely, a maintenance unavailability will be assigned to each maintainable train, not to individual components. Unavailability of components due to test or maintenance and human errors associated with failing to restore components to their operable state, following test or maintenance, will be included along with random hardware faults (see items d) and f)).

   In order to avoid counting test or maintenance faults that are not allowed by tech specs, such as having two trains of a system simultaneously out for test or maintenance, "not" gates will be used where appropriate, making the test/maintenance of each train a mutually exclusive event.

b) Only those components whose failure is detected by normal testing conducted during power operation of the plant will be considered maintainable. Additionally, if maintenance on any component causes the plant to operate at less than nominal power then that component will still be considered to be maintainable.

c) The test mode of a pump and its associated valves and other components that prevent a system from meeting its design safety function will be considered as a credible failure mode, unless automatically realigned within acceptable time limits.

d) The failure of test personnel to return valves or pump trains to their normal position after a test will be considered as a credible event if they 1) do not receive an "S" signal; and 2) are not alarmed or annunciated at the control board. This event will be considered equivalent to a random failure and will be included in the fault tree as "failure to restore component XXX after test".

e) A component is considered maintainable if it can be flow isolated from the system by a manual valve or power operated valve (XV or AV) in series with the component. Check valves cannot be used to isolate a component for maintenance due to backflow leakage.

f) The failure of maintenance personnel to return valves or pump trains to their normal position after valve or pump maintenance will be considered as credible events if (1) proper positioning can not be detected using the required pump flow test, (2) valve misposition is not immediately detected at the control board by alarm or annunciation, or 3) the component does not receive an "S" signal. Credit is not taken for control indication. If credible, this event will be considered equivalent to a random failure and will be included in the fault tree as "failure to restore component XXX after maintenance". Common cause failure to restore valves will also be considered as discussed in Section 3.10.3.

g) Maintainable components will be separately addressed only if they cannot be considered in the maintenance of a train.

3.10.1.4 INCLUSION OF OPERATION ACTION

a) Operator errors which fail to align valves or fail to operate other components in response to the accident will be included only for those components which are specifically identified in procedures as requiring operator manipulation.

3.10.1.5 HEATING, VENTILATION AND AIR CONDITIONING SYSTEM (HVAC)

Failures of HVAC are not deemed to be of significant contributors in system failures. The major pumps have their own cooling through CCWS and do not depend upon room cooling.

Also, the loss of switchgear room cooling will lead to a long term flow heat-up.

The loss of HVAC functions in the operating room can be countered by moving to the auxiliary shutdown panel in the auxiliary building.

3.10.2 FAULT TREE CONSTRUCTION

3.10.2.1 GENERAL

The fault tree construction shall be performed according to procedures suggested in SAND81-0062 "Fault Tree Analysis Procedures for the Interim Reliability Evaluation Program (IREP)" (December 1980).

First, the fluid systems interfacing with the system of interest are to be determined from P and IDs.

The system piping drawings are to be simplified by canceling those pipe segments which either cannot affect system performance significantly, or contain normally closed manual valves which could only improve system performance if opened (i.e. some types of test and bypass lines).

On the basis of system failure criteria, system TOP event is set and a failure logic for the discharge ends of the system is developed as input to the TOP event.

The development of system fault trees is continued by working back through the system and considering, initially, only the basic faults at the segment or component level that will affect the system probability of failure.

Finally, the component fault logic is developed as shown in Section 3A.3.3.

3.10.2.2 COMPONENT LOGIC MODULES

Modular logic models have been developed for the following components to assure consistency between fault trees.

- motor-driven pump (Fig. 3.10.2-1)
- turbine-driven pump (Fig. 3.10.2-2)
- motor-operated valve (Fig. 3.10.2-3 and Fig. 3.10.2-4)

- solenoid-operated valve (Fig. 3.10.2-5 and 3.10.2-6)
- air-operated valve (Fig. 3.10.2-7 and Fig. 3.10.2-8)
- check valve (Fig. 3.10.2-9)
- manual valve (Fig. 3.10.2-10)
- heat exchanger (Fig. 3.10.2-11)
- tank (Fig. 3.10.2-12)
- test or maintenance at the train level (Fig. 3.10.2-13)
- failure to restore a component following test or maintenance (Fig. 3.10.2-14)

Each module should include the following types of events:

- local fault
- support system faults
- component unavailability due to test or maintenance.

The local fault is a basic event including a wide variety of causes resulting in the same failure mode. Component support systems could be the electric power, the control power, the actuation, the cooling water, the control system and other systems whose failure directly or indirectly affect component correct operation.

The ESF (4160 V) electric power and essential service water are considered to be support systems.

Control, Actuation, and Loss of Control Power in Logic Modules

The logic modules for pumps and valves (Figures 3.10.2-1 through 3.10.2-8) have basic undeveloped electrical faults involving the control circuit, the actuation circuit, and the power supplied to these circuits. The control circuit is made up of components such as switches, relays, contacts, and wiring that control the normal operation of the pump or valve. The actuation circuit is made up of switches and devices that automatically activate the component for emergency safety-related operation upon receipt of an "S" or other ESFAS signal. The control power opens or closes the contact, relay, or circuit breaker that connects or disconnects the source of main (or motive) power to the pump or valve. The fault boundaries are shown on Figures 3.10.2-15 through 3.10.2-17. Figure 3.10.2-15 shows two motor-operated valves connected to the same bus in a motor control center. Loss of 480 V power affects both valves and therefore, a transfer out is used in the logic module to indicate that other valves or trains of the system may be affected.

The classification of electrical faults into "control" and "actuation" is based on previous work done for Millstone Unit 3 Probabilistic Safety Study.

3.10.2.3 FAULT EVENT IDENTIFICATION

The codes to be used for component failure identification will result in four to eight characters. The format of component failures in system fault trees is XXYYYYZZ where:

- XX is the component identification code (see Table 3.10.2-1)
- YYYY is the number individuating the single component in system P and I drawings (from one to four characters may be used)
- ZZ is the specific component failure mode (see Table 3.10.2-2).

AC = air cooler

B = BREAKER
- BB = bus feed
- BC = circuit
- BT = trip/bypass
- BU = bus
- BX = battery charger
- BY = battery

C = CIRCUIT
- CA = actuation
- CC = control
- CT = trip
- CP = control power
- DA = damper
- DC = DC generator
- DE - diesel engine
- DG = diesel driven generator
- DX = motor driven generator

E = ELECTRONICS
- EB = comparator/bistable
- EC = signal conditioning
- EG = general instrumentation
- EM = analog processing module
- ES = solid state device
- ET = terminal board
- FL = screen/filter
- FU = fuse

E = ELECTRONICS (Cont.)

HE = human error
HX = heat exchanger
IN = power inverter
LG = logic gate
MC = motor control center
OR = orifice
PI = pipe

P = PUMP

PD = diesel driven
PM = motor driven
PT = turbine driven
PS = loop power supply

R = RELAY

RE = regular
RP = protective (overvoltage, overcurrent, underfrequency, etc.)
RT = time delay
RM = radiation monitor

S = SWITCH

SB = pushbutton
SL = level
SP = pressure
SR = manual rotary
ST = static transfer
SV = valve limit/torque
SS = scram system
TK = tank
TR = main/auxiliary transformers

COMPONENT IDENTIFICATION CODE (Continued)

T = SIGNAL TRANSMITTERS

TD = differential pressure
TE = temperature element
TF = flow
TL = level
TP = pressure
TT = temperature

V = VALVES

VA = air operated
VB = butterfly
VC = normal check
VD = air operated check valve
VE = stop check valve
VM = motor operated
VR = relief
VS = solenoid operated
VU = spring loaded safety valve
VX = manual operated

WR = wiring

FAILURE MODES

ZZ	Failure Mode
C	Valve, Check, Fails to Open
	Valve, Manual, Transfers Closed
	Valve, Motor Operated, Transfers Closed
O	Valve, Manual, Transfers Open
	Valve, Relief, Sticks Open
	Valve, Motor Operated, Transfers Open
	Circuit Breaker, Spuriously Opens
Q or D	Valve, Manual, Fails to Operate
	Valve, Air Operated, Fails to Operate
	Valve, Solenoid, Fails to Operate
	Valve, Motor Operated, Fails to Operate
	Circuit Breaker, Fails to Close
HM	Valves, All, Failure to Restore Following Maintenance
HT	Valves, All, Failure to Restore Following Test
FS	Pump, Fails to Start
FR	Pump, Fails to Run
M	Component, Unavailable Due to Maintenance
T	Component, Unavailable Due to Test
F	Component, Miscellaneous Failure
CC	Common Cause
P	Plugged

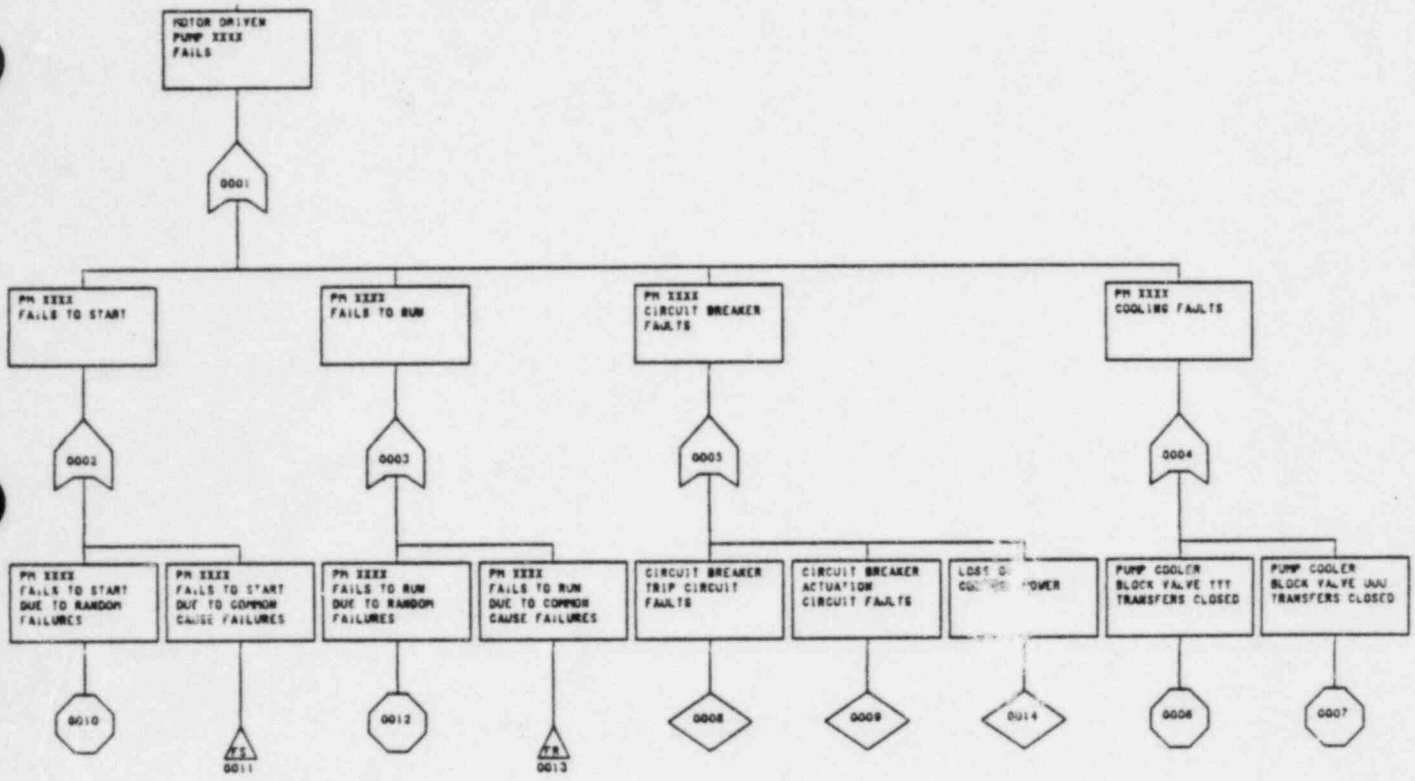


Figure 3.10.2-1

Logic Module MDP for 4160 VAC Motor-Driven Pump

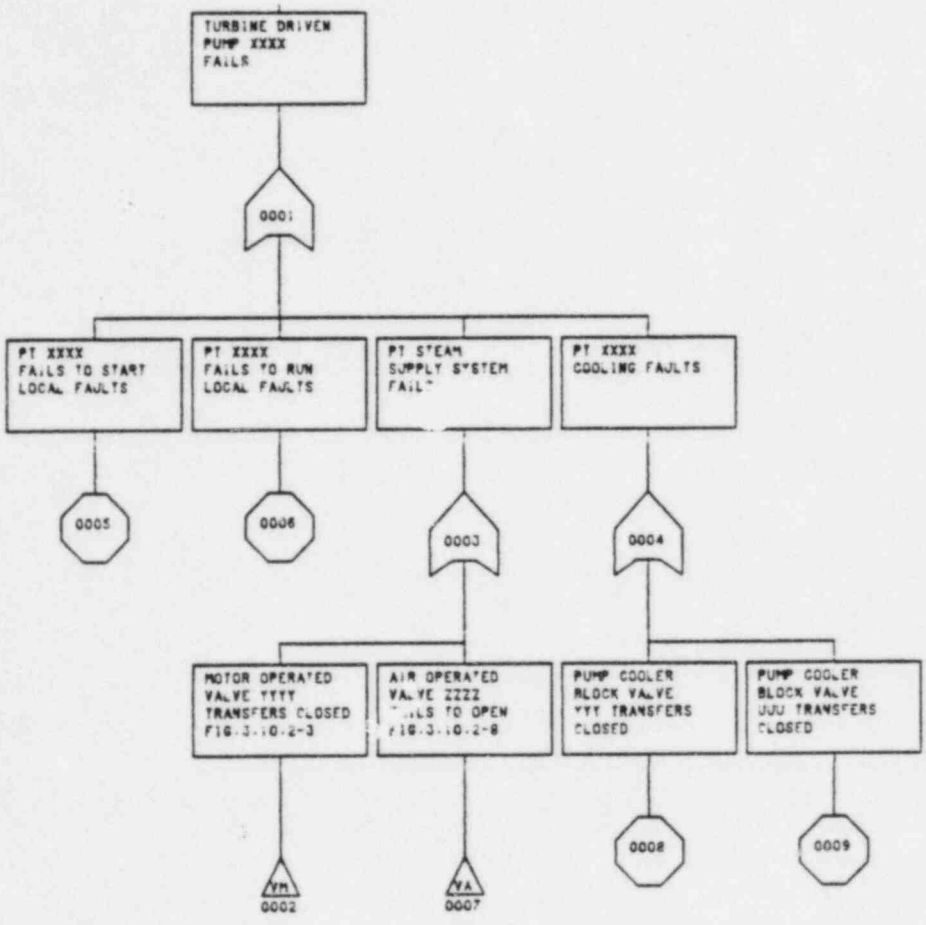


Figure 3.10.2-2

Logic Module TDP for Turbine-Driven Pump

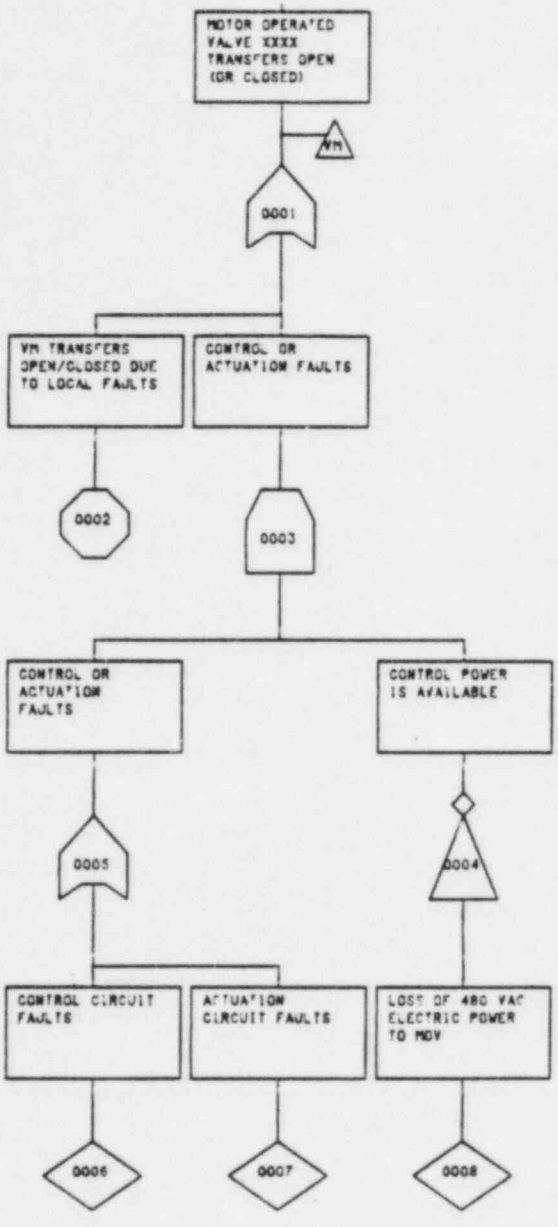


Figure 3.10.2-3
Logic Module MOV for Motor-Operated Valve
Not Required to Move

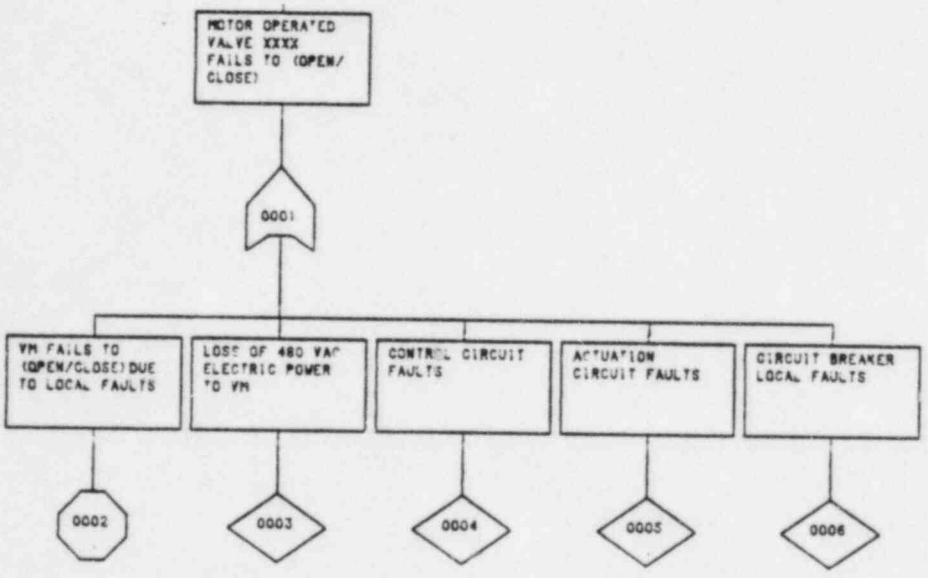


Figure 3.10.2-4
Logic Module MV for Motor-Operated
Valve Fails to Move

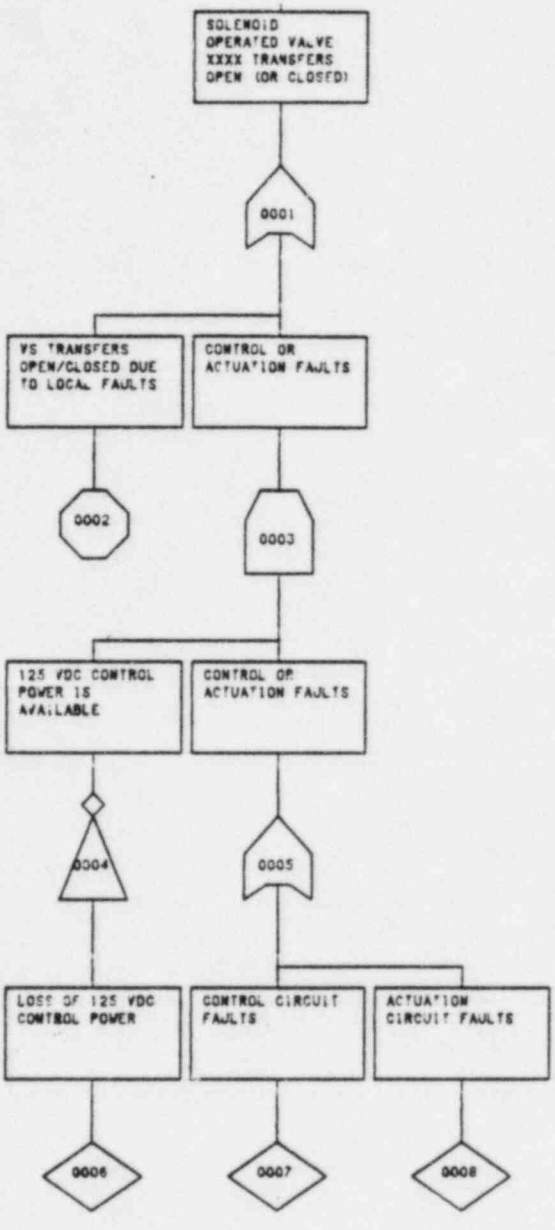


Figure 3.10.2-5
Logic Module SOV for Solenoid-Operated
Valve Not Required to Move

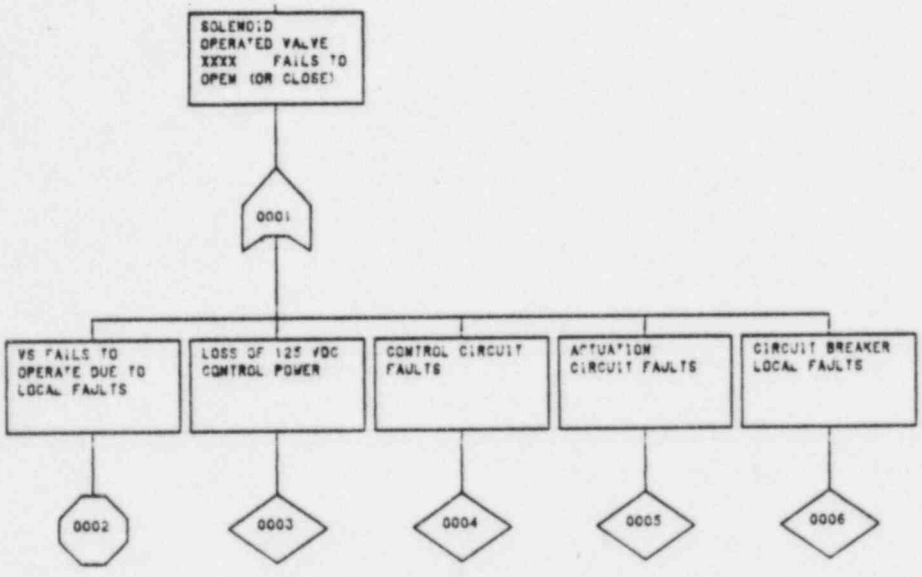


Figure 3.10.2-6
Logic Module SV for Solenoid-Operated
Valve Fails to Move

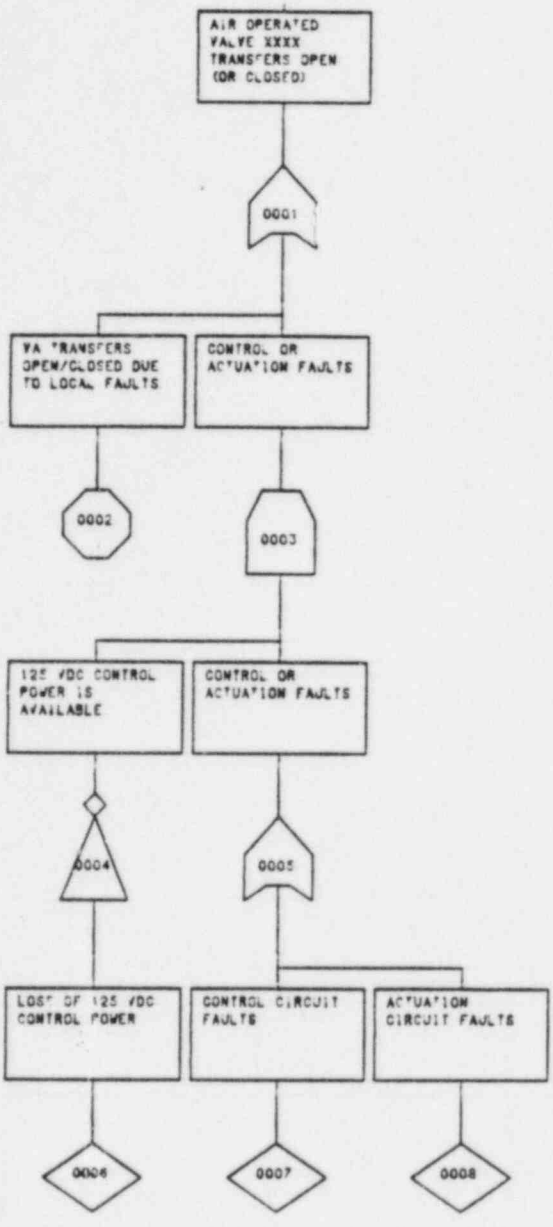


Figure 3.10.2-7
Logic Module AOV for Air-Operated
Valve Not Required to Move

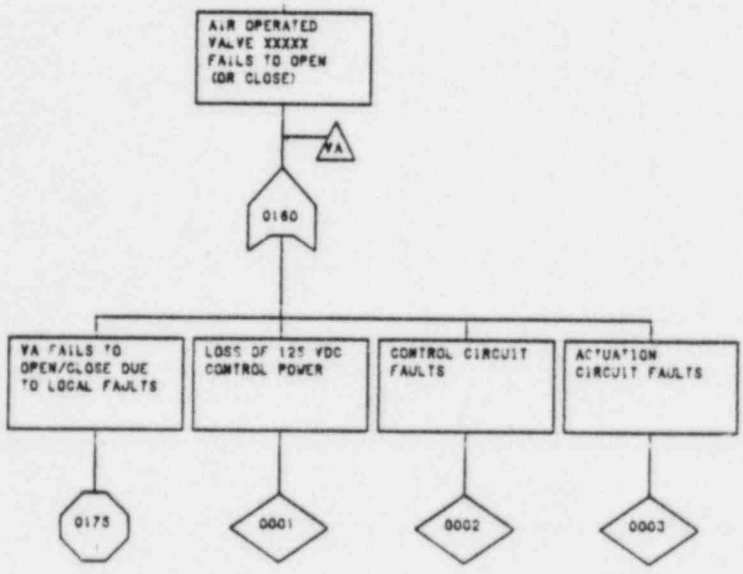


Figure 3.10.2-8
Logic Module AV for Air-Operated
Valve Fails to Move

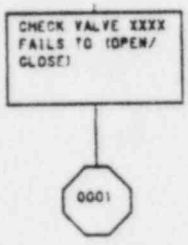


Figure 3.10.2-9
Logic Module CV for Check Valve
Excessive Leakage or Blocked

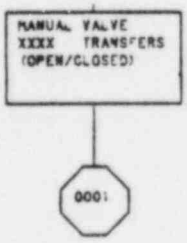


Figure 3.10.2-10
Logic Module XV for Manual Valve

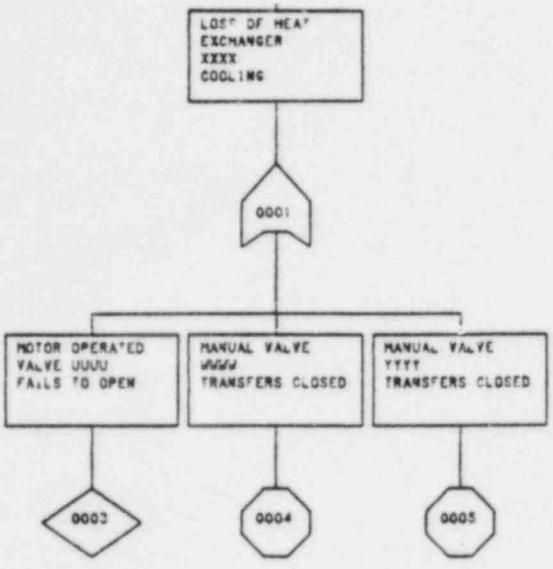


Figure 3.10.2-11
Logic Module HX for Heat Exchanger

Figure 3.10.2-12
Logic Module TK for Tank

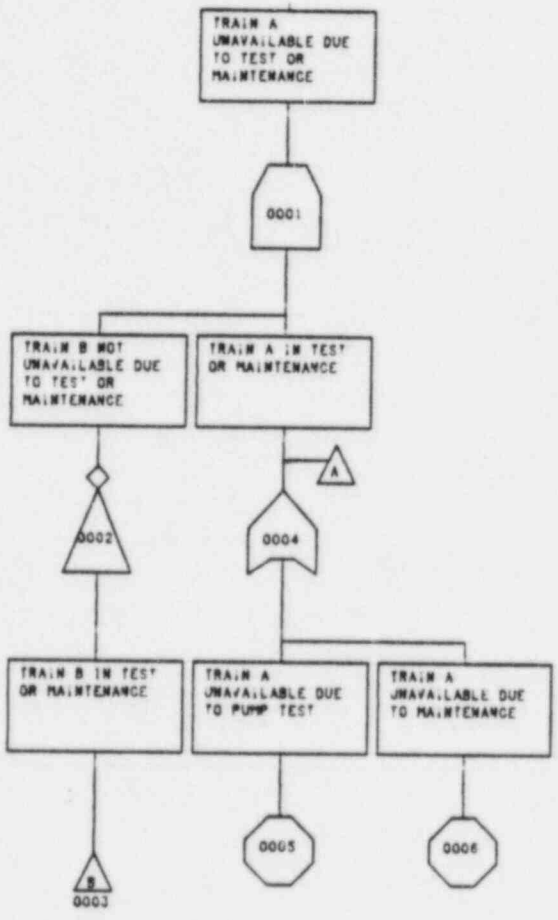


Figure 3.10.2-13

Logic Module TM for Train Test and Maintenance

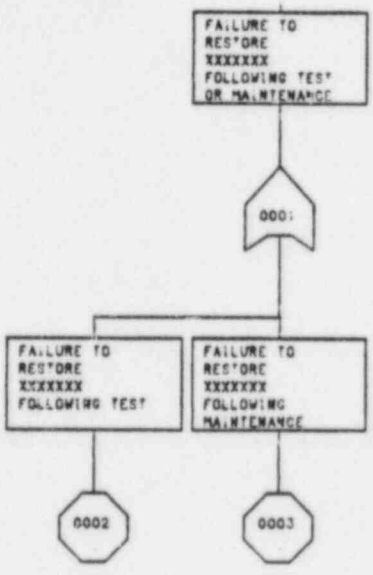


Figure 3.10.2-14
Logic Module FTR for Failure to Restore
Component Following Test and Maintenance

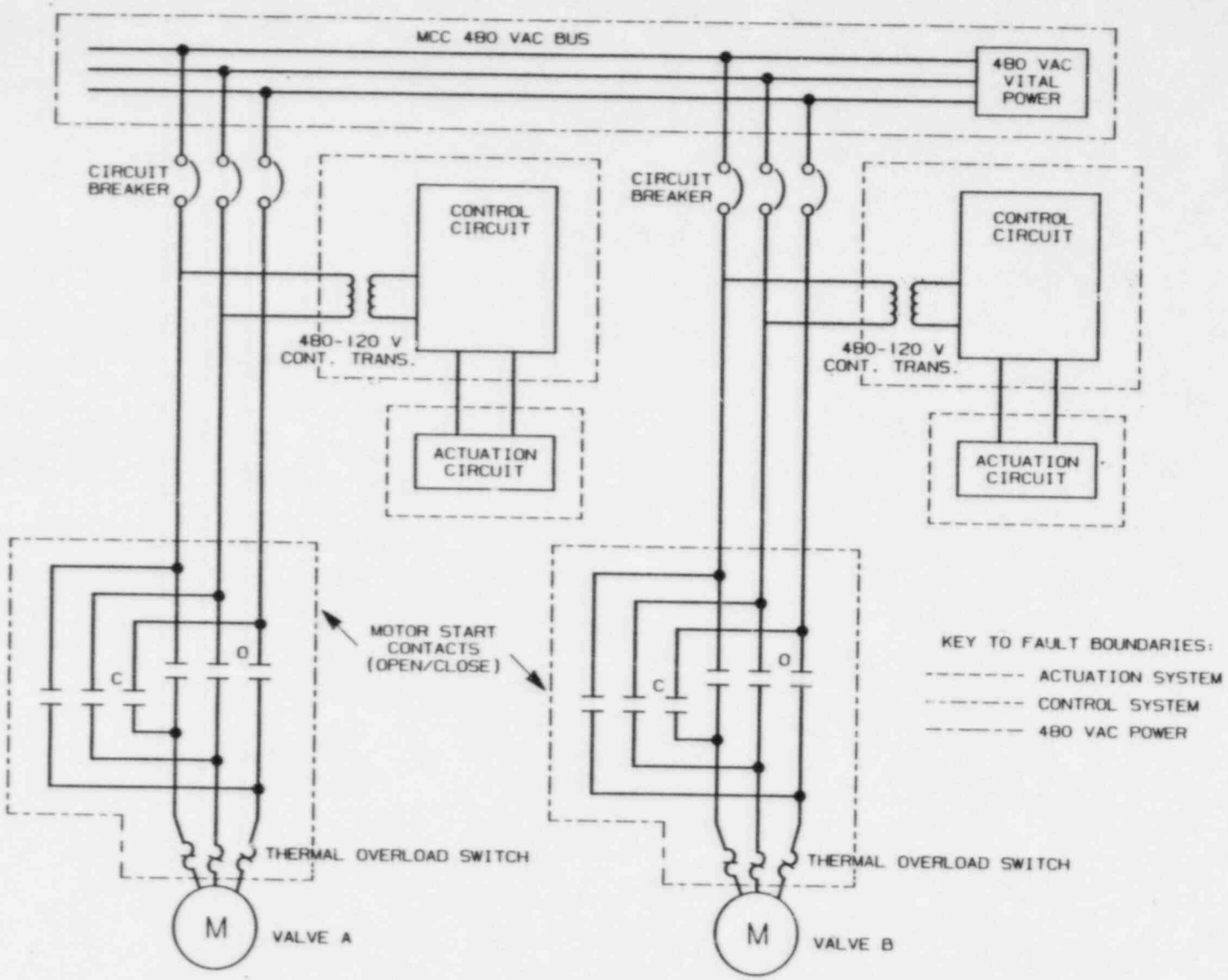


Figure 3.10.2-15. Motor -Operated Valves
Electrial Fault System Boundaries for Figures 3.10.2-3 and 3.10.2-4

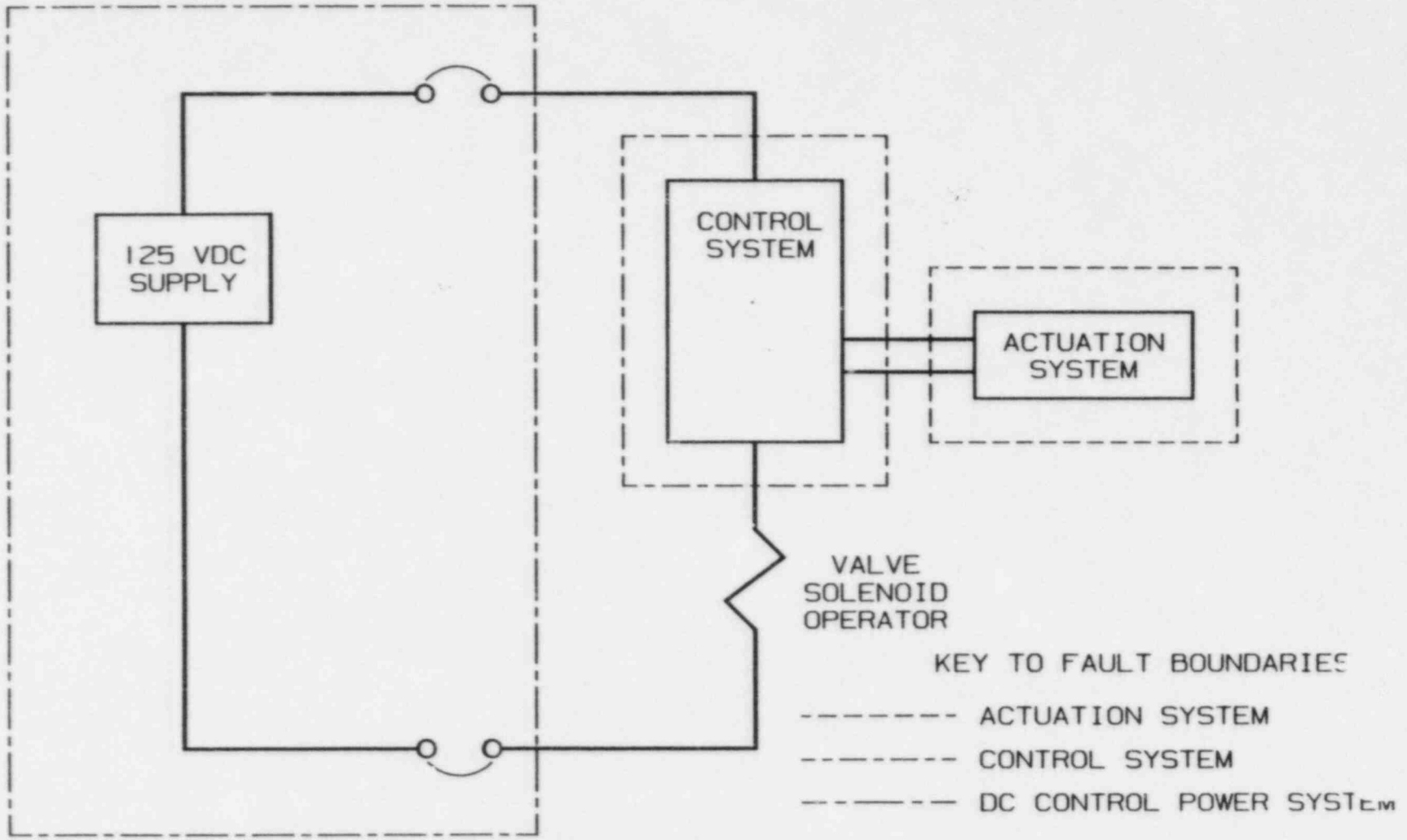


Figure 3.10.2-16. Solenoid-Operated and Air-Operated Valves
Electrical and Control System Boundaries for Figures 3.10.2-5 Thru 3.10.2-8

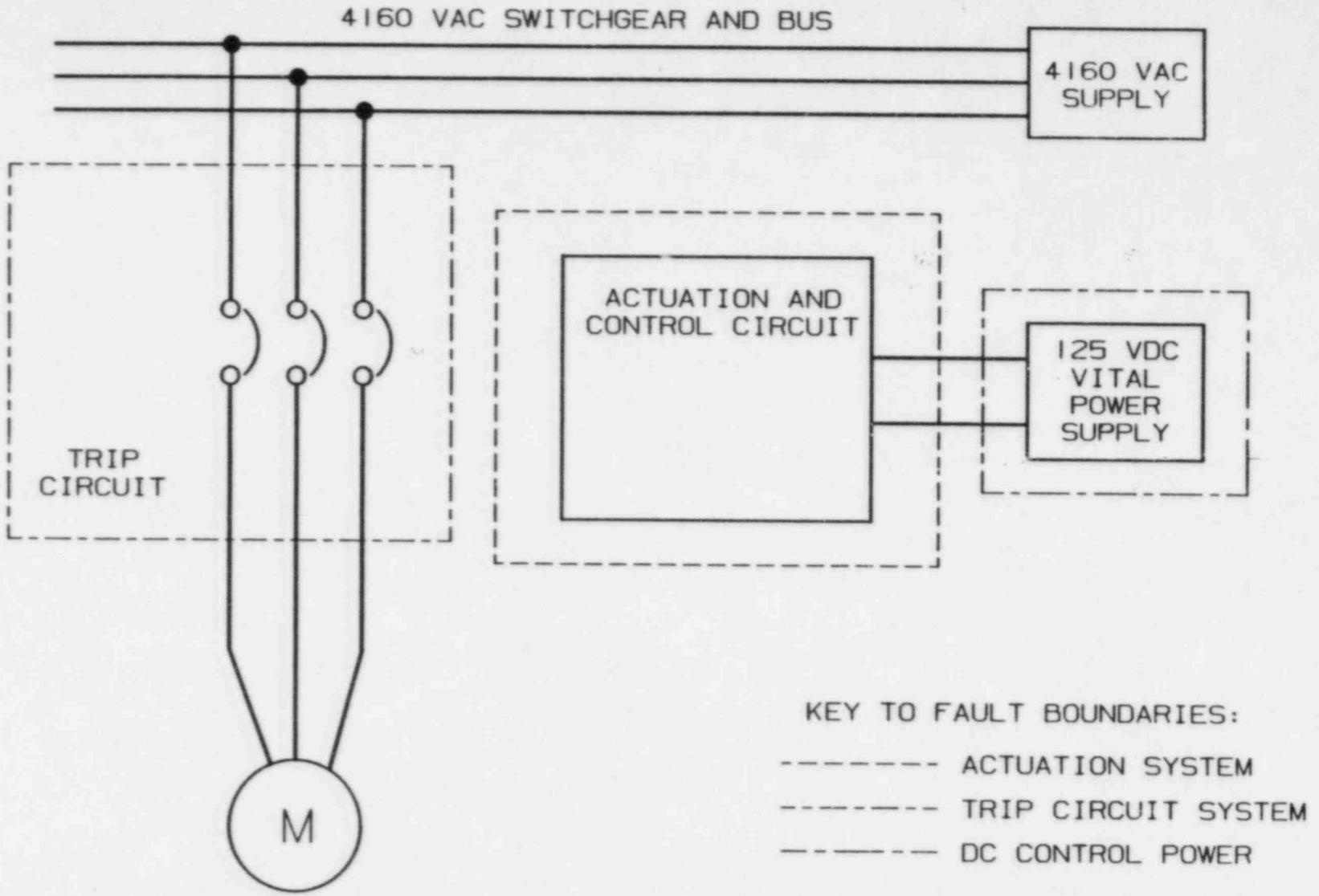


Figure 3.10.2-17. Motor-Driven Pump
Electrical and Control System Boundaries for Figure 3.10.2-1

3.10.3 COMMON CAUSE MODEL

3.10.3.1 MODEL

The following guidelines are used for common cause modeling in fault trees:

A. Explicitly identifiable common cause sources, such as AC/DC power, service water, component cooling water, will be specifically modeled with transfers within the fault tree.

B. For common causes that are not explicitly addressed, the common cause contribution will be either placed near the top of the tree, as shown by Figure 3.10.3-1 or at the component level as illustrated by Figure 3.10.3-2.

C. Common cause will be addressed at least for active components in the system, e.g. pumps and valves that change position.

D. ß factor approach will be used for cases involving 2 components/trains. The ß factors to be used are given by Table 3.10.3-1 for active components. Common cause failure is obtained by multiplying the ß factor times the appropriate random failure probability. For valves required to move, the ß factor is applied to the sum of the random failure due to local faults plus failure due to control and actuation faults. For pumps, the ß factor is applied to actuation, control, and trip circuit faults and to random failures to start and run.

e. For components not addressed in Table 3.10.3-1, if the analyst finds out that common cause potential exists and must be modeled, a ß value of 0.1 is suggested, unless specific data can be found which results in a more reliable reproduction of common cause.

F. For modeling of highly redundant systems (3 or 4 component/train redundancy), the following extended ß factor method will be used:

The $ß_2$, $ß_3$ and $ß_4$ factors will be defined as follows:

β_i = fraction of random failures of a given train/component that will result in failure of a total of i specific train(s)/Component(s) with i = 2,3,4.

For a system involving a m/n (m out of n trains or components) success criteria, the equations to calculate the common cause contribution to system failure are given by Table 3.10.3-2. The value of β_2 is estimated conservatively as:

$$\beta_2 = \beta$$

The other β factors, based on engineering judgment, are estimated as follows:

$$\beta_3 = \frac{1}{5}\beta_2$$

$$\beta_4 = \frac{1}{2}\beta_3 = \frac{1}{10}\beta_2$$

The physical implications of the above definitions are as follows:

Changing a 1 out of 2 system to a 1 out of 3 system will decrease the system unreliability approximately by a factor of 5; adding a fourth redundant train/component will decrease the system unreliability by another factor of 2. No credit will be taken for a fifth train/component. Thus going from a 1/2 success criteria to a 1/4 success criteria will approximately improve system failure probability by an order of magnitude.

3.10.3.2 A CALCULATIONAL EXAMPLE

The following example is provided to illustrate the above model for a 1/n success criteria.

Given that

Q_T = 1 train unavailability = 1.0×10^{-2}

$\beta_2 = \beta = 0.1$,

The following system availabilities (Qs) are calculated using equations from Table 3.10.3-2:

m/n	Q_s	System Unavailability Equation
1/1	1.0×10^{-2}	$Q_s = Q_T$
1/2	1.1×10^{-3}	$Q_s = Q_T^2 + \beta_2 Q_T$
1/3	2.3×10^{-4}	$Q_s = Q_T^3 + 3\beta_2 Q_T^2 + \beta_3 Q_T$
1/4	1.1×10^{-4}	$Q_s = Q_T^4 + 6\beta_2 Q_T^3 + 4\beta_3 Q_T^2 + \beta_4 Q_T$
1/5	1.1×10^{-4}	(no credit is taken for the fifth train)

The general equation for Q_s is:

$$Q_s = Q_R + Q_{cc}$$

where Q_{cc} is the common cause failure probability, and Q_R is the random failure probability. For a 1/n system, Q_R is given by:

$$Q_R = Q_T^n$$

TABLE 3.10.3-1

COMMON CAUSE FAILURE TYPES

Component/Failure Type

Diesel Generators

Pumps

- Running Pumps/fail to operate
- Alternating Pumps/fail to start
  /fail to operate
  /fail to operate
  no command faults
- Auxfeed Pumps/fail to start MDP
  /fail to operate MDP
  /fail to start TDP
  /fail to operate TDP
  /fail to start DDP
  /fail to operate DDP
- Standby Pumps/fail to start
  /fail to operate

Valves

- AOV/fail to open, close or operate
- AOV/improper valve configuration*
- MOV/fail to open, close or operate
- MOV/improper valve configuration*

$\beta = 0.1$ For the common cause failures given above (explanation and justification for $\beta = 0.1$ will be included in final guidelines)

* Improper valve configuration is failure to restore following test or maintenance, to be used if improper valve positions are not alarmed.

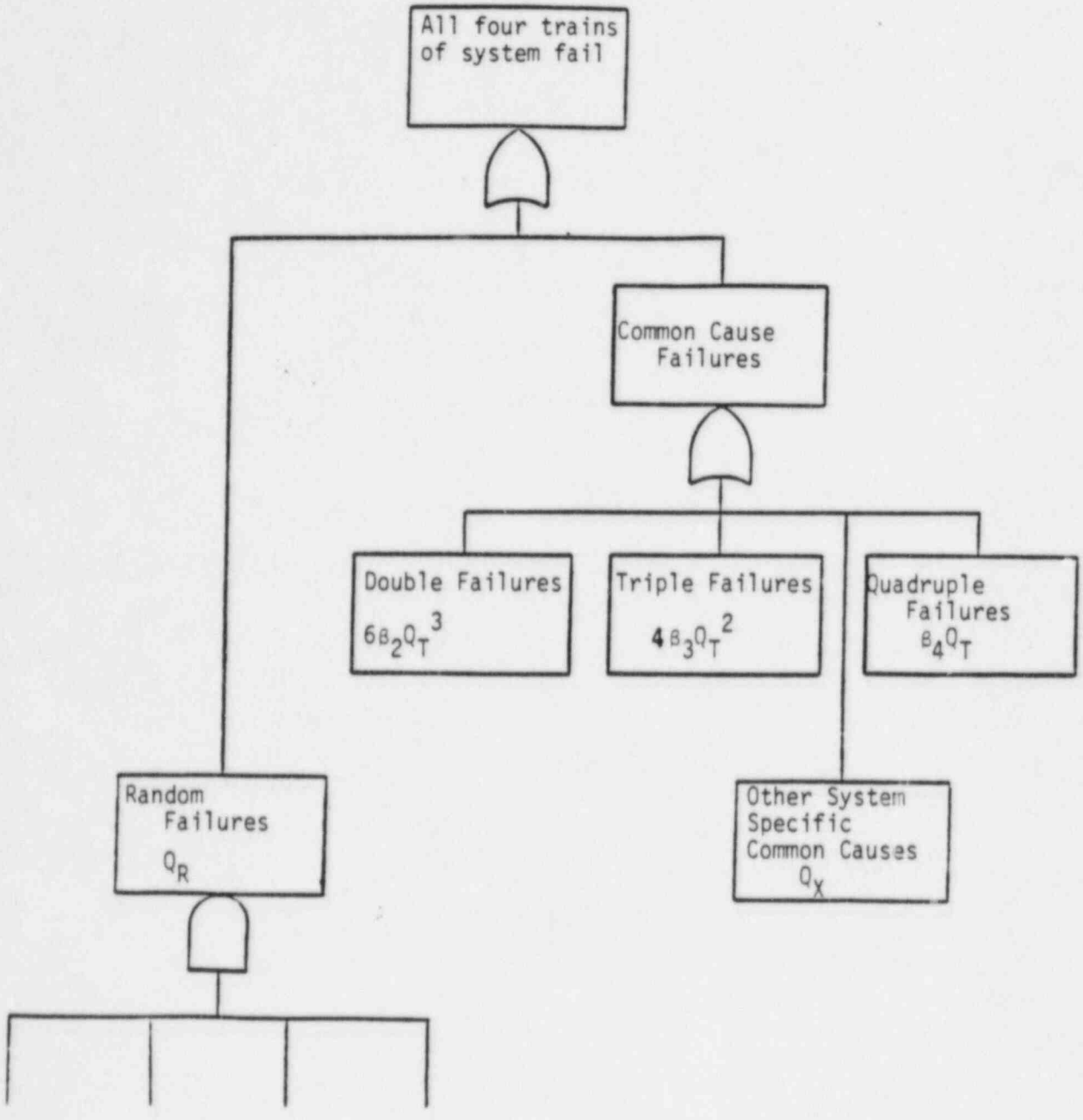


Figure 3.10.3-1

Common Cause in Fault Tree: 1/4 System

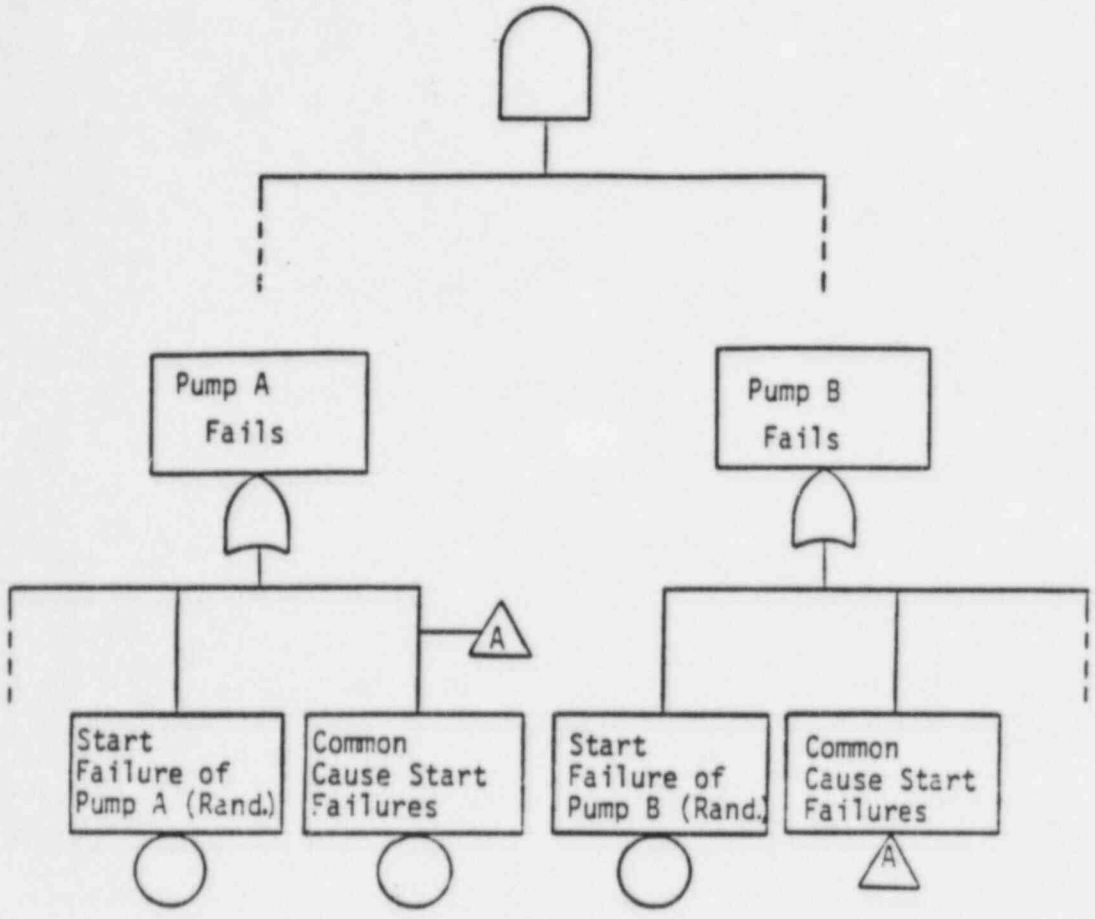


Figure 3.10.3-2
Placement of Common Cause At Component Level

3.10.4 HUMAN ERROR MODEL

3.10.4.1 INTRODUCTION

The operator errors in fault trees will be considered for the following cases:

1. Failure to restore a component to its normal position after a test or maintenance action.

2. Failure to carry out an action specified by written procedures, if the action is needed for successful operation of the system in question.

If the operator actions are complicated in nature (e.g. consist of many subtasks), they may require special modeling in terms of diagnosis, action and recovery phases. In such cases, the human error modeling will be done outside of the fault tree. The hardware and human error failure probabilities will be combined at the top level of the formal fault tree structure.

For human error probability calculations in fault tree analysis, a data bank is constructed. This data bank is summarized in Table 3.10.4-1.

TABLE 3.10.4-1

HUMAN ERROR DATA BANK FOR
FAULT TREE ANALYSIS

Type of Error	Operator Error	ESF System	HEP Per Demand	HEP Variance	Comments
1. Omission	Failure to restore a manual valve to normal position after test or maintenance act.	All ESF Systems	8.5×10^{-4}	5.1×10^{-7}	
2. Omission	Failure to restore a motor-driven pump or an air or motor operated valve to normal position after test or maintenance act.	All ESF Systems	8.5×10^{-5}	5.1×10^{-9}	Valve or pump status displayed at Control Board (CB) switch. Procedures have short list of checkoff provisions ($\leq$ 10 special instructions).
3. Omission	Failure to restore an alarmed motor-driven pump or an air or motor operated valve to normal position after test or maintenance act.	All ESF Systems	8.5×10^{-5}	5.1×10^{-9}	Valve or pump status displayed at CB switch. CB has valve out-of-position annunciator. Procedures have short list of checkoff provisions ($\leq$ 10 special instructions). Currently no credit is being taken for the annunciator alarm.
4. Omission	Failure to initiate corrective action in response to multiple annunciators alarming closely in time.	All ESF Systems	8.1×10^{-2}	1.0×10^{-2}	Operator fails to initiate action given that 10 alarms are competing for his attention in stress situation.
5. Omission and failure to recover	Omission and failure to recover from it (item 4 above) when an important alarmed system fails.	All ESF Systems	8.1×10^{-3}	1.0×10^{-4}	An order of magnitude credit is taken for recovery from error No. 4 above. Service water is an important support system which will be monitored.

3.10.5 TEST AND MAINTENANCE MODEL

Maintenance of system components is modeled explicitly in the fault tree developed for each system. The frequency of maintenance for each train was taken from the following: Zion Probabilistic Safety Study, Table 1.5.1-29, Indian Point Probabilistic Safety Study, Table 1.5.1-21 (Unit 2) and 1.6.1-19 (Unit 3). Several assumptions were made regarding the analysis of maintenance unavailability of components since there is no maintenance data on the APWR systems and to maintain consistency in the application of the model. The first assumption was that the maintenance frequency of given components was the same as the arithmetic average of similar components in the above plants. Frequency of maintenance for different plant components is presented in Table 3.10.5-1. The second assumption is that the times to restore components will follow a log-normal distribution, as assumed for a prior distribution in the Zion study. This results in the use of the mean times to restore components in maintenance as derived on Table 3.10.5-2 (3 day LCO). A mean time to repair of 19 hrs is calculated from this generic model and is used for all systems. Any deviation that may exist between different systems can only be addressed as plant operating experience is gained, where the average time of maintenance of a specific component may be compared to that analyzed. The unavailability of a component or train is calculated as the product of maintenance frequency (hr^{-1}) multiplied by the mean time to restore (19 hr) and is given in Table 3.10.5-3. While these mean restoration times and frequencies of maintenance are just estimates, the model exists in a form that allows updating of the results as plant data is accumulated.

TABLE 3.10.5-1

SPECIALIZED COMPONENT MAINTENANCE FREQUENCY DATA

Component	Specialized Frequency Distribution*	
	Mean (Events/Hour)	Variance
Motor-Driven Emergency Feedwater Pumps	1.48×10^{-4}	1.55×10^{-9}
Turbine-Driven Emergency Feedwater Pumps	2.96×10^{-4}	7.53×10^{-9}
Centrifugal Charging Pumps	1.45×10^{-4}	1.07×10^{-9}
Component Cooling Water Pumps	1.46×10^{-4}	1.82×10^{-9}
Containment Spray Pumps	7.30×10^{-5}	5.43×10^{-10}
Residual Heat Removal Pumps	6.90×10^{-5}	5.24×10^{-10}
Safety Injection Pumps	6.37×10^{-5}	4.51×10^{-10}
Fan Cooler Units	6.55×10^{-5}	3.63×10^{-10}
Diesel Generators	6.7×10^{-4}	8.7×10^{-9}
Essential Service Water Pumps	2.60×10^{-4}	1.67×10^{-9}
SWS Strainers	5.0×10^{-5}	2.5×10^{-9}

*Distributions are assumed to be lognormal.

TABLE 3.10.5-2

PRIOR DISTRIBUTION FOR MEAN DURATION OF MAINTENANCE

Component Inoperability Limit: 72 hours
Parameters characterizing range of lognormal duration distributions:

5th Percentile (hours/event)	Probability	95th Percentile (hours/event)	Probability
1.0	.05		
2.0	.50	24	.05
3.0	.15	36	.05
4.0	.10	48	.15
5.0	.05	60	.50
6.0	.05	72	.15
7.0	.05	84	.05
8.0	.05	96	.05

Distribution: Lognormal
5th percentile: 2 hours/event
95th percentile: 60 hours/event
Mean: 18.7 hours/event
Variance: 668

Basis: Only the most routine maintenance can be performed with a component unavailability time (including removal and return to service operations) or less than two hours. The 72-hour time limit for operation dictates that major maintenance and repair activities be performed during cold shutdown periods. The majority of relatively routine maintenance and some extensive repairs will be completed within two and one-half days, given the high priority assigned to returning the equipment to service within the LCO limit.

Resulting Prior Distribution of Mean Duration of Maintenance:

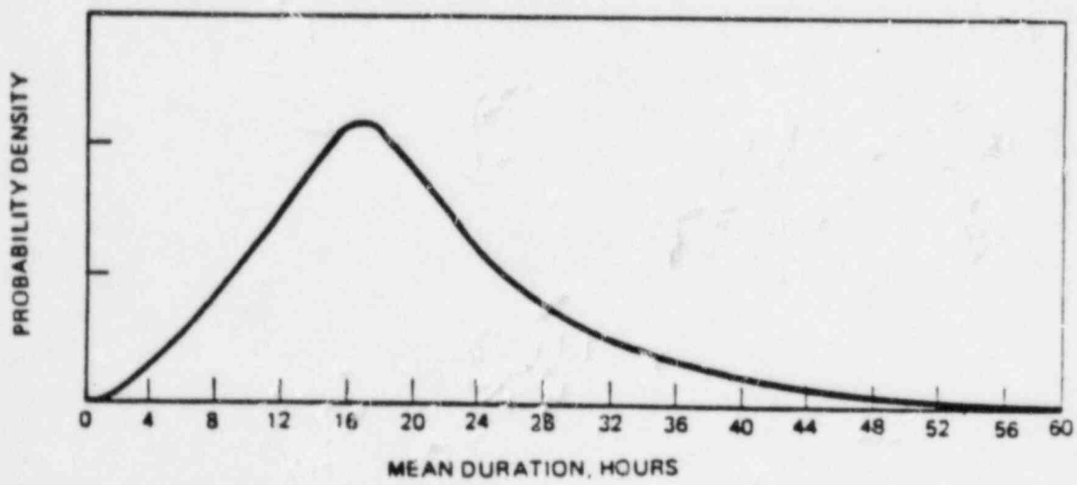


TABLE 3.10.5-3

MAINTENANCE UNAVAILABILITIES

		Q	V
1.	MDP train in maintenance EFWS	2.8 - 03	5.6×10^{-7}
2.	TDP train in maintenance EFWS	5.6 - 03	2.7×10^{-6}
3.	MDP train in maintenance Charging Pump	*2.8 - 03	3.9×10^{-7}
4.	MDP train in maintenance CCWS	2.8 - 03	6.6×10^{-7}
5.	MDP train in maintenance CS	1.4 - 03	2.0×10^{-7}
6.	MDP train in maintenance RHR	1.3 - 03	1.9×10^{-7}
7.	MDP train in maintenance ISS	1.2 - 03	1.6×10^{-7}
8.	MDP train in maintenance SWS	4.9 - 03	6.0×10^{-7}
9.	Fan Cooler Unit in maintenance Fan Cooler System	1.2 - 03	1.3×10^{-7}
10.	Diesel Generator in maintenance DNP	1.3 - 02	3.1×10^{-6}
11.	Strainer in maintenance SWS**	9.5 - 04	9.0×10^{-7}

$T = 19 hours

* Zion information only.
** Based on an assumed 8 hour per year unavailability per strainer.

3.10.6 SUPPORT STATE MODEL

3.10.6.1 GENERAL GUIDELINES

Essential 4160 volt power, service water (SW) and Integrated Protection System (IPS) are the three major support systems in APWR fault tree analysis. Loss of AC power in one essential bus usually leads to the loss of one or more trains of a system. Loss of SW leads to the unavailability of subordindate cooling trains such as component cooling water and high pressure injection. Loss of IPS is treated as the same as loss of SW or AC power.

Often, one fault tree can be used to analyze all of the support states. A component that lacks one of the necessary support states is assigned a failure probability of one and variance of zero at an appropriate basic fault. For example, the failure of a pump to run due to an unavailable bus can be indicated by substituting a failure probability of one and variance of zero at the basic fault labeled "fails to run due to random failures". When support states are available, the component random failure to run is based upon the fractional rates given in Table 3.10.7-1. The following subsection 3.10.6.2 gives some additional modeling guidelines which the analyst should use to verify that each support state in correctly modeled.

3.10.6.2 USE OF PROBABILITY ONE AND VARIANCE ZERO IN SUPPORT STATE MODELING

For systems made up of redundant trains, a probability of one and variance zero input will usually lead to the failure of the train. For most trees the effect of the one, zero input can be determined from inspection by applying the following rules:

1. If one or more of the inputs to an OR gate is probability one and variance zero, the output of the gate will also be probability one and variance zero.

2. If one of the inputs to an AND gate is probability one and variance zero, the output of the gate will be the same as if the one, zero input were removed from the gate.

3. If one of the inputs to an M out of N combination gate is probability one and variance zero, the output of the gate will be the same as if the one, zero input were removed from the gate and M and N were each reduced by one.

WAMCUT was tested to determine how well it conformed to the three previously mentioned rules. Rule number 1 was confirmed in several tests of OR gates. Rule number 2 was tested by comparing a fault tree with two redundant trains (one train having a one, zero input) with a similar tree having the failed train physically removed. The probability and variance determined by WAMCUT for the complete tree agreed exactly with that determined for the modified tree. For rule number 3, fault trees having two-out-of-three and three-out-of-four combination gates were tested. One of the trains in each tree was given a probability one and variance zero, and a comparison was again made with modified trees having the failed train removed. The WAMCUT-determined probability and variance of the complete two-out-of-three tree agreed exactly with that of the modified tree. However, small errors were found in the probability and variance of the three-out-of-four tree when the WAMCUT results were compared to those of the modified tree. The reason for the errors is not known but could be due to the use of unrealistically high test probabilities.

Since WAMCUT is not in complete conformance with rule number 3, modeling of support states in a system having a three-out-of-four combination gate must be checked against a modified tree. In order to be acceptable, the probability and variance of the complete support state model should differ from that of the modified model by less than 5%.

3.10.7 DATA BANK

A master data bank has been compiled to be used for the fault tree analysis. In compilation of this data bank, a comparative study of the following data sources has been carried out:

1. Westinghouse Data Bank as used in Millstone Unit 3 Probabilistic Safety Study (1982)

2. NREP Data Bank (NUREG/CR-2728)

3. NREP Data Bank (NUREG/CR-2815)

4. Atwood Common Cause Studies (NUREG/CR-2098, 2099, 2770)

5. IEEE Std. 500 Reliability Data (1984)

The data bank compiled for the WAPWR study is given by Table 3.10.7-1.

Table 3.10.7-1

Master Data Bank

[ ] (a,c)

Table 3.10.7-1

MASTER DATA BANK (Continued)

[ ] (a,c)

Table 3.10.7-1

MASTER DATA BANK (Continued)

[ ] (a,c)

Table 3.10.7-1

MASTER DATA BANK (Continued)

[ ] (a,c)

Table 3.10.7-1

MASTER DATA BANK (Continued)

[ ] (a,c)

MASTER DATA BANK (Continued)

[ ] (a,c)

3.10.8 UNCERTAINTY GUIDELINES

The treatment of uncertainty in the plant systems analysis is accomplished in several stages. First, basic statistical techniques are applied to the component data base to expand the failure rates of key components from point estimates to probability distributions of failure frequency. The method of moments is used to propagate uncertainties through the system fault trees and to obtain estimates of the mean and variance of the event distribution. This is done by running the WAMCUT computer code. A log-normal distribution is used in this procedure and in situations where the variance does not exist it is approximated by using the square of the mean.

Dominant accident sequences are then taken from the event trees where the mean and variance is calculated from each failed system. This is then applied to the method of moments and the results will be used to determine core melt frequency and risk quantification.

3.10.9 REFERENCES

1. Zion Probabilistic Safety Study, 1981.

2. Indian Point Probabilistic Safety Study, 1982.

3.11 SCREENING MODEL FOR OPERATOR ACTIONS IN EVENT TREES

In this section a set of human error probabilities are assigned to the operator actions that are in the event trees. Fire operator actions are defined in the event tree nodes:

OFB Open pressurizer PORVs to initiate "feed and bleed" core cooling

OST Termination of RCS leak following SGTR

ORT Manual Reactor Trip following ATWS

OLT ATWS Long-Term Shutdown, boration via CVCS

ORH Operator Depressurizes and Switches to RHR pumps after failure of all 4 SI pumps.

ORL Open pressurizer PORVs to depressurize RCS and terminate RCS leak following SGTR will failure of operator (OST) and failure of SG overfill protection system.

These operator Actions appear in the following initiating events:

OFB Transients, Loss of Offsite Power, SGTR, Secondary Side Break, Small LOCA, ATWS,

OST SGTR

ORT ATWS

OLT ATWS

ORH All events where SI cooling appears.

ORL SGTR

The operator action failure probabilities assigned are summarized in Table 3.11-1.

The operator actions in support state 3 assume either recovery of power or considers actions that are not dependent of support systems.

The operator action failures are estimated to be driven by cognitive errors rather than omission errors or failure of components. The probabilities used are consistent with diagnostic HEP from NUREG-1278.

TABLE 3.11-1

OPERATOR ACTION FAILURE PROBABILITIES

Operator Action	Failure Probability by Support State SS1	SS2	SS3
OFB	0.005	0.01	-
OST	0.01	0.01	0.1
ORT	0.01	0.01	0.1
OLT	0.01	0.01	-
ORH	0.01	0.01	-
ORL	0.01	0.01	-

3.12 LONG TERM COOLING

The failure of long-term cooling is calculated in this section for various cases.

3.12.1 FOR TRANSIENTS WITHOUT LOCA

If no LOCA is in progress, the EFWS cooling is modeled to take care of long-term cooling. For this purpose, EFWS failure is already quantified for a 24 hour mission time. Thus,

$$q = 0.0$$

for this case.

3.12.2 SMALL LOCA - CONTAINMENT FAN COOLERS AVAILABLE

In this case, RHR heat exchanger cooling is not needed. From Table 3.4-1, the difference between 24 hour and 3 hour mission time failures is used for failure of long-term cooling:

(a,c)

q_2 = [ ] system

q_1 = [ ] 1 division

3.12.3 SMALL LOCA - CONTAINMENT FAN COOLERS UNAVAILABLE

In this case, RHR heat exchanger cooling is needed. From Table 3.4-1, the difference between 24 hour and 3 hour mission time failures is used for failure of long-term cooling:

(a,c)

q_2 = [ ] system

q_1 = [ ] 1 division

In this case, RHR heat exchanger cooling is not needed. From Table 3.4-2, the difference between 24 hour and 1 hour mission time failures is used for failure of long-term cooling:

q_2 = [ ] system (a,c)

q_1 = [ ] 1 division

3.12.5 LARGE LOCA - CONTAINMENT FAN COOLERS UNAVAILABLE

In this case, RHR heat exchanger cooling is needed. From Table 3.4-2, the difference between 24 hours and 1 hour mission time is used for failure of long-term cooling:

q_2 = [ ] system (a,c)

q_1 = [ ] 1 division

The above calculations are summarized in Table 3.12-1.

TABLE 3.12-1

LONG-TERM COOLING FAILURE PROBABILITIES

Case	System Failure	1 Division Failure
Small LOCA CFC available	[	]
Small LOCA CFC fail		
Large LOCA CFC available		
Large LOCA CFC fail		

(a,c)