NUREG/CR-3627
BNL-NUREG-51738

FRANTIC II
APPLICATIONS TO STANDBY SAFETY SYSTEMS

T. Ginzburg, J.L. Boccio, and R.E. Hall

December 1983

RELIABILITY & PHYSICAL ANALYSIS GROUP
DEPARTMENT OF NUCLEAR ENERGY
BROOKHAVEN NATIONAL LABORATORY
UPTON, NEW YORK 11973

Prepared for
United States Nuclear Regulatory Commission
Washington, D.C. 20555

NUREG/CR-3627
BNL-NUREG-51738
AN, R7

FRANTIC II
APPLICATIONS TO STANDBY SAFETY SYSTEMS

T. Ginzburg, J.L. Boccio, and R.E. Hall

Manuscript Completed — October 1982

RELIABILITY & PHYSICAL ANALYSIS GROUP
DEPARTMENT OF NUCLEAR ENERGY
BROOKHAVEN NATIONAL LABORATORY
UPTON, NEW YORK 11973

PREPARED FOR
UNITED STATES NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555
UNDER CONTRACT NO. DE-AC02-76CH00016
NRC FIN A-3230

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

The views expressed in this report are not necessarily those of the U.S. Nuclear Regulatory Commission.

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
and
National Technical Information Service
Springfield, Virginia 22161

ABSTRACT

This report deals with practical applications of the FRANTIC II code in analyzing the reliabili*y of standby safety systems. Time-dependent unavailability models such as FRANTIC II have two important advantages over more simplistic time-independent models: (1) accountability for the "burn in" and "wear out" effects in describing component failure distribution; and (2) distinguishability between two systems having the same average unavailability, but with different periods of high risk. Thus, studies can be performed to assess the percentage of time the system spends with unavailability above a prescribed threshold level.

This report demonstrates the capability of FRANTIC II to evaluate the standby safety system unavailability on a more realistic basis and perform a detailed examination of periodic testing policies. Once the requisite input parameters to FRANTIC have been described and interpreted, and estimates made from the available data, the code is applied to the three systems:

Emergency Feedwater System (PWR)

Automatic Depressurization System (BWR)

High Pressure Coolant Injection System (BWR)

The analysis includes system description, fault tree quantification, unavailability calculation, and error propagation evaluation. Current test policies are also addressed. In each case, emphasis is placed on those features specific to time-dependent unavailability analysis which makes it more suitable than the traditional approaches, based on mean estimates, for analyzing all aspects of reliability associated with standby safety systems. Conclusions are drawn and recommendations are made on strategies to decrease system unavailabilities of the selected real systems. In addition, suggestions are made on how to optimize gathering plant reliability data.

ACKNOWLEDGEMENT

The authors wish to acknowledge the contributions made to this study by Mr. Ennio Traini, who, during 1982, acted in the capacity of visiting scientist from Ente Nazionale per l'Energia Elettrica, Rome, Italy. In addition, we wish to acknowledge Mr. Joseph Fragola of Science Applications, Inc., for his helpful assistance in critiquing and culling some of the requisite data needed in our analysis of the Emergency Feedwater System.

And, finally, special thanks go to our secretary, Ms. Susan Monteleone, without whose dedicated efforts and attention to detail this report would not have been completed in a timely fashion.

CONTENTS

CONTENTS (Cont'd.)

CONTENTS (Cont'd.)

TABLES

FIGURES

FIGURES (Cont'd.)

SUMMARY

Usually, engineering judgement and manufacturers' recommendations are used as the basis for establishing test frequencies for nuclear power plant equipment. Test intervals that are either too short or too long could, however, be adverse to safety by increasing the overall risk to the public. Also, frequent periodic testing of systems with no compensating reduction in risk to the public results in an unnecessary diversion of control room auxiliary operators, could increase system failure due to human errors and may well accelerate component aging. It is now recognized that although engineering judgement must still be a primary basis for establishing component/system test and maintenance policies, insights gained from probabilistic methodologies can be a significant aid in arriving at these judgements.

In this regard, analytical tools such as FRANTIC have been developed to augment engineering judgement, so that existing plant operational policies can be examined (and possibly optimized) from a plant safety standpoint. Briefly, this family of codes can compute the time-dependent and average unavailability for any general system model whose component failures can be described by a coherent fault tree. Continuous changes in the failure rate of system components are modeled, as well as those discontinuous changes brought about by test and maintenance procedures. The instantaneous unavailability of every component in the system fault tree is calculated before and after each time point at which any component might have a discrete change in its availability. These times, for example, can correspond to passage from standby to active testing, to repair of failures found during testing, and to various component renewal options employed. By integrating these collective results over a prescribed time period, one can discern differences between system designs which, although exhibiting the same overall average unavailability, differ in vulnerability during periods of interest such as testing. Also, considering that a demand on a particular system is equally probable at each time point, an important risk characteristic to measure, besides the average unavailability, is the percentage of time the system spends with unavailability above certain preassigned levels (i.e., vulnerability).

To give some insights into how 1) the attributes of FRANTIC can be utilized to augment engineering judgement pertaining to system test and maintenance policies, 2) how uncertainties in the requisite input data can be effectively explored through sensitivity analyses and bounding assumptions, as well as 3) how other plant safety aspects can be addressed probabilistically, the FRANTIC code has been applied to three real standby safety systems of the Arkansas Nuclear One Unit 1, Caorso, and Pilgrim 1 facilities, respectively, viz.,

- Emergency Feedwater System (EFWS)
- Automatic Depressurization System (ADS)
- High Pressure Coolant Injection System (HPCIS)

For each, the analysis includes:

- Description of the system with particular attention to the interaction of component testing policies within the system and types of component failures mechanisms;
- Quantification of the fault tree using generic data and, to the extent that they are available, plant-specific data;
- Calculation of the pointwise unavailability in order to obtain useful information about vulnerable periods and the average system unavailability over a one-year period;
- Use of the bounding approach and sensitivity analysis of the effects of data variations;
- Consideration of time dependence in the failure rates;
- Analysis of periodic test procedures to estimate quantitative test input parameters;
- Sensitivity studies of a number of testing options to determine the most important contributors to safety function unavailability and the effect that the testing policy can have on these contributors.

For these three real systems, some of the more salient facts this study has yielded based upon the assumptions employed are:

<u>EFWS</u>:

1) For approximately 43% of the time, this system achieves higher pointwise unavailability levels than the average system unavailability which, for a loss of main feedwater without loss of offsite power transient (LMFW), is 3.00×10^{-4}. For this particular system, this vulnerability is mainly attributed to the specific plant maintenance policies for the turbine-driven pump and motor-driven pump of each redundant train.

2) Mean average unavailability is sensitive primarily to the hazard rates and failure distributions ascribed to check valves. The mean unavailability differs by a factor of 7 between valve burn-in and wear-out stages. Next in order are the pumps. Variability in the shapes of their failure distributions investigated in this study yields a factor of 2 difference in the average unavailability. For motor-operated valves, the shape of the failure distribution is relatively not an important factor in determining system unavailability. Finally, the analysis indicates that the failure distribution of diesels and batteries have the least influence in system unavailability.

3) Although this phase of the study has shown that changes in the fa lure rate distribution for some components may have little effect on tne average system unavailability, significant effects in system vulnerability have been discerned. For motor-operated valves (AC) for example, although only a 26% change in system unavailability is calculated between their burn-in and wear-out stages, the system vulnerability differs by 64%. Thus, from a system vulnerability point of view, better assurance on knowing the failure distribution of these components is warranted.

ADS:

1) Common-mode failures (human error) significantly affect system unavailability. Its contribution is of the order of 10^{-3}; other failure sources contribute at least an order of magnitude less.

2) Discounting common-mode failures, ADS unavailability is approximately 1×10^{-4} with very little time spent at higher values over a one-year period.

3) On relative terms, calculations for the average system unavailability and system vulnerability are particularly sensitive to the failure distributions related to relays and switches within the two logic trains.

HPCIS:

1) Analysis performed to assess the periodic testing policy for the automatic initiation function logic indicate that the three steps required for testing this feature should be consolidated into one procedure which verifies that all components receive the necessary initiation signal.

2) Performing the logic test in conjunction with the initiation sensor tests then provides an integrated test of the entire logic train. If this is performed during annual refueling, the longer time required for the integrated test will not contribute to the unavailability of the system.

3) Considering, however, the current design and testing policy of the HPCI's initiation logic, the analysis shows that staggering the three logic tests instead of testing sequentially yields a lower system unavailability. A minimum in testing policy is observed if the staggered test interval is 60 days.

4) Analysis of the three periodic test procedures performed to verify the auto isolation function has indicated that a) the auto isolation function has a relatively large potential for common cause failures; b) common cause notwithstanding, only two cut sets in the fault tree contribute significantly to the unavailability of this function; and c) autoisolation tests affect the unavailability of the injection function as well.

5) The three autoisolation functional tests are currently accomplished monthly over a two-day period. However, because these tests are performed in quick succession, the second two tests are performed before standby failures have had an opportunity to occur. Thus, although the valves and relays are cycled a total of three times during the month, their periodic test interval is still approximately 30 days. This testing policy can also accelerate the wearout of the associated valves and relays.

6) A staggered testing policy for this function is shown to be superior to the sequential testing policy because the relays and valves would now be tested at the staggering interval with the less important cut sets tested less often.

Further details regarding these observations, and others, can be found within the main body of this report.

I. INTRODUCTION

1.1 BACKGROUND

The primary function of a standby safety system is to prevent or mitigate the ensuing consequences of postulated accidents. As such, these systems are designed to transit, upon demand, from an idle state to an active state. Depending upon the design basis accident and its likelihood of occurrence, a standby safety system can be in the idle phase for long periods of time. In most respects, the operational status of standby systems cannot be either monitored or assessed while in the idle phase. The reliability characteristics of an engineered safety system clearly depend on the unavailability of components in the system. Recognizing this, the Nuclear Regulatory Commission (NRC) requires that systems important to safety "be designed to permit appropriate periodic inspection of important areas and features..." (10 CFR 50). Establishing a quantitative basis for judging appropriate plant operational policy is difficult for a complex safety system containing many components. As a result, periodic testing and inspection policies are frequently based on "engineering judgement" or on the analysis of equivalent single-component systems, rather than on a quantitative appraisal between the advantages and disadvantages for accomplishing a particular testing program in the context of the entire system's safety function. Establishing a quantitative basis for periodic testing was one of the main purposes of the development of the FRANTIC code by NRC. Such a basis must, therefore, utilize risk-based principles which not only account for random failures but must also account for failure modes which are (1) caused by testing but detected and repaired after the test; (2) caused by testing but not detected or repaired until the next test; (3) due to true demands on the system.

There are three versions of the FRANTIC code currently available: FRANTIC, FRANTIC II, and FRANTIC III. FRANTIC [1] calculates both instantaneous and average unavailability of standby safety systems, including contributions from component failures, testing, and repair and it applies an exponential failure distribution to describe hardware failures. Frantic II incorporates a Weibull distribution and provides additional flexibility for its use. Accordingly, assessments regarding time-dependent as well as constant hazard rates can be made with the more recent version while the original version can only assess effects attributable to constant hazard rates.

Time dependent unavailability models, such as FRANTIC II, take into account "burn-in" and "wear-out" effects and can differentiate between systems which may exhibit the same average unavailability but can differ in vulnerability during periods of high risk. A system may thus have a low average unavailability, and yet at particular times the instantaneous unavailability may be quite high. Therefore, when the demand on a system is equally probable at each time point, the important characteristic from which to measure the risk, in addition to the average unavailability, is the percentage of time the system spends with unavailability above certain preassigned levels, i.e., its vulnerability.

Added features of using the Weibull formulation are that appropriate choice of Weibull-related parameters will allow burn-in or wear-out phenomena to be addressed; and since the exponential distribution is a special case of the Weibull distribution, periods of normal operation can be modeled as well. A major feature of the FRANTIC II code is its ability to account for the effects of imperfect testing through the use of a variety of component input parameters. It can also model time-dependent failure rates as a function of both time and test frequency. The code calculates the instantaneous unavailability of every component in the system before and after each time point at which any component might have a discontinuous jump in its unavailability. (These times correspond to passage from standby, to active testing, to repair of failures found during testing in periodically tested components.) It then calculates the system unavailability at each time point and time averages the instantaneous system unavailabilities over the calculation period (generally a minimum of one year.) It outputs the average system unavailability over the calculation period and the instantaneous unavailabilities at each time point. Any system whose failure can be described by a fault tree can be quantitatively analyzed using FRANTIC II.

For both FRANTIC I and II, the data required can be categorized as (1) parameters that describe the failure characteristics of the primary events, and (2) parameters that depend on the operational procedures. For (1), the requisite information should be based upon empirical data culled from appropriate sources, e.g., PRA's, etc. For (2), the pertinent information is test interval and duration time, repair time or allowed test downtime, override capability,detection inefficiency and test staggerings, and test-caused failures. Common-cause and human errors associated with operational procedures can also be modeled. A Boolean expression representing the system fault tree is required.

The FRANTIC III code[3] combines the FRANTIC II code methodology for component and system unavailabilities with various operating component models for calculating system failure-to-operate as well as standby-to-operating transition failure probabilities. Input data require additional data groups describing the failure and maintenance characteristics in the operational phase.

The goal of the present project is to demonstrate the capability of FRANTIC II to obtain realistic evaluation of the standby safety system unavailability and perform a detailed examination of periodic testing programs utilizing time-dependent unavailability analysis.

1.2 OBJECTIVES

To accomplish the above goal, the specific objectives are:

1. Data analysis and parameters estimation (Chapter 2). This includes:

   - An engineering interpretation of failure mechanisms of standby components subject to periodic testing and repair
   - Correlation of FRANTIC II input parameters with these mechanisms
   - FRANTIC II input parameter estimations

2. FRANTIC II application to the standby safety systems. The following systems will be considered:

   a. Emergency Feedwater System (EFWS) of a Pressurized Water Reactor (Chapter 3)

   b. Automatic Depressurization System (ADS) of a Boiling Water Reactor (Chapter 4)

   c. High Pressure Coolant Injection System (HPCIS) of a Boiling Water Reactor (Chapter 5)

   The analysis includes:

   - Description of the system with particular attention to the interaction of component testing policies within the system and types of component failures mechanisms;
   - Quantification of the fault tree using generic data and, to the extent that they are available, plant-specific data;
   - Calculation of the pointwise unavailability in order to obtain useful information about vulnerable periods and the average system unavailability over a one-year period.
   - Use of the bounding approach and sensitivity analysis of the effects of data variations
   - Consideration of time dependence in the failure rates
   - Analysis of periodic test procedures to estimate quantitative test input parameters
   - Sensitivity studies of a number of testing options to determine the most important contributors to safety function unavailability and the effect that the testing policy can have on these contributors.

3. Error Propagation

   - Evaluation of the effects created by the fault tree reduction
   - Influence of the unknown shape of the failure distribution and error in mean time estimates
   - Evaluation of the vulnerability as a percentage of time during which the system unavailability is higher than a given threshold
   - Identification of the leading directions for the future data collections

1.3 LIMITATIONS

Making an analysis tractable, in general, entails certain restrictive assumptions in developing the mathematical model which limits the direct applicability to real systems. Some of these restrictions are inherent in the basic modeling approach; others are more system specific. The latter are discussed in the body of the report; the more general limitations are the following:

1. The code is not able to model the effects of status of other components which must be aligned away from emergency position during tests but are themselves not being tested. If these components belong to the same branch of the fault tree as the tested component, there will be no immediate effect on the pointwise unavailability during the test period. Human error contributions resulting from test realignment which may show up after the test period can be taken into account (Chapters 3 and 5) by assigning an appropriate constant probability for the contributors.

2. Being a deterministic model of the process, the code does not deal with the randomly distributed test duration and repair times. Both parameters assume fixed input values for each run. Given sufficient data about the distributions of test duration times and repair times, one can make runs with high and low estimates thereby bracketing the true unavailability. This is the procedure adopted in this report.

3. The chance inspecting which does not follow any predictable schedule and the noncatastrophic failures which are repaired without jeopardizing the availability of the systems are not modeled by FRANTIC codes. To be conservative, one can include the data on such failures in the data pool. This will lead to a slight overestimation of the hazard rate.

4. FRANTIC codes use a variant of the Weibull distribution as a descriptor of time-dependent hazard rates. A variety of other distributions have been suggested as models for time-dependent hazard rates for different components. One appropriate model, the First Passage Time (FPT) distribution, seems to be of special interest with respect to components having a leading cause of failures. The comparative analysis of this distribution with the Weibull is given in Appendix 1 of this report. If proven sufficiently useful, this distribution can be incorporated into the FRANTIC code to further enhance its capability to model time-dependent failure rates.

2. ENGINEERING INTERPRETATION OF FRANTIC

This chapter presents an engineering interpretation of the FRANTIC code. First, the overall structure of the code is introduced. Next, the input parameters to the code are interpreted in terms of the physical failure mechanisms they can represent. Those familiar with the analysis contained in the FRANTIC codes should not find it necessary to read this chapter; those in need of more detailed information should find it useful, including the references cited herein. In addition, Sections 2.1-2.5 of this chapter draw heavily on the work of A. Dykes[14].

The FRANTIC II code uses four sets of equations to calculate component unavailability. Therefore, it models four types of components:

1. Constant unavailability components
2. Nonrepairable components
3. Periodically tested components
4. Monitored components

By definition, a constant unavailability component is described by a per demand (or per cycle) unavailability which is independent of time. Human error (per demand), common causes can also be modeled as a constant unavailability component. A nonrepairable component is one which, if it fails, is not repaired during plant operation. A periodically tested component is one which is tested at regular intervals, and their failures are not detectable until a test is performed. A monitored component is one whose failure is immediately detected and repair is then begun.

There are 13 potential parameters, from which the user may choose a necessary subset to model the different types of components under a variety of testing schemes (see the FRANTIC II manual[2]). Limitations imposed by the way in which the code performs calculations, with a particular parameter set, are discussed and suggestions are made for ways to represent common modeling problems that the systems engineer might encounter. The estimation of input parameters that represent time dependent failure rates is presented in Section 2.6.

2.1 CALCULATION PROCEDURE

FRANTIC II is a series of subroutines driven by a main program which is controlled by keywords and formatted input. The user may input data for any number of runs that he desires. After the code has completed the calculations generated by one set of keyword input, it will automatically shift to the next. Figure 2.1 briefly describes the computational flow of the code.

A major feature of FRANTIC II is its ability to account for discontinuities in the time-dependent system unavailability brought about by, e.g., periodic test and repair of individual components for a two-component parallel system. Fig. 2.2 depicts how discontinuous changes in component unavail

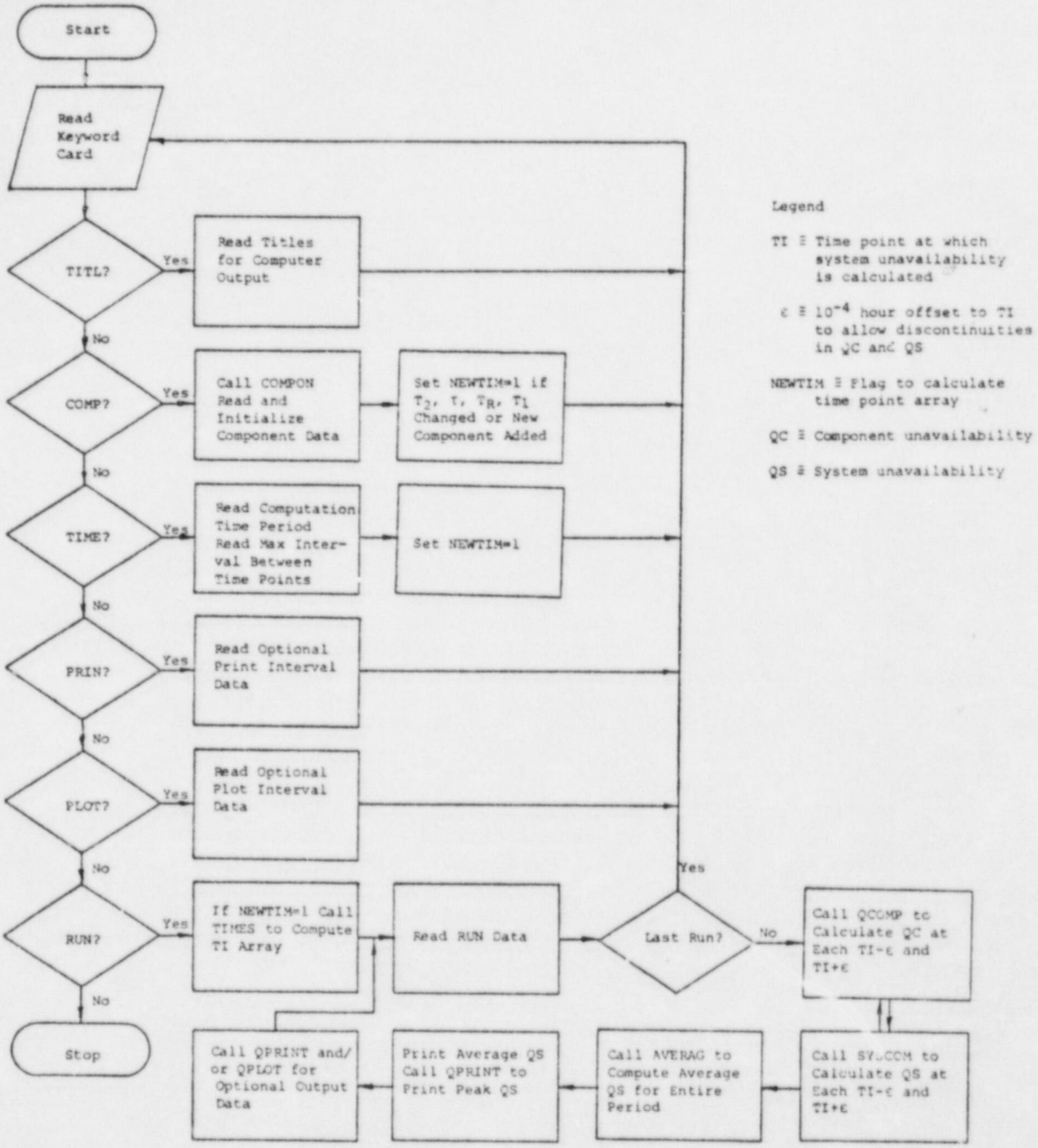

Start
Read Keyword Card
TITL?
Yes
Read Titles for Computer Output
No
COMP?
Yes
Call COMPON Read and Initialize Component Data
Set NEWTIM=1 if T_2, τ, T_R, T_1 Changed or New Component Added
No
TIME?
Yes
Read Computation Time Period Read Max Interval Between Time Points
Set NEWTIM=1
No
PRIN?
Yes
Read Optional Print Interval Data
No
PLOT?
Yes
Read Optional Plot Interval Data
No
RUN?
Yes
If NEWTIM=1 Call TIMES to Compute TI Array
Read RUN Data
Last Run?
Yes
No
Call QCOMP to Calculate QC at Each TI-ε and TI+ε
Call SYSCOM to Calculate QS at Each TI-ε and TI+ε
Call AVERAG to Compute Average QS for Entire Period
Print Average QS Call QPRINT to Print Peak QS
Call QPRINT and/or QPLOT for Optional Output Data
No
Stop
Legend
TI ≡ Time point at which system unavailability is calculated
ε ≡ 10^{-4} hour offset to TI to allow discontinuities in QC and QS
NEWTIM ≡ Flag to calculate time point array
QC ≡ Component unavailability
QS ≡ System unavailability

Figure 2.1. Computational flow of the FRANTIC II computer programs.

ability reflect discontinuous changes in the system unavailability. Based upon user-supplied information, Subroutine TIMES essentially searches for these particular time points. Subroutine QCOMP calculates the unavailability of each component within the -neighborhood of each discrete timepoint. Overall system unavailability is determined via a user-supplied subroutine, SYSCOM, which must contain the Boolean expressions for the fault tree of the particular system under study.

After the system unavailabilities, before and after each time point, have been calculated, SUBROUTINE AVERAGE time integrates the unavailability by assuming that unavailability varies linearly between the time points. The subroutine divides the time interval of the calculation to obtain the average system unavailability.

A new SUBROUTINE VULNER (not shown in Fig. 2.1 but called from QCOMP) has been added to the FRANTIC II code to calculate the percentage of time the system spends with unavailability above the preassigned level. This feature will be further discussed in Section 2.7.

With the QPRINT and QPLOT subroutines, one obtains formatted output of the average system unavailability over the calculated time period; instantaneous system unavailabilities; average system unavailability during intermediate time intervals; and plots of the time-dependent system unavailability. (The plot routine must be user updated to interface with local plotting software.)

The portion of FRANTIC II's output which subdivides the average system unavailability into contributions arising from testing, repairs, and failures requires some elaboration. The FRANTIC II manual[2] calls them contributions "due to" testing repair and failures. However, this connotation is not precise. The rules for apportioning instantaneous system unavailability to one of the three categories is as follows:

1. If at least one component is under test, then the instantaneous system unavailability is counted toward the test contribution.

2. If no components are under test and at least one component is down for repair, then the instantaneous system unavailability is counted towards the repair contribution.

3. If no components are under test or repair, the instantaneous system unavailability is counted towards the failure contribution (i.e., between test contribution).

What is actually listed under these three categories is the system unavailability due to various causes during specifically defined time periods. It is not the average system unavailability over just those specific time periods, but more precisely the time-integrated unavailability over the specific periods divided by the total calculation time. The unavailability given under each category therefore has no direct meaning. The only numbers that can be interpreted are the percentage figures. For example, the test percentage can be interpreted as the percentage of the average total system unavailability over the total calculation time which accumulates while at least one component is under the test.

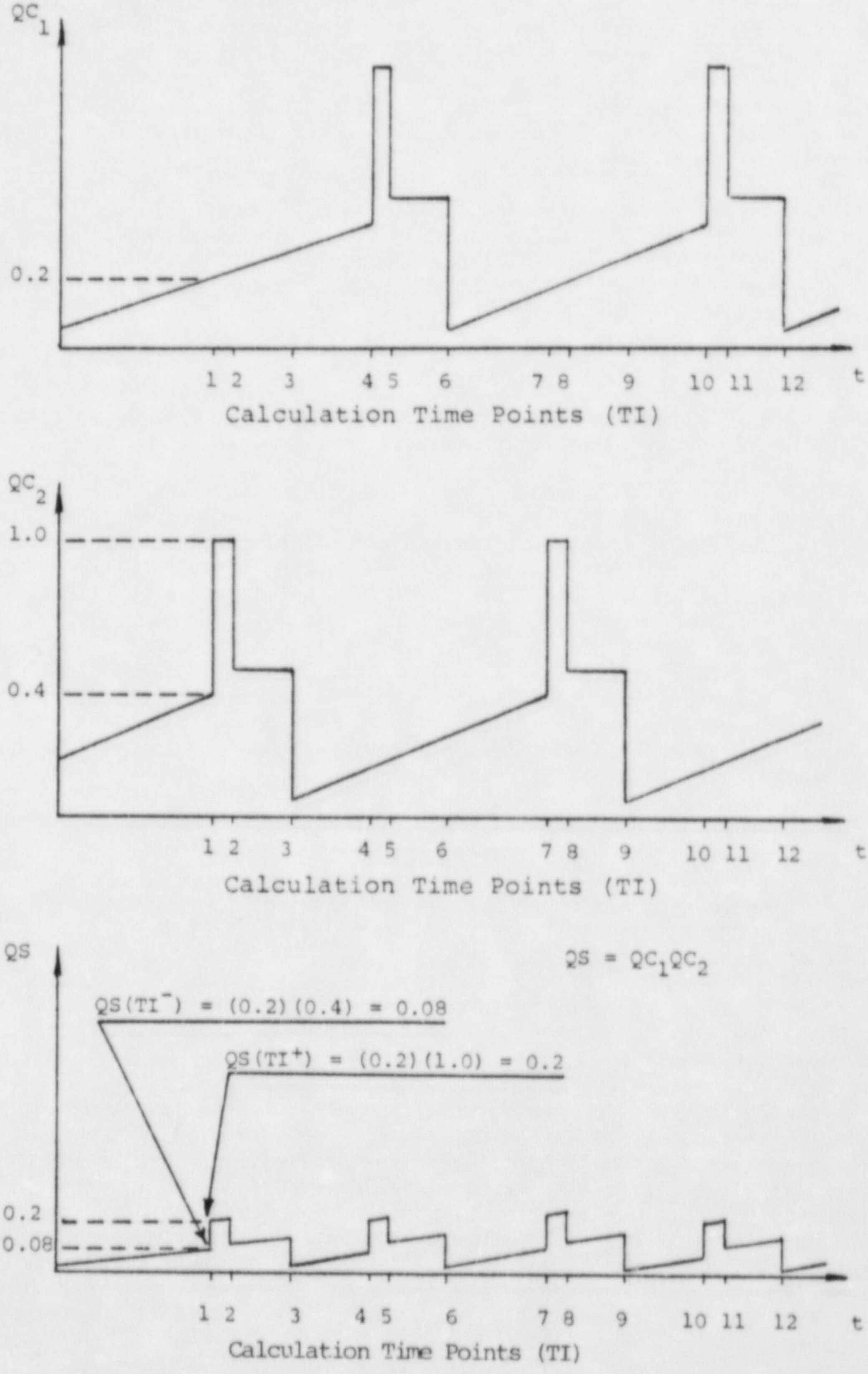


Figure 2.2. Example of FRANTIC'S use of time points to calculate the instantaneous unavailability of a two-component parallel system.

2.2 STANDBY FAILURE RATE

Both the detectable and undetectable standby failure rates are represented by a hazard rate for a Weibull failure distribution. Given the component is not failed at time t, the probability that it will fail between t and t + dt is

$$P(\text{Fail}) = \lambda(t)dt = \beta\lambda(t - t_r)^{\beta-1}dt \quad ,$$

where

$\lambda(t)$ = Conditional Failure Rate or Hazard Rate [sometimes designated by others as $z(t)$ or $h(t)$].

λ = Scale Factor. The probability of failure is proportional to the scale factor, as it establishes the length (or scale) of time the component is expected to function before it fails.

β = Shape Factor. This is used to specify how the failure rate varies with time (thereby determining its shape). It can be any value greater than zero. It produces the time dependence in $\lambda(t)$ which best matches the failure rate obtained from failure data and/or engineering judgement.

t_r = Renewal Time.* This represents the time at which the component is either reconditioned or replaced.

The remainder of this section discusses the physical interpretation of standby failure input parameters.

2.2.1 Scale Factor for Detectable Standby Failures

The Scale Factor for Detectable Standby Failures, λ_0, models detectable failure mechanisms that occur during a component's standby period. The scale factor establishes the magnitude (in conjunction with β) of the probability that a fault will occur per unit time at any given time. The scale parameter is used with both monitored and periodically tested components.

Monitored components normally perform some function while the safety system is on standby. Failures are either immediately announced in the control room or detected a short time later during normal operator rounds. The failure rate can therefore represent both internal hardware failure mechanisms and the effects of external shocks. Examples of monitored components are power supplies and sensors. The output voltage of a power supply can be constantly monitored, and shorts will be detected immediately. The outputs of many sensors are checked on a routine basis during the standby period, during which time malfunctions or suspicious output can be checked and repair effected if necessary.

*This parameter is automatically calculated by the code, based on component renewal type (see section 2.2.4).

Periodically tested components are normally idle during standby and must transfer to an active state when a demand occurs. For these components, the scale factor models failure mechanisms which occur during the standby period, but which are not revealed until the component is required to operate (either from a test or a true demand). Since the component is idle, these failures are primarily due to external random "shocks" resulting from the standby environment. Examples would be exposure to vibrations, process fluid flow, moisture, and human errors of commission during the standby period. A more specific example might be a leak which soaks the windings of an electric motor so that it will short out when called upon to start and run.

2.2.2 Scale Factor for Undetectable Standby Failures

The Scale Factor for Undetectable Standby Failures, λ_u, models failure mechanisms which occur during the standby period that cause the component to fail to perform when called upon during a true demand, but which are not revealed by monitoring or periodic tests. It establishes the magnitude (in conjunction with β) of the probability that an undetectable fault will occur per unit time. Although the component apparently performs its safety function during a test, it fails during a true demand because of a failure mechanism not addressed by the test. Undetected faults can occur when periodic tests require reconfiguration of the safety system from its operational alignment. For example, during an operational test, the High Pressure Coolant Injection System's discharge is routed to the condensate storage tank. An obstruction beyond the test bypass line would not be detected by the test. A second example is the inability to simulate the environmental conditions of the accident during an operational test.

Monitored components can also suffer undetectable failures. An example would be a breakdown of insulation in a sensor which does not short under normal operating conditions, but causes failure of the sensor in the steam environment of a true demand. The shock which causes the transition to the failed state occurs during the standby period, but it is a failed state only under the highly stressed conditions of a true demand.

2.2.3 Failure Rate Shape Factor

The Failure Rate Shape Factor, β, specifies how the instantaneous conditional failure rate (hazard rate) changes with time. When β is equal to 1, the failure rate is constant and independent of time. For values of β less than 1, the failure rate decreases with time. For values greater than 1, it increases.

The shape factor models the fact that a component's susceptibility to standby failure mechanisms can change with the past standby service life of the component. For example, the specification of $\beta = 2$ implies that the failure rate of that component is increasing linearly with time. The implication is that environmental factors acting on the component during standby are gradually degrading the component's resistance to failure causes which can transfer it into a failed state. For example, gradual buildup of corrosion products might be considered as an accumulation of small shocks which can transfer a valve into a stuck state with increased probability as its exposure to the process fluid increases. This in turn results in a higher probability that the valve will stick when called upon to open. Time-dependent failure rates will be discussed in more detail in Section 2.3.2.

Conversely, if $\beta = 1$, the conditional probability of, say, a component failing during its 10,000th hour of standby (given it has survived until then) is the same as the conditional probability of its failure at any other time during the standby period. By implication, the constant failure rate model assumes that if the random shocks of the standby period do not cause a transition to a failed state, they have no impact whatsoever on the component. This is called the exponential failure model because the time dependence of the availability (cumulative probability of survival to time t) follows an exponential distribution and the hazard rate, by definition, is constant in time.

2.2.4 Component Renewal Type

In FRANTIC II, a component can be renewed by either periodic testing (which cycles a component through an active phase of operation) or repair. Renewal has the mathematical effect of resetting the Weibull hazard rate following the test and repair.

New-New (NN) Renewal Both test and repair reset the hazard rate. The renewal time, t_r, is automatically set equal to the end of the most recent scheduled test period when the component is not failed, and is set equal to the end of the repair time when it is failed. This type of renewal might model a failure mechanism in which two metallic surfaces cold weld during the standby period (exhibiting a $\beta > 1$ hazard rate). When the component is operated, the effect of the cold weld is broken and the cold welding process must begin again.

Old-Old (OO) Renewal. Neither test nor repair resets the hazard rate. The renewal time is kept at $t = 0$, the beginning of the FRANTIC II calculation. The hazard rate follows its time dependence for the entire period of the calculation. This renewal type might be used to model the failure rate of a large component where various parts exhibit wearout due to abrasion and corrosion. Testing has no effect on these mechanisms; and, repair of breakdowns can correct only local problems. The component's failure rate is resumed as it was before test or repair.

Complete replacement of a large component would probably justify recalculation of unavailability using the newer component's estimated failure rates. This type of repair is beyond that envisioned for the repair time modeled in the code, since it would require shutdown of the plant.

Old-New (ON) Renewal. Testing has no effect on the hazard rate, but repair resets it. When the component is found failed at a periodic test, the renewal time is set as thc time of the end of repair. (For further information, see the FRANTIC II manual.) This component type most often models components that wear out or gradually deteriorate and are replaced when they fail. For example, a circuit board gradually deteriorates in a humid environment. Testing cannot reverse the deterioration, but when the circuit board is found to be failed, it is replaced with a new one.

2.2.5 Unavailability Due to Standby Failures

Unavailability due to standby failures depends on whether the component is monitored or periodically tested.

Monitored Components

The equations for monitored components used in FRANTIC II depend upon the assumption of "Good as New" or "Good as Old," (see FRANTIC II manual).

Inspection of this equation shows that for short operating times compared to the life time, $T<<T_F$, unavailability for both renewal options tends to follow the same simple expression:

$$q(t) \quad \lambda\beta T_R t^{\beta-1} \quad .$$

This means that when few failures are likely to have occurred, the renewal option is relatively unimportant.

The behavior for long operating times, however, differs for the two options. Whereas in the "Good as New" case, q(t) tended to an asymptotic value which depends only on T_R and average life time T_F, viz.,

$$q_\infty = T_R/(T_R + T_F) \quad .$$

The effect of nonrenewal becomes significant at long times. The asymptotic value is approached only for the case $\beta = 1$ where there is no change in the failure rate with time. For $\beta > 1$, the component eventually becomes "worn out" and so the unavailability tends to 1. For $\beta < 1$, the component eventually becomes "debugged" or perfect, so the unavailability tends to 0.

If certain failure modes are not detectable by the monitoring device, then the appropriate fraction of failures can be treated as being nonrepairable (using $\lambda_u = p\lambda$ for the nonrepairable component failure rate where p is the failure detection inefficiency and $\lambda_0 = (1 - p)\lambda$ for the monitored contribution).

Periodically Tested Components

In periodically tested components, standby failures can produce three different types of unavailability contributions:

1) they occur but remain undetected during the standby period;

2) they are revealed during a test period;

3) they keep the component down until repair is completed.

The relative importance of the three contributions depends on the values of the parameters used for periodically tested components.* During the standby period, the unavailability is given by

$$q(t) = 1\text{-exp } (-\lambda[(t - t_r)^\beta - (t_w - t_r)^\beta]) \quad .$$

*See the FRANTIC II manual for a detailed description of these equations.

In Eqn. 2.2, t_w, is defined as the time at which the component was last known to be operational. From this point, the instantaneous unavailability monotonically increases, as described by Eqn. 2.2. After a periodic test, the current time becomes the time the component was last known to be working, so the detected unavailability returns to zero.

For the undetected failures, the component is assumed to be last known to be working at the last renewal, t_r ($t_w = t_r$). Consequently, for the NN option, where renewal occurs at every test, there is no difference between detectable and undetectable failures.

As shown in a previous report[5], the optimal test period for the periodically tested component is

$$T_2^* = \sqrt{2 q_0 \tau / (\lambda(1 - p))} \quad = \quad \sqrt{2 q_0 \tau T_F / (1 - p)} \quad ,$$

where

q_0 test override unavailability, (the probability that a component cannot transfer from a test mode to an operate mode if a demand occurs)

p probability of not detecting a failure,

λ $1/T_F$ (constant hazard rate),

test duration time.

In the case of the Weibull distribution, the optimal test interval is

$$T_2^* = (\tau(\beta+1)/(\lambda\beta))^{1/(1+\beta)}$$

for $p = o$ and $q_0 = 1$, and

$$T_2^* = (q_0 \tau(\beta+1)/(\lambda\beta(1-p)))^{1/(\beta+1)}$$

for $p \neq o$ and $q_0 \neq 1$.

2.3 DEMAND FAILURE RATE

2.3.1 Engineering Interpretation

The demand failure rate, q_d, models failure mechanisms which are independent of the time of the true demand. It can be input with either monitored or periodically tested components and contributes a constant value to the calculated unavailability for that component at every time point.

The demand failure rate is used to model failure mechanisms other than those which occur during the standby period. It can represent the probability of

- o Conditions at the time of the true demand that defeat the component's ability to perform its function. An example would be the probability than an el:ctric motor will be flooded by a particular Loss-of-Coolant Accident, and will therefore short and fail to function.

- Failure mechanisms caused by transitions between states. For example, the accelerations of starting and stopping may cause failures during demand, or too much force during the previous transition may jam a valve and consequently prevent its opening.

- Errors during test and maintenance that leave an originally operable component in an undetected failed condition. An example of this is leaving the Auxiliary Feedwater System valve out of the secondary system following a periodic test.

Note that when applying this parameter to periodically tested components, a demand to operate implies two transitions, both of which can cause failures. A previous transition to standby could have left the component in an undetected failed state, and the current demand to operate can also cause the failure. (Operator error and jammed valves due to closure are examples of failures occurring during transitions to the standby condition.)

2.3.2 Special Uses

Because the demand failure rate is a convenient way to input an unavailability that remains constant throughout the calculation, it can be used in conjunction with other parameters to produce more flexible modeling of time-dependent system unavailability. The following paragraphs present two such applications, but are in no way a complete listing of the possibilities.

Monitored Failures in Periodically Tested Components

Some periodically tested components may have some portion of their function monitored while they are at standby. For example, the voltage across electrically operated machinery may be constantly monitored, or idle equipment may be subjected to visual inspections which can reveal some failure mechanisms. Other failure mechanisms may be revealed only by operating the equipment. If the monitored failures are assumed to have a constant failure rate or the component has NN renewal, the average monitored unavailability is asymptotically constant. One could then calculate the average and input it directly using the parameter q_d.

If the monitored hazard rate is increasing, one could use q_d in conjunction with the undetectable standby failure parameter, λ_μ, to model an average unavailability due to monitored components which increases gradually throughout the calculation.

Common Cause Failures

When more than one component can be made ineffective because of the conditions of the true demand, the resultant common cause failure can be modeled by a separate failure event in series with whatever failure event those components affect. Since the true demand is assumed to occur at random, it can be modeled by a constant unavailability represented by q_d. In this circumstance q_d would equal the fraction of true demands for which the components fail to perform their function.

2.4 TIMES ASSOCIATED WITH PERIODIC TESTING

2.4.1 Periodic Inspection Interval

The Periodic Inspection Interval, T_2, sets the time between the start of successive periodic tests. It is input in days, but is automatically rounded off to an integer number of hours by the code.

2.4.2 First Periodic Inspection Interval

The First Periodic Inspection Interval, T_1, allows the user to stagger the periodic testing of various components to reflect the sequence and interval spacing in which tests are actually accomplished. Because the calculations start by assuming all time-dependent unavailabilities are zero, the system unavailability near the beginning of a calculation may not reflect actual unavailability. First-interval effects can be minimized by averaging over many inspection intervals and not selecting instantaneous system unavailabilities near the beginning of the calculation.

2.4.3 Scheduled Test and Maintenance Period

The Scheduled Test and Maintenance Period, τ, represents the average duration of scheduled periodic testing and maintenance and is input in units of hours. This includes the actual testing time for which the component is unavailable and the time for repairs of the component done routinely to prevent future safety-related failures. It does not include unexpected failures which require additional time for repair. For example, consider a component that is inspected every month and found capable of performing its safety function. However, minor problems are discovered which, if not corrected, could cause the component's failure at some time in the future. The plant policy is to make minor repairs and repeat the operational test as a matter of course. Since the component was not in a failed condition at the beginning of the test and the repair is not unexpected, this maintenance policy should be accounted for in the specification of τ .

2.4.4 Unscheduled Repair Time

The Unscheduled Repair Time, T_R, accounts for repair that is performed when a component is found to be failed, either by monitoring or by periodic testing. The unscheduled repair time accounts for the total time from the discovery of the fault through retesting and qualification of the component for standby service. It does not include normal maintenance that is done on a component, which is accounted for in τ .

During unscheduled repair a component is assumed to be totally unavailable. The (unconditional) unavailability calculated by the code during T_R is equal to the probability that the component requires repair times one (because it failed). Therefore, the user should account for partial availability by shortening his estimate of T_R. For example, if on-line repair of a component takes an average of 10 hours, during which time the component is not available to perform its safety function, requalification for standby takes an additional 4 hours, during which the component is only 25% unavailable. The average unscheduled repair time should be calculated as

$$T_R = 10 + 0.25(4) = 11 \text{ hours} \quad .$$

2.5 EFFECTS OF IMPERFECT TESTING

The parameters discussed below are directly associated with testing. However, failures during testing which also have a large impact on system unavailability are modeled by q_d. These, of course, refer to the probability of leaving a component in an undetected failed state following the completion of the test period. See Section 2.3.1.

2.5.1 Probability of Test-Caused Failure

The Probability of Test-Caused Failure, P_f, represents the probability of failures occurring during periodic tests that would not cause the component to fail to perform its function in the event of a true demand at any time, but which generate the requirement for an unscheduled repair following a normal periodic test. This includes repairs to prevent leakage and contamination, or repairs to correct precursor faults which currently do not interfere with the functioning of the component, but could lead to a safety-related failure in the future if left uncorrected. It also includes failures generated by the conditions of the test which do not occur during an accident.

Since a test cycles some components to an operating mode, with its potentially much higher failure rate, a component can fail because of active mode failures unrelated to the standby period during a test. The parameter P_f also accounts for these types of failures.

Test caused failures are assumed to be immediately detected, but the component becomes unavailable for the additional unscheduled repair time discussed above. This parameter increases the unavailability of the component by P_f during the test and repair periods, τ and T_R. The component returns to an available status at the end of the unscheduled repair period.

An example of test-caused failure is a pump which blows a seal during a flowrate test. The pump is capable of completing its mission with the blown seal during a true demand. However, to prevent excessive contamination and further damage to the pump, repair must be effected, and the pump is assumed to be not available to accomplish its safety function for both τ and T_R.

2.5.2 Unavailability to Override Test and Maintenance

Unavailability to Override Test and Maintenance represents the probability that a good component cannot be used for its intended function should a true demand occur while it is undergoing periodic test and maintenance. It models the fact that periodic tests often require some reconfiguration from the component's standby "ready" mode. It also accounts for the fact that maintenance and minor repair might make the component unavailable for some fraction of the test and maintenance time.

This parameter should be estimated considering all of the activities that could go on during a scheduled test and maintenance period, τ. It is actually the fractional downtime of the component averaged over τ. It is derived from an assessment of both the test procedure and the maintenance activities which normally occur during τ.

2.6 DATA SOURCES AND PARAMETER ESTIMATION

Both the data collection and the estimation of reliability parameters are independent areas of research in their own right. A very brief discussion given below serves only as an introduction, to explain the origin of the parameters applied herein.

Reliability data for Nuclear Power Plants are dispersed in a variety of publications, e.g., the Nuclear Plant Reliability Data System (NPRDS) collects system and component data of Safety Classes 1 and 2 in ANSI 18.2 and ANSI/ANS 52.1 and Class 1E in IEEE-38-type equipment of all operating nuclear plants within the U.S. The NPRD reports contain data on failures and maintenance. The problem with this source, as well as with many other sources, is that real systems are inherently quite reliable, so that few failures have been reported. It will probably take another five years before significant data are accumulated (see the detailed review of a number of other data sources in Ref. 4, Ref. 15, and a complementary annotated list in Ref. 6).

Two classes of parameters should be estimated on the basis of these data sources in order to use the FRANTIC code: failure rates and maintenance parameters (test periods and durations, repair durations, test-caused probabilities, failure detection inefficiencies, unavailabilities of the test override capability). The estimation of failure rates from the raw data is a problem in itself with major difficulties being not mathematical but rather a result of the paucity of data and variability of conditions under which data were collected. A crude division of "in-plant" versus "generic" data, between components manufactured by different companies, and similar components operating in the BWR versus PWR are examples of the kind of heterogeneity of data encountered. The element of engineering judgement is therefore present to some extent in every estimation process.

In many cases, because of the limited data, it is very difficult to estimate the degree of time dependence in the failure rates (parameter β in the case of the Weibull distribution). In such cases, the failure rate is usually estimated as constant and the failure distribution becomes exponential. The estimate for the constant failure rate is given by following simple formulas; based on the situation where failed components are repaired or replaced,

$$\lambda = n/T$$

and

$$T = \sum_{i=1}^{m} t_i \quad ,$$

where

m = the number of components in the population;

t_i = the accumulated time of the ith component during the reporting period (hours)

n = the number of failures occurred within the population

T = the total calendar hours for the components in the population

FRANTIC can be used as a tool for evaluating the importance of uncertainty in the failure rate estimates. If, for instance, the shape of an actual distribution is uncertain, one can vary the shape parameter, β, in the Weibull failure rate ($\lambda(t) = \lambda\beta t^{\beta-1}$) and determine the sensitivity of the system unavailability to this variation. The sensitivity evaluated for different kinds of components will indicate the relative importance of collecting additional data for a component or a group of components. This approach will be illustrated in the next two chapters in the context of the Emergency Feedwater System (EFWS) and the Automatic Depressurization System (ADS) unavailability analysis.

Maintenance data also are quite variable. The distribution of repair time often indicates bimodality exhibiting higher frequency for the shorter periods. In this case, the use of the boundary approach is most appropriate and a sensitivity study allows comparison of different test strategies. Since FRANTIC considers constant maintenance duration, two separate runs using low and high values for the average repair duration times can be performed to bracket the pointwise unavailability. This approach will be illustrated in Chapter 3 when analyzing the unavailability of the EFWS.

2.7 VULNERABILITY OF SAFETY SYSTEMS

It is pointed out in Ref. 5 that time-dependent reliability analysis performed by the FRANTIC II code has an important advantage of identifying periods when a system is most vulnerable, i.e., periods of high risk. This information is important as an addition to the average unavailability. Two systems may have equal average unavailabilities (equal average risk of failure over a period of time) but very different vulnerabilities, i.e., spend different percentages of time at the high risk periods. This second characteristic is an important parameter which can be used in addition to the mean risk in the evaluating the degree of safety of a given system.

Assume that the moment of a demand on a safety system is uniformly distributed over a period of time. Choosing an arbitrary threshold q^*, the vulnerability of a system can be defined as a percentage of time at which the time dependent unavailability $q(t)$ exceeds q^*:

$$V_q{}^* = \text{prob.} \; \{ q(t) > q^* \} \quad .$$

The value of $V_q{}^*$ will depend strongly on the threshold q^* chosen, decreasing monotonically with increasing q^*. The other implicit argument is the overall time (integration) period, T, of consideration. For the "good as old" replacement and the wearing-out components, $V_q{}^*$ will grow with increased integration period and will decrease in the case of "burn-in" components. It will stay unchanged if the replacement is "good as new" for both "wear-out" and "burn-in" components.

All the parameters of the system, including the hardware failure characteristics and operational parameters (test and repair periods and durations, for instance) will influence the value of vulnerability as well as the mean unavailability. For the hardware failure, it is common to assume the constant hazard rate due to insufficient data for the time dependence in the hazard rate. The question as to what extent collection of data will improve the evaluation of safety can be investigated using the index of vulnerability suggested above. The answer, of course, will not be universal and will depend strongly on the actual role of the component (or components) in the fault tree of the system. In general, however, the following methodology can be used.

Using the existing data, one can check a variety of different distributions producing the same mean life time for the component in question, but having different shapes. FRANTIC runs for all such distributions within the Weibull family will generate basically the same average unavailability; the differences in the average unavailability will be insignificant. At the same time, vulnerabilities can change drastically for different shapes of Weibull distributions. One can expect, for instance, higher V_q^* in the "wear-out" case than in the "burn-in" case, since the periods of high unavailability will be longer for the former and shorter for the latter.

The changes in the vulnerability of a system with respect to the shape of the failure distribution may then serve as a guide to the direction of the future data-collecting efforts. Components whose vulnerability is shown to be insensitive to the shape of failure distribution can be classified as less important in this respect than the components with high sensitivity.

It should be pointed out again before considering real examples that not only the value of V_q^*, but its sensitivity as well, will strongly depend on q^*, the threshold value, which is considered as high risk. For the investigated systems $V_{10^{-1}} = 0$ and will essentially be insensitive to changes in the failure rate; $V_{10^{-7}} = 0.99$, and will not change much either. The interesting results appear in the range of vulnerabilities for q^* between 10^{-5} and 10^{-4}. This is the sensitive region, and it will be considered below for a number of different components.

3. EMERGENCY FEEDWATER SYSTEM

3.1 INTRODUCTION

The Arkansas Nuclear One, Unit 1 Nuclear Power Plant (ANO-1) Emergency Feedwater System (EFWS) functions as an emergency system for the removal of post-shutdown decay heat from the reactor coolant system via the steam generators (SG). The EFWS is automatically initiated in case of loss of main feedwater (loss of both main feedwater pumps), or loss of all four reactor coolant pumps (RCPs), or low level or low pressure in either SG. During normal shutdowns, however, the main feedwater (MFW) is throttled down to the level capable of removing decay heat and the EFS is not utilized. At some other PWRs, the MFW is tripped during normal shutdowns and the backup feedwater system, the Auxiliary Feedwater System (AFWS), functions during all shutdowns. For this reason, the ANO-1 backup feedwater systems are labeled "emergency" rather than auxiliary.

The ANO-1 EFWS consists of two interconnected pump trains, capable of supplying feedwater to either or both SGs from one of two water sources under automatic or manual initiation and control.

Two interconnected trains supplying emergency feedwater have isolation valves, check valves, control valves, flow instrumentation, and pressure instrumentation to control the flow of emergency feedwater to the SGs.

The success criterion of the system is removal of reactor coolant system decay heat from one of two steam generators; for this it is sufficient that the system supply a minimum of 500 gpm of emergency feedwater to the SGs at 1050 psig within 50 seconds of system initiation signal. The piping diagram is included as Fig. 3.1.

3.2 OVERALL CONFIGURATION

3.2.1 Suction

The primary water source condensate storage tank T-41 is required by the plant Technical Specifications to have a capacity of 107,000 gallons for emergency feedwater. Water is supplied from this tank to a common suction header via a single 8-in. line.

There is an alternative EFWS suction source which is available from the nuclear service water system, loops one and two. Suction may be manually transferred from the condensate storage tank to the nuclear service water system by means of AC motor-operated valves CV2803 and CV2800 and DC motor-operated valves CV2806 and CV2802. A common control switch for each pair causes the valves to assume opposite positions; that is, if one valve (e.g., CV2806) is open, the other valve (CV2802) is closed and vice versa. Operator action is required to open the AC motor-operated valves CV3850 and CV3851. Operators are alerted to perform this suction transfer by a low-suction pressure alarm on the common suction header.

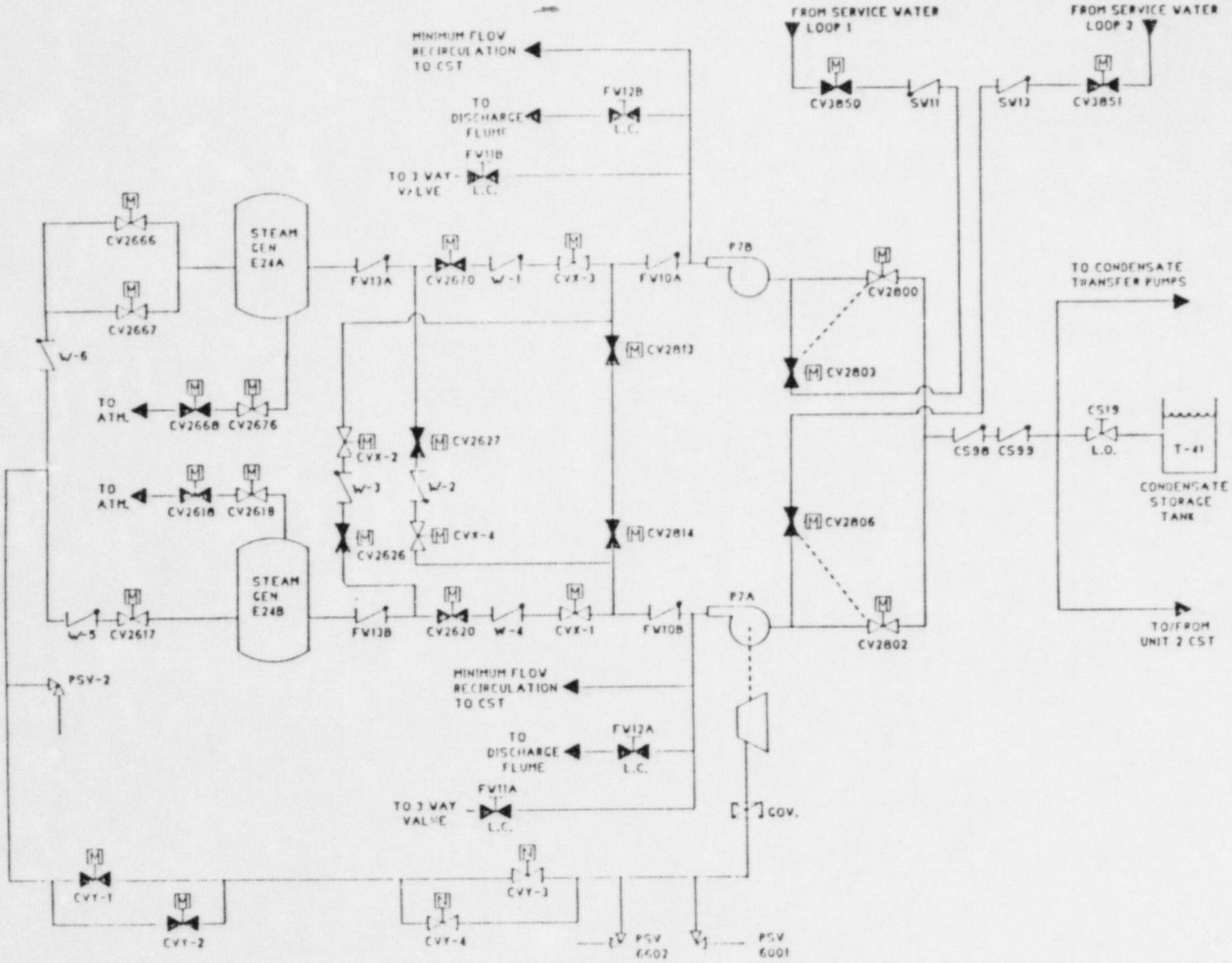


Figure 3.1 Emergency Feedwater System

3.2.2 Discharge Paths

Each pump is connected to each steam generator by an independent train: train A contains a turbine-driven pump; train B has a motor-driven pump. If AC power is not available, the A train can still provide complete system function relying on DC power. Two trains are interconnected beyond a check valve downstream of each pump into 4 in. cross-connected discharge lines. Since there is no pump isolation valve between the pump and the interconnection of the two trains, isolating the pump requires the closure of CVX-2, CVX-3 or CVX-1, CVX-4. The cross-connection line contains two normally closed motor-operated valves (CV2813 and CV2814). This cross-tie permits either pump to feed either or both steam generators. Each SG can be isolated from EFW flow by normally open motor-operated valves (CV2620, CV2670, CV2626, and CV2627).

3.2.3 Steam Supply for the EFWS Turbine

Steam for EFWS pump P7A turbine passes from both SGs through motor-operated locked-open valves CV-2666, CV-2667, and CV-2617 and check valves. A check valve is installed in each line to preclude "blowing down" the good steam generator in the event of steam line or feed line break. Two normally closed redundant DC motor-operated valves (CVY-1 and CVY-2) are opened automatically on EFWS initiation. They may also be opened manually, but this consideration is beyond our scope. Steam then passes through two pressure-reducing valves in parallel (CVY-3 and CVY-4). Two overpressure relief valves (PV6601 and PV6602) protect the piping and turbine downstream of the pressure-reducing valves in the event of the latter failure.

Turbine exhaust is vented directly to the atmosphere.

3.2.4 Actuation and Control Logic

The initiation of EFWS is provided by the "Initiate Logic" which is located in two channels (A and B). The initiate logic derives its input from the input logic and provides signals when any of the following occurs:

1) all four RC pumps are tripped,

2) both main feedwater pumps are tripped,

3) the level of either steam generator is low,

4) either steam generator pressure is low, or

5) either of two anticipatory trips (trips not yet assigned) are present.

The fault tree shows each logic channel (A and B) is connected to both pumps. Therefore, failure of one channel does not fail the system; the other channel activates both pumps. The automatic initiation fails in case of the failure of both channels.

3.2.5 Supporting Systems and Power

Except for electric power, the EFWS pumps, pump motor, and turbine are self-contained entities without dependence on secondary support systems. The bearings on the turbine and both pumps are self-lubricated.

The two EFWS trains are powered from diverse power sources. The motor-driven pump (P7B) train is powered by 4160 VAC. AC power for all components needed to obtain emergency feedwater flow is derived from diesel generator-backed 4160 VAC busses. In addition to pump P7B, the following valves are on AC power: CV2800, CV2803, CV2813, CV2814, CV2626, CV2667, CV3850, CV2666, CV3851, CV2670, CV2617, CVX-2 and CVX-3. (Some of these components will not appear in the Table 3.1 and 3.2 since they were in cut sets with probabilities below the threshold cutoff.)

To ensure EFWS flow in the event of a loss of all AC power, the turbine-driven pump (P7A) train derives its motive power from the SGs for the pump and from a battery-backed DC bus for its valves. Valves requiring DC power are as follows: CV2620, CV2627, CV2802, CV2806, CV2815, CV2816, CVY-1, CVY-2, CVX-1, CVX-4.

3.3 FAULT TREE ANALYSIS

The objective of this phase of study is to estimate pointwise and average system unavailability to prevent dryout of the SGs, given each of the three initiators:

1. Loss of main feedwater (LMFW)
2. Loss of offsite power (LOOP)
3. Loss of all AC (LOAC)

In the analysis it is assumed that there is insufficient time for any recovery action (except that the operator successfully switches suction from the condensate storage tank to alternative suction from the nuclear service water system). Thus no credit is given for operator actions to recover from malfunctions or maintenance errors.

The fault tree and the failure data for the faults presented in the fault tree are given in Appendix 2 and Table 3.1. The fault tree has been derived from the EFWS initiation fault tree of "Emergency Feedwater System Upgrade Reliability Analysis for the Arkansas Nuclear One Nuclear Generating Station Unit No. 1."[11] All the modifications and assumptions used in the analysis will be described in the subsection 3.3.1. There are no single component minimal cut sets for this event. In formulating the Boolean expression for the FRANTIC input, all cut sets with mean unavailability $< 10^{-10}$ were eliminated. Failure characteristics for components which enter only in the eliminated cut sets are, therefore, not shown in Tables 3.1 and 3.2. The leading cut sets involve two components as listed in Appendix 3.

TABLE 3.1

Failure Characteristics for Components - EFWS

Component I.D.	Component Name	Failure Mode	Unavail. per Demand $\times 10^{-3}$	Hazard Rate/hr $\times 10^{-6}$	Info. Source
CV2670	Motor-Operated Valve (AC)	Fail to close	2.9	5.7	1
CV226	" " " "	" "	2.9	5.7	"
W-2	Check Valve	Flow blockage		0.8	"
W-4	" "	" "		0.8	"
FW13A	" "	" "		0.8	"
FW13B	" "	" "		0.8	"
CVX-3	Motor-Operated Valve (AC)	Fail to open	2.9	5.7	"
CVX-2	" " " "	" "	2.9	5.7	"
CV2620	" " " (DC)	Fail to close	2.9	19.3	"
CV2627	" " " "	" "	2.9	19.3	"
CVX-1	" " " "	Fail to open	2.9	19.3	"
CVX-4	" " " "	" "	2.9	19.3	1
W-3	Check Valve	--		0.8	"
W-1	" "	--		0.8	"
BAD07	Battery	Failure		1.6	2
BAD06	"	"		1.6	"
FW10A	Check Valve	Flow blockage		8.2	1
CST41	Cond. Storage Tank	Failure		0.1	7
CS98	Check Valve	Flow blockage		8.2	1
CS99	" "	" "		8.2	"
CV2803	Motor Operated Valve (AC)	Mech. failure		5.7	"
CV3850	" " " "	" "		5.7	"
CV2806	" " " (DC)	" "		19.3	"
CV3851	" " " (AC)	" "		5.7	"
FW10B	Check Valve	Flow blockage		8.2	"
CVY-3	Air Operated Valve	Fails High	2.3	4.5	"
CVY -4	" " "	" "	2.3	4.5	"
PV6601	Relief Valve	Fails to reset	3.1	5.1	"
PV6602	" "	" " "	3.1	5.1	"
CVY-1	Motor Operated Valve (DC)	Fail to open	2.9	19.3	"

TABLE 3.1 (Cont'd.)

Component I.D.	Component Name	Failure Mode	Unavail. per Demand $x10^{-3}$	Hazard Rate/hr $x10^{-6}$	Info. Source
W-5	Check Valve	Mech. failure		0.8	"
W-6	" "	" "		0.8	"
CVY-2	Motor-Operated Valve (DC)	Fail to open	2.9	19.3	"
CV2802	" " " "	Mech. failure		19.3	"
P7A	Turbine-Driven Pump	Mech. failure		34.0	6
P7B	Motor-Driven Pump	Mech. failure		6.3	6
CV2800	Motor-Operated Valve (AC)	Mech. failure		5.7	1
W7	Check Valve	Flow blockage		0.8	1
DG2	Diesel Generator	Fail to start	17.0	50.0	5
"	"	Fail to cont. to run		1000.0	"
DG1	Diesel Generator	Fail to start	17.0	50.0	"
"	"	Fail to cont. to run		1000.0	"
SW13	Check Valve	Flow blockage		0.8	1
	Safety Valve	Fail tc reseat	80.0		3
	Safety Valve	Fail to open	6.2		3
	Circuit Breaker	Failure to open	0.2		2
	Inverter	Failure		10.0	2

1. European Plant Data (unpublished)*
2. IEEE STD 500-1977
3. LER, NUREG/CR-1363
4. In Plant Reliability Data Base for Nuclear Plant Components: Data Report - The Pump Components NUREG/CR-2886
5. Diesel Generators Reliability at Nuclear Power Plants: Data and Preliminary Analysis EPRI-NP-2433
6. LER, NUREG/CR-1205
7. Based on engineering judgement for catastrophic failure.

* Rates derived as follows: No. of failures/demand spectrum; No. of failures/exposure hours; were no failures, the 50% Chi Square distribution was used.

TABLE 3.2

Summary of Emergency Feedwater System Testing and Maintenance

Component	Test Procedure	Test interval (days)	Length of first test interval (days)	Average test time (hours)	Average repair time (hours)	Unavailability override capability during test
Pump P7A	Start turbine pump measure suction and discharge pressures, bearing vibrations.	30.	10.	1.	7.	0.
CVY-1	Stroke tested (position checked before start-up from refueling) position indication in control room checked three times per day.	60.	10.	.08	4.	0.
CVY-2	"	60.	40.	.08	4.	0.
CV2802	Stroke tested w/CV2806, CV3851 (Position checked before start-up from refueling.)	90.	40.	.08	4.	0.
CV2806	Stroke tested w/CV2802 and CV3851. (Position checked before start-up from refueling.)	90.	40	.08	4.	0.
CV3851	Stroke tested w/CV2802, CV2806	90.	40.	.08	4.	0.
CVY-3	(P7A pump test assures that either CVY-3 or CVY-4 is truly open, not both.) The functioning checked at refueling.	60.	10.	.08	4.	0.
CVY-4		60.	40.	.08	4.	0.
SW13	Checked for plug	90.	40.	.08	4.	0.
CV2617 W-5 CV2666 W-6 CV2667	P7A pump test assures that either CV217 Ø W-5 are not plugged or W-6 0 CV2666 are not plugged or CV2667 is not plugged. The functioning checked at refueling	Modeled as nonrepairable between refueling components				
CS98	Checked for plugs with pumps test through line back to CST.	Alternates of 15830 days	10.	.08	4.	0.
CS99			25.	.08	4.	0.

TABLE 3.2 (Cont.)

Component	Test Procedure	Test interval in days	Length of first test interval in days	Average testing time in hours	Average repair time in hours	Unavailability override capability during test
Pump P7B	Manual start w/ one assure of suction of discharge pressure and test for bearing vibration	30.	25.	1.	7.	0.
CV2800	Stroke tested w/CV2803, CV3850; opening measured and then realigned (Position checked before start-up from refueling)	90.	85.	.08	4.	0.
CV2803	Stroke tested w/ CV2800, CV3850; opening measured, then realigned (Position checked before start-up from refueling)	90.	85.	.08	4.	0.
CV3850	Stroke tested w/ CV2800, CV2803; opening measured then realigned. (Position checked before start-up from refueling)	90.	85.	.08	4.	0.
SW11	Checked for plugs	90.	85.	.08	4.	0.
W-1 W-3 W-4 FW10A FW10B FW13A FW13B	Checked for leaks plugs during pump test at refueling shutdown and "tested" each time a transient requires emergency feed (This occurs about once per year)	Modelled as nonrepairable between refueling components.				
CVX-1 CVX-2 CVX-3 CVX-4	Tested at refueling shutdown or during transient.	Modelled as nonrepairable between refueling components.				
Diesel DG1		30.	14.	1.	25.	.08
DG2		30.	2[illegible]	1.	25.	.08
BAD06	Quarterly all cells measured; every third qrtrly test, battery cell charges are equalized.	90.	90.	2.	2.	0.
BAD07		90.	45.	2.	2.	0.

3.3.1 Assumptions

The following assumptions were accepted in this study:

1. Failures of the logic controlling flow rate to the SGs are not considered, nor are failures of the overfill protection logic or the "feed only good generator" (FOGG) logic, which is supposed to isolate a depressurized steam generator.

2. A failure mode involving degradation of EFWS flow due to excessive recirculation capacity is included. A normal recirculation flow of 15 gpm is provided for pump P7B (through valve FW1056) and pump P7A (through valve FW1055) to allow for pump cooling. Under low flow conditions whenever normal pump discharge flow is blocked, the 78-gpm recirculation path is open. Given loss of AC, CVX-2 and CVX-3 will not open. As a result, CV2815 and CV2816 are commanded to open, assuming that the motor-operated P7B pump needs more recirculation capacity. This will degrade the flow from the only working turbine-driven pump given that LOCA has occurred. In this analysis, this event is considered as a system fault.

3. Electrical power has not been modeled in any detail. Unavailability of AC power has been considered to be essentially the unavailability of the emergency diesel generator in the event of loss of offsite power. Similarly, DC unavailability is essentially that of the batteries.

4. The effect of support systems (e.g., cooling and lubrication) is assumed included in pump failure probabilities.

5. No credit is given in this analysis for the use of the Unit 2 condensate storage tank as an alternative water supply.

6. Credit is not given for operator corrective actions in any case, except it is assumed that the operator properly switches suction from the condensate storage tank to alternative suction from the nuclear service water system.

3.4 QUANTITATIVE ANALYSIS

All the input parameters related to test and maintenance of pumps and valves are summarized in Table 3.2.

Before proceeding with the result of analysis, one comment should be made. Although many components of the system are checked thoroughly during the refueling period (approximately every 18 months), they are not tested between refuelings. These components are modeled as nonrepairable. The following analysis can thus be regarded as a study of the first year of functioning after refueling. Wearing out of the components of the system may contribute to changes in parameters on the time scale of many years. Within this time scale, the refueling period can be considered as an overall test with a period of 18 months. The FRANTIC code allows consideration of such long-term processes with the wearing out being described by the Weibull distribution. However, the data available are presently insufficient to estimate the wearout (or burn-in) parameters; and as such, this study is limited to consideration of a one-year period following refueling.

3.4.1 Unavailability of Pumps as a Consequence of Test and Maintenance

Pump P7A (or P7B) can be left isolated after maintenance if the valve CV2800 (or CV2802) is accidently left closed and the operator fails to open it upon EFWS demand. These contributions to the unavailability of either or both trains are different depending on the availability of the offsite power. Since performance of maintenance on different components can leave certain valves unrestored afterward, no credit is given in this analysis for the discovery of the error by subsequent testing. Therefore, the error of leaving pump P7B isolated will be modeled as q_d, a time independent constant contribution to the pump P7B unavailability. Similar consideration is made concerning the error of leaving pump P7A isolated after maintenance. Maintenance errors associated with pump P7A are also modeled accordingly, noting however that P7A derives its power from feeds off the SGs and DC-power for valve actuation. Thus P7A pump unavailability is conditional on DC-power availability whether or not loss of offsite power (LOOP) is considered.

Another contribution to unavailability of either or both trains is a failure to reclose the pump's 4-in. test line after the pump test. Again, this error is considered unrecoverable between pump tests and modeled as a constant unavailability contribution to the pump unavailabilities.

All the results of the analysis discussed above are summarized in Table 3.3.

3.4.2 Unavailability of Diesels as a Consequence of Test and Maintenance

Diesel generators are tested monthly. Only part of the test makes them unavailable, for 5 min/test, so the unavailability to override test is 5 min/60 min = $8\text{x}10^{-2}$.

DG1 is tested at days 14, 44, 74, etc. and DG2 is tested at days 29, 59, 89, etc. If either diesel requires maintenance, the other must be tested immediately and every day thereafter until maintenance is completed or 7 days have elapsed, whichever is less. Seven days is the technical specification limit before shutdown is required. Historically, two maintenance jobs have been performed per year with the average outage of 25 hours. In order to evaluate the possible unavailability of diesel due to a combination of test and maintenance, the following calculations have been made. Given a conservative estimate of the outage time of tested diesel as 5 min x 7 days = 35 min, the average unavailability per year is 35 min/1 year = 7×10^{-5}. The average outage time for diesels repair is 25 hr per year so the probability of being in repair is 25 hrs/1 year = 3×10^{-3}. Therefore, total diesel unavailability due to the test and maintenance overlap is

$$(7 \times 10^{-5})\ (3 \times 10^{-3}) = 2 \times 10^{-7}\ .$$

This value was input as q_d for both diesels - constant unavailability.

TABLE 3.3

Unavailability of Pumps as a Consequence of Test and Maintenance

	P7A Inadvertently Left Isolated after Pump Maint.		P7B Inadvertently Left Isolated after Pump Maint.		P7A 4 Recirc. Left Open After Test	P7B 4 Recirc. Left Open After Test
	Given LOOP	No LOOP	Given LOOP	No LOOP		
Operator fails to realign valves in suction corrective action	$5x10^{-4}$	$5x10^{-4}$	$5x10^{-4}$	$5x10^{-4}$		
Operator does not fail to ...	$6x10^{-6}$	$1x10^{-7}$	$1x10^{-5}$	$3x10^{-7}$		
Operator fails to realign recirc. valves corrective action					$5x10^{-3}$	$5x10^{-3}$
Operator does not fail to ...					0	0

3.4.3 System Unavailability

With the input parameters described above, the average unavailability of the EFWS on demand to avoid dryout of the steam generators (for the one-year period) has been evaluated. The following results were obtained for different loss of main feedwater conditions (where vulnerability is as defined in Section 2.7):

1) Loss of main feedwater without loss of offsite power (LMFW):

   Average unavailability $\overline{q} = 3.00 \times 10^{-4}$,

   Vulnerability $V_{3x10^{-4}} = 0.43$,

The time-dependent behavior of the system unavailability, q(t), is shown in Fig. 3.2. Alternating peaks of the system unavailability correspond to the possible maintenance following pump tests for pumps P7A and P7B. (A conservative assumption is adopted, i.e., all components are being tested together with pumps, and those found failed will be in maintenance immediately after test, so their repair downtimes overlap.) The overall trend upward comes from the presence of a number of influential nonrepairable-between-refueling components which accumulate unavailability with time.

2) Loss of main feedwater associated with loss of offsite power (LOOP):

   Average unavailability $\overline{q} = 9.1 \times 10^{-4}$,

   Vulnerability $V_{9x10^{-4}} = 0.52$,

   Time-dependent unavailability is shown in Fig. 3.3.

3) Loss of main feedwater associated with loss of offsite and onsite power (LOAC)

   Average unavailability $\overline{q} = 1.0$. This conservative estimate follows from the assumption 2 (Section 3.3.1.)

Since maintenance data for pumps and valves often follow bimodal distribution with the lower mode of about 7 hours for pumps and 4 hours for valves and a higher mode of about 19 hours, the analysis was repeated twice in order to bracket the system unavailability in case of LMFW. For the average repair time, T_R, of 19 hours, the result is very similar:

$\overline{q} = 3.03 \times 10^{-4}$,

$V_{3x10^{-4}} = 0.43$.

The conclusion is that repair time does not significantly influence the mean results and therefore is not one of the critical parameters.

This completes the analysis of the base cases. The next section is devoted to uncertainty analysis. It will be performed by perturbing the first base case in order to see how much the mean unavailabiity will deviate from $\overline{q} = 3.0 \times 10^{-4}$ with different assumptions about the failure rates.

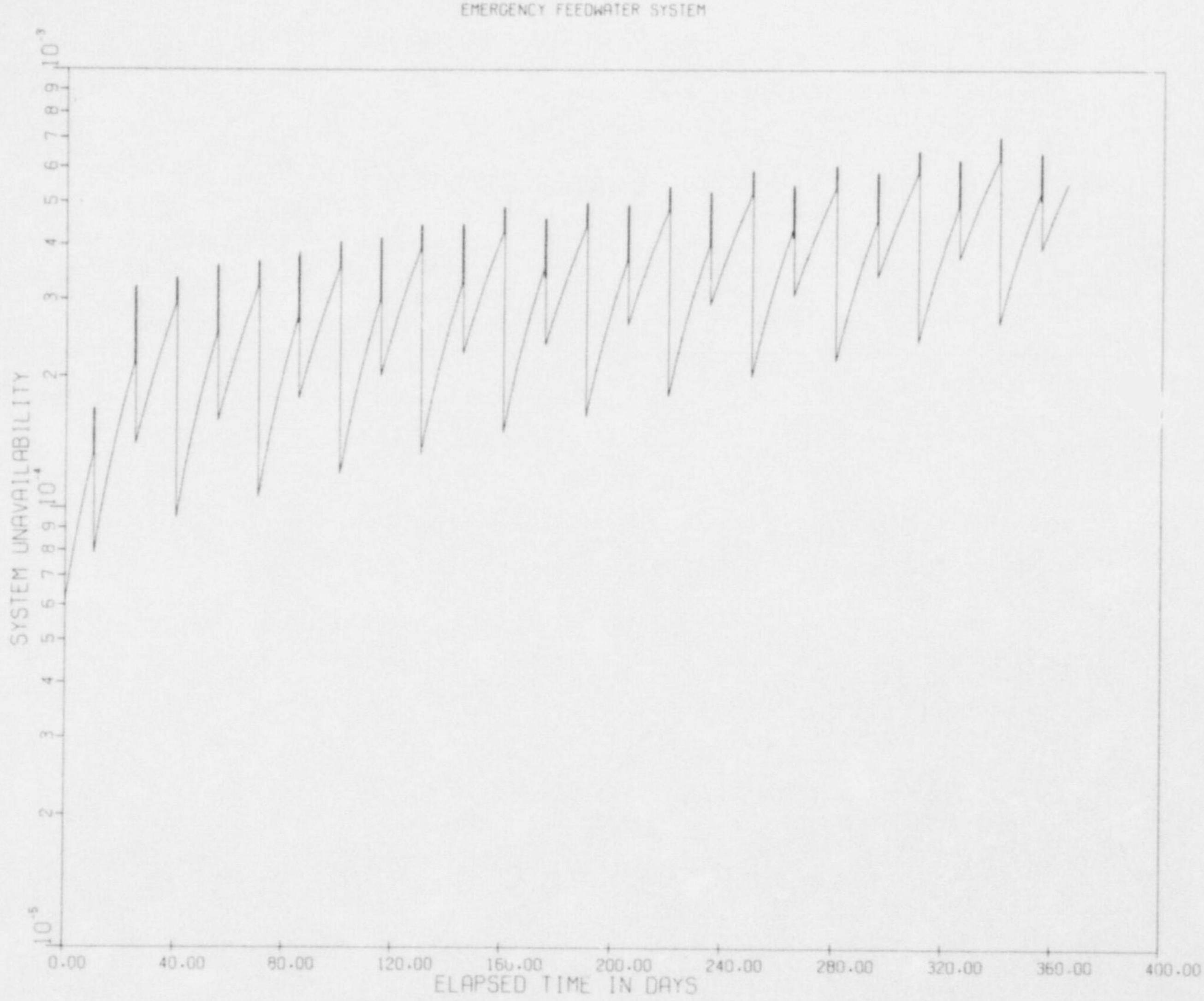


Figure 3.2. EFWS unavailability under LMFW condition.

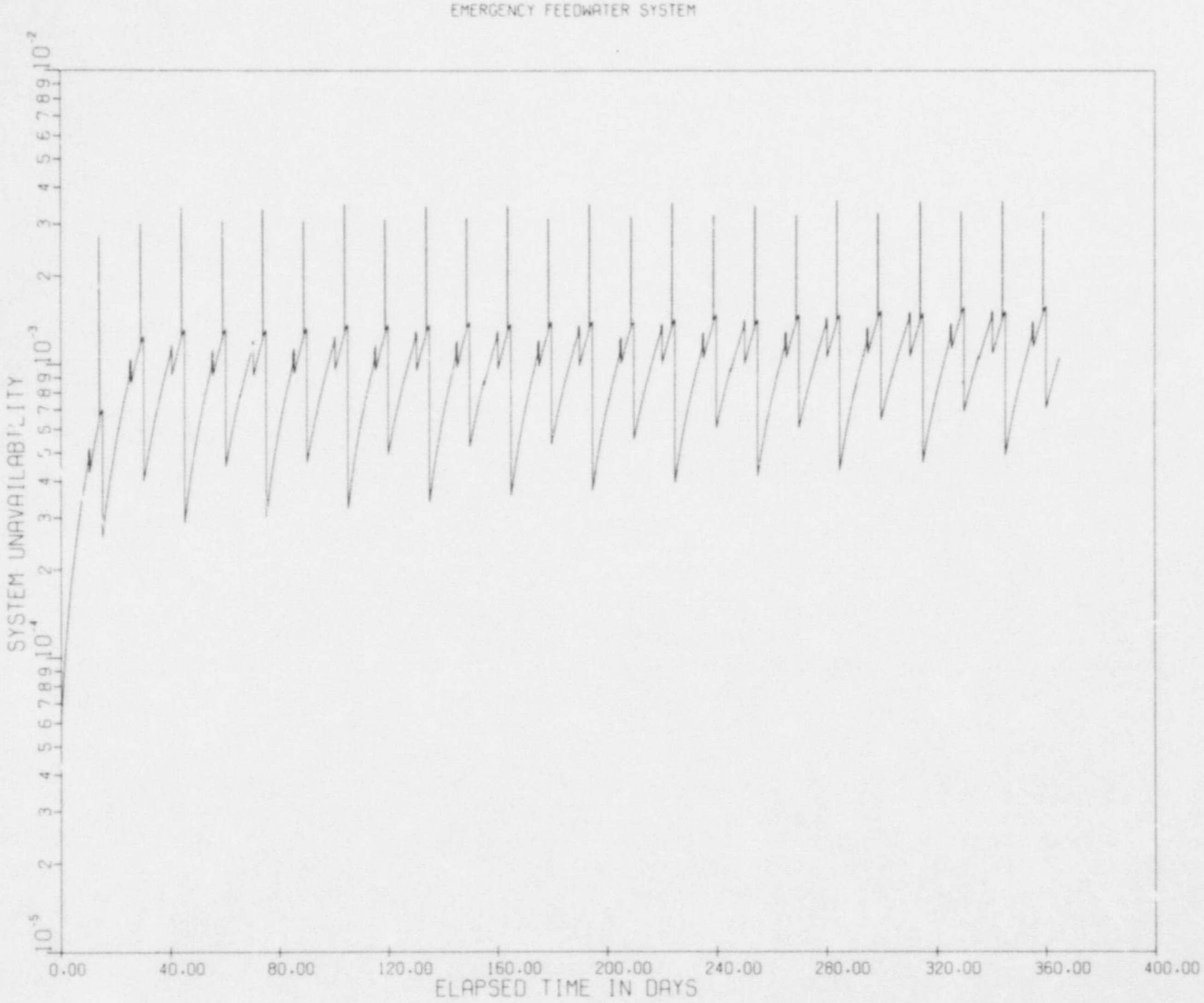


Figure 3.3. EFWS unavailability under LOOP condition.

3.5 UNCERTAINTY ANALYSIS

As mentioned before, an important feature of the FRANTIC II code is its ability to perform a comprehensive sensitivity analysis of the system unavailability with respect to failure, repair, and operational characteristics. In this section an analysis is performed for the EFWS with respect to possible errors in defining the shape and the scale of the failure distribution.

First, consider the base case where all failure distributions are assumed to be exponential and corresponding hazard rates, λ, are given in the first column of the Table 3.4.

Now, assume that the actual failure distribution is not exponential but follows a Weibull distribution. To evaluate only the influence of the shape of the distribution, it is assumed that the mean life time of every component remains the same. This imposes a relationship on the pair of the Weibull parameters, λ and β:

$$\lambda = (\Gamma[(\beta+1)/\beta]/T_F)^{\beta} \quad .$$

Two alternative cases will be considered for all major components and groups of components: $\beta = 1.5$ (wear out) and $\beta = 0.7$ (burn in). Corresponding values of λ for all components are listed in the second and third columns of Table 3.4. Clearly, when $\beta = 1.5$ the scale parameter, λ, is always lower than in the base case. This follows from the constraint that the mean life time, T_F, remains equal in all cases.

The results of varying one component at a time from the base case are given in Table 3.5. In order to evaluate these results properly, one should remember that the base case gave

$$\begin{aligned} \bar{q} &= 3.0 \times 10^{-4} \\ V_{3 \times 10^{-4}} &= 0.43 \end{aligned} \tag{3.1}$$

for average system unavailability and vulnerability.

The value of the threshold in the vulnerability definition is, in principle, arbitrary. It makes sense to choose this level at the mean unavailability of the base case for purely comparative purposes. In all cases then, one can see the percentage of time that the system spends with the unavailability higher than the base case average.

A number of interesting conclusions can be made from the Table 3.5. For mean average unavailability, check valves are the most influential group of components from the point of view of the shape of their failure distribution. The mean unavailability differs by a factor of 7 between the burn-in (highest) and wear-out (lowest) cases (Figs. 3.4 and 3.5). Next are both motor- and turbine-driven pumps. Variability in shapes of their distributions yields a factor of 2 in comparison to the average unavailability. Correspondingly, motor-operated valves exhibit a smaller change than do pumps and check valves. The shape of their failure distributions is clearly not an important factor of system unavailability. Finally, diesels and batteries have the least influence in system unavailability.

TABLE 3.4

Scale Parameter λ for Different Shapes of Weibull Distribution for Components of EFWS

Component Name	λ (β = 1) base case	λ (β = 0.7) burn-in	λ (β = 1.5) wear out
Turbine-driven pump P7A	3.4×10^{-5}	6.8×10^{-4}	1.7×10^{-7}
Motor-driven pump P7B	6.3×10^{-6}	2.1×10^{-4}	1.4×10^{-8}
Check valves	8.2×10^{-7}	5.0×10^{-5}	1.0×10^{-9}
Motor-operated valves (AC)	5.7×10^{-6}	2.0×10^{-4}	1.2×10^{-8}
Motor-operated valves (DC)	1.9×10^{-5}	4.6×10^{-4}	7.1×10^{-8}
Diesels	5.0×10^{-5}	9.0×10^{-4}	3.0×10^{-7}
Batteries	1.6×10^{-6}	8.0×10^{-5}	2.0×10^{-9}

TABLE 3.5

Average Unavailability and Vulnerability of EFWS for Different Shapes of Failure Distributions

Component Name	EFWS Mean Unavailability $\beta = 0.7$	EFWS Vulnerability $V_{3x10^{-4}}(\beta=0.7)$	EFWS Mean Unavailability $\beta = 1.5$	EFWS Vulnerability $V_{3x10^{-4}}(\beta=1.5)$
Turbine-driven pump P7A	6.1×10^{-4}	.87	2.4×10^{-4}	.23
Motor driven pump P7B	5.3×10^{-4}	.85	2.6×10^{-4}	.31
Check Valves	1.3×10^{-3}	.92	1.9×10^{-4}	.02
Motor operated valves (AC)	3.9×10^{-4}	.64	2.9×10^{-4}	.39
Motor operated valves (DC)	3.0×10^{-4}	.44	3.0×10^{-4}	.42
Diesels	3.0×10^{-4}	.43	3.0×10^{-4}	.43
Batteries	3.0×10^{-4}	.43	3.0×10^{-4}	.43

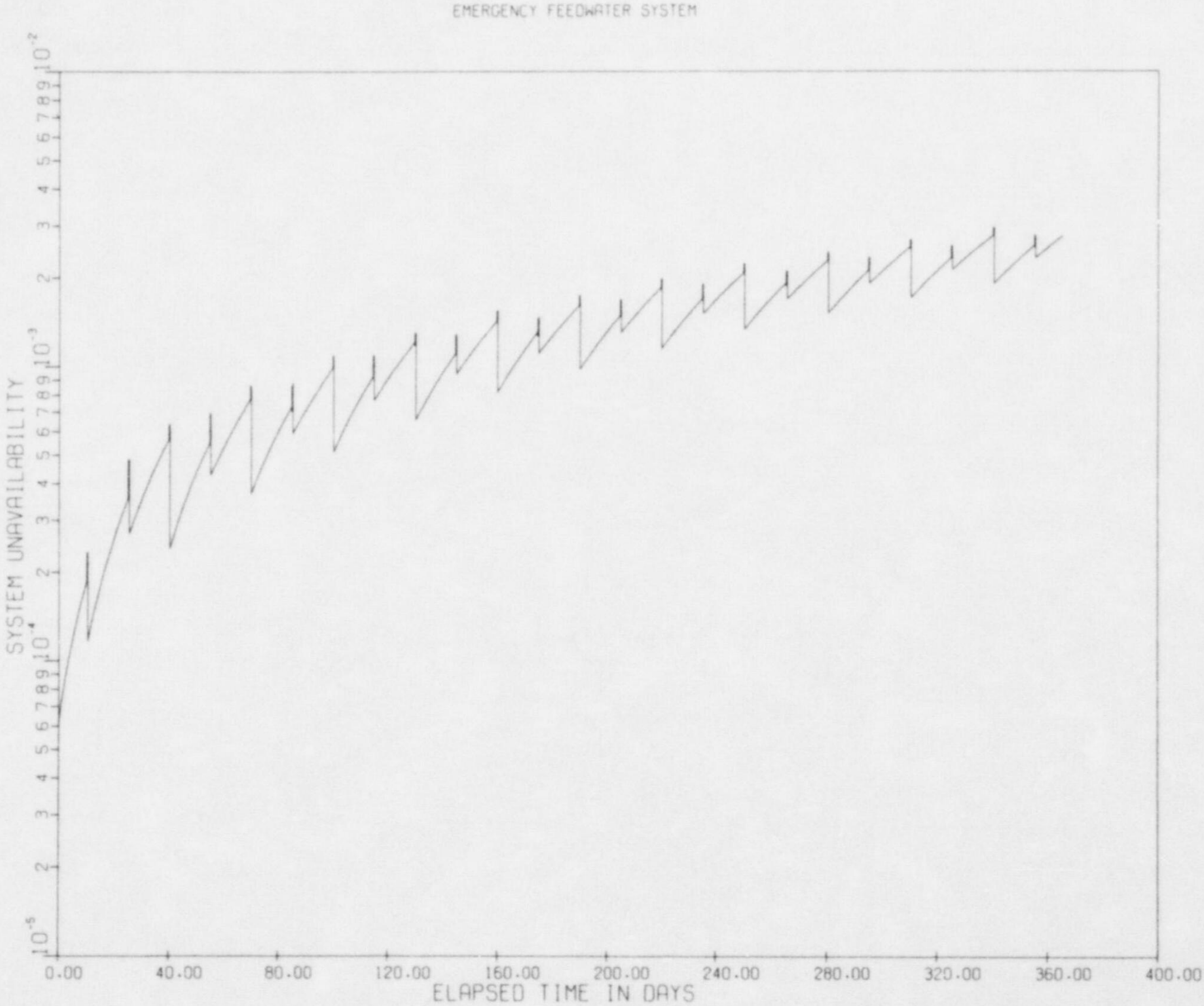


Figure 3.4. EFWS unavailability with "burn-in" assumption for check valve failure rates.

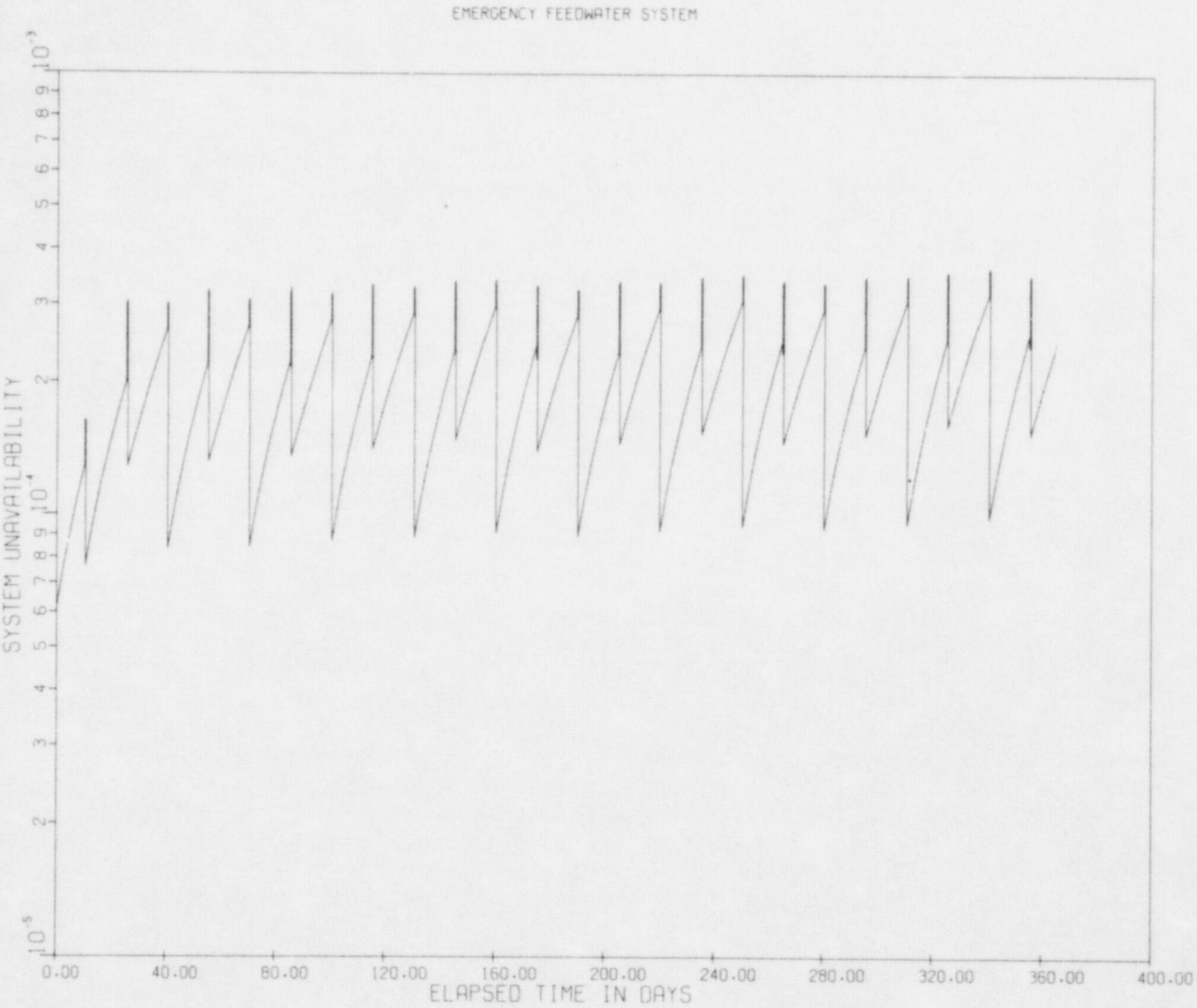


Figure 3.5. EFWS unavailability with "wear-out" assumption for check valve failure rates.

The values of mean unavailability and vulnerability, listed in Table 3.5, are, as shown, in direct accordance. However, the respective rate of change differs for different components.

For motor-operated valves (AC), for example, the mean unavailability decreases by 26% from 3.9 x 10^{-4} to 2.9 x 10^{-4} between the burn-in and wear-out case, while the vulnerability is reduced by 64%. This indicates that knowing the precise shape of the failure distribution for these valves may not be critical from the point of view of average unavailability, but it could be very critical from the point of view of vulnerability.

Note that these results were obtained by separately considering for each component the effect of the shape of the failure distribution on both mean unavailability and system vulnerability. Joint consideration of two or more components may yield results that differ from the base values by about an order of magnitude. This exercise amplifies the need for additional data for these components in order to substantiate their respective failure-distribution shape.

Besides considering the influence of the shape of the failure distribution, one must also consider the effect of the error propagation in the hazard rate, λ. Thus, the hazard rate of every group of tested components was increased by an order of magnitude and the effect of such a change on the system mean unavailability and vulnerability was calculated. The results are presented in Table 3.6 and should be compared with the aforenoted base case results.

By comparison with the previous example, it is not surprising that check valves have a marked influence on the system (Fig. 3.6) followed by the turbine-driven pump (Fig. 3.7), and then the motor-driven pump (Fig. 3.8). Note however that the motor-operated valves (AC) hazard rate is also influential (Fig. 3.9), even though its failure distribution shape is not as critical (Table 3.5 indicates the effect is about 26%). The error in estimating the hazard rate by an order of magnitude may more than triple the system unavailability. By contrast, the motor-operated valves (DC) show little influence as it did in the previous example. These tend to show the importance of performing error propagation studies with respect to both mean life time and shape of the failure distribution. The latter is not possible to do on the basis of the codes dealing only with the average unavailabilities of components.

TABLE 3.6

Error Propagation of the Mean Life Time Estimates with Respect to the Average System Unavailability and Vulnerability

Component	Base Case	Modified		V
Name	λ	λ	$\bar{q}$	3.10^{-4}
Steam driven pump P7A	$3.4x10^{-5}$	$3.4x10^{-4}$	$1.4x10^{-3}$	0.94
Motor driven pump P7B	$6.3x10^{-6}$	$6.3x10^{-5}$	$1.1x10^{-3}$	0.94
Check valves	$8.2x10^{-7}$	$8.2x10^{-6}$	$4.3x10^{-3}$	0.94
Motor operated valves (AC)	$5.7x10^{-6}$	$5.7x10^{-6}$	$1.1x10^{-3}$	0.88
Motor operated valves (DC)	$1.9x10^{-5}$	$1.9x10^{-4}$	$3.2x10^{-4}$	0.48

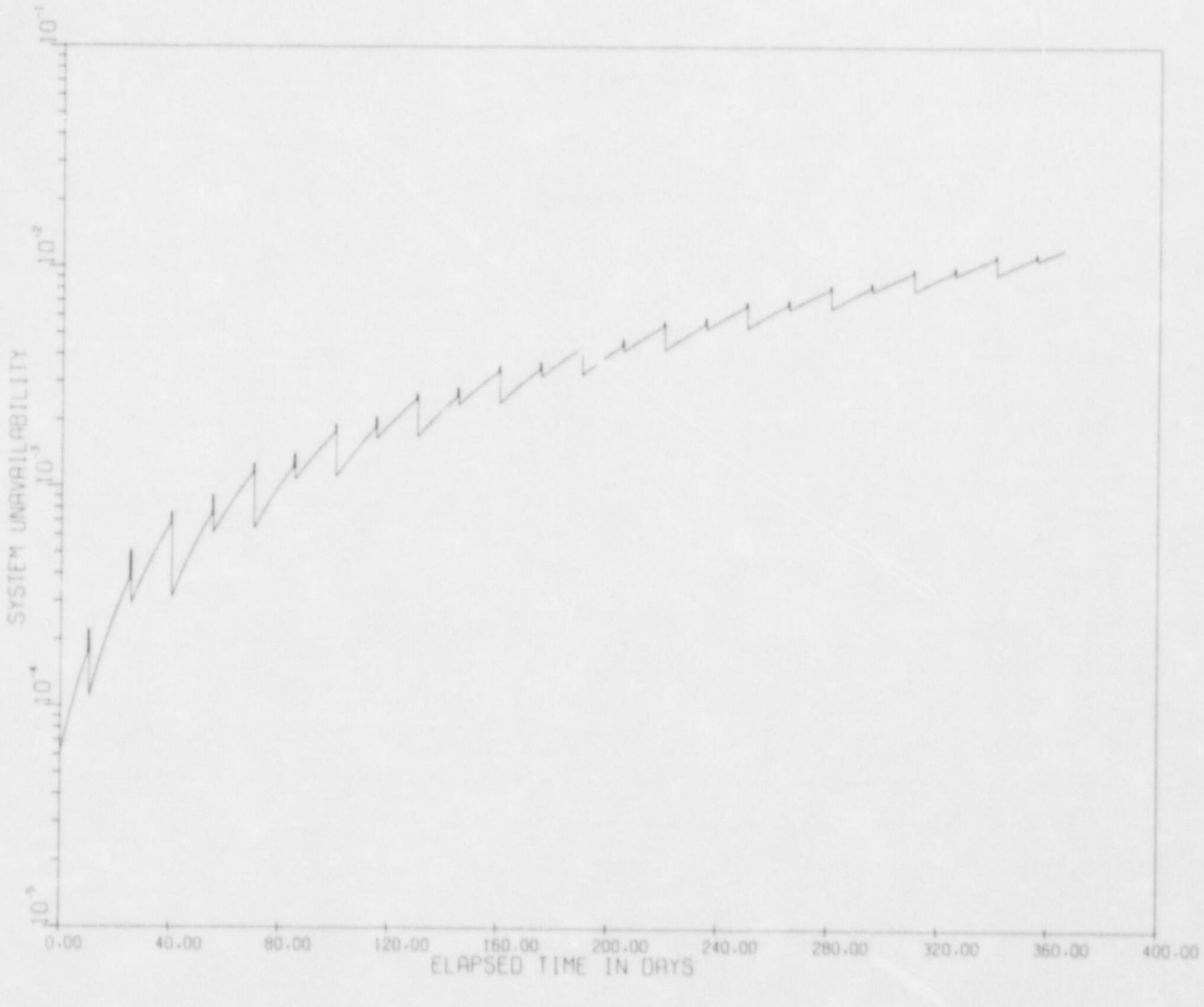


Figure 3.6. EFWS unavailability with an order of magnitude lower mean life time of check valves.

EMERGENCY FEEDWATER SYSTEM

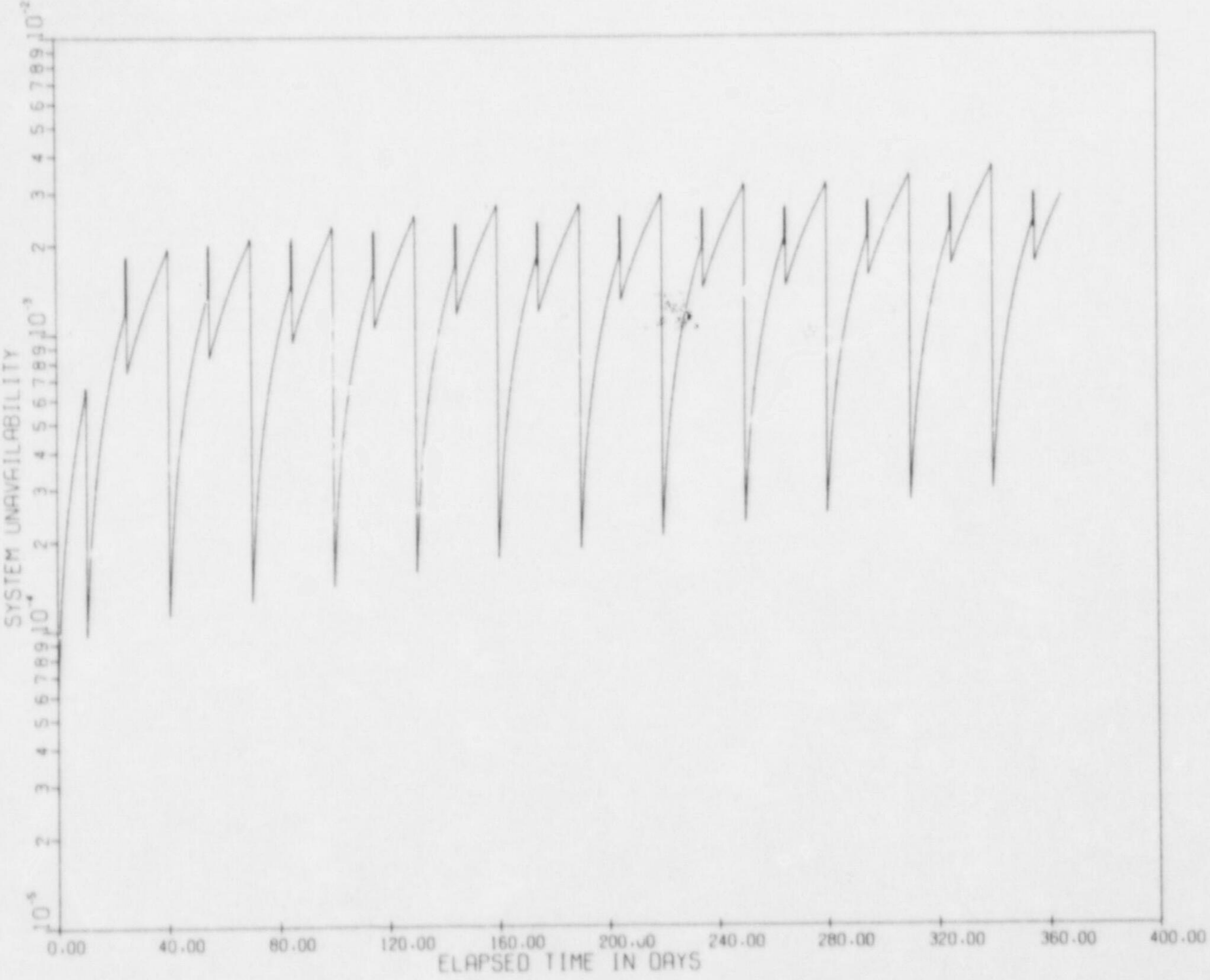


Figure 3.7. EFWS unavailability with an order of magnitude lower mean life time of turbine-driven pump.

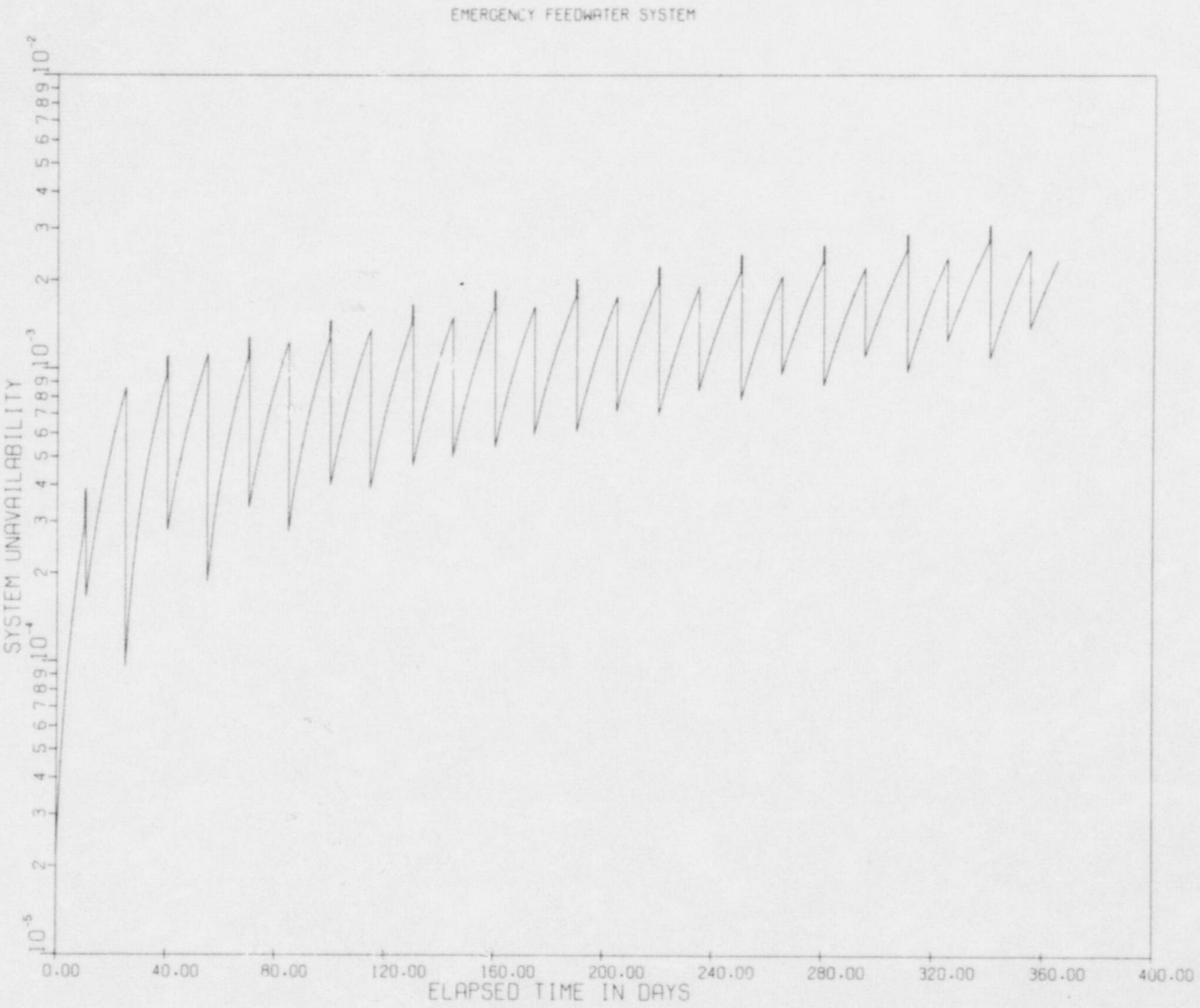


Figure 3.8. EFWS unavailability with an order of magnitude lower mean life time of motor-driven pump.

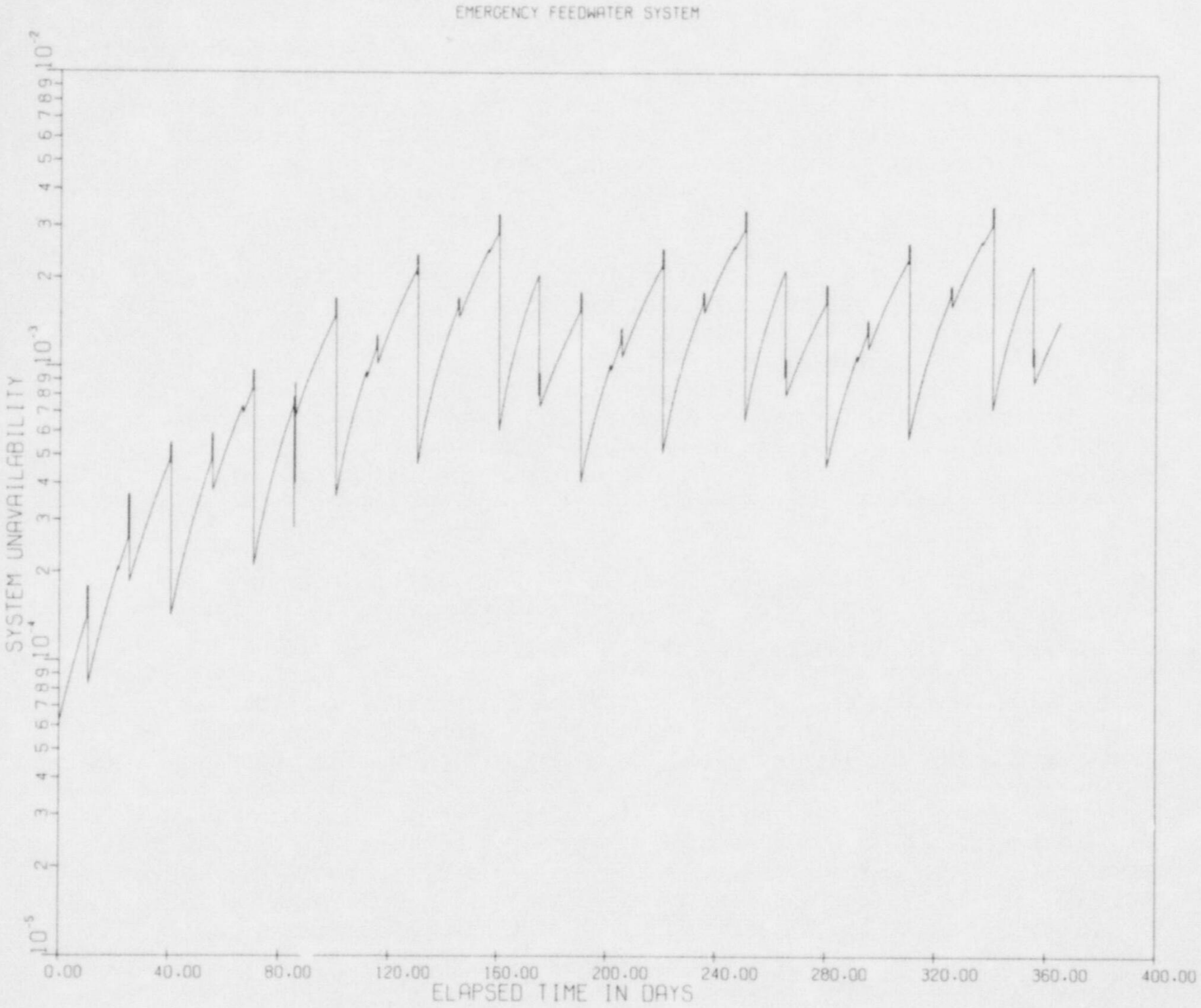


Figure 3.9. EFWS unavailability with an order of magnitude lower mean life time of motor-operated (AC) valves.

4. AUTOMATIC DEPRESSURIZATION SYSTEM

4.1 INTRODUCTION

The Automatic Depressurization System (ADS) in Caorso is designed to actively function in the event that the High Pre‿sure Coolant Injection System (HPCIS) and the Reactor Core Isolation Cooling System (RCICS) fail to reflood the reactor after a small LOCA. If HPCIS and RCICS fail to perform their respective design functions, the ADS will vent the reactor pressure vessel steam into the suppression pool, thus reducing reactor pressure so that the Low Pressure Coolant Injection System (LPCIS) and the Core Spray Injection System (CSIS) can inject coolant into the reactor vessel. A brief description of the ADS for the BWR4, Mark II, is given below. A similar system is fully described in WASH-1400[12].

One reason for the choice of the ADS for this study is the evaluation of the effects created by the fault tree reduction. Combining primary components is a common procedure in the reduction of fault trees. This not only simplifies the fault tree logic but is often the only recourse due to insufficient data or inability to treat common mode failure mechanisms. The shape of the failure distribution for the combination of primary components may vary widely even if the distributions for primary components are exponential. Using the reduced fault tree for the ADS, the error incurred through fault tree simplification together with considering the "combined" components failure distribution as exponential will be analyzed.

The second point in the ADS study relates to the vulnerability analysis. While doing test optimization, one should note the changes in vulnerability. An increase in the frequency of tests may sometimes be beneficial from the mean unavailability point of view. Also, the optimum is often very flat so that the gain in the mean unavailability due to increased testing is very small; and the vulnerability is often directly proportional to the number of tests performed and will increase significantly with the frequency of tests.

Common cause failures are generally accepted as dominant contributors to the ADS unavailability. The numerical estimates of the frequencies for the common cause are quite conservative (10^{-3} or an order of magnitude higher than all the other contributions combined). To assess the error in the fault tree reduction, the system reliability will be studied excluding common causes, since they are modeled as a separate component on the fault tree, which constitutes a minimal cut set by itself.

4.2 SYSTEM DESCRIPTION

Consider a BWR 4, Mark II plant, which has 16 safety relief valves. The Automatic Depressurization System (ADS) consists of eight of these valves and of the necessary instrumentation for their operation. The (ADS) valves can operate automatically following a small LOCA. These valves are located on the main steam lines (see Fig. 4.1). Initiation of the ADS requires a simultaneous signal from the following instrumentation (see Fig. 4.3):

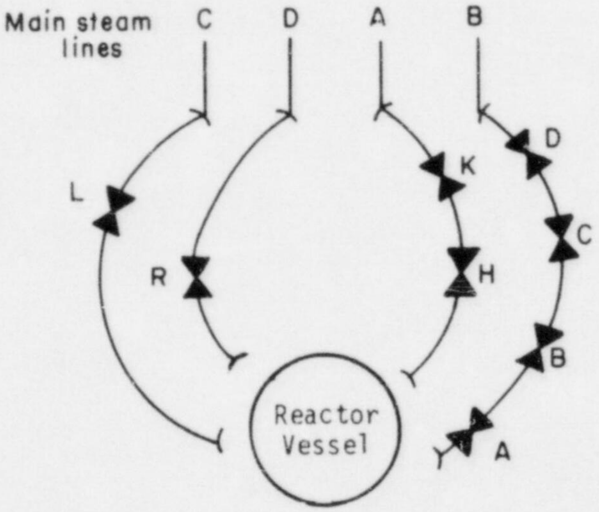


Figure 4.1. Location of eight Automatic Depressurization System (ADS) valves.

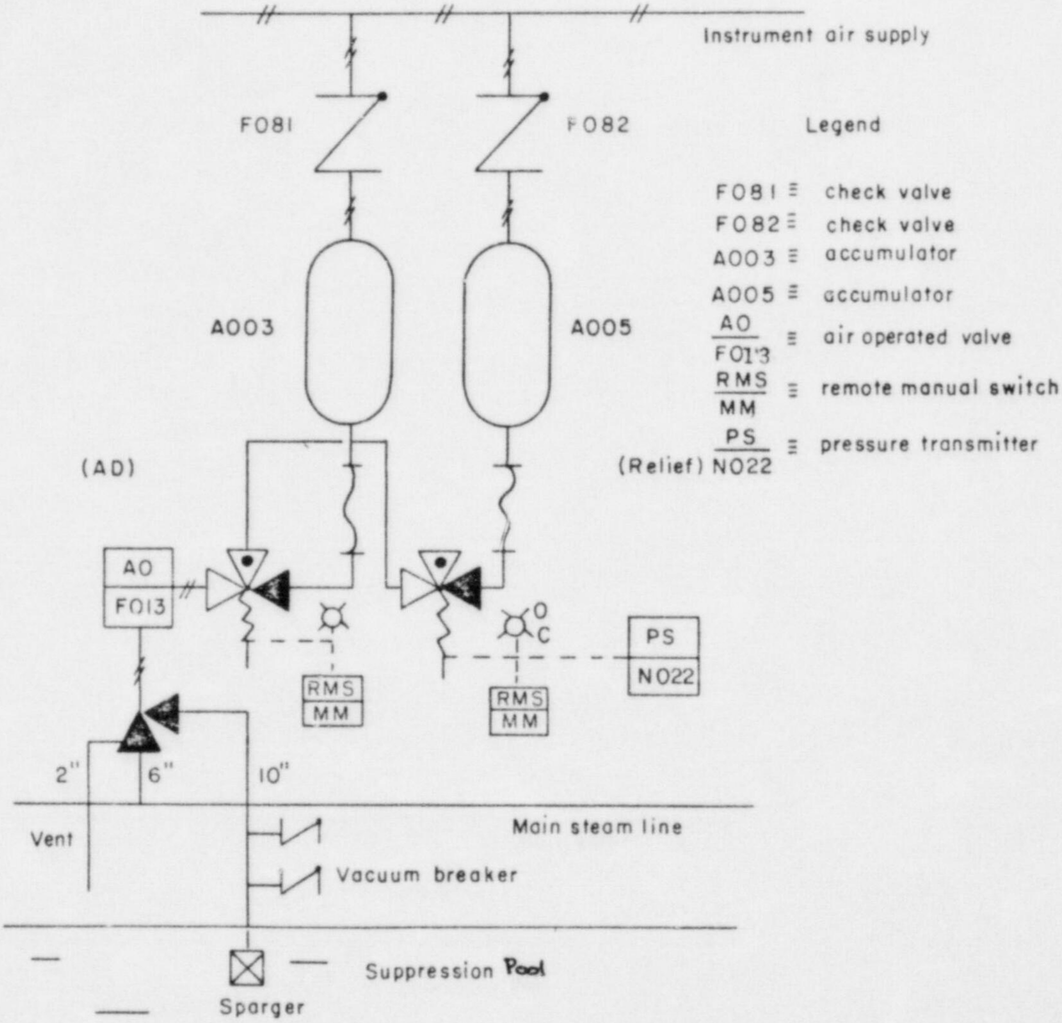


Figure 4.2. Valve diagram.

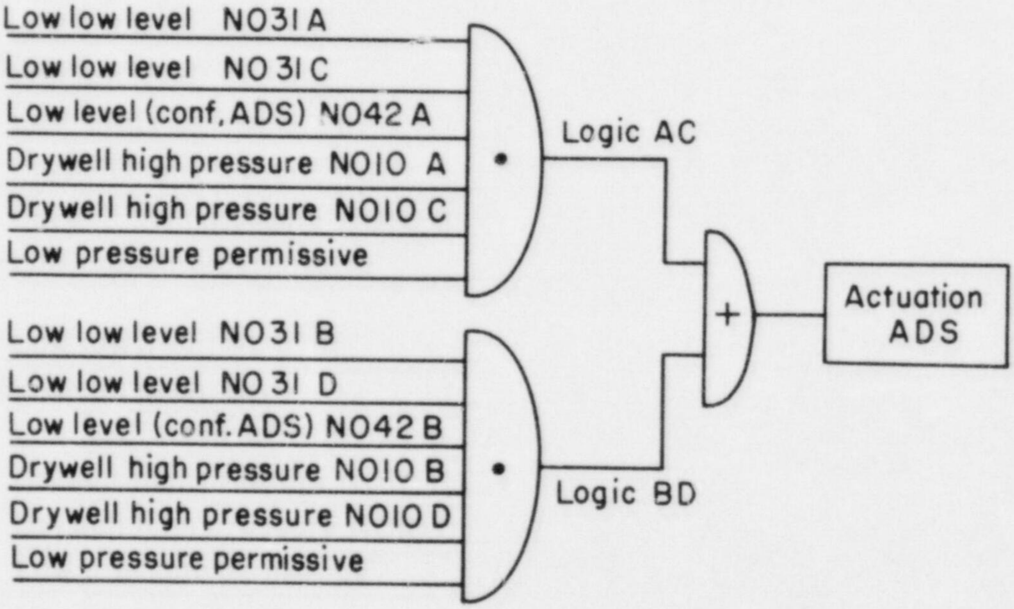

Low low level NO31 A
Low low level NO31 C
Low level (conf. ADS) NO42 A
Drywell high pressure NO10 A
Drywell high pressure NO10 C
Low pressure permissive
Low low level NO31 B
Low low level NO31 D
Low level (conf. ADS) NO42 B
Drywell high pressure NO10 B
Drywell high pressure NO10 D
Low pressure permissive
•
•
Logic AC
Logic BD
+
Actuation ADS

Figure 4.3. Automatic Depressurization System (ADS) logic.

-- Drywell high pressure and reactor vessel low low water level.

-- ADS confirmatory reactor vessel low water level.

-- Actuation of at least one of the low pressure coolant systems.

The actuation logics with the related power supplies are redundant. The solenoids that actuate the pilot valves are normally deenergized. They can be energized by one of the two redundant logics AC or BD (see Fig. 4.3).

Each ADS valve has an air accumulator which supplies control air to operate the valve during a LOCA. This accumulator is able to open the valve and keep it open against the maximum expected pressure in the primary containment following a LOCA (23 psig).

Although ADS (Mark II, BWR 4) has eight ADS valves, only seven are considered in the fault tree. Since the analysis of Emergency Core Cooling System (ECCS) for compliance with Appendix K of 10CFR50 is performed with only seven valves. One valve can be continuously out of service. The system failure is reached when at least two other valves are out of service (see Fig. 4.4). Therefore, the system is considered failed with a logic "two out of seven" instead of a logic "three out of eight."

The faults, which involve the unavailability of the two logic circuits, are also important contributors to the system unavailability. They belong to the triple minimal cut sets. In the case of logic circuit failures, the operator can manually open each of seven ADS relief valves. However, because of the potential for stress under accident conditions, no credit is given for operator action.

Test and maintenance contributions to system unavailability are assumed unimportant. Maintenance is performed only during plant shutdown, since the valves and ancillary equipment are inside the primary containment. Periodic testing and calibration of the level and pressure switches are performed with a frequency of one month. Test contributions are considered insignificant to the system unavailability. However, coupled human errors involving miscalibration or failure to properly configure the sensors following calibration is a dominant contributor to the system unavailability. Surveillance tests on the logic part of the system are performed every six months. A diagram of a single valve is shown in Fig. 4.2.

4.3 DATA SOURCES AND FAULT TREE QUANTIFICATION

The data for the elementary components are derived from the following documents:

-- Reactor Safety Study - WASH-1400, Appendix III

-- Recommended Component Failure Rates for Use in Reliability/Availability Analysis - Doc. GE 22A2689

In order to reduce the fault tree, the elementary components are grouped into subsystems as shown in Table 4.1. The following assumptions are made for the components that are grouped:

-- the failure rates of elementary components are constants

-- for the components connected in series, the failure rate of the resultant subsystem is calculated as the sum of the elementary component's failure rates

-- for the parallel components the failure rate of the resultant subsystem calculated following the standard procedure[13], i.e.,

a) for two components:

$$\frac{1}{\frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}}$$

b) for three components:

$$\frac{1}{\frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} - \frac{1}{\lambda_1+\lambda_2} - \frac{1}{\lambda_1+\lambda_3} - \frac{1}{\lambda_2+\lambda_3} + \frac{1}{\lambda_1+\lambda_2+\lambda_3}}$$

c) for n components with the same failure rate,

$$\frac{1}{\frac{1}{\lambda} + \frac{1}{2\lambda} + \frac{1}{3\lambda} + \ldots + \frac{1}{n\lambda}} = \frac{1}{\sum\limits_{i=1}^{n} \frac{1}{i\lambda}}$$

In cases when the values of the average unavailability of elementary components are known, the unavailability of the resultant subsystems can be computed using Boolean expressions for unavailability of parallel and series configurations.

These expressions are approximate, and are based on the idea of equating the mean life time of the particular combination of components to the correct value, keeping the assumption of exponentiality which is, in most cases, not totally valid [13]. Combining exponentially distributed components into subsystems does change the shape of the distribution for the subsystems. The formulas used guarantee only that the mean life time of the subsystem is evaluated correctly. Clearly, when analyzing the overall system, it is necessary to investigate the sensitivity to the shape of the subsystem's failure rate distributions. Within the framework of the FRANTIC code, this entails that the shape parameter, β, will vary and the overall system will be evaluated on the basis of a range of β values rather than on one value, namely for β=1, which corresponds to the exponential failure rate assumption.

TABLE 4.1

The List of Subsystems

F013X* : Block valve mechanical failure, it includes failures of valve F018X (check valve), accumulator A003X, F018 valve piping rupture, pilot valve rupture, actuator and relief valve rupture, pilot valve solenoid, contacts of solenoid supply KC20X, coil of solenoid actuation relays KB20X.

NCLSX : Includes failures of commutation relay coil KB19X, fuses FnB, FmB, contacts 1K19X, 2K19X

FU78X : Includes failures of fuses FrA, FsA, contacts 3K19X, 4K19X

BUSA,
BUSB : DC power supplies.

XK67A,
XK67B : Include failures of contacts XK6A(B) and XK7A(B) (actuation relays)

KAC6 : Includes failures of coils KB6A and KB7A (actuation relays for logic AC)

KBD6 : Includes failures of coils KB6B and KB7B (actuation relays for logic BD)

LOGAC : Includes failures of coils and contacts of relays K2A, K3A, low pressure permissive relays K9A, K10A, timer relay K5A, manual switch MM613A, level switches N031A, N031C(-370 indicator), N042A (+32), pressure switches N010A, N010C.

LOGBD : Includes failures of relays K2B, K3B, K9B, K10B, K5B, MM613B, N031B, N031D, N042B, N010B, N010D, transmitter relays K12, K13, K14, K15

BUS A&F : Includes Bus A, Fuses F1A, F2A, Contacts 1KC1A, 2KC1A

BUS B&F : Includes Bus B, Fuses F3, F4, F5, F6, F55, F56

KC1X : Commutation relays from Bus A to Bus B

NCLOG : Includes failures of coils of commutation relay KB1A, contacts 3KC1A, 4KC1A, Fuses F1B, F2B

*X stands for the name of the valves which are denoted as A, B, C, D, H, K, L.

Test intervals are assumed so that there is no overlap of test and repair periods between different components.

An approximate formula for the system unavailability is used. Using $q_s(t)$ as the notation for the system unavailability, we have:

$$q_s = \sum_{j=1}^{3} \sum_{i=1}^{n_j} q\ (MCS_{ij})$$

where MCS_{ij} is the ith minimal cut set of the jth order for the system fault tree. The maximum order taken into account is 3. This allows one to obtain the upper bound for the system unavailability, neglecting the contributions of the minimal cut sets of higher orders.

4.4 TIME DEPENDENT UNAVAILABILITY ANALYSIS

Average unavailability of the ADS is known to be dominated by the common mode failure[12]. Since the various sensors are assumed to be calibrated by groups of related sensors which can thus lead to coupled human error, it is conservatively assumed that if failure in calibrating sensors occurs once, the chances of subsequent mistakes are not independent but grow significantly. This common mode produces a contribution on the order of 10^{-3} to the ADS. Subsequent analysis will show that all other sources contribute at least an order of magnitude less than that from common mode. The reduced fault tree of the ADS is shown on Fig. 4.4 with common mode represented as a separate constant unavailability component.

Table 4.2 shows the input parameters of ADS for the FRANTIC II code "Components" data group. The primary components of ADS were considered as either components with constant unavailability or as those tested periodically.

In order to demonstrate simply the results one can obtain by using the FRANTIC II code, all periodically tested components have been subdivided into four groups. Each group contains analogous components (see Table 4.3). The components which are not included in this classification are constant unavailability components. With these input parameters the average unavailability of ADS (neglecting common mode) to fail on demand is

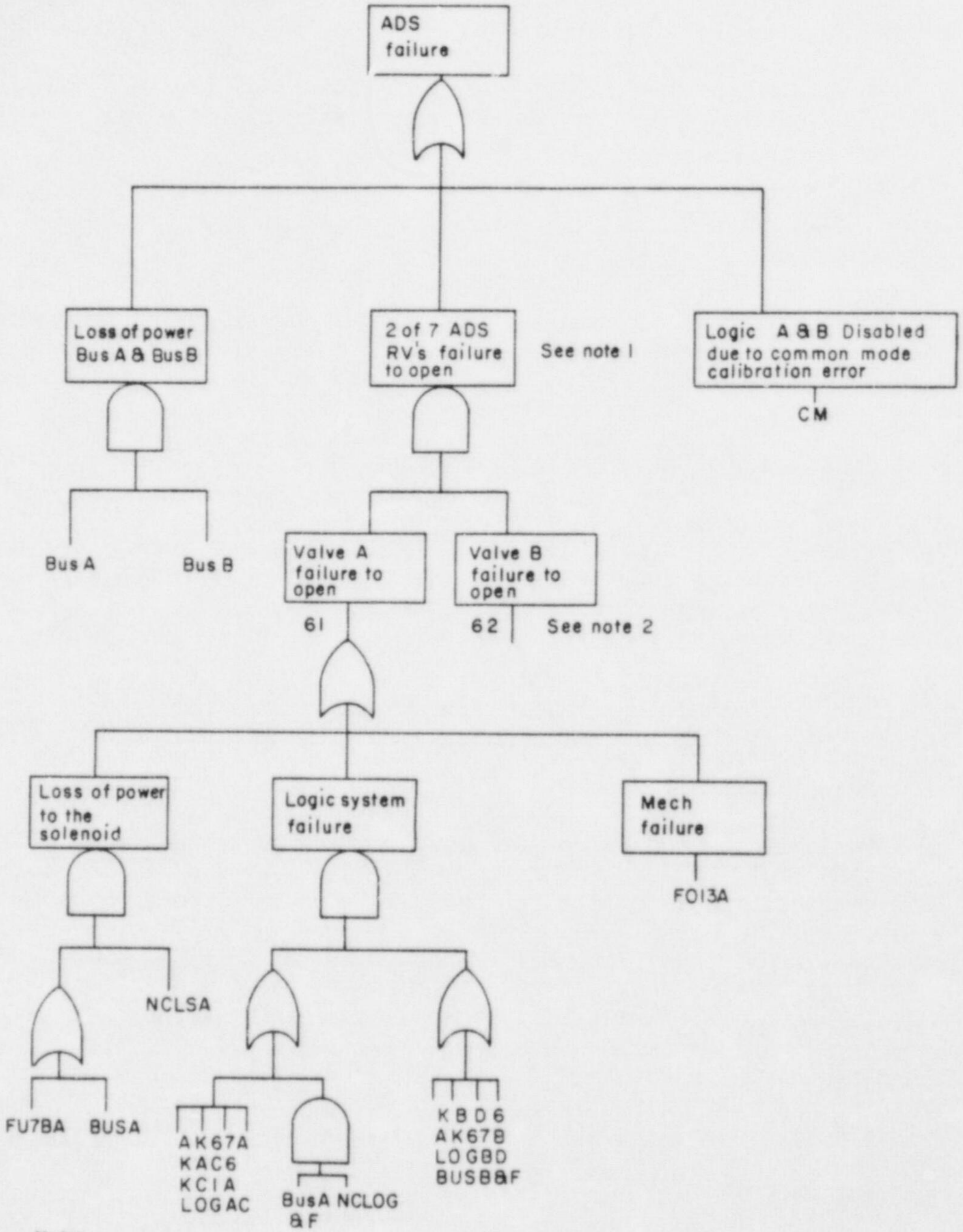
$$\bar{q} = 8.51 \times 10^{-5}$$

and the vulnerability (percentage of time with unavailability exceeding 10^{-4}) is

$$V_{10^{-4}} = 5.1 \times 10^{-3}$$

The pointwise unavailability curve is shown on Figure 4.5.

In Figure 4.6 a ten-day segment of the pointwise unavailability is depicted during which time components from Group III and Group IV categories are sequentially tested daily.



Notes:

1. Typical "pair" failure of two ADS valves — there are 21 such possible pairs.

2. G 2, the branch for valve B is the same as G1 for valve A.

Figure 4.4. Automatic Depressurization System (ADS) fault tree.

TABLE 4.2

Input Parameters of ADS for FRANTIC II "Components" Data Group

INDX	NAME	LAMDA	TEST2	TEST1	TAU	REPAIR	QOVRD	QRESID
		x10^{-6}						x10^{-4}
1-7	F013X*							2.0
8-14	NCLSX	3.1	180.0	15.0-21.0	1.0	12.0	1.0	
15-21	FU78X							1.0
22	BUSA							5.0
23	BUSB							5.0
24-30	XK67A							2.0
31-37	XK67B							2.0
38	LOGAC	5.5	30.0	28.0	1.0	12.0	1.0	
39	KAC6	0.2	180.0	2.0	1.0	12.0	1.0	
40	KBD6	0.2	180.0	3.0	1.0	12.0	1.0	
41	BUS A&F							5.0
42	BUS B&F							5.0
43	LOGBD	7.0	30.0	29.0	1.0	12.0	1.0	
44-50	KC1X	0.1	180.0	4.0-10.0	1.0	12.0	1.0	
51	NCLOG							2.0
52	CM (Common Mode)							50.0

*X stands for the name of the values which are denoted as A, B, C, D, H, K, L

TABLE 4.3

Subdivision for ADS into the Groups of Analogous Periodically Tested Components

I	II	III	IV
NCLSZX*	LOGAC	KAC6	KCIX
	LOGBD	KBD6	

*X stands for the name of the valves which are denoted as A, B, C, D, H, K, L.

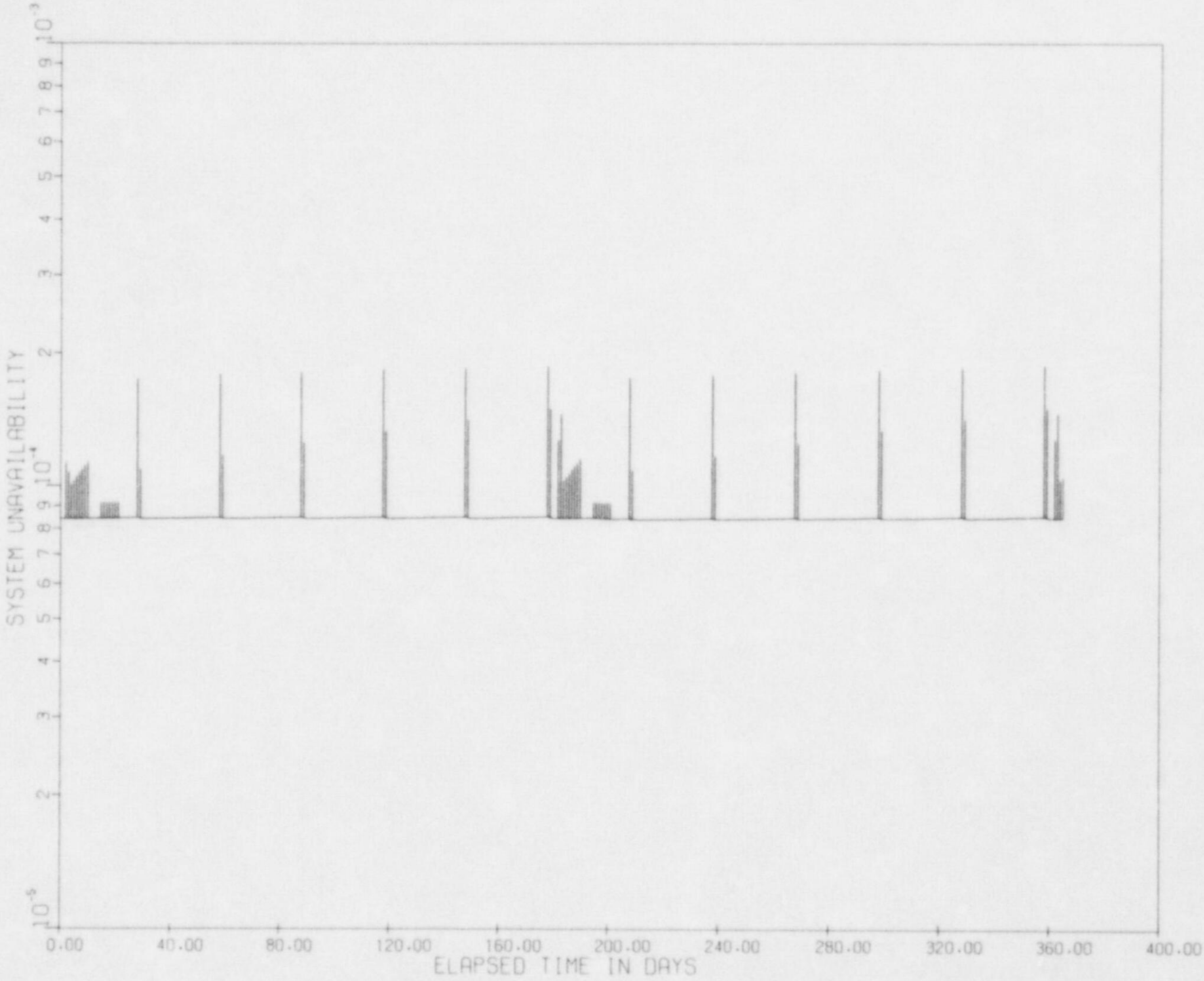


Figure 4.5. ADS unavailability during a one-year period.

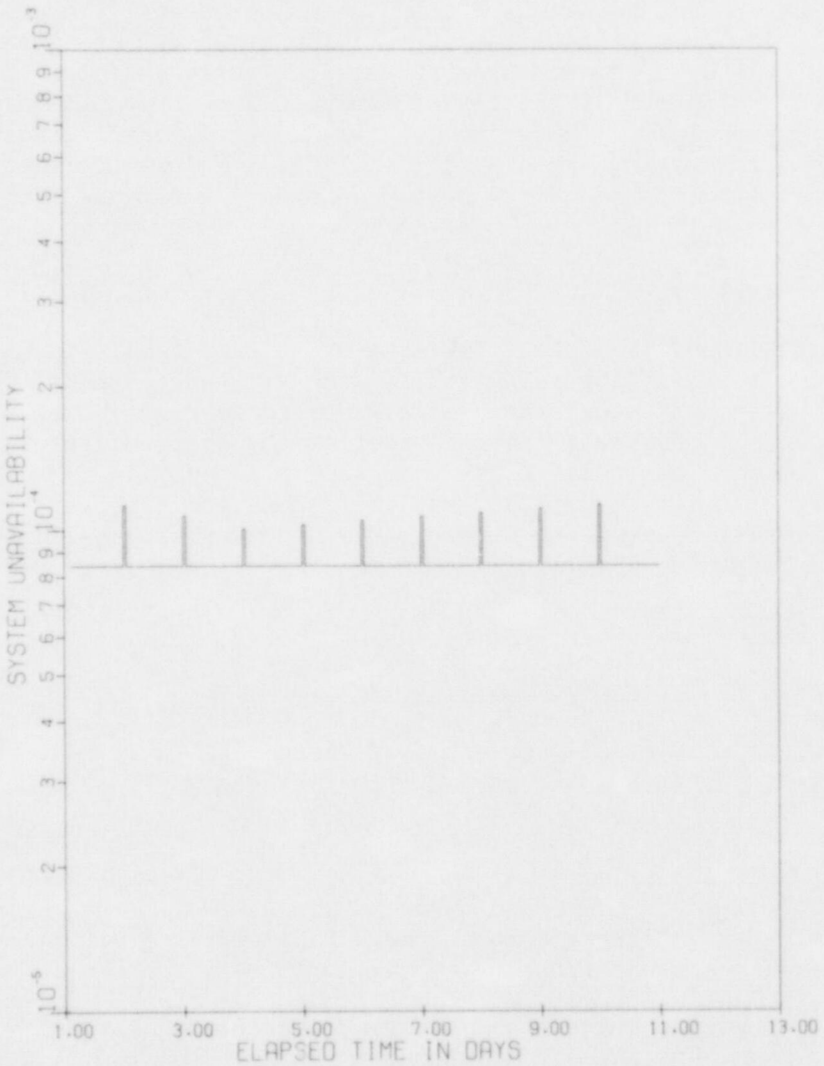


Figure 4.6. ADS unavailability (elapsed time from 1st to 11th day).

ability, q_0, for each test has been considered equal to 1. This means that the unavailability of each tested component during its test interval equals 1. The heights of the peaks on the unavailability curve depend on system configuration and accumulated hardware contribution between tests. The unavailability of a periodically tested component increases from 0 to $1 - \exp(-\lambda T_2)$ during the test interval T_2 (with the assumption of exponential failure distribution). This effect can be clearly seen on Figs. 4.7 and 4.8. Fig. 4.7 shows the unavailability of ADS when components from group II are tested; at that time components with a test interval of 180 days had been tested 13 to 26 days before. Fig. 4.8 shows the unavailability of the ADS again when components of group II are tested, while other components had been tested 163 to 176 days before. Their accumulated hardware contribution affects the height of the peaks. Repair contributions are insignificant compared to the other contributions, so it can hardly be seen after the test peaks.

4.3.1 Influence of the Unknown Shape of the Failure Distribution

As mentioned in Section 4.2, the elementary faults in the reduced fault trees are actually subsystem faults with an unknown shape to the failure distribution. As usual the base assumption for every subsystem was a constant hazard rate. To assess the influence of the shape of the failure distribution, two time dependent hazard rates were separately considered: $\lambda(t)$ increasing with time ($\beta = 1.5$) and $\lambda(t)$ decreasing with time ($\beta = 0.7$). These assumptions were used for each group, I to IV, separately, keeping other components fixed (see Table 4.2). In each case the scale parameter, λ, was fitted in such a way that the mean life time of a component was not changed, using the formula:

$$\lambda = \{\Gamma([\beta+1]/\beta)/T_F\}^{\beta}$$

The results of the influence of time dependence in the hazard rate of each group to the system average unavailability are given in Table 4.4.

TABLE 4.4

Influence of the Shape of the Failure Distribution

Group Number	Modified Parameter for the Group	ADS Mean Unavailability of Modified System (x10)	ADS Vulnerability V of Modified System
	$\beta = 0.7$	8.56	5.1
	$\beta = 1.5$	8.49	5.1
	$\beta = 0.7$	8.59	5.1
	$\beta = 1.5$	8.48	3.4
	$\beta = 0.7$	8.57	5.1
	$\beta = 1.5$	8.51	5.1
	$\beta = 0.7$	8.58	5.1
	$\beta = 1.5$	8.50	5.1

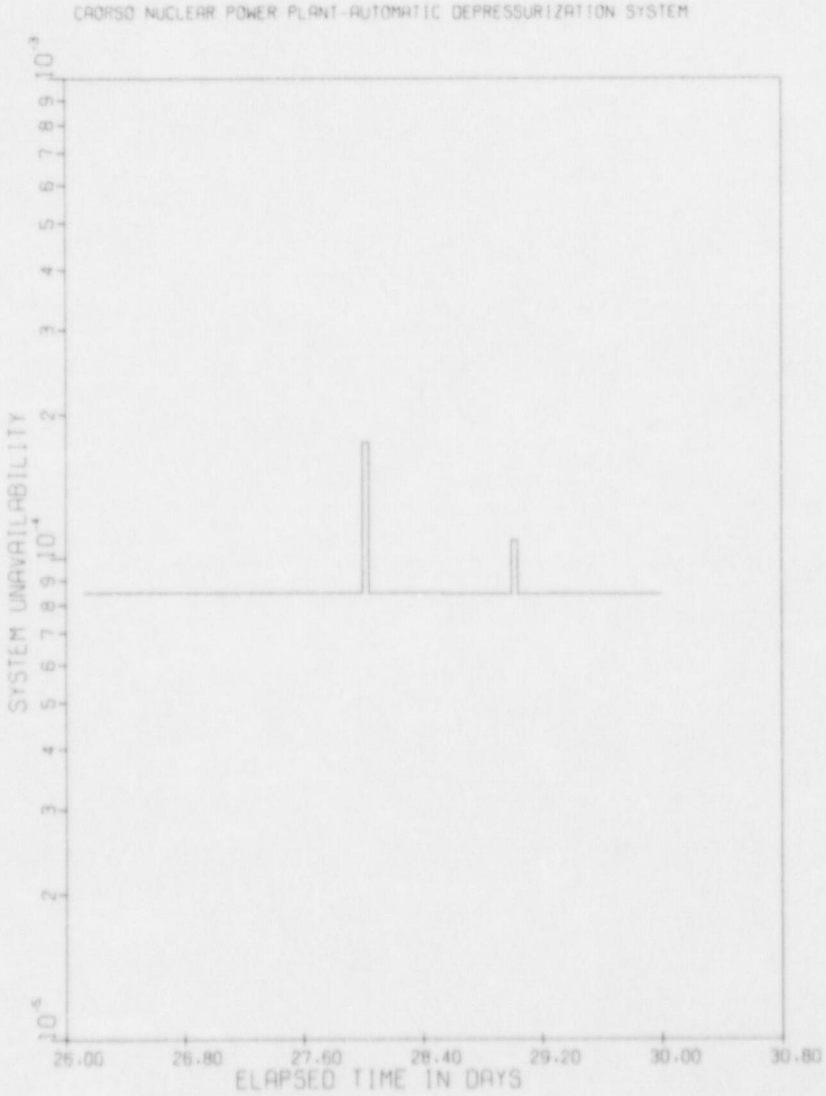


Figure 4.7. ADS unavailability (elapsed time from 26th to 31st day).

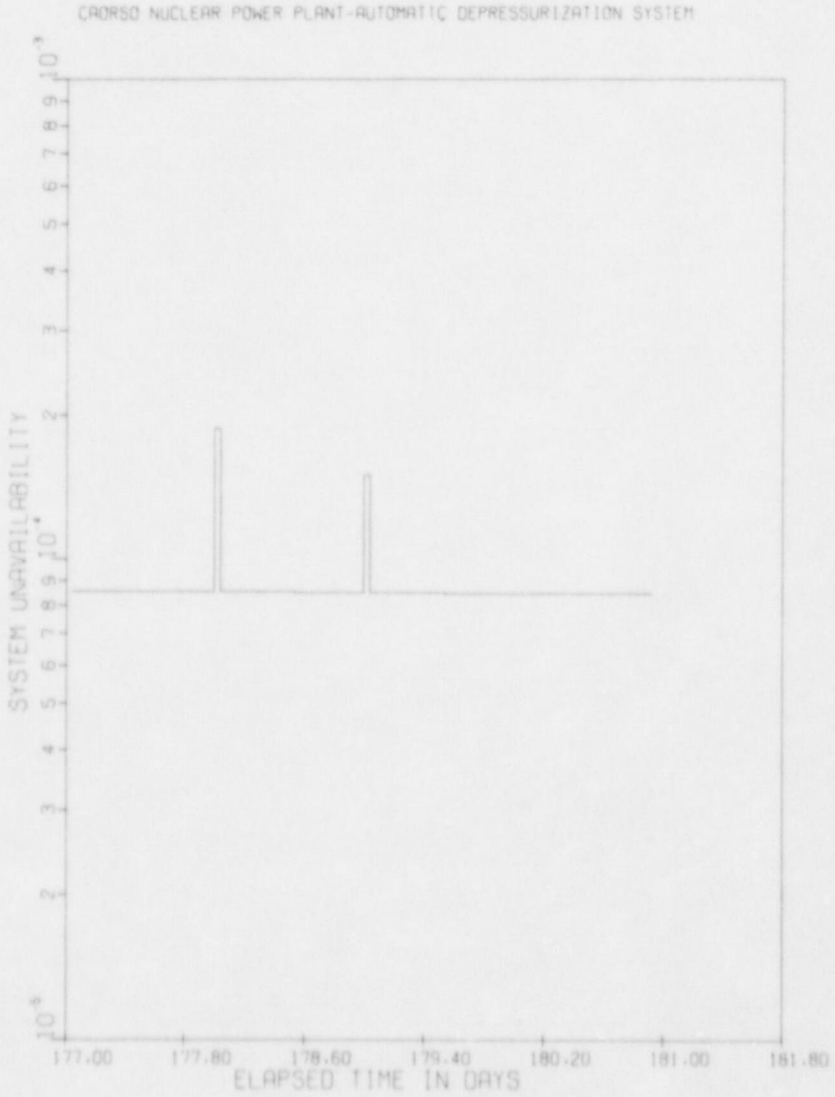


Figure 4.8. ADS unavailability (elapsed time from 177th to 181st day).

Clearly, the shape of failure distribution does not influence the mean unavailability in any significant way for this system. The constant unavailability components are dominant contributors to the ADS unavailability compared to periodically tested components. Note, that the right column contains values for the vulnerability, $V_{10^{-4}}$ (percentage of time with unavailability exceeding 10^{-4}). There is a slight change from 5.1^{-3} to 3.4^{-3} for the wear out case in group II.

4.4.2 Influence of the Error in Mean Life Time Estimates

Consider the influence of an order of magnitude change in the average life time estimates. The analysis is applied to each group of periodically tested components, again keeping $\beta = 1$ and increasing λ's by an order of magnitude. The results of this analysis are given in Table 4.5. For the original system $q = 8.51 \times 10^{-5}$, $V_{10^{-4}} = 5.1 \times 10^{-3}$.

TABLE 4.5

Error Propagation of Mean Life Time Estimates
With Respect to ADS Unavailability and Vulnerability

Group No.	Original λ $\times 10^{-6}$	Modified λ $\times 10^{-6}$	Mean Unavailability of Modified System $(\times 10^{-5})$	Vulnerability $V_{10^{-4}}$ of Modified System
I	3.1	31.0	8.52	5.1 x 10
II	5.5 & 7.0	55. & 70.	9.62	2.9 x 10
III	0.2	20.0	8.54	6.7 x 10
IV	0.1	10.0	8.60	5.1 x 10

There is clearly a significant change in both average unavailability and vulnerability when the hazard rate for the second group is increased. Changes in the hazard rate for other components are not as critical. Of course, when the hazard rate is increased 10 times for group II, the mean unavailability is 9.6×10^{-5} which is very close to 10^{-4}. Therefore, approximately 29% of its time the system is defined with an unavailability above 10^{-4}. Consider the optimum test interval, viz.,

$$T_2^* = 2\tau/\lambda$$

as derived in Reference 5 for the conditions: 100% test efficiency, p - o, and with no test override, q = 1, then increasing λ by an order of magnitude reflects a decrease in the test interval by about a factor of 3. Thus, in this case changing the optimal test interval from 30 days to 10 days brings the mean unavailability down from 9.62×10^{-5} to 9.0×10^{-5}. But more significant the vulnerability, $V_{10^{-4}}$, is changed by an order of magnitude. Therefore, with the optimal test interval, the system spends only 2.8% of its time with unavailabilities above 10^{-4} instead of 29%.

In conclusion, average unavailability and system vulnerability of the ADS are shown to be particularly sensitive to the value of λ in the group II components. The recommendation is, therefore, to concentrate the data collecting efforts such as the LER, NPRDS. and IPRDS systems on this group in order to improve the reliability estimates for the ADS.

Referring to Table 4.1, this preliminary analysis for the ADS indicates that error data assessment should emphasize failures related to relays and switches within logic trains A and B.

THE HIGH PRESSURE COOLANT INJECTION SYSTEM*

5.1 INTRODUCTION

The High Pressure Coolant Injection (HPCI) System in Pilgrim 1 will be considered for illustrating the practical application of FRANTIC II to quantitative evaluation of test policies. On the surface, the system is quite straightforward. Its major components are not redundant, so the primary contributors to its unavailability are rather obvious, single-component cut sets which account for failures to make transitions during initiation. However, the system contains many good examples of considerations that one must make in applying time dependent unavailability analysis to real systems. Currently, 21 separate procedures test various components and functions of the system. The resulting testing requirement is over 150 tests per year. Given the effort necessary to perform these tests, there is good reason to investigate the testing policy for the system from the point of view of unavailability.

This chapter considers only two subsystems of the HPCIS: the automatic initiation function and autoisolation function from the point of view of the optimal testing policy. Analysis of these two subsystems resulted in a number of recommendations regarding changes in existing test policies.

5.2 OVERALL CONFIGURATION

HPCI is a single leg, steam turbine-powered pump and associated piping designed to provide up to 4,250 gpm of water to the reactor vessel via feedwater line "B". It operates over a pressure range of approximately 150 to 1,000 psig. Steam produced by decay heat is used to drive the turbine. The steam is taken from the main steam supply line upstream of the main isolation valves. The water supply to the pump is provided by the Condensate Storage Tank (CST) or the Suppression Pool. The system is designed to operate independently of AC power with the exception of one (of two) autoisolation valves. A simplified diagram of the HPCI system is given in Figure 5.1.

In the event of a loss-of-coolant accident the HPCI system must accomplish one of two safety functions:

1) If the break has occurred elsewhere in the pressure boundary, the HPCI System must automatically deliver its rated output of water to the core upon demand.

2) If the break has occurred within the HPCI steam supply line, the system must automatically isolate the break from the reactor.

*This chapter follows the analyses performed by Dr. Andrew Dykes, under BNL contract, using a slightly modified version of the FRANTIC II code, named FRANTIC II-MIT[14], p. 186.

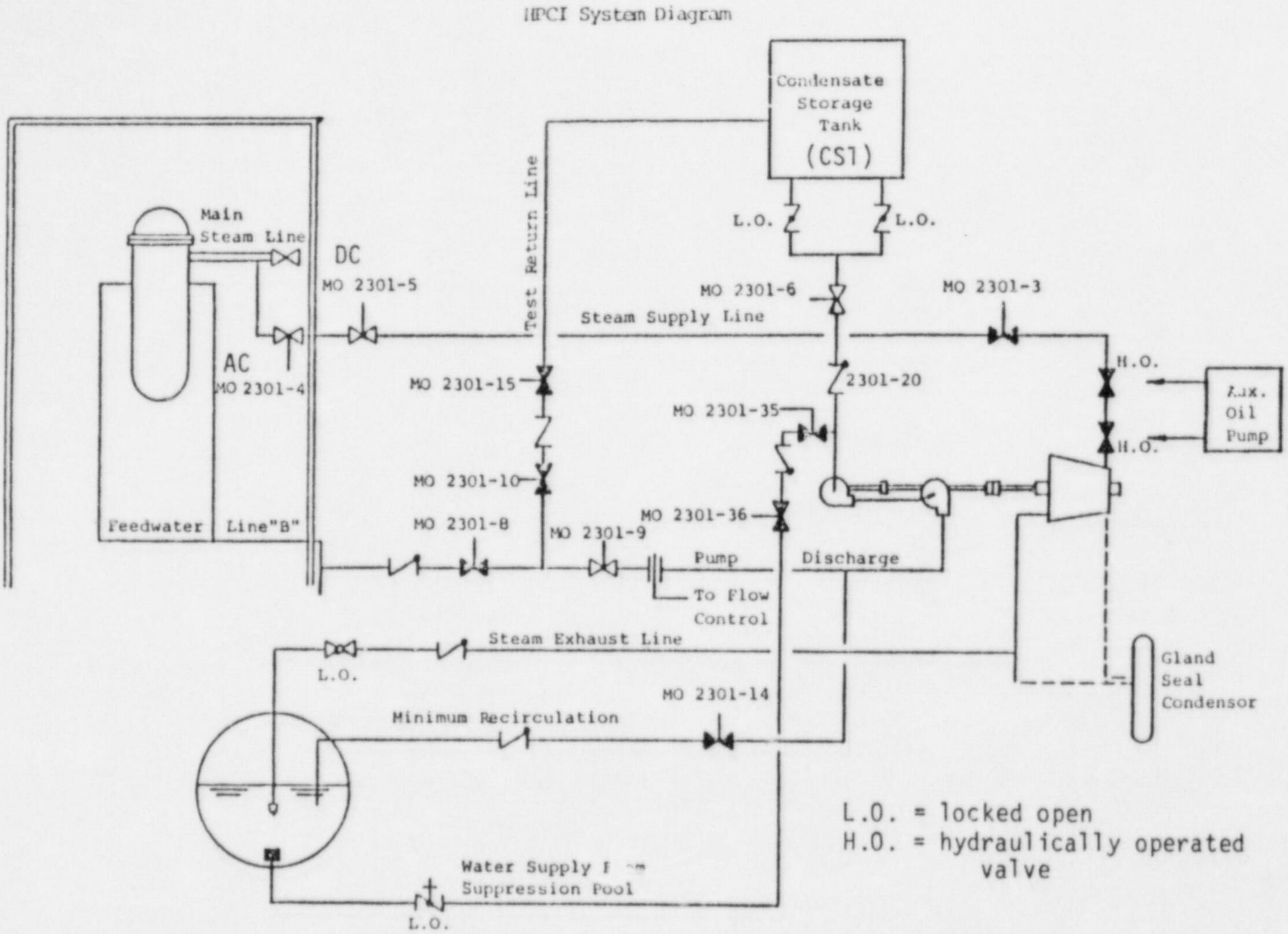


Figure 5.1. Simplified diagram of the High Pressure Coolant Injection System of a Boiling Water Reactor.

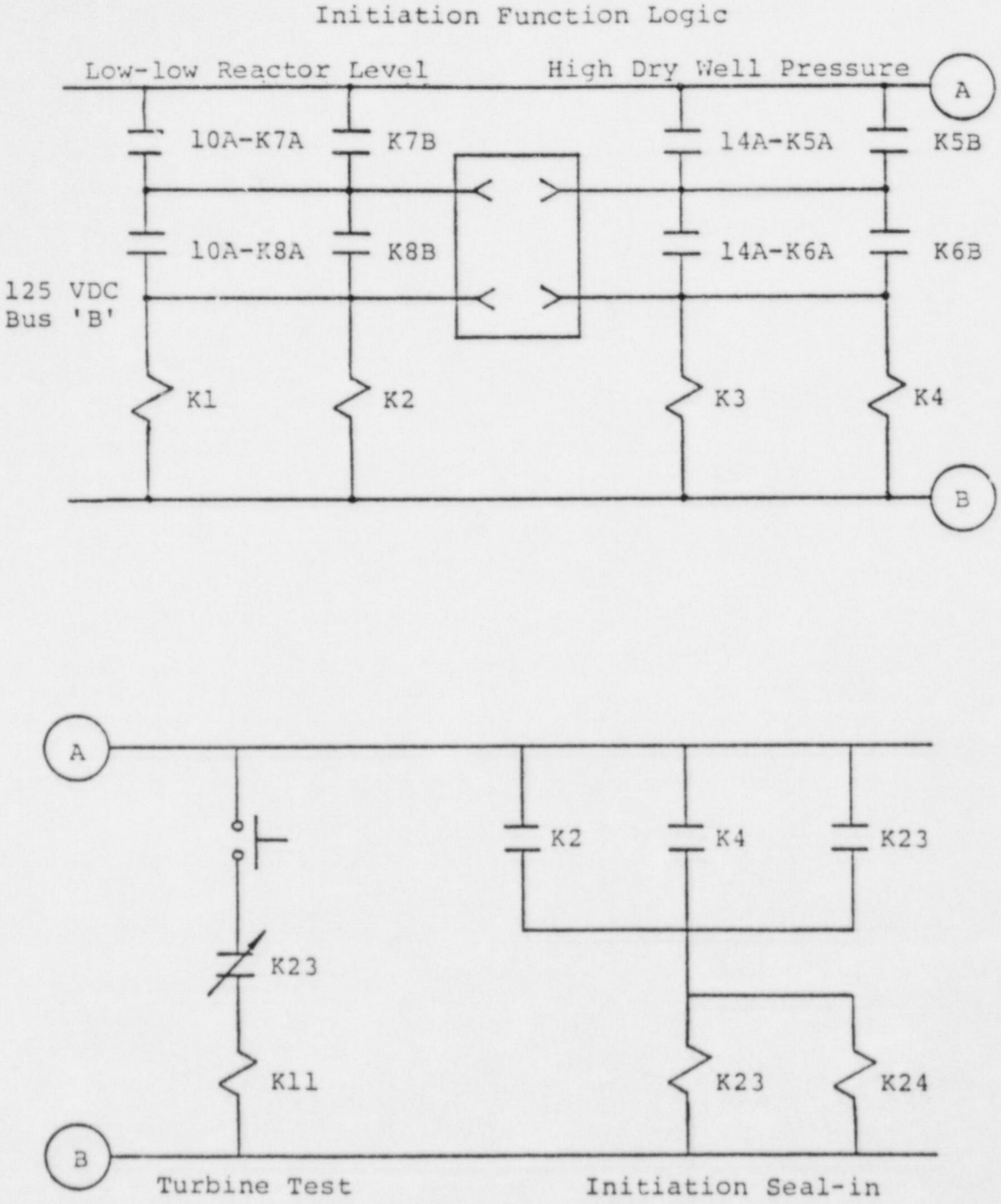


Figure 5.2. Simplified diagram of HPCIS initiation function components.

Component	Standby Condition	Signal To	Signal From
*Steam Supply Valve MO 2301-3	Closed	Open	K1,K3
*Injection Valve MO 2301-8	Closed	Open	K1,K3
*Auxillary Oil Pump	Off	On	K24
Minimum Recirculation Valve MO 2301-14	Closed	Open	K2,K4
CST Supply Valve MO 2301-6	Open	Open	K1,K3
Test Return Valve MO 2301-10	Closed	Close	K1,K3
Test Return Valve MO 2301-15	Closed	Close	K1,K4
Injection Valve MO 2301-9	Open	Open	K2,K4
*Seal-in Relay 23A-K23	Open	Close	K2,K23,K4
*Seal-in Relay 23A-K24	Open	Close	K2,K23,K4
Gland Seal Condensor	Off	On	K24
Turbine Test Override	Open	Open	K23
*Steam Isolation Valve MO 2301-4	Open	Open	K2,K3
*Steam Isolation Valve MO 2301-5	Open	Open	K1,K3
Seal-in Indicator on Operator Panel	Off	Lit	K24

Figure 5.3. Initiation logic signal flow. Starred components are those currently verified to receive an initiation signal.

In the manual or test mode the HCPI System is also used to provide cooling and/or controlled depressurization to the nuclear vessel in conjunction with the Automatic Depressurization System (ADS) during transients which isolate the primary containment. When decay heat generation has been reduced to about 2% of full power (at approximately 20 minutes after shutdown), the HPCI System can provide this function without the use of the ADS. Water discharged from the pump can be routed back to the Condensate Storage Tank, with the HPCI being used primarily as an energy sink for decay heat steam, or a controlled amount of makeup water can be provided to the reactor (via the feedwarter spargers) by splitting flow between the injection line and the test return line using MO 2301-10.

5.2.1 Automatic Initiation Function

Simplified diagrams of the HPCI automatic initiation function are given in Figs. 5.2 and 5.3. The automatic initiation function requires that 1) either the low-low reactor water level switches or the high dry-well pressure switches activate their associated logic relays, and 2) the logic relays activate the appropriate circuits in the HPCI's active components. Failure to accomplish automatic initiation is assumed to produce system failure.

The initiation logic consists of relays associated with either the low-low reactor water level switches or the high drywell pressure switches, an initiation signal seal-in relay, and a relay to activate the controller. Figs. 5.2 and 5.3 show the signal flow of these relays.

As the relay logic is currently designed, at least four relays must function for successful activation of the system. Relays 23A-K1 and 2 are redundant with 23A-K3 and 4 (designations are abbreviated on Figs. 5.2 and 5.3), provided that both the low-low reactor level and the high drywell pressure sensors are capable of detecting the LOCA. However, essential functions are also initiated by two nonredundant relays, 23A-K23 and K24.

5.2.2 Autoisolation and Termination

The HPCI injection function will be disabled for any one of the following reasons:

1) LOCA in the HPCI steam supply line,

2) low reactor vessel pressure,

3) turbine protection functions, or

4) high reactor vessel water level.

The first three result in isolation of the HPCI System from the reactor vessel, with the consequent disabling of the injection function. The fourth results from two of the sensors that generate the low-low reactor water level signal and indicates that the injection function is no longer required.

The HPCI System is automatically isolated from the reactor and the turbine is tripped if a break or leak is detected in the HPCI steam lines. The autoisolation signal is produced by any one of four different groups of sensors.

Each has independent sets of sensors powered by both 125 VDC buses A and B to provide redundancy with respect to power supply. An autoisolation signal can be produced by one of the following:

1) Temperature of 170°F in the torus room north west quadrant mezzanine behind rack 2257 in two-out-of-two temperature switches (one circuit on each bus).

2) Temperature of 170°F in the Reactor building, north side above the HPCI valve station in two-out-of-two temperature switches (one circuit on each bus).

3) Temperature of 190° to 200°F in the Turbine/Pump Room, west wall, elevation 31 ft. in two-out-of-two temperature switches (one circuit on each bus).

4) High differential pressure of at least 180 in. H_2O (corresponding to 300% rated flow) across a 90 degree turn in the HPCI steam supply line (one circuit on each bus). The autoisolation signal produced by any one of the above eight circuits will close the two steam supply isolation valves, trip the steam turbine, and inhibit both manual and automatic HPCI initiation until an operator manually resets the autoisolation "seal-in" on Panel 903 in the Control Room.

The eight leak-detection circuits are not as redundant as they appear to be. They are located in different areas and may not all be able to detect a leak that is occurring at one specific location. For this reason they complement rather than duplicate each other. In the fault tree for the autoisolation function, a conditional event is included which gives the probability that a given set of detectors can detect the leakage steam.

The system will also autoisolate if reactor vessel steam pressure falls below the level at which it will no longer be sufficient to turn the turbine. The logic consists of four pressure switches (set point at 77 psig) connected in a two-out-of-one logic configuration. This circuit does not "seal-in" the autoisolation signal. If vessel pressure subsequertly rises, the HPCI may be reinitiated without a manual reset.

A turbine trip without closure of the steam supply line isolation valves will occur when the following sensor switches are closed:

1) Low water pressure at pump suction (set point: 15 in. Hg, one-out-of-one logic).

2) High steam turbine exhaust pressure (set point: 150 psig, one-out-of-two logic).

No manual reset is required to enable the HPCI initiation circuit after a turbine trip due to turbine protection functions. The HPCI can be started either manually or by the reoccurrence of vessel low-low water level or high drywell pressure, provided the trip signal no longer exists.

HPCI System operation is terminated by a high water level signal (approx. 48 in. above the reference level) in both of the level switches used for this logic. The termination signal produces a turbine trip and a seal-in which must be manually reset before reinitiation is possible by any means other than a low-low reactor water signal.

5.3 FAULT TREE ANALYSIS

The assumptions used in the fault tree are as follows:

1) The fault trees are developed down to the level at which individual components are periodically tested.

2) Individual component failure rates include:

- Failures of wires from the respective power bus to the component.
- Failures in sensor conduits or taps into process lines which would prevent a sensor from being exposed to the environment being measured.

3) The following faults are not considered:

- No water in the CST.
- No water in the suppression pool.

4) Failures of relays include failures of wires from the activating relay contacts to the control circuits of the operating equipment.

5) Common cause failures which occur at the time of a true demand are accounted for using a separate failure event and are modeled with q_d. This assumption makes their probability of occurrence unaffected by a periodic testing policy. Common cause failures modeled by q_d in^lude

- Design errors
- Dependent failures
- Extreme environments for which the sensors are not qualified
- Human and calibration errors during sequential testing of redundant components. All sensors performing a given function are normally calibrated on the same month. Human error can result in a failure to recognize that the sensors are improperly calibrated when put back into service.

Common cause failures due to calibration may also be modeled by a standby failure rate. In fact, calibration drift is a candidate for a time- dependent hazard rate. Since all sensors of a given type are calibrated during the same month, they all drift from their setpoints for the same period of time. There is normally a range in which the sensor can respond without hindering the effectiveness of the system, so there is a period during which the sensors have little chance of being far enough from the setpoint to degrade system performance. As the time since last calibration increases, the probability increases that the next small drift will cross the tolerance limit. This failure behavior can be modeled with a generalized Weibull hazard rate with a shape factor greater than 2. The conditional failure rate in this case would increase as the time since the last calibration increases.

6) No credit is taken for a manual initiation of the injection function during a small LOCA. It is a constant per-demand probability and reduces the probability that the initiation function will fail. It should be noted that manual initiation of HPCI requires that the operator activate at least four separate components, and in a high-stress situation, the probability for error can be quite high. However, this is offset by the fact that the operator manually initiates the HPCI System for the monthly Turbine/Pump Operability Test. The reliability of manual initiation could be increased by allowing the operator to directly energize autoisolation relays with one switch. However, this can increase the probability of inadvertent HPCI initiation without a LOCA present.

Because there are two safety functions which the system must satisfy, two fault trees are necessary to describe the system's safety unavailability:

a. a fault tree describing in detail the failures which can prevent HPCI injection upon demand;

b. the autoisolation function fault tree.

5.4 QUANTITATIVE ANALYSIS OF AUTOMATIC INITIATION FUNCTION TESTS

To assess the periodic testing policy for the initiation function, the intermediate event, "Failure to Generate Automatic Initiation Signal at Active Components" of the Injection Function Fault Tree is made into the Top Event of an intermediate level fault tree (App. 4.) Cut sets which contribute to this Top Event will also contribute to the more general failure definition of the HPCI System.

Currently, five tests are accomplished on the initiation logic. Two monthly tests verify the functioning of the two types of initiation sensors, and require a quarterly calibration. Three tests check the initiation logic relays semiannually. Despite the very low unavailability obtained for the initiation sensor tests an increase in the test interval is not recommended. These sensors activate more than just the HPCI System. The level sensors also contribute to the activation of the Reactor Core Isolation Cooling System, Automatic Depressurization System, standby diesels, Low Pressure Coolant Injection System, and the Core Spray System. The pressure sensors also contribute to the activation of the Low Pressure Coolant Injection System and the Core Spray System. For this reason it is reasonable to continue testing them at the current 30-day interval (used by the utilities) to ensure that their unavailability remains very low.

There are currently three steps for testing the initiation logic:[14]

1) HPCI Initiation Logic Test;

2) HPCI Steam Supply Isolation Valve Logic;

3) HPCI Injection Valve Logic.

Each one is accomplished in approximately the same manner. First circuit breakers to most active components are opened. Then the low-low reactor water and high drywell pressure switches are closed in a sequence which tests their wiring logic and the activation of the required logic relays is verified. The procedures differ primarily in the components which are kept active during the test. The tests verify that only four of the eleven different components receive signals from the initiation logic and function in response to the signal, specifically: Auxiliary Oil Pump, MO 2301-4, MO 2301-5, and MO 2301-8 (these valves are verified to open on an initiation signal, given they are closed. The only time when they will be closed during normal operation is during testing of the autoisolation signal function). Before proceeding with a quantitative determination of recommended test intervals, T_2, two comments are in order:

1) The three initiation logic tests should be consolidated into one procedure which verifies that all components receive the necessary initiation signal. In most cases the signal path can be checked without requiring activation of the component itself. For example, in the circuit which opens MO 2301-3, the manual switch is parallel to the automatic initiation circuit contacts. Therefore, closure of the initiation contact should produce a short circuit across the manual switch. Activation of the valve by the manual switch would then, by inference, verify activation by the automatic initiation circuit.

2) Accomplishing the logic tests in conjunction with the initiation sensor tests will provide an integrated test of the entire logic train. If the logic tests are done during annual refueling, as recommended later in this section, the longer time required for the integrated test will not contribute to the system's unavailability.

Failure Event 5 (see Appendix 5) models system unavailability resulting from the initiation logic tests. It has been given a standby failure rate of 1.0E-6/hr to "switch on" the periodic test logic of the code. System downtime for injection logic testing is then modeled using q_o, τ, and T_2 (see pg. 13 for definitions) derived from analysis of the logic tests. Fig. 5.4 shows the contribution of Failure Event 5 to average system unavailability. [Although the data points were generated by the FRANTIC II-MIT code, they could easily be calculated using the idea of effective downtime (EDT). The resulting average unavailability would be $q_{av} = (q_o\tau)/T_R$.] An important consideration in the quantitative analysis is the fact that if the logic tests are done when the reactor is down for refueling and maintenance, they do not contribute to the system's unavailability.

To obtain a comparison with the current design and test policy, the first series of calculations assume that three different tests of the HPCI initiation logic will continue to be made, but with procedures so modified that proper transmission of the initiation signal to one-third of the active components will be verified by each test. (If the procedures are not changed, a

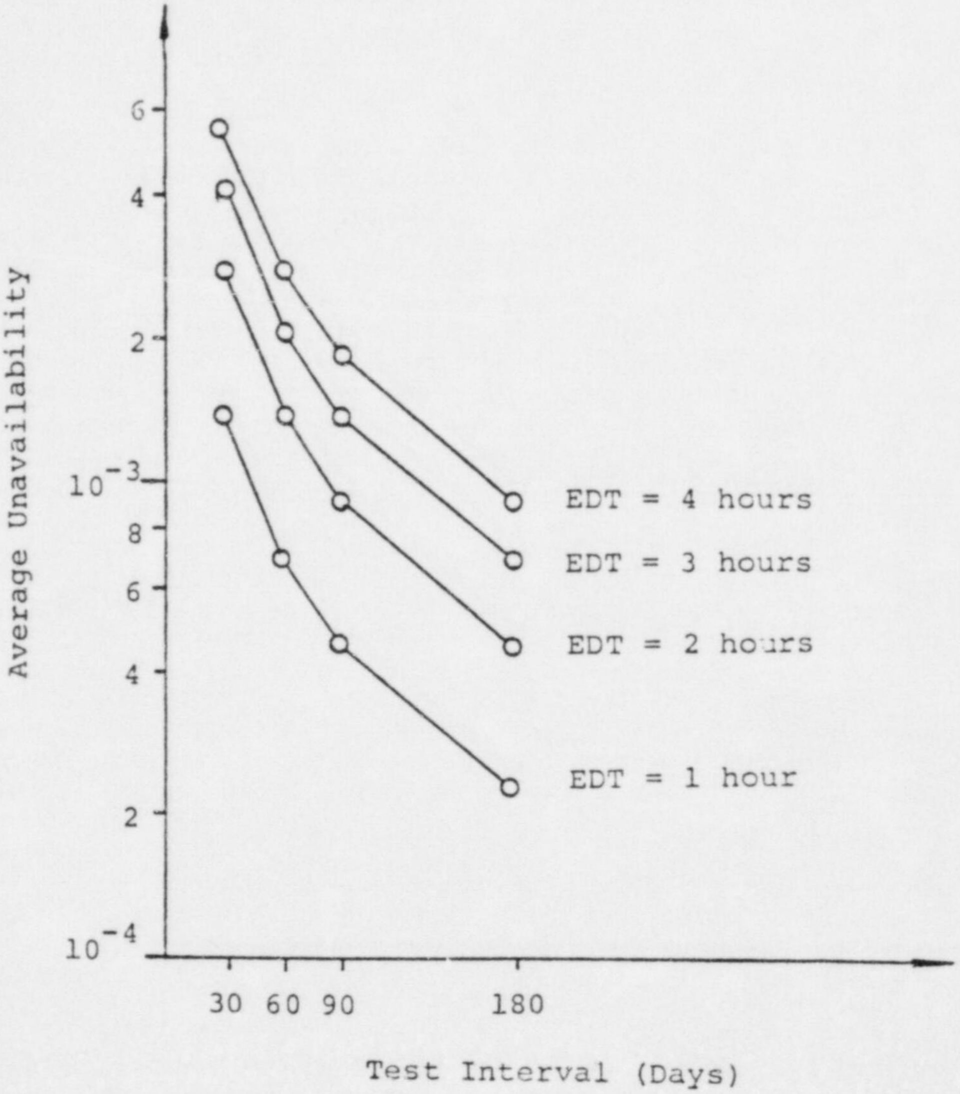


Figure 5.4. Average unavailability due to online testing of the initiation logic relays.

failure in the circuit from the initiation relays to one of the seven unverified components will remain undetected until a true demand; and the probability that such a failure has occurred will increase monotonically throughout the life of the plant. Since implementation of the procedural change is reasonable, the magnitude of the undetectable is not estimated.) With this policy, the automatic initiation of each active component will be tested every six months, which is the intent of the current policy.

The current logic tests result in the HPCI System being disabled for approximately one hour per test. During the test, circuit breakers to most of the active components are opened to prevent inadvertent injection into the reactor due to the test initiation signal, and it is conservatively estimated that there is a 0.5 probability that the system cannot be activated in the event of an actual demand. This yields an Effective Downtime (EDT) of 0.5 hours per test. For the initial calculation, it is assumed that an additional two or three components can be verified to activate without adding significantly to the EDT of an individual test.

Under the existing schedule, the three logic tests are all accomplished during the same month. With this schedule, the second and third tests have little opportunity to detect standby failures in the relays, since there is little time for them to occur. Consequently, a policy similar to that currently being used would result in the relays being tested once every six months with a test time of 3.0 hours and an unavailability to override the test, q_0= 0.5, yielding an EDT of 1.5 hours per logic relay test.

Fig. 5.5 shows the effect of staggering the three logic tests. When the three tests are staggered, the number of tests accomplished in a six-month period remains the same. However, since every test requires tripping the initiation relays, a staggering policy would result in their being tested at the staggered interval instead of once every six months. Also, since tests are no longer being made sequentially, the test duration for any given month decreases. The calculations are made for a variety of assumed failure rates which cover those expected for control relays. A 365-day calculation is also made. At this interval, testing is done when the reactor is down and EDT = 0. It can be seen in Fig. 5.5 that with the current design the staggered testing policy yields the lowest unavailability. Note also that testing more often (each test every three months, with a resultant staggering interval of 30 days) increases the average unavailability, because of the unavailability to override the test. A minor design change to the initiation logic relays was recommended in Ref. 14 and the effects of this modification on the unavailability of the initiation function were analyzed.

5.5 QUANTITATIVE ANALYSIS OF AUTOISOLATION FUNCTION TESTS

Currently two procedures are used to verify the steam line break sensor functions. These procedures are: HPCI Steam Line High Flow Isolation and HPCI Steam Line High Temperature. A third procedure, HPCI Steam Line Low Pressure, verifies the low-pressure sensor functions. All three of these procedures test the entire train of the autoisolation logic and cause both Steam Line Isolation Valves, MO 2301-4 and 5, to close. A fourth procedure, Autoisolation Logic, tests the autoisolation logic semiannually. This procedure is redundant with the three sensor tests and can be dropped without affecting the safety of the plant.

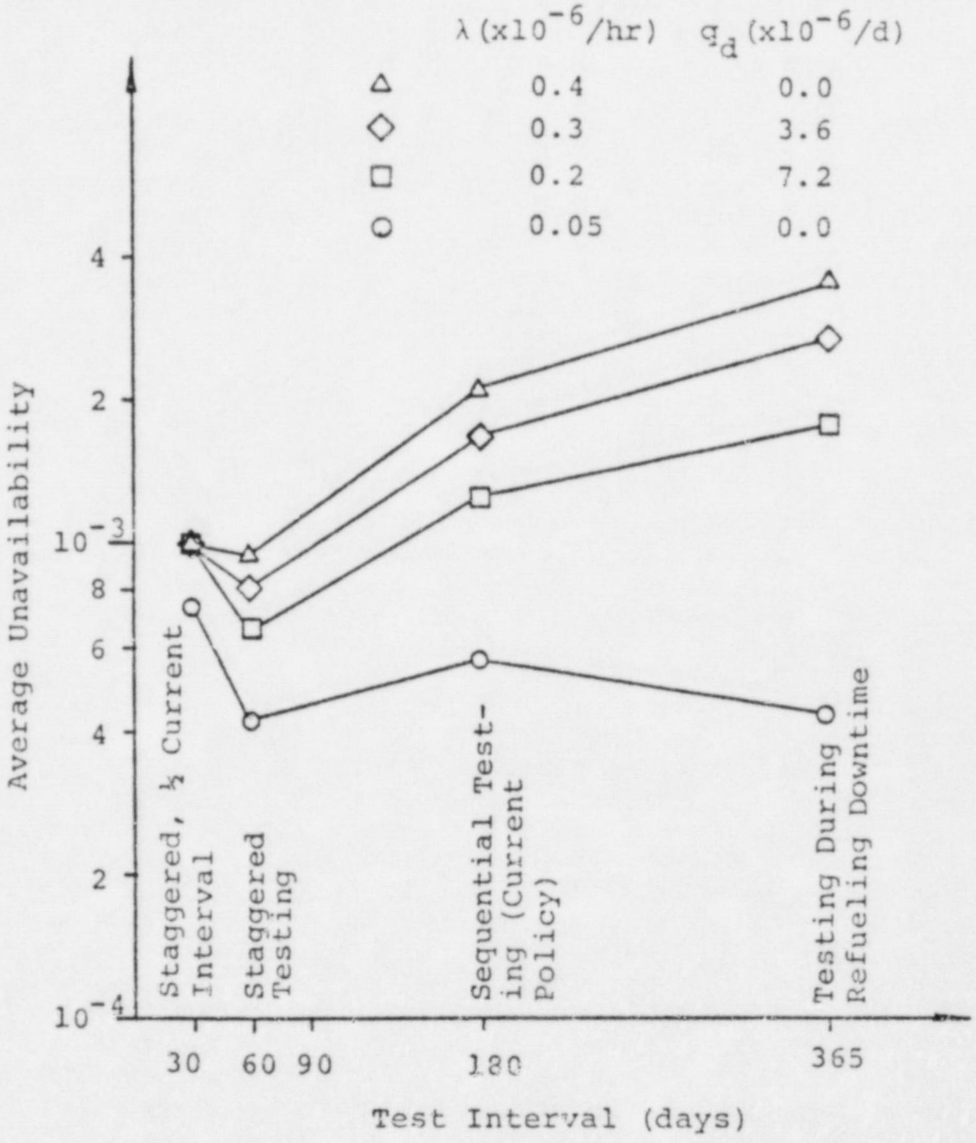


Figure 5.5. Unavailability of initiation logic relays with current design and current test procedures and staggering.

The procedures are described in Ref. 14 and some suggestions are made for improving their ability to check the functioning of all isolation circuits.

The quantitative analysis of the autoisolation function periodic tests is very strongly influenced by three important facts revealed by the fault tree analysis (App. 6) which are discussed in the following section:

1) The autoisolation function has a relatively large potential for common cause failures.

2) Aside from combinations of common cause failures, only two cut sets contribute significantly to the unavailability of the autoisolation function.

3) Autoisolation tests affect the unavailability of the injection function as well as the autoislation function. This influence is considered in Ref. 14

Because of the high degree of redundancy in this function, nine potential common cause failures are modeled in the fault tree. Three of them account for the necessity of locating the temperature sensors in three separate rooms to detect steam-line breaks. There is a probability that a sensor at one location cannot detect a break at one of the other locations in time to initiate the safety function. In this analysis we assume a probability of 0.01 that the temperature sensors cannot detect a steam-line break because of their location. One accounts for a break which is not large enough to trip the ΔP sensors. The others account for potential calibration errors or calibration drift.

A design which provides the necessary redundance and diversity of sensors to overcome a 1% chance of failure due to location reduces the importance of individual sensor failures. If one designs against a 1% chance that a break will occur where the sensor cannot detect a steam leak because of its location, one assumes a minimum unavailability for that sensor. That probability tends to dominate the probability that the sensor has failed during standby.

The fault tree analysis revealed no single component and only 12 two-component cut sets in the autoisolation fault tree. Of these, seven involve loss of power, which is monitored and consequently the unavailability is assumed quite low. An eighth pertains to the suppression pool, which is normally isolated during standby. The ninth and tenth contain a combination of common cause failures of all the temperature sensors plus and common cause failures of the ΔP sensors, which are judged to be primarily demand or human error in this function. The final two are the major contributors to the unavailability of the autoisolation function which are sensitive to test interval variations:

- Coincident failure of the two steam line isolation valves, and
- Coincident failure of the two autoisolation relays.

The testing intervals of the components in these cut sets will dominate the quantitative analysis of the periodic test policy for the autoisolation function.

The three autoisolation functional tests are currently accomplished monthly over a two-day period. Because the initial test signal produces closure of the two isolation valves, every sensor test checks the functioning of all four components in the two important cut sets. However, because of their quick succession, the second two tests are performed before standby failures have had an opportunity to occur. Therefore, although the valves and relays are cycled a total of three times during the month, their periodic test interval is still 30 days.

The lower curves on Figure 5.5 compare the current sequential testing policy with one in which the sensor tests are staggered. These curves give the unavailability of the autoisolation function versus the periodic test interval of the sensor tests. When the sensor tests are accomplished sequentially, the relays and valves are tested at the sensor testing interval. In the staggered tests the isolation relays and valves are tested at one third the interval shown. The staggered testing policy is superior to the sequential policy, because the relays and valves are tested at the staggering interval, while the less important cut sets are tested less often. The decreased test interval for these dominant components reduces the function's unavailability.

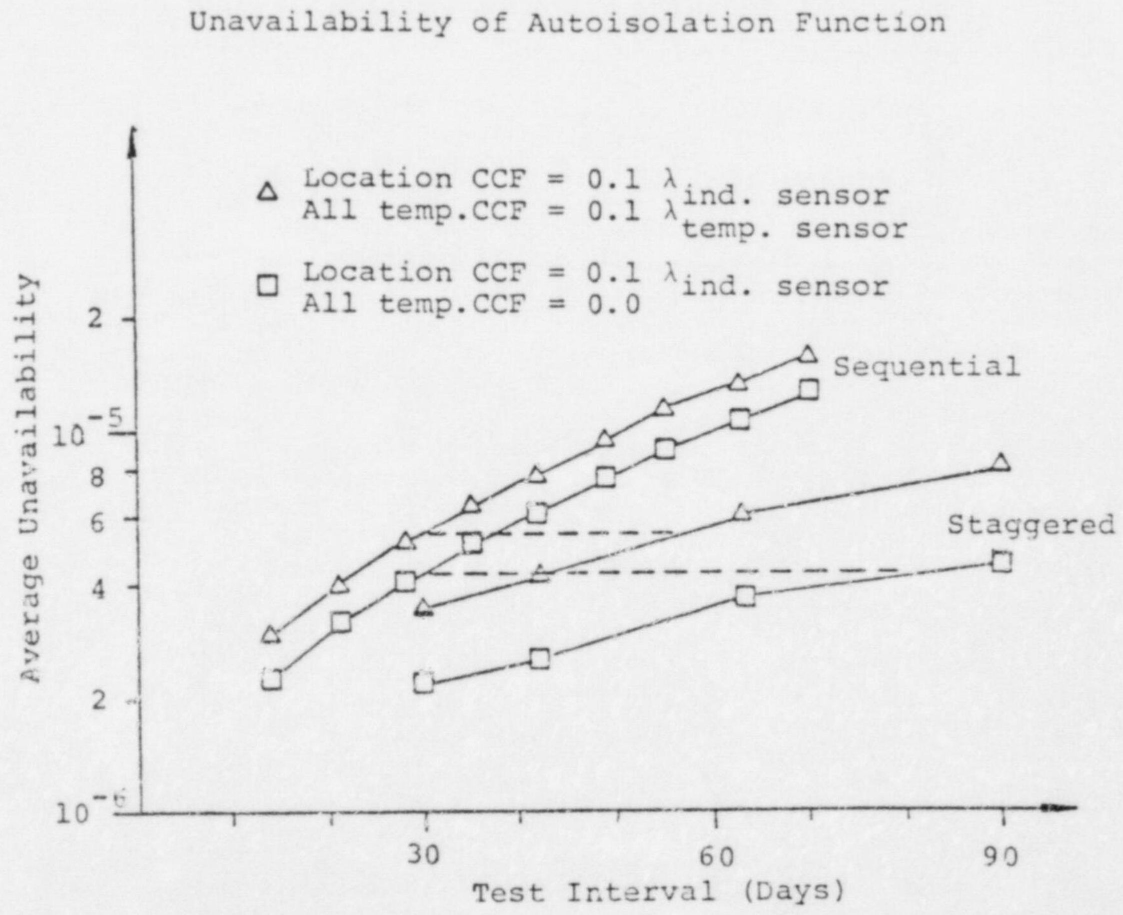


Figure 5.6. Autoisolation function unavailability as a function of autoisolation sensor test intervals.

The curves plotted with square data points are the result of assuming dependent failures of up to 10% among sensors at any one location. The curves plotted with the triangular data points also assume that all the temperature sensors can fail with a $\lambda_{CCF}= 0.1_{\lambda \mathrm{ind}}$. Because this assumption can defeat the designed redundancy of the temperature sensors, there is a larger percentage rise in the staggered testing unavailability than in the sequential testing. However, the clear advantage of sequential testing is still evident.

It can be seen in the figure that, if we assume no common cause initiator can fail all temperature sensors (the only plausible mechanism being calibration drift of all the sensors in one direction), the sensor tests can be accomplished once every nine weeks instead of at the current 30-day interval, with a reduction of 60% in the function's unavailability, because the 9-week sensor test interval translates into a 3-week test interval for the isolation relays and valves. Since an all-temperature sensor λ_{CCF} increases the relative importance of them with respect to the valves and relays, the unavailability of staggered testing at 9 weeks is about the same as the current policy for that assumption.

6. CONCLUSIONS AND RECOMMENDATIONS

A prime objective of this study has been to provide examples for the quantitative evaluation of the reliability of stand-by safety systems in nuclear power plants using an advanced time-dependent reliability technique. The quantitative evaluation of system reliability couples the fault tree framework, as the qualitative structure upon which to assess system reliabiity, with a quantitative evaluation of individual component reliability, as analyzed within the FRANTIC II code.

Three systems were analyzed: the Emergency Feedwater System (EFWS) of the Arkansas Nuclear One, Unit 1 Nuclear Power Plant (ANO-1)[11]; the Automatic Depressurization System (ADS) of the Caorso Nuclear Power Plant; and the High Pressure Coolant Injection (HPCI) system of the Pilgrim 1 facility. Through examples, this report has shown the feasibility of the FRANTIC II code applications for assessing the reliability of stand-by safety systems. Significant emphasis was placed on describing the input parameters in engineering terms, the data sources (or lack thereof) and the methodology for translating these data in the language familiar to FRANTIC.

For each of the systems, the following analyses were performed:

- o fault-tree quantification using both generic and, to the extent possible, plant-specific data including evaluation of all the input parameters;
- o calculation of the pointwise unavailability, average unavailability and system vulnerability* over a one-year period; and
- o sensitivity analysis on the average unavailabiity and vulnerability with respect to the uncertainties in the estimates of the component failure distributions and maintenance characteristics.

Analyses performed on the EFWS and the ADS have identified groups of components which have a more profound influence on the reliability of each system. For the EFWS these are, in order of importance: check valves, turbine-driven and motor-driven pumps. Whereas for the ADS, the more influential components are those associated with the actuation logic. Of course, as more emphasis is placed upon the collection of additional, requisite data for these more-important components, the evaluation of system reliability will improve commensurately.

Optimal test and maintenance strategies, as reflected by changes in HPCIS reliability, were also investigated using FRANTIC II. In this regard, specific recommendations to improve this system's current testing policies are outlined.

* System vulnerability has been introduced in this report to differentiate between two systems which have the same average unavailability but, due to different periods of high risk, one will exhibit a higher percentage of time spent above a preassigned level of system unavailability than the other.

In conclusion, this report has, by specific examples of real systems, attempted to show the utility and practicality of time-dependent unavailability models, such as FRANTIC, for addressing problems not readily reconcilable through the use of simpler, more restrictive time-independent models. More definitive assessments can be made once the sophistication of failure data achieves a level compatible with the failure-mechanism modeling capabilities inherent in FRANTIC. Even with the use of existing data bases, conclusions regarding standby system reliability, including the effects of different test and maintenance strategies, can be drawn.

Recommended areas for further study, therefore, include:

1. Determination of parameters deemed useful in identifying the relevant failure mechanisms;

2. Description and implementation of a reporting system to cull the needed data;

3. Investigation as to the effect of specific types of maintenance on component system reliability.

REFERENCES

1. W.E. Vesely and F.F. Goldberg, "FRANTIC - A Computer Code for Time Dependent Unavailability Analysis," NUREG-0193 (USNRC), October 1977.

2. W.E. Vesely, et al., "FRANTIC II - A Computer Code for Time-Dependent Unavailability Analysis," NUREG/CR-1924, BNL, July 1980.

3. J.T. Powers, "FRANTIC III - A Comouter Code for Time-Dependent Total System Unreliability Analysis," SAI, (unpublished), October 1981.

4. L.O. Hecht and J.R. Fragola, "Reliability Data Bases - A Review," PLPC-1977, IEEE, New York.

5. T. Ginzburg, J.M. Dickey, and R.E. Hall, "Sensitivity Study Using the FRANTIC Code for the Unavailability of a System to the Failure Characteristics of the Components and Operating Conditions," NUREG/CR-2542, BNL, February 1982.

6. "PRA Procedures Guide," NUREG/CR-2300, (2 vols.) Nuclear Regulatory Commission, January 1983.

7. D.R. Cox and H.D. Miller, The Theory of Stochastic Processes, John Willey and Sons, Inc., NY, 1965.

8. A.M. Freudenthal and M. Shinozuka, Wright Air Development Document TR 61-177, Aeronautical Systems Div., October 1961.

9. J.T. Fong, "Uncertainties in Fatigue Life Prediction and a Rational Definition of Safety Factors," Nuclear Engineering and Design 51 Vol. 51, pp. 45-54, North-Holland Publishing Company, 1978.

10. I. Bazovsky, "Chance and Wearout Failure Rates," Electronic Equipment Engineering, March 1960.

11. Emergency Feedwater System Ugrade Reliability Analysis for the Arkansas Nuclear One Nuclear Generating Station Unit No. 1, prepared by B&W Plant Performance Engineering, submtted to NRC by AP L in October 1981; herein called the AP L Report.

12. "Reactor Safety Study - An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants," WASH-1400, USNRC, NUREG-75/1014, October 1975.

13. I. Bazovsky, Reliability Theory and Practice, Prentice Hall, 1961.

14. A.T. Dykes, N.C. Rasmussen, W. Wesely, Jr., "Application of Time-Dependent Unavailability Analysis to Standby Safety Systems," Massachusetts Institute of Technology, MITNE-251, June 1982.

APPENDIX 1

APPLICATION OF THE FIRST PASSAGE TIME (FPT) DISTRIBUTION TO THE TIME DEPENDENT UNAVAILABILITY ANALYSIS

1. INTRODUCTION

A variety of distributions have been suggested as models describing the probability of failure as a function of a component's age. They include normal, lognormal, exponential, and Weibull distributions. The latter is the most widely applied in reliability theory since it can describe "burn-in" and "wear-out" processes as well as the period of normal operation. The Weibull distribution is a purely phenomenological model; it is not based on any particular underlying mechanism of failure. In its most general three-parameter form, it can approximate a wide class of distributions. This is the reason it was accepted as the standard distribution in a multiplicity of applications.

In this report, attention will be focused on another distribution which has not been widely used in reliability theory, despite its obvious advantages. This is the First Passage Time (FPT) distribution.[7] This distribution appears naturally from the consideration of the physical process underlying the failure event. This appendix discusses the application of the FPT distribution to help bridge the gap between information based on knowledge of physical mechanism of failure and parameter estimation needed for the time dependent unavailability analysis, (when statistical data on failure times are insufficient). To illustrate this potential, the properties of Weibull distributions (two and three parameters) and FPT distribution will be compared and an example of FPT distribution applied to the fatigue failure data will be given.

1.1 CHARACTERISTICS OF THE PROCESS

For any time t, where $t''_{n-1} \leq t < t'_n$, a local characteristic of the unit's reliability, the failure hazard rate, $\lambda_r(t)$, can be defined as follows:

$$\lambda_r(t) = \lambda(t_0 + t - t_r), \; t \geq t_r \geq t_0$$

where t_r is the time prior to t, that the unit's reliability characteristics were the same as at $t = t_0$, when the unit was first turned on;

$\lambda(t)$ is the hazard rate for a given failure distribution F(t), defined by

$$F(t) = 1 - \exp\left[-\int_0^t \lambda(u)du\right]$$

Now the product $\lambda_r(t)dt$ is simply the probability that the unit fails in the interval (t, t + dt), given that the unit has not failed in the interval (t_r, t).

The unit is considered to be "Good as New" at t_r, where $t_r \geq t_o$.

The failure hazard rate $\lambda_r(t)$ can be used to determine the reliability of the unit in the interval $(\bar{t}, t)$, where $t''_{n-1} \leq \bar{t} < t < t'_n$. Thus, the probability that the unit will not fail in the interval is given by

$$R_r\ (t, \bar{t}) = \exp\ [\ - \int_{\bar{t}}^{t} \lambda_r\ (u)du]$$

and conversely the probability that the unit will fail during $(\bar{t}, t)$ is:

$$F_r\ (t, \bar{t}) = 1 - R_r\ (t, \bar{t}) = 1 - \exp\ [\ - \int_{\bar{t}}^{t} \lambda\ (u)du]\ .$$

Introducing the quantities that described the total process characteristics, namely;

$P_k(t)$ which defines the probability that the unit is in state X_k at a given instant of time t, where $t \geq t_o$

then for the two-state unit (i.e. "safe" or "failed") considered here, where k = s or f, the following relation holds:

$$P_s(t) + P_f(t) = 1\ .$$

Note that $P_s(t)$ is also called the pointwise availability of the unit, while $P_f(t)$ is called the pointwise unavailability.

For different components classified for example as nonrepairable, monitored, periodically tested, the pointwise unavailability can be calculated from corresponding equations that require a variety of parameters, i.e., repair time, test period, test duration time, etc. The equations are different for each class of components, but a fundamental assumption for all models is the curve describing the failure distribution, F(t), or the hazard rate, $\lambda(t)$.

For a hazard rate, $\lambda(t)$, that is invarient with time and defined by the constant λ, where $\lambda > 0$, the failure distribution takes the form

$$F(t) = 1 - \exp\ [-\lambda t]$$

Another failure distribution other than the above exponential distribution is the so-called Weibull distribution. The two-parameter version is defined as

$$F(t) = 1 - \exp\ [-\lambda t^{\beta}]$$

where the hazard rate $\lambda(t) = \lambda\beta t^{\beta-1}$ with the parameters λ and $\beta > 0$.

It should be noted that in case of nonrepairable components the curve F(t) coincides with the curve $P_f(t)$ for all $t \geq 0$.

1.2 THE WEIBULL DISTRIBUTION

What are the ideal conditions under which the Weibull distribution should work. The well-known limit theorem says that the distributon of the minimum of n variables which are sampled from the same distribution independently tends to the Weibull form when $n \to \infty$. A close real-life example would be a string of light bulbs wired in series. A failure of the string is fully dependent on the worst bulb in a sequence. The string will stop functioning as soon as the weakest light burns out. Now when the number of lights in the strings is large, the Weibull distribution is expected to describe the reliability of a string of light bulbs. Therefore, the Weibull distribution can be expected to represent the safe/failed state of a component when the component is built from equally reliable elements, or when a multiplicity of failure causes are equally probable. There should not be any one dominant cause, otherwise the failure distribution of a component will follow the distribution of this dominant cause.

If one cause is predominant, a very different picture emerges in which the state of the component will be fully defined by the characteristics of this one cause. This "Leading Cause" phenomena tends to show up in systems having a particular part that wears out faster than the other component parts. Wearout is a natural phenomenon resulting from a gradual degradation of component strength by physical and chemical processes. Component wearout failures may very well be responsible for the majority of equipment failures.

Consider the example of incandescent lamps.[10] In most cases the cause of failure is intermixed wearout, chance, and even early failures. But wearout failures are heavily leading even if other failures occur occasionally. In this case, when one physical cause dominates all other causes, we cannot expect the Weibull distribution to work well and, as such, alternative distributions should be formulated.

One of the alternatives is the consideration of the dominant physical process itself which may be an operational wear of the surfaces, corrosion, fatigue due to vibration, etc. The First Passage Time Distribution would describe the failure distribution for components with a dominant failure cause.

1.3 THE FIRST PASSAGE TIME MODEL

Consider a parameter, x, that for example defines one of the physical properties of a component. Consider further that at some time, t_0, $x = x_0$ and, on the average, x is either monotonically increasing with time (or monotonically decreasing with time, t). The trajectory of x(t) is a random process (Fig. 1). However, as soon as x(t) crosses some critical level, the component fails. So x(t) represents the "leading cause of failure," physical parameter as a function of time with a given threshold at $x = x_c$.

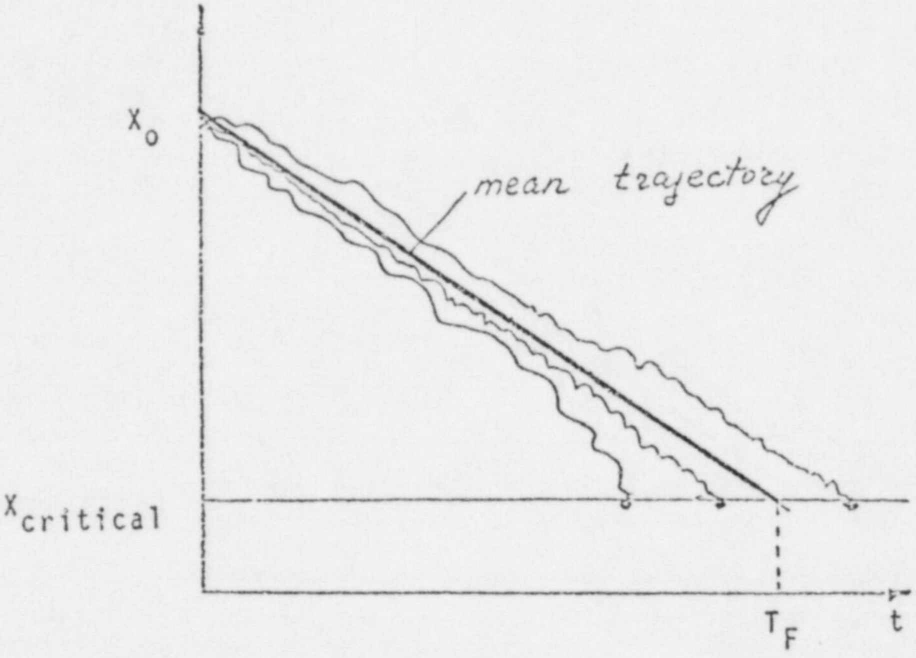


Figure 1. x(t) a random process which represents the "leading cause of tailure" physical parameter as a function of time.

The following equation describes the model:

$$x(t) = r + \sigma\varepsilon(t)$$

$$x(o) = x_o$$

where

r is the trend parameter (the mean rate of change of x (t) which for this example a constant negative trend, $r < 0$ is assumed)

$\varepsilon(t)$ is the standard normal white noise:

a) $M[\varepsilon(t)] = 0$, $M[(\varepsilon(t))^2] = 1$;

b) at each time moment t $\dot{x}(t)$ is normally distributed;

c) the value of $\dot{x}(t_1)$ is independent of the value of $\dot{x}(t_2)$ for every t_1 and t_2: $\mathrm{cov}(\varepsilon(t_1), \varepsilon(t_2)) = 0$ for every t_1, t_2.

σ is the standard deviation of the noise.

x_o is the initial level of x.

x_c is the critical level of x, $(x_c < x_o)$.

Define $G(x_o, x_c, t)$ to be the probability of crossing the critical level x_c at least once beginning with x_o within the interval (0, t).

The distribution of the first passage time for a given threshold is given by (see Reference 7):

$$G(x_o, x_c, t) = \tfrac{1}{2}\left\{1\text{-Erf}\,[(-\alpha+\gamma t)/\sqrt{2t}] + \exp(-2\alpha\gamma)\,[1\text{-Erf}(-\alpha-\gamma t)/\sqrt{2t}]\right\}$$

where $\mathrm{Erf}(z) = 2/\sqrt{\pi} \displaystyle\int_0^z \exp(-u^2)\ du$,

$$\alpha = |x_c - x_o|/\sigma \ ,$$

$$= r/\sigma < o \ .$$

The p.d.f or the time derivative of $G(x_o, x_c, t)$ is given by

$$g(x_o, x_c, t) = dG/dt = \alpha/\sqrt{2\pi}\ t^{3/2} \exp\left[-(\alpha+\gamma t)^2/(2t)\right]$$

One can show that the mean life time, T_f, is simply

$$T_f = \int_0^\infty t g(x_o, x_c, t)\ dt = -\ \alpha/\gamma\ > 0$$

or

$$T_f = |x_o\ x_c|/|r|$$

yielding

$$g(x_o, x_c, t) = -\gamma T_f \exp\left[-\gamma^2(t-T_f)^2/(2t)\right]/(\sqrt{2\pi}t^{3/2})$$

If $\sigma \to 0$ in the FPT model, i.e., if the process tends to be nonrandom, then $g(x_0, x_c, t)$ tends to a δ-function at $t = T_f$:

$$g(x_0, x_c, t) \Big|_{\sigma \to 0} \to \delta\,(t-T_f).$$

In other words with the deterministic wear the component takes exactly

$$T_f = |x_0 - x_c| / |r|$$

to live and it dies exactly at T_f. The bigger the σ, more spread is in the failure distribution.

Physically the curve has four parameters: initial value, critical value, rate of wear and its variability. Mathematically, there are only two: T_f, γ. If real physical parameters are not known to describe a specific component, a curve fit to the data using the best two parameters can be used.

The failure densities, generated respectively by a Weibull distribution and by the FPT theory are depicted in Fig. 2 (see Appendix A for the derivation of this comparison).

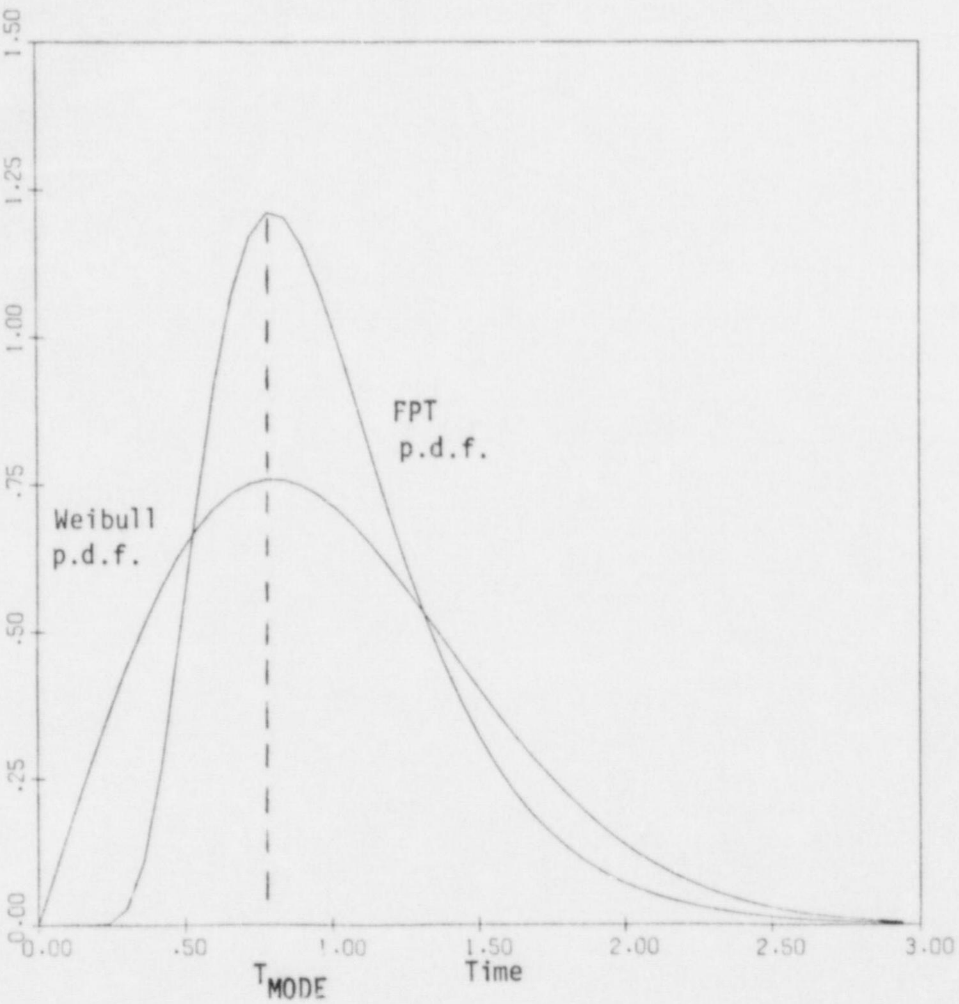
Each of these curves are constrained by two conditions: 1) mean time to failure for both theories are the same, and 2) most probable times of failure modes are also the same. Since the FPT distribution has two parameters, these two conditions fix both curves as long as β in the Weibull distribution is fixed. The FPT theory depicts in Fig. 2 more concentrated failures around the mean than the Weibull distribution, growing more slowly at the beginning and decaying faster at the end.

Fig. 3 shows the corresponding unavailability, $q(t)$ relationship. For the times up to about 40% of the mean life span, the FPT theory predicts unavailabilities that are much smaller than the Weibull distribution.

In Fig. 4 the hazard rate, $\lambda(t)$, is plotted for both theories. Clearly, the FPT theory has much lower rates for short times but exceeds the Weibull rate before the mean failure time. In some cases this theory may approximate the "bathtub" curve better than Weibull. It covers two parts of the curve, "normal operation" and "wear out" regimes. One can also model the "burn in" and "normal" regimes together by this theory.

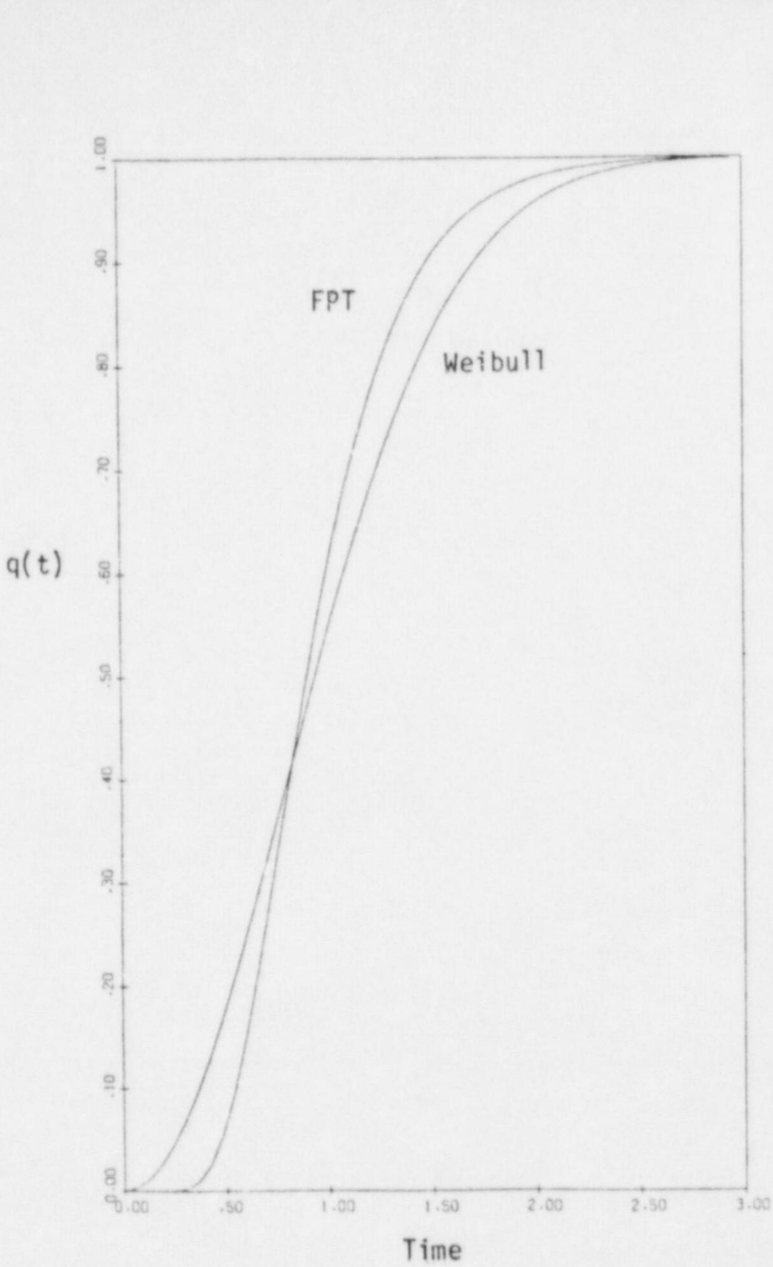
If the condition that the modes should coincide is relaxed, a better fit between the Weibull and FPT theories can be reached. However, for approximately the first 30% of the mean lifetime, the Weibull distribution will always overestimate the unavailability as compared to the FPT theory. In other words, in a short time the random process which begins at x_0 has very little chance to reach x_c. However, after a while, due to the trend shown in Fig. 1, the chance of reaching x_c, and therefore failure for the FPT theory, is even higher than for the Weibull theory.

Around the mean life time, both models can approximate each other with the suitable choice of parameters. For $t < 30\%\ T_f$ the Weibull failure distribution cannot adequately approximate the FPT distribution and only detailed data analysis can answer the question as to which of the two models would better represent component wear and life time.



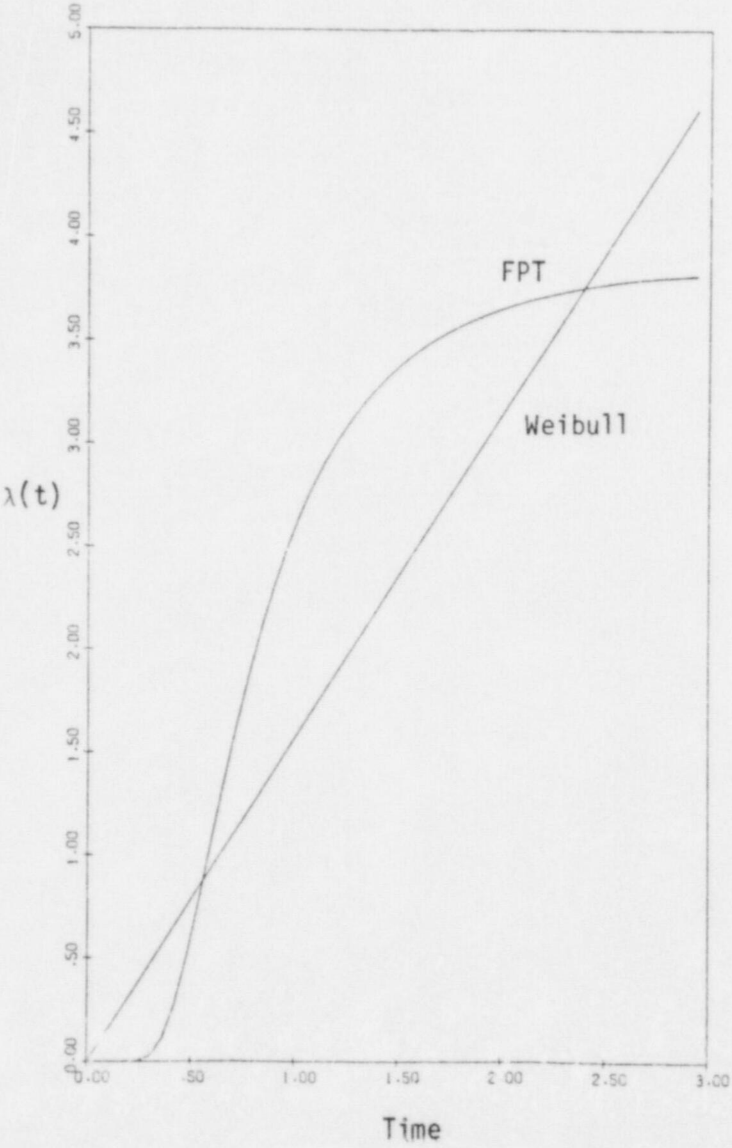
a. Mean times to failure are equal.
b. Most probable times of the first failure are equal (modes).
c. $\beta = 2$.

Figure 2. Comparison of the p.d.f.'s based on the first passage time (FPT) and Weibull distributions.



a. Mean times to failure are equal.
b. Most probable times of the first failure are equal (modes).
c. $\beta = 2$.

Figure 3. Comparison of unavailability q(t) based on first passage time (FPT) and Weibull distributions.



a. Mean times to failure are equal.
b. Most probable times of the first failure are equal (modes).
c. $\beta = 2$

Figure 4. Comparison of hazard rates $\lambda(t)$ based on the first passage time (FPT) and Weibull distributions.

The more general three-parameter Weibull distribution allows for the initial period ($t<\varepsilon$) with no failures after which the failure rate follows the same curve. It corresponds to the hazard rate

$$\lambda(t) = \begin{cases} 0, & t < \varepsilon \\ \lambda\beta(t-\varepsilon)^{\beta-1}, & t \geq \varepsilon \end{cases}$$

The class of distributions approximated by this assumption is much wider. The third parameter allows a better approximation of the FPT distribution (see Appendix B) than the two-parameter Weibull distribution.

1.4 EXAMPLE

The following ordered data set consists of fatigue life data for 100 specimens of 6061-T6 aluminum at maximum stress of 31000 psi, Freudenthal Shinozuka[8]

70	90	96	97	99	100	103	104	104	105
107	108	108	108	109	109	112	112	113	114
114	114	116	119	120	120	120	121	121	123
124	124	124	124	124	128	128	129	129	130
130	130	131	131	131	131	131	132	132	132
133	134	134	134	134	134	136	136	137	138
138	138	139	139	141	141	142	142	142	142
142	142	144	144	145	146	148	148	149	151
151	152	155	156	157	157	157	157	158	159
162	163	163	164	166	166	168	170	174	196

This set represents the failure time for each specimen measured in thousands of cycles. The mean life time of a specimen is 132.95 and the standard deviation is 21.03. The three parameter Weibull distribution with $\varepsilon = 64.3$ and $\beta = 3.648$ fits the data reasonably well[9], but so does the FPT distribution with $\alpha = 7.5$ (Fig. 5). Note that the Weibull fit was obtained using three parameters. One cannot fit this data set by the two parameter Weibull because of the long period of no failure at the beginning. The FPT distribution has only two parameters and is, therefore, a superior model for this particular experiment. The reason lies in the physical process underlying the failure event. In this particular case, we are dealing with a clear "leading cause" phenomena - fatigue, when cracks grow under cyclic loading and eventually reach a critical size and sudden fracture occurs. This example illustrates the idea of the application of the FPT distribution in cases when the wearing out leading cause of failure dominates other causes.

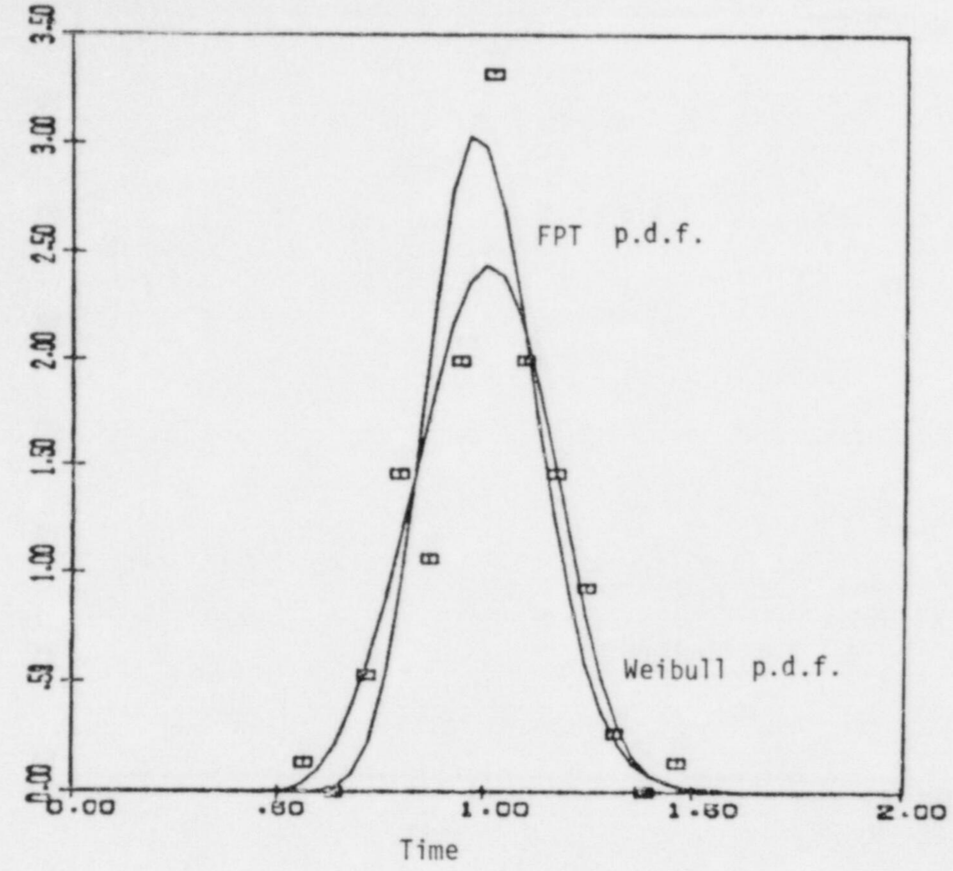


Figure 5. Weibull and FPT fits for sample of 100 fatigue life data specimens for 6061-T6 aluminum.[8]

2. SUMMARY

This work indicates that the FPT distribution may become a necessary complement of existing quantitative time-dependent unavailability analyses. This distribution has two parameters vs. three in the generalized Weibull. However, these parameters reflect the physical mechanism of failure and when data are not sufficient, engineering judgement can be used to estimate one of these parameters.

An important feature of this approach is this use of engineering judgement for estimation of the unknown key parameters λ and β of the Weibull distribution. The idea is that one seeks the parameters which have physical meaning, e.g., initial value, critical value, rate of wear and its variability. From these, the FPT distribution can be generated and then fitted by the best Weibull distribution, thereby identifying the unknown ε, λ and β. From a sensitivity study one can ascertain the error in the unavailability estimates produced by the error in the Weibull parameters. Combining this knowledge with the detailed engineering analysis of the process results in realistical appraisal of reliability in cases where data are minimal.

APPENDIX A

COMPARISON OF THE TWO-PARAMETER WEIBULL AND FPT DISTRIBUTIONS

To compare these distributions first the mean life time of a component, T_f, will be set to 1 for both. In other words, time will be measured in units of the mean life time. For the Weibull distribution, it means that a relationship between the scale parameter, λ, and the shape parameter, β, is:

$$\lambda = [\Gamma[(\beta+1)/\beta])]^{\beta} \tag{A.1}$$

For the FPT distribution, setting $T_f = 1$ means that

$$\gamma = -\alpha \; . \tag{A.2}$$

Now there is one free parameter in both distributions and one can require, for instance, that the modal values for both distributions are equal. The expressions for the modal values, t_m, can be obtained by setting the derivative of the probability density function to zero.

For the two-parameter Weibull distribution, one can have

$$f(t) = \lambda t^{\beta-1} e^{-\lambda t^{\beta}} \; .$$

Setting up the derivative f'(t) = 0, after simple algebraic transformations, one can obtain

$$t^{\beta}{}_m = (\beta-1)/(\lambda\beta)$$

and, finally,

$$t_m = ((\beta-1)/(\lambda\beta))^{1/\beta} \; . \tag{A.3}$$

Here λ and β are constrained by the relationship (A.1).

For the FPT distribution, one can have

$$g(t) = \alpha/(\sqrt{2\pi}\; t^{3/2}) \exp\left\{-(\alpha+\gamma t)^2/(2t)\right\}$$

Setting up the derivative g'(t) = 0, omitting trivial calculations, one can obtain

$$-3t_m - \gamma^2 t^2{}_m + \alpha^2 = 0.$$

Taking into account the constraint (A.2), one can express α as a function of t

$$\alpha^2 = 3t_m/(1-t^2{}_m)$$

or, finally,

$$\alpha = \sqrt{3t_m/(1-t^2{}_m)} \tag{A.4}$$

The formula makes sense clearly only when $t_m < 1$, i.e., the modal value is less than the mean value. In other words, the most probable failure time should be less than the average failure time. For the Weibull distribution, this can be shown to occur [from (A.1) and (A.3)] only when $\beta < 3.3$ and $\lambda > 0.7$. For the greater values of β, we cannot keep the models of two distributions coinciding.

Another way of comparing two distributions would be to equalize their means and variances. The variance of the FPT distribution is given by the simple formula:

$$\mathrm{Var}_{FPT} = \int_0^\infty (t-T_f)^2 g)X_o,\ X_c,\ t)dt = \sigma^2 |X_o-X_c|/|r|^3$$

or in terms of above notations

$$\mathrm{Var}_{FPT} = \alpha/|\gamma^3| \quad .$$

Taking into account the condition (A.2), we have

$$\mathrm{Var}_{FPT} = 1/\gamma^2 \quad . \tag{A.5}$$

At the same time, variance for the Weibull distribution is

$$\mathrm{Var}_W = [\Gamma(1+2/\beta) - (\Gamma(1+1/\beta))^2] \;/\; \lambda^{2/\beta} \tag{A.6}$$

Setting up $\mathrm{Var}_{FPT} = \mathrm{Var}_W$ we can calculate the value of and compare two distributions on the basis of their means and variances.

The calculations above give the basis for comparison of two distributions. One starts with the arbitrary β, then finds λ from (A.1), generates t_m value from (A.3), and α from (A.4). The distributions obtained in this way will have equal means ($T_f = 1$) and equal modes ($t_m < 1$). The other way is to use formula (A.6) and (A.5) and obtain equal means and variances.

APPENDIX B

COMPARISON OF THE THREE-PARAMETER WEIBULL AND FPT DISTRIBUTION

For the more general case,

$$f(t) = \begin{cases} o, & t < \varepsilon \\ \lambda(t-\varepsilon)^{\beta-1} e^{-\lambda(t-\varepsilon)^{\beta}} & , t \geq \varepsilon \end{cases}$$

To keep the same units of time measurement, $T_f = 1$, one can set

$$\lambda = [\Gamma((\beta+1)/\beta)/(1-\varepsilon)]^{\beta}$$

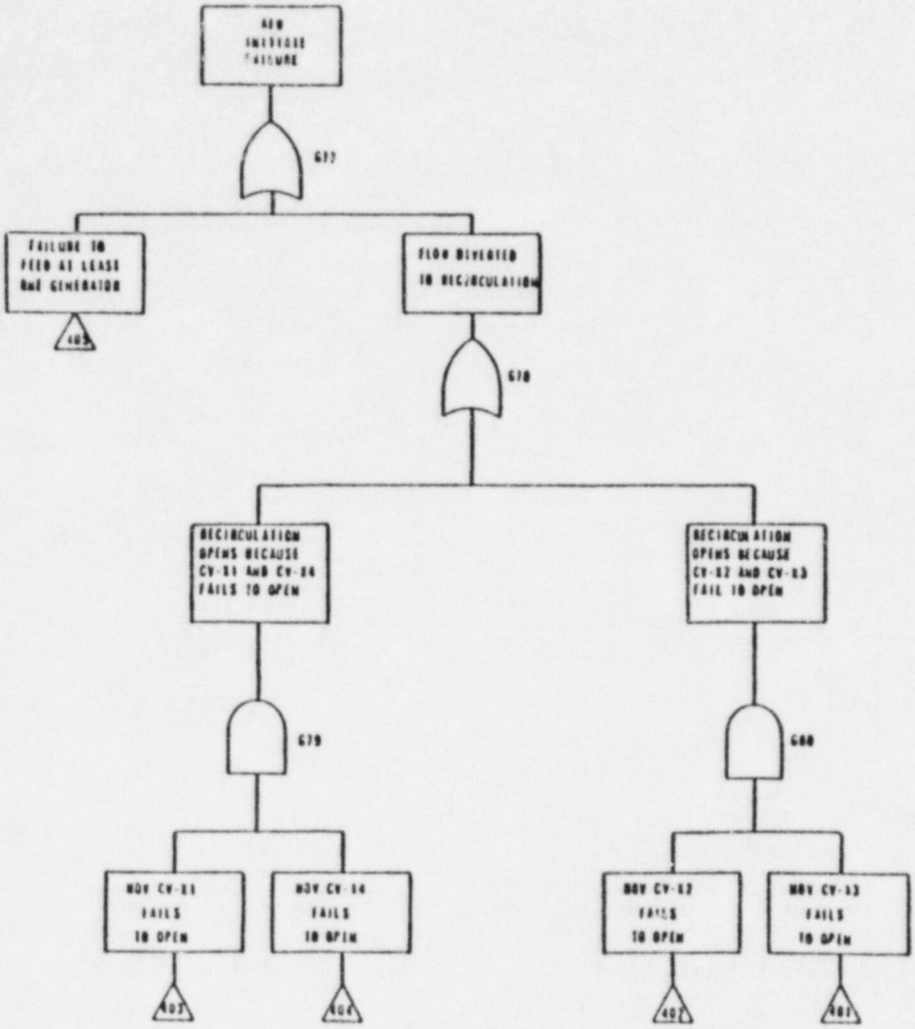
and shift the t_m value as

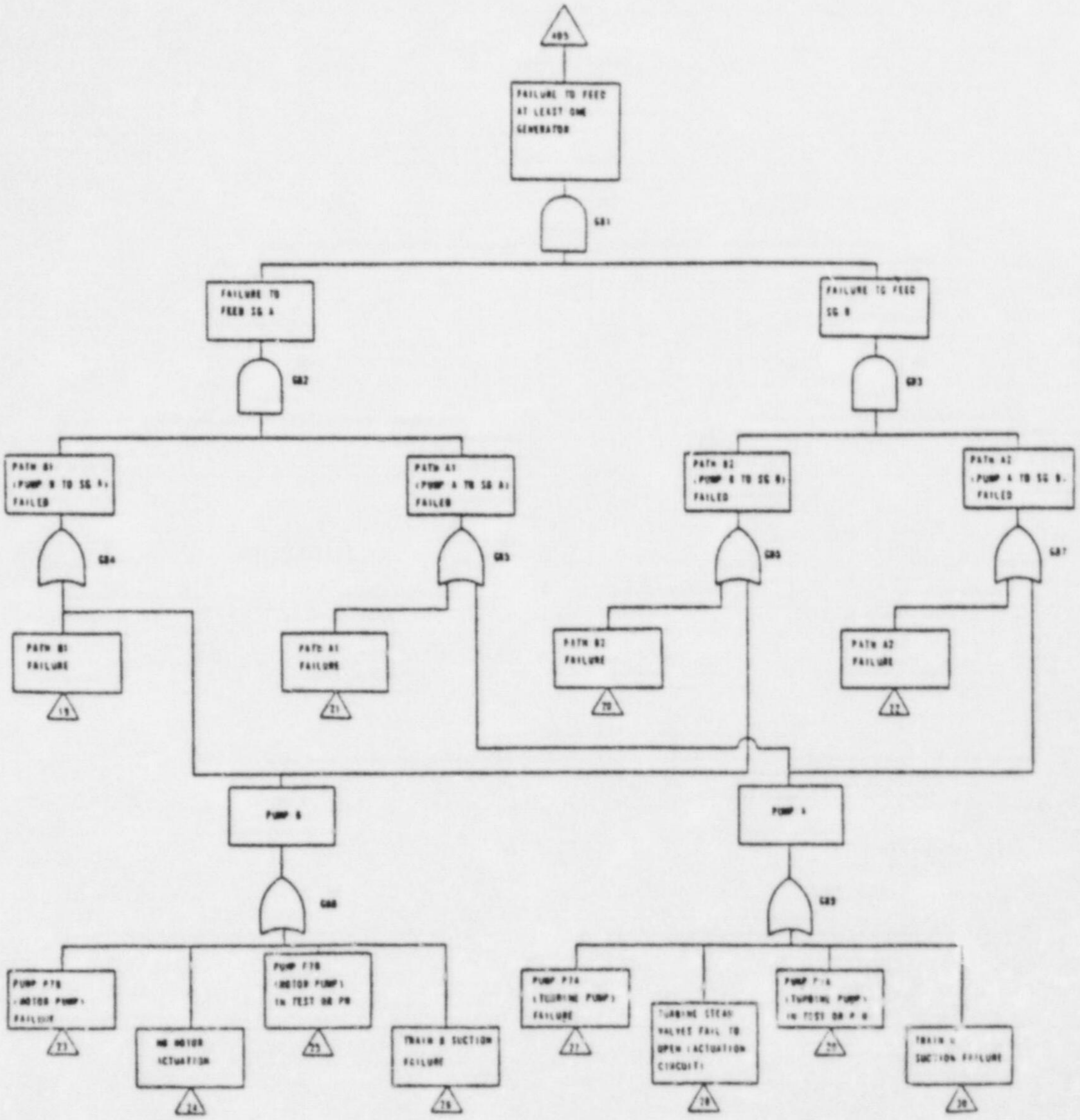
$$t_m = ((\beta-1)/(\lambda\beta))^{1/\beta} + \varepsilon$$

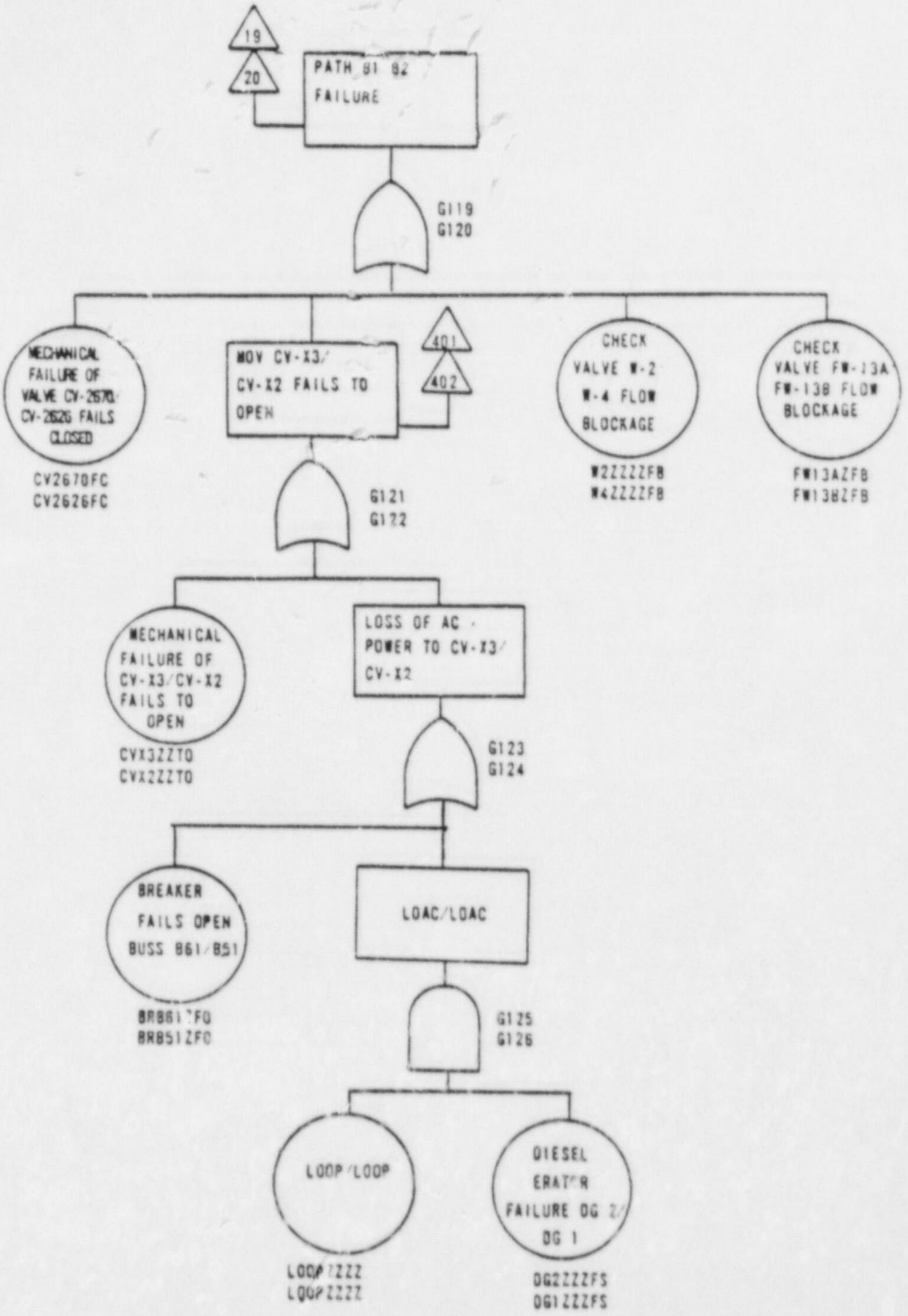
The rest of the calculation is the same as in Appendix A. Here we have, of course, two free parameters for the Weibull distribution, ε and β, and only one for the FPT distribution, α.

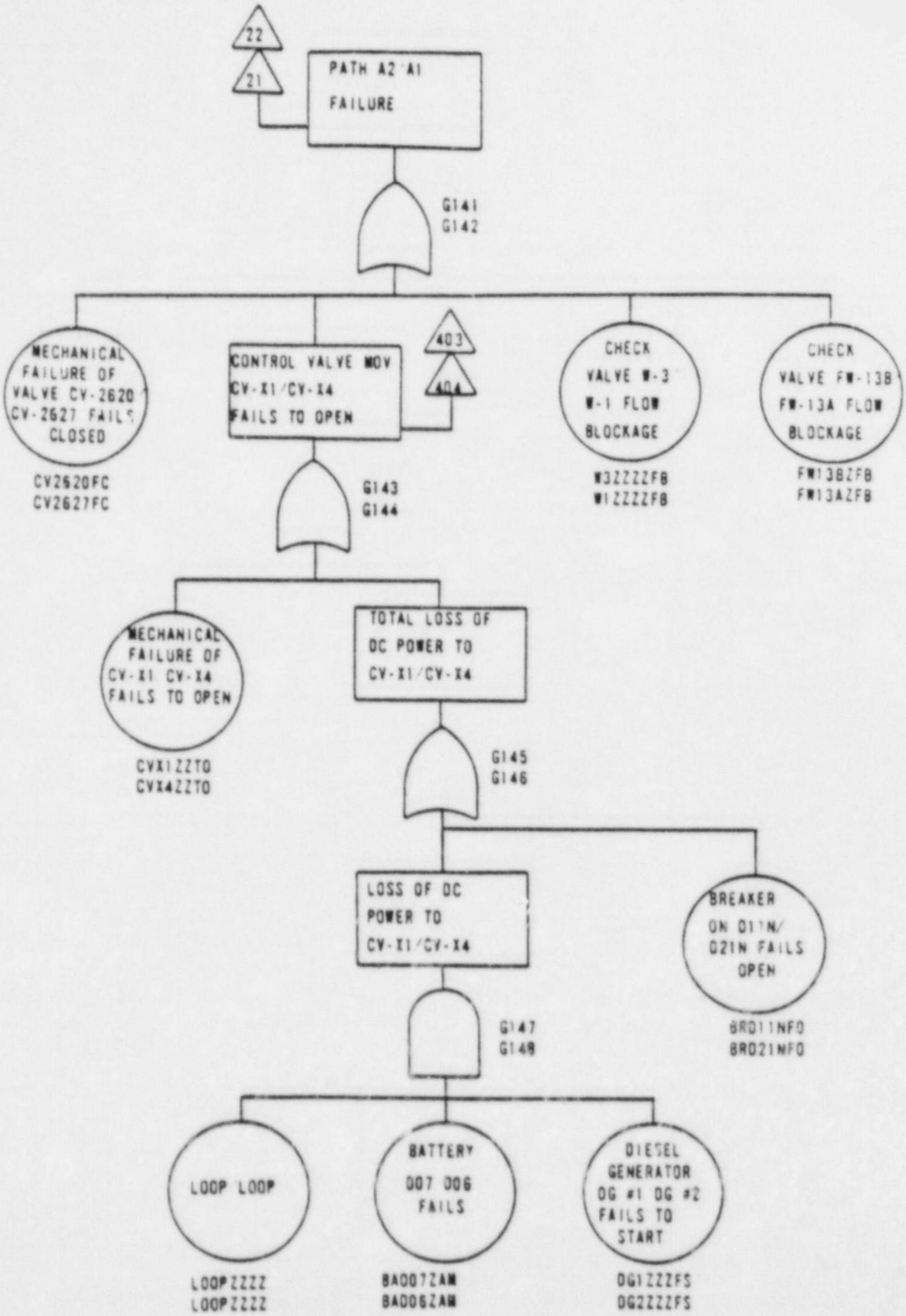
APPENDIX 2

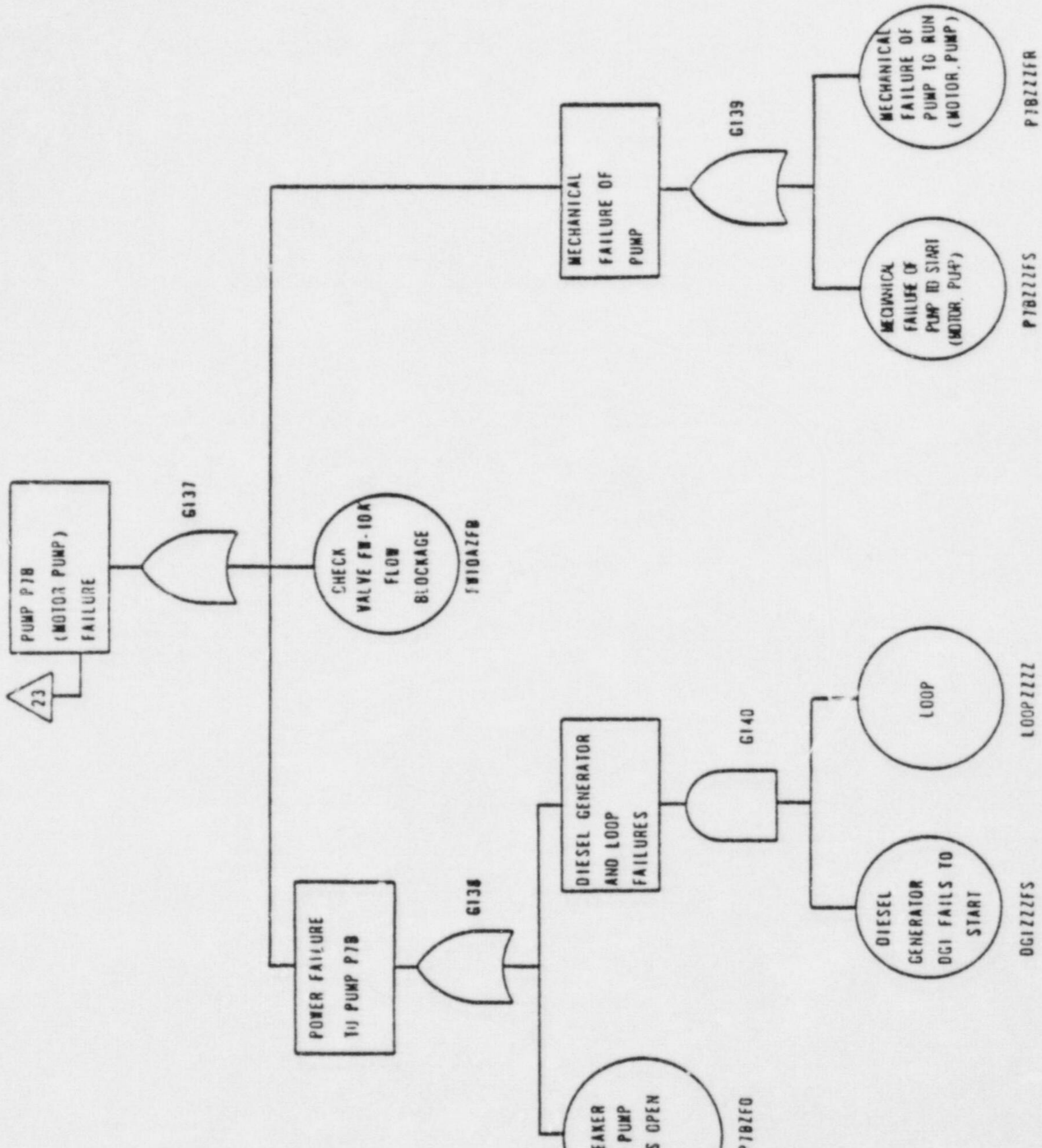
EFWS INITIATION FAULT TREES

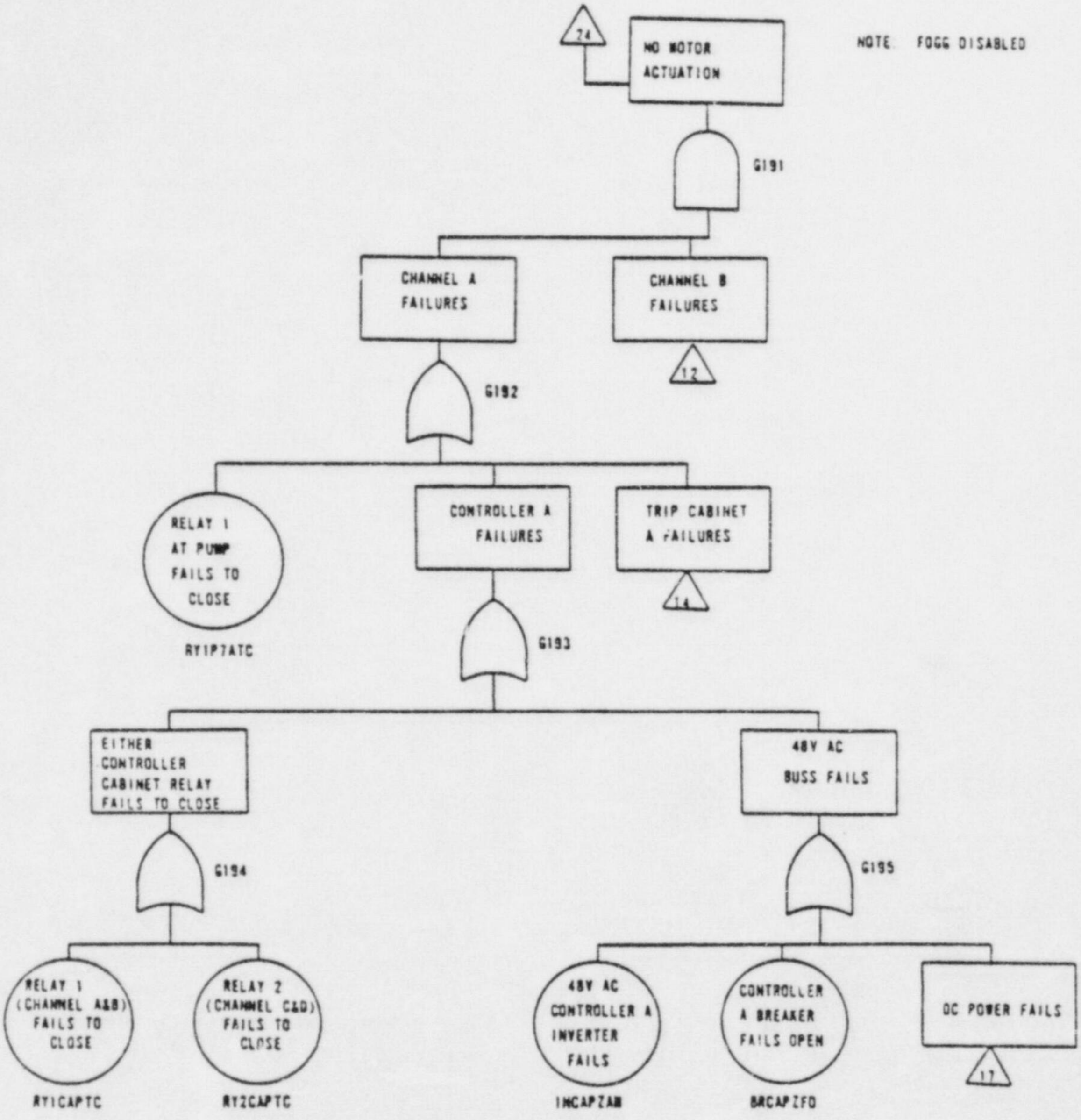

AFW INITIATE FAILURE
677
FAILURE TO FEED AT LEAST ONE GENERATOR
405
FLOW DIVERTED TO RECIRCULATION
678
RECIRCULATION OPENS BECAUSE CV-11 AND CV-14 FAILS TO OPEN
RECIRCULATION OPENS BECAUSE CV-12 AND CV-13 FAIL TO OPEN
679
680
MOV CV-11 FAILS TO OPEN
MOV CV-14 FAILS TO OPEN
MOV CV-12 FAILS TO OPEN
MOV CV-13 FAILS TO OPEN
403
404
402
401

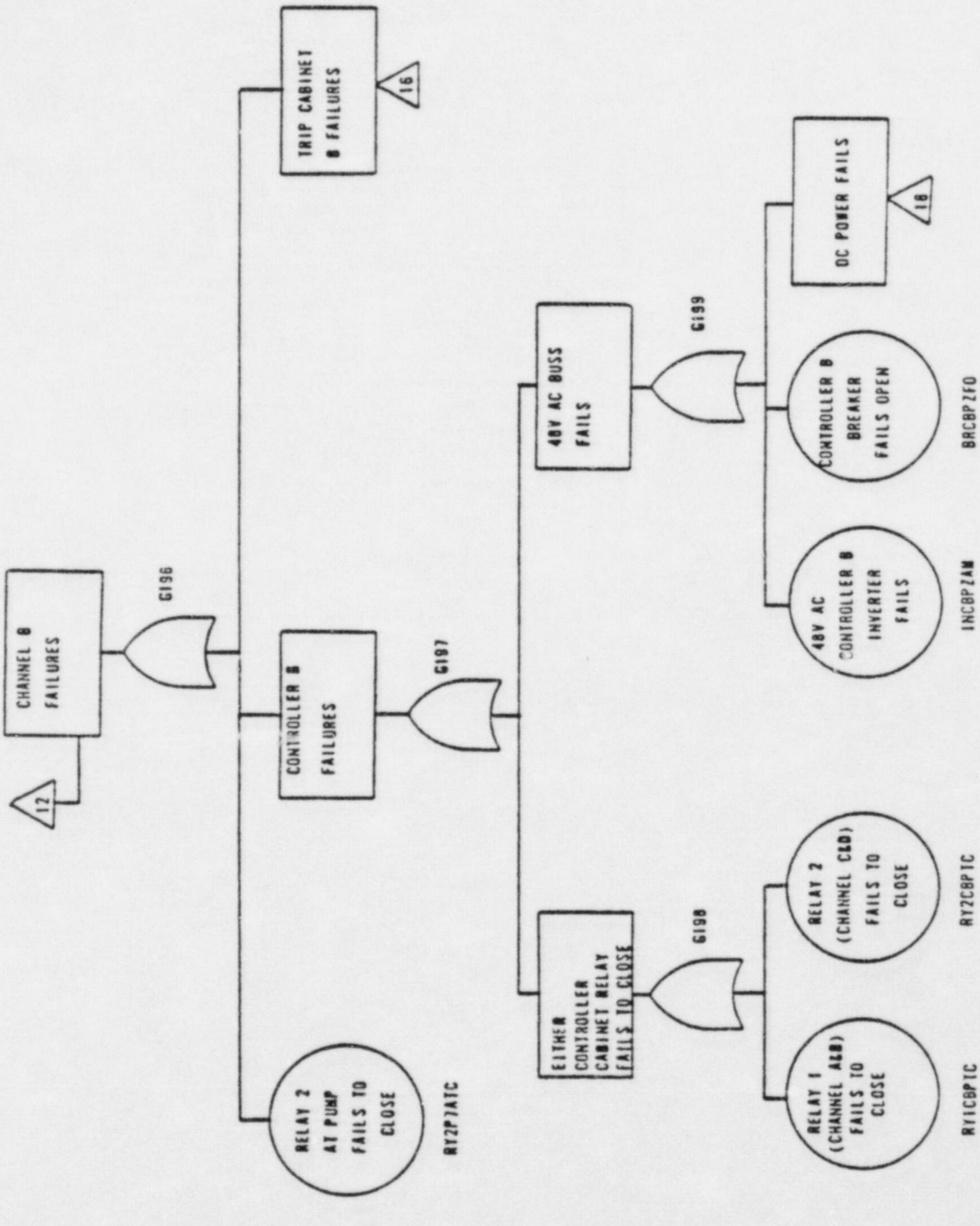

405
FAILURE TO FEED AT LEAST ONE GENERATOR
G01
FAILURE TO FEED SG A
FAILURE TO FEED SG B
G02
G03
PATH B1 (PUMP B TO SG A) FAILED
PATH A1 (PUMP A TO SG A) FAILED
PATH B2 (PUMP B TO SG B) FAILED
PATH A2 (PUMP A TO SG B) FAILED
G04
G05
G06
G07
PATH B1 FAILURE
19
PATH A1 FAILURE
21
PATH B2 FAILURE
20
PATH A2 FAILURE
22
PUMP B
PUMP A
G08
G09
PUMP P7B (MOTOR PUMP) FAILURE
23
NO MOTOR ACTUATION
24
PUMP P7B (MOTOR PUMP) IN TEST OR PM
25
TRAIN B SUCTION FAILURE
26
PUMP P7A (TURBINE PUMP) FAILURE
27
TURBINE STEAM VALVES FAIL TO OPEN (ACTUATION CIRCUIT)
28
PUMP P7A (TURBINE PUMP) IN TEST OR P M
29
TRAIN A SUCTION FAILURE
30

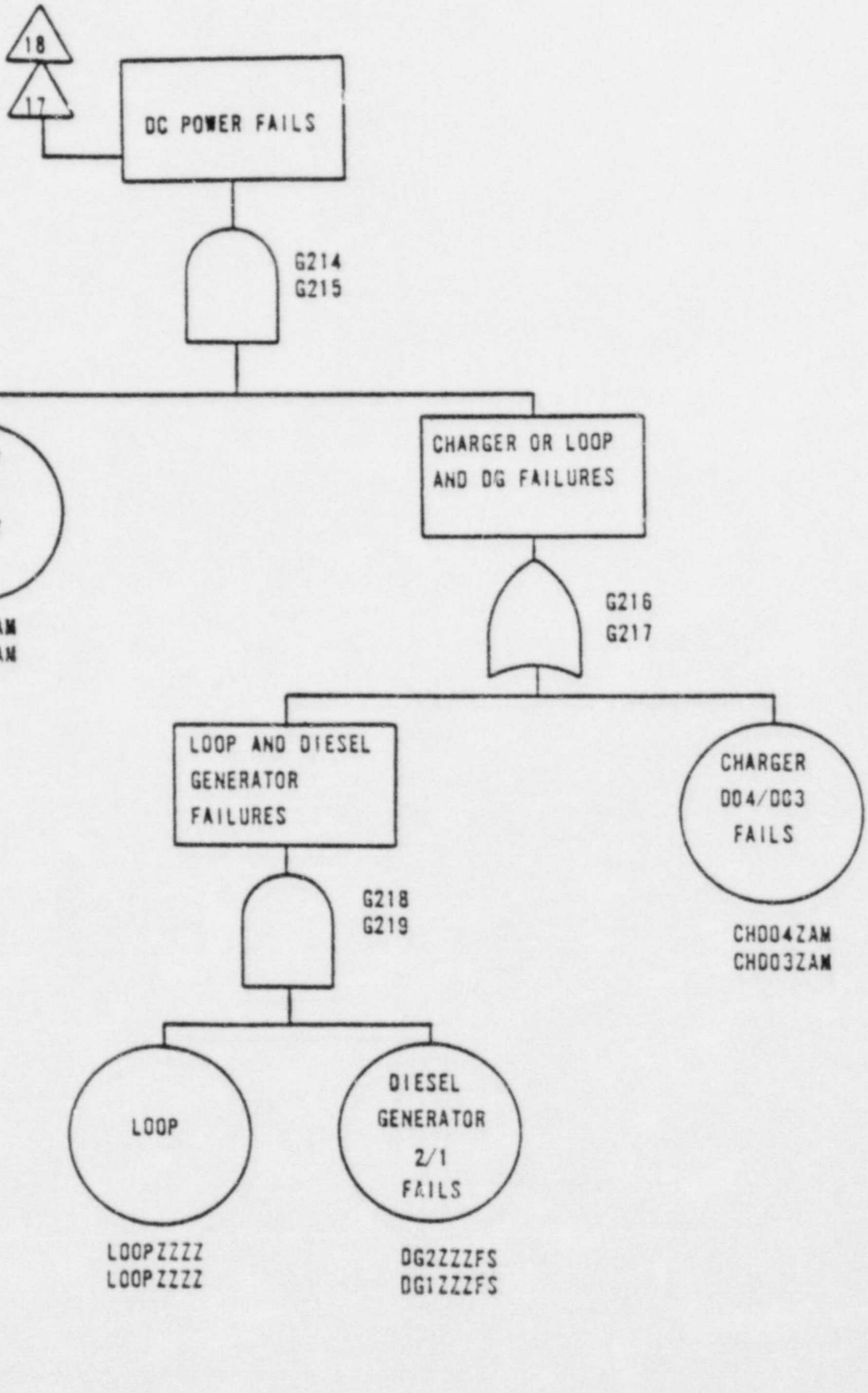

19
20
PATH 81 82
FAILURE
G119
G120
MECHANICAL
FAILURE OF
VALVE CV-2670/
CV-2626 FAILS
CLOSED
CV2670FC
CV2626FC
MOV CV-X3/
CV-X2 FAILS TO
OPEN
401
402
CHECK
VALVE W-2
W-4 FLOW
BLOCKAGE
W2ZZZZFB
W4ZZZZFB
CHECK
VALVE FW-13A
FW-13B FLOW
BLOCKAGE
FW13AZFB
FW13BZFB
G121
G122
MECHANICAL
FAILURE OF
CV-X3/CV-X2
FAILS TO
OPEN
CVX3ZZTO
CVX2ZZTO
LOSS OF AC
POWER TO CV-X3/
CV-X2
G123
G124
BREAKER
FAILS OPEN
BUSS B61/B51
BRB61ZFO
BRB51ZFO
LOAC/LOAC
G125
G126
LOOP/LOOP
LOOPZZZZ
LOOPZZZZ
DIESEL
ERATOR
FAILURE DG 2/
DG 1
DG2ZZZFS
DG1ZZZFS

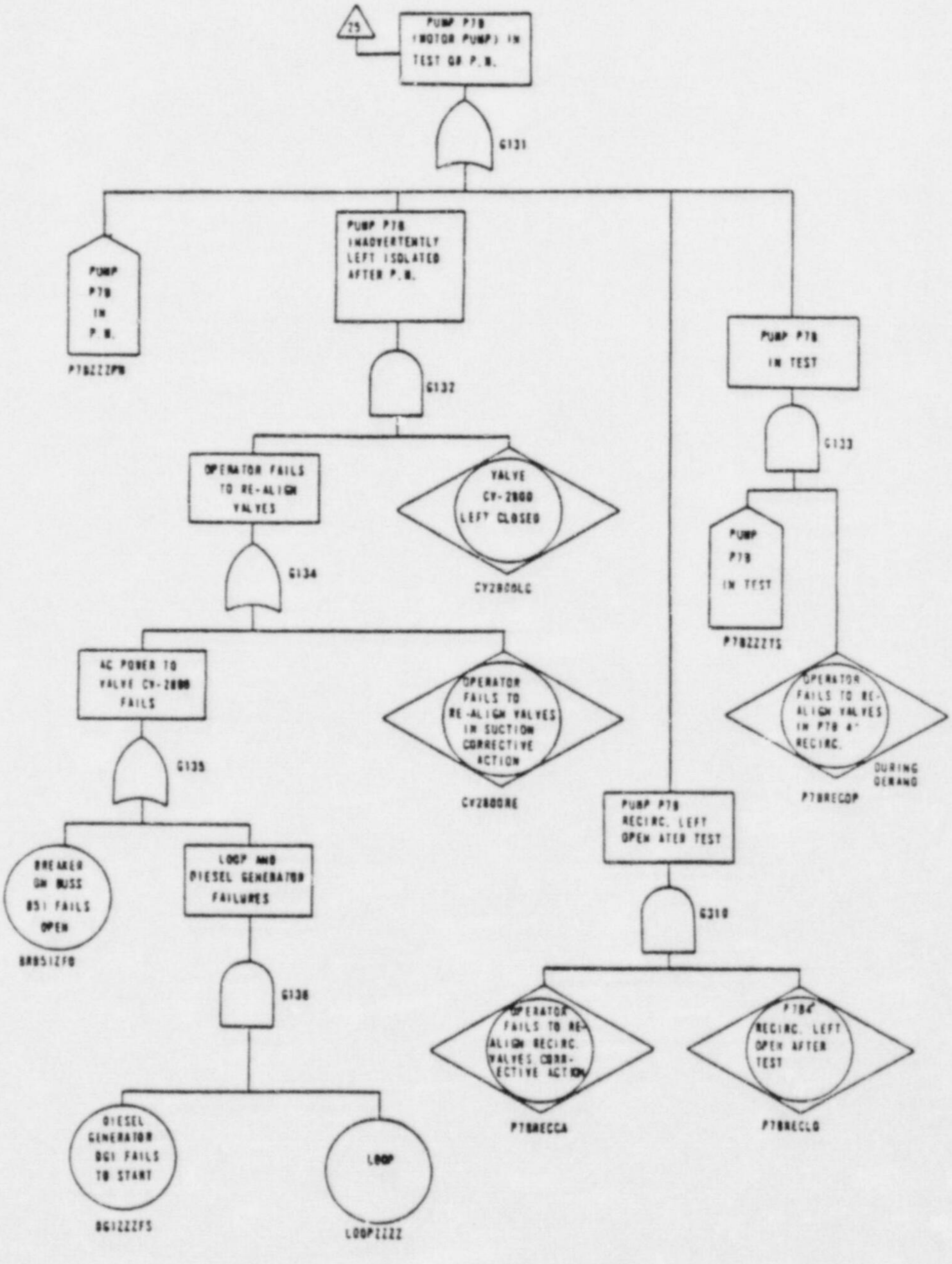

22
21
PATH A2/A1 FAILURE
G141
G142
MECHANICAL FAILURE OF VALVE CV-2620/ CV-2627 FAILS CLOSED
CV2620FC
CV2627FC
CONTROL VALVE MOV CV-X1/CV-X4 FAILS TO OPEN
403
404
CHECK VALVE W-3/ W-1 FLOW BLOCKAGE
W3ZZZZFB
W1ZZZZFB
CHECK VALVE FW-13B/ FW-13A FLOW BLOCKAGE
FW13BZFB
FW13AZFB
G143
G144
MECHANICAL FAILURE OF CV-X1/CV-X4 FAILS TO OPEN
CVX1ZZTO
CVX4ZZTO
TOTAL LOSS OF DC POWER TO CV-X1/CV-X4
G145
G146
LOSS OF DC POWER TO CV-X1/CV-X4
BREAKER ON D11N/ D21N FAILS OPEN
BRD11NFO
BRD21NFO
G147
G148
LOOP/LOOP
LOOPZZZZ
LOOPZZZZ
BATTERY D07/D06 FAILS
BAD07ZAM
BAD06ZAM
DIESEL GENERATOR DG #1/DG #2 FAILS TO START
DG1ZZZFS
DG2ZZZFS

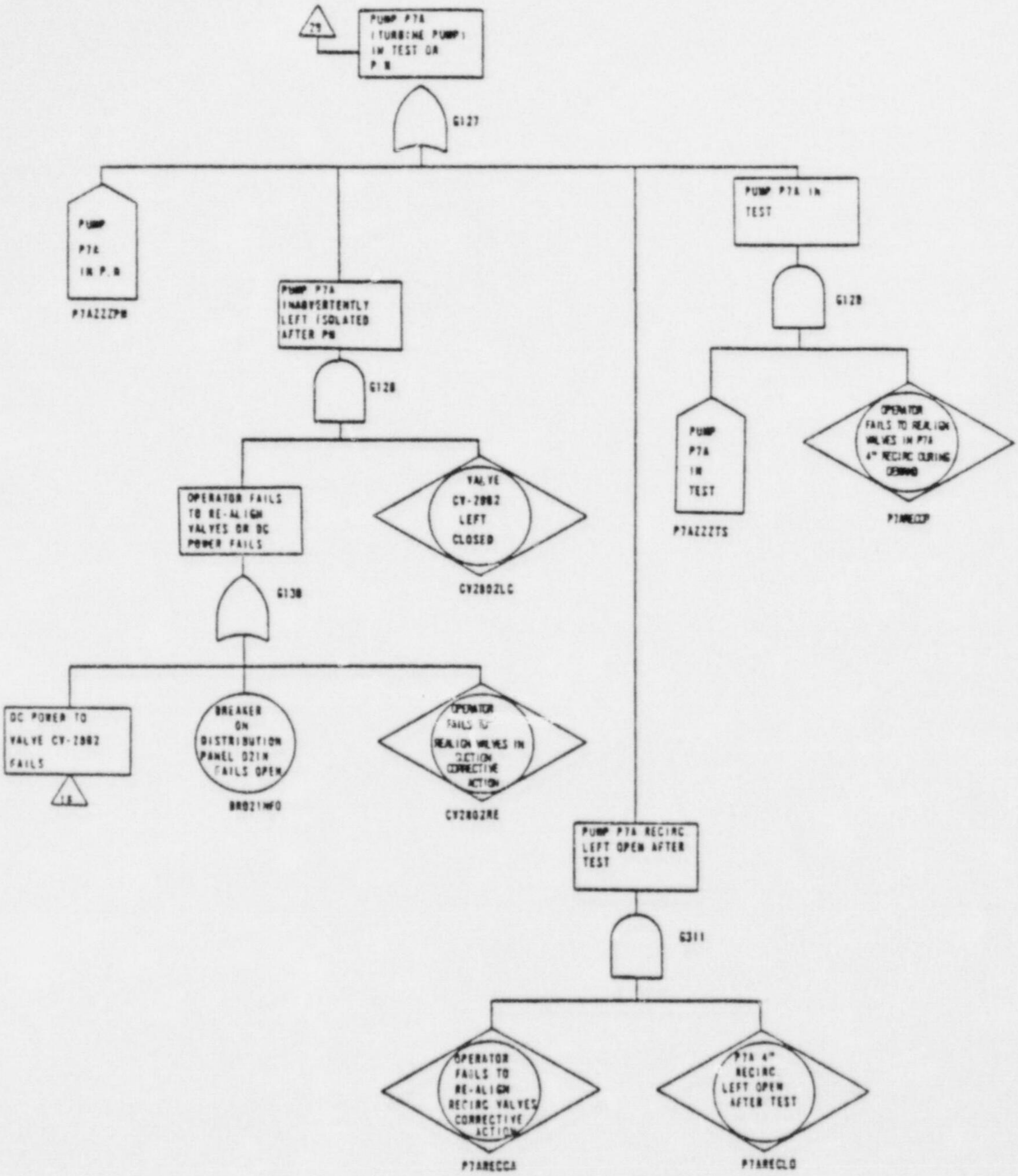

23
PUMP P7B (MOTOR PUMP) FAILURE
G137
CHECK VALVE FW-10K FLOW BLOCKAGE
FW10AZFB
POWER FAILURE TO PUMP P7B
G138
BREAKER ON PUMP FAILS OPEN
BRP7BZFO
DIESEL GENERATOR AND LOOP FAILURES
G140
DIESEL GENERATOR DG1 FAILS TO START
DG1ZZZFS
LOOP
LOOPZZZZ
MECHANICAL FAILURE OF PUMP
G139
MECHANICAL FAILURE OF PUMP TO START (MOTOR, PUMP)
P7BZZZFS
MECHANICAL FAILURE OF PUMP TO RUN (MOTOR, PUMP)
P7BZZZFR

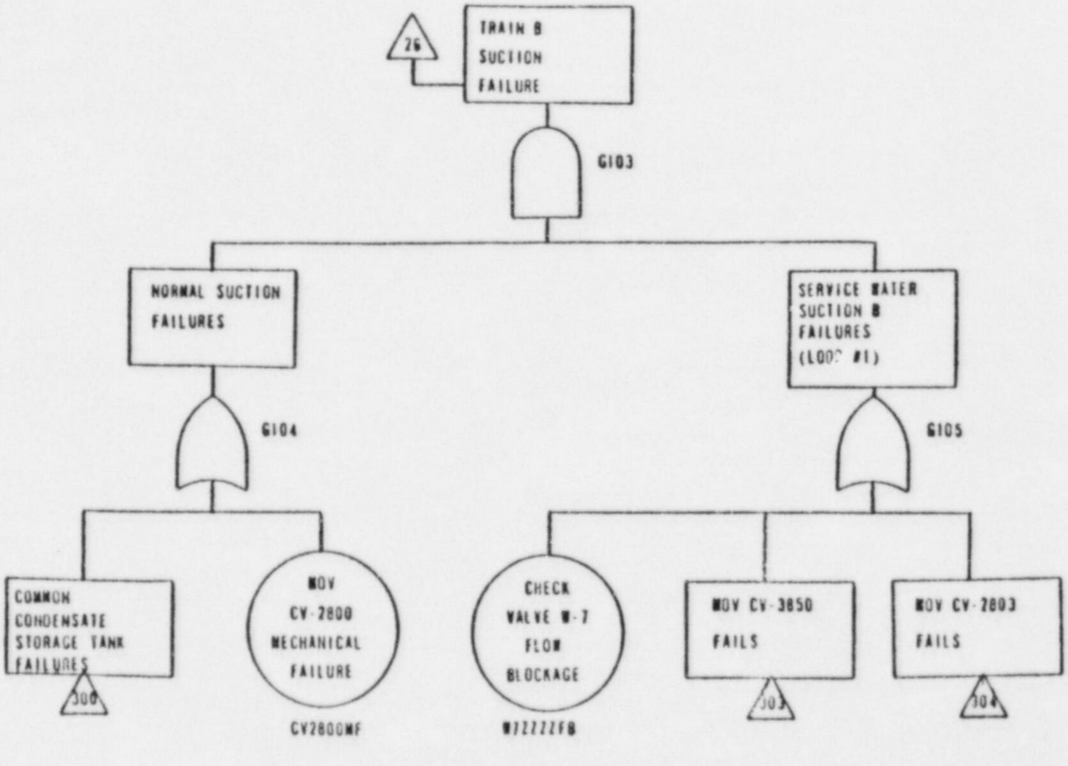

24
NO MOTOR ACTUATION
NOTE: FOGG DISABLED
G191
CHANNEL A FAILURES
CHANNEL B FAILURES
12
G192
RELAY 1 AT PUMP FAILS TO CLOSE
RY1P7ATC
CONTROLLER A FAILURES
TRIP CABINET A FAILURES
14
G193
EITHER CONTROLLER CABINET RELAY FAILS TO CLOSE
48V AC BUSS FAILS
G194
G195
RELAY 1 (CHANNEL A&B) FAILS TO CLOSE
RY1CAPTC
RELAY 2 (CHANNEL C&D) FAILS TO CLOSE
RY2CAPTC
48V AC CONTROLLER A INVERTER FAILS
INCAPZAM
CONTROLLER A BREAKER FAILS OPEN
BRCAPZFO
DC POWER FAILS
17

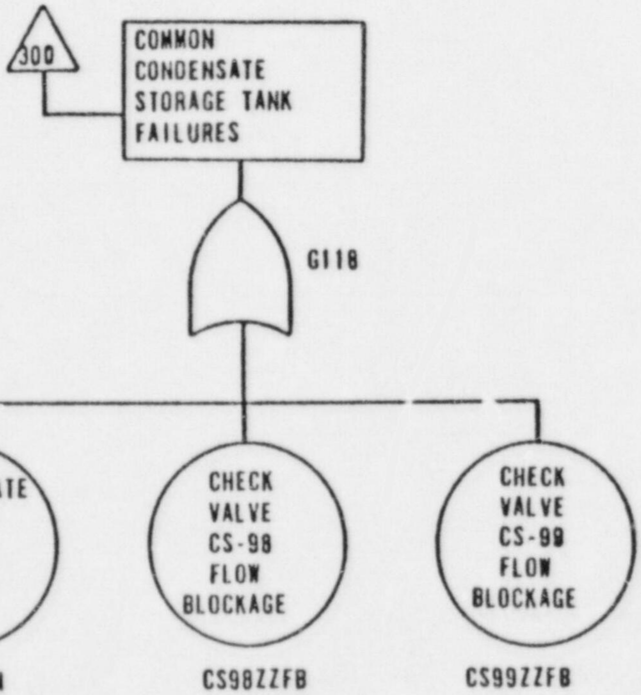

12
CHANNEL B FAILURES
G196
RELAY 2 AT PUMP FAILS TO CLOSE
RY2P7ATC
CONTROLLER B FAILURES
G197
TRIP CABINET B FAILURES
16
EITHER CONTROLLER CABINET RELAY FAILS TO CLOSE
G198
48V AC BUSS FAILS
G199
RELAY 1 (CHANNEL A&B) FAILS TO CLOSE
RY1CBPTC
RELAY 2 (CHANNEL C&D) FAILS TO CLOSE
RY2CBPTC
48V AC CONTROLLER B INVERTER FAILS
INCBPZAM
CONTROLLER B BREAKER FAILS OPEN
BRCBPZFO
DC POWER FAILS
18

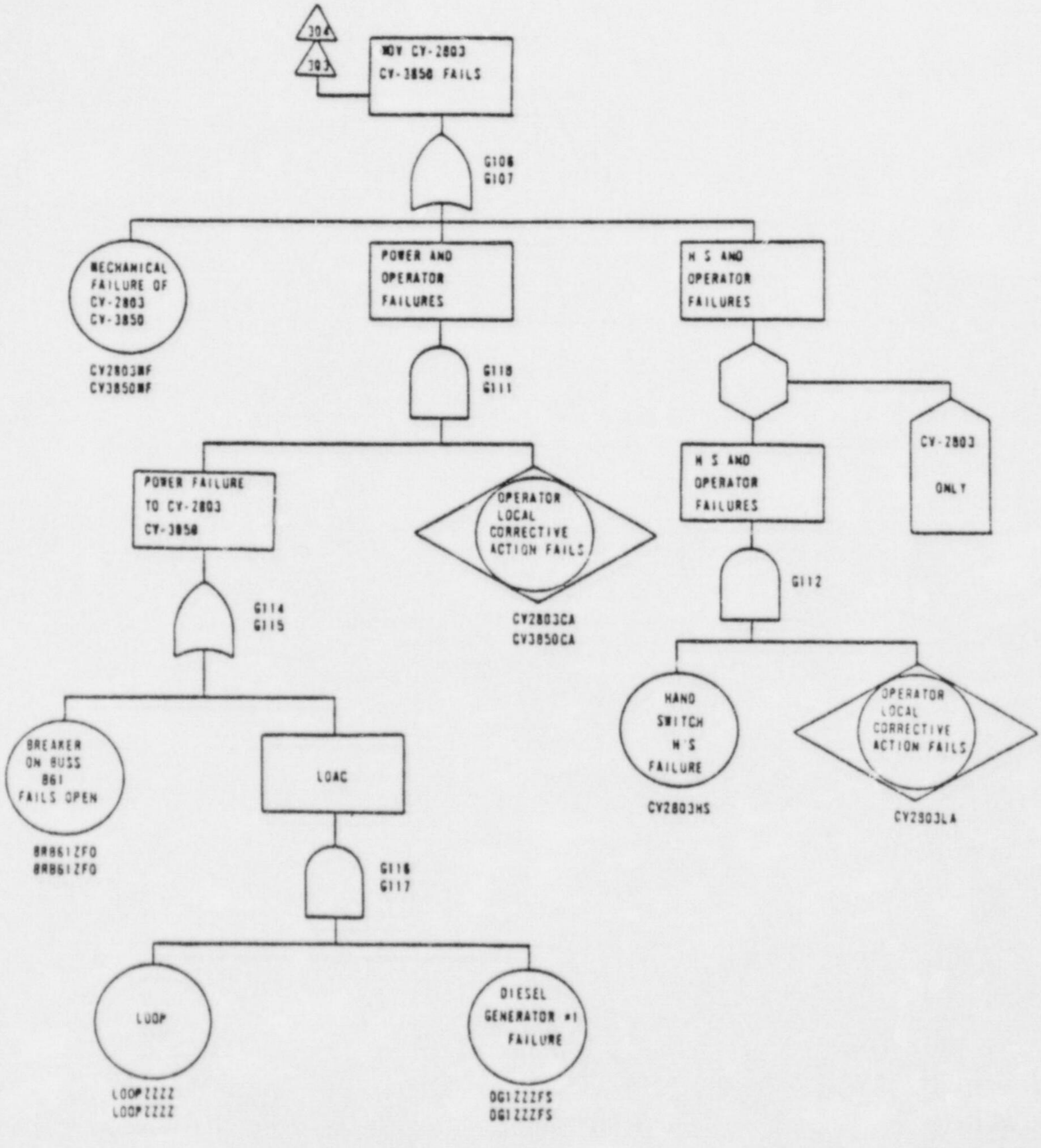

18
17
DC POWER FAILS
G214
G215
BATTERY BANK D06/D07 FAILS
BAD06ZAM
BAD07ZAM
CHARGER OR LOOP AND DG FAILURES
G216
G217
LOOP AND DIESEL GENERATOR FAILURES
CHARGER D04/DC3 FAILS
CH004ZAM
CH003ZAM
G218
G219
LOOP
LOOPZZZZ
LOOPZZZZ
DIESEL GENERATOR 2/1 FAILS
DG2ZZZFS
DG1ZZZFS

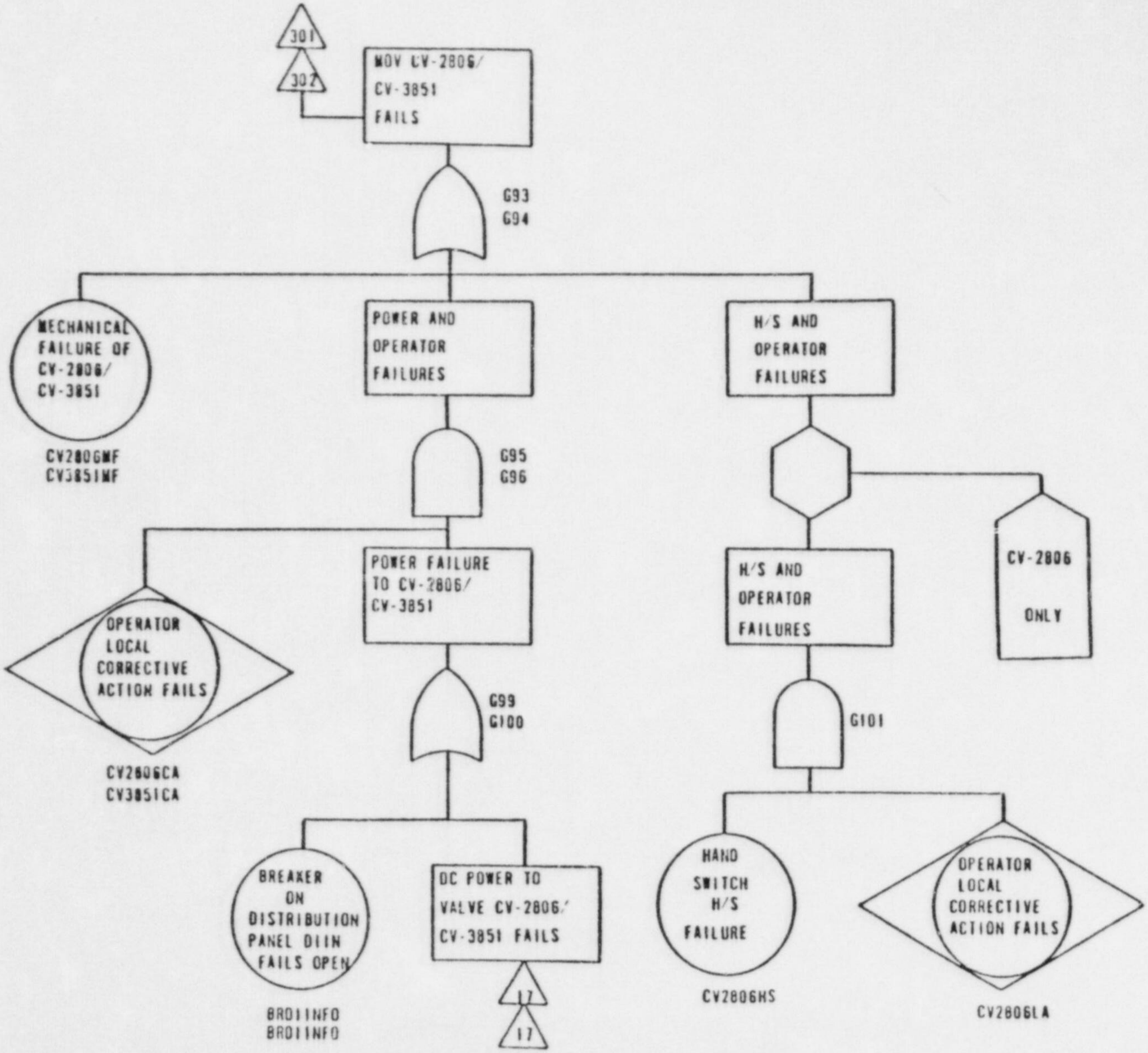

25
PUMP P7B (MOTOR PUMP) IN TEST OR P.M.
G131
PUMP P7B IN P.M.
P7BZZZPM
PUMP P7B INADVERTENTLY LEFT ISOLATED AFTER P.M.
G132
OPERATOR FAILS TO RE-ALIGN VALVES
VALVE CV-2800 LEFT CLOSED
CY2800LC
G134
AC POWER TO VALVE CV-2800 FAILS
OPERATOR FAILS TO RE-ALIGN VALVES IN SUCTION CORRECTIVE ACTION
CV2800RE
G135
BREAKER ON BUSS B51 FAILS OPEN
BRB51ZFO
LOOP AND DIESEL GENERATOR FAILURES
G136
DIESEL GENERATOR DG1 FAILS TO START
DG1ZZZFS
LOOP
LOOPZZZZ
PUMP P7B IN TEST
G133
PUMP P7B IN TEST
P7BZZZTS
OPERATOR FAILS TO RE-ALIGN VALVES IN P7B 4" RECIRC.
DURING DERANG
P7BRECOP
PUMP P7B RECIRC. LEFT OPEN ATER TEST
G310
OPERATOR FAILS TO RE-ALIGN RECIRC. VALVES CORR-ECTIVE ACTION
P7BRECCA
P7B4" RECIRC. LEFT OPEN AFTER TEST
P7BRECLO

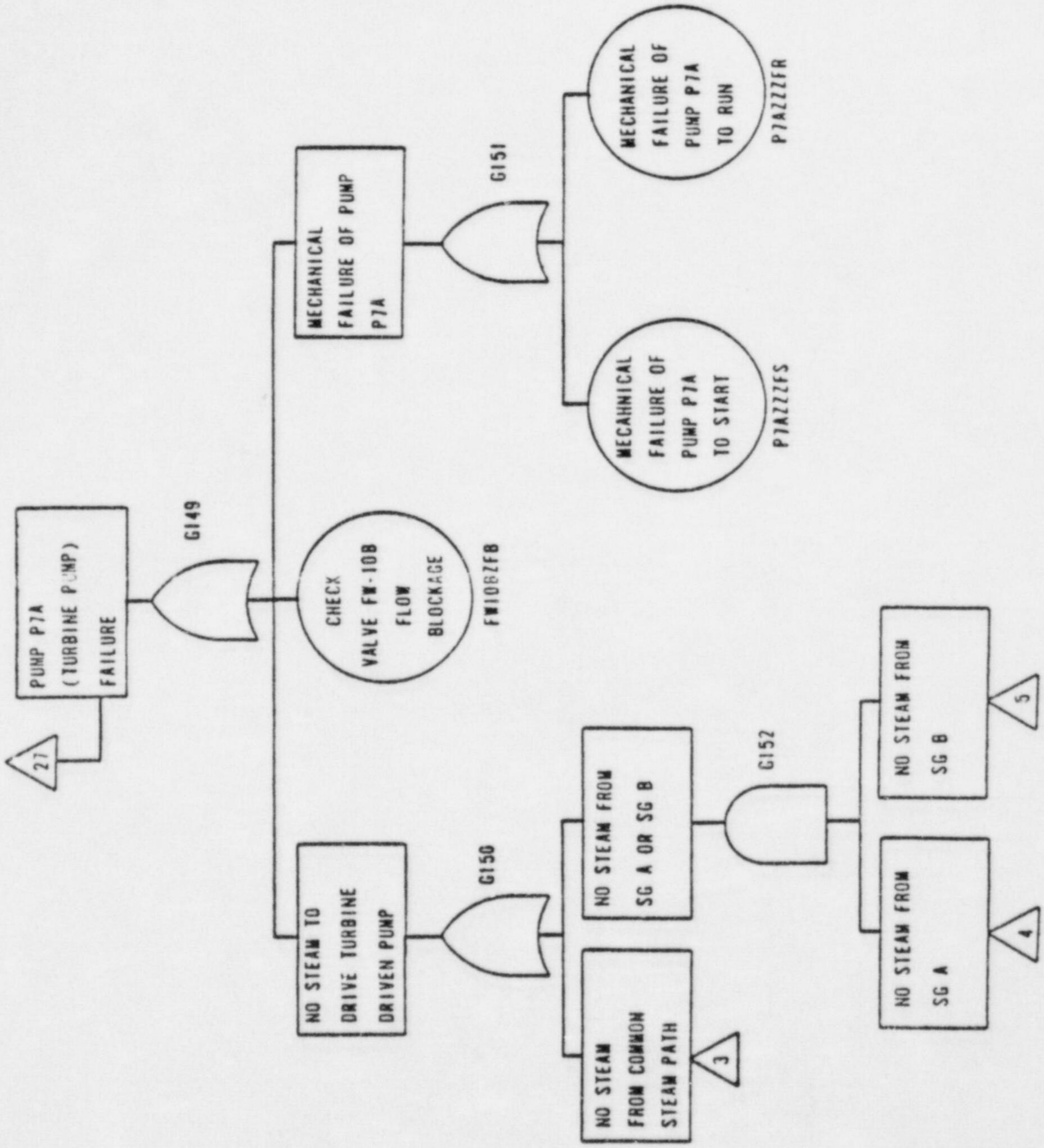

29
PUMP P7A (TURBINE PUMP) IN TEST OR P M
G127
PUMP P7A IN P.M
P7AZZZPM
PUMP P7A INADVERTENTLY LEFT ISOLATED AFTER PM
G128
OPERATOR FAILS TO RE-ALIGN VALVES OR DC POWER FAILS
VALVE CV-2082 LEFT CLOSED
CV2802LC
G130
DC POWER TO VALVE CV-2802 FAILS
18
BREAKER ON DISTRIBUTION PANEL D21N FAILS OPEN
BRD21NFO
OPERATOR FAILS TO REALIGN VALVES IN SUCTION CORRECTIVE ACTION
CV2802RE
PUMP P7A IN TEST
G129
PUMP P7A IN TEST
P7AZZZTS
OPERATOR FAILS TO REALIGN VALVES IN P7A 4" RECIRC DURING DEMAND
P7ARECCP
PUMP P7A RECIRC LEFT OPEN AFTER TEST
G311
OPERATOR FAILS TO RE-ALIGN RECIRC VALVES CORRECTIVE ACTION
P7ARECCA
P7A 4" RECIRC LEFT OPEN AFTER TEST
P7ARECLO

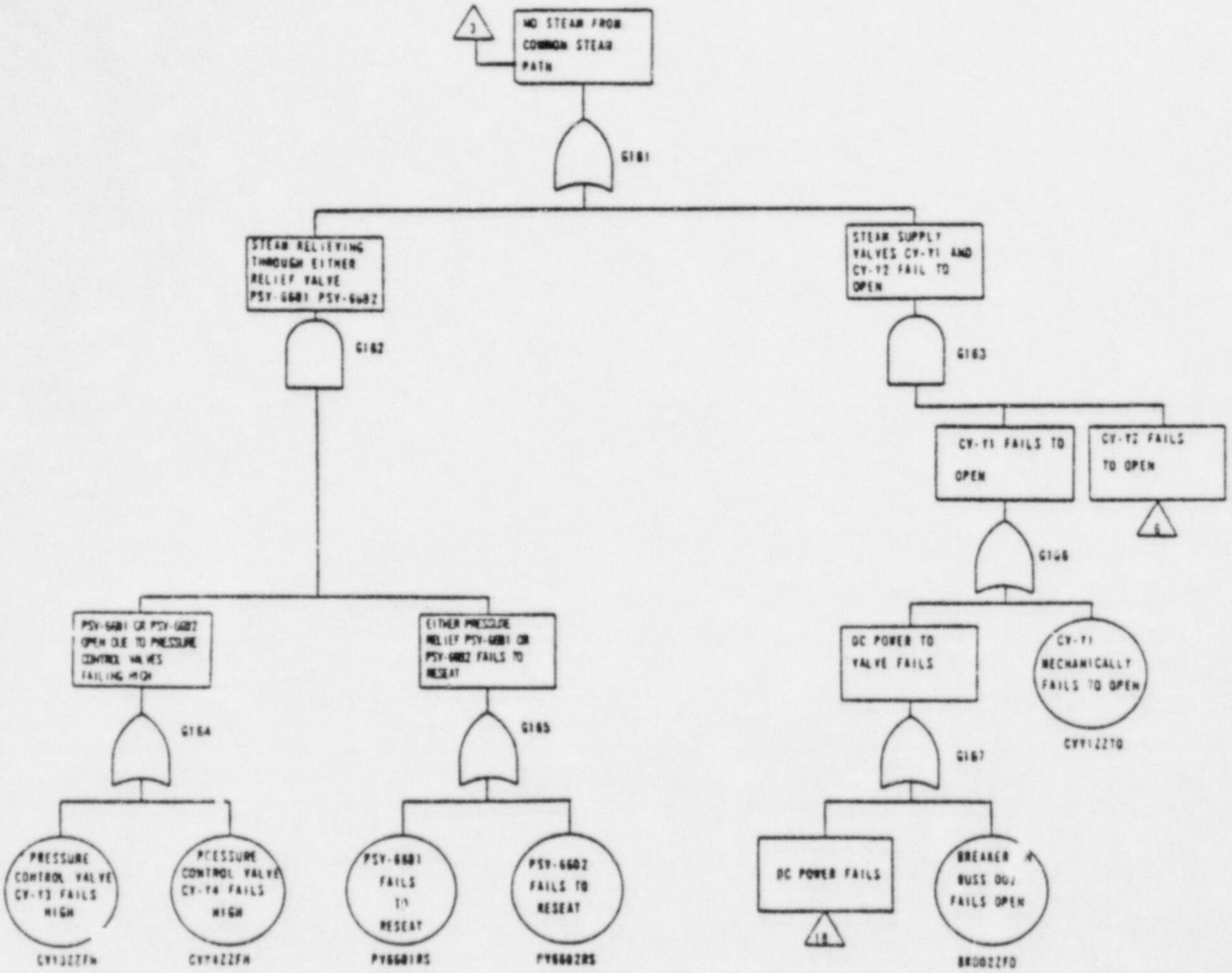

26
TRAIN B
SUCTION
FAILURE
G103
NORMAL SUCTION
FAILURES
SERVICE WATER
SUCTION B
FAILURES
(LOO? #1)
G104
G105
COMMON
CONDENSATE
STORAGE TANK
FAILURES
300
MOV
CV-2800
MECHANICAL
FAILURE
CV2800MF
CHECK
VALVE W-7
FLOW
BLOCKAGE
W7ZZZZFB
MOV CV-3850
FAILS
303
MOV CV-2803
FAILS
304

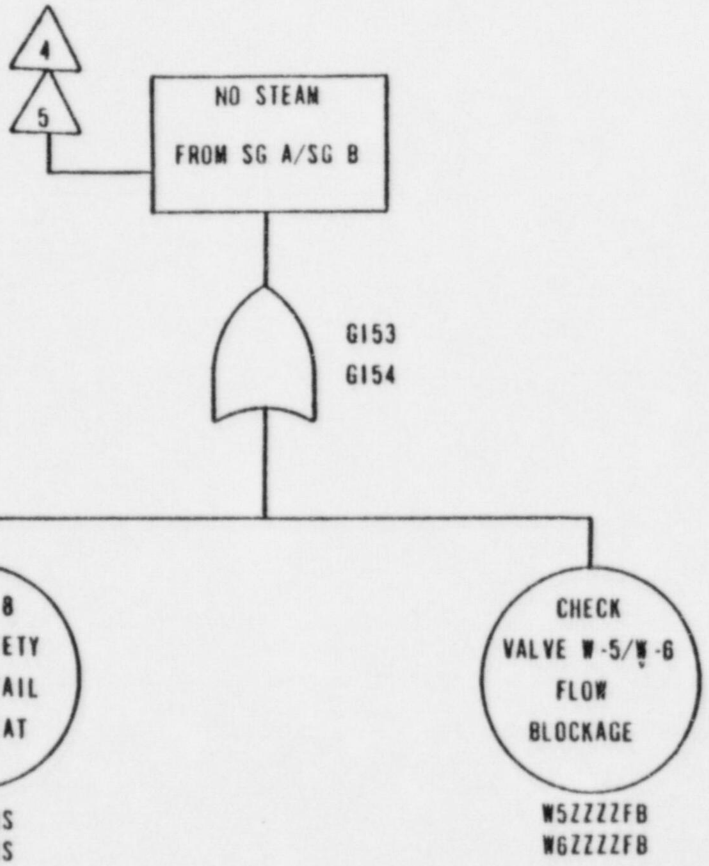

300
COMMON
CONDENSATE
STORAGE TANK
FAILURES
G118
CONDENSATE
STORAGE
TANK
FAILURE
CST41ZAM
CHECK
VALVE
CS-98
FLOW
BLOCKAGE
CS98ZZFB
CHECK
VALVE
CS-99
FLOW
BLOCKAGE
CS99ZZFB

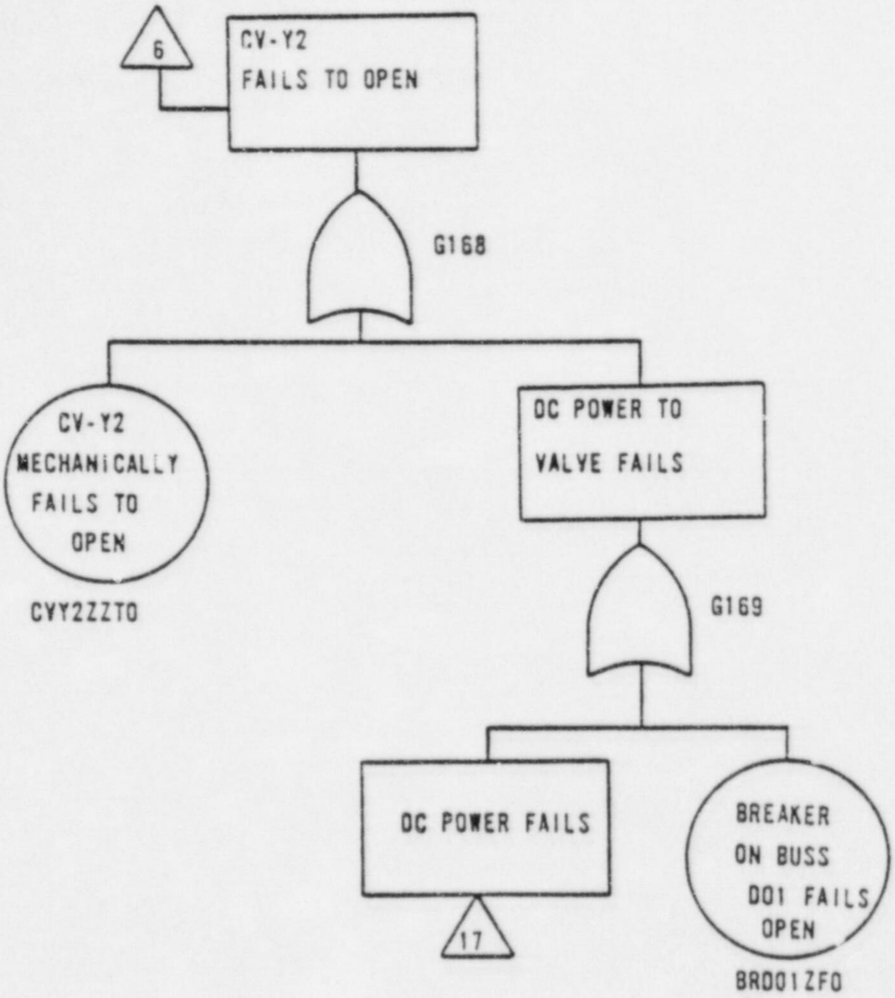

304
303
MOV CY-2803 CY-3850 FAILS
G106
G107
MECHANICAL FAILURE OF CY-2803 CY-3850
CY2803MF
CY3850MF
POWER AND OPERATOR FAILURES
G110
G111
H S AND OPERATOR FAILURES
CY-2803 ONLY
POWER FAILURE TO CY-2803 CY-3850
OPERATOR LOCAL CORRECTIVE ACTION FAILS
CY2803CA
CY3850CA
H S AND OPERATOR FAILURES
G112
G114
G115
BREAKER ON BUSS B61 FAILS OPEN
BRB61ZFO
BRB61ZFO
LOAC
G116
G117
HAND SWITCH H'S FAILURE
CY2803HS
OPERATOR LOCAL CORRECTIVE ACTION FAILS
CY2803LA
LOOP
LOOPZZZZ
LOOPZZZZ
DIESEL GENERATOR #1 FAILURE
DG1ZZZFS
DG1ZZZFS

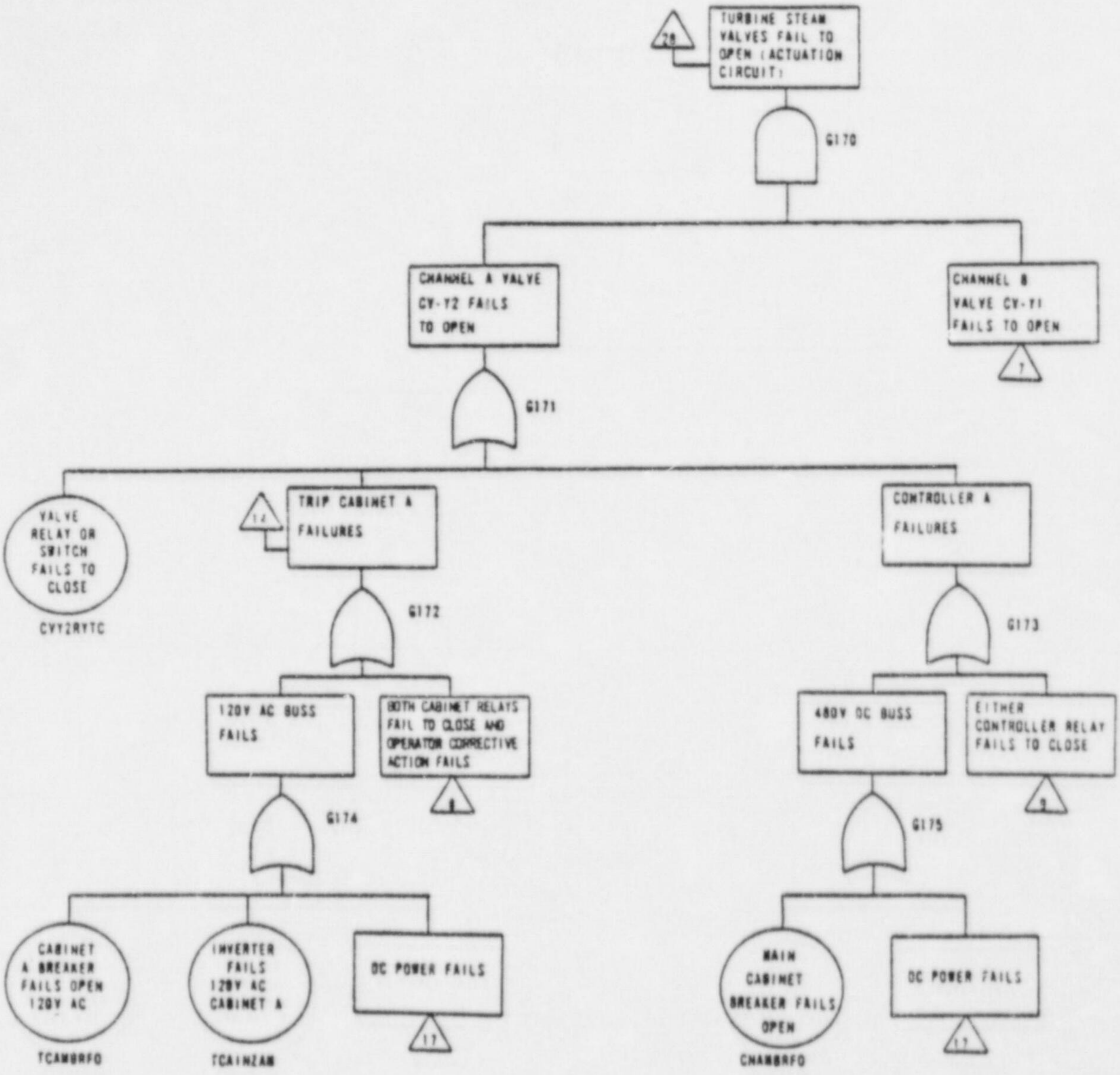

301
302
MOV CV-2806/ CV-3851 FAILS
G93
G94
MECHANICAL FAILURE OF CV-2806/ CV-3851
CV2806MF
CV3851MF
POWER AND OPERATOR FAILURES
H/S AND OPERATOR FAILURES
G95
G96
CV-2806 ONLY
OPERATOR LOCAL CORRECTIVE ACTION FAILS
CV2806CA
CV3851CA
POWER FAILURE TO CV-2806/ CV-3851
H/S AND OPERATOR FAILURES
G99
G100
G101
BREAKER ON DISTRIBUTION PANEL D11N FAILS OPEN
BR011NFO
BR011NFO
DC POWER TO VALVE CV-2806/ CV-3851 FAILS
17
17
HAND SWITCH H/S FAILURE
CV2806HS
OPERATOR LOCAL CORRECTIVE ACTION FAILS
CV2806LA

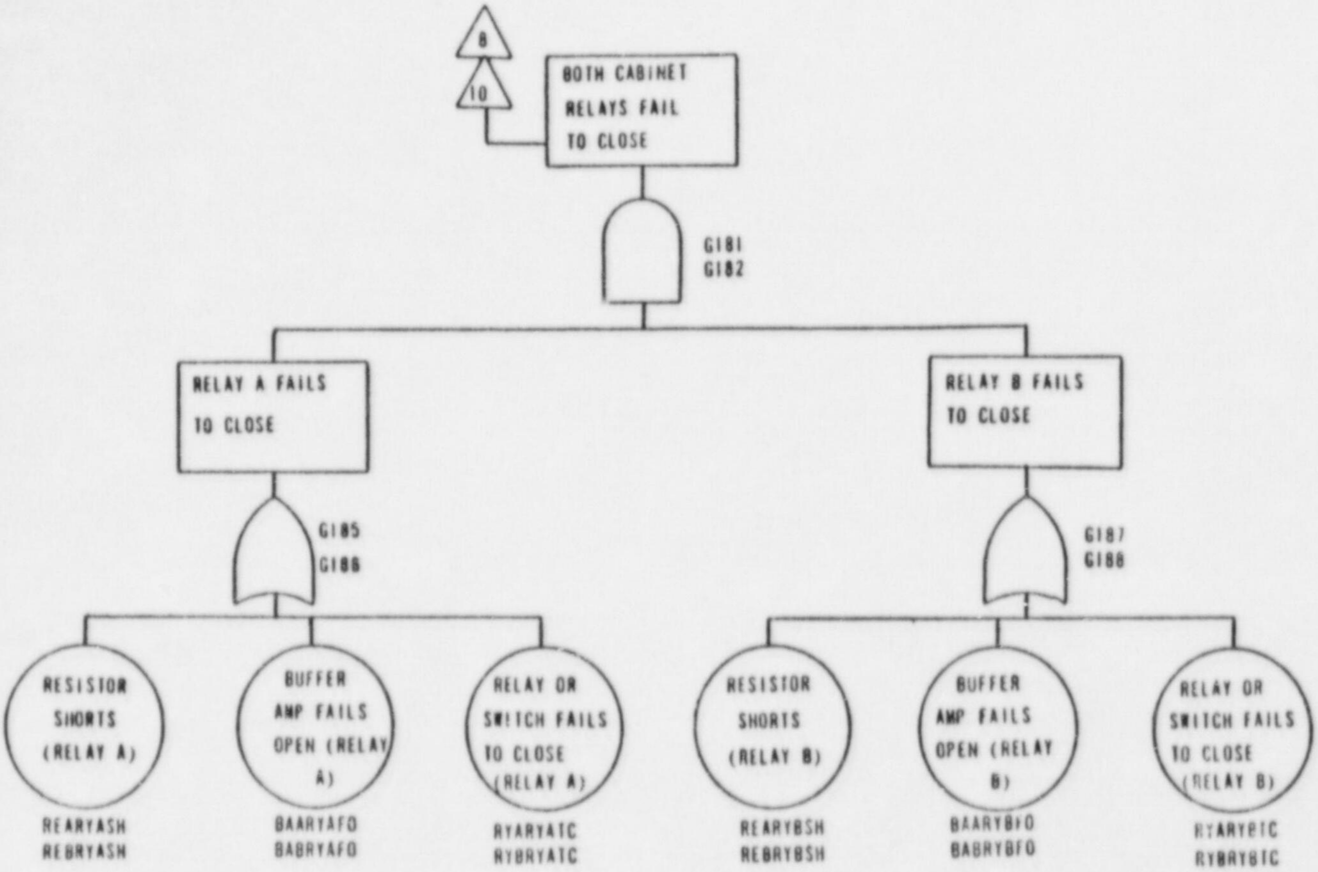

27
PUMP P7A (TURBINE PUMP) FAILURE
G149
CHECK VALVE FW-10B FLOW BLOCKAGE
FW10BZFB
MECHANICAL FAILURE OF PUMP P7A
G151
MECAHNICAL FAILURE OF PUMP P7A TO START
P7AZZZFS
MECHANICAL FAILURE OF PUMP P7A TO RUN
P7AZZZFR
NO STEAM TO DRIVE TURBINE DRIVEN PUMP
G150
NO STEAM FROM COMMON STEAM PATH
3
NO STEAM FROM SG A OR SG B
G152
NO STEAM FROM SG A
4
NO STEAM FROM SG B
5

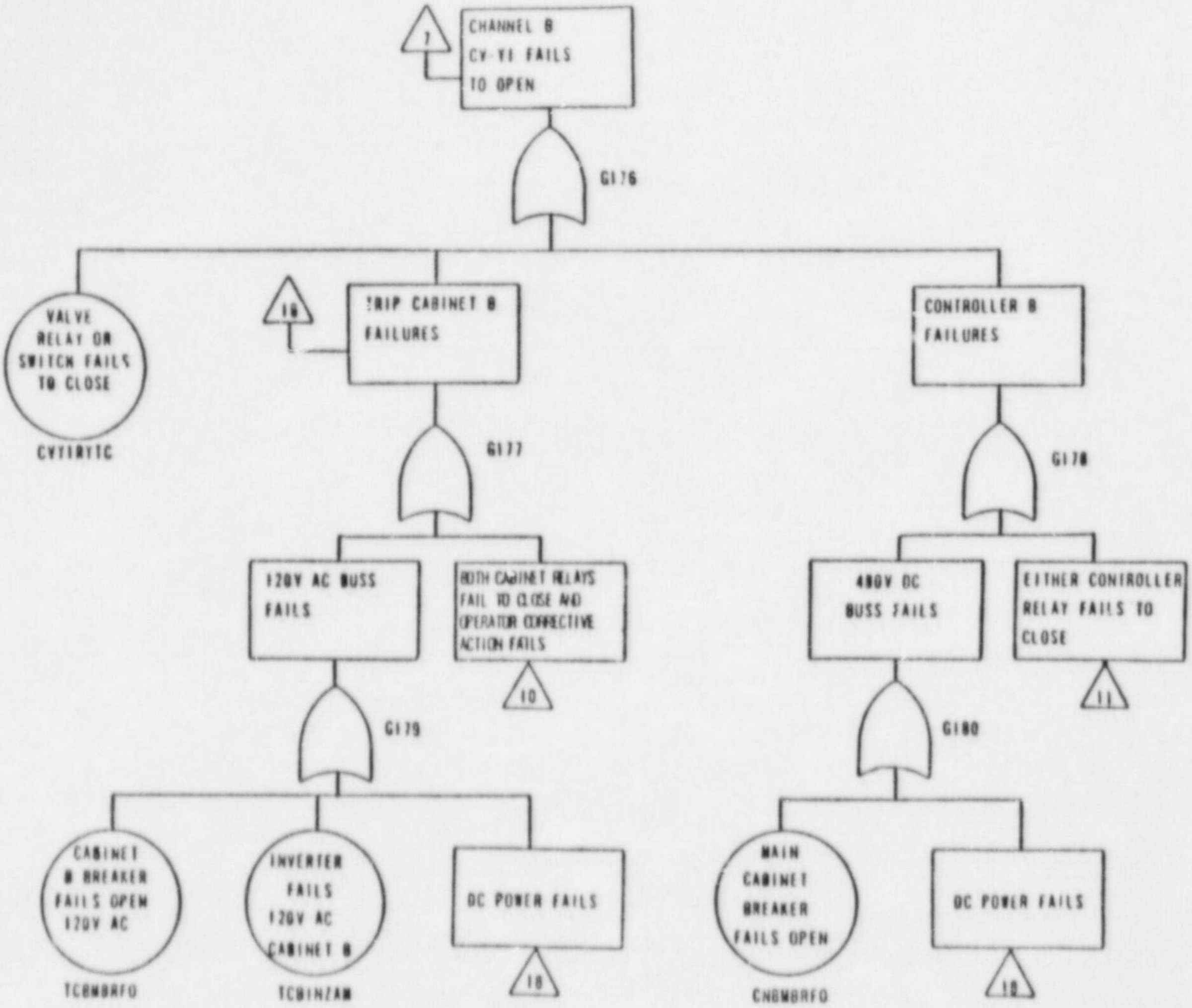

3
NO STEAM FROM COMMON STEAM PATH
G161
STEAM RELIEVING THROUGH EITHER RELIEF VALVE PSY-6681 PSY-6682
G162
STEAM SUPPLY VALVES CV-Y1 AND CV-Y2 FAIL TO OPEN
G163
CV-Y1 FAILS TO OPEN
CV-Y2 FAILS TO OPEN
6
G166
PSV-6681 OR PSV-6682 OPEN DUE TO PRESSURE CONTROL VALVES FAILING HIGH
EITHER PRESSURE RELIEF PSY-6681 OR PSY-6682 FAILS TO RESEAT
DC POWER TO VALVE FAILS
CV-Y1 MECHANICALLY FAILS TO OPEN
CVY1ZZTO
G164
G165
G167
PRESSURE CONTROL VALVE CV-Y3 FAILS HIGH
PCESSURE CONTROL VALVE CV-Y4 FAILS HIGH
PSY-6681 FAILS TO RESEAT
PSY-6682 FAILS TO RESEAT
DC POWER FAILS
18
BREAKER A BUSS 002 FAILS OPEN
CVY3ZZFH
CVY4ZZFH
PY6681RS
PY6682RS
BR002ZFO


4
5
NO STEAM
FROM SG A/SG B
G153
G154
ANY OF 8
CODE SAFETY
VALVES FAIL
TO RESEAT
CSVSGARS
CSVSGBRS
CHECK
VALVE W-5/W-6
FLOW
BLOCKAGE
W5ZZZZFB
W6ZZZZFB

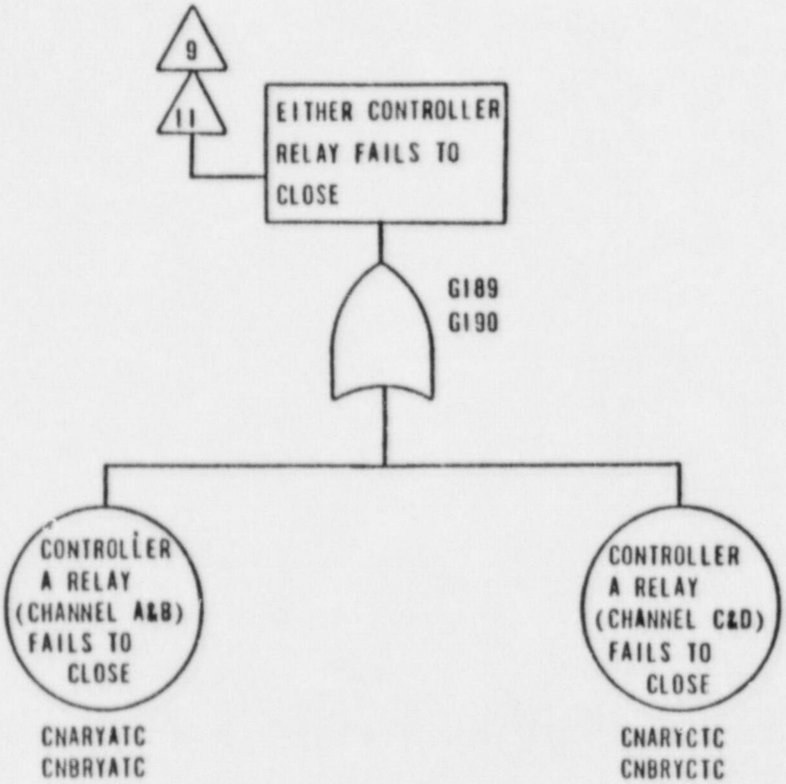

6
CV-Y2
FAILS TO OPEN
G168
CV-Y2
MECHANICALLY
FAILS TO
OPEN
CVY2ZZTO
DC POWER TO
VALVE FAILS
G169
DC POWER FAILS
17
BREAKER
ON BUSS
D01 FAILS
OPEN
BRD01ZFO

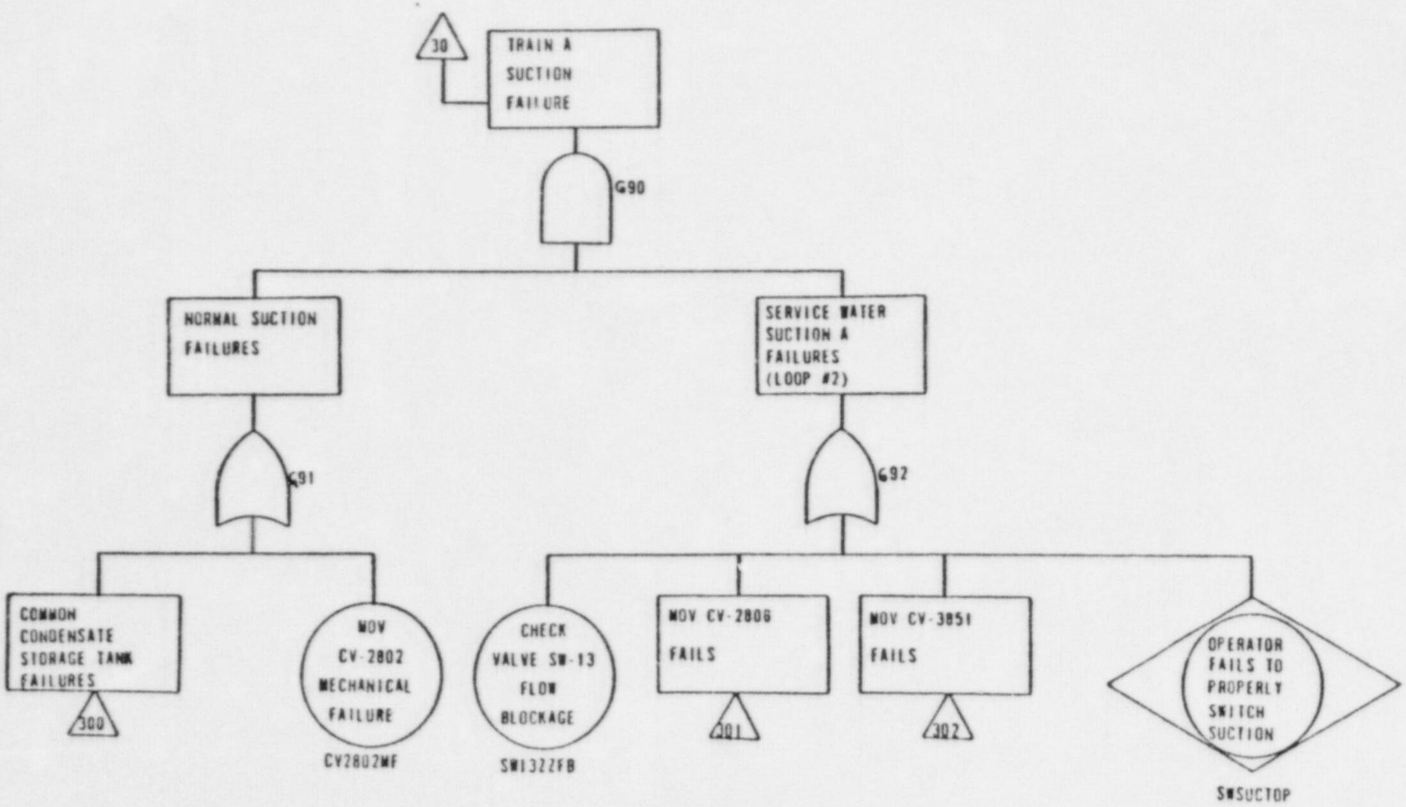

28
TURBINE STEAM VALVES FAIL TO OPEN (ACTUATION CIRCUIT)
G170
CHANNEL A VALVE CY-Y2 FAILS TO OPEN
CHANNEL B VALVE CY-Y1 FAILS TO OPEN
7
G171
VALVE RELAY OR SWITCH FAILS TO CLOSE
CVY2RYTC
14
TRIP CABINET A FAILURES
CONTROLLER A FAILURES
G172
G173
120V AC BUSS FAILS
BOTH CABINET RELAYS FAIL TO CLOSE AND OPERATOR CORRECTIVE ACTION FAILS
8
480V DC BUSS FAILS
EITHER CONTROLLER RELAY FAILS TO CLOSE
9
G174
G175
CABINET A BREAKER FAILS OPEN 120V AC
TCAMBRFO
INVERTER FAILS 120V AC CABINET A
TCAINZAM
DC POWER FAILS
17
MAIN CABINET BREAKER FAILS OPEN
CHAMBRFO
DC POWER FAILS
17


8
10
BOTH CABINET RELAYS FAIL TO CLOSE
G181
G182
RELAY A FAILS TO CLOSE
RELAY B FAILS TO CLOSE
G185
G186
G187
G188
RESISTOR SHORTS (RELAY A)
REARYASH
REBRYASH
BUFFER AMP FAILS OPEN (RELAY A)
BAARYAFO
BABRYAFO
RELAY OR SWITCH FAILS TO CLOSE (RELAY A)
RYARYATC
RYBRYATC
RESISTOR SHORTS (RELAY B)
REARYBSH
REBRYBSH
BUFFER AMP FAILS OPEN (RELAY B)
BAARYBFO
BABRYBFO
RELAY OR SWITCH FAILS TO CLOSE (RELAY B)
RYARYBTC
RYBRYBTC



CHANNEL B
CV-YI FAILS
TO OPEN
7
G176
VALVE
RELAY OR
SWITCH FAILS
TO CLOSE
CVYIRYTC
16
TRIP CABINET B
FAILURES
CONTROLLER B
FAILURES
G177
G178
120V AC BUSS
FAILS
BOTH CABINET RELAYS
FAIL TO CLOSE AND
OPERATOR CORRECTIVE
ACTION FAILS
10
480V DC
BUSS FAILS
EITHER CONTROLLER
RELAY FAILS TO
CLOSE
11
G179
G180
CABINET
B BREAKER
FAILS OPEN
120V AC
TCBMBRFO
INVERTER
FAILS
120V AC
CABINET B
TCBINZAM
DC POWER FAILS
18
MAIN
CABINET
BREAKER
FAILS OPEN
CNBMBRFO
DC POWER FAILS
19


9
11
EITHER CONTROLLER RELAY FAILS TO CLOSE
G189
G190
CONTROLLER A RELAY (CHANNEL A&B) FAILS TO CLOSE
CNARYATC
CNBRYATC
CONTROLLER A RELAY (CHANNEL C&D) FAILS TO CLOSE
CNARYCTC
CNBRYCTC


30
TRAIN A SUCTION FAILURE
G90
NORMAL SUCTION FAILURES
SERVICE WATER SUCTION A FAILURES (LOOP #2)
G91
G92
COMMON CONDENSATE STORAGE TANK FAILURES
300
MOV CV-2802 MECHANICAL FAILURE
CV2802MF
CHECK VALVE SW-13 FLOW BLOCKAGE
SW1322FB
MOV CV-2806 FAILS
301
MOV CV-3851 FAILS
302
OPERATOR FAILS TO PROPERLY SWITCH SUCTION
SWSUCTOP

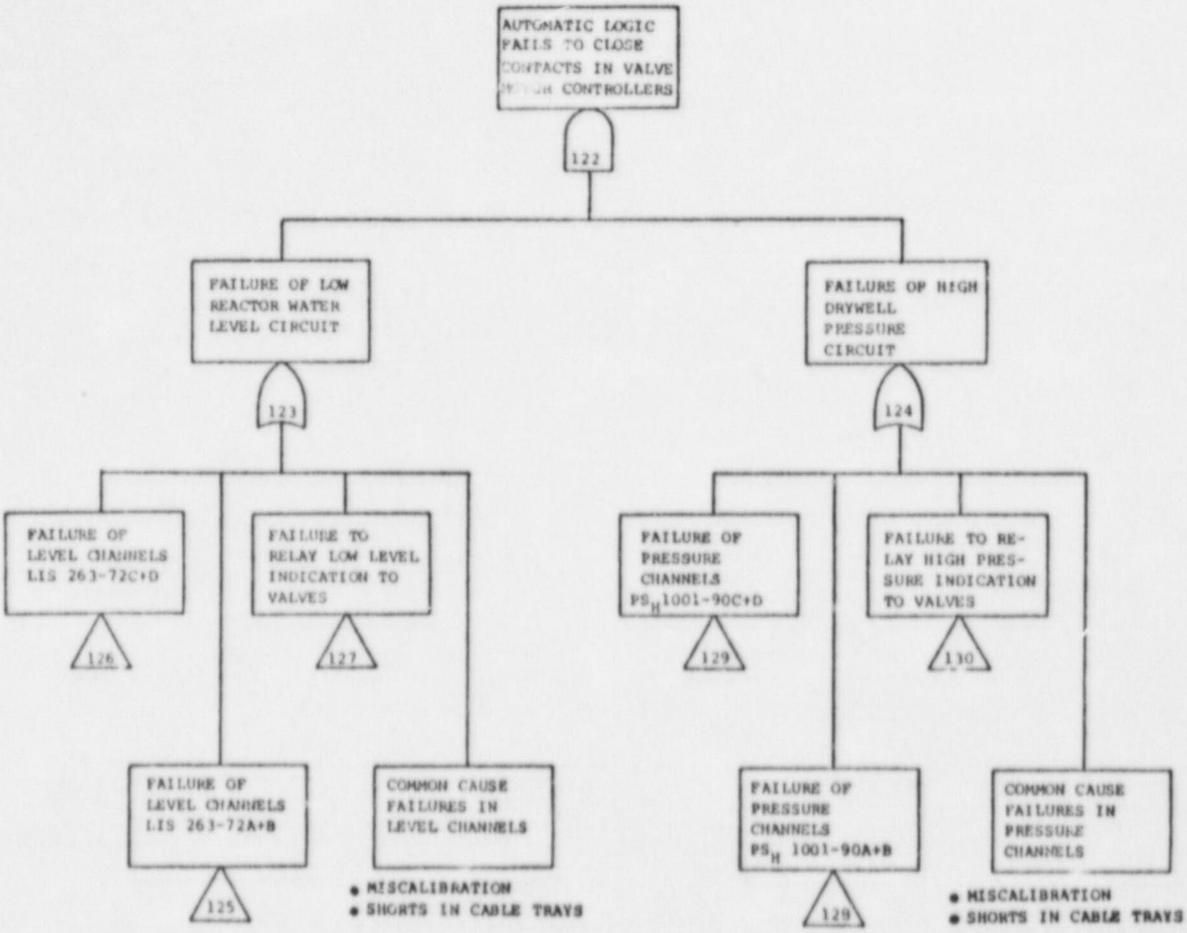
APPENDIX 3

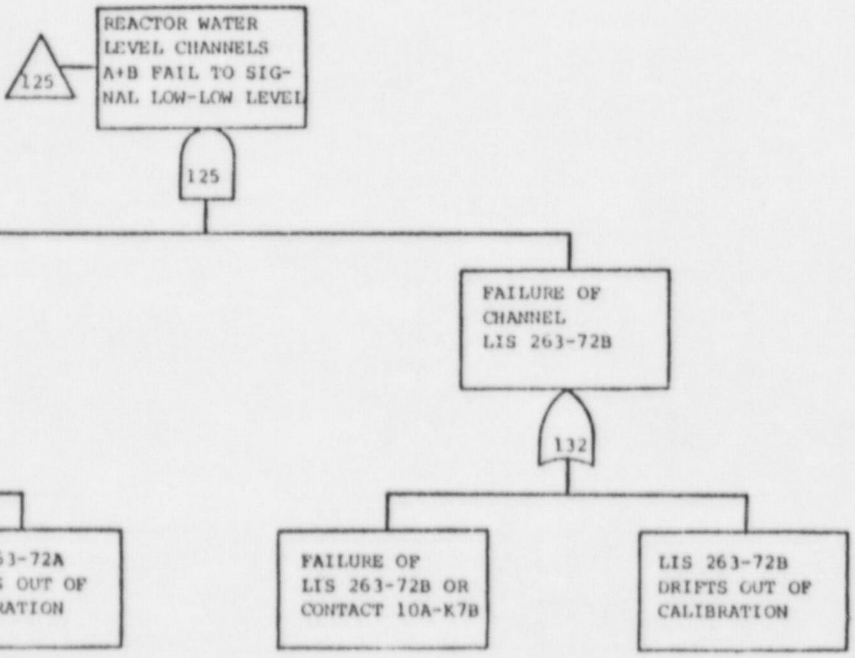
EFWS Double-Component Cut Sets

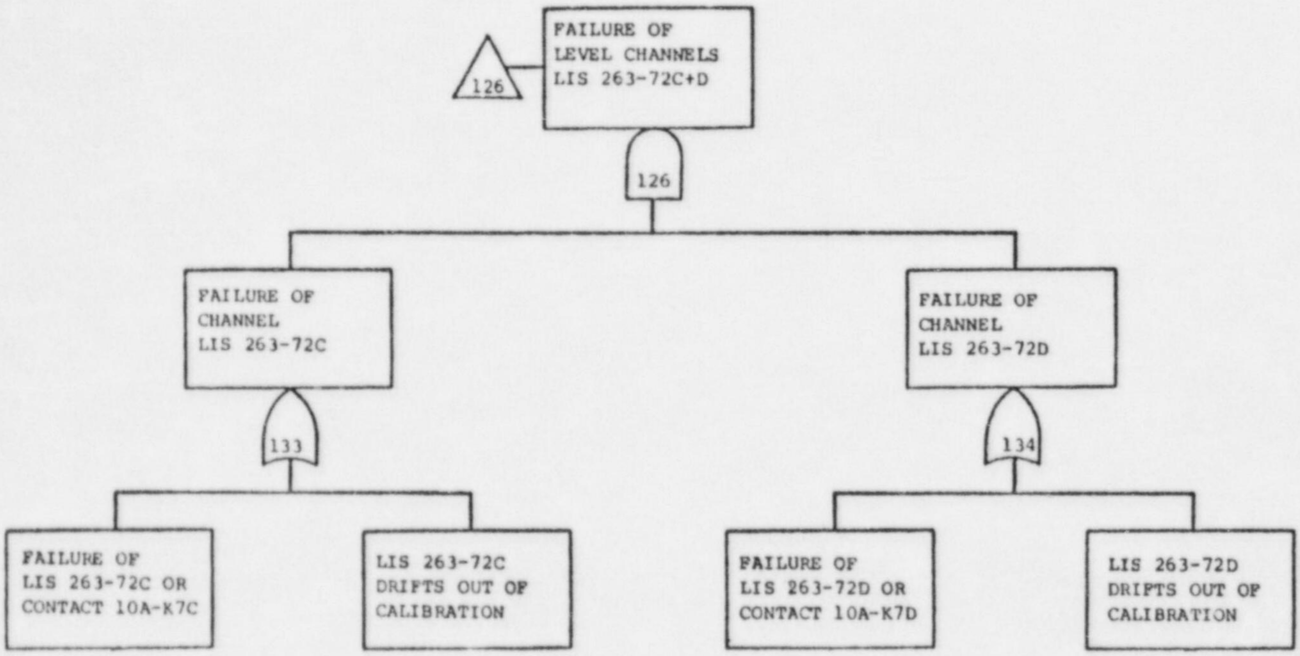
1. Flow blockage of check valves FW13A and FW13B.
2. Breaker BRP7B on pump P7B fails to open and mechanical failure of pump P7A.
3. Breaker BRP7B on pump P7B fails to open and flow blockage of check valve FW10B.
4. Mechanical failure of pump P7A and pump P7B.
5. Flow blockage of check valve FW10B and mechanical failure of pump P7A.
6. Flow blockage of check valve FW10A and mechanical failure of pump P7A.
7. Flow blockage of check valves FW10A and FW10B.
8. Cabinet A breaker TCAMBR and cabinet B breaker TCBMBR fail to open.
9. Cabinet A breaker TCAMBR fails to open and inverter TCBIN fails.
10. Inverter TCAIN fails and cabinet B breaker TCBMBR fails to open.
11. Inverter TCAIN and inverter TCBIN fail.
12. Breaker BRD11 and breaker BRD21 fail to open.
13. Motor operated valve CVX-4 fails to open and breaker BRD11 fails to open.
14. Motor generated valve CVX-1 fails to open and breaker BRD21 fails to open.
15. Motor operated valve CVX-1 and motor operated valve CVX-4 fail to open.
16. Breaker BRB61 and breaker BRB51 fails to open.
17. Motor operated valve CVX-3 fails to open and breaker BRB51 fails to open.
18. Motor operated valve CVX-2 fails to open and breaker BRB61 fails to open.
19. Motor operated valve CVX-3 and motor operated valve CVX-2 fail.

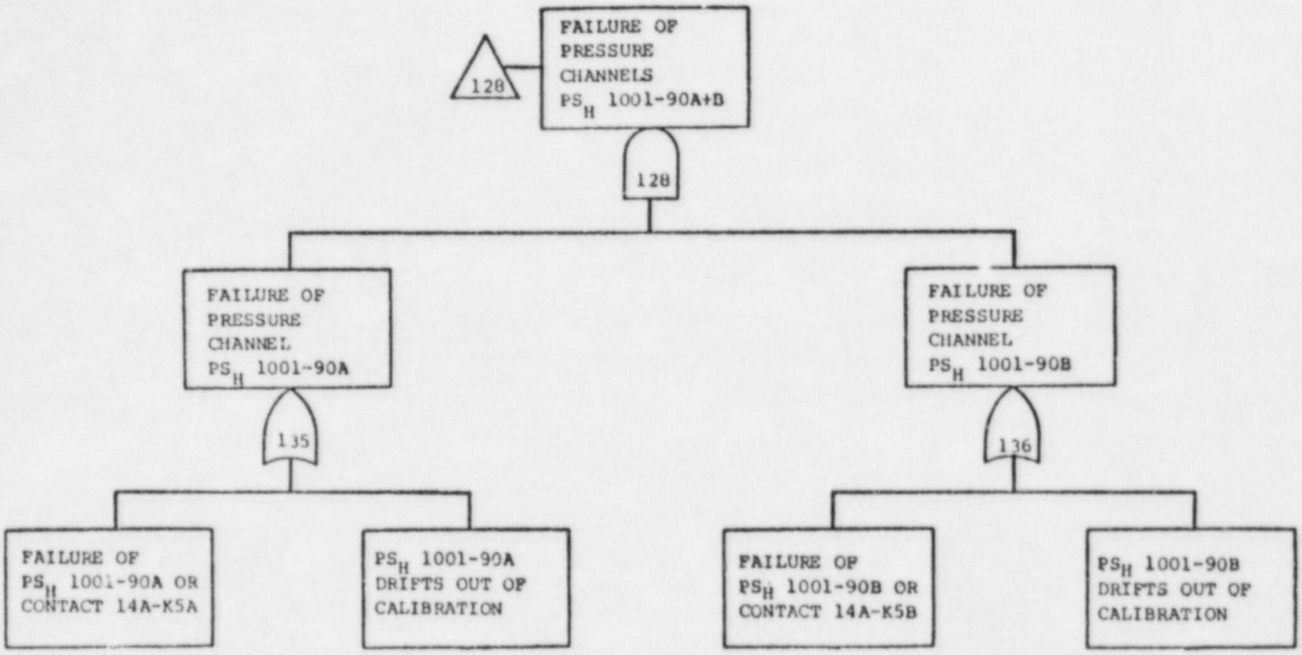
APPENDIX 4

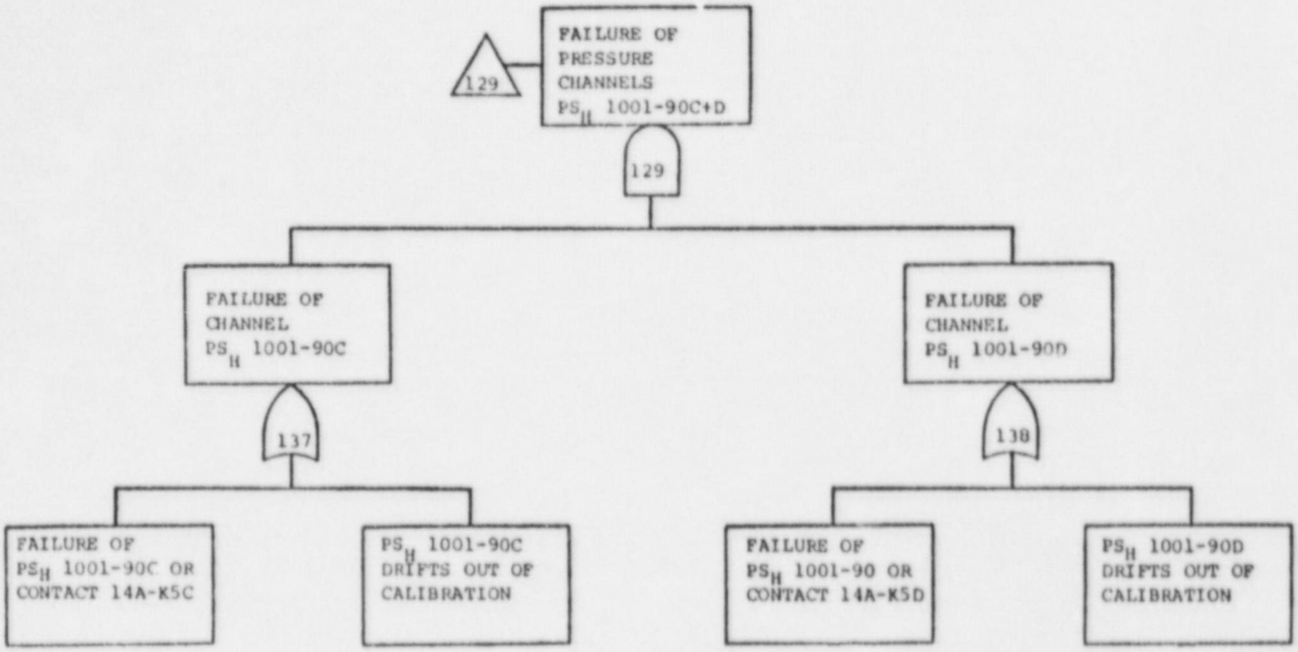
HPCI AUTOMATIC LOGIC FAULT TREE

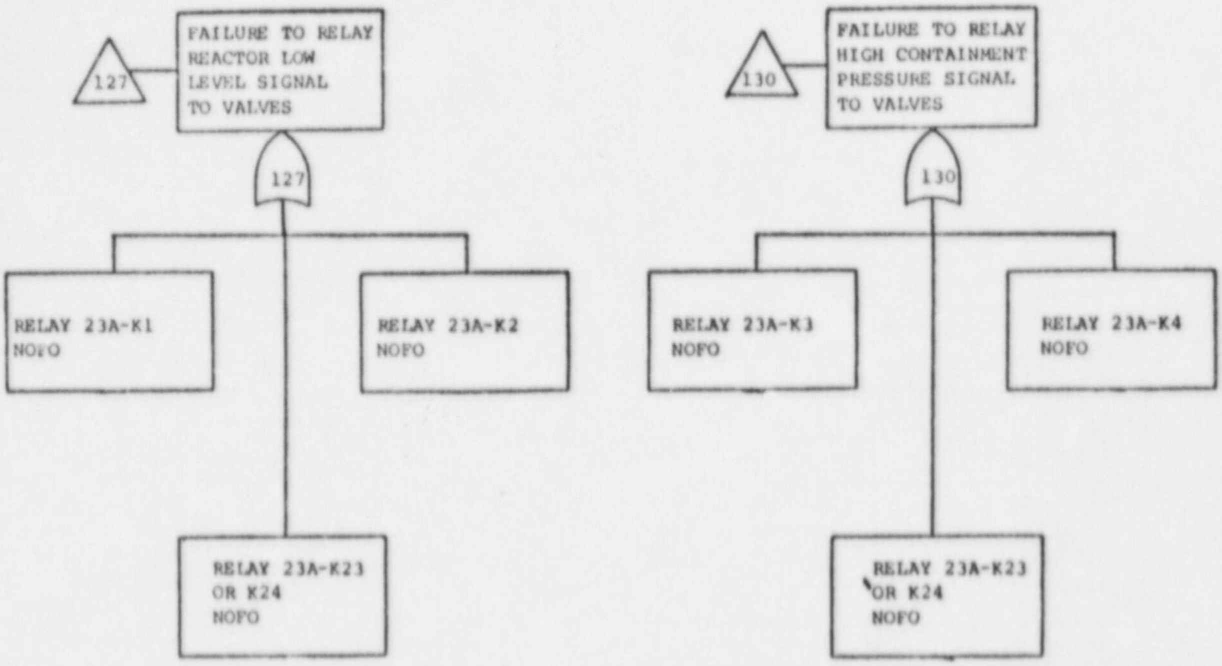

AUTOMATIC LOGIC FAILS TO CLOSE CONTACTS IN VALVE MOTOR CONTROLLERS
122
FAILURE OF LOW REACTOR WATER LEVEL CIRCUIT
FAILURE OF HIGH DRYWELL PRESSURE CIRCUIT
123
124
FAILURE OF LEVEL CHANNELS LIS 263-72C+D
126
FAILURE TO RELAY LOW LEVEL INDICATION TO VALVES
127
FAILURE OF PRESSURE CHANNELS PS$_H$1001-90C+D
129
FAILURE TO RELAY HIGH PRESSURE INDICATION TO VALVES
130
FAILURE OF LEVEL CHANNELS LIS 263-72A+B
125
COMMON CAUSE FAILURES IN LEVEL CHANNELS
• MISCALIBRATION
• SHORTS IN CABLE TRAYS
FAILURE OF PRESSURE CHANNELS PS$_H$ 1001-90A+B
129
COMMON CAUSE FAILURES IN PRESSURE CHANNELS
• MISCALIBRATION
• SHORTS IN CABLE TRAYS


REACTOR WATER LEVEL CHANNELS A+B FAIL TO SIGNAL LOW-LOW LEVEL
125
125
FAILURE OF CHANNEL LIS, 263-72A
131
FAILURE OF CHANNEL LIS 263-72B
132
FAILURE OF LIS 263-72A OR CONTACT 10A-K7A
LIS 263-72A DRIFTS OUT OF CALIBRATION
FAILURE OF LIS 263-72B OR CONTACT 10A-K7B
LIS 263-72B DRIFTS OUT OF CALIBRATION


126
FAILURE OF LEVEL CHANNELS LIS 263-72C+D
126
FAILURE OF CHANNEL LIS 263-72C
133
FAILURE OF CHANNEL LIS 263-72D
134
FAILURE OF LIS 263-72C OR CONTACT 10A-K7C
LIS 263-72C DRIFTS OUT OF CALIBRATION
FAILURE OF LIS 263-72D OR CONTACT 10A-K7D
LIS 263-72D DRIFTS OUT OF CALIBRATION


128
FAILURE OF PRESSURE CHANNELS PS$_H$ 1001-90A+B
128
FAILURE OF PRESSURE CHANNEL PS$_H$ 1001-90A
135
FAILURE OF PRESSURE CHANNEL PS$_H$ 1001-90B
136
FAILURE OF PS$_H$ 1001-90A OR CONTACT 14A-K5A
PS$_H$ 1001-90A DRIFTS OUT OF CALIBRATION
FAILURE OF PS$_H$ 1001-90B OR CONTACT 14A-K5B
PS$_H$ 1001-90B DRIFTS OUT OF CALIBRATION


129
FAILURE OF PRESSURE CHANNELS PS_H 1001-90C+D
129
FAILURE OF CHANNEL PS_H 1001-90C
FAILURE OF CHANNEL PS_H 1001-90D
137
138
FAILURE OF PS_H 1001-90C OR CONTACT 14A-K5C
PS_H 1001-90C DRIFTS OUT OF CALIBRATION
FAILURE OF PS_H 1001-90 OR CONTACT 14A-K5D
PS_H 1001-90D DRIFTS OUT OF CALIBRATION


FAILURE TO RELAY REACTOR LOW LEVEL SIGNAL TO VALVES
127
127
RELAY 23A-K1 NOFO
RELAY 23A-K2 NOFO
RELAY 23A-K23 OR K24 NOFO
FAILURE TO RELAY HIGH CONTAINMENT PRESSURE SIGNAL TO VALVES
130
130
RELAY 23A-K3 NOFO
RELAY 23A-K4 NOFO
RELAY 23A-K23 OR K24 NOFO

APPENDIX 5

HPCI INJECTION FUNCTION SINGLE COMPONENT CUT SETS

1 System down for repair of support equipment

2 Loss of 125 VDC Power from Bus D5

3 Loss of 125 VDC Power from Bus D8

4 Loss of 250 VDC Power from Bus D9

5 System unavailable due to initiation logic testing

6 23A-K23 or 23A-K24 (initiation seal-in relays) normally open, fails open

7 MOV 2301-3 (steam to turbine valve) normally closed, fails closed

8 MOV 2301-4 (inboard steam supply line isolation valve, AC operated), normally open, fails closed

9 Turbine driven pump failure

10 Steam turbine loss of function

11 Turbine lubrication system failure

12 HPCI room cooler failed and required

13 LOCA in HPCI steam supply line

14 2301-45 (steam discharge check valve) stuck closed

15 2301-74 (steam discharge manual valve) locked open, fails closed

16 Coolant discharge line rupture

17 AO 2301-7 (air operated testable check valve) fails stuck closed

18 MOV 2301-8 (pump discharge valve from MOV 2301-9) normally closed, fails closed

19 MOV 2301-9 (pump discharge valve) normally open, fails closed

20 MOV 2301-14 (minimum flow bypass to suppression chamber) normally open, fails open

21 Feedwater 57B line discharge isolation valve normally open, fails closed

22 Feedwater 58B line discharge check valve normally open, fails closed

23 Human error probability: failure to reset HPCI

24 Common cause failures in steam line low pressure sensors

25 Human error, common cause: miscalibration of high temperature sensors in steam line space

26 Human error, common cause: miscalibration of turbine trip sensors, a) pressure, 2) level

27 23A-28 (autoisolation initiation relay) normally open, fails closed

28 False signal indicates turbine overspeed

29 PSL 2360 (pump suction low pressure) false signal indicating low pressure caused by contacts failing shorted

30 23A-K17 (relays pump suction low pressure to turbine trip relay) false signal caused by contacts failing shorted

31 dPIS 2352 or 2353 (steam line differential pressure sensor) false signal indicating:

1) low range contacts failed shorted
2) high range contacts failed shorted
3) human error: calibration
4) transient steam flow

32 23A-K9/K36 (relays from differential pressure sensors to autoisolation circuit), primary, calibration and common cause failures

33 High turbine steam exhaust pressure false signal, due to:

PSh 2368A pressure switch: contacts fail shorted
PSh 2368B pressure switch: contacts fail shorted
(Note: these sensors are not tested directly)

34 23A-K12 (relay from steam line pressure sensors to turbine trip circuit) contacts fail shorted

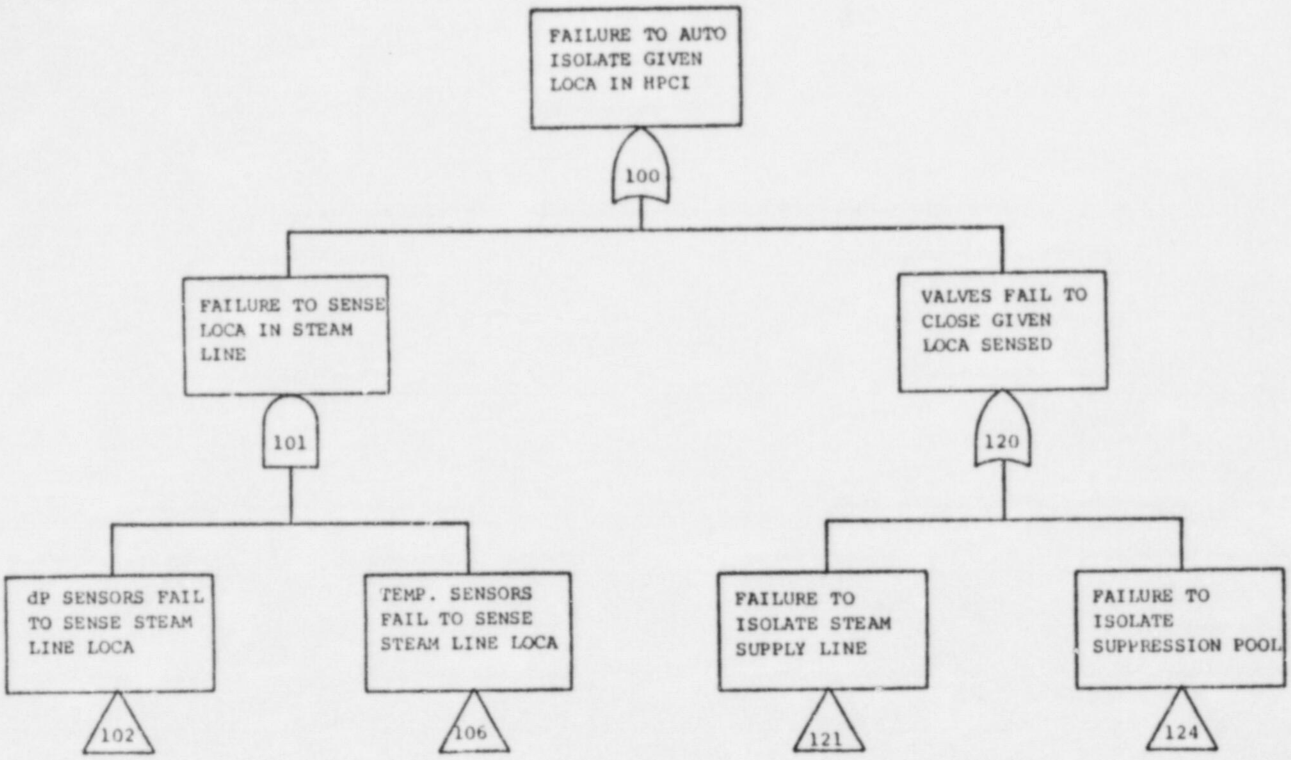
35 23A-K6/K34 (relays turbine/pump room temperature sensors to autoisolation circuit) primary, common cause, and calibration failures, normally open, fails closed

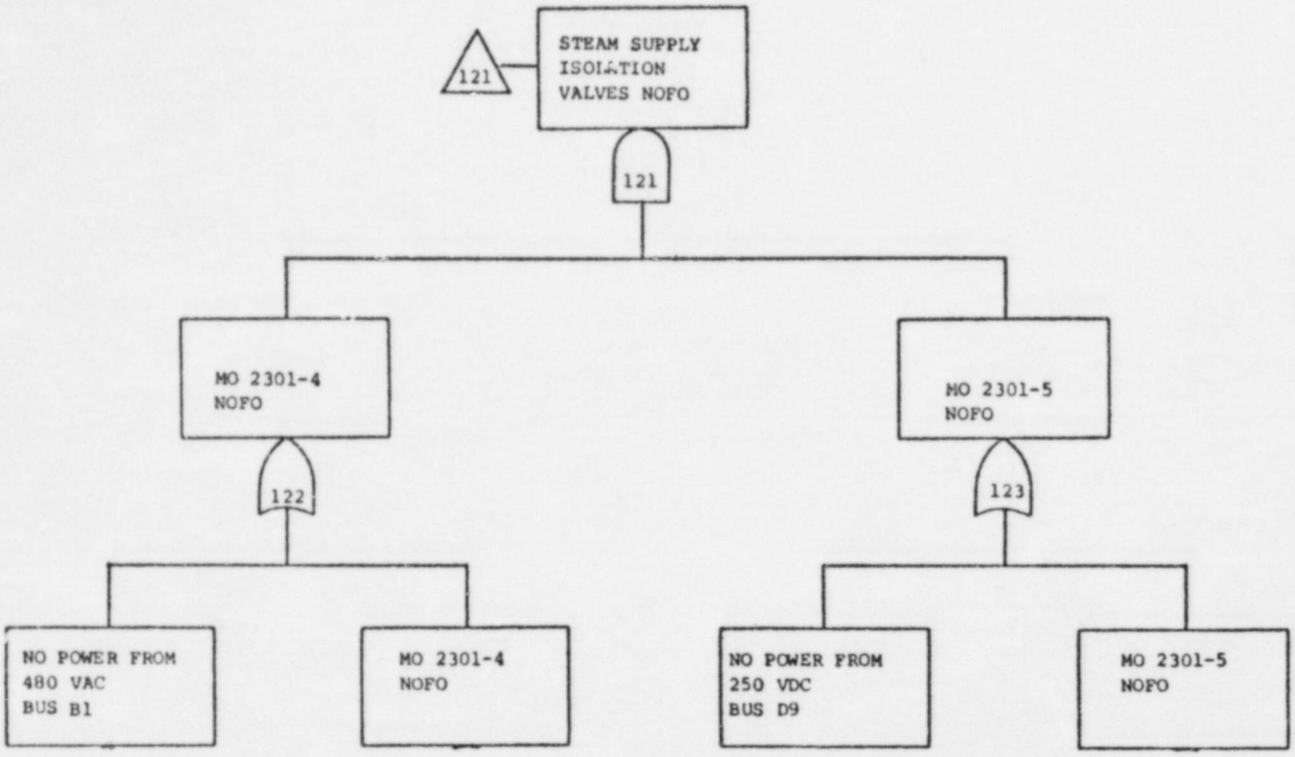
36 23A-K8/K35 NOFC (relays from valve station above 23 feet and torus compartment temperature sensors to autoisolation circuit) primary, common cause, and calibration failures

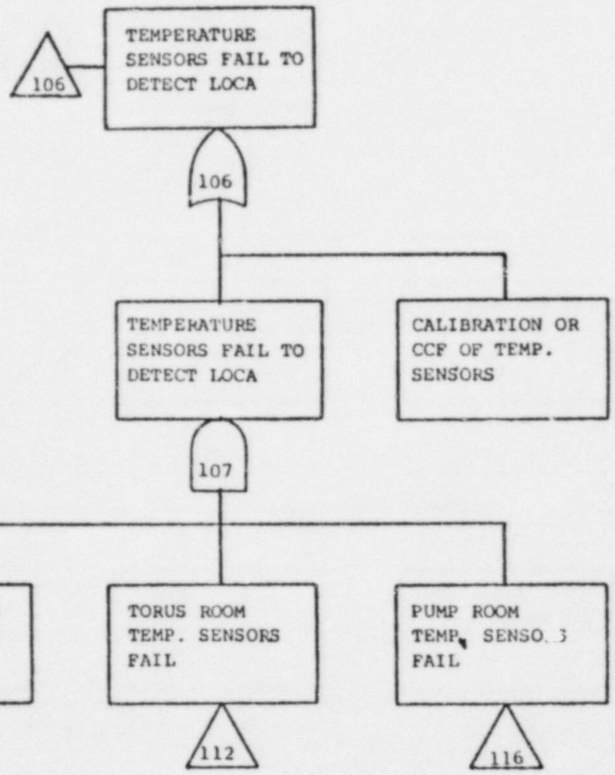
37 23A-K20 (relay indicating high turbine exhaust) fails shorted

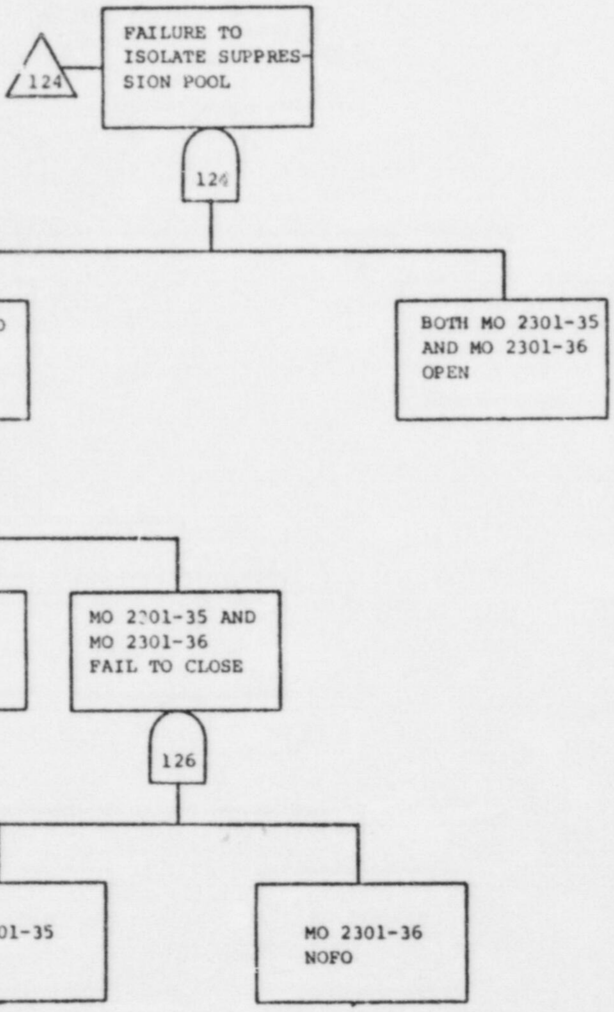
APPENDIX 6

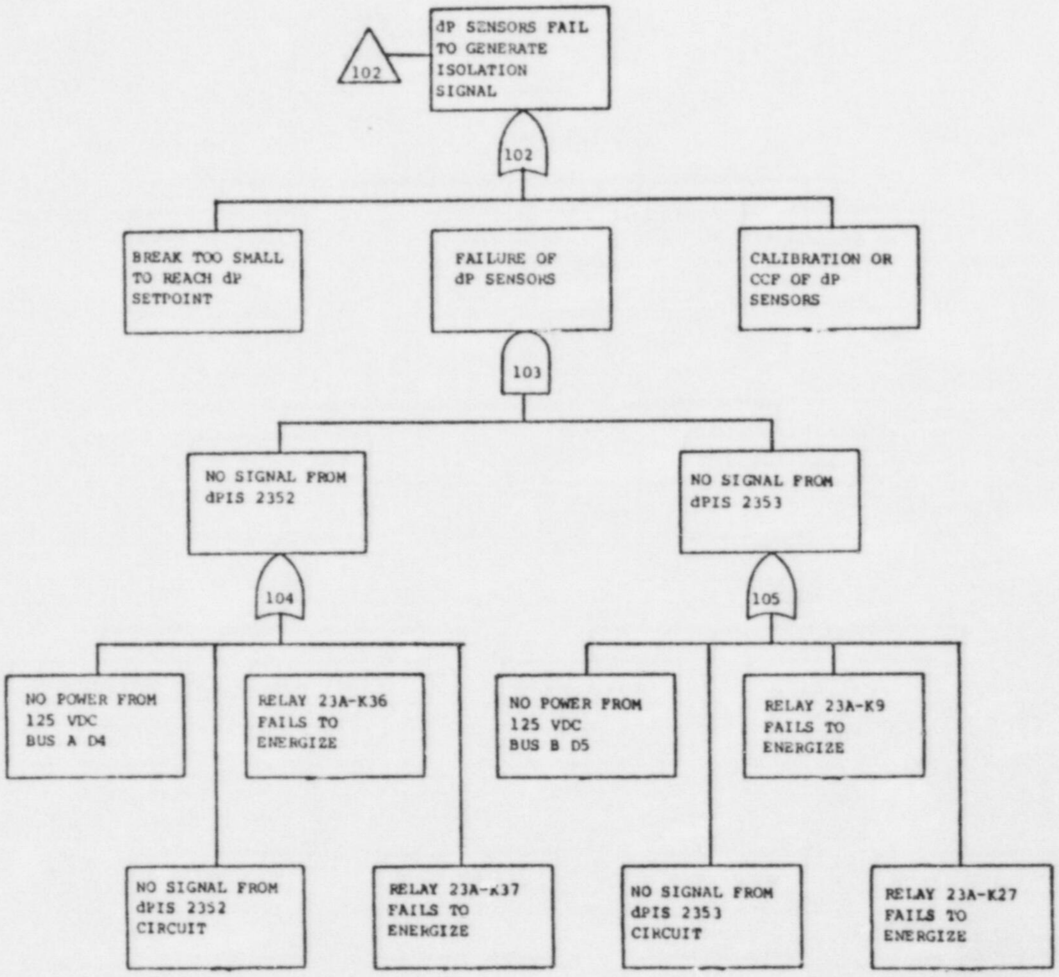
HPCI AUTOISOLATION FUNCTION FAULT TREE

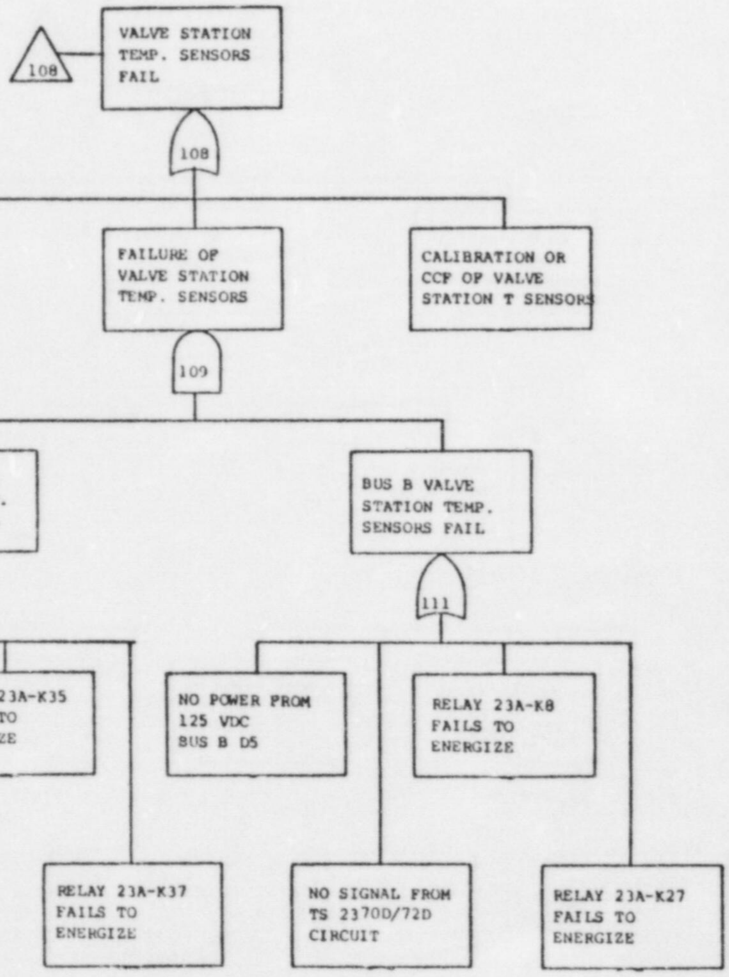

FAILURE TO AUTO ISOLATE GIVEN LOCA IN HPCI
100
FAILURE TO SENSE LOCA IN STEAM LINE
VALVES FAIL TO CLOSE GIVEN LOCA SENSED
101
120
dP SENSORS FAIL TO SENSE STEAM LINE LOCA
TEMP. SENSORS FAIL TO SENSE STEAM LINE LOCA
FAILURE TO ISOLATE STEAM SUPPLY LINE
FAILURE TO ISOLATE SUPPRESSION POOL
102
106
121
124

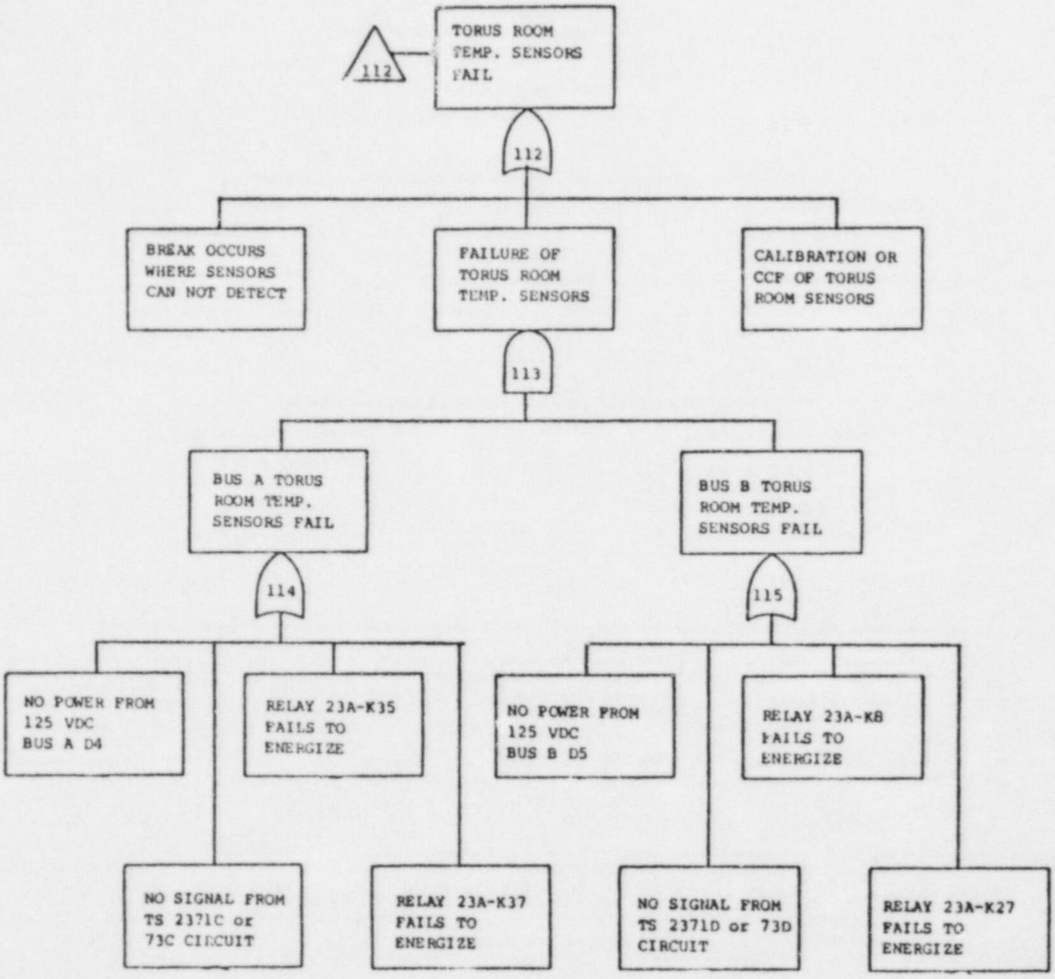

121
STEAM SUPPLY
ISOLATION
VALVES NOFO
121
MO 2301-4
NOFO
MO 2301-5
NOFO
122
123
NO POWER FROM
480 VAC
BUS B1
MO 2301-4
NOFO
NO POWER FROM
250 VDC
BUS D9
MO 2301-5
NOFO

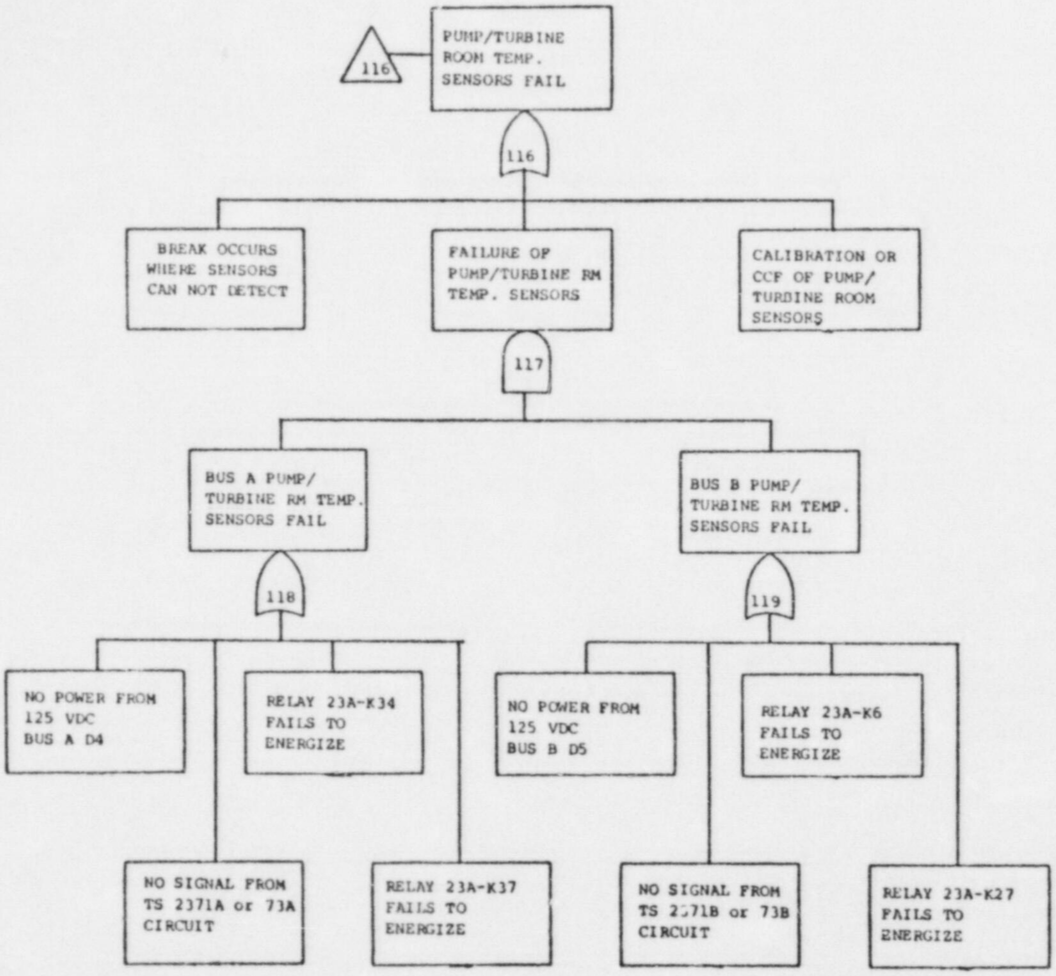

TEMPERATURE SENSORS FAIL TO DETECT LOCA
106
106
TEMPERATURE SENSORS FAIL TO DETECT LOCA
CALIBRATION OR CCF OF TEMP. SENSORS
107
VALVE STATION TEMP. SENSORS FAIL
TORUS ROOM TEMP. SENSORS FAIL
PUMP ROOM TEMP. SENSO.3 FAIL
108
112
116


124
FAILURE TO ISOLATE SUPPRESSION POOL
124
MO 2301-35 AND MO 2301-36 FAIL TO CLOSE
BOTH MO 2301-35 AND MO 2301-36 OPEN
125
NO POWER FROM 125 VDC BUS B D8
RELAY 23A-K28 FAILS TO ENERGIZE
MO 2201-35 AND MO 2301-36 FAIL TO CLOSE
126
MO 2301-35 NOFO
MO 2301-36 NOFO


102
dP SENSORS FAIL TO GENERATE ISOLATION SIGNAL
102
BREAK TOO SMALL TO REACH dP SETPOINT
FAILURE OF dP SENSORS
CALIBRATION OR CCF OF dP SENSORS
103
NO SIGNAL FROM dPIS 2352
NO SIGNAL FROM dPIS 2353
104
105
NO POWER FROM 125 VDC BUS A D4
RELAY 23A-K36 FAILS TO ENERGIZE
NO POWER FROM 125 VDC BUS B D5
RELAY 23A-K9 FAILS TO ENERGIZE
NO SIGNAL FROM dPIS 2352 CIRCUIT
RELAY 23A-K37 FAILS TO ENERGIZE
NO SIGNAL FROM dPIS 2353 CIRCUIT
RELAY 23A-K27 FAILS TO ENERGIZE


108
VALVE STATION TEMP. SENSORS FAIL
108
BREAK OCCURS WHERE SENSORS CAN NOT DETECT
FAILURE OF VALVE STATION TEMP. SENSORS
CALIBRATION OR CCF OF VALVE STATION T SENSORS
109
bUS A VALVE STATION TEMP. SENSORS FAIL
BUS B VALVE STATION TEMP. SENSORS FAIL
110
111
NO POWER FROM 125 VDC BUS A D4
RELAY 23A-K35 FAILS TO ENERGIZE
NO POWER FROM 125 VDC BUS B D5
RELAY 23A-K8 FAILS TO ENERGIZE
NO SIGNAL FROM TS 2370C/72C CIRCUIT
RELAY 23A-K37 FAILS TO ENERGIZE
NO SIGNAL FROM TS 2370D/72D CIRCUIT
RELAY 23A-K27 FAILS TO ENERGIZE


112
TORUS ROOM TEMP. SENSORS FAIL
112
BREAK OCCURS WHERE SENSORS CAN NOT DETECT
FAILURE OF TORUS ROOM TEMP. SENSORS
CALIBRATION OR CCF OF TORUS ROOM SENSORS
113
BUS A TORUS ROOM TEMP. SENSORS FAIL
BUS B TORUS ROOM TEMP. SENSORS FAIL
114
115
NO POWER FROM 125 VDC BUS A D4
RELAY 23A-K35 FAILS TO ENERGIZE
NO POWER FROM 125 VDC BUS B D5
RELAY 23A-K8 FAILS TO ENERGIZE
NO SIGNAL FROM TS 2371C or 73C CIRCUIT
RELAY 23A-K37 FAILS TO ENERGIZE
NO SIGNAL FROM TS 2371D or 73D CIRCUIT
RELAY 23A-K27 FAILS TO ENERGIZE


116
PUMP/TURBINE ROOM TEMP. SENSORS FAIL
116
BREAK OCCURS WHERE SENSORS CAN NOT DETECT
FAILURE OF PUMP/TURBINE RM TEMP. SENSORS
CALIBRATION OR CCF OF PUMP/ TURBINE ROOM SENSORS
117
BUS A PUMP/ TURBINE RM TEMP. SENSORS FAIL
BUS B PUMP/ TURBINE RM TEMP. SENSORS FAIL
118
119
NO POWER FROM 125 VDC BUS A D4
RELAY 23A-K34 FAILS TO ENERGIZE
NO SIGNAL FROM TS 2371A or 73A CIRCUIT
RELAY 23A-K37 FAILS TO ENERGIZE
NO POWER FROM 125 VDC BUS B D5
RELAY 23A-K6 FAILS TO ENERGIZE
NO SIGNAL FROM TS 2371B or 73B CIRCUIT
RELAY 23A-K27 FAILS TO ENERGIZE