GA-A14653
UC-77

A RELIABILITY ANALYSIS OF THE RESIDUAL HEAT REMOVAL SYSTEMS FOR A 300 MW(e) GCFR

by
A. P. KELLY, JR., and T. TANIGUCHI

Prepared under
Contract EY-76-C-03-0167
Project Agreement No. 23
for the San Francisco Operations Office
Department of Energy

GENERAL ATOMIC PROJECT 3228
DATE PUBLISHED: JANUARY 1978

GENERAL ATOMIC COMPANY

ABSTRACT

This report represents a summary of work accomplished as part of a Department of Energy (DOE) funded program of safety studies for the gas-cooled fast breeder reactor (GCFR). The work reported herein involved an analysis of the reliability of the residual heat removal (RHR) systems for a 300 MW(e) GCFR demonstration plant design. Qualitative and quantitative reliability techniques were employed to critique the conceptual designs of the RHR systems and support systems under various operation assumptions, to indicate areas in which the reliability might be improved or for which closer analysis might be desirable. It is concluded that, in principle, the two independent RHR systems employed in the GCFR design are capable of meeting a design objective of failure of less than 10^{-6} per reactor year but that support systems envisioned for the current design would probably not adequately support such an objective. Other areas relating to the adequacy of RHR system diversity are also identified where closer analysis is warranted.

CONTENTS

FIGURES

FIGURES (Continued)

TABLES

1. INTRODUCTION AND SUMMARY

1.1. TASK DESCRIPTION

The measurement and prediction of reliability was first introduced in the U.S. as a useful technique in the aircraft industry and then expanded and used widely in the missile program. The application of probability techniques to the analysis of reactor plant incidents has received increasing attention in the nuclear industry, both in quantifying the risks of nuclear accidents (Refs. 1-1 through 1-3) and in the analysis and assurance of nuclear plant system and component reliabilities (Ref. 1-4).

Of particular concern in the design of nuclear power plants is the prevention of functional failures which may lead to significant core damage. Such functional failures include loss of residual heat removal (RHR) from the shutdown reactor, failure to terminate the reactor fissioning process by reactor shutdown when necessary, and failure to maintain the integrity of key plant structures.

The purpose of the study described herein was better understanding of the residual heat removal function for a 300 MW(e) gas-cooled fast reactor (GCFR) demonstration plant design developed by General Atomic Company (GA). The method of this study was to use qualitative and quantitative reliability analysis techniques to critique the conceptual designs of the GCFR core cooling systems under various operation assumptions, to indicate areas in which the reliability might be improved or for which closer analysis might be desirable.

1.2. SYSTEM DESCRIPTION

Two separate RHR systems provide the reliability required for forced-convection shutdown core cooling in the GCFR. The normal operational RHR is provided by the three main cooling loops (MLCS)

with their associated steam-driven helium circulators and steam generators. A diverse backup safety RHR capability is provided by a core auxiliary cooling system (CACS), which consists of three independent auxiliary loops with electric-motor-driven helium circulators and pressurized water heat exchangers. The reactor coolant circuit components of both systems are completely contained within a prestressed concrete reactor vessel (PCRV), as shown in Fig. 1-1.

Heat rejection for the MLCS is accomplished through the normal power conversion system components or, if necessary, by direct steam relief to the atmosphere for a limited time. For the initial shutdown heat removal phase of main loop cooling, reactor decay heat provides the heat source for generating circulator drive steam and makeup feedwater supplied by individual shutdown feedwater pumps, as shown in Fig. 1-2. This initial phase lasts for about 30 min following shutdown. Following this, long-term decay heat removal is initiated, with oil-fired auxiliary boilers providing circulator drive steam and the steam generators serving as heat dumps.

Heat rejection for the CACS is accomplished through individual pressurized water loops with heat rejection to the atmosphere by air-cooled heat exchangers, as shown in Fig. 1-3.

1.3. ANALYSIS APPROACH

The basic approach taken in this study has followed these steps:

1. A quantitative framework for assessing the adequacy of the current GCFR design was provided by selecting less than 10^{-6} per reactor year as a target for the probability of failure of the RHR function to prevent loss of coolable core geometry. A suballocation of 10^{-2}/yr of this target was then made to the MLCS, leaving the remainder, 10^{-4} per demand, to the CACS.

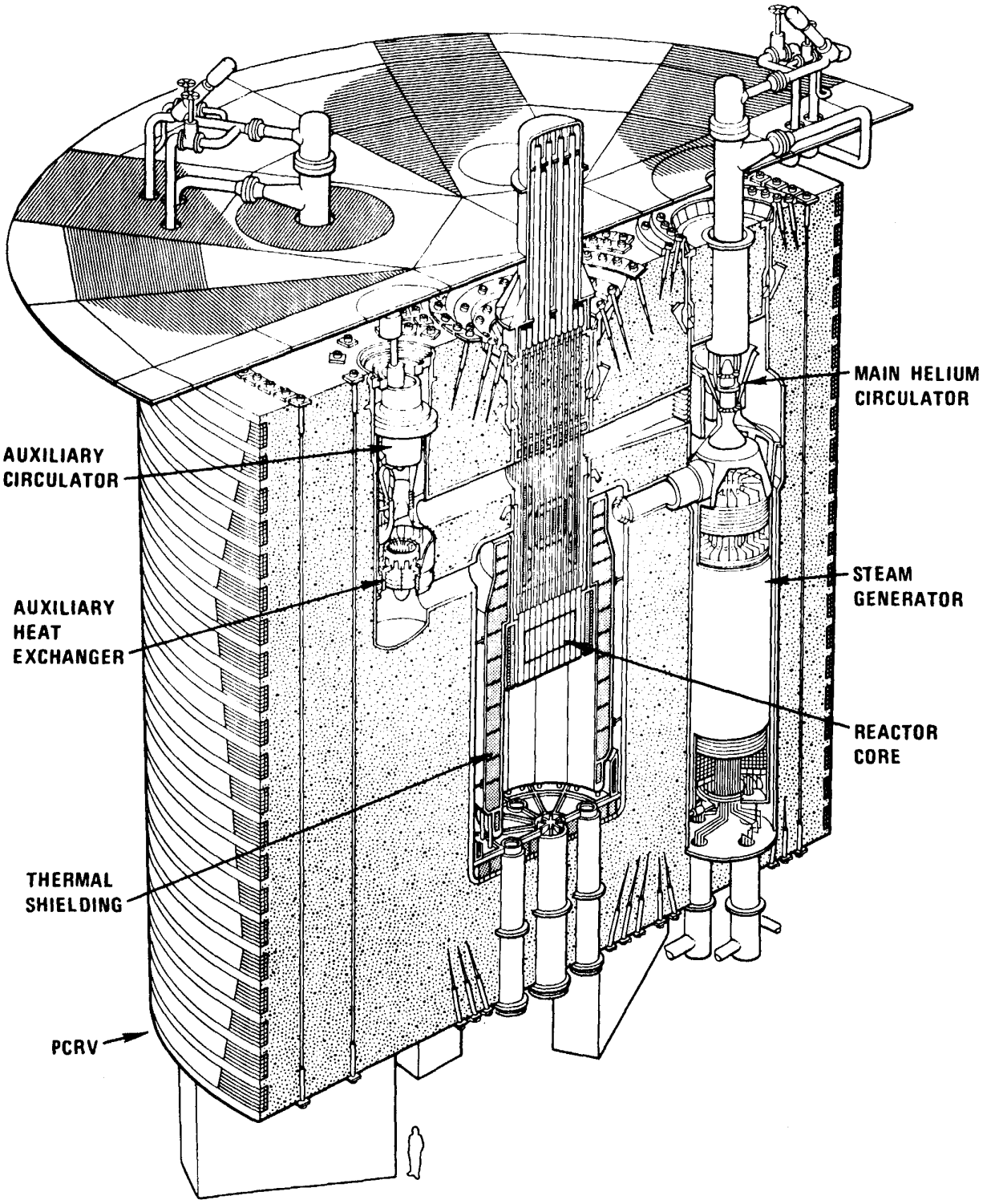


Fig. 1-1. RHR system equipment arrangement in the PCRV

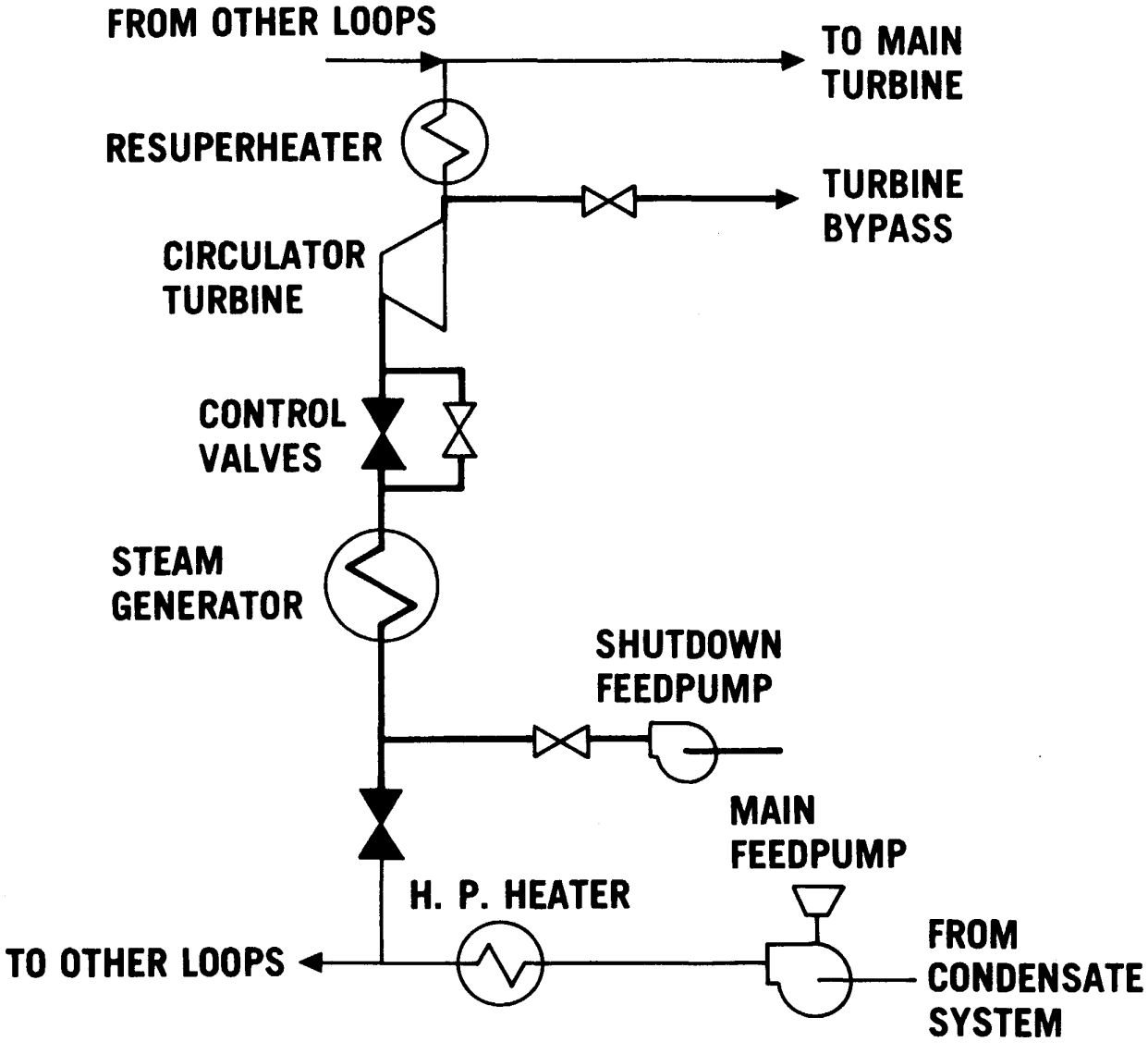


Fig. 1-2. Shutdown operation of main loop cooling system

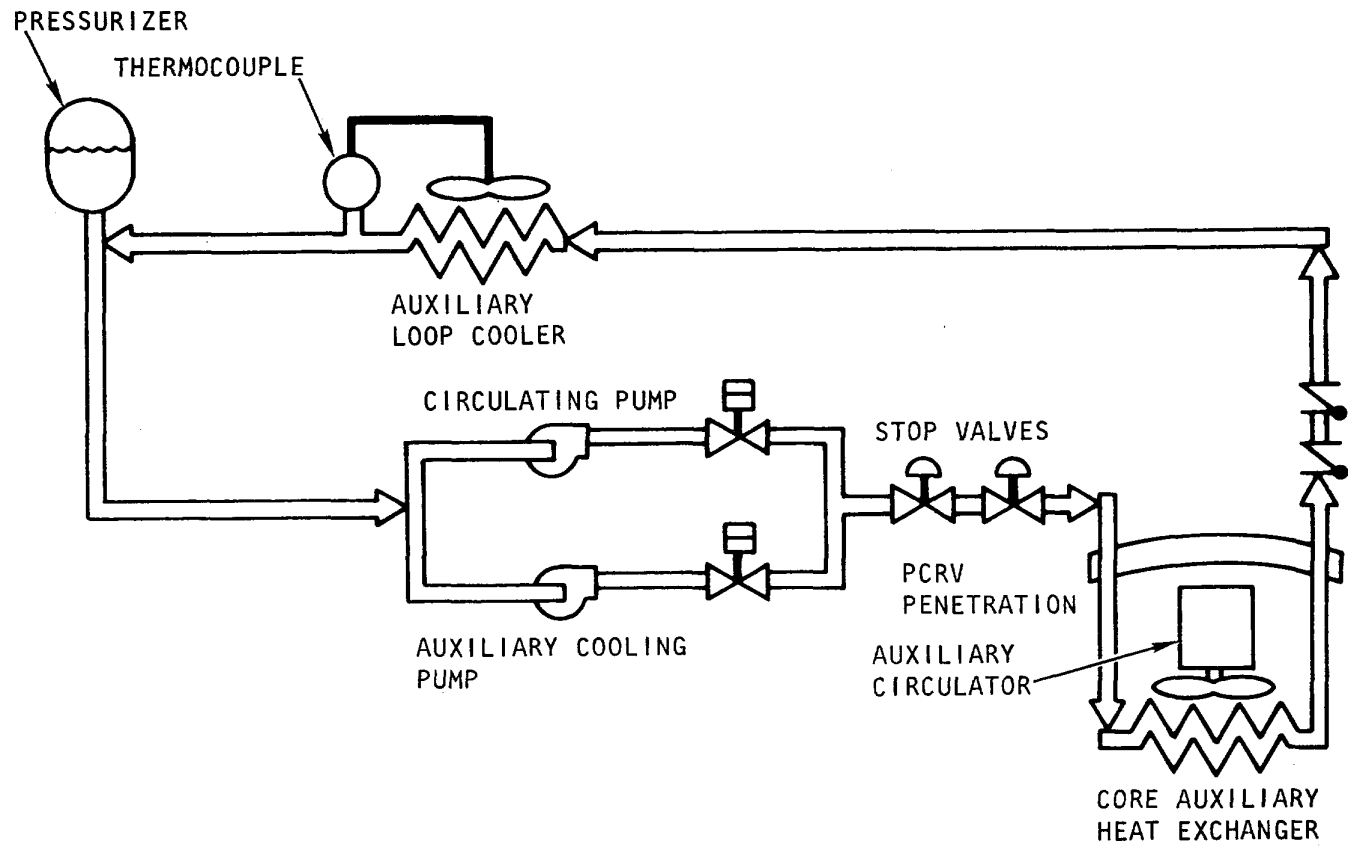


Fig. 1-3. Core auxiliary cooling system operation

The high reliability target adopted here is not anticipated to be readily achievable; nor is it possible to demonstrate such a high reliability goal. Rather, this target is selected as a point against which design improvements may be considered. Notably, probabilistic-risk studies (Refs. 1-1 and 1-3) of other reactor types have calculated RHR function unavailabilities of 6×10^{-5}, 3×10^{-5}, and 2×10^{-5}/yr for PWR, BWR, and LMFBR designs respectively.

2. The two RHR systems and support system designs were analyzed for single failure points and significant inter-system dependencies. Failure modes and effects analyses (FMEA) were completed to accomplish the former objective, and detailed reliability block diagram models were developed to accomplish the latter.

3. The RHR system models were quantified using the generic data base described in Appendix A. Because of the significant uncertainties involved in the application of the generic failure rate data to specific GCFR components, the use of sophisticated computational methods was considered unwarranted. Approximate solutions were therefore obtained and considered adequate for the purposes of this study.

4. The two RHR systems were then reviewed with respect to diversity in component type, specification, location, and potential system degradations from initiating failures to ensure that assumptions of system independence were reasonable.

5. Analysis results were then compared with the allocated results. Potential design improvements were considered and recommended where necessary.

Sections 2 and 3 to this report summarize the analysis of the MLCS and CACS respectively. Section 4 describes the analysis of the RHR support systems. Section 5 summarizes the review of the RHR system diversity.

1.4. ANALYSIS CONSTRAINTS

Several important analysis constraints are noted below:

1. The results of this analysis apply only to the current conceptual design of the GCFR demonstration plant as given in Refs. 1-5 and 1-6. The designs analyzed in many cases were developed for preliminary cost estimation purposes and therefore detailed engineering considerations are not always included. The design examined will undergo change in future years, and such changes can be expected to alter the results reported herein.

2. System failure criteria used in this analysis have been based upon conservative system transient analyses performed for licensing documents. It was beyond the scope of this study to repeat such analyses with more realistic assumptions; thus the results of this study may include significant conservatisms.

3. The results of this analysis apply only to fluid and electrical systems involved in the RHR function. Control systems and protective systems involved in the RHR process were not analyzed, as detailed designs are not yet available.

4. The reported values from this analysis were quantified by extrapolation of existing relevant component experience to predict GCFR system reliabilities. For a majority of the components considered, this extrapolation is made with high confidence because of the similarity of the equipment. For some components (principally those in the NSSS), this extrapolation is made with less confidence, as the hardware is unique. Efforts are being directed under other DOE-funded GCFR safety tasks toward providing additional confidence in the appropriateness or conservatism of the values employed.

1.5. RHR RELIABILITY ALLOCATIONS

To assess the adequacy of the GCFR RHR system designs analyzed in this study, a quantitative framework made by selecting target reliabilities is useful. For this purpose a target of less than 10^{-6} per reactor year was selected for failure of the RHR function to prevent loss of coolable core geometry. This target is generally consistent (but considered conservative) with Nuclear Regulatory Commission guidance that the likelihood of exceeding 10 CFR 100 dose guidelines at the plant site boundaries be less than 10^{-6} per reactor year.

Since the RHR function in the GCFR can be accomplished by either of two independent and diverse systems, suballocations to measure the adequacy of the individual systems are useful. Such a suballocation also serves to recognize that there are practical limits to what reliability can be achieved by the redundant but identical hardware within each cooling system due to common cause failures.

To measure the propensity for such common cause failures within redundant systems with identical components, an approach suggested by Fleming (Ref. 1-7) can be employed. Fleming suggests that a fraction of the failure rate of a given component may be common cause in nature and calls this fraction beta (β). Reviews (Ref. 1-2) of U.S. nuclear plant experience further suggest that the common cause fraction β may be in the range of 1% to 10% for active redundant equipment. Detailed review of this experience indicates that the lower end of the range (1%) is more typical of operating systems, whereas the upper end (10%) is more typical of standby systems.

Considering that the range of failure rates (see Appendix A) for the individual MLCS components that share a dual purpose in providing core cooling while the reactor is at power as well as shut down is of the order of 10^{-4} to 10^{-5}/hr, the MLCS failure rate may be practically limited to 10^{-6}/h or 10^{-2}/yr by common cause failures. Also considering that the range of demand failure rates for the individual CACS components is of the

order of 10^{-3} to 10^{-4} per demand, the CACS unavailability may be practically limited to of the order of 10^{-4} per demand by common cause failures.

Thus a suballocation of the overall RHR failure target of 10^{-6}/yr can reasonably be made to the MLCS and CACS of 10^{-2}/yr and 10^{-4} per demand respectively, taking into consideration the potential for common cause failures within redundant systems with nondiverse hardware.

To assess the unreliability of the RHR systems two distinct modes of cooling following plant shutdown should be considered:

1. Decay Heat Removal

   Long term decay heat removal is required following all scheduled and forced plant outages. For the design considered, decay heat levels are very quickly reached (approximately 20 min after shutdown) at which one of three main or auxiliary loops can provide adequate heat removal.

2. Shutdown Heat Removal

   This demand failure type is of concern following those unscheduled plant outages which result in a prompt demand for shutdown heat removal. For the design considered, initial shutdown heat levels following reactor trip from 100% power are such that two of three main or auxiliary loops are required for adequate heat removal within 20 min of shutdown. Plant outages caused by a main or auxiliary loop fault do not make shutdown heat removal demands because such faults result in a plant load reduction and subsequent orderly shutdown from a reduced power level. (Reactor trip is avoided by an operational protective system.)

For assessment of the capability of the RHR systems to meet the goals outlined above, an average annual plant availability of 80% has been assumed, including a total of three reactor trip demands per year. The

resulting plant outage time of 1752 hr/yr is further divided into outages caused by a main loop fault (20%), outages caused by an auxiliary loop fault (5%), and outages not directly caused by a cooling loop fault (75%). Outages caused by multiple loop faults are negligible contributors to the RHR system failure probability if the time during which the plant can operate with a faulted loop is limited (i.e., $\leq$24 hr).

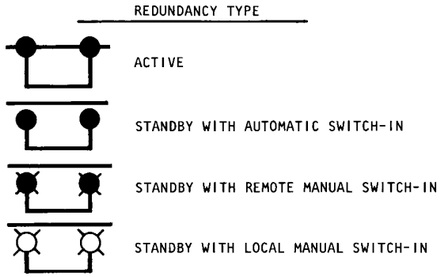
1.6. RHR SYSTEM ANALYSIS

Figure 1-4 shows the reduced and simplified reliability block diagram of the GCFR RHR systems which has been derived from the qualitative analysis process described previously. As the figure shows, both RHR systems evidence considerably redundancy in their equipment features. Analysis has shown that this redundancy varies depending upon the core power level and coolant pressure existing at the time of residual heat removal demand. Following pressurized shutdowns, one main or auxiliary primary (helium) loop can provide adequate coolant circulation. Two main or auxiliary primary loops are required following the design basis depressurization accident (DBDA) to provide adequate coolant circulation. One main or auxiliary secondary (steam/water) loop can provide adequate heat removal from the coolant following plant shutdowns at reduced power levels (i.e., following a controlled plant shutdown or one at the reduced decay heat levels existing at times in excess of 1/2 hr following reactor trip). Two main or auxiliary secondary loops are required following reactor trip from nominal power to provide adequate heat removal.

Based on the above, three decreasing states of redundancy may be evidenced in the RHR systems:

1. Following a normal controlled plant shutdown, six independent loops (three main and three auxiliary) must fail to cause RHR failure.

2. Following plant shutdown with the outage of one main or auxiliary loop, five independent loops must fail to cause RHR failure.



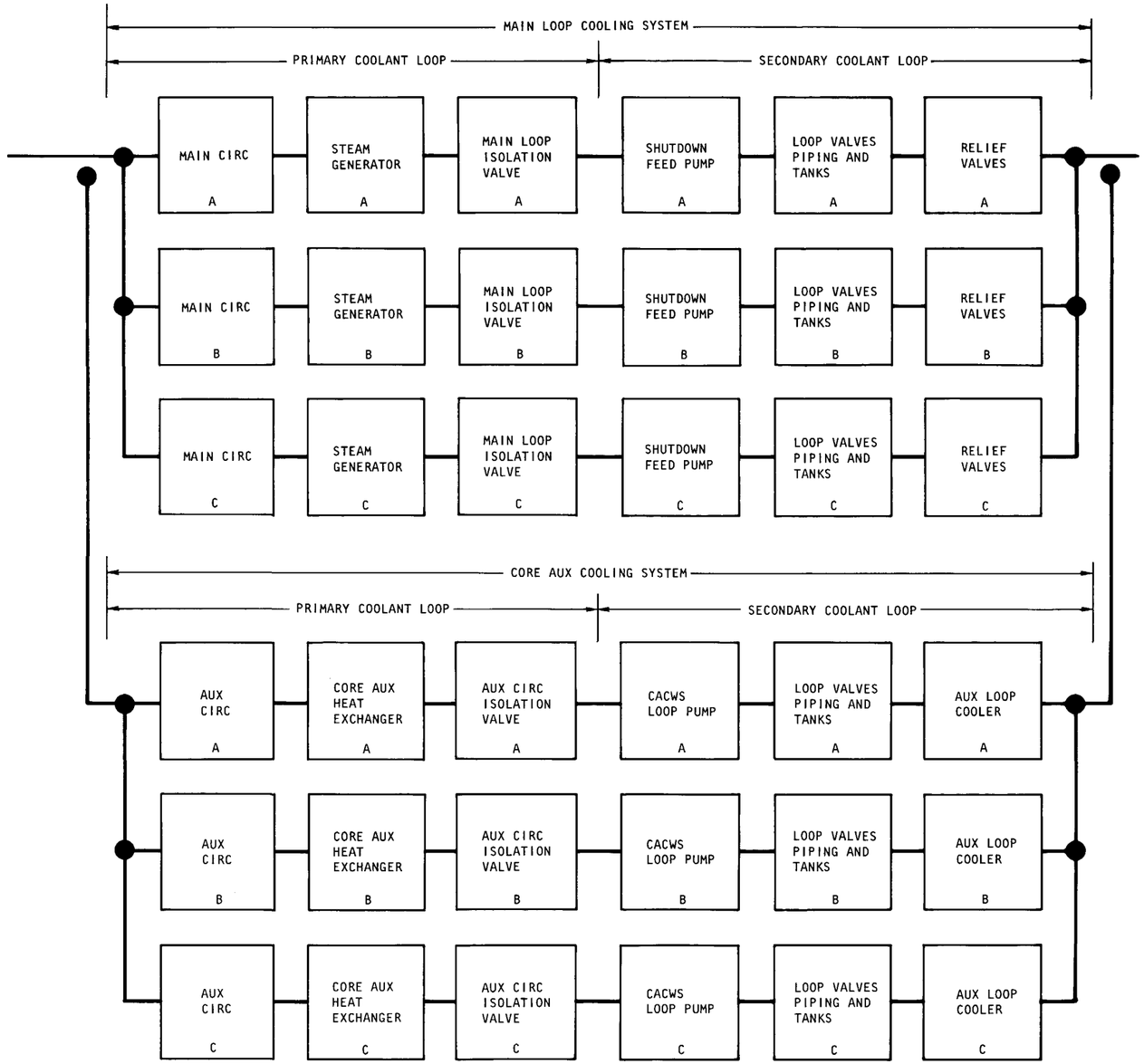


Fig. 1-4. Simplified reliability block diagram of RHR systems

Since the outage of a main or auxiliary loop results in plant load reduction, a subsequent plant shutdown would occur from a reduced power level.

3. Following a reactor trip from 100% power, four independent loops must fail to cause RHR failure. For pressurized shutdowns, the RHR system redundancy is limited by the heat rejection capability. For depressurized shutdowns, the redundancy is equally limited by the heat rejection and coolant circulation capability.

The minimal redundancy evidenced in the RHR systems thus is four; that is, a minimum of four independent failures must occur to cause RHR failure.

The results of quantifying the reliability models and the comparison of these results with the system allocations are shown in Table 1-1. The unreliability of the MLCS has been assessed at 2.1×10^{-2}/yr, only slightly higher than the allocation. The unreliability of the CACS has been assessed at 2.0×10^{-5} per demand, below the allocation of 10^{-4} per demand. The total RHR failure assessment is 4.3×10^{-7}/yr. The principal contribution to the unreliability of the MLCS has been shown to be failures while running rather than upon startup. This is consistent with the fact that relatively few components need to change state to provide a continuity of main loop cooling following plant shutdown as compared to the number of MLCS components which must continue to operate to provide long-term residual heat removal. The dominant contribution to the assessed value for RHR failure has been shown to be failures following plant outages occurring from nominal power with reactor trip. This is consistent with the fact that the RHR systems evidence their minimum redundancy following such events.

1.7. SUPPORT SYSTEM ANALYSIS

Figure 1-5 shows the reduced and simplified reliability block diagram of the systems which support the RHR. Four major systems support the MLCS.

TABLE 1-1
RHR SYSTEM UNRELIABILITY ASSESSMENTS

Cooling Mode	MLCS (yr^{-1})	CACS ($demand^{-1}$)	Total (yr^{-1})
Decay Heat Removal	1.9×10^{-2} (a)	1.4×10^{-6}	2.6×10^{-8}
Shutdown Heat Removal	2.0×10^{-3} (b)	2.0×10^{-4}	4.0×10^{-7}
Total	2.1×10^{-2}	2.0×10^{-5} (c)	4.3×10^{-7}
Allocation	10^{-2}	10^{-4}	10^{-6}

(a) Based on a plant availability of 80%.

(b) Based on a total of three reactor trip events per year.

(c) Represents the frequency-weighted average unavailability of the CACS.

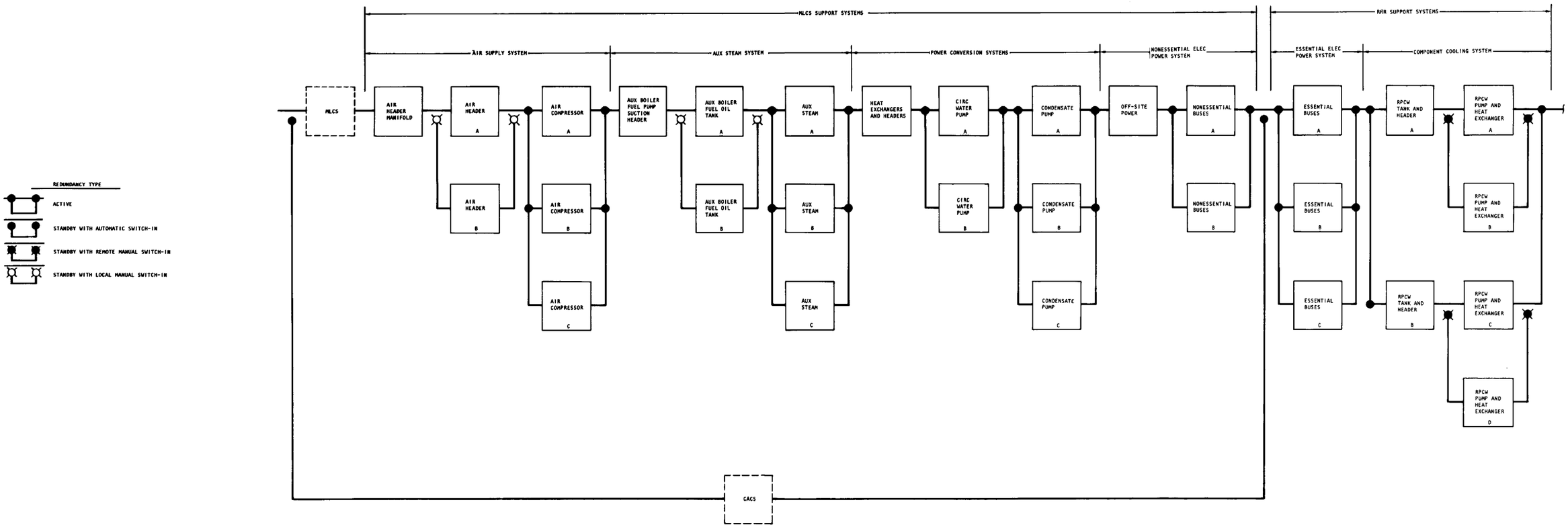


Fig. 1-5. Simplified reliability block diagram of RHR support systems

These are the air supply system, which provides valve control air, the auxiliary steam system, which provides circulator drive steam for long-term RHR, the power conversion system, which provides the ultimate heat sink, and the nonessential electric system, which provides power to power conversion and auxiliary steam system components. Two major systems may also be noted that support both RHR systems. These are the essential electric power system and the component cooling water system, which provide electrical power and cooling water to essential components in both the MLCS and CACS.

The redundancy evidenced in MLCS support systems is considerably less than that evidenced in the MLCS itself. Single failure points are in all four systems in passive features. The redundancy evidenced in systems commonly supporting both RHR systems is also less than that evidenced in the RHR systems themselves. Double failure points are in one of the systems in passive features, and triple failure points are evidenced in active features. However, these common support systems do not show diversity in these failure points, as do the RHR systems.

The summarized results of quantifying the reliability models for the RHR support systems and the comparison of these results with the RHR system allocations are shown below.

	System Supported	
	Main Loop Cooling System	Total System (MLCS and CACS)
Allocation	10^{-2}	10^{-6}
Prediction	10^{-1}	10^{-3}

The total failure probability of systems supporting the MLCS has been assessed as 10^{-1}/yr, in excess of the allocation. The total failure probability of systems supporting both RHR systems has been assessed as 10^{-3} per year, well in excess of the allocation. These quantitative conclusions are consistent with the lesser redundancy evidenced in the support systems as compared to that found in the RHR systems.

1.8. ANALYSIS CONCLUSIONS

The analysis results described above lead to the following two major conclusions with regard to the reliability of residual heat removal in the conceptual GCFR design studied:

1. With the possible exception of the concerns identified below, the two independent systems employed in the GCFR design are capable of meeting a design objective of failure of less than 10^{-6} per reactor year. The suballocation of 10^{-2}/yr to the MLCS also appears feasible.

2. The RHR support systems provided in the current design would not appear to adequately support the redundance or diversity provided by the RHR systems. It does not appear that a design objective of RHR failure of less than 10^{-6} per reactor year or MLCS failure of less than 10^{-2}/yr could be achieved with the support systems currently envisioned.

The second conclusion has been reached despite the fact that the support systems studied meet the conventional safety requirements (i.e., single failure criterion, seismic category, etc.). This clearly demonstrates the advantage of a reliability-based approach in integrating all interfacing system and component failures into the consideration of design adequacy. This also points out the need for strengthening design criteria with respect to safety-related support systems, to ensure that they adequately support the primary system goals.

1.9. DESIGN DIVERSITY

In addition to considerations of dependencies on support systems, other potential system dependencies were also considered which might limit the reliability of residual heat removal in the GCFR. These included considerations of potential common cause failures (multiple failures traceable to a single event in the design, engineering, or operation of the plant), casual or propagating failures (multiple failures which occur as the result

of propagation of a single failure event), and external initiators of failure (such as earthquakes, tornadoes, aircraft impact, etc.). Because of the subtleties of such common mode failure events and their potential for development in the advanced stages of a design, it was not possible to conduct a complete review of potential areas of susceptibility to common mode failures in a conceptual design which is inherently limited in detail. The RHR system designs were considered, however, with respect to each of the common mode failure categories to identify the less obvious areas of potential unwanted design dependencies.

The major area of concern identified as a result of this review is that of the dependence of the CACS on an initial period of MLCS flow coastdown. Reliance is placed on some continuation of main circulator drive power following reactor trip for this coastdown. Because of the potential complexity of control and protection functions which must operate correctly to prevent loss of drive power, it may be difficult to ensure that a common loss of circulator drive power has a probability of less than the target of 10^{-6}/yr for the conceptual design analyzed.

1.10. DESIGN RELIABILITY IMPROVEMENTS

Based on the analysis results and conclusions described previously, the following general design reliability improvements are recommended for consideration in decreasing order of priority. Analysis indicates that these improvements would increase the assessed reliability of residual heat removal to a level consistent with the 10^{-6} per reactor year objective.

1. Common Cooling Water System

   It is recommended that the dependence of the MLCS and CACS on a common (albeit redundant) component cooling water system be eliminated. A possible approach would be to provide independent component cooling systems with air-cooled heat exchangers for each CACS loop. This approach was taken on the Delmarva HTGR design.

2. Common Electrical Supplies

It is recommended that the dependency of the MLCS and CACS on a common (albeit redundant) ac and dc electrical power supply be reduced. Because the mean repair time estimate for the electrical power system is relatively short, it appears that a fix which extends the capability (i.e., several hours) of the design to operate without a common electrical supply would sufficiently decrease the estimated unreliability. Two possible design approaches would appear to accomplish this:

a. Extend the capability of the MLCS to operate with nuclear decay heat as a prime energy source. Current LWR designs have this capability for a period of many hours following shutdown.

b. Provide batteries for short term CACS operation. Pressurized helium pumping power requirements appear to be modest enough to make this approach feasible. A similar approach has been taken in the design of the CRBR, to provide pony motor power, as well as in the design of British GCRs.

It is recommended that both approaches be pursued to determine the most advantageous solution.

3. RHR System Diversity

It is recommended that the CACS design have a pressurized startup capability based upon the thermal inertia of the reactor core or on the mechanical inertia of the main circulators only, or, alternatively, that steps be taken to reduce the complexity of control and protection functions which must operate correctly to prevent simultaneous loss of drive power to the main circulators. For the conceptual design analyzed, it would be difficult to ensure that a common mode loss of drive power to the circulators will have a

frequency of less than 10^{-6} per reactor year. The analysis presented in Section 5 indicates that this aspect of the design is dominant with respect to ensuring sufficient RHR system diversity.

4. MLCS Support System Redundancy

It is recommended that the redundancy of systems supporting the MLCS be improved (i.e., that single failure points be eliminated), or alternatively, that the dependence of the MLCS on these systems be decreased. The following possible approaches might be employed:

a. Eliminate the common air header manifold in the design of the control air system or provide a local independent control air supply to key MLCS valves.

b. Eliminate the common auxiliary boiler fuel pump suction header and fuel return header or provide a means for extended MLCS operation in the decay heat removal mode without an auxiliary steam supply.

c. Consider the incorporation of independent maintenance condensers for long term main loop heat rejection to eliminate the common dependence on the power conversion system.

5. MLCS Redundancy

It is recommended that a capability for cross-connecting the shutdown feedwater trains be provided to effectively increase the redundancy of the MLCS. In the current design the outage of a main loop voids the use of the associated shutdown feedwater train and vice versa. Since the assessment of the MLCS identifies the failure rate of the shutdown feedwater train as a significant contributor to the total loop failure rate, this design change would cause the MLCS unreliability assessment to fall within the allotted 10^{-2}/yr.

1.11. FUTURE WORK

It is recommended that the goal of future work be to minimize the four analysis constraints which have been mentioned previously in this section.

The first three of these constraints deal with analysis limitations caused by the conceptual nature of the design and lack of detail for some systems. It is therefore recommended that reliability analyses be continued to update the results presented in this report as new design information is available. This report provides a basis and framework for such an updating process. Such work is planned, to be carried on under the DOE-funded GCFR safety tasks.

The fourth constraint deals with analysis limitations caused by the uniqueness of some of the equipment. The quantification of the reliability models described in this report has been performed by the assignment of generic failure data to GCFR components and systems. For the major portions of the plant design employing conventional nuclear plant systems or components, these assignments can be made with reasonable confidence. For those portions of the design employing new systems or components, these assignments must be made with relatively greater uncertainty. It is therefore useful to identify, develop, and apply engineering and analytical methods to help reduce the uncertainty that these new design items meet the desired reliability assignments. Efforts are being directed under a DOE-funded GCFR safety task during FY-77 and FY-78 to identify such methods.

REFERENCES

1-1. "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," USNRC WASH-1400, October 1975.

1-2. "HTGR Accident Initiation and Progression Analysis Status Report," ERDA Report GA-A13617, General Atomic Company, 1975-1977.

1-3. "CRBRP Risk Assessment Report," CRBRP-1, March 1977.

1-4. "Reliability Manual for Liquid Metal Fast Breeder Reactors," General Electric Report SRD-75-064, December 1975.

1-5. "Gas-Cooled Fast Breeder Reactors - Preliminary Safety Information Document," Gulf General Atomic Report GA-10298, February 1971.

1-6. "300 MW(e) Gas-Cooled Fast Breeder Reactor - Balance of Plant," Job 10437, Bechtel Corp. August 1973.

1-7. Fleming, K. N., "A Reliability Model for Common Mode Failures in Redundant Safety Systems," Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation, April 1975 (General Atomic Report GA-A13284).

2. MAIN LOOP COOLING SYSTEM

2.1. DESCRIPTION

The main loop cooling system (MLCS) is designed to automatically provide adequate core cooling from plant shutdown to long term decay heat removal. The initial transition from normal plant operation to residual heat removal is called the shutdown heat removal mode, and cooling subsequent to this is called the decay heat removal mode. The three independent loops of the MLCS are safety class, Seismic Category I.

The shutdown heat removal mode is first accomplished with the main loops, using the steam generator inventories and the residual heat in the reactor core to create steam for sustaining main circulator operation, and subsequently by supplying feedwater to the main loop steam generators. Heat rejection is accomplished through the normal power conversion system components, or, if necessary, for a limited time by direct steam relief to the atmosphere.

The long term decay heat removal mode is accomplished by sustaining the main circulator operation with oil-fired auxiliary boilers that provide auxiliary steam. Heat from the primary coolant is transferred to the steam generators, with subsequent heat rejection through the normal power conversion system components, or, if necessary, for a limited time by direct steam relief to the atmosphere.

2.2. QUALITATIVE ANALYSIS

A reliability functional block diagram (RFBD) was drawn for the MLCS. The RFBD includes the major equipment items, the active mechanical components, and single passive failure mechanical components. Control and

protective systems were not included as designs are not yet available. The major support system requirements are indicated by dashed blocks primarily to identify interrelationships. The support systems are discussed in Section 4. The RFBD is shown in Fig. 2-1, sheets 1 through 5.

A failure modes and effects analysis (FMEA) was performed on the major equipment items and the active mechanical components. Each component was analyzed for its failure mode(s) and the effect on the system for RHR operation. This FMEA is presented in Table 2-1.

2.2.1. Shutdown Heat Removal Mode

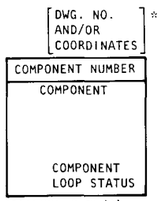
For the shutdown heat removal mode, the MLCS items which are required to function are shown in the RFBD (Fig. 2-1, sheets 1 through 5). As indicated in this model, the three main loops are redundant and independent of each other. No single active or passive failures were uncovered for the MLCS mechanical components in the shutdown heat removal mode.

Immediately after plant shutdown, the primary loop (helium) components, (i.e., the steam generators and the circulators) are only required to sustain operation. The circulator service systems continue to operate with adequate bearing water supply in their surge tanks.

Very shortly after plant shutdown or trip, the secondary (steam/water) loop components, namely valves, are the only active mechanical components required to change state. For each main loop, the following valves are designed to operate:

1. The feedwater flow control valve or the containment isolation stop-check valve closes (Fig. 2-1, sheet 3).

2. The main circulator large turbine control valve is closed in 3 sec after the measured neutron flux decreases below the 50% level (Fig. 2-1, sheet 4).



COMPONENT STATUS (100% PLANT OPERATION)

NO - NORMALLY OPEN
NC - NORMALLY CLOSED
NE - NORMALLY ENERGIZED
ND - NORMALLY DE-ENERGIZED
NM - NORMALLY MODULATING

*REFERENCES

"300 MW (E) GAS COOLED FAST BREEDER REACTOR - BALANCE OF PLANT-PRELIMINARY ENGINEERING AND COST ESTIMATE," JOB 10437, BECHTEL, AUGUST 1973

"750 MW (E) GAS COOLED FAST BREEDER REACTOR - BALANCE OF PLANT-PRELIMINARY ENGINEERING AND COST ESTIMATE," JOB 10437-004, BECHTEL, OCTOBER 1974

FUNCTIONAL COMPONENT OF SYSTEM

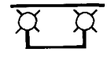
SUPPORT COMPONENT CONSIDERED SEPARATELY OR FOR INFORMATION.

REDUNDANCY TYPE

ACTIVE

STANDBY WITH AUTOMATIC SWITCH-IN

STANDBY WITH REMOTE MANUAL SWITCH-IN



STANDBY WITH LOCAL MANUAL SWITCH-IN

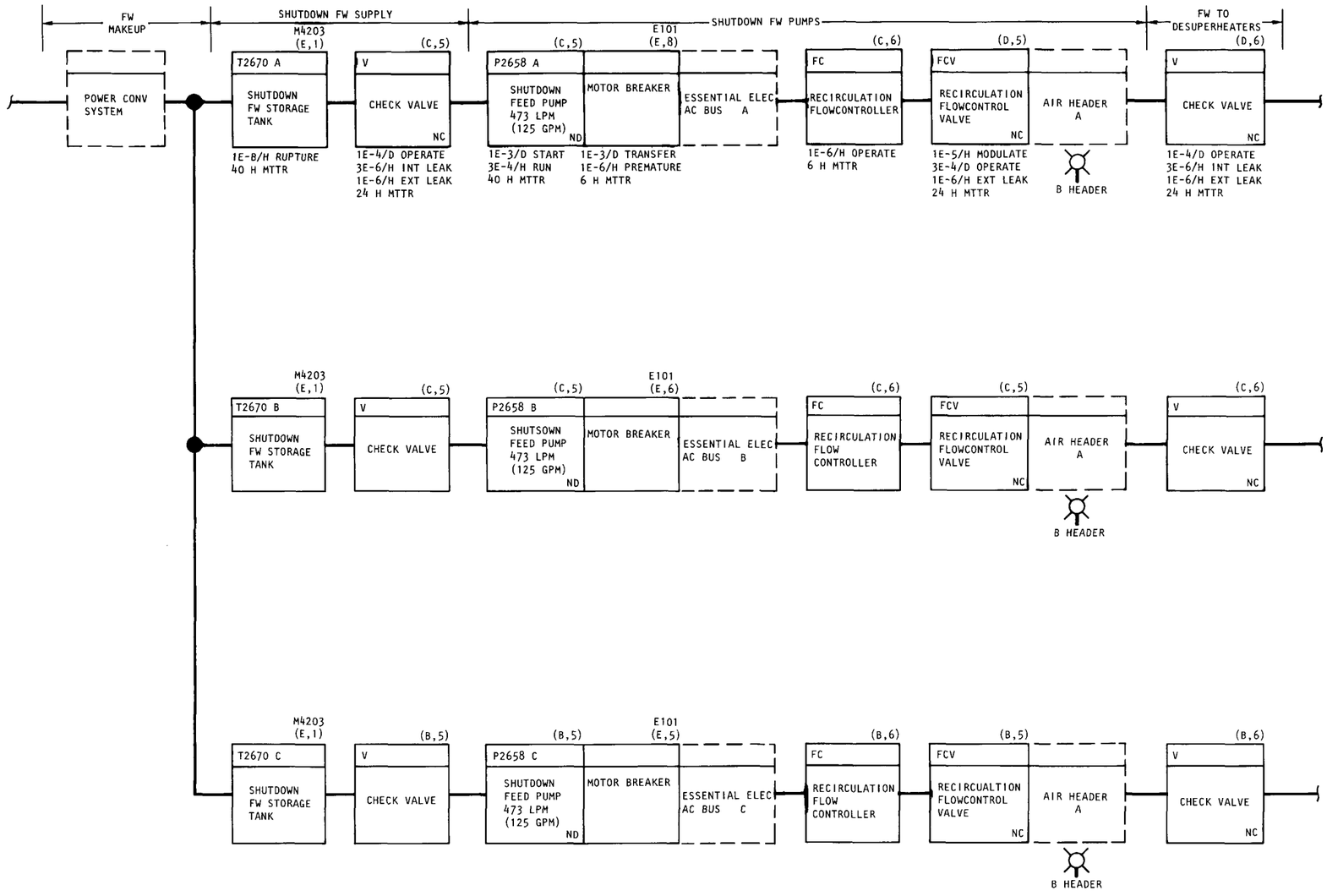


Fig. 2-1. GCFR main loop cooling system (MLCS) reliability function diagram, sheet 1 of 5

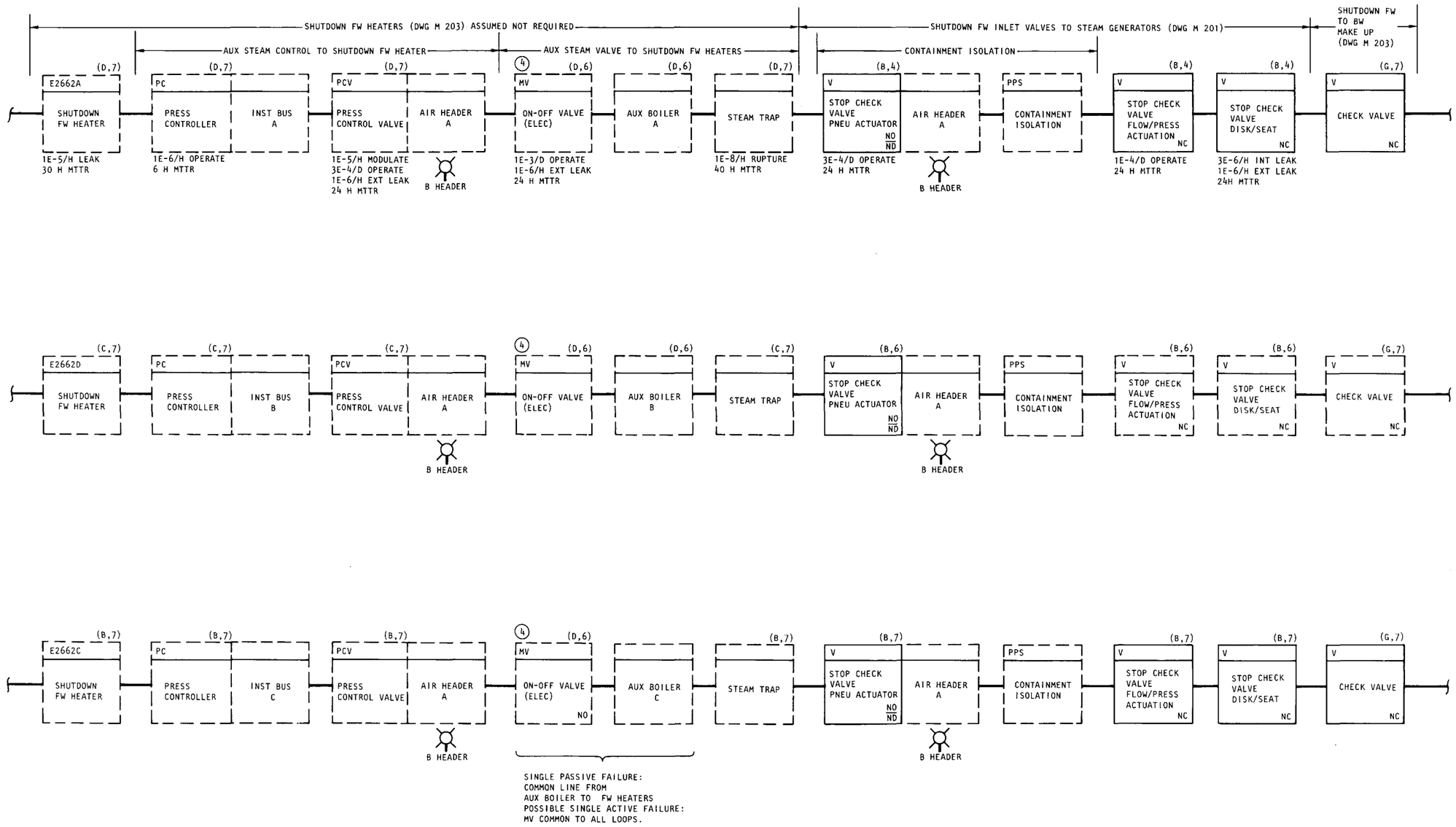


Fig. 2-1. GCFR main loop cooling system (MLCS) reliability function diagram, sheet 2 of 5

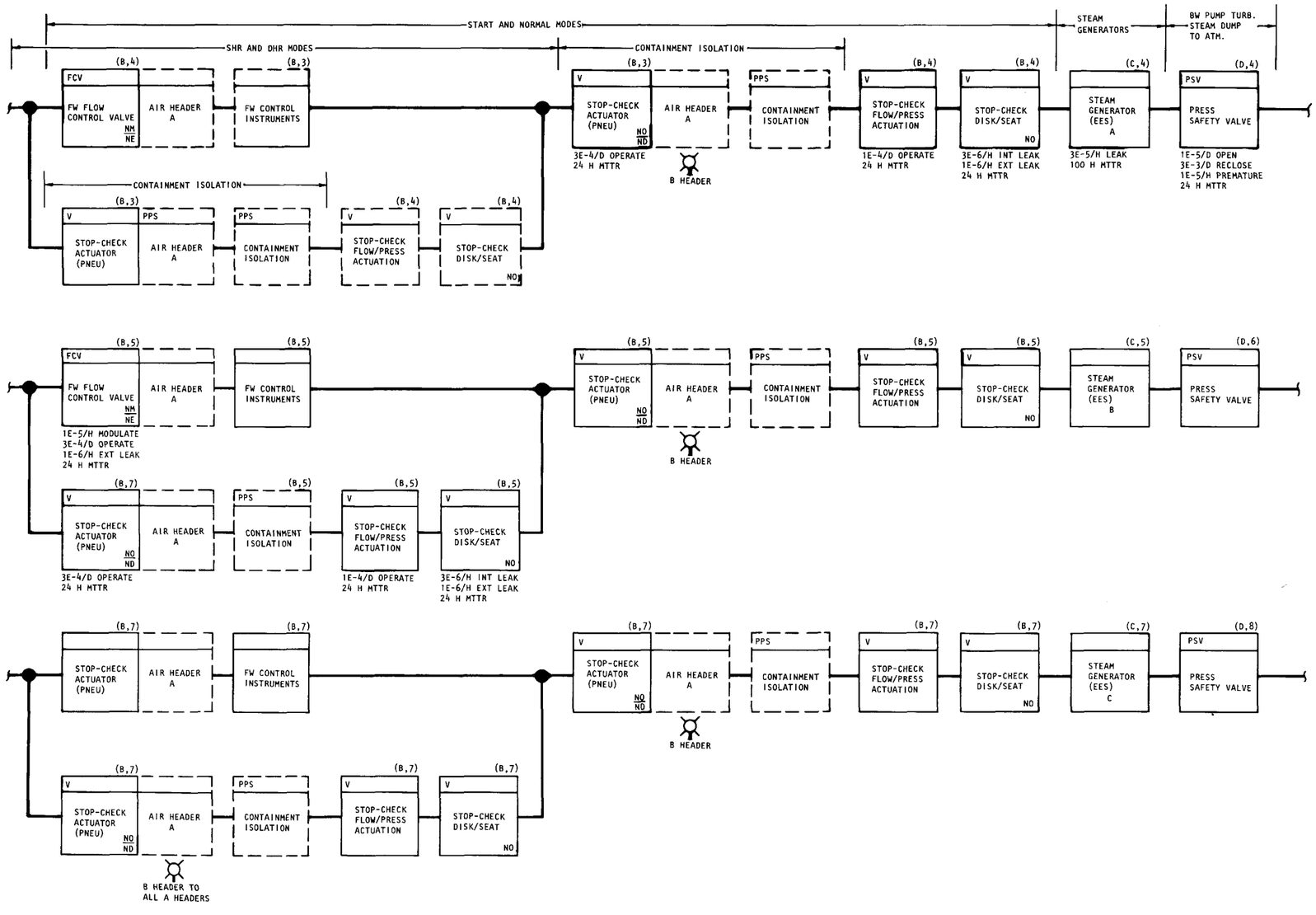


Fig. 2-1. GCFR main loop cooling system (MLCS) reliability diagram, sheet 3 of 5

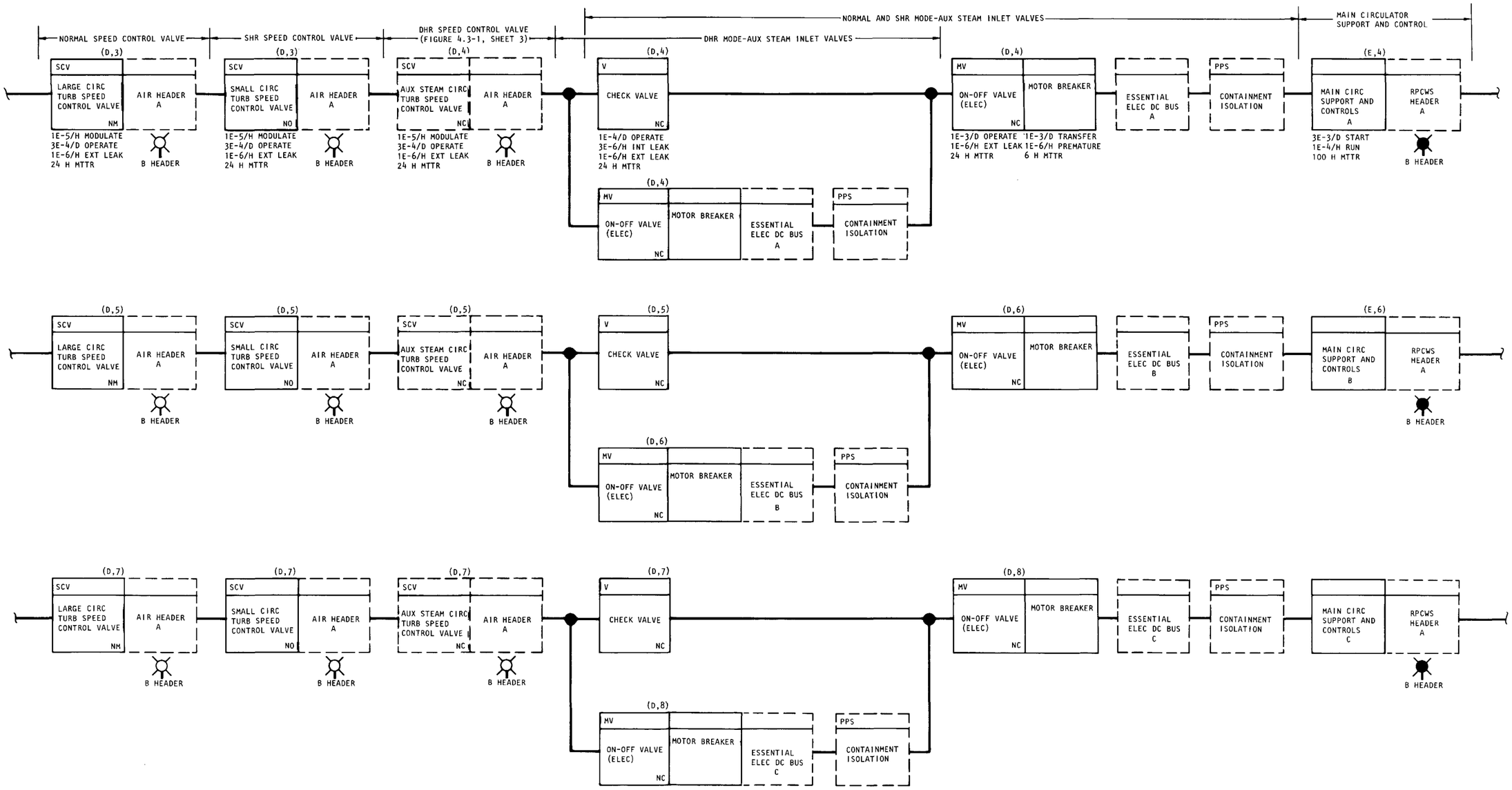
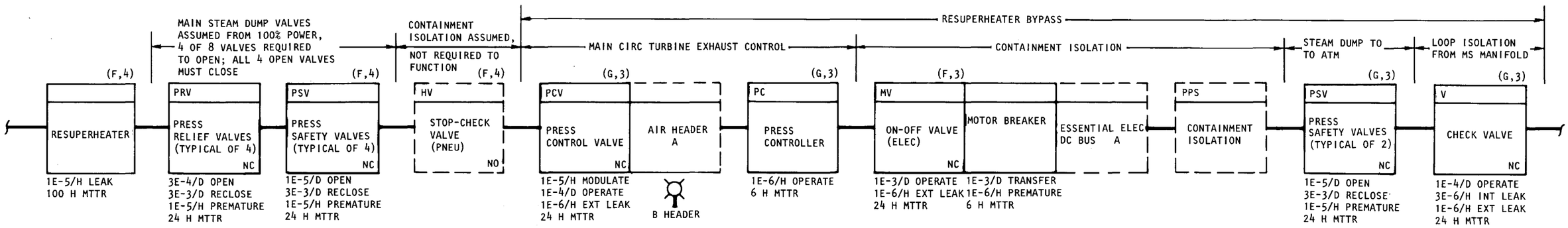
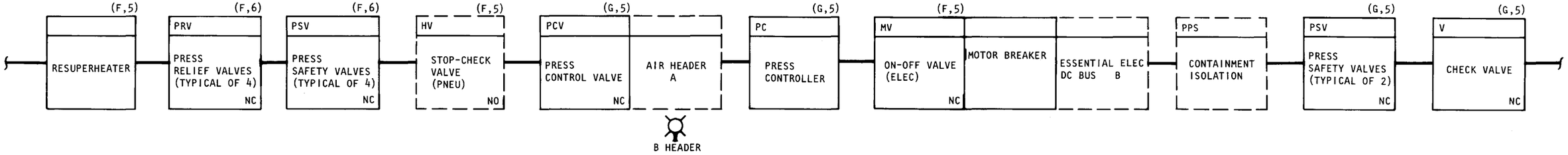


Fig. 2-1. GCFR main loop cooling system (MLCS) reliability function diagram, sheet 4 of 5





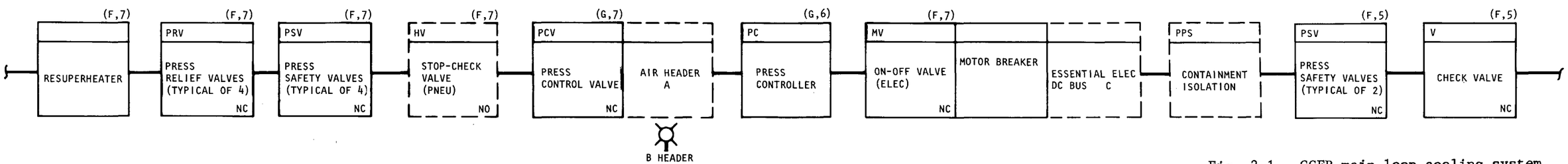


Fig. 2-1. GCFR main loop cooling system (MLCS) reliability function diagram, sheet 5 of 5

TABLE 2-1

FAILURE MODE AND EFFECT ANALYSIS OF GCFR MAIN LOOP COOLING SYSTEM (MLCS) FOR RHR INITIAL CONDITIONS: FULL POWER AND PLANT SHUTDOWN (PSD)

Component(s)	Function	Failure Mode	Single Failure Effect	Need CACS After PSD	Common Mode Failure Effect	Need CACS After PSD
1. Shutdown FW Storage Tank (T2670 A,B,C) (P&I M4203) one per loop.	2. Provide feedwater (FW) to the shutdown feed pumps.	1a. Rupture.	1a. Loss of one loop after 13 minutes. No FW to a shutdown feed pump, thus pump trip and no FW to a steam generators (SG).	No	1a. Loss of all loops. No FW to steam generators (SG)	>13m
2. Check Valves (NC) Shutdown Feed Pump Section. (P&I M4203) one per loop.	2. Not required.	2a. Fail as is (NC at start).	2a. Loss of one loop at 13 minutes. Same as 1a.	No	2a. Loss of all loops. Same as 1a.	13m
		2b. External leak.	2b. Loss of one loop after 13 minutes. Same as 1a.	No	2b. Loss of all loops. Same as 1a.	>13m
3. Shutdown Feed Pumps. (P2658 A,B,C) (P&I M4203) one per loop.	3. Provide motive power to circulate secondary fluid.	3a. Fail to start	3a. Loss of one loop at 13 minutes. No FW to a SG.	No	3a. Loss of all loops. Same as 1a.	13m
		3b. Fail to run.	3b. Loss of one loop after 13 minutes. Same as 3a.	No	3b. Loss of all loops. Same as 1a.	>13m
4. Flow Controllers (FC) (Elec) (P&I M4203) one per loop.	4. Provide proper flow to SG and control FCV to recirculate excess back to condenser hot well.	4a. Fail to operate opens FCV full.	4a. Loss of one loop at 13 minutes. Cause total flow to recycle, thus no FW to the SG.	No	4a. Loss of all loops. Same as 1a.	13m
		4b. Fail to operate-closes FCV.	4b. Loss of one loop after 15 minutes. Cause total flow (2% of full power) to a SG. After 15 minutes, less than 2% flow is required, thus this failed loop shutdown feed pump can be remote manually tripped and RHR can be maintained with the other two MLC loops.	No	4b. Loss of all loops. Each loop will be providing 2% flow. At one minute when the shutdown feed pumps are started, about 4% flow is required, thus some over cooling can exist. By remote manually tripping out one pump within a few minutes and at about 15 minutes, tripping out the other pump, RHR can be maintained by the remaining loop without going to the CACS. Likely, the SG floods out before 20 minutes when aux. steam becomes available thus, CACS will be required then.	>8m

TABLE 2-1 (Continued)

Component(s)	Function	Failure Mode	Single Failure Effect	Need CACS After PSD	Common Mode Failure Effect	Need CACS After PSD
5. Flow Control Valves (FCV) (NC) (Pneu) (P&I M4203) one per loop.	5. Receive signal from FC and by-pass the FW to the hot well and thus maintain proper FW to the SG's.	5a. Fails as is (NC at start).	5a. Loss of one loop after 15 minutes. Same as 4b.	No	5a. Loss of all loops. Same as 4b.	>8m
		5b. Fails open or external leak.	5b. Loss of one loop at 13 minutes. Same as 4a.	No	5b. Loss of all loops. Same as 1a.	13m
		5c. Fails closed.	5c. Loss of one loop after 15 minutes. Same as 4b.	No	5c. Loss of all loops. Same as 4b.	>8m
6. Check Valves (NC) (P&I M4203) one per loop.	6. Provide FW to desuperheaters.	6a. Fail as in (NC at start).	6a. None. Each loop provides FW.	No	6a. Loss of all loops. Feedwater to resuperheater by-pass required to close the secondary loop	>22H
		6b. External leak.	6b. Loss of one loop at 13 minutes. Same as 4a.	No	6b. Loss of all loops. Same as 1a.	13m
7. Stop-Check Valve Actuator (NO/ND) (Pneu) Check (NC) (P&I M201) one per loop.	7. Containment isolation valve; prevent backflow during normal operation and allow FW to SG's during SHR and DHR.	7a. Fails as in (NC at start).	7a. Loss of one loop at 13 minutes. Same as 4a.	No	7a. Loss of all loops. Same as 1a.	13m
		7b. External leak.	7b. Loss of one loop at 13 minutes. Same as 4a.	No	7b. Loss of all loops. Same as 1a.	13m
		7c. Internal leak.	7c. None. Upstream FCV (Component #9) will stop any backflow, thus FCV and this valve are redundant for this mode.	No	7c. None. Same as single failure.	No
8. Check valves (NC) (P&I M4203) one per loop.	8. Provide make up water to the bearing water system.	8a. Fails as is (NC at start).	8a. Loss of one loop after 13 minutes. Main circulator trip.	No	8a. Loss of all loops. Same single failure.	>13m
		8b. External leak.	8b. Loss of one loop after 13 minutes. Main circulator trip.	No	8b. Loss of all loops. Same single failure.	>13m
9. Flow Control Valve (FCV) (No) (Pneu) & Controller (Elec) (P&I M201) one per loop.	9. FW control to the SG's during normal operation and close during RHR mod.	9a. Fail as is (NO at start).	9a. None. With main boiler feed pumps stopped and the upstream PPS stop-check valve will close, thus the stop-check valve is redundant to this FCV.	No	9a. None. Same as single failure.	No
		9b. External leak.	9b. N/A requires double failure. First, the downstream stop-check valve (Component #7) must fail due to "internal leak" and then this valve must fail due to external leak."	No	9b. None. Same as single failure.	No
		9c. Fail to operate.	9c. N/A. Not required to modulate for RHR.	No	9c. None. Same as single failure.	No

TABLE 2-1 (Continued)

Component(s)	Function	Failure Mode	Single Failure Effect	Need CACS After PSD	Common Mode Failure Effect	Need CACS After PSD
10. Steam Generator (SG) (Economizer, Evaporator & Superheater-EES) (P&I M201) one per loop.	10. Transfer reactor residual heat from primary coolant (He) to secondary coolant (H_2O).	10a. Excessive leak that will require dumping of SA.	10a. Loss of one loop. Loss of heat transfer capability.	No	10a. Inhibit in the PPS will preclude dumping of all loops. Time to start CACS and then MLCS can be removed.	No
		10b. Small leak	10b. Loss of one loop. Same as 10a.	No	10b. Can manually dump 2 loops to minimize in-leakage to the PCRV and cool on/loop. Time to start CACS and then MLCS can be removed.	No
11. Large Main Circulator Turbine Speed Control Valve (NO or NM normally modulating) (P&I M201) one per loop.	11. Close on PSD.	11a. Fail as is (near full opening at start)	11a. Loss of one loop. Cause that loop to overspeed until it exhausts its SG inventory (about 35 sec. with no FW flow). Cause stalling of the other 2 circulators. (Circulator designer states that the circulators can be stalled at low power levels for "hours" without damage and remain functional). The two circulators will be stalled until the failed loop exhausts its SG inventory and then resume their cooling function.	No	11a. Loss of all loops in about 35 seconds. Note: "SG inventory boil out in 35 seconds is from memo 760610152, Chung to Buttermer.	35S
		11b. External leak	11b. Loss of one loop. Loss of circulator drive or loss of secondary coolant. Circulator coast down is estimate to be about 30 seconds.	No	11b. Loss of all loops. Same as single failure. Note: Circulator coast down from memo 760726151.	>30S
		11c. Fail to operate	11c. N/A. Not required to modulate for RHR.	No	11c. None. Same as single failure.	No
		11d. Inadvertent opening	11d. Loss of one loop. Similar to 11a and if the SG is flooded, flood out main circulator and bearing water (BW) turbines.	No	11d. Loss of all loops. Same as single failure.	>30S

TABLE 2-1 (Continued)

Component(s)	Function	Failure Mode	Single Failure Effect	Need CACS After PSD	Common Mode Failure Effect	Need CACS After PSD
12. Small Main Circulator Turbine Speed Control Valve (NO (P&I M201) one per loop.	12. Maintain circulator speed control during SHR mode. During plant operation, this valve is fully open and will flow 20% of the full steam flow. After PSD, this valve will modulate inversely proportional to the decay heat level.	12a. Fail as is (NO at start)	12a. Loss of one loop. Cause that loop to ramp down to 20% and remain until it exhaust its SG inventory (about 3 minutes). The balance will be similar to 11a except the other circulators will be stalled for about 3 minutes.	No	12a. Loss of all loops in about 3 minutes. Balance similar to single failure.	3m
		12b. Fail to modulate (fail closed)	12b. Loss of one loop. Loss of motive power to the circulator coast down (about 30 seconds)	No	12b. Loss of all loops with circulator coast down.	>30S
		12c. Fail to modulate (fail open) or external leak	12c. Loss of one loop. Similar to 12a, except after 3 minutes.	No	12c. Loss of all loops after 3 minutes.	>3m
13. Check Valve (NC) (P&I M201) one per loop	13. Prevent steam back flow during normal and SHR modes and allow aux steam to drive circulators in DHR mode.	13a. Fail as is (NC at start)	13a. Loss of one loop. Loss of aux steam motive power to circulator in about 30 minutes.	No	13a. Loss of all loops at about 30 minutes.	30m
		13b. Internal leak	13b. None. Redundant closed valves upstream will prevent back flow of steam during SHR mode.	No	13b. None. Same as single failure.	No
		13c. External leak	13c. Loss of one loop. Similar to 13a except can occur from start with circulator coast down.	No	13c. Loss of all loops. Same as single failure.	>30S
14. On-Off Valve (Elec) (NC) (P&I M201). One per loop.	14. PPS Containment isolation valve. Open to allow aux steam to drive circulators in the DHR mode.	14a. Fail as is (NC at start)	14a. Loss of one loop. Same as 13a.	No	14a. Loss of all loops at about 30 minutes.	30m
		14b. External leak	14b. Loss of one loop. Same as 13a.	No	14b. Loss of all loops at about 30 minutes.	30m
15. Main Circulator Support & Controls (P&I M201) One per loop.	15. Provide motive power to the primary coolant to remove heat from the core and transfer to S.G's.	15a. Fail to start.	15a. N/A. Circulators are running at start.	No	15a. N/A. Same as single failure.	No
		15b. Fail to run.	15b. Loss of one loop. Circulator coast down.	No	15b. Loss of all loops.	>30S

Table 2-1 (Continued)

Component(s)	Function	Failure Mode	Single Failure Effect	Need CACS After PSD	Common Mode Failure Effect	Need CACS After PSD
16. Resuperheaters (P&I M201) one per loop.	16. None for RHR except to maintain its integrity.	16a. Leak.	16a. Loss of one loop. Steam leak into PCRV during SHR mode or primary coolant leak into secondary coolant. Loop will be isolated.	No	16a. Loss of all loops. Same as single failure. Time to start CACS and then MLCS can be isolated.	No
17. Pressure Relief Valves (PRV) (NC) (P&I M201) 4 per loop. Assumed: Exactly 4 PRV's or PSV's out of 8 valves must open, but all 4 valves that open must reclose.	17. Relieve hi pressure main steam in the event of turbine trip from near full power for about 2 1/2 to 3 min. and then close. From 100% power, 75% of the steam will be relieved by the PRV's and 25% will be by-passed.	17a. Fail as is (NC at start)	17a. None. The 4 PRV's are backed by 4 pressure safety valves (PSV) and thus a single PRV "fail to open" will not effect the loop.	No	17a. None. PSV's will back up the PRV's.	No
		17b. Fail to reclose	17b. Loss of one loop. Loss of circulator back pressure. Circulator coast down.	No	17b. Loss of all loops. Same as single failure.	3m
		17c. Premature opening	17c. Loss of one loop. Same as 17b.	No	17c. Loss of all loops. Same as 17b except anytime after 3 min.	>3m
18. Pressure Safety Valves (PSV) (NC) (P&I M201) 4 per loop	18. Relieve hi pressure and back up PRV's	18a. Fail as is (NC at start)	18a. N/A, requires mutiple failure. First, the PRV must "fail to open".	No	18a. N/A. Same as single failure.	No
		18b. Fail to release	18b. N/A, same as 18a.	No	18b. N/A. Same as single failure.	No
		18c. Premature opening	18c. Loss of one loop. Same as 17b.	No	18c. Loss of all loops. Same as 17b.	>3m
19. On-Off Valve (Elec) (NC) (P&I M201) one per loop.	19. PPS Containment Isolation. Open to allow resuperheater bypass steam to condenser or vent to atmosphere.	19a. Fail as is (NC at start)	19a. Loss of all loops. No circulator control. Relief valve will oscillate or coast down.	No	19a. Loss of all loops. Same as 17b.	3m
		19b. External leak	19b. Loss of one loop. Same as 17b.	No	19b. Loss of all loops. Same as 17c.	>3m
20. Pressure Control Valve (NC) (P&I M201) one per loop.	20. Maintain adequate circulator back pressure and to reduce pressure to desuperheater.	20a. Fail as is (NC at start)	20a. Loss of one loop. Same as 19a.	No	20a. Loss of all loop. Same as 17b.	3m
		20b. Fail to modulate (fail open) or external leak.	20b. Loss of one loop. Same as 17c.	No	20b. Loss of all loop. Same as 17c.	>3m
		20c. Fail to modulate (fail closed)	20c. Loss of one loop. Same as 19a except after 3 minutes.	No	20c. Loss of all loop. Same as single failure.	>3m

TABLE 2-1 (Continued)

Component(s)	Function	Failure Mode	Single Failure	Need CACS After PSD	Common Mode Failure Effect	Need CACS After PSD
21. Pressure Controller (P&I M201) one per loop.	21. Maintain adequate circulator back pressure.	21a. Fail to operate (fail valve closed)	21a. Loss of one loop. Same as 19a.	No	21a. Loss of all loop. Same as single failure.	3m
		21b. Fail to operate. (fail valve open).	21b. Loss of one loop. Same as 20c.	No	21b. Loss of all loop. Same as single failure.	>3m
22. Pressure Safety Valve (PSV) (NC) (P&I M201) 2 per loop. Assumption: From full power and relief to atmosphere will require both valves to function.	22. Relieve low pressure steam to atmosphere in the resuperheater by-pass circuit.	22a. Fail as is (NC at start) one PSV.	22a. Loss of one loop. This circulator will run slower than the others due to a higher back pressure, thus will be stalled. Therefore will probably trip circulator.	No	22a. Less cooling capability per loop, but with 3 loops functioning, cooling is likely adequate.	No
		22b. Fail as is (NC at start) both PSV's.	22b. Loss of one loop. Same as 19a.	No	22b. Loss of all loops. Same as 19a.	3m
		22c. Fail to reclose.	22c. Loss of one loop. Cannot close secondary loop.	No	22c. Loss of all loops. Same as single failure. *Loss of* secondary fluid in about 22 hours.	22H
23. Check Valve (NC) (P&I M201) one per loop.	23. Prevent back flow when that loop is shutdown while the other loop(s) are operating.	23a. Fail as is (NC at start)	23a. Loss of one loop. Cannot close secondary loop.	No	23a. Loss of all loops. Same as 22c.	22H
		23b. Internal leak.	23b. None. During steam relief to atmosphere, not required. During closed secondary loop operation, valve will be open.	No	23b. None. Same as single failure.	No
		23c. External leak.	23c. Loss of one loop. Same as 23a.		23c. Loss of all loops. Same as 22c.	22H

3. The normally open circulator small turbine valve modulates steam flow in proportion to the decay heat level (Fig. 2-1, sheet 4).

4. For a plant trip from 100%, the four main steam relief valves dump 75% (by volume) of the steam to atmosphere and close. Four pressure safety valves act as a backup to the four main steam relief valves. Thus, it was assumed that exactly four of eight relief or safety valves are required to open, but all four valves that open are required to close. For a normal controlled plant shutdown, the steam relief valves would not open (Fig. 2-1, sheet 5).

5. The normally closed resuperheater bypass containment isolation valve must open (Fig. 2-1, sheet 5). About 25% of the steam is diverted through the resuperheater bypass line.

6. The resuperheater bypass pressure controller and pressure control valve will maintain adequate back pressure for the main circulator turbine exhaust (Fig. 2-1, sheet 5). This exhaust is normally returned to the main condenser, or, if necessary, rejected for a limited time by direct steam relief to the atmosphere via two relief valves (Fig. 2-1, sheet 5).

7. The bearing water pump turbine continues to operate. Its exhaust is normally returned to the main condenser, or, if necessary, rejected for a limited time by direct steam relief to the atmosphere via one pressure safety valve (Fig. 2-1, sheet 3).

Assuming no feedwater supply, the three primary and secondary loops will operate for about 13 min before the initial steam generator steam/water inventories are depleted.

In about one minute after a plant shutdown, the electrically driven positive displacement shutdown feedwater pumps are started. As indicated

above, this time is not critical. With the start of the feedwater train, the following additional secondary loop components are designed to operate in each loop:

1. The shutdown feedwater pump is started (Fig. 2-1, sheet 1).

2. The feedwater bypass modulating valve and controller for the positive displacement pump operates (Fig. 2-1, sheet 1).

3. The upstream normally closed pump suction check valve opens (Fig. 2-1, sheet 1).

4. The downstream normally closed shutdown feedwater stop-check valve (actuator assumed to be in the open position) to the steam generator opens (Fig. 2-1, sheet 2).

5. The shutdown feedwater heater provides preheated feedwater to the steam generators; however, this function is not necessary for successful loop operation (Fig. 2-1, sheet 2).

6. The check valve to the main circulator bearing water system opens to supply makeup water (Fig. 2-1, sheet 2).

The shutdown heat removal mode as accomplished by the above actions is currently estimated to be operable for about 30 min after plant shutdown when the residual heat in the core is no longer adequate to maintain steam production to drive the circulators and the bearing water turbine pumps.

2.2.2. Decay Heat Removal Mode

The long term decay heat removal mode is accomplished by sustaining the main circulator operation with oil-fired auxiliary boilers that provide auxiliary steam. The auxiliary boilers are designed to reach rated conditions in about 20 min from hot standby condition. Section 4 provides

details on auxiliary boiler operation. Other components of the MLCS continue operation as described previously.

2.2.3. MLCS Support Systems

For the MLCS to function, support systems are required. Section 4 provides the detailed description and analysis of these systems.

Immediately following a plant shutdown and until the shutdown feedwater is started, the following support systems are required by the MLCS:

1. The Class IE 125V dc system (one for each loop) provides power to the dc motor-operated valves/circuit breakers and to the uninterruptible power supply (UPS) buses (see Fig. 4-7, sheet 2).

2. The UPS buses (one for each loop) provide power to the instrumentation and control functions (see Fig. 4-7, sheet 2).

3. The air supply system provides motive power for valves and air source for instrumentation and control functions (see Fig. 4-1).

When the shutdown feedwater is supplied, as required, to the MLCS, one additional support system, the Class IE ac electrical system (one for each loop), which provides power to the shutdown feedwater pumps (see Fig. 4-7, sheet 1), is required.

In order to sustain MLCS operation for long term decay heat removal, the following additional support systems are required:

1. Auxiliary boilers (Fig. 4-3).

2. Condensate and shutdown feedwater makeup (a portion of the power conversion system) (Fig. 4-4).

3. Non-Class IE ac electrical system to provide power to the auxiliary boiler feed and fuel pumps and the condensate pumps (Fig. 4-2).

4. Service water and reactor plant cooling water systems for component cooling (namely, the main circulator support system) (Figs. 4-8 and 4-9).

When the closed secondary loop is required, the following additional support systems are required:

1. Main condenser (a portion of the power conversion system) (Fig. 4-5, sheet 2).

2. Circulating water system (a portion of the power conversion system) (Fig. 4-5).

2.3. QUANTITATIVE ANALYSIS

The RFBD was used to estimate the loop failure rates (λ) and the mean times to restore (MTTR) from which the MLCS failure probabilities could be estimated. To estimate the λ and the MTTR of a loop, tables were set up with the components of the RFBD with all the failure rates and the MTTR, using the generic data base as described in Appendix A. The assumed initial condition was that the plant was online and producing 100% power.

As indicated by the RFBD, the MLCS consists of three independent and identical loops. Thus the λs and the MTTRs for one loop are required to estimate the failure probabilities of the MLCS.

The MLCS components, as discussed in Section 2.2.1, were separated into the primary (helium) loop components and the secondary (steam/water) loop components. The λs and MTTRs for one loop, excluding the support systems, were estimated as follows:

	Primary Loop Components		Secondary Loop Components		Total	
	λ_D	$MTTR_D$	λ_D	$MTTR_D$	λ_D	$MTTR_D$
MLCS Loop (λ_D = failure rate per demand)	--	--	1.5×10^{-2}/D	25	1.5×10^{-2}/D	25
	λ_t	$MTTR_t$	λ_t	$MTTR_t$	λ_t	$MTTR_t$
MLCS Loop (λ_t = failure rate per hour)	1.4×10^{-4}/hr	100	5.5×10^{-4}/hr	32	6.9×10^{-4}/hr	46

The indicated greatest contributor to the secondary loop component λ_D was the reclosing of the four main steam relief or safety valves after a plant trip from 100% power. This was estimated to be (3×10^{-3}/D x 4 = 1.2×10^{-2}/D), or about 80% of the secondary loop demand failure rate. Assuming a controlled shutdown of the plant, the λ_D was estimated to be 2.9×10^{-3}, of which the start of the shutdown feed pump and the cycling of the electrically operated resuperheater bypass valve, each contributing 1×10^{-3}/D, were the most significant.

The indicated greatest contributor to the primary loop component λ_t was the main circulator and its support and control. This was estimated to be 1×10^{-4}/hr, or about 70% of the primary loop component running failure rate.

The indicated greatest contributor to the secondary loop component λ_t was the positive displacement shutdown feedwater pump. This was estimated to be 3×10^{-4}/hr, or about 55% of the secondary loop component running failure rate.

Assuming that 20% of the plant outage time may be caused by main loop faults and basing calculations on the standard reliability approximations given in Appendix A, the following system failure rates may be calculated:

	System Failure Rates	
	Λ_D	Λ_t
MLCS	$6.7 \times 10^{-4}/D$ [a]	$1.1 \times 10^{-5}/hr$ [b]

[a] A minimum of two main loops required.

[b] Only one main loop required.

Based upon a plant outage of 1752 hr and a total of three reactor trip demands per year, the system failure probability may be estimated as $2.1 \times 10^{-2}/yr$.

2.4. DESIGN IMPROVEMENTS

The following suggested design improvements to enhance reliability of the MLCS are a result of the analysis previously described.

Suggested Improvements	Reliability Effect
1. Provide the capability for the shutdown feedwater loops to be cross-connected to any secondary loop.	1. Will increase the number of success paths, thus increasing reliability.
2. Provide the capability for the main loops to better use the core residual heat to extend the time before feedwater is required or before auxiliary steam is required to maintain the MLCS (i.e., drive the circulator by self-turbining with the bearing water pumps, thus using the boot-strapping steam for the bearing water pump only, not for the main circulator turbine).	2. Current estimate indicates that the core residual heat can provide adequate steam for 30 min after shutdown. As the auxiliary boilers take about 20 min to rated steam conditions, there is possibly only a 10 min overlap. If the boot strapping can be increased to provide a longer overlap, it will be more likely that auxiliary steam will be available to maintain MLCS for RHR.

2.5. AREAS FOR FURTHER STUDIES

During the FMEA, certain failure effects were either not clearly known or not available because of the conceptual state of the design,

and so the best assumptions available at this time were made. As they are open to question, some of these assumptions may indicate areas for further studies, as is suggested below:

1. Failure: Main steam line rupture at 100% power.
   Effect: Assumption - plant protection system (PPS) will detect steam leak and isolate all loops. No loss of MLCS.
   Question: Can the main circulators withstand the sudden reduction in pressure and remain operable?

2. Failure: Overspeed of one circulator.
   Effect: Assumption - the other two circulators will stall until the failed loop boils out or is manually tripped, and then the stalled circulator will recover and resume functioning.
   Question: Is the assumption valid?

3. Failure: Loss of heating to shutdown feedwater heaters.
   Effect: Assumption - feedwater heating is not absolutely required. Loss will give slight thermal shock to steam generator tube sheets, but will not effect RHR capabilities.
   Question: Is the assumption valid?

4. Failure: Loss of a main loop during transition from core residual heat steam to auxiliary steam.
   Effect: Assumption - transition can be accomplished easily within the time constraint of about 10 min (see Section 2.4, the second suggested improvement).
   Question: What are the steam conditions at this time? If they are sufficiently different from assumption, will this require shutting down the main loop before resuming on auxiliary steam and is 10 min then adequate time?

3. CORE AUXILIARY COOLING SYSTEM

3.1. DESCRIPTION

The core auxiliary cooling system (CACS) is designed to automatically provide an independent means of RHR when the MLCS fails to function. Each CACS loop includes the auxiliary circulator, a circulator service system, a core auxiliary heat exchanger (CAHE), an auxiliary loop isolation valve, and the core auxiliary cooling water system (CACWS).

Each auxiliary circulator consists of an electric-motor-driven centrifugal compressor and diffuser. Circulator speed is controlled by the variable-frequency power supply.

An auxiliary circulator service system accomplishes the following: (1) provides cooling water to the auxiliary-circulator motor windings and bearings, (2) supplies purified buffer helium for preventing leakage of motor bearing lubrication into the reactor coolant or leakage of reactor coolant into the motor casing, (3) removes oil vapor carried over in purge helium from the circulator, and (4) removes and replaces motor lubricant.

Each CAHE is a helically wound, axial flow tube bundle with an integral shroud. The tubes in the heat-exchanger tube bundle will be segregated into subgroups, each having approximately the same number of tubes. Separate cooling-water supply and return lines will connect each of these tube subgroups to the cooling-water headers outside the PCRV. The arrangement of the tubes will minimize the effect of inleakage from a tube failure. Subheaders are to be plugged outside the PCRV, and the corresponding subgroup of tubes containing the leaking tube will be isolated.

An isolation valve is provided for each cooling loop. Each valve consists of two semielliptical ribbed plates supported at a common hinge

joint and functions in a way that is similar to check valve functions. In its closed position, the valve is required to limit to an acceptable amount the helium bypassing the reactor core through the auxiliary loop. The valve is required to open automatically when its auxiliary circulator is brought into operation and to close automatically when the circulator ceases to function.

Each CACWS consists of a pressurized water loop capable of removing heat from the CAHE and rejecting it to the atmosphere by means of a forced-convection air heat exchanger. Each closed loop has an air-cooled heat exchanger, two circulating water pumps, a pressurizer, and a demineralizer tank and filter for periodic cleanup. A makeup storage tank and two pumps for supplying makeup water are common to all three loops in the event of low level in the pressurizer tank.

3.2. QUALITATIVE ANALYSIS

An RFBD was drawn for the CACS. The RFBD, shown in Fig. 3-1, sheets 1 through 4, includes the major equipment items and the active mechanical components. Control and protection systems are not included, as designs are not yet available. The major support system requirements are indicated by dashed blocks primarily to show the inter-relationships discussed in Section 4.

An FMEA was performed on the major equipment items and the active mechanical components. This FMEA is presented in Table 3-1. No single passive mechanical failure of a CACS component was uncovered.

The three CACS loops were indicated to be functionally independent (excluding support systems) and identical, both from active and passive failure standpoints.

The following principles govern actions upon startup of a core auxiliary cooling loop:

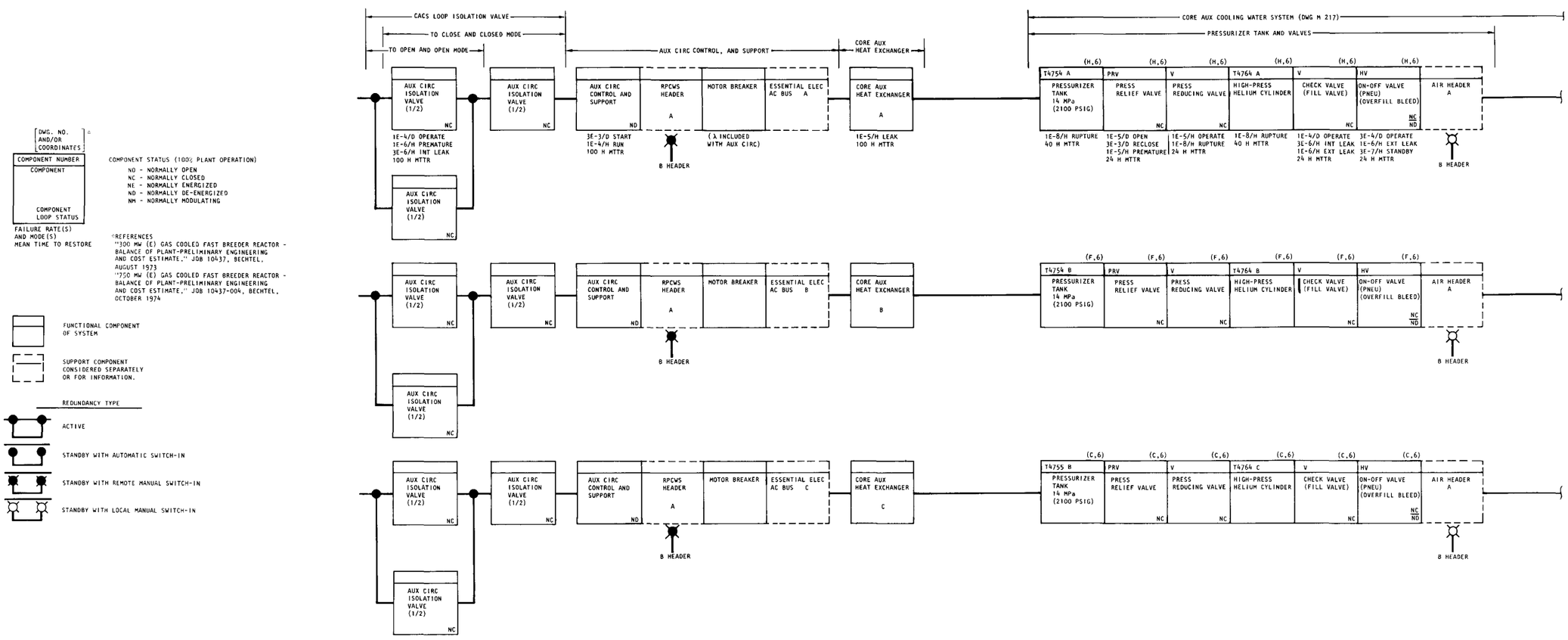


Fig. 3-1. GCFR core auxiliary cooling system (CACS) reliability function diagram, sheet 1 of 4

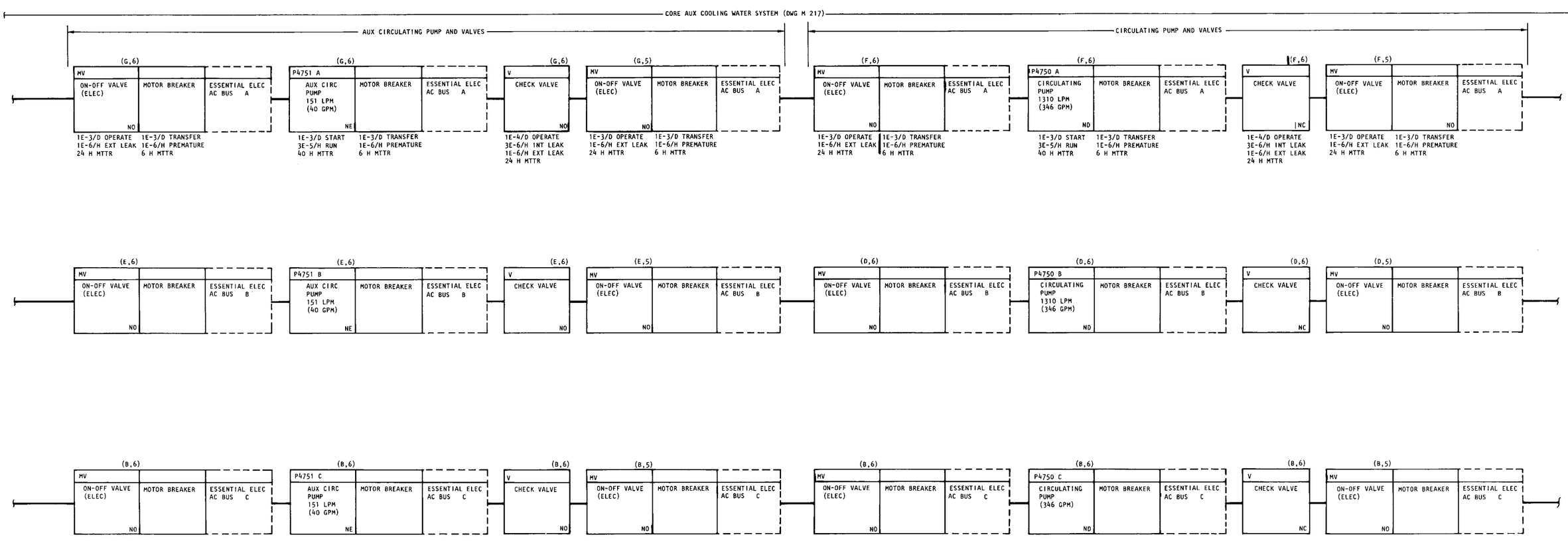


Fig. 3-1. GCFR core auxiliary cooling system (CACS) reliability function diagram, sheet 2 of 4

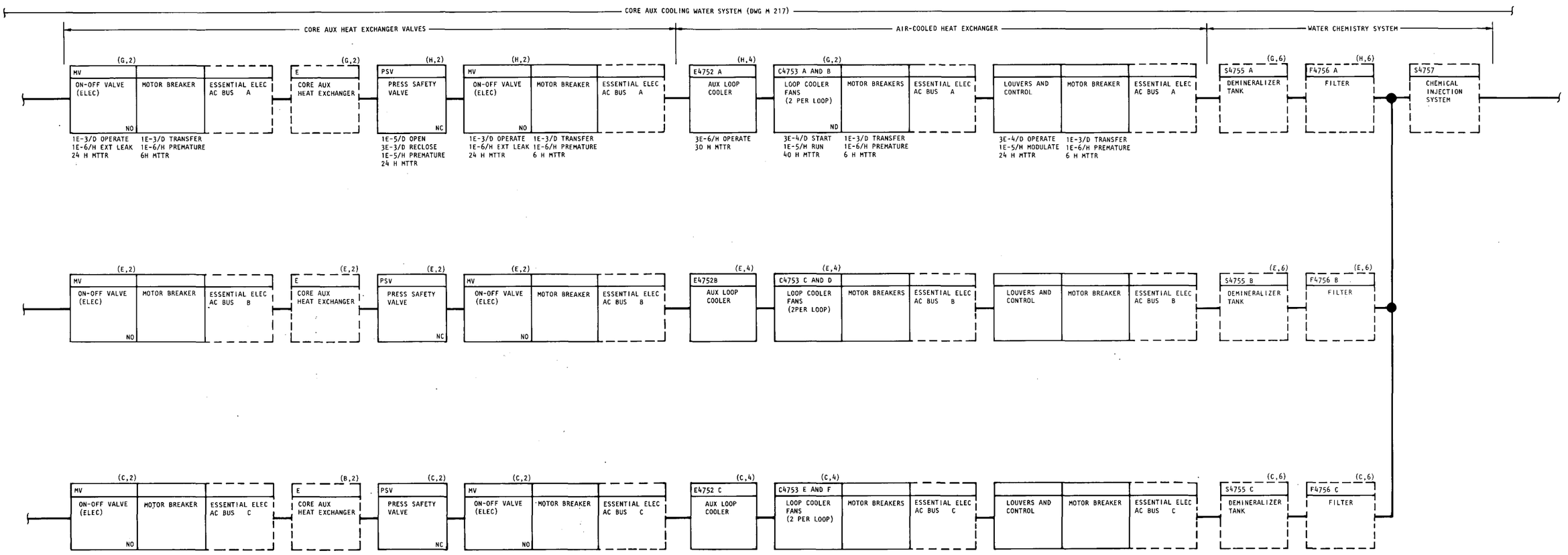


Fig. 3-1. GCFR core auxiliary cooling system (CACS) reliability function diagram, sheet 3 of 4

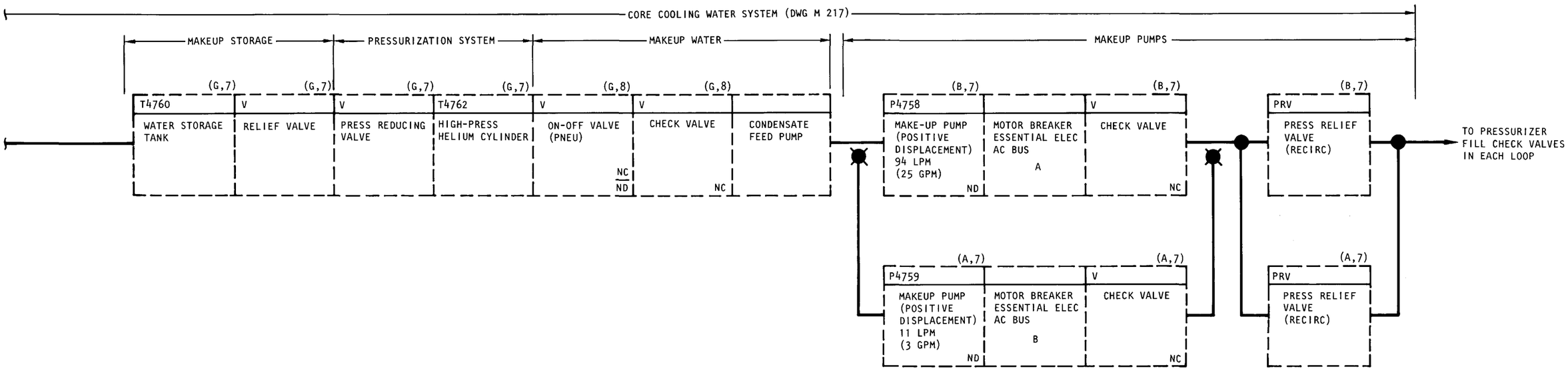


Fig. 3-1. GCFR core auxiliary cooling system (CACS) reliability function diagram, sheet 4 of 4

TABLE 3-1

FAILURE MODES AND EFFECTS ANALYSIS, CORE AUXILIARY COOLING SYSTEM

Initial Condition: (a) Loss of main loop RHR in <15 minutes after turbine trip & reactor scram.
(b) Loss of main loop RHR in >15 minutes after turbine trip & reactor scram.

Component In One Loop	Function	Failure Mode	Failure Mechanism	Failure Effect On CACS Cooling Capability	Remaining CACS Capability (%)
1. Auxiliary Circulator Helium Isolation Valve (two half sections in each valve)	Allow primary coolant to flow through loop and inhibit back flow during standby mode.	One valve section fails	Jammed or frozen	Valve provide adequate flow area with one section closed	(a) 150 (b) 300
		Both valve sections fail to open	Jammed or frozen	Loss of a loop	(a) 100 (b) 200
2. Auxiliary Circulator	Forced circulation of primary coolant.	Fail to operate	Motor or bearing failure, mechanical obstruction or blade failure.	Loss of a loop	(a) 100 (b) 200
3. Auxiliary Circulator Motor Control	Start and control motor speed	Fail to operate	Circuit failure	Loss of a loop	(a) 100 (b) 200
4. Auxiliary Circulator Water Cooling Module (two modules per circulator)	Remove heat from motor windings and bearings.	Loss of one cooling module	Pump, pipe, valve or tube failure.	None; cooling modules are redundant	(a) 150 (b) 300
5. Service Water Header	Provide cooling water to the aux. circ water cooling module.	Loss of cooling	Pipe or valve failure from header to cooling module.	None; redundant header available by remote manual control	(a) 150 (b) 300
6. Buffer Helium and Oil Adsorption Module	Supply purified helium for preventing leakage of motor bearing lubricant into reactor coolant or leakage of reactor coolant into motor casing and to remove oil vapor carry over into helium recycle system.	Loss of buffer helium	Flow control, pipe or valve failure.	None; not required for loop operation	(a) 150 (b) 300
7. Bearing Oil Module	Remove and replace motor bearing lubricant, normally valved off	Loss of bearing oil module to shut off valve	Tank, pipe or valve failure	None; not required during loop operation	(a) 150 (b) 300
		Loss of bearing oil from motor bearing cavities	Pipe or valve failure	Loss of a loop	(a) 100 (b) 200
8. Pressurizer Tank	Compensate for water volume changes; prevent boiling and makeup for small leakages	Low water volume in tank	Leakage in excess of makeup capacity or sensor failure	Loss of a loop	(a) 100 (b) 200

TABLE 3-1 (Continued)

Component In One Loop	Function	Failure Mode	Failure Mechanism	Failure Effect On CACS Cooling Capability	Remaining CACS Capability (%)
9. Pressure Relief Valve	Prevent over pressurization of the loop.	Inadvertant opening	Valve failure	Loss of a loop.	(a) 100 (b) 200
10. Pressure Reducing Valve	Maintain adequate loop pressure.	Fail to operate	Valve failure	Loss of a loop.	(a) 100 (b) 200
11. High Pressure Helium Cylinder	Provide pressure source for the loop.	Loss of pressure	Cylinder, valve or pipe failure.	No short term effect; closed system so that pressure decrease will be slow; time to repair	(a) 150 (b) 300
12. Check Valve (NC)	Prevent backflow into make-up water system	Internal Leak	Worn, corrosion or vibration	None. Check valves upstream will prevent over pressurization of make-up water system.	(a) 150 (b) 300
		Rupture	Valve body failure	Loss of a loop.	(a) 100 (b) 200
13. On-off Valve (Pneu) (NC/ND) (assumed FC valve)	Return valve to the make-up water system if the pressurizer tank over fill.	Internal leak or rupture	Valve failure	Loss of a loop.	(a) 100 (b) 200
14. Air Header	Motive power to actuate valve.	Loss of air	Tubing or valve failure.	None. Not required for loop operation. Assumed a FC (failed closed) valve	(a) 150 (b) 300
15. On-off Valve (Elec) (No) (Pump Inlet)	Isolate auxiliary circulator for maintenance and repair	Rupture	Valve failure	Loss of a loop.	(a) 100 (b) 200
16. Electric Power	Motive power to actuate valve.	Loss of electricity	Circuit failure	None. Not required for loop operation. Double failure	(a) 150 (b) 300
17. Auxiliary Circulator Pump and Drive.	Forced circulation of secondary coolant during CACS standby mode.	Fail to operate	Motor or pump failure.	None. Not required during cooling mode.	(a) 150 (b) 300
18. Check Valve (No)	Prevent back flow during cooling mode.	Fail to close	Wear, jammed or foreign material	Loss of a loop	(a) 100 (b) 200
19. On-off Valve (Elec) (No) (Pump Outlet)	Isolate auxiliary circulator for maintenance and repair	Rupture	Valve failure	Loss of a loop	(a) 100 (b) 200

TABLE 3-1 (Continued

Component In One Loop	Function	Failure Mode	Failure Mechanism	Failure Effect On CACS Cooling Capability	Remaining CACS Capability (%)
20. Electric Power	Motive power to actuate valve.	Loss of electricity	Circuit failure	None. Not require for loop operation. Double Failure	(a) 150 (b) 300
21. On-Off Valve (Elec) (No) (Pump Inlet)	Isolate circulator pump for maintenance and repairs.	Rupture	Valve failure	Loss of a loop	(a) 100 (b) 200
22. Electric Power	Motive power to actuate valve.	Loss of electricity	Circuit failure	None. Not required for loop operation. Double Failure	(a) 150 (b) 300
23. Circulator Pump and Drive	Forced circulation of secondary coolant during cooling mode.	Fail to operate	Motor or pump failure	Loss of a loop	(a) 100 (b) 200
24. Check Valve (NC)	Prevent backflow during CACS standby mode and allow flow during cooling mode.	Fail to open	Wear or jammed	Loss of a loop	(a) 100 (b) 200
25. On-Off Valve (Elec) (No) (Pump Outlet)	Isolate circulator pump for maintenance and repairs	Rupture	Valve failure	Loss of a loop	(a) 100 (b) 200
26. Electric Power	Motive process to actuate valve	Loss of electricity	Circuit failure	None. Not required for loop operation. Double failure	(a) 150 (b) 300
27. On-Off Valve (Elec) (No) (CAHE Inlet)	Isolate CAHE for maintenance and repair.	Rupture	Valve failure	Loss of a loop	(a) 100 (b) 200
28. Electric Power	Motive power to actuate valve.	Loss of electricity	Circuit failure	None. Not required for loop operation. Double failure	(a) 150 (b) 300
29. CAHE (Core Auxiliary Heat Exchanger)	Transfer primary coolant heat to the secondary coolant	Leak	Tube or header failure.	Loss of a loop	(a) 100 (b) 200
30. Pressure Safety Valve	Prevent over pressurization of the CAHE.	Inadvertent opening	Valve failure	Loss of a loop	(a) 100 (b) 200
31. On-Off Valve (Elec) (No) (CAHE Outlet)	Isolate CAHE for maintenance and repairs	Rupture	Valve failure	Loss of a loop	(a) 100 (b) 200
32. Electric Power	Motive power to actuate valve	Loss of electricity	Circuit failure	None. Not require for loop operation. Double failure	(a) 150 (b) 300
33. Auxiliary Loop Cooler	Ultimate heat sink. Transfer secondary coolant heat to the atmosphere	Leak	Tube or Header failure	Loss of a loop	(a) 100 (b) 200

TABLE 3-1 (Continued)

Component In One Loop	Function	Failure Mode	Failure Mechanism	Failure Effect On CACS Cooling Capability	Remaining CACS Capability (%)
34. Loop Cooler Fans & Drive	Force air flow past cooler surface	Fail to operate	Motor or fan failure	Loss of a loop	(a) 100 (b) 200
35. Louvers & Control	Adjust air flow past cooler to cooler outlet temperature	Fail to operate	Louver or circuit failure	Loss of a loop	(a) 100 (b) 200
36. Dimineralizer Tank	Remove dissolved solids from the secondary coolant	Fail to operate	Require recharging	None. Normally valved out. Not required during cooling.	(a) 150 (b) 300
37. Filter	Remove particulates from the secondary coolant.	Fail to operate	Clogged filter	None. Normally valved out. Not required during cooling.	(a) 150 (b) 300
38. Chemical Injection System	Maintain proper water chemistry	Fail to operate	System failure	None. Not required during cooling.	(a) 150 (b) 300
39. Make up Water System Common to all Loops	Provide make up water	Fail to operate	System failure	None. Not required during cooling. Pressurizer Tank has adequate supply for normal loop leakage rate for >168 hr	(a) 150 (b) 300

1. The auxiliary circulator drive motor is energized to produce a flow corresponding to that of the reactor coolant. The head produced by the circulator causes the isolation valve to open and establish coolant flow through the auxiliary heat exchanger and the core.

2. Cooling-water flow in the auxiliary heat-dump system is switched to the large-capacity circulating pump.

3. The power supply, and thus the auxiliary circulator speed, is automatically adjusted until the set point of the helium temperature at the core inlet is achieved. This provides the increase in speed needed for core cooling when the reactor is depressurized and the decrease in speed that should accompany repressurization.

In the event of the loss of MLCS, the major equipment items which must start and run for each loop are:

1. The auxiliary circulator (Fig. 3-1, sheet 1).
2. The circulating water pump (Fig. 3-1, sheet 2).
3. The two loop cooler fans (Fig. 3-1, sheet 3).
4. The loop cooling tower louvers (Fig. 3-1, sheet 3).

In addition, the following valves must change state for each loop:

1. The auxiliary loop isolation valves must open (Fig. 3-1, sheet 1). [It was assumed that half of the valve opening is adequate and thus the two halves were assumed to be redundant for the change from normally closed to open mode (Fig. 3-1, sheet 1)].

2. The upstream check valve of the circulating pump must open (Fig. 3-1, sheet 2).

3. The upstream check valve of the auxiliary circulating pump must close (Fig. 3-1, sheet 2).

Each CACS loop requires four major equipment items to start; however, it has been so designed that the very minimum number of valves are required to change state for the loop to function.

3.2.1. CACS Support Systems

For the CACS to function, the support systems listed below are required. Section 4 provides the detailed descriptions and analysis of these systems.

1. The Class IE ac electrical system (one for each loop), which provides power to the auxiliary circulators (Fig. 3-1, sheet 1), circulating pump (Fig. 3-1, sheet 2), loop cooler fans, and louvers (Fig. 3-1, sheet 3).

2. The service water/reactor plant cooling water, which provides component cooling to the auxiliary circulator support (Fig. 3-1, sheet 1, not specifically indicated).

3. The air supply system (Fig. 3-1, sheet 1), which is associated with the overfill bleed pneumatically operated valve. However, this valve will not function during CACS operation because the water level in the pressurizer tank will drop as a result of the CACWS water temperature being lower during operation than at standby.

4. Remote manual electrically operated on-off valves are shown; however, these valves are component isolation valves for repair and are not to be actuated except in the case of an equipment failure.

3.3. QUANTITATIVE ANALYSIS

The RFBD was used to estimate the failure rates (λ) and the MTTR from which the CACS failure probabilities could be estimated.

As indicated by the RFBD, the CACS consists of three independent and identical loops. Thus the λ and the MTTR for one loop are required to estimate the failure probabilities of the CACS.

The λs and the MTTRs for one loop, excluding the support systems, were estimated as follows:

	Primary Loop Components		Secondary Loop Components		Total	
	λ_D	$MTTR_D$	λ_D	$MTTR_D$	λ_D	$MTTR_D$
CACS Loop (λ_D = failure rate per demand)	3.1×10^{-3}/D	100	5.1×10^{-3}/D	16	8.2×10^{-3}/D	47
	λ_t	$MTTR_t$	λ_t	$MTTR_t$	λ_t	$MTTR_t$
CACS Loop (λ_t = failure rate per hour)	1.1×10^{-4}/hr	100	1.8×10^{-4}/hr	25	2.9×10^{-4}/hr	53

The indicated greatest contributor to the primary loop λ_D was the "fail-to-start" of the auxiliary circulator and control (Fig. 3-1, sheet 1). This was estimated to be 3×10^{-3}/D, or about 97% of the primary loop demand failure rate.

The indicated greatest contributor to the primary loop λ_t was the "fail-to-run" of the auxiliary circulator and control. This was estimated to be 1×10^{-4}/hr, or about 91% of the primary loop running failure rate.

The indicated greatest contributor to the secondary loop λ_D was the "fail-to-start" of the circulating pump (Fig. 3-1, sheet 2). This was

estimated to be 2 x 10^{-3}/D, or about 39% of the secondary loop demand failure rate.

The indicated greatest contributor to the secondary loop λ_t was the "fail-to-run" of the circulating pump. This was estimated to be 3 x 10^{-5}/hr, or about 17% of the secondary loop running failure rate.

The greatest contributor to the total λ_D and λ_t was the "fail-to-start" and "fail-to-run" of the auxiliary circulator and control. This contributed to about 58% of the total demand failure rate and 34% of the total running failure rate.

Assuming that 20% of the plant outage time may be caused by main loop faults and 5% by auxiliary loop faults and basing calculations upon the standard reliability approximations given in Appendix A, the following RHR system (MLCS and CACS) failure rates may be calculated:

	System Failure Rates	
	Λ_D	Λ_t
MLCS and CACS	1.35 x 10^{-7}/D[a]	1.4 x 10^{-11}/hr[b]

[a] A minimum of two main loops or two CACS loops required.

[b] Only one main loop or one CACS loop required.

Based upon a plant outage of 1752 hr and a total of three reactor trip demands per year, the system failure probability may be estimated as 4.3 x 10^{-7}/hr. Dividing out the MLCS failure probability of 2.1 x 10^{-2}/yr given in Section 2 gives a CACS failure probability of 2.0 x 10^{-5} per demand.

3.4. DESIGN IMPROVEMENTS

The following design improvement to enhance reliability of the system is suggested:

Improvement	Reliability Effect
1. Independent auxiliary circulator motor cooling system (i.e., independent air-cooled heat exchanger for each loop).	1. Will eliminate one of the inter-dependencies with the MLCS and the intradependency within the CACS.

3.5. AREAS FOR FURTHER STUDIES

The GCFR CACS is basically designed in a fashion similar to the HTGR CACS, and this system has been studied extensively under the HTGR program. Thus no area for further study is recommended.

4. RHR SUPPORT SYSTEMS

The reliability analysis of the residual heat removal systems has identified four major systems which solely support the RHR function of the MLCS. These are:

1. Instrument and Service Air

   This system supplies valve control air to support valve operations for the MLCS RHR function.

2. Nonessential Electric Power

   This system provides electrical power to power conversion and auxiliary steam supply equipment for long term MLCS operation.

3. Auxiliary Steam Supply

   This system provides the circulator driving steam for long term MLCS operation.

4. Power Conversion

   This system provides the ultimate heat sink and feedwater supplies for long term MLCS operation.

Two major systems have been identified which commonly support the RHR function of both the MLCS and CACS. These are:

1. Essential Electric Power

   This system provides electrical power to MLCS and CACS equipment for the RHR function.

2. Component Cooling Water

This system provides component cooling water to MLCS and CACS equipment for the RHR function.

No major systems have been identified which solely support the RHR function of the CACS.

The qualitative and quantitative analysis presented in subsequent sections shows that a limiting dependence of both RHR systems exists in their reliance upon the above support systems as currently configured. Single failure points are in evidence in passive features in all four systems supporting the MLCS. As summarized in Table 4-1, this lesser redundancy gives a total failure probability of systems supporting the MLCS of the order of 10^{-1}/yr, well in excess of the MLCS allocation. The limiting dependence of both RHR systems is that of common reliance on the doubly redundant component cooling water system and triply redundant redundant electrical power system. The lesser redundancy and lack of diversity which exists because of this dependence gives a total failure probability of systems supporting both the MLCS and CACS of the order of 10^{-3}/yr, also well in excess of the allocation.

4.1. AIR SUPPLY SYSTEM

4.1.1. Description

The instrument and service air system performs two functions: (1) it provides instrument air to valve operators and controllers and clean air for other area requirements, and (2) it provides service air to portable tools and pressurized air for other area requirements.

The air supply system consists of the following:

1. Three independent sets of compressors, aftercoolers, and receivers. Each receiver, if initially charged to a minimum

TABLE 4-1
RHR SUPPORT SYSTEM UNRELIABILITY ASSESSMENT

Plant Outage Event	Assessed Unreliability[(a)]	
	MLCS	MLCS and CACS
Loss of Instrument and Service Air	5×10^{-2}	--
Loss of Power Conversion System	1×10^{-1}	--
Loss of Auxiliary Steam Supplu	4×10^{-2}	--
Loss of Nonessential Electric Power	4×10^{-3}	--
Loss of Essential Electric Power	--	2×10^{-4}
Loss of Reactor Plant Cooling Water	--	1×10^{-3}
Total[(a)]	1.9×10^{-1}	1.2×10^{-3}
Allocation[(a)]	10^{-2}	10^{-6}

[(a)] Values are per reactor year.

pressure of 0.5 MPa (125 psig), is capable of 1-min instrument air demand without electric power to the compressor.

2. Two independent air headers with cleanup trains, one header on-line and the other header on standby with a local manual switch-in.

3. A single manifold connecting the compressors with the headers.

The air supply system provides instrument air to the air-operated valves and to controllers for the following systems required for RHR:

1. MLCS

   - Feedwater controllers and valve operators.
   - Circulator controllers and valve operators.
   - Resuperheater bypass controllers and valve operators.
   - Main steam relief valves.
   - Shutdown feedwater pump recirculating flow controllers and valve operators.

2. CACS

   - Valve operators in the service system motor coolers. These valves are normally open (NO) valves and are only operated to isolate the cooling water to the motor when a failure occurs in the system. Thus, air supply is not required for normal operation.
   - Valve operators in the buffer helium and oil adsorber system. These are desirable, but not absolutely required for circulator

operation. Thus, air supply is not absolutely required for circulator operation.

- Valve operators of the excess water bleed valve on the pressurizer in the core auxiliary cooling water system. During CACS core cooling mode, the circulating water temperature will be reduced from about 315°C (600°F) to 82°C (180°F); thus the water level in the pressurizer will be lowered and it will then be very unlikely that the excess water bleed valve will be required.

The conclusion is that the air supply system is not required for CACS operation.

3. Component cooling systems (service water and reactor plant cooling water systems).

- Remote manual valve switching in the event of an on-line component cooling water failure in at least the following RHR areas:

  a. CACS service system motor coolers.
  b. Main helium circulator water coolers.
  c. Air compressor jackets and aftercoolers.
  d. Emergency diesel/generator room cooler.

4. Power Conversion System

- Level controller and fill valve actuators for the condenser hotwell level.

- Level controller and fill valve actuator for the mechanical draft cooling tower basin in the circulating water system.

4.1.2. Air Supply System Qualitative Analysis

An RFBD (Fig. 4-1) was developed for the air supply system. A FMEA of this system on MLCS operation is given in Table 4-2. The air supply system was assumed to operate as follows:

1. One of three air compressing loops is adequate for RHR. The air receivers in each loop are open to the header manifold and thus all air compressing loops are on-line and will automatically switch on and off with load demands.

2. A single pipe header connects the compressor loops to the air headers.

3. The two independent air headers operate so that one is on-line and the other is on standby with a local manual switch-in.

The air supply system is normally operating during plant operation so that no system start-up is required. The switching on and off of the air compressors with load demand is considered normal for this system.

A single passive mechanical failure, that of the pipes and valves in the manifold header, was indicated on the piping and instrumentation drawing. The two air headers, one normally on-line with the other on standby with local manual switch-in, thus cannot quickly and easily be switched in the event of the loss of a header.

4.1.2.1. Air Supply System Support Systems. For the air supply system to function, the following support systems are required:

1. The Class IE ac electrical system, one bus for each compressor.

2. The service water system, which provides cooling water to the compressors and aftercoolers.

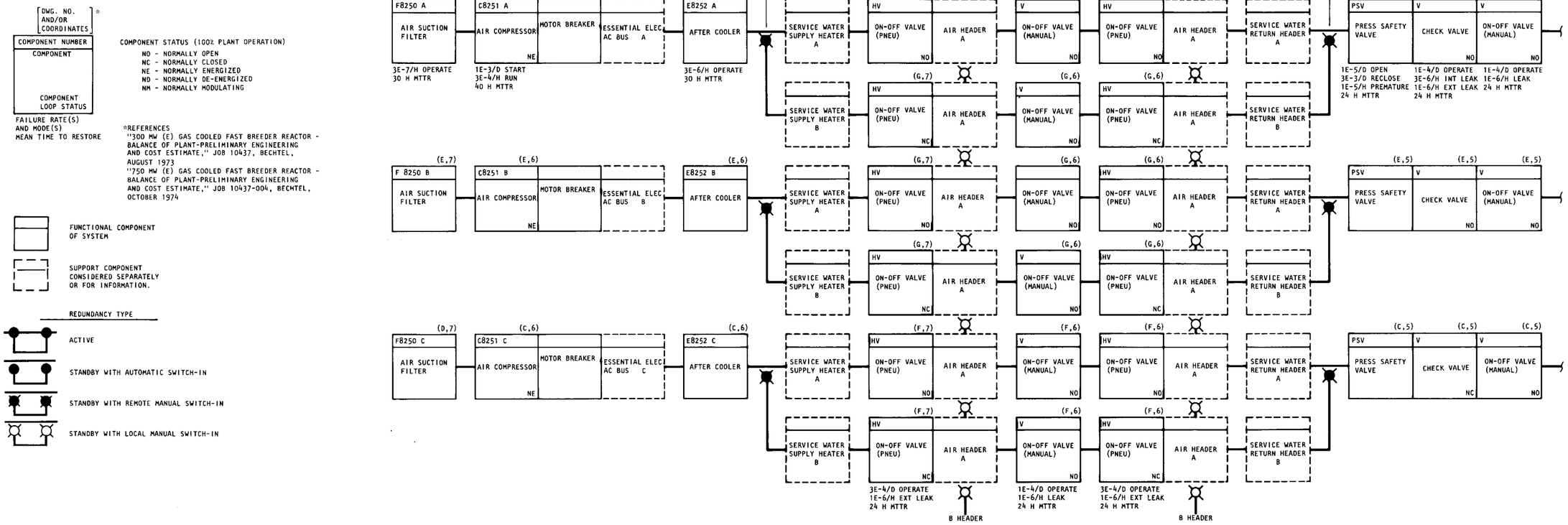


Fig. 4-1. GCFR instrument air system reliability function diagram for RHR (Drawing M218), sheet 1 of 2

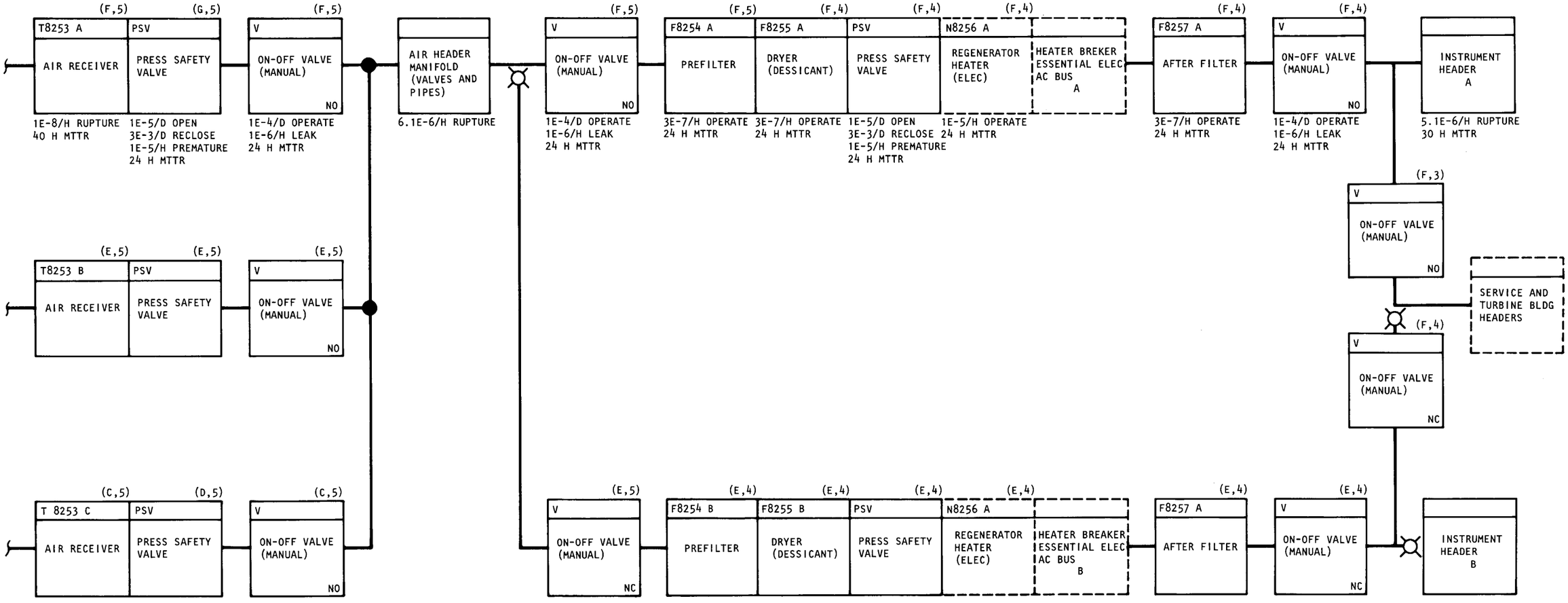


Fig. 4-1. GCFR instrument air system reliability function diagram for RHR (Drawing M218), sheet 2 of 2

TABLE 4-2
FAILURE MODE AND EFFECT ANALYSIS OF SUPPORT SYSTEMS FOR GCFR MAIN LOOP COOLING SYSTEM (MLCS) RHR

Initial Conditions: Full Power & Plant Shutdown (PSD) & Loss of Support Systems

Support System	Function	Failure Mode	MLCS Failure Effect	Need CACS after PSD	Ref: RFBD/FMCA Component No.
1. Air Supply System	1. Provide motive power for valves and controller.	1a. Loss of Air	1a. Loss of motive power to the following MLCS components:	>30S	
			Feedwater controllers and valve operators	(1)	Fig. 2-1, Sheets 3/9
			Circulator controllers and valve operators	>30S	Fig. 2-1, Sheets 4/11 & 12
			Resuperheater by-pass controllers and valve operators	>3m	Fig. 2-1, Sheets 5/20 & 21
			Shutdown FW pump recirculating flow controllers & valve operators	>13m	Fig. 2-1, Sheets 1/4 & 5
			Main Steam Pressure relief valves	(1)	Fig. 2-1, Sheets 5/17
2. Non-Class IE Elec Power System (Non-essential)	2. Provide electric power to the non-safety system	2a. Loss of electric power	2a. Loss of electric power to the following support systems to maintain MLCS:	>13m	
			Condensate System	13m	Fig. 4-4
			Auxiliary Steam Supply System	30m	Fig. 4-3
			Circulating Water System	22H	Fig. 4-5
3. Auxiliary Steam Supply System	3. Provide auxiliary steam to the MLCS after loss of core residual heat.	3a. Fail to operate	3a. Loss of motive force to drive the main helium circulator turbines and bearing water pump turbines.	30m	Fig. 4-3
4. Power Conversion Systems:					
a. Condensate System	4a. Provide makeup water to the shutdown FW storage tank and the feedwater source for the aux steam system.	4a. Fail to operate	4a. Loss of make-up water to the shutdown FW storage tank	13m	Fig. 4-4
			4a. Loss of aux steam (Same as 3a).	30m	Fig. 4-3
b. Circulating Water System	4b. Provide heat rejection for MLCS during RHR.	4b. Fail to operate	4b. Loss of "closed" secondary loop operation.	22H	Fig. 4-5

(1) Redundant component(s) in each loop.

TABLE 4-2 (Continued)

Support System	Function	Failure Mode	MLCS Failure Effect	Need CACS after PSD	Ref: RFBD/FMCA Component No.
5. Class IE Electric Power System (Essential)	5. Provide electric power to all safety related equipments and provide UPS for the instrumentation and control (I&C) system.	5a. Fail to operate	5a. Loss of I&C power to the following:	>30S	
			Feedwater controllers and valve operators	(1)	Fig. 2-1, Sheet 3/9
			Circulator controllers and valve operators	>30S	Fig. 2-1, Sheet 4/11 & 12
			Resuperheater by-pass controllers and valve operators	>3m	Fig. 2-1, Sheet 5/20 & 21
			Shutdown FW pump recirculating flow controllers and valve operators	>13m	Fig. 2-1, Sheet 1/4 & 5
			5a. Loss of motive power to the following components or systems:	>13m	
			Shutdown feed pumps	>13m	Fig. 2-1, Sheet 1/3
			Reactor plant cooling water system	(2) >1.5H	Fig. 4-8
			Service Water System	>>1.5H	Fig. 4-9
6. Component Cooling Water Systems					
a. Reactor Plant Cooling Water System (RPCWS)	6a. Provide cooling water to components carrying radioactive and potentially radioactive fluids.	6a. Fail to operate	6a. Loss of cooling water to bearing water systems. Failure criteria was assumed to be 56°C (100°F) above nominal temperature which will cause failure of the BW pump with no heat transfer from the BW system.	>1.5H	Fig. 4-8
b. Service Water System.	6b. Provide cooling water to the RPCWS heat exchangers and transfers heat ultimately to the cooling tower.	6b. Fail to operate	6b. Loss of cooling to the RPCWS which in turn will cause loss of BW cooling. Heat capacity of the RPCWS is probably much greater than the BW system, thus the loss of the MLCS will be much longer than 6a.	>>1.5H	Fig. 4-9

(1) Redundant component(s) in each loop.

(2) Assumed Bearing Water Pumps will fail when bearing water exceeds 100°F above average temperature with no heat transfer from the BW system.

3. Its own air supply for the component cooling water valve operators in the event of a failure.

4.1.3. Air Supply System Quantitative Analysis

The RFBD was used to estimate the failure rate (λ) and the MTTR from which the air supply system failure probabilities could be determined.

As indicated by the RFBD, the air supply system consists of three independent air compressing loops, a header manifold, and two independent headers. Thus the λs and MTTRs for each of the three portions are required. Excluding the support systems, the following λs and MTTRs were estimated from the air supply system:

		Per Loop Estimates			
		λ_D	$MTTR_D$	λ_t	$MTTR_t$
Compressor, etc.	Triple Failures	$3.2 \times 10^{-3}/D$ [a]	24	3.2×10^{-4}/hr	36
Manifold	Single Failures	--	--	6.1×10^{-6}/hr	24
Header	Double Failures	$3.0 \times 10^{-4}/D$ [b]	24	1.2×10^{-5}/hr	24

[a] Estimate for one compressor cycling, including motor breaker.
[b] Estimate for valve cycling when switching-in standby header.

The greatest contributor for the compressor loop demand failure rate was the compressor and its breaker. This was estimated to be $3 \times 10^{-3}/D$, or about 93% of the λ_D.

The greatest contributor for the compressor loop running failure rate was the compressor "fail-to-operate." This was estimated to be 3×10^{-4}/hr, or about 93% of the λ_t.

The greatest contributors for the manifold headers were the isolation valves' rupture or excessive leak. This was estimated to be 6×10^{-6}/hr, or about 98% of the running λ_t.

The greatest contributors for the air header demand failure rate, given a required header switch-in, were four required manual valves. The four valves contributed to all of the λ_D.

The greatest contributor to the running failure rate for a header was the pressure safety valve premature opening. This was estimated to be 1×10^{-5}/hr, or about 83% of the λ_t.

Based upon the standard reliability approximations given in Appendix A the following system failure rates may be calculated:

	System Failure Rate (Λ_t)
Triple Failures	9.8×10^{-9}/hr
Double Failures	7.2×10^{-9}/hr
Single Failures	6.1×10^{-6}/hr
Total	6.1×10^{-6}/hr

The system single failure point dominates the system failure rate. Based upon a system operating time of 8760 hr/yr, the calculated system failure probability is 5.2×10^{-2}/yr. As the FMEA in Table 4-2 shows, the time during which the MLCS can operate without a control air supply is short in comparison to air supply system repair times. The probability of a control air supply failure, causing MLCS failure, may therefore be estimated at 5×10^{-2}/yr.

4.1.4. Air Supply System Design Improvements

The following design improvements to the air supply system to enhance the MLCS reliability are suggested:

Improvement	Reliability Effect
1. Eliminate single failure points: common air manifold header.	1. Increases the number of success paths, thus increasing reliability or decreasing failure probability.
2. Incorporate an active redundant air header A&B system instead of a local manual standby redundant system or add a separate air supply (i.e., pressurized air bottle) for the key MLCS valves.	2. Will give at least two constant air supplies to each key MLCS component.

4.1.5. Air Supply System Areas for Further Studies

None.

4.2. NON-CLASS IE (NONESSENTIAL) ELECTRIC POWER SYSTEM

4.2.1. Description

The principal function of the Non-Class IE power system is to provide electrical power to the nonsafety systems or to the operational portion of the plant. This system is a non-Category I seismic system.

There are two 4160-volt buses that are independent of each other. There are two 480-volt load centers, one for the turbine building and one for the circulating water cooling tower. Each is arranged as a double ended substation with a bus tie circuit breaker. The bus tie breaker is open in normal operation. In case of a failure of one of the supplies, an automatic transfer to the other one will take place. Each load center transformer is sized to carry the full load of both bus sections. Motor control centers are supplied from the 480-volt load centers.

There are two non-Class IE storage batteries, a 125-volt battery and a 250-volt battery. The 125-volt battery supplies power for switchgear control, annunciators, and indicating lights for the nonessential systems.

It is sized to trip all circuit breakers required, to carry the annunciators and indicating lights for 4 hr, and then to close all circuit breakers required.

During normal plant operation, the non-Class IE buses are supplied by the main generator through the unit auxiliary transformer (also supplying the Class IE buses) with the off-site power (OSP) supplied through the reserve auxiliary transformer as a backup. With the loss of the generator, only the OSP can supply electric power to the non-Class IE buses.

4.2.2. Qualitative Analysis

An RFBD (Fig. 4-2, sheets 1 and 2) was developed for the non-Class IE system. An FMEA of this system on MLCS operation is given in Table 4-2. For RHR, the two non-Class IE buses are independent of and redundant to each other except for the single normally open circuit breaker tying the 480-volt buses.

The non-Class IE buses are assumed to operate from plant operation to RHR mode as follows:

1. During normal plant operation, these buses are supplied by the main generator through the unit auxiliary transformer (UAT) and a normally closed (NC) circuit breaker to each bus. The OSP through the reserve auxiliary transformer (RAT) and a normally-opened (NO) circuit breaker to each bus are on standby.

2. Following a loss of off-site power, the turbine generator can supply in-house loads without causing plant trip.

3. When a generator trip occurs, a circuit breaker in the switchyard opens; the NC circuit breaker will then automatically open and the NO circuit breaker will automatically close. This transfer is designed to occur without load losses.

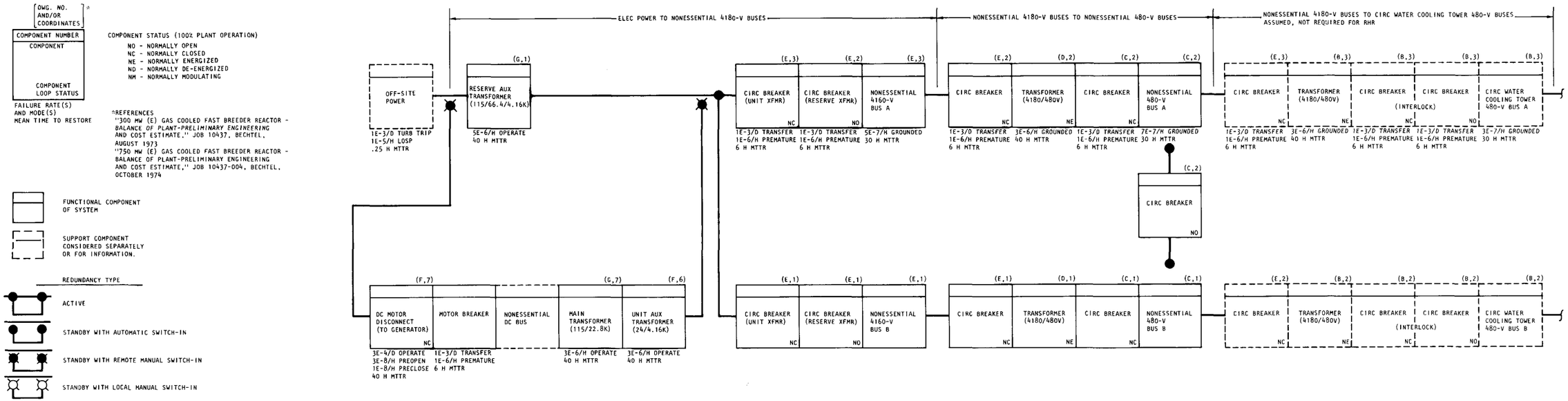


Fig. 4-2. GCFR nonessential dc electric power bus reliability function diagram for RHR (Drawing E102), sheet 1 of 2

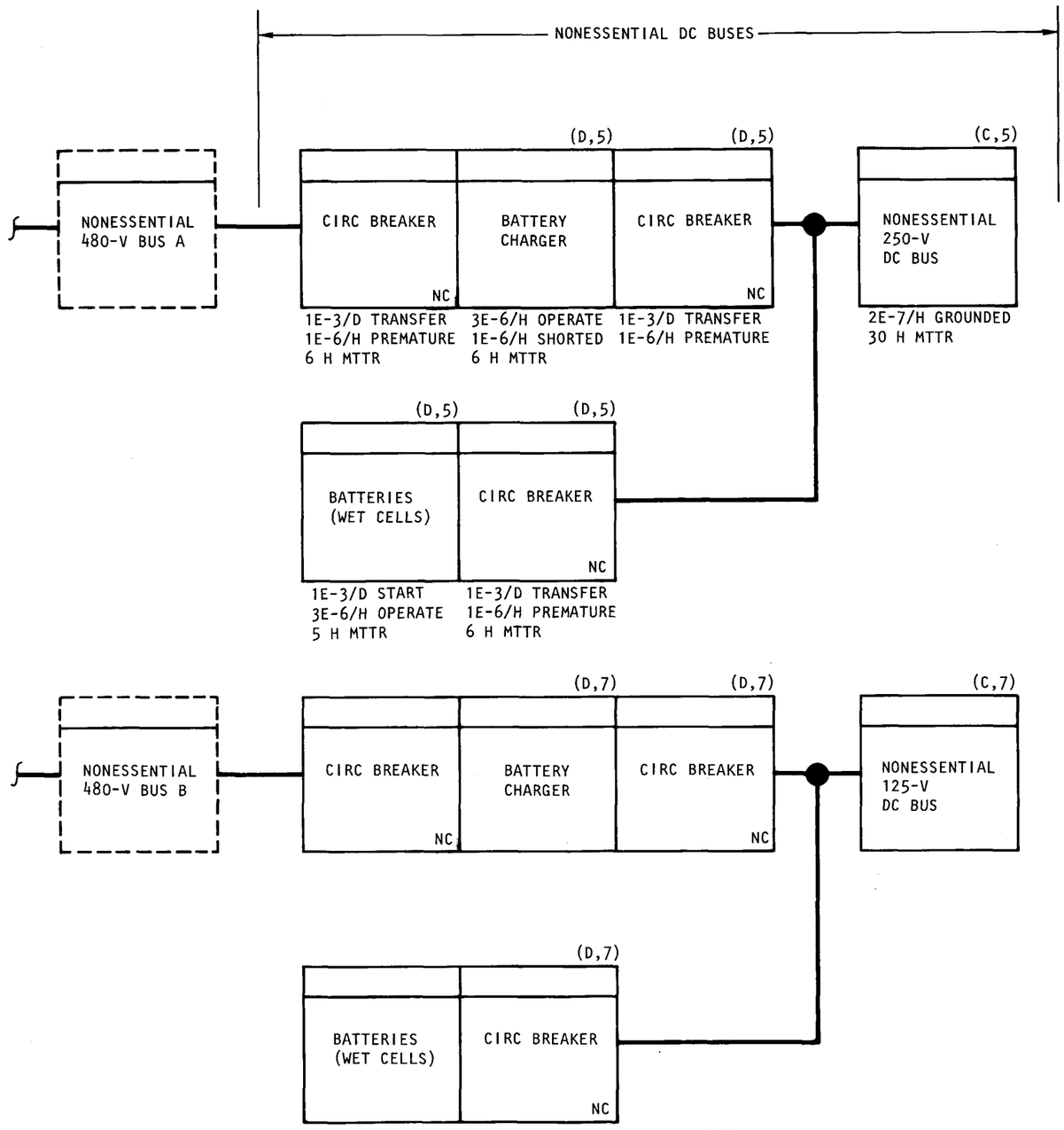


Fig. 4-2. GCFR nonessential dc electric power bus reliability function diagram for RHR (Drawing E102), sheet 2 of 2

4. After the transfer, the NC dc motor-disconnect may be remote-manually opened and the switchyard circuit breaker closed, thus placing the UAT and main transformer on automatic standby to the RAT.

5. The 125-volt and 250 volt dc buses are normally supplied from the 480-volt motor control center through an ac or dc converter (battery charger). Each dc bus is backed up with wet cell batteries.

Thus, for the non-Class IE buses to operate during RHR, the following are required:

1. Off-site power.

2. Proper transfer of the breakers in at least one of two buses, excluding the switchyard circuit breaker.

3. Continued operation of the balance of the system.

The non-Class IE buses provide power to the following systems during the MLCS decay heat removal mode:

1. Auxiliary steam supply system, which supplies auxiliary steam to the MLCS.

2. Condensate system, which provides makeup water for the shutdown feedwater storage tanks.

3. Circulating water system, which provides cooling water to the condenser.

4.2.3. Quantitative Analysis

The RFBD (Fig. 4-2, sheets 1 and 2) was used to estimate the failure rates (λ) and the MTTR from which the failure probabilities could be determined.

As indicated by the RFBD (in Fig. 4-2, sheet 1) the non-Class IE ac system consists of two independent buses and two transformers from which the off-site power can be supplied to the buses. The following λs and MTTRs were estimated for the non-Class IE ac system:

	Per Loop Estimates			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Plant Initially Operating				
Off-site power	10^{-3}/D	1/4 hr	10^{-6}/hr[(a)]	1/4 hr
ac buses (redundant)	2×10^{-3}/D	6 hr	8.2×10^{-6}/hr	22 hr
Plant Initially Shut Down				
Off-site power	--	--	10^{-5}/hr	1/4 hr
ac buses (redundant)	--	--	8.2×10^{-6}/hr	22 hr

[(a)] The turbine generator failing to maintain in-house loads was estimated to be 10^{-1} per loss of off-site power based upon British GCR experience. Thus the λ_t for the OSP was estimated to be $10^{-1} \times 10^{-5}$/hr = 10^{-6}/hr.

The greatest contributor to the failure rates was estimated to be the OSP, because it was assumed to be a single failure point.

The total contribution of 2×10^{-3}/d to the loop demand failure rate was from the two circuit breaker "fail-to-transfers," transfer being required when switching from house power to the OSP.

The greatest contributor to a loop running failure rate was the load center transformer. This was estimated to be 3×10^{-6}/hr, or about 37% of the λ_t. The four inter-tie circuit breakers, each with a failure rate of 1×10^{-6}/hr for premature transfer, contributed 4×10^{-6}/hr, or about 49% of the λ_t.

The circulating water tower 480-volt buses (for fans) were assumed to be not required for the RHR because the heat capacity of the water and the natural draft in the cooling towers were assumed to be adequate.

As indicated by the RFBD in Fig. 4-2, sheet 2, the non-Class IE dc system consists of a 125-volt dc subsystem and a 250-volt dc subsystem. Each dc subsystem is normally supplied from one of the 480-volt load control center buses with back-up batteries. The following λs and MTTRs were estimated for each of the non-Class IE dc subsystems:

	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Battery Charger (redundant)	--	--	5×10^{-6}/hr	6
Batteries (redundant)	1×10^{-3}/D	5	4×10^{-6}/hr	5
DC Bus	--	--	2×10^{-7}/hr	30

The greatest contributor to the charger circuit failure rate was estimated to be the battery charger "fail-to-operate" at 3×10^{-6}/hr, or about 60% of the λ_t.

The greatest contributor to the battery circuit failure rate was estimated to be the batteries for all of the demand failure rate, λ_D, and 75% of the running failure rate, λ_t.

The inadvertent grounding of the two breakers, each at 1×10^{-7}/hr, contributed to the total estimated bus failure rate.

Based upon the standard reliability approximations given in Appendix A, the following system failure rates may be calculated for the non-Class IE systems:

	System Failure Rate	
	Λ_D	Λ_t
Plant Initially Operating		
Off-site power	1×10^{-3}/D	1×10^{-6}/hr[a]
Buses	4×10^{-6}/D	2×10^{-7}/hr
Total	1×10^{-3}/D	1.2×10^{-6}/hr
Plant Initially Shut Down		
Off-site power	--	1×10^{-5}/hr
Buses	--	2×10^{-7}/hr
Total	--	1×10^{-5}/hr

[a] It was estimated that the turbine generator failing to maintain in-house loads to be 10^{-1} per loss of OSP. Thus the λ_t for OSP was estimated to be $10^{-1} \times 10^{-5}$/hr = 10^{-6}/hr.

It may be seen that the ac system single failure point (off-site power) dominates the system failure rate. Based on the plant operating 80% of the year with three reactor trip demands per year, one system failure probability would be 2.7×10^{-2}/yr. As may be noted from the FMEA in Table 4-2, the time during which the MLCS can operate without nonessential power is approximately 30 min or twice the mean restoration time of off-site power. Allowing for this grace period, the probability of nonessential power failure causing MLCS failure is approximately 4×10^{-3}/yr.

4.2.4. Design Improvements

The following design improvements to enhance MCLS reliability in the non-Class IE system are suggested:

Improvement	Reliability Effect
1. Replace the remote-manual motor disconnect with a quick disconnect circuit breaker to isolate the main generator.	1. Only one circuit breaker will be required to operate instead of two circuit breakers for each loop. In addition, the two circuit breakers in each loop are still on a standby mode with an automatic switch-in to provide power to each loop.

4.2.5. Areas for Further Studies

None.

4.3. AUXILIARY STEAM SUPPLY SYSTEM

4.3.1. Description

The auxiliary steam supply system provides steam to drive the main helium circulator turbines and the bearing water pump turbines during plant startup and during decay heat removal operations following a reactor shutdown. This system is a non-Category I system.

Three oil-fired auxiliary boilers, each with its own feedwater pump and fuel oil pump, provide steam to the three main helium circulator loops. During normal plant operation, the auxiliary boilers are on hot standby and can attain rated conditions in about 20 min. Feedwater is supplied from the condenser hot well, and fuel oil is supplied from two 100,000 gallon fuel oil storage tanks. Each feedwater pump normally supplies an individual boiler; however, by proper valve manipulations, any one of the three can provide feedwater to any one of the boilers. Similarly, any one of the three boilers can provide auxiliary steam to any one of the main circulator and bearing water turbines.

4.3.2. Qualitative Analysis

An RFBD (Fig. 4-3, sheets 1 through 3) was developed for the auxiliary steam supply system. An FMEA of this system on MLCS operation is given in Table 4-2. The auxiliary steam was assumed to operate as follows:

1. The auxiliary boilers are on hot standby in a quick restart condition.

2. Shortly after a plant shutdown, about 1 min, the auxiliary steam supply systems are started (Fig. 4-3, sheets 1 and 2). The

boilers can attain rated conditions in about 20 min. Assuming that transition from the core residual heat steam to auxiliary steam is easily and quickly accomplished, the auxiliary boilers may be started as much as 10 min after plant shutdown.

3. The steam generator alternate discharge circuit in each loop is established (Fig. 4-3, sheet 3).

   a. The normally closed containment isolation valve must open.

   b. The pressure controller and the pressure control valve will reduce the steam generator pressure to about 0.3 MPa (50 psia).

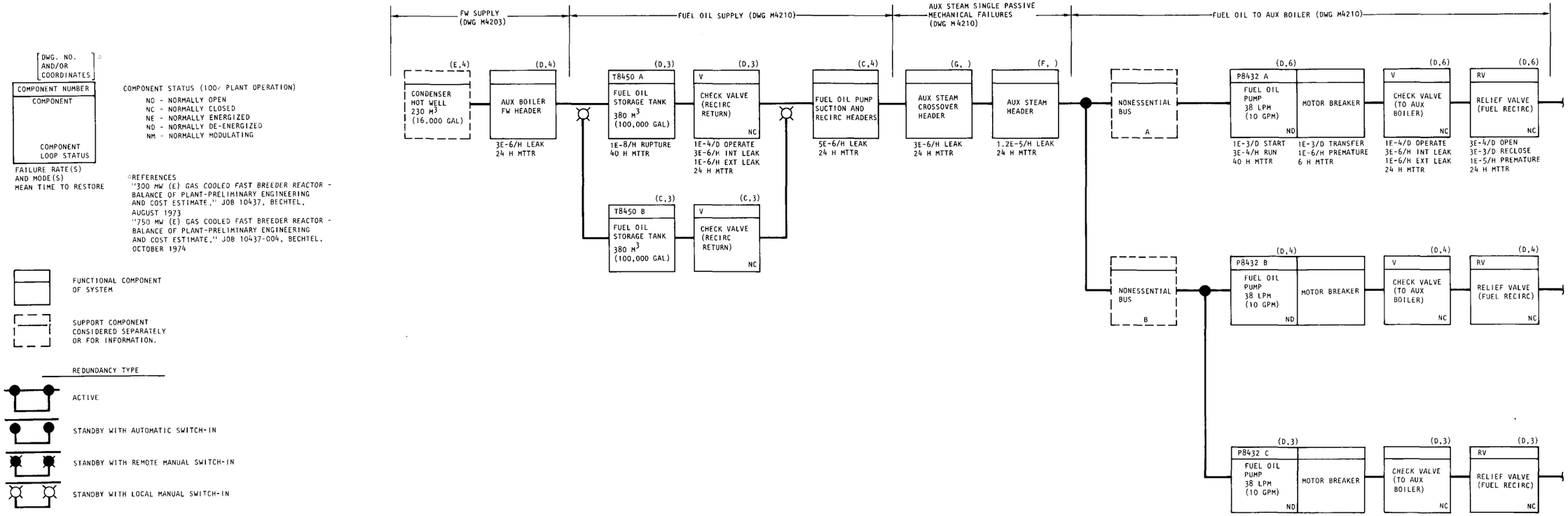
   c. Heat rejection is through the normal power conversion system components, or, if necessary, for a limited time by direct steam relief to the atmosphere through four pressure relief valves.

No single active failure was uncovered in the auxiliary steam supply system.

Four areas of single passive mechanical failures (Fig. 4-3, sheet 1) are:

1. Auxiliary boiler feedpump suction header.
2. Fuel oil pump suction and recirculating headers.
3. Auxiliary steam crossover header.
4. Auxiliary steam header.

4.3.2.1. Auxiliary Steam Supply Support Systems. The auxiliary steam supply system requires the following support systems to perform its function:



[DWG. NO. AND/OR COORDINATES]

COMPONENT NUMBER
COMPONENT
COMPONENT LOOP STATUS
FAILURE RATE(S) AND MODE(S) MEAN TIME TO RESTORE

COMPONENT STATUS (100% PLANT OPERATION)

NO - NORMALLY OPEN
NC - NORMALLY CLOSED
NE - NORMALLY ENERGIZED
ND - NORMALLY DE-ENERGIZED
NM - NORMALLY MODULATING

*REFERENCES

"300 MW (E) GAS COOLED FAST BREEDER REACTOR - BALANCE OF PLANT-PRELIMINARY ENGINEERING AND COST ESTIMATE," JOB 10437, BECHTEL, AUGUST 1973

"750 MW (E) GAS COOLED FAST BREEDER REACTOR - BALANCE OF PLANT-PRELIMINARY ENGINEERING AND COST ESTIMATE," JOB 10437-004, BECHTEL, OCTOBER 1974

FUNCTIONAL COMPONENT OF SYSTEM

SUPPORT COMPONENT CONSIDERED SEPARATELY OR FOR INFORMATION.

REDUNDANCY TYPE

ACTIVE

STANDBY WITH AUTOMATIC SWITCH-IN

STANDBY WITH REMOTE MANUAL SWITCH-IN

STANDBY WITH LOCAL MANUAL SWITCH-IN

Fig. 4-3. GCFR auxiliary steam supply system reliability function diagram, sheet 1 of 4

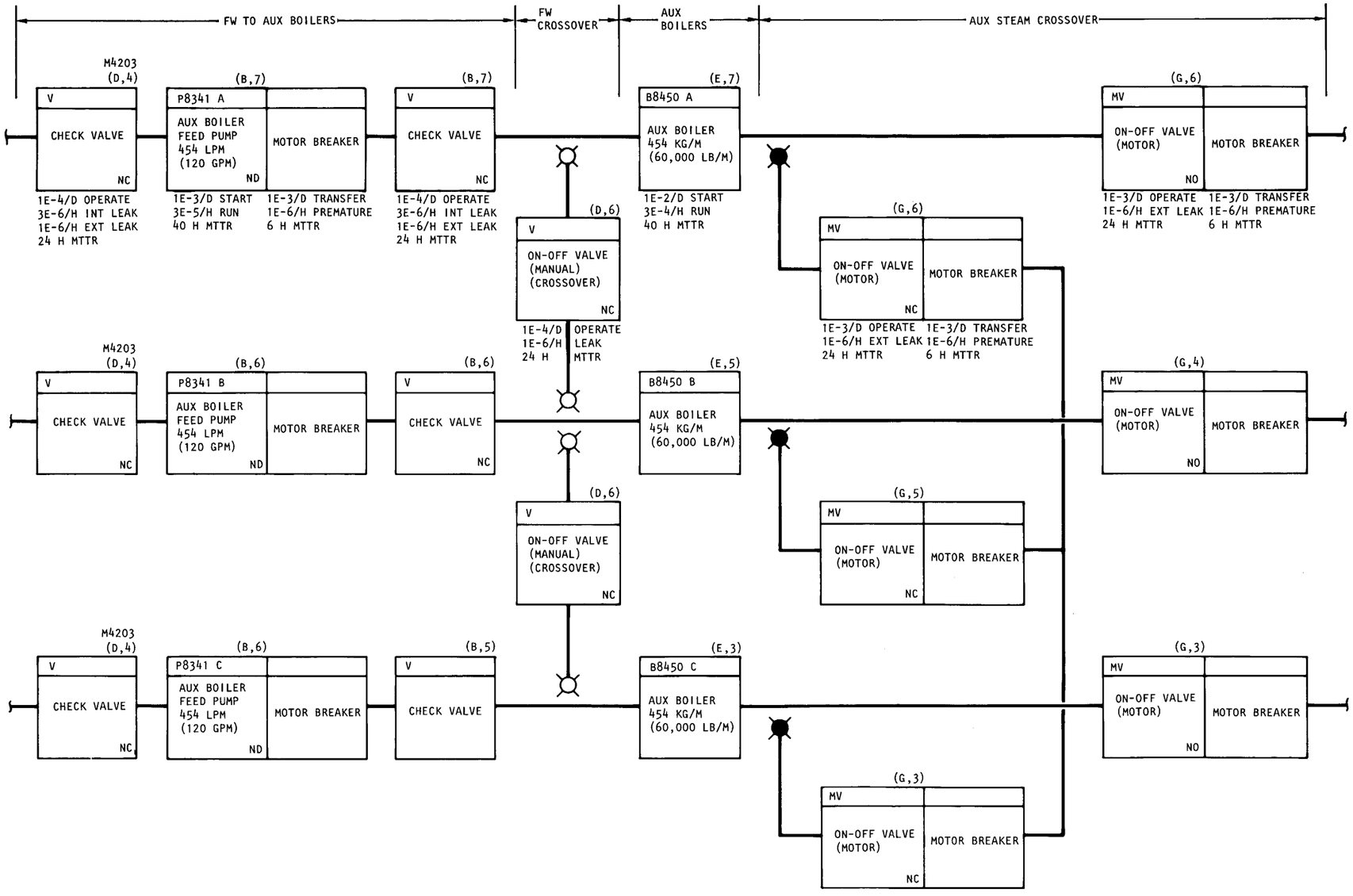


Fig. 4-3. GCFR auxiliary steam supply system reliability function diagram, sheet 2 of 4

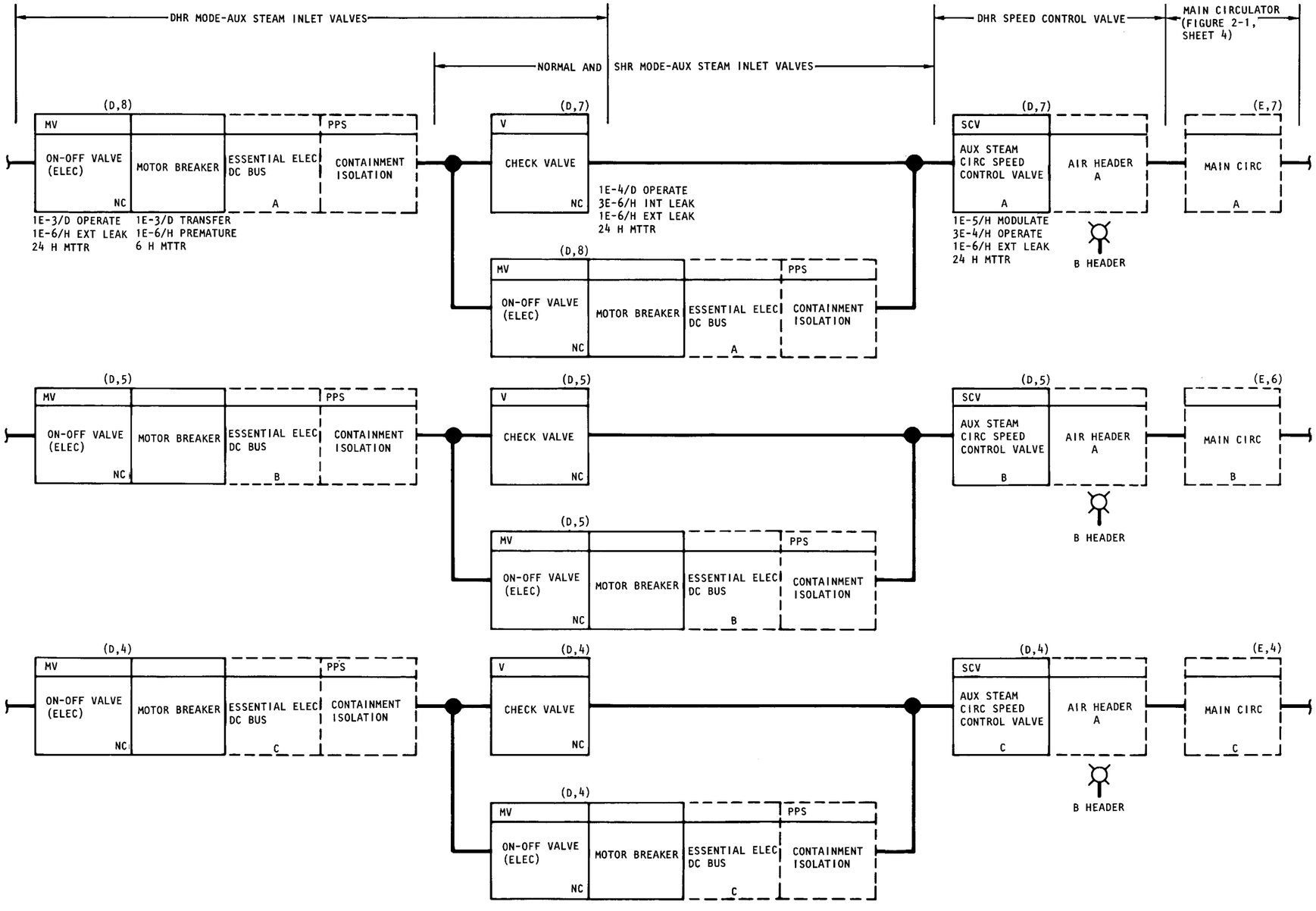


Fig. 4-3. GCFR auxiliary steam supply system reliability function diagram, sheet 3 of 4

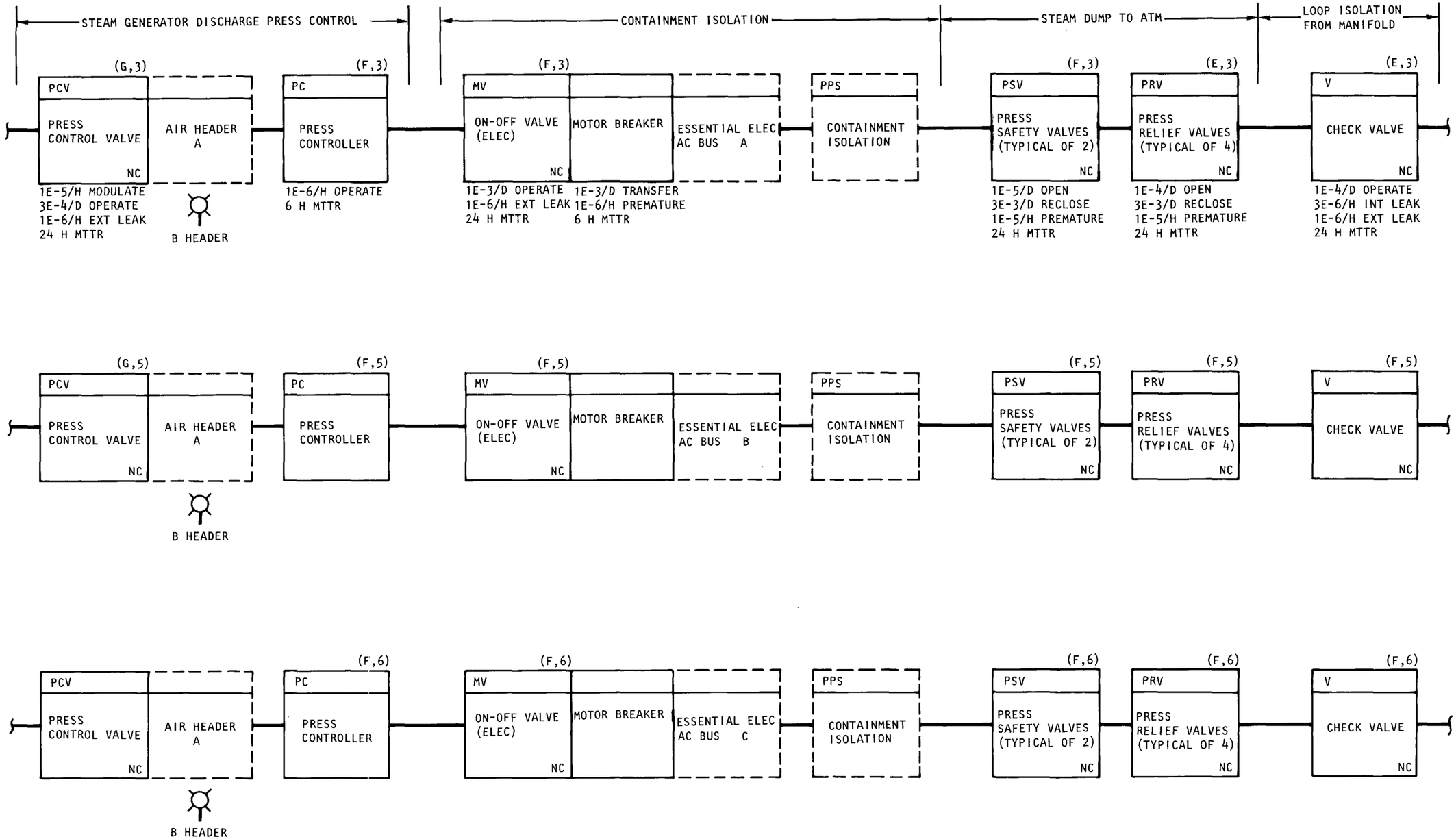


Fig. 4-3. GCFR auxiliary steam supply system reliability function diagram, sheet 4 of 4

1. The non-Class IE buses (nonessential) (Fig. 4-3, sheet 1), as described in Section 4.1, provide electric power to drive the feedwater and fuel oil pumps.

2. The condenser hot well (Fig. 4-3, sheet 1), a portion of the power conversion system as described in Section 4.4, provides the feedwater.

3. The Class IE buses (essential) (Fig. 4-3, sheet 3), as described in Section 4.6, provide power to the containment isolation valve.

4. The air supply system (Fig. 4-3, sheet 3), as described in Section 4.1, provides air power to the pressure control valve and possibly to the pressure controller.

4.3.3. Quantitative Analysis

The RFBD was utilized to estimate the failure rates (λ) and the MTTR from which the auxiliary steam supply system failure probabilities could be estimated.

As indicated by the RFBD, the auxiliary steam supply consists of portions that have single, double, and triple failure areas. The λs and MTTRs for one loop in each of these areas (excluding the support systems) were estimated as follows:

	Per Loop Estimate			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Single Failures	--	--	2×10^{-5}/hr	24
Double Failures	--	--	1×10^{-6}/hr	24
Triple Failures	2×10^{-2}/D	31	7.4×10^{-4}/hr	38

The greatest contributor to the single running failure rate was valve external leak, with an estimated failure rate of 1×10^{-6}/hr. Twenty

valves in the various single headers contributed cumulatively to the significant total λ_ts. The less significant portion consisted of pipe rupture, estimated to be at least two orders of magnitude less than valve leaks.

For the double running failure rate, the tank shut-off valve external leaks, with an estimated failure rate of 1×10^{-6}/hr, contributed most significantly to the total of the λ_t.

The greatest contributor to the triple demand failure rate was the auxiliary boiler "fail-to-start." This was estimated to be 1×10^{-2}/D, or about 50% of the λ_D.

The greatest contributors to the triple running failure rate were the auxiliary boiler and positive displacement fuel oil pump fail-to-operate. These were both estimated to be 3×10^{-4}/hr each, or about 40% each of the λ_t.

Based upon the standard reliability approximations given in Appendix A, the following system failure rates may be calculated:

	System Failure Rates	
	Λ_D	Λ_t
Triple Failures	8.0×10^{-6}/D	1.7×10^{-6}/hr
Double Failures	0.0	4.8×10^{-11}/hr
Single Failures	0.0	2.0×10^{-5}/hr
Total	8.0×10^{-6}/D	2.2×10^{-5}/hr

The system single failure point dominates the system hourly failure rate. Based upon a system operating time of 1752 hr (20% of a year) and three reactor trip demands per year, the system failure probability is 3.8×10^{-2}/yr. As the FMEA in Table 4-2 shows, the time during which the MLCS can operate without an auxiliary steam supply is short in comparison to auxiliary steam system repair times. The probability of an auxiliary steam supply system failure causing MLCS failure may therefore be estimated at 4×10^{-2}/yr.

1. The non-Class IE buses (nonessential) (Fig. 4-3, sheet 1), as described in Section 4.1, provide electric power to drive the feedwater and fuel oil pumps.

2. The condenser hot well (Fig. 4-3, sheet 1), a portion of the power conversion system as described in Section 4.4, provides the feedwater.

3. The Class IE buses (essential) (Fig. 4-3, sheet 3), as described in Section 4.6, provide power to the containment isolation valve.

4. The air supply system (Fig. 4-3, sheet 3), as described in Section 4.1, provides air power to the pressure control valve and possibly to the pressure controller.

4.3.3. Quantitative Analysis

The RFBD was utilized to estimate the failure rates (λ) and the MTTR from which the auxiliary steam supply system failure probabilities could be estimated.

As indicated by the RFBD, the auxiliary steam supply consists of portions that have single, double, and triple failure areas. The λs and MTTRs for one loop in each of these areas (excluding the support systems) were estimated as follows:

	Per Loop Estimate			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Single Failures	--	--	2×10^{-5}/hr	24
Double Failures	--	--	1×10^{-6}/hr	24
Triple Failures	2×10^{-2}/D	31	7.4×10^{-4}/hr	38

The greatest contributor to the single running failure rate was valve external leak, with an estimated failure rate of 1×10^{-6}/hr. Twenty

valves in the various single headers contributed cumulatively to the significant total λ_ts. The less significant portion consisted of pipe rupture, estimated to be at least two orders of magnitude less than valve leaks.

For the double running failure rate, the tank shut-off valve external leaks, with an estimated failure rate of 1×10^{-6}/hr, contributed most significantly to the total of the λ_t.

The greatest contributor to the triple demand failure rate was the auxiliary boiler "fail-to-start." This was estimated to be 1×10^{-2}/D, or about 50% of the λ_D.

The greatest contributors to the triple running failure rate were the auxiliary boiler and positive displacement fuel oil pump fail-to-operate. These were both estimated to be 3×10^{-4}/hr each, or about 40% each of the λ_t.

Based upon the standard reliability approximations given in Appendix A, the following system failure rates may be calculated:

	System Failure Rates	
	Λ_D	Λ_t
Triple Failures	8.0×10^{-6}/D	1.7×10^{-6}/hr
Double Failures	0.0	4.8×10^{-11}/hr
Single Failures	0.0	2.0×10^{-5}/hr
Total	8.0×10^{-6}/D	2.2×10^{-5}/hr

The system single failure point dominates the system hourly failure rate. Based upon a system operating time of 1752 hr (20% of a year) and three reactor trip demands per year, the system failure probability is 3.8×10^{-2}/yr. As the FMEA in Table 4-2 shows, the time during which the MLCS can operate without an auxiliary steam supply is short in comparison to auxiliary steam system repair times. The probability of an auxiliary steam supply system failure causing MLCS failure may therefore be estimated at 4×10^{-2}/yr.

4.3.4. Design Improvements

The following design improvement to enhance reliability of the auxiliary steam supply system is suggested:

Suggested Improvement	Reliability Effect
Eliminate single failure points:	
a. Common feedwater suction header.	a. Will increase the number of success paths and make loops independent of each other.
b. Common fuel oil suction and recirculation header.	b. Same as a.
c. Steam header cross-over header. (Use double valves.)	c. Will make loops independent of each other.
d. Auxiliary header. (Use double valves.)	d. Same as c.

4.3.5. Areas for Further Studies

None.

4.4. POWER CONVERSION SYSTEM (PCS)

4.4.1. Description

The PCS consists of the condensate and feedwater system and the circulating water system. The condensate and feedwater system takes condensate from the main condenser hotwell and delivers it as feedwater to the nuclear steam supply system during normal plant operation and to the shutdown feedwater circuit during RHR. It also provides the feedwater source for the auxiliary boiler system. The circulating water system provides the heat rejection for the turbine cycle during normal operation and for the MLCS during RHR. Except for the shutdown feedwater circuit, these systems are non-Category I.

For RHR, the condensate and feedwater system consists of the condensate pumps and condensate storage tank, which provide makeup water to the shutdown feedwater storage tank. The circulating water system consists of the condenser, the circulating water pumps, and the mechanical draft cooling tower, which provide the long term closed-loop heat removal system for the MLCS.

4.4.2. PCS Qualitative Analysis

An RFBD was drawn for the condensate system (Fig. 4-4, sheets 1 and 2), for the circulating water system (Fig. 4-5, sheets 1 and 2), and for the desuperheaters in the resuperheater bypass and steam generator alternate discharge circuits (Fig. 4-6, sheet 1). An FMEA of this system on MLCS operation is given in Table 4-2.

Except for the desuperheaters, these systems normally operate during plant operation, and, for 100% plant operation, all the major active equipment items operate. Thus, when the plant is shut down, these active equipment items, primarily pumps and fans, will continue to operate without any startup if off-site power is available. The only valves requiring change-of-state are the condensate pump recirculation valves in each condensate pump loop (Fig. 4-4, sheet 1), the hotwell overfill bypass valve (Fig. 4-4, sheet 2), which will return the condensate water back to the condensate storage tank, and the makeup water valves in each of the shutdown feedwater storage tanks (Fig. 4-4, sheet 2).

During a normal plant shutdown, the feedwater makeup will be started shortly after the shutdown feedwater pumps are started. As discussed in Section 2.2.1, the shutdown feedwater pumps are started in about 1 min after plant shutdown, but this time is not critical. With the steam generator inventory and the shutdown feedwater storage tank inventory, it was assumed that the feedwater makeup to the MLCS, as indicated on a portion of Fig. 4-4, sheet 1, and all of sheet 2, is not required for about 30 min.

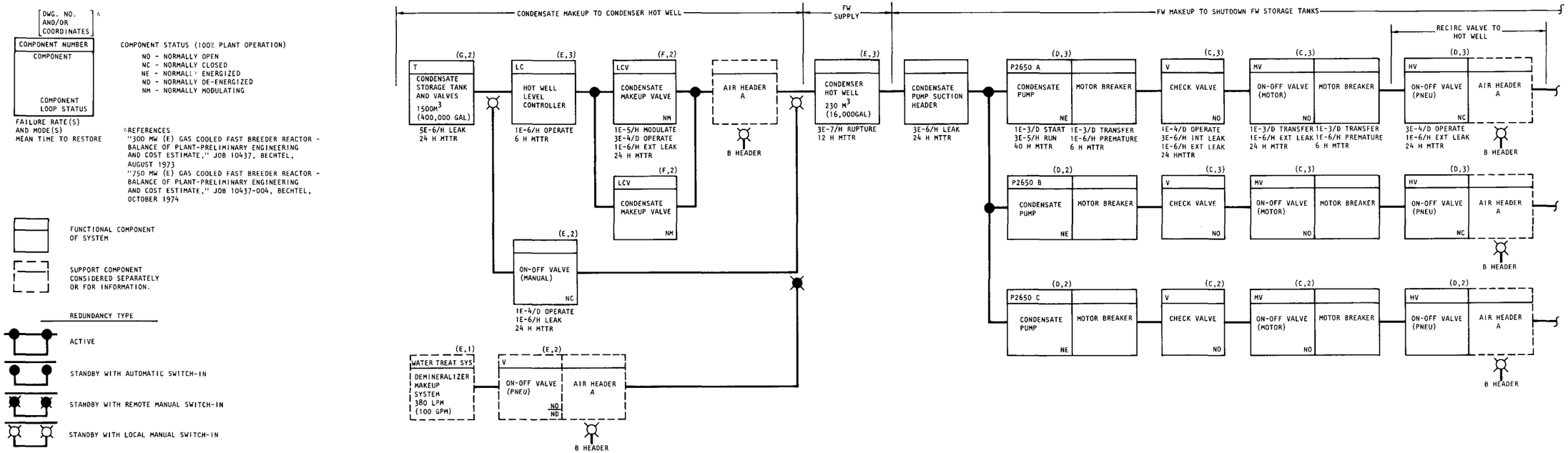


Fig. 4-4. GCFR condensate and feedwater system reliability function diagram for RHR, sheet 1 of 2

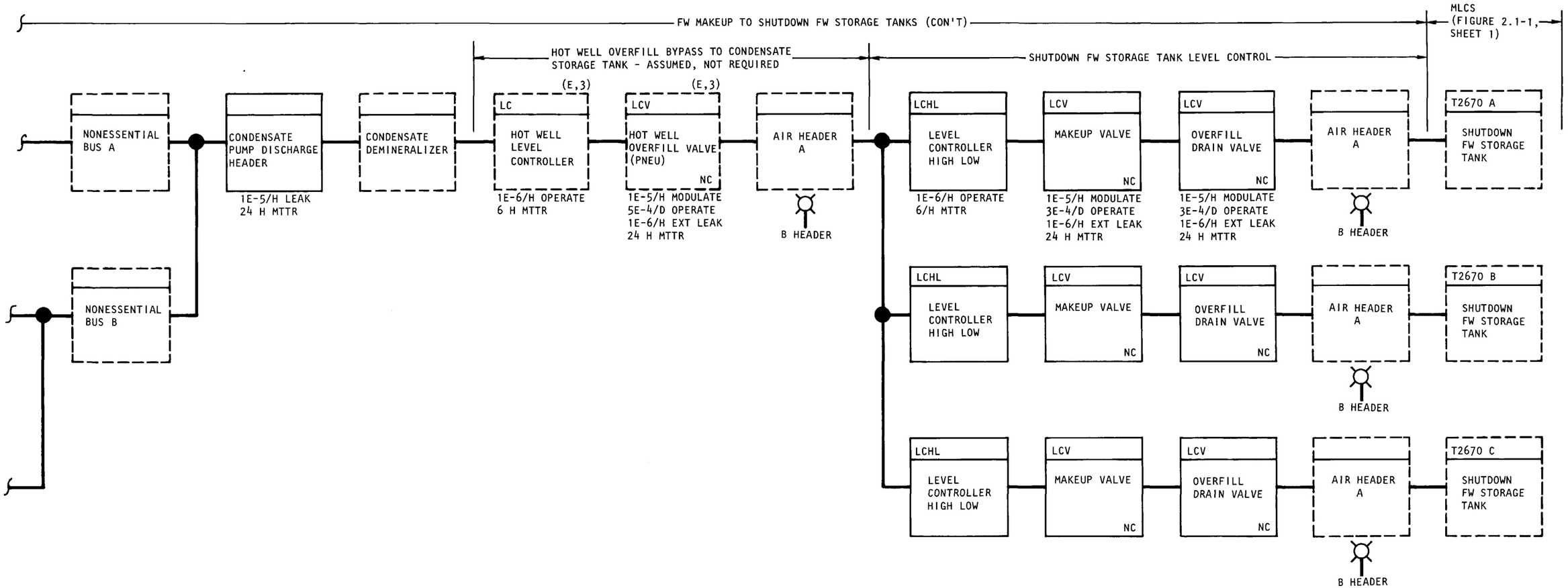


Fig. 4-4. GCFR condensate and feedwater system reliability function diagram for RHR (Drawing M4203), sheet 2 of 2

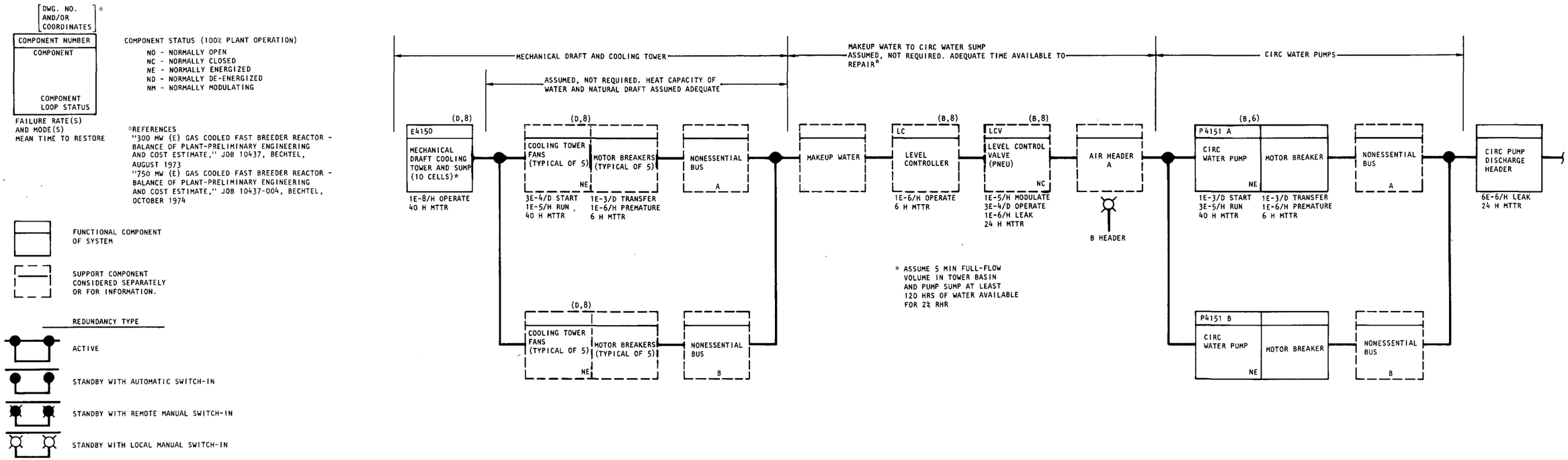


Fig. 4-5. GCFR circulating water system reliability function diagram (Drawing M204), sheet 1 of 2

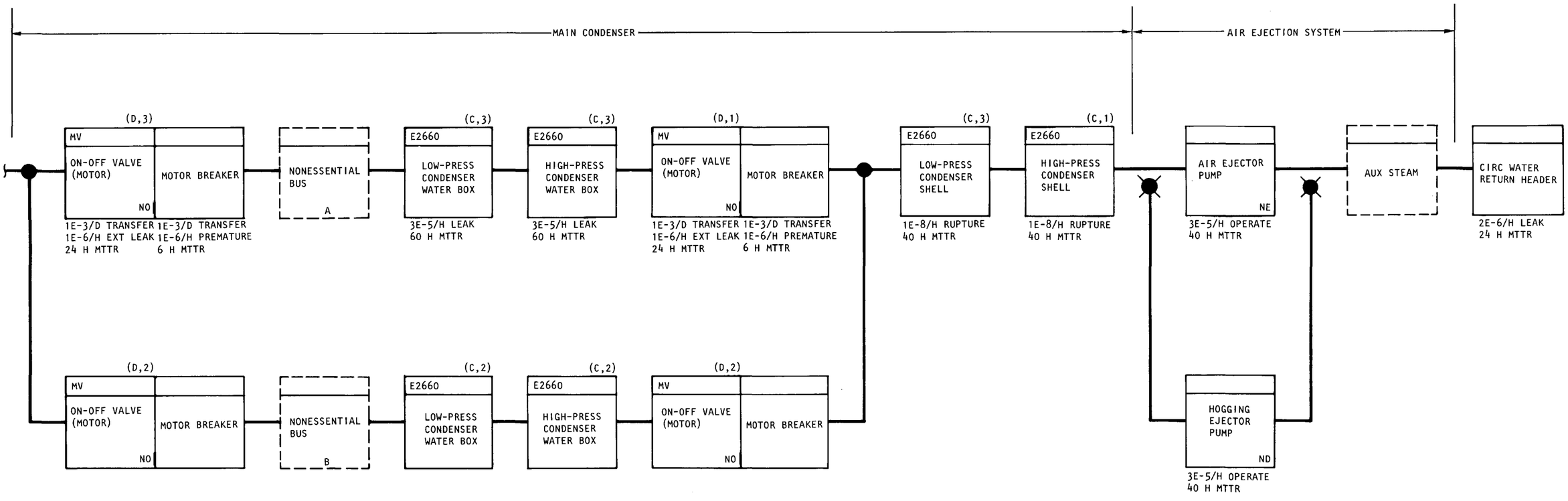


Fig. 4-5. GCFR circulating water system reliability function diagram (Drawing M204), sheet 2 of 2

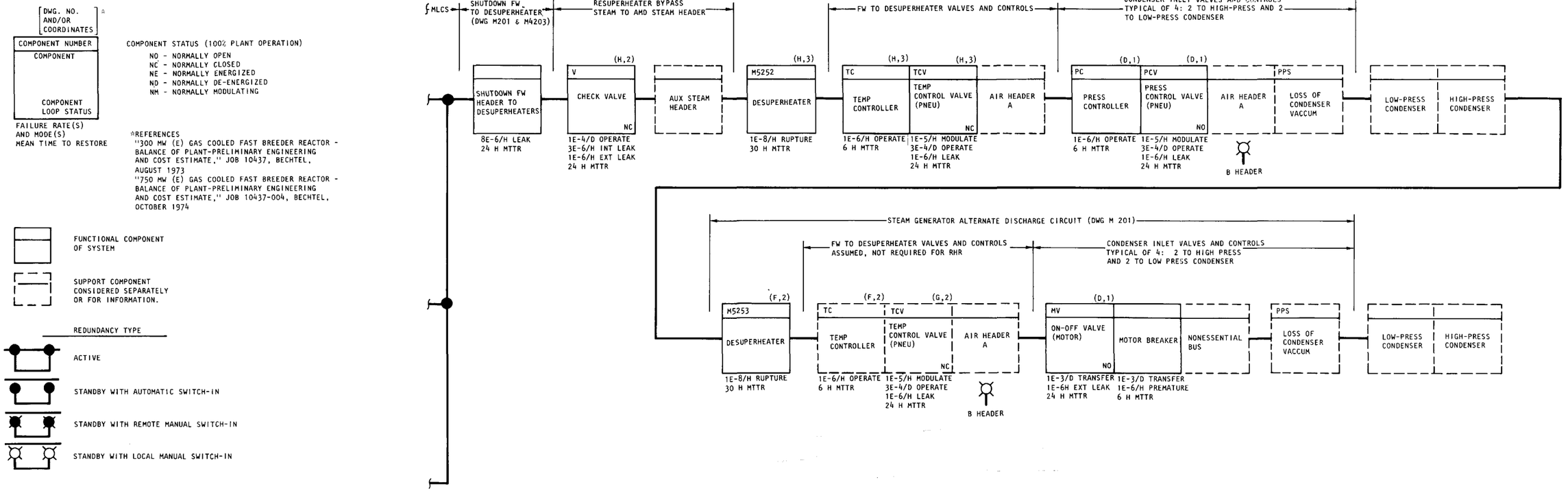


Fig. 4-6. GCFR resuperheater bypass and steam generator alternate discharge circuit reliability function diagram for RHR

The condenser hotwell supplies feedwater directly to the auxiliary steam supply system (Fig. 4-3, sheet 1) and, via the condensate pumps, to the shutdown feedwater storage tanks (Fig. 4-4). With the steam generator inventory, about 1 hr of RHR with the MLCS can be accomplished without makeup to the hotwell. With the available makeup water to the hotwell from the condensate storage tank, the demineralizer storage tank, and the demineralizer makeup system, a conservative figure of 21 added hours of operation was estimated before the MLCS would have to close the PCS loop. Thus heat rejection to the atmosphere could last for about 22 hr before the PCS loop would have to be closed to maintain RHR with the MLCS.

For the long-term RHR with a closed loop, the circulating water system and the main condenser are required to function. In addition, the resuperheater bypass circuit with its desuperheater must be operable, and the steam generator alternate discharge circuit (assuming the desuperheater in this circuit is not required for RHR) must remain intact.

A few active single failures and many passive mechanical failures were noted in the PCS. Assuming heat rejection to the atmosphere during the first 22 hr of RHR, one single active failure point of an automatic component exists in the makeup water to the condenser hotwell (Fig. 4-4, sheet 1). However, with the hotwell inventory, which contains at least 30 min of supply during RHR, and with the capability to add remotely (by hand) about 100 gpm from the demineralizer makeup system and the shutdown feedwater storage tank inventory, adequate time is indicated to be available to open the local manual bypass valve thus circumventing the controller and control valves to provide makeup to the hotwell.

During this period of heat rejection to the atmosphere, the following single passive mechanical failure points are indicated (Fig. 4-4, sheets 1 and 2):

1. Condensate storage tank and two on-off manual valves.
2. Condenser hotwell.
3. Condensate pump suction header.
4. Condensate pump discharge header.

For the long term RHR mode when the closed-loop secondary water system is required, the components as shown in Figs. 4-5 and 4-6 are required to function. One single active failure point indicated is the feedwater control to the resuperheater bypass desuperheater (Fig. 4-6, sheet 1). Steam of a higher temperature than desirable will enter the condenser, possibly causing some thermal expansion problems; however, the basic function of the condenser will not be lost. Thus, time is available to start the CACS without immediate need for the steam.

During long term RHR with the closed-loop secondary water system, the following single passive mechanical failure points were indicated (Figs. 4-5 and 4-6) in addition to those indicated in Fig. 4-4:

1. Circulating pump discharge header.

2. L.P. condenser shell.

3. H.P. condenser shell.

4. Circulating pump return header.

5. Shutdown feedwater header to desuperheaters.

6. Resuperheater bypass desuperheater.

7. Valves in the resuperheater bypass to condenser circuit.

8. Steam generator alternate discharge circuit desuperheater.

9. Valves in the steam generator alternate discharge circuit to condenser circuit.

4.4.2.1. PCS Support Systems. For the PCS to function, the following support systems are required:

1. The non-Class IE ac (nonessential) electrical system, which supplies power to the condensate pumps, the circulating water pumps, and the cooling tower fans.

2. The air supply system for valve actuations and controllers.

3. The auxiliary steam supply for condenser air ejection.

4. The shutdown feedwater, which quenches steam in the resuperheater bypass desuperheater.

4.4.3. PCS Quantitative Analysis

The RFBD were used to estimate the failure rate (λ) and the MTTR from which the PCS's failure probabilities could be determined.

As indicated by the RFBD for the condensate and feedwater system for RHR (Fig. 4-4, sheets 1 and 2), the system consists of single failure points, an alternate path configuration (makeup water to the hotwell), and three independent redundant configurations in two of the functions. The failure rate for the redundant identical level control valve was determined by using a common mode β factor of 0.1 and thus the λ was estimated to be $1 \times 10^{-5}/hr \times 0.1 = 1 \times 10^{-6}/hr$. Excluding the support systems, the following λs and MTTRs were estimated for the condensate and feedwater system for RHR:

	Per Loop Estimate			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Single Failures	--	--	$1.8 \times 10^{-5}/hr$	24
Double Failure				
Normal path	--	--	$2 \times 10^{-5}/hr$	15
Alternate path	$1 \times 10^{-4}/D$	24	(a)	(a)
Triple Failure				
Condensate pump circuit	$3 \times 10^{-4}/D$	24	$3.2 \times 10^{-5}/hr$	38
Shutdown feedwater storage tank level control	$3 \times 10^{-4}/D$	24	$2.1 \times 10^{-5}/hr$	15

(a) Valve leak included in the single failure number.

The greatest contributors for the single failure running failure rate were the valves in the manifolds and headers that will cause the loss of feedwater or the loss of condenser vacuum. A valve failure rate was estimated to be 1×10^{-6}/hr for severe leaks.

The contributors for the normal circuit for the double failure running failure rate were evenly distributed between the controller "fail-to-operate" and the level control valve "fail-to-modulate," each estimated to be 1×10^{-5}/hr.

The contributor for the alternate circuit for the double failure demand failure rate was the local manual on-off valve "fail-to-operate," which was estimated to be 1×10^{-4}/D. The running failure rate of the valve leak was included with the single failure because a severe leak of this valve would cause a loss of condenser vacuum, causing the MLCS to shut down.

The contributor to the condensate pump circuit demand failure rate was the recirculation valve that must be open when the plant is shut down to recirculate condensate to hotwell.

The greatest contributor to the running failure rate for the condensate pump circuit was the condensate pump "fail-to-operate." This was estimated to be 3×10^{-5}/hr, or about 94% of the λ_t.

The contributor to the shutdown feedwater storage tank level control demand failure is the level-control valve "fail-to-open," which is estimated to be 3×10^{-4}/D. The running failure rate is evenly distributed between the level controller "fail-to-operate" and the level control valve "fail-to-modulate," each estimated to be 1×10^{-5}/hr.

As indicated on the RFBD for the circulating water system (Fig. 4-5), this system consists of single failure points and dual redundant independent circuits. Excluding the support systems, the following λs and MTTRs were estimated for the circulating water system for RHR:

	Per Loop Estimates			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Single Failures	--	--	8×10^{-6}/hr	24
Double Failures				
Circulating water pump	--	--	3.1×10^{-5}/hr	39
Condenser water box	--	--	6×10^{-5}/hr	60
Air ejector pumps	--	--	3×10^{-5}/hr	40

The greatest contributor for the single failure running failure rate were the valves in the manifold and headers that would cause the loss of circulating water to cool the condenser. A valve failure rate was estimated to be 1×10^{-6}/hr for severe leaks.

The contributor to the running failure rate for the circulating water pump circuit was the circulating water pump "fail-to-operate." This was estimated to be 3×10^{-5}/hr, or about 97% of the λ_t.

The contributors to the running failure rate of the condenser water box circuit were the divided water boxes in the LP and the HP condensers. Each water box leak was estimated to be 3×10^{-5}/hr.

Each of the air ejector pump running failure rates was estimated to be 3×10^{-5}/hr for "fail-to-operate."

As indicated on the RFBD for the resuperheater bypass and the steam generator alternate discharge circuits (Fig. 4-6), these circuits consist of all single failure points. Excluding the support systems, the following λs and MTTRs were estimated for RHR:

	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Single failure	3.0×10^{-4}/D	24	7.3×10^{-5}/hr	23

The contributor to the demand single failure rate is the temperature control valve that allows the feedwater into the desuperheater "fail-to-open," estimated to be 3×10^{-4}/D.

Active single failure points in the running failure rate were:

1. The temperature controller and the temperature control valve that provide the proper amount of feedwater to saturate the steam in the resuperheater bypass circuit.

2. The four pressure controller and pressure control valves (two at the LP and two at the HP condensers) that modulate the saturated steam pressure from the resuperheater bypass desuperheater into the condenser.

Each of the controller and modulating valve running failure rates was estimated to be 1×10^{-5}/hr; i.e., the five components contributed 5×10^{-5}/hr, or 68% of the λ_t.

The system failure rates for the PCS are dominated by the single failure points in the system. The following system failure rates may therefore be calculated:

	System Failure Rates	
	Λ_D	Λ_t
Plant Initially Operating	3.0×10^{-4}/D	2.6×10^{-5}/hr
Plant Initially Shut Down	--	9.9×10^{-5}/hr

The running failure rate of the PCS while the plant is operating includes contributions from the condensate, feedwater, and circulating water systems; when the plant is shut down, it also includes a contribution from the resuperheater bypass circuit. The demand failure rate of the PCS considers the unavailability of the resuperheater bypass circuit following reactor trip.

Based on the plant operating 80% of the year with three reactor trip demands per year, the system failure probability would be 3.6×10^{-1}/yr. As the FMEA in Table 4-2 shows, the time during which the RHR systems can operate without the PCS is 22 hr, or approximately equal the PCS mean repair time. Allowing for this grace period, the probability of PCS failure causing MLCS failure is approximately 1×10^{-1}/yr.

4.4.4. PCS Design Improvements

The following design improvements to enhance the MLCS reliability in the PCS were suggested:

Suggested Improvements	Reliability Effect
Eliminate the single failure points:	
1. Condenser hotwell. Devise a method to use the LP and HP condenser hotwells independently.	1. Will increase the number of success paths, thus increasing reliability.
2. Many common suction and discharge headers.	2. Same as 1.
a. Auxiliary feedwater suction header. Make independent.	
b. Condensate pump suction header, recirculation header. Make independent. From independent recirculation line to the hotwell, tap independent fill lines to the shutdown feedwater storage tank. In addition, have independent overfill return line from shutdown feedwater storage tank back to the hotwell.	
c. Circulating water pump discharge and return headers. Make independent to the divided water box with cross-over capability and, similarly, make return lines	

independent to the cooling tower with cross-over capability.

d. Desuperheaters in the resuperheater bypass and steam generators alternate discharge circuits. Make independent to each loop with cross-over capability. Also make the shutdown feedwater to each desuperheater independent to each loop with cross-over capability. This will necessitate independent controller for each desuperheater and thus eliminate this as a single failure. The condenser inlet valves could be sized for each loop, one each going to the LP and HP condensers.

3. Incorporate a smaller maintenance condenser(s) with its own small condensate pump and small circulating water pump for long term main loop heat rejection.

3. Same as 1.

4.4.5. PCS Areas for Further Studies

None.

4.5. CLASS IE (ESSENTIAL) ELECTRIC POWER SYSTEM

4.5.1. Description

The principal function of the Class IE power system is to provide electric power to all of the safety related equipment in the plant. This is a seismic Category I system. The normal supply is the unit auxiliary transformer. The alternate supply is the reserve auxiliary transformer. Loss of the normal source will result in the immediate, automatic, high

speed dead bus transfer to the alternate source with the automatic start of the emergency diesel generators, which will be kept on a standby status.

The Class IE system consists of three independent subsystems and three uninterruptible power systems (described below). In addition, there are two service-water cooling tower 480-volt load centers, each fed from a different 4160-volt bus.

Each subsystem is a simple radial system and is always operated as such. Each consists of a 4160-volt bus, a 480-volt load center and associated 460-volt motor-control centers, and a 4160-volt emergency diesel generator.

The three subsystems correspond to the three reactor cooling loops, and auxiliaries are so grouped on the associated buses. Bus ties between the essential 4160-volt buses permit a bus to be energized for maintenance purposes when off-site power is off and its emergency generator is out of service. Interlocking prevents closing of a bus tie circuit breaker when the bus is being energized from another source.

There are three Class IE system storage batteries. Each battery supplies 125-volt dc power for switchgear control annunciators and indicating lights for one of the three subsystems, one third of the dc emergency lights, and one of the uninterruptible power systems. Each is sized to: (1) trip all circuit breakers required and close all dc motor-operated valves on its bus; (2) carry its assigned emergency lighting, annunciators, indicating lights, and inverter for an uninterruptible power system for 4 hr; and (3) close all breakers required.

Each of the three uninterruptible power systems consists of a battery charger, an inverter, a static switch, and a bypass transformer for maintenance purposes. The battery charger is supplied from a 460-volt motor control center and feeds into a 125-volt dc bus. The battery is connected to the bus. The battery charger is sized to supply the inverter annunciators and indicating lights and simultaneously recharge the battery in

less than 8 hr. The inverter is supplied from the 125-volt dc bus and feeds an uninterruptible ac bus through a static switch. The bypass transformer is supplied from a motor control center different from the battery charger and feeds into the static switch. In normal operation, the battery charger carries the full inverter load (plus any additional required dc load), and the battery is floating. In the event of an ac failure, the battery automatically picks up the uninterruptible (inverter) load. The bypass transformer carries the load should any of the dc system components be out of service because of failure or for maintenance purposes. Circuit breakers are provided to bypass the static switch for the same reasons.

4.5.2. Qualitative Analysis

An RFBD (Fig. 4-7, sheets 1 and 2) was developed for the Class IE (essential) electric power system during RHR. An FMEA of this system on MLCS and CACS is given in Tables 4-2 and 4-3.

The Class IE system was assumed to function from plant operation to RHR mode as follows:

1. During normal plant operation, the Class IE system is supplied by the main generator through the unit auxiliary transformer (UAT) and a normally-closed (NC) circuit breaker to each of the essential 4160-volt buses. The off-site power (OSP) is on standby through the reserve auxiliary transformer (RAT) and a normally-opened (NO) circuit breaker to each essential 4160-volt bus.

2. When a generator trip occurs, a circuit breaker in the switchyard opens, causing the NC breaker from the UAT to open and the NO breaker from the RAT to close. This transfer is designed to occur without load losses at any of the buses.

3. After the transfer, the NC dc motor-disconnect may be remotely opened and the switchyard circuit breaker closed, thus placing the UAT through the main transformer on automatic standby to the RAT.

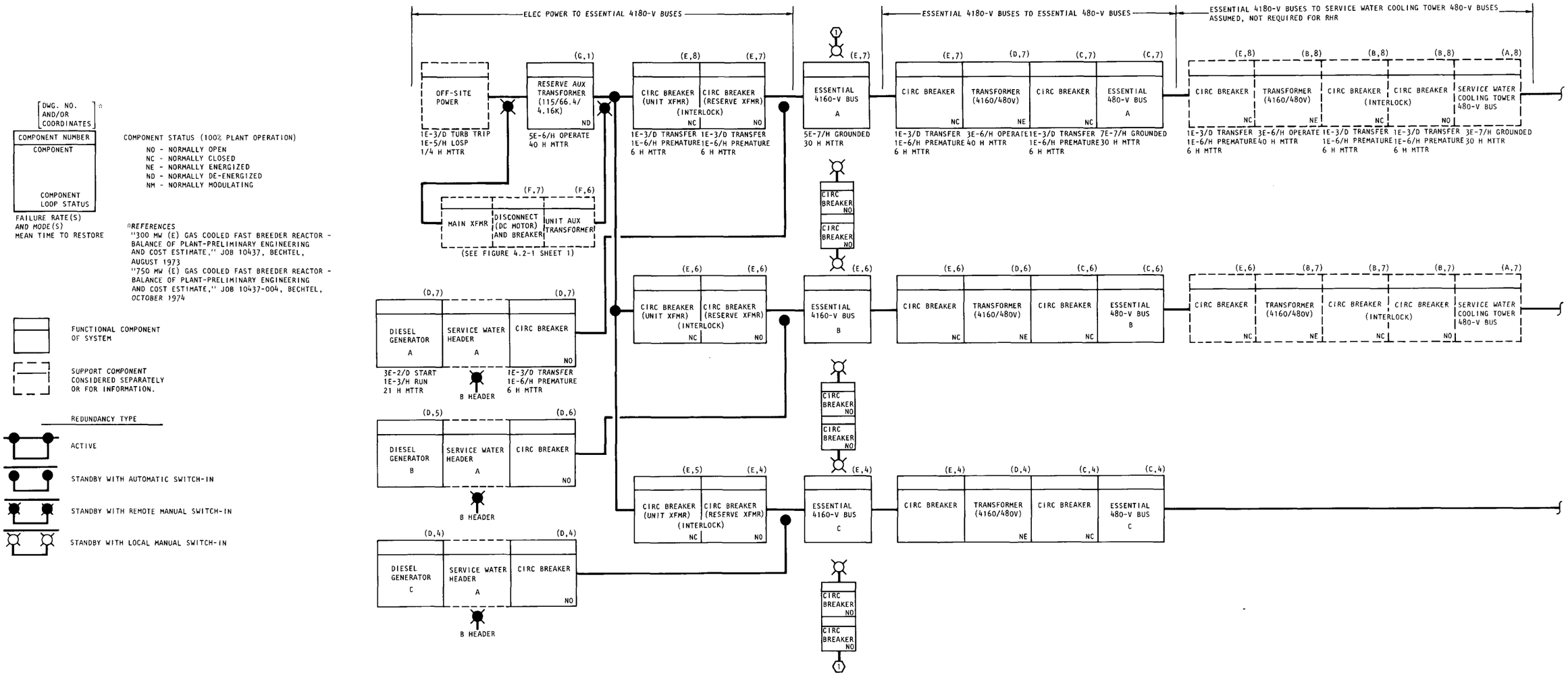


Fig. 4-7. GCFR class IE (essential) electric power system functional block diagram for RHR (Drawing E101), sheet 1 of 2

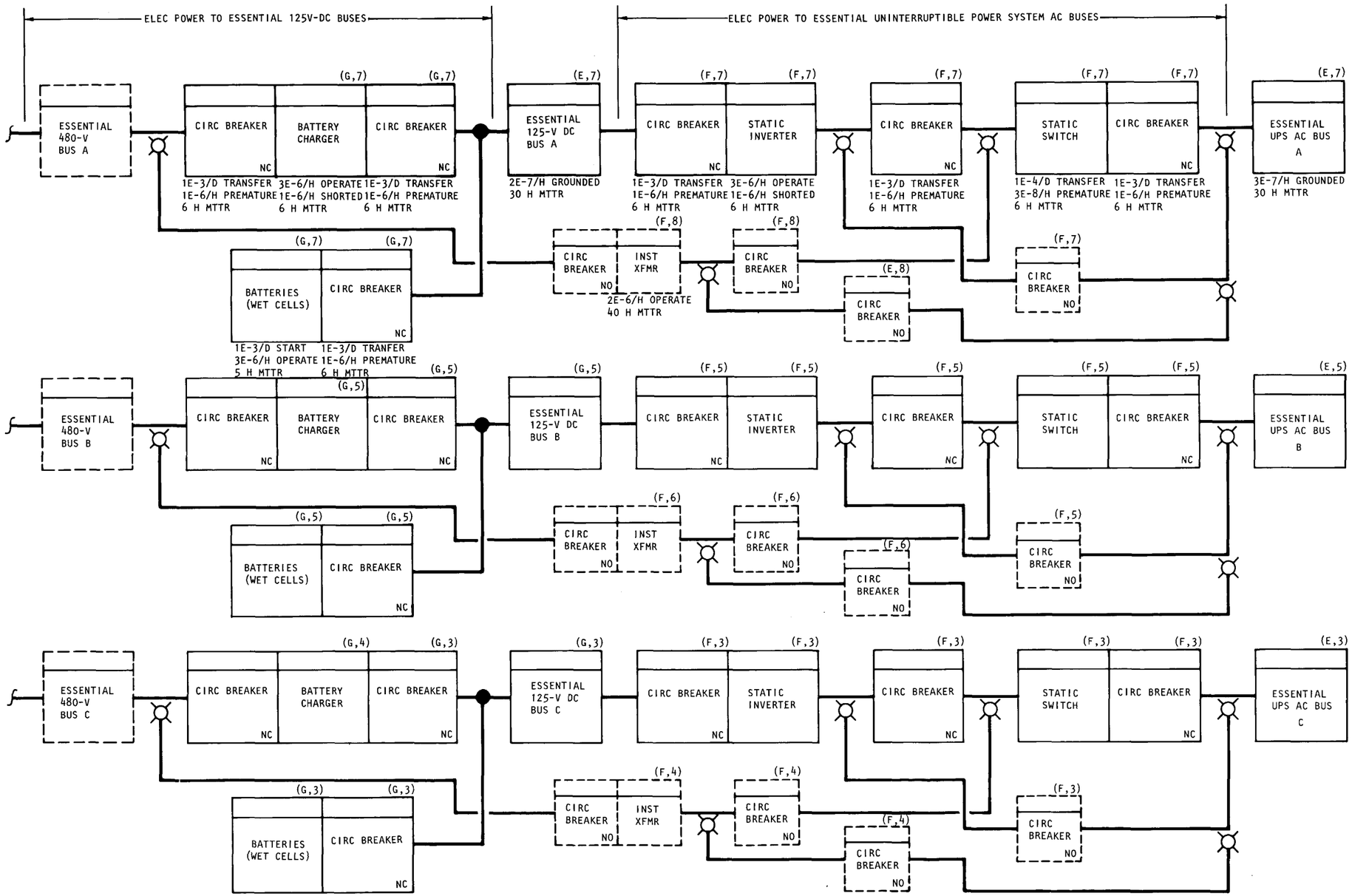


Fig. 4-7. GCFR class IE (essential) electric power system functional block diagram for RHR (Drawing E101), sheet 2 of 2

TABLE 4-3
FAILURE MODE AND EFFECT ANALYSIS OF SUPPORT SYSTEMS FOR GCFR CORE AUXILIARY COOLING SYSTEM (CACS) RHR
Initial Conditions: Full Power & Plant Shutdown (PSD)

Support System	Function	Failure Mode	CACS Failure Effect	(1)	Ref. RFBD/FMEA Component No.
1. Class IE Electric Power System (Essential)	1. Provide electric power to all safety related equipments and provide UPS for the instrumentation and control (I&C) system.	1a. Fail to operate	1a. Loss of I&C power to the following:	>0	
			Auxiliary circulator controls.		Fig. 3-1, Sheet 1/3
			Louver Controls		Fig. 3-1, Sheet 3/35
			1a. Loss of motive power to the following:	>0	
			Auxiliary Circulators		Fig. 3-1, Sheet 1/2
			Circulating Water Pumps		Fig. 3-1, Sheet 2/23
			Loop Cooler Fans		Fig. 3-1, Sheet 3/34
2. Component Cooling Water Systems					
a. Reactor Plant Cooling Water System (RPCWS)	2a. Provide cooling water to components carrying radio-active or potentially radio-active fluids.	2a. Fail to operate	2a. Loss of cooling to auxiliary circulator motor.	(2)	Fig. 4-8/4
b. Service Water System	2b. Provide cooling water to RPCWS heat exchangers and transfers heat ultimately to the cooling tower.	2b. Fail to operate	2b. Loss of cooling to the RPCWS which in turn will cause loss of auxiliary circulator motor coolers, thus will be much longer than 2a.	>>(2)	Fig. 4-8/4

(1) CACS capability, given loss of support system.

(2) ~15 minutes (PCRV pressurized) & ~2 minutes (PCRV de-pressurized).

4. The diesel-generators are automatically started and remain on standby; in the event of the loss of OSP, they will automatically supply adequate power to the 4160-volt buses.

As indicated on the RFBD, there are two sources of electric power to the Class IE buses during RHR, off-site power and diesel-generators as a back-up. The off-site source is not safety class. The diesel-generators and Class IE buses are safety class, Seismic Category 1 systems. Thus for safety purposes, except for the double breaker cross connects between the 4160-volt buses, the Class IE system has three independent loops. The loops are identical except for the two service-water cooling water tower 480-volt load centers, each fed from a different 4160-volt bus. In this analysis, it was assumed that the heat capacity of the water and the natural draft of the cooling tower were adequate; thus, since these cooling tower buses are not required, the Class IE bus subsystems were assumed to be identical.

The Class IE buses can provide independent ac electrical power to each of the CACS and MLCS loops. The instrumentation electric control power was assumed to be provided from the uninterruptible power systems (UPS).

4.5.3. Quantitative Analysis

The RFBD (Fig. 4-7, sheets 1 and 2) was used to estimate the failure rates (λ) and the MTTR from which the failure probabilities could be determined.

As indicated by the RFBD (Fig. 4-7, sheet 1), the Class IE ac system consists of three independent bus and diesel-generator combinations and two transformers from which off-site power can be supplied to these buses. The following λs and MTTRs were estimated for the Class IE ac system:

	Per Loop Estimates			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Plant Initially Operating				
Off-site power	10^{-3}/D	1/4 hr	10^{-6}/hr[(a)]	1/4 hr
Diesels (redundant)	3×10^{-2}/D	21 hr	--	
ac buses (redundant)	1×10^{-3}/D	6 hr	8.2×10^{-6}/hr	24 hr
Plant Initially Shut Down				
Off-site power	--		10^{-5}/hr	1/4 hr
Diesels (triply redundant)	3×10^{-2}/D	21 hr	3×10^{-3}/hr	21 hr
ac buses (triply redundant)	--		8.2×10^{-6}/hr	24 hr

(a) Turbine generator failure to maintain in-house loads was estimated to be 10^{-1} per loss of OSP. Thus the λ_t for OSP was estimated to be $10^{-1} \times 10^{-5}$/hr = 10^{-6}/hr.

The greatest contributors to the demand failure rate for one ac bus was the normally-closed UAT breaker "fail-to-open," which will inhibit the automatic closure of the RAT breaker or the diesel/generator breaker. A breaker "fail-to-transfer" was estimated to be 1×10^{-3}/D. The greatest contributor to the running failure rate for one ac bus was the 4160/480-volt transformer, with an estimated failure rate of 3×10^{-6}/hr.

If the off-site power source should not be available, the greatest contributor to both the demand and running failure rates of the buses would be the diesel-generator. The diesel-generator was estimated to contribute about 97% of the λ_D and about 99% of the λ_t for each loop.

As indicated by the RFBD in Fig. 4-7, sheet 2, the Class IE, 125-volt dc buses and uninterruptible power systems (UPS) are normally supplied from the essential 480-volt bus. In the event of the loss of ac power, the battery will automatically carry the load.

The following failure rates and MTTRs were estimated for quantification of the dc and UPS Class IE system:

	Per Loop Estimates			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
dc buses (redundant)	--		7.5×10^{-6}/hr	8 hr

The greatest contributor to the running failure rate of the charger circuit was the charger, with an estimated failure rate of 4×10^{-6}/hr, or about 66% of the λ_t.

Based upon the standard reliability approximations given in Appendix A, the following system failure rates may be calculated:

	System Failure Rates	
	Λ_D	Λ_t
Plant Initially Operating		
Off-site power and diesels[a]	2.7×10^{-6}/D	2.7×10^{-9}/hr[c]
Buses[a]	3.0×10^{-6}/D	2.4×10^{-8}/hr
Total	5.7×10^{-6}/D	2.7×10^{-8}/hr
Plant Initially Shut Down		
Off-site power and diesels[b]	--	2.7×10^{-10}/hr[c]
Buses[b]	--	3.0×10^{-12}/hr
Total	--	2.7×10^{-10}/hr

[a] Two out of three required.

[b] One out of three required.

[c] Off-site power failure rate times diesel start failure probability.

The failure of the Class IE buses dominates the system failure rate when the plant is initially at power, whereas failure of the Class IE power sources (off-site and diesel power) dominates the system failure rate when the plant is initially in a shutdown mode. Based upon the plant operating 80% of the year with three reactor trip demands per year, the system failure probability would be 2.0×10^{-4}/yr. As the FMEA in Tables 4-2 and 4-3 show, the time during which the RHR systems can operate without essential power is short in comparison to the mean repair time of the electrical buses.

Thus the probability of essential electrical supply failure leading to RHR failure may be estimated at 2×10^{-4}/yr.

4.5.4. Design Improvements

The following design improvements to enhance RHR reliability in the Class IE power system are suggested:

Suggested Improvement	Reliability Effect
1. Provide batteries for short term CACS operation or otherwise improve the time during which the RHR system can operate without Class IE power.	1. As the electrical power system MTTR for both Class IE and non-Class IE is relatively short, the capability (i.e., several hours) to operate without a common electrical supply would sufficiently decrease the estimated RHR unreliability.
2. Provide independent diesel generator and room cooling system (i.e., air-cooled heat exchanger for each loop).	2. Will eliminate the interdependency between the diesel generator system and the service water system.
3. Provide off-site power (OSP) for the normal source of power to the Class IE buses and for rapid switching to in-house power in the event of the loss of OSP.	3. Will eliminate the rapid breaker transfer each time the generator is tripped. Current estimate of total loss of OSP is about 0.1/yr whereas plant trips are estimated to be more than 3/yr.

4.5.5. Areas for Further Studies

None

4.6. COMPONENT COOLING WATER SYSTEMS

4.6.1. Description

The CACS and the MLCS use the reactor plant cooling water system (RPCWS) to cool their components. The RPCWS cools components carrying

radioactive and potentially radioactive fluids. It provides a monitored intermediate barrier between these fluids and the service water system (SWS) which transfers the heat ultimately to cooling towers. The RPCWS and the SWS are safety class seismic Category I systems.

The RPCWS consists of two independent closed-loop water circuits. Each circuit has two 100% heat exchangers and pumps with crossover capability, a surge tank, purification equipment, piping, and valves. Heat is removed and transferred to the SWS.

The SWS consists of a two cell mechanical draft cooling tower, three 100% SW pumps, and two separate and independent headers with check valves to prevent the flow of water between them. The return headers to the cooling tower also consist of two independent loops. Each header is connected to the circulating water system, which can be used in case the SWS is unavailable.

4.6.2. Qualitative Analysis

4.6.2.1. Reactor Plant Cooling Water System. An RFBD (Fig. 4-8) was developed for the RPCWS. The RPCWS header A provides the normal cooling water to both the MLCS and the CACS circulator service coolers. These coolers use about 24% of the operational duty of the RPCWS.

The RFBD indicates that the RPCWS headers A and B are actively redundant to each other. However, at each component, the valves to and from the A supply and return headers are normally open with the valves to the B headers normally closed. Thus, although the headers are actively redundant to each other, each component is configured as an on-line header and a standby header with a remote manual switch-in capability.

During normal operations, both loops of the RPCWS will be operating. In each loop, one pump and heat exchanger will be on-line, with the other pump and heat exchanger as a backup with a remote manual switch-in capability. Loop A uses the SWS header A as its normal cooling water, with

the SWS header B as a backup, again with a remote manual switch-in capability. Loop B uses the SWS header B as its normal cooling water with header A as a backup. Although RPCWS header A normally provides cooling water to the RHR systems, as indicated on the RPCWS RFBD, many alternative paths of success are available to provide cooling water to the RHR system. However, in the event that the on-line header must be isolated, all the supply and return valves must be remotely closed and the standby header supply and return valves remotely opened. The RPCWS drawing indicates 10 components, which means that 40 valves must be remotely operated. The three MLCS loops (12 valves) must be transferred. The three CACS loops are assumed to have both cooling loops actively redundant; thus no manual actions are required.

There are two unlikely abnormal conditions considered in the design of the RPCWS. One is the maximum PCRV cooling load condition and the other is the maximum fuel pool load.

The maximum PCRV cooling load condition assumes a design basis depressurization accident (DBDA) and the entire 100% heat load carried by either cooling loop. Thus, this will require at least one of two RPCWS loops.

During maximum fuel pool load condition, when 1-1/3 core is stored in the fuel pool and PCRV cooling is not required, this condition will require both RCPWS loops.

4.6.2.2. Service Water System. An RFBD (Fig. 4-9) was developed for the SWS. The SWS removes heat from the RPCWS, which in turn removes heat from the MLCS and CACS. The interrelationship of the SWS and RPCWS is described in Section 4.6.2.1.

During normal operation the SWS is assumed to operate as follows:

1. The cooling tower with one of its cells and fans is on-line; the other cell and fan are on standby. The fans were assumed to have

the capability of remote manual switch-in, but the return headers A and B to the stand-by cell require a local manual switch-in. During RHR, it was assumed that the heat capacity of the water volume and the natural draft of the cooling tower were adequate; thus the fan is not absolutely required.

2. One of the three 100% SW pumps is on-line, with the other two on standby with automatic switch-in capability. Each pump discharges into two separate independent headers with check valves to prevent back-flow in the standby pumps.

3. Except for the RPCWS loop B heat exchangers, each safety-related component is normally supplied from the A header with a backup connection from the B header. All backup switch-ins can be remotely controlled. The non-safety related components are supplied only from the B header. In addition, each header is connected to the circulating water system, which can be used in case of the total loss of the SWS.

The SWS RFBD (Fig. 4-9) indicates no single active or passive failures. However, the switch-in of the standby cooling tower cell indicated that local manual actions are required. Thus should the on-line cooling tower fail at plant shutdown, the local manual switch-in may be inadequate to maintain component cooling for RHR.

As is true in the RPCWS, should the on-line A header require isolation, indications are that all components must be remotely transferred to the standby, or B, header. The SWS drawing indicates 30 components on the A header. It may be that only the standby valves require operation; however even this means that 60 remote manual valves must be actuated to completely transfer the SW to all the components.

4.6.2.3. Support Systems. The RPCWS requires the following support systems:

1. Class IE buses, which provide electric power to drive the pumps and some of the valves.

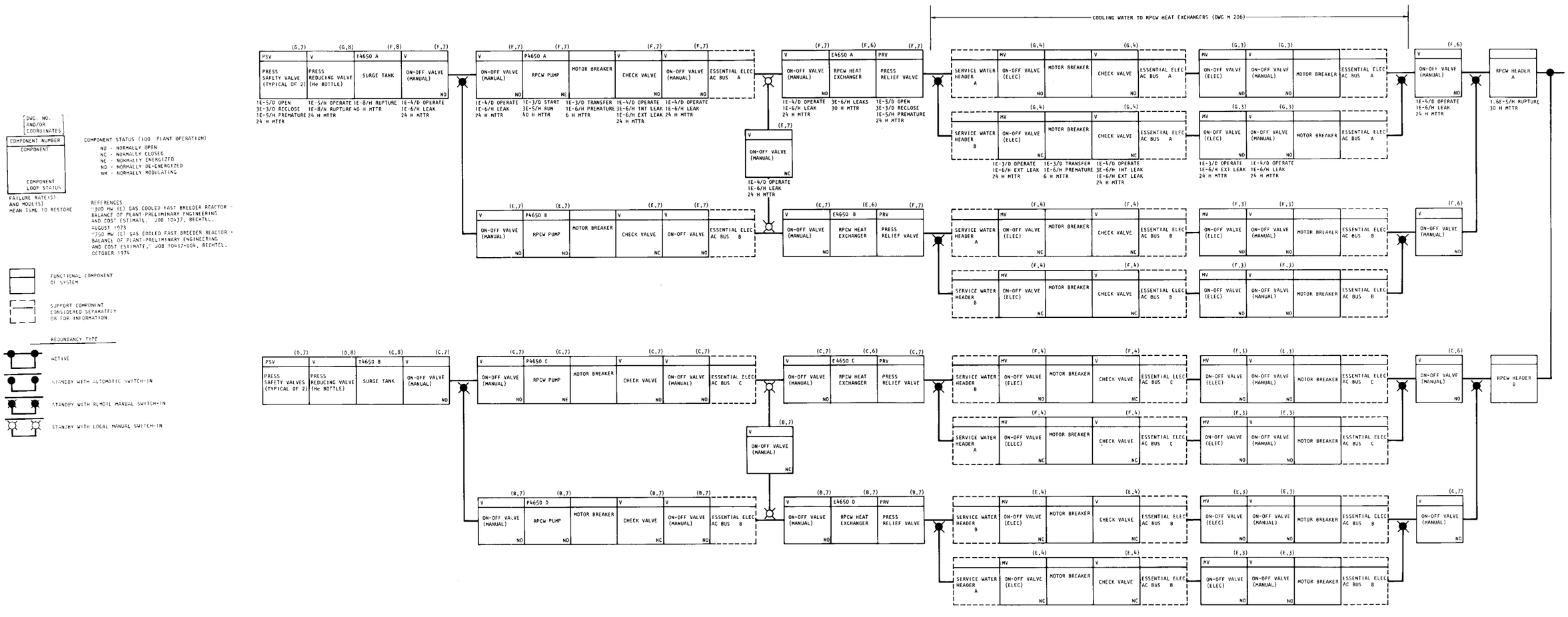


Fig. 4-8. GCFR reactor plant cooling water (RPCW) system reliability function diagram for RHR (Drawing M207)

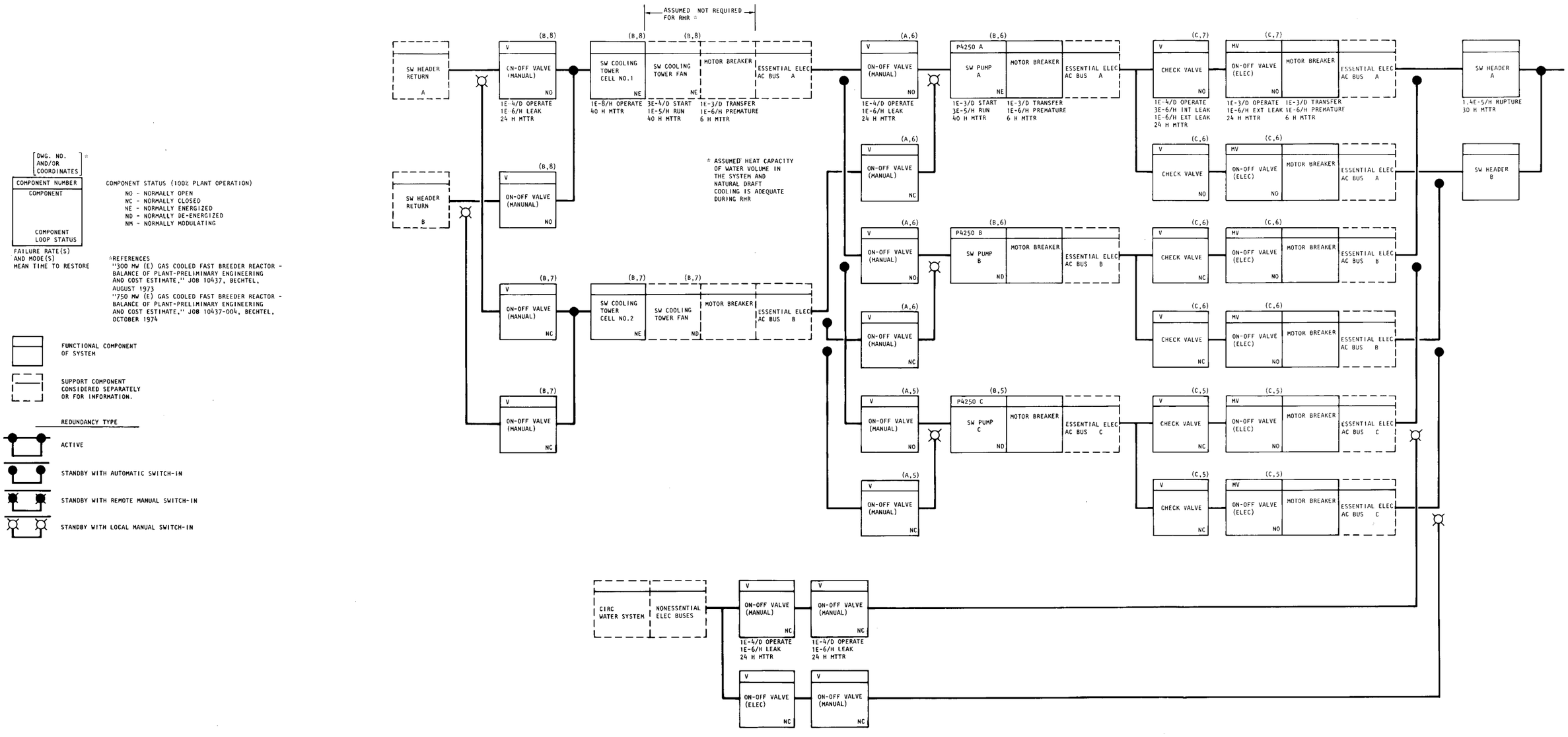


Fig. 4-9. GCFR service water (SW) system reliability function diagram (Drawing M206)

2. SWS, which removes heat.

3. Air supply system, which drive the valves for the MLCS and CACS circulator service cooler cooling water plus other components (not shown on the RFBD).

The SWS requires the following support systems:

1. Class IE buses, which provide electric power to drive the pumps, the fans, and some of the valves.

2. Air supply system, which drives some of the valves for the safety and non-safety related components' cooling water (not shown on RFBD).

4.6.2.4. RHR Dependencies in the SWS. In addition to direct cooling water support for RHR to the MLCS and the CACS, the SWS provides component cooling water to the following systems which are also required for RHR:

1. Air supply system, which requires cooling water to the air compressor jackets and aftercoolers.

2. Emergency electrical system, which requires cooling water to the diesel generator jacket coolers and the room coolers.

3. Control room emergency system, which requires cooling water to coolers.

4. Cable spreading room, which requires cooling water to coolers.

5. Switch gear room, which requires cooling water to coolers.

6. Reactor auxiliary building, which requires cooling water to coolers.

4.6.3. Quantitative Analysis

The RFBD were used to estimate the failure rates (λ) and the MTTR from which the failure probabilities of the RPCWS and the SWS could be estimated.

4.6.3.1. RPCWS. As indicated by the RPCWS RFBD (Fig. 4-8) no single active or passive failure exists for RHR. Redundancies exist within each loop. Assuming remote manual switch-ins only and excluding support systems, the λs and the MTTRs within one loop were estimated as follows:

	Within Each Loop Estimates			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Tank and Header (redundant)	--		4.8×10^{-5}/hr	26
Pump and Heat exchanger (quadruply redundant)	4.4×10^{-3}/D[(a)]	19	5.9×10^{-5}/hr	32

(a) Switch-in λ_D from standby to on-line.

The greatest contributors to the single running failure rate for each loop were the pressure reducing valve "fail-to-operate" and the two pressure relief valve "premature operations," each with an estimated failure rate of 1×10^{-5}/hr. In addition, 17 valves in each header with an estimated failure rate of 1×10^{-6}/hr for excessive leaks contributed 1.7×10^{-5}/hr to the running λ_t.

The greatest contributor to the double running failure rate for each loop was the RPCW pump "fail-to-operate." This was estimated to be 3×10^{-5}/hr, or about 50% of the λ_t.

The greatest contributors to the demand failure rate for the standby circuit to be placed on-line were the motor breaker "fail-to-transfer"/pump "fail to start" and the motor breaker "fail-to-transfer"/motor operate valve "fail-to-operate," each with an estimated failure rate of 1×10^{-3}/D for a total of 4×10^{-3}/D, or about 90% of the λ_D.

4.6.3.2. SWS. As indicated by the SWS RFBD (Fig. 4-9) no single active or passive failure exists. The system consists of one cooling tower cell on-line with one cooling tower cell on standby, one pump on-line with two pumps on standby, and two active redundant headers. Excluding support systems and the circulating system backup, the λs and MTTRs for the SWS were estimated as follows:

	Per Loop Estimate			
	λ_D	$MTTR_D$	λ_t	$MTTR_t$
Cooling Tower (redundant)	$4 \times 10^{-4}/D$ [(a)]	24	1×10^{-8}/hr	40
Pump (triply redundant)	$2.4 \times 10^{-3}/D$ [(a)]	23	3.3×10^{-5}/hr	38
Header (redundant)	--		1.4×10^{-5}/hr	24

[(a)] Switch-in λ_D from standby to on-line.

The contributor to the cooling tower running failure rate, excluding the fan, was one cell "fail-to-operate." This was estimated to be 1×10^{-8}/hr, similar to a rupture of a tank.

The contributors to the cooling tower demand failure rate were the minimum number of local manual valves which required closing and opening to isolate one cell and put the standby cell on-line. It was estimated that at least 4 valves had to operate, and, with an estimated λ_D per valve of $1 \times 10^{-4}/D$, the total was $4 \times 10^{-4}/D$.

The greatest contributor to the pump circuit running failure rate was the pump "fail-to-operate." This was estimated to be 3×10^{-5}/hr, or about 90% of the λ_t.

The greatest contributors to the pump circuit demand failure rate were the pump "fail-to-start" and the motor breaker "fail-to-transfer." Each was estimated to be $1 \times 10^{-3}/D$, or about 42% each of the λ_D.

The greatest contributors to the header running failure rate were the valve "excessive leaks." The drawing indicated 14 valves in the header

that could potentially cause excess leakage in the header. Each valve leakage failure rate was estimated to be 1×10^{-6}/hr, for a total of 1.4×10^{-5}/hr.

The system redundancy of both the RPCWS and SWS is limited by the doubly redundant headers. The following system failure rates may therefore be estimated:

	System Failure Rates (Λ_t)
RPCWS	1.2×10^{-7}/hr
SWS	9.6×10^{-9}/hr
Total	1.3×10^{-7}/hr

Based on a system operating time of 8760 hr, the system failure probability may be estimated as 1.1×10^{-3}/yr. As the FMEA in Tables 4-2 and 4-3 show, the time during which the RHR systems can operate without RPCWS or SWS is short in comparison to the system mean repair times. Thus the probability of RPCWS or SWS failure leading to RHR system failure may be estimated as 1×10^{-3}/yr.

4.6.4. Design Improvements

The following design improvements to enhance reliability of the component cooling systems are suggested:

Suggested Improvement	Reliability Effect
1. Eliminate the remote manual switch-in for the components and provide at least automatic switch-in or an active redundant system.	1. Loss of a safety header indicates too many manual actions. Will minimize immediate manual actions.
2. Eliminate the local manual switch-in of the return line header valves to the cooling tower cells and pump suction valves. Provide at least a	2. Will increase reliability. In most cases local manual action is probably adequate, but in the event of a safe-shutdown-earthquake, when the likelihood

	remote manual capability to these valves.	of cooling tower cell failure increases, local manual switch-in may be inadequate, this being a safety system.
3.	Provide independent component cooling for the CACS and emergency diesel generators with individual air coolers for each loop.	3. Eliminates interdependencies between systems as well as intradependencies within these safety systems.

4.6.5. Areas for Further Studies

None.

5. RHR SYSTEM DIVERSITY

The unreliability assessment described previously in this report was based upon assumptions of independence between the redundant loops of each of the RHR systems. In the limiting case (following reactor trips) a minimum redundancy of two was evidenced in each system, with the failure of four or more loops required to cause RHR failure by both systems. Under question here is whether there are dependencies which could further reduce the redundancy of either the MLCS or the CACS beyond that assumed previously.

As shown in Table 5-1, potential common mode mechanisms which could further reduce the RHR system redundancy can be divided into several categories (Refs. 5-1 and 5-2). Three general categories of common mode failure are identified. The first category, common cause failures, is the case where multiple component failures can be traced to a single event in the design, engineering, or operation of the plant. The second category, causal or propagating failures, occurs when a single equipment failure propagates, resulting in multiple equipment failures. The third category, external initiators of failure, occurs when an external natural or manmade phenomenon such as fire, flood, earthquake, tornadoes, aircraft impact, explosion, or the like causes multiple equipment failures.

Because of the many subtleties of such common mode failure events and their potential for development in the advanced stages of a design, it is not possible to conduct, in any sense, a complete review of potential areas of susceptibility to common mode failures in a conceptual design which is inherently limited in detail. In the following sections, however, the reliability of the GCFR RHR system design is considered with respect to each of the common mode failure categories to identify the more obvious areas of potential unwanted design dependencies.

TABLE 5-1
CAUSE CATEGORIES OF COMMON MODE FAILURE

Common cause failures

- Common design error made in all components.
- Common fabrication/manufacturing defect in all components.
- Common storage, shipping, or installation error made in all components.
- Common human error made by plant personnel in maintaining or operating all components.
- Common environmental variation affects all components.

Causal or propagating failures

- All components placed in close proximity.
- Components depend on common time sequence of operation.
- All components degraded by initiating failure.

External initiators of failure

- All components degraded or made to fail by external man-made or natural phenomena.

5.1. COMMON CAUSE FAILURES

Common cause failure, as considered here, is multiple component failures that can be traced to a single event which has occurred in the design, engineering, or operation of the system under consideration. Such failures may be generally traced to common design errors, common fabrication or manufacturing defects, common storage, shipping, or installation errors, common maintenance or operating errors, or common environmental effects. Table 5-2 shows the relative importance of each of these common cause failure types for a number of redundant systems based on current U.S. nuclear experience. More than half of the common cause failures are related to equipment design, more than a quarter are related to human operator and maintenance errors, and the bulk of the remainder are from environmental causes.

Common cause failure concerns may be centered both within the individual RHR systems (intra-system common cause failures) and between the two RHR systems (inter-system common cause failures). Nuclear experience has shown the occurrence rate of common cause failures within redundant systems with identical parallel components to be relatively high. For this reason, as described previously in this section, reliance upon simple redundancy in design is not sufficient if a low unreliability goal such as 10^{-6}/yr is to be achieved. Therefore, diverse design features (summarized in Table 5-3) have been employed in the GCFR MLCS and CACS to help enforce a low probability of occurrence for inter-system common cause failures.

The following sections, where possible, review the aspects of GCFR RHR system design with respect to each of the common cause failure types, particularly with respect to potential inter-system common cause failures.

5.1.1. Design Errors

Common cause failures resulting from design error may arise from an unforeseen interdependence between otherwise independent design features or from erroneous prediction of plant or system behavior. The latter failure

TABLE 5-2
RELATIVE CONTRIBUTIONS OF CAUSES TO COMMON CAUSE FAILURE[a]

Generic Equipment Type[b]	Relative Contributions of Causes to Common Cause Failure (%)				
	Design Error	Fabrication/ Manufacturing Error	Storage/ Shipping Error	Human Operator Error	Environmental Cause
Diesel Generators [6]	50.0	0	16.7	16.7	16.7
Reactor Trip Input Channels [14]	64.3	0	7.1	28.6	0
Valves [6]	33.3	0	0	16.7	50.0
Pressure Switches [14]	50.0	0	0	36.0	14.0
Pumps [1]	100.0[c]	0	0	0	0
All Equipment Listed Above [41]	53.7	0	4.9	26.8	14.6

[a] Taken from Ref. 5-1.

[b] Information in brackets indicates sample size.

[c] Only one instance of common mode found in this sample for pumps.

TABLE 5-3
COOLING SYSTEM DIVERSITY

	Main Cooling System	Auxiliary Cooling System
Helium Circulators		
Type	Axial flow	Centrifugal
Drive	Steam turbine	Electric motor
Bearings	Water lubricated	Oil lubricated
Power source	Nuclear steam for 30 min or oil-fired boilers after 20 min	Essential electric power, separate diesel for each loop
Loop Isolation Valves		
Type	Multiple louver	Flapper
Position in Power Operation	Open	Closed
Actuation	Reverse flow	Auxiliary circulator pressure rise
Heat Dump		
Heat exchangers	Main steam generators	Auxiliary heat exchangers
Coolant	Steam/water	Pressurized water
Feed source	Main condenser hot well or condensate storage	Closed loop
Heat Sink	Main condenser or steam exhaust to atmosphere	Atmosphere via air-cooled heat exchangers

type is largely guarded against by involving diverse groups in the analysis of plant and system behavior and by prototypical testing where possible. For the GCFR demonstration plant, the possibility of multinational participation in the designs exists, with the Federal Republic of Germany responsible for design of the CACS and the U.S. responsible for MLCS design. Such an approach might be uniquely advantageous with respect to ensuring design diversity.

A significant area for potential RHR system dependencies, however, exists in the design of interfacing electrical and mechanical systems such as control and protective systems, component cooling water systems, valve control fluid systems, and electrical power systems. RHR system dependence on support systems which evidence a lesser redundancy or diversity can potentially void the high design reliability otherwise obtainable.

Because designs have not yet been developed for the control and protective systems necessary to support the RHR function, their reliability impact could not be reviewed. Designs do exist, however, for the other support system types and therefore in performing the reliability analysis of the MLCS and CACS (described in Sections 2 and 3 to this report) connections to external support systems have been carefully identified. The support systems so identified were analyzed as described in Section 4 of this report.

The qualitative and quantitative analysis presented in Section 4 shows that a limiting dependence of both RHR systems exists in their reliance upon the support systems as currently configured. Single failure points are in evidence in all four systems supporting the MLCS in passive features. This lesser redundancy gives a total failure probability of systems supporting the MLCS of approximately 10^{-1}/yr, well in excess of the MLCS allocation. The limiting dependence of both RHR systems is that of common reliance on the doubly redundant component cooling water system and the triply redundant electrical power system. The lesser redundancy and lack of diversity which exists because of this dependence gives a total

failure probability for systems supporting both the MLCS and CACS of 10^{-3}/yr, also well in excess of the allocation.

In sum, many of the support systems currently envisioned for the GCFR design would not support a RHR reliability consistent with the allocated targets.

5.1.2. Fabricated and Manufacturing Defects

Fabrication or manufacturing defects resulting in common cause failures may come from variations in quality control of materials, tolerance of misinterpretation, noncompliance with specifications, or process errors in manufacturing equipment. Because of the conceptual nature of the GCFR, it was not possible to review the design with respect to such common cause failure types.

5.1.3. Storage, Shipping, and Installation Errors

Common cause failures from storage, shipping, and installation error may result from shipping events such as improper packaging or unpacking, vibration or impact damage during equipment movement, storage events involving environmental degradation, or installation errors such as misalignment, improper procedures, or destructive testing. Because of the conceptual nature of the GCFR, it was not possible to review the design with respect to such common cause failure types.

5.1.4. Human Errors

Common cause failures from human error by plant personnel may result from miscalibration errors, maintenance or repair errors, improper record keeping, or improper (incorrect response) operator action. Because of the conceptual nature of the GCFR, it was not possible to review the design with respect to such common cause failure types.

5.1.5. Environmental Variations

Common cause failures from environmental variation may result from a common susceptibility to abnormal environmental conditions such as temperature, pressure, moisture, vibration, or other stresses. Since the MLCS and CACS share the common environment of the reactor coolant system, off-design reactor coolant system conditions could potentially affect both main and auxiliary loop components such as circulators, heat exchangers, and isolation valves. The available system diversity will be considered with respect to the environmental conditions listed below:

1. Reactor coolant pressure
2. Reactor coolant temperature
3. Moisture in reactor coolant system
4. Self-welding
5. Dust or debris
6. Vibrations
7. Radiation
8. Abnormal gaseous mixtures

5.1.5.1. Reactor Coolant System Pressure. Changes of the coolant pressure in the primary system can have three common effects on the main and auxiliary loop components: (1) axial thrust forces on the circulator bearings, (2) effects on the bearing lubrication system, and (3) stresses in heat exchangers and steam generators.

The helium pressure influences the load on the thrust bearings of the main and auxiliary circulators. The highest possible load on the thrust bearing of the steam-driven main circulators exists during startup when the steam pressure is low and the helium pressure close to the operating level. A depressurization causes a smaller thrust load on the axial bearings of the main circulators than does startup. Consequently, there is an inherent safety margin, since the thrust during this accident does not exceed operating limits. Auxiliary circulators are completely submerged in the helium coolant of the primary system. The upper part of the electric motor casing

of the auxiliary circulator serves as the primary PCRV closure of the auxiliary loop cavity. A labyrinth seal prevents oil vapors in the motor casing from escaping into the primary system. During depressurization, the helium atmosphere in the motor casing remains at a higher pressure than that of the primary system because of the seal resistance. The bearings of the auxiliary circulators are designed to withstand the largest resulting thrust with a wide safety margin. In addition, the relatively short duration of the increased thrust load tends to reduce the importance of this effect. As a backup, a pressure equalization line could be provided to reduce the pressure difference between motor casing and auxiliary loop cavity further.

Thrust loads can also be generated by pressure differences across the circulator wheels caused by a depressurization accident. Although these pressure differences are relatively small, the area of the wheel is much larger than that of the seal and the resulting thrust forces on the axial bearings could be substantial. However, the thrust load is well within the design limits of the two different circulators and so no common cause for failures exists. Also, the pressure differences across the wheels can be reduced by a pressure equalization mechanism. Additional seals between the discharge side and the shaft area are necessary for this purpose.

During plant operation at full system pressure, helium dissolves slowly in the lubricants and could be released by a pressure reduction or complete depressurization. Oil lubricants foam under these conditions, resulting in a change in the lubrication properties. The effect is less drastic in water, but the bearing water system of the main circulators has to be designed to prevent cavitation in orifices and pumps. Experiments have verified the design basis for the HTGR components. Similar experiments will be necessary for corroboration of the design data of the GCFR bearing systems.

Differential pressures generated within the intact loops by a design basis depressurization accident are too small to cause significant stresses in the auxiliary heat exchangers, the steam generators, or their support structure. Only the component of the leaking loop could be damaged and

then only if extremely large leaks, one to two orders of magnitude larger than the design basis leak, should occur. This would require a failure of a cavity closure as well as its flow restrictor. Although the probability of such an event is extremely low, it would still not cause a common-mode failure of heat exchangers and steam generators.

The water overpressures in both components increase as the primary system undergoes a depressurization. However, the auxiliary heat exchanger and the steam generator are designed for the full pressure on the water side, and thus a depressurization accident does not induce tube stresses that exceed the design limits of the components.

5.1.5.2. Reactor Coolant System Temperature. The coolant temperature of the primary system influences the material properties of the components in the system. A severe temperature transient of the reactor coolant would affect the main loops and, with some delay, the auxiliary loops. Two temperature effects, that caused by temperature rise and that caused by temperature decrease, should be considered.

Sudden undercooling of the core will result in an increase of the core outlet temperature. If the temperature transient is severe enough, the thermal stresses in the steam generators may exceed the design limit, and a simultaneous failure of steam generator tubes in different loops may occur. The transient of the core outlet temperature would not affect the auxiliary loop since the higher pressure in the upper reactor plenum induces leakage from the cold side of the system through the closed auxiliary loop valves, thus keeping the auxiliary components at low temperature. The thermal inertia of the steam generators would protect the auxiliary loops from the temperature transient.

Failure of the steam generators within a short time period will cause a pressure transient in the primary system which, in turn, affects the axial thrust on the auxiliary bearings before the equalization of the pressure between primary system and auxiliary circulator motor casing. If the

motor casing vents and the seals are properly designed, the thrust generated by the differential pressure does not exceed the maximum load of the bearings.

In the event of a reactor trip with full coolant flow, the inlet temperature to the steam generator would drop about 150° to 205°C (300° to 400°F) in 5 sec. The components are designed to withstand accidents of this severity. However, accumulated fatigue damage after years of service can so reduce the safety margin that a failure occurs. Because of the reduced helium pressure during overcooling, the pressure transient in the primary system should be smaller than that caused by steam generator failure at high temperature. Consequently, potential common-cause effects are expected to be less severe than those described in the previous paragraph.

The above also applies to steam generator failures caused by flooding after scram.

5.1.5.3. Moisture in Reactor Coolant System. The immediate effect of water or steam ingress into the reactor coolant system is a local change of the coolant density. Long term effects such as corrosion can be prevented by continuous monitoring and periodic inspection. When the helium is replaced locally by rapid discharge of steam, the pressure difference across the wheel, the axial thrust of the circulator, and the bending stresses in the circulator blades change. Theoretically, the radial load on the bearings also could be affected if only a part of the circulator wheel is filled with steam.

Because of the higher power consumption by the circulator owing to increased coolant density, the machine will slow down rapidly and the peak load on the bearings and blades will last only a short period. Since the bending stresses in the blades are small during normal operation, an increase caused by a higher coolant density is not expected to pose major problems. However, the circulator has to be designed for these additional stresses as well as for a possible excitation of blade vibrations caused

by the stronger wake of the inlet support waves. Since the axial thrust bearing of the circulator is designed for the extreme conditions during startup (when the steam pressure is low but the full helium pressure causes the full thrust in the upward direction), the transient load owing to coolant density changes in the well-balanced operating mode during full-power operation is not expected to pose any problem.

In addition, circulator problems caused by sudden steam ingress or density changes would only affect the operating circulators, e.g., those in the main loops. Since in any operating mode main and auxiliary circulators do not operate simultaneously at full power, moisture or density changes cannot cause common-mode failures of the diverse circulators. This is true of accidental water ingress and water carry-over.

Another potential common-cause effect related to moisture ingress into the reactor coolant system is wrong-loop or unwanted-loop trip or dump by the plant operator or by protective systems. In the current design of the GCFR, the secondary loops of both RHR systems operate at pressures higher than the normal primary side pressure; therefore, the potential exists for water ingress into the helium coolant from either system. With such a potential, careful attention must be given to the protective system designs and operating procedures to prevent unwanted loop trips in both systems from moisture ingress. Alternatively, CACS designs in which the secondary loop pressure is below that of the primary system might be considered to ensure diversity of protection against such events.

5.1.5.4. Self-Welding of Helium Valves. The lack of an oxide layer on metal surfaces in a pure and dry helium atmosphere at high temperature could result in a self-welding process which would prevent operation of the helium isolation valves in the main loop (in which the valve sticks open) and the auxiliary loop (in which the valve sticks closed). However, this is not an inter-system common-cause failure since only the auxiliary loops are rendered inoperative. The main loops can continue to operate.

5.1.5.5. Dust or Debris. Because of the utmost care in design, construction, quality control, and inspection, dirt or debris as possible causes of component failures are very unlikely. Even if dust or debris should come into the coolant stream, the design of the GCFR would preclude serious safety hazards.

Tests during the development of the Fort St. Vrain circulator have shown that the machine can withstand the impact of large steel fragments such as 1-cm (3/8-in.) nuts. The clearance between steam generator tubes limits the size of the debris passing through the steam generator to 0.64 cm (0.25 in.).

Particles passing through the circulator would impinge on the helium isolation valves. Because of the relatively low flow velocity of the helium in the duct, no damage is expected.

The above described incidents affect one loop only. Damage to all circulators could only occur if debris were generated simultaneously in all loops. The only way that such an accident can occur is through an extremely rapid depressurization of the primary system, which would damage insulation in all loops. The probability of a depressurization accident of such a severity is extremely low, and therefore, outside of the design basis envelope. However, should it occur, most of the damage would be done to the operating circulators a result of rapid depressurization; at the reduced density, objects of sufficient weight to damage the auxiliary blowers could not be lifted by the gas stream.

5.1.5.6. Vibration. The operation of a high-power compressor in the pressurized primary system generates some vibration and noise. Careful testing of the components before plant commissioning together with a large safety margin in the design of the individual circulator wheel precludes any interaction between components of different loops. A circulator in one loop is separated from all other circulators by two cross ducts and the core cavity, with many internals, baffles, valves, etc. The amplitude of a vibration generated by a main circulator is, therefore, reduced

substantially before it reaches the auxiliary loops. The prestressed concrete reactor vessel's (PCRV) rigidity and its massive walls contribute to the shielding effect and absorption of vibrations.

5.1.5.7. Radiation. Axial and radial shielding are provided in the PCRV to protect the steel components in the reactor cavity from radiation damage. In addition, the thick concrete walls resulting from structural requirements provide biological shielding. The natural shielding characteristics of the PCRV have been so utilized that the induced radioactivity in primary loop components is at a minimum. Since helium, unlike sodium, is not activated during reactor operation and is continuously cleaned in the helium purification system, a very low level of radioactivity is maintained in the loop cavities.

As a consequence, the radiation dose for loop components such as circulators, heat exchangers, and isolation valves is low enough to provide biological protection for the personnel during contact maintenance. This level is far below any metallurgical damage threshold of components. Material degradation can be ruled out, therefore, as cause for a common-mode failure between loop components.

5.1.5.8. Abnormal Gaseous Mixtures. Changes in coolant properties such as density and viscosity would affect the heat removal mechanism in the reactor. In particular, the circulator performance level may decrease under changed conditions.

Abnormal gaseous mixtures in the primary system with a concentration high enough to influence the circulators are very unlikely except for moisture (previously discussed). Air cannot leak into the system because of the high helium pressure. The amount of noble gases and iodine generated by fission in the core is very small and continuously vented into the pressure equalization system or absorbed by fission product traps. Small traces of gaseous impurities escaping from the fuel rods would be sensed long before they could affect the heat removal process.

Hydrogen from metal-water reaction can occur only as a result of moisture in the system in contact with steel near the melting temperature. The moisture concentration is monitored during plant operation, and corrective action would be taken at a moisture level which is far below the concentration that influences the circulator performance or causes hydrogen release by metal-water reaction.

After a depressurization accident, air could leak into the reactor coolant system and mix with the remaining helium. The pressure level at the time of potential air ingress is approximately 24 MPa (35 psia). Main or auxiliary circulators cannot be damaged by coolant composition changes at that pressure level up to full circulator speed. Gaseous mixtures cannot, therefore, cause common-mode failures in main and auxiliary loops.

5.2. CAUSAL OR PROPAGATING FAILURES

Causal or propagating failures, as considered here, come about through a single equipment failure propagation resulting in multiple equipment failures. Examples include a pipe rupture with the resulting pipe whip causing failure of a redundant loop in close proximity, components whose proper operation depend upon the functioning of other components in a certain time sequence, and components that all fail or are degraded because of an initiating failure, such as an extra load placed on a second pump through the first failure.

Concerns with respect to causal or propagating failures are centered both within the individual RHR systems (intra-system failures) and between the two diverse RHR systems (inter-system failures). The following sections, where possible, review the aspects of GCFR RHR system design with respect to each of the causal failure types, particularly with respect to potential inter-system causal failures.

5.2.1. Component Location

Although the adequacy of separation of RHR systems components can only be judged after more detailed design layouts are prepared, aspects

of the conceptual design have been reviewed to indicate the potential for preventing causal failures resulting from proximity. No obvious failure points have been found. Aspects of the design relating to component location are noted below.

The primary loop components of both the MLCS and CACS are housed within the PCRV of the GCFR. Each of the six loops is contained within its own PCRV cavity (as shown in Fig. 5-1), which is connected by independent ducting to the inlet and outlet plenums of the central reactor cavity. The shared location feature of the primary loop components therefore is the PCRV structure itself. It may reasonably be expected that the PCRV structure will support the RHR unreliability allocation of 10^{-6}/yr (Ref. 5-3). Aspects of the commonality of the primary coolant for both systems were discussed in Section 5.4.5.

The secondary loop components of both the MLCS and CACS commonly connected through the PCRV top head penetrations extend radially outward from the PCRV at 60 deg angles from about half the radial distance from the PCRV center to the outermost edge of the PCRV. The steam generator piping is routed to and from the turbine building through the containment to the bottom of the PCRV, where the steam generator piping PCRV penetrations are located. The main circulator turbine steam piping is routed to and from the steam generators vertically along the containment wall to the top of the PCRV, shaped into a U between the top of the PCRV and the operating floor, and then routed above the operating floor, where the valves and pipes are connected to the main circulators. Support structures will be required to support the steam piping and to prevent damage from pipe whip to adjacent main loops, auxiliary loops, control rod drive mechanisms, and PPS cable trays, as well as the containment liner, in the event of a major pipe rupture. In principle, however, the current design allows adequate separation between loop pipings so that even in the event of no restraining structures a loop whip arc would not interfere with any other loop.

The core auxiliary heat exchanger piping, auxiliary circulator electric cablings, and motor cooling lines are routed radially from their

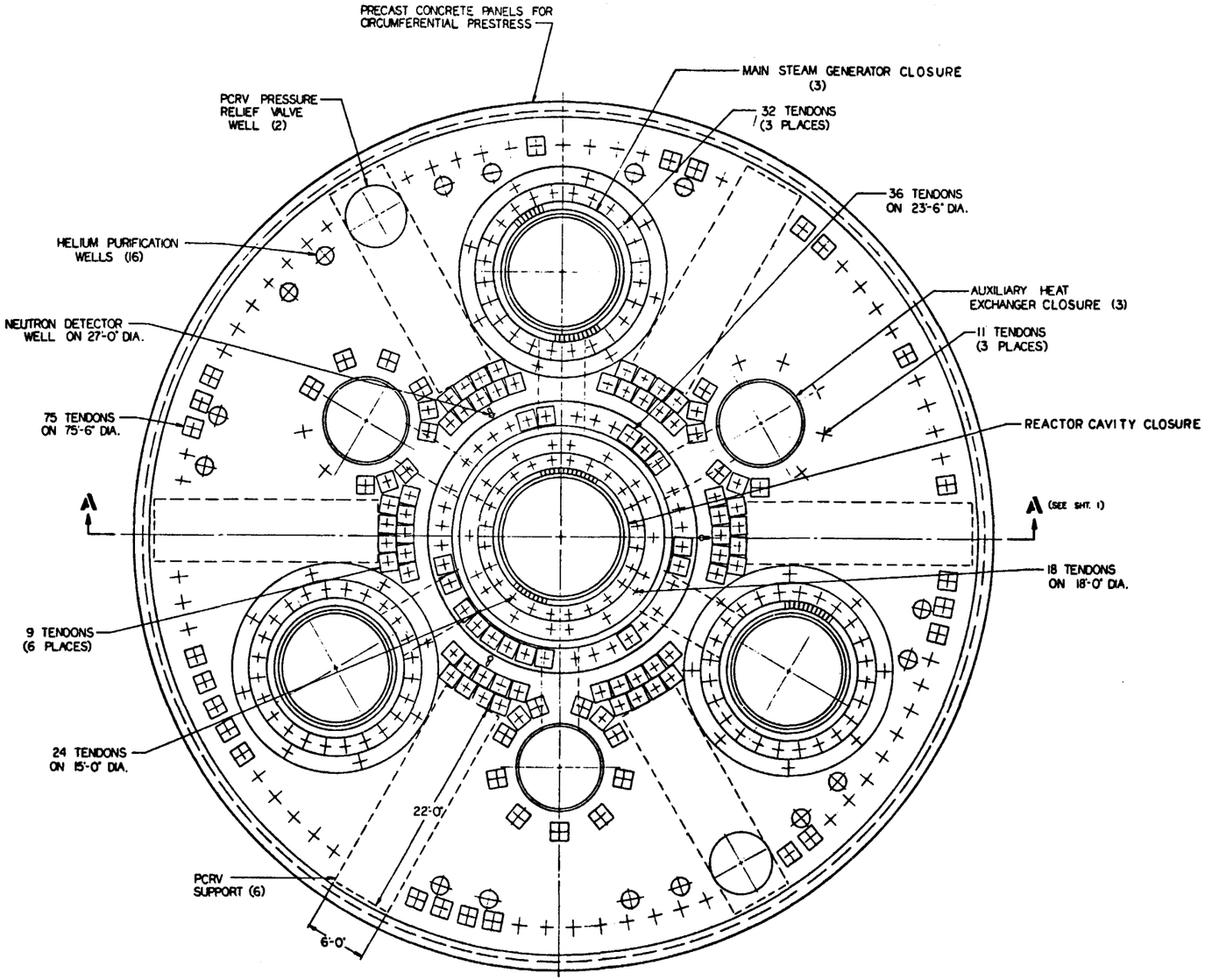


Fig. 5-1. Primary loop cavity arrangements in the PCRV

penetrations between the operating floor and the PCRV to the containment wall. These pipes and cables are then routed to their respective core auxiliary cooling water system components through protective barriers in the reactor auxiliary building.

The major secondary loop equipment items for both the MLCS and CACS are contained within the seismic category I reactor auxiliary building. Each of the redundant secondary loop equipment items is housed within a separately shielded enclosure, with both horizontal and vertical separation provided between the main and auxiliary loop equipment items.

5.2.2. Time Sequence of Operation

Figure 5-2 summarizes the time-dependent capability of the two RHR systems to remove the shutdown core heat load following reactor trip from 100% power. The MLCS capability varies depending on the operations of various main loop equipment items. The reduction in capability from improbable common mode outages of each of these equipment items is shown in the MLCS column. Without operation of the auxiliary boilers for long-term drive steam to the circulators, MLCS capability is limited to about 30 min of shutdown cooling. Without a shutdown feed supply, MLCS capability is limited to about 13 min on the stored water inventory in the steam generators. Without steam from the steam generator, MLCS capability is limited to about 1-1/4 min on the stored mechanical inertia in the main circulators. With no main circulation capability at all, about 1/2 min is available to prevent core damage from the thermal inertia of the core itself.

The CACS capability also varies according to auxiliary loops available. One auxiliary loop's heat rejection capability equals the decay heat level at approximately 20 min following shutdown. The capability of two or more auxiliary loops is limited by the design startup time of the system, currently set at 85 sec based upon considerations of the design basis depressurization accident (DBDA) PCRV blowdown time (Ref. 5-4).

SYSTEM CAPABILITY TO REMOVE SHUTDOWN HEAT LOAD

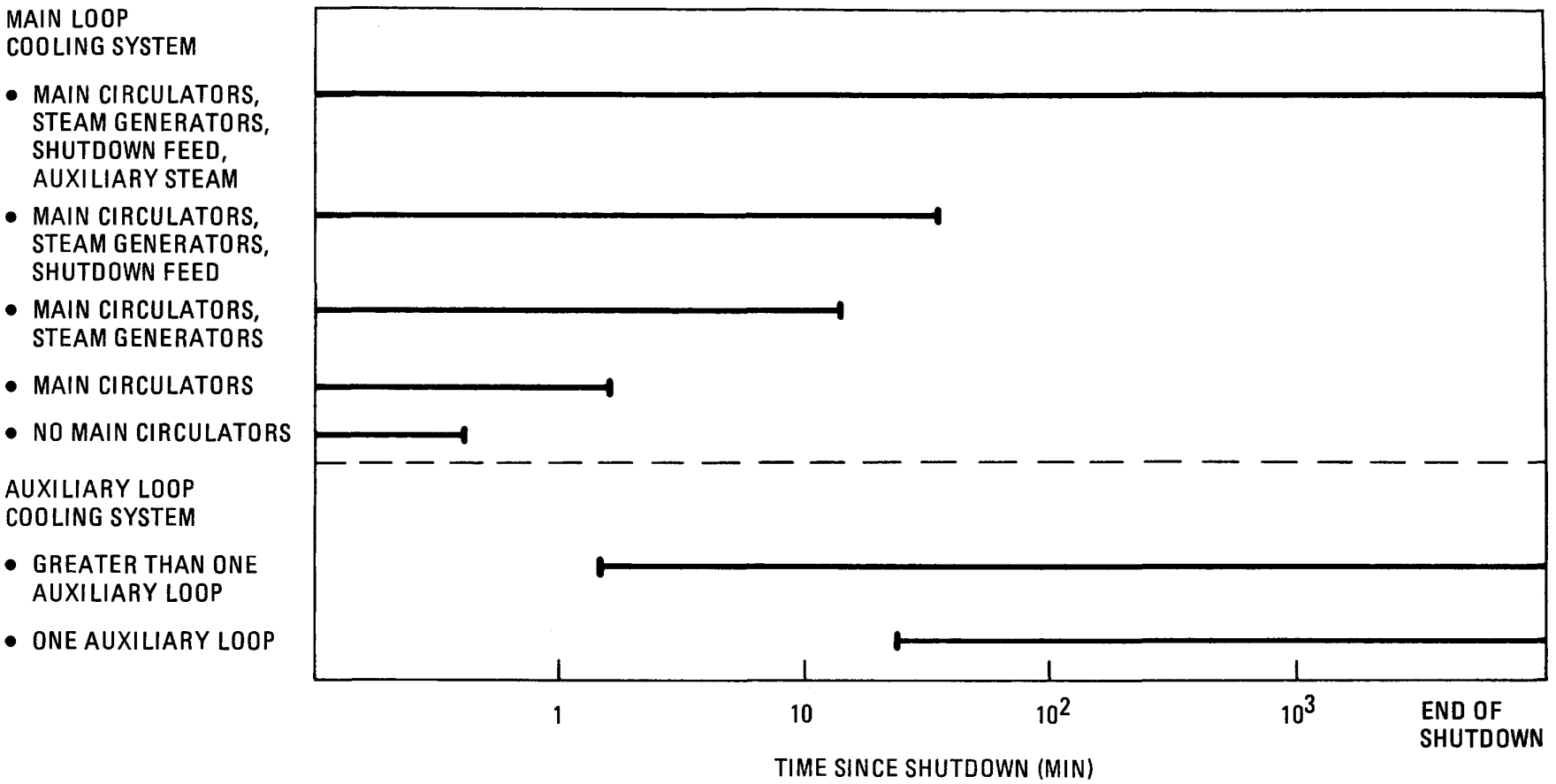


Fig. 5-2. System capability to remove shutdown heat load

As Fig. 5-2 shows, based on the current CACS startup time there is a brief period of reliance on the MLCS to bridge the time gap. Because the CACS does not serve as an independent backup during this period, the MLCS must perform this bridging function with high reliability, specifically with an unreliability lower than the target allocation of 10^{-6} per reactor year.

The lower end common cause failure fraction of 1% identified in Section 1 will serve to illustrate the difficulty of achieving an unreliability of less than 10^{-6}/yr for a redundant system with identical components. With such a common-cause failure fraction the individual equipment items must have failure rates of less than 10^{-8}/hr to achieve a system failure rate of less than 10^{-6}/yr. Such a low failure rate can only be found in passive or structural equipment features (as the summarized data in Appendix A show).

The design approach which has been taken to ensure that the MLCS can reliably bridge the CACS startup is to employ the stored thermal inertia of the steam generators for an ample period of circulator rundown. In principle this approach relies only upon maintenance of the more passive structural integrity of the steam generators, which could reasonably meet the 10^{-6} goal. In practice, however, the design has evolved with a number of complicating active component features (as indicated in Section 2) which could prevent the reliable continuation of this circulator drive source. Of particular concern are the operational protective system actions, which inhibit the steam generator supply to protect the main circulators and reactor core from damage. Although in principle such action can be limited to a single main loop by interlock devices, in practice it may be extremely difficult to ensure such interlocks provide a level of reliability commensurate with the 10^{-6}/yr goal.

If an unreliability of less than 10^{-6}/yr is to be achieved by the MLCS alone in a bridging function, reliance should be limited to passive features of the design. As described above, sole reliance upon the structural

integrity of the steam generators without the complexity of active equipment features may not be practical. As an alternative, it may be possible to ensure a high reliability of inertial flywheel coastdown of the main circulators using only passive features. As shown in Fig. 5-2, this may provide enough bridging capability even with the current CACS startup time.

As an alternative to designing the MLCS to provide a highly reliable bridging function, designs for the CACS which avoid any reliance upon the MLCS may be useful. As shown in Fig. 5-2, such a design could require very rapid (i.e., 1-1/2 min) but not necessarily impossible startup times for the CACS or provision of a CACS that is continuously running.

In sum, in the current design of the GCFR RHR systems a dependency does exist between the two RHR systems in that the CACS depends on a limited period of MLCS operation following shutdown. Either of two approaches can be taken to reduce the effect on reliability of this dependency: (1) assurance by design that the reliability of the MLCS in performing the bridging function is extremely high or (2) elimination of the dependency by providing a very rapid CACS capability. As noted previously, it is not clear that the current design approach employing the thermal inertia of the steam generators can, in practice, provide sufficient reliability assurance in consonance with the first approach. It is therefore recommended that steps be taken to improve the design capability in this area.

5.2.3. Degradation From Initiating Failures

The areas of commonality between the MLCS and CACS which are inherent in the design of the GCFR are the primary coolant and portions of the primary coolant circuit. Degradation in either area can commonly degrade the performance of both RHR systems.

5.2.3.1. Primary Coolant. The principal initiating failure which can significantly degrade the performance of both RHR systems in the GCFR is

the loss-of-coolant-pressure accident. This initiator effects a reduction in the primary coolant density, increasing the pumping requirements for both the main and auxiliary circulators. Because of this, the depressurization accident has been studied extensively and serves as the design basis accident for both RHR systems.

Events of concern, such as depressurization accidents, are failures of passive components providing part of the primary coolant boundary that result in loss of coolant. Figure 5-3 shows the basic elements of the primary coolant system and coolant boundary provided by the PCRV. Except for some small diameter outside lines and two PCRV relief trains, the GCFR reactor coolant system is entirely contained within the PCRV. The ultimate boundary for the reactor coolant is therefore provided by the PCRV liners and penetration liners and closures.

Figure 5-4 shows the basic relationship between PCRV depressurization rate and leak area. For leak areas smaller than 6 cm^2 (1 $in.^2$) (corresponding to the area of the largest outside line providing part of the primary coolant boundary) the depressurization rate is slow, taking several hours to reach equilibrium. More rapid PCRV depressurizations are limited in the GCFR design by incorporating flow restrictors in the major penetration closures. These flow restrictors limit the maximum depressurization area from a closure seal failure to less than 484 cm^2 (75 $in.^2$). This area therefore provides the upper limit for depressurization events other than those which might result from a gross structural failure of the PCRV. Because the class of leak areas designated as slow depressurizations [less than 6 cm^2 (1 $in.^2$)] have depressurization times commensurate with the annual PCRV depressurization for refueling, they do not pose a significantly abnormal cooling demand upon the RHR systems. Leak areas designated as rapid depressurizations are consequently of greater concern with respect to degradation of the normal performance of both RHR systems.

Because the PCRV is designed and constructed to the equivalent codes and standards for LWR vessels, the high reliability attained for LWR

vessels should apply as well (or better) to the GCFR PCRV. Disruptive failures of such vessels have been assessed to be less than 10^{-6} per vessel year (Ref. 5-2). The limiting rapid depressurization event may therefore be the rupture of a portion of the only large piping in the PCRV, which is associated with the PCRV relief train. The failure frequency for such an event may be conservatively assessed as less than 10^{-3} per reactor year based upon similar assessments for LWRs (Ref. 5-2) (a conservative assessment because the length of relief train piping is less than 1% of the large LOCA sensitive piping in a LWR). To achieve a target of less than 10^{-6}/yr for RHR failure, it is only necessary then that the combined failure probability of the MLCS and CACS be less than 10^{-3} per demand following a rapid depressurization.

Two separate redundancy states may be considered for the RHR systems following a rapid depressurization event. If the containment is isolated following the depressurization, the coolant backpressure is maintained at an equilibrium value which is approximately 2% of the normal operating pressure, and two of three main or auxiliary loops are capable of providing adequate coolant circulation and heat removal. This redundancy state is equivalent to that provided for pressurized plant trips, except that for pressurized trips the loop redundancy state is limited by heat removal capability only. Thus, since both systems are designed with margin for this low coolant density state and evidence the same redundancy following this accident as following the more frequent pressurized plant trips, the target should be met with ample margin. Since the allocated demand failure probability of the CACS is 10^{-4} per demand, the target might even be met by the CACS alone.

If the containment does not become isolated following the depressurization event, the coolant pressure will reach an equilibrium value which is approximately 1% of the normal operating pressure, and all three main or auxiliary loops may be required to provide adequate coolant circulation. Other sources (Refs. 5-1 and 5-2) estimate the failure probability of containment isolation to be in the range of 10^{-3} to 10^{-4} per demand.

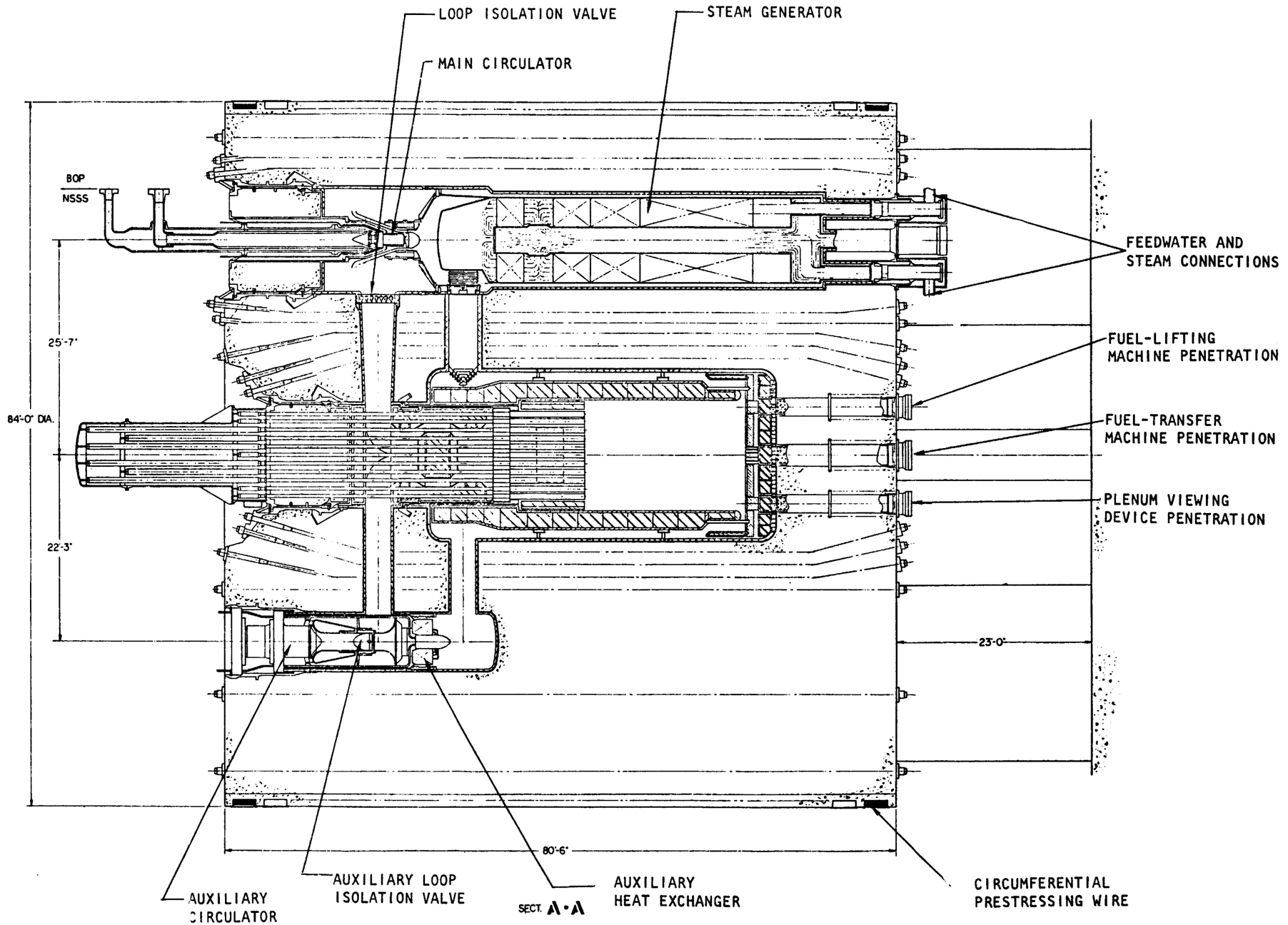


Fig. 5-3. Vertical section through PCRV showing reactor coolant system components

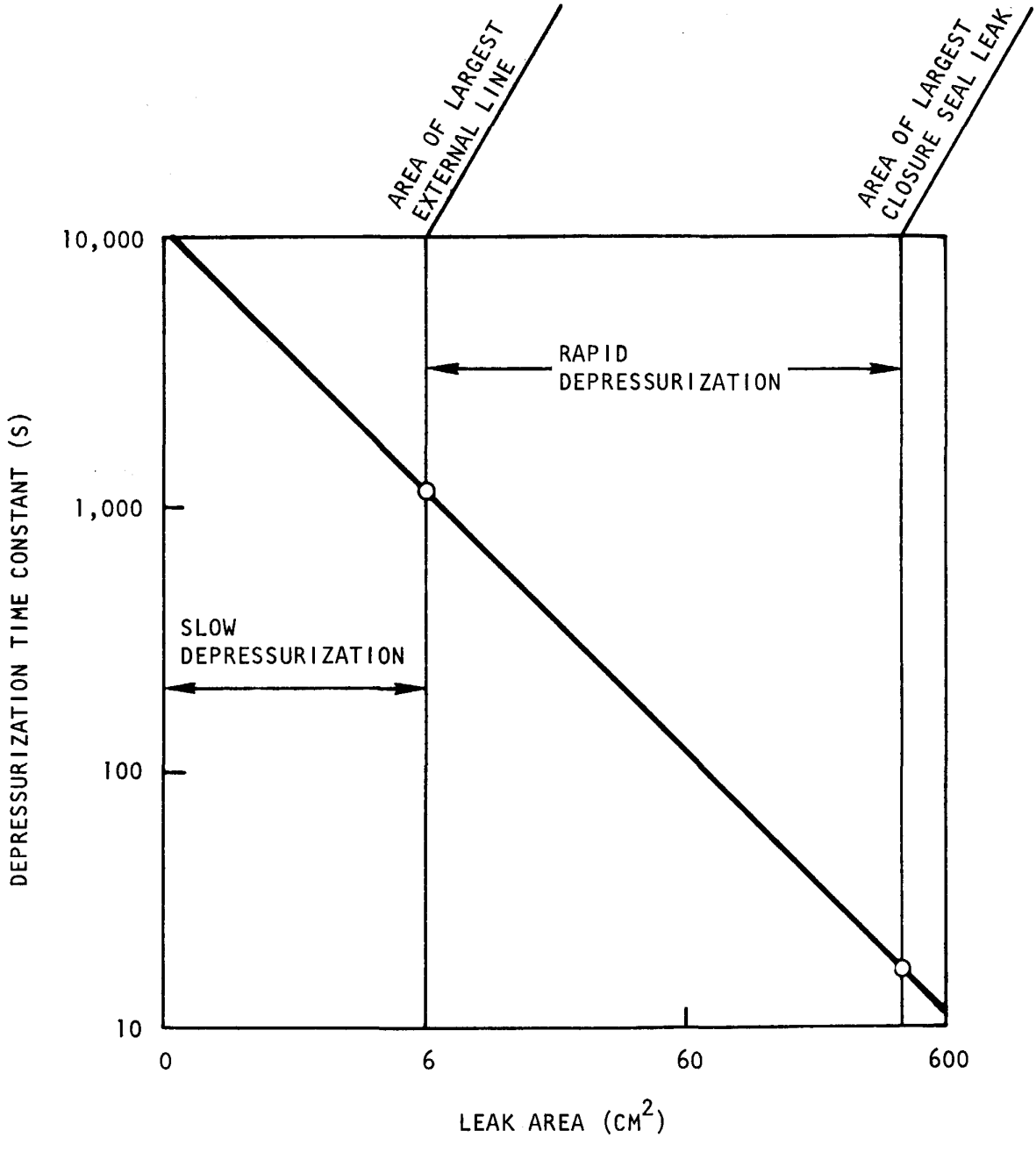


Fig. 5-4. Relationship between depressurization rate and leak area

The combined probability of a rapid depressurization and containment isolation failure would then be in the range of 10^{-6} to 10^{-7}/yr, requiring little or no margin in RHR system unreliability.

In sum, ample margin is provided in the RHR system design against the coolant-degrading effects of a rapid depressurization. This, coupled with the low probability of accident occurrence, should lead to an extremely low probability of RHR failure following a depressurization accident.

5.2.3.2. Primary Coolant Circuit. Except for potential isolation valve failures (see Fig. 5-3) a significant degradation of the primary coolant circuit in the GCFR would require the occurrence of a gross structural failure of the PCRV or core support structure. It is reasonable to expect that such structural failures can and will be made to be less probable than the 10^{-6}/yr goal considered here for RHR system failure.

Failure of the main loop isolation valves to close after a transfer to the CACS would allow some coolant flow to bypass the core through the shutdown main loops. With the reactor at full pressure, all three main loop isolation valves could fail to shut without degrading the redundancy of the CACS because of the margin provided in auxiliary circulator design for the design basis depressurization accident. Even following a rapid depressurization accident, multiple main loop isolation valve failures must occur to invalidate the auxiliary core cooling function. Appendix A shows that the generic failure rate for gas check valves is on the order of 10^{-4} per demand. Inability to frequently operate the main loop isolation valves may give a higher unavailability; therefore an unavailability of 10^{-3} (which is an order of magnitude higher than the generic failure rate) may be assigned to these valves. Allowing for a common cause failure fraction of 10%, the probability of common cause failure of all main loop isolation valves to shut would be of the order of 10^{-4} per demand. Since the allocated demand failure probability of the CACS is 10^{-4} per demand, the contribution of main loop isolation valve failures would not be significant.

In sum, no higher order primary coolant circuit faults have been identified which could degrade the RHR system operation to the point that the 10^{-6}/yr goal could not be attained.

5.3. EXTERNAL EVENTS

Potential external forces include both natural and manmade hazards. Severe external events such as large earthquakes, windstorms, floods, aircraft or turbine missiles, explosions, and acts of sabotage have the potential to cause common mode failure of plant equipment or structures, leading to failure of RHR. Such external events and their potential effects upon a reactor plant are largely generic with respect to reactor type. These events and similar occurrences are guarded against by design practices which adhere to the universally applicable industry and regulatory codes and standards. Such events have therefore not been analyzed in detail for purposes of this study. However, it may again be shown that the RHR support systems limit design reliability which might otherwise be achieved.

Possibly one of the most significant external forces in terms of potential common mode effects is a large earthquake. There is wide disagreement among experts, however, as to the frequency of large earthquakes, and there is evidence that the frequency of such events may vary by orders of magnitude from site to site. Hsieh (Ref. 5-5), whose work is used in WASH-1400 (Ref. 5-2), has estimated the frequency of design basis earthquakes [operating basis earthquake (OBE) and safe shutdown earthquake (SSE)] to be in the range of 10^{-3} to 10^{-4} and the frequency of earthquakes beyond design basis (up to 1.0 g ground accelerations) to be in the range of 10^{-4} to 10^{-6}/yr for typical eastern U.S. sites. Okrent (Ref. 5-6), in a survey of expert opinion on earthquake probabilities, indicates a frequency of 10^{-4}/yr for earthquakes of SSE magnitude and one of 10^{-6}/yr for earthquakes twice the magnitude of the SSE. Raabe (Ref. 5-1) indicates a range of 10^{-8} to 10^{-10}/yr for earthquakes of SSE magnitude to twice SSE magnitude based on a sampling of four U.S. reactor sites. Recent European work (Ref. 5-7) gives a range for central European sites of 10^{-4} to 10^{-7}/yr for

earthquakes equal to or greater than design basis. With this wide range of predicted frequencies for large earthquakes, it can only be estimated that the frequency of design basis earthquakes is in the range of 10^{-3} to 10^{-4}/yr and that the frequency of a seismic event greater than design basis is less than 10^{-4}/yr and may be highly site-dependent.

To estimate the probability of an earthquake-caused RHR failure, the likelihood of RHR equipment failure following the earthquake must also be considered. Estimates of earthquake-caused equipment failures have been provided in Refs. 5-2 and 5-8.

For illustrative purposes Table 5-4 summarizes an estimate of earthquake caused failure of both RHR systems. Table 5-5 summarizes the estimate of earthquake caused failure of RHR from support system dependencies. The former requires a failure of two independent seismic category I systems, the MLCS and CACS. The latter requires the failure of only one seismic category system, since systems supporting the MLCS are not seismic category I. In either case, however, it appears that the frequency of seismic caused RHR failure may present an external limit which closely approximates the allocated unreliability goal of 10^{-6}/yr.

REFERENCES

5-1. "HTGR Accident Initiation and Progression Analysis Status Report," ERDA Report GA-A13617, Volumes I - VIII, General Atomic Company, 1975-1977.

5-2. "Reactor Safety Study," USNRC Report WASH-1400, October 1975.

5-3. "Gas-Cooled Fast Breeder Reactor Accident Initiation and Progression Analysis Progress Report for the Period July 1, 1975 through June 30, 1976," ERDA Report GA-A14079, General Atomic Company, March 1977.

5-4. "Gas-Cooled Fast Breeder Reactor Preliminary Safety Information Document," Gulf General Atomic Report GA-10298, February 1971.

5-5. Hsieh, T., et al., "On the Average Probability Distribution of Peak Ground Acceleration in the U.S. Continent Due to Strong Earthquakes," University of California at Los Angeles Report UCLA-ENG-7516, March 1975.

TABLE 5-4
PROBABILITY OF EARTHQUAKE-CAUSED RHR SYSTEM FAILURE

Type of Earthquake	Probability of Earthquake (per yr)	RHR Failure Probability		Total (per yr)
		MLCS	MLCS and CACS	
OBE	1×10^{-3}	10^{-3}(a)	10^{-7}(a)	10^{-10}
SSE	1×10^{-4}	10^{-3}(b)	3×10^{-5}(b)	3×10^{-9}
>SSE	1×10^{-5}	10^{-1}(b)	3×10^{-2}(b)	3×10^{-7}
Total	--	--	--	3×10^{-7}

(a) Based on allocated system goals.

(b) Based on Ref. 5-2.

TABLE 5-5
PROBABILITY OF EARTHQUAKE-CAUSED RHR SUPPORT SYSTEM FAILURE

Type of Earthquake	Probability of Earthquake (per yr)	RHR Support System Failure Probability		Total (per yr)
		MLCS	MLCS and CACS	
OBE	1×10^{-3}	10^{-1}(a)	10^{-4}(b)	1×10^{-7}
SSE	1×10^{-4}	1	10^{-3}(b)	1×10^{-7}
>SSE	1×10^{-5}	1	10^{-1}(b)	1×10^{-6}
Total	--	--	--	1×10^{-6}

(a) Based on Ref. 5-8.

(b) Based on Ref. 5-2.

5-6. Okrent, D., "A Survey of Expert Opinion on Low Probability Earthquakes," Ann. Nucl. Energy 2 (1975), pp. 601-614.

5-7. Ahorner, L., and W. Rosenhaver, "Probability Distribution of Earthquake Accelerations with Applications to Sites in the Northern Rhine Area, Central Europe," J. Geophys. 41 (1975), pp. 581-594.

5-8. "CRBRP Risk Assessment Report," CRBRP-1, March 1977.

6. ACKNOWLEDGMENTS

This document was prepared by the Reactor Safety and Reliability Branch of the GCFR program. The authors would like to thank A. Torri, J. H. Broido, O. W. Reinsch, and G. W. Hannaman for their contributions to this report.

APPENDIX A
METHODOLOGY AND DATA

A.1. FAILURE DATA

The failure and repair data used in this analysis are taken from Ref. A-1, "GCR Data Bank Status Report," produced under the GCR Reliability Data Bank task. The purpose of the reliability data bank task is to obtain, supply, and store component and system reliability data required as the basic input in quantification of the event tree, fault tree, and reliability models. Data source inputs have been gathered over a number of years at GA but previously have not been formally tabulated for ease of source comparison and traceability to original references. The sources of reliability data are divided into four groups, (1) gas cooled reactor data, (2) U.S. nuclear, fossil, and industrial data, (3) summarized data, and (4) special reliability analysis estimates. The first two classifications include information found in literature describing actual failure incidents for a specified time period and number of components. In addition, most of the sources in classifications 1 and 2 contain considerable information regarding modes of failure and actual time to restore the system to operation. Classifications 3 and 4 include sources of reliability data which report failure rates but do not clearly specify the actual failures or time base experience. As a result, they are probably not independent of the data sources in the first two classifications. Based on the amalgamation of the tabulated data in Ref. A-1, realistically achievable reliability parameters have been assessed which are compatible with present component production technology.

Tables from Ref. A-1 are presented in this appendix. Tables A-1 and A-2 present the data used for the mechanical and electrical components generic to all power plants. Table A-3 presents the data used for

TABLE A-1
RELIABILITY DATA TABULATION

Mechanical Components Generic to Power Plants		Assessed Experience Values				
		Failure Rate (λ)	Range, Upper and Lower		Repair Time hr	Range, Upper and Lower
Component - System Identification	Failure Mode	hr = per hour D = per demand	Upper: 95%	Lower: 5%	Typical Hr	Lower: 5% Upper: 95%
Pumps - General						
Electric motor driven	Fail to start	1E-3/D	3	10	40	4 to 400
	Fail to run	3E-5/hr	3	10	40	4 to 400
Steam turbine driven	Fail to run	1E-4/hr	3	3	40	4 to 400
Condensate pumps	Fail to run	3E-5/hr	7	3	40	4 to 400
Positive displacement	Fail to start	1E-3/D	3	3	40	4 to 400
	Fail to run	3E-4/hr	3	10	40	4 to 400
Air ejector pumps	Fail to run	3E-5/hr	3	3	40	4 to 400
Blower/fans	Fail to operate	1E-5/hr	3	10	40	4 to 400
	Fail to start	3E-4/D	3	3	40	4 to 400
Valves - General						
Motor operated (includes valve operator)	Fail to change state	1E-3/D	3	3	24	3 to 3000
	External leak	1E-6/hr	3	80	24	3 to 3000
	Rupture	1E-8/hr	30	100	24	3 to 3000
Air solenoid	Fail to change state	3E-4/D	3	3	24	3 to 3000
	Fail to remain open	3E-6/hr	3	3	24	3 to 3000
	External leak	1E-6/hr	3	30	24	3 to 3000
	Rupture	1E-8/hr	30	100	24	3 to 3000
Manual	Fail to operate	1E-4/D	3	3	24	3 to 3000
	Leak	1E-6/hr	3	3	24	3 to 3000
Check valve	Fail to operate	1E-4/D	3	3	24	3 to 3000
	Reverse leak	3E/6hr	3	10	24	3 to 3000
	External leak	1E/6/hr	3	3	24	3 to 3000
	Rupture	1E-8/hr	30	100	24	3 to 3000
Relief valve	Fail to open	1E-5/D	3	3	24	3 to 3000
	Premature open	1E-5/hr	3	3	24	3 to 3000
	Fail to reclose	3E-3/D	10	10	24	3 to 3000
Modulating valve	Fail to modulate	1E-5/hr	10	10	24	3 to 3000
	Fail to open or close	3E-4/D	10	10	24	3 to 3000
	External leak	1E-6/hr	3	3	24	3 to 3000
Regulator valve	Fail to operate	1E-5/hr	10	10	24	3 to 3000
	Rupture	1E-8/hr	30	100	24	3 to 3000
Heat Exchangers		3E-5/hr	10	30	100	4 to 6000
Feedwater heater	Tube leak	1E-5/hr	3	3	30	4 to 200
Cooler	Tube leak	3E-6/hr	3	3	30	4 to 200
Desuperheater	Tube leak	1E-5/hr	10	10	30	4 to 200
Condenser	Leak	3E-5/hr	3	3	60	4 to 200
	Rapid loss of vacuum	1E-5/hr	3	10	60	4 to 200
Auxiliary Boiler	Fail to start	1E-2/D	3	3	40	4 to 500
	Fail to run	3E-4/hr	10	30	40	4 to 500
Tanks, Vessels	All modes	1E-8/hr	3	10	40	8 to 10^4
	Disruptive failure	1E-10/hr	30	30	40	8 to 10^4
Piping Per Section						
<3 in. diameter	Rupture/plug	1E-9/hr	30	30	30	2 to 100
>3 in. diameter	Rupture/plug	1E-10/hr	30	30	30	2 to 100

TABLE A-2
RELIABILITY DATA TABULATION

Electrical Components Generic to Power Plants		Assessed Experience Values				
		Failure Rate (λ)	Range, Upper and Lower		Repair Time (hr)	Range, Upper and Lower
Component - System Identification	Failure Mode	hr = per hour D = per demand	Upper: 95%	Lower: 5%	Typical Hr	Lower: 5% Upper: 95%
Electric Motors & Assoc. Equipment	Fail to start	3E-4/D	3	3	40	4 to 400
	Fail to run	1E-5/hr	3	3	40	4 to 400
Transformers	Open/short per winding	1E-6/hr	3	3	40	5 to 5000
	Short between winding(s)	1E-6/hr	3	3	40	5 to 5000
Circuit breakers	Fail to change state	1E-3/D	3	3	6	1 to 3000
	Premature transfer	1E-6/hr	3	3	6	1 to 3000
Batteries	Low output, shorted	3E-6/hr	3	3	5	1 to 100
	Fail to start	1E-3/D	3	3	5	1 to 100
Instrumentation					6	25 to 70
Solid state device	Fail to operate	1E-6/hr	10	3	6	25 to 70
	No output	3E-7/hr	3	3	6	25 to 70
	Calibration shift	3E-5/hr	3	3	6	25 to 70
Systems Diesel generator	Fail to start and load - 1st try	3E-2/D	3	10	21	1 to 400
	Fail to run	1E-3/hr	3	3	21	1 to 400
Off-site Power (OSP)	Loss due to turbine trip	1E-3/D	10	10	0.25	0.01 to 10
	Total loss of OSP	1E-5/hr	3	3	0.25	0.01 to 10

TABLE A-3
RELIABILITY DATA TABULATION

Selected Unique Gas-Cooled Reactor Components		Assessed Experience Values				
		Failure Rate (λ)	Range, Upper and Lower		Repair Time hr	Range, Upper and Lower
Component - System Identification	Failure Mode	hr = per hour D = per demand	Upper: 95%	Lower: 5%	Typical Hr	Lower: 5% Upper: 95%
Gas Circulators						
Steam driven machine, support system and control system	Fail to start	3E-3/D	3	3	100	2 to 1200
	Fail to operate	1E-4/hr	3	3	100	2 to 1200
Electricity driven machine, support system and control system	Fail to start	3E-3/D	3	10	100	2 to 300
	Fail to operate	1E-4/hr	3	3	100	2 to 300
Primary Coolant						
Heat exchangers		3E-5/hr	3	3	100	30 to 7000
Steam generator	Leak	3E-5/hr	3	3	100	30 to 7000
Reheator	Leak	1E-5/hr	3	3	100	30 to 7000
Core auxiliary heat exchanger	Leak	1E-5/hr	10	3	100	30 to 7000
Gas Valves						
Main loop isolation	Fail to change state	1E-4/D	3	3	100	2 to 1000
	Spurious operation	3E-6/hr	10	10	100	2 to 1000
	Bypass leak	3E-6/hr	10	10	100	2 to 1000
Auxiliary loop check valve	Fail to change state	1E-4/D	3	3	100	2 to 1000
	Spurious operation	1E-6/hr	10	10	100	2 to 1000
	Bypass leak	3E-6/hr	10	3	100	2 to 1000

components unique to gas-cooled reactors. For the latter data tabulation an experience base of over 500 reactor years of European GCR operation has been utilized.

A.2. QUANTITATIVE ESTIMATE OF LOOP FAILURE RATES AND REPAIR TIMES

Standard reliability methods and approximations were utilized in order to estimate the loop failure rates and repair times from the component data given in Section A-1. For each loop an RFBD was constructed as described in Sections 2 through 4. To estimate a loop failure rate (λ) and its MTTR, tables were set up listing each component in the RFBD along with its λs and MTTR.

The assumed initial condition was that the plant was on-line and producing 100% power. The components were assumed to be in their normal operating status for the plant at 100%. Assuming plant shutdown, the applicable λs were used and summed as follows:

a. If the component was required to continue running, only the hourly λs were used.

b. If the component was required to start and run (pumps, diesel generators, etc.), both the demand and hourly λs were used.

c. If the component was required to change state (valves) and not leak, the demand and hourly λs were used.

The demand and hourly λs were separately summed.

If components are in series within a loop, the $\Sigma\lambda$s will be the equivalent λ for the loop. However, if redundancies exist within a loop, these λs can no longer be summed. Redundancies within a loop, primarily valves, were handled as follows:

1. For demand failure rates (λ_D):

   a. For diverse actuation, the product of the λ_Ds was used.

   b. For common actuation, a common cause factor of 0.1 was assumed; thus $0.1\lambda_D$ was assumed.

2. For running failure rates (λt):

   The λ_ts for valves are relatively low; thus these terms will not significantly affect the failure rates of a loop and were not therefore considered.

For the loop MTTR, a weighted average was calculated for the loop, as follows:

$$\text{MTTR Loop} = \frac{\sum \lambda_i \times \text{MTTR}_i}{\sum \lambda_i} \quad . \qquad \text{(A-1)}$$

A.3. QUANTITATIVE ESTIMATE OF SYSTEM FAILURE RATES

Standard reliability methods and approximations were used to estimate the system failure probabilities from the loop estimates calculated, as described in Section A.2.

A.3.1. Demand Failure Rate

For calculation of the demand failure rate of Λ_D of a system with n identical redundant loops, r of which must fail to cause system failure, the following was used:

$$\Lambda_D = \sum_{i=r}^{n} n_i \cdot \lambda_D^{\,i} \cdot (1 - \lambda_D)^{n-i} \quad . \qquad \text{(A-2)}$$

A.3.2. Running Failure Rate

For calculation of the running failure rate (Λ_t) of a system with n identical loops, all of which must fail to cause system failure, the following was used:

$$\Lambda_t = n\, q^{n-1}\, \lambda_t \quad , \qquad \text{(A-3)}$$

where q is the total component unavailability (i.e., $q = \lambda_D$ if the loops are in passive redundancy and $q = \lambda_t \cdot MTTR_t$ if the loops are in active redundancy).

For the special case where either the MLCS or CACS can be used and where different redundancy levels may exist, the running failure rate (Λ_t) may be approximated by:

$$\sum \Lambda_{RHR} = \sum_{j=1}^{3} \sum_{i=1}^{3} f_{ij} \left[i q_{ML}^{i-1}\, q_{AL}^{j}\, \lambda_{ML} + j\, q_{AL}^{j-1}\, q_{ML}^{i}\, \lambda_{AL} \right] \quad , \text{(A-4)}$$

where:

f_{ij} = fraction of outages with i main loops and j auxiliary loops available,*

q = main loop unavailability,

q_{AL} = auxiliary loop unavailability,

λ_{ML} = main loop failure rate per hour,

λ_{AL} = auxiliary loop failure rate per hour.

*As described in Section 1, for the purpose of this study $f_{3,3} = 0.75$; $f_{2,3} = 0.20$; $f_{3,2} = 0.05$; all other f_{ij} were assumed negligibly small.

Similarly the failure rate of the MLCS (λ_{MLCS}) may be approximated by:

$$\lambda_{MLCS} = \sum_{j=1}^{3} \sum_{i=1}^{3} f_{ij} \left[{}^{i-1}q_{ML} \quad \lambda_{ML} \right] \quad . \qquad \text{(A-5)}$$

Because the main loops do not have a rapid start capability, it may be assumed that they must be maintained in a near operational readiness condition to be effective. For this reason the main loop unavailability is given by the unrepaired loop unavailability contribution, so that the loop unavailability is of the form:

$$q_{ML} = \lambda_t \cdot MTTR_t \quad , \qquad \text{(A-6)}$$

where $\lambda_t = \lambda_{ML}$ = main loop failure rate per hour,

and

$MTTR_t$ = main loop mean repair time in hours.

Since the auxiliary loops do have a rapid start capability, it is assumed that they are maintained in a dormant standby condition so that the loop unavailability is of the form:

$$q_{AL} = \lambda_d \quad ,$$

where λ_d = auxiliary loop demand failure rate.

REFERENCE

A-1. Hannaman, G.W., "GCR Reliability Data Bank Status Report," DOE Report GA-A14839, General Atomic Company, to be published.

APPENDIX B
FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

FMEAs were performed for the MLCS (Table 2-1) and the CACS (Table 3-1). These FMEAs considered the major equipment items, active mechanical components, and single passive mechanical components.

The MLCS FMEA (Table 2-1, Sheets 1 to 6) assumed the following:

1. The design is adequate

2. Initial conditions were as follows:

   a. Plant at full power

   b. Plant shutdown (PSD)

3. Limiting conditions for heat rejection to atmosphere.

   a. 13 min operation with steam generator inventories (3 loops) until feedwater is required.

   b. 30 min operation with core residual heat until auxiliary steam is required.

   c. 22 hr of operation before plant water inventories are depleted and closed secondary loop is required.

The MLCS FMEA also indicates the time when all MLCS will be lost and CACS will be required. The following times were used:

30 sec	Circulator coastdown
35 sec	SG boil-out with main control valve open
3 min	SG boil-out with small control valve open

The CACS FMEA assumed the following:

1. Loss of MLCS in <15 min after reactor scram and turbine trip from full power, requiring at least 2 of 3 CACS loops.

2. Loss of MLCS in > 15 min after reactor scram and turbine trip from full power, requiring at least 1 of 3 CACS loops.

Two other FMEAs were performed regarding the effect of the MLCS and the CACS, given the loss of a support system. These effects are shown in Table 4-2 for the support systems associated with the MLCS and CACS.

Table 4-2, sheets 1 through 4, the FMEA of support systems for MLCS, also indicates the time when MLCS will be lost and CACS will be required.

Table 4-3, sheet 1, the FMEA of support systems for CACS, indicates the best current estimate of the CACS capability, given the loss of its support system.