DOE-HTGR-86-011
Revision 3
Volume 1

PROBABILISTIC RISK ASSESSMENT FOR THE STANDARD MODULAR HIGH TEMPERATURE GAS-COOLED REACTOR

AUTHORS/CONTRACTORS

GA TECHNOLOGIES INC.

ISSUED BY GA TECHNOLOGIES INC.
FOR THE DEPARTMENT OF ENERGY
CONTRACT DE-AC03-84SF11963

JANUARY 1987

Department of Energy
Washington, DC 20585

February 8, 1995

Project No. 672

Mr. Jack Donohew
MHTGR Project Manager
Advanced Reactor Project Directorate
Associate Directorate for Advanced Reactors
and License Renewal
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

Dear Mr. Donohew:

In the May 26, 1993, letter from Mr. J. D. Griffith to Mr. D. M. Crutchfield, the Department of Energy committed to release the "Applied Technology" material associated with the preapplication review for the Standard Modular High Temperature Gas-Cooled Reactor in a timeframe to support the issuance of the Preapplication Safety Evaluation Report (PSER) by the Nuclear Regulatory Commission (NRC). It is our current understanding, based on our meeting with NRC personnel of September 29, 1994, that the PSER is to be completed by February 28, 1995.

We hereby authorize NRC to remove the "Applied Technology" distribution restriction and place the following reports into the NRC Public Document Room. These reports are titled "Preliminary Safety Information Document for the Standard Modular High Temperature Gas-Cooled Reactor" and "Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor." These documents are identified as follows:

HTGR-86-024, Volumes 1 through 6, and
DOE-HTGR-86-011, Volumes 1 and 2

Sincerely,

Frank J. Goldner, for

John W. Herczeg
Civilian Reactor Development
Office of Nuclear Energy

cc: R. M. Forssell, GA
R. R. Mills, PDCO

Department of Energy
Washington, DC 20585
February 7, 1995

Project Number 672

Document Control Desk
U.S. Nuclear Regulatory Commission
Mail Station P1-137
Washington, D.C. 20555

In the meeting between the Department of Energy (DOE) and the Nuclear Regulatory Commission (NRC) held September 29, 1994, the question was raised about the proprietary classification of Volume 2 of the Modular High Temperature Gas-Cooled Reactor (MHTGR) Probabilistic Risk Assessment (PRA).

Please note that in a May 21, 1991, letter from G. C. Bramblett to J. Donohew, it was reported that the proprietary information in Volume 2 had been released with unlimited rights to the U.S. government. For NRC purposes, this can be interpreted to mean that DOE no longer requests that the document be withheld from the Public Document Room under the provisions of 10 CFR 2.790.

However, as noted in that May 21, 1991, correspondence, the MHTGR PRA is still considered Applied Technology and should be so protected.

Sincerely,

John W. Herczeg
Civilian Reactor Development
Office of Nuclear Energy

DOE–HTGR–86–011
Revision 3
GA–C18718
Volume 1

PROBABILISTIC RISK ASSESSMENT FOR THE STANDARD MODULAR HIGH TEMPERATURE GAS–COOLED REACTOR

Issued By:
GA Technologies Inc.
P.O. Box 85608
San Diego, California 92138-5608

DOE Contract No. DE–AC03–84SF11963

GA Project 6300

JANUARY 1987

LIST OF EFFECTIVE PAGES

Page	Revision	Date
Cover	3	1/87
i (Title Page - reverse side blank)	3	1/87
iii (reverse side blank)	3	1/87
v through xiii (reverse side blank)	3	1/87
xv through xvi	3	1/87
1-1 through 1-4	3	1/87
2-1 through 2-6	3	1/87
3-1 through 3-11	3	1/87
4-1 through 4-68	3	1/87
5-1 through 5-31	3	1/87
6-1 through 6-101	3	1/87
7-1 through 7-8	3	1/87
8-1 through 8-15	3	1/87
9-1 through 9-19	3	1/87
10-1 through 10-2	3	1/87
A-1 through A-27	3	1/87

CONTENTS

SUPPLEMENT

FIGURES

FIGURES (Continued)

FIGURES (Continued)

FIGURES (Continued)

FIGURES (Continued)

TABLES

TABLES (Continued)

ABBREVIATIONS

AIPA	accident initiation and program analysis
ATWS	anticipated transients without scram
BOP	balance of plant
EAB	exclusion area boundary
ECS	energy conversion system
EPZ	emergency planning zone
HPS	helium purification system
HTGR	high-temperature gas-cooled reactor
HTS	heat transport system
LBE	licensing basis event
LOSP	loss of normal station power
LWR	light water reactors
MHTGR	modular high-temperature gas-cooled reactor
NCSS	neutron control subsystem
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
OBE	operating basis earthquake
PAG	protective action guides
PPIS	plant protection instrumentation system
PRA	probabilistic risk assessment
PSID	preliminary safety information document

RCCS	reactor cavity cooling system
RPCWS	reactor plant cooling water subsystem
RSCE	reserve shutdown control equipment
RSCM	reserve shutdown control material
RSS	reserve shutdown system
SCS	shutdown cooling system
SCWS	shutdown cooling water subsystem
SPS	safety protection subsystem
SSE	safe shutdown earthquake
SWS	service water subsystem
TBCCWS	turbine building closed cooling water subsystem
UPS	uninterruptible power supply
U.S.	United States

1. SUMMARY

With the concurrence of the U.S. Nuclear Regulatory Commission (NRC) (Ref. 1-1), the Licensing Plan for the Standard High Temperature Gas-Cooled Reactor (HTGR) (Ref. 1-2) describes an application program consistent with 10CFR50, Appendix O to support a U.S. NRC review and design certification of an advanced Standard Modular High Temperature Gas-Cooled Reactor (MHTGR) design. Consistent with the NRC's Advanced Reactor Policy (Ref. 1-3), the Plan also outlines a series of preapplication activities which have as an objective the early issuance of an NRC Licensability Statement on the Standard MHTGR conceptual design.

This Probabilistic Risk Assessment (PRA) Document has been prepared as one of the submittals to the NRC in support of preapplication activities on the Standard MHTGR. Other submittals to be provided include a Preliminary Safety Information Document (PSID) (Ref. 1-4), a Regulatory Technology Development Plan (Ref. 1-5), and an Emergency Planning Bases Report (Ref. 1-6).

The basis for the PRA assessment is the conceptual MHTGR design as presented in the PSID. The MHTGR plant is comprised of four reactor modules and two turbine generator sets which combine to achieve a nominal plant rating of 558 MW(e). Each reactor module is housed in a vertical cylindrical concrete enclosure which is fully embedded in the earth. Each module contains separate, vertically positioned reactor and steam generator vessels connected by a horizontal coaxial cross duct. Located within the reactor vessel is the reactor core comprised of an annular array of fueled prismatic graphite blocks. Graphite reflectors, support structures, and restraining devices are installed in the reactor vessel as well. Each reactor module has a thermal rating of 350 MW.

A unique aspect of the MHTGR is that design features and parameters have been selected so as to minimize the need for reliance on active safety components such as pumps, motors, valves, and associated support systems. In particular, the reactor core size, geometry, and power density have been selected such that decay heat can be removed from the core solely by the inherent mechanisms of radiation and conduction, thus eliminating any reliance on forced coolant convection, or even the need for coolant, to prevent a significant radionuclide release from occurring. Additionally, the fuel type and enrichment have been selected so as to favor an intrinsically strong negative temperature coefficient, thus the reactor tends to inherently shut itself down in the event of undercooling or overpower transients. This combination of features results in a design which displays an unusually high level of safety.

The objective of the PRA is to

1. Provide a means of characterizing the safety of the MHTGR such that the conceptual design can be evaluated in a logical fashion.

2. Provide the basis for the selection of the licensing basis events (LBEs) evaluated in the PSID.

3. Evaluate a wide spectrum of events with offsite consequence to show compliance with Protective Action Guides (PAGs) at the exclusion area boundary in support of the Emergency Planning Bases report.

4. Evaluate the risk to the public due to accident releases from the standard MHTGR to show compliance with the NRC safety goals.

The scope includes frequency and consequence assessments for a wide spectrum of events with frequencies greater than once in one

hundred million years. An uncertainty evaluation for both the frequency and the consequence assessment is included.

Relative to the three levels of PRA defined in the Procedures Guide (Ref. 1-7), this study is similar to the most comprehensive (level 3) study. However, the conceptual status of the design clearly limits both the breadth and depth of this assessment relative to a level 3 PRA for an existing plant.

The PRA assessment examined a broad event spectrum in order to identify events potentially dominant with respect to plant safety. From this examination, seven initiating events were selected for detailed evaluation:

1. Primary coolant leaks.
2. Loss of main loop cooling.
3. Seismic activity.
4. Loss of offsite power and inadvertent turbine trip.
5. Anticipated transients requiring reactor scram.
6. Control rod group withdrawal.
7. Steam generator leaks.

From these seven initiating events only primary coolant leaks, seismic activity, and steam generator leaks were found to result in potential offsite releases. The fission product release scenarios include depressurization of the reactor vessel under dry and wet core conditions with or without forced cooling. The accidents under dry conditions are initiated by primary coolant leaks and earthquakes. The accidents under wet conditions are initiated by the steam generator leaks. In these accidents the core cooling can be provided either by one of two forced cooling systems or by conduction through the reactor to remove heat out to the reactor cavity cooling system.

A review of the assessment results confirms the selection of the Licensing Basis Events included within the PSID to be appropriate and consistent with this latest study. The PRA results confirm that even when a broad range of accidents that cover both a large cross section of initiating events and an extreme frequency spectrum is considered, the assessment of plant risk shows the MHTGR to be insensitive to failures in active and engineered systems. The frequency of potential radioactivity releases is essentially dictated by the failure of passive structures in the MHTGR. By virtue of its high reliance on passive features and inherent characteristics in this small MHTGR, the overall safety of the concept is shown to display unusually high levels of safety. The concept is shown to comply with the risk limits of the NRC Safety Goals and to do so with substantial margin. The MHTGR is even shown to satisfy the very stringent user-imposed requirement that PAG doses related to public evacuation and sheltering are met at the 425 m (1400 ft) site Exclusion Area Boundary. PRA results demonstrate that releases with frequencies as low as 5×10^{-7} per year are below the PAG sheltering limits of 1 Rem whole body and 5 Rem thyroid at the site EAB.

1.1. REFERENCES

1-1. U.S. Nuclear Regulatory Commission, Letter from William Dircks to James Vaughn, July 11, 1985.

1-2. "Licensing Plan for the Standard HTGR," DOE Report HTGR-85-001, Rev. 3, February 1986.

1-3. U.S. Nuclear Regulatory Commission, "Policy for the Regulation of Advanced Nuclear Power Plants," 51FR24643, July 8, 1986.

1-4. "Preliminary Safety Information Document for the Standard MHTGR," DOE Report HTGR-86-024, September 1986.

1-5. "Regulatory Technology Development Plan for the Standard MHTGR," DOE Report HTGR-86-064, January 1987.

1-6. "Emergency Planning Bases for the Standard MHTGR," DOE Report HTGR-87-001, (to be issued).

1-7. "PRA Procedures Guide," NRC Document NUREG/CR-2300, January 1983.

2. INTRODUCTION AND OBJECTIVES

Probabilistic Risk Assessment (PRA) provides a logical and structured method to evaluate the overall safety characteristics of a large and relatively complex engineered system, such as a nuclear power station. As with any evaluation of safety, the PRA presents radionuclide releases and health consequences that might result from various accident scenarios. Since the PRA is a realistic, plant-wide evaluation, it considers the interdependence of the many plant systems both within and outside the nuclear island. Furthermore, the use of probabilistic techniques in the analysis allows for explicit accounting of uncertainty. Finally, only a probabilistic assessment, by associating frequencies and consequences with each of the accident sequences, allows for comparison of their relative importance to safety and allows quantification of the cumulative risk to the public from operation of the plant.

PRA has been utilized extensively since the inception of the MHTGR project both to evaluate the developing concept relative to its design goals and to provide guidance to the designers regarding trade-offs and optimizations that are considered. In addition, risk assessment results have been used in the selection of licensing basis events (LBEs) (Ref. 2-1) and the safety classification of plant systems, structures, and components (Ref. 2-2) for the Preliminary Safety Information Document (PSID) (Ref. 2-3). With the MHTGR now in the conceptual design phase, this work represents the most extensive evaluation yet made. Relative to the levels, one through three, of PRA defined in the Procedures Guide (Ref. 2-4), this study is closest to the most comprehensive (level 3) study. Clearly, however, the early stage of the design still limits this assessment relative to a level 3 PRA for an existing plant.

2.1. INTRODUCTION

The basis for this PRA is the conceptual design as presented in the PSID. The scope includes frequency and consequence assessments for a wide spectrum of events with frequencies greater than one in one hundred million years (10^{-8} per year). The assessment considers both events in which the system failure probabilities are not strongly coupled (e.g., loss of main loop cooling) and two of the most important external events (loss of offsite power and earthquakes) in which the initiating event can simultaneously threaten multiple plant systems.

The methodology employed includes the standard features of a PRA: (1) initiating event selection, event tree construction, fault tree, common mode failure, and uncertainty analyses leading to sequence probability quantification; and (2) transient, radionuclide transport, dose, and uncertainty analyses leading to sequence consequence quantification. An important element in the methodology is the use of a master logic diagram (similar to fault tree). A master logic diagram provides a logical framework to guide the selection and grouping of accident-initiating events and ensure completeness. The data bank employed draws upon nonnuclear, light water reactor and gas-cooled reactor power plant experience. The Beta Factor method utilized for the assessment of common mode failures compensates for the lack of sufficient design detail to explicitly model systems' interactions. The event tree quantification appropriately utilizes the fault tree probabilities by accounting for conditional probabilities. The transient and radionuclide transport analyses consider the physical phenomena and the timing specific to the MHTGR. For both the sequence frequency and consequence quantification, Monte Carlo uncertainty propagation techniques are employed.

2.2. PROGRAMMATIC OBJECTIVES

This PRA of the conceptual design of the Standard MHTGR is one of several documents submitted as part of the MHTGR's Licensing Plan to

obtain a preapplication licensability statement from the Nuclear Regulatory Commission (NRC). In particular the PRA is a companion document to the PSID which describes the design and presents the accident analyses to show compliance with the top-level regulatory criteria 10CFR50 Appendix I and 10CFR100 offsite doses. In addition, this PRA document is a key basis for the Emergency Planning Bases Document (Ref. 2-5) which will present the approach to emergency planning. Specifically, this approach uses the PRA results to show that accidental releases from the MHTGR are less than the Protective Action Guides (PAGs) (Ref. 2-6) measured at the site boundary for all events with mean frequency greater than 5×10^{-7} per year (Ref. 2-7).

In fulfilling this role, the principal programmatic objectives of the PRA are as follows:

1. Provide a means of characterizing the safety of the MHTGR such that the conceptual design can be evaluated in a logical fashion.

2. Provide the basis from which to select the MHTGR LBEs evaluated in the PSID.

3. Evaluate a wide spectrum of events with offsite doses to show compliance with PAGs at the site boundary in support of the Emergency Planning Basis document.

4. Evaluate the MHTGR risk to the public to show compliance with the NRC safety goals.

2.3. RISK ASSESSMENT OBJECTIVES

There are a number of primary objectives for the risk assessment. The assessment should

1. Be systematic in that the relations of events to each other in an accident can be clearly seen, and that the range of alternatives in the stages of an accident are evident.

2. Include quantitative estimates of likelihoods or probabilities in such a way as to make coherent probabilistic statements.

3. Strive for balanced completeness in failure modes, without excluding significant cases of multiple failures.

4. Assess physical phenomena on a realistic basis without use of conservatisms which violate physical laws.

5. Deal explicitly with statistical uncertainties.

The resulting analyses should provide technical insight regarding accidents important to safety. This includes the kind of accident, the equipment involved, and the transport paths for fission products if they pose a hazard to the public. These results are a starting point for considering any design options which may be important. The results also contribute toward the technical basis for verifying the safety of the power plant.

2.4. REPORT CONTENT

This report documents the analysis and results of a safety risk assessment for the Standard MHTGR using PRA techniques. Section 3 describes the methodology followed for the probabilistic safety risk assessment. Section 4 gives a brief description of the plant systems

important to safety risk. These systems were analyzed in the risk assessment. Initiating events with a potentially significant safety impact are identified in Section 5. Section 6 provides an overview of the MHTGR plant response to the initiating events. System fault trees are then presented. Section 7 presents a summary of the event frequency assessment, while Section 8 summarizes the dose consequences in terms of physical phenomena leading to fission product release. The results, in terms of safety risk, are discussed in Section 9. Specifically, Section 9 includes

1. Quantification of risk and identification of the important accident sequences which dominate risk.

2. An interpretation of what the results imply about the MHTGR design and what they mean in terms of public health.

3. Confirmation of the LBE selection (Ref. 2-1) made in support of the PSID.

4. A judgment as to the acceptability of the calculated radiological doses by comparing them to the dose criteria of Section 2.2.

Section 10 identifies specific responses requested of the NRC with respect to PRA. Four technical appendices are also provided. Appendix A contains data for predicting the frequency and size distribution of primary coolant leaks. Appendix B contains the probabilistic data base used in the frequency quantification of Section 7. Appendix C contains a detailed description of the accident frequency assessment. Appendix D discusses in greater detail the dose assessments made.

2.5. REFERENCES

2-1. Licensing Basis Events for the Modular HTGR," DOE Report HTGR-86-034, April 1986.

2-2. "Equipment Classification List for the Modular High-Temperature Gas-Cooled Reactor," DOE Report HTGR-86-032, Rev. 1, September 1986.

2-3. "Preliminary Safety Information Document for the Standard MHTGR," DOE Report HTGR-86-024, September 1986.

2-4. "PRA Procedures Guide," NRC Report NUREG/CR-2300, January 1983.

2-5. "Emergency Planning Bases for the Standard MHTGR," DOE-HTGR-87-001 (to be issued).

2-6. Manual of Protective Action Guides and Protective Actions for Nuclear Incidents, EPA Report EPA-520/1-75-001, September 1975 (Revised June 1980).

2-7. "Licensing Basis Event Selection Criteria," DOE Report HTGR-86-001, Rev. 1, February 1986.

3. PROBABILISTIC RISK ASSESSMENT METHODOLOGY

The PRA analysis tasks and the application of the risk assessement results are shown in Fig. 3-1*. The rectangles represent the major analysis tasks and the ovals indicate the important sources of information required to perform each task.

The overall method, consistent with Ref. 3-1, is to select initiating events on as broad and rational a basis as possible and to develop event trees that form the basis for identifying various accident sequences that could result from the initiating events. The probability of occurrence of each event along each of the accident sequences in the event trees is obtained with the use of fault trees which logically relate the events in question to more basic events that are quantified in terms of reliability experience data with similar systems and components. It is important that dependencies among events are identified in the event trees and fault trees and that the effects of common mode failures are considered so that realistic probability predictions can be obtained.

The consequences of the accident sequences are then estimated in terms of the effect on the health and safety of the public. Generally, this is in terms of radiological dose in Rem. In performing the sequence consequence quantification, emphasis is directed toward a physically realistic assessment instead of a conservative assessment. Since uncertainty analyses are part of the consequence assessment, a PRA provides the expected (mean) consequences that result from an accident (along with confidence limits on the consequences), instead of a "bounding" estimate of unknown conservative magnitude.

*Figures are located at the end of each section.

PRA results are ultimately used to support plant design and licensing.

3.1. INITIATING EVENT SELECTION

The analysis begins with the selection of initiating events. Initiating events are events which disturb the plant from its normal states, either operating or shutdown sufficiently to result in conditions which could culminate in a release of radioactivity. With regard to fuel inventory, initiating events affecting this source of radioactivity would also likely lead to conditions requiring a plant trip (i.e., either a reactor trip, turbine trip, or both). The selection of initiating events considers each radioactivity source in the plant. Events are postulated which may defeat or degrade the barriers to release from each source. Plant outage causes are also evaluated as candidate initiating events, since they disturb the plant from its normal power producing state.

An analytical tool used to organize the process of selecting initiating events is the master logic diagram. The master logic diagram for this risk assessment is presented in Section 5. The master logic diagram provides a logical framework to identify ways in which uncontrolled or unscheduled radiological releases may occur from the plant. The events which may initiate such release sequences are initiating events. Beginning with the topmost level in the master logic diagram, each succeeding level can be constructed in a logical manner. This is accomplished in the upper regions of the master logic diagram by identifying all radionuclide sources in the plant (e.g., the MHTGR fuel body inventory) and the barriers that retain them (e.g., the fuel particle coatings and primary coolant boundary). Also implicitly included in the master logic diagram are plant structures and systems that can mitigate offsite doses if a release occurs. The lower regions of the master logic diagram are completed by incorporating the physical mechanisms capable of breaching the barrier identified in the upper portion of the

diagram and transporting the radionuclides to the environment. Ultimately various event sequences are postulated, each involving different combinations of events, and resulting in a particular type of release. By comparing estimates of the doses associated with each type of release, as well as the likelihood that the various event sequences occur, the dominant safety risk event sequences are identified. The events which initiate these dominant event sequences are then selected for detailed study in the PRA event trees.

Not all initiating events that are identified in the master logic diagram developed for this study have been analyzed. Detailed design information (e.g., cable tray layouts) is not available at this conceptual design stage for a meaningful evaluation of some initiating events (e.g., events introducing spatial dependencies such as internal fires). Analysis of such events will be added as additional design information becomes available. The basis for selecting the initiating events which were evaluated in this study is provided in Section 5.

3.2. EVENT TREE CONSTRUCTION

Once the initiating events are defined, the accident sequences initiated by each such event are systematically identified. This is performed by the construction of event trees for each initiating event. The event trees describe the progression of the accident sequences from initiation to termination. The development of these event trees is systematic in that all of the systems which protect or influence the barriers to release affected by the initiating event are considered in the evaluation. For example, in considering releases from the core, those systems which mitigate or otherwise influence the potential transporting of radioactivity from the core and through the primary circuit and reactor building, are considered in the event tree construction. The status of each of these systems is determined by the top events in the event trees. As illustrated in Fig. 3-1, the process of constructing the

event trees requires knowledge of the plant systems, their capabilities, and design functions. Such detailed system analysis information is provided in Section 6.1. Intersystem dependencies, which may influence the capabilities of one system to perform its intended function depending on the status of another system, are also key inputs to the event tree construction task. Intersystem dependencies are discussed in Section 6.2. Knowledge of the plant transient response to each initiating event and subsequent system failures dictates the sequencing in which each system comes into play. Knowledge of whether a system is actuated automatically or not, and the specific conditions in which the system will be asked to perform its function is also required. The plant transient response is determined by a series of computer programs which predict, among other things, core temperatures, primary coolant pressures and temperatures, and radiological transport rates. Such computer programs allow one to predict the response of systems, such as the ability of cooling systems to remove plant decay heat, under the conditions specified in the accident sequence. Knowledge of the plant response is incorporated into the event sequence definition task by assuring that the branches in the event trees that are constructed reflect the capabilities of each system as well as the system availabilities.

3.3. SEQUENCE PROBABILITY QUANTIFICATION

The sequence probability quantification task is described in Section 7. It begins with the determination of the numerical branching ratios for each branch point in the event trees. The probability of occurrence of each event along each of the accident sequences within the event tree is obtained from fault tree analysis. A fault tree is a logic diagram which gives the probability of an undesired state of a system (e.g., loss of cooling) when the various basic event failure modes, probabilities, and dependencies are known (Ref. 3-2). The fault trees are developed from knowledge of the plant design of the specific systems being modeled and the specific operator actions that impact

system reliability. Algebraic expressions for the event failure probabilities are formulated per Ref. 3-3 in terms of reliability models and parameters (e.g., failure rates, failure on demand probabilities, mission times, and repair times). These algebraic expressions are combined in accordance with the fault tree logic to determine the top event probabilities for each of the fault trees. Often the basic events can be considered independent, and the basic event probabilities are multiplied to determine the probability. When basic events involve failures of identical components in redundant trains, common mode failures cause these events to be dependent. Then, the algebraic equations are written to account for both the independent and common mode failures which constitute the total failure probability. Common mode failures were accounted for in systems involving a number of different sets of identical components in redundant trains (e.g., pumps, motor-operated valves, check valves, and heat exchangers). Common mode failure model parameters were derived from numerous published sources. The specific parameters developed for this study are presented in Appendix B.

The fault tree top event probabilities, which give rise to the event tree branching ratios, are multiplied together to obtain the individual sequence probabilities in each tree. This approach is correct, as long as the evaluations of fault trees for systems appearing later in the event tree are performed in a conditionally dependent manner. The event trees were constructed in a way in which some top events, along a single sequence, share common support systems. The shared systems introduce a dependency which is accounted for by evaluating the branching ratios for the second top event conditional on the outcome of the first event. For example, suppose the systems considered in top events 1 and 2 share a common support system. If the system in top event 1 fails, it may be due to failure of the common support system, or from other causes. In evaluating the failure probability of the system in top event 2, the conditional probability of failing the common support system is first computed and then used in the evaluation of top

event 2. In this way the shared support system is correctly incorporated into the model.

Uncertainties in the quantification of each sequence probability are computed using Monte Carlo uncertainty propagation techniques consistent with those used in Ref. 3-4. The Monte Carlo technique samples from the reliability model parameter distributions provided in Appendix B, and then computes the top event probabilities and sequence probabilities from that sample. This sampling process is repeated many times to obtain probability distributions for both the top event probabilities and the sequence probabilities. It is from these distributions that the mean values provided in Section 7 were determined.

At this preconceptual design stage, a number of design details have not been completed. This introduces another type of uncertainty. The resultant sequence probability distributions were not modified to account for this design uncertainty. Rather, for systems in which few details were available, the logic models developed assumed that the detailed design would resemble related systems that had been evaluated previously and for which much more detailed design information is available. It was judged that, when the MHTGR design is completed, these systems will be about as reliable as the systems analyzed previously. Moreover, this supposition will be checked in the periodic PRA revisions that will be performed as the plant design evolves. In this fashion, design deviations from the assumed system configurations that alter the system reliability predictions are monitored, and their impact on overall safety goal compliance is fed back to the designers as part of the reliability allocation process mentioned in Section 2.2.

A third type of uncertainty present in the sequence quantification task is modeling uncertainty. Such uncertainties stem from limited knowledge of the plant response to different events and the capabilities of systems to perform functions under conditions other than those specified by the system design descriptions. A limited assessment of this

type of uncertainty is included in the sequence models, for a small number of events judged to be important (e.g., whether a challenge to a primary relief valve occurs). The probability distributions for these modeling uncertainties were assigned subjectively, reflecting the current study team's state of knowledge.

It should be recognized that in any PRA study there is a need to cut off further exploration of event sequences at some frequency level simply to conserve finite resources. In some cases, this is done implicitly by engineering judgment; that is, the analyst may simply conclude that a sequence is so improbable that it is simply not included in the event tree. For example, coupling external events such as a severe earthquake simultaneous with a severe tornado are generally discarded as being too remote to have an impact on assessed risks, even though coupling the events could have consequences more serious than the occurrence of either event alone. In other cases, the sequence may be identified, but after quantification the sequence is identified as being so improbable that further development of consequences is not warranted.

In this study, accident sequence development was curtailed if it was determined both that the sequence had a frequency of less than 10^{-8} per year and that the projected consequences of the sequence did not greatly exceed (i.e., orders of magnitude larger) other events to be analyzed. This cutoff guideline is believed to be justified for two reasons. First, the selected frequency is sufficiently below the NRC's mortality safety goal target of 5×10^{-7} per year that any cumulative residual risks associated with events below that frequency level would be adequately included in the final assessed risks. Thus the level of risk assessment is deemed suitable for determining whether or not the NRC's safety goal has been met, a key objective of the risk assessment. Secondly, it is believed that a frequency of 10^{-8} per year represents a level beyond which the risk assessment result lose useful meaning. For example, at such low frequencies, one may be comparing reactor accidents

with the consequences of large meteor strikes. The latter event would clearly overwhelm the former in consequences to the public.

3.4. SEQUENCE CONSEQUENCE QUANTIFICATION

The analysis of consequences and physical phenomena for the accident sequences is simplified by grouping the event sequences into a smaller number of release categories such that the salient physical responses in sequences within a given category are judged to be similar and therefore result in about the same consequences. The accident sequences judged to result in approximately the same release of radionuclides are assigned to the same release category. A representative event sequence for each release category is then chosen for detailed consequence evaluation, as described in Section 8.

The consequence evaluation of each representative event sequence consists of four parts: thermal-hydraulic transient analysis, radionuclide transport analysis, dose and public health impact assessment, and uncertainty analysis. Thermal-hydraulic transient analyses are used to determine key component temperatures, coolant pressures, and flow rates to establish the mechanisms, timing, and the driving forces for radionuclide transport from the initial location across the barriers to release. The radionuclide transport analysis utilizes the thermal-hydraulic analysis results as input to define the driving forces (i.e., temperatures, flows, shear forces) for release. The radionuclide transport analysis then models the time-dependent release through the radionuclide barriers, properly accounting for radioactive decay and removal mechanisms such as gravitational settling and plateout. The dose and public health impact assessment utilizes the estimated time-dependent radionuclide releases as input and determines the expected impact on a hypothetical individual at the Exclusion Area Boundary (EAB) in terms of dose to the whole body and major organs. These doses are then scaled to obtain the estimated latent fatality risk of this hypothetical individual.

As with the quantification of sequence probabilities, the quantification of sequence consequences is subject to a number of uncertainties. However, unlike the models to quantify the probabilities, the full consequence models are much too complicated to use in a Monte Carlo calculation to derive dose uncertainties. Therefore, simplified representations of the consequence models, benchmarked against the detailed model results, are instead prepared to use as the sample function in a Monte Carlo uncertainty propagation, consistent with the methods used in Refs. 3-5 and 3-6. Not all consequence model input parameters and their uncertainties are modeled explicitly. Instead, some uncertainties are assigned to intermediate results in the consequence calculations (i.e., to the radionuclide core release fractions) using engineering judgments. A more detailed uncertainty assessment of the basic parameters which govern these release fractions must await the development of more suitable models for the uncertainty propagation and an expanded data base. Finally, the consequence uncertainty analysis does consider the variability of dose assessment parameters such as wind velocity and stability class. The simplified consequence models are used in a Monte Carlo sampling scheme to determine the complete consequence uncertainty distributions for each dominant release category. At this preconceptual design stage, a number of design details have not been completed. This introduces uncertainty into the predicted transient behavior and release characteristics of the plant. Rather than include these uncertainties in the sequence consequence quantification it was judged that, when the MHTGR design is completed, its physical behavior will resemble the behavior shown in Sections 6.1 and 8. This supposition will be checked in the periodic PRA revisions that will be performed as the plant design evolves. In this fashion, design variations that alter the plant response and release models are monitored, and their impact on overall safety goal compliance is fed back to the designer through the process for establishing radioactivity retention requirements mentioned in Section 2.2.

3.5. UTILIZATION OF RESULTS

The final task in Fig. 3-1 is concerned with the utilization of results. The frequencies and consequences of the event sequences analyzed are combined and presented in Section 9 both in tabular form and as complementary cumulative distribution curves. In these formats, the results of this PRA are compared directly to the NRC safety goals and PAGs for sheltering evacuation. Although the selection of LBEs and designer feedback (in the form of reliability allocations and radioactivity retention requirements) are not performed as part of this PRA, Section 9 is structured to provide the information needed in those separate licensing and design tasks.

3.6. REFERENCES

3-1. "PRA Procedures Guide," U.S. Nuclear Regulatory Commission Report NUREG/CR-2300, January 1983.

3-2. Haasl, D. F., et al., "Fault Tree Handbook," U.S. Nuclear Regulatory Commission Report NUREG-0492, January 1981.

3-3. Henley, E. J., and H. Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1981.

3-4. "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. Appendix III, Failure Data; Appendix IV, Common Mode Failure," U.S. Nuclear Regulatory Commission Report WASH-1400 (NUREG-75/104), October 1975.

3-5. "HTGR Accident Initiation and Progression Analysis Status Report. Vol. II, AIPA Risk Assessment Methodology," GA Report GA-A13617, October 1975.

3-6. "HTGR Accident Initiation and Progression Analysis Status Report, Phase II Risk Assessment," GA Report GA-A15000, April 1978.

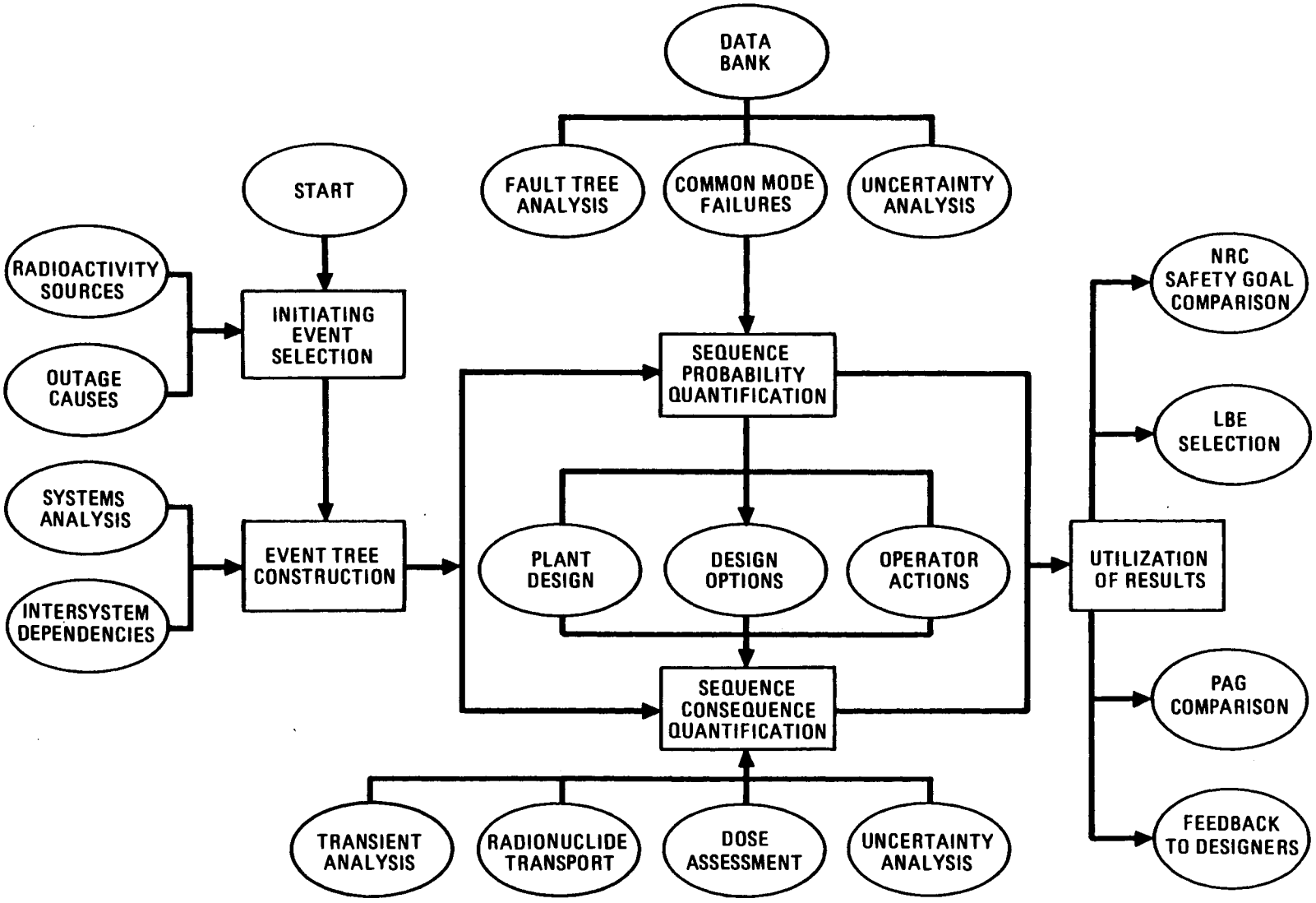


Fig. 3-1. PRA methodology and uses

4. PLANT DESCRIPTION

The Standard MHTGR plant design upon which the PRA has been based is described in this section. Major aspects of the design will be discussed with emphasis placed upon those features of particular relevance to the performed assessment.

The Standard MHTGR plant consists of four reactor modules and two turbine generator sets to achieve the nominal 558-MW(e) plant rating. Each reactor module is housed in a vertical cylindrical concrete enclosure which is fully embedded in the earth. Each module consists of separate vertical reactor and steam generator vessels connected by a horizontal coaxial cross duct. The major components of the nuclear steam supply system (NSSS) portion of the plant are contained within the MHTGR as shown in Fig. 4-1. The design parameters for the NSSS are listed in Table 4-1.

A number of the plant systems and subsystems comprising the MHTGR are important for control of radionuclide release. Other systems and subsystems have functions that are not directly related to controlling the release of radioactivity and have not been addressed in the PRA analyses. Table 4-2 gives a list of all MHTGR systems and subsystems that have been analyzed in the Section 6.2 fault trees or the Appendix C event trees. Those systems not addressed in Sections 6.2 and 7 are either of negligible importance relative to MHTGR safety risk, or lack adequate design definition upon which to judge their safety risk significance (see Section 5). The intersystem dependencies of the systems and subsystems analyzed in this assessment are shown in Table 4-3. Note that several subsystems listed in Table 4-2 do not appear in Table 4-3. The reactor internals, reactor core, vessels and duct, buildings, vessel

TABLE 4-1
NSSS DESIGN PARAMETERS

Item	Parameter
Reactor System	
Modules per station	4
Power per module, MW(t)/MW(e)	350/140 nominal
Coolant (helium) pressure at rated power	Helium at 6.38 MPa (925 psia) at circulator discharge
Cold helium temperature (at circulator discharge)	258°C (497°F)
Hot helium temperature (at core exit)	687°C (1268°F)
Feedwater temperature/pressure	193°C/20.68 MPa (380°F/3000 psia)
Steam temperature/pressure	541°C/17.3 MPa (1005°F/2515 psia)
Configuration description	Side-by-side (SBS)
Vessel material	Carbon steel - Mn-Mo, SA 533, Grade B, Class 1
Reactor vessel overall height, with CRDS and shutdown circulator	28.9 m (94.8 ft)
Reactor vessel outside diameter	6.8 m (22.4 ft)
Number of Components Per Module	
Steam generators	1
Circulators	1 main, submerged electric motor-driven
	1 shutdown cooling, electric motor-driven
Shutdown heat exchangers	1
Control rods	30 (6 inner, 24 outer reflector rods)
Reserve shutdown channels	12 (inner row of core fuel elements)
Start-up system (flash tank)	1
Core and Fuel Cycle	
Fuel element configuration	Prismatic hex-block, 20.78 cm (8.18 in.) sides x 79.3 cm (31.22 in.) height
Fissile material	UCO
Power density	5.91 W/cm^3 (330.43 $Btu/h\text{-}in.^3$)
Power peak/average axial ratio	1.4:1
Average enrichment	19.9% U-235
Fertile material	ThO_2

TABLE 4-2
STANDARD MHTGR PLANT SYSTEMS AND SUBSYSTEMS INCLUDED IN THE PRA ANALYSES

System Title
Main circulator
Steam generator
Shutdown circulator
Shutdown cooling heat exchanger
Shutdown cooling water
Reactor cavity cooling
Investment protection
Safety protection
Special nuclear area instrumentation
Vessels and duct
Pressure relief
Vessel support
Neutron control
Reactor internals
Reactor core
Helium purification
Helium storage and transfer
Circulating water
Service water
Turbine generator and auxiliaries
Feedwater and condensate
Main and bypass steam
Heater drains and condensate returns
Condensate polishing
Turbine building closed cooling water
Reactor building
Standby power building
Turbine building
Switchgear building
Cooling tower basin and circulating water pump house

TABLE 4-2 (Continued)

System Title
Reactor plant cooling water
Plant supervisory control
NSSS control
BOP control
Data management
Radiation monitoring
Instrument and service air
Non-class 1E ac distribution
Class 1E uninterruptible power supply
Class 1E dc power
Steam and water dump

TABLE 4-3
MHTGR FUNCTIONAL INTERSYSTEM DEPENDENCIES

Systems	Support Systems: Non 1E ac	1E dc	Non 1E dc	1E UPS	Non 1E UPS	Instrument and Service Air	RPCW	Circ. Water	Service Water	TBCCW	PPIS	He S/T	Turbine/ Generator	PCDIs	Condensate Polishing	Heater Drains
Non 1E ac	--	X	X	X	X								X			
1E dc	X	--		X												
1E UPS	X	X		--												
Instrument and service air	X					--				X						
RPCW	X					X	--		X			X				
Circulating water	X							--								
Service water	X								--							
TBCCW	X					X			X	--						
PPIS				X	X		X		X		--			X		
Turbine/ generator	X							X		X			--	X	X	X
Feedwater and condensate	X	X				X		X		X	X			X	X	X
Main and bypass steam	X	X									X					
SG dump	X										X					
HPS	X				X		X				X	X				
Neutron control	X	X		X	X		X				X					
Pressure relief											X	X				
SCS	X					X			X		X	X				
HTS	X				X	X	X		X	X	X	X		X		
PCDIS																
Radiation monitoring	X				X									X		
Condensate polishing	X					X									--	
Heater drains	X					X										--

support, and the reactor cavity cooling system are not listed because they are passive and have no active systems supporting them. Table 4-3 indicates how a mechanical or electrical failure in one system or subsystem results in multiple system failures. Adequate understanding of these dependencies is crucial for modeling conditional system and subsystem failure probabilities.

Each subsystem listed in Table 4-2 is briefly described in the following subsections. For each subsystem a figure is given in the following subsections, when available, that corresponds to the design that has been evaluated in the fault trees of Section 6.2 or the top-level event tree headings of Section 7. The design of passive systems such as the reactor cavity cooling system, reactor internals, and reactor building is important in Section 7 as well as in the consequence assessment of Section 8.

4.1. REACTOR CORE SUBSYSTEM

The reactor core subsystem consists of fuel elements, hexagonal graphite reflector elements, plenum elements, startup sources, and reactivity control material, all located inside the reactor pressure vessel. The reactor core, together with graphite components of the reactor internals subsystem, constitutes a graphite assembly which is supported on a graphite support structure and restrained by a core lateral restraint structure. (See Figs. 4-2 and 4-3.)

The standard hexagonal fuel elements (Fig. 4-4) are stacked in columns that form an active core annulus. Columns of hexagonal graphite reflector elements are in the central region and surround the active core, as shown in Fig. 4-3. The core produces 350 MW(t) of power at a power density of 5.9 MW/m^3 (5.7×10^5 $Btu/hr\text{-}ft^3$).

Placed on top of the upper graphite reflector are plenum elements, one per column, for channeling the coolant flow. These plenum elements also contain radiation shielding material. Beneath the active core are hexagonal graphite reflector elements. These lower reflector elements continue the coolant hole pattern from the active core. Flow in these channels exits into the core support blocks.

The reactor core subsystem contains both fixed and movable poison for normal operation. The fixed poison is in the form of lumped burnable poison rods and the movable poison is in the form of metal clad control rods. In the event that the control rods become inoperable, backup reserve shutdown control is provided in the form of boronated pellets that may be released into the core.

The functions of the reactor core subsystem are to generate heat from fission energy produced in a well controlled self-sustaining neutron chain reaction, and to transfer the heat to the helium primary coolant flowing through the core.

The reactor core subsystem also performs the function of retaining radionuclides in the fuel with fuel particle coatings upon which the safety of the MHTGR is based. As a part of accomplishing this, the annular geometry of the core functions to promote passive heat removal via conduction and radiation while other features function to control the effect of chemical attack and control the generation of heat under off-normal conditions.

MHTGR fuel particles consist of both fertile (ThO_2) and fissile (UCO) material. Both fuel types are in the form of dense microspheres coated with a TRISO coating whose primary purpose is to retain fission products. Figure 4-5 illustrates the TRISO coating concept. The fuel kernel and particle coating layers provide resistance to gaseous and metallic fission product release. The coated particles are blended and bonded together with a carbonaceous binder into the form of fuel rods.

The rods are then used to construct the fuel elements. The bonding of fuel particles into rods provides an additional barrier to metallic fission product release through graphite adsorption mechanisms.

4.2. REACTOR INTERNALS SUBSYSTEM

The reactor internals subsystem consists of the core lateral restraint, permanent side reflector, graphite core support structure, metallic core support structure, upper plenum thermal protection structure, and the hot duct. Figure 4-6 illustrates the location of the components of the reactor internals subsystem within the reactor system, and Fig. 4-7 shows the core support structure.

The core lateral restraint and the permanent side reflector surround the core; the graphite core support structure and metallic core support structure are located below the core; the upper plenum thermal protection structure is located above the core; and the hot duct is located within the cross duct between the reactor vessel and the steam generator vessel.

The principal function of the reactor internals subsystem is to provide support and lateral restraint for the reactor core. Other important functions are to channel the primary coolant flow to the core, to control the amount of core coolant bypass flow, and to mix the core exit coolant flow. The reactor internals also augment shielding of the reactor vessel from core radiation. Furthermore, the core lateral restraint, permanent side reflector, graphite core support structure, and metallic core support structure remove core heat and assist in controlling heat generation. These functions are performed by maintaining cooling pathways and the geometry necessary for reactivity control material movement.

4.3. NEUTRON CONTROL SUBSYSTEM

The neutron control subsystem consists of the drive mechanisms for positioning the control rods, the rod controls, the reserve shutdown control equipment (RSCE) with its controls, and the instruments for measuring neutron flux levels within the reactor vessel (i.e., in-vessel flux mapping units and startup detectors) and around the perimeter of the reactor outside the vessel (i.e., ex-vessel flux detectors). Most of this equipment is configured into assemblies which are normally installed in penetrations in the top or bottom of the reactor vessel. These assemblies are periodically removed either to provide access to the core for refueling or for maintenance of the equipment.

Five types of assemblies are provided for each reactor module:

1. Twelve outer neutron control assemblies.
2. Six inner neutron control assemblies.
3. Six ex-vessel neutron detector assemblies.
4. Three startup detector assemblies.
5. Five in-vessel flux mapping units.

Each outer neutron control assembly is equipped with two independent control rod and drive assemblies. These assemblies are interchangeable in any of the penetrations assigned for neutron control.

Each inner neutron control assembly is equipped with one control rod and drive assembly and two independent sets of RSCE. These assemblies are also interchangeable in any of the assigned penetrations. Figure 4-8 shows the outer neutron control assemblies and inner neutron control assemblies installed in the reactor vessel. Figure 4-9 depicts the relative locations of the neutron control subsystem in-vessel components.

The ex-vessel neutron detection equipment consists of fission chamber neutron detectors mounted in six equally spaced vertical wells located just outside the reactor vessel. The signals from these detectors are supplied to the nuclear instrumentation cabinets and safety protection subsystem equipment. These data are used by the automatic control systems to operate the control rod drives or the reserve shutdown equipment, thereby changing the neutron flux levels within the reactor core.

The outer control rods are inserted automatically by gravity upon receipt of a signal from the safety protection subsystem (SPS) of the plant protection and instrumentation system (PPIS), which disconnects the power to the holding brakes of the control rod drive motors.

Insertion of the reserve shutdown control material is also automatically actuated by signals from the SPS. The material is dumped from hoppers located above the core which are opened by the electrical destruction of fusible links.

The inner control rods are normally used only during startup conditions. Insertion of the inner control rods during high power operation would expose them to temperatures in excess of their thermal damage limit. It is for this reason that use of the inner control rods is extremely limited during conditions other than low-power operation.

4.4. VESSELS AND DUCT SUBSYSTEM

The vessels and duct subsystem for each module consists of a reactor vessel and a steam generator vessel placed side-by-side and connected by a cross duct. The vessels and duct subsystem includes the vessel penetrations, closures, and thermal insulation and the main steam and feedwater isolation valves. The principal functions of the subsystem are to contain the primary coolant inventory and to provide a coolant flow path for transfer and transport of thermal energy. In

addition, the subsystem provides support for the reactor core and internals, for the steam generator and main circulator, and for the shutdown cooling heat exchanger and circulator. The vessels and duct subsystem is located below grade level and is enclosed in a concrete structure. The steam generator vessel is located at a somewhat lower elevation than the reactor vessel. This allows the steam generator to be thermally protected and isolated following a loss of forced circulation. The vessels and duct subsystem is bottom-supported by the reactor cavity through attachments anchored to the vessels at or below the level of the cross duct. The cross duct is supported through its connections to the vessels.

4.5. REACTOR BUILDING SUBSYSTEM

The reactor building is a multi-cell, reinforced concrete structure housing the nuclear steam supply system (NSSS) and ancillary systems and components. Set below grade, the reactor building is configured as a 18.3-m (60-ft) inside diameter, vertically oriented right cylinder topped by a rectangular prism. Minor portions of the building extend above grade, principally the reactor cavity cooling system (RCCS) intake and exhaust structure, and the main steam and feedwater isolation valve enclosure. Four such buildings are arranged in a row and are served by a bridge crane running their entire length. A steel-framed maintenance enclosure shelters the entire crane service area.

In general, the reactor building's functions and associated requirements are dictated by the needs and characteristics of the equipment it houses. However, the reactor building also serves to protect that equipment from external hazards and contributes to the capability to control both normal and post-accident onsite radiation levels.

An isometric view through the reactor building is provided in Fig. 4-10.

The cylindrical portion of the below-grade cavity is subdivided into a number of vertical cells which house NSSS equipment and provide access. Those cells housing the reactor and steam generator occupy the major portion of the building. The steam generator and reactor are separated by a 1.5-m (5-ft)-thick wall which is penetrated by the cross-duct. Other cells provide personnel and equipment access and pipe and cable ways.

The rectangular portion of the building is divided into two levels and subdivided into several compartments. The majority of this area is occupied by RCCS ducting and the cavity vent path. Other spaces house helium purification system (HPS) equipment, PPIS equipment, and other nuclear auxiliaries which are dedicated to each reactor.

The reactor building serves as an enclosure that can be vented in a controlled manner providing an additional attenuating barrier to radionuclide releases. The vent paths from the reactor cavity to the steam generator cavity and from the steam generator cavity to the atmosphere, as well as the RCCS ducts, follow tortuous routes to limit neutron streaming from the reactor building. To maintain the requisite reactor cavity environmental conditions while limiting the heat load on the steam generator cavity chiller, the reactor cavity vent path is fitted with blowout panels. Similarly, to maintain control of the steam generator cavity environment, the steam generator cavity vent path is fitted with gravity dampers, which open on overpressure and then reshut. These dampers are located below elevation -7m (-23 ft) to provide them protection from external hazards, with ultimate release of steam or helium to the atmosphere made through louvered openings located above elevation 3.6 m (12 ft) adjacent to the main steam isolation and relief valve enclosure.

The entire reactor building is designed structurally to withstand the requisite levels of intensity for external and internal hazards to ensure that the equipment it houses can function as required to meet the

investment protection and public health and safety criteria. This includes the structural framework for the maintenance enclosure, which is to be designed not to collapse under design basis conditions.

4.6. HEAT TRANSPORT SYSTEM

The heat transport system (HTS) consists of the steam generator subsystem and the main circulator subsystem.

The principal function of the HTS is to transfer heat from the reactor to the secondary coolant under energy production, shutdown, refueling, and startup/shutdown conditions. In addition, portions of the HTS have the function of containing the primary coolant inventory during these modes of operation. The HTS is shown in Fig. 4-11.

The steam generator subsystem serves to limit the release of radionuclides by maintaining its primary/secondary coolant pressure boundary integrity, thereby containing radionuclides (contaminated primary coolant), controlling radionuclide transport (tritium diffusion) from the primary coolant, and preventing chemical attack.

The steam generator and the associated main circulator fit within the boundary of the vessel system. Hot primary helium flows from the reactor core through the inner duct of the crossduct into the steam generator vessel. A duct extended from the inner duct leads helium to the top of the steam generator bundle for downflow through the bundle. Cooled helium flows out of the steam generator and then up along the inside of the vessel to the circulator mounted at the top of the vessel. Steam is discharged out of the top side of the steam generator while feedwater is introduced at the bottom.

The steam generators are once-through tubular type units, each with an economizer, an evaporator, and a first-stage superheater forming one, helically wound tube bundle and a second stage super heater that is a

separate but connected helical tube bundle. Helium flow is downward on the shell side and is cross-counter flow to the steam/water upflow.

The main circulator subsystem consists of a main circulator assembly (compressor, motor, housing), a main loop shutoff valve and ducting, magnetic bearings, and control and power modules. The main circulator is a single-stage axial flow compressor mounted directly on the shaft of the electric motor rotor. The integral rotor is fully floating on a set of two radial bearings and one double-acting thrust bearing, all of the active magnetic field type. Antifriction-type catcher bearings are provided to prevent damage in the case of functional failure of the magnetic bearings. The variable speed electric motor is capable of precise speed adjustment.

4.7. SHUTDOWN COOLING SYSTEM

The shutdown cooling system (SCS) consists of the shutdown cooling circulator subsystem, the shutdown cooling heat exchanger subsystem, and the shutdown cooling water subsystem (SCWS).

The principal function of the SCS is to provide a second means of forced circulation residual heat removal from the shutdown reactor by transferring this heat to the service water subsystem when the HTS is unavailable. In addition, portions of the SCS have the function of containing the primary coolant inventory.

The shutdown cooling heat exchanger subsystem provides for helium-to-water heat transfer in the SCS and is located below the core support floor shield at the bottom centerline of the reactor vessel. The subsystem comprises one heat exchanger per reactor module positioned within the reactor vessel. The shutdown heat exchanger (Fig. 4-12) is a vertically oriented shell-and-tube, cross-counterflow unit with subcooled water in the tubes which are supported by drilled plates. Pressurized cooling water removes heat from the reactor primary coolant. The heat

exchanger limits the release of radionuclides by maintaining its primary/secondary coolant pressure boundary integrity, thereby containing radionuclides (contaminated primary coolant) and controlling radionuclide transport (tritium diffusion) from the primary coolant.

The SCS has a single loop (per module) on the helium side consisting of a shutdown cooling heat exchanger in series with a shutdown cooling circulator and shutdown loop shutoff valve assembly. The SCS has a single secondary cooling loop servicing all four reactor modules. Heat is rejected from the secondary cooling loop to the service water system. The SCS is shown in Fig. 4-13.

In the decay heat removal mode with the SCS operating, helium is drawn from the reactor core and is channeled through the lower plenum shield/manifold to the top of the shutdown cooling heat exchanger. Flow is directed downward across the heat exchanger, through the shutdown loop shutoff valve and to the shutdown cooling circulator inlet. The circulator increases the helium pressure, turns the flow 180 deg, and discharges it upward to the reactor vessel through the annulus between the circulator inlet duct and reactor vessel. Approximately 90% of the flow is used for core cooling. The remainder is allowed to backflow through the closed main loop shutoff valve to cool the steam generator.

The shutdown cooling water subsystem is shown in Fig. 4-14. The cooling loop consists of one 15% capacity pump, two 100% capacity pumps, and two 50% capacity heat exchangers. Each of these pumps and heat exchangers is equipped with valves, controls, and instrumentation. All rated component capacities are with respect to the residual heat loads from all four modules.

Although the heat exchangers within the water cooling loop are rated at 50% capacity each, preliminary analyses indicate that if only one heat exchanger is available to remove the residual heat from all four modules, the resultant thermal transients experienced by the

modules are well within the limits needed to assure that no uncontrolled radiological release occurs. Thus, in the Section 6.2 fault trees, both heat exchangers must fail before there is any potential safety impact.

The shutdown cooling water subsystem operates when the SCS is started following loss of the HTS. The subsystem serves as a heat sink for the SCS and maintains appropriate thermal conditions for the shutdown cooling circulator motors.

To provide functional and operational flexibility, the pumps and heat exchangers of the subsystem are connected through header systems such that any pump can operate with any heat exchanger to remove heat from all four reactors simultaneously. The 100% capacity pumps are used to remove heat loads ranging from 94.96 MW (324 x 10^6 Btu/h) during a pressurized cooldown (i.e., a loss of all forced convection cooling while the vessel remains pressurized), to 12.24 MW (41.8 x 10^6 Btu/h) at the start of a depressurized shutdown condition.

To conserve power when the SCS is in standby condition, a jockey pump with 15% of full load capacity is provided to remove the much smaller heat loads, ranging from 12.24 MW (41.8 x 10^6 Btu/h) to 1.16 MW (3.96 x 10^6 Btu/h), during depressurized shutdown conditions and normal power operation for all four reactors, respectively.

A surge tank is connected at the pump suction to maintain the shutdown cooling water heat exchangers cooling water outlet pressure at a minimum of 5.06 MPa (720 psig) to prevent boiling during the core cooldown mode. Also, the surge tank accommodates anticipated system thermal expansion without exceeding 5.13 MPa (730 psig) at the shutdown cooling heat exchanger outlet, thus maintaining the water pressure below the helium pressure during full power reactor operation.

System pressure is automatically maintained and controlled at the surge tank using a helium blanket supplied from the helium storage and

transfer subsystem. The water quality is controlled by a chemistry control package.

During normal plant power operation, the water loop is maintained in the standby mode as depicted in Fig. 4-14. In this mode, the jockey pump continuously circulates cooling water through the shutdown cooling heat exchanger to maintain appropriate thermal conditions for the shutdown circulator motors and to minimize the thermal transient encountered during initiation of cooldown operation. The resultant parasitic heat load is rejected to the service water subsystem via the shutdown cooling water heat exchangers.

When the SCS is started following the loss of the HTS, the shutdown cooling water subsystem is brought into the cooldown operating mode. The switch from the standby mode to cooldown operating mode is accomplished by switching to the 100% capacity pumps from the jockey pump.

4.8. REACTOR CAVITY COOLING SYSTEM

The RCCS is required to remove heat from the reactor cavity during normal power producing operations in order to protect the concrete structures from overheating. When the reactor is shut down, decay heat is normally removed from the vessel through the steam generators to the main condenser, or by the SCS. However, in the event these paths are not available, decay heat is removed from the core and vessel by conduction and radiation. During such passive cooling, the vessel side walls and concrete structure temperatures are limited to acceptable values by the RCCS. Under these conditions decay heat is radiated from the vessel wall to the air cooled RCCS cooling panels, and then transported to the atmosphere by natural convection air flow.

Since the RCCS must remove both normal and decay heat loads, the system must function continuously while the reactor is at power or generating significant decay heat. The RCCS is a completely passive, air-cooled system which provides a high degree of reliability. The system removes heat from the reactor cavity by the natural convection of outside air through the cooling panels located in the reactor cavity. The cooling panels are divided into four quadrants, each quadrant having an annular inlet air duct and rectangular outlet duct routed inside the inlet passage as shown in Fig. 4-15. This arrangement protects the structural concrete from the hot outlet air. The outlet duct is insulated to minimize heating of the inlet air. Gratings and screens are provided on the inlet passages to prevent entry of foreign objects. Each reactor module has its own completely independent RCCS.

The RCCS has multiple inlets and outlets and has parallel, cross-connected air ducts to minimize the probability of total flow blockage, as shown in Fig. 4-16. The system is classified as safety-related and is seismically designed and protected from tornado missiles.

4.9. STEAM AND WATER DUMP SUBSYSTEM

The steam and water dump subsystem serves to further limit ingress of water into the primary coolant as a result of a steam generator tube leak or rupture. This is accomplished by dumping the steam/water inventory of the steam generator into the subsystem's dump tank following isolation of the steam generator from the feedwater and steam headers. The subsystem dump action minimizes possible damage to the reactor core by limiting the amount of water made available for fuel hydrolysis and graphite oxidation.

Figure 4-17 is a conceptual schematic of the steam and water dump subsystem. When a high moisture level is detected in the primary coolant of a module, the normal response is for the PPIS to close both sets of isolation valves for the leaking steam generator and initiate the

steam and water dump cycle. If successful steam generator isolation is not achieved, steam and water dump cycle initiation is inhibited.

The dump subsystem isolates the steam generator steam/water inventory, including any inleakage from the primary coolant, for subsequent disposal through the gaseous and liquid radioactive waste subsystems. This ensures that no primary coolant is released directly to the environment.

Separate dump subsystems serve each of the four steam generator modules independently. The portion of the subsystem associated with each steam generator consists of a dump tank, two trains of dump valves, a drain pump, and interconnection piping and valves with the gaseous and liquid radwaste subsystems. Dumping is executed by two parallel 100% capacity trains of dump lines, each equipped with two dual-actuated motor-operated valves mounted in series. The dump valves are powered from a reliable power source (normal power supply with backup standby power).

The components of the steam and water dump subsystem are housed in the reactor building and located at the bottom of the steam generator cavity. The dump tank centerline is approximately 2.44 m (8 ft) below the feedwater inlet to the steam generator. The dump valves are located as near as possible to the dump tank.

The dump tank is 1.93 m (6.3 ft) i.d. x 7.01 m (23 ft) long and has a capacity of about 19.7 m^3 (696 ft^3). The tank is designed for a pressure of 7.58 MPa (1100 psia) at 291°C (556°F). A tank initial water inventory of about 6245 1 (1650 gal) at 38°C (100°F) will normally be maintained to quench the dumped fluid.

The dump tank is equipped with a 10.16 x 15.24 cm (4 x 6 in.) safety valve set at 7.58 MPa (1100 psia). The safety valve is sized to protect the tank from feedwater overpressurization. The pressure of the

primary coolant is the maximum pressure the dump tank is designed to reach. This condition determines the setpoint of the safety valves on the dump tank [0.414 MPa (60 psi) higher than the primary coolant safety valve setpoint]. The difference in safety valve setpoints assures that primary coolant cannot be released to the environment through the dump tank.

A vent line is provided from the tank to the gaseous radioactive waste subsystem to permit processing and disposal of any primary coolant entering the tank.

4.10. PRESSURE RELIEF SUBSYSTEM

The pressure relief subsystem prevents the vessel system from exceeding its design pressure, hence providing overpressure protection for the primary coolant pressure boundary. The subsystem is composed of two identical pressure relief trains interlocked so that at least one is available at all times. Both trains are connected to the steam generator vessel upper head at the main circulator discharge where the primary coolant pressure is nominally the highest. Each train consists of a pilot-actuated, spring-loaded safety relief valve in series with a rupture disk, both of which must be activated to achieve pressure relief. The effluent is discharged to the steam generator cavity. To provide isolation, a motor-driven, operator-actuated block valve is placed between the steam generator vessel and the relief valve in each train. This allows valve maintenance as well as a method to prevent excessive primary coolant leakage in the event the relief valve fails to reseat after opening. Piping from the helium purification subsystem and helium storage and transfer subsystem allows helium to be collected, purified, and returned to the reactor vessel. Helium leaking through the relief valve is piped to the gaseous radioactive waste subsystem for processing. The pressure relief subsystem is depicted in Fig. 4-18.

4.11. MAIN AND BYPASS STEAM SUBSYSTEM

The main steam subsystem interconnects the four steam generator/reactor modules with two turbine generator sets. During normal operation, superheated steam is conveyed from the steam generators to the turbines. Suitable branch connections are also provided to supply auxiliary steam through a pressure reducing station.

The bypass steam subsystem allows transient dumping of main steam directly to the condenser following a large drop in steam demand by the turbine. Main steam will continue to bypass the turbine until reactor power can be run back to match the reduced steam demand.

During certain abnormal and accident conditions, the main steam subsystem is designed to remain operational to support heat removal from the steam generators. The subsystem also provides steam for various auxiliary services including turbine gland sealing and feedwater heating during startup and cooldown.

The main and bypass steam subsystem is shown in Fig. 4-19. Of particular interest in this subsystem are the steam generator relief valves and main steam line isolation valves. Two steam generator relief trains are provided to protect the steam generator from overpressure. Steam generator isolation is accomplished by closing the block valve in the main steam line. A line check valve, in series with the main steam block valve, prevents steam flow back to the steam generator from the balance of plant (BOP).

4.12. PLANT PROTECTION AND INSTRUMENTATION SYSTEM

The plant protection and instrumentation system (PPIS) is composed of three major subsystems: investment protection, safety protection, and special nuclear area instrumentation. An overview of the sense,

command, and execute features of the safety and investment protection subsystems of the PPIS is given in Fig. 4-20.

The safety protection subsystem provides the safety system sense and command feature necessary to sense plant process variables, detect abnormal plant conditions, and initiate plant protective actions. Each reactor module has a separate and independent safety protection subsystem which consists of four separate (redundant) safety channels and redundant two-out-of-four coincidence solid-state logic to command initiation of a protective action. Each safety channel includes the field mounted process variable sensors, electronic signal conditioning equipment, and electronic trip setpoint comparators to provide a trip signal when the process variable value reaches the trip setpoint. The two-out-of-four coincidence logic circuitry provides a protective action initiation signal when any two or more separate safety system channels reach the trip setpoint. The protective action initiation signal is sent to separate and redundant actuation devices.

The special nuclear area instrumentation subsystem provides interlocks and instrumentation that monitor protection systems' status and the plant under normal operating and accident conditions. The interlock feature of the special nuclear area instrumentation is the reactor vessel pressure relief block valve closure interlock. The vessel pressure relief block valve closure interlock consists of redundant electrical sensors and electrical interlocks to prevent the simultaneous closure of both vessel relief valve trains. This prevents the complete bypass of the vessel overpressure protection. The reactor vessel pressure relief block valve interlock utilizes interlock limit switches located on the valve actuator. The actuator relays are located in the motor control centers associated with the block valve.

The investment protection subsystem provides the sense and command features necessary to sense plant process variables, detect abnormal

plant conditions, and initiate plant protective actions required to protect the plant investment. The investment protection subsystem's prime purpose is to protect major plant equipment and is, therefore, investment risk oriented. The investment protection provides an integrated response to various plant upsets and events to ensure equipment damage limits are not exceeded. The subsystem uses redundancy and other system characteristics to meet the plant investment and availability goals. Each reactor module has a separate and independent investment protection subsystem.

4.13. FEEDWATER AND CONDENSATE SUBSYSTEM

The feedwater and condensate subsystem originates at the condenser associated with each turbine generator set and delivers feedwater to the steam generator in each of four reactor modules. In normal operation, one of two 80% capacity condensate pumps takes suction from the condenser hotwell and discharges flows through polishing demineralizers to adjust chemistry, and then through a series of feedwater heaters into the deaerator. One of two 80% capacity feedwater pumps takes suction from the deaerator storage tank and discharges feedwater at a specified pressure and flow rate to the steam generators.

The feedwater and condensate subsystem contains suitable storage and branch connections to permit operation through plant transients (surges and volume fluctuation) and to supply condensate to other systems. The subsystem is shown in Fig. 4-21.

4.14. SERVICE WATER SUBSYSTEM

The service water subsystem (SWS) removes waste heat from process systems located in the appropriate buildings in the nuclear island and conveys the waste heat to the cooling tower.

The SWS originates at the cooling tower basin where three 100% capacity normal service water pumps circulate water to appropriate buildings in the nuclear island. The subsystem removes process heat from the reactor plant cooling water subsystem, shutdown cooling water subsystem, spent fuel pool cooling water subsystem, turbine building closed cooling water subsystem, and station chilled water subsystem during normal operation, and returns the water to the station cooling tower. The SWS is shown in Fig. 4-22.

In addition to the normal SWS pumps, Fig. 4-22 depicts the shutdown service water pumps which function during SCS operation to cool the shutdown cooling water subsystem heat exchangers. This portion of the SWS consists of three 100% capacity pumps which can be powered from offsite power, turbine house load, or the backup power generators.

4.15. REACTOR PLANT COOLING WATER SUBSYSTEM

The reactor plant cooling water subsystem (RPCWS) removes heat from the following reactor plant components:

1. HPS coolers and compressors.
2. HPS regeneration coolers and compressors.
3. HTS circulator motors.
4. Moisture monitor compressor modules.
5. Neutron control assemblies.
6. Miscellaneous components.

The RPCWS consists of one cooling water loop with three 100% capacity pumps and two 100% capacity heat exchangers. The functional arrangement of the cooling loop is shown in Fig. 4-23. During normal plant conditions, three pumps and one heat exchanger are in operation at a time. This allows for the failure of a pump or heat exchanger without sustained loss of cooling, and permits on-line maintenance on a failed pump or heat exchanger. To provide reliability and flexibility, the

pumps and heat exchangers are connected in such a way that any one pump and any one heat exchanger can provide the required cooling capability. Each of the pumps is powered from an independent 480-V bus.

A surge tank is provided and connected at the pump suction to maintain coolant pressure at 1.13 MPa (150 psig) and to accommodate anticipated system thermal expansion without exceeding the design pressure limit of 1.48 MPa (200 psig). System pressure is automatically maintained by a helium blanket supplied from the helium storage and transfer subsystem. A relief valve in the surge tank provides overpressure protection.

4.16. TURBINE BUILDING CLOSED COOLING WATER SUBSYSTEM

The turbine building closed cooling water subsystem removes waste heat from the turbine-generator auxiliary equipment located in the turbine building and conveys the waste heat through the component cooling water heat exchangers to the service water subsystem.

The turbine building closed cooling water system consists of two, independent closed flow paths which serve equipment associated with each respective turbine-generator unit. Two 100% capacity pumps and two full-size heat exchangers are provided for each path. One of the two subsystem pumps is normally isolated and provides backup in the event the normally operating pump fails. A surge tank is located at the high point of each flow path to provide the required net positive suction head for proper operation of the pumps and to allow for thermal expansion and contraction. In addition, a component chemical addition tank is furnished to maintain proper water chemistry. This subsystem is shown in Fig. 4-24 for one turbine-generator unit.

4.17. CIRCULATING WATER SUBSYSTEM

The circulating water subsystem removes waste heat from the condenser by delivering circulating water at the specified temperature, pressure, flow rate, and chemistry. The waste heat is then conveyed to the station cooling tower.

In normal plant operation, circulating water is pumped from the cooling tower basin through the condensers and heat exchangers, and back to the cooling tower where the waste heat is released to the atmosphere via mechanical draft cooling towers. The system consists of two 100% capacity, vertical pumps. A check valve and motor-operated block valve are provided in each pump exit line to allow isolation. Inlet and exit isolation valves are also provided for the condensers. Figure 4-25 shows the circulating water subsystem for one turbine-generator unit. Although mechanical draft cooling is required during power production operations, this subsystem can function without the cooling tower fans during periods of decay heat removal.

4.18. TURBINE GENERATOR AND AUXILIARIES SUBSYSTEM

The turbine-generator converts the thermal energy in steam produced by the steam generator(s) to electrical energy and provides extraction steam for regenerative heating and deaeration of condensate and feedwater.

The turbine-generator auxiliaries complement, support, and assist in the operation of the turbine-generator to ensure high reliability and availability of the turbine-generator and the energy conversion system (ECS). The ECS (which includes the turbine-generators) is shown in Fig. 4-26.

Each unit consists of high-pressure, intermediate-pressure, and low-pressure turbine components, the generator, exciter, and several

auxiliary subsystems that provide supportive services for the operation of the turbine-generator. Each turbine-generator is a tandem compound, two-flow steam turbine rated 300 MW(e) at inlet steam conditions. Each turbine has a single-flow high-pressure component, a two-flow intermediate-pressure component, and one two-flow low-pressure component with 88.9 cm (35 in.) last stage blades. Each generator is rated 370 MVA at 0.9 power factor, 0.58 short circuit ratio, and excitation response ratio of 0.5. Each generator has a water-cooled stator and rotor with supplemental hydrogen cooling at 0.31 MPa (45 psig).

The turbine generator auxiliaries are

1. Turbine generator lube oil subsystem.
2. Hydrogen seal oil subsystem.
3. Gland steam subsystem.
4. Stator winding cooling water subsystem.
5. Turbine supervisory instrumentation subsystem.
6. Electrohydraulic control subsystem.
7. High-pressure hydraulic subsystem.
8. Overspeed trip protection system.

4.19. INSTRUMENT AND SERVICE AIR SUBSYSTEM

The function of the instrument and service air subsystem is to provide compressed air of suitable quality and pressure for all instrumentation, controls, and services required by the plant. Air supplied to instrument control is filtered to remove 40 micron and larger particulates, and dried to a -20°C (-4°F) dewpoint. Service air piping connections are located in all nuclear island buildings to provide service air to utility stations.

4.20. HELIUM PURIFICATION SUBSYSTEM

The helium purification subsystem (HPS) for each reactor module consists of a specific sequence of gas processing components, plus related piping, valves, controls, and instrumentation. This system purifies a helium side stream from the primary coolant system at a rate of 386.4 kg/h (850 lb/h) for each reactor module during normal full-power operation. The HPS removes chemical impurities in order to maintain their concentration in the primary coolant helium within prescribed limits and removes the gasborne activity contained in the side stream flow. Excess flow is returned to the primary system or transferred to storage as appropriate.

The HPS provides purified helium to equipment such as the main circulator, shutdown circulator, the pressure relief equipment on the reactor vessel, and valve penetrations in the vessel. A simplified HPS flow schematic for each reactor module is shown in Fig. 4-27 along with an indication of the primary function for each principal component in a helium purification train. Also shown in the figure is the separate regeneration train used to regenerate the dryers and low-temperature adsorbers in the HPS. One regeneration train services two reactor modules.

During depressurization of the reactor vessel for refueling and maintenance operations, the HPS purifies the discharged helium at no more than four times the normal flow rate. Following depressurization, the HPS maintains the reactor vessel pressure slightly below atmospheric pressure.

Should a small primary coolant leak be detected by a drop in primary coolant pressure, the HPS is used to depressurize the reactor vessel automatically, in order to minimize the effect of the leak. The HPS is actuated manually by the operator in the event forced convection cooling and the RCCS are unavailable to cool the reactor core. This

action is taken to prevent overstress conditions that would exist if the vessel were pressurized.

4.21. HELIUM STORAGE AND TRANSFER SUBSYSTEM

The helium storage and transfer subsystem consists of two parts. The first consists of nine high-pressure storage tanks containing helium at 15.6 MPa (2250 psig). These tanks provide makeup and purge helium at a rate of 1216 kg per year (2680 lb/yr). Purge and makeup needs are provided through pressure control stations, without the use of compressors. The subsystem is sized to satisfy the needs of all four modules, simultaneously. The tanks are replaced as needed.

The second, later part of the subsystem, provides for the low-pressure storage of 6078 kg (13,400 lb) of primary coolant helium in 180 storage tanks at 7.0 MPa (1000 psig). The system serves all four reactor modules. The low-pressure storage part of the subsystem receives helium from the discharge of the HPS and is normally used only during depressurization and pump-up operations. It is not required to operate continuously. Storage capacity is provided for primary helium coolant from two reactor modules. However, since depressurization and pump-up operations are performed for only one reactor module at a time, two 50% capacity low-pressure transfer compressors are provided having a total transfer capacity of 3400 m^3/h (200 acfm) which is sufficient to service one module. No standby or backup capacity is provided. If one compressor is inoperative, the other can perform all functions at a slower rate. The storage pressure, which is the same as the compressor discharge pressure, is established by the requirement to repressurize the reactor module at somewhat less than the primary coolant operating pressure, 6.6 MPa (925 psig) and by cost considerations. The helium storage and transfer subsystem is shown in Fig. 4-28.

4.22. NON-CLASS 1E AC DISTRIBUTION SYSTEM

The non-class 1E ac distribution subsystem provides electric power at 4160 V (three phase) and 480 V and less (both three phase and single phase) at 60 Hz to electrical switchgear and distribution panels associated with the auxiliaries of each unit generator. The non-class IE ac power sources and associated switch gear are located in the switch gear building. The normal feed to the system is from the unit generators through unit auxiliary transformers. For plant startup, and in the event of loss of the unit auxiliary transformer feeds, the unit generator buses are fed from the grid through the startup auxiliary transformers.

Each pair of reactor modules associated with a unit generator operates from a 4160-V nuclear island bus divided by a circuit breaker into two buses, each feeding one reactor module load. This is shown (for reactor modules 1 and 2) as buses 111 and 112 in Fig. 4-29, which illustrates the overall plant medium voltage non-class 1E ac distribution subsystem. The turbine-generator auxiliaries, and the components common to the unit, are fed from a 4160-V energy conversion area bus which can also be fed by a backup generator in case the normal and startup sources are lost, to supply investment protection loads. This energy conversion area bus for unit generator 1 is shown as buses 121 and 122 in Fig. 4-28. There are unit substations and motor control centers which are fed from both 4160-V nuclear island and energy conversion area buses. Investment protection loads are fed from 480-V unit substations and/or motor control centers, as required. These loads can also be supplied from the backup generators. For example, the SCS circulator motors, at 0.15 MW (200 hp), are supplied by this type of equipment. Figure 4-30 shows a typical arrangement.

The backup generators supply backup 4160 V ac power to the energy conversion area buses in the event of loss of station and offsite power to the investment protection loads. A 2500-kW (8.53×10^6 Btu/h) gas

turbine generator is provided for each unit generator, with associated combustion, startup, speed governing, cooling, lubricating, output circuit breaker, and load sequencing components.

Examples of the types of loads served by the backup generators are the SCS circulators, the SCS pumps, turbine lube oil and turning gear, and 480 V MCC power supplies to the class 1E UPS and class 1E 125 V dc power subsystems. Each pair of reactor modules contains safety-related and investment protection loads which can be served by either the normal non-class 1E ac distribution subsystem through the unit auxiliary transformers or the startup auxiliary transformers, or the backup generators in case of loss of all ac power.

4.23. CLASS 1E DC POWER SUBSYSTEM

The class 1E dc power subsystem supplies 125 V dc power to four redundant dc control and instrument switchboard buses. These buses provide four independent channels of dc control and instrument power to all four reactor modules for safety-related loads which are required for radionuclide control or safe shutdown.

The principal loads on the class 1E dc power subsystem are the RSCE power supplies, the main steam and feedwater isolation valves, the class 1E battery room fans, and in the event of loss of the non-class 1E ac power supply, the rectifier/inverters which supply the class 1E uninterruptible power supply subsystem. Figure 4-31 shows one typical channel of the class 1E dc power subsystem. Each channel has both a normally operating battery charger and a backup battery charger. Each charger is fed from a separate non-class 1E 480-V motor control center. Both non-class 1E 480-V motor control center supplies are served with power from three sources: the unit auxiliary transformers, the startup auxiliary transformers, or the backup generators. Either charger can supply the rated load while rectifying the incoming current to 125 V dc to charge the channel battery within 12 h from a discharged state. The

batteries provide dc power for up to 1 h at rated load, in the event of a loss of all ac power.

4.24. CLASS 1E UNINTERRUPTIBLE POWER SUPPLY SYSTEM

The class 1E uninterruptible power supply (UPS) system provides 120 V ac power to four redundant ac vital buses that feed safety-related control instrumentation and plant protection circuits for all four reactor modules. Each of the four independent UPS channels consists of a rectifier/inverter assembly, normally supplied by power from a non-class 1E 480 V ac motor control center. An alternate (bypass) power supply from a separate 480 V MCC feeding a 480 to 120 V regulating transformer, and a backup power supply from a class 1E 125 V dc bus are also provided. The rated loads on each channel consist primarily of safety protection, and investment protection logic modules which contain associated circuits (non-1E) requiring four channels. Figure 4-32 shows a typical class 1E UPS system channel arrangement. In the event of outages, power transients, or voltage dips caused by inverter failure or faults on the vital bus circuits, transfer to the alternate (bypass) ac power supply is accomplished automatically by the static switch. Failure of the rectifier dc output reverses the polarity of the blocking diode and permits immediate power flow from the class 1E dc batteries and chargers. The manual bypass switch allows electrical isolation of the static switch or inverter for repairs.

4.25. PLANT CONTROL, DATA, AND INSTRUMENTATION SYSTEM

The plant control, data, and instrumentation system is an integrated, yet functionally hierarchical, set of hardware (control initiators and monitoring devices) and software that enables the multiple-reactor, multiple-turbine plant to be automatically controlled and operated by a single operator from a single control room. The plant control, data, and instrumentation system performs control, monitoring, and data management functions given automatic and/or plant operator

generated commands. Digital computers are used for control, data processing, and single transmission. The system consists of four subsystems: plant supervisory control, nuclear steam supply system (NSSS) control, BOP control, and data management which collectively perform overall plant control.

The plant supervisory control subsystem automatically supervises and coordinates regulation and matching of load levels between the energy production and energy conversion areas during all plant operating states. Plant states are controlled automatically or by a combination of manual and automated control functions. As the plant power output demands or operating mode commands are changed, the NSSS control subsystem automatically responds by regulating reactor module thermal power and module steam conditions. The BOP control subsystem automatically regulates feedwater pump speed and main steam flow to the turbine generators. Data and single transfer between the initiating and receiving subsystems are carried out by the data management subsystem. This subsystem acquires, processes, transmits, distributes, and records all control initiating and monitoring signals.

4.26. COOLING TOWER BASIN AND CIRCULATING WATER PUMP HOUSE

The cooling tower basin is a reinforced concrete pool containing a portion of the circulating water subsystem inventory. It provides a foundation for the cooling tower. The circulating water pump house is a reinforced concrete structure located at the boundary of the cooling tower basin. It houses the pumps, valves, and some of the piping comprising the circulating water subsystem. These structures are located in the energy conversion area of the plant.

4.27. SWITCHGEAR BUILDING

The switchgear building is a grade-founded, single story, steel-framed structure located adjacent to the turbine building in the energy

conversion area of the plant. It has a reinforced concrete foundation and slab on grade level and insulated sheet metal exterior walls and roof decking. The switchgear building houses non-class 1E 4160-V switchgear, motor control centers, and load center transformers.

4.28. TURBINE BUILDING

The turbine building is a steel-framed structure with insulated metal siding and roof decking which houses the turbine-generator sets and associated power generation systems and equipment. The building arrangement has the parallel turbine-generator centerlines perpendicular to the common reactor centerline and the feedwater heater bays at the high-pressure ends of the turbines, an arrangement which minimizes turbine missile risk. The building arrangement also incorporates three floor levels and conventional reinforced concrete, high-tuned turbine pedestals. Provisions are also made for an overhead bridge crane for equipment handling. The turbine building houses the following subsystems: (1) main and bypass steam, (2) heater drains and condensate returns, (3) condensate polishing, (4) turbine building closed cooling water, (5) feedwater and condensate, and (6) turbine-generator and auxiliaries.

4.29. STANDBY POWER BUILDING

The standby power building houses equipment and components comprising the non-class 1E ac distribution subsystem and power supply. The building houses switchgear, motor control centers, and two backup generators each located within a separate cubicle. The standby power building is a grade-founded, reinforced concrete structure located in the nuclear island.

4.30. HEATER DRAINS AND CONDENSATE RETURNS SUBSYSTEM

The heater drains subsystem removes condensed extraction steam from the shell side of the low-pressure heaters. The low-pressure heaters and drains are shown in Fig. 4-21 for the feedwater and condensate subsystem. The condensate returns subsystem collects condensate from the auxiliary steam subsystem, and returns the drains to the condensate subsystem. All heater drains and condensate returns ultimately gravitate to the condensate subsystem via the condenser hotwell.

4.31. CONDENSATE POLISHING SUBSYSTEM

The condensate polishing subsystem removes suspended and dissolved impurities from the condensate resulting from condenser inleakage and condensate and feedwater subsystem corrosion. Two separate condensate polishing trains are included, one for each of the two turbine generator arrangements. Each train consists of the three 50% polisher vessels and regeneration equipment and is designed to treat 100% of the condensate flow. The polishing demineralizer vessels, as a part of the feedwater and condensate subsystem are depicted in Fig. 4-21.

4.32. RADIATION MONITORING SUBSYSTEM

The radiation monitoring subsystem is comprised of area, airborne, and process monitoring. The subsystem displays are used in assessing normal, abnormal, and accident operating conditions throughout the plant, in effluents from the plant and at the site boundary. Of importance to the risk assessment are the airborne radioactivity monitors which in the event of primary coolant leakage, are required to initiate primary coolant pumpdown to storage. Potential release paths for radionuclides to the envrionment are monitored including the normal ventilation exhaust duct from each reactor building, the blowdown vent path, and the reactor cavity cooling system exhaust ducts.

4.33. VESSEL SUPPORT SUBSYSTEM

The vessel support subsystem serves to support the reactor vessel, steam generator vessel, cross duct, and the control rod drive housings. Support for the reactor vessel consists of three flexing columns anchored on the vessel at or slightly below the level of the cross duct. Three keys are provided at both the top of the reactor vessel and at the support lug elevation to accommodate vertical and radial thermal expansions while providing lateral seismic restraint. The steam generator vessel load bearing support is slightly below the crossduct elevation and consists of two sliding bases, supported by ledges from the steam generator cavity, in line with the cross duct. A pair of keys and a pair of snubbers are provided near the bottom of the steam generator. Lateral restraints are also provided to limit tangential motion on the sliding supports. These components accommodate radial and vertical expansion translation along the axis of the cross duct, and seismic excitations. The reactor vessel-to-steam generator vessel cross duct is supported solely through its connections to the vessels.

This vessel support concept maintains the radial center of the reactor core stationary at all times. The steam generator, due to a rigid cross duct connection with the reactor vessel, can slide in-line with the cross duct at the various operating conditions to accommodate thermal expansion.

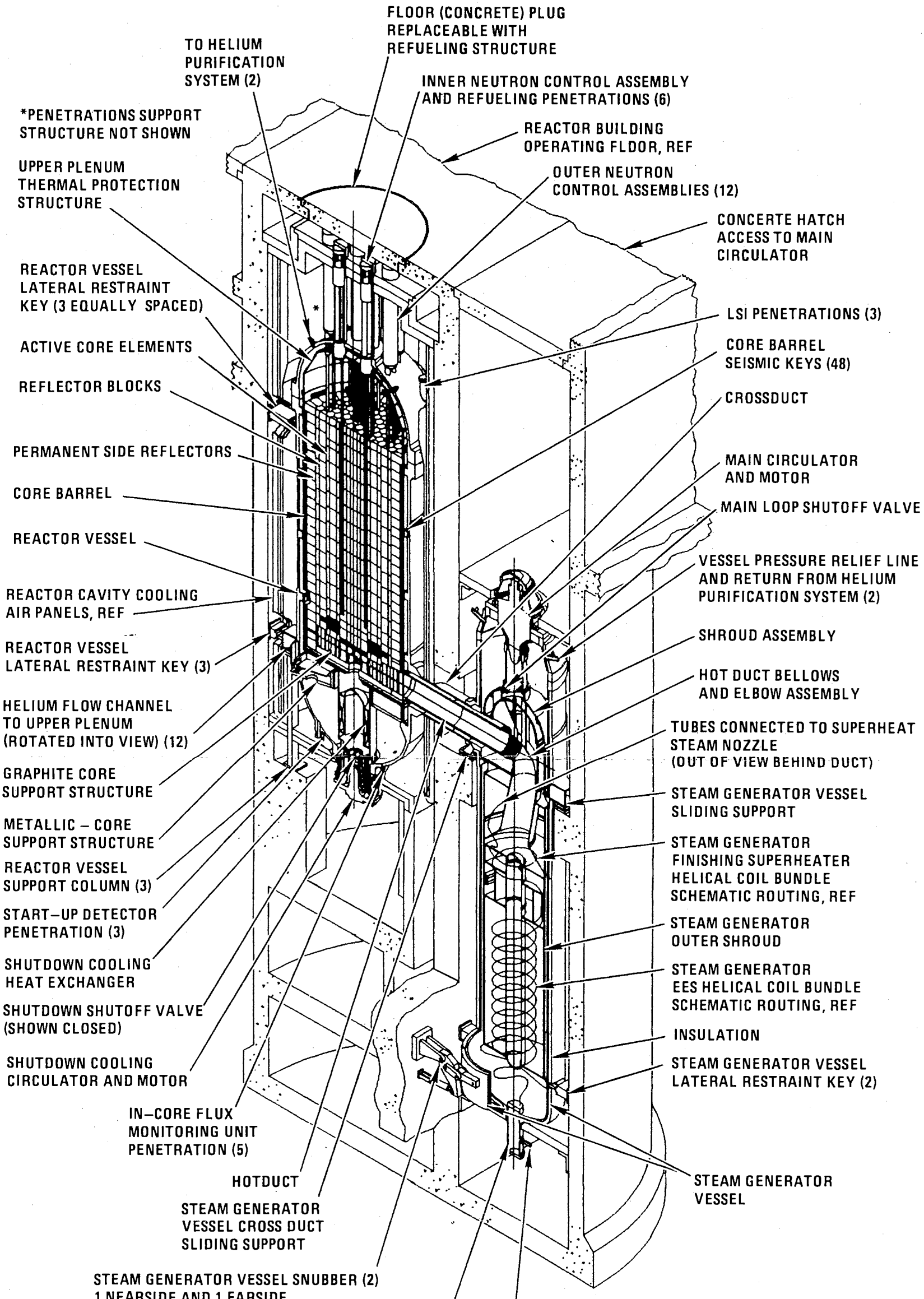


Fig. 4-1. NSSS arrangement drawing

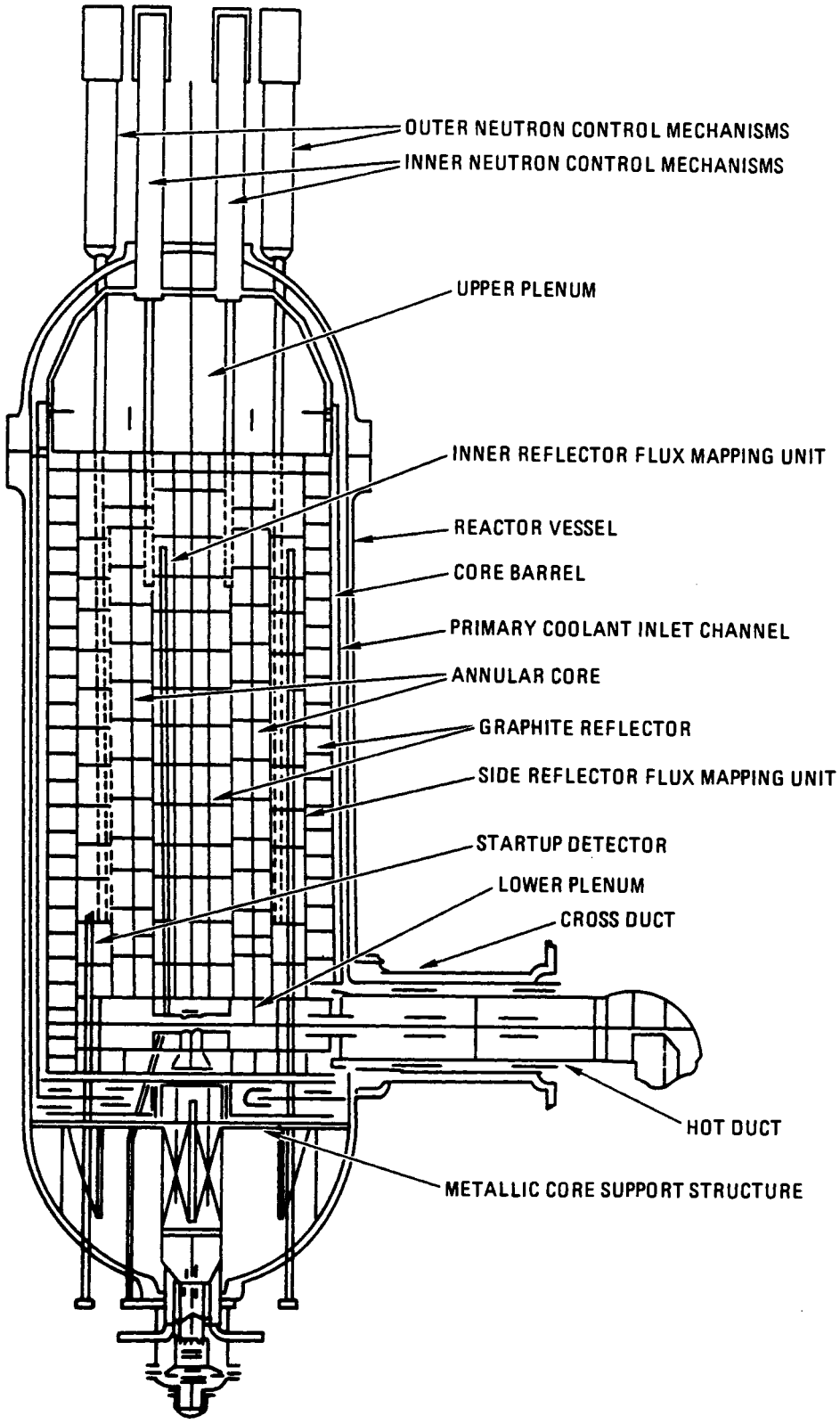


Fig. 4-2. Reactor system - elevation view

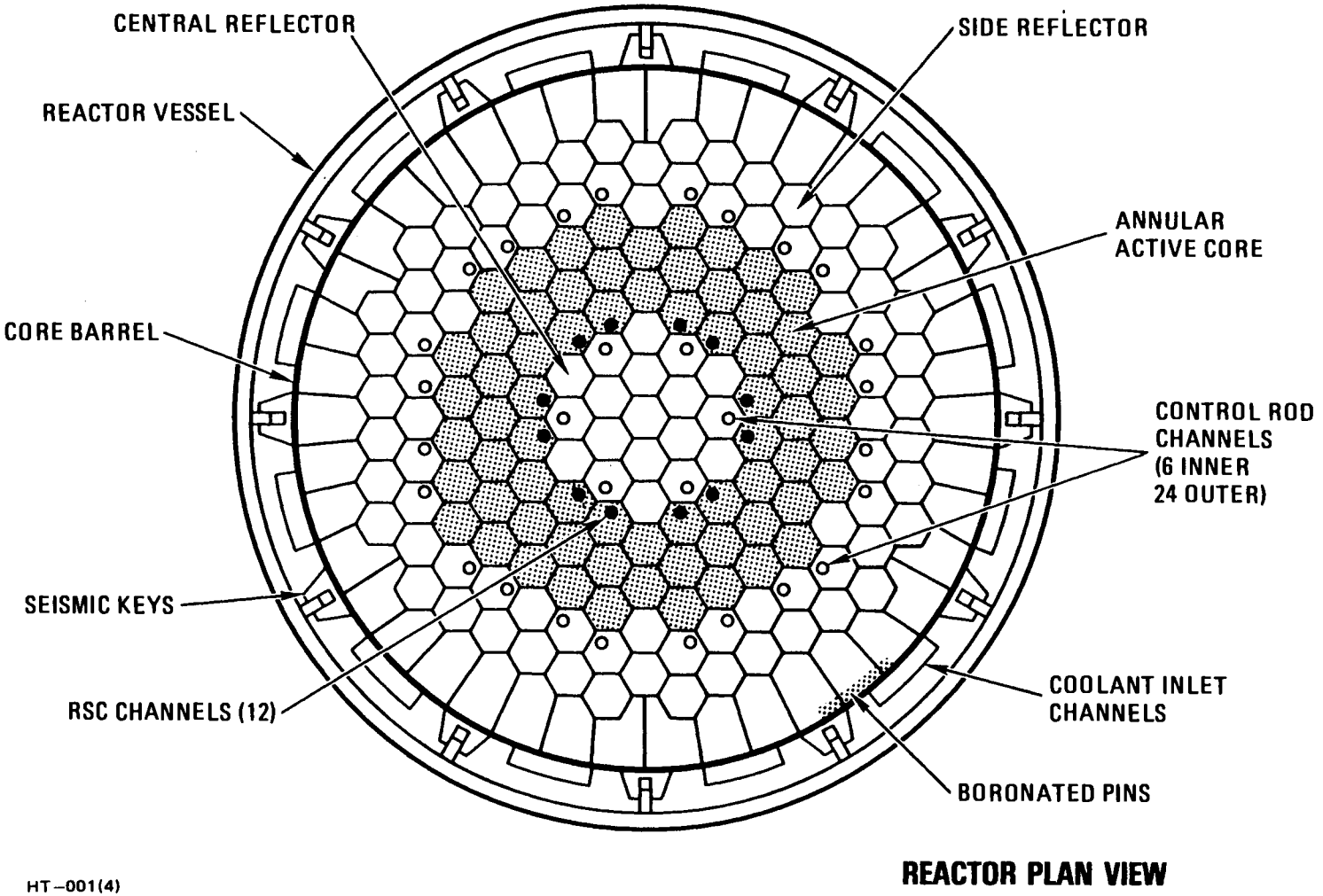


Fig. 4-3. Reactor - plan view

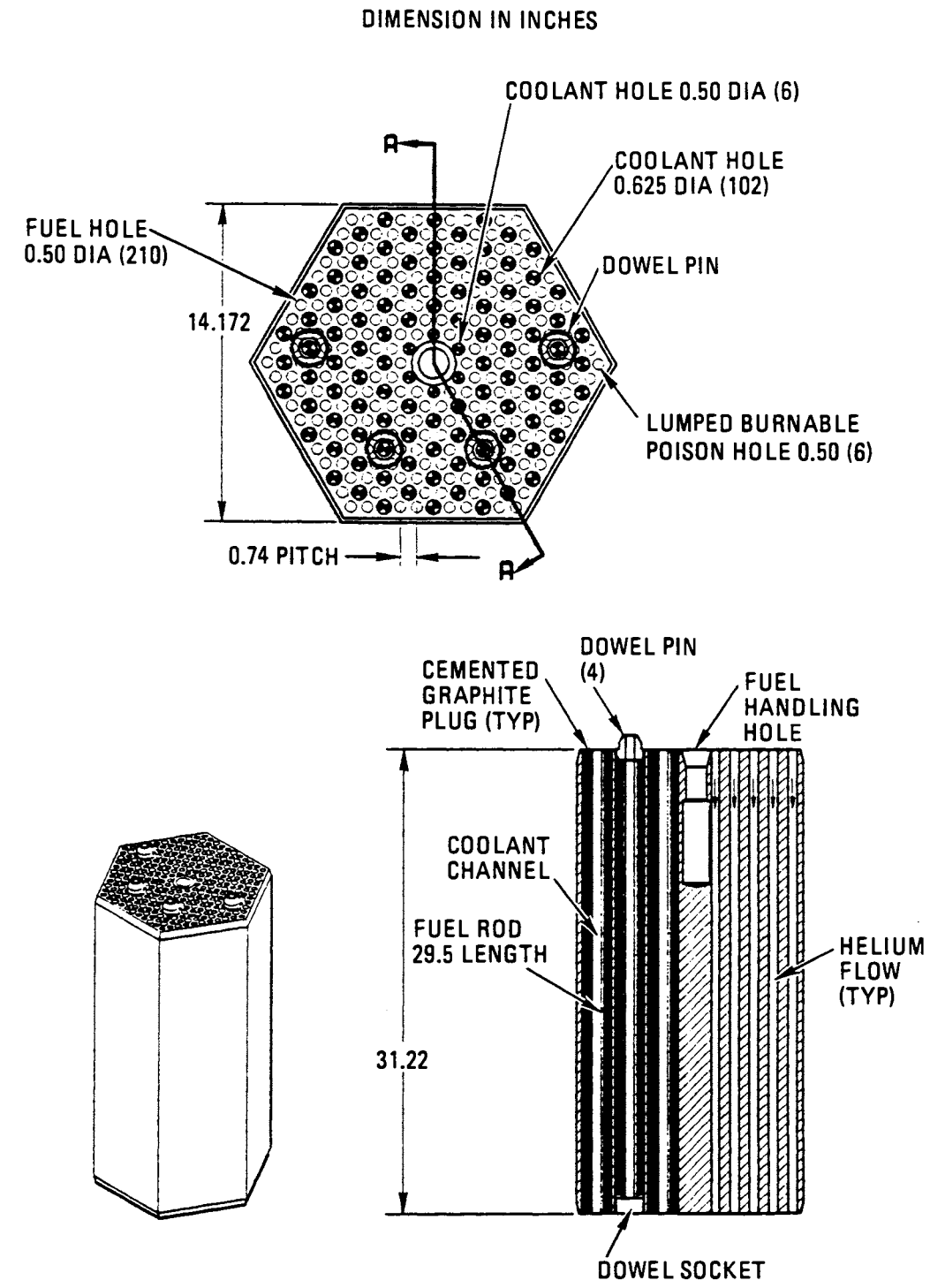
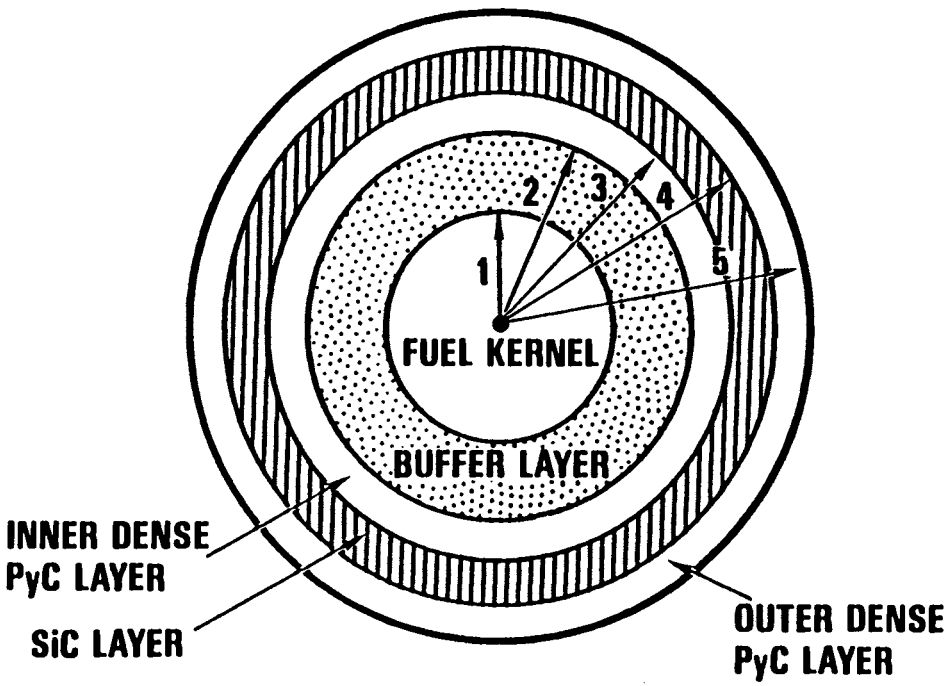


Fig. 4-4. Standard fuel element



1 - FUEL KERNEL
- HEAVY METAL

2 - BUFFER LAYER
- ATTENUATE FISSION RECOILS
- VOID VOLUME FOR FISSION GASES

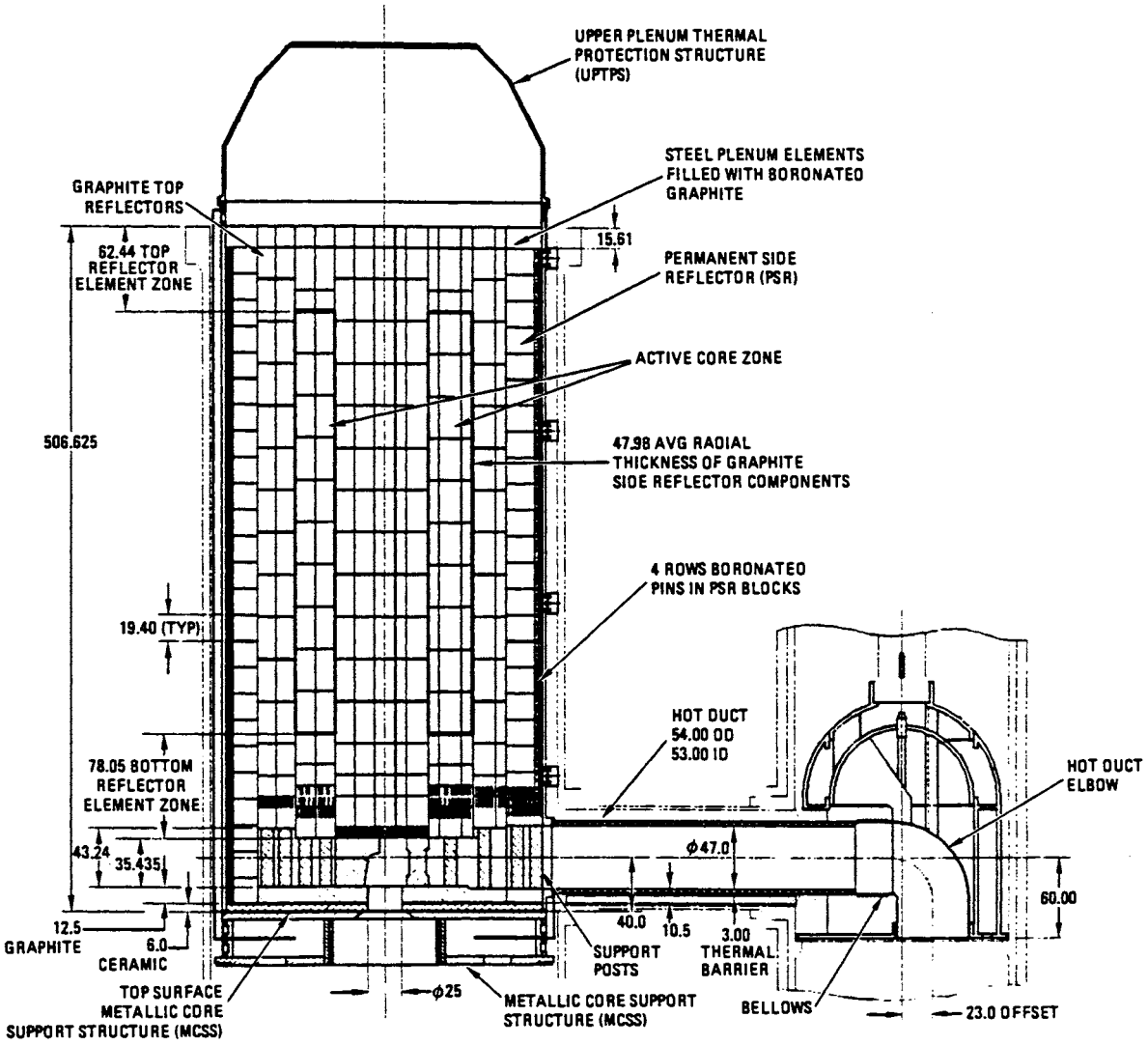
3 - INNER PyC (IPyC)
- PREVENT Cl INGRESS DURING SiC DEPOSITION

4 - SILICON CARBIDE (SiC)
- LOAD-BEARING LAYER
- PREVENT METALLIC FP RELEASE

5 - OUTER PyC (OPyC)
- ADDED STRUCTURAL SUPPORT
- ADDITIONAL FP RELEASE BARRIER
- BONDING SURFACE

Fig. 4-5. TRISO-coated fuel description

DIMENSIONS IN INCHES



HT-001(7)

Fig. 4-6. Reactor core and internals arrangement - elevation view

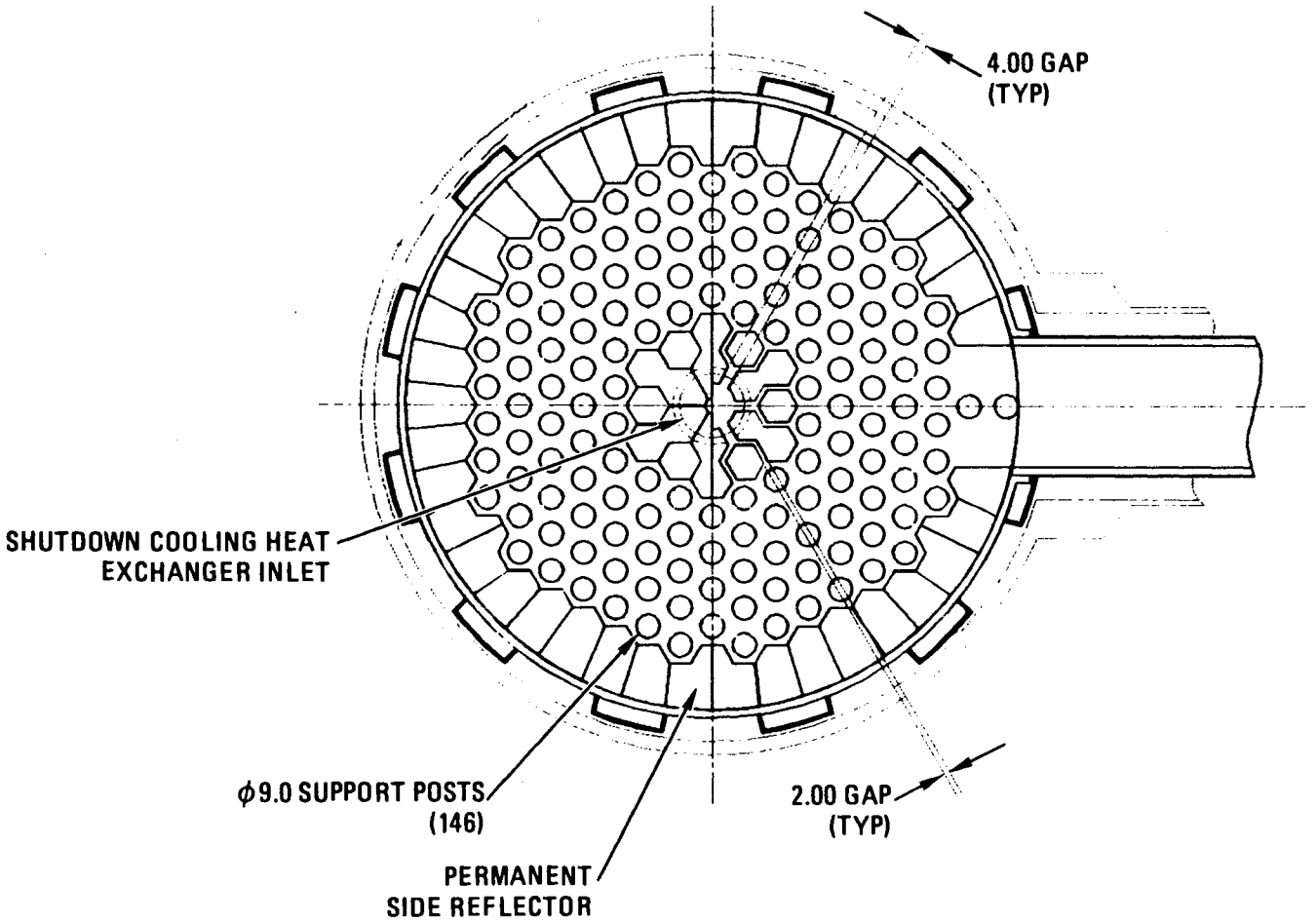


Fig. 4-7. Graphite core support structure - plan view

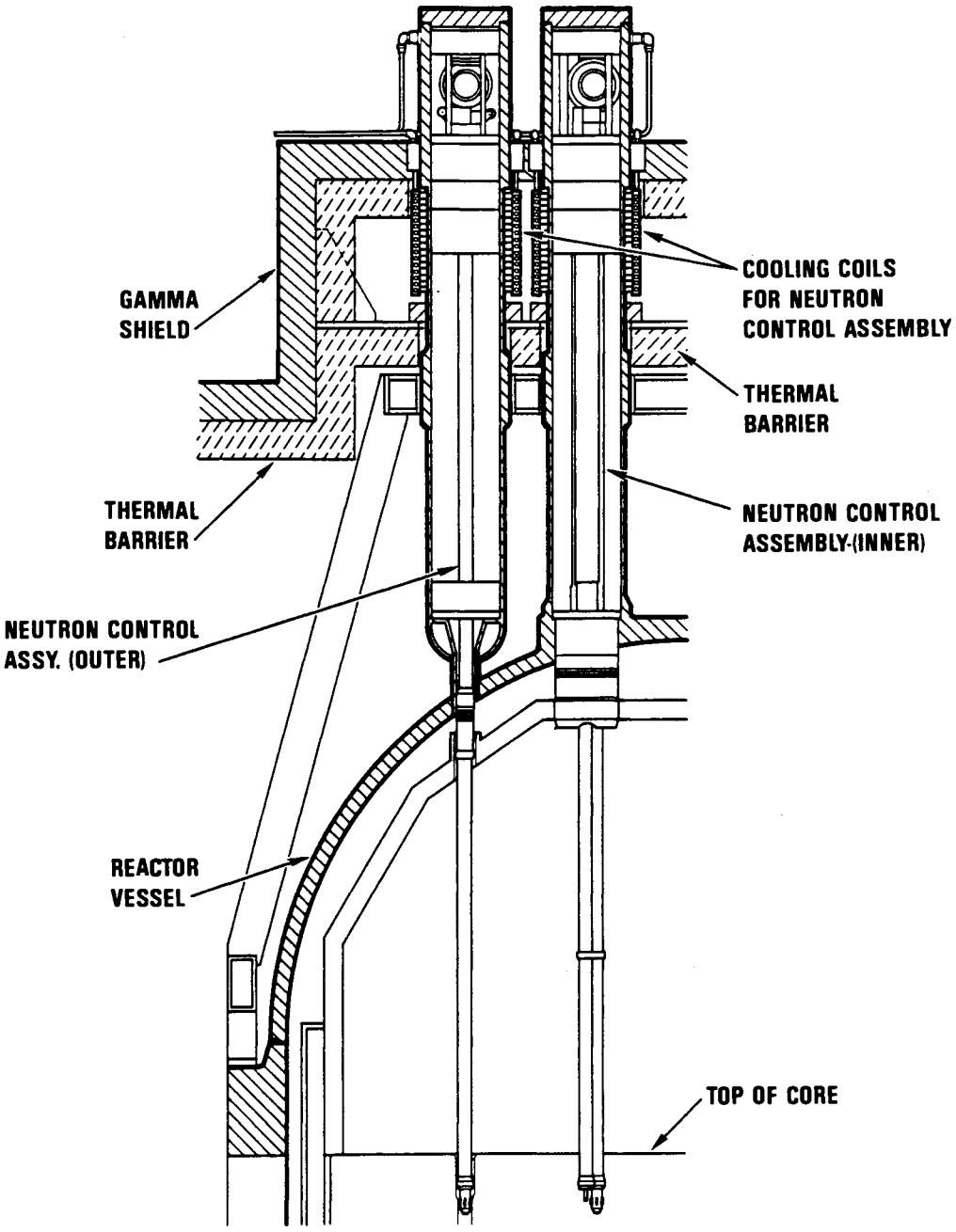
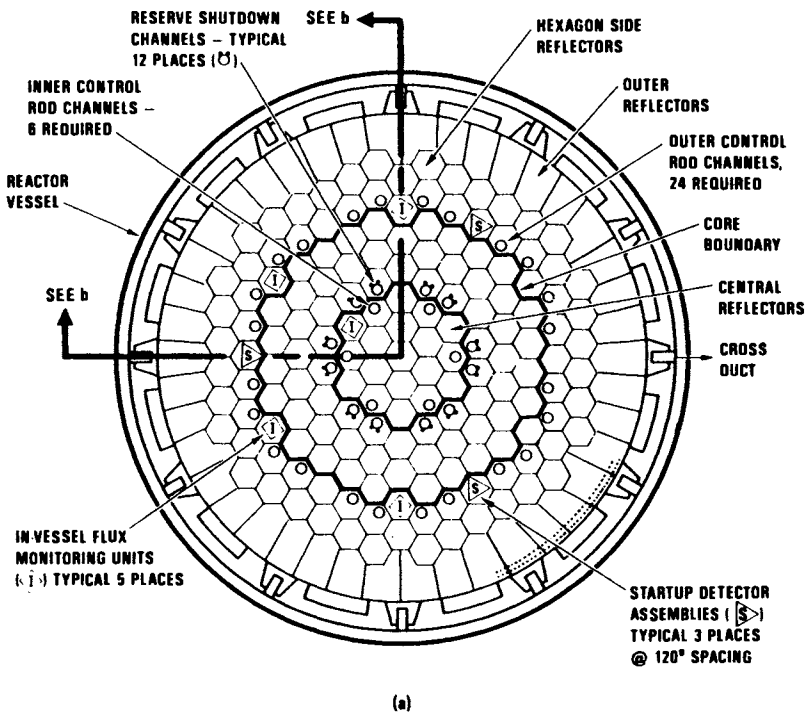
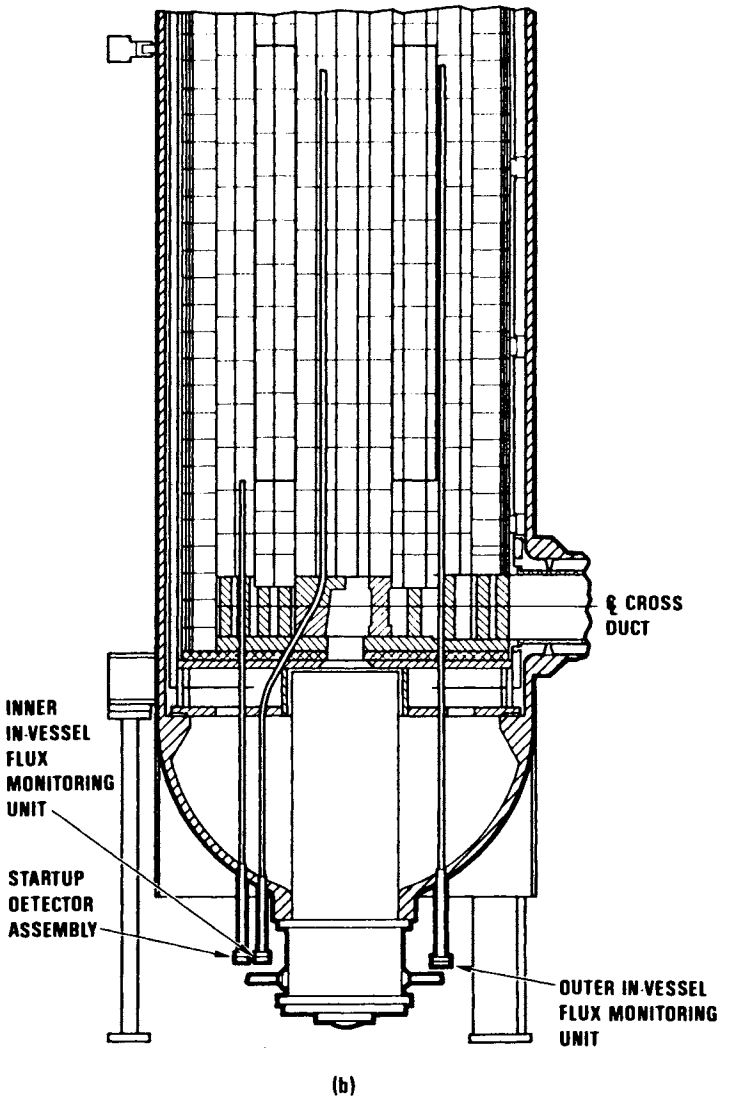


Fig. 4-8. Control assemblies installed in reactor vessel





HT–001(10)

Fig. 4-9. Reactor core

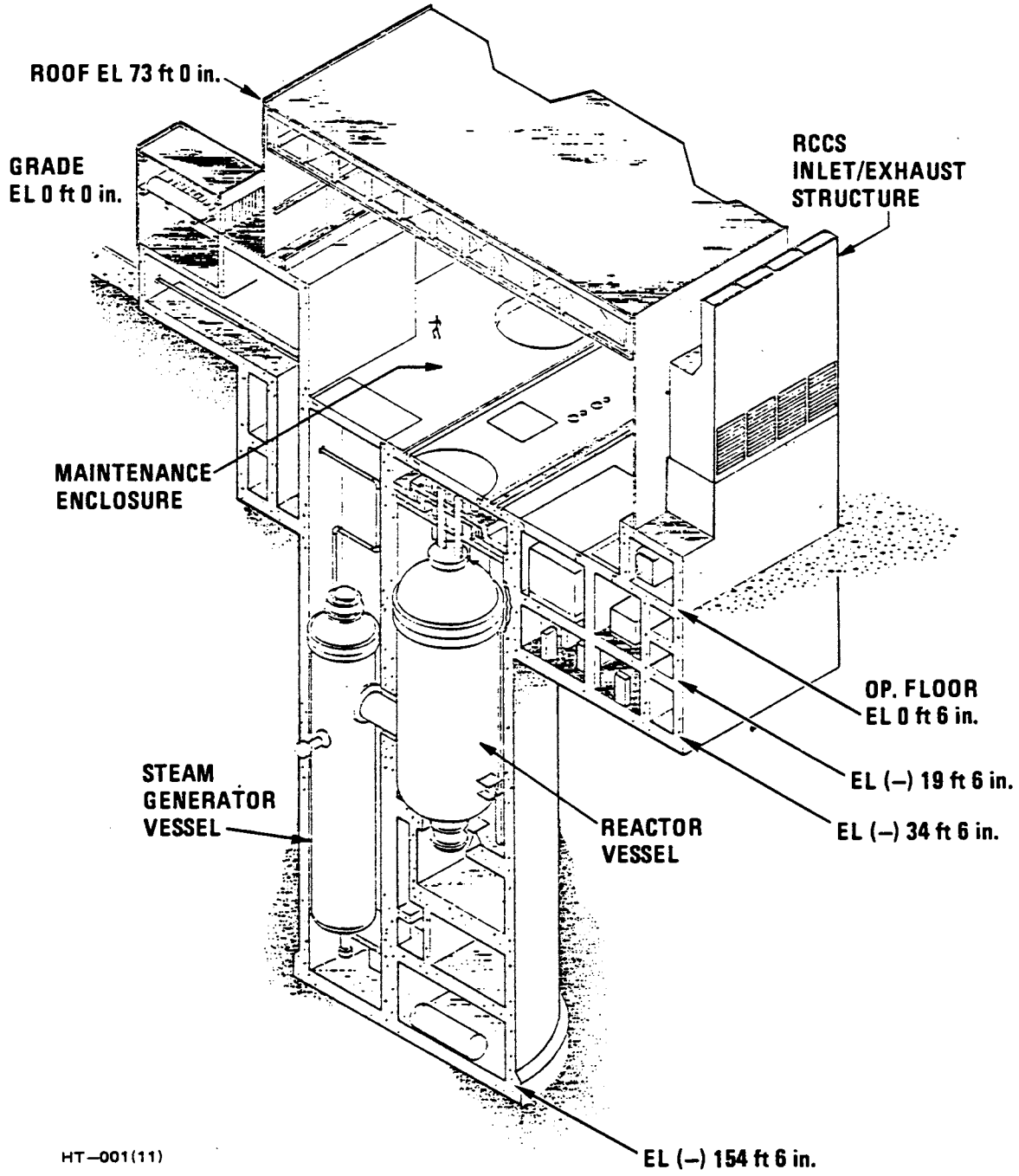


Fig. 4-10. Isometric view through reactor building

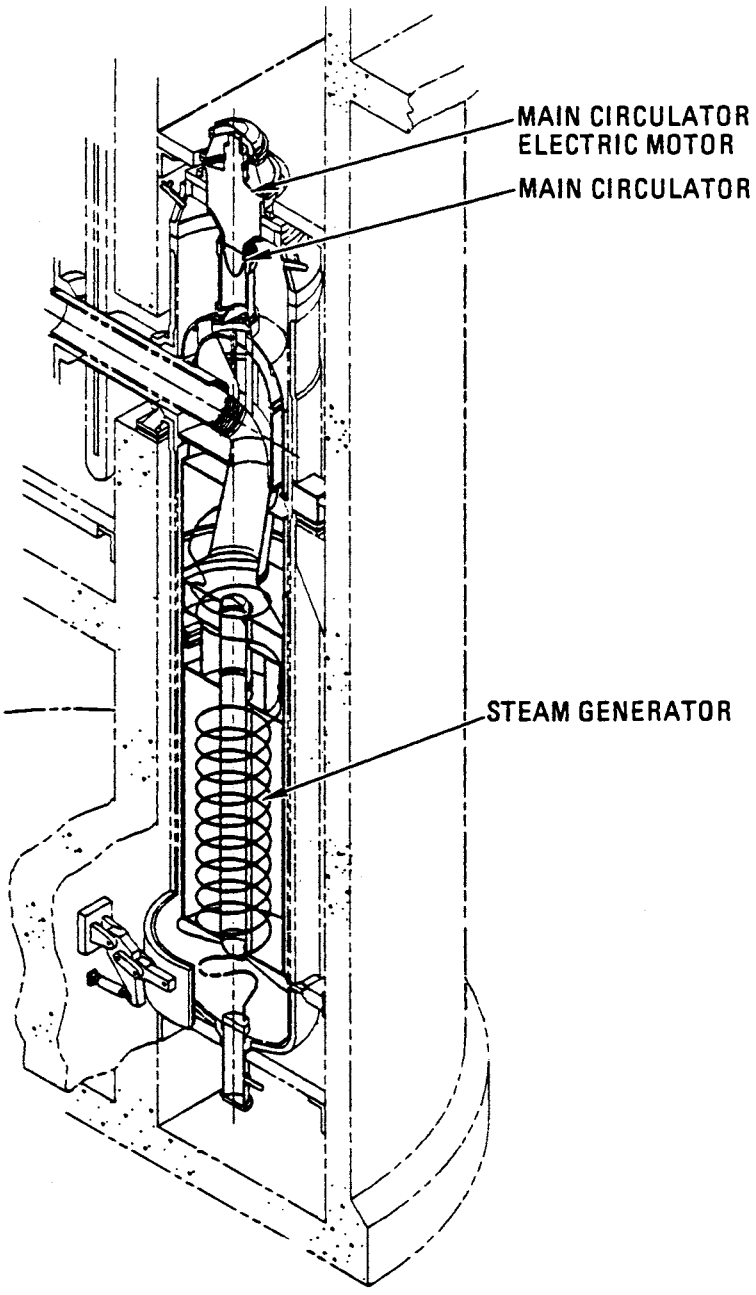
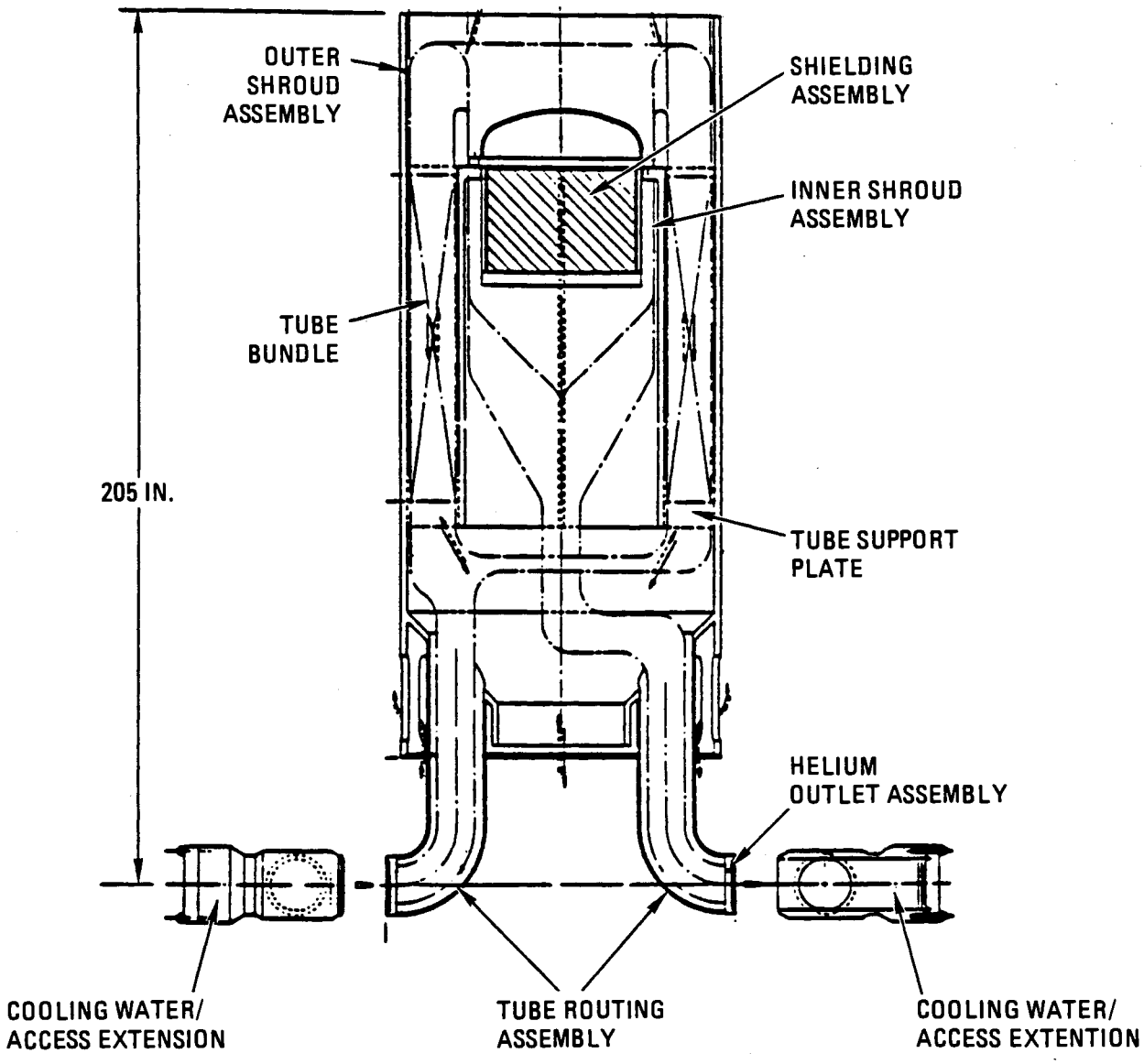


Fig. 4-11. Heat transport system arrangement



HT-001(13)

Fig. 4-12. Shutdown cooling heat exchanger subsystem configuration

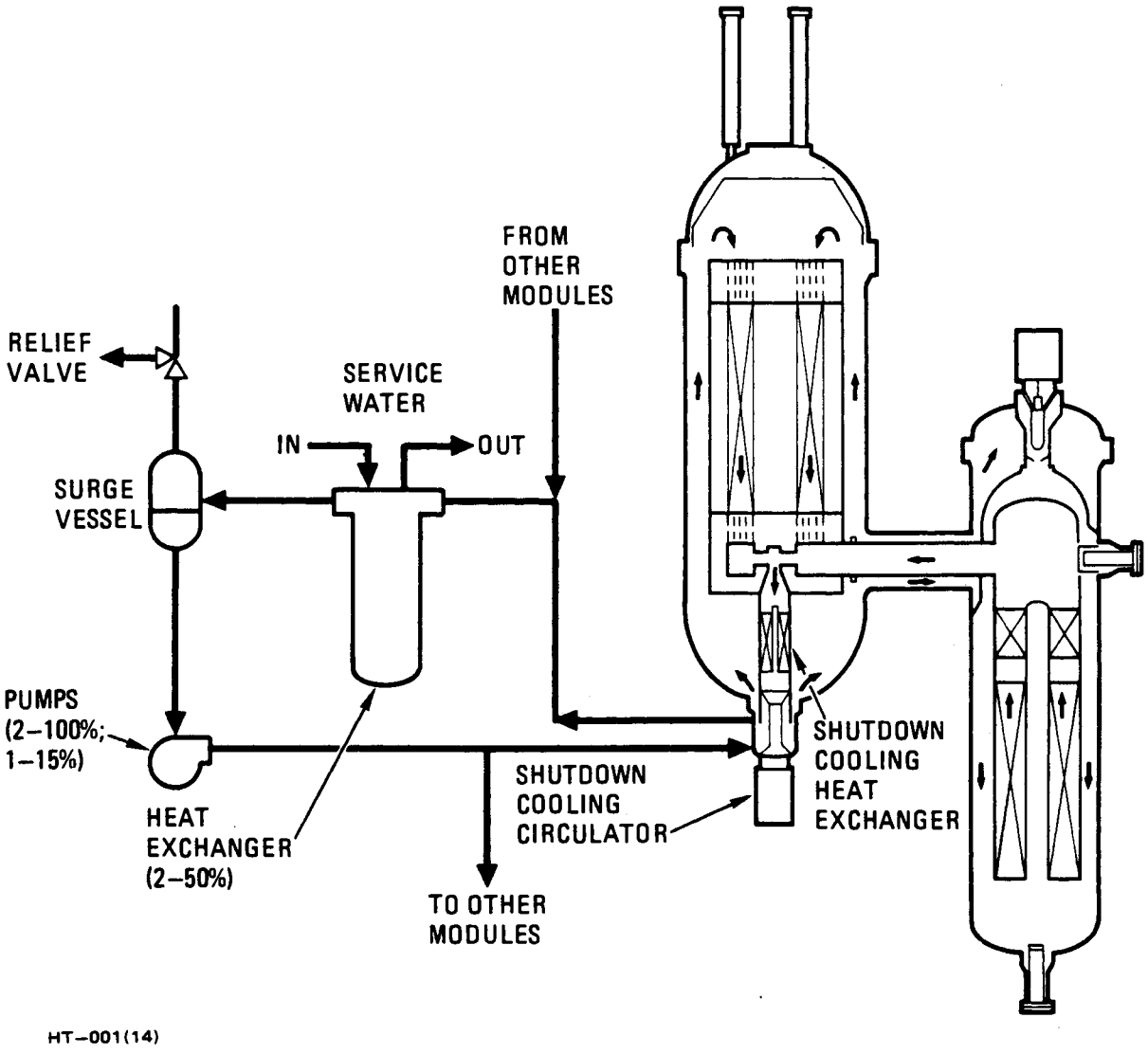


Fig. 4-13. Shutdown cooling system arrangement

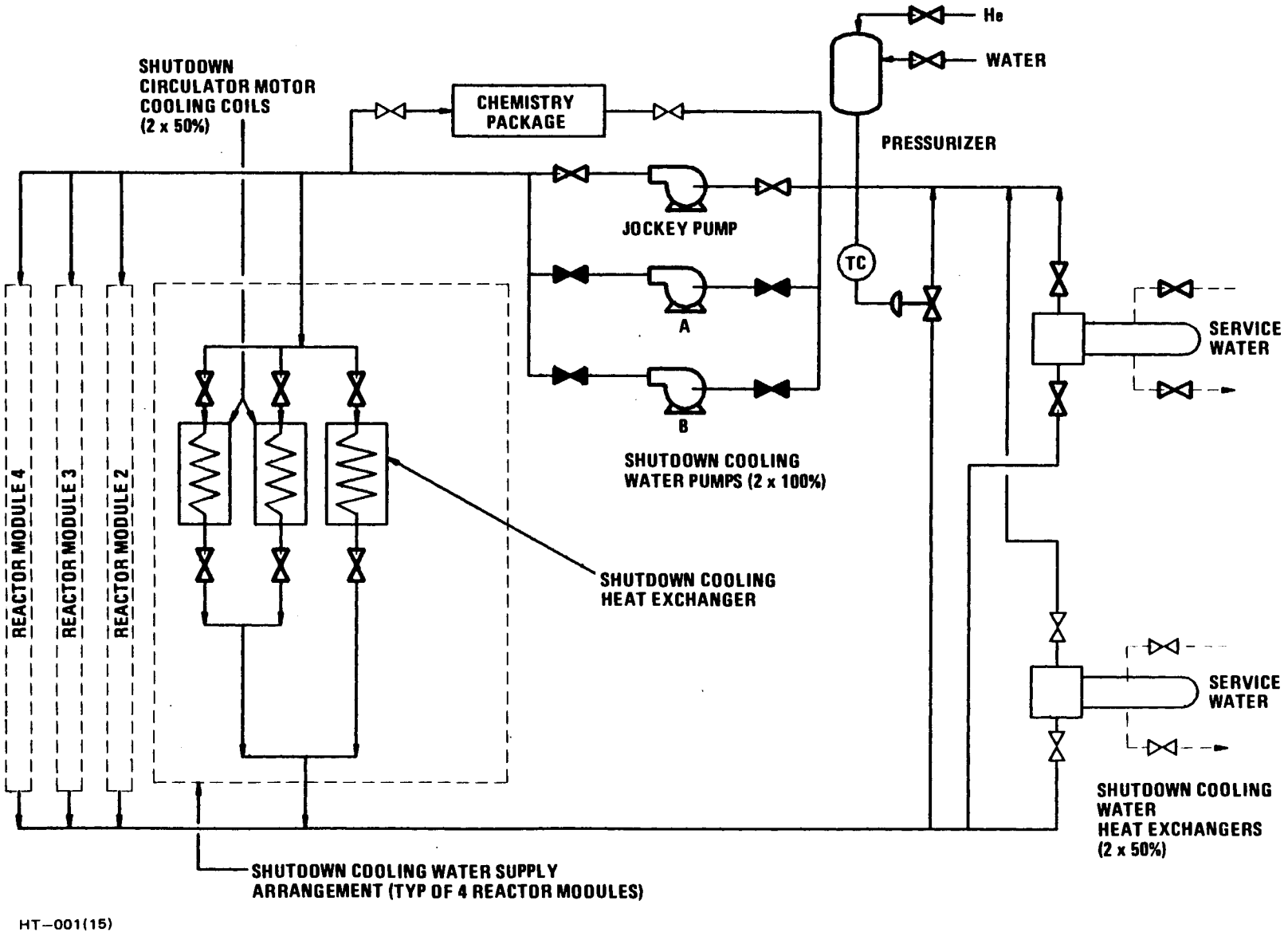


Fig. 4-14. Shutdown cooling water subsystem

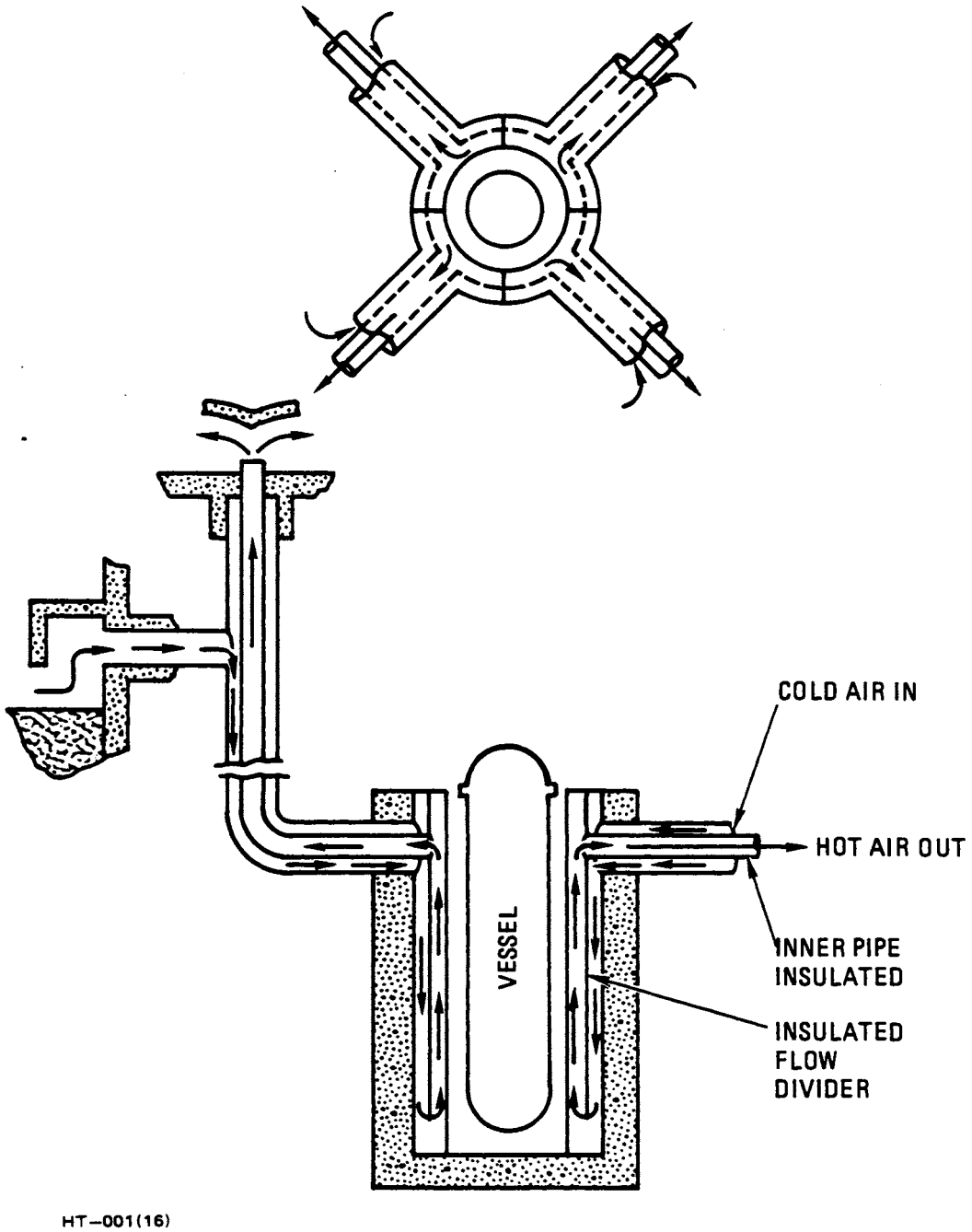


Fig. 4-15. Reactor cavity cooling system

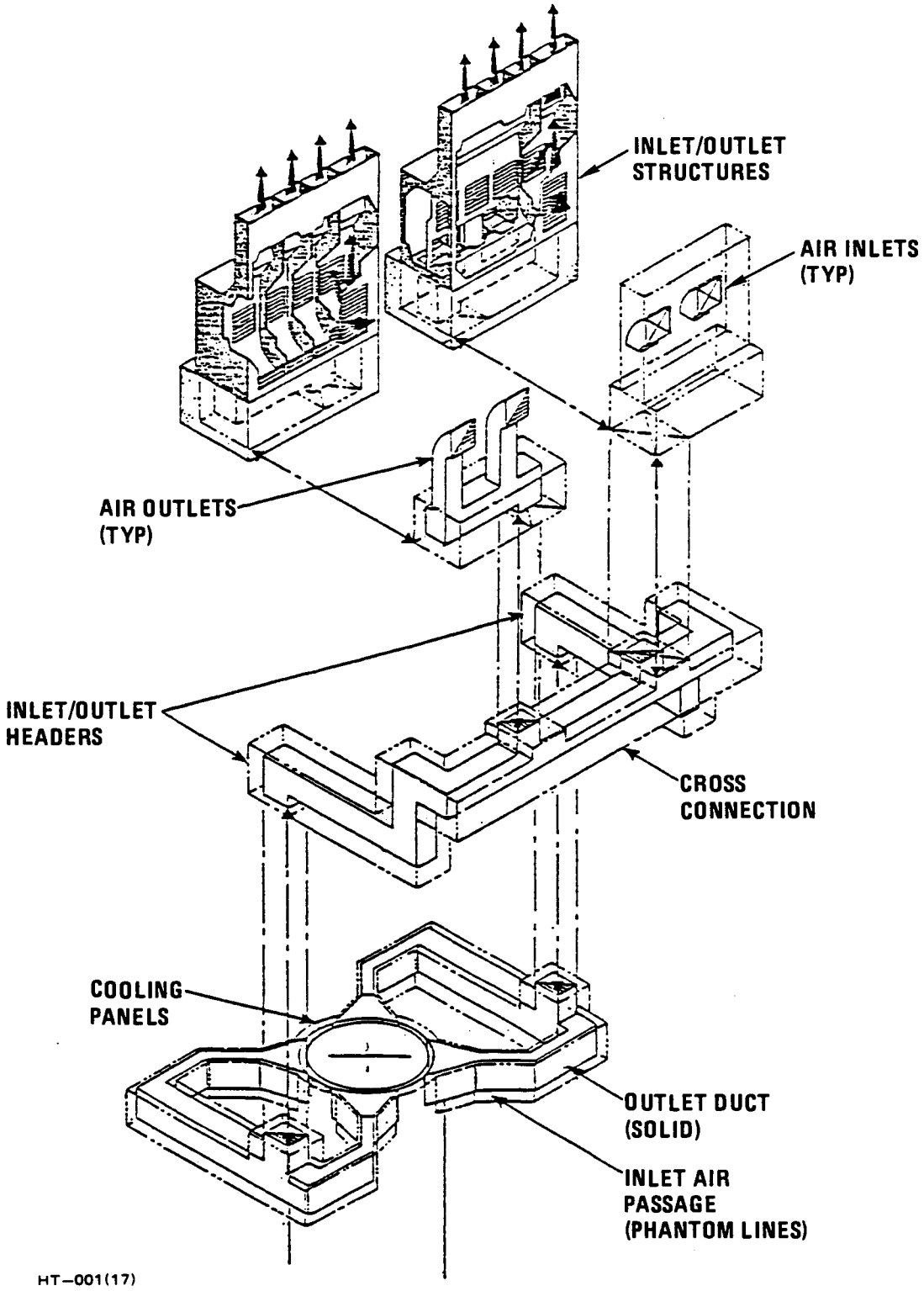
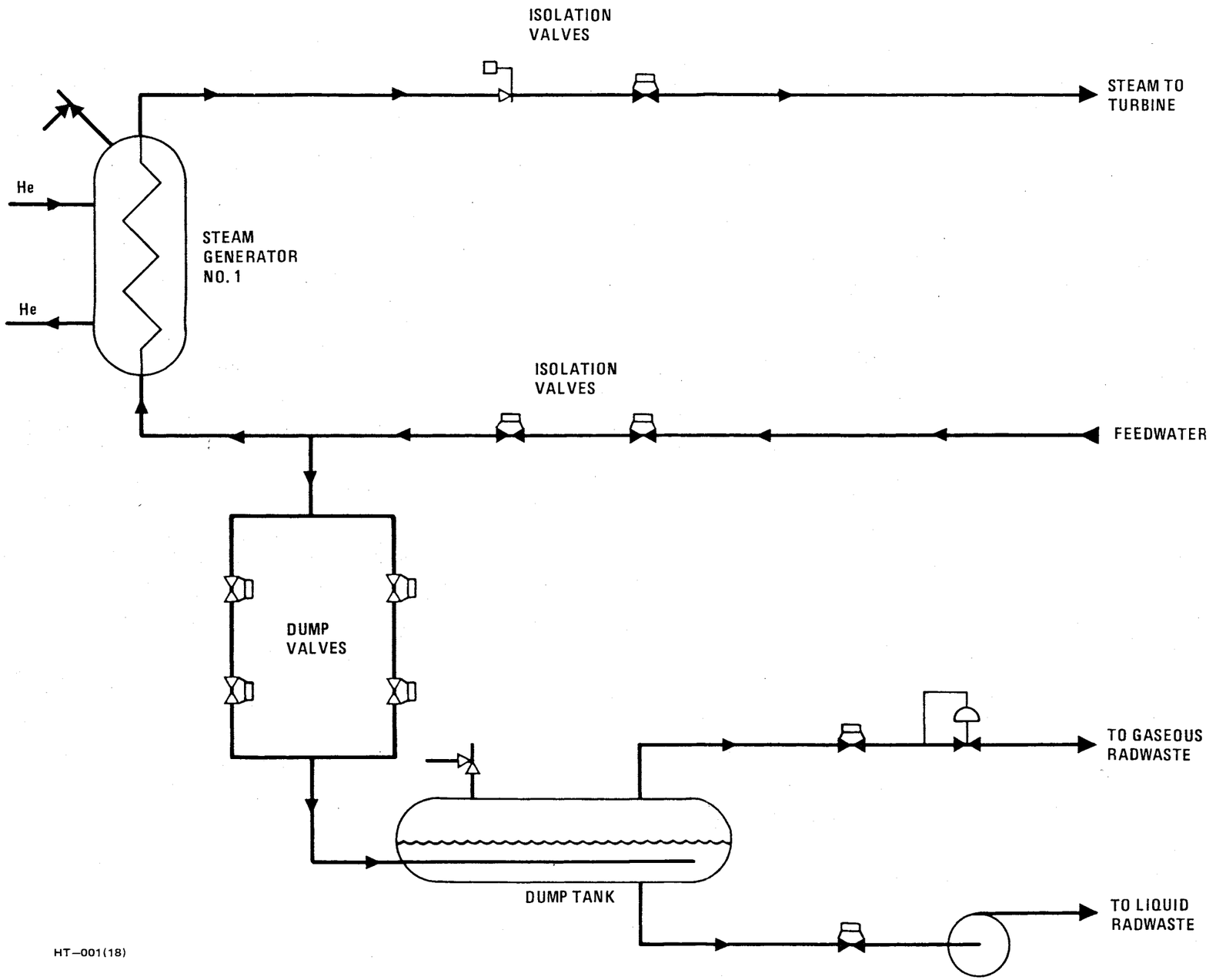


Fig. 4-16. Air RCCS ductwork isometric



HT—001(18)

Fig. 4-17. Steam and water dump subsystem schematic

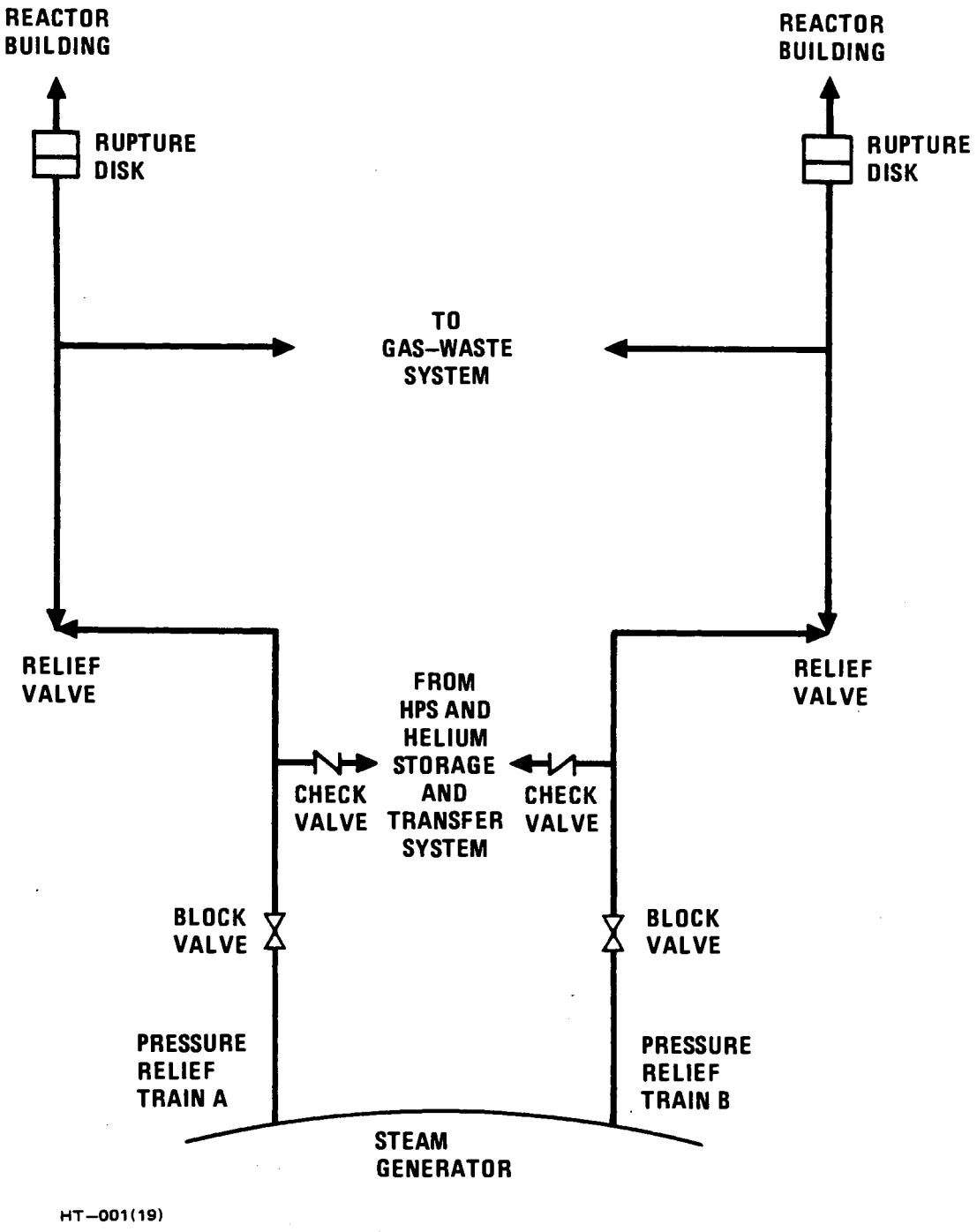


Fig. 4-18. Pressure relief subsystem schematic

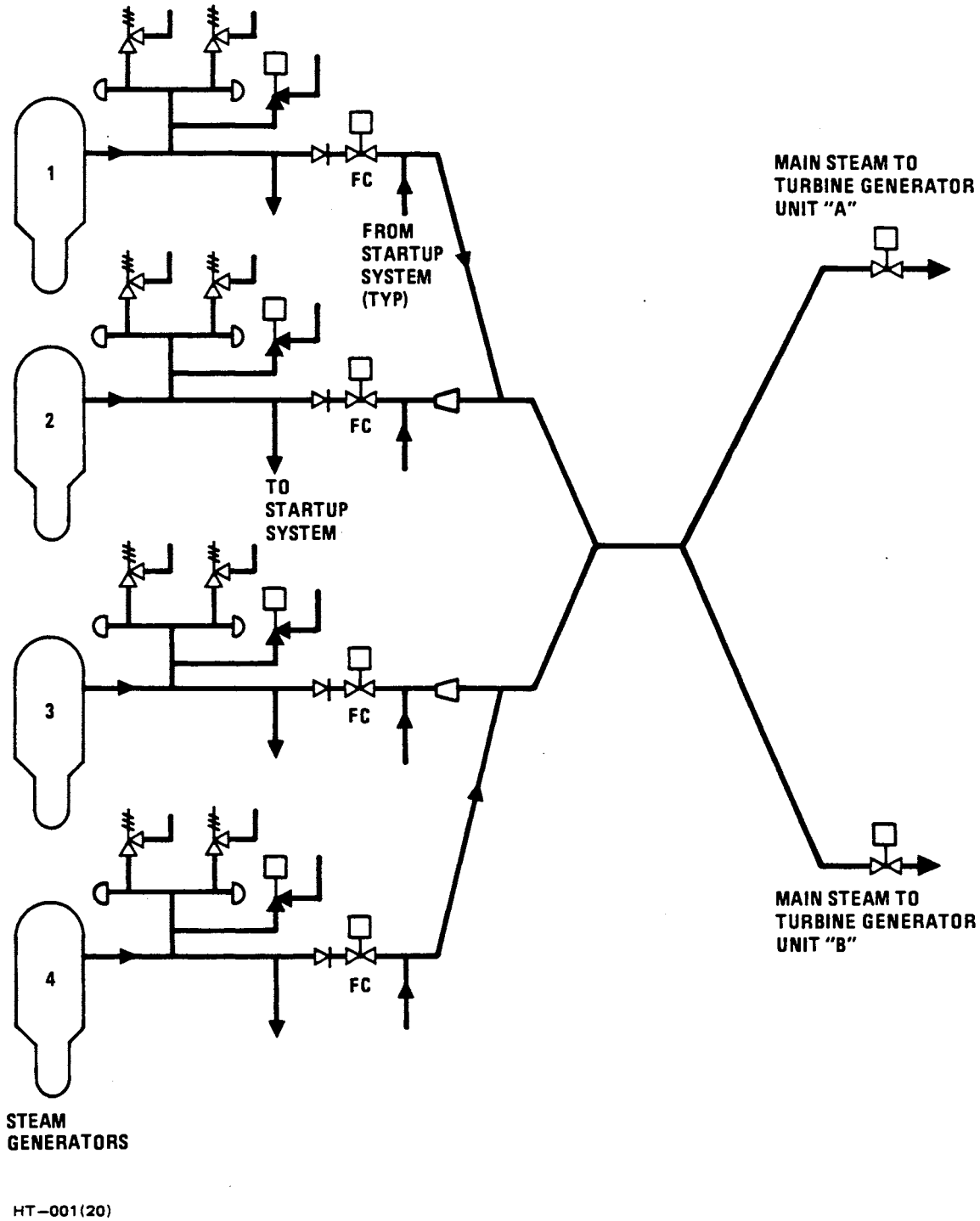


Fig. 4-19. Main and bypass steam subsystem

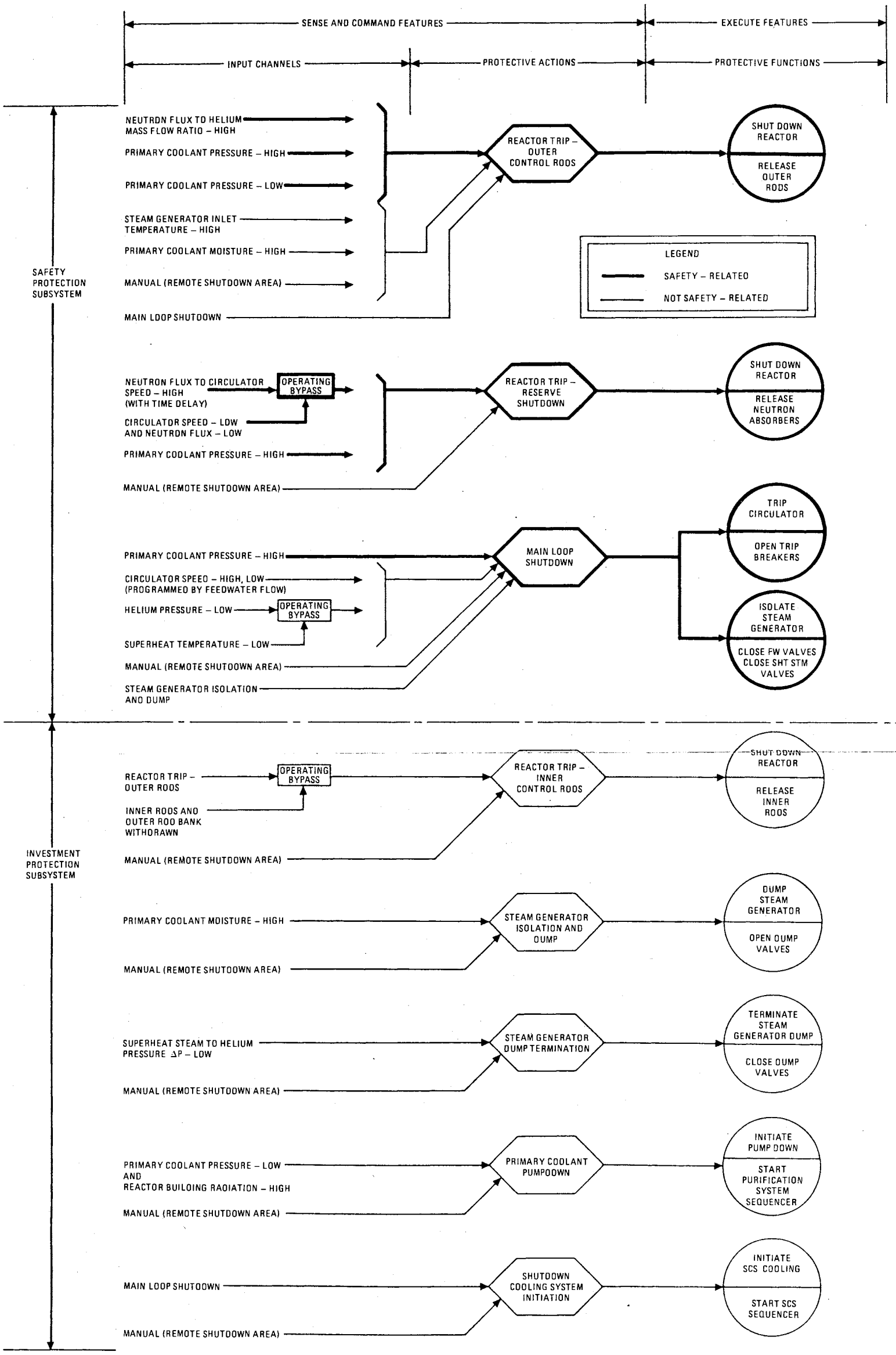
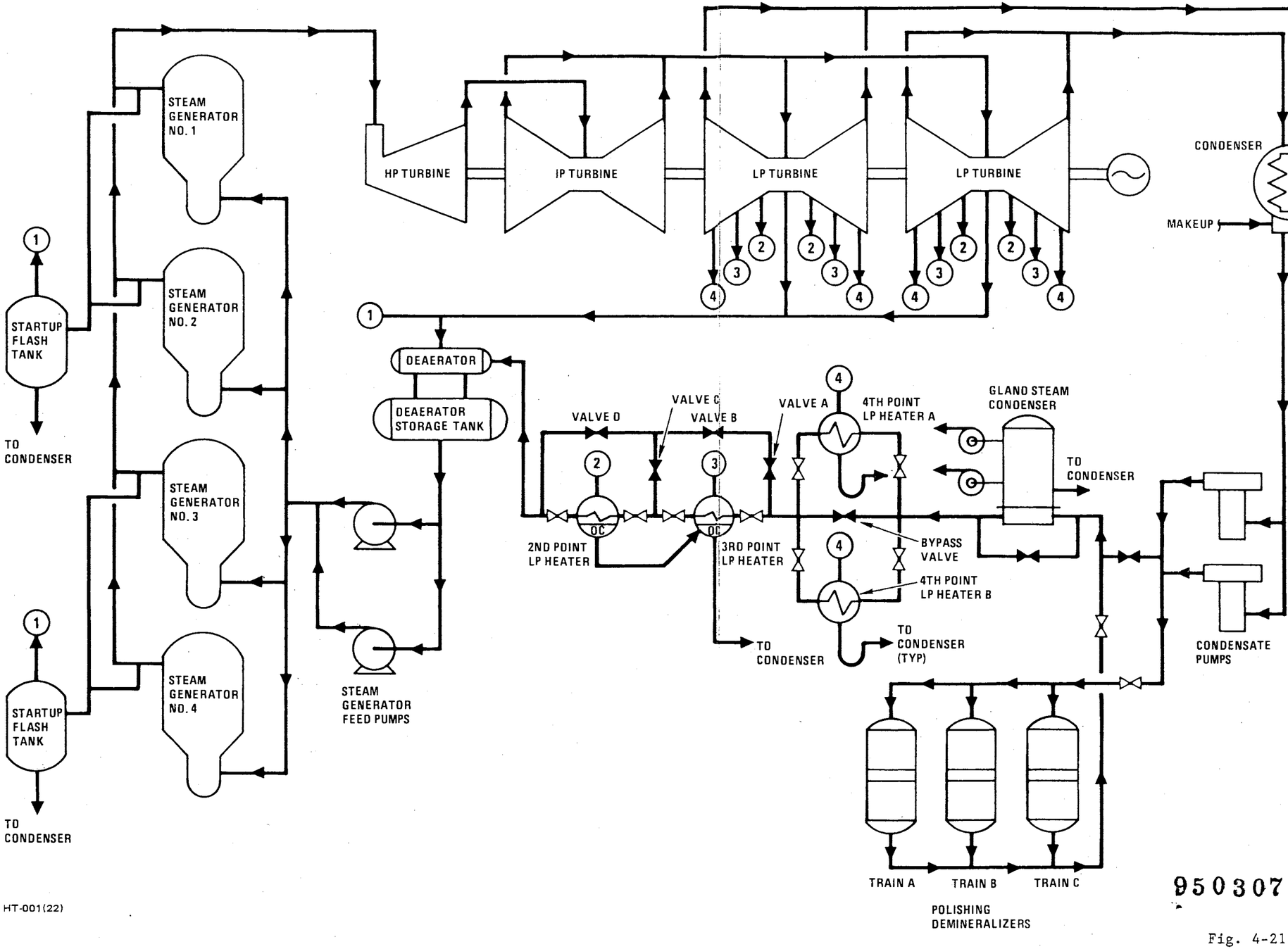
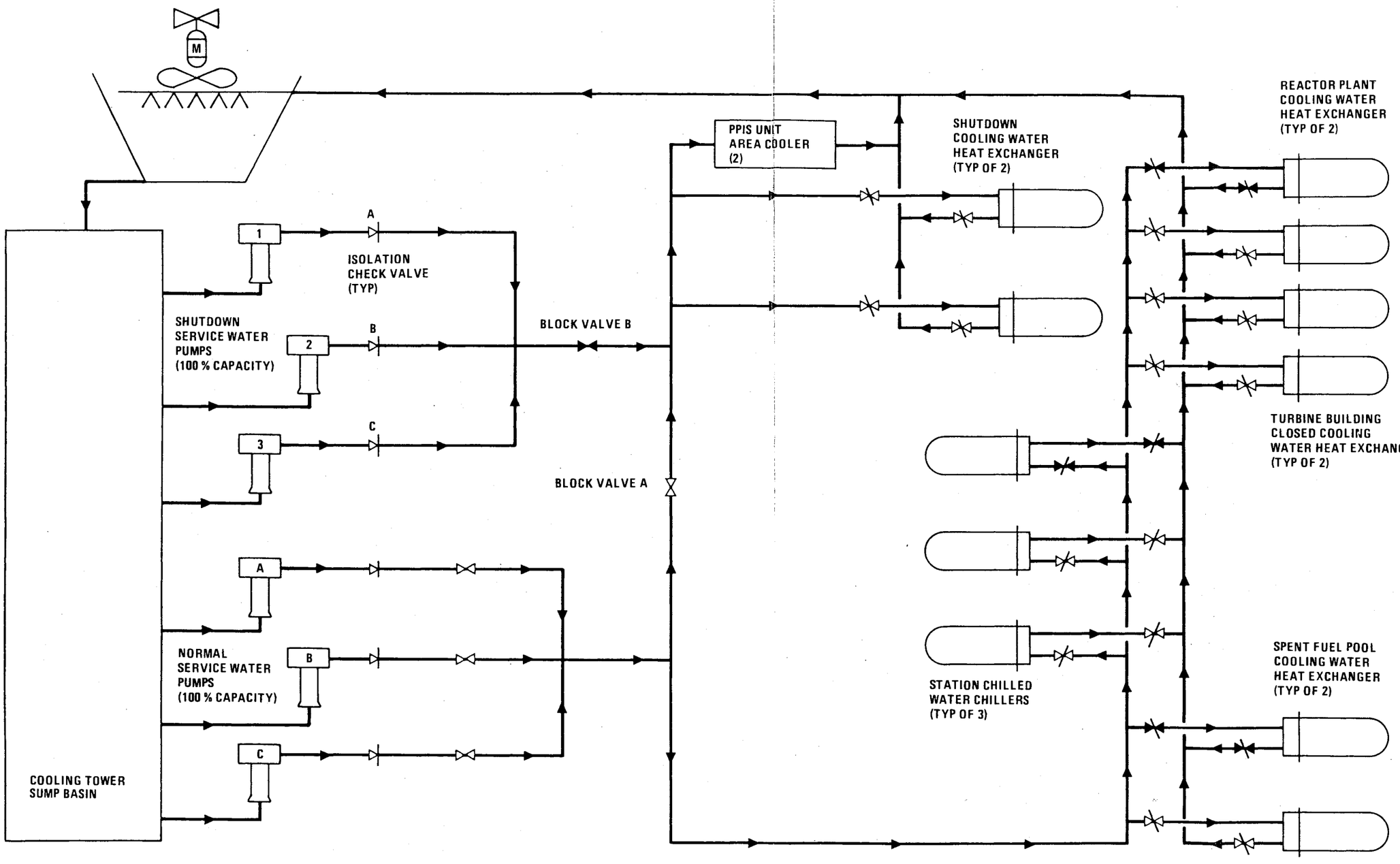


Fig. 4-20. Functional overview – PPIS trip subsystem



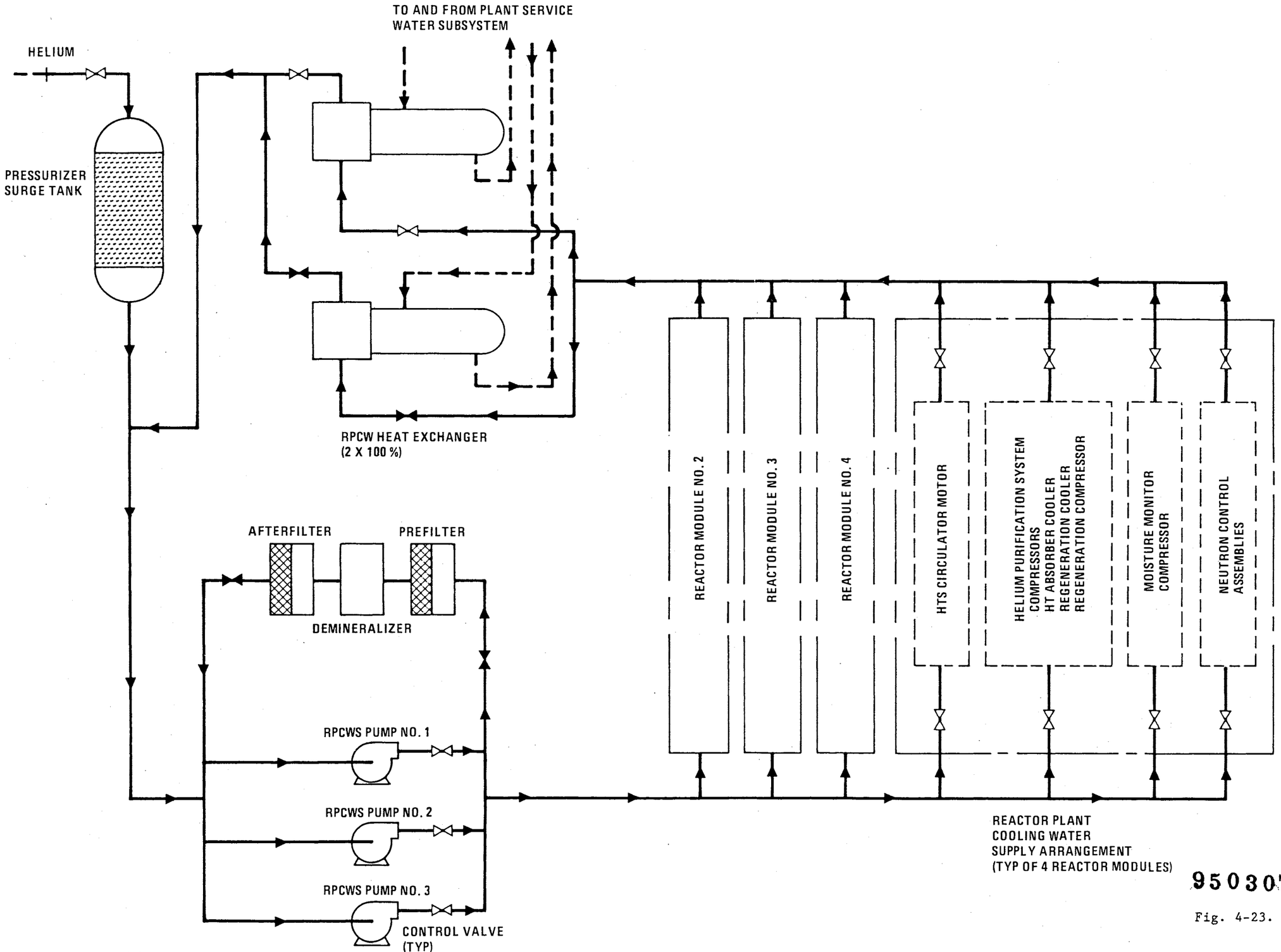
HT-001(22)

Fig. 4-21. Feedwater and condensate subsystem



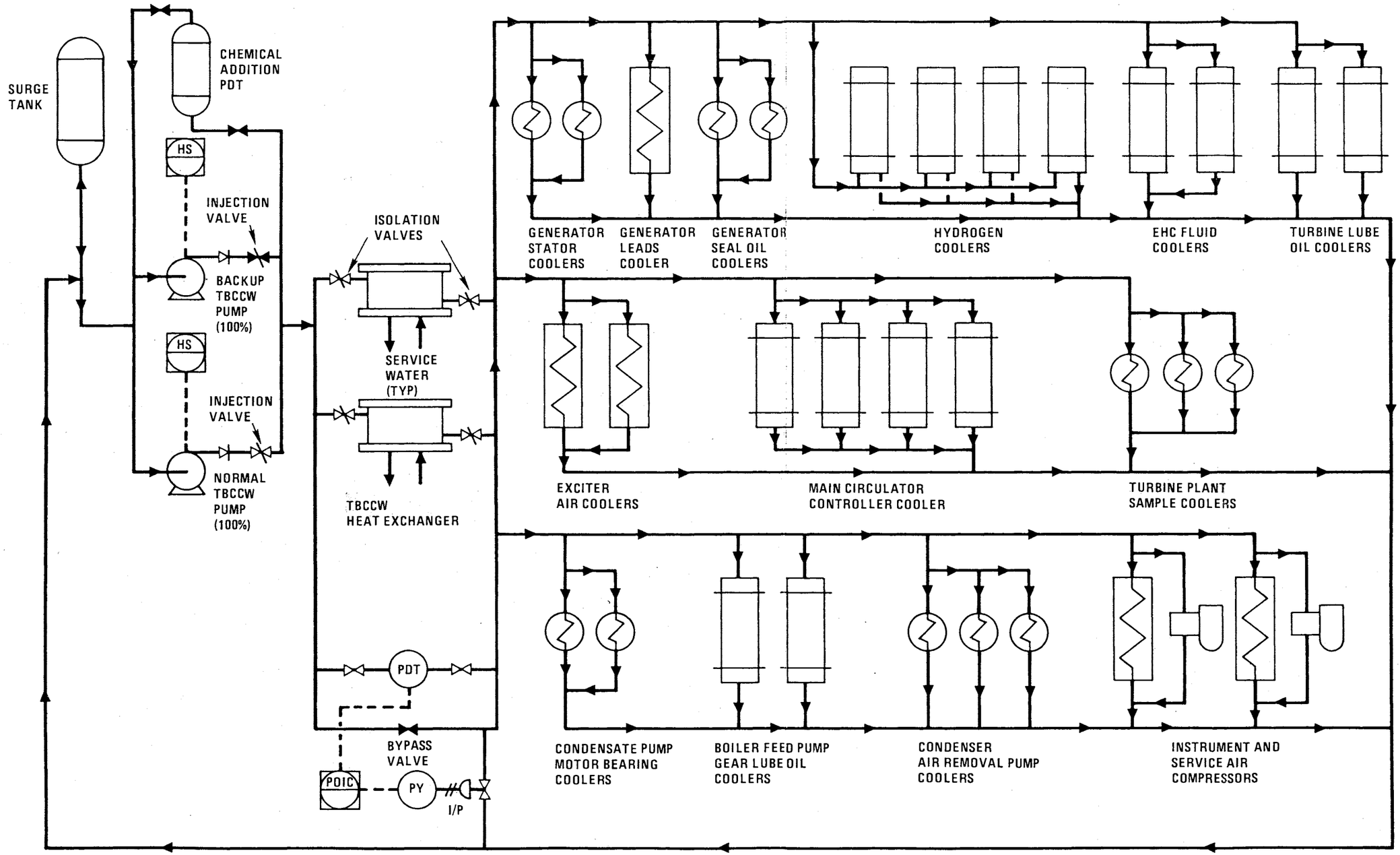
HT-001(23)

Fig. 4-22. Service water subsystem



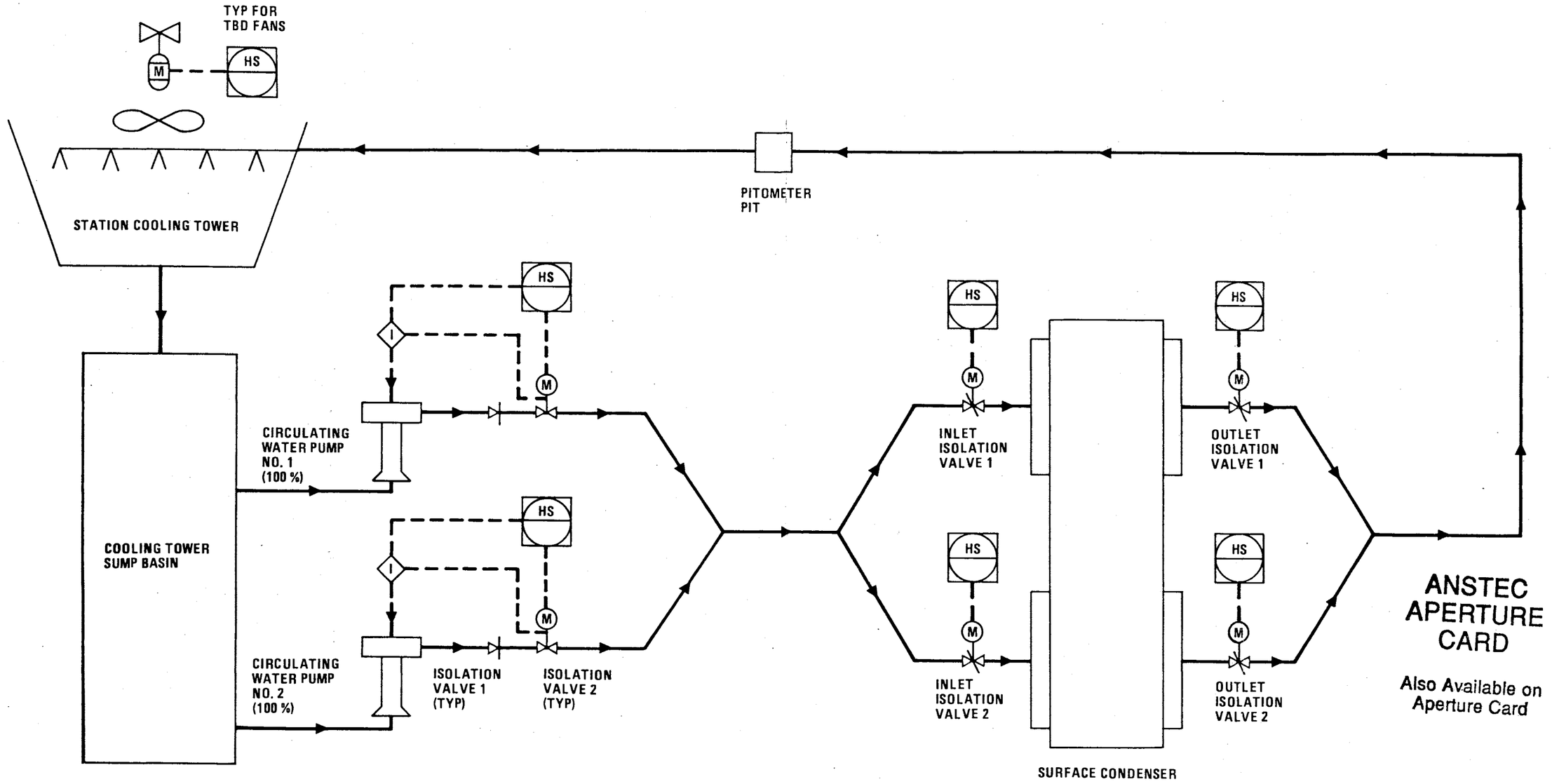
REACTOR PLANT COOLING WATER SUPPLY ARRANGEMENT (TYP OF 4 REACTOR MODULES)

Fig. 4-23. Reactor plant cooling water subsystem



HT-001(25)

Fig. 4-24. Turbine building closed cooling water subsystem



HT–001(26)

Fig. 4-25. Circulating water subsystem

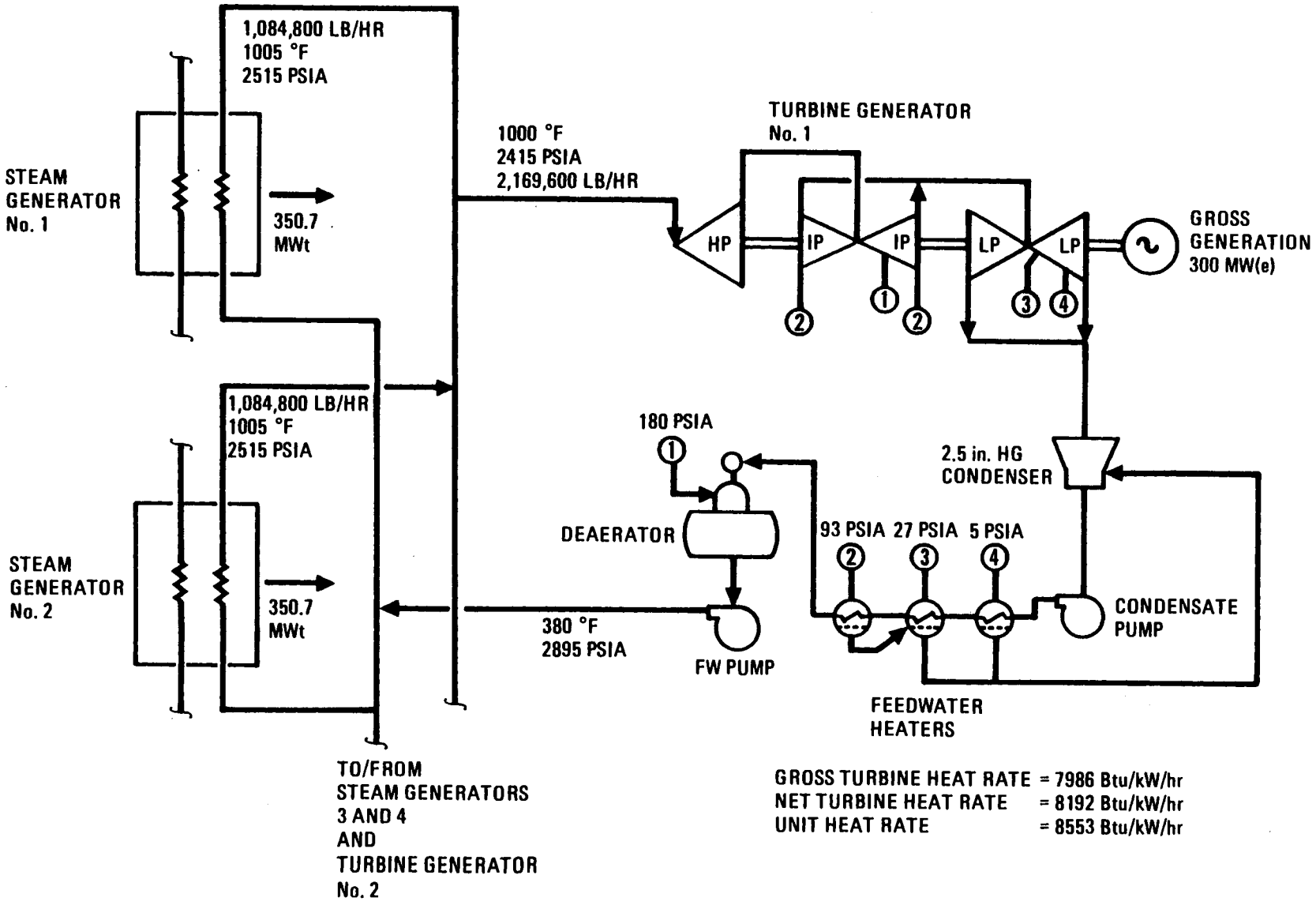
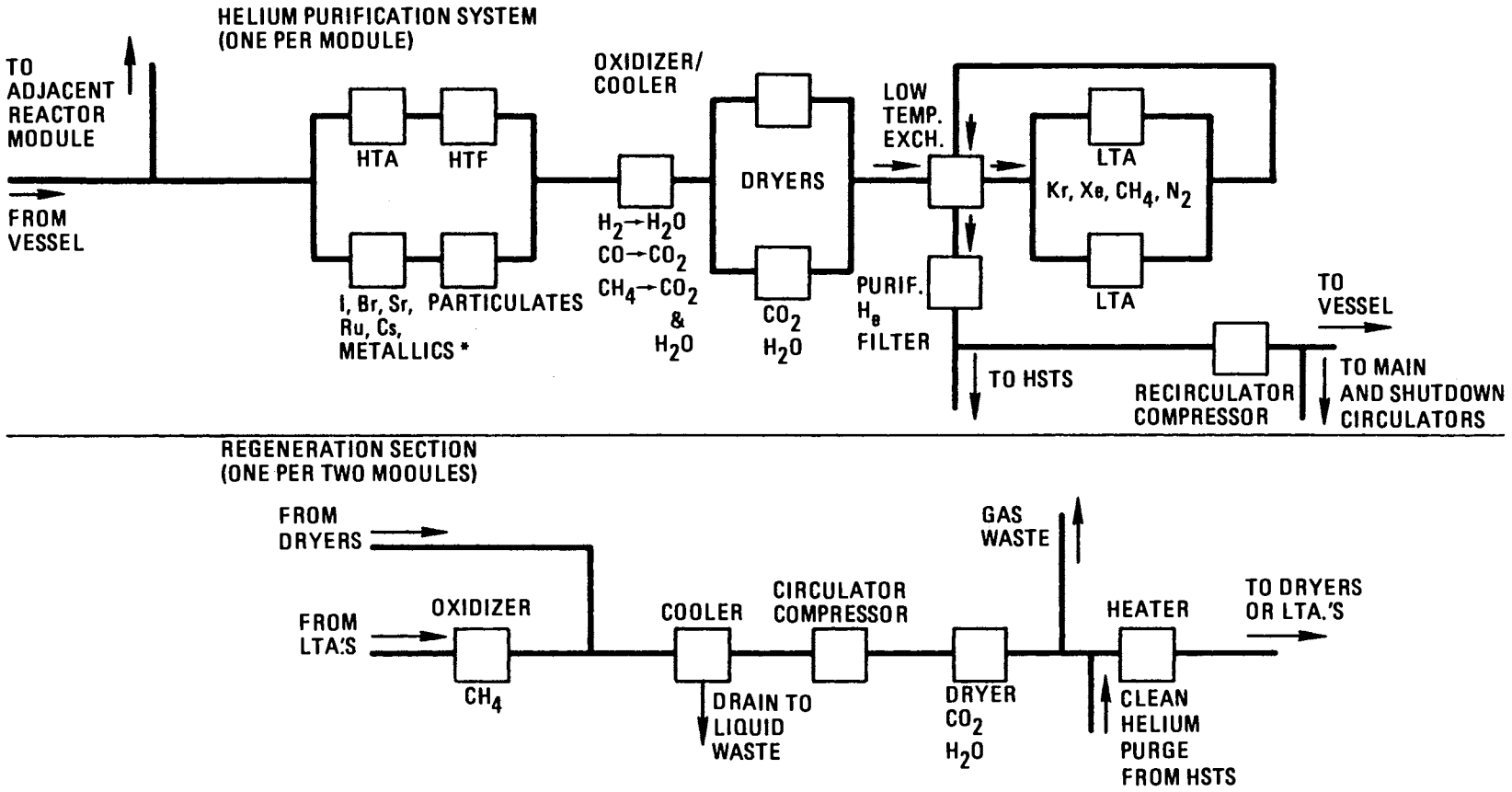


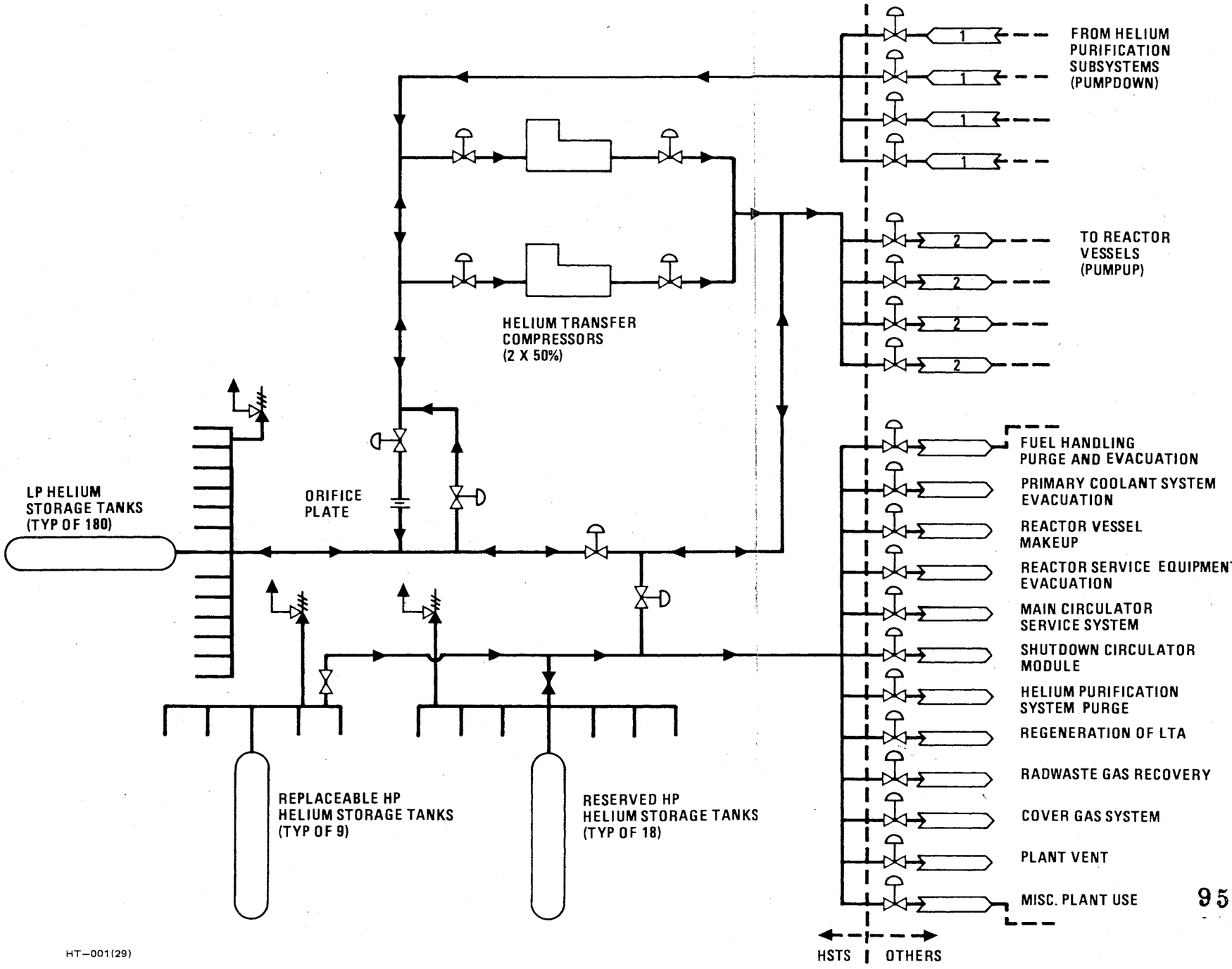
Fig. 4-26. Energy conversion system



* IMPURITIES REMOVED IN EACH COMPONENT ARE TYPICALLY LISTED BELOW THE COMPONENT.

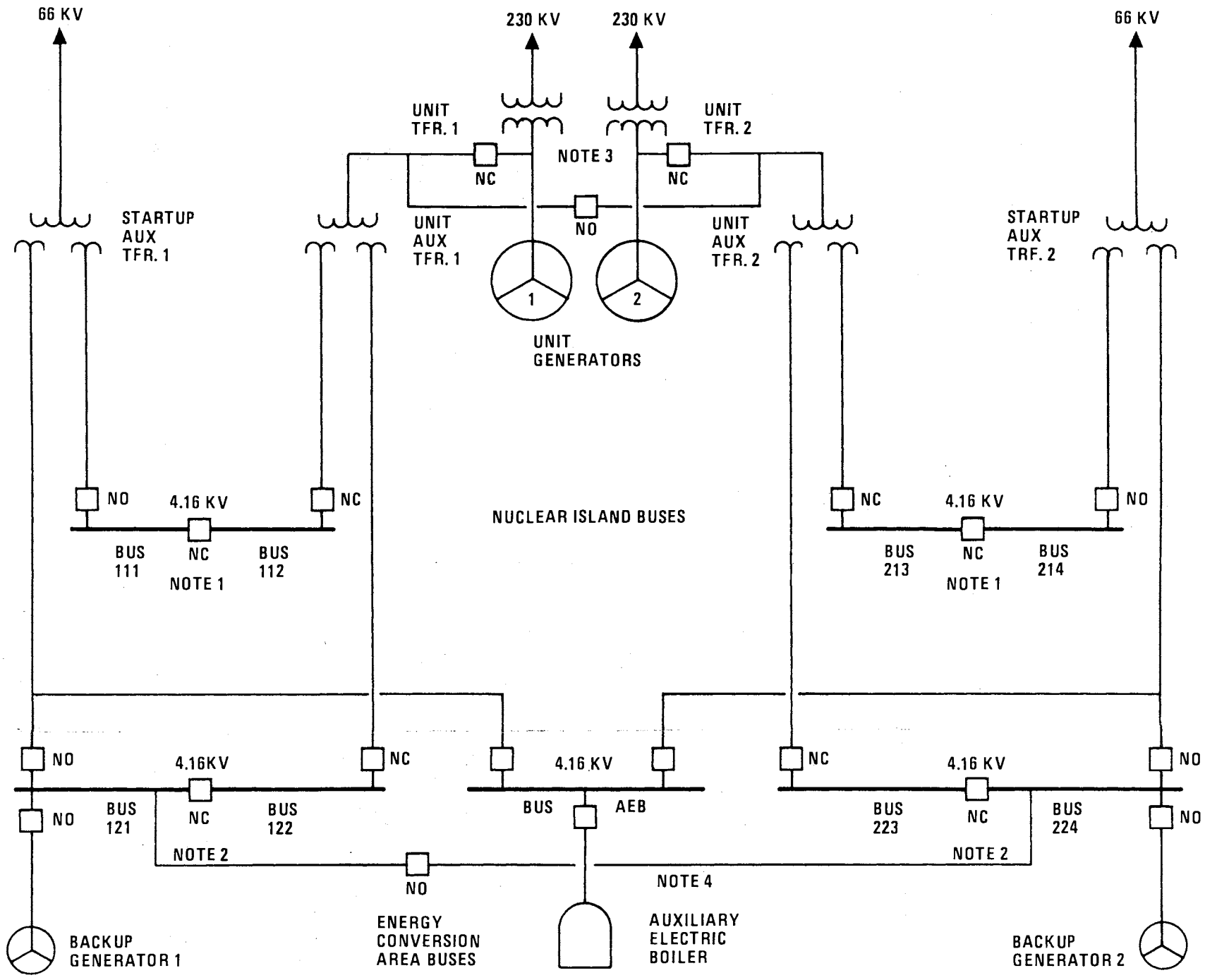
HT-001(28)

Fig. 4-27. Helium purification subsystem flow schematic



HT-001(29)

Fig. 4-28. Helium storage and transfer subsystem flow diagram

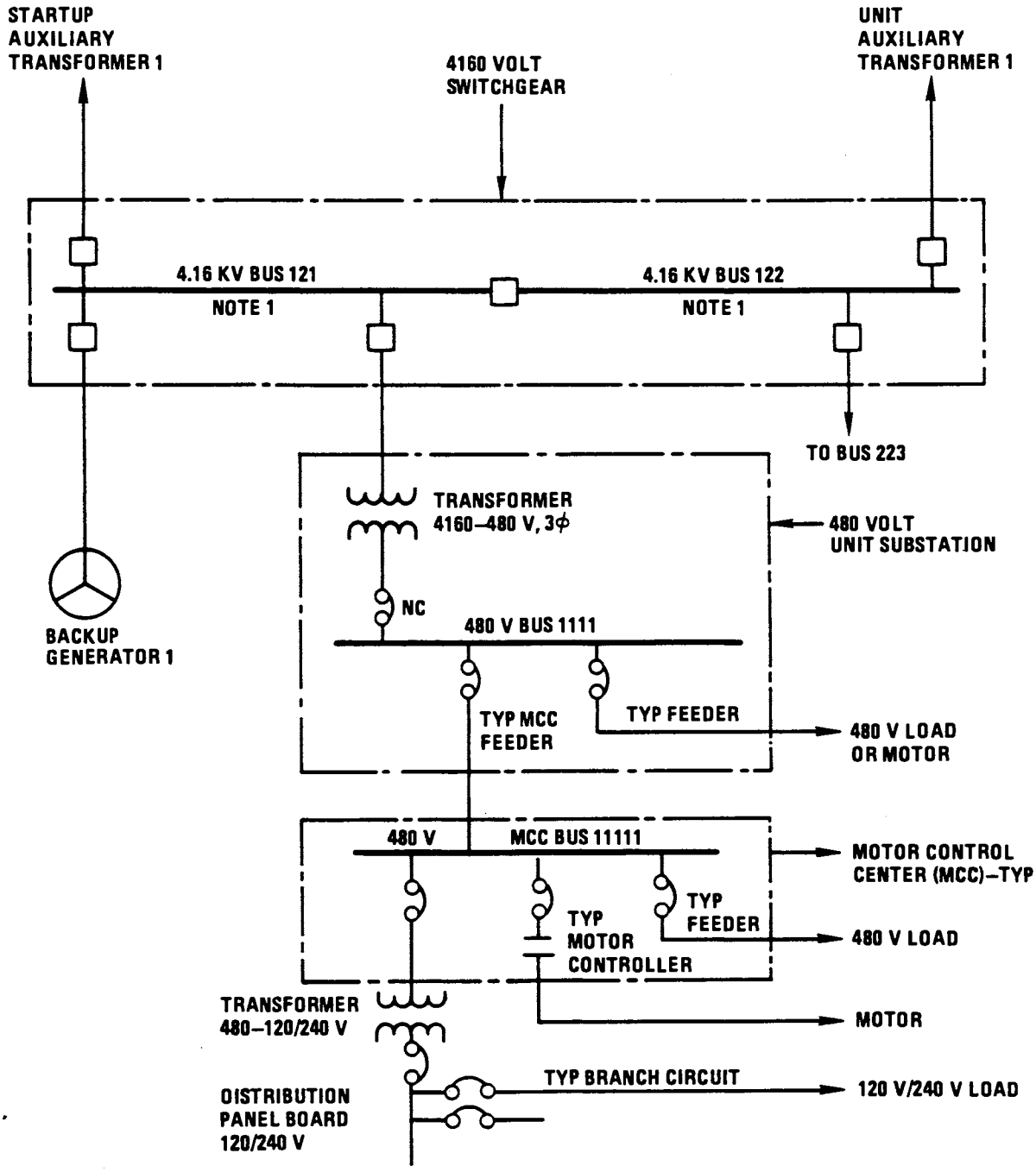


NOTES:

1. SWITCHGEAR BUSES 111/112 AND 213/214 ARE LOCATED IN THE NUCLEAR ISLAND (NI).
2. SWITCHGEAR BUSES 121/122 AND 223/224 ARE LOCATED IN THE TURBINE BUILDING.
3. TIE USED ONLY WHEN ALL OFFSITE POWER AND ONE UNIT GENERATOR IS LOST TO SUPPLY POWER TO BOTH GENERATOR AUXILIARIES FROM THE REMAINING UNIT GENERATOR.
4. TIE IS USED ONLY WHEN ONE BACKUP GENERATOR IS REQUIRED TO SUPPLY SELECTED INVESTMENT PROTECTION LOADS OF BOTH UNITS.

HT-001(30)

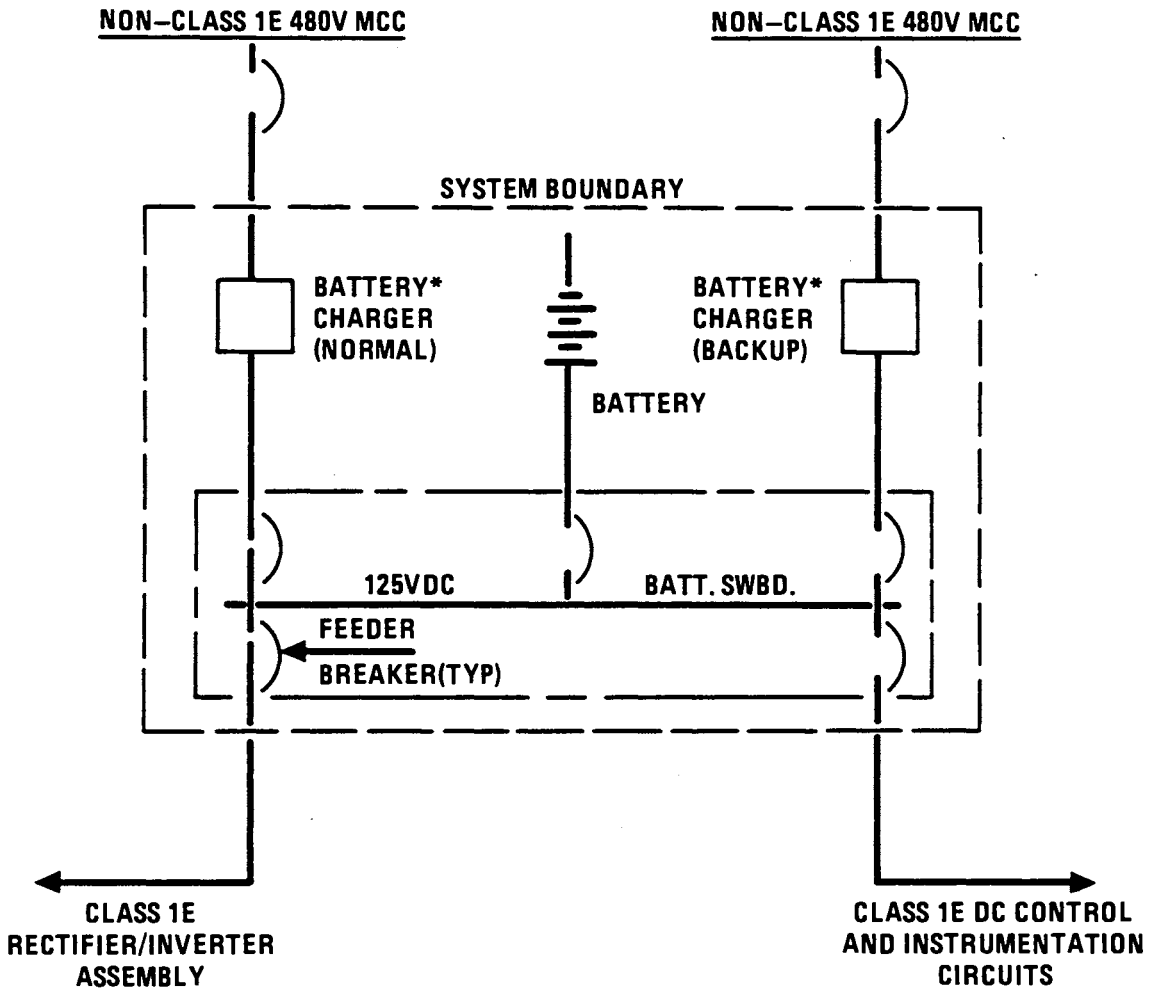
Fig. 4-29. Overall plant median voltage non-class 1E ac distribution subsystem



NOTE:
1. TYPICAL FOR UNIT GENERATOR 1
   AND SWGR. BUSES 121/122

HT–001(31)

Fig. 4-30. Non-class 1E ac distribution subsystem

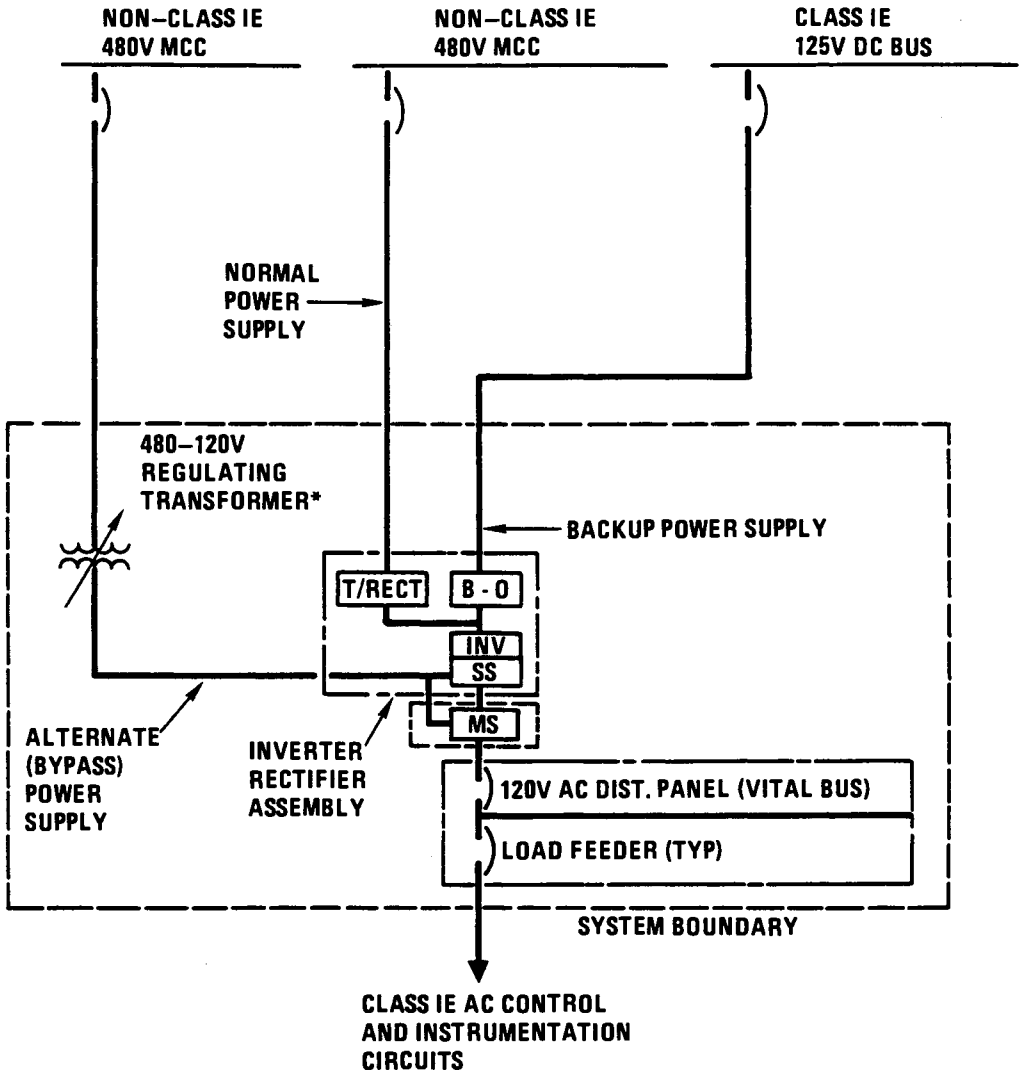


NOTE: SYSTEM SHOWN IS
TYPICAL FOR 4
CHANNELS

TYP – TYPICAL
– NON–CLASS 1E

HT–001(32)

Fig. 4-31. Class 1E dc power system



LEGEND

RECT – RECTIFIER
INV – INVERTER
B - O – BLOCKING DIODE
SS – STATIC TRANSFER SWITCH
T – TRANSFORMER
MCC – MOTOR CONTROL CENTER
TYP – TYPICAL
MS – MANUAL BYPASS SWITCH
* – NON–CLASS IE

NOTE: SYSTEM SHOWN TYPICAL FOR 4 CHANNELS

HT–001(33)

Fig. 4-32. Class 1E UPS system

5. IDENTIFICATION OF ACCIDENT INITIATORS

As identified in Section 3, the first step in the risk assessment process is the selection of the events which may initiate the accident sequences described in the event tree construction process. A major issue in performing the PRA, especially in this initial step, is completeness. Specifically, the issue of completeness is concerned with whether there are events, not included in the event trees, that can appreciably increase the predicted plant safety risk envelope. In practice, however, the risk assessment can never be complete in the sense of having analyzed all events which may involve the release of radioactivity; there are literally an infinite number of such events. Instead, the analyst must be selective in the identification of events, striving to identify a manageable number or grouping of events which are judged to envelope the potential plant risks. To aid in this process, a systematic method is required.

The systematic process for identifying accident initiators is shown in the block diagram of Fig. 5-1. As indicated in the first block, the first step was to identify the critical radionuclide functions that must be performed to control the plant radiation hazard. For this risk assessment, emphasis has been placed on functions important to controlling releases from the largest radiation source in the plant, namely the reactor core.

Having established the critical safety functions, Fig. 5-1 shows that two parallel paths of similar steps were followed. The left hand steps focus on the identification of potential mechanical, electrical, control, or operator initiating faults in the frontline systems and support systems that make up the plant. As shown on the right hand side of Fig. 5-1, explicit attention has also been given to potential faults in

structures which perform a safety function. While faults in passive structures may generally be considered to be less likely than faults in the generally active frontline safety systems, they must be considered for two reasons. First, as has been described in Section 4, the MHTGR has been designed to minimize reliance on active safety systems for accomplishing safety functions. Thus, it may be supposed that if the designer has done his job well, the consequences of active system faults may be small, hence the risks of such events may not be bounding compared to potential structural faults. Second, faults in the structures that form a radionuclide barrier may be especially risk critical if they simultaneously threaten the retention of radionuclides in the core while allowing release from secondary radionuclide barriers.

As shown in each of the parallel paths in Fig. 5-1, the second step was to identify the subset of all plant systems and structures which are critical to function accomplishment. The third step was to then identify the failure modes of these systems and structures which have potential safety consequences. In identifying failure modes and effects, it was necessary to consider the various plant operating states and their potential impact on accident likelihood or consequence.

With the critical failure modes established, the last step was to identify potential failure mode initiators and select those initiators which were believed to be most important to characterizing the safety risk envelope. For convenience, the last step was broken into two parts as shown in Fig. 5-1. First, initiators which are a direct cause of a critical failure mode were identified and second, initiators which might less directly lead to a critical failure mode were considered. The latter events logically cannot alter the failure modes and effects identified for the frontline systems and structures, but their risk impact could still be important for two reasons. First, the likelihood of event sequences occurring could be increased as a result of common dependency of the event tree branch points on a support system or common failure of structures due to an external event. Second, in a

multiple reactor plant such as the MHTGR, multiple reactors could be impacted at one time if support systems are shared or if an external event threatens all units. In such cases, the consequences of the event sequence could be increased in proportion to the number of units affected. The indirect initiator sources that were considered were faults in key support systems (e.g., electrical, component cooling, and control systems) and potential external plant events (e.g., earthquakes, tornados, floods, etc.).

It should be recognized that in performing the above steps, the analyst continually screens events on the basis of potential consequence, frequency, or combination of both. In a sense then, a scoping PRA is being performed during the event selection process. Since such scoping estimates are predicted upon prior experience, events may be identified for further study for one of two reasons: (1) prior experience indicates the event will bound the risk analysis; or (2) the risks associated with the event are not well known. In the latter case, the detailed analysis may simply disclose that an event sequence has negligible safety impact.

It should also be recognized that the MHTGR is presently in the conceptual design phase. Therefore, in establishing the representative initiators, it is sometimes necessary to use engineering judgment regarding final plant design details and the response of systems to transients. As the design evolves, the validity of these suppositions must be ascertained in order to assure PRA completeness.

In the following sections, the result of performing the steps diagramed in Fig. 5-1 is described. Section 5.1 identifies the critical safety functions for the MHTGR. Sections 5.2 and 5.3 identify the systems and structures, failure modes, and initiators established for each such function. Finally, Section 5.4 provides a summary of the selected accident initiators.

5.1. RADIONUCLIDE CONTROL FUNCTIONS

The functions required to be accomplished by the MHTGR to produce safe, economical electrical power have been elaborated extensively via a process known as Functional Analysis. One product of the Functional Analysis is a tree shaped logic diagram which describes the hierarchy of plant functions and associated subfunctions. Pertinent to the safety risk analysis described herein is the portion of the tree which elaborates the functions required to "Maintain Control of Radionuclide Release" shown in Fig. 5-2.

As the tree in Fig. 5-2 shows, there is a combination of two first level functions which may be performed to control radionuclide release. The first is to control the radiation release; the second is to control personnel access to the radiation source. This risk assessment focuses on potential risks to the offsite public which is controlled to be outside the plant's exclusion area boundary of 425 m (1394 ft). Although a failure to keep the public at this distance could increase the risks of assessed accidents, this has not been considered in the PRA. Conversely, no credit has been taken in the PRA for the decrease in risk which would occur from the evacuation of the offsite public to a distance greater than 425 m (1394 ft). The latter factor is believed to be the more probable, hence the lack of further development of this function is believed to be conservative.

The next level of the tree identifies the sources of radiation which must be controlled in the plant. Three principal sources are identified: (1) the reactor core itself, (2) radionuclides in process systems such as the steam, feedwater, and condensate system, and (3) radiation stored in gas, liquid or solid waste systems. Table 5-1 compares the activity stored in these various sites. It may be seen that, by far, the largest activity site is the reactor core itself. Additionally, the design of the MHTGR presents no unusual challenges to controlling the risks from these other sources of activity. Thus, the

TABLE 5-1
MAGNITUDE OF ACTIVITY SITES IN THE MHTGR

Activity Site	Approximate Magnitude (in curies)	
Reactor core	2×10^9	Design core equilibrium
Primary coolant system	3×10^3	Design circulating and plateout
Secondary coolant system	1	Tritium in secondary water
Helium purification system	5×10^3	Design purification
Gaseous waste	2×10^2	Regeneration of low-temperature absorber
Liquid waste	1×10^2	Decon drains from hot service facility
Solid waste	2×10^6	Spent fuel

risk assessment activity has focused on core activity releases and has not further developed the risks from other sources (assessments performed later in the development of the MHTGR design will be required to confirm that the risks from these other sources are acceptably low, however).

The fourth level in the tree identifies that control of radiation from the core involves the control of both direct radiation (i.e., containment of gamma or neutron energy release) and transport of fission products from the core. The offsite public is inherently protected from the former hazard by the subgrounding of the reactor and distance from the source. Any threat which could remove this inherent protection is considered extremely remote. The risk assessment, therefore, has only focused on events which affect the possibility of activity transport from the core (although any future consideration of risks to operations will have to consider direct radiation consequences).

The fifth level in Fig. 5-2 identifies four functions associated with the barriers to fission product release from the core: (1) control release from the core itself, (2) control the transport from primary circuit, (3) control transport from the reactor building, and (4) control transport from the site. Conventional reactor designs have placed considerable emphasis on all these functions, but especially the third function. Accordingly, the performance or nonperformance of the reactor building in conventional designs has a significant influence on assessed risks. As has been discussed in earlier sections, however, the safety philosophy of the MHTGR has been to place primary reliance on the achievement of the first function to minimize risks. Intentionally less reliance has been placed on other functions (barriers). Accordingly, the risk envelope of the MHTGR is projected to be less sensitive to failures of barriers beyond the core itself. This risk assessment has, therefore, focused on initiators which affect the ability to control radionuclides in the core itself.

The sixth and final level in Fig. 5-2 identifies the three functions which have been identified as critical to containing the activity in the MHTGR core, specifically within the fuel particle coatings. The first two are necessary to ensure the thermal limits of the particle coating are not exceeded. Heat generation must be controlled and adequate heat removal provided to prevent temperature conditions that could result in particle coating failure. Additionally, the particle coating must be protected against any chemical attack which could cause its failure. Subsequent sections focus on the potential threats of these three critical functions.

5.2. INITIATORS RESULTING FROM FAULTS IN PLANT SYSTEMS

5.2.1. Initiators Challenging Heat Generation Control

The principal means of controlling heat generation is the control of neutrons in the core as is performed by the NCSS. As described in Section 4.3, the NCSS consists of a system of control rods used for normal power control and independent RSCE. The various structures which support this function have been deferred for consideration to Section 5.3.

Table 5-2 identifies potential failure modes and associated effects of failure for the systems identified above. The left hand column in the table identifies failure modes considered and examples of failure causes. The next column identifies the plant condition under which the failure mode may be important. Four conditions or plant states are considered: (1) power operation, (2) change of state startup or shutdown operations, (3) shutdown, and (4) refueling. The condition listed first is that for which the failure mode is believed to have the greatest potential consequence. The third column identifies the potential effects or consequences of the failure. The final column shows the disposition of the failure mode in terms of further event tree analysis.

TABLE 5-2
CHALLENGES TO HEAT GENERATION CONTROL

Failure Mode	Condition	Failure Effect	Disposition
System: NCSS - Control Rods			
Undesired rod insertion Rod drop Spurious scram	Power	Power decrease resulting in overcooling if HTS not ramped down. No direct threat to core, but thermal shock to other primary system components must be considered.	Cover under anticipated transient requiring scram event tree
Undesired rod removal Rod bank withdrawal	Power Startup/shutdown	Power increase resulting in undercooling of core. Reactor trip normally terminates. If no trip, temperatures limited by negative temperature coefficient, but incremental fuel release possible. Possible system overpressure due to coolant temperature increase.	Construct rod withdrawal event tree
No rod movement when desired Trip failure Rods stuck	Power	Power generation can continue in excess of heat removal should HTS cooling decrease. Reactor normally tripped by insertion of RSCE. If no trip, temperatures limited by negative temperature coefficient, but incremental fuel release is possible. Possible system overpressure due to coolant temperature increase.	Construct anticipated transient requiring scram event tree (ATWS)
System: NCSS - Reserve Shutdown Control Equipment			
Undesired poison insertion Spurious trip	Power	Power decrease resulting in overcooling if HTS not ramped down. No direct threat to core, but thermal shock to other primary system components must be considered.	Cover under anticipated transient requiring scram event tree

TABLE 5-2 (Continued)

Failure Mode	Condition	Failure Effect	Disposition
Undesired rod removal Poison withdrawal	Startup/shutdown	None expected. RSCE removed prior to control rods during startup. Thus, even with complete removal of RSCE, core maintained subcritical by control rods. At power, RSCE fully withdrawn. Thus, no reactivity effect from withdrawal.	N/A
No poison movement when desired Trip failure Poison held up in hoppers	Power	Power generation can continue in excess of heat removal should HTS cooling decrease. If no trip, temperatures limited by negative temperature coefficient, but incremental fuel release possible due to increased temperatures. Possible system overpressure due to coolant temperature increase.	Cover under ATWS event tree and in other trees where reactor shutdown is required.

In general, it has been found that with regard to plant condition, the full power operating mode is limiting for the MHTGR. This is because the reliability of cooling systems is not significantly impacted by plant operating states. In the MHTGR, the same cooling systems may be employed whether the plant is pressurized or depressurized, for example. Furthermore, since the safety philosophy of the MHTGR has been to control radionuclides primarily within the fuel particle coatings, operating mode changes to secondary boundaries have less impact. Thus, the risk limiting condition has been found to be when the reactor is at power and core fuel and component temperatures are highest.

Two consequence types may be discerned in Table 5-2. A failure may lead to a state in which the heat removal exceeds the heat generated and the fuel is overcooled. Such events are not a threat to the integrity of the ceramic and graphite materials used in the MHTGR; the plant has to be designed to withstand a number of reactor trip events over its lifetime, which represent relatively severe overcooling events. Additionally, cooldown rates are strictly limited by the large thermal inertia of the graphite core. Overcooling events, however, may be of concern to other primary circuit metallic components and, therefore, must be considered in assessing the likelihood of primary circuit structural faults as discussed in Section 5.3.

Alternatively, a condition arises wherein the heat generated by the core exceeds the heat removal. This can be from one of two causes: (1) heat generation is not decreased when required by a decrease in heat removal; or (2) an undesired increase in heat generation occurs which exceeds the heat removal capability. Either has the potential to result in localized overheating of fuel particles and potential releases which require further consideration.

As shown in Table 5-2, events resulting in a decrease in heat removal without a consequential decrease in power generation might be initiated by an event which leads to a heat removal reduction followed

by failure to reduce power or trip the reactor. Events which may lead to heat removal decrease are generally considered in the next section. Failure to trip the reactor results if neither appropriate automatic nor manual action is taken. An automatic trip failure might be caused by instrumentation failure, control logic failure, or a mechanical failure which prevents the insertion of an adequate quantity of control material. Similarly, manual failure to trip could result from instrumentation failures, mechanical failures or operator failure. In assessing the likelihood of a successful manual trip, consideration must be given to the nature of the initiating transient. For example, the probability of the operator failing to trip manually during a rapidly occurring event may be high; while in slowly developing transients, the probability of operator error is lower.

The above events may generally be classified under the heading of Anticipated Transients Without Scram (ATWS) events. The severity of such events in the MHTGR is generally limited by a strong negative temperature coefficient which inherently serves to reduce heat generation. This negative temperature coefficient, however, does not reduce power levels to normal decay heat levels and thus core and coolant temperatures above those encountered in decay heat removal scenarios will be encountered in the core. Thus, these events require further consideration in this assessment.

Failure modes are also identified in Table 5-2 which might lead to undesired increases in heat generation (i.e., reactivity insertion events) that also require further consideration. Of these, the event which results in the largest reactivity insertion into the core is the control rod bank withdrawal event, the consequences of which would be generally worse under normal operating conditions. Based upon current control schemes for the MHTGR, a control rod group withdrawal would result in the removal of three outer control rod pairs with a combined reactivity worth well in excess of one dollar. Again, the severity of

such a withdrawal is inherently limited by the strong negative temperature coefficient. However, core power level would exceed 100% causing core and coolant temperatures to exceed those encountered in typical decay heat removal scenarios. Therefore, further consideration of these events is required in this assessment.

5.2.2. Initiators Challenging Heat Removal

The principal means of heat removal in the MHTGR is by the Heat Transport System (HTS). As described in Section 4.6, the HTS consists of a single loop subsystem of a motor-driven helium circulator, a steam generator and associated feedwater and condensate system. The HTS removes heat from the core in normal operation as well as under shutdown conditions. An independent backup SCS, as described in Section 4.7, is also provided in the design to remove core heat when the HTS is unavailable for maintenance or other reasons. The SCS consists of a single loop system with a motor driven helium circulator, a shutdown heat exchanger and associated pressurized water cooling system. The SCS is designed only for decay heat removal operation. A third system, the RCCS, is also provided for heat removal. Even should the RCCS fail, the function of heat removal from the core can still be maintained as heat is transported to the surrounding environment. While operation of the RCCS does reduce core temperatures somewhat in the event of the loss of all other cooling systems, its main function is to limit vessel temperature, thus ensuring vessel integrity. Additionally, the RCCS is totally passive with only structural components. Therefore, consideration of RCCS failure modes is reserved for Section 5.3 which deals with structural faults.

Table 5-3 identifies potential failure modes and associated effects of failure for the systems identified above. Two general consequence types may be discerned. A failure may lead to a state in which the heat

TABLE 5-3
CHALLENGES TO HEAT REMOVAL CONTROL

Failure Mode	Condition	Failure Effect	Disposition
System: Heat Transport System			
Undesired cooling increase or no cooling decrease when required Control faults Operator error	Power Startup/shutdown Shutdown Refueling	Core overcooling. No direct threat to core, but thermal shock to other primary system components must be considered.	Cover under steam generator leaks
Undesired cooling decrease Control faults Operator error Mechanical failures	Power Startup/shutdown Shutdown Refueling	Core undercooling. If no trip, temperatures limited by negative temperature coefficient, but incremental fuel release possible. If trip but SCS cooling not provided, core undergoes conduction cooldown with decay heat conducted to RCCS and some incremental fuel release.	Cover no trip cases in ATWS tree Construct loss of HTS tree for decay heat removal losses
System: Shutdown Cooling System			
Undesired cooling increase or no cooling decrease when required Control faults Operator error	Shutdown Refueling	Core overcooling. No direct threat to core, but thermal shock to other primary system components must be considered.	Cover under steam generator leaks

TABLE 5-3 (Continued)

Failure Mode	Condition	Failure Effect	Disposition
Undesired cooling decrease Control faults Operator error Mechanical failures	Shutdown Refueling	Core undercooling. Core undergoes conduction cooldown with decay heat being conducted to RCCS and some incremental fuel release.	Cover in loss of HTS tree

removal exceeds the heat generated and the fuel is overcooled. As discussed in the prior section, such events are not a threat to the integrity of the ceramic and graphite materials used in the MHTGR and are not given any further consideration in this assessment.

The second failure consequence involves undercooling of the core fuel. As shown in Table 5-3, this could result from a number of potential causes. However, the most limiting in terms of consequences is a loss of the HTS from power operation. This general class of accident is therefore identified for further study.

5.2.3. Initiators Challenging Control of Chemical Attack

The principal means of controlling chemical attack in the MHTGR is accomplished by maintaining the core fuel in its environment of chemically inert helium. The major systems which accomplish this, as described in Sections 4.2 and 4.2.1, are the Helium Purification Subsystem and the Helium Storage and Transfer Subsystem. The various structures which support this function are deferred for consideration in Section 5.3.

Table 5-4 identifies potential failure modes and associated effects of failure for the systems identified above. No significant consequence is determined for any such fault. Therefore, no initiators resulting from faults in plant systems have been identified which significantly challenge this function. However, as will be seen in the next section, a number of structural faults need to be considered which pose a significant challenge to the function of controlling chemical attack.

5.2.4. Support System Initiators

The prior sections have considered failure modes in the frontline plant systems which control the functions critical to retaining radionuclides in the core fuel. These are the systems which directly perform

TABLE 5-4
CHALLENGES TO CONTROL CHEMICAL ATTACK

Failure Mode	Condition	Failure Effect	Disposition
System: Helium Purification System			
Helium not purified Control faults Mechanical faults Operator errors	Power Startup/shutdown Shutdown Refueling	Buildup of oxidants in coolant system. Limited oxidation or hydrolysis of fuel, graphite, or metallics. Rate dependent on contaminant ingress from other sources and core temperatures.	Insignificant risks - event tree not required. [Cover more serious events under primary coolant leak (air ingress) and steam generator leak (water ingress) trees.]
System: Helium Storage and Transfer			
Introduction of Contaminated helium Control faults Mechanical faults Operator errors	Power Startup/shutdown Shutdown Refueling	Buildup of oxidants in coolant system. Limited oxidation or hydrolysis of fuel, graphite, or metallics. Rate dependent on contaminant ingress and core temperatures.	Insignificant risks - event tree not required. [Cover more serious events under primary coolant leak (air ingress) and steam generator leak (water ingress) trees.]

such functions. This section considers faults in systems which support these frontline systems. Faults in these support systems cannot impact the consequences of the failures considered previously; but they may impact the frequency of occurrence of a given consequence, and hence, impact the plant risk. Of particular interest are any support systems which commonly support many frontline systems such that the failure of the support system could result in the common cause failure of multiple frontline systems and challenge one or more of the critical safety functions.

Table 4-3 shows the dependency of frontline systems on the MHTGR support systems. Systems listed across the top are the so-called support systems. The vertical listing identifies the frontline systems as well as any dependencies between support systems.

A study of Table 4-3 indicates that three support systems, in particular, support many, if not the majority, of the frontline systems. These support systems are PPIS, electrical power (non-1E ac, 1E dc, and 1E UPS) and the plant service water system. Hence, further consideration of faults in these systems is logically dictated.

In general, the PPIS is designed to fail in a safe mode such that if power is lost to the system or open circuits occur the plant is protected. Thus, the failure mode of more interest is spurious or misoperations of the PPIS. Unfortunately, at the conceptual stage of the MHTGR design, the PPIS is not developed enough to adequately determine the possibility of such failure modes. Thus, although the PPIS is a good candidate for further assessment, its consideration has been deferred to later studies.

The frontline systems which depend on service water may be seen to be those involved in the heat removal function. Thus, it is sufficient to consider the loss of service water as a potential initiator in the

loss of HTS event tree as opposed to creating a separate event tree (see Appendix C, Section C.2 Loss of Main Loop Cooling).

Table 4-3 shows that virtually all the frontline systems rely on electrical power. Other risk assessments have similarly shown plant risk sensitivities to faults in electrical power supplies. Further, Table 4-3 shows that within the electrical system there is a common dependency on the non-Class 1E system as the normal power system. For this reason, a logical initiator to consider further is an event which causes the normal electrical supply to be lost, namely a loss of offsite power event.

5.3. INITIATORS RESULTING FROM FAULTS IN PLANT STRUCTURES

5.3.1. Internal Initiators

The structures which perform a critical safety function are those which either support the frontline systems identified in the previous section or which perform a function as a radionuclide barrier. Three general groups of such structures may be considered: (1) the reactor core and its associated structural supports, (2) the primary coolant boundary components, and (3) the reactor building.

Table 5-5 identifies the failure modes of these structures which should be considered for their impact on plant risks. In general, the structural failure modes of concern are leaks (i.e., the radionuclide barrier capability is compromised) or structural failures (i.e., other functions may be compromised).

Faults in the fuel particle coatings which allow the leakage of fission products into the primary coolant stream must be considered in the design of the MHTGR. The principal consequence of such faults is a pre-existing radionuclide source within the primary coolant system in

TABLE 5-5
CHALLENGES TO CRITICAL STRUCTURES

Failure Mode	Condition	Failure Effect	Disposition
Structure: Reactor Core and Supports			
Leaks in fuel particle coatings Manufacturing defects Faults during operation	Power Startup/shutdown Shutdown Refueling	Release of fission products to primary system resulting in circulating and plateout activity sources.	Consider circulating/ plateout activity in all event trees
Core structural fault Core support failure Core barrel failure Graphite block breakage	Power	Prevention of control rod and/or RSCE insertion. Reduction in cooling flow to core fuel. Reactivity change due to core configuration change.	Cover under earthquake tree
Structure: Primary Coolant Boundary Components			
Helium leaks Pressure relief open Instrument line leaks Helium purification leaks	Power Startup/shutdown Shutdown	Depressurization of primary system through opening. Release of activity stored in the primary coolant system. Reduction in forced cooling effectiveness due to density decrease challenging heat removal function. Some air ingress challenging control of chemical attack.	Construct primary coolant leak event tree

TABLE 5-5 (Continued)

Failure Mode	Condition	Failure Effect	Disposition
Water leaks System generator tube leak SCS heat exchanger leak Circulator auxiliaries leak	Power Startup/shutdown Shutdown Refueling	Depends on system and plant condition. Worst case is failure of steam generator tube at power resulting in water/steam ingress into primary system. Water in coolant improves core moderation challenging the control of heat generation. Mass increase raises primary pressure leading to opening of primary reliefs. Moisture may cause hydrolysis of failed fuel and oxidation of core graphite threatening the control of chemical attack and generation of flammable gases.	Construct steam generator leak event tree
Vessel structural faults or breaks Reactor vessel S/G vessel SCS closure Circulator closure Crossduct Support failure	Power Startup/shutdown Shutdown Refueling	Depressurization through a range of activity in the primary coolant system. Reduction in forced cooling effectiveness due to density decrease challenging heat removal function. Air ingress challenging control of chemical attack. If leak is larger than design basis, pressure forces may threaten other critical structures and components (i.e., reactor building, RCCS, control rods, circulators).	Cover in primary coolant leak tree Cover other structural faults in earthquake tree
<u>Structure: Primary Coolant Boundary Components</u>			
Reactivity control system structural fault	Power Startup/shutdown	Similar to above. However, possibility of pressure forces ejecting control rod pair contained by housing challenging control of heat generation.	Cover loss of coolant effects in primary coolant leak tree

TABLE 5-5 (Continued)

Failure Mode	Condition	Failure Effect	Disposition
NSSS closure failure causing rod ejection			Cover reactivity effects in rod withdrawal tree
Heat exchanger structural faults Steam generator tube sheet failure SCS heat exchanger tube sheet failure	Power Startup/shutdown Shutdown Refueling	Similar to water leaks described above, except greater ingress rate. If ingress rate exceeds design capacity of pressure reliefs, vessel integrity threatened.	Consider in steam generator leak event tree
Structure: Reactor Building			
Leaks Overpressure louvers fail to close Closure failures	Power Startup/shutdown Shutdown Refueling	Reduction in effectiveness of reactor building as a radionuclide barrier.	Consider building leak failure in all event trees
Loss of structural integrity Missiles Pressure loads Seismic loads	Power Startup/shutdown Shutdown Refueling	Failure of reactor building as radionuclide barrier. Threat to heat removal function performed by the RCCS in its structural integrity affected. No impact if other cooling systems continue to operate. Moderate impact on core temperatures if no other cooling systems operate, excessive vessel temperatures possible.	Cover internal threats (e.g., building overpressure) under primary coolant leak tree Cover external threat in earthquake tree

terms of activity circulating within the coolant or plated out on internal surfaces. The release of this activity must be considered in any event sequence which involves a release of primary coolant.

A structural fault in the core or its associated support structures may be of concern because it can affect the functions of heat generation control and heat removal control. The challenge to the former function is likely more serious in the MHTGR. This is because the core has been designed such that only the heat transfer mechanisms of radiation and conduction are required to remove decay heat. Thus, even if a core geometry is altered such that coolant flow is impaired, consequences are minimal. In any case, the loss of forced convection cooling through the core is more likely to occur from cooling system failures than from core structural faults.

Geometry changes that might impact reactivity control systems are those of greater concern, particularly if a geometry change are significant enough to affect the insertion of both control rods and the reserve shutdown poison. Because of the diversity of these two systems, either of which is capable of making the core subcritical, no internal mechanism has been identified with a likelihood high enough to be worthy of further consideration. However, as identified in Table 5-5, such structural faults do need to be considered from external initiators, particularly earthquakes.

As shown in Table 5-5, a structural fault in the primary coolant boundary components can present a potential threat to all three of the functions necessary to control radionuclides within the core fuel. In addition, such faults are of concern because they simultaneously cause a loss of the primary coolant system as a radionuclide barrier. Thus, considerable further analysis is warranted for these events. As shown in the table, two events in particular were selected for further analysis: a leak in the primary coolant boundary and a water ingress event caused by a failure in the steam generator.

With one exception, the selection of these two events is believed to adequately cover the range of failure modes possible to the primary coolant boundary. The exception, a fault in the NCSS vessel closure which might lead to rod ejection and a rapid reactivity insertion, is believed to be covered by the rod withdrawal event identified previously. This is justified, on the one hand, by the consideration that, based upon past reactor experience, the likelihood of a structural fault (i.e., a failure of a Class 1 pressure vessel component) leading to a rod ejection is orders of magnitude less than a control or operator fault leading to a control rod withdrawal. On the other hand, the consequences of the rod ejection have been assessed to be only slightly greater than the rod withdrawal event. This may be attributed to a number of factors. First, the worth of a control group is greater than that of the rod pair which might be ejected. Second, the rod ejection is be limited by structures located above the rod enclosures. And finally, studies have shown the low power density fuel in the MHTGR experiences only a few hundred degree temperature rise before the negative temperature coefficient terminates the event even for step reactivity insertions as large as the control rod pair which might be considered here (see Section 6.1.6). Thus, with the probability of the event being orders of magnitude lower and the potential consequences in terms of fuel behavior only slightly higher, the risks of the ejection accident are believed to be relatively insignificant.

Structural faults in the reactor building could minimize its effectivenss as a radionuclide barrier. This fault, however, if not coupled with another event which results in failures of the other radionuclide barriers (i.e., the core and the primary coolant boundary) would have virtually no consequence. A fault in the building could also impact the effectiveness of the RCCS since it is supported off the building. Again, this fault, by itself, would have little consequences unless the other cooling systems failed (i.e., the HTS and SCS). The failure of the building combined with these other failures is believed to be

extremely unlikely unless coupled by some event, such as a large earthquake. For this reason, reactor building failure was selected for consideration under the earthquake event tree identified in the following section.

5.3.2. External Initiators

The safety characterizations in the prior sections have been for potential internal hazards in which the events are initiated by malfunctions in plant systems or structures. External events are initiated by forces outside the plant and are generally unrelated to the plant design. In order to complete the safety characterization, it is necessary to reexamine the previously identified internal failure modes and determine whether there are potential external events (e.g., tornadoes, external flooding, earthquakes) that can cause widely separated and normally independent plant systems to fail concurrently thus increasing the likelihood of significant event consequences.

The candidate external events which have been considered for further evaluation in this risk assessment are identified in Table 5-6 (from Ref. 5-1). Due to site specificity of external hazards and limitations in the availability of previous external event hazard assessments that are readily applicable to the MHTGR, the total safety risk impact from these events cannot be characterized without additional analysis exceeding the scope of this study. Other risk assessments, however, have shown that for a well designed plant (i.e., one whose risk are relatively low from internal faults), earthquakes may dominate the high consequence/low frequency end of the risk spectrum. Further, external events such as floods and fires generally only threaten the active safety systems, while large earthquakes pose a threat to key structures as well. Since the MHTGR has been designed to inherently minimize the consequence of active system faults, the structural threat from earthquakes to passive structures may be similarly limiting. For

TABLE 5-6
EXTERNAL INITIATING EVENTS

Event	Remarks
Aircraft impact	Site specific; requires detailed study.
Avalanche	Can be excluded for most sites in the United States
Coastal erosion	Including in the effects of external flooding.
Drought	Excluded because ultimate heat sink is not affected by drought (e.g., air cooling).
External flooding	Site specific; requires detailed study.
Extreme winds and tornadoes	Site specific; requires detailed study.
Fire	Plant specific; requires detailed study.
Fog	Could increase the frequency of man-made hazard involving surface vehicles or aircraft; accident data include the effects of fog.
Forest fire	Fire cannot propagate to the site because the site is cleared; plant design and fire-protection provisions are adequate to mitigate the effects.
Frost	Snow and ice govern.
Hail	Other missiles govern.
High tide, high leak level, or high river stage	Included under external flooding.
High summer temperature	Ultimate heat sink is designed to operate with air.
Hurricane	Included under external flooding; wind forces are covered under extreme winds and tornadoes.
Ice cover	Ice blockage of river included in flood. Potential loss of airflow passage is considered in plant design.
Industrial or military facility accident	Site specific; requires detailed study.
Internal flooding	Plant specific; requires detailed study.
Landslide	Can be excluded for most sites in the United States.
Lightning	Considered in plant design.

TABLE 5-6 (Continued)

Event	Remarks
Low lake or river water level	Ultimate heat sink is designed for operation with air.
Low winter temperature	Thermal stresses and embrittlement are insignificant or covered by design codes and standards for plant design.
Meteorite	All sites have approximately the same frequency of occurrence.
Pipeline accident (gas, etc.)	Site specific; requires detailed study.
Intense precipitation	Included under external and internal flooding.
Release of chemicals in onsite storage	Plant specific; requires detailed study.
River diversion	Not applicable for air-cooling.
Sandstorm	Included under tornadoes and winds; potential blockage of air intakes with particulate matter is considered in plant design.
Seiche	Included under external flooding.
Seismic activity	Site specific; requires detailed study.
Snow	Plant designed for higher loading; snow melt causing river fooding is included under external flooding.
Soil shrink-swell consolidation	Site-suitability evaluation and site develment for the plant are designed to preclude the effects of this hazard.
Storm surge	Included under external flooding.
Transportation accidents	Site specific; requires detailed study.
Tsunami	Included under external flooding and seismic events.
Toxic gas	Site specific; requires detailed study.
Turbine-generated missile	Plant specific; requires detailed study.
Volcanic activity	Can be excluded for most sites in the United States.
Waves	Included under external flooding.

this reason, only earthquakes were selected for further evaluation in this study.

5.4. SUMMARY OF EVENTS RECOMMENDED FOR FURTHER STUDY

Table 5-7 lists the events selected for evaluation by event tree analysis in subsequent sections. The table is arranged in terms of event initiator source (frontline system fault, support system fault, structure fault, or external event), safety function threatened (control core heat generation, heat removal, or control chemical attack), and radionuclide barrier threatened (core, primary coolant boundary, or reactor building).

As indicated by the table, the range of initiators selected pose challenges to the full range of safety functions and radionuclide barriers. Initiators involving anticipated transients without scram and inadvertent control rod withdrawal have significance because they jeopardize the ability to control heat generation. Loss of HTS cooling is included because of the challenge to core heat removal. All three of these events have the potential for initiating sequences which could lead to incremental fission product release from the fuel. Loss of offsite power is selected as a representative support system fault because of its potential to initiate a loss of electrical power supplies which commonly impacts the systems providing heat generation and removal control.

Accidents initiated by primary coolant leaks are addressed because they involve primary coolant boundary failure which subsequent release of circulating activity and a fraction of plateout activity. Further, the loss of pressure affects the functions of heat removal and may challenge fuel particle coating integrity owing to chemical attack by any introduction of air. Steam generator leaks into the primary coolant system are considered in addition because of the potential for chemical

TABLE 5-7
SUMMARY OF ACCIDENT INITIATORS SELECTED FOR FURTHER ANALYSIS

Initiating Event	Function Challenged			Barriers Challenged		
	Heat Generation	Heat Removal	Chemical Attack	Fuel Particle	Primary Coolant	Reactor Building
Critical System Faults						
Anticipated transient without scram	X			X		
Control rod group withdrawal	X			X		
Loss of heat transport system		X		X		
Support System Faults						
Loss of offsite power	X	X		X		
Critical Structure Faults						
Primary coolant system leaks		X	X	X	X	X
Steam generator leaks	X		X	X	X	
External Faults						
Earthquakes	X	X	X	X	X	X

attack of the fuel by hydrolysis as well as having a positive reactivity effect which challenges control of heat generation.

Finally, earthquakes merit attention because they can cause normally independent plant systems or, potentially more important to the MHTGR, passive plant structures to fail concurrently. Thus, their ability to initiate common mode failures presents a potential challenge to all functions as well as all physical radionuclide barriers.

5.5. REFERENCE

5-1. "PRA Procedures Guide," NUREG/CR-2300, Vol. 1, January 1983.

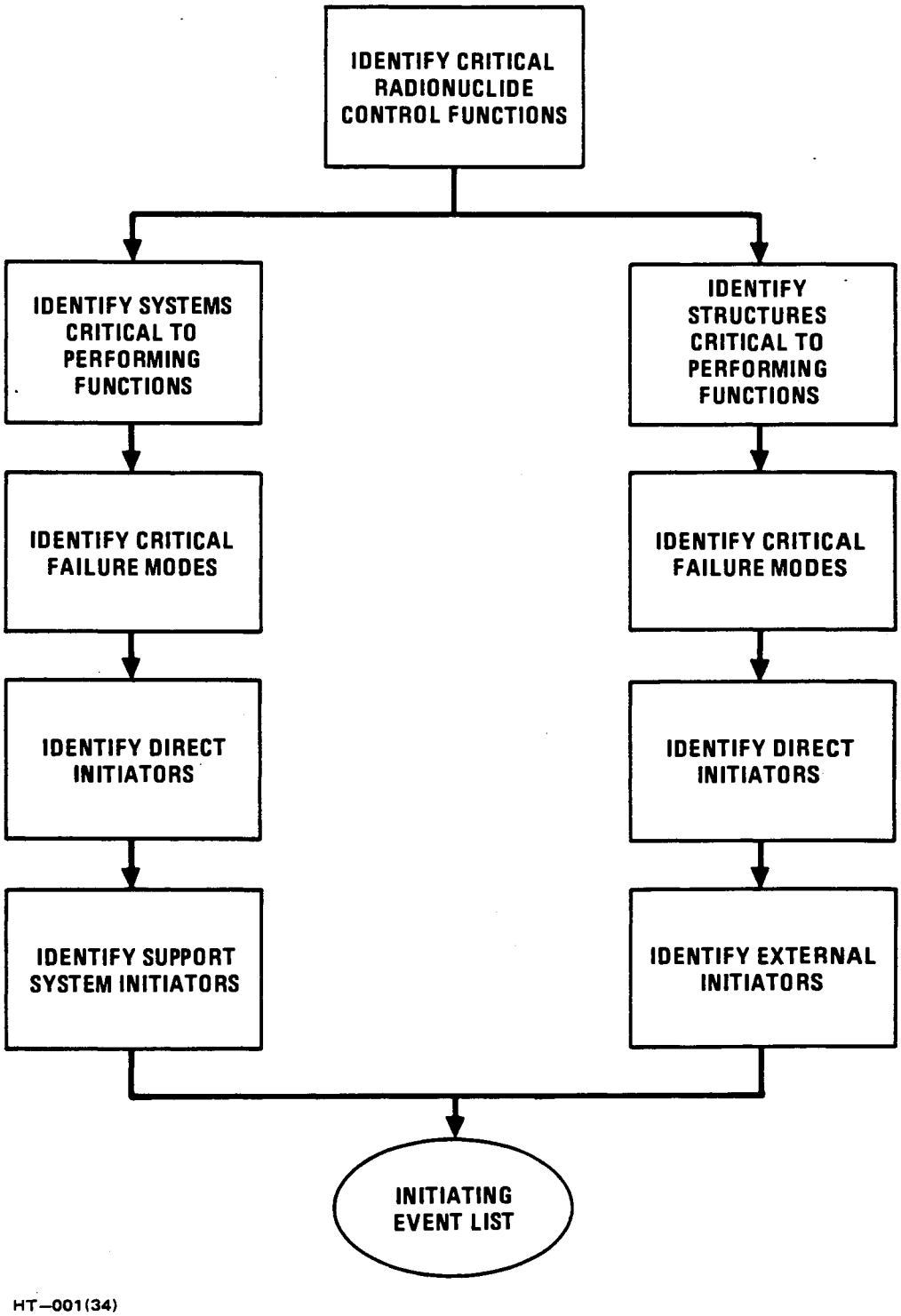


Fig. 5-1. Approach to identifying accident initiators

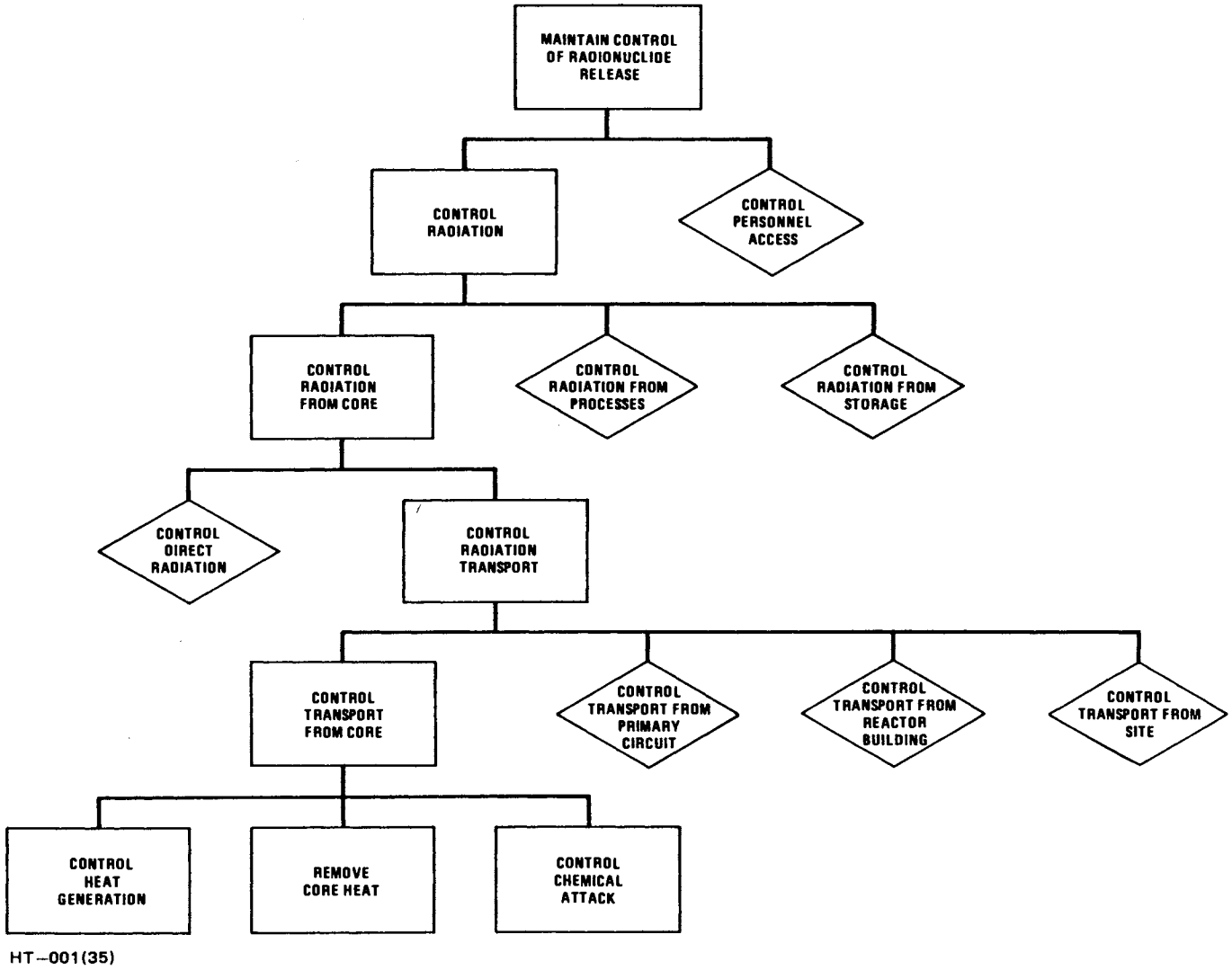


Fig. 5-2. Identification of risk critical safety functions

6. PLANT RESPONSE AND SYSTEM RELIABILITY MODELS

In the risk assessment, initiating events are first identified that have the potential to lead to uncontrolled or unscheduled radiological release. An evaluation is then performed to determine the plant response to these initiating events so as to identify the many possible resulting accident scenarios and single out plant systems whose function can influence the transient.

In the first part of this section, the plant response to the seven initiation events is described. This includes discussion of the thermal-hydraulic neutronic and chemical transients that might result from the various initiating events. These transients are often dependent upon the success or failure of plant features to operate. In such cases the multiple possibilities are discussed.

The second part of this section describes the reliability models used to evaluate the failure probability for the key systems whose operation or failure can influence the course of the transient. Brief descriptions of these major systems are found in Section 4. In this section, support systems are also described which are required in order for the top-level systems to perform their necessary functions of controlling heat generation, chemical attack, and removing core heat. Together, the top-level systems assure that the function of maintaining control of radionuclide release is performed.

The plant response and system reliability models described in this section are used to logically construct and quantify event trees for each of the initiating events. Section 7 discusses the frequency portion of this assessment, and Section 8 discusses the manner in which

appropriate consequences are were calculated for event sequences of interest.

6.1. PLANT RESPONSE

Section 6.1 discusses plant response during various transients. Section 5 identifies important initiating events which may lead to radiological release. For each of the accident initiators identified in Section 5, this section provides a brief description of how the initiator might occur, followed by descriptions of the manner in which the plant is expected to respond including transients in which various features of the plant fail to perform as designed.

For each transient described in this section, the response of the plant protection and instrumentation system (PPIS) to the transient under consideration is provided. The PPIS receives the actuation signals from its sensors and responds accordingly. The PPIS initiates reactor trip, heat transport system (HTS) shutdown, shutdown cooling system (SCS) initiation, steam generator isolation and dump, and primary coolant pumpdown as necessary. Because it is an integral part of virtually all transients considered, the PPIS trip parameters, trip setpoints, and actuated equipment are given in Table 6-1 for easy reference. Note that for some of the PPIS actions, several input parameters may initiate the same function, thus providing a logical backup for faulty sensors or other equipment failures that may result in a failure to transmit a trip signal to the PPIS when conditions warrant.

6.1.1. Primary Coolant Leaks

Failure of the primary coolant pressure boundary to retain the helium inventory may result from a variety of causes. Included as possible failure locations are instrument lines, neutron control system guide tubes, valves, vessel penetrations, flanged or bolted closures, and welds. Response of the plant varies depending upon the size of the

TABLE 6-1
PPIS TRIP PARAMETERS AND SETPOINTS

PPIS Action	Trip Parameter	Nominal Setpoint
Reactor trip with the outer control rods	Neutron flux to helium mass flow ratio high	>1.4
	Primary coolant pressure low	<5757 kPa (<835 psia)
	Primary coolant pressure high	<6929 kPa (>1005 psia)
	Primary coolant moisture high	>1000 ppmv
	HTS shutdown	N/A[a]
	SG inlet helium temperature high	>746°C (>1375°F)
Reactor trip with the reserve shutdown control equipment	Neutron flux to HTS circulator speed ratio high and time delay ≤50 s. (Inhibited at low HTS circulator speed and low neutron flux)	>1.8 30 s time delay inhibit at ≤5% circulater speed ≤10% neutron flux
	Primary coolant helium pressure high	6998 kPa (>1015 psia)
Heat transport system shutdown	HTS circulator speed to feedwater flow ratio high	≥1.20
	HTS circulator speed to feedwater flow ratio low	≤0.80
	Primary coolant pressure low and main steam temperature not low	≤4412 kPa (≤640 psia) ≥393°C (≥739°F)
	Primary coolant helium pressure high	>6929 kPa (>1005 psia)
	Steam generator isolation and dump signal	N/A
Steam generator isolation	Primary coolant pressure high	>6929 kPa (>1005 psia)
Steam generator isolation and dump	Primary coolant moisture concentration high	>1000 ppmv
Steam generator dump terminate	Main steam pressure and primary coolant pressure difference low	<517 kPa (<75 psia)
Primary coolant pumpdown with helium purification system	Primary coolant pressure low and reactor building radiation high	<5515 kPa (<800 psia) TBD
Shutdown cooling system start	HTS shutdown	N/A

[a]N/A - not applicable.

leak area and the consequent depressurization rate of helium from the reactor vessel.

6.1.1.1. Planned Plant Response. The expected plant response to a primary coolant leak begins with reactor trip with the control rods. This trip is initiated by the PPIS when reactor vessel pressure is reduced to 5688 kPa (825 psia). The helium purification system (HPS) pumpdown function is started on a signal from the PPIS when a primary coolant pressure of 5515 kPa (800 psia) is reached and high reactor building radiation levels are detected. This action is ineffective when the leak size is large enough, since the pumpdown rate is negligible compared to the depressurization rate of the reactor vessel through the breach in the pressure boundary (Fig. 6-1). Core cooling continues on the HTS for leak sizes smaller than 0.65 cm^2 (0.1 $in.^2$). For larger leak sizes, HTS trip is initiated by the PPIS upon detection of low primary system pressure [<4412 kPa (<640 psia)] and a relatively high steam temperature [>393°C (>739°F)]. HTS shutdown in turn signals an SCS startup following which the SCS serves to remove the core decay heat. Although the PPIS trips the HTS in response to 0.65 cm^2 (0.1 $in.^2$) and larger primary coolant leaks, decay heat removal with the HTS can be resumed within an hour. Thus, the normal response to 0.65 cm^2 (0.1 $in.^2$) and larger primary coolant leaks is reactor trip, HPS pumpdown initiation, HTS trip, SCS initiation, and eventual resumption (manually) of HTS cooling following an interval of decay heat removal with the SCS.

6.1.1.2. Plant Response to Abnormal Conditions. Failure to provide forced core cooling following a primary coolant leak or failure to pumpdown the primary coolant inventory to storage may occur. Depending upon the leak location and size, HTS or SCS failure may result from damage directly attributable to the depressurization. Otherwise, failure of these systems is independent of the initiating event.

Another consequence of primary coolant leaks which must be considered is the possible entry of air into the primary system and the

potential for air-graphite reaction. Figure 6-2 shows the results of an analysis of the fraction of graphite reacted as a function of time following a 33 cm^2 (13 $in.^2$) leak (the flow area of the largest pipe, relief valve line, connected to the vessel). In such an event the air ingress is relatively limited, occurring as a result of hydrostatic displacement and thermal contraction. As seen in the figure, the amount of graphite oxidized in such an event is small (<0.01%) with no significant threat to core integrity. The quantity of flammable gas generated in such an event (CO) and released to the reactor building through the leak area has also been calculated and is well below flammability or explosive limits.

For still larger though extremely unlikely leak areas (i.e., those involving a failure in the Class 1 vessel or vessel closures), there is the concern of pressure induced failure of critical structures. Large pressure forces might, for example, cause disruptions in the core geometry convection cooling pathways or neutron control poison pathways. However, gross changes in the convection cooling pathway would be no more significant than the loss of forced cooling events considered in the next section and clearly less likely. Similarly, alterations in the poison pathway would be no more serious than the ATWS events described in Section 6.1.5.

Another possible concern, is that overpressurization of the reactor building and failure of the RCCS cooling panels might occur. The consequences of such an event are considered later in Section 6.1.3 as a result of earthquake caused damage.

There is also concern that in the event of a large leak, greater core oxidation might occur. The air flow which can access the core is generally limited through any single hole. The worst case may be considered to be the hypothetical simultaneous occurrence of holes at the bottom and top of the vessel which might allow air to freely convect through the core. Even in such an event the amount of air which could

react with the core would be limited by the air in the building volume and subgrounded reactor cavity. Analysis of the reaction of the complete reactor building volume of air with th core graphite indicates that less than 1% of the graphite would be reacted, and no significant threat to fuel integrity would be expected.

If the reactor building and subgrounded core cavity are postulated to be ineffective in limiting air ingress, the graphite reaction would be limited only by the pressure drop across the core. Because the graphite-air reaction is exothermic there is the concern that the heat added by the reaction might accelerate the fuel heatup and increase the ultimate temperature leading to significant incremental fuel failures. Bounding analyses of this event have therefore been conducted to determine the additional heat added owing to the graphite reaction. Such analysis indicates the exothermic energy added by this reaction would only be a few percent of decay heat levels after plant shutdown. As such, core heatup would remain slow with peak temperatures and incremental fuel fission product release not occurring until days after the event, allowing ample time to take mitigating actions before such actions would be hampered by high radiation levels.

6.1.2. Loss of the Heat Transport System

Loss of the HTS may be engendered by failures either within the BOP or nuclear steam supply system (NSSS) portions of the plant. BOP failures may eventually result in a loss of feedwater flow to all four modules. NSSS failures should only impact one module.

6.1.2.1. Planned Plant Response. The planned response to a loss of HTS cooling caused by a secondary cooling system failure is to disengage the circulator motor contacts and close the steam generator steam and feedwater block valves. Complete HTS shutdown is accomplished following detection by the PPIS of a circulator speed to feedwater flow mismatch (i.e., ratio greater than 1.20). Following HTS shutdown, the reactor is

tripped with the control rods. This is accomplished through detection of two separate trip parameters. The safety protection subsystem (SPS) initiates a reactor trip upon sensing a high neutron flux to helium mass flow ratio. The Investment Protection Subsystem initiates reactor trip on a redundant trip signal (i.e., HTS shutdown) and also initiates a startup of the SCS for each module that has lost HTS cooling. In the event that the outer control rods are not inserted into the reactor core, a second trip setpoint for RSCE actuation is reached when the neutron flux to HTS circulator speed ratio reaches 1.80 and a 30 s time delay has passed since signaling the outer control rods to drop. In this manner, redundancy is achieved in the ability to control neutron flux levels in the reactor core.

Failures within the NSSS portion of the plant include spurious circulator trip and other localized failures of the HTS. Identical reactor trip signals as indicated above apply to this type of failure as well, except only one module is affected. The SCS is again started automatically for the module that has lost HTS cooling.

6.1.2.2. Plant Response to Abnormal Conditions. Loss of HTS cooling may be followed by the failure of the SCS to start or run. Cooldown of the reactor core is then accomplished by conduction and radiation to the RCCS cooling panels. The vessel pressure rises initially but remains low enough to avoid lifting the primary relief valves [which are nominally set to open at 7177 kPa (1041 psia)] thus containing fission products within the reactor vessel. The primary coolant pressure transient which corresponds to a pressurized cooldown on the RCCS, without any HTS or SCS decay heat removal, is depicted in Fig. 6-3.

6.1.3. Earthquakes

Plant response to an earthquake may vary depending upon the seismic intensity range under consideration. Ground accelerations below 0.2 g are not expected to result in system failures. At intensities below an

operating basis earthquake (OBE) (0.15 g for the MHTGR) reactor trip may not be required and normal power production can be maintained. For large earthquakes above a 0.4 g ground acceleration, forced cooling systems may be lost and plant damage may occur.

6.1.3.1. Planned Plant Response. The initial response of the plant to large earthquakes, on the order of the 0.3 g safe shutdown earthquake (SSE), is an HTS trip of all modules. The cause of the trip may arise from a variety of disturbances which lead to abnormalities in the feedwater or helium flow. Seismically induced electrical faults are generally responsible for these disturbances during such an event. HTS trip is typically initiated following detection of the circulator speed to feedwater flow mismatch created by the disturbance. The reactors are tripped automatically by the PPIS following the signal to trip the HTS in all modules. The main circulators coast down in approximately 2 min, at which time the helium shutoff valve closes by gravity due to decreased helium flow. Following reactor trip, decay heat levels are quickly reached and the reactor pressure remains essentially constant, rising only slightly, until core heat removal is resumed by the SCS. The main loop trip signal initiates cooling on the SCS in all four modules 400 s after the transient begins. Following SCS startup, the pressure in the primary system begins to decrease.

6.1.3.2. Plant Response to Abnormal Conditions. Following a large earthquake and HTS trip, heat removal capabilities may be challenged by failure of the SCS in one or more modules. The response of the plant in such an event is to remove heat from the core by conduction and radiation to the RCCS cooling panels.

In the extremely remote event of earthquakes occurring much larger than the design basis SSE event (i.e., earthquakes with accelerations much larger than 0.3 g), critical structures may be threatened. In particular, failure of the passive RCCS may need to be considered in addition to failures of the active forced cooling systems. It should

be recognized that the RCCS is designed with considerable margin and redundancy. Thus the earthquake would have to cause multiple structural failures and such failures would have to be virtually total in terms of cutting off the air flow to the vessel cooling panels.

In such a remote event, core heat would be removed only by the mechanisms of radiation and conduction to the structures and earth surrounding the reactor cavity. Natural convection currents in the silo cavities also aid heat removal. Analyses have been conducted to determine fuel temperature response in this case with no heat removal via the RCCS. In such a case, peak and average fuel temperatures exceed those which are calculated when the RCCS is functioning by some several hundred degrees. The core maximum and average temperaturees reached are approximately 1870°C (3398°F) and 1600°C (2912°F). At these higher fuel temperatures, incremental fission product release from the core does occur. As identified in Section 8, in fact, the activity release from this event involving all the four reactor modules (designated DC-1), bounds all other events assessed in this risk assessment. However, even with these degraded heat removal conditions, the inherent thermal response of the core and fuel particle retention are still adequate to limit releases to a fraction of a percent (0.02% of halogens for example) and thus prevent any truly gross release of core fission products.

6.1.4. Loss of Offsite Power

MHTGR electrical loads are supplied by the house turbine-generator sets and offsite power sources. If offsite power is lost, the house electrical loads are supplied by the turbine-generators. Either turbine-generator set is capable of sustaining house loads.

Loss of offsite power accompanied by an inadvertent turbine trip results in a sustained loss of all nonuninterruptible ac power. Electrical systems which still remain available to serve vital components are the uninterruptible power supplies, dc battery power systems, and

the backup generators. DC battery power is available for up to 1 h at rated load to supply the uninterruptible power sources until standby generators are started.

6.1.4.1. Planned Plant Response. The MHTGR control system is similar in design to the British gas-cooled reactors insofar as both are designed to remain online in the event of loss of offsite power. The probability is high that at least one of the two turbine-generators will remain online and provide power to in-house electrical loads following the loss of offsite power.

6.1.4.2. Plant Response to Abnormal Conditions. The plant response to a loss of offsite power and inadvertent trip of both ECS turbines is a concomitant trip of the HTS circulators in all four modules and of the feedwater pumps, due to the loss of ac power to these components. Power continues to be supplied to the PPIS through the uninterruptible power source which is supplied by the dc power system batteries. HTS shutdown is signaled by the PPIS upon detecting a circulator speed to feedwater flow mismatch. The signal to shut down the HTS results in (1) the main steam and feedwater block valves being closed, (2) a signal to trip the reactor, and (3) a signal to initiate the SCS for decay heat removal. Reactor trip may also be initiated by detection of a high neutron flux to helium mass flow ratio. If the control rods are not dropped, reserve shutdown material is inserted into the reactor core within 30 s, thus providing redundant and diverse capability for reactor trip. Power to the SCS to provide decay heat removal is accomplished by relying on the backup generator sets. Since SCS cooling is provided, there is no challenge to retention of radionuclides in the fuel. In addition, the resulting pressure transient while on the SCS does not challenge radionuclide retention by the reactor vessel.

If the backup generators fail to power SCS cooling, this results in a loss of all forced cooling mechanisms. Core decay heat is than

removed by conduction and radiation of heat to the RCCS. In this abnormal plant condition, the pressure transient does not challenge radionuclide retention by the reactor vessel. Figure 6-3 again provides the resultant pressure transient.

6.1.5. Anticipated Transients Requiring Scram

The most common transients that require a reactor trip involve failures that inhibit the ability of the plant to sustain power production in all operating modules. For example, during normal full power operations the loss of one ECS train requires that two of the four operating modules be tripped. Failure to successfully insert control rods automatically could be due to either a control system fault, mechanical failure in the control rod drive mechanisms, or the scram contractors failing closed.

6.1.5.1. Planned Plant Response. The normal plant response to an anticipated transient requiring scram depends upon the nature of the transient. In most cases, the normal plant response involves reactor trip in one or more modules, followed by decay heat removal through the HTS of the tripped modules. If, for example, one ECS train fails when all four modules are at full power, the normal plant response is to trip two modules and use their HTSs to convey decay heat from their reactor cores to the operational ECS train.

A small fraction of all anticipated transients requiring scram involves reactor trip with a loss of HTS cooling in at least one module. The normal plant response to loss of HTS cooling is to close both the steam and feedwater isolation valves. The HTS trip signal normally initiates a reactor trip with control rods. Following the HTS trip signal the main circulator coasts down in the affected module and helium flow rapidly decreases. At approximately 2 min following the transient initiation, the helium shutoff valve closes when flow has reached 1% of full flow. Core heat removal is resumed by the SCS 5 min after the HTS

is lost. The delay time between HTS failure and SCS heat removal is due to the transition from standby to full power operation of the SCS. The secondary coolant flow rate is first increased and the circulator attains minimum operational speed. The automatic circulator speed controller is activated and circulator speed is subsequently varied based upon the heat exchanger water outlet temperature.

6.1.5.2. Plant Response to Abnormal Conditions. Two abnormal conditions merit attention following an anticipated transient requiring scram:

1. Failure to trip, given a loss of HTS cooling.
2. Failure to provide SCS cooling, when required.

The response of the reactor core power is shown in Fig. 6-4 for the condition when a module does not trip subsequent to a loss of HTS cooling. Initially, the reactor continues to operate at full power until increased core temperature introduces negative reactivity. The core power level subsequently drops until at 56 s into the transient, the reserve shutdown control material (RSCM) is inserted into the reactor core by a signal from the PPIS. The PPIS signal is initiated by the core power-to-circulator speed being greater than 1.8 for more than 50 s as given in Table 6-1. Following this action, the core power level drops rapidly to the decay power level. Failure of the SCS results in a pressurized conduction cooldown condition to the RCCS. Even if the outer control rods are not inserted, the response of the core power level is similar to the previously described plant response because the SCS is not called upon to operate prior to insertion of RSCM at 56 s into the transient. Failure of the SCS results in increased core temperatures which in turn cause an increase in system pressure during the initial stages of the transient. The pressure response throughout the transient is shown in Fig. 6-5. The pressure increases do not reach the relief valve setpoint and slowly decrease with time as core heat is removed by conduction and radiation to the RCCS cooling panels. Note

that the initial pressure increase is slightly higher than in Fig. 6-3 for a pressurized conduction cooldown with successful control rod trip. This is due to the 56 s delay in actuating the reserve shutdown control equipment (RSCE).

The preceding discussion presumes that the RSCE will be successfully activated as the secondary mechanism to provide reactor trip in the event the outer control rods fail to be inserted. The plant response to a condition in which both outer control rod and reserve shutdown reactor trip fail, in addition to loss of all forced core cooling mechanisms, is described here. During the first phase of the transient, negative temperature reactivity feedback reduces the reactor power to decay heat levels after approximately 300 s, effectively shutting the reactor down. The concentration of xenon rises to a peak value and then begins to decay away. Eventually the xenon level becomes low enough that the combination of xenon poisoning and negative temperature defect is no longer sufficient to keep the reactor subcritical. This occurs at about 38 h into the transient. The second phase of the transient begins at the point recriticality is reached. From this point on the reactor maintains a power level which results in reactor temperatures that just offset the decay of xenon. Should the power fall below that level, reactor power will rise in response to the reduction in overall core temperatures. Temperature reduction results in minimizing the effect of negative temperature reactivity feedback. Conversely, if the power is too high, the reactor will become subcritical and the power will decrease because of the initial increase in reactor temperatures. Steady state is reached when the decay of xenon is complete. The transient is complete when remedial action is finally successful in inserting control rods, reserve shutdown material, or a sufficient quantity of the fuel in the core has been used up. The pressure response of the system during this event is depicted in Fig. 6-6. As indicated in the figure, system pressure remains below the relief valve opening setpoint with margin, thus preventing the release of fission products from the primary coolant pressure boundary. The thermal response of the system

during the transient has been shown to be acceptable in terms of maintaining structural integrity. The reactor vessel, core support, and other structurally important internal temperatures are maintained at acceptable levels. Although temperatures in excess of 1600°C (2912°F) are sustained in 20% to 25% of the core, the resultant fission product releases are contained within the primary pressure boundary.

6.1.6. Control Rod Bank Withdrawal

The most likely cause of spurious rod withdrawal is a failure of the neutron flux controller to operate properly. Control rods are normally moved in groups of three symmetrically located rods (control rod banks) to minimize flux tilting. A spurious uninhibited withdrawal would therefore result in an outer control rod group of three rods being withdrawn from the core.

6.1.6.1. Planned Plant Response. The normal plant response following a spurious control rod bank withdrawal is a reactor trip with the outer control rods. The reactor trip signal is initiated by the PPIS upon detection of a high neutron flux to helium mass flow ratio of 1.5 at approximately 106 s after the initiation of the transient. Prior to reaching the trip setpoint, the reactor power level increases as the rod bank becomes fully withdrawn. The increasing core temperatures introduce negative reactivity and thereby assist in reducing the rate of power increase caused by the rod bank withdrawal. Core cooling is expected to continue on the HTS. Although the initial rod withdrawal increases reactor power by almost 50% at very early times, the reactor core power level is reduced to decay levels within 200 s following the reactor trip at 106 s. The post-reactor trip cooldown does not jeopardize containment of radionuclides within the reactor pressure vessel.

6.1.6.2. Plant Response to Abnormal Conditions. Failure to provide HTS cooling is the most likely abnormal response to a control rod bank withdrawal. In this event, HTS shutdown initiates forced core cooling

by the SCS. Core power level versus time for this event is shown in Fig. 6-7. As indicated in the figure, reactor trip is accomplished at 106 s into the transient. All outer reflector control rods, including those initially withdrawn, are inserted into the reactor core at this time. An HTS rampdown is initiated, and at 120 s the HTS fails to remain online. Prior to reactor trip, the reactor power level increases in response to reactivity addition as the group of rods is withdrawn. As core temperature increases, negative reactivity is introduced but is insufficient to fully compensate for the positive reactivity addition. The inflection in the curve occurs as the withdrawn rod group approaches a pull out position and the reactivity addition per unit length withdrawn increases. At this point, the temperature induced reactivity reduction is much smaller in relation to the reactivity addition; hence, the steeper gradient of the curve.

Additional failure of the SCS requires heat removal to the RCCS in order to limit core temperatures and system pressure. Failure to provide forced core cooling does not, however, result in exceeding the primary system relief valve setpoint pressure (Fig. 6-8). The primary relief train is, therefore, not required to respond to the transient and radionuclides are retained in the primary circuit.

Abnormal conditions may also exist if the reactor is not successfully tripped with the control rods when a high neutron flux to helium mass flow condition is present. As the core power level increases because of the withdrawn control rod bank, the system pressure and helium temperature begin to increase as well. Additional reactor trip setpoints are eventually reached as the transient progresses. Other control rod trip setpoints are reached when primary coolant pressure reaches 6929 kPa (1005 psia) and the steam generator inlet helium temperature reaches 746°C (1375°F). The RSCE is signaled to actuate when primary system pressure reaches 6998 kPa (1015 psia), or when the reactor power to circulator speed trip point is reached. In addition, the reactor can be manually tripped by an operator.

The preceding discussion presumes that the reactivity insertion occurs at a rate controlled by the maximum withdrawal speed of the control rods and that the reactivity inserted is limited to the worth of a rod bank. The sensitivity of the plant response to a more rapid or larger reactivity insertion is described here.

The concern with a more rapid reactivity insertion is that core power may significantly overshoot the power levels reached in the slower withdrawal event before the negative temperature coefficient counteracts the overpower condition. Even though the overpower condition is brief, if more energy is deposited in the fuel than in the withdrawal case, higher fuel temperatures may be reached. The most rapid potential for reactivity insertion into the core may be associated with a control rod ejection. The likelihood of such an event in the MHTGR is extremely remote. The event would first require the total failure of the Class 1 vessel penetration which houses the individual rod drives. Secondly, the ejection would have to be energetic enough to force the rods through the structures located above the rod housings. In particular, they would have to penetrate the fairly massive refueling floor above the upper vessel. And finally, a failure of the other rods or RSCE to be inserted must be postulated.

Despite the remoteness of a rod ejection event, the consequences of such an event with failure to scram have been explored both from a zero power condition and a full power core condition as shown in Figs. 6-9 and 6-10. In this analysis, a rod (worth 1.1% Δk) is assumed to be ejected from the core in a matter of seconds, with the resulting core power and fuel temperatures calculated. It may be seen from the two figures, that the rapid reactivity insertion at power is the most severe in terms of the fuel temperatures which are reached. The core power swing in this case may indeed be seen to be large, peaking at some eight times full power. Since the negative temperature feedback in the MHTGR is primarily driven by the prompt fuel pin doppler feedback (as opposed to slower acting moderator block heatup), this power swing is seen to be

very brief with the temperature feedback rapidly bringing power level back to normal. The resulting fuel temperature increase, although rapid, peaks well below temperatures which would be expected to cause any significant incremental fuel particle failures.

To clearly bound the size of the reactivity insertion which might be encountered by any credible reactivity insertion events (whether associated with neutron control systems or with water ingress events as discussed in Sections 6.1.7 and 6.1.8), an analysis has been conducted of a hypothetical withdrawal of all control rods (worth 3% Δk) at full power without scram and loss of all forced core cooling, the results of which are shown in Fig. 6-11. Again, it may be seen that core power increases until the negative worth of the resulting temperature increase in the fuel balances the positive worth associated with the rod withdrawal. The fuel, in such a case, heats up, but stabilizes at a temperature well below the point at which experimental evidence indicates there would be any significant incremental failures in the fuel particle coatings.

Considering the extreme remoteness of the above reactivity events and the relatively benign consequences which are calculated owing to the inherent behavior of the core, can be concluded that neither of the above reactivity insertion events is limiting in terms of MHTGR risks.

6.1.7. Small Steam Generator Leaks

Steam generator leakage can result form a number of causes including corrosion, fretting, wear, and weld failure. The plant response to moisture inleakage resulting from a tube failure varies depending upon the leak rate. This section considers the plant response to moisture inleakage resulting from a small tube leak of $\leq$0.1 lbm/s.

6.1.7.1. Planned Plant Response. The plant response to a small moisture ingress event begins with the automatic neutron flux controller

compensating for the moisture reactivity effect by inserting the control rods to maintain a power level of essentially 100%. A single of high primary coolant moisture (≥1000 ppmv) from the moisture monitors to the PPIS serves to trip the HTS and to trip the reactor with the control rods. A high moisture trip signal also initiates isolation and dump of the steam generator which terminates the moisture ingress. HTS shutdown initiates the startup of the SCS by the PPIS to provide forced core cooling. Since moisture ingress is terminated normally, the RSS is not called upon to provide additional shutdown margin. Primary system pressure increases are not large enough to challenge the pressure retaining capabilities of the primary system and the primary relief valve remains closed.

6.1.7.2. Plant Response to Abnormal Conditions. Failure of the moisture monitors to detect high primary coolant moisture levels would lead to greater amounts of moisture ingress. Moisture reactivity effects are still compensated for by the automatic neutron flux controller. Reactor trip eventually occurs on high system pressure >6998 kPa (>1015 psia) at which time the RSCE control material is inserted into the core as well as all of the outer control rods. HTS trip is activated automatically following which the steam generator is automatically isolated and dumped, terminating the inflowing moisture. HTS shutdown automatically signals the initiation of SCS cooling.

6.1.8. Moderate Steam Generator Tube Leak

A moderate sized leak may range from 0.1 to 12.5 lbm/s, the latter leak rate corresponding to an offset tube rupture. Plant response to moisture inleakage resulting from a tube failure may very depending upon the leak rate. This section considers the plant response to a moisture inleakage rate approximately corresponding to that of a single offset tube rupture.

6.1.8.1. Planned Plant Response. The initial plant response to a moderate steam generator tube leak occurs within a few seconds when moisture reaches the core and produces a sharp increase in reactivity. Core power reaches a peak at approximately 9 s. At this time and given the maximum ingress rate within the range described the reactor power can reach a peak as high as 180% of rated power because of the moisture reactivity excursion. The effects of the temperature coefficient and partial control rod insertion arrest the transient quickly, and the power returns to 100%. At about 22 s, high primary coolant moisture is detected (1000 ppmv) by the moisture monitors. A high primary coolant moisture signal to the PPIS then results in a reactor trip with the control rods and the power drops quickly to decay heat levels. The change in the reactor power level to changes in core reactivity is depicted in Fig. 6-12. Initially the neutron flux controller does not fully compensate and the core power level increases. At roughly 11 s, sufficient control rod groups have been inserted to compensate and the core power level falls. The reactor trip at 22 s is evident in the figure.

High primary coolant moisture levels also initiate isolation and dump of the steam generator by the PPIS. This signal in turn causes the HTS to be shutdown. The tripped circulator coasts down and reaches about 1% of nominal flow in approximately 2 min following which the flapper-type helium shutoff valve closes by gravity. When HTS shutdown is completed, the SCS is signaled to start by the PPIS. Startup of the SCS begins by switching the cooling water pumps from standby to pressurized operation. Ninety seconds later the SCS circulator is started and increases in speed to maintain the SCS heat exchanger water outlet temperature. The circulator speed increases until the speed becomes power limited by the circulator motor. This occurs about 1.5 h following startup. At this time the water outlet temperature begins to decrease and the core heat removal rate is reduced.

The primary coolant pressure response to a moderate moisture ingress event which is followed by a successful plant response is shown in Fig. 6-13. As shown in Fig. 6-13, the primary circuit pressure rises sharply in the initial few seconds due to the moisture ingress. As the ingress is terminated, the pressure essentially remains constant, being influenced only by the steam-graphite reaction products and a slight increase in core temperatures during the transition from HTS and SCS cooling. The sharp inflection in the pressure transient is due to forced core cooling being re-established by the SCS. As depicted in Fig. 6-13, primary system pressure remains below the primary relief valve opening setpoint of 7177 kPa (1041 psia). Successful response to a moderate moisture inleakage event, therefore, mitigates adverse consequences by retaining radionuclides within the confines of the reactor vessel.

6.1.8.2. Plant Response to Abnormal Conditions. Failure of the SCS to provide forced core cooling following HTS shutdown constitutes an abnormal condition in the plant response to a moderate steam generator leak. The response of the reactor core power level to reactivity changes is identical to that for the planned response to the transient (Fig. 6-12). The primary coolant pressure response of the system differs significantly, however, from the response during the planned sequence of events. Since system temperatures are higher in this instance as a result of the loss of forced helium circulation, the pressure increases approach the primary system relief valve setpoint pressure as indicated in Fig. 6-14. For nominal conditions, the relief valve will not be lifted, however, and radionuclides are retained within the pressure boundary. Variability in the actual relief valve opening setpoint and in the total helium inventory, however, present the possibility of a relief valve lifting. Failure of the SCS then degrades the plant response by potentially causing a challenge to one of the primary relief valves.

A second abnormal condition that may be encountered is the failure of the moisture monitors to detect moisture. The initial response is for the neutron controller to insert multiple control rod banks to mitigate the core power increase. Core power continues to rise such that the PPIS reactor trip setpoint on a high core power-to-flow ratio of 1.4 is achieved at 8 s. The reactor trip is delayed until 22 s at which time the outer reflector rods are fully inserted. The delay time of 22 s accounts for the transit time of the control rods from their withdrawn position to full in. The core power transient for this abnormal condition is shown in Fig. 6-15. Failure to automatically isolate and dump the leaking steam generator results in continued moisture ingress into the primary system which in turn increases the total system pressure. The reserve shutdown control material is inserted by the PPIS at 250 s when the trip setpoint of 6998 kPa (1015 psia) is reached. The RCSM is inserted into the core to maintain reactor subcriticality. The high pressure signal also initiates HTS trip with steam generator isolation but without dump. The ingress of moisture continues at a lower rate. The response of the primary coolant pressure relief valve during this condition is to open when the setpoint of 7177 kPa (1041 psia) is reached. Normally, the relief valve will cycle [i.e., open at a nominal 7177 kPa (1041 psia) setpoint and close at a nominal 6101 kPa (885 psia) setpoint] until the moisture ingress is terminated by the operator by manual opening of the steam generator dump values. However, if the relief valve fails open, the module depressurizes in minutes. Figure 6-16 shows the primary coolant pressure during the first 600 s of a transient in which the relief valve cycles successfully.

Potentially combustible gases are produced by the chemical reaction of steam from a moisture ingress with hot core graphite. This water gas (a mixture of equal moles of H_2 and CO) requires oxygen to allow combustion, so that as long as there is no venting to the reactor building, there can not be a combustible mixture formed. The case of a moderate moisture ingress with primary coolant relief valve opening (described

above) has been assessed for combustible mixtures in the reactor building. The results show that there are no global flammability or detonability consequences for this event since the mixture is too lean for combustion. Figure 6-17 shows the flammability diagram for water gas. The CARCAS code (Ref. 6-1) results indicate that the reactor building mixture remains outside the flammable region. Also, an assessment of flammability for an unterminated moisture ingress shows that the large amount of diluent (moisture) prevented the formation of a combustible mixture. Thus it is believed that the formation of combustible gas mixtures from moisture ingress events is not a problem for the MHTGR system.

The above analysis is based upon the offset rupture of a single steam generator tube. In the extremely unlikely event that more tubes are assumed to rupture, the water ingress rate would obviously be increased. However, since the protective actions are prompted by the mass increase caused by water entry into the primary system, the more rapid water entry would simply prompt such actions earlier such that the total mass entry into the primary system would only be slightly greater. Thus, a more rapid ingress of water than analyzed above is projected to be much less probable with only slightly higher consequences and would thus not be a significant risk contributor.

In the extremely unlikely event that no protective action is taken to insert the control rods or RSCE into the core, power level increase would occur due to the positive reactivity worth of the water. At power, the reactivity effects of such a continued ingress have already been bounded, however, by the analysis of total control rod withdrawal provided in Section 6.1.6 and are seen there not to be overly severe.

In the extremely unlikely event that no protective action is taken to terminate the water ingress as analyzed above (i.e., by isolation of the feed and steam lines to the steam generator) steam ingress

into the primary system would continue. In such a case, the consequences of greater steam-graphite and steam-fuel (hydrolysis) reaction must be considered. Fuel hydrolysis, however, is bounded by the number of particles in the core which are already defected or failed. The worst case therefore would be significant hydrolysis of the failed fuel particles, a consequence which already may occur as a result of the water ingress described above (see Appendix D.4.2 - release category WC-1). The steam-graphite reaction is endothermic and strongly temperature driven. Thus as the reaction continues, the core is inherently cooled, reducing the reaction rate. Therefore analysis has shown that any such unlimited oxidation of the core graphite proceeds very slowly, and literally days would be available to take the innumerable measures available to terminate the water ingress.

6.2. SYSTEM RELIABILITY MODELS

Table 6-2 presents the top-level systems addressed in the event trees of Appendix C and the systems which serve to support them. In some cases a system will support more than one top-level system. Loss of these common support systems will affect the probability of multiple system failures. For each top-level system a success criteria can be defined as well as the systems that must function properly to assure successful operation is attained. The following subsections will address reliability models for each top-level system separately. Included will be a discussion of the support systems required in order for the top-level system to perform its function. Besides reliance on common support systems (e.g., for service water, control, or electric power) the reliability of some top-level systems is influenced by the failure modes of other top-level systems. Of particular concern is the number of modules which require that certain top-level systems successfully operate. For example, if an HTS circulator trip occurs in one module, only that module requires SCS cooling. However, if HTS cooling is lost to all modules (due, for example, to a common mode failure of both ECS trains), then all four modules require SCS cooling and the SCS

TABLE 6-2
CROSS REFERENCE OF PLANT SYSTEMS/SUBSYSTEMS TO FAULT TREE AND EVENT TREE TOP EVENT MODELS

Systems/Subsystems Analyzed in the PRA	Top-Level Fault Trees			Event Tree Top Events
	Loss of HTS Cooling	Loss of SCS Cooling	Loss of HPS	Other Systems/Subsystems Supported
Heat transport system	X			
Shutdown cooling system		X		
Feedwater and condensate subsystem	X			Steam generator isolation
Condensate polishing subsystem	X			
Neutron control subsystem				Reactor trip
Pressure relief subsystem				Pressure relief
Plant protection and instrumentation system	X	X	X	Moisture monitors, reactor trip, S/G isolation and dump
Turbine generator and auxiliaries subsystem	X	X		
Main and bypass steam subsystem	X			Steam generator isolation and dump
Helium purification subsystem			X	
Helium storage and transfer subsystem			X	
Service water subsystem	X	X	X	
Circulating water subsystem	X			
Reactor plant cooling water subsystem	X		X	Moisture monitors, reactor trip, steam generator dump
Instrument and service air subsystem	X			Steam generator isolation

TABLE 6-2 (Continued)

Systems/Subsystems Analyzed in the PRA	Top-Level Fault Trees			Event Tree Top Events
	Loss of HTS Cooling	Loss of SCS Cooling	Loss of HPS	Other Systems/Subsystems Supported
Turbine building closed cooling water subsystem	X			
Non-class 1E ac distribution system	X	X	X	Steam generator isolation and dump
Class 1E uninterruptible power supply system	X	X	X	Moisture monitors
Class 1E dc power system	X	X		Reserve shutdown reactor trip

failure probability is concomitantly higher since more SCS equipment (e.g., four SCS circulators instead of one) must operate.

Maintaining the ability to adequately remove decay heat is of concern in all event sequences evaluated in subsequent sections. Included in the evaluation of sequences where all cooling systems are lost, is the ability to repair at least one of those systems before important safety limits are exceeded. The component found to be most sensitive to excessive thermal transients was the reactor vessel. Under pressurized conditions, the vessel is conservatively assumed to fail if it exceeds 482°C (900°F). Under depressurized conditions, the vessel material undergoes a phase change at 760°C (1400°F). The mission time for the HTS, SCS, and RCCS cooling systems under depressurized and pressurized accident conditions was evaluated and used to construct Fig. 6-18 which depicts maximum time to repair a cooling system versus the prior cooling time. The mission time is defined as the time any cooling system must operate (HTS, SCS, or RCCS) to prevent vessel failure resulting from exposure to excessive temperatures.

6.2.1. HTS Cooling

The primary means by which heat is removed from a module during both normal operation and shutdown conditions is by the HTS. Heat is transferred to the circulating helium in the core which then is routed through the steam generator. As the helium flows through the steam generator, heat is transferred through the steam generator tubes to the secondary side water. Figure 6-19 depicts the top-level fault tree for failure of the HTS in at least one module. In Fig. 6-19 the failures of interest are those that result in the inability to remove decay heat from at least one module with the HTS. Failures that engender a loss of power production in at least one module, but which do not preclude decay heat removal, are excluded from the Fig. 6-19 fault tree. As shown, nine system failures have been identified, any one of which can result in HTS failure as indicated by the "OR" gate-G1. Proceeding from left

to right, each failure category will be discussed in the following sections. Systems and subsystems appearing in the fault trees are described in the plant description of Section 4.

6.2.1.1. Energy Conversion System (ECS) Failure. Failure of both ECS trains engenders the loss of HTS cooling in all four plant modules. Figure 6-19 is the fault tree for ECS failure which applies to both trains. The ECS is the heat sink for the HTS. As outlined in the plant description of Section 4, the ECS removes heat as hot helium gas is circulated through the steam generator. Cold feedwater flows upward through the steam generator tubes and exits as superheated steam as heat is transferred through the tubes from the hot helium gas. Four subsystems are identified in Table 6-2 which support the heat removal function of the ECS. Failure of the feedwater and condensate subsystem (including the demineralizers), circulating water subsystem, turbine generator and auxiliaries subsystem, or main steam and turbine bypass subsystem would result in an ECS failure. As noted in Fig. 6-20, steam generator tube failure will result in a loss of the ECS. Plant response to a steam generator leak, however, differs from the response to other ECS failures. This failure mode is, therefore, considered as a separate initiating event, rather than as part of the loss of HTS initiating event evaluated in Section 7.2.

The fault trees for feedwater and condensate subsystem failure are given in Figs. 6-21 through 6-23. Basic and undeveloped terminal events include valve failures, pump failures, and heat exchanger failures. Failure of electrical systems other than local electrical failures and instrument and service air has not explicitly been evaluated here. They are rather included as second-level events in Fig. 6-19. Demineralizer failure is considered separately and the fault trees are given in Figs. 6-24 and 6-25. The transfer point "J3" is located in Fig. 6-23 for feedwater and condensate subsystem failure.

Failure in the circulating water subsystem that lead to loss of the ECS are given in the fault trees of Figs. 6-26 through 6-30. The circulating water subsystem serves as the heat sink for the feedwater and condensate subsystem.

6.2.1.2. Service Water Subsystem Failure. Proceeding to the second HTS failure mechanism of Fig. 6-19, the failure of the service water subsystem results in the loss of HTS cooling to all four plant modules. The fault tree describing service water subsystem failure is given in Fig. 6-31. The service water subsystem serves as the heat sink for a number of other water systems including the RPCWS and TBCCWS, to be discussed later.

6.2.1.3. Plant Protection and Instrumentation System Failures. The third failure mechanism which engenders HTS failure is a spurious, PPIS-initiated, HTS trip signal. Spurious trip of more than one module is very unlikely since each module has a separate and independent PPIS. PPIS failure will therefore result in only one module losing HTS cooling. PPIS failures due to loss of the class 1E uninterruptible power supply are considered in another branch of the loss of HTS fault tree.

6.2.1.4. Turbine Building Closed Cooling Water Subsystem Failure. The fourth failure that leads to loss of HTS cooling, as shown in Fig. 6-19, is loss of the TBCCWS. The fault trees of Figs. 6-32 through 6-34 describe the failures leading to the loss of the TBCCWS. The TBCCWS provides cooling for a variety of components important to maintaining HTS cooling and rejects heat to the service water system. Service water system failure (Fig. 6-31) is included in Fig. 6-33 as a mechanism by which the TBCCWS can lose its heat sink. In addition to providing cooling to the HTS circulator controller, the TBCCWS cools turbine/generator components, instrument and service air compressors, and feedwater and condensate subsystem components. Failure of the TBCCWS may also be the result of the failure of the non-class 1E ac power supply to

provide power to the normal and backup pumps as shown in Figs. 6-32 and 6-34. Fault trees for loss of this subsystem will be discussed later.

6.2.1.5. Instrument and Service Air Failure. Failure of the instrument and service air subsystem results indirectly in the loss of HTS cooling. An adequate air supply is required in order to provide the actuation mechanism for a number of valves in the secondary water and other support systems.

6.2.1.6. Reactor Plant Cooling Water Subsystem Failure. The RPCWS provides cooling for the HTS circulator. Loss of this subsystem, therefore, results in circulator unavailability and loss of HTS cooling capability. The fault trees for failure of the RPCWS are given in Figs. 6-35 through 6-37.

6.2.1.7. Non-Class 1E Electric Power Supply Failure. Non-class 1E ac power is required to operate the HTS circulator, controls, and instrumentation in each module. Loss of the entire system results in the loss of HTS cooling to all four modules. As described in Section 4.22, buses 111/112 and 213/214 supply nuclear island electrical loads which include the HTS components. Each bus supplies power for two modules. Fault trees describing the loss of power to nuclear island bus 111/112 are given in Figs. 6-38 and 6-39. The fault trees are applicable to loss of power to bus 213/214 as well. Power supply failure results from the inability to feed the buses from both the unit generators and off-site power source. Unit generator failure considers the availability of a crosstie between units 1 and 2 in the event one generator fails and the other is operable.

6.2.1.8. NSSS Failures. Failures in the NSSS portion of the plant that engender failure of the HTS to remove decay heat are those failures that occur within the HTS itself. As shown in Fig. 6-19, mechanical circulator failures, loss of motor control, magnetic bearing failure, or

local electrical failures of the motor render the HTS incapable of performing its heat removal function. Failures in more than one module are considered essentially independent.

6.2.1.9. Class 1E Uninterruptible Power Supply Failure. The final identified cause of HTS failure is loss of the class 1E uninterruptible power supply. This power supply serves the PPIS which is responsible for providing control and trip signals to the HTS. Failures of the PPIS other than the logic failures considered earlier are a result of failure of the class 1E UPS. Fault trees for this power supply system are given in Figs. 6-40 through 6-49. The class 1E UPS normally depends on power from the non-class 1E ac power supply. If the non-class 1E power supply is lost, the 1E dc power supply is used as a backup power source. The fault trees for the loss of non-class 1E power differ from those presented earlier (Section 6.2.1.7) in that the class 1E UPS receives its power from buses 121/122 and 223/224 rather than from buses 111/112 and 213/214. The buses serving the 1E UPS have backup generators as an additional power source whereas those previously described do not.

6.2.2. SCS Cooling

In the event the HTS fails to remove decay heat in one or more modules, the alternative is decay heat removal by the SCS. The SCS is normally in a standby mode, and is signaled to start by the PPIS once the HTS has been lost for any reason. In some cases, the SCS reliability is degraded if HTS failure was a result of failure of a support system common to both the HTS and SCS. Successful operation of the SCS results in a redundant means of decay heat removal following plant shutdown.

The SCS may be required to operate in more than one module if the HTS failure was a result of the failure of systems which support the HTS in all modules, such as the plant service water subsystem, RPCWS, TBCCWS, or electrical systems. If the HTS failure was localized in the

NSSS or due to a spurious PPIS trip, only one module will require SCS cooling. Figures 6-50 through 6-52 depict the logic diagram representing the SCS failure probability in one or more modules. As shown, SCS failure may be either a failure to start or failure to operate for a sufficient amount of time to complete its mission. In both subtrees A and B, the probability that the HTS fails in two or three modules is negligibly small. SCS failure will, therefore, be important in the cases of HTS failure in one module or four modules. The failure probability of the HTS in one or more modules is derived from the fault trees of Section 6.2.1.

Failure of the SCS when one module requires cooling is given by the fault tree of Fig. 6-53. The fault tree has been divided into two major segments, one for NSSS failures and one for BOP failures. These are further subdivided into three failure mechanisms discussed in the following subsections. Systems and subsystems appearing in the fault trees are described in the plant description of Section 4.

Failure of the SCS when four modules require cooling is given by the fault tree of Fig. 6-54. The fault tree for loss of SCS cooling to four modules is similar to that for loss of the SCS in one module. The transfer points E, A, B, G, and G6 are the same for both trees and will, therefore, be discussed only once.

6.2.2.1. SCS Heat Exchanger Failure. The fault tree describing SCS heat exchanger failure is given in Fig. 6-55. Heat exchanger failure results in a loss of the mechanism to transport heat from the primary cooling to the secondary water system.

6.2.2.2. SCS Circulator Failure. Failures leading to the loss of the SCS circulator are described in Figs. 6-56 and 6-57. Included in the failure mechanisms are control failures, motor cooling failures, isolation valve failures, and mechanical failures in the rotating machinery. Notice that failure to close the HTS helium isolation valve also results

in an SCS failure, since most of the forced convection flow would bypass the core.

6.2.2.3. Actuation Failure. Failure to start the SCS can be the result of failure of the PPIS to transmit a signal, failure of the control system to act upon the signal, or failure of the operator to manually initiate start of the SCS as shown in Figs. 6-53 and 6-54. Failure to start is quantified here and used in the logic diagram of Figs. 6-49 and 6-50 for SCS failure in at least one module.

6.2.2.4. Loss of Cooling to Modules. Failure to provide adequate decay heat removal may be the result of failure of either the primary or secondary SCS heat sinks. Figures 6-58 through 6-63 depict the fault trees for failure of either the service water subsystem or the shutdown cooling water subsystem.

Figures 6-59 and 6-60 are the fault trees for loss of service water. The service water subsystem includes both the normal service water pumps and shutdown service water pumps. During normal plant operation, the normal service water pumps provide service water flow through the shutdown cooling water heat exchangers, maintaining them in a standby condition. If the SCS is required to remove decay heat loads, the shutdown service water pumps are used to remove heat from the heat exchangers while the normal service water pumps continue to remove heat from their other loads. If the shutdown service water pumps fail, the normal service water pumps may be used as a backup. Failure mechanisms which may result in a loss of the SCWS heat sink include a loss of service water flow, pipe rupture, pump intake blockage, or heat exchanger failure.

Figures 6-61 through 6-63 are the fault trees for failure of the SCWS. Failure of this system to perform its function may be a result of heat exchanger failure, pipe rupture, pressurizer leakage, pump failure,

or failures in the water chemistry package. A system description is provided in the plant description of Section 4.

6.2.2.5. Loss of Class 1E UPS Power Supply. The fault trees describing failures in the class 1E UPS electrical system are given in Figs. 6-40 through 6-49 for loss of the SCS in one or four modules. The trees are the same as those given for loss of HTS cooling in Section 6.2.1.9.

6.2.2.6. Loss of Non-Class 1E 480 V ac Power Supply. An electrical failure which may result in the failure of the SCS to perform its function is loss of the non-class 1E 480 V ac power supply. Figures 6-44 to 6-49 describe the fault trees from either loss of the medium voltage supply or the 480-V distribution. Medium voltage power failure of the SCS considers loss of offsite power, backup generator power, and unit auxiliary transformers, as well as circuit breakers. This differs from the loss of HTS fault trees in that the backup generators do not support the HTS.

Quantification of the loss of 480 V ac power is dependent upon the HTS failure mode. For example, in event sequences initiated by a loss of offsite power accompanied by both turbine generators being tripped, the conditional probability that offsite and house power are both initially unavailable is unity. Conversely, in event sequences involving a loss of HTS cooling in only one module, the conditional probability that offsite and house power are both initially unavailable is zero since such an initiating event causes all four modules to lose HTS cooling.

6.2.3. Intentional Depressurization

Intentional depressurization of the reactor vessel is accomplished by the HPS. This action can be initiated either automatically by the PPIS or manually, by operator action. In the event of primary coolant leakage, the PPIS will actuate the HPS pumpdown feature when primary coolant pressure is low and reactor building radiation levels are high,

in order to decrease the amount of primary coolant available for leakage out of the reactor vessel. The only other situation in which primary coolant pumpdown is required is in the event that HTS, SCS, and RCCS cooling systems are nonfunctional. Success of the HPS in this case serves to prevent overpressurizing the reactor vessel because of the combination of excessive heat and pressure loads.

Failure of the HPS pumpdown is characterized by the fault tree in Fig. 6-64. The first identified failure mode is failure to initiate the pumpdown sequence either through PPIS failure or failure of the operator to pumpdown manually. Failures in the RPCWS can engender HPS failure because this water system is the heat sink for many HPS components. The plant service water system is in turn the heat sink for the RPCWS. Electrical power is provided to the HPS through the non-class 1E ac system. Failure of this system will cause failure of the HPS as well as other systems which rely on it as a power source. Failures in the Helium Storage and Transfer Subsystem result in a failure of HPS pumpdown since there is no pathway by which to pump the primary circuit helium to storage. Failure to open a valve in a normally closed position is an example of failures of this type. Localized failures in the mechanical/electrical equipment of the HPS may also lead to system failure as shown in the last failure mode of Fig. 6-63. Some of the failure modes have been presented earlier and include failure of the class 1E UPS, RPCWS, plant service water, non-class 1E electrical system, and PPIS actuation failure.

6.2.4. Reactor Trip

Reactivity control during abnormal conditions is accomplished by actuating a trip with the outer control rods or the RSCE. If trip with the control rods is not successful, the PPIS signals actuation of the reserve shutdown control material hopper release mechanism. If the PPIS fails to successfully trip the reactor, operator intervention is required.

Failure to trip a module may be the result of common mode sensor failure, PPIS logic failure, scram contactor failure, failures in the control rod drive mechanisms, RSCE hopper faults, or operator error. Reactor trip system reliability is based upon assessments performed in Refs. 6-2 and 6-3.

6.2.5. Reactor Cavity Cooling System Failure

Successful operation of the RCCS serves to remove decay heat from the reactor core if both HTS and SCS cooling are unavailable. The RCCS has been designed as a completely passive system, relying only on the natural circulation of air through cooling panels. As described in Section 4, the RCCS is composed of four interconnected cooling quadrants each of which possess separate intake and outlet ducts. For failure of the RCCS to occur, at least two quadrants must be blocked.

Failure of the RCCS results if blockage of the air intake or exit ducts occurs to such an extent that normal air flow is lost. The likelihood of events which would catastrophically fail the RCCS by preventing air flow is extremely low. The reliability of the RCCS has been estimated based on engineering judgment, predicted upon the simplicity of the design and structural margins available that allow the incorporation of large safety factors.

6.2.6. Moisture Monitor Failure

Moisture monitors are provided in each module to assure that if excessive moisture enters the primary system corrective actions will be taken. Detection of high moisture results in a signal to the PPIS to isolate and dump the steam generator and open the main circulator contacts.

Moisture monitor reliability data has been taken from Ref. 6-2 because of similarities in the designs.

6.2.7. Steam Generator Isolation and Dump

Steam generator isolation is required in response to both HTS shutdown and steam generator tube leak detection. Steam generator dump is initiated following a tube leak to minimize the amount of water available for ingress into the primary circuit.

Successful isolation of the steam generator requires closure of steam and feedwater side isolation valves. Isolation failure is predicted upon Ref. 6-2 assessments because of similarities in the system designs. Additional considerations were made to assess the impact of common mode failure when PPIS logic faults prevent various functions from being performed. The MHTGR design also includes a check valve in series with the steam side isolation block valve. The effect of this additional component was also considered in the failure assessment.

Successful dump of the steam generator requires the isolation procedure to have been successful. The PPIS signals the dump system valves to open whereupon the steam generator water/steam inventory is transferred to the dump tank.

6.2.8. Steam Generator Relief Valve Failure

The steam generator relief valve functions to relieve steam generator pressure in the event overpressure occurs. This condition arises if the steam side isolation valves are closed and the feedwater valves fail open. Two relief trains are provided as described in the plant description of Section 4. Failure occurs if the trains either do not open or fail to reclose following pressure relief.

6.2.9. Primary Relief Train Failure

The primary coolant relief train operates successfully if it opens to relieve excessive pressure and subsequently recloses. The block

valve in the primary relief path adds another success/failure possibility for this subsystem.

6.3. REFERENCES

6-1. Landoni, J. A., "Containment Atmosphere Response (CAR) Program-Second Status Report," GA Report GA-A15582, March 1980.

6-2. Fleming, K. N., et al., "HTGR Accident Initiation and Progession Analysis Status Report - Phase II Assessment," GA Report GA-A15000, April 1978.

6-3. Pfremmer, R. D., et al., "HTGR Accident Initiation and Progression Analysis Status Report Volume IV - Phase I Analysis and R&D Recommendations," GA Report GA-A13617, December 1975.

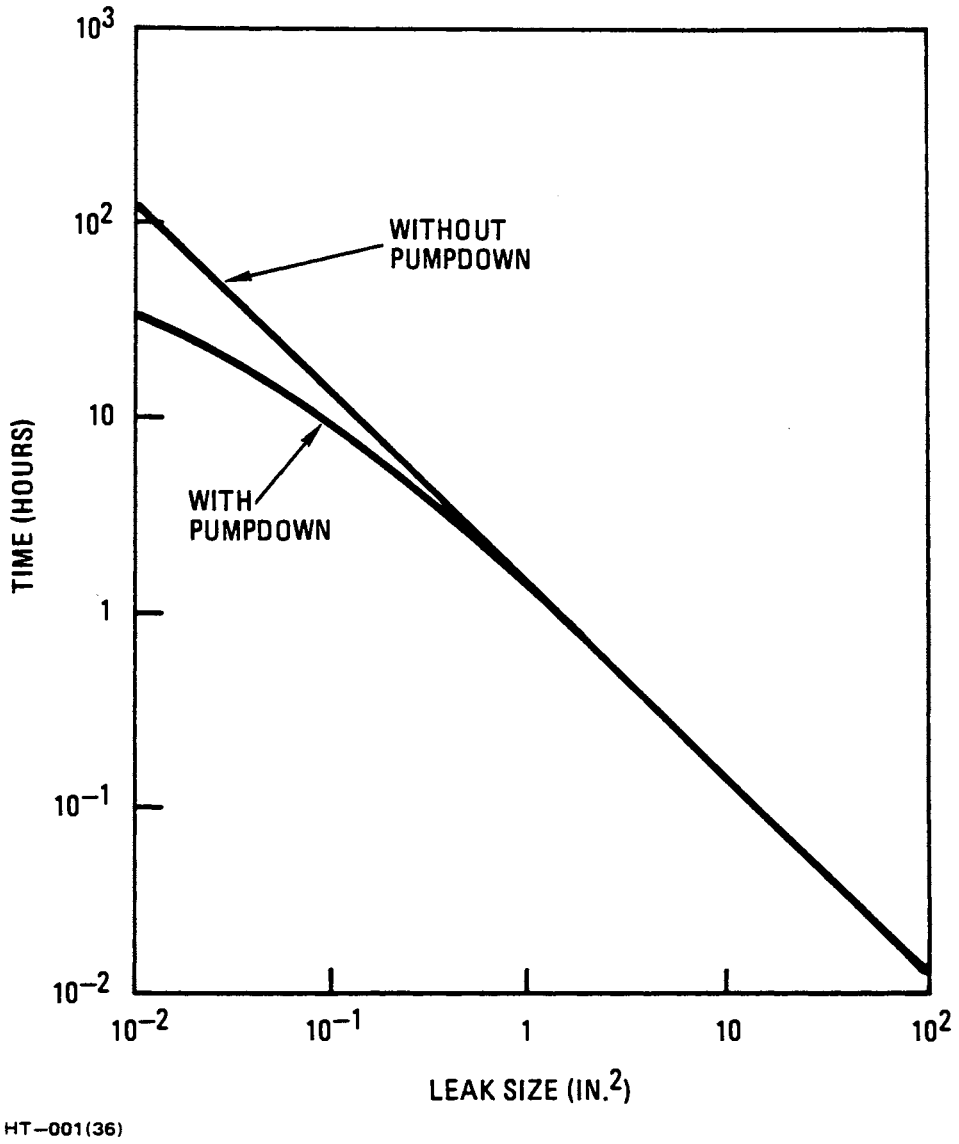
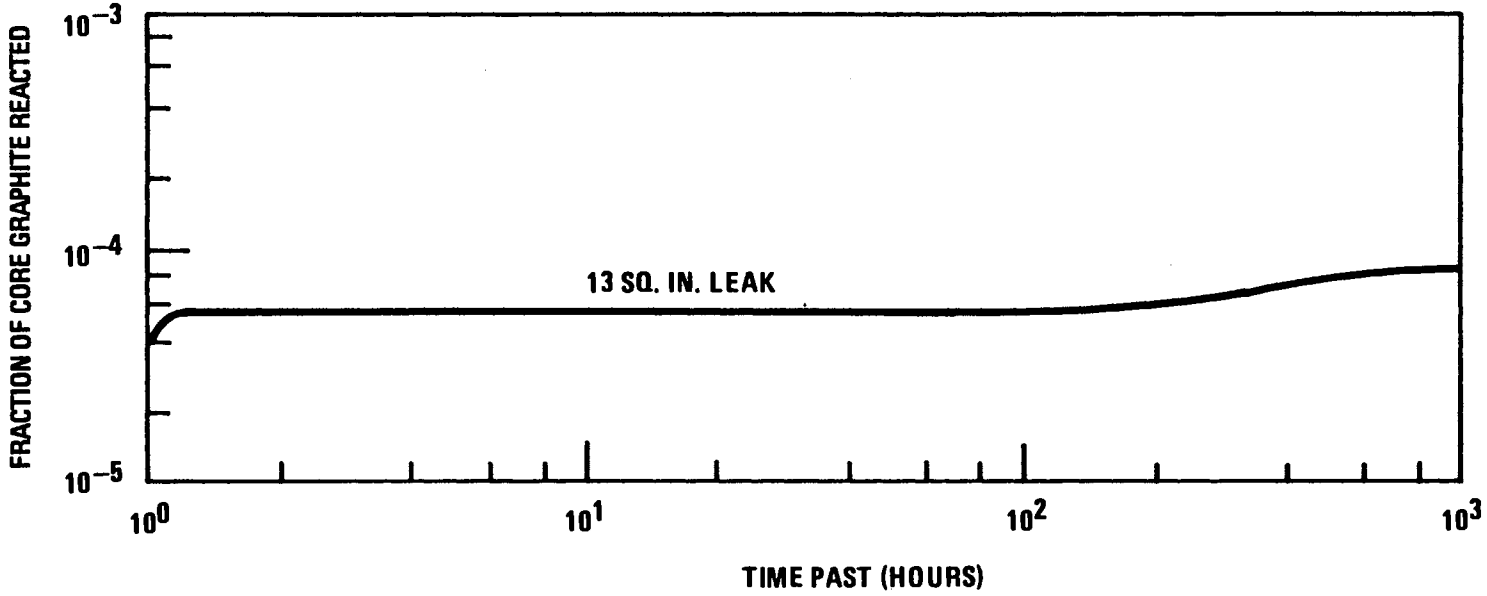


Fig. 6-1. Primary coolant leak depressurization times



HT-001(37)

Fig. 6-2. Limited air graphite reaction retains radionuclides in core

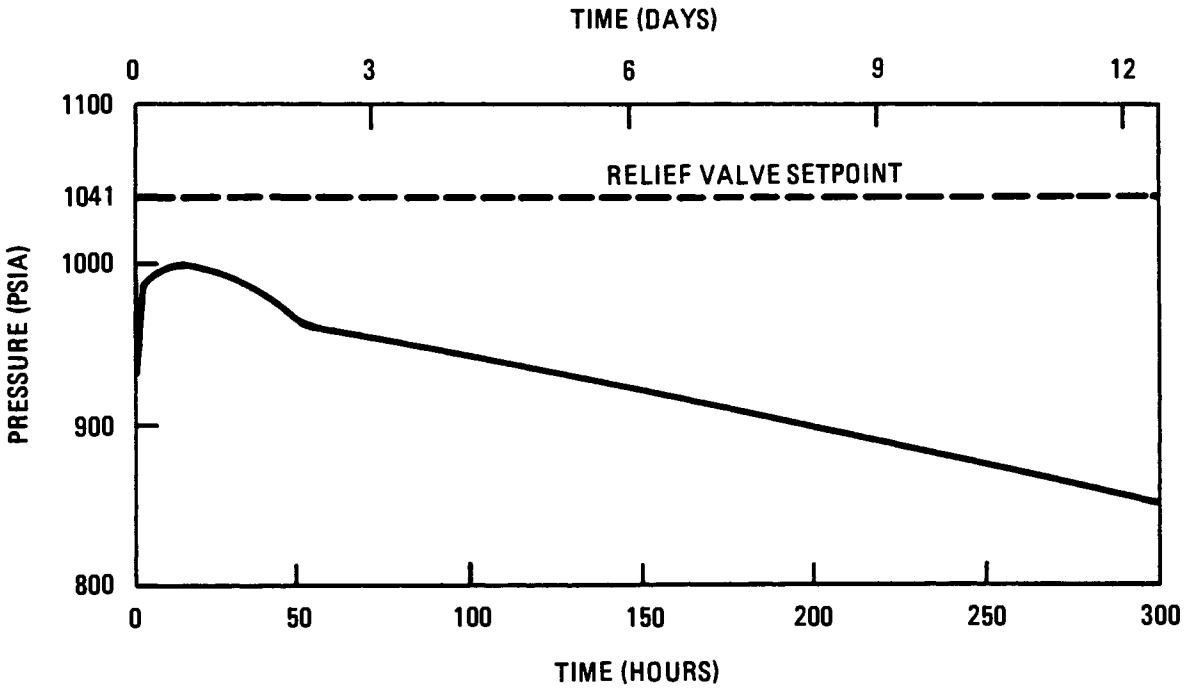


Fig. 6-3. Primary coolant pressure during a pressurized loss of forced circulation

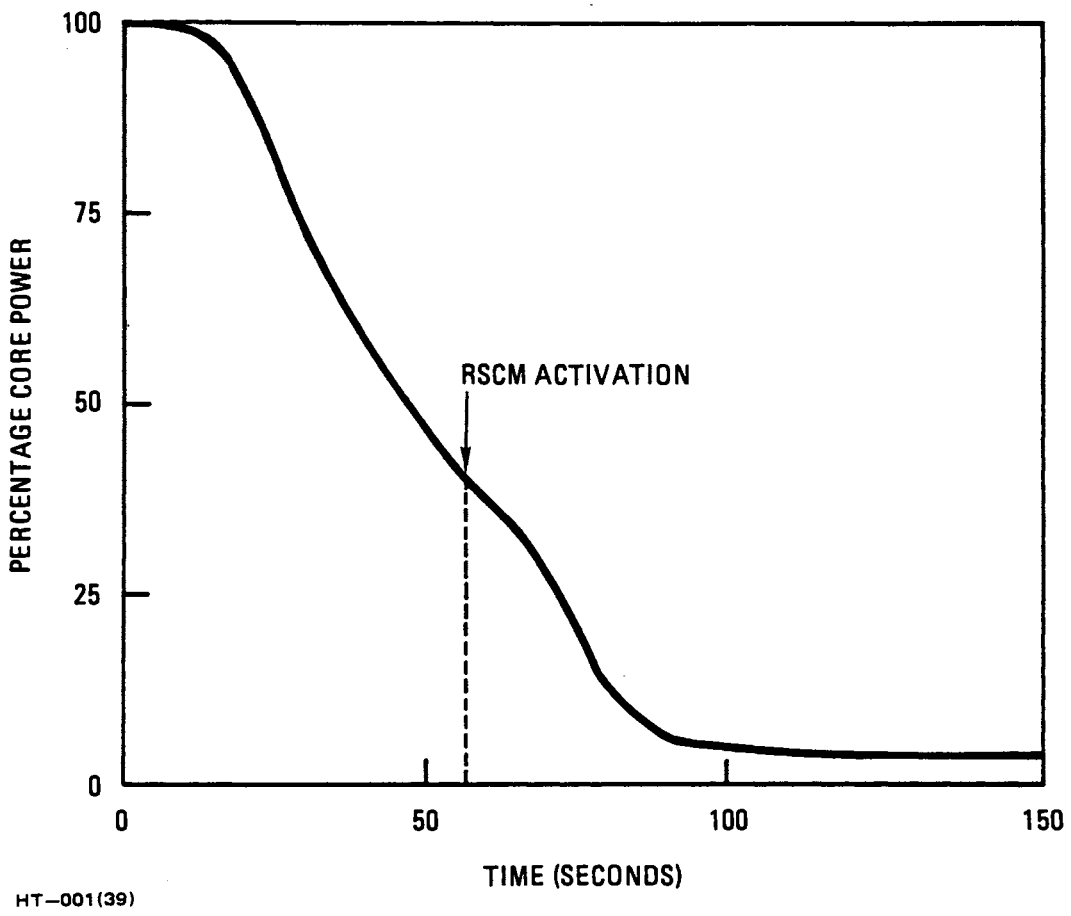


Fig. 6-4. Reactor power following a loss of HTS cooling with failure to insert the outer control rods

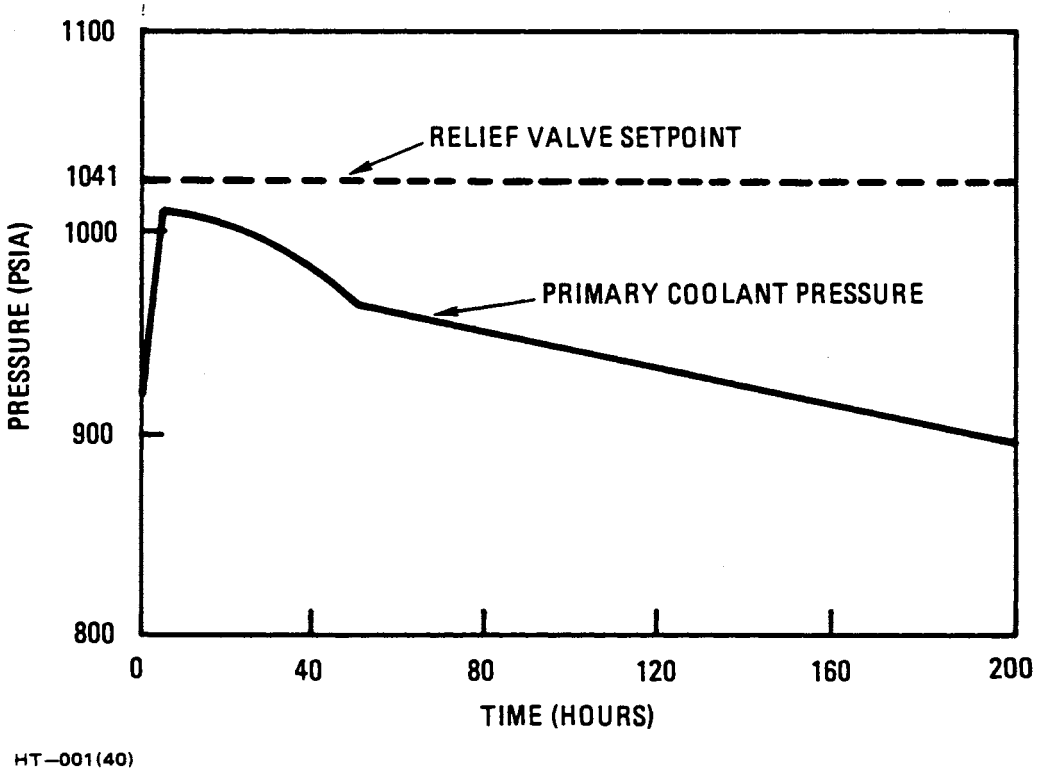


Fig. 6-5. Primary coolant pressure during a pressurized conduction cooldown with reactor trip delayed 56 s

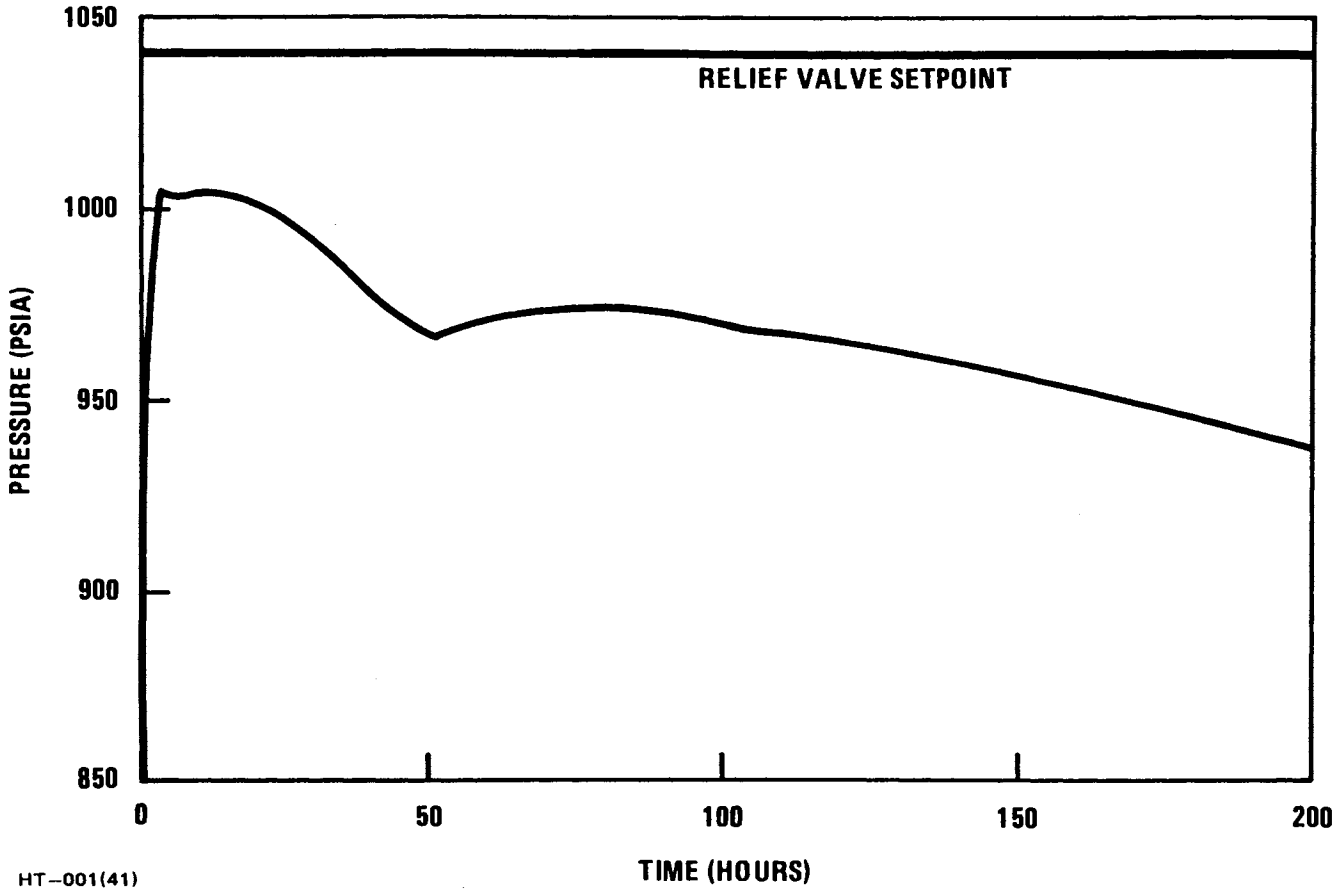


Fig. 6-6. Primary coolant pressure during a pressurized conduction cooldown without reactor trip

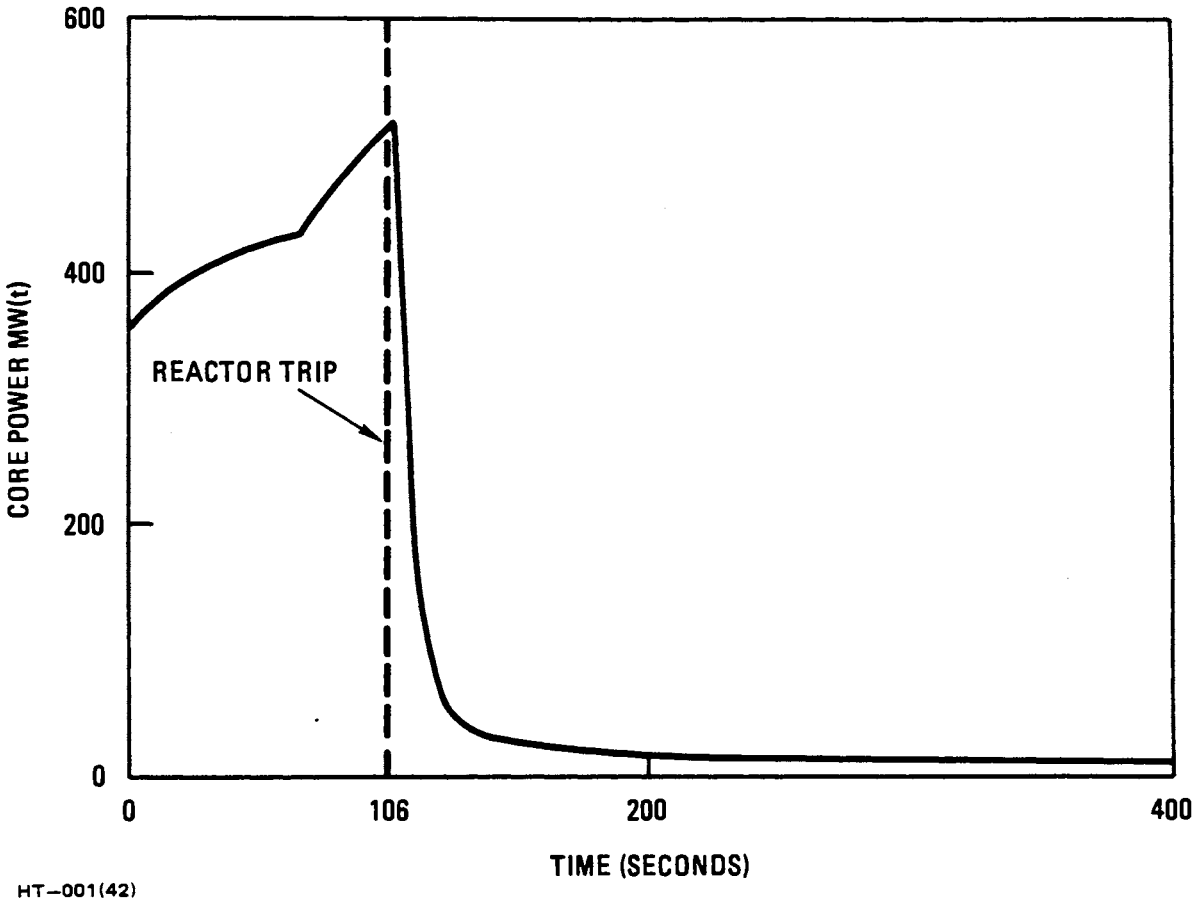


Fig. 6-7. Core power during a rod withdrawal without HTS cooling

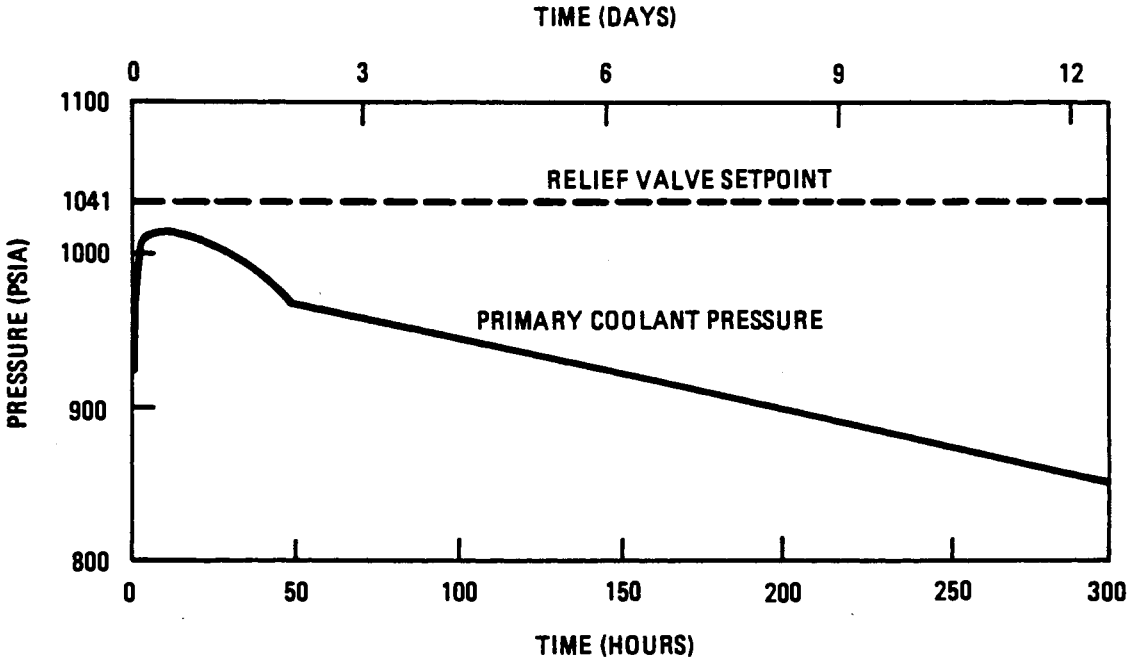


Fig. 6-8. Primary coolant pressure during a rod withdrawal without HTS and without SCS cooling

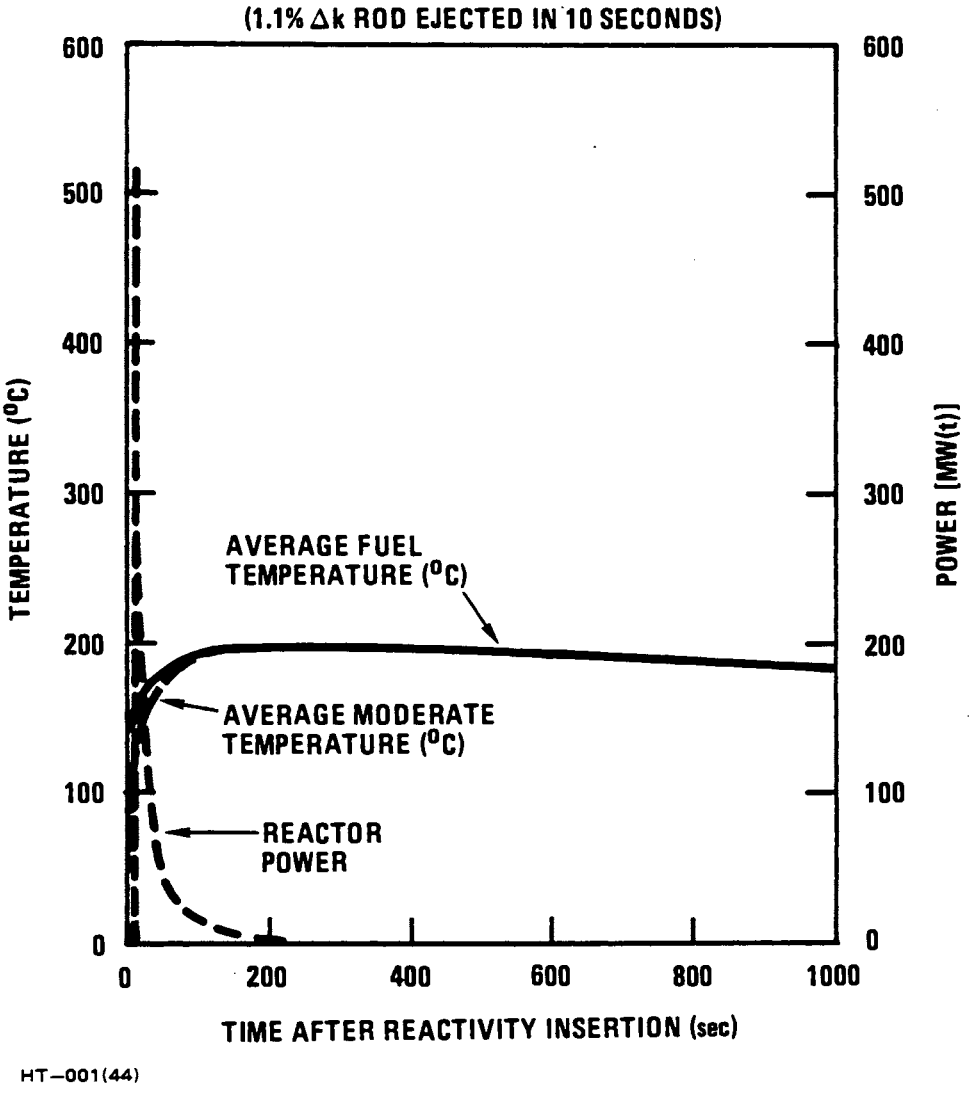


Fig. 6-9. Hypothetical control rod ejection from zero power without scram

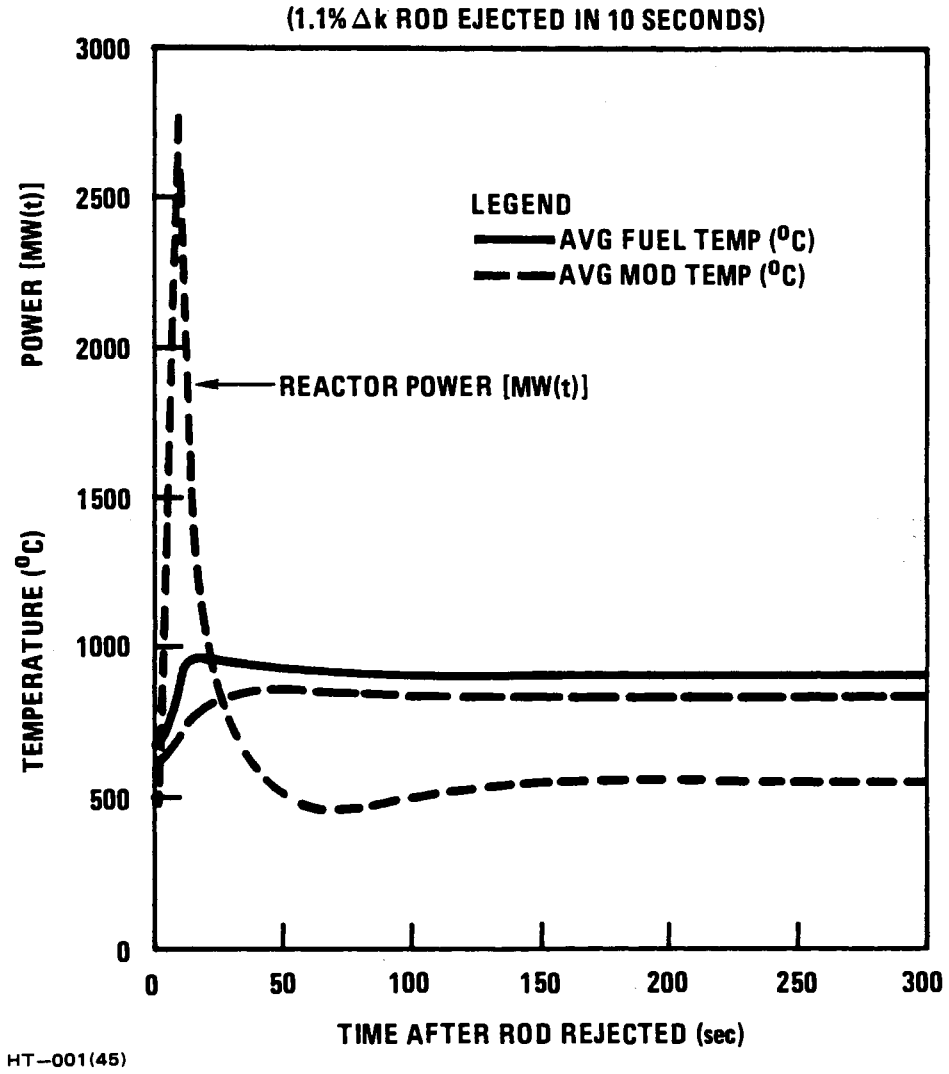


Fig. 6-10. Hypothetical control rod ejection at power without scram

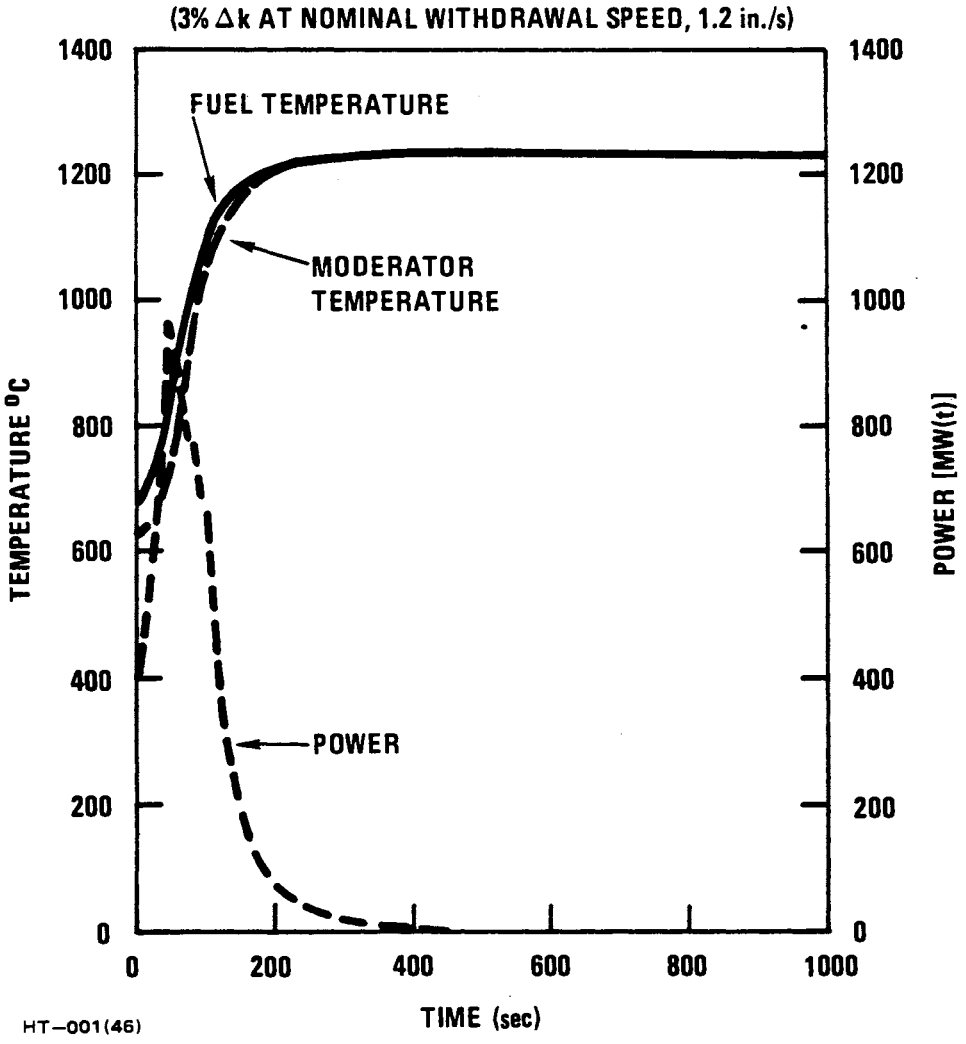


Fig. 6-11. Hypothetical removal of all control rods at full power without scram

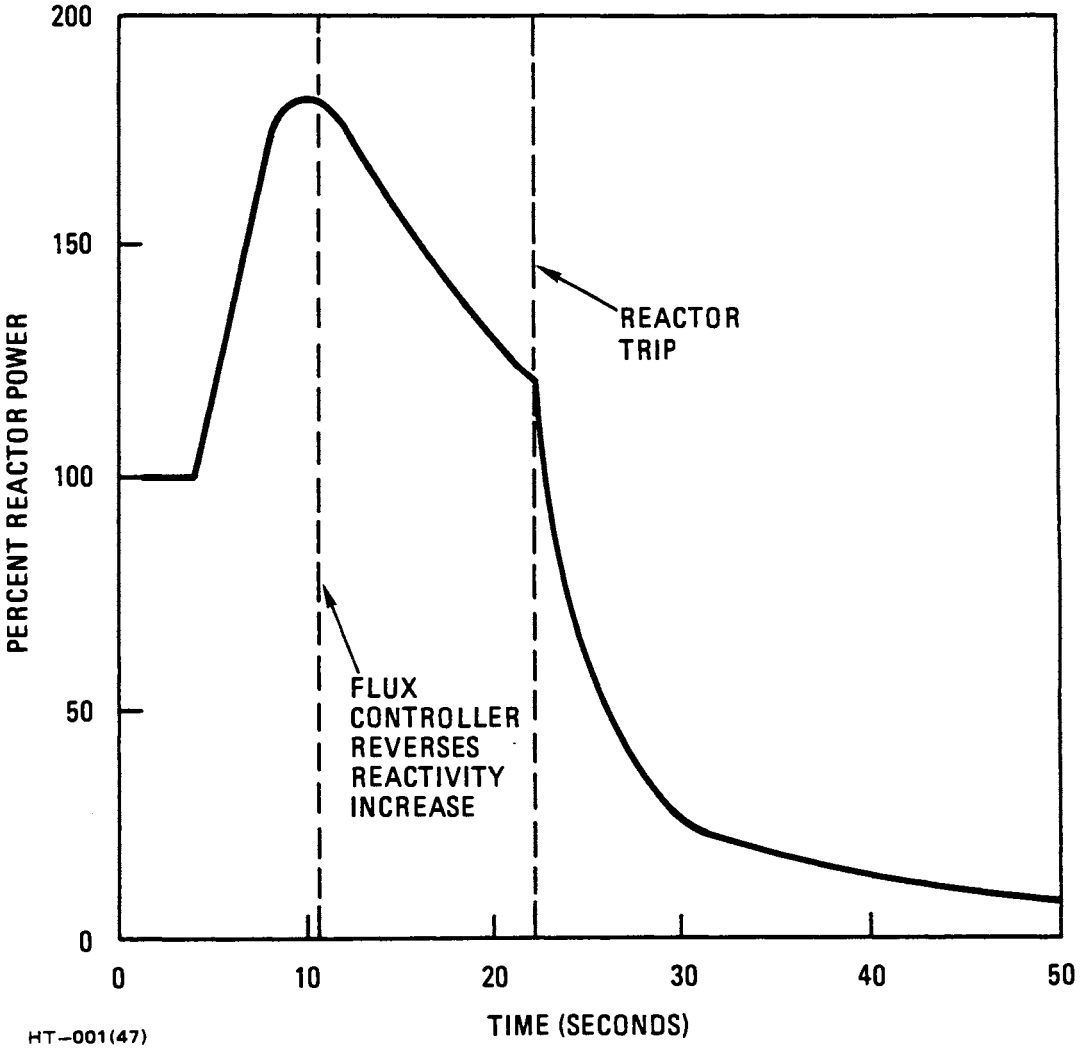


Fig. 6-12. Core power during a moderate moisture ingress event without a normal plant response

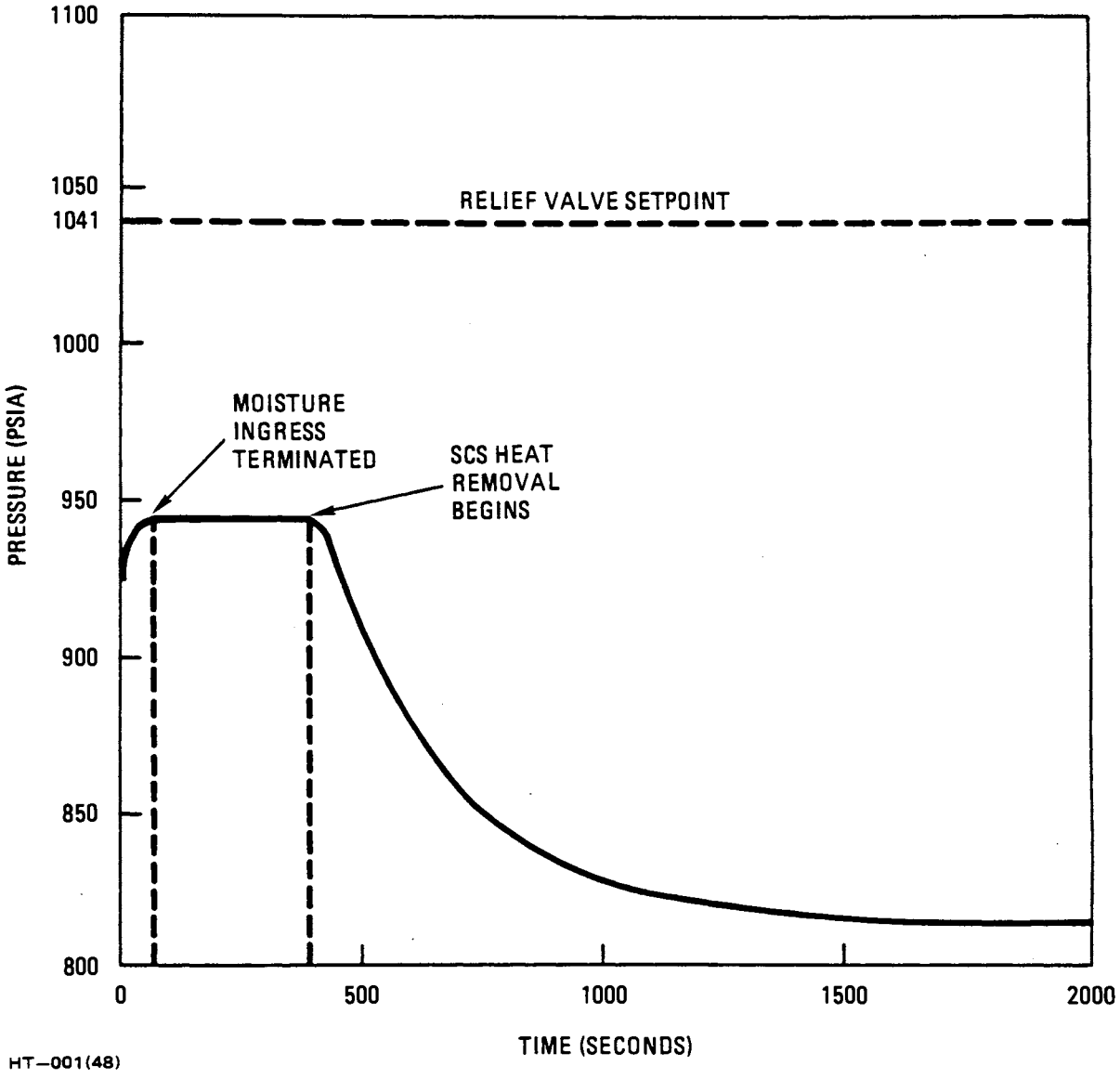


Fig. 6-13. Primary coolant pressure during a moderate moisture ingress event with a normal plant response

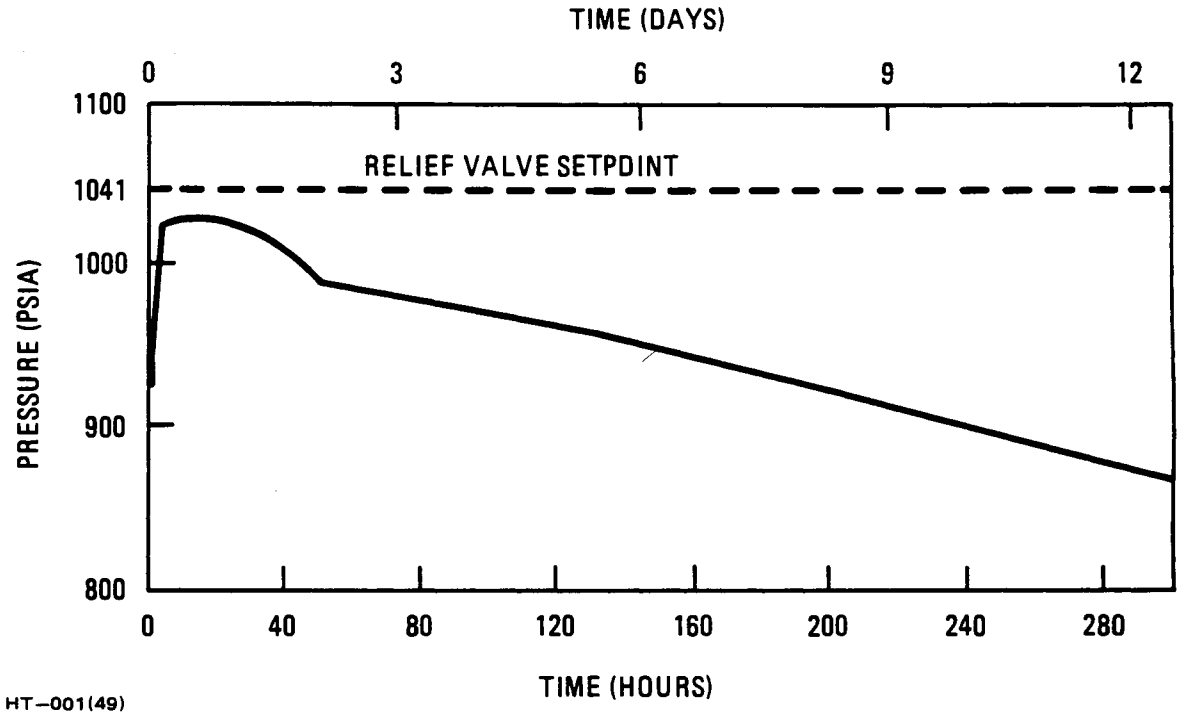


Fig. 6-14. Primary coolant pressure during a moderate moisture ingress event with moisture monitor and forced cooling failure

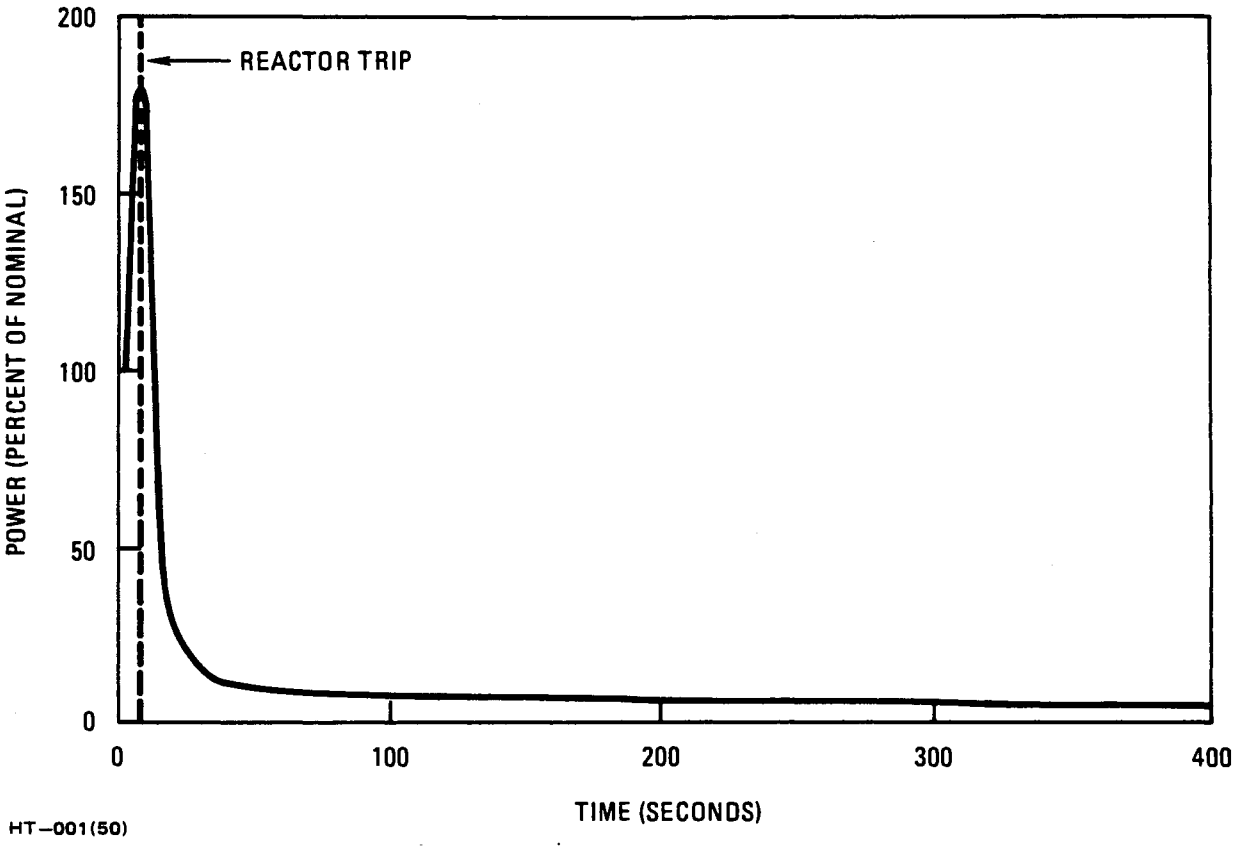


Fig. 6-15. Core power during a moderate moisture ingress event without forced cooling

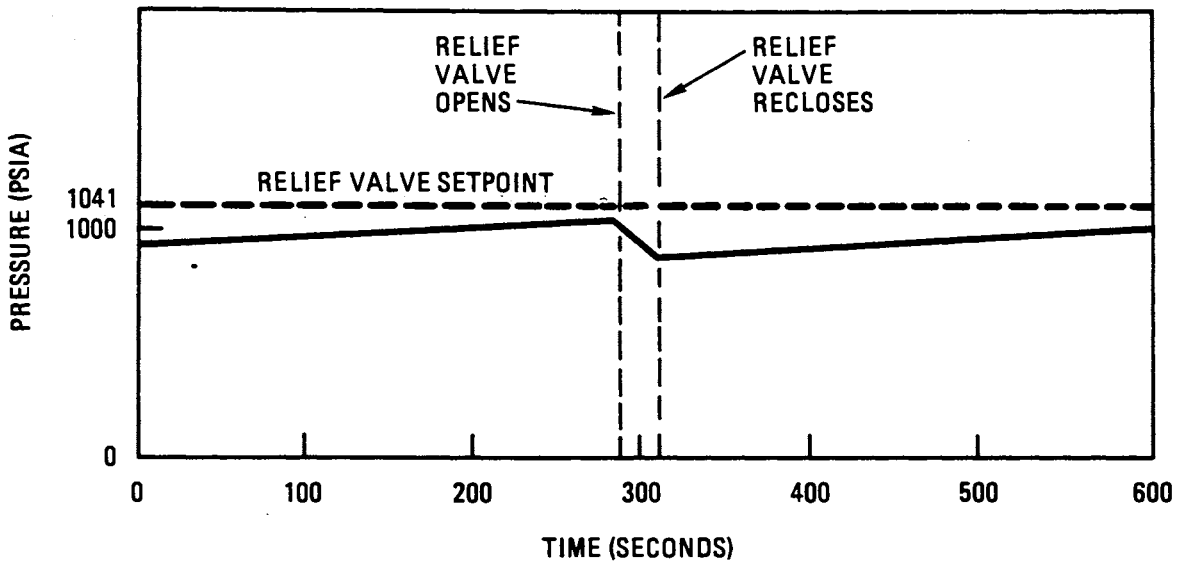


Fig. 6-16. Primary coolant pressure during a moderate moisture ingress event with moisture monitor and forced cooling failure

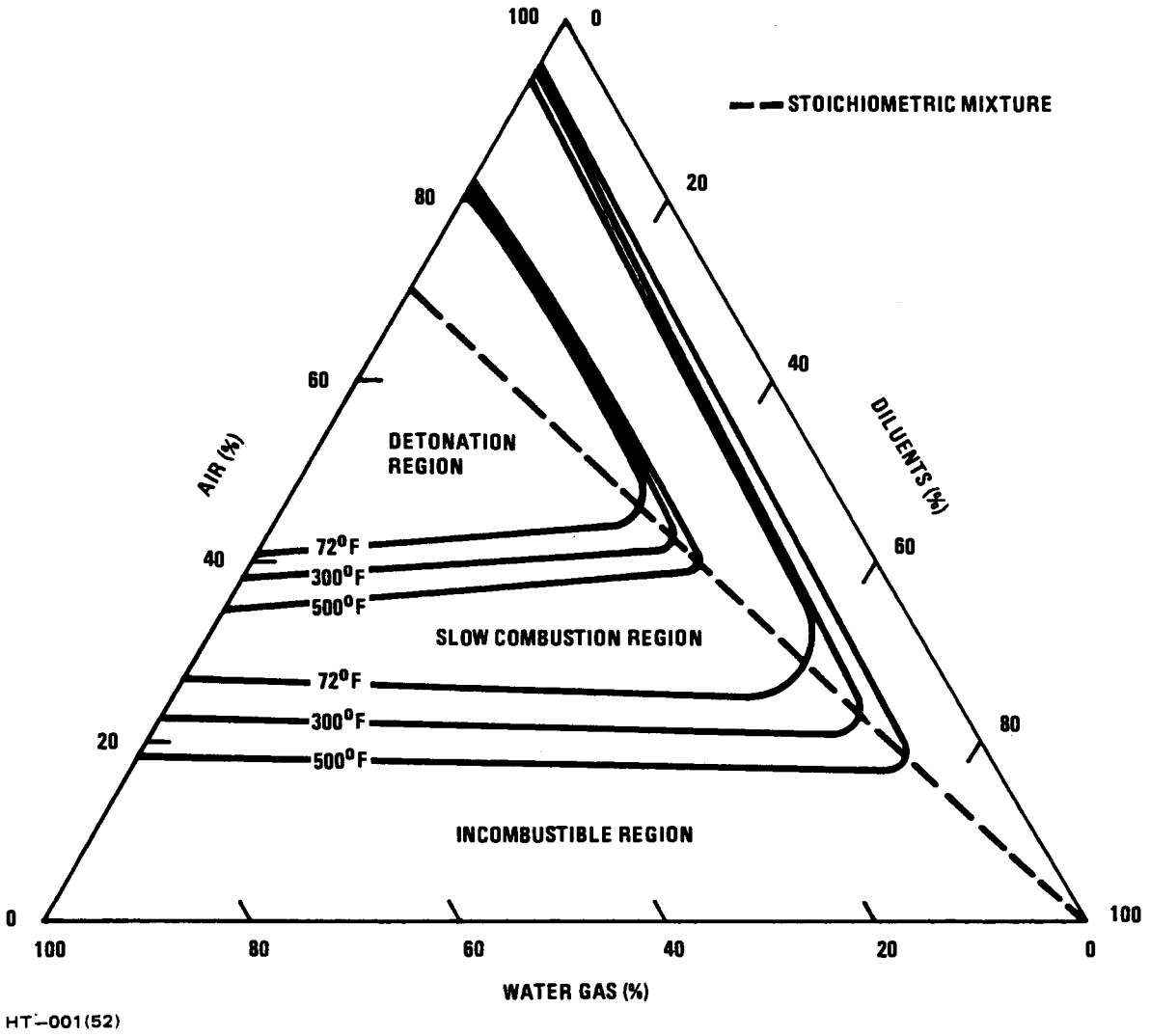


Fig. 6-17. Limit of flammability and detonability for water gas

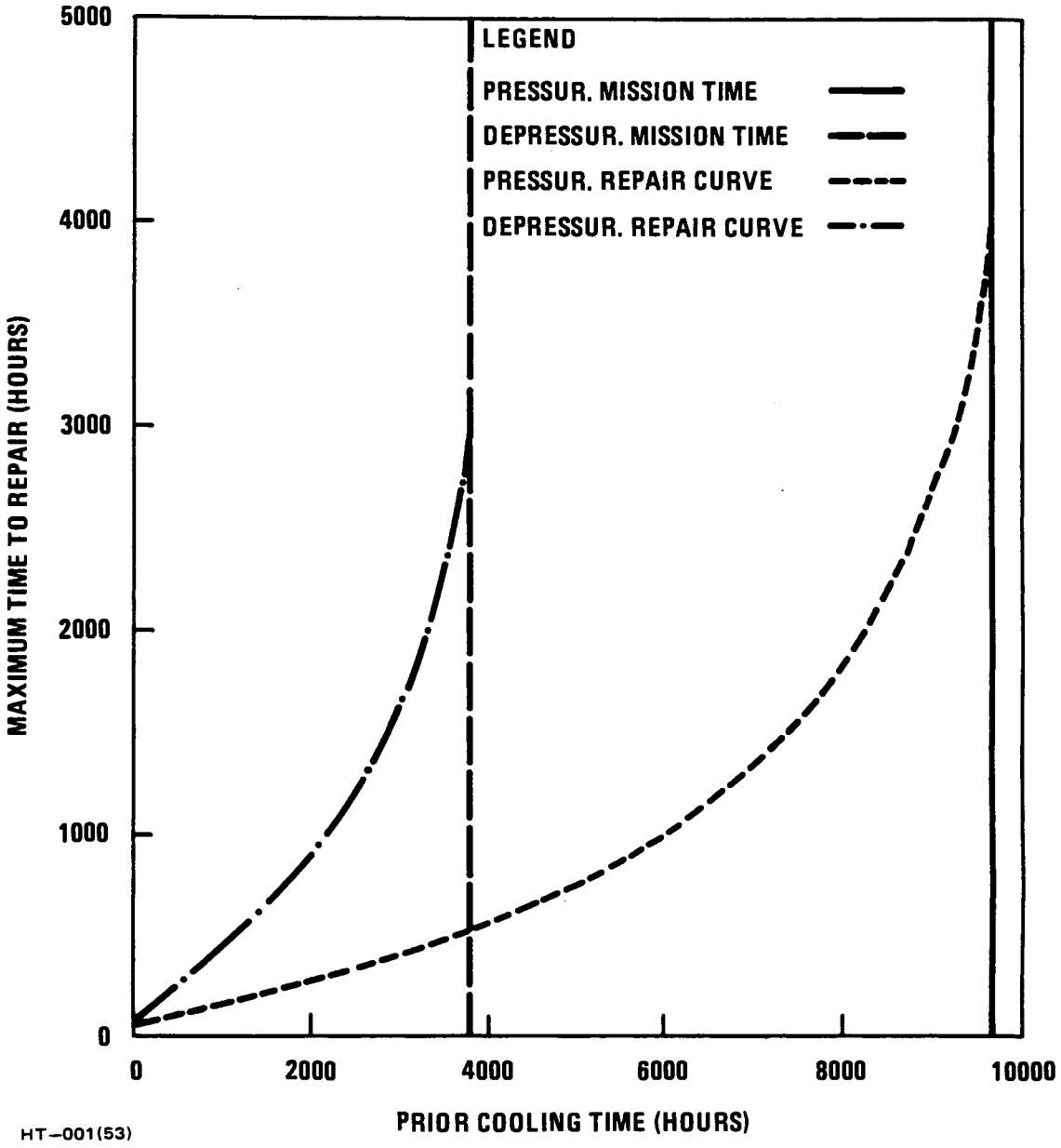
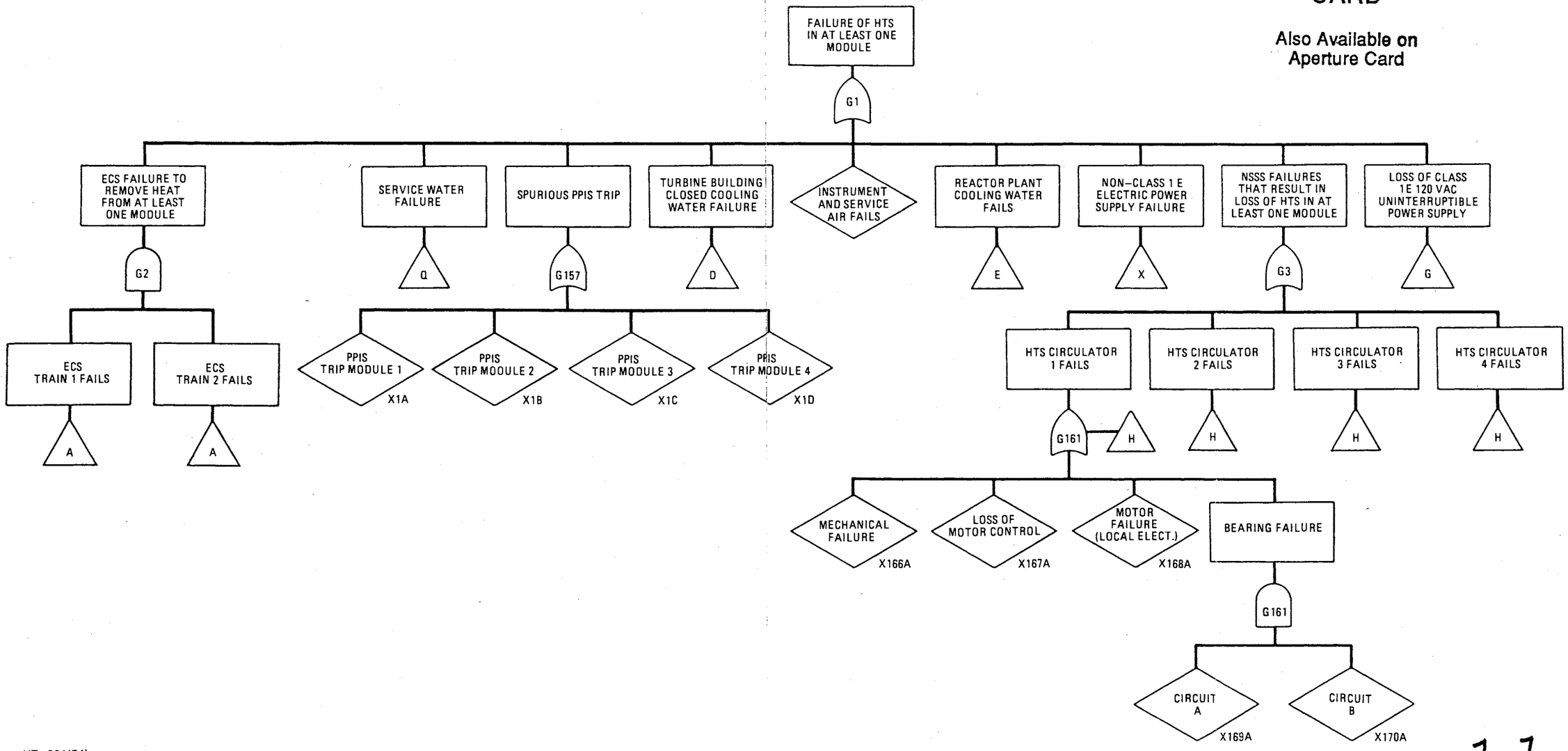


Fig. 6-18. HTS, SCS, and RCCS repair curves for MHTGR under pressurized and depressurized conduction cooling



HT–001(54)

Fig. 6-19. Top-level fault tree for loss of HTS cooling

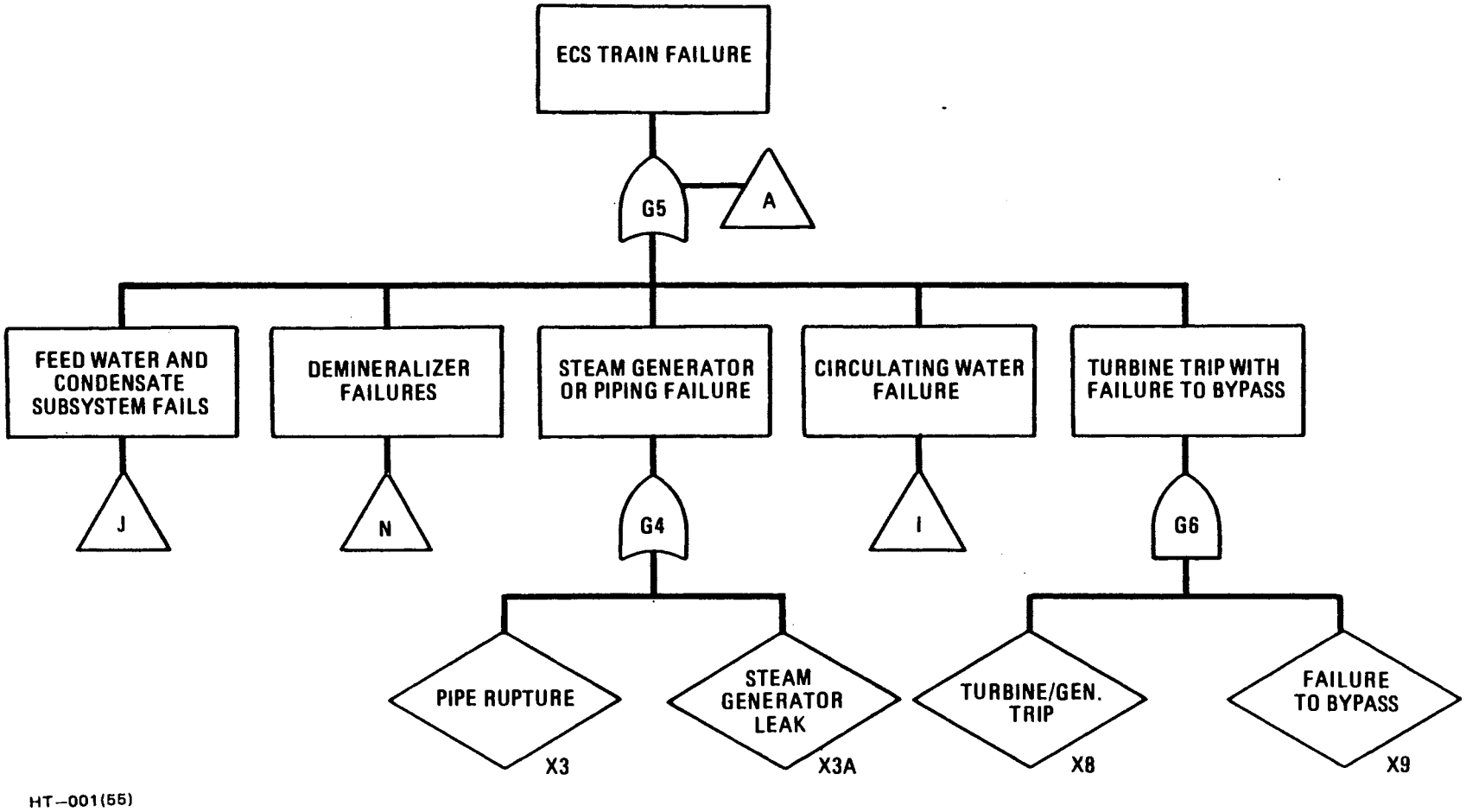


Fig. 6-20. Fault tree for loss of the energy conversion system

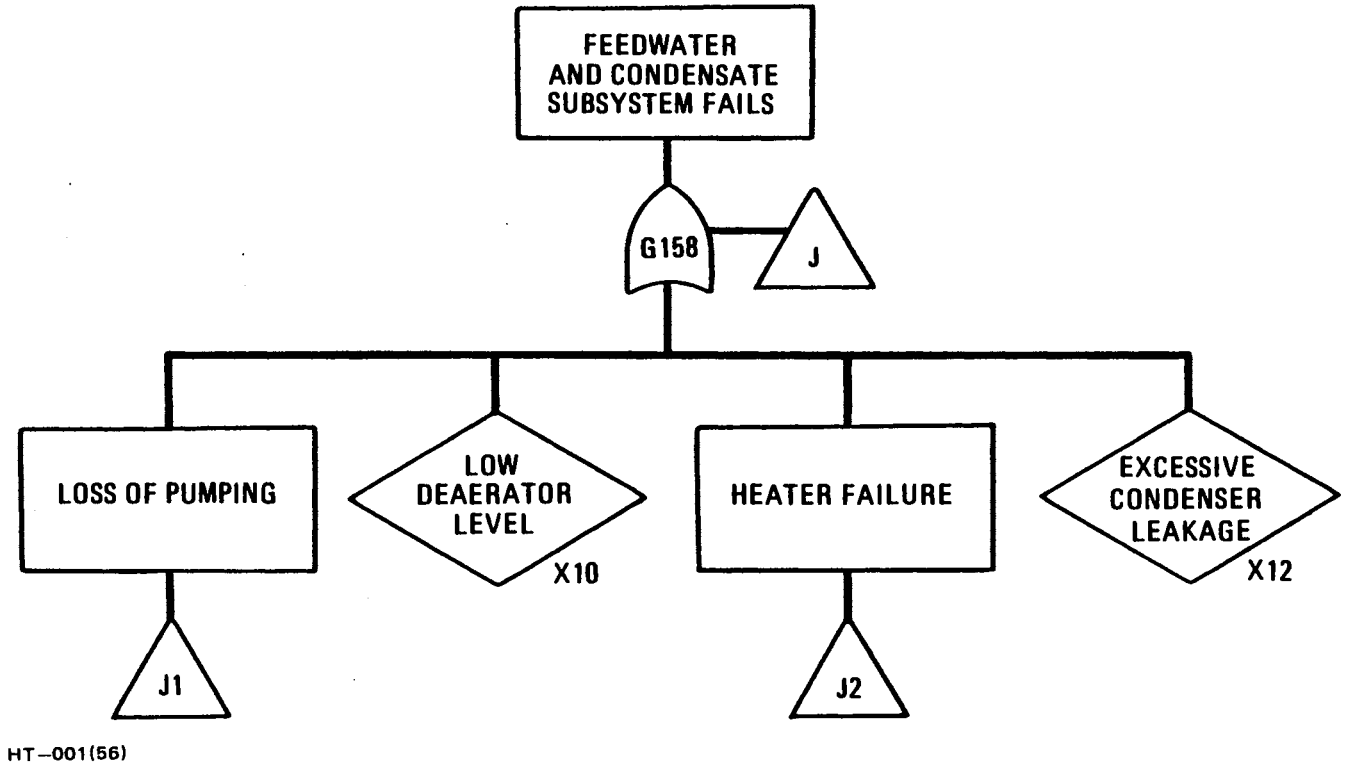


Fig. 6-21. Fault tree for loss of the feedwater and condensate subsystem

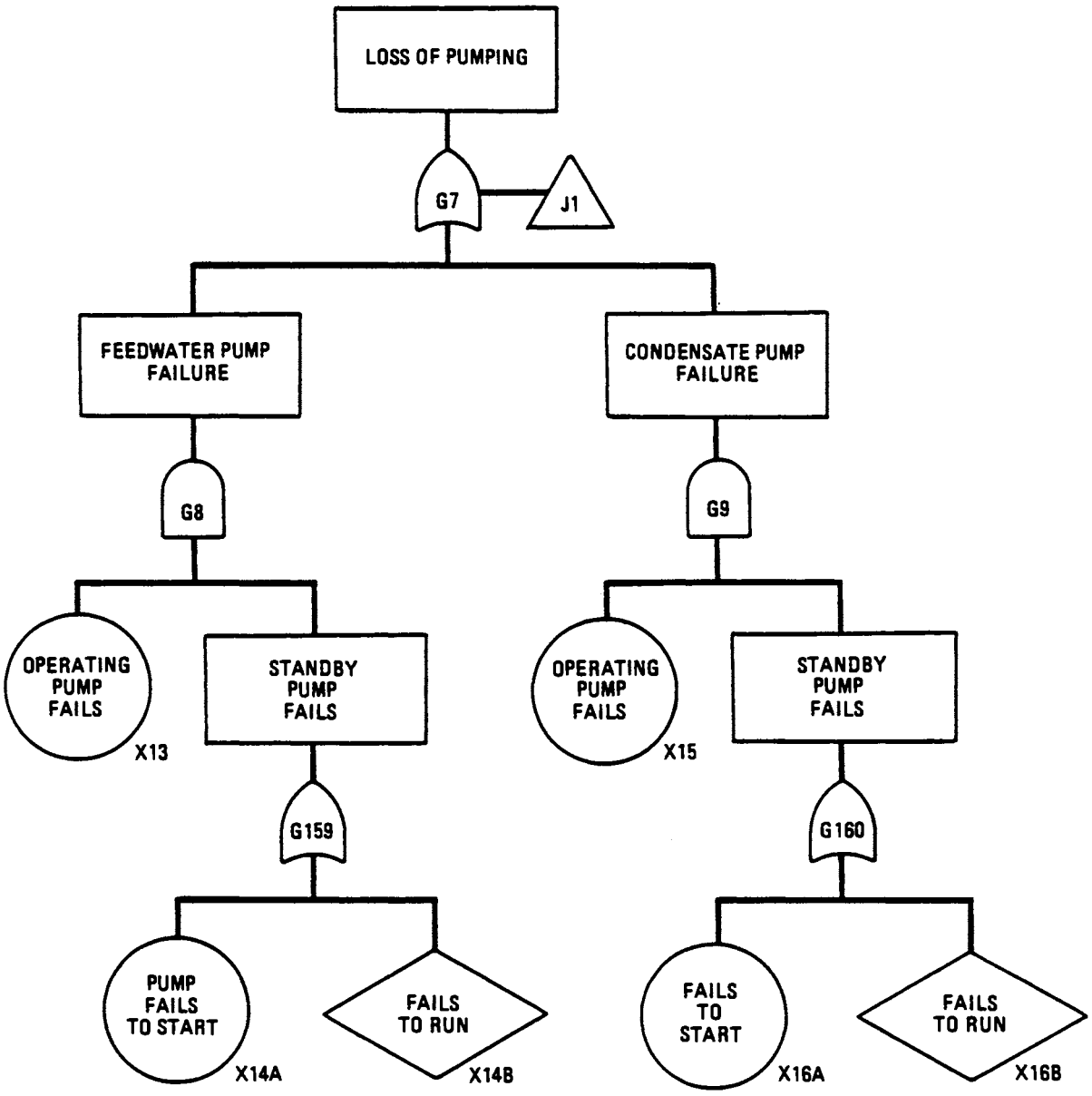
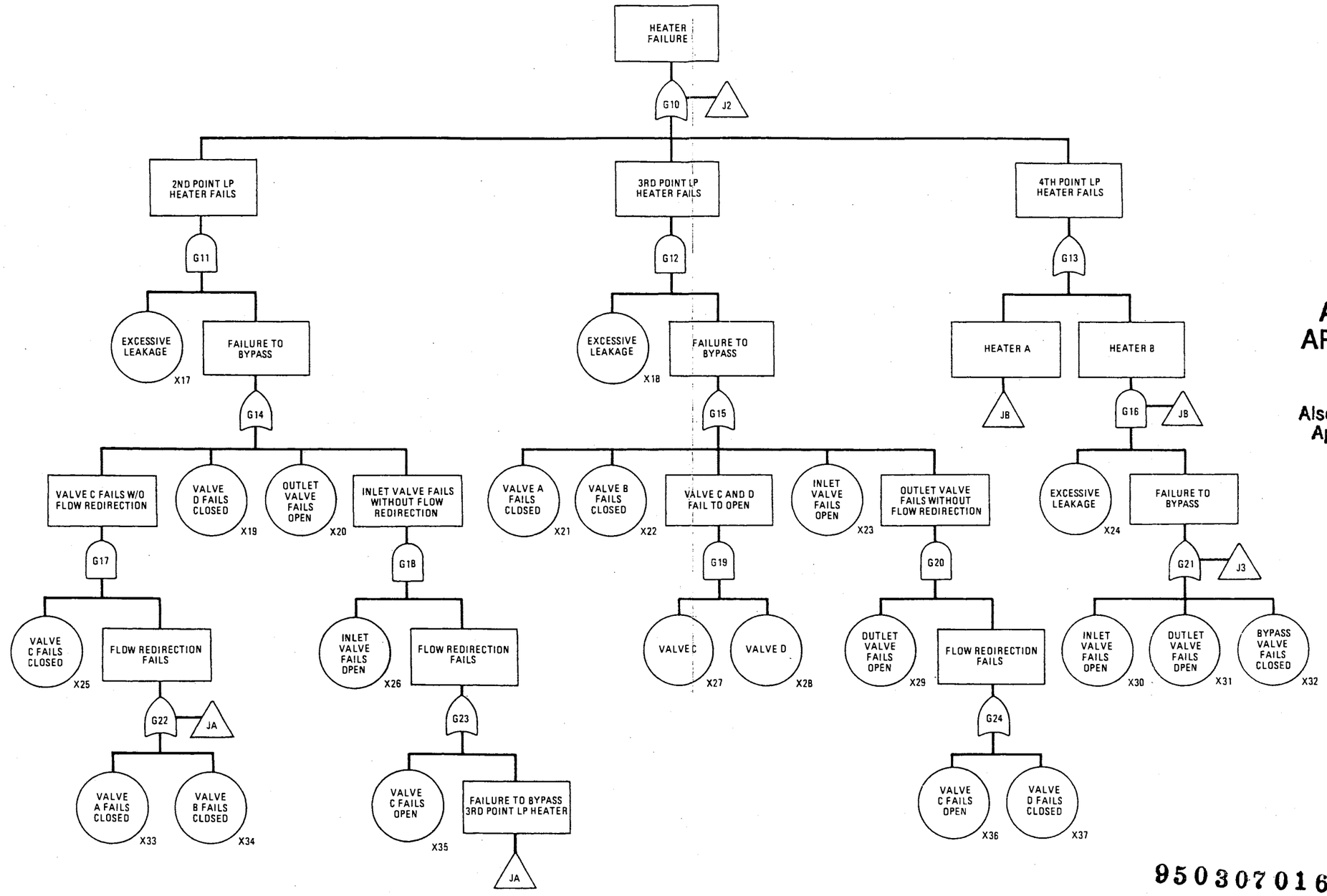


Fig. 6-22. Subtree J1 for loss of pumping



HT-001(58)

Fig. 6-23. Subtree J2 for heater failure

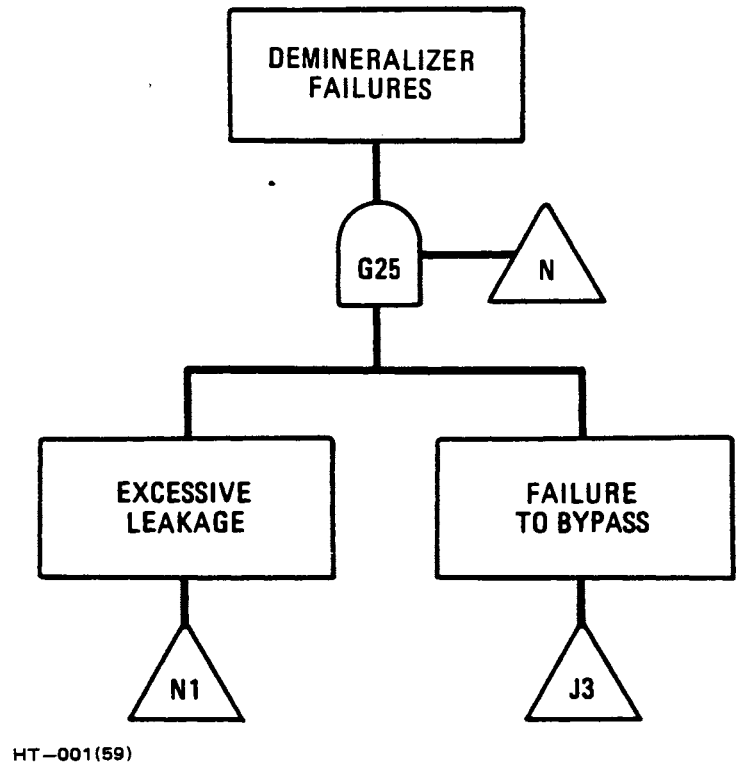


Fig. 6-24. Fault tree for demineralizer failure

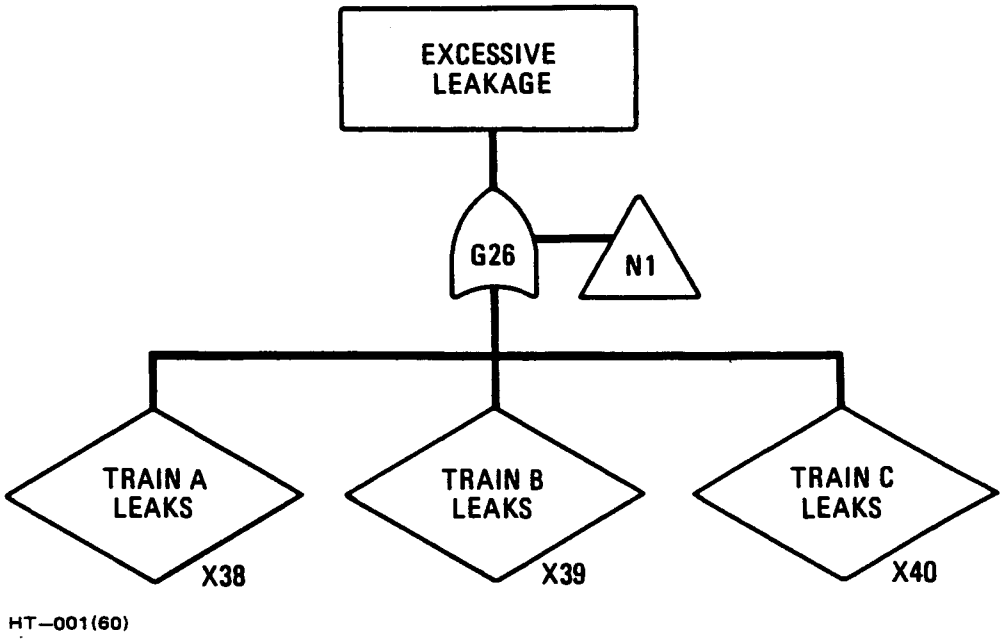


Fig. 6-25. Subtree N1 for excessive leakage

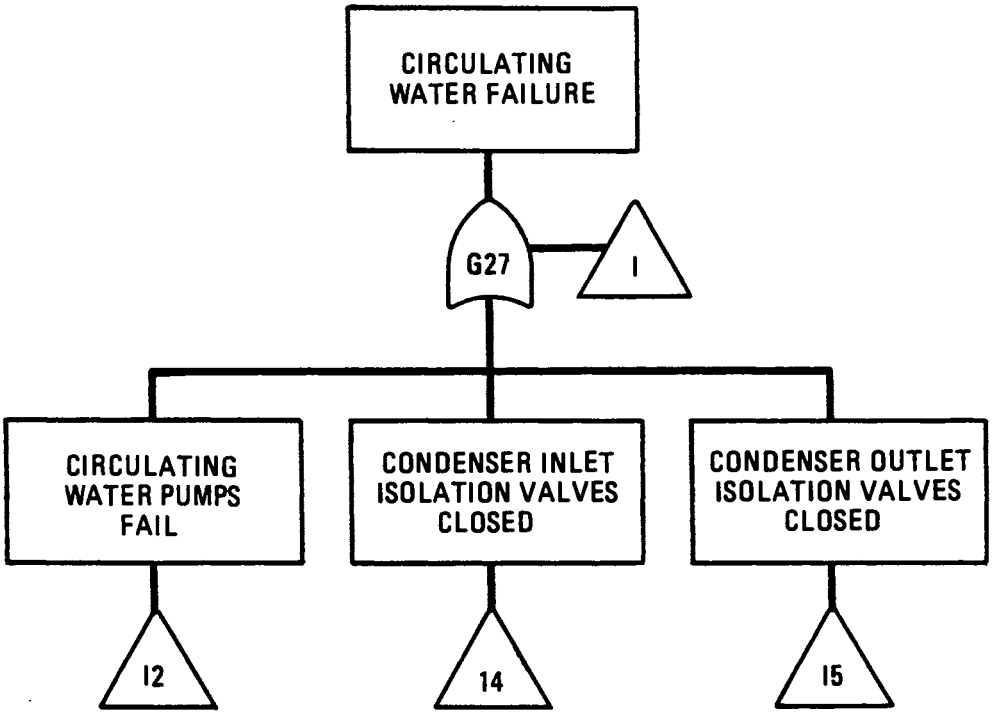
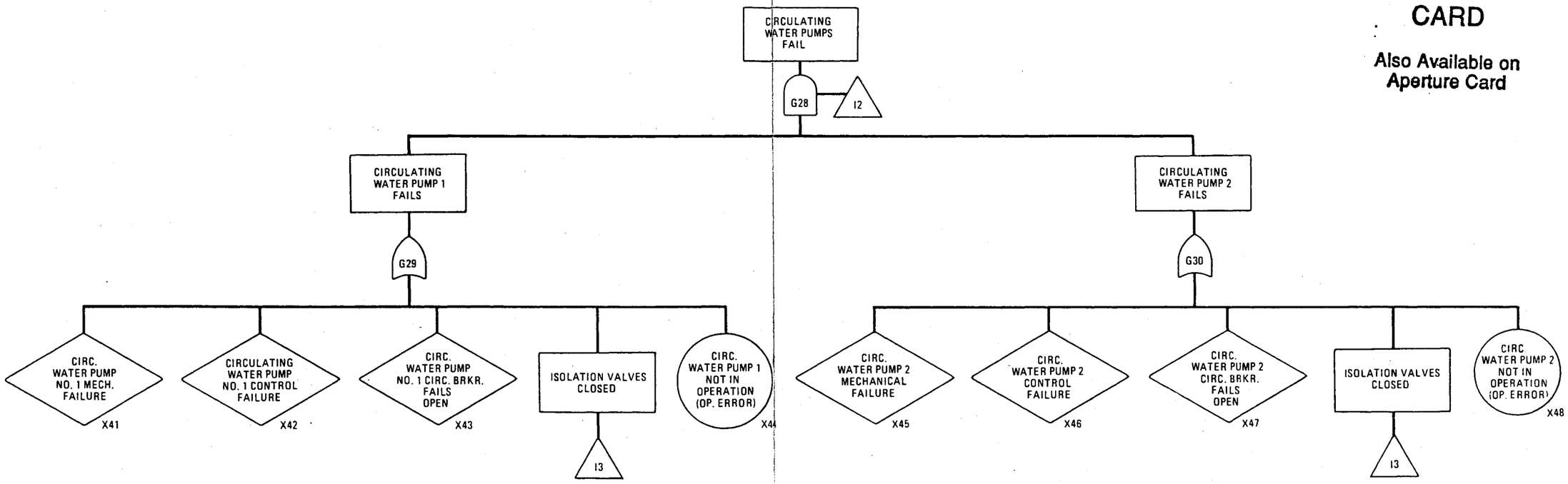


Fig. 6-26. Fault tree for circulating water subsystem failure



HT-001(62)

9503070161 - 13

Fig. 6-27. Subtree I2 for circulating water pump failure

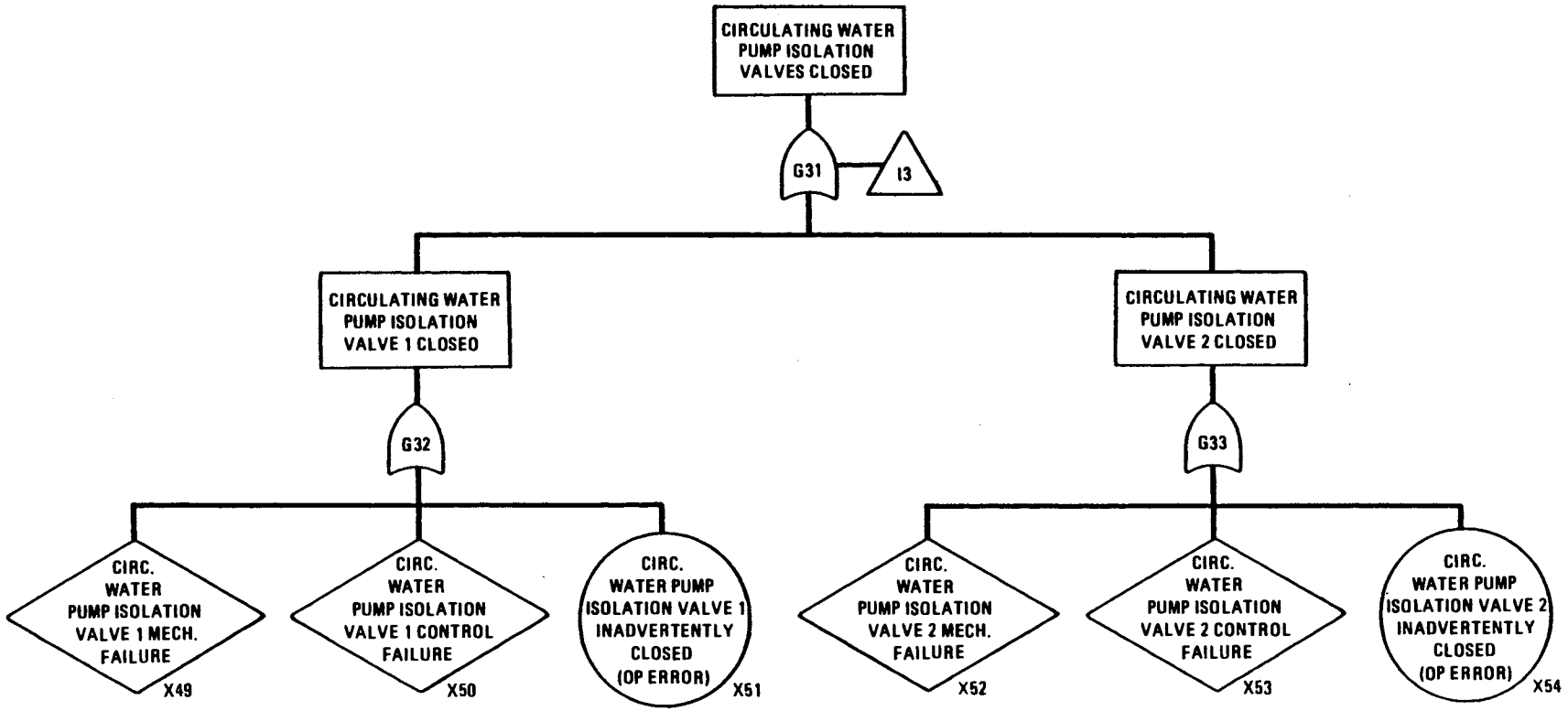


Fig. 6-28. Subtree I3 for pump isolation valve failure

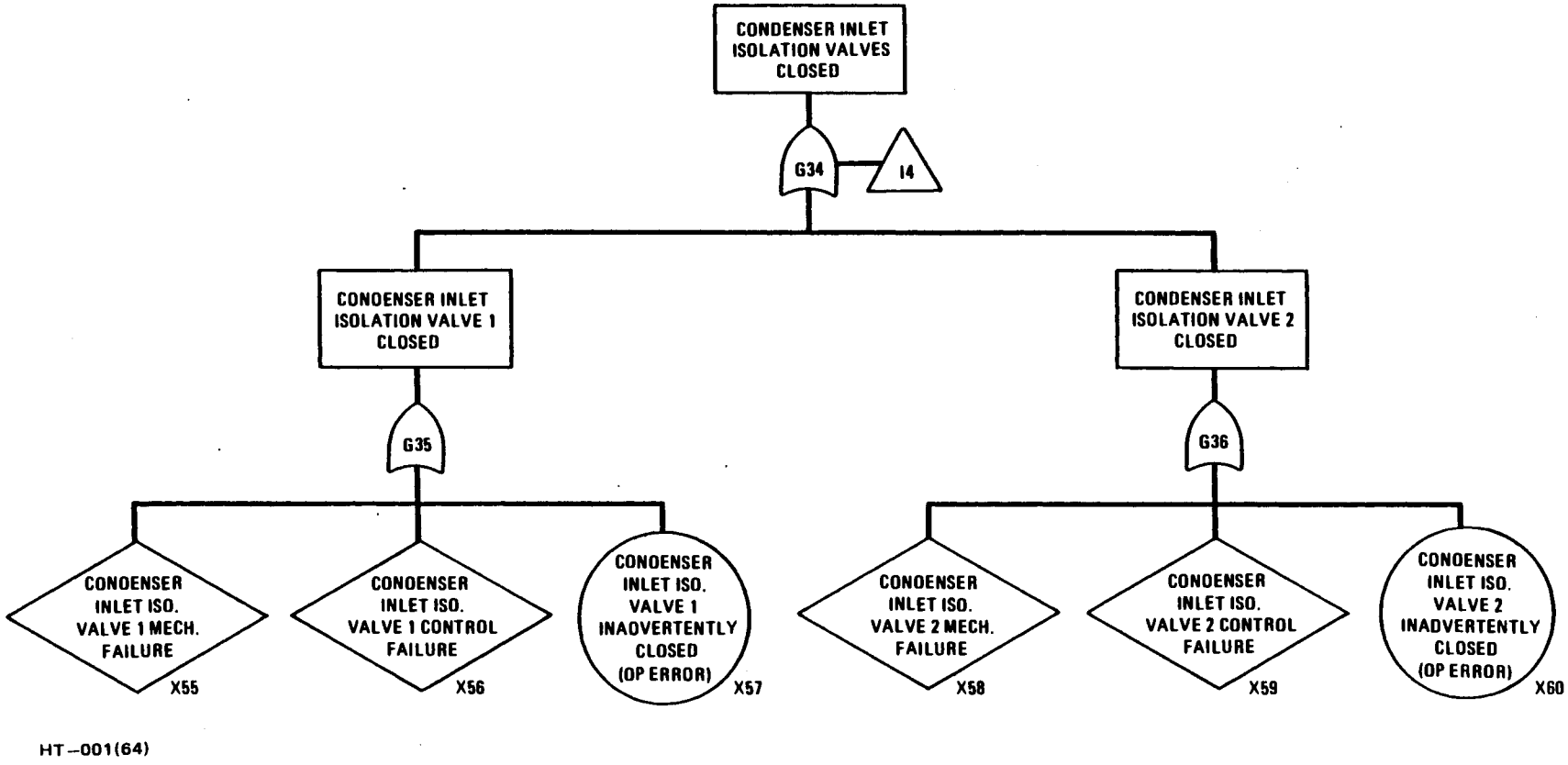


Fig. 6-29. Subtree I4 for condenser inlet isolation valve failure

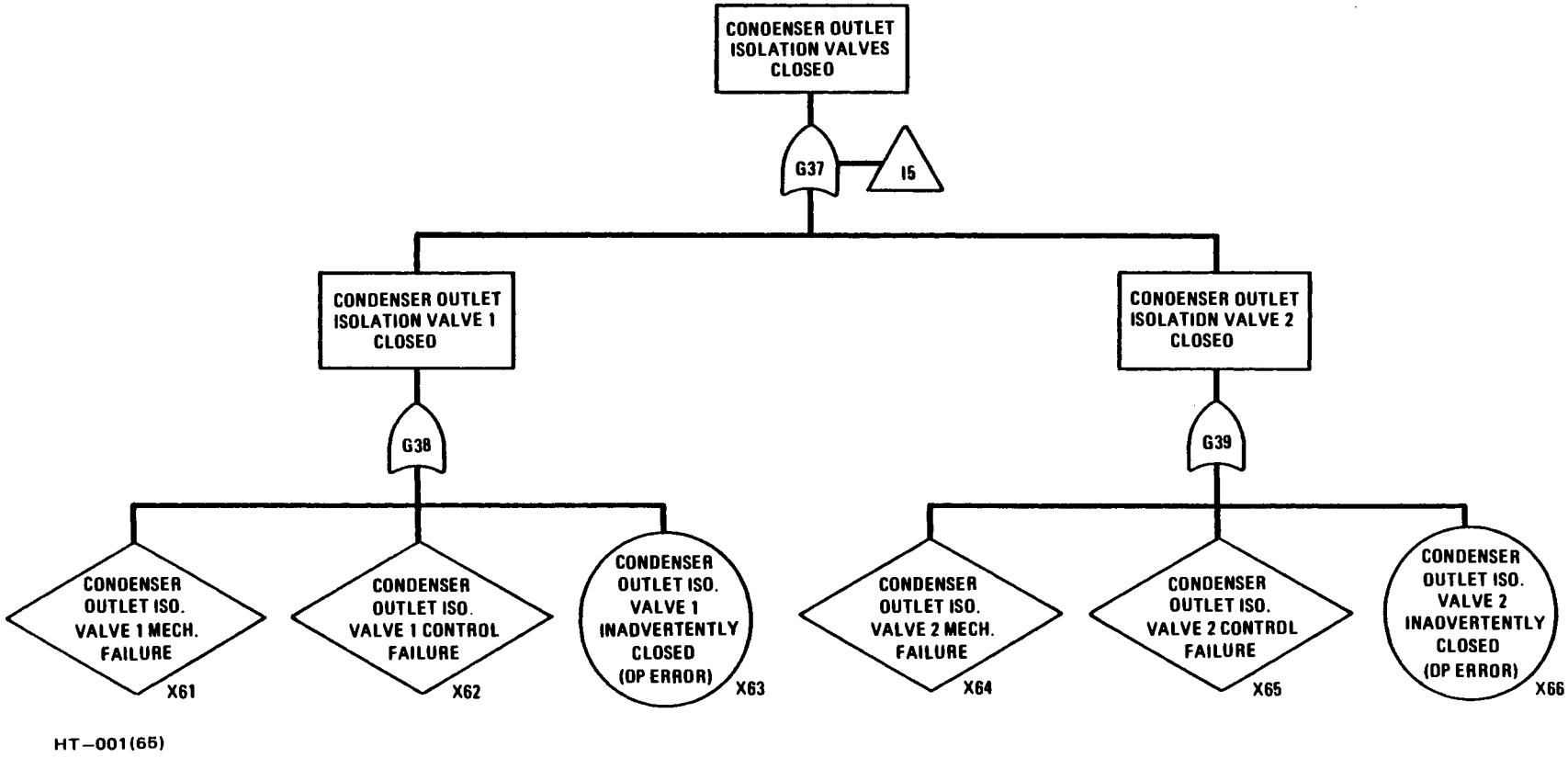


Fig. 6-30. Subtree I5 for condenser outlet isolation valve failure

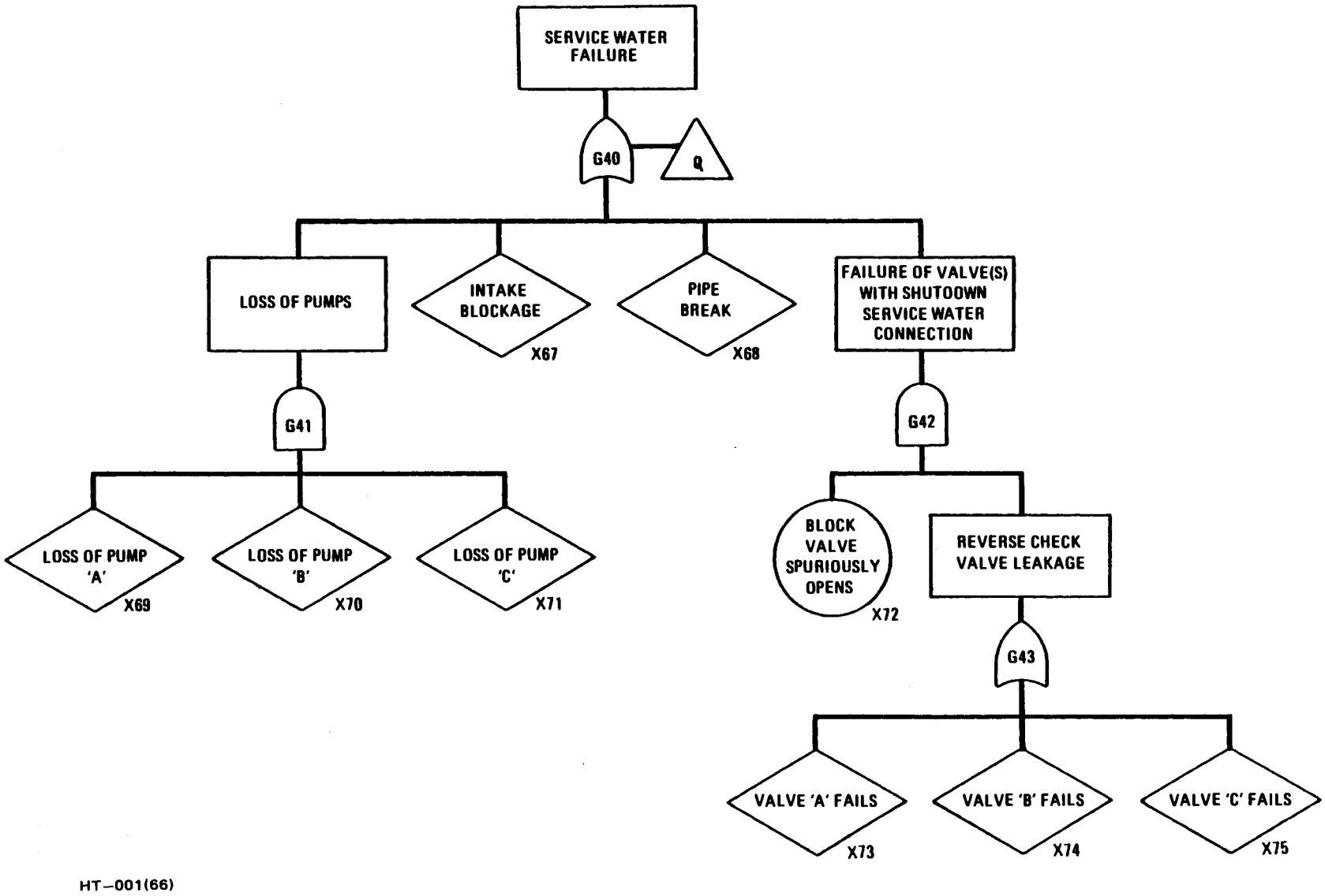


Fig. 6-31. Fault tree for service water subsystem failure

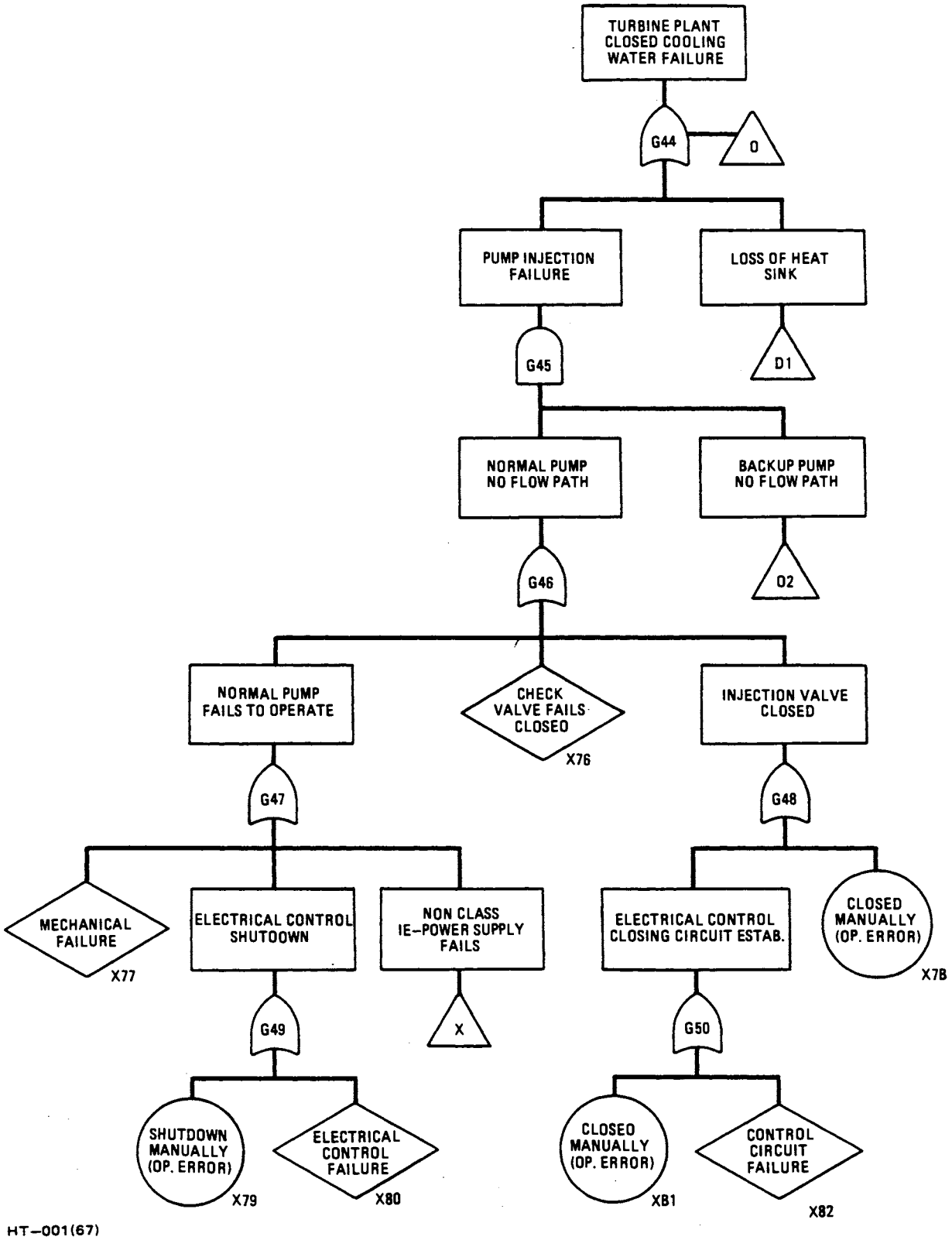
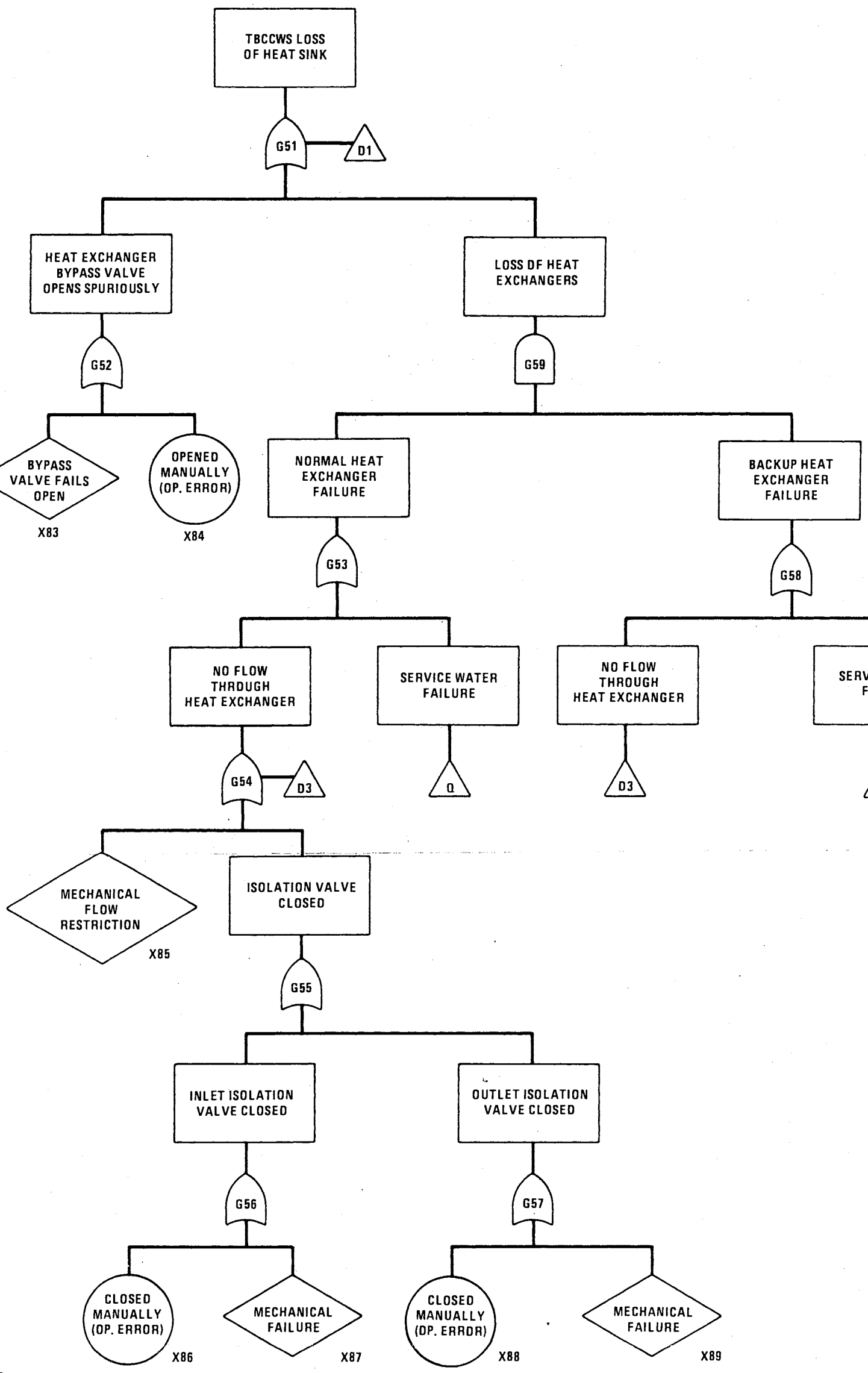
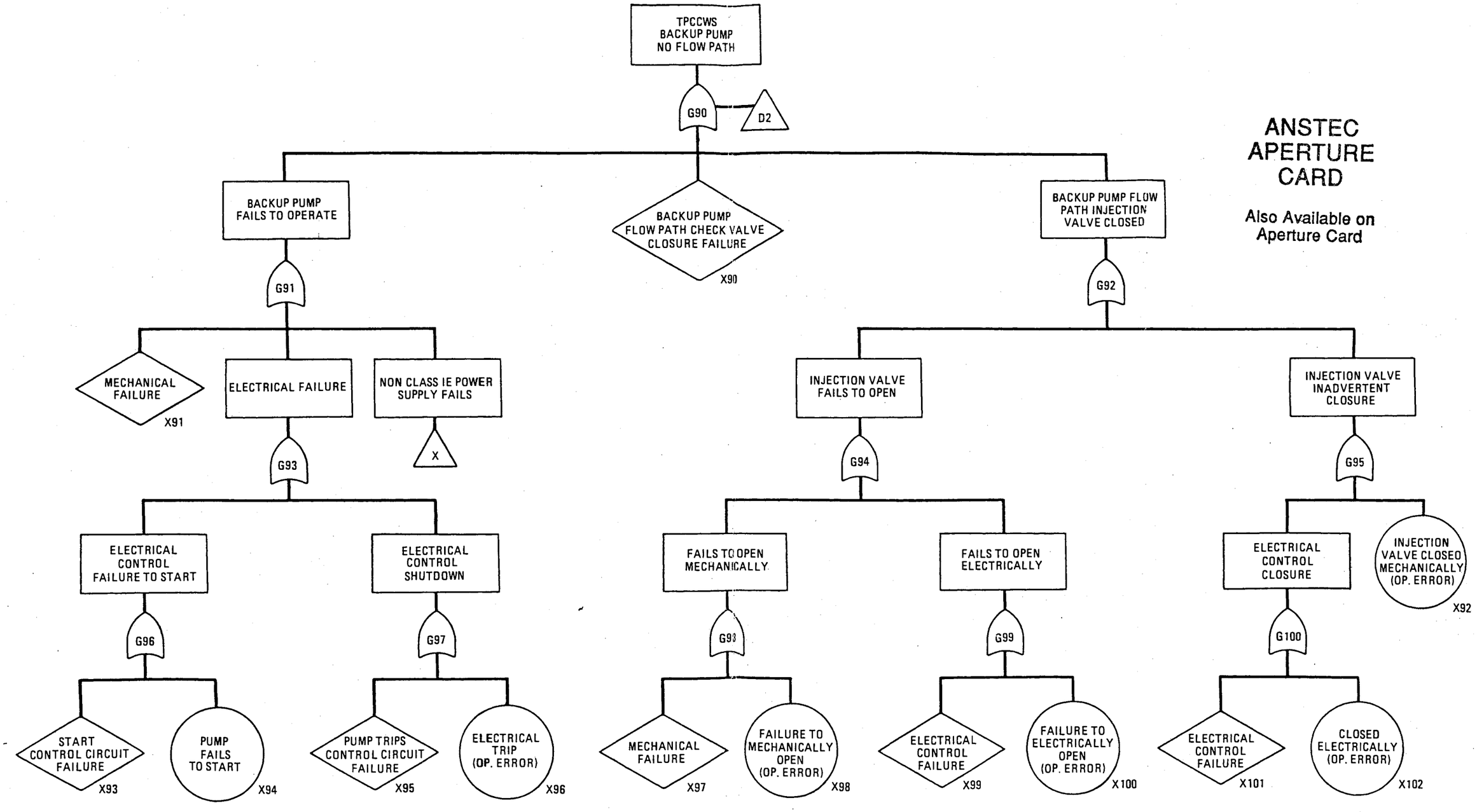


Fig. 6-32. Fault tree for turbine building closed cooling water subsystem failure



HT-001(68)

Fig. 6-33. Subtree D1 for loss of heat sink



HT-001(69)

Fig. 6-34. Subtree D2 for loss of backup pump flowpath

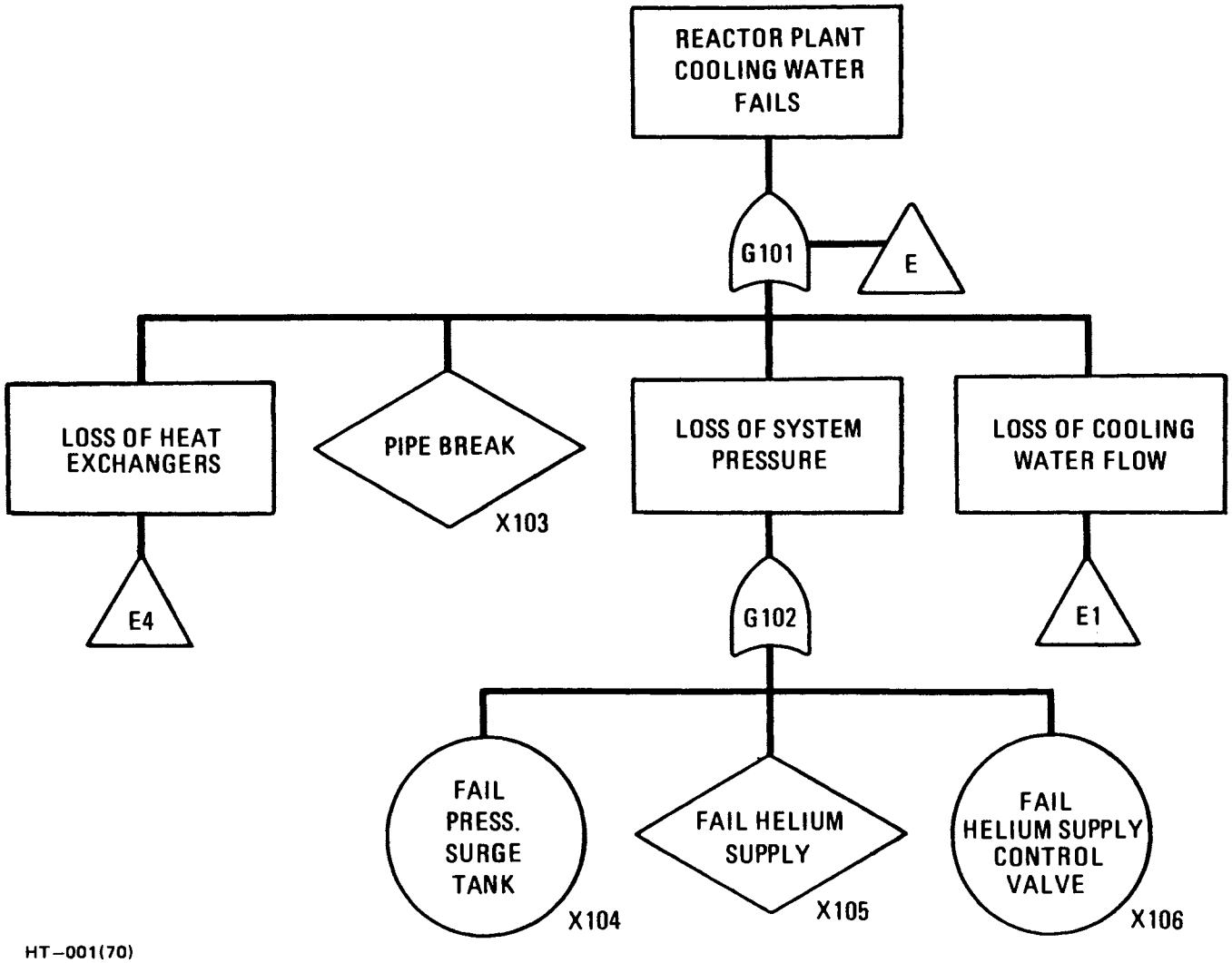


Fig. 6-35. Fault tree for reactor plant cooling water subsystem failure

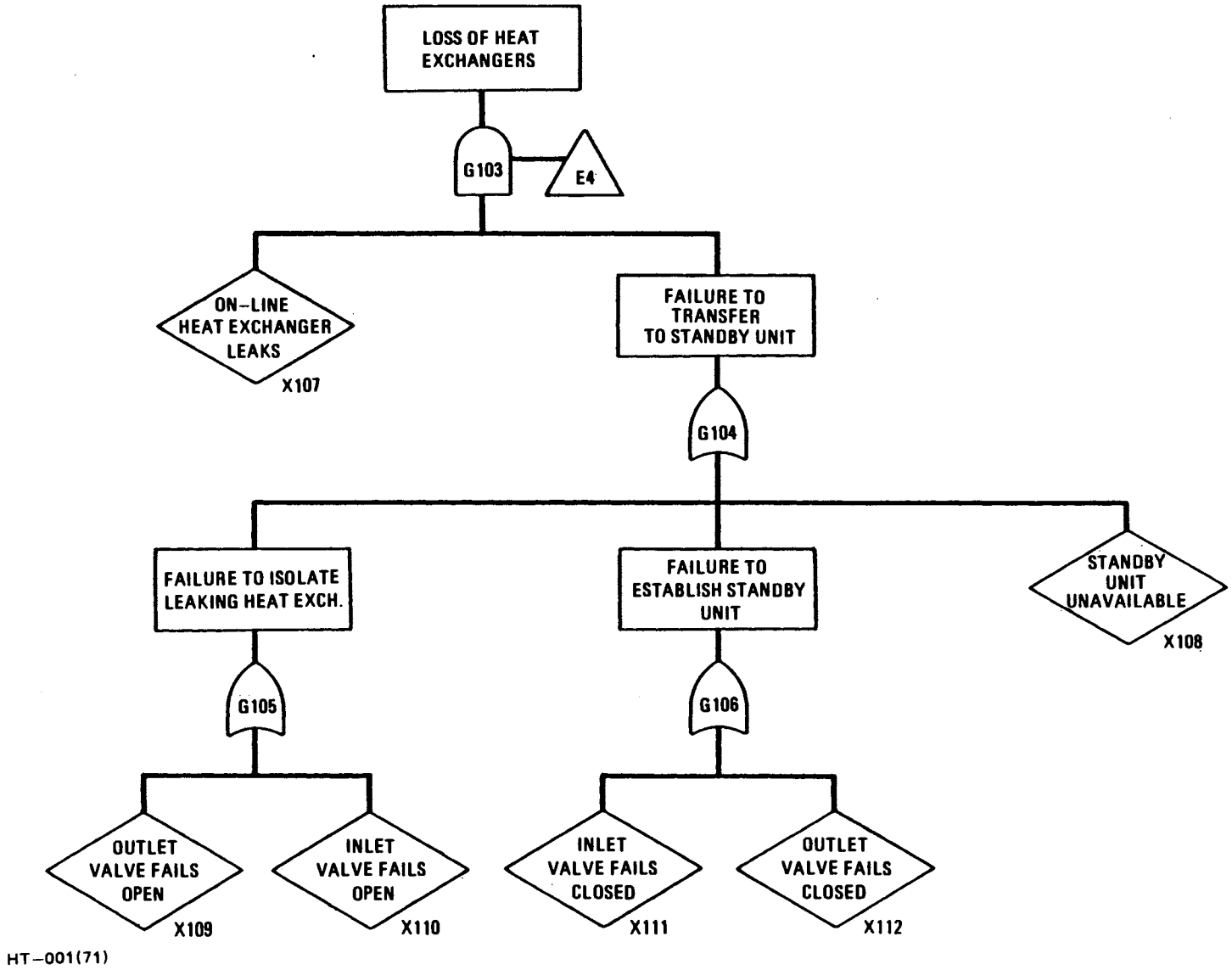


Fig. 6-36. Subtree E4 for loss of heat exchangers

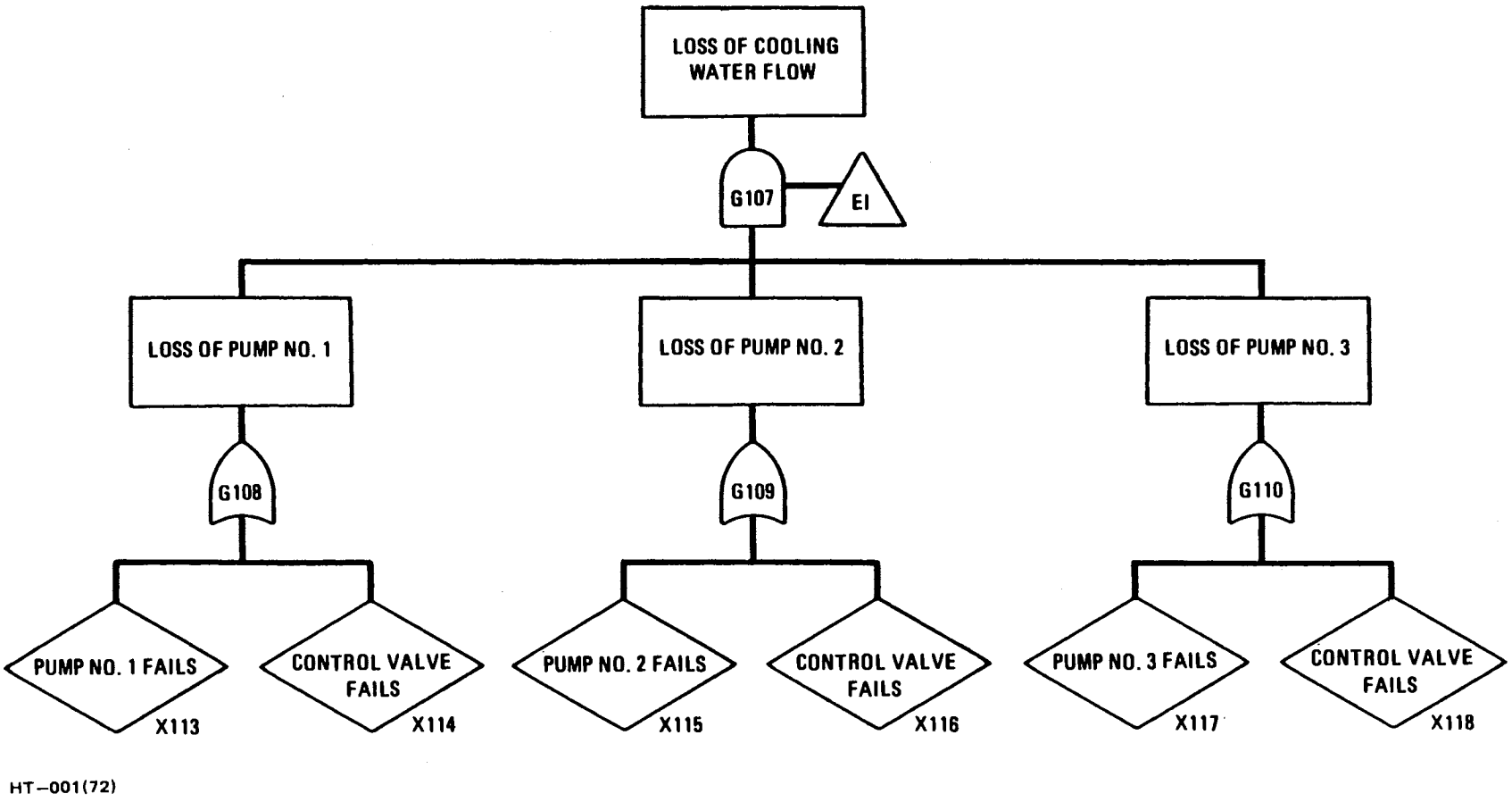


Fig. 6-37. Subtree E1 for loss of cooling water flow

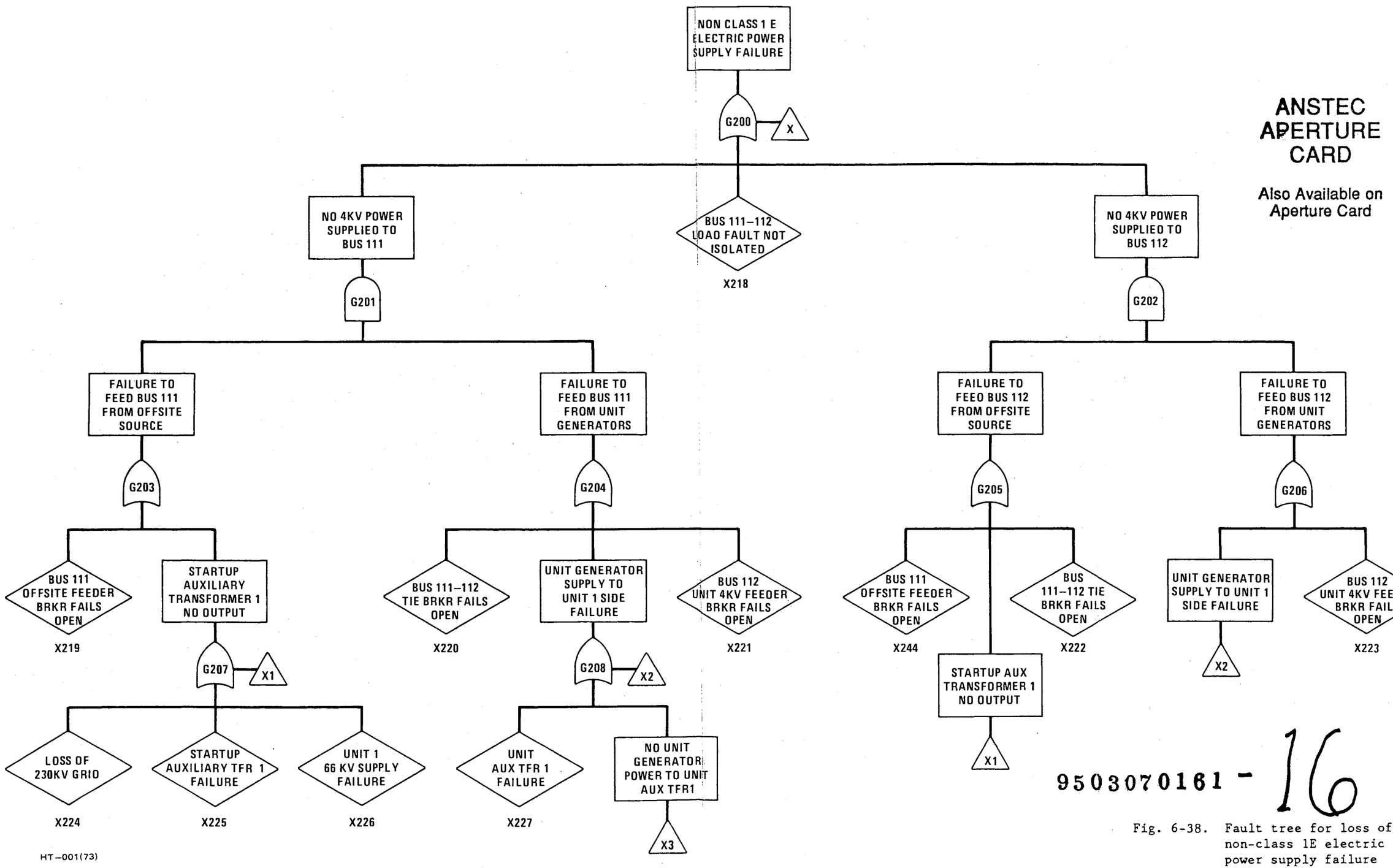
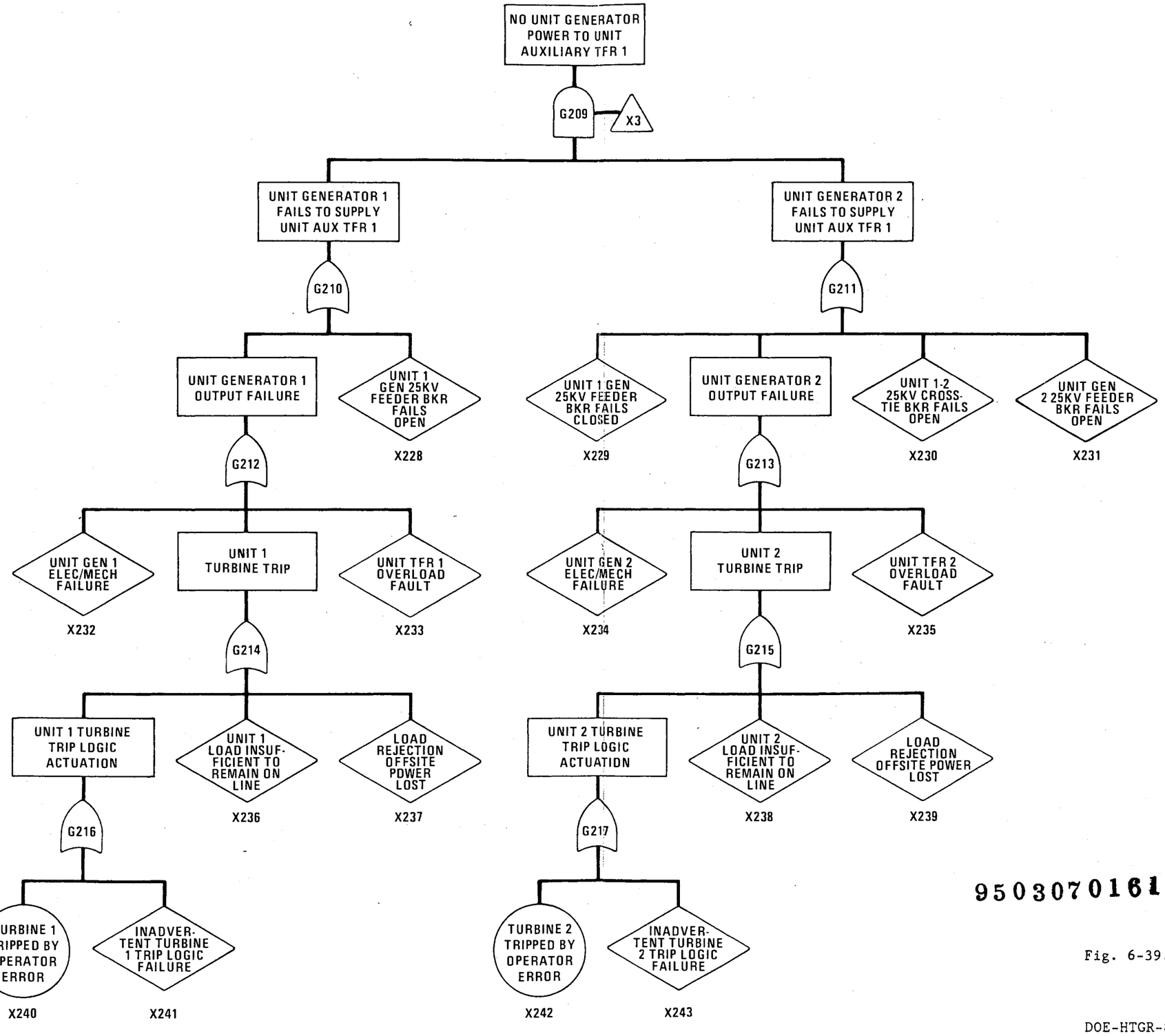
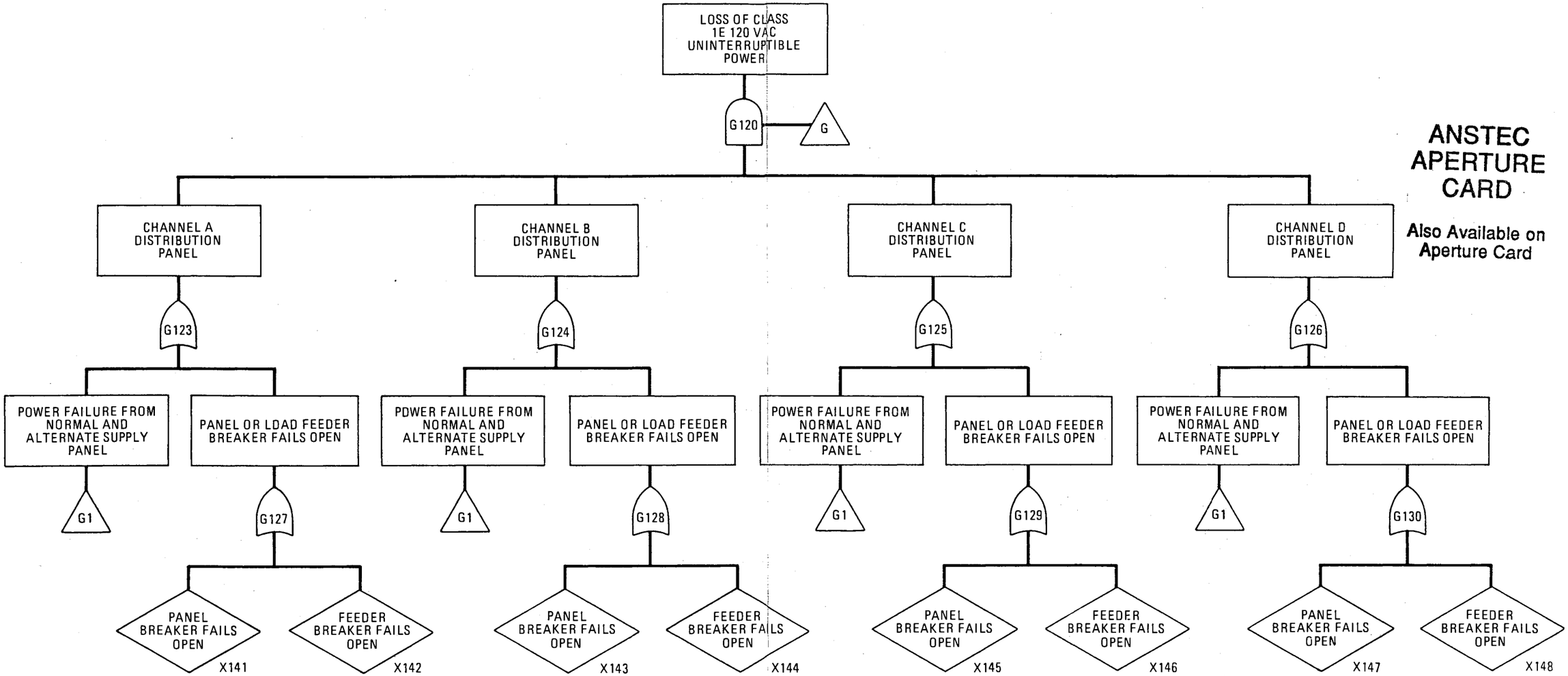


Fig. 6-38. Fault tree for loss of non-class 1E electric power supply failure



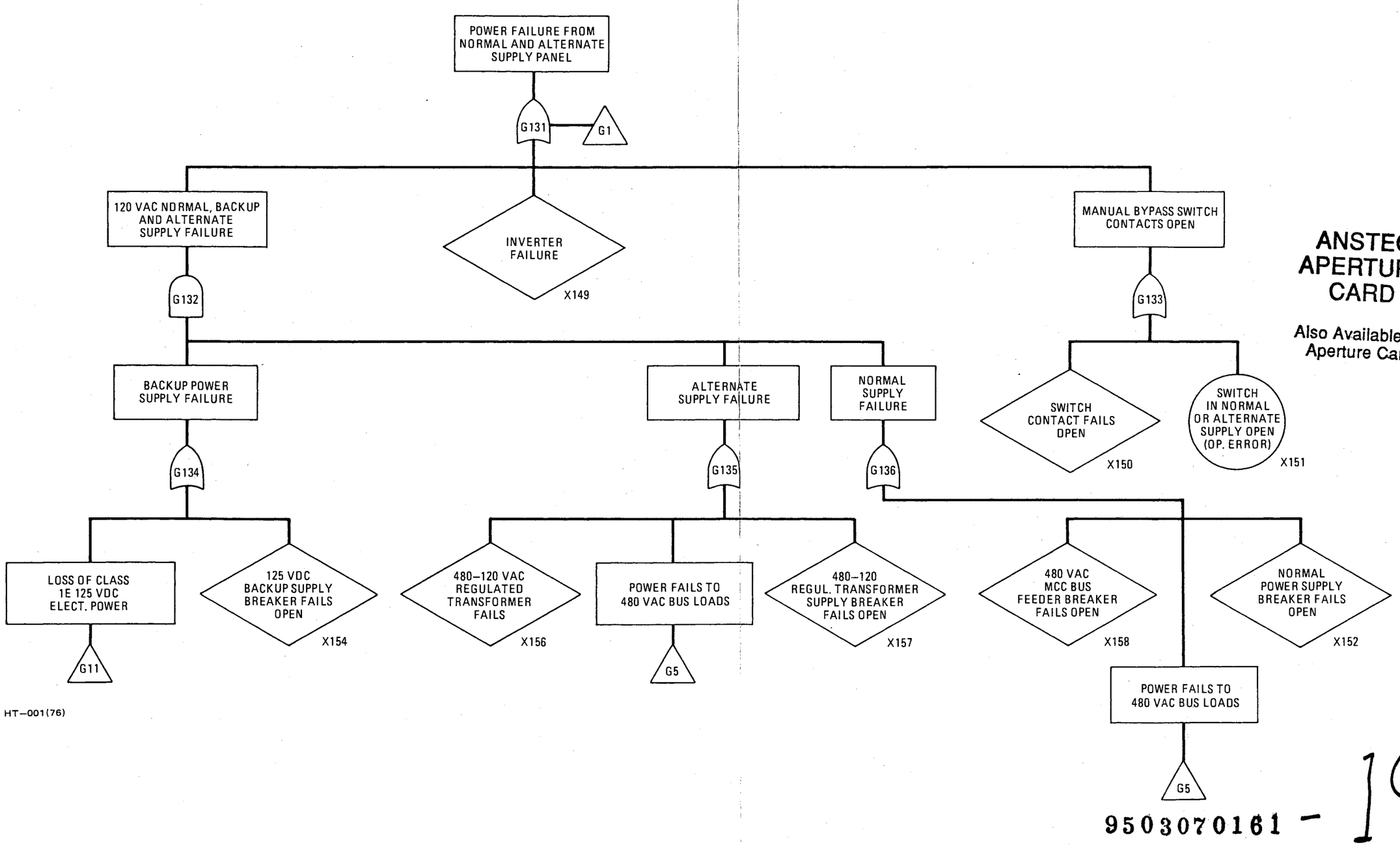
HT-001(74)

Fig. 6-39. Subtree X3 for no unit generator power to unit auxiliary transformer 1



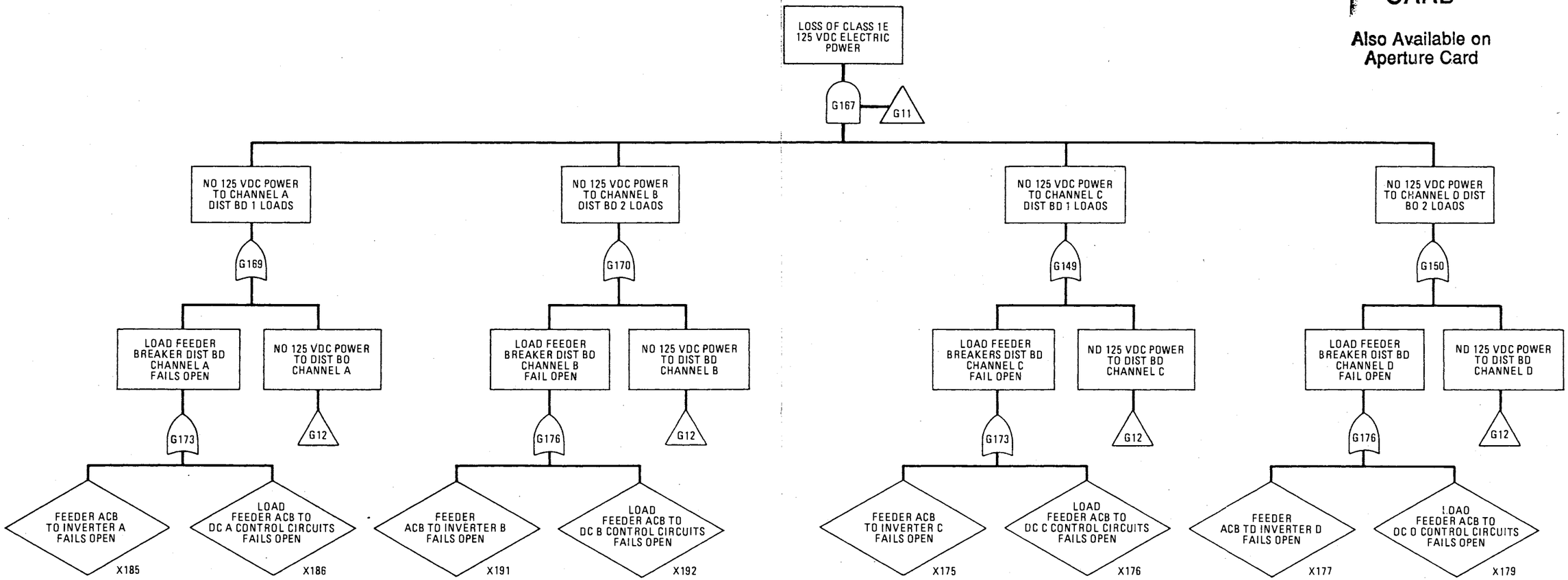
HT—001(75)

Fig. 6-40. Fault tree for loss of class 1E 120 V ac uninterruptible power supply



HT–001(76)

Fig. 6-41. Subtree G1 for power failure from normal and alternate supply panel



HT—001(77)

9503070161 - 20

Fig. 6-42. Subtree G11 for loss of class 1E 125 V dc electric power

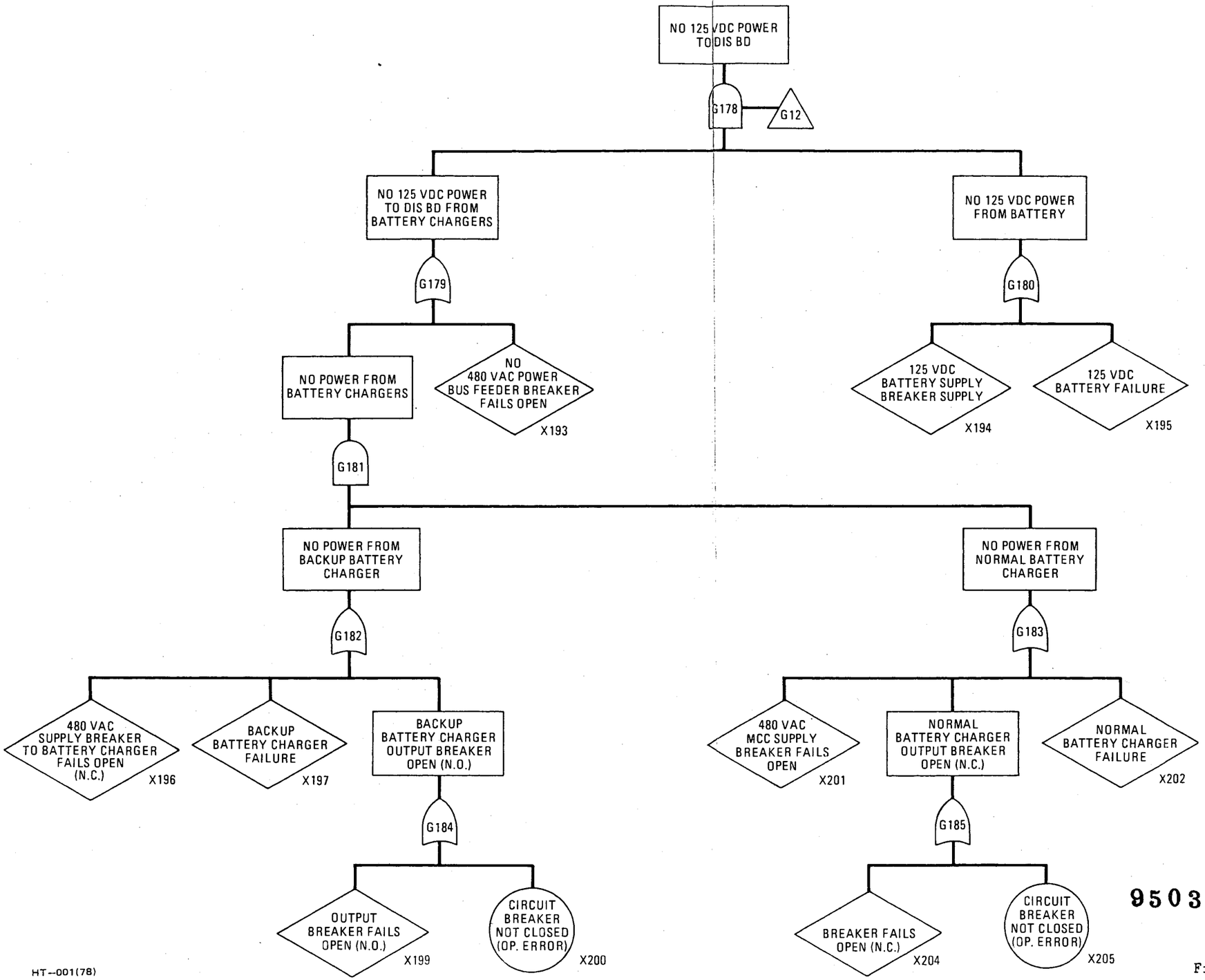


Fig. 6-43. Subtree G12 for loss of 125 V dc power to distribution board

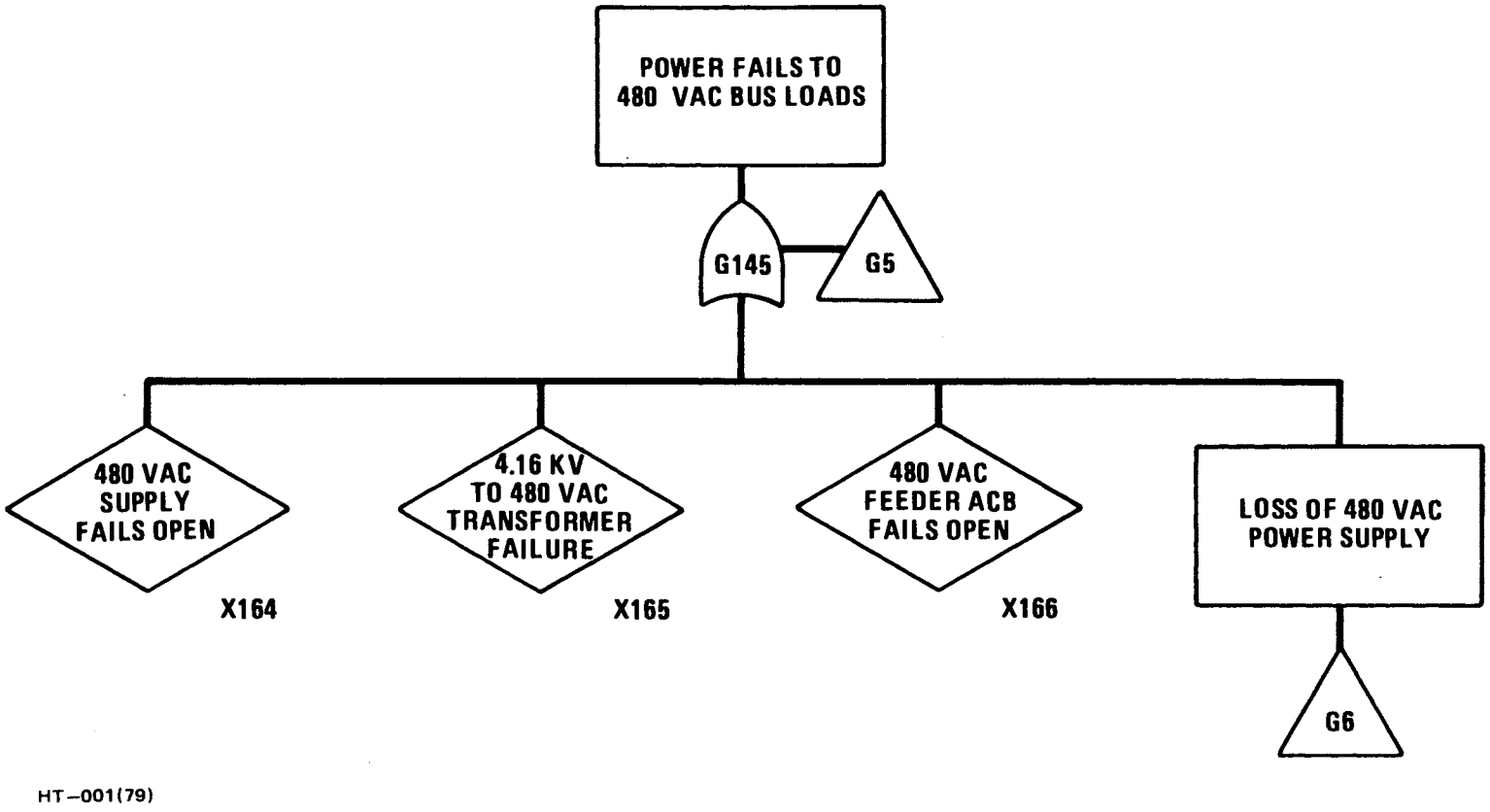
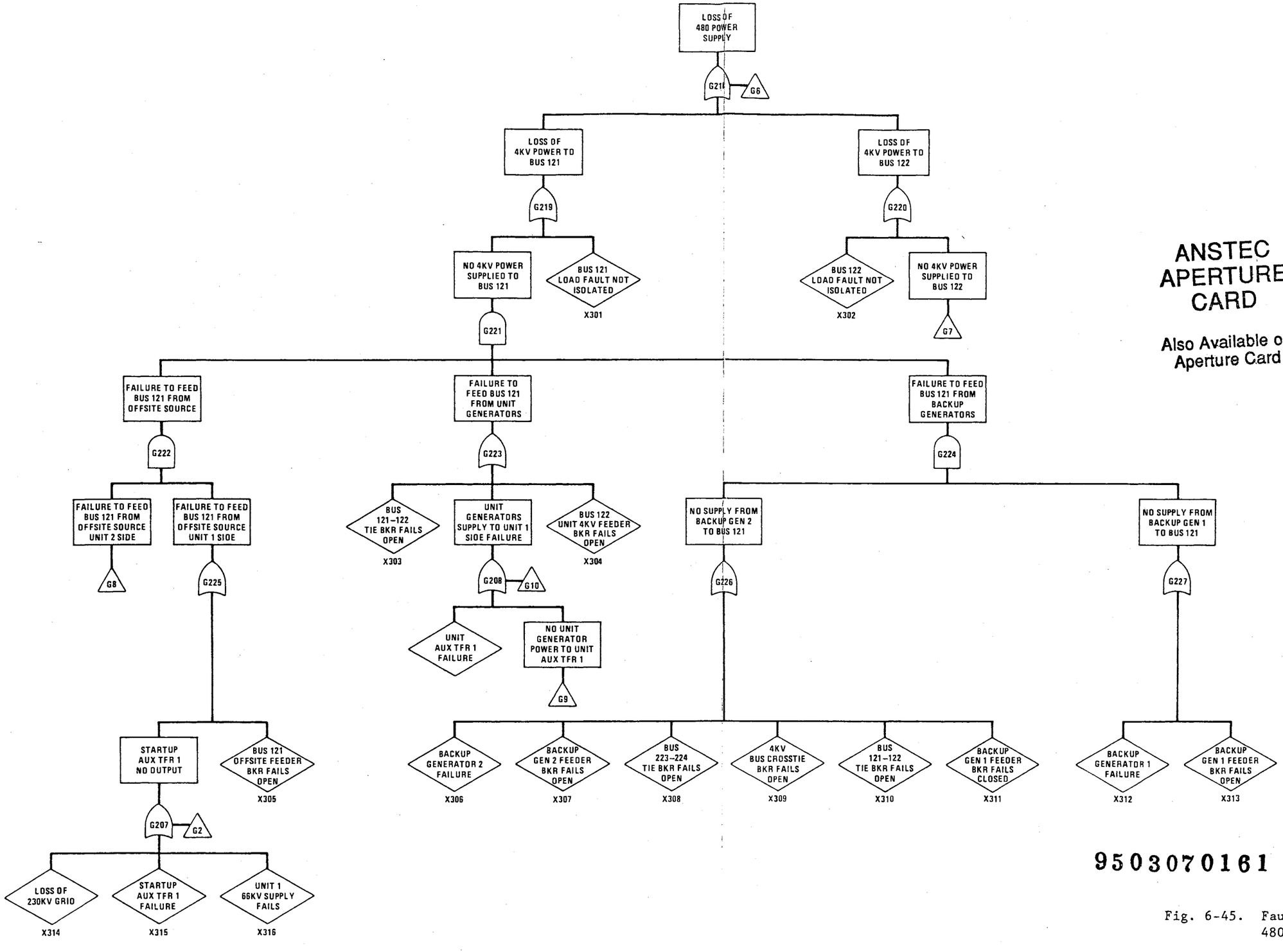


Fig. 6-44. Subtree G5 for loss of ac power to 480 V ac loads



HT–001(80)

Fig. 6-45. Fault tree for loss of 480 V ac power supply

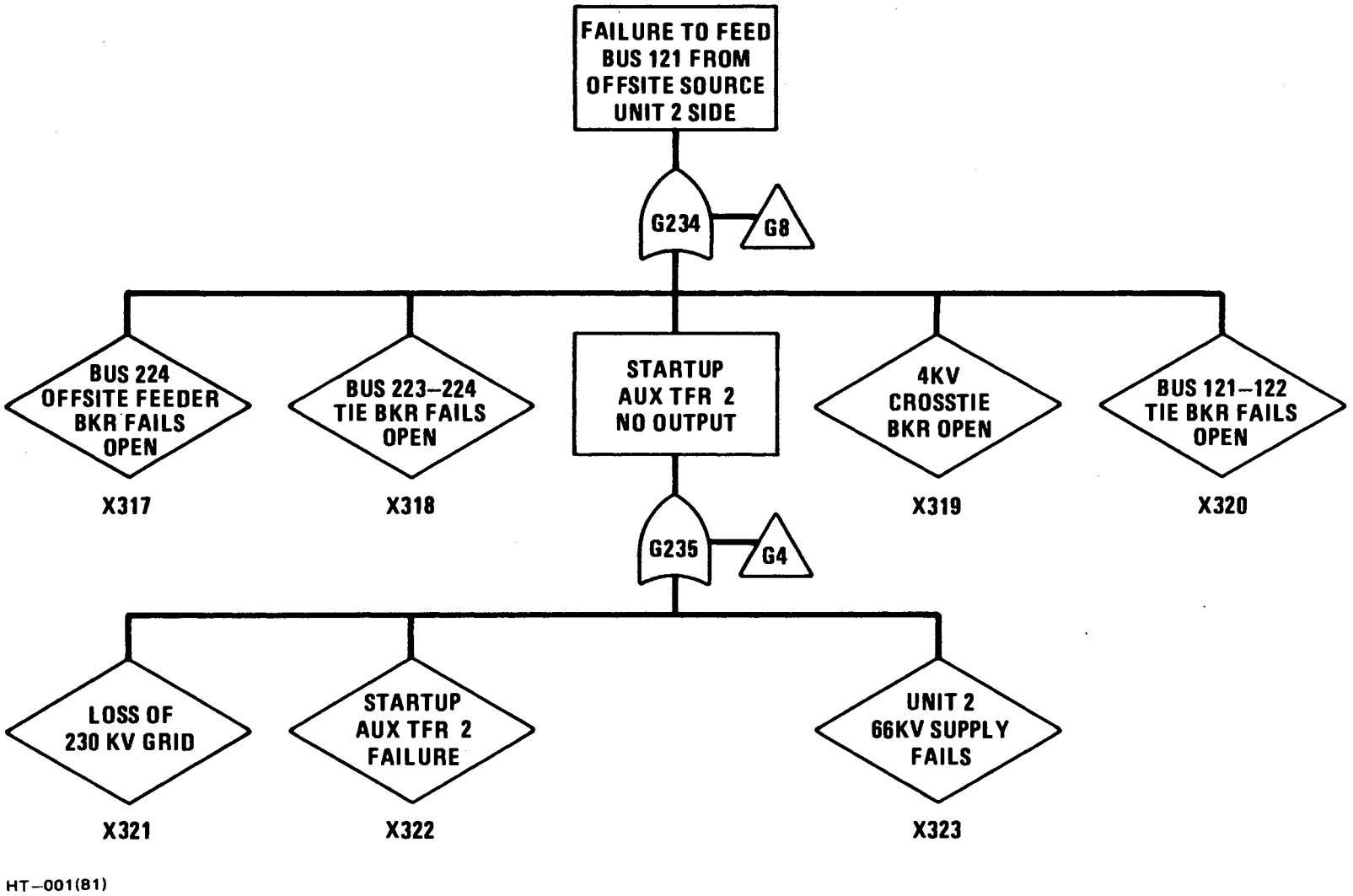
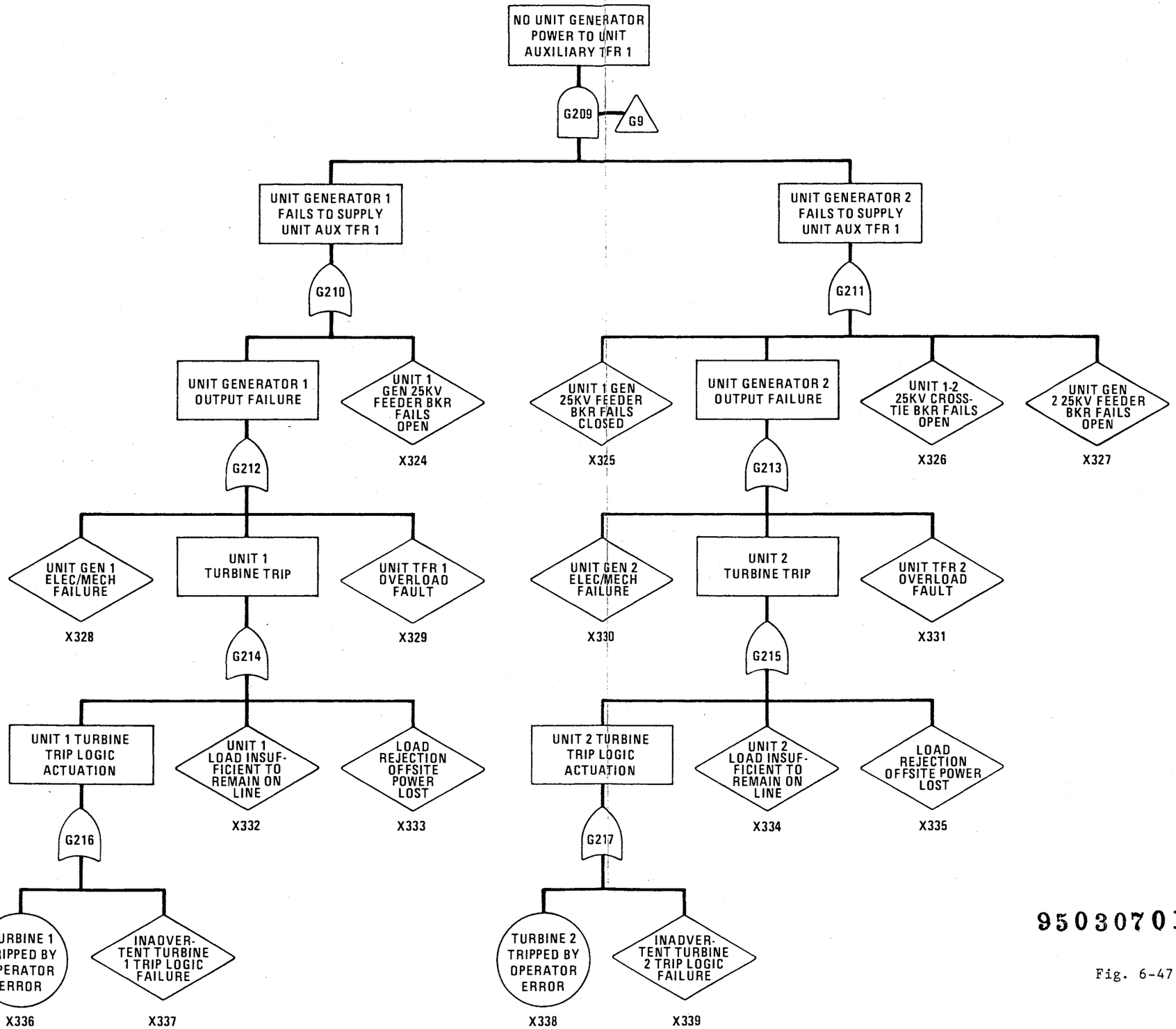
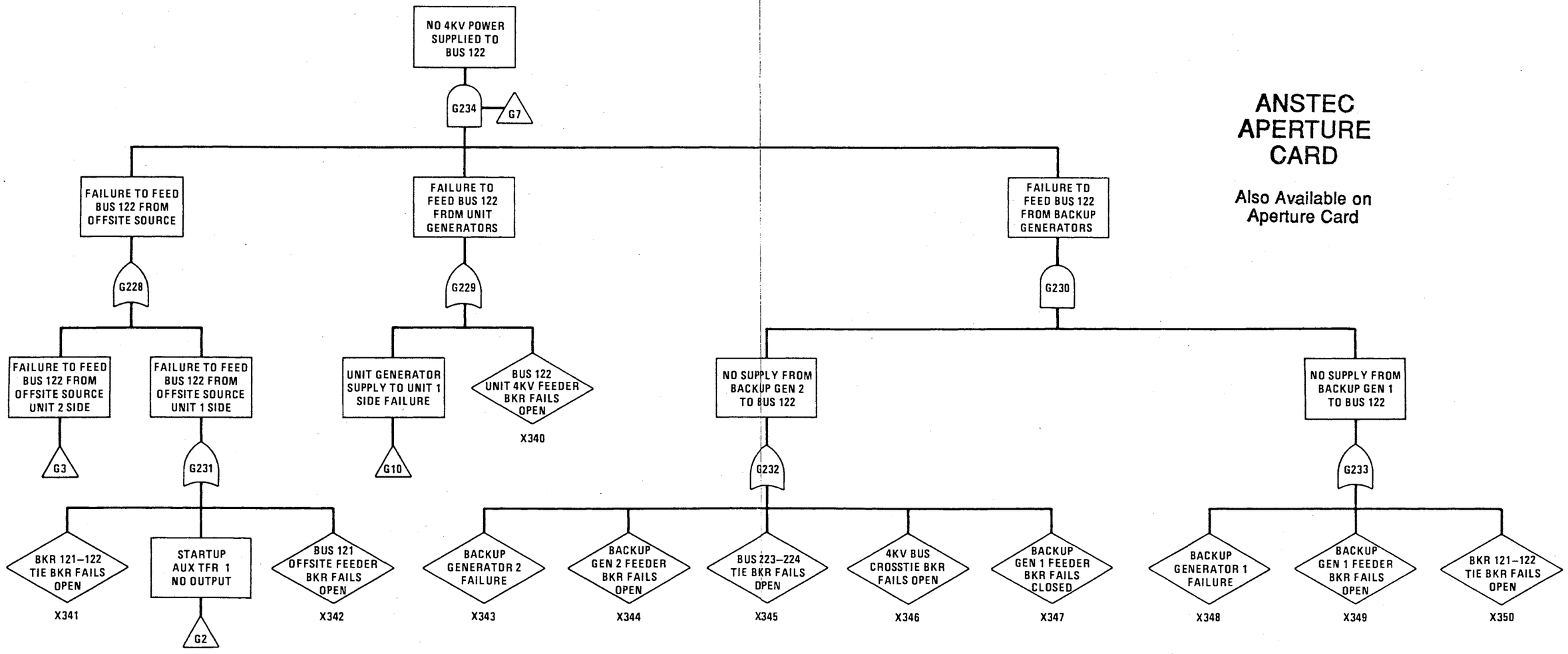


Fig. 6-46. Subtree G8 for failure to feed bus 121 from offsite source



HT-001(82)

Fig. 6-47. Subtree G9 for no unit generator power to unit auxiliary transformer 1



HT–001(83)

Fig. 6-48. Subtree G7 for failure to supply 4-kV power to bus 122

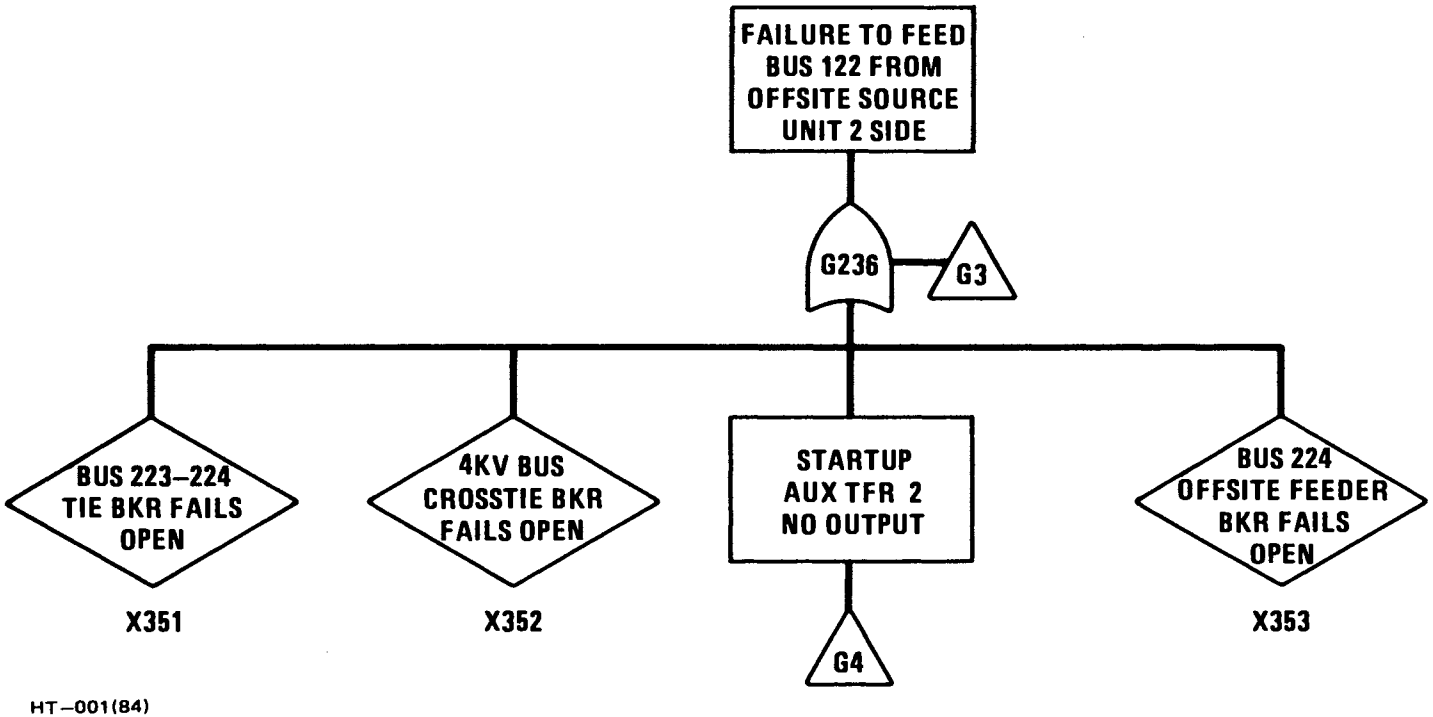


Fig. 6-49. Subtree G3 for failure to feed bus 122 from offsite source - unit 2 side

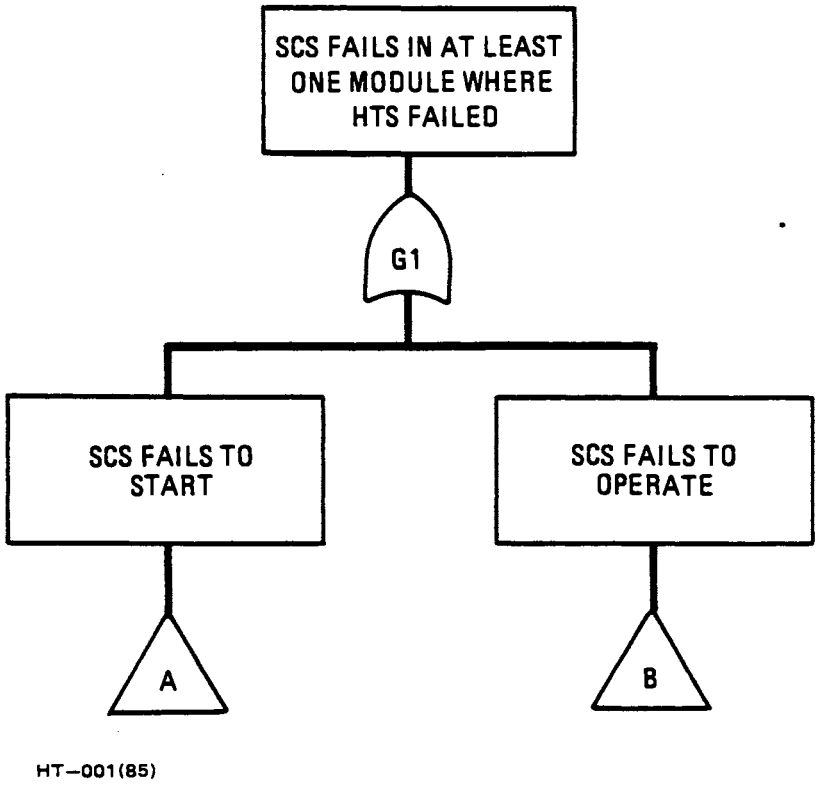
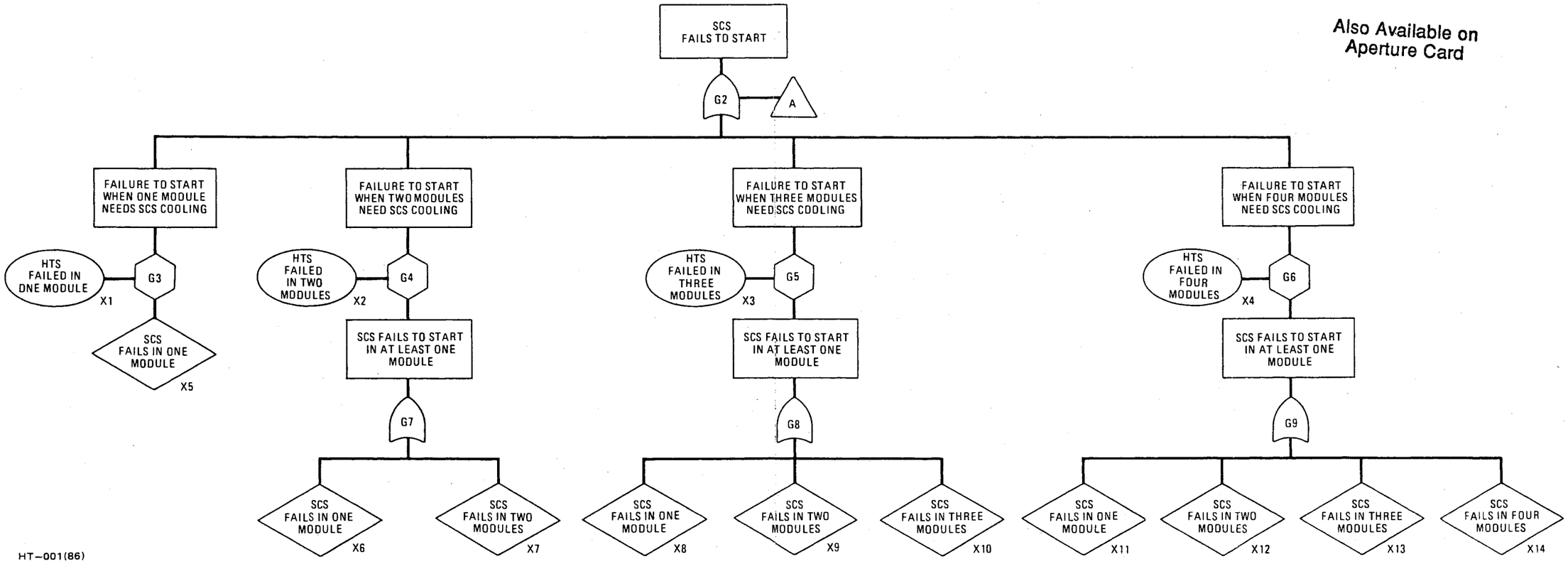
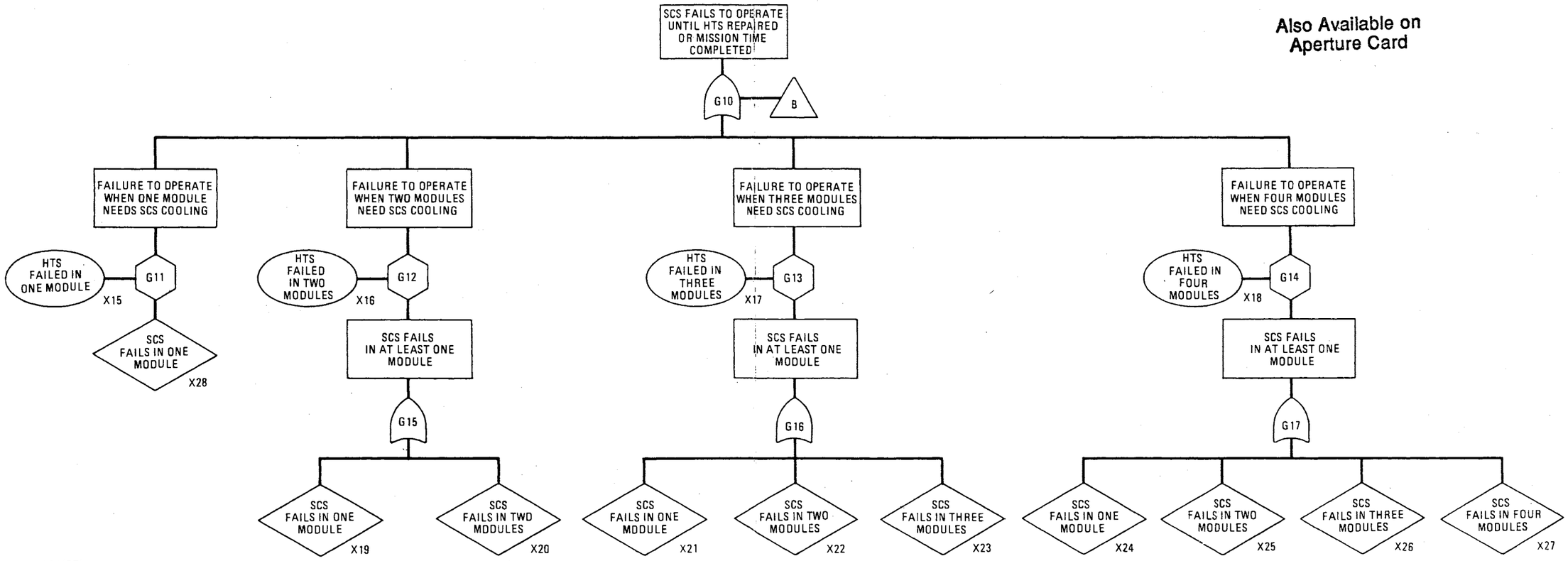


Fig. 6-50. Fault tree for SCS failure in at least one module where the HTS has failed



HT-001(86)

Fig. 6-51. Subtree A for SCS failure to start



HT-001(87)

Fig. 6-52. Subtree B for SCS failure to operate

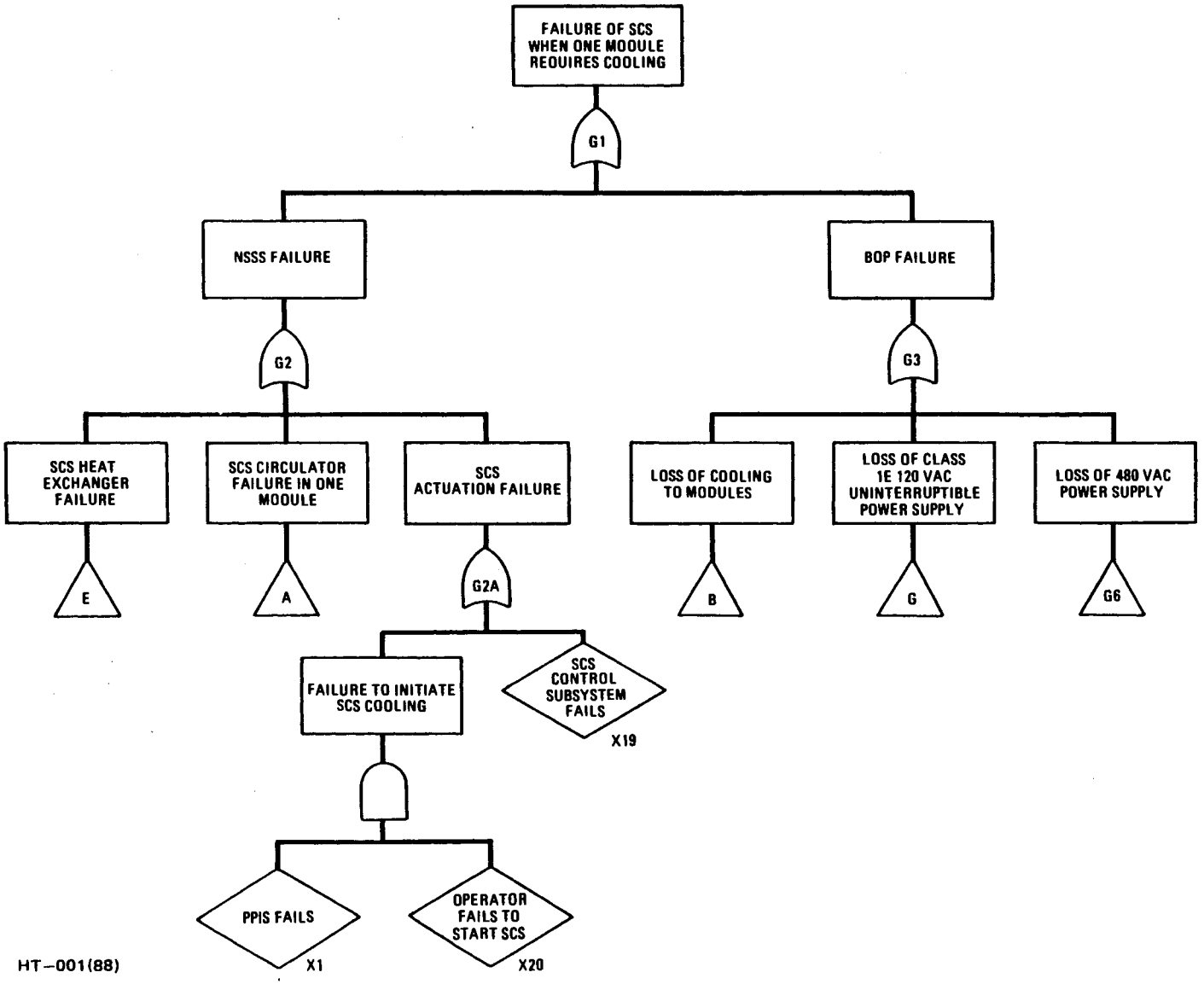
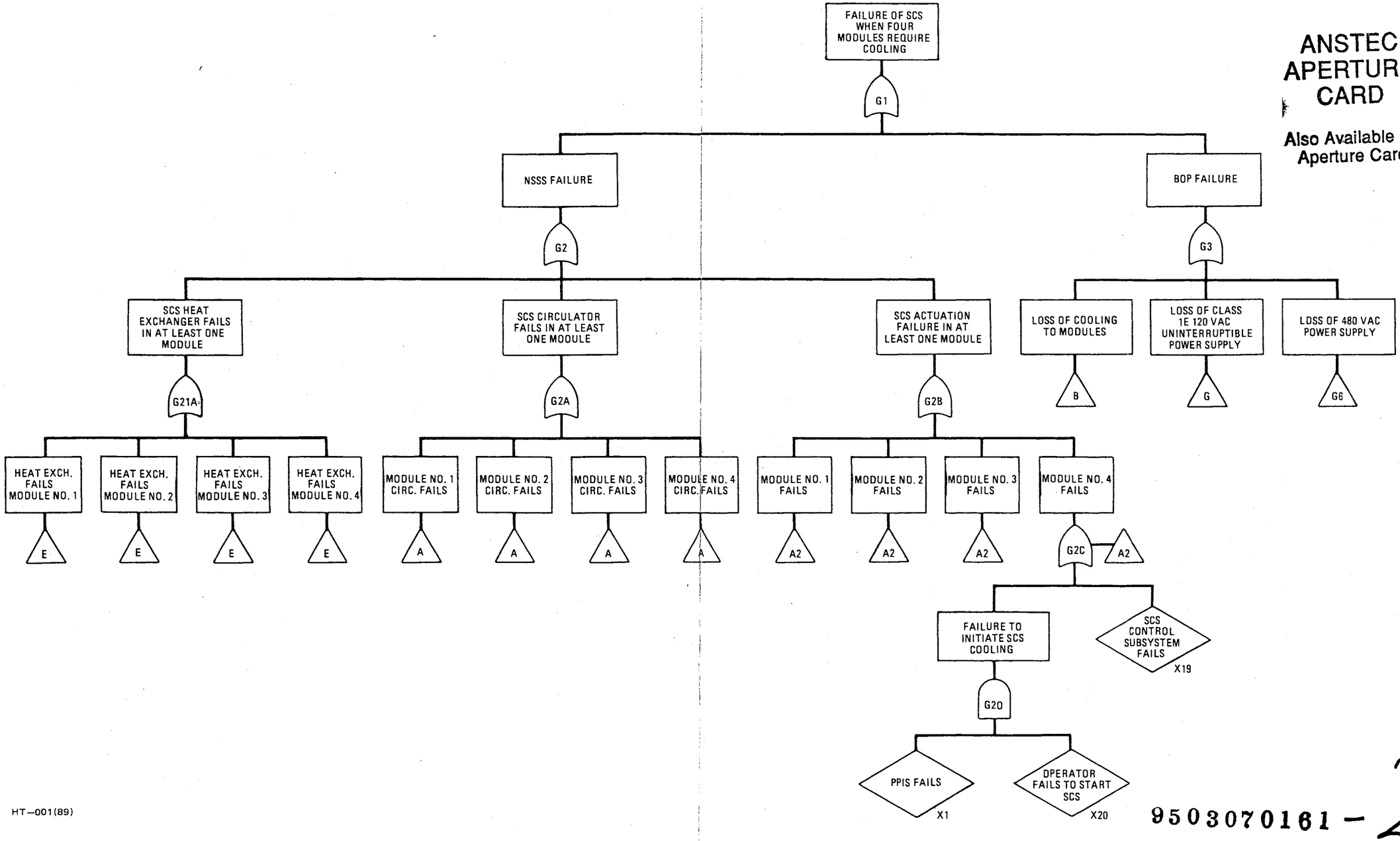


Fig. 6-53. Fault tree for loss of SCS cooling when one module require cooling



HT—001(89)

9503070161 - 27

Fig. 6-54. Fault tree for loss of SCS cooling when four modules require cooling

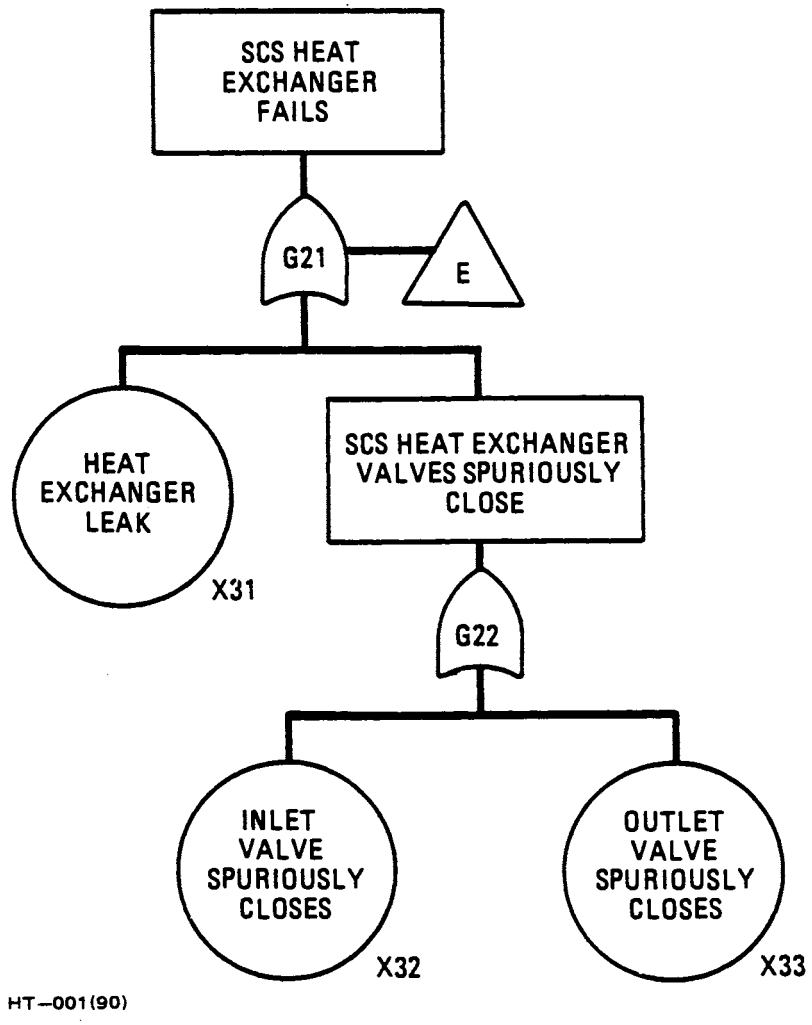


Fig. 6-55. Subtree E for SCS heat exchanger failure

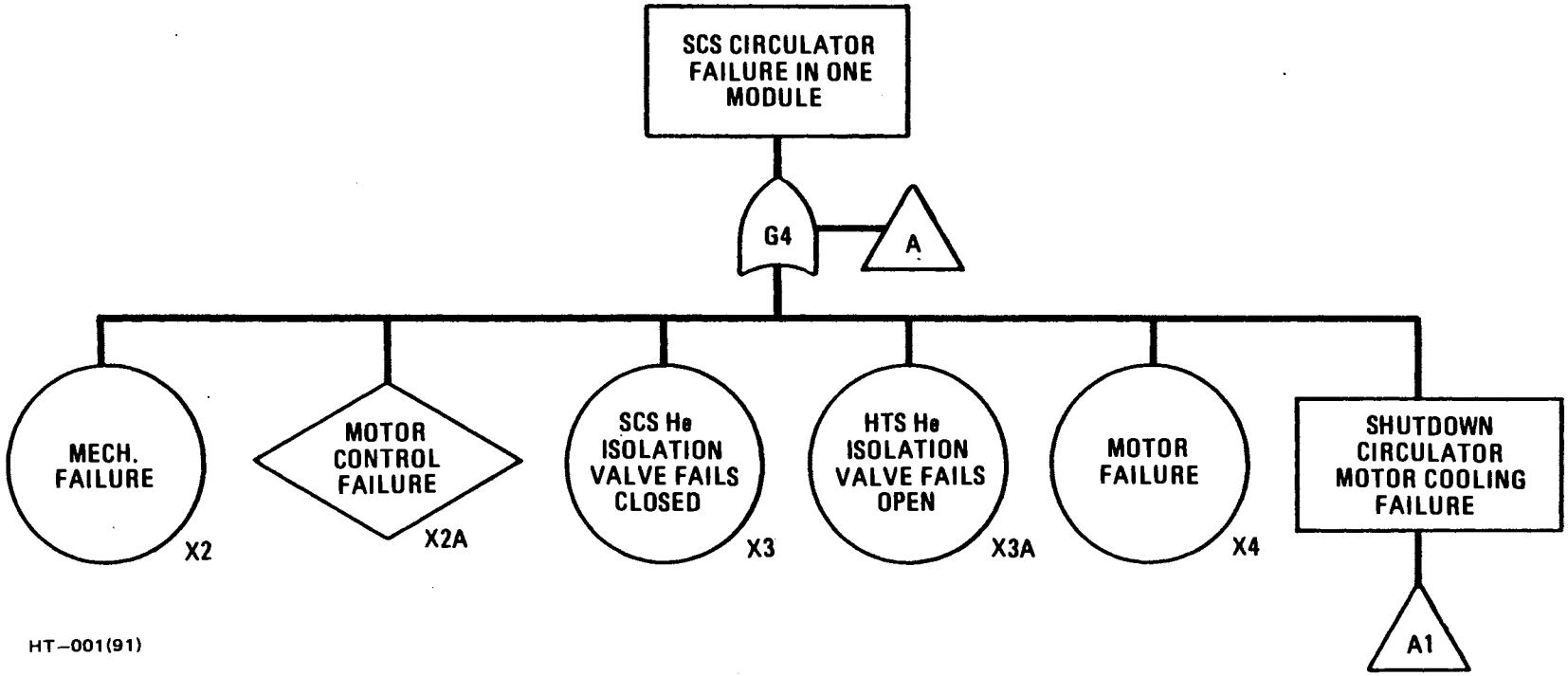


Fig. 6-56. Subtree A for SCS circulator failure in one module

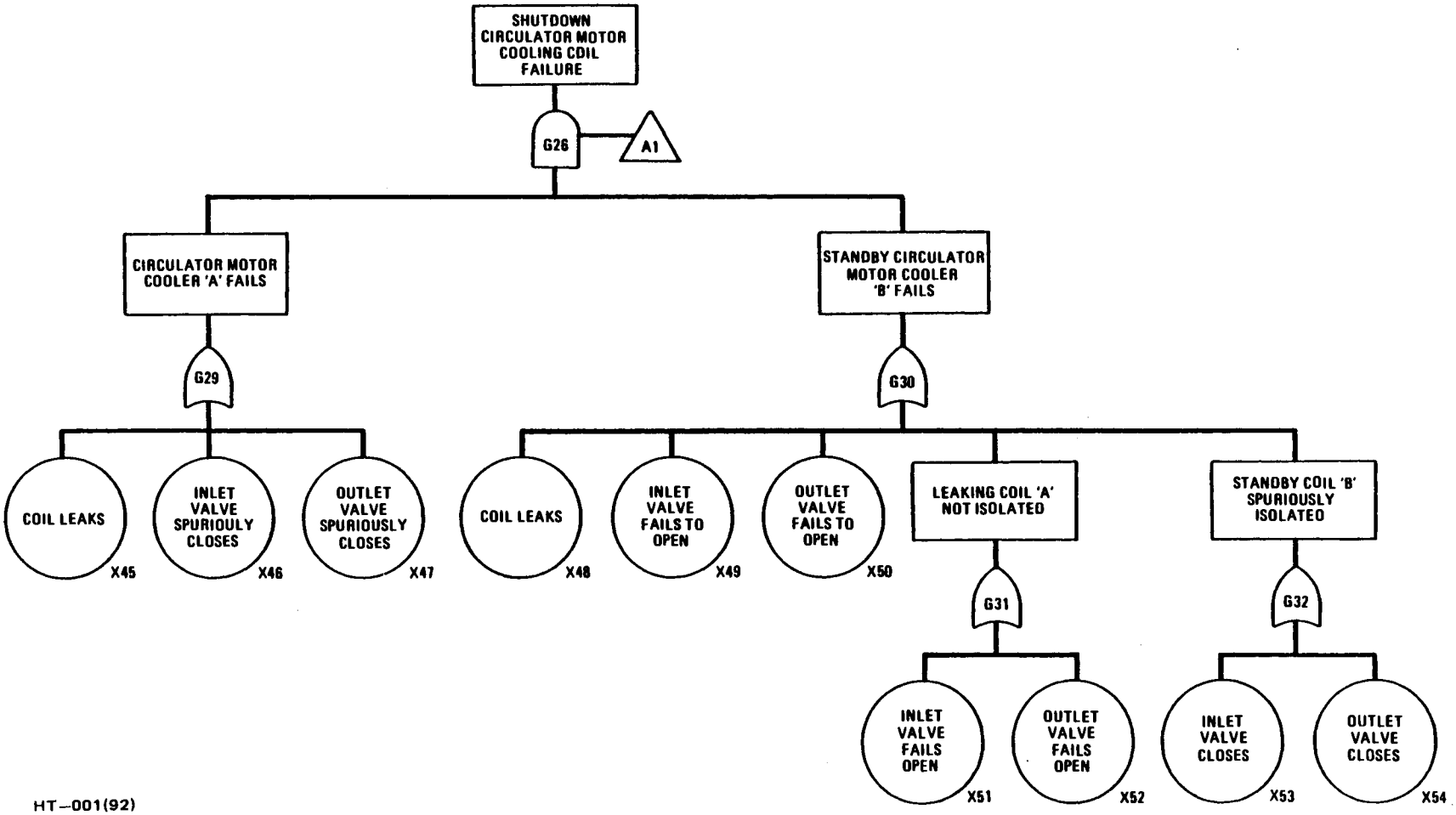


Fig. 6-57. Subtree A1 for shutdown circulator motor cooling failure

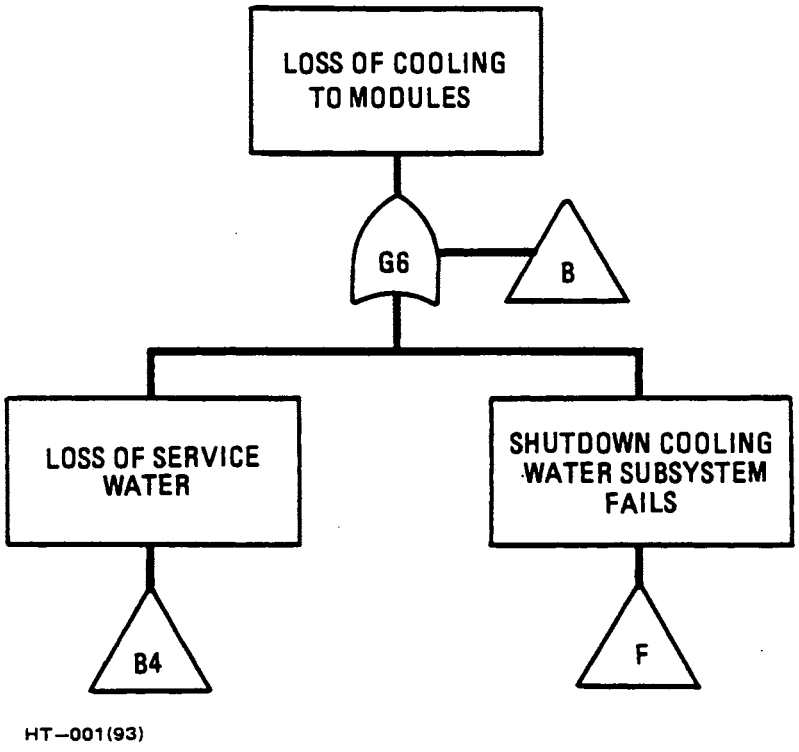
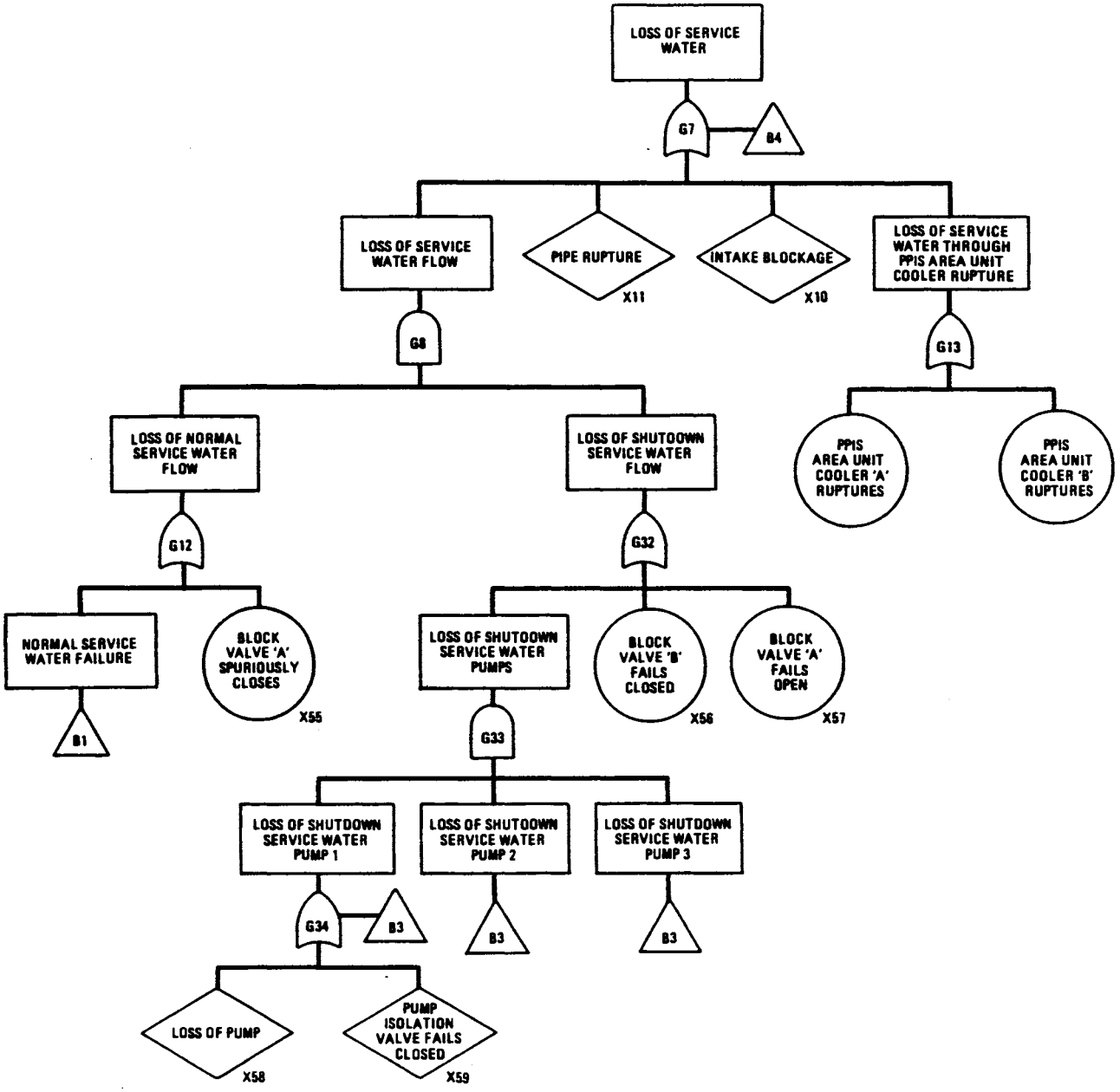


Fig. 6-58. Subtree B for loss of cooling to modules



HT-001(94)

Fig. 6-59. Subtree B4 for loss of service water

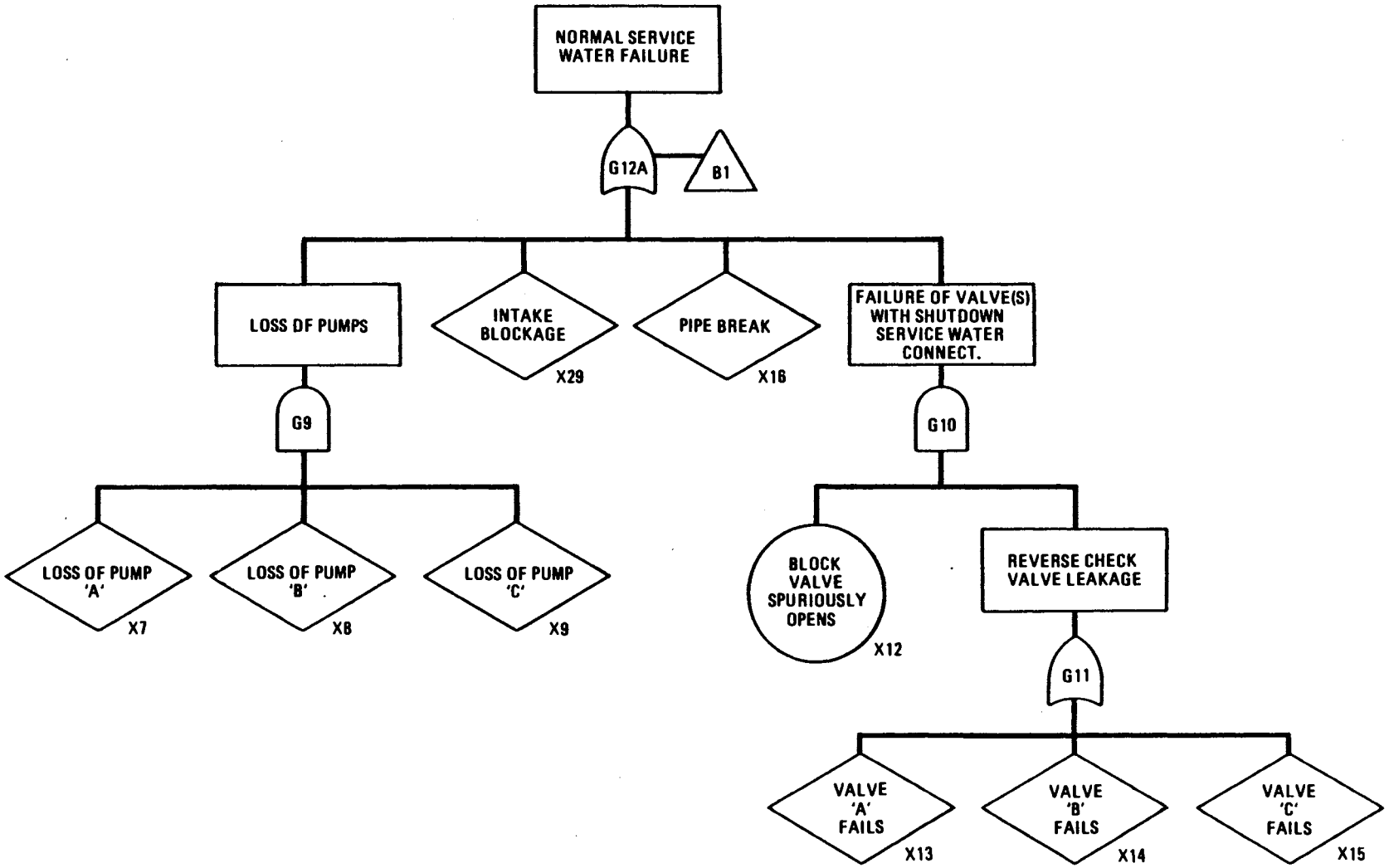
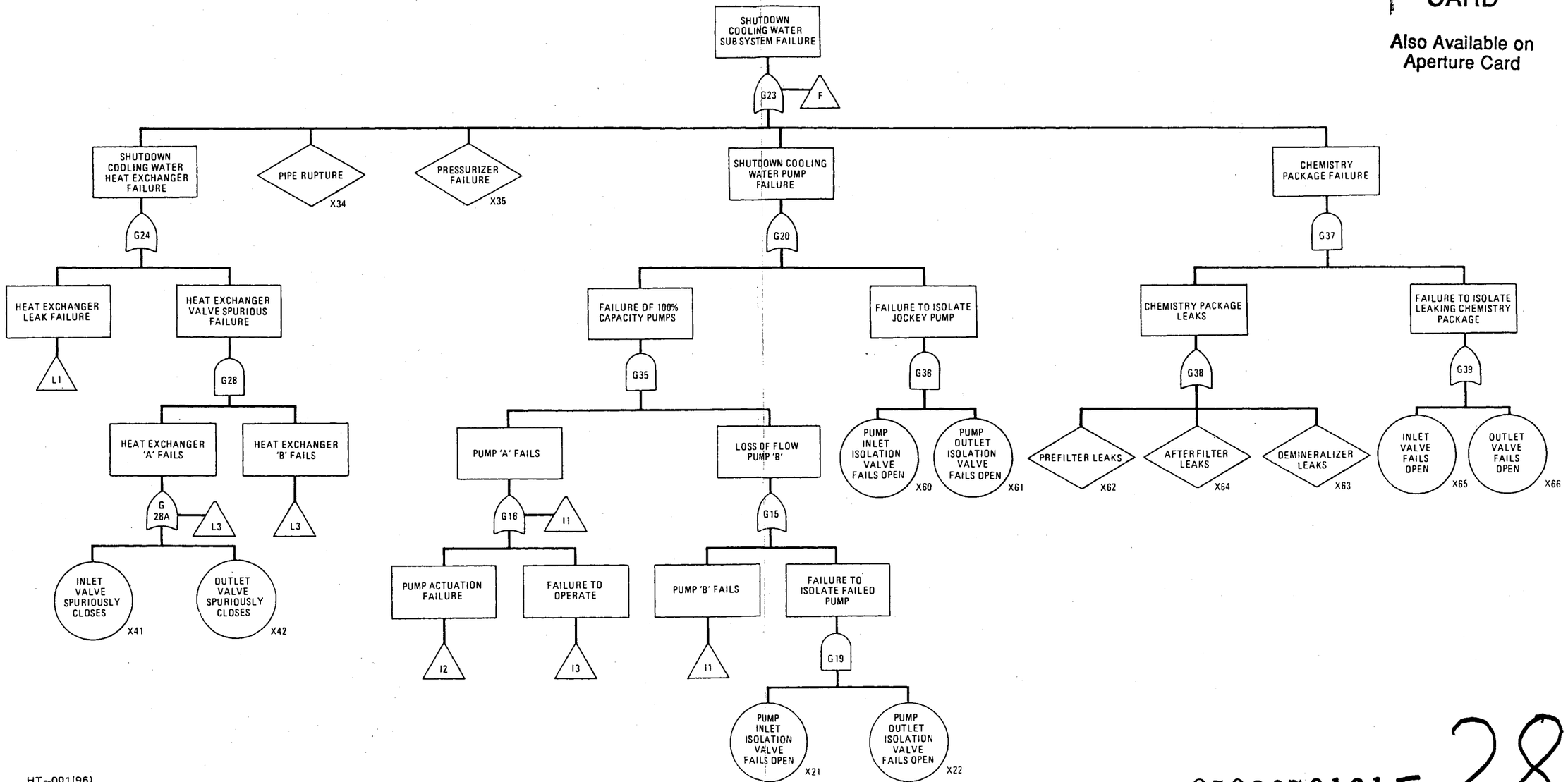


Fig. 6-60. Subtree B1 for normal service water failure



HT-001(96)

9503070161 - 28

Fig. 6-61. Subtree F for shutdown cooling water subsystem failure

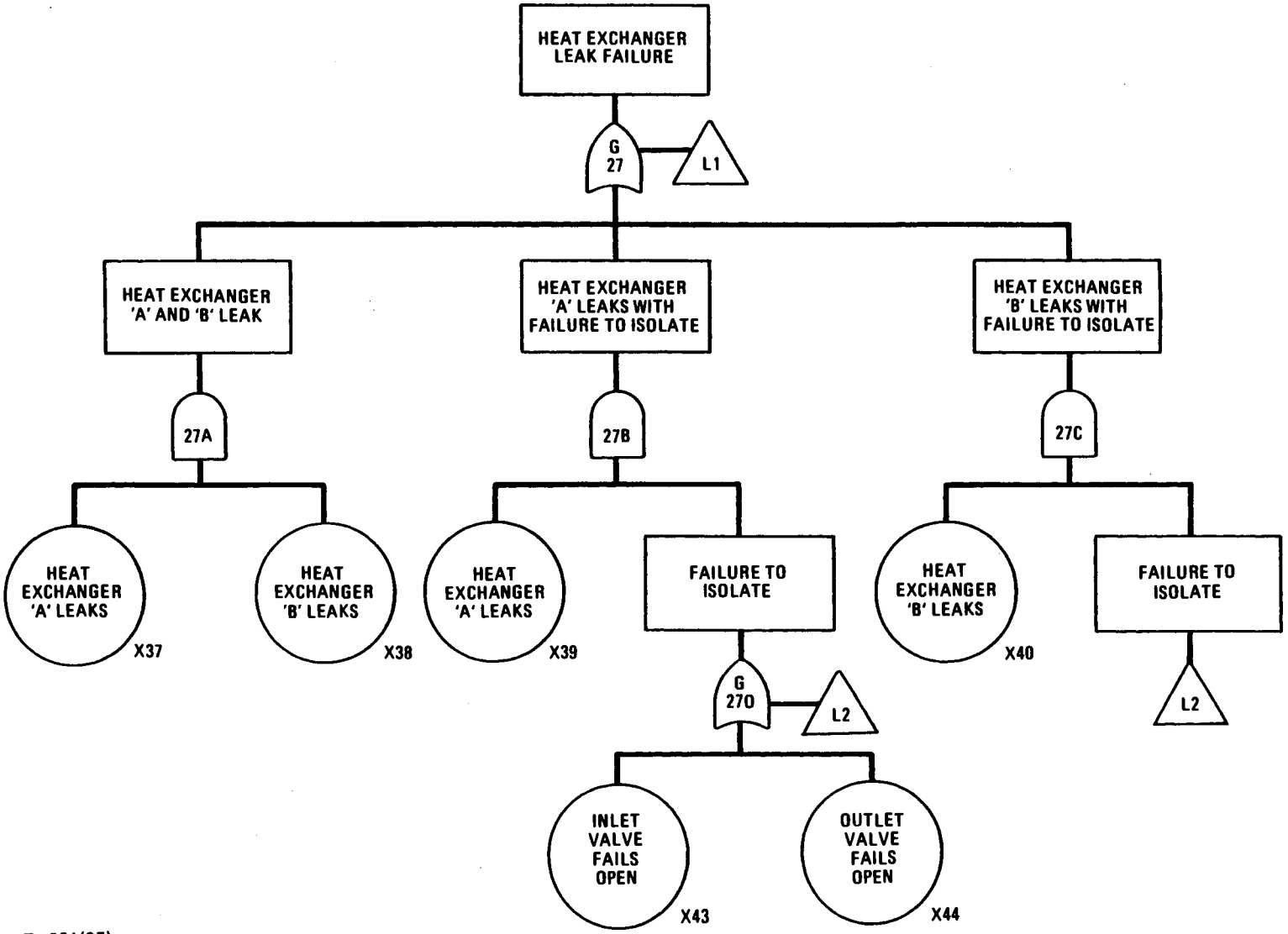


Fig. 6-62. Subtree L1 for heat exchanger leakage

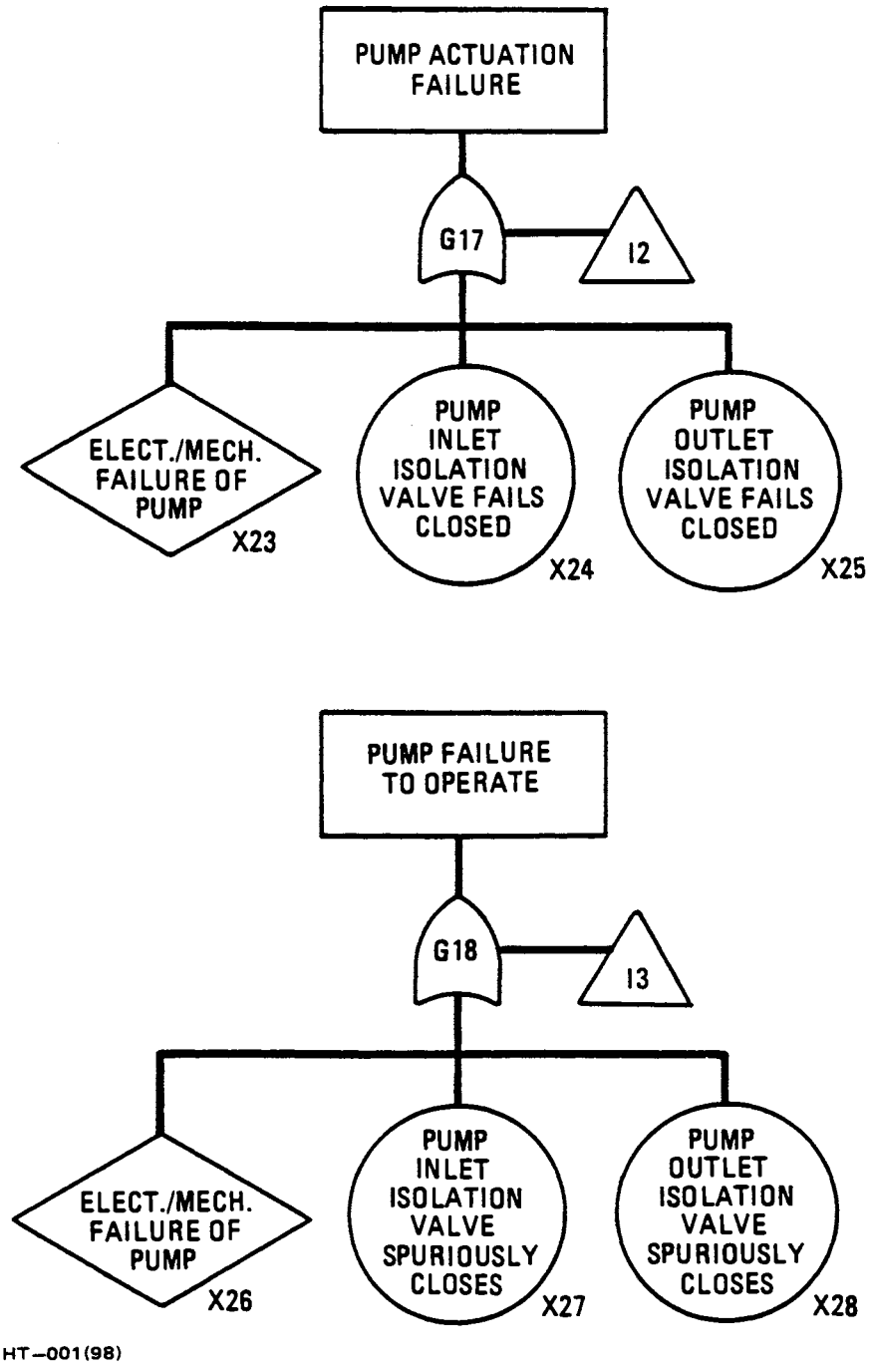


Fig. 6-63. Subtrees I2 and I3 for failure to actuate and operate pumps

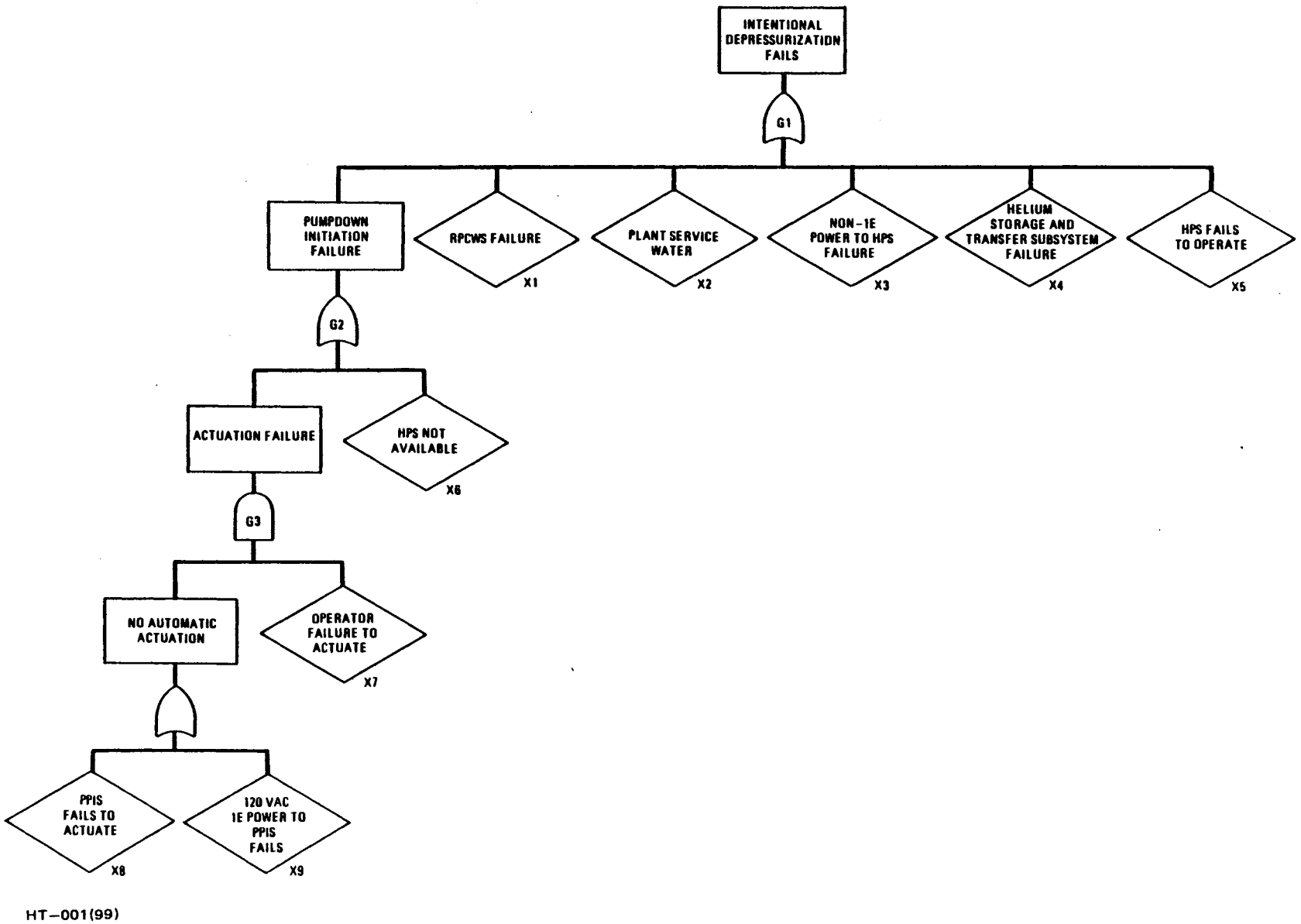


Fig. 6-64. Fault tree for intentional depressurization failure

7. ACCIDENT FREQUENCY ASSESSMENT

In the risk assessment, initiating events are first identified which may lead to an uncontrolled or unscheduled radiological release. From each of these initiating events, a number of end states are possible depending upon the plant's response. Event trees are utilized to systematically identify the various accident sequences which follow an initiating event. This section summarizes the manner in which the event tree methodology was applied in this risk assessment. A detailed discussion of the manner in which event trees were constructed and quantified is found in Appendix C.

Section 5 identifies important initiating events which may lead to radiological release. Plant response to these initiating events and system reliability models are discussed in Section 6. This description of plant behavior was utilized to construct event trees, which depict the various event sequences possible following each initiating event. Each event sequence's frequency was then assessed by evaluating the initiating event frequency and the many branch point conditional probabilities within an event tree using fault tree or other appropriate methodologies as described in Section 3. Finally, the initiating event frequency and subsequent event probabilities were statistically combined to yield a frequency for each event tree sequence.

The primary focus in the MHTGR safety approach is on the retentive properties of the ceramic, high-temperature fuel. The events considered in this assessment present a spectrum of challenges to this design goal of maintaining control of radionuclide release through retention by the

fuel. These challenges can be deemed as being associated with one of three major manners in which the fuel retention can be compromised: failure to control heat generation; failure to maintain core heat removal; and failure to prevent chemical attack. Thus, beyond the release of circulating activity involved in a primary coolant leak, the real threat from such a breach of the primary coolant boundary is the potential for chemical attack of the core. The reliability of core heat removal and the possible incremental fuel releases due to thermal transients are considered in the loss of main loop cooling event tree. The analysis of loss of main loop cooling also addresses possible breaches in the primary coolant pressure boundary induced by the thermal transient. Earthquakes and loss of offsite power focus on these same release mechanisms but are addressed separately because they encompass the simultaneous challenge to multiple systems typical of external events. Transients threatening the continued control of heat generation (reactivity-related transients) are considered in the anticipated transients requiring scram and rod withdrawal event trees. Finally, the steam generator leak analyses, in addition to addressing water-induced reactivity transients, also cover chemical attack of the core and fuel due to water.

Each of the accident initiators are discussed with their corresponding event trees in Sections C.1 through C.8. Sequential subsections of Appendix C describe the manner that each tree's initiating event frequency, as well as branching probabilities of subsequent events, were quantified. Events considered concern the success or failure of various plant systems in their response to the initiating event. In cases where the median frequency of an event sequence exceeded 10^{-8} per year and a radionuclide release occurred, the sequence is designated with an appropriate release category designation as shown on the Appendix C event trees. Frequency distributions for event sequences contributing to the same release category are then statistically summed to determine the frequency distributions for the release category. These

category frequency distributions are listed in Section C.9, and the mean frequency for each release category is reported in Table 9-1.

The component level data base used in the frequency assessment is described in Appendix B. This data base includes component operating failure rates, demand failure probabilities, common mode failure fractions, repair times, and uncertainty distributions. Appendix B also contains the offsite power reliability and restoration model used in the assessment. Appendix A contains the probabilistic failure models used in predicting the failure rate and size distribution for primary coolant leaks.

The technique used to quantify the uncertainty in frequency probabilities is the same as that used in the Reactor Safety Study (Ref. 7-1) and is known as the Monte Carlo method of error propagation. The method consists of statistically combining the uncertainty distribution for the input parameters associated with each fault tree using Monte Carlo simulation to arrive at an uncertainty distribution for the branch point probability. In a similar manner, the various probability distributions for the event tree branch points may be combined to yield the uncertainty distribution for an event sequence. With the use of the methods introduced earlier, an algebraic expression is obtained relating the desired branch point probabilities to the input parameters, e.g., failure rates, repair times, and common mode parameters. Uncertainties in the input parameters are considered by assigning an uncertainty distribution to each parameter. This information is then input to the computer code STADIC-2 (Ref. 7-2), which uses Monte Carlo simulation of the distributions to generate an uncertainty distribution in the branch point probability as well as the mean and median estimates for the accident sequence frequencies. More discussion of the methods used to quantify the uncertainties is found in Appendix C.

The following are the seven initiating events identifed for further study in Section 5:

1. Primary coolant leaks,
2. Loss of main loop cooling,
3. Earthquakes,
4. Loss of offsite power with turbine trip,
5. Anticipated transients requiring scram,
6. Inadvertent control rod withdrawal,
7. Steam generator leaks.

This set of initiating events was selected as covering the dominant precursors to radiological release commensurate with the current stage of the MHTGR design. As such, they are believed to provide adequate bases for meeting the objectives of this study as discussed in Section 1.

A summary of the analyses of these seven initiating events is given in the following seven sections (Section 7.1 through 7.7) while Section 7.8 contains references for this section.

7.1. PRIMARY COOLANT LEAKS

As an initiating event, primary coolant leaks are of interest for several reasons. Because of the activity circulating with the primary coolant or plated out around the primary coolant circuit, failure of the primary coolant pressure boundary necessarily results in some, albeit limited, release of radionuclides to the environment regardless of any subsequent plant response. Additionally, if the leak is of sufficient size, the damage to surrounding equipment resulting from the leak may threaten the integrity of core cooling systems, and allow for graphite oxidation as a result of air ingress. Given that a leak occurs, various possible plant responses which affect consequence determination are possible. The assessment shows primary coolant leaks to be the most likely

source of radionuclide release. Very small leaks <0.65 cm^2 (<1 $in.^2$) are predicted to occur more often than once in four years of plant operation. Larger leaks, up to failures of the relief valve train line, are shown to be significantly less likely. Further, the assessment shows the likelihood of a loss of forced circulation cooling occurring in combination with a primary coolant leak to be approximately twice in a thousand years of plant operation (2×10^{-3} per plant year).

7.2. LOSS OF MAIN LOOP COOLING

The loss of main loop cooling is initiated by equipment failures within the plant which preclude continued operation of the HTS in one or more modules. As an initiating event, the loss of main loop forced circulation core cooling is of interest as a challenge to the function of removing core heat and consequently a potential precursor to the incremental releases from fuel as discussed in Section 5 (see Fig. 5-2). Given that such an event occurs, various possible MHTGR responses resulting in differing alternative cooling modes are possible. The assessment shows the likelihood of event sequences that could lead to a radionuclide release as a consequence of a loss of main loop coding to be extremely remote. The mean frequency of any such sequence has been assessed at just under 1×10^{-7} per plant year.

7.3. EARTHQUAKES

The equipment damage produced by the vibrations during an earthquake causes seismic events to be the most important class of external events because it (1) simultaneously challenges redundant equipment in each of the modules; and (2) poses one of the few potential risks to passive equipment. The radiological risk from seismic events is nevertheless limited because severe earthquakes with intensities sufficient to damage key systems and structures are very unlikely, and only a few components are required to function in any case. No event sequence with a radionuclide release is predicted to occur with a mean frequency of

greater than 7 x 10^{-7} per year, at which point earthquakes of sufficient severity to damage the primary coolant boundary are predicted.

7.4. LOSS OF OFFSITE POWER

The normal station electrical power equipment refers to the normal loads in the energy conversion train for power production such as the HTS circulators, condensate pumps, and feed pumps. A loss of normal station power (LOSP) occurs when, for any reason, the power flow from the grid (via the main or auxiliary transformers) is lost and the turbine generators inadvertently trip instead of maintaining their load and continuing to remove heat.

A LOSP is of interest as an initiating event because it is externally caused, and because it can simultaneously challenge multiple systems. For example, if offsite power is lost and both turbines trip, main cooling loops in all four modules are shut down which challenges core heat removal and, consequently, may result in incremental fuel releases from thermal mechanisms as discussed in Section 5. Nevertheless, the passive features at the MHTGR are such that no event sequence which could result in radionuclide release is predicted to occur within the frequency range considered in this study.

7.5. ANTICIPATED TRANSIENTS REQUIRING SCRAM

There are a number of off-normal plant transients for which the PPIS is designed to detect the upset condition and as a part of the automatic response, reduce the heat that must be removed from the core by initiating a reactor shutdown (scram) in one or more modules with the control rods. Such a transient without successful scram is of interest as a challenge to the continued control of core heat generation. In challenging this function, the ATWS represents a potential precursor to failure of the primary coolant boundary (relief valve lifting) simultaneous with the incremental releases from fuel involving thermal

effects discussed in Section 5. However as described in Section 6 of this report, the negative temperature coefficient and high temperature integrity of the ceramic core provide the MHTGR with the capability to sustain such an ATWS for extended periods of time without adverse consequence. This, when considered with the high reliability of two diverse shutdown systems, results in the assessment showing no event sequences with radiological release within the range of frequencies studied.

7.6. INADVERTAINT CONTROL ROD WITHDRAWAL

Inadvertent control rod withdrawal is initiated by failures in the rod control equipment that lead to the undesired withdrawal of one or more control rods from the core. As an accident initiating event, rod withdrawal is of interest because of its potential challenge to the continued control of core heat generation. In challenging this function, the rod withdrawal represents a potential precursor to failure of the primary coolant boundary (relief valve lifting) simultaneous with the incremental releases from fuel involving thermal effects discussed in Section 5. However, as described in Section 6, withdrawal of a complete control rod group results in only localized fuel temperature rise and by itself is not expected to result in any offsite consequence. This has been shown to be true even in the case where reactor trip fails to occur.

As a result, the frequency assessment for this accident initiator has shown no event sequence of meaningful probability initiated by control rod withdrawal and having the potential to result in offsite release.

7.7. STEAM GENERATOR LEAKS

Water ingress is selected as an initiating event because of the potential for primary coolant release due to relief valve venting and for incremental fuel releases due to chemical attack (hydrolysis) of the

fuel. Furthermore, water ingress is of interest due to its reactivity effect on the core. In the assessment it is shown that the most likely event sequences following a moisture ingress result in no dose. Only in those sequences where certain mitigating features (e.g., steam generator isolation and dump) fail to perform their functions, are offsite doses predicted. The likelihood of such a water ingress induced release is assessed at somewhat less than once in 10,000 yr (1×10^{-4} per plant year) as shown in Appendix C. Further the assessment shows the likelihood of a water ingress induced release in combination with a failure of forced circulation core cooling to be approximately four times in 100,000 yr of plant operation (4×10^{-5} per plant year).

7.8. REFERENCES

7-1. U.S. NRC, "Reactor Safety Study," NUREG-75/014, (WASH-1400), 1975.

7-2. Koch, P. K., and H. E. St. John, "STADIC-2, A Computer Program for Combining Probability Distributions," GA Report GA-A16227, July 1983.

8. ACCIDENT CONSEQUENCES

In the risk assessment, accident sequences are identified that may lead to an uncontrolled or unplanned radiological release. In this section, the consequences of representative accident sequences are evaluated in terms of the resultant dose to an individual at the plant exclusion area boundary (EAB). The results are reported for whole body gamma, thyroid, bone, and lung doses.

Section 5 identifies important initiating events which may lead to radiological release. Plant response to these initiating events and system reliability models are discussed in Section 6. The description of plant response was utilized in Section 7 to construct event trees, which depict the various event sequences possible following each initiating event. Each event sequence's frequency was then assessed. In this section, the consequences of each event sequence were considered, and similar consequence events were grouped into one of several release categories. For a representative sequence in each release category, the resultant plant transient, radiological release, and dose consequences were evaluated.

The accidents considered in Section 7 that result in dose consequences are evaluated in this section. These accidents include fission product releases from forced convection cooldowns under dry and under wet conditions, and from conduction cooldowns under dry and wet conditions. Forced convection cooldowns under dry conditions are initiated by primary coolant leaks. The fission product release is due to fractional release of circulating and plateout activity. Forced convection cooldowns under wet conditions are initiated by steam generator leaks. The fission product release is due to fractional releases from oxidation of graphite and hydrolysis of failed fuel in addition to fractional

release of circulating and plateout activity. Conduction cooldowns involve loss of forced convection cooling and therefore rely on conduction and radiation to remove heat from the reactor core out to the RCCS. The incremental fission product release is due to fractional releases from heatup of the fuel particles. Conduction cooldowns under dry conditions are initiated by primary coolant leaks, loss of main loop cooling, and seismic activity. Conduction cooldowns under wet conditions are initiated by steam generator leaks. The consequences from forced convection cooldowns under dry conditions are discussed in Section 8.1. The consequences from forced convection cooldowns under wet conditions are presented in Section 8.2. The consequences from conduction cooldowns under dry conditions are discussed in Section 8.3. The consequences from conduction cooldowns under wet conditions are presented in Section 8.4.

The details of the accident categories and for each category the supporting data and models, the fission product release and the resultant dose assessment, and the uncertainty analysis are discussed in Appendix D.

8.1. CONSEQUENCES FROM FORCED CONVECTION COOLDOWNS UNDER DRY CONDITIONS

A number of release categories that are initiated by primary coolant leaks have been identified in Section 7 as forced convection cooldown under dry conditions. The categories are labeled DF-1 through DF-4 where DF-1 has the greatest consequence and DF-4 has the least nonzero consequence. The categories are described in Table 8-1. The consequence source term for forced convection cooldowns under dry conditions includes a portion of the circulating activity and the liftoff of a fraction of the activity plated-out on primary circuit surfaces. Incremental release of radionuclides from the fuel body inventory is prevented by forced convection cooling of the reactor core, which is provided in all cases by either the HTS or the SCS.

TABLE 8-1
RELEASE CATEGORY DESCRIPTIONS FOR FORCED
CONVECTION COOLDOWNS UNDER DRY CONDITIONS

Release Category	Descriptions
DF-1	Primary coolant leak occurs where 6.5 $cm^2 \leq$ Area $<$ 84 cm^2 (1 $in.^2 \leq$ Area $<$ 13 $in.^2$). Reactor is tripped. HTS or SCS maintains forced convection cooling. HPS pumpdown is ineffective. Radionuclides are released through the reactor building dampers.
DF-2	Primary coolant leak occurs where 0.2 $cm^2 \leq$ Area $<$ 6.5 cm^2 (0.03 $in.^2 \leq$ Area $<$ 1 $in.^2$). Reactor is tripped. HTS or SCS maintains forced convection cooling. HPS pumpdown is ineffective. Radionuclude release leaks to the environment after some retention in the reactor building.
DF-3	Primary coolant leak occurs where 2 x 10^{-4} $cm^2 \leq$ Area $<$ 0.2 cm^2 (3 x 10^{-5} $in.^2 \leq$ Area $\leq$ 0.03 $in.^2$) Reactor is tripped. HTS or SCS maintains forced convection cooling. HPS pumpdown fails. Radionuclide release leaks to the environment after some retention in the reactor building.
DF-4	Primary coolant leak occurs where 2 x 10^{-4} $cm^2 \leq$ Area $<$ 0.2 cm^2 (3 x 10^{-5} $in.^2 \leq$ Area $<$ 0.03 $in.^2$). Reactor is tripped. HTS or SCS maintains forced convection cooling. HPS pumpdown occurs. Radionuclide release leaks to the environment after some retention in the reactor building.

The circulating and liftoff activities are released through the breach in the primary coolant boundary into the reactor building. For smaller leak sizes, the consequences are reduced by pumpdown of primary coolant to storage bottles by the HPS. For larger leak sizes pumpdown becomes ineffective, and essentially 100% of the circulating activity is released into the reactor building. The fraction of material lifted-off at a given location in the primary circuit increases when helium flow velocities increase at the location. Once in the reactor building, fission products are depleted by the natural processes of radioactive decay, plateout on building surfaces, and by particulate settling. The fission products can be transported from the reactor building to the atmosphere by building leakage or through the building dampers if the depressurization rate from the vessel exceeds the building leak rate.

The consequences from forced convection cooldowns under dry conditions are discussed in Appendix D.1. The median, ninety-fifth percentile, and fifth percentile results of the dose uncertainty analysis for each release category are presented in Table 8-2 for 30-day EAB thyroid and whole body gamma doses.

8.2. CONSEQUENCES FROM FORCED CONVECTION COOLDOWNS UNDER WET CONDITIONS

A number of event sequences that are initiated by small and moderate steam generator leaks have been identified in Section 7. Only those sequences that result in fission product release to the environment are addressed here. These sequences have been grouped and categorized as forced convection cooldowns under wet conditions. The categories are labeled WF-1 through WF-4 where WF-1 has the greatest consequence and WF-4 has the least nonzero consequence. The categories are described in Table 8-3. Release categories that exhibit doses have release paths that vent to the reactor building through the primary coolant relief valves before reaching the environment. The consequence source term for forced convection cooldowns under wet conditions consists of (1) circulating activity, (2) steam-induced recirculation of activity plated-out

TABLE 8-2
DOSE UNCERTAINTY ANALYSIS AT THE EAB FOR FORCED CONVECTION COOLDOWN UNDER DRY CONDITIONS

Release Category	Leak Size ($in.^2$)	Dose in Rem					
		Whole Body γ			Thyroid		
		5%	Median	95%	5%	Median	95%
DF-1	1.0	4.5-05	2.9-04	2.7-03	2.5-04	1.4-03	9.1-03
DF-2	0.1	2.3-05	1.4-04	1.1-03	2.6-05	3.5-04	4.5-03
DF-3	0.01	2.6-06	1.7-05	1.8-04	4.6-06	6.6-05	8.5-04
DF-4	0.01	1.5-06	9.2-06	9.0-05	1.4-06	2.5-05	3.0-04

TABLE 8-3
RELEASE CATEGORY DESCRIPTIONS FOR FORCED
CONVECTION COOLDOWNS UNDER WET CONDITIONS

Release Category	Descriptions
WF-1	Moderate steam generator leak occurs. Reactor trip occurs. Steam generator isolation from steam heater is delayed. Isolation and dump of the steam generator occurs within 20 min. SCS maintains forced convection cooling. Primary relief valve opens and fails to reclose. Radionuclides are released through the reactor building dampers.
WF-2	Moderate steam generator leak occurs. Reactor trip occurs. Steam generator isolation and dump is delayed up to 30 min. SCS maintains forced convection cooling. Primary relief valve opens and fails to reclose. Radionuclides are released through the reactor building dampers.
WF-3	Moderate steam generator leak occurs. Moisture monitors detect leak. Steam generator isolation is delayed. Isolation and dump of the steam generator occurs within 30 min. SCS maintains forced convection cooling. Primary relief valve opens and successfully recloses. Radionuclides are released through the reactor building dampers.
WF-4	Moderate steam generator leak occurs. Reactor trip occurs. Steam generator isolation and dump is delayed up to 30 Min. SCS maintains forced convection cooling. Primary relief valve opens and successfully recloses. Radionuclides are released through the reactor building dampers.

on primary circuit surfaces, (3) release from initially failed fuel due to hydrolysis, and (4) release from oxidized graphite. In all cases, the reactor core is cooled by forced convection provided by the SCS, which prevents any thermally induced incremental release of radionuclides from the fuel body inventory.

The frequency assessment in Appendix C.7 for small steam generator leaks covers a spectrum of leak sizes ranging from pinhole to approximately 0.053 cm^2 (8×10^{-3} $in.^2$). The maximum size considered for small steam generator leaks corresponds to a flow rate of 0.05 kg/s (0.1 lbm/s) which will be used in the consequence assessment for all small leaks. The frequency assessment in Appendix C.8 for moderate steam generator leaks covers a spectrum of leak sizes ranging from 0.053 to 6.6 cm^2 (8×10^{-3} to 1 $in.^2$). The flow rates may range from 0.05 to 5.7 kg/s (0.1 to 12.5 lbm/s) with the latter flow rate corresponding to a single tube offset rupture. The consequence assessment for moderate steam generator leaks has been based on a leak rate of 5.7 kg/s (12.5 lbm/s). In all of the release categories considered in this section, forced convection cooling is present. Conduction cooldowns initiated by steam generator leaks are considered in Section 8.4.

The consequences from forced convection cooldowns under wet conditions are discussed in Appendix D.2. The median, ninety-fifth percentile, and fifth percentile results of the dose uncertainty analysis for thyroid and whole body gamma doses for a 30-day exposure at the EAB are presented in Table 8-4.

8.3. CONSEQUENCES FROM CONDUCTION COOLDOWNS UNDER DRY CONDITIONS

A number of event sequences that are initiated by primary coolant leaks and seismic activity have been identified in Section 7. Only those sequences that result in fission product release are addressed here. These sequences have been grouped and categorized as conduction cooldowns under dry conditions. The categories are labeled DC-1 through

TABLE 8-4
DOSE UNCERTAINTY ANALYSIS AT THE EAB FOR FORCED CONVECTION COOLDOWNS UNDER WET CONDITIONS

Release Category	Doses at EAB (Rem)					
	Whole Body γ			Thyroid		
	5%	Median	95%	5%	Median	95%
WF-1	2.6-04	2.2-03	1.9-02	3.8-02	3.4-01	3.1+00
WF-2	2.0-04	1.7-03	1.4-02	3.1-02	2.8-01	2.5+00
WF-3	3.9-05	3.3-04	2.8-03	5.8-03	5.2-02	4.6-01
WF-4	4.8-05	2.6-04	2.2-03	4.7-03	4.2-02	3.8-01

DC-9 where DC-1 has the greatest consequence and DC-9 has the least nonzero consequence. The categories are described in Table 8-5. The consequence source term for conduction cooldowns under dry conditions includes (1) the circulating activity, (2) fission product release from the fuel due to high temperatures, and (3) liftoff of a portion of the activity plated-out on primary circuit surfaces.

The consequences from conduction cooldowns under dry conditions are discussed in Appendix D.3. The median, ninety-fifth percentile, and fifth percentile results of the dose uncertainty analysis for thyroid and whole body gamma doses for a 30-day exposure at the EAB are presented in Table 8-6.

8.4. CONSEQUENCES FROM CONDUCTION COOLDOWNS UNDER WET CONDITIONS

A number of event sequences that are initiated by small and moderate steam generator leaks have been identified in Section 7. Only those sequences that result in fission product release and on offsite dose to the public are addressed here. These sequences have been grouped and categorized as conduction cooldowns under wet conditions. The categories are labeled WC-1 through WC-7 where WC-1 has the greatest consequence and WC-7 has the least nonzero consequence. The categories are described in Table 8-7. The consequence source term for conduction cooldowns under wet conditions includes (1) the circulating activity, (2) fission product release from the fuel due to high temperatures, (3) steam-induced vaporization and recirculation of a portion of the activity plated-out on primary circuit surfaces, (4) release from failed fuel due to hydrolysis, and (5) release from oxidized graphite.

The consequences from conduction cooldowns under wet conditions are discussed in Appendix D.4. The median, ninety-fifth percentile, and fifth percentile results of the dose uncertainty analysis for thyroid and whole body gamma doses for a 30-day exposure at the EAB are presented in Table 8-8.

TABLE 8-5
RELEASE CATEGORY DESCRIPTIONS FOR CONDUCTION
COOLDOWNS UNDER DRY CONDITIONS

Release Category	Descriptions
DC-1	Earthquake with ground accelerations greater than 0.8 g causes instrument line failure in all four modules. Reactor is tripped. HTS, SCS, and RCCS fail in all four modules due to high ground accelerations. HPS pumpdown is also not available. Reactor vessel is depressurized. Radionuclides are released to the atmosphere after some retention in the reactor building.
DC-2	Loss of main loop cooling occurs. Reactor is tripped. SCS fails to maintain forced convection cooling. RCCS cooling fails. Primary system is depressurized using HPS pumpdown within 2 days. Radionuclides release leaks to the environment after some retention in the reactor building. Reactor building silo is sealed some time after 100 h.
DC-3	Primary coolant leak occurs in all four modules due to earthquake where Area $\geq$ 0.19 cm^2 (Area $\geq$ 0.03 $in.^2$). Reactor is tripped. HTS and SCS fail to maintain forced convection cooling. Passive cooling by the RCCS continues. HPS pumpdown fails. Radionuclides release leaks to the environment after some retention in the reactor building.
DC-4	Primary coolant leak occurs where 0.013 cm^2 < Area < 0.19 cm^2 (2×10^{-3} < Area < 0.03 $in.^2$). Reactor is tripped. HTS and SCS fail to maintain forced convection cooling. Passive cooling by the RCCS continues. HPS pumpdown fails. Radionuclide release leaks to the environment after some retention in the reactor building.

TABLE 8-5 (Continued)

Release Category	Descriptions
DC-5	Primary coolant leak occurs where 0.19 $cm^2 \leq$ Area $\leq$ 6.5 cm^2 (0.03 $in.^2 \leq$ Area $\leq$ 1 $in.^2$). Reactor is tripped. HTS and SCS fail to provide forced convection cooling. Passive cooling by RCCS continues. HPS pumpdown fails. Radionuclides release leaks to the environment after some retention in the reactor building.
DC-6	Primary coolant leak occurs where 0.013 $cm^2 \leq$ Area $\leq$ 0.19 cm^2 (2×10^{-3} $in.^2 \leq$ Area $\leq$ 0.03 $in.^2$). Reactor is tripped. HTS and SCS fail to provide forced convection cooling. Passive cooling by RCCS continues. HPS pumpdown is successful. Radionuclide release leaks to the environment after some retention in the reactor building.
DC-7	Primary coolant leak occurs where 0.19 $cm^2 \leq$ Area $\leq$ 6.5 cm^2 (0.003 $\leq$ Area $\leq$ 1 $in.^2$). Reactor is tripped. HTS and SCS fail to maintain forced convection cooling. Passive cooling by RCCS continues. HPS pumpdown is successful. Radionuclide release leaks to the environment after some retention on the reactor building.
DC-8	Primary coolant leak occurs where Area $\geq$ 6.5 cm^2 ($\geq$ 1 $in.^2$). Reactor is tripped. HTS and SCS fail to maintain forced convection cooling. Passive cooling by RCCS continues. HPS pumpdown is ineffective for this leak size. Radionuclides are released through the reactor building dampers.
DC-9	Primary coolant leak where 1.9×10^{-4} $cm^2 \leq$ Area $<$ 0.013 cm^2 (3×10^{-5} $in.^2 \leq$ Area $<$ 2×10^{-3} $in.^2$). HTS and SCS fail to maintain forced convection cooling. Passive cooling by the RCCS continues. HPS pumpdown is ineffective. Radionuclide release leaks to the environment after some retention in the reactor building.

TABLE 8-6
DOSE UNCERTAINTY ANALYSIS AT THE EAB FOR CONDUCTION COOLDOWNS UNDER DRY CONDITIONS

Release Category	Dose in Rem					
	Whole Body γ			Thyroid		
	5%	Median	95%	5%	Median	95%
DC-1	1.0-02	6.4-02	4.5-01	6.0+00	5.0+01	4.3+02
DC-2	2.7-03	1.6-02	1.1-01	3.0+00	2.5+01	2.1+02
DC-3	4.8-05	2.9-04	2.3-03	2.0-02	2.1-01	2.2+00
DC-4	1.5-05	1.5-04	1.5-03	7.6-03	7.6-02	7.6-01
DC-5	1.2-05	7.3-05	5.8-04	5.1-03	5.3-02	5.5-01
DC-6	1.2-05	7.3-05	5.8-04	5.1-03	5.3-02	5.5-01
DC-7	6.5-05	3.2-04	2.2-03	3.0-03	4.9-02	5.9-01
DC-8	6.5-05	3.2-04	2.2-03	3.0-03	4.9-02	5.9-01
DC-9	2.1-06	1.0-05	7.2-05	3.4-04	5.5-03	6.6-02

TABLE 8-7
RELEASE CATEGORY DESCRIPTIONS FOR
CONDUCTION COOLDOWNS UNDER WET CONDITIONS

Release Category	Descriptions
WC-1	Small steam generator leak occurs. Moisture monitors detect leak. Reactor is tripped. Automatic isolation of the steam generator occurs. Steam generator dump valves fail to open. SCS fails to maintain forced convection cooling. Passive cooling by the RCCS continues. Primary relief valve opens and fails to reclose. Radionuclides are released through the reactor building dampers.
WC-2	Moderate steam generator leak occurs. Reactor is tripped. Steam generator is isolated within at most 6 min. Steam generator dump is delayed or malfunctions. SCS fails to maintain forced convection cooling. Passive cooling by the RCCS continues. Primary relief valve opens and fails to reclose. Radionuclides are released through the reactor building dampers.
WC-3	Small steam generator leak occurs. Moisture monitors detect leak. Reactor is tripped. Automatic isolation of the steam generator occurs. Steam generator dump valves fail to open. SCS fails to maintain forced convection cooling. Passive cooling by the RCCS continues. Primary relief valve opens and successfully recloses. Radionuclides are released through the reactor building dampers.
WC-4	Moderate steam generator leak occurs. Reactor is tripped. Moisture monitors detect leak. Steam generator isolation is delayed when steam valves fail open. Manual isolation and dump of the steam generator occurs within 20 min. SCS fails to maintain forced cooling. Passive cooling by RCCS continues. Primary relief valve opens and successfully recloses.

TABLE 8-7 (Continued)

Release Category	Descriptions
	Radionuclides are released through the reactor building dampers.
WC-5	Moderate steam generator leak occurs. Reactor is tripped. Moisture monitors detect leak. Automatic isolation of the steam generator occurs. SCS fails to maintain forced convection cooling. Passive cooling by the RCCS continues. Primary relief valve opens and fails to reclose. Radionuclides are released through the reactor building dampers.
WC-6	Moderate steam generator leak occurs. Reactor is tripped. Steam generator is isolated with at least 6 min (either by moisture monitor detection or high pressure signal). Steam generator dump is delayed or malfunctions. SCS fails to maintain forced convection cooling. Passive cooling by the RCCS continues. Primary relief valve opens and successfully recloses. Radionuclides are released through the reactor building dampers.
WC-7	Moderate steam generator leak occurs. Reactor is tripped. Moisture monitors fail to detect leak. Automatic isolation and dump of the steam generator occurs. SCS fails to maintain forced convection cooling. Passive cooling by the RCCS continues. Primary relief valve opens and successfully recloses. Radionuclides are released through the reactor building dampers.

TABLE 8-8
DOSE UNCERTAINTY ANALYSIS AT THE EAB FOR FORCED CONVECTION COOLDOWNS UNDER WET CONDITIONS

Release Category	Doses at EAB (Rem)					
	Whole Body γ			Thyroid		
	5%	Median	95%	5%	Median	95%
WC-1	5.1-04	6.2-03	7.4-02	1.7-01	2.4+00	3.4+01
WC-2	1.6-04	1.6-03	1.6-02	3.6-02	3.7-01	3.8+00
WC-3	1.9-05	2.3-04	2.7-03	6.7-03	9.6-02	1.4+00
WC-4	1.2-05	1.4-04	1.7-03	3.8-03	5.4-02	7.7-01
WC-5	1.1-04	8.0-04	6.1-03	4.5-03	4.7-02	4.8-01
WC-6	5.5-06	5.5-05	5.6-04	2.1-03	2.1-02	2.2-01
WC-7	3.2-06	3.9-05	4.6-04	1.7-04	2.4-03	3.5-02

9. RISK ASSESSMENT RESULTS

The results of this safety risk assessment show the MHTGR to behave in an extraordinarily benign manner with only limited offsite releases predicted during even extremely unlikely accidents. Accordingly, the concept is shown to comply with the risk limits of the NRC Safety Goals (Ref. 9-1) and to do so with substantial margin. The MHTGR is also shown to be capable of satisfying the very stringent user-imposed requirement that to Protective Action Guideline (PAG) doses related to public evacuation and sheltering are met at the 425 m (1400 ft) site Exclusion Area Boundary (EAB). PRA results demonstrate that releases with frequencies as low as 5×10^{-7} per year are below the PAG sheltering limits of 1 Rem Whole Body and 5 Rem Thyroid at the site EAB.

The results of this PRA substantiate that the Licensing Basis Events (LBEs) selected in the Preliminary Safety Information Document form a complete set as also shown in Ref. 9-3.

In this section, the quantification of the incremental addition to public risk attributable to abnormal occurrences during MHTGR operation is described described. The results of this quantification are further discussed in more detail as they relate to the safety of the concept in the following four major areas:

1. Quantification of risk and identification of the important accident sequences which either dominate risk or have the highest consequences (Sections 9.1 and 9.2).

2. An interpretation of what the results imply about the MHTGR design and what they mean in terms of public health (Section 9.3).

3. Confirmation of the completeness of Licensing Basis Event selection (Ref. 9-3) made in support of the Preliminary Safety Information Document (Section 9.3).

4. A numerical judgment as to the acceptability of the results by comparing them to the risk and dose criteria mentioned in Section 2.2 (Section 9.3).

Assessment results are presented in Section 9.1 using two formats, as an annualized expectation of offsite dose (mean risk) and, as complementary cumulative frequency curves to present the uncertainty ranges associated with assessment results. In both cases, whole body gamma and thyroid doses for a 30-day exposure at the EAB are developed. Section 9.2 describes the dominant contributors to the cited risk. Finally, in Section 9.3, conclusions that can be drawn from these results are discussed.

9.1. QUANTIFICATION OF RISK

The safety risk for the MHTGR is a function of the frequency of occurrence and the consequence to the public of the various accidents examined in this assessment. Quantification of that risk is performed by combining the accident frequencies and their uncertainties from Appendix C with the consequences and their uncertainties from Section 8.

9.1.1. Mean Risk Estimate

Mean risk is defined as the product of mean frequency and consequence. One method of interpreting the risk assessment results is to find this product for each of the different accident categories considered, sum the individual risks, and view the result as a single expectation value for plant risk. This approach, while having certain limitations, is simple and necessary if the plant is to be compared against risk limits that are included in the NRC Safety Goals. Such a

treatment of mean risk has been done for the MHTGR in tabular form and is described here.

Table 9-1 shows the values for mean frequency and consequence for each of the catagories release identified in Section 8. As can be seen, the consequence for every category includes both a whole body and a thyroid exposure expressed in Rem. These calculated doses may be thought of as the expected doses to the maximum exposed individual remaining at the plant EAB without evacuation. For each of the release categories, the frequency and consequence values have been combined, giving the mean risk to that theoretical individual, in Rem per year. The mean risk represents the individual risk at the EAB from each of the accident categories. The total mean risk estimate is 3×10^{-5} Rem per year whole body and 3×10^{-4} Rem per year thyroid. Note that release category dose and risk estimates in Table 9-1 are conservative relative to compliance with NRC Safety Goal and not directly comparable to other risk assessments since they were evaluated for an individual remaining at the plant EAB of 425 for 30 days and nights. Risk assessments calculations, as specified in Ref. 9-1, typically are based on a group of individuals exposed within a 10-mile emergency planning zone (EPZ) surrounding the plant and that many of these individuals may be evacuated. However, the calculation of risk in this assessment is based upon the maximum dose at a much smaller EPZ beyond which user requirements (Ref. 9-4) specify public shelter or evacuation shall be unnecessary.

9.1.2. Risk Envelope Plot

The complementary cumulative distribution curve of frequency versus consequence (typically called a risk curve or envelope) is a second method used to display risk assessment results. At a glance, it shows the likelihood of having an accident whose consequence exceeds a severity of interest. Because of this, it is a useful tool for showing how the plant compares when measured against a frequency-dependent consequence (dose) design goal. Furthermore, while total plant risk is not

TABLE 9-1
PUBLIC RISK FROM RELEASE CATEGORIES

Release Category	Mean Frequency of Release Category (per year)	Mean Dose[a] (rem)		Mean Risk[a] (rem/yr)	
		Whole Body	Thyroid	Whole Body	Thyroid
DF-1	1×10^{-2}	1×10^{-3}	3×10^{-3}	1×10^{-5}	3×10^{-5}
DF-2	4×10^{-2}	3×10^{-4}	1×10^{-3}	1×10^{-5}	4×10^{-5}
DF-3	1×10^{-2}	1×10^{-4}	2×10^{-4}	1×10^{-6}	2×10^{-6}
DF-4	0.3	4×10^{-5}	9×10^{-5}	1×10^{-5}	3×10^{-5}
WF-1	5×10^{-8}	5×10^{-3}	0.8	3×10^{-10}	4×10^{-8}
WF-2	4×10^{-6}	4×10^{-3}	0.7	2×10^{-8}	3×10^{-7}
WF-3	1×10^{-6}	8×10^{-4}	0.1	8×10^{-10}	1×10^{-7}
WF-4	6×10^{-5}	6×10^{-4}	0.1	4×10^{-8}	6×10^{-6}
DC-1	9×10^{-8}	0.1	1×10^{2}	9×10^{-9}	9×10^{-6}
DC-2	8×10^{-8}	3×10^{-2}	5×10^{1}	2×10^{-9}	4×10^{-6}
DC-3	7×10^{-7}	8×10^{-4}	0.5	6×10^{-10}	4×10^{-7}
DC-4	5×10^{-5}	4×10^{-4}	0.2	2×10^{-8}	1×10^{-5}
DC-5	3×10^{-5}	2×10^{-4}	0.1	6×10^{-9}	3×10^{-6}
DC-6	5×10^{-4}	2×10^{-4}	0.1	1×10^{-7}	5×10^{-5}
DC-7	3×10^{-4}	8×10^{-4}	0.1	2×10^{-7}	3×10^{-5}
DC-8	8×10^{-5}	8×10^{-4}	0.1	6×10^{-8}	8×10^{-6}
DC-9	2×10^{-3}	2×10^{-5}	2×10^{-2}	4×10^{-8}	4×10^{-5}
WC-1	2×10^{-7}	2×10^{-2}	9	4×10^{-9}	2×10^{-6}
WC-2	3×10^{-7}	4×10^{-3}	1	1×10^{-9}	3×10^{-7}
WC-3	6×10^{-6}	7×10^{-4}	0.4	4×10^{-9}	2×10^{-6}
WC-4	2×10^{-7}	4×10^{-4}	0.2	8×10^{-11}	4×10^{-8}
WC-5	1×10^{-6}	2×10^{-3}	0.1	2×10^{-9}	1×10^{-7}
WC-6	8×10^{-6}	1×10^{-4}	6×10^{-2}	8×10^{-10}	5×10^{-7}
WC-7	4×10^{-5}	1×10^{-4}	9×10^{-3}	4×10^{-9}	4×10^{-7}
		Total Risk:		3×10^{-5}	3×10^{-4}

[a]Doses and risk values evaluated for a maximum exposed individual located at the plant EAB of 425 m without evacuation.

explicitly plotted, the curve can be used to quickly identify the major contributors to that total risk. This differs from the approach taken in Section 9.1.1 because mean risk signifies what is expected to occur when considered on an annualized average basis. This average, though, does not necessarily correspond to any real accident scenario. In contrast, using a risk curve, doses that would result from specific accident scenarios, despite their being unlikely, can be seen.

Complementary cumulative frequency curves are generated by combining the mean (expected) frequency, based upon uncertainty distributions from a frequency assessment with the dose uncertainty distributions from an analysis. A complementary cumulative frequency curve for a given accident category is generated by multiplying the mean or expected frequency of occurrence with the complementary cumulative dose uncertainty distribution. The complementary cumulative dose distribution asymptotes to unity at low doses indicating that given the accident sequence occurs the probability of exceeding small doses is certain. Hence, the complementary cumulative frequency curves asymptote on the left to the mean accident frequency and display the expected frequency per plant year at which a specified level of accident consequence is exceeded.

Figures 9-1 and 9-2 are two such curves showing the total probability of exceeding specified doses considering all release categories evaluated in the assessment. The two curves depict whole body gamma and thyroid dose consequences, respectively. In addition, these figures also show how the sum of the release categories, grouped into four major accident types, making up the total envelope.

As described in Section 8, the release categories are defined based upon accident sequence variables that can impact release and that allow the releases to be characterized relative to one another. While there are many variations among the release categories, the categories fall into one of four accident types. Differentiation among these accident types is made depending on whether water ingress has occurred (W) or not

(D) and whether heat removal from the core is accomplished with forced circulation core cooling (F) or conduction and radiation (C). Since no release can occur without the primary coolant boundary being breached in some manner, all the release categories imply some primary coolant leakage or release.

For example, the accident type made up of the several release categories prefixed DF is a transient where forced convection cooling is maintained with dry primary coolant conditions. This accident type includes events initiated by primary coolant leaks. The accident type made up of the several WF release categories is a transient where forced convection cooling is also maintained but where moisture ingress has led to "wet" primary coolant conditions. Category WF includes events initiated by small and moderate steam generator leaks. The accident types comprised of DC and WC release categories are conduction cooldown events in which all forced convection cooling provided by the HTS and the SCS is lost. Release categories designated DC are conduction cooldowns under dry conditions and include events initiated by primary coolant leaks, loss of main loop cooling, and seismic activity. Release categories prefixed with WC are conduction cooldowns under wet conditions and include events initiated by small and moderate steam generator leaks.

Figures 9-3 and 9-4 also contain complementary cumulative distribution curves of frequency. These figures, however, show the various release categories and how they make up the four accident types. Each plot, on the figures, shows sets of curves, each curve depicting one release category. On each of these plots is also shown an accumulated curve for representing the total for a single type of accident. It is these accumulated curves that are shown as making up the total risk envelope in Figs. 9-1 and 9-2. Tables 8-2, 8-4, 8-6, and 8-8 define, in greater detail, the individual release categories that contribute to

the accident types DF, WF, DC, and WC, respectively. The dominant contributors to individual release categories are discussed further in Section 9.2.

9.2. DOMINANT CONTRIBUTORS

The ability to quantify the plant risk is only one of the values of the PRA. Of equal, if not greater, value is that the PRA allows for identification of the important accident sequences. That is, PRA draws attention not only to those sequences that have the potential for the highest dose, but also to those sequences that while of only moderate consequence may, because of their frequency, be of high risk. For each release category, the dominant accident sequences in Appendix C event tree making up the category, have been identified in Table 9-1. This section discusses the sequences and release categories that are dominant contributors to plant risk.

Referring again to Table 9-1, it can be seen that the highest whole body risks are from release categories designated DF. These categories are initiated by leaks in the primary coolant boundary with a resulting release of circulating activity and reentrained material normally plated out around the primary coolant circuit. Because forced cooling is maintained, there is no incremental fuel release. Note that even at the low frequency, higher consequence end of these release categories, EAB doses in excess of one Rem are not predicted. None of the DF release categories has a particularly large dose associated with it. Rather, the importance of the DF categories to total risk stems from their relatively high frequency as compared to other release categories.

Viewing Fig. 9-1, it can be seen that not only are accidents belonging to category DF the largest whole body risk contributors, but also that they dominate the risk envelope for whole body gamma doses across the range of frequencies evaluated. This risk dominance occurs inspite of the low consequencies associated with this accident category

because of the relatively higher probability at which they occur. Referring to Fig. 9-3, it is noted that at high frequencies, the high risk categories DF-1, DF-2 and DF-4 define the risk envelope; but at low frequencies, the risk envelope is dominated by DF-1. The DF-1 release category is similar to the other DFs mentioned but is differentiated by a larger (greater than 1 in.) characteristic leak size.

In Table 9-1, it can be seen that the highest thyroid risks are from the DF and DC categories. Again, most accidents contributing to these release categories are initiated by primary coolant leaks in which the doses are not particularly large. As in the case of whole body dose, the importance of these categories to total risk stems from their relatively high occurrence frequencies compared to other release categories.

Figure 9-2 indicates that accidents belonging to category DF define the overall risk envelope for thyroid doses at high frequencies (i.e., within a plant lifetime). As for the whole body dose, release categories DF-1, DF-2 and DF-4 dominate the thyroid risk envelope at these high frequencies. At moderate to low frequencies, however, categories of the DC type are dominant. Figure 9-4 shows that among the several DC release categories, DC-5 through DC-8 are the most important at these frequencies. The accident scenario typifying these DC category are also primary coolant leaks. However, in this case, forced cooling is lost after some period of time and the core experiences a temperature transient which results in some release.

Also contributing to the low frequency portion of the Fig. 9-2 risk curve is WC-3, the water ingress event without forced cooling. This category is characterized by a small steam generator leak in which the moisture monitors successfully detect the leak and the steam generator is successfully isolated. However, the steam generator dump system malfunctions and the SCS is unable to provide forced convection cooling.

In WC-3 the pressure rise due to moisture entering the primary system causes the relief valve to open and reclose.

9.3. COMPARISON WITH MHTGR DESIGN AND REGULATORY LIMITS

This assessment of plant safety, in considering a broad range of accidents covering both a cross section of initiating events and an extreme frequency spectrum, shows the MHTGR to display an exceptionally high-level of safety. By virtue of its high reliance on passive features inherent in this small MHTGR, the overall safety of the concept is shown to be relatively insensitive to failures in active systems or operator action.

Furthermore, the assessment supports the underlying approach to safety that has been taken with the MHTGR. This approach focuses on assuring retention within the high-temperature ceramic HTGR fuel to prevent the gross release of fission products. Throughout the assessment, no accident scenarios of meaningful probability were identified that could compromise the fuel and lead to such a release. Rather, the accident scenarios identified all relate to releasing some portion of the fission product inventory associated with the very small fraction of fuel that is defective in its fabrication. As a result, it is observed that despite the range of frequencies considered in the assessment, none of the releases identified would be sufficient to cause any measurable health effect in the population surrounding the plant.

A review of the dominant accident sequences identified in Section 9.2 leads to the notable observation that the risk attributable to the MHTGR, small as it is, largely results from the failure of passive components rather than failures in active or powered systems. For example, Table 9-1 shows the highest risk scenarios to result from leakage of primary coolant as a result of failures in the primary pressure boundary. In contrast, accident scenarios initiated by loss of forced cooling or loss of offsite power contribute essentially nothing to plant

risk. This characterization of the dominant risk contributors is a direct result of the high reliance placed on passive features in the MHTGR design. Thus, by eliminating or reducing the number of active systems whose failure can lead to fission product release, accident frequency is reduced, plant risk is reduced, and the remaining release scenarios tend to involve failures in passive equipment.

The operator's contribution to risk is also seen to be reduced in the MHTGR. In general, no operator actions are required in response to accidents. The various features of the plant previously described are sufficient to assure that no or only small releases will occur. Where operator actions can help further mitigate accident consequences, the passive safety and longer thermal response time in the MHTGR design provide the operator greater time, improving the likelihood of successful action.

The Licensing Basis Events selected (Ref. 9-3) in support of the Preliminary Safety Information Document are generally confirmed by this PRA. No new anticipated operational occurrences are identified. No new Design Basis Events are identified. No new types of Emergency Planning Basis Events have been identified. Furthermore, with few exceptions, all of the Licensing Basis Events identified in Ref. 9-3 would have been selected using this PRA. Thus, the assessment results confirm the third objective stated in the introduction of this section.

Sections 9.1 and 9.2 present results that quantify plant risk and identify accident sequences which dominate risk or have the highest consequences. This quantification process is the first objective outlined in the introduction of this section. These risk results are measured against two safety design goals for the MHTGR: (1) the calculated dose limits at which the Protective Action Guides (PAG) recommend public sheltering (Ref. 9-2) and, (2) the NRC Safety Goal limits on public risk due to nuclear power plant operation (Ref. 9-1). The ability of the

MHTGR to meet these goals is discussed below to accomplish the second and fourth objectives listed in this section's introduction.

9.3.1. Comparison With PAG Dose Limits

A design requirement imposed by the user on the MHTGR is to ensure that potential accidental releases are below regulatory criteria without taking credit for public sheltering or evacuation. Hence, the MHTGR is designed so that emergency planning will not be required beyond the 425-m site exclusion area boundary (EAB) (Ref. 9-4). As a part of meeting this requirement, the PRA is used to demonstrate that the frequency of a release that would result in a dose (measured at the EAB) in excess of the PAG that would trigger shelter of the surrounding public is less than 5×10^{-7} per year of plant operation. The PAG for sheltering is specified as being 1 Rem whole body and 5 Rem thyroid.

Referring to Figs. 9-1 and 9-2, the MHTGR's compliance with the user-imposed MHTGR safety requirement can be verified. Viewing Fig. 9-1, it can be seen that an accidental release which would result in a calculated whole body gamma dose at the EAB in excess of the 1 Rem PAG limit is not predicted to occur even as rarely as 5×10^{-7} per year. Likewise, Fig. 9-2 shows calculated thyroid doses also fall within allowable limits for any release predicted to occur within the range of probabilities of interest. While admittedly this first assessment reflects little margin in meeting this stringent goal, it can be concluded that the MHTGR safety design approach with its reliance on passive and inherent features makes compliance feasible.

9.3.2. Comparison With Safety Goals for the Operations of Nuclear Power Plants

The NRC has established Safety Goals with the objective to define an acceptable level of radiological risk from nuclear power plants that

was not a significant increase over other societal risks. Two quantitative health effect objectives are stated that can be used to determine whether the NRC qualitative safety goals (Ref. 9-1) are met:

1. "The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

2. The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes."

Based upon Ref. 9-5, the second objective corresponds to a latent fatality risk of 1.9×10^{-6} per year.

An "average individual" is defined in Ref. 9-6 as the "average individual biologically (in terms of age and other risk factors) and locationally who resides within a mile from the plant boundary." In Ref. 9-1, it is suggested this risk be calculated by accumulating the individual risks to persons residing in the vicinity of the plant and dividing by the number of individuals residing in the vicinity of the plant. For evaluation of the prompt fatality risk criterion, the Commission suggests that since individuals within a mile of the plant boundary would be subject to the greatest risk, if there are no individuals within a mile of the plant, an individual should be assumed to reside one mile from the boundary. In applying the latent fatality criterion, the Commission suggests that the population within 10 miles of the site be considered.

The assumption that the individual closest to the site should be subjected to the largest aggregate risk is based upon the fact that atmospheric dispersion of the airborne radioactive materials sharply

reduces the radiation exposure levels. As noted in Ref. 9-1, an "average individual" is considered because an additional risk that exceeds 0.1 percent does not, by itself, constitute a significant additional risk. Instead, it is felt that "the 0.1 percent ratio to other risks is low enough to support an expectation that people living or working near nuclear power plants would have no special concern due to the plant's proximity."

Instead of averaging the latent cancer fatality risk over a number of individuals exposed in a region near the plant boundary, this assessment has been simplified and has conservatively evaluated the total plant risk as the exposure to a theoretical individual who remains at the EAB throughout the accident to a time of 30 days. As listed in Table 9-1, this total plant risk calculated at the EAB is 3×10^{-5} Rem per year due to whole body exposure and 3×10^{-4} Rem per year due to thyroid exposure. Although the exposure to an individual at the EAB is obviously higher than the exposure to an "average individual" within a one-to-ten mile radius (the suggested method to illustrate compliance with the Safety Goals in Ref. 9-1) or even to the individual most at risk at one mile from the site boundary the fact that the MHTGR risk to an individual at the site boundary satisfies the Safety Goals is very conservative and guarantees compliance with these limits.

To illustrate this compliance, the following method was employed. First, the risk due to whole body gamma exposure in Rem was converted to a fatality risk by applying a linear, low dose response model conversion factor of 1.7 fatality risks per 10,000 man-Rem exposure (Ref. 9-7). The thyroid exposure risk in Rem could be converted to a latent fatality risk by applying another linear, low-dose response model conversion factor of 0.019 fatality risks per 10,000 man-Rem exposure (Ref. 9-8). The latent cancer fatality risk corresponding to operation of an MHTGR plant could then be computed as shown below. For whole body exposure (3×10^{-5} Rem/yr) (1.7×10^{-4} fatality risk/man-Rem) = 5×10^{-9} fatality

risk/yr, and, for thyroid exposure (3×10^{-4} Rem/yr) (1.9×10^{-6} fatality risk/man-Rem) = 6×10^{-10} fatality risk/yr. These risks were then summed to obtain a latent fatality risk of 6×10^{-9} per year. This conservative estimate of individual risk is still over three hundred times smaller than the NRC Safety Goal for latent fatality risk (1.9×10^{-6} fatality risk per year). Calculated as suggested in Ref. 9-1 this factor of margin would be significantly larger. Hence, the risk to an "average individual" within a one-to-ten mile radius is orders of magnitude within the latent fatality limit suggested in the Safety Goals.

No acute fatality risk is predicted for the MHTGR because the doses in Table 9-1 are well below doses where acute fatalities are observed (around 300 Rem, assuming supportive treatment is provided) (Ref. 9-4).

The results from this risk assessment have been applied to illustrate that the operation of the MHTGR will easily comply with the quantitative limits suggested in the NRC Safety Goals. By satisfying these criteria, it is expected that the MHTGR would not provide any significant increase to the public risk over other societal risks, which is the objective of the NRC Safety Goals.

9.4. REFERENCES

9-1. NRC, "Safety Goals for the Operation of Nuclear Power Plants," Policy Statement for 10CFR50, Federal Register, Volume 51, No. 149, August 4, 1986.

9-2. "Manual of Protective Action Guides and Protective Actions for Nuclear Incidents," United States Environmental Protection Agency, EPA - 520/1-75-001, September 1975.

9-3. "Licensing Basis Events for the Modular HTGR," DOE Report HTGR-86-034, April 1986.

9-4. "User/Utility Design Requirements for the Modular High Temperature Gas-Cooled Reactor Plant," GCRA Report GCRA 86-002, Revision 1, March 1986.

9-5. U.S. NRC, "Safety Goals for Nuclear Power Plant Operation," NUREG-0880, Rev. 1, May 1983.

9-6. "Reactor Safety Study," WASH 1400, Appendix VI, PP 9-33, 9-34, 9-37.

9-7. National Research Council, Committee on the Biological Effects of Ionizing Radiation, "The Effects on Population of Exposure to Low Levels of Ionizing Radiation," (BEIR-III), 1980.

9-8. National Council on Radiation Protection and Measurements "Induction of Thyroid Cancer by Ionizing Radiation," NCRP Report No. 80, March 1985.

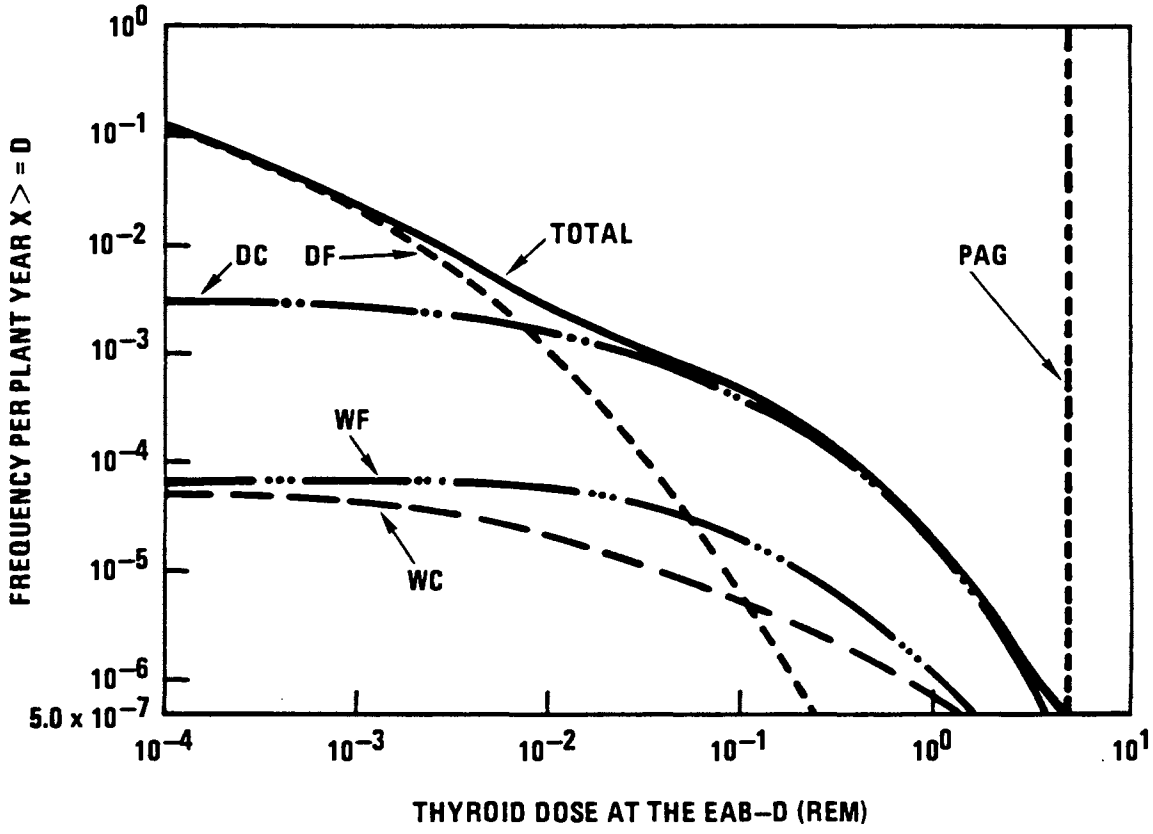


Fig. 9-1. Cumulative frequency for whole body dose from all release categories

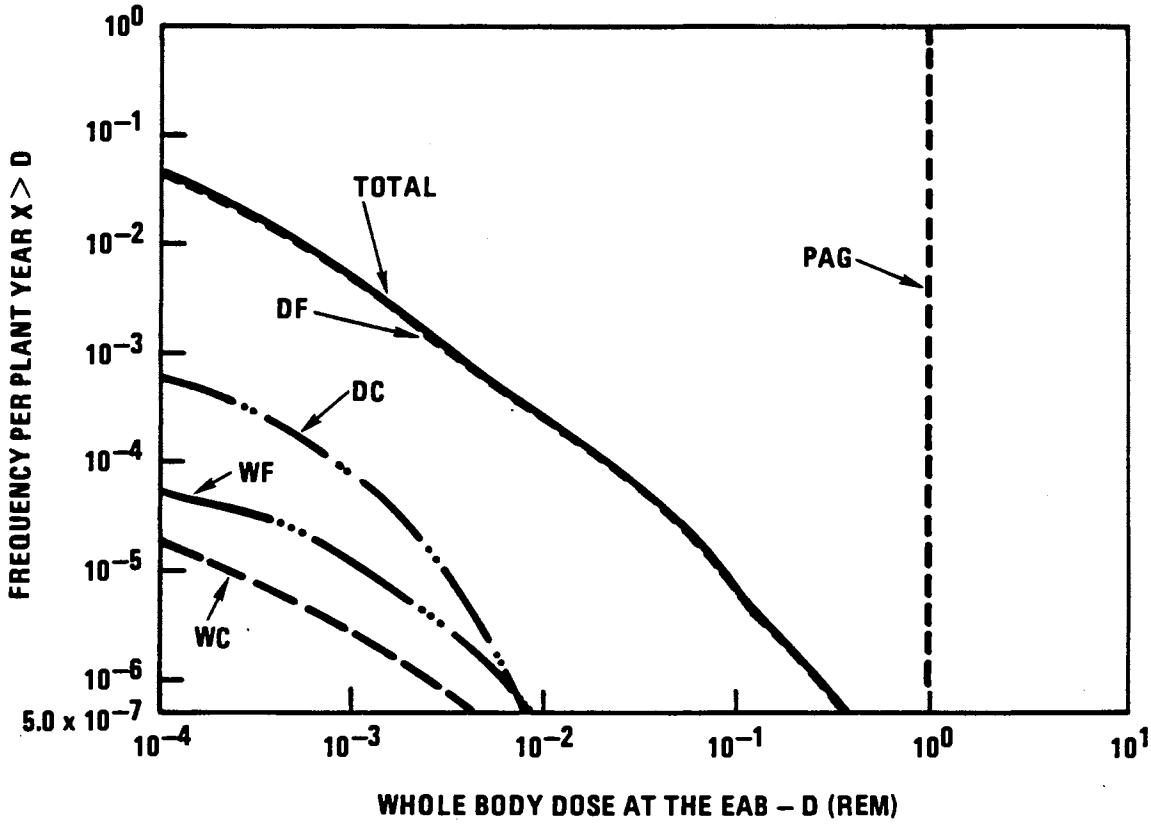
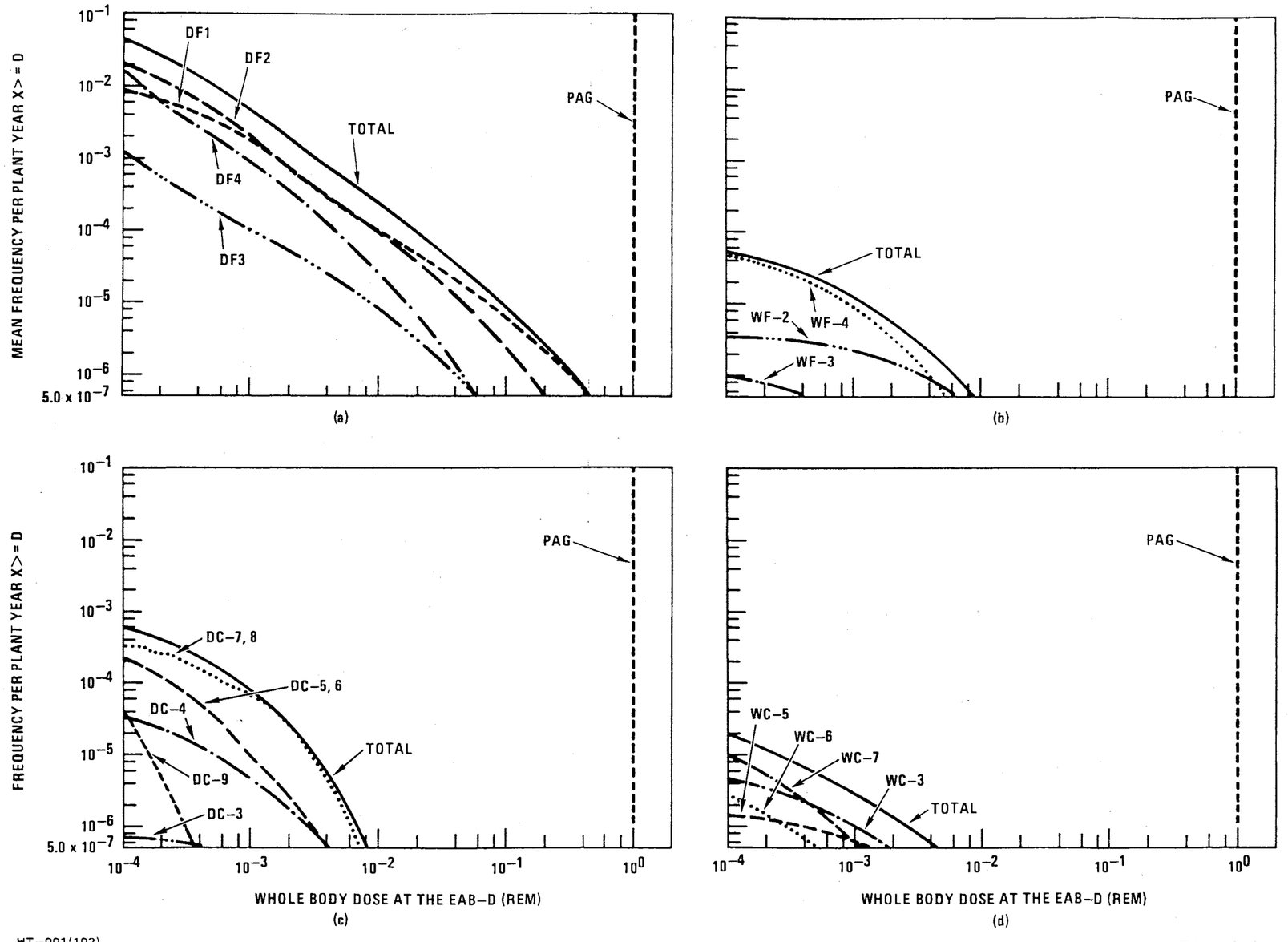
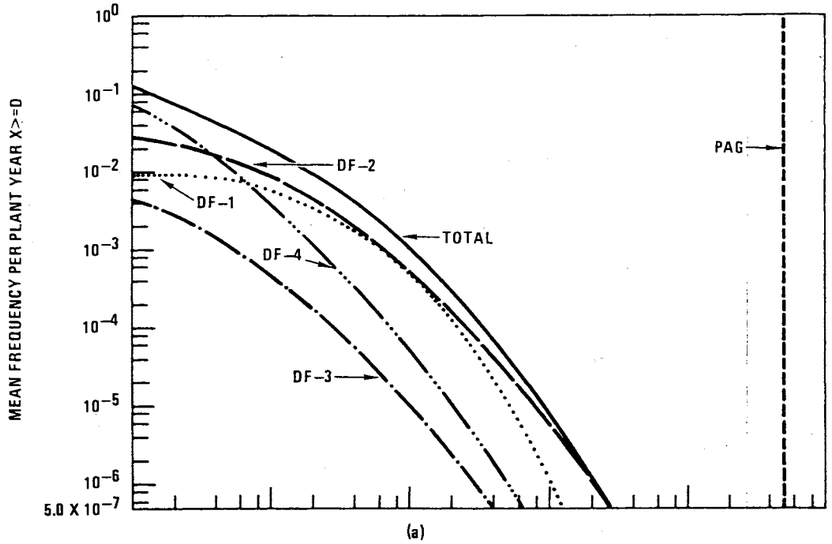


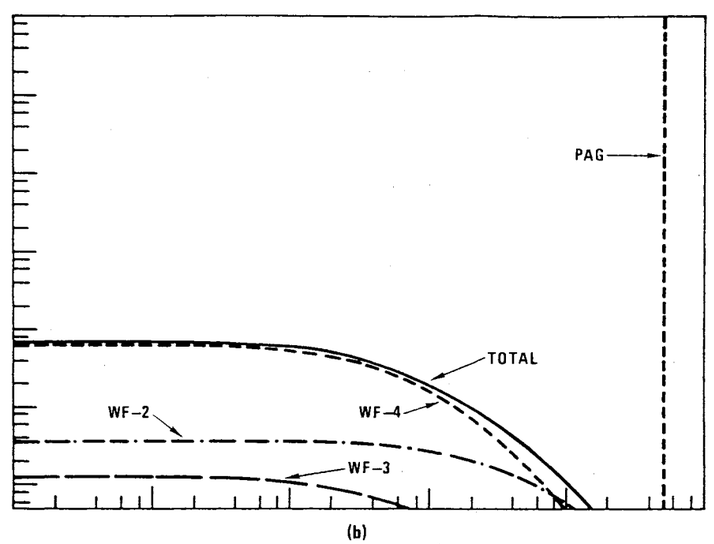
Fig. 9-2. Cumulative frequency for thyroid dose from all release categories

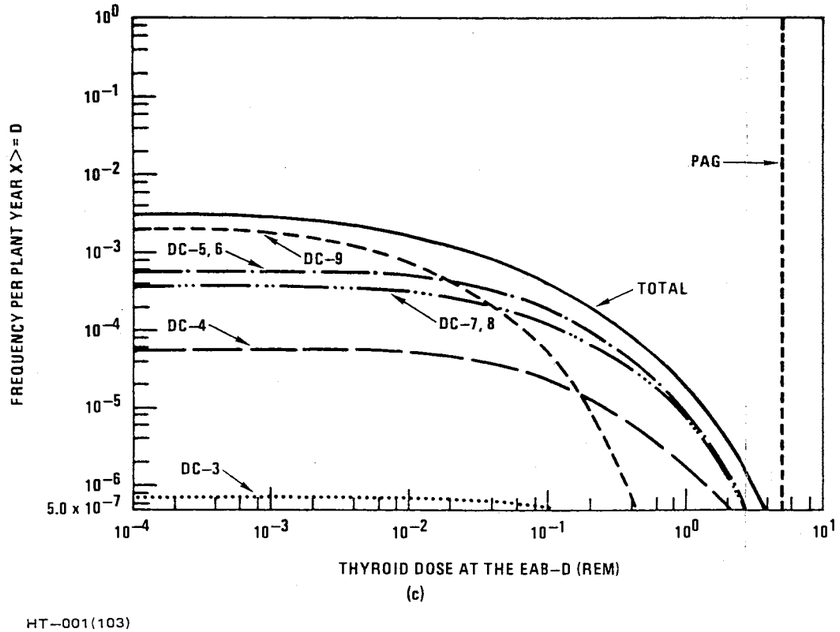


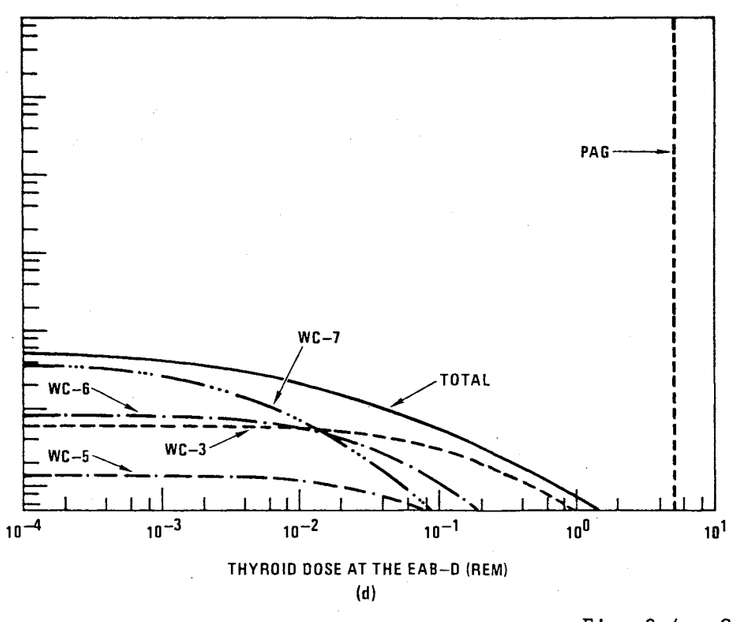
HT-001(102)

Fig. 9-3. Cumulative curves for release categories contributing to whole body dose accident types (a)DF, (b)WF, (c)DC, and (a)WC









HT-001(103)

Fig. 9-4. Cumulative curves for release categories contributing to thyroid dose accident types (a)DF, (b)WF, (c)DC, and (d)WC

10. REQUESTED NRC RESPONSE

This document has been prepared for submittal to the Advanced Reactor Group of the Nuclear Regulatory Commission (NRC) in support of the HTGR Licensing Plan (Ref. 10-1). It, along with its companion document, the Preliminary Safety Information Document (PSID) (Ref. 10-2), is intended to demonstrate the MHTGR's compliance with the top-level regulatory criteria (Ref. 10-3). In addition, the PRA provides the key basis for the MHTGR's approach to emergency planning (Ref. 10-4). Consistent with these intended uses, the NRC is requested to address and respond to the following questions:

1. Does the NRC agree that for the MHTGR conceptual design the PRA provides a logical and structured method to evaluate the adequacy of the design?

2. Does the NRC agree that the level and extent of the PRA provides a sufficient basis from which to select the MHTGR licensing basis events?

3. Does the NRC agree that the PRA shows the MHTGR design to be capable of meeting the NRC Safety Risk Goals (Ref. 10-5)?

4. Does the NRC agree that the PRA shows that an accidental release from the MHTGR resulting in a thyroid or whole body dose at the EAB in excess of the Protective Action Guides (Ref. 10-6) is extremely improbable?

10.1. REFERENCES

10-1. "Licensing Plan for the Standard HTGR," HTGR-85-001, Rev. 3, Issued by Gas-Cooled Reactor Associates for the Department of Energy, February 1986.

10-2. "Preliminary Safety Information Document for the Standard Modular High-Temperature Gas-Cooled Reactor," HTGR-86-024, Issued for the Department of Energy, September 1986.

10-3. "Top-Level Regulatory Criteria for the Standard HTGR," Issued by GA for the Department of Energy, January 1985.

10-4. "Emergency Planning Bases for the Standard Modular High-Temperature Gas-Cooled Reactor," To be Issued by GA for the Department of Energy.

10-5. "Safety Goals for the Operation of Nuclear Power Plants; Policy Statement," 51FR28044, U.S. Nuclear Regulatory Commission, August 4, 1986.

10-6. "Manual of Protective Action Guides and Protective Actions for Nuclear Incidents," U.S. Environmental Protection Agency, EPA - 520/1-75-001, September 1975.

APPENDIX A
PRIMARY COOLANT LEAK FREQUENCY METHODOLOGY

A.1. INTRODUCTION

The primary focus in the MHTGR safety approach is on maintaining the retentive properties of the ceramic, high-temperature fuel. In the probabilistic risk analysis (PRA), breachment of the primary coolant boundary is considered one of the initiating events which could challenge this retention. In particular, as an initiating event, primary coolant leaks are of interest for several reasons. Failure of the primary coolant pressure boundary can result in some, though limited, release of radionuclides to the environment. Also, if the leak is of sufficient size and located appropriately, it may allow for the ingress of air and chemical attack on the graphite core and fuel.

The frequency assessment of the risk posed by primary coolant leaks is described in Section C.1 of Appendix C. In making this assessment both the likelihood of leaks occurring and how large these leaks might be had to be ascertained to quantify events 1 and 2 of the primary coolant leak tree discussed in Section C.1. The following sections describe the basis upon which these quantifications were made. Appendix A contains the probabilistic failure models which were used in predicting the failure rate and size distribution for primary coolant leaks.

In general, there are two requirements for determination of size-dependent leak frequencies:

1. Determination of the frequency, λ_L, at which a leak of any size can occur.

2. Determination of the conditional probability that the leak can exceed a particular size, given that a leak has occurred.

Two methodologies were utilized in order to assess the size-dependent frequency of primary coolant boundary leaks in the MHTGR. The models are a log-log-linear model and a semi-empirical probabilistic model.

The log-log-linear model was used to determine the size-dependent leak frequency of primary coolant leaks for bolted closures and joints, isolation and relief valves, and rupture disc components. Operating experience data was obtained in order to determine the frequency λ_L, at which leaks of any size can occur and the conditional probability that a leak exceeds a particular size.

The semi-empirical method was utilized to determine the size-dependent leak frequency λ_L for vessel walls, pipe walls, and welds. In this model the conditional probability that the leak exceeds a particular size given a leakage occurs was obtained by utilizing principles from fracture mechanics which relate leak size to crack half-length. Probability distributions for the crack half-length are available from published literature.

The primary coolant leak frequency assessment consisted of first identifying the locations and sizes of welds, vessel penetrations, pipes, etc., which comprise the primary coolant boundary and secondly applying the appropriate model to the component to determine its size dependent leak frequency. The composite of these component evaluations form the basis for evaluating the risk of leaks. Table A-1 lists the individual components evaluated by the two models for the six component types described above which define the primary coolant boundary (vessel walls, pipe walls, welds, bolted closures and joints, isolation and relief valves, and rupture discs).

TABLE A-1
VESSEL SYSTEM COMPONENT LIST

Component
Reactor vessel wall (welds)
Reactor vessel wall (axial leaks)
Reactor vessel head (weld)
Refueling penetration (welds)
Refueling penetration (bolted seams)
Refueling penetration (axial leaks)
Control rod penetrations (welds)
COntrol rod guide assemblies (welds)
Control rod guide assemblies (bolted seams)
Control rod guide assemblies (axial leaks)
Reactor vessel cross duct nozzle (weld)
Reactor vessel SCHE nozzle (weld)
SCHE enclosure (welds)
SCHE enclosure (bolted seams)
SCHE enclosure (axial leaks)
SCHE cooling water nozzle (welds)
Reactor vessel HPS lines (welds)
Reactor vessel HPS lines (axial leaks)
Reactor vessel HPS lines (valves)
IFMU penetration (welds)
Startup detector penetration (welds)
Reactor vessel instrumentation nozzle (welds)
Core differential pressure taps (welds)
Core differential pressure taps (valves)
Core differential pressure taps (axial leaks)
Cross duct (welds)
Cross duct (axial leaks)
Bottom S/G vessel wall (welds)
Bottom S/G vessel wall (axial leaks)
Superheater outlet wall section (welds)
Superheater outlet wall section (axial leaks)
S/G cross duct wall section (welds)
S/G cross duct wall section (axial leaks)
Top S/G vessel wall (welds)
Top S/G vessel wall (axial leaks)
S/G vessel head (weld)
S/G vessel top head (bolted seam)
Feedwater nozzle (weld)
Superheater outlet nozzle (weld)
S/G vessel HPS lines (welds)
S/G vessel HPS lines (valves)
S/G vessel HPS lines (axial leaks)
Pressure relief train (welds)
Pressure releif train (valves)
Pressure relief train (axial leaks)

TABLE A-1 (Continued)

Component
Pressure relief train nozzles (welds)
HTS circulator nozzle (weld)
S/G vessel cross duct nozzle (weld)
Moisture monitor line nozzle (weld)
Moisture monitor line (welds)
Moisture monitor line (valves)
Moisture monitor line (axial leaks)
S/G electronic instrument nozzle (weld)
HTS circulator enclosure (welds)
HTS circulator enclosure (bolted seams)
HTS circulator enclosure (axial leaks)
HTS circulator instrument penetration (weld)
HTS circulator motor coolant water nozzle (weld)
HTS circulator buffer helium nozzle (weld)
HTS circulator buffer helium lines (welds)
HTS circulator buffer helium lines (valves)
HTS circulator buffer helium lines (axial leaks)
SCS circulator enclosure head (bolted)
SCS circulator instrument penetration (weld)
SCS circulator motor coolant water nozzle (weld)
SCS circulator buffer helium nozzle (weld)
SCS circulator buffer helium lines (weld)
SCS circulator buffer helium lines (valves)
SCS circulator buffer helium lines (axial leaks)

Section A.2 describes the log-log-linear method, and Section A.3 describes the semi-empirical methodology based on which were used for determination of the size-dependent frequency. Section A.4 provides additional discussion and consideration on the failure frequency for large leaks, where large is meant to include any leaks larger than the largest attached pipe (13 $in.^2$). Section A.5 presents the results of the primary coolant leak frequency/size distribution utilized in the PRA.

A.2. LOG-LOG-LINEAR METHOD AS APPLIED TO BOLTED CLOSURES, ISOLATION AND RELIEF VALVES, AND RUPTURE DISCS

The log-log-linear model was utilized for determination of the conditional probability that a leak exceeds a particular size, given that a leak has occurred for these components. A detailed description of this methodology is contained in Ref. A-1. A brief description is given below.

This methodology takes the frequency at which small leaks occur and the frequency at which large leaks (usually disruptive component failures or ruptures) occur, associates a characteristic leak size with each frequency, and utilizes these data to quantify the constants, α_1 and α_2, in the equation:

$$\lambda\ (x \geq A) = \alpha_1 A^{-\alpha_2} \quad , \qquad \text{(A-1)}$$

where $\lambda\ (x \geq A)$ = frequency (per component year) at which a leak of size A or larger occurs,

A = leak area.

This methodology is known as the log-log-linear method because, when $\lambda\ (x \geq A)$ as a function of A is plotted on log-log paper, the point corresponding to a small leak is connected to the point representing the large leak by a straight line.

The uncertainty in λ_ℓ, the frequency at which a leak of any size occurs, is modeled as the dominant contributor to the log-log-linear model. Standard lognormal distributions are utilized. With respect to the components listed in Table A-2, block valves and relief valves are assigned uncertainty factors of 10 while an uncertainty factor of two is assigned to λ_ℓ for bolted seams.

Operating experience data, required for determination of λ_ℓ, is listed in Table A-2. Key assumptions made in developing this data base are described below.

The block valves are assumed to have redundant bellows as seals. Reference A-2 cites 3×10^{-3} per component year as a generic bellows failure frequency. Using a common mode factor of 0.25 (Ref. A-3) renders a common mode failure frequency of 8×10^{-4} per component year. The independent failure contribution to λ_ℓ is simply the independent failure frequency of one bellows multiplied by the probability that the second bellows experiences an independent failure within its lifetime. Taking the lifetime as 40 yr renders an independent leak frequency of 2×10^{-4} per component year. Thus, λ_ℓ is 1×10^{-3} per component year, with an uncertainty factor of 10. The rupture frequency and uncertainty factor are from Ref. A-4.

The primary coolant relief valve and rupture disc are in series. To first order, the frequency of leakage through the relief valve and rupture disc is the frequency at which both are improperly calibrated. Reference A-4 cites 9×10^{-2} per component year as the frequency of spurious He relief valve operation. Since such failures are expected to result principally from maintenance errors, and assigning a common mode factor of 3×10^{-2} as the probability that both the relief valve and rupture disc are improperly calibrated, λ_ℓ is estimated to be 3×10^{-3} per component year. Although the uncertainty factor for the relief valve leak frequency is three (Ref. A-4), there is appreciable uncertainty in the common mode factor for a maintenance error due to a lack

TABLE A-2
LOG-LOG-LINEAR LEAK FREQUENCY DATA

Component	Frequency (per component year)	
	Leaks of Any Size	Rupture
Block valve (double steam seals)	1×10^{-3}/yr	9×10^{-5}/yr
Relief valve with rupture discs	3×10^{-3}/yr	2×10^{-4}/yr
Bolted seams	3×10^{-4}/yr	1×10^{-9}/yr

of available maintenance procedures. Hence, an uncertainty factor of 10 is judgmentally assigned to λ_{ℓ}.

Full flow through the relief train will occur if the relief valve body ruptures, or the relief valve and rupture disc both fail in fully open positions. The frequency of valve body rupture is 9×10^{-9} per component year (Ref. A-4). The derivation data of λ_{ℓ} and Ref. A-4 indicate that full flow through the relief valve and rupture disc has an 8×10^{-9} per component year frequency (retaining a factor of 3×10^{-2} for common mode maintenance errors). Therefore, the effective rupture frequency is 2×10^{-4} per component year.

Reference A-5 documents six leaks in 1.681×10^{6} operating hours. It is hypothesized that all involved bolted seams on vessel penetrations. Since there are ~100 such penetrations per LWR reactor vessel, λ_{ℓ} has a median value of 3×10^{-4} per component year and an uncertainty factor of two. The rupture frequency estimate is from Ref. A-6.

A.3. SEMI-EMPIRICAL METHOD AS APPLIED TO VESSEL WALLS, PIPE WALLS, AND WELDS

A semi-empirical method was developed because other available methods were phenomonologically incompatible with the observed behavior of materials in situations where crack propagation under cyclic loading is the dominant leakage mechanism. This becomes an important factor for such components as vessel and pipe walls, and welds. A semi-empirical method was developed incorporating these observations and is applicable, in general, in cases where crack propagation is an important leakage mechanism. The development of the methodology is described in detail.

A.3.1. Probabilistic Development

The mathematical expression for λ ($x > A$), or the frequency per component year at which a leak of size A or larger occurs, is given by

$$\lambda\ (x \geq A) = \lambda_{\ell} \int_{A}^{\infty} f_A(x)\ dx \quad , \tag{A-2}$$

where λ_{ℓ} = the frequency at which leaks of any size occur,

$f_A(x)$ = the probability density function for leak size, given that component leakage has occurred.

The median value of λ_{ℓ} is given by Eq. A-3:

$$\lambda_{\ell} = \frac{C_{\ell}\ (R_i + R_o)\ L \times 10^{-8}}{\tau^2}\ \text{(per component year)} \quad , \tag{A-3}$$

(Ref. A-3). Here

$$C_{\ell} = \begin{cases} 1; \text{ pipe and vessel walls} \\ 50; \text{ pipe and vessel welds} \end{cases}$$

where L is the component length (when applied to pipe and vessel walls) and R_i and R_o are the interior and exterior pipe or vessel radii, respectively. When the frequency of pipe or vessel weld leakage is being evaluated,

$$L = 1.75\ \tau \quad , \tag{A-4}$$

where τ is the component wall thickness.

Due to a large inherent uncertainty in λ_{ℓ}, it is postulated to have a standard lognormal uncertainty distribution with an uncertainty

factor (defined as the ratio of the ninety-fifth percentile to the median) of 10.

Principals from fractor mechanics were utilized in the development of the equation for $f_A(x)$, the probability density function for leak size, given that component leakage has occurred.

An important parameter in fracture mechanics is the crack aspect ratio, β. The aspect ratio is the crack half-length (measured parallel to the component surface) divided by the crack depth (measured through the component). Given that component leakage has occurred, the crack depth equals the component wall thickness, τ. Information about the probability density function of β is scarce. Available field experience indicates that cracks seldom have aspect ratios below unity, and a standard assumption in fracture mechanics studies is to model the probability that β is zero when it is less than unity (Refs. A-7 and A-8). This supposition implies that the half-length of a crack must be greater than or equal to τ if the crack is leaking.

The leak size A is a function of the crack half-length, a and is represented by the following expression:

$$A = \frac{4\pi\sigma}{E} \int_0^a x\, M^2\,(x)\, dx \cong G\,(a, \sigma, E\,) \quad \sim(1) \quad , \qquad \text{(A-5)}$$

where σ = hoop, flow, or longitudinal stress,
E = generalized material property,
a = crack half-length,
M = Folias bulging factor.

This relationship establishes that there is a minimum leak area, A_ℓ, given by the following formulation:

$$A_\ell = G\,(\tau, \sigma, E\,) \quad . \qquad \text{(A-6)}$$

The existance of a minimum leak area results from the available probabilistic models, which restrict the crack aspect ratio to the following range:

$$\beta \geq 1 \quad , \tag{A-7}$$

or let β_L = lower bound of β, so

$$A_{\ell} = G\ (\beta_L\ \lambda,\ \sigma,\ E') \quad . \tag{A-8}$$

Given that component leakage has occurred:

$$\int_A^{\infty} f_A(x)\ dx = 1 \quad , \tag{A-9}$$

when

$$0 \leq A < A_{\ell} \quad ,$$

since it is a physical certainty that

$$A \geq A_{\ell} \quad ,$$

whenever leakage occurs.

Equation A-8 is only valid when

$$\beta_{\ell}\ \tau \leq a < a_c \quad . \tag{A-10}$$

The parameter a_c, denotes the critical half-length for component rupture. When

$$a \geq a_c \quad ,$$

the material essentially loses its ability to resist deformation. Thus, the crack experiences rapid growth until the leak area is large enough to relieve the stresses on the component due to pressure differences. There are no known techniques for accurately predicting the rupture area, A_R. Nevertheless, A_R can be estimated as the minimum leak area which does not impede the primary coolant depressurization that occurs subsequent to the rupture. Such an approximation is acceptable from a safety risk perspective since the principal interest there focuses on depressurization rates, rather than the actual rupture size. Moreover, this approximation is phenomonologically reasonable because, if the leak opening offered significant flow resistance to the escapting fluid, it would have retained its ability to resist deformation (which is incompatible with the behavior of materials that rupture). For the simple case of primary coolant piping:

$$A_R = \Pi R_i^2 \quad , \tag{A-11}$$

where R_i = the interior pipe radius.

Introducing the notation

$$A_c = G\ (a_c, \sigma, E\ ) \quad , \tag{A-12}$$

it follows that whenever

$$\beta_{\ell}\ \tau < a < a_c \quad , \tag{A-13}$$

the leak size is in the range

$$A_{\ell} < A < A_c \quad . \tag{A-14}$$

Under this condition

$$\int_{G(a,\sigma,E)}^{\infty} f_A(x)\,dx = \int_a^{\infty} f_a(x)\,dx \quad , \tag{A-15}$$

with $f_a(x)$ = probability density function for the crack half-length.

With data obtained from Ref. A-7, the following functional relationship for the frequency per component year at which a leak of size A or larger occurs is given by Eq. A-16:

$$\lambda\,(x \geq A) = \lambda_\ell \left\{ \int_A^{\infty} \delta\,(x - A_\ell)\,dx + \int_{-\infty}^{A} \delta\,(x - A_\ell)\,dx \right.$$

$$\times \left[\int_{G^{-1}(A,\sigma,E)}^{\infty} f_a(x)\,dx \int_A^{\infty} \delta\,(x - A_c)\,dx \right. \tag{A-16}$$

$$\left. \left. + \int_{a_c}^{\infty} f_a(x)\,dx \int_{-\infty}^{A} \delta\,(x - A_c)\,dx \int_A^{\infty} \delta\,(x - A_R)\,dx \right] \right\} \quad .$$

Here $\delta\,(x - A_i)$ designates the Dirac delta function.

A.3.2. Physical Development

The development that follows is predicted upon Refs. A-9 through A-14. Pertinent variables are defined in Table A-3.

The area of the pressure boundary opening associated with a leaking crack is

$$A = \frac{4\pi\sigma}{E} \int_0^{a} M^2\,(x)\,x\,dx \quad . \tag{A-17}$$

TABLE A-3
PHYSICAL VARIABLES

Variable	Definition
P_i	Internal pressure
P_o	External pressure
R_i	Interior radius
R_o	Exterior radius
τ	Wall thickness
σ_A	Hoop stress
σ_F	Flow stress
σ_c	Longitudinal stress
S_y	Yield strength
E	Young's modulus
r_p^*	Length of plastic region axial cracks
r_p	Length of plastic region for circumferential cracks
a	Crack half-length
A_{UB}	Upper bound leak size
A	Actual leak size
A_{LB}	Lower bound leak size
E'	Generalized material property
σ	Generalized stress
M(x)	Folias bulging factor
a_c	Critical crack half-length for rupture
ν	Poisson's ratio
k	Material toughness
α	Crack half-angle

For a given material, the solution to this equation depends upon the geometry of both the crack and pressure boundary. Two crack types - axial and circumferential - are considered, utilizing "thin wall" and "thick wall" pressure boundary approximations, as appropriate. Due to the approximate nature of the current theory, exact solutions to Eq. A-17 are unavailable. Instead, certain physical suppositions are employed which permit upper and lower bound estimates for A to be obtained. The lower bound estimate (A_{LB}) includes an Irwin-type correction of the crack length by adding the radius of the plastic zone to the physical crack size. However, the Folias bulging factor was estimated using linear-elastic theory and does not account for bulging in the plastic zone. For this reason, in calculating an upper bound of A, (A_{UB}), the Folias bulging factor is calculated based on the length of plastic zone plus the physical length of the crack. The upper bound estimate, however, has to be studied in detail and verified by a comparison with experimental results (Ref. A-9). Although this limits knowledge of A to a range, calculated values of A_{LB} and A_{UB} are comparable in many applications. Hence, a nominal value for A can be obtained from the relationship:

$$A \cong \frac{A_{LB} + A_{UB}}{2} \quad . \tag{A-18}$$

It can be shown that for axial cracks:

$$A_{LB} = \frac{2\pi\, \sigma_A\, a^2}{E'} \left\{ 1 + \frac{0.2a}{\sqrt{(R_o + R_i)_\tau}} \left[3\,(1 - \nu^2)\right]^{1/4} + \frac{0.64\, a^2}{(R_o + R_i)_\tau} \sqrt{3\,(1 - \nu^2)} \right\} \left[\left(1 + \frac{\sigma_A^2}{2\sigma_F^2} \right)^{3/2} - \left(\frac{\sigma_A}{\sigma_F \sqrt{2}} \right)^3 \right] , \tag{A-19}$$

where

$$\sigma_A = \frac{(P_i R_i^2 - 2P_o R_o^2 + P_i R_o^2)}{(R_o^2 - R_i^2)} \quad ,$$

and

$$\sigma_F = S_y + 10^4 \quad .$$

(An alternate method for σ_F is the average of S_y and the ultimate strength.)

For thin wall pressure boundaries

$$E = E \quad ,$$

while

$$E = \frac{E}{1 - \nu^2} \quad ,$$

if the pressure boundary wall is thick. A wall is considered to be "thin" when

$$\tau \leq \frac{R_o + R_i}{20} \quad , \qquad \text{(A-20)}$$

and "thick" if

$$\tau > \frac{R_o + R_i}{20} \quad .$$

The upper bound estimate for A is

$$A_{UB} = \frac{2\pi\,\sigma_A\,(a + r_p^*)^2}{E'}\left\{1 + \frac{0.2\,(a + r_p^*)}{\sqrt{(R_i + R_o)_\tau}}\,[3\,(1 - \nu^2)]^{1/4} + \frac{0.64\,(a + r_p^*)^2}{(R_o + R_i)_\tau}\sqrt{3\,(1 - \nu^2)}\right\}\left[\left(1 + \frac{\sigma_A^2}{2\sigma_F^2}\right)^{3/2} - \left(\frac{\sigma_A}{\sqrt{2}\sigma_F}\right)^3\right] \quad . \tag{A-21}$$

The plastic region length is

$$r_p^* = \frac{a\,\sigma_A^2}{2\,S_y^2} \quad , \tag{A-22}$$

and all other variables are evaluated as before.

Upper and lower bounds for A when leakage involves a circumferential crack are

$$A_{LB} = \frac{2\pi\,\sigma_c\,a^2}{E'}\sqrt{1 + \frac{0.468\,a^2}{(R_o + R_c)_\tau}}\sqrt{3\,(1 - \nu^2)}\left[\left(1 + \frac{\sigma_A^2}{2\sigma_F^2}\right)^{3/2} - \left(\frac{\sigma_A}{\sqrt{2}\sigma_F}\right)^3\right] \quad ,$$

and

$$A_{UB} = \frac{2\pi\,\sigma_c\,(a + r_p)^2}{E'}\sqrt{1 + \frac{0.468\,(a + r_p)^2}{(R_o + R_i)_\tau}}\sqrt{3\,(1 - \nu^2)} \times \left[\left(1 + \frac{\sigma_A^2}{2\sigma_F^2}\right)^{3/2} - \left(\frac{\sigma_A}{\sqrt{2}\sigma_F}\right)^3\right] \quad . \tag{A-23}$$

Longitudinal stresses are given by Eq. A-24

$$\sigma_c = \frac{(P_i - P_o)\,R_i^2}{R_o^2 - R_i^2} \quad , \tag{A-24}$$

while the plastic region length is

$$r_p = \frac{\sigma_c^2 \, a}{2 \, S_y^2} \quad . \tag{A-25}$$

In addition to the leak size, physical considerations leading to a formulation for a_c are also needed. As happened during the derivation of the equations for A, the value of a_c depends upon whether the crack is axial or circumferential.

There are two different ways of calculating the critical axial crack length and the choice depends on the fracture toughness properties of the material. A material of very high toughness is said to be a flow-stress dependent material, whereas a low toughness material is called a toughness dependent material. When

$$M\,(a)\,\frac{\sigma_A}{\sigma_F} > 0.8 \quad , \tag{A-26}$$

the flow stress criterion can be used to predict a_c. This criterion predicts crack rupture when

$$\sigma_A > \sigma_F / M\,(a_c) \quad . \tag{A-27}$$

Since

$$M\,(a_c) = \sqrt{1 + \frac{3.22 \; a_c^2}{(R_o + R_i)_\tau}} \quad .$$

Axial crack rupture in flow stress dependent materials occurs at a critical half-length given by

$$a_c = \sqrt{\left[\left(\frac{\sigma_F}{\sigma_A}\right)^2 - 1\right] \frac{(R_o + R_i)_\tau}{3.22}} \quad . \tag{A-28}$$

The axial crack rupture criterion in toughness dependent materials is

$$\frac{2\sigma_F}{\pi\ \sigma_A} \cos^{-1}\left[\exp\left(\frac{-\pi\ k^2}{8\ a_c\ \sigma_F^2}\right)\right] = M\ (a_c) = \sqrt{1 + \frac{3.22\ a_c^2}{(R_o + R_i)_\tau}} \quad . \quad \text{(A-29)}$$

Since this equation is transcendental, a_c must be evaluated iteratively.

A circumferential crack will rupture if the criterion in Eq. A-30 is satisfied:

$$\sigma_F = \frac{\pi\ \sigma_c}{\pi-\alpha} + \frac{2\pi\ (P_i - P_o)\ R_i^2\ (R_o + R_i)\ \sin\ (\alpha)\ [(\pi-\alpha)\ \cos\ (\alpha) + \sin\ (\alpha)]}{(\pi-\alpha)\left\{\left[(\pi-\alpha) - \frac{1}{2}\sin\ (2\alpha)\right]\ (\pi-\alpha) - 2\ \sin^2\ (\alpha)\right\}\ (R_o + R_i)^2\ \tau} \quad . \quad \text{(A-30)}$$

Again, an iterative solution for a_c is necessary. The crack half-angle is

$$\alpha = \frac{2\ a_c}{R_o + R_i} \quad . \quad \text{(A-31)}$$

Table A-4 contains the material properties used in the semi-empirical method.

A.3.3. Uncertainties

Uncertainty in λ ($x \geq A$) arises from uncertainties in both the probabilistic and physical aspects of the model. The largest single contributor to the uncertainty in λ ($x \geq A$) is the uncertainty in λ_ℓ, the frequency at which leaks of any size occur. Statistically, λ_ℓ is postulated to be standard lognormally distributed with an uncertainty factor (defined as the ratio of the ninety-fifth percentile to the median) of 10 (Ref. A-3).

TABLE A-4
NOMINAL MATERIAL PROPERTIES[a]

Material	Property	Value
316 stainless steel	Yield strength	2.0×10^4 psi
	Young's modulus	2.6×10^7 psi
	Material toughness	N/A[b]
	Poisson's ratio	0.284
SA 533, grade B, Cl 1	Yield strength	4.32×10^4 psi
	Young's modulus	2.64×10^7 psi
	Material toughness	N/A[b]
	Poisson's ratio	0.26

[a]Material properties evaluated at 260°C (500°F).

[b]This is a flow-stress-dependent material.

A.3.4. Comparison of Log-Log-Linear and Semi-Empirical Methods

Figure A-1 is a comparison between the log-log-linear and semi-empirical methods. Both methods generate the same value for the frequency at which leaks of any size occur (λ_{ℓ}) because they both utilize the same data base. They differ appreciably, however, in the variation of leak frequency with leak size. For example, the log-log-linear model predicts that component rupture occurs at a frequency equal to $6 \times 10^{-2}\ \lambda_{\ell}$. The factor of 6×10^{-2} is a statistical average derived from nonnuclear power generation experience and generally applied to all pipe walls, vessel walls, and welds. The semi-empirical method, however, utilizes the component geometry, material properties, and operating stresses to predict the rupture frequency. Results from the semi-empirical model are therefore, an improvement over the log-log-linear model because of their mechanistic foundations.

A.3.5. Sample Application of Semi-Empirical Method

To further elucidate the semi-empirical method, the model was applied to a top steam generator wall section. The steps in applying this method are

1. Obtain pertinent material properties (Table A-4).

2. Ascertain the geometrical and operational related parameters needed to quantify the physical formulas described in Section A.3.2.

3. Quantify the physical formulas in Section A.3.2.

4. Calculate the probability that the crack half-length exceeds a, for several values of a in the range

$$\tau \leq a \leq a_c$$

Evaluate the median leak size A associated with each value of a.

5. Quantify λ_L for each component and combine it with the probabilities and leak sizes obtained in step 4.

6. Quantify the uncertainty in λ $(x \geq A)$.

Figure A-2 illustrates the results of applying the semi-empirical method to a top steam generator wall section weld.

A.4. FAILURE FREQUENCY FOR LARGE LEAKS

Consistent with the findings in Ref. A-12, leak sizes greater than that corresponding to a break in the largest connecting pipe, the primary coolant relief valve line, (13 $in.^2$) are assessed as having a negligible probability of occurrence (a frequency considerably less than that frequency chosen as a lower bound for events considered in this assessment as described in Section 5 (10^{-8} per year). The reasons for this are:

1. The primary coolant boundary is designed, fabrication, tested, and installed in accordance with the ASME Section III rules for a pressure-retaining boundary.

2. The steel vessel material will retain its ductility throughout its service life. The fluence level for the MHTGR steel vessel is at least an order of magnitude less than for current generation pressurized water reactor steel vessels.

3. Pressurized thermal shock is not identified as a concern for the MHTGR steel vessel.

4. The material is not subject to intergranular stress corrosion cracking, extreme repetitive loads, water hammer, or thermal fatigue.

5. Both preservice and in-service inspections are provided for the entire primary coolant boundary to detect flaws which could lead to failure.

6. Helium leak detection (i.e., primary coolant pressure measurement) is provided.

7. The leak-before-break approach can be applied. The criteria for applying the leak-before-break approach are applicable to MHTGR steel vessels. Those criteria are

   a. Initial flaws must tend to propagate through the wall rather than in the circumferential or axial direction.

   b. Through wall cracks must open sufficiently to allow detection by normal leakage monitoring under normal full power loading conditions.

   c. Cracks of detectable length must remain stable even under severe loading.

   d. Fracture mechanics analysis of the crossduct has shown that a circumferential crack of sufficient size to cause reactor trip due to low helium pressure is stable under the most severe postulated loads. Such a crack area is

much smaller than the postulated design basis event leak area.

8. The component material used (SA-533, Grade B, Class 1) is identical to the material used in current generation pressurized water reactor vessels.

9. A quality assurance program is employed which is comparable to that used for current generation pressurized water reactors.

A.5. RESULTS

The overall frequency of a leak of any size in the primary coolant boundary is the summation of λ_L over all primary coolant boundary components which were listed in Table A-1. The median frequency λ_L for a leak of any size in the primary coolant boundary was determined to be 0.26 per plant year [P_r ($x \geq A$) where $A = 10^{-6}$ in.^{2}].

There is a sharp break in the frequency distribution at a primary coolant leak size greater than 13 in.^{2}. This leak size corresponds to a rupture of the largest pipe connected to the reactor vessel, the primary coolant pressure relief trains. For leak sizes greater than 13 in.^{2}, it is argued in Section A.4 that the frequency of such an occurrence is extremely small, that is, considerably less than the frequency of the lower bound of this risk assessment.

A.6. REFERENCES

A-1. Fleming, K. N., et al., "HTGR Accident Initiation and Progression Analysis Status Report Phase II Assessment," GA Report GA-A15000, April 1978.

A-2. Project Staff, "The Contents of the Reliability Data Store at First February 1982," SRS/DB/37, February 1982.

A-3. Thomas, H. M., "Pipe and Vessel Failure Probability," Reliability Engineering, 1981.

A-4. Hannanan, G. W., "GCR Reliability Data Bank Status Report," GA Report GA-A14839, July 1978.

A-5. Project Staff, "Nuclear Plant Reliability Data System 1979 Annual Reports of Cumulative System and Component Reliability," NUREG/CR-1635, September 1980.

A-6. Pasternak, T., et al., "HTGR Accident Initiation and Progression Analysis Status Report Volume III, Preliminary Results (Including Design Options)," GA Report GA-A13617, Vol. III, November 1975.

A-7. Hong, S. Y., M. L. Yeater, "Critical Parameter Study and PWR Primary Coolant Pipe Leak Failure Using Probabilistic Fracture Mechanics," Nuclear Engineering and Design, 78, 1984.

A-8. Lo, T., et al., "Failure Probability of PWR Reactor Coolant Loop Piping," UCRL-86249, February 1984.

A-9. Wuthrich, W., "Crack Opening Areas in Pressure Vessels and Pipes," Engineering Fracture Mechanics, Vol. 18, No. 5, pp. 1049-1057 (1983).

A-10. Keifner, J. F., et al., "Failure Stress Levels of Flaws in Pressurized Cylinders," Progress in Flaw Growth and Fracture Toughness Testing, ASTM STP 536, American Society for Testing and Materials, pp. 461-481 (1972).

A-11. Kastner, W., et al., "Critical Crack Sizes in Ductile Piping," Int. J. Press. Ves. and Piping, pp. 197-219 (1981).

A-12. "Report of the U.S. Nuclear Regulatory Commission Piping Review Committee - Evaluation of Potential Pipe Breaks," NUREG-1061, Volume 3, November 1984.

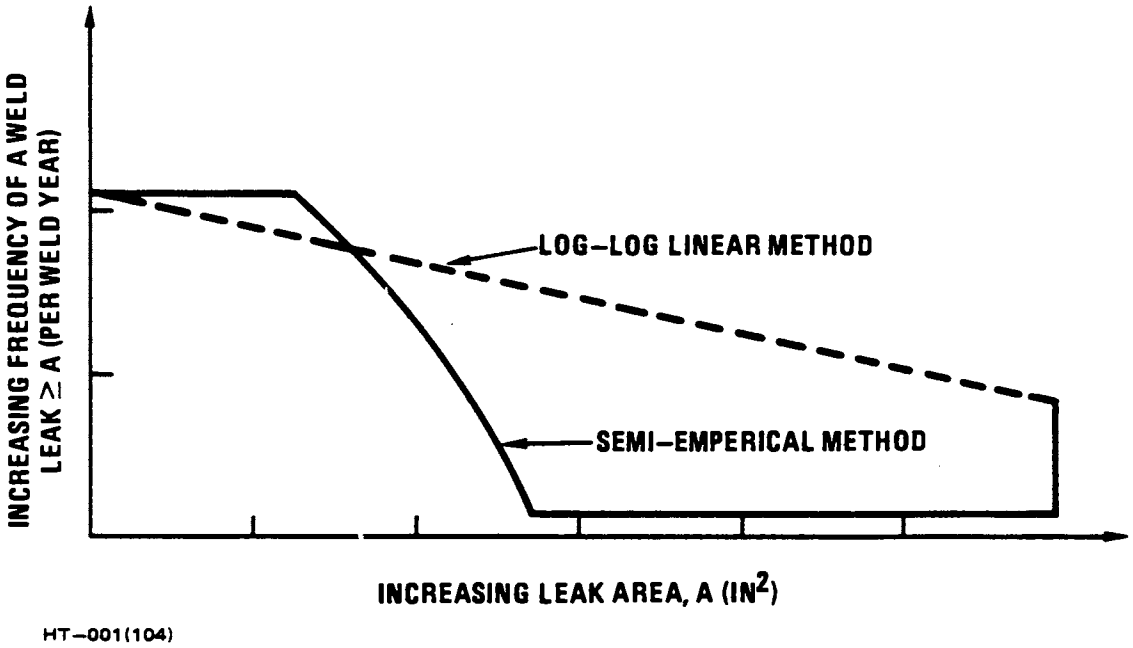


Fig. A-1. Comparison of the log-log-linear and semi-emperical methods

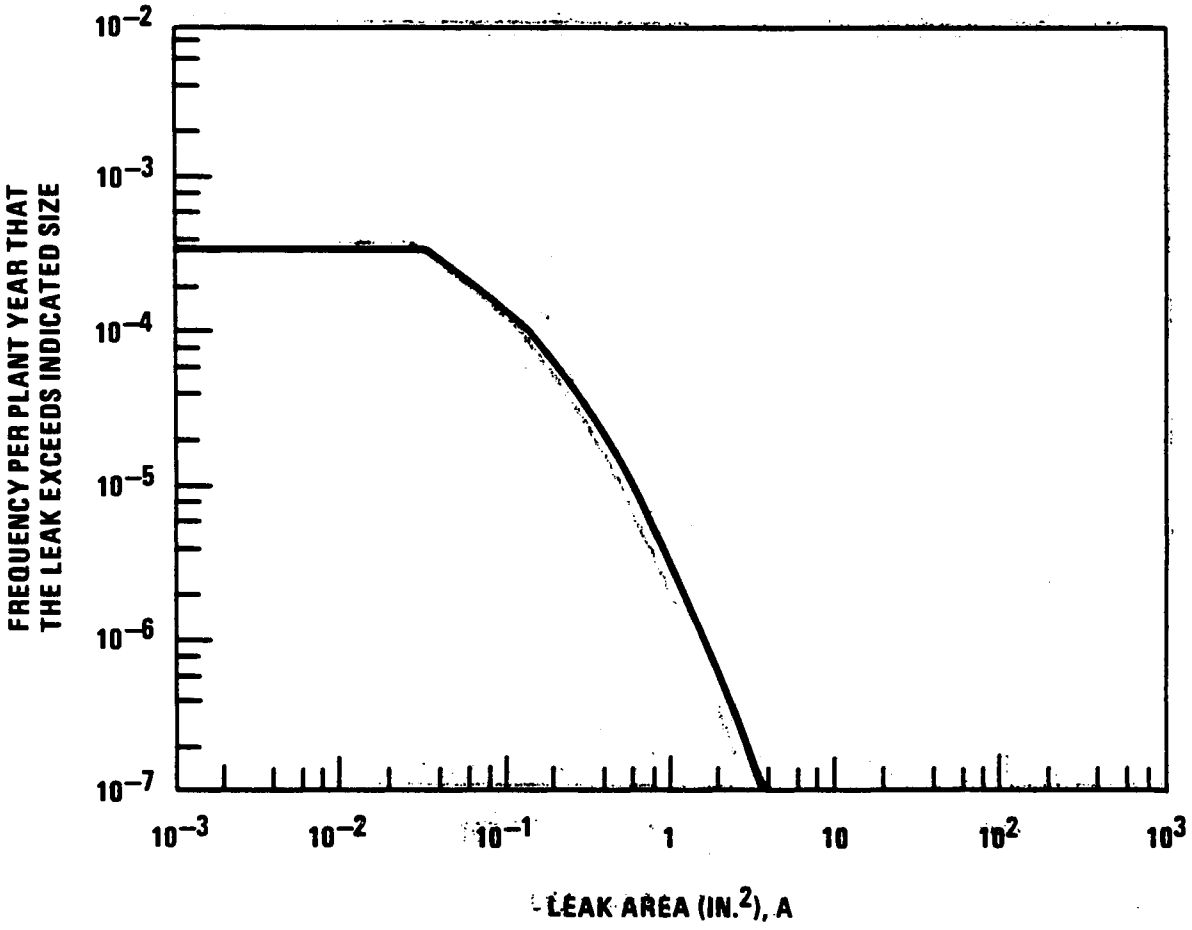


Fig. A-2. Example of semi-emperical method applied to a top steam generator wall section (welds)