archive

NUCLEAR PLANT RELIABILITY ANALYSIS

Optimization of Test Intervals for Standby Systems in Nuclear Power Plants

by
R. Karimi, N. C. Rasmussen
J. Schwartz & L. Wolf

Energy Laboratory Report No. MIT-EL 78-027
November, 1978

NUCLEAR PLANT RELIABILITY ANALYSIS

Optimization of Test Intervals for Standby Systems in Nuclear Power Plants

by

R. Karimi, N. C. Rasmussen,
J. Schwartz &
L. Wolf

Energy Laboratory
and
Department of Nuclear Engineering

Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Final Report for Research Project Sponsored by

Northeast Utilities Service Company
Public Service Electric and Gas Company
Yankee Atomic Electric Company

under the

M.I.T. Energy Laboratory Electric Utility Program
Energy Laboratory Report No. MIT-EL 78-027

November, 1978

ACKNOWLEDGEMENTS

This research work was started by Jim Schwartz who joined the Department in the summer of last year. His experience in this area helped us a lot to successfully start the reliability and availability calculations summarized in this report. Jim's patience in debugging and implementing computer codes paid off and we appreciate his efforts as well as those provided by Rachel Morton throughout the whole project period.

When Jim decided to leave the Department in January 1978 in order to join a vendor, we were fortunate enough to get Roy Karimi interested in this project. Roy overcame all the initial difficulties in a new area in a remarkably short period of time and his contributions have constituted the main part of the research summarized in this report.

To both gentlemen, we owe a great deal of gratitude for their efforts in achieving the goals of this research.

Finally, we would like to express our gratitude for the financial support as well as for the encouraging discussions with the sponsors of this project as part of the Nuclear Reactor Safety Research Program under the M.I.T. Energy Laboratory's Electric Utility Program.

Lothar Wolf
Norman C. Rasmussen
Principal Investigators

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This report Summarizes the research work performed under the project

"Nuclear Plant Reliability Analysis - Optimization of Test Intervals for Standby Systems in Nuclear Power Plants"

as outlined in the Agreement or Detailed Scope of Work as of November 21, 1977. The section numbers used below refer to those employed in this agreement.

1. Collection and Review of Available Information on Test Interval Optimization

An extensive literature review on analytical methods for test interval optimization has been performed and its results are reported. It has been found that analytical methods are only available for single component systems and a limited number of majority voting systems (k-out-of-n systems). This analysis of complex technical systems with these formulations is questionable, although they provide first estimates. Some of the equations found in the literature differ from others with respect to the extent of handling imperfect testing, test caused failures and the like. When these effects are included in the analysis, an explicit solution for the test interval is no longer possible even for a single component. At the end of this literature review it became quite apparent, that the analytical methods must be recognized as convenient guidance into this special area of reliability analysis. However, on the other hand, the limitation for practical work became also obvious, especially for systems of technical interest.

2. Review and Assessment of Technical Specification

The information supplied by the utilities has been reviewed. All efforts were concentrated upon subtask 2a, involving diesel generators.

3. Data Collection and Analysis of Diesel Generators

A literature review has been performed on diesel generator failures covering reports issued after the publication of WASH-1400. The data are listed in Appendix A which also summarizes the analysis and the comparison with the WASH-1400 results. For the purpose of this study a conservative set of data has been used consisting of the most conservative data found in either assessment. There are some indications, that the data unavailability upon demand of D.G.s may be lower by a factor of about 3.

5. Development of the Methodology for the Optimization of Test Intervals

Starting point of the development of a methodology was the optimization study of test intervals for a diesel generator unit by applying various strategies suggested by different authors. All of these methods were compared and recommendations given. Based on these findings a simplified Auxiliary Feedwater System as an example of a multi-component system was studied. The purpose of this study was primarily to answer the question whether optimum test intervals for single component systems can be equally well applied for multicomponent systems. Our results indicate that this is generally not the case. Under certain circumstances, lumping procedures may be found which make the single component formulation work, however, a much more reliable way to obtain the optimum test interval for complex systems is by using a computer code in an iterative manner. For this purpose, the NRC-code FRANTIC has been made operational at MIT and benchmarked against a variety of analytical and numerical codes. The results of this study indicate that FRANTIC is a useful engineering tool with a high degree of flexibility.

The tested code is available for the sponsors upon request.

6. Applications

The results obtained from the analytical procedures were compared to FRANTIC results for the Aux-Feed System. It was found that they do not necessarily agree. After the limitations of the analytical formulations have been detected, it was decided to perform all other optimization studies by using FRANTIC. These studies included the Emergency Power System, a blackout study and a special study concerning test caused failures and detection inefficiency.

Each of these studies addressed different aspects of test interval optimization which are given in full detail in the main report.

During the work various shortcomings of FRANTIC became apparent, among them

- the inconvenience for user to derive the system unavailability function rather than providing the fault tree as input
- the lack of the code to account for wearout
- the lack of any physical model behind test caused failures, detection inefficiencies, etc.
- the need for the propagation of uncertainties in the input data with proper account of possibly different distributions to the fault tree top event

Despite all of these drawbacks, it is felt that with the methodology developed during this project a technically sound basis and starting point are given for the utilities to enter the field of probabilistic system analysis in the near future.

1. INTRODUCTION

Engineered safety systems are standby systems. They are tested periodically to confirm that they are operational and then returned to the standby status. Although some failures of components in standby systems are self-annunciating, there are other unsafe failures that are not revealed until the next periodic test. The longer the interval between test, the higher the probability that a failure has occurred since the last test. On the other hand, testing the system too frequently may take it out of service too often or even wear it out prematurely both of which lead to increased unavailability.

To be meaningful, any reliability goal must be enforced throughout the lifetime of the nuclear power plant. As a result, these goals are of concern to the design engineer at the conceptual stage, as well as to the plant operator, who must demonstrate continued performance capability of systems.

The purpose of this research in the general subject of testing engineered safety systems and concentrates specifically on the following areas:

1. The time interval between tests as a design consideration;
2. Optimizing the availability by proper selection of the time interval between tests;
3. Adjusting the time interval between tests on the basis of field data on failure rates to assure conformance to an availability goal over the nuclear power plant lifetime.

Before any further reference is made to availability and unavailability, it seems to be appropriate to give their definitions as summarized in the IEEE - Standard [1]:

> Availability: The characteristic of an item expressed by the probability that it will be operational at a randomly selected future in time.
>
> Unavailability: The numerical complement of availability. Unavailability may occur as a result of the item being repaired or it may occur as a result of undetected malfunctions.

If records are maintained in an operating system, availability and unavailability may be simply determined from the following equations:

$$\text{Availability} = \frac{\text{Up Time}}{\text{Up Time} + \text{Down Time}}$$

$$\text{Unavailability} = \frac{\text{Down Time}}{\text{Up Time} + \text{Down Time}}$$

It should be noticed that both measures are actually time-dependent functions. However, it can be shown that after several cycles of testing and repair both, availability and unavailability approach a long-term asymptotic value which is time invariant. It is this time invariant value which is mostly used as an approximation for calculational purposes.

Some of the failures that occur in systems annunciate themselves, and any repair process may start immediately. However, in standby systems failures are not self-annunciating and can be discovered only by periodic testing. This way, the down time is a strong function of the test interval, test time as well as repair time. As a result, the test interval is one of the most important parameters that can be readily adjusted to parametrically study the predicted unavailability of a system. As will be shown later, it is also the test strategy among redundant systems which also plays a major role.

It should be recognized right from the outset, that although the test interval may be adjustable seemingly at will it is limited to the following constraints [1].

a) Wearout: The frequency of tests should be limited such that wearout does not become the dominant cause of failure.

b) Test Duration: If the system is out of service while undergoing a test, then the tests should not be done too frequently, since the unavailability due to testing may become as high or even higher than that due to random failures.

c) Fatigue: There is no incentive to test for failures due to fatigue if all the fatigue is induced by the tests themselves.

d) Judgement: The designer would do well to apply good judgement and not to design a system wherein an extremely short test interval is necessary or one wherein an extremely long test interval is allowed.

It is especially the last point which will be illuminated for typical standby systems of nuclear reactor power plant in what follows. Thus, it will be tried to quantify the engineering judgement related to test interval apportionments within the limitations set forth in the available analytical and computational tools.

It must be stressed that none of the analytical and computational procedures used in this study is able to simulate continuously distributed parameters. Therefore, questions related to wearout and fatigue cannot and will not be addressed in what follows. This is certainly one of the shortcomings encountered by using any method which is solely based upon system success or system failure and does not account for partial failure or degradation effects. Therefore, in areas or procedure where wearout effects may play an important role, engineering judgement is still needed in its qualitative capacity because it cannot be quantified. It is important to comprehend this limitation because at the same time it is the explanation for unresolved problems with respect to the results provided by this study.

Recently methods have been developed for determing test intervals for certain simple systems such as the "one-out-of-two" system, "two-out-of-three" system and "two-out-of-four" system [2]. The test interval for each component is such that the system will meet system availability goals assuming that unavailability due to failure equals that due to testing. These test intervals may not yield a minimum for system unavailability which is desirable.

The availability of a single component affects the overall system availability but it is not true that the optimum test interval for a single component is the same as the optimum test interval for that component when it is an integrated part of a complex system. The purpose of this study is to determine the optimum test interval for a system's components such that the system's unavailability is minimized.

The availability is a function of many parameters. One of the most general models was developed by Coleman and Abrams [3]. This model allows for imperfect testing, failure due to testing along with differentiating between test time and repair time. Jacobs [4] derived a very simple formula for calculating the optimum test interval for a single component. The methods of Hirsch, Jacobs, and Coleman and Abrams will be used to check the applicability of their methods for determining the optimum test intervals that minimize system availability.

For the purpose of calculating the pointwise and mean system unavailabilities as a function of the component test intervals the computer code, FRANTIC [5], will be used. This computer code has the capabilities of determining the system unavailability as a complex function of component parameters. The effect of staggering component tests is also a capability of the code.

2. REVIEW OF ANALYTICAL METHODS AND COMPUTATIONAL TOOLS FOR TEST INTERVAL OPTIMIZATION

2.1 Introduction

Many safety systems are standby systems. Therefore they remain idle during their expected lifetime. There is a certain possibility that the equipment, particularly passive components in these systems, may fail prior to demand and make the system inoperable. Critical standby systems, such as engineered safeguard systems in nuclear reactor plants, are therefore tested periodically to decrease the likelihood that the equipment will be unavailable upon demand.

If active components are tested frequently and maintained, it is reasonable to assume that their failure rate remains constant during the system mission time.

The following factors contribute to the system unavailability:

1) The possible existence of undetected failures for some period of time caused by either human or hardware related events;

2) The system downtime due to scheduled maintenance or testing.

Table 2.1 summarizes Vesely's [6] compilation of the relative contribution of the hardware, test and maintenance and human errors to the system unavailability. It should be noticed that the contributions listed in the individual columns do not add to 100% because failure causes, such as the combination of human errors and hardware fialures, are not included. As the table depicts, the various Engineered Safeguard Systems are

TABLE 2.1 Contribution to System Unavailability for Various Engineered Safeguard Systems [6]

System	Hardware	Test & Maintenance	Human
Low pressure recirculation system	14%		47%
Sodium hydroxide system		75%	18%
Safety injection control system	51%	38%	
Low pressure injection system	15%	20%	53%
Consequence limiting control system			91%
Containment leakage	65%		
Reactor protection	44%	33%	

subject to fairly different impacts upon their unavailabilities by the four contributors. Specifically, the sodium hydroxide system shows a remarkable sensitivity to test and maintenance procedures.

2.2 Mathematical Models

Neglecting the human error effects, availability model calculations fall into three general classifications depending upon the relative importance of the repair and test interval.

1) In case the mean time to repair is short compared to the test interval, it can be shown that the effect of the repair rate may be neglected. Thus, the availability calculation is solely based on failure rates and test intervals. This approximation may work well for systems which are tested manually once every week, for instance. For a single system, the availability, A, can be calculated from

$$A = \frac{T_2 - (\lambda T_2)(T_2/2)}{T_2} \qquad (2.1)$$

where T_2 is the average time per test interval and λ is the constant failure rate characteristic of the exponential distribution. Using the following assumptions

a) $\lambda T_2 << 1$

b) The system is known to be in a working state at the beginning of each test.

c) Every test interval has a test duration time of T_2.

d) Failure is only detected when the system is tested.

e) If a failure has been detected at the end of a test interval, the system is renewed either by repair or replacement.

Eq. (1) reduced to

$$A = 1 - \frac{\lambda T_2}{2} \qquad (2.2)$$

for the availability and gives for the unavailability

$$\bar{A} = \lambda \frac{T_2}{2} \qquad (2.3)$$

This approximation has been used for accounting for periodic testing in the Reactor Safety Study - WASH 1400 [7].

2) In case the mean time to repair is very long compared to T_2, the test interval may be neglected. Thus the availability calculation can be solely based upon the failure and repair rates. For this approximation, the availability and unavailability are given by

$$A = 1 - \lambda\tau_r \qquad (2.4)$$

and

$$\bar{A} = \lambda\tau_r \qquad (2.5)$$

respectively. The underlying assumption may be valid for systems which are automatically tested on a very short period. Here, τ_r is the mean time to repair. The approximation is valid provided $\lambda\tau_r << 1$ and the time-to-repair process is exponentially distributed.

3) For the situation where mean time to repair is of the same general order of magnitude as the test interval, the accurate determination of the availability becomes more difficult. By assuming that the time it will take to test and repair or renew the system is on the average τ_r and that failure cannot occur during testing, then the availability is given by

$$A = \frac{1 - e^{-\lambda T_2}}{\lambda(T_2 + \tau_r)} \qquad (2.6)$$

provided that the failure is exponentially distributed. From Eq. (2.6) the optimum test interval can be determined as

$$T_2 = \sqrt{\frac{2\tau_r}{\lambda}} \qquad (2.7)$$

Naturally, for systems consisting of several subsystems and components, the failure distribution is determined by the individual distributions as well as the logical interconnections between them.

Engineered Safeguard Systems most often work in some sort of redundancy for safety reasons. In redundant systems a failure can be detected only when the system is tested. This test can be conducted in either of two ways. During simultaneous testing all the components are tested consecutively whereas in staggered tests the components are tested at different times and as a result, the components or subsystems have been in operation for different times at any instant of time. It is obvious that by planning to test at certain times one can increase the availability of the system. The objective then is to estimate the availability of the system under a given policy and to select the best test interval and/or repair time according to some criterion. This approach is widely used and various aspects of it are discussed in [8]. Green and Bourne [9] give the unavailability for some redundant configurations due to undetected failures of the system for simultaneous and symmetrically staggered testing. Their results indicate that the unavailability is always greater or just equal for a uniformly staggered test than for a simultaneous test for any configuration.

The foregoing discussion was confined to estimate the effects of testing and renewal on the availability of the system. It should be noticed that these results may be used to choose T_2 and τ_r such that a predetermininé availability can be achieved. Hirsch [2] used the criterion that during testing and repair the unavailability of the system should be equal to its unavailability during normal operation. Presentation of other general models can be found in References [9-12]. A general model which allows for imperfect test distinction between testing time and repair time and failure during test was developed by Coleman and Abrams [3] who made the following assumptions:

a) The system fails according to the exponential distribution

b) Test is performed every T_2 units of time

c) Inspection takes T_c units of time

d) The probability that a failure will be detected is θ

e) The probability of a false alarm is α

f) Inspection introduces stresses on the system and the probability that the system will fail during the checkout period is β

g) The probability that the failure, which occurs during the checkout period, occurs before the actual testing is κ

h) If a failure is detected the duration of repair is on the average T_R

Under these assumptions the availability of the system is found to be

$$A = \frac{\theta(1 - e^{-\lambda T_2})}{\lambda(T_2+T_c)\{1+e^{-\lambda T_2}[\beta(1-\alpha+\alpha\kappa-\kappa\theta)-(1-\theta)]\}+\theta\lambda T_R[1-(1-\beta)(1-\alpha)e^{-\lambda T_2}]} \qquad (2.8)$$

In case that the system cannot fail during the test (β=0) and if no false alarm is possible (α=0), than A is given by

$$A = \frac{\theta(1 - e^{-\lambda T_2})}{\lambda(T_2+T_c)[1-e^{-\lambda T_2}(1-\theta)] + \theta\lambda T_R(1-e^{-\lambda T_2})} \qquad (2.9)$$

If in case the detection of failure is perfect, i.e. θ = 1, this equation reduces further to

$$A = \frac{1 - e^{-\lambda T_2}}{\lambda[T_2 + T_c + T_R(1 - e^{-\lambda T_2})]} \qquad (2.10)$$

which can be compared to Eq.(2.6). It turns out that both equations are similar with the exception that in Eq.(2.6) the test duration time and the repair time are lumped together into the constant τ_r whereas Eq.(2.10)treats these terms separately and the time for repair is additionally multiplied by the probability of the system being unavailable at the end of T_2.

2.3 General Review

It should be noticed that Eq. (2.8) seems to cover quite a broad spectrum of possible events during testing. Thus, it will serve as the starting point of the analytical efforts in the course of this research. However, it should be recognized that this model does not account for the effect of human errors and has not been extended yet to treat redundant systems. The former effect has been examined recently by Apostolakis and Bansal [13] who developed a set of equations for the commonly used redundant configurations by using the model of coupling of successive human actions as developed by Young and Conradi [14] for use in WASH-1400.

Dressler and Spindler [15,16] presented a self-consisting study concerning the effects of test and repair strategies on reactor safety for commonly used logic configurations. However, they neglected the impact of human error. Their results show that the effect of repair times on the mean unavailability is usually negligible for cold-standby systems which supports the approximation used in the aformentioned category 1.

Although the literature on reliability theory is filled with methods for optimally designing multi-component systems subject to various constraints, very little is indeed available on methods for optimally testing such systems. It is obvious that in terms of the unavailability of a single system there must exist a minimum as function of test frequency, test duration, failure and repair rate. The existence of this minimum has been demonstrated by Kontoleon et al. [17] who imposed additional cost constraints upon the system which was subject to both partial and catastrophic type of failures. Problems of this type call upon the use of the Markovian process, continuous in time with three discrete states. This approach was already used by Flehinger [12] who examined the effect of marginal testing in 1962.

If the system consists of several components, some components are probably tested more often than others because of their reliability, cost of testing, or importance in the system. Mastran [18] provides Bayesian decision rules for testing components sequentially to minimize the sum of the cost of testing.

Another approach is to minimize, for instance, the impact to the system unavailability by human error [13] or to divide the unavailability goal equally between the test interval and test duration [13]. The latter approach actually was devised by Hirsch [2]. It allows to calculate both the testing interval and the allowable repair time τ_r.

In summary, it is believed that the literature provides some interesting and promising concepts which can be used as starting points for the analytical search of optimal testing strategies provided that the quantities and their distributions which enter these formulations are known for the systems under consideration. In what follows advantage will be taken of these formulations for the present study.

2.4 Jacobs' Solution to the Test Interval Optimization

2.4.1 Formulation

Jacob's [4] solution procedure start out by considering one cycle of test interval as shown in Fig. 2.1.

The availability of the system is defined as the probability that the system is operational at any future time. The probability that the system is up can be given in terms of conditional probabilities as

$$P(S) = P(S|A)\ P(A) + P(S|B)\ P(B) \qquad (2.11)$$

where

$P(S)$: probability that the system is operational

$P(S|A)$: conditional probability that the system is up, given that the random point in future time falls into the time domain designated as A

$P(A)$: probability that the random point in future time falls into A

$P(S|B)$: conditional probability that the system is up, given that the random point in future time falls into the time domain designated as B

$P(B)$: probability that the random point in future time falls into B

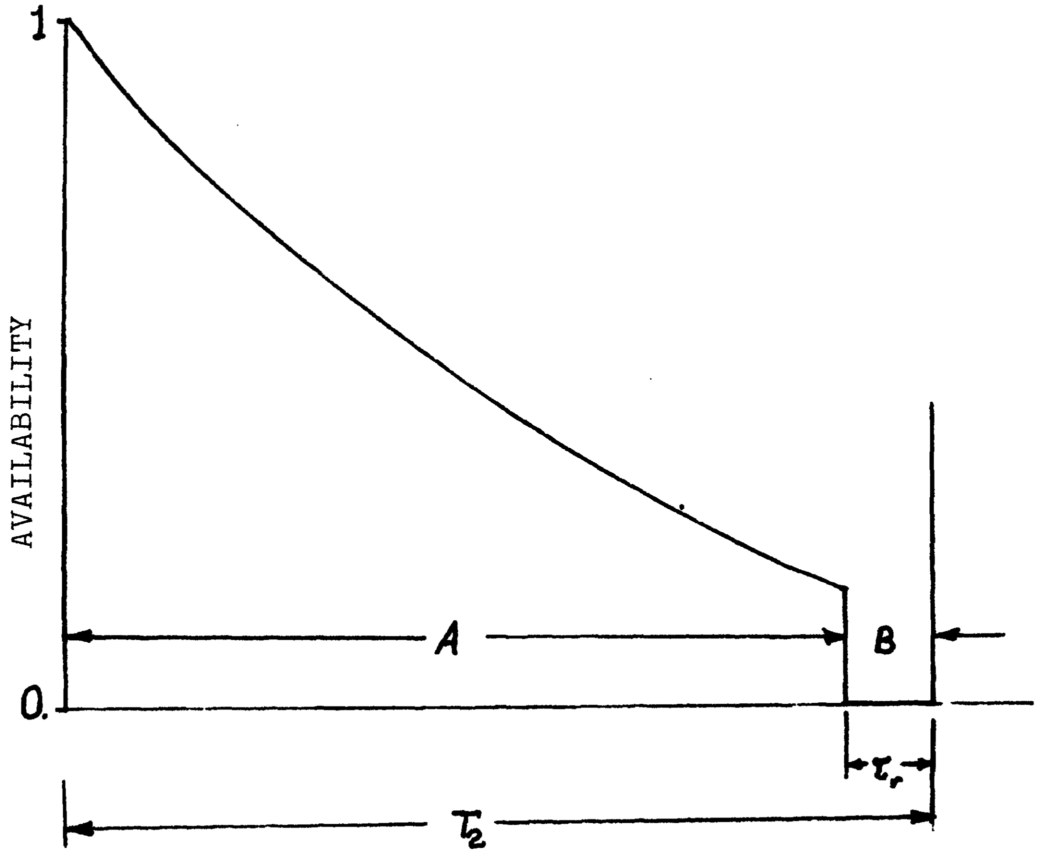


Figure 2.1: One Cycle of Test Interval

It is apparent from the foregoing discussion, that P(S|B) is zero because the system is known to be completely inoperative during test, i.e.

$$P(S|B) = 0 \qquad (2.12)$$

P(A) can be derived as

$$P(A) = \frac{T_2-\tau_r}{T_2} \qquad (2.13)$$

because all times are equally probable.

P(S|A) is taken to be the average reliability over the interval, i.e.

$$P(S|A) = \frac{1}{\lambda(T_2-\tau_r)}\int_0^{T_2-\tau_r} e^{-\lambda x}dx \qquad (2.14)$$

which yields

$$P(S|A) = \frac{1}{\lambda(T_2-\tau_r)}[1-e^{-\lambda(T_2-\tau_r)}] \qquad (2.15)$$

after substituting Eqs. (2.12), (2.13) and (2.15) into Eq. (2.11) one obtains for P(S)

$$P(S) = \frac{1}{\lambda\tau_r}[1-e^{-\lambda(T_2 - \tau_r)}] \qquad (2.16)$$

As a result, the availability of the system is a function of the three parameters λ, T_2, and τ_r.

2.4.2 Test Interval Optimization

In order to derive analytically the optimum τ, one has to assume that the other two parameters, λ and t are known and fixed constants of the system. Then, by differentiating Eq. (2.16) with respect to T_2 and by setting this equal to zero, one obtains

$$\frac{dP(S)}{\partial T_2} = \frac{1}{\lambda T_2^2}\left[e^{-\lambda(T_2 - \tau_r)}(1 + \lambda T_2)\right] - \frac{1}{\lambda T_2} = 0 \quad (2.17)$$

which is a transcendental equation not readily solvable in an explicit manner for T_2. However, Eq. (2.17) can be brought into the following form

$$\bar{e}^{\lambda T_2} + \lambda T_2 \bar{e}^{\lambda T_2} = \bar{e}^{\lambda \tau_r} \quad (2.18)$$

which is an exact equivalent of Eq. (2.17). Eq. (2.18) can be solved explicity for T_2 if the exponential terms are approximated by

$$e^{x} = 1 + x - \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \quad (2.19)$$

By neglecting terms higher than second order yields

$$T_2^2 = 2\tau_r\left(\frac{1}{\lambda} - \frac{\tau_r}{2}\right) \quad (2.20)$$

Generally, $\frac{1}{\lambda} >> t$, so that with little error

$$T_2 = \sqrt{\frac{2\tau_r}{\lambda}} \quad (2.21)$$

With respect to the various approximations introduced into the last equations, Eq. (2.21) is an approximate solution for T_2. The λT_r vs. λT_2 curve derived from Eq. (2.21) and labeled "Approximate Solution" is compared to the "Exact Solution" in Fig. 2.2. As can be seen it compares very favorably to the latter as long as $\lambda T_2<0.1$. For λT_2 = al the error amounts to 6.7% However, for most technical problems and their respective values for λ, T_r and T_2 the approximate solution for T_2 given by Eq. (2.21) can be considered adequate.

2.5 Discussion of Jacobs' Result

As already indicated in the introduction, Jacobs' result applies directly to any nonredundant system. However, as Jacobs noticed, the result can be used euqally well to any redundant system in which the level of redundancy is reduced during the test. If for instance in a one-out-of-two system, one channel is bypassed for test, it becomes a 1-out-of-1 system, and safety is impaired for the test duration. The availability is highest when the availability of each channel in any 1-out-of-n system is the highest, such that the results can be applied to each independently.

It should be noticed however, that for a majority logic, for instance a 2-out-of-3 system, the test usually results in a 1-out-of-2 system for which the Eq.(2.11)does not apply. With the solution of Eq.(2.11)on hand, it must be recognized that it

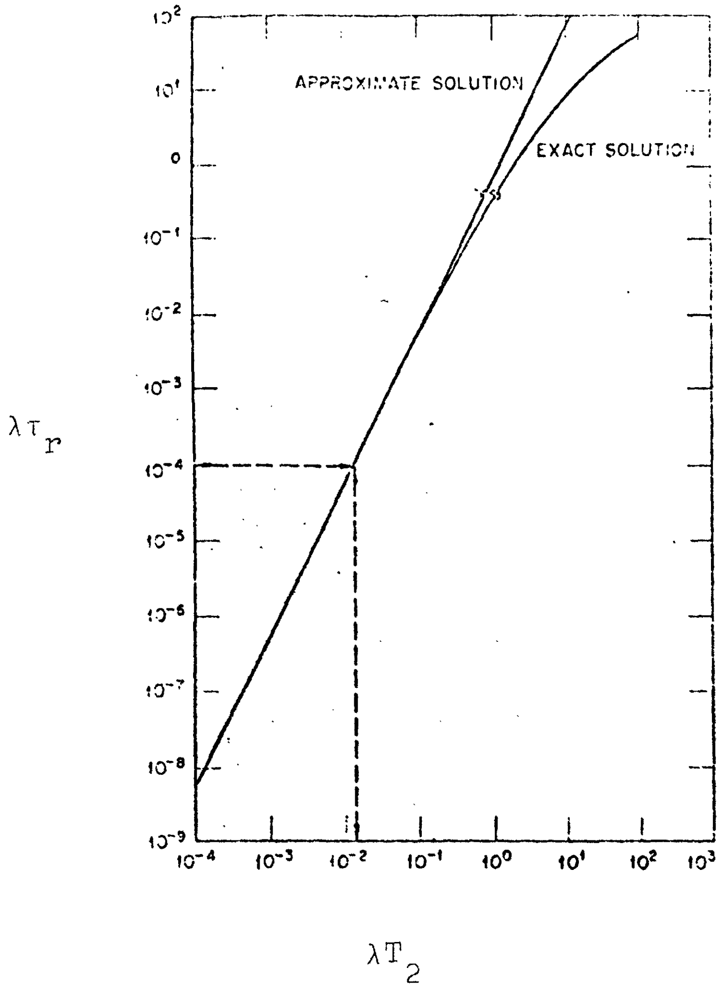


Figure 2.2: Plot of $\lambda \tau_r$ vs. λT_2

is not conservative to formulate the test interval on the assumption of a higher than expected failure rate. Moreover, once this test interval is properly formulated, it is not conservative to test more frequently. These are the most important conclusions which result from the study so far.

Fig. 2.3 illustrates the effect of testing on system availability. In the upper part, a, of the figure, the system is tested once each τ_1 hours as compared to the lower part, b, of the figure, where the system is tested every τ_2 hours, with $\tau_2 < \tau_1$. The test requires t hours where the system is rendered inoperable. Furthermore, it is assumed that the system may fail with a constant failure rate, λ and the availability is perfect (unity) immediately following a test but decreases exponentially until the next test. For the duration of the test, the availability is essentially zero (unavailability is unity).

By comparing both parts of Fig. 2.3, it becomes apparent that in part b the availability degrades along the same curve as in part a due to the same failure rate assumption. However, due to the shorter test interval the curve does not reach as low a level as in part a.

Under the extreme condition, that the interval between tests is decreased until it is equal to the testing time, τ_r, the system would be on test all the time and its availability would be clearly zero. On the other hand, if the interval between the tests is made extremely long, the system would degrade down

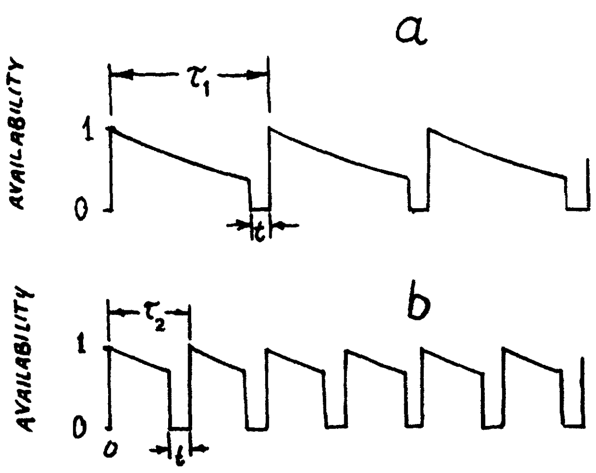


Figure 2.3: Effect of Test Interval on Availability

to a very low level of availability. Intuitively then, it can be expected that there may be a test interval that is optimum for a given system failure rate, characteristic of the whole system, and test duration that maximizes availability thereby minimizing unavailability.

Finally, it must be pointed out that the aforementioned ideas are only valid for a system which can be treated as one component characterized by a constant failure rate, constant testing time and where applicable constant repair rate. However, most technical systems and especially engineered safety systems are multi-component systems and are characterized by redundancy. Most of these components may display failure rates, test times and repair rates ranging over a broad spectrum. Under these circumstances, the considerations performed above do not hold, and it should be recognized that there is no analytical procedure available to optimize multi-component system availability

As a result and in view of the goals of this research, two conclusions can be drawn

a) If there are sufficient data available which allow to characterize uniquely a total system, without breaking it down to sub-system or even component levels, then, analytical procedures exist which allow the determination of an optimum test interval.

b) No analytical procedure for test interval optimization exist for systems which are characterized by redundancy and sub-systems or components whose reliability parameters vary over a broad range, and when no sufficient data base exists to characterize those systems uniquely by failure rate, testing time, test interval and repair rate. Under these circumstances complicated computer codes must be used on a trial-and-error basis.

Accordingly, this research has to focus on both approaches.

2.6 Fault Tree Analysis and Evaluation

Because use will be made of the features of the fault tree analysis later in this report it seems to be appropriate here to outline some of its underlying principles.

Fault tree analysis is a formalized deductive analysis technique that provides a systematic approach to investigating the possible modes of occurrence of a defined system state or undesired event.

Undesired events are identified either by inductive analysis as a preliminary hazard analysis or as a failure mode and effect analysis.

The events are usually undesired system states that can occur as a result of sub-system functional faults.

Fault tree analysis consists of two major steps:

1) The construction of the fault tree.
2) The evaluation of the fault tree.

It should be noticed that the evaluation of the fault tree can be qualitative, quantitative, or both depending upon the scope and extent of the analysis. This study calls for a qualitative and quantitative analysis with major emphasis on the latter.

The objectives of a fault tree analysis are:

a) To identify systematically all possible occurrence of a given undesired event.

b) To provide a clear and graphical record of the analytical process.

c) To construct a baseline for the evaluation of design and procedural alternatives.

2.6.1 Fault Tree Construction

The construction of the fault tree necessitates a thorough understanding of the system. The undesired event, called the "top event" must be carefully defined. Furthermore, the limit of resolution should be stated, potential system interfaces identified and constraints of the analysis realized.

A fault tree is a deductive logic model that graphically displays the various combinations of possible events, both fault and normal occurring in a system that lead to the top event. The term "event" denotes a dynamic change of state that occurs to a system element. If the change of state is such that the intended function of the particular element is not achieved or an unintended function is achieved, the event is an abnormal system function of fault event.

Fault events may be classified according to two types:

1) A system element fails to perform an intended function.

2) A system element performs an inadvertant function.

System elements include hardware, software, human and environmental conditions.

In order to apply Boolean logic in fault tree analysis, the outcome of each event must exhibit two states only, the OFF state and the ON state. This limits the application of fault tree analysis to two-state systems. In fact multi-valued state systems are difficult to handle with this technique.

More details about fault tree analysis can be found in special reports such as for instance Vesely [19].

2.6.2 Evaluation of the Fault Tree

In view of the fact that the FRANTIC code is used in this study, the fault tree will be qualitatively specified by a system unavailability function which is input to the code as described in the next section. The evaluation of the tree, specifically the occurrence of the top event will use the time-dependent methodology which forms the mathematical basis of FRANTIC.

2.7 Computational Tool - The FRANTIC Code

2.7.1 Introduction

The FRANTIC computer code [5] evaluates the point and mean unavailabilities for any general system model. Non-repairable components, monitored components, and periodically tested components are handled. This flexibility together with the fact that FRANTIC has been devised and tested by NRC led to the selection of this code as the appropriate computational tool for this analysis. One of the more unique features of FRANTIC is the detailed, time dependent modeling of periodic testing which includes the effects of test downtimes, test overrides, detection inefficiencies, and test-caused failures. With regard to these features, FRANTIC has to be considered the most flexible tool in engineering unavailability analysis. The exponential distribution is used for the component failures and equations are developed for the testing and repair contributions. In addition, human errors and common mode failures can be included by assigning an appropriate constant probability for these contributions.

It should be noticed, that in order to accommodate the various processes, FRANTIC uses a variety of mathematical approximations all of which add to the conservative character of the calculations.

The only real drawback of FRANTIC is that it needs the system unavailability equation of the system under consideration as input. This formula expresses the system unavailability in terms of the component unavailabilities and is obtained either from a block diagram, event tree, or fault tree by using standard Boolean techniques. This requires a certain in-depth knowledge of these methods by the user. The functions needed for the systems studied for this analysis were derived from the respective fault trees of the systems. These trees will be discussed in detail in the following chapters.

2.7.2 Summary of Mathematical Models for Various Types of Components Handled by FRANTIC

Four types of components are handled by the FRANTIC code:

1) Constant unavailability components
2) Non-repairable components
3) Monitored components
4) Periodically tested components

In what follows, the unavailability equations as used by the code are summarized:

1) Constant Unavailability Components

By definition, a constant unavailability component is characterized by a per demand (or per cycle) unavailability which is independent of time, i.e.

$$q = q_d \qquad (2.22)$$

2) Non-repairable Components

A non-repairable component is one, if it fails, is not repaired during plant operation

$$q(t) = 1 - \bar{e}^{\lambda t} \qquad (2.23)$$

$$q(t) = \lambda t$$

where λ is the constant component failure rate.

3) Monitored Components

A monitored component is one for which the failure is immediately detected and repair is then begun. The detection device can be any kind of signal

$$q = \frac{\lambda T_R}{1+\lambda T_R} \approx \lambda T_R \qquad (2.24)$$

where T_R is the average (detection plus repair) time.

4) Periodically Tested Components

A periodically tested component is one for which tests are performed at regular intervals. The failure of the component is not detectable until the test is performed. For this type of component, one has to account for the following contributions:

a) Between test contribution:

$$q(t) = \lambda(t - T_c) \text{ for } T_c<T<T_2 \qquad (2.25)$$

b) Test contribution:

$$q_1 = P_f + (1 - P_f)\, q_o + (1 - P_f)\, (1 - q_o)Q \qquad (2.26)$$

c) Repair contribution:

$$q_2 = P_f + (1 - P_f)\, Q + (1 - P_f)\, (1 - Q)\, 1/2\, \lambda T_R \qquad (2.27)$$

where

t = the time from the preceding test

T_2 = Test interval

T_c = test period

T_R = Repair period

P_f = Probability of test-caused failure

Q = $\lambda\, (T_2 - T_c)$ = between test failure probability

q_o = test override unavailability

For the first test interval T_1, the between test contribution is modified to $q(t) = \lambda t$ and Q changes to λT_1. In case of periodic detection inefficiencies, λ gets modified to $\lambda\,(1 - p)$ and an undetected contribution q' is added, with $q' = \lambda pt$.

It should also be noticed, that human error and common mode contributions can be handled. This is usually done by using $q = q_d$

Fig. 2.4 illustrates the instantaneous unavailability benavior as generated by FRANTIC with all three contributions included.

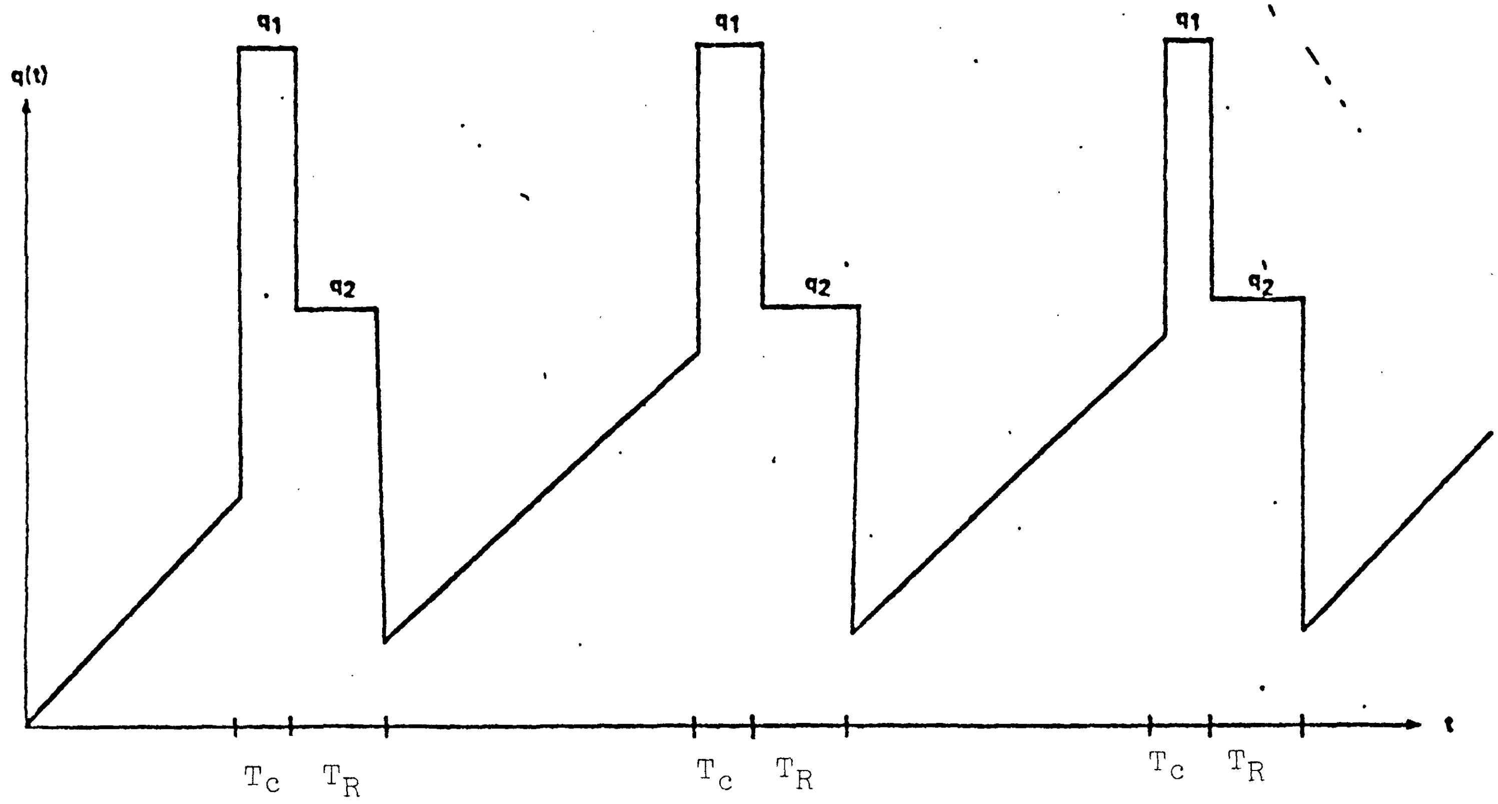


Figure 2.4: The Instantaneous Unavailability Including Test and Repair Contributions (q_1 and q_2)

The graph shows the familiar saw-tooth shape with the test and repair plateaus given by q_1 and q_2. It should be noticed, that even though test and repair period T_c and T_R are usually of short duration, the contributions by q_1 and q_2 can be important to the peak and average unavailabilities.

The average unavailability $\bar{q}$ is computed by FRANTIC as the area of the time dependent instantaneous unavailability curve divided by the total time interval, the latter being any interval of interest, for instance one year. Thus, by considering Fig.2.4 and taking T_2 to be the cycle time (neglecting the effect of the different first test interval T_1, because it is usually small) the average unavailability $\bar{q}$ can be approximately given as:

$$\bar{q} = \frac{1}{2} \lambda T_2 + q_1 \frac{T_c}{T_2} + q_2 \frac{T_R}{T_2} \qquad (2.28)$$

where the first term on the right hand side constitutes the between tests contribution, the second term is the test contribution and the third term is the repair contribution.

It is obvious from the foregoing discussion that FRANTIC not only provides average values for the unavailability but also its total time dependent behavior. Therefore, in what follows, both the average as well as the peak unavailabilities will be reported for the systems under consideration. The peak unavailability is a good indicator for the increase in system unavailability no matter how short the test period is. Thus, it is an additional parameter of interest for system design, although it should be recognized that only the average unavailability of systems has been considered in the relevant literature (WASH-1400).

2.8 Connection Between FRANTIC-Methodology and WASH-1400

It is certainly interesting to show how the aforementioned methodology compares with that used by the Reactor Safety Study. The following arguments follow these given by Vesely and Goldberg [5].

In WASH-1400, the system unavailabilities were calculated in order to predict the accident sequence probabilities and then the corresponding accident risks.

The system unavailabilities which were applicable for the WASH-1400 predictions were the average unavailabilities, averaged over a one year time period.

In addition to the average unavailability, the time dependent, instantaneous unavailability can also be important in probabilistic evaluations as discussed in the foregoing section.

$$\bar{q} = \frac{1}{T}\int_0^T q(t)dt \qquad \text{where } T = 1 \text{ year} \qquad (2.29)$$

By definition the instantaneous unavailability q(t) is the probability that the system is unavailable at the given instant of time t. The $\bar{q}$ is the average fraction of time that the system is down.

To illustrate the roles of $\bar{q}$ and q(t) in probabilistic analysis consider a particular accident sequence consisting of one initiating event and one system which is called upon to operate. Let Λ be the constant occurrence rate for the initiating event. The probability f(t)dt that the accident sequence will occur in some time interval dt at time t is:

$$f(t)dt = \Lambda q(t)dt \qquad (2.30)$$

and hence $\Lambda q(t)$ is the instantaneous accident frequency, i.e., the probability of an accident occurring per time at time t.

The yearly accident frequency P, which is what WASH-1400 considered is the integral of q(t)dt over a one year period T.

$$p = \int_0^T \Lambda q(t)dt = \Lambda T \frac{1}{T} \int_0^T q(t)dt \qquad (2.31)$$

or

$$P = \Lambda T\bar{q} \qquad (2.32)$$

Thus from Eq.(2.30)the instantaneous unavailability q(t) enters into the instantaneous accident frequency rate $\Lambda q(t)$ and from Eq.(2.32)the average unavailability $\bar{q}$ enters into the yearly accident probability $\Lambda T\bar{q}$.

The instantaneous accident frequency $\Lambda q(t)$ describes the detailed time behavior of the accident likelihood. The time at which $\Lambda q(t)$ is a maximum, i.e., the time at which the instantaneous system unavailability q(t) is a maximum, is the time at which the accident is most likely to occur. A safety system may have a low average unavailability $\bar{q}$ and yet at particular times the instantaneous unavailability q(t) may be quite high indicating the plant is most vulnerable to accidents at these times.

Fig. 2.5 compares two systems which have the same average unavailability but show quite different instantaneous unavailability behaviors. Certainly, the system with the highest unavailability maxima in q(t) is the more loosely controlled system. Thus it becomes apparent that for a more complete evaluation of system design or system operation, both

a) the instantaneous unavailability, particularly the maxima

and

b) the average unavailability $\bar{q}$

should be assessed. Because FRANTIC is providing these informations, they will be both displayed for each system to be studied in what follows.

2.9 Benchmark Tests of the FRANTIC Code Against the REBIT Code

2.9.1 Introduction

Because FRANTIC will be heavily used later in this study and due to the fact that NRC upon releasing this code has not provided the general public with any information as to how this code compares to others, it seems to be appropriate to perform benchmark tests with the code before it is employed. For this purpose,

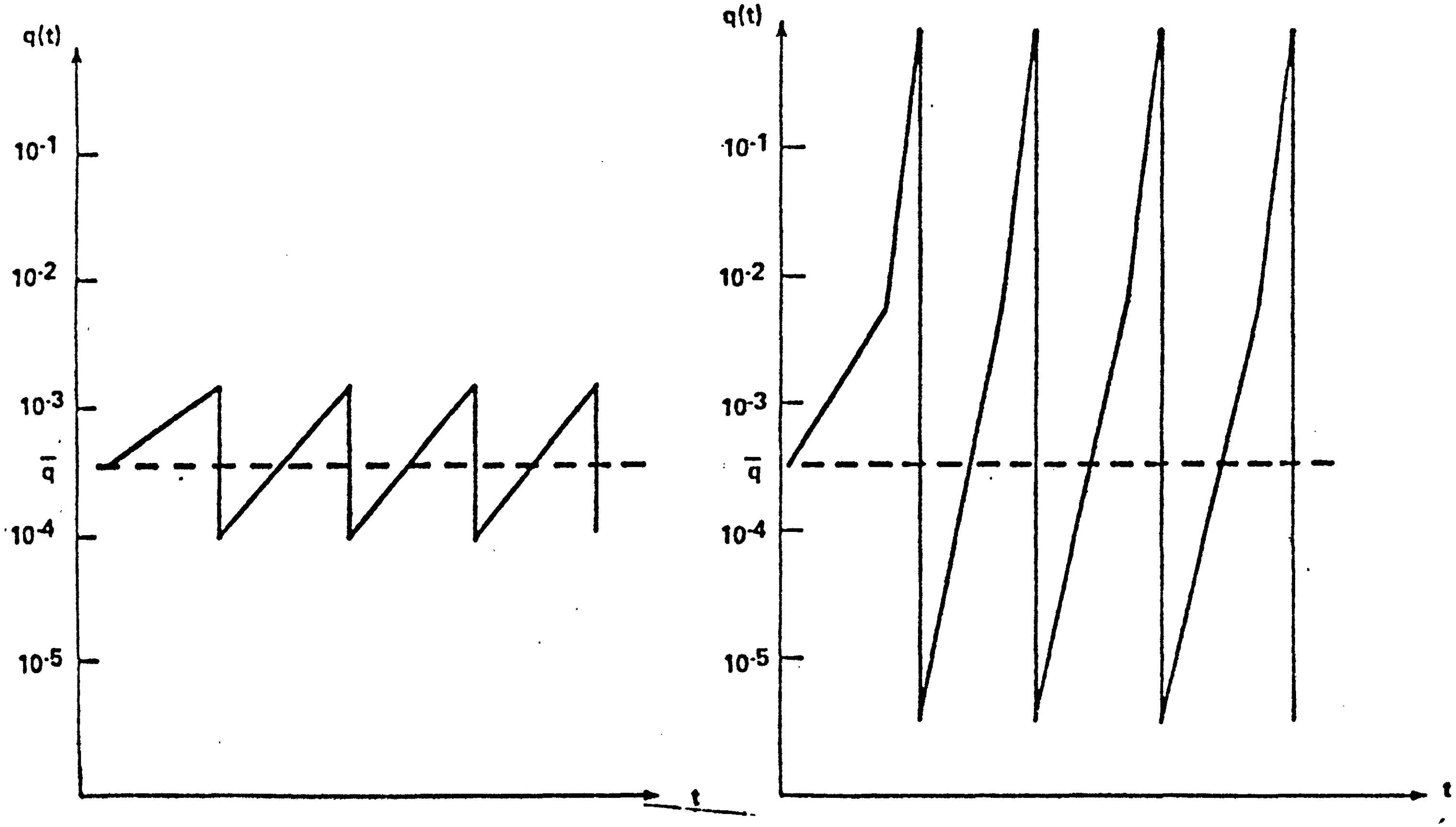


Figure 2.5: Two Systems with the Same Average Unavailability ($\bar{q}$) but with Different Instantaneous Unavailabilities ($q(t)$)

FRANTIC results will be compared to those obtained by the REBIT [20] and the PL-MODT [21] codes for simple systems.

The code REBIT [20] (REliability by BIT handling) is a small but powerful computer code ($\sim$ 350 statements) written in FORTRAN-IV language which determines the minimal cut sets of a fault tree by Boolean expressions using convenient bit-handling techniques and calculates various reliability and availability characteristics by employing analytical techniques. The limitation in the size of fault tress which can be analyzed by REBIT is primarily dependent on the dimensions of the arrays. In its present version the code can be considered as an interesting alternative to much more complex and time-consuming codes for treating small to medium sized fault trees. It is of special importance to those users who have no access to a PL/1 compiler to run PL-MODT [21,22]. In contrast to the FRANTIC code [5], REBIT accepts a fault tree as input, determines the minimal cut sets for the system under consideration and continues by calculating the unavailability, the cumulative failure probability and other relevant data for both the minimal cut sets and the system.

2.9.2 Classes of Components Treated by REBIT

In its present version, REBIT is set up to handle components of the following classes. Below, each class is shown with its associated analytical expression for the component unavailability.

1. Periodically maintained components

$$\bar{A} = 1 - \exp [- \lambda(t - nT_n)]$$

2. Non-repairable components

$$\bar{A} = 1 - \exp (- \lambda t)$$

3. Repairable components

$$\bar{A} = \frac{\lambda}{\lambda+\mu} [1 - \exp [-(\lambda+\mu)t]]$$

Where

λ : component failure rate

T_n: component maintenance interval

n : n-th maintenance interval

μ : component repair rate

REBIT determines the point unavailability for the minimal cut sets and the system every Δt hours for a prespecified number of time increments. Both quantities are given as inputs. It should be noticed that the time step size primarily determines the accuracy of the calculation for the mean unavailability as well as the magnitude of the peak unavailabilities. The effect of this variable upon the calculated results will be discussed in the following section.

REBIT uses the following expression for calculating the mean unavailability $\bar{A}_{mean}$

$$\bar{A}_{mean} = \frac{1}{n} \sum_{j=1}^{n} \bar{A}(j \Delta t) \qquad n\text{: number of time increments.}$$

2.9.3 Comparison of Results Between REBIT and FRANTIC for Two Sample Problems

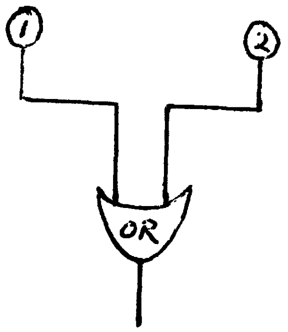
Due to the fact that REBIT does not handle periodically inspected components at present, the approach which has been taken in REBIT to compare it with FRANTIC has been to approximate periodically tested components by periodically maintained components. To clarify this difference, a periodically maintained component has zero testing time and zero repair time, that is, the component is instantaneously renewed at each maintenance. To perform an honest comparison the appropriate parameters have been set equal to zero in FRANTIC in order to give the best simulation in the component models used by both codes.

The results for a parallelsystem of two components and a 3-out-of-4 gate are summarized in Tables 2.2 and 2.3 , respectively. Figures 2.6 and 2.7 compare the point unavailabilities obtained by both codes for the two sample cases, respectively. The results shown for the REBIT calculations are those for the larger time increments.

As can be seen from Figure 2.6 and Table 2.2, both codes are in general agreement for the peak system unavailabilties and the mean system unavailability. The agreement becomes even closer for the case where REBIT was run with the smaller time increment. Fig. 2.6 clearly indicates that the first term approximation for the exponential distribution employed by FRANTIC gives very reasonable results. For all practical pur-

TWO COMPONENT PARALLEL SYSTEM

FAULT TREE



DATA

Component	1	2
$\lambda \cdot 10^{+6}$HR	2	3
T_n or T_2 Day	20	15
T_{Test}	0	0
T_{Repair}	0	0

		FRANTIC	REBIT 182.5 Day Period	
		183 Day Period	100 Time Steps 43.8 HRS/Step	1000 Time Steps 4.38 HRS/Step
Mean Unavailability		1.006×10^{-3}	9.828×10^{-4}	1.008×10^{-3}
Maximum Peaks of Unavailability (Time) of Occurrence)	1	2.039×10^{-3} (1440 HRS)	1.900×10^{-3} (4292 HRS)	2.032×10^{-3} (4318 HRS)
	2	2.039×10^{-3} (2880 HRS)	1.844×10^{-3} (2847 HRS)	2.027×10^{-3} (2878 HRS)
	3	2.039×10^{-3} (4320 HRS)	1.847×10^{-3} (1402 HRS)	2.022×10^{-3} (1437 HRS)

TABLE 2.2

TWO COMPONENT PARALLEL SYSTEM, INPUT AND COMPARISON OF RESULTS OF THE FRANTIC AND REBIT CODES

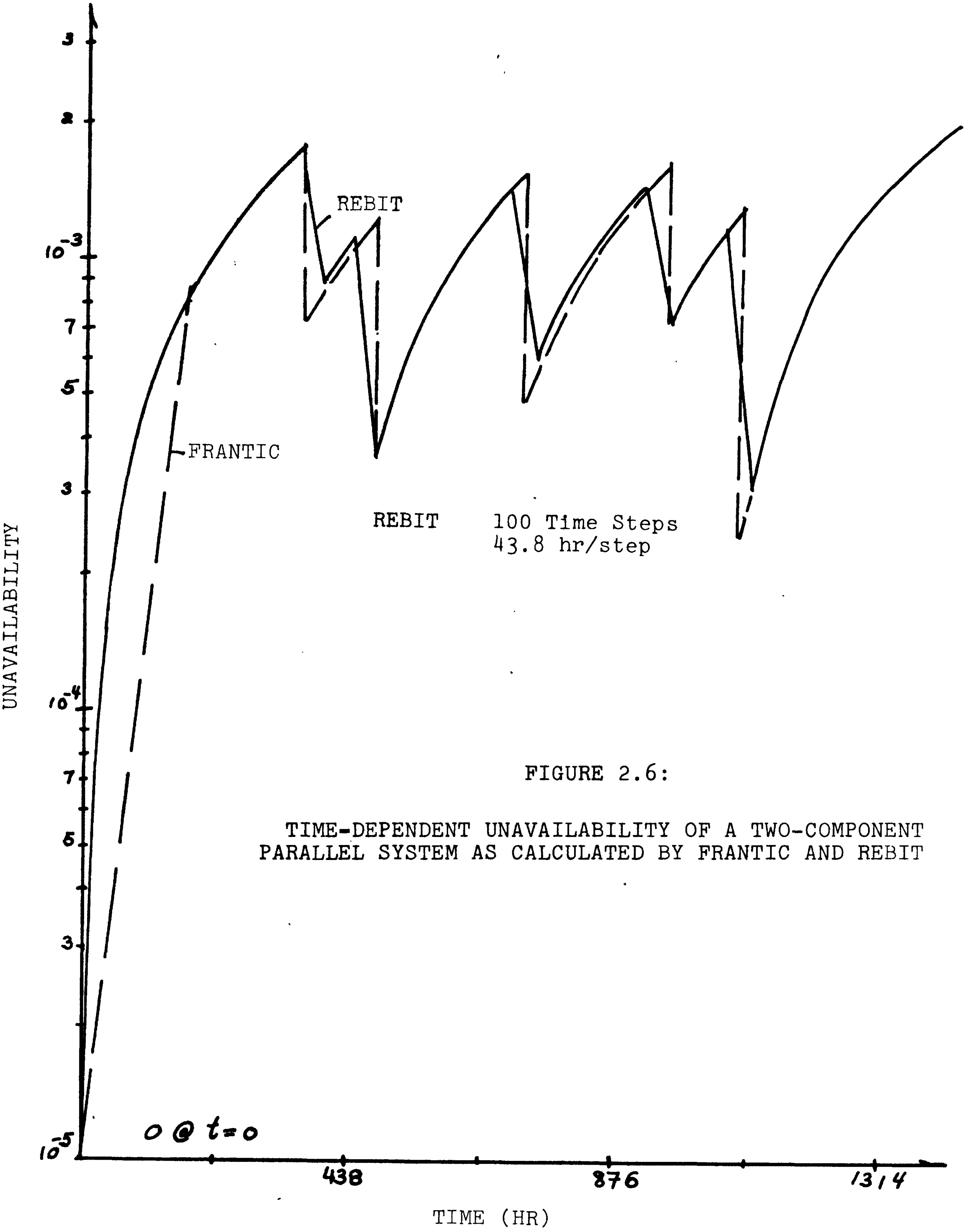
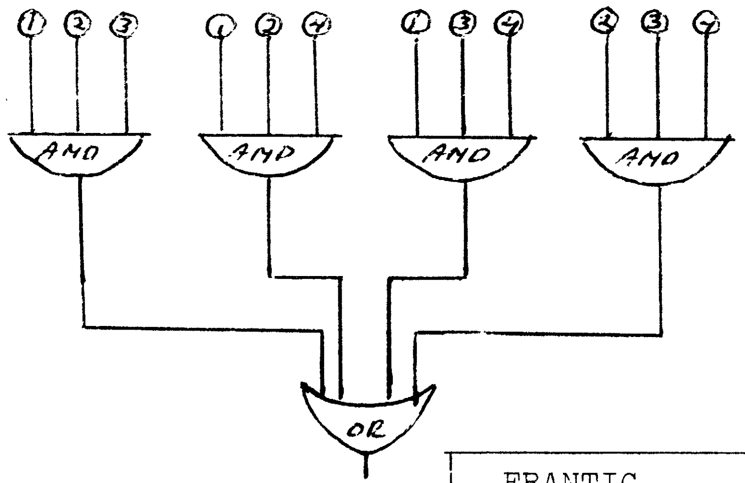


FIGURE 2.6:

TIME-DEPENDENT UNAVAILABILITY OF A TWO-COMPONENT PARALLEL SYSTEM AS CALCULATED BY FRANTIC AND REBIT

THREE-OUT-OF-FOUR

FAULT TREE



DATA

Component	1	2	3	4
$\lambda \cdot 10^{+6}$HR	2	3	5	7
T_n or T_2 (Days)	20	15	10	7
T_{Test}	0	0	0	0
T_{Repair}	0	0	0	0

	FRANTIC	REBIT 182.5 Day Period	
	183 Day Period	100 Time Steps 43.8 HRS/STEP	1000 Time Steps 4.38 HRS/STEP
Mean Unavailability	9.97×10^{-10}	6.943×10^{-10}	7.298×10^{-10}
Maximum Peaks of Unavailability (Time of Occurrence)	4.5125×10^{-9} (2856 HRS)	4.036×10^{-9} (2897 HRS)	4.488×10^{-9} (2856 HRS)
	4.1714×10^{-9} (4320 HRS)	2.843×10^{-9} (4292 HRS)	4.086×10^{-9} (4319 HRS)
	3.5859×10^{-9} (1440 HRS)	3.429×10^{-9} (2146 HRS)	3.41×10^{-9} (1437 HRS)

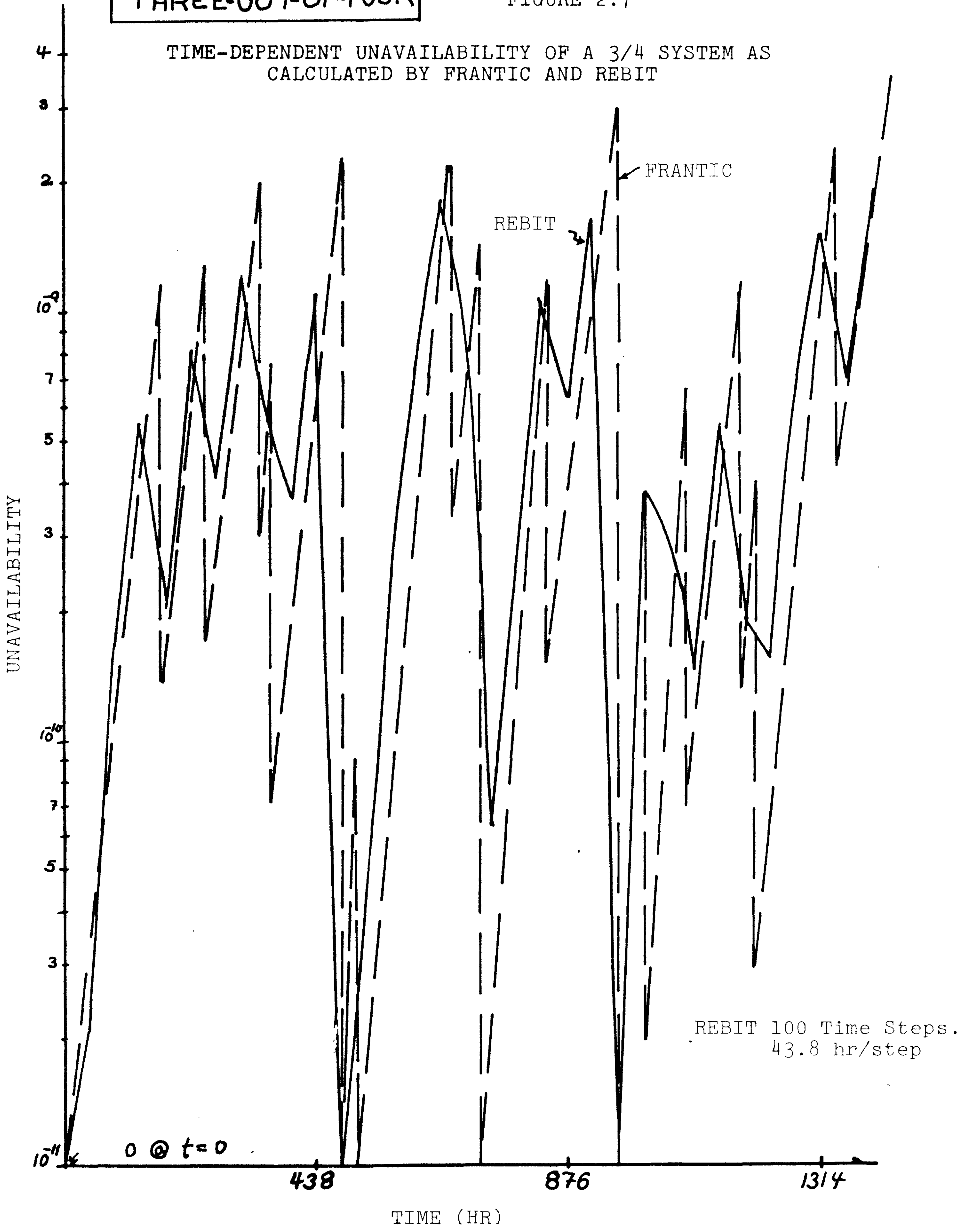
TABLE 2.3

3/4 SYSTEM, INPUT AND COMPARISON OF THE RESULTS OF THE FRANTIC AND REBIT CODES.

THREE-OUT-OF-FOUR

FIGURE 2.7

TIME-DEPENDENT UNAVAILABILITY OF A 3/4 SYSTEM AS CALCULATED BY FRANTIC AND REBIT



poses the comparison with REBIT shows a very satisfactory behavior of the FRANTIC results.

For the 3/4 problem the two codes do not agree to the extent that they did for the previous case. This is especially true for the case where REBIT was run with the larger time increment. For this case, REBIT obviously misses relative minima and maxima which are calculated by FRANTIC. This deviation is mainly caused by the time step size and partly by the maintenance times selected for the components. With respect to the mean system unavailability, Table 2.3 reveals that the results of the two codes agree only in magnitude and that an increase in the number of time steps from 100 to 1000 in REBIT has only little effect in bringing the results closer to each other. FRANTIC is not supposed to give precise answers either because it is based also on several approximations whose overall impact on the final results are difficult to assess. The only way to decide what approach is closest to reality would be to benchmark both codes against one employing the Markovian approach.

As the complexity of the systems under study increases, it can be expected that the agreement between the two codes will greatly depend on the time increment chosen for REBIT and the maintenance intervals selected for the components. Some disagreement will always exist due to the fact that REBIT and FRANTIC use different expressions for the unavailability of non-repairable components as shown below.

REBIT	FRANTIC
$\bar{A} = 1\text{-}\exp(-\lambda t)$	$\bar{A} = \lambda t$

Differences in $\bar{A}$ between these two expressions are certainly small for $\lambda t << 1$. On the other hand, FRANTIC is limited by its approximation since it can lead to unavailabilities greater than one in certain cases.

Finally, it is of interest to compare the computation times for both codes. These are given in the table below.

CPU Time in Minutes

REBIT		FRANTIC
100 time steps 0.353	1000 time steps 0.392	0.431

This table reveals the interesting fact that FRANTIC although it only obtains the unavailability for a given system unavailability function is still slower than the REBIT code which generates both the minimal cut sets as well as the unavailabilities. Furthermore, it is surprising to see that an increase in the number of time steps from 100 to 1000 does not lead to a substantial increase in computation time for REBIT which is certainly the result of the benefit of using analytical expressions.

In conclusion, although the two examples do not constitute a complete basis, these results are the first published which show how FRANTIC compares to other methods. A broader spectrum of comparison is offered by PL-MODT and will be addressed in the following section.

2.10 Benchmark Tests of the FRANTIC Code Against the PL-MODT Code

2.10.1 Introduction

The apparent advantages of modularizing fault trees rather than taking the commonly employed cut-set approach have been highlighted by the recent development of the code PL-MOD [23] which uses the list processing features provided by the PL/1 language. This code is limited to the analysis of steady-state problems.

In the meantime, analytical models have been added to PL-MOD which allow the analysis of time-dependent problems and still maintain the advantages of modularization. Thus, a new version of the code, PL-MODT, has been devised which still uses the unaltered scheme for finding the modular structure and importances of the fault tree. The following three classes

Class 1: Nonrepairable components

Class 2: Repairable components, failures of which are detected immediately

Class 3: Repairable components, failures of which are detected upon inspection.

The latter class includes the treatment of test override unavailabilities. Additional features of PL-MODT are the calculation of the Vesely-Fussell importance as function of time and the possibility to arbitrarily refine the time mesh which is an important feature for getting detailed representations of test and repair intervals. With all these features, PL-MODT is certainly better suited to test FRANTIC's validity than REBIT. Thus, more insight can be expected from a comparison of these two codes, which adds to the observations described in the foregoing section.

2.10.2 Results for the Comparison Between FRANTIC and PL-MODT

Two examples have been run with both codes for illustrative purposes. The first one concerns the special fault tree given and analyzed by Vesely in his original paper [24] by PREP-KITT. This fault tree is shown in Fig. 2.8 The data assigned to the primary events in this fault tree are summarized in Table 2.4 below

TABLE 2.4

FAILURE AND REPAIR RATES FOR SAMPLE TREE IN FIGURE 2.8

Primary Failure Index	$\lambda(hr^{-1})$	$\mu(hr^{-1})$
1	2.6×10^{-6}	4.1×10^{-2}
2	2.6×10^{-6}	4.1×10^{-2}
3	2.6×10^{-6}	4.1×10^{-2}
4	3.5×10^{-5}	1.66×10^{-1}
5	3.5×10^{-5}	1.66×10^{-1}
6	3.5×10^{-5}	1.66×10^{-1}
7	5.0×10^{-6}	0
8	5.0×10^{-6}	0
9	8.0×10^{-6}	0
10	8.0×10^{-6}	0

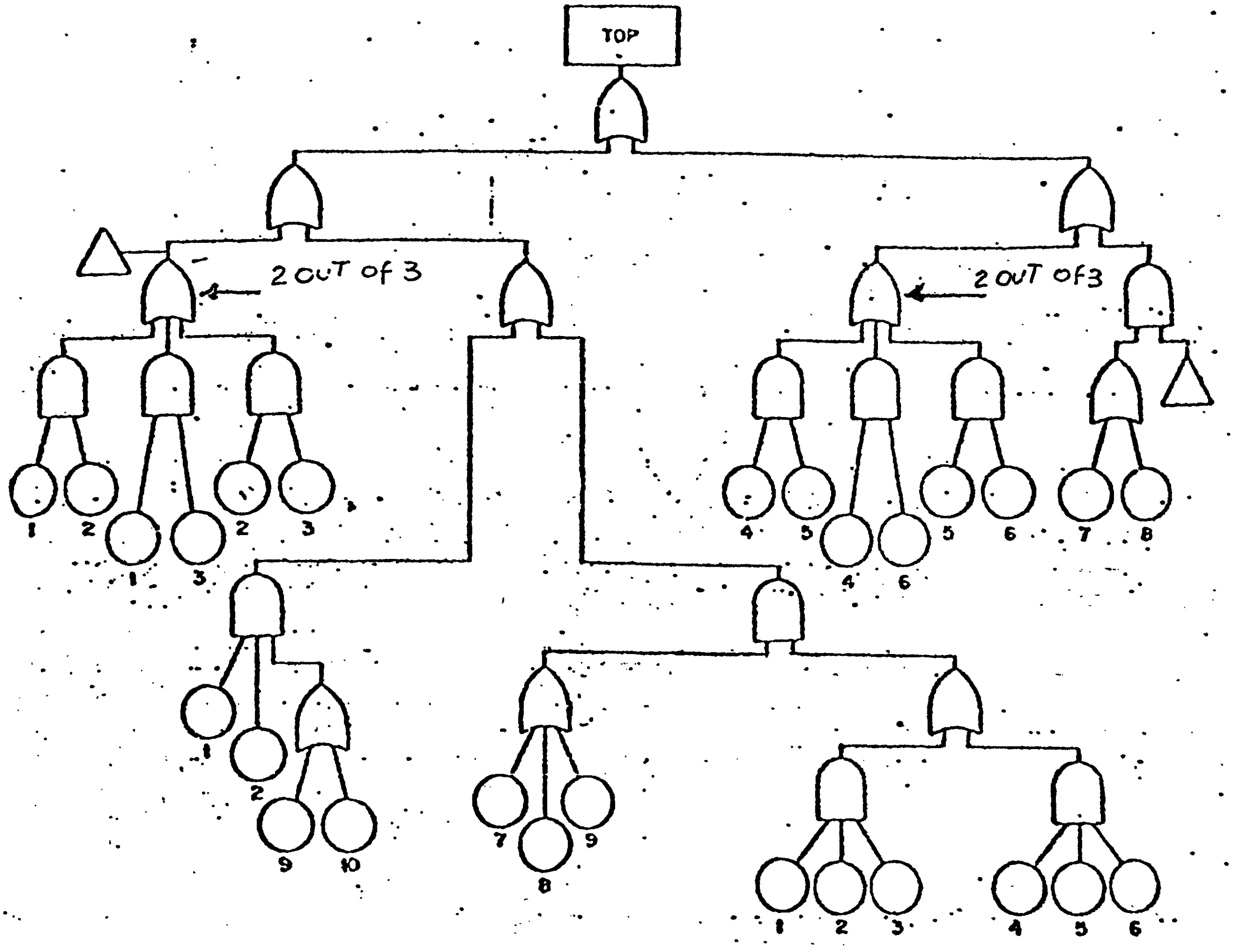


Figure 2.8: Fault Tree Example Given by Vesely

The results obtained from the various codes are shown in Fig.2.9 which indicates that all methods give essentially the same asymptotic value for the unavailability. In fact, FRANTIC is predicting only this value by neglecting the transient period over the first 20 hrs. of system operation, whereas PL-MODT and KITT are suited for handling even this transition period. Obviously PL-MODT is closer to the exact solution than KITT. The computation time for PL-MODT to analyze the tree and to calculate the top event unavailability for 15 time steps is 0.62 seconds.

The solution which is called "exact" has been generated by using the exact system function and the analytical unavailability expression for a single component which is failing randomly and gets repaired, which is derived from a Markovian model. The reason for the small differences between PL-MODT and the "exact" result lies in the fact that the former contains some approximations concerning the time-dependent behavior of moduler. However, it becomes quite obvious from this figure that the modular approach is in fact quite superior over the kinetic tree procedure employed by KITT. On the other hand it should be honestly mentioned that these differences show up only in the minute details, whereas for engineering calculations the correct determination of the asymptotic value is of most importance.

The second example concerns the simple electric system as discussed by Lambert [25] and shown in Fig. 2.10. The purpose of this system is to provide light by the bulb when the switch is

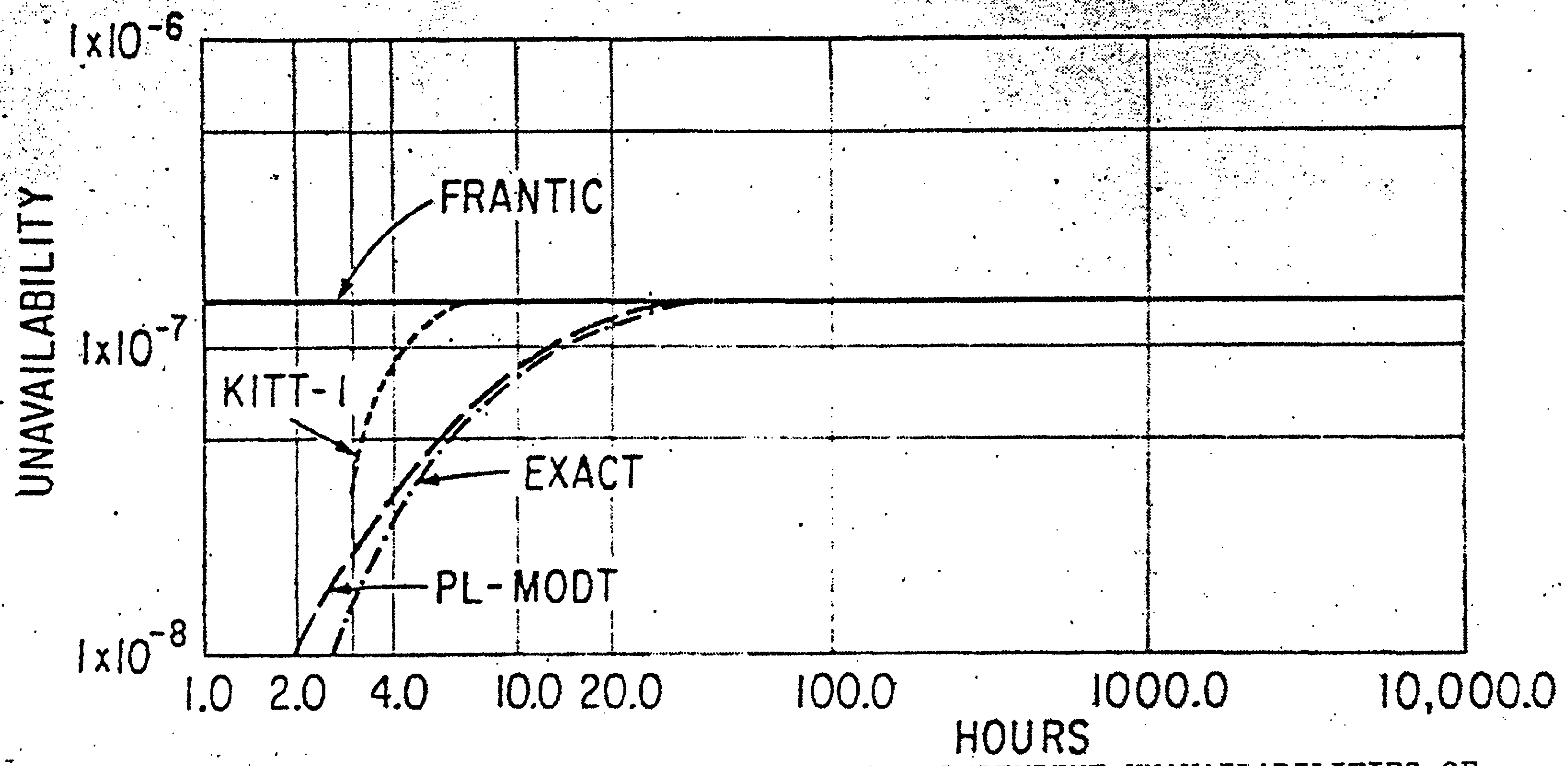


FIGURE 2.9 COMPARISON OF THE TIME-DEPENDENT UNAVAILABILITIES OF REPAIRABLE COMPONENTS FOR THE SAMPLE TREE GIVEN IN FIGURE 2.8 AS CALCULATED BY FRANTIC, PREP, KITT AND PL-MODT

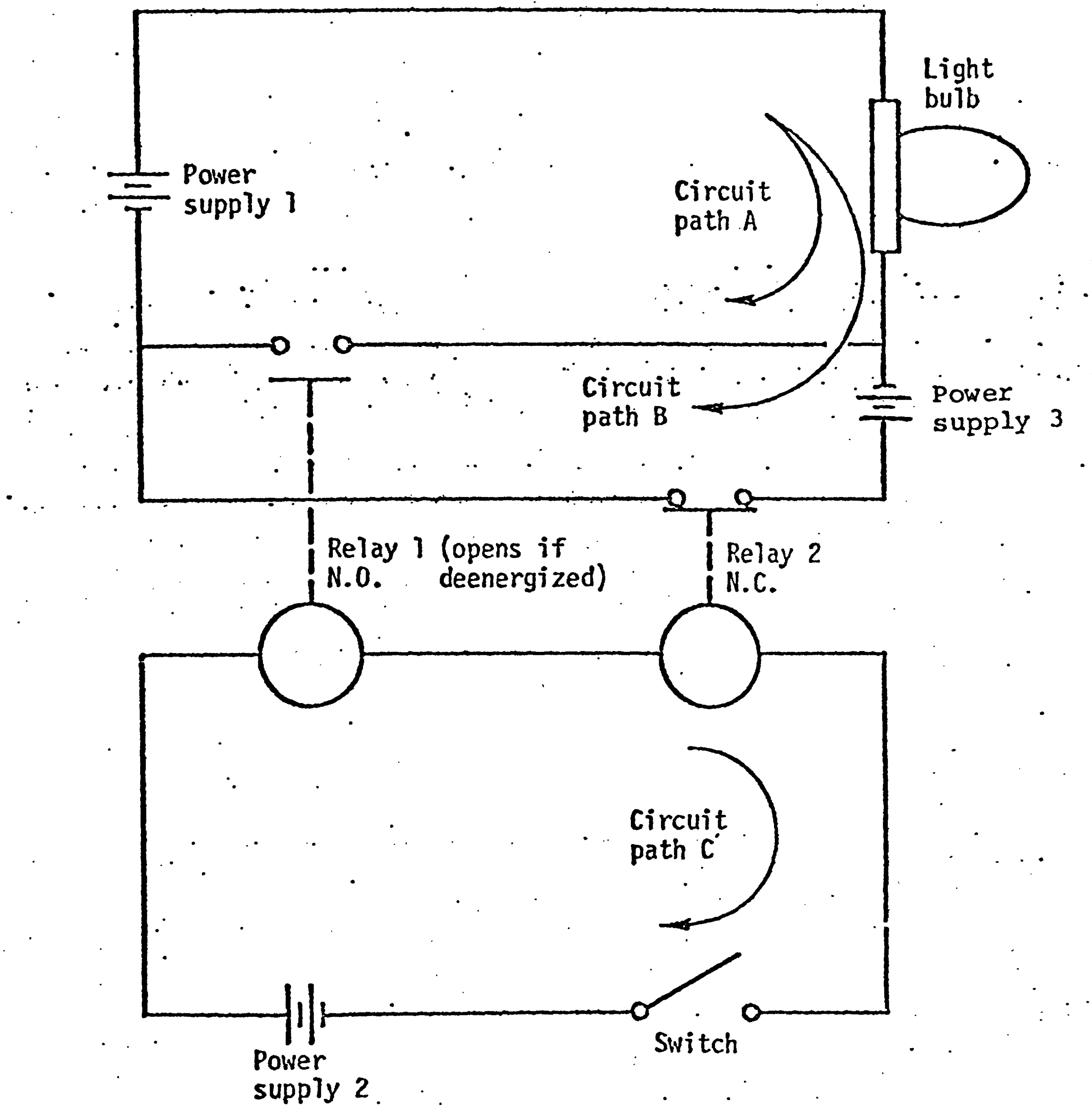


Figure 2.10. Sample System for Mutually Exclusive Events

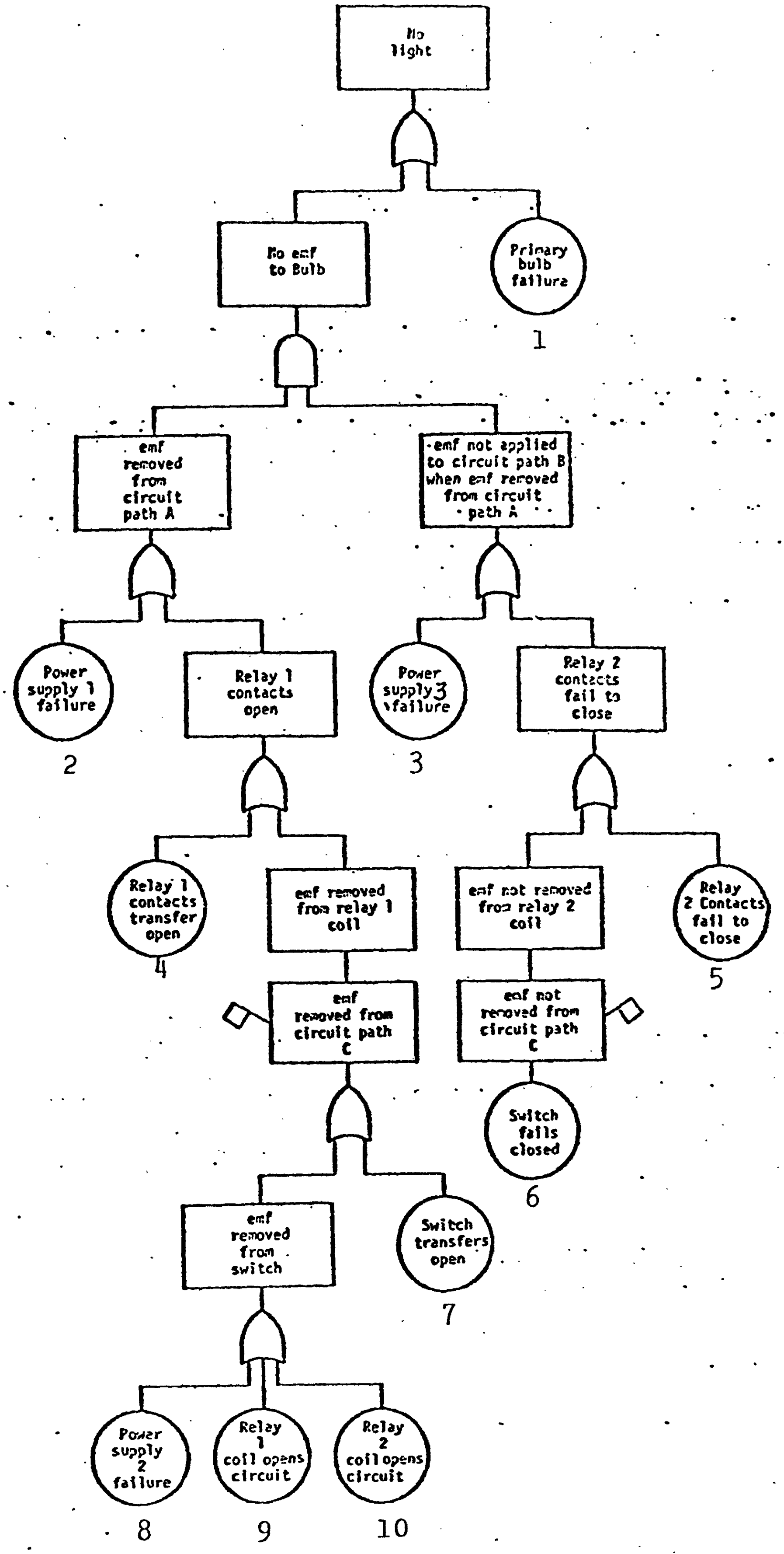

No light
No emf to Bulb
Primary bulb failure
1
emf removed from circuit path A
emf not applied to circuit path B when emf removed from circuit path A
Power supply 1 failure
2
Relay 1 contacts open
Power supply 3 failure
3
Relay 2 contacts fail to close
Relay 1 contacts transfer open
4
emf removed from relay 1 coil
emf not removed from relay 2 coil
Relay 2 Contacts fail to close
5
emf removed from circuit path C
emf not removed from circuit path C
Switch fails closed
6
emf removed from switch
Switch transfers open
7
Power supply 2 failure
8
Relay 1 coil opens circuit
9
Relay 2 coil opens circuit
10

Figure 2.11 Fault Tree for Sample System in Figure 2.10.

TABLE 2.15

PARAMETERS FOR THE CIRCUIT EXAMPLE

Component #	Failure rate hr^{-1}	Inspection Time (hrs)	First (Days) Time Interval	Repair Time (hrs)	Override Unavailability	Test 1(days) Interval
1	$2.0x10^{-4}$	1.0	7	2.0	1.0	7
2	$2.8x10^{-5}$	0.5	7	1.0	1.0	14
3	$2.8x10^{-5}$	1.0	7	1.5	1.0	14
4	$3.2x10^{-3}$	0.5	7	2.0	1.0	7
5	$4.1x10^{-4}$	0.5	14	1.5	1.0	21
6	$3.2x10^{-4}$	1.0	28	1.5	1.0	28
7	$2.8x10^{-3}$	0.5	14	2.0	1.0	21
8	$2.8x10^{-3}$	1.0	14	1.5	1.0	14
9	$4.5x10^{-3}$	0.5	7	2.5	1.0	7
10	$4.5x10^{-3}$	1.5	7	3.0	1.0	7

is closed, the relay 1 contacts are closed and the contacts of relay 2 (a normally closed relay) are opened. Should the contacts of relay 1 open, the light will go out and the operator will immediately open the switch which in turn causes the contacts of the relay 2 to close which restores the light. The fault tree, with the top event of "No Light" shown in Fig. 2.11 neglects operator failures, wiring failures as well as secondary failures. Failure rates, repair times and test periods for the various components are summarized in Table 2.5. No replicated component or module exists in the system. In order to enable FRANTIC to analyze this system, its unavailability function must be developed and provided as input. This function was found to be

$$QS = \{1.0-(1-Q(1))\{1-[(1-Q(2))(1-Q(4))(1-Q(7)91-Q(8))*$$
$$* (1-Q(9))(1-Q(10))][1-(1-Q(3))(1-Q(6))(1-Q(5))\}\}$$

On the other hand, for PL-MODT the fault tree was directly inputted and the code modularized the tree as follows:

Module #4: components 5, 6, and 3
Module #3: components 4, 7, 8, 9, 10, and 2
Module #2: modules 4 and 3
Module #1: component 1 and module 2

Fig. 2.12 compares the results of both codes for one complete period of 28 days. As can be seen, the results are in close agreement. Again, FRANTIC gives conservative results compared to PL-MODT, primarily due to the comparatively high failure rates

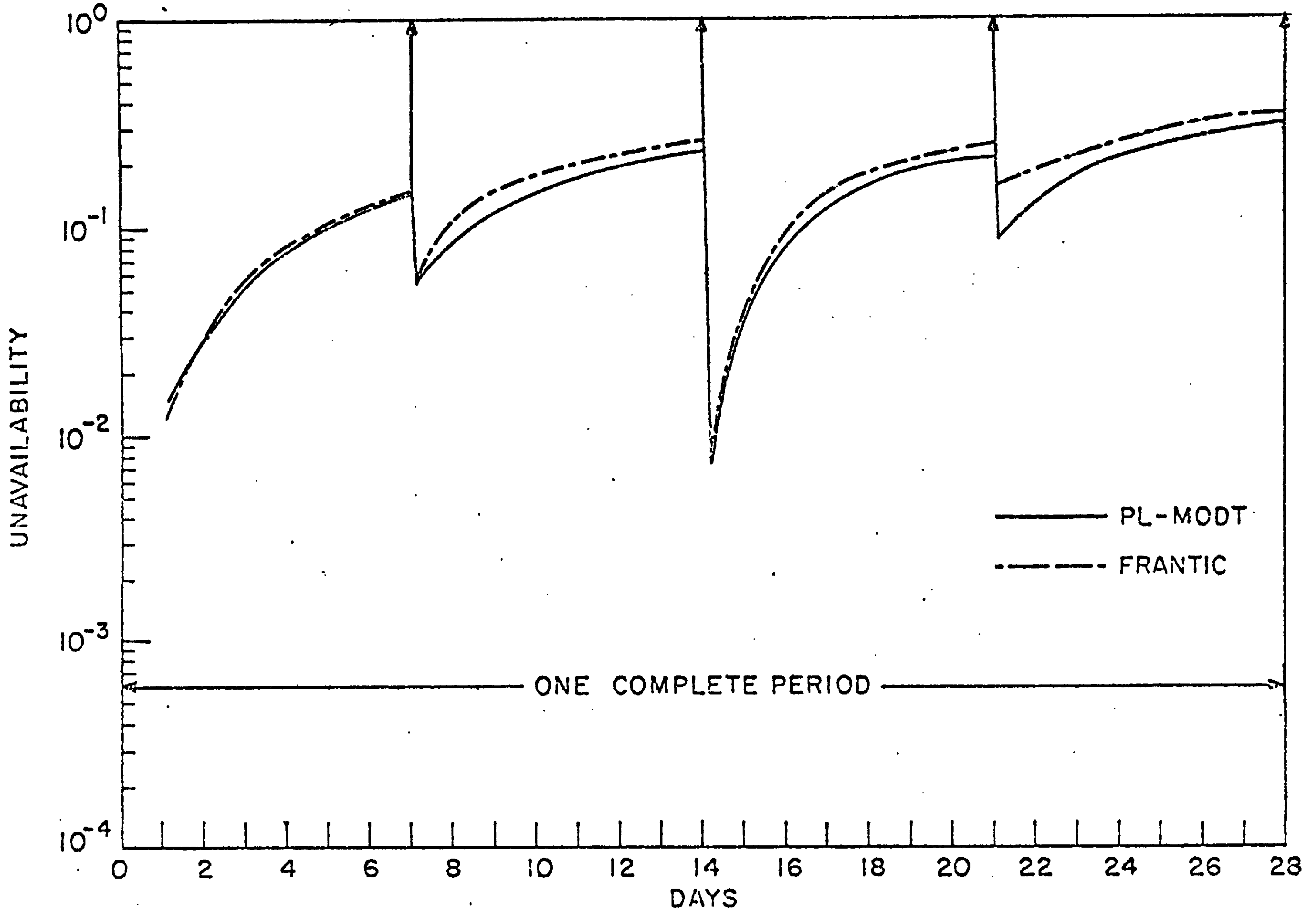


Figure 2.12 Comparison Between the Unavailabilities for the Electrical System During Its Operation as Calculated by FRANTIC and PL-MODT

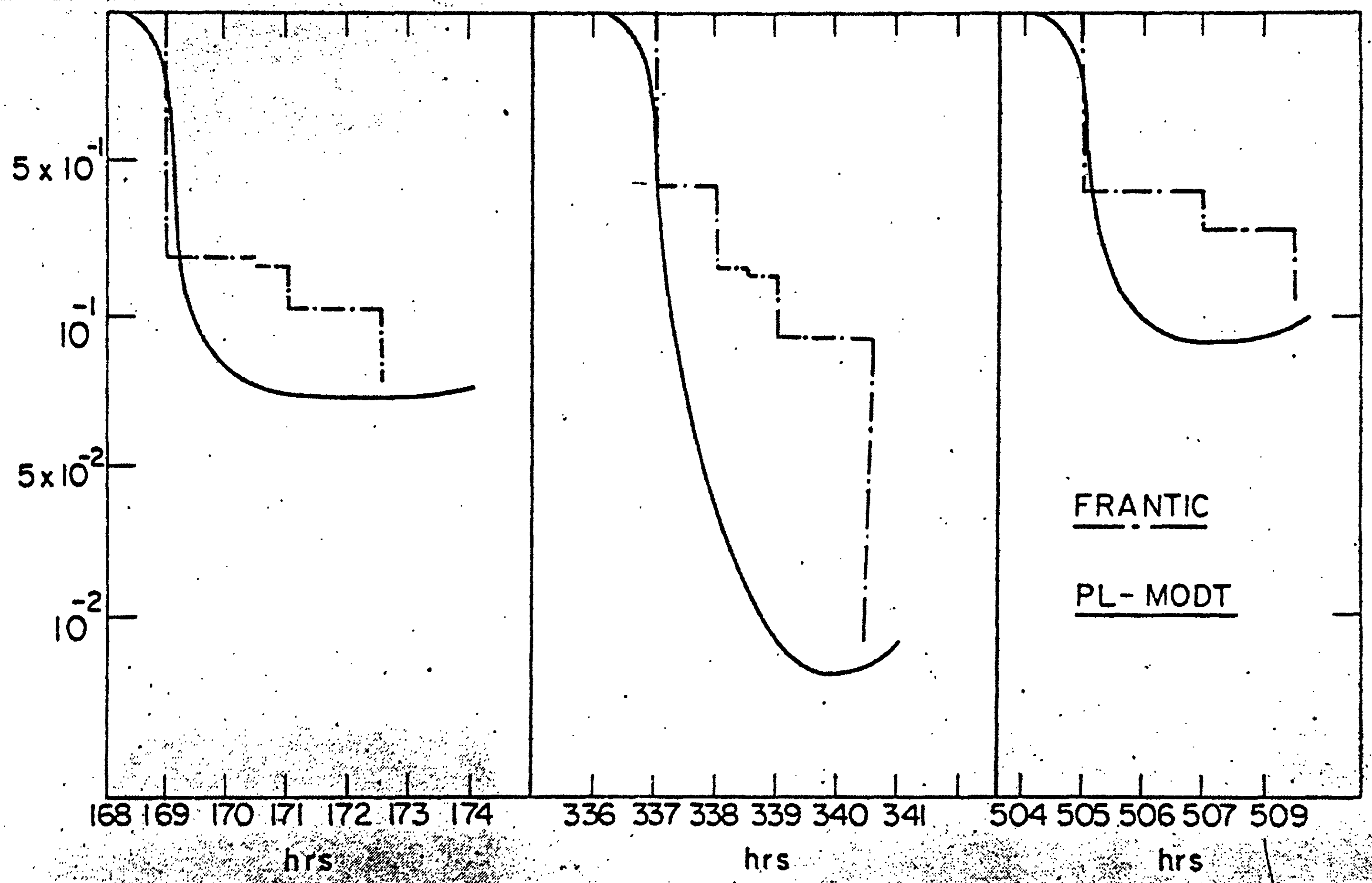


FIGURE 2.13 COMPARISON BETWEEN THE UNAVAILABILITIES DURING TEST AND REPAIR PERIODS AS CALCULATED BY BOTH CODES

which have been selected as well as the straight line approach for the exponential function employed by FRANTIC.

As can be seen from Fig. 2.13 both codes give essentially the same results during the test time but differ during the repair time because of the different procedures used in the codes. However, as discussed previously, these differences show up only during a very brief period of time and therefore do not affect the overall results.

The CPU time for PL-MODT was 0.98 seconds for the modularization and the evaluation of the unavailabilities of the components, modules and the top event for 32 time steps as well as for the determination of the importances for the components and modules.

For the same tree and data, FRANTIC needs 1.12 seconds for the calculation of the system unavailability alone. It does not provide any structural information about the fault tree.

2.11 Comments and Discussion

It has been demonstrated in the last two sections that FRANTIC is in fact a reliable engineering tool for unavailability calculations. The comparisons shown before are the first published for FRANTIC. They show that the code can be safely applied for this tudy and our finding support NRC views on FRANTIC as recently indicated by Levine [26].

However, despite all of these favorable indications about FRANTIC it should not be overlooked that it has the fundamental drawback of needing the system unavailability equation as input. The formulation of this equation mandates knowledge in Boolean Algebra by the user even for smaller systems. Large and complex systems are difficult to handle by FRANTIC. Despite this shortcoming, the following study is based on the application of FRANTIC because this code is used now in the regulating process [26]. However, the foregoing remarks clearly indicate that FRANTIC can only be applied to small systems. In order to overcome this limitation, the code must be coupled to a minimal cut set generating preprocessor such as PREP, WAM-CUT, etc., in future.

3. TEST INTERVAL OPTIMIZATION STUDY FOR A DIESEL GENERATOR UNIT

3.1 Introduction

The diesel generator is one of the most vital subsystems of the Emergency Power System. This chapter is concerned with the optimization of the test interval for the D.G. by considering it as one component which allows the application of the analytical procedures discussed previously. One of the most general models was developed by Coleman and Abrams [3]. Jacobs [4] neglected the repair time contribution and derived a very simple formula for calculating the optimum test interval which minimizes the unavailability of a single component. Hirsch [2] extended this analysis, whereas Vesely [5] simplified the model by Coleman and Abrams.

In what follows, these four methods will be applied to evaluate the optimum D.G. test interval, and possible differences will be discussed.

3.2 Optimum Test Interval Derived from the Coleman & Abrams Procedure

These authors derived the following equation for the unavailability of a single component under very broad and general conditions

$$A=\frac{\theta(1-e^{-\lambda T})}{\lambda(T+T_c)\{1+e^{-\lambda T}[\beta(1-\alpha+\alpha P_c-P_c\theta)-(1-\theta)]\}+\lambda T_R[1-(1-\alpha)(1-\beta)e^{-\lambda T}]} \tag{3.1}$$

where

A Component availability

λ Component failure rate

β Probability of the failure during a test period

T_c Testing period

T_R Repair time period

α Probability of a false alarm

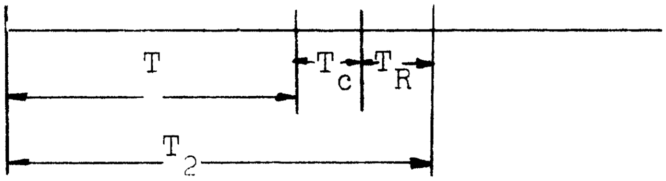
P_c Probability of failure occurring before actual test of the failure occurs during testing period

θ Probability that a failure will be detected

T Time between repair time of previous interval to the next testing period as shown below

T_2 Test interval

The various time periods are depicted in the sketch below.



Eq. (3.1) is a very good starting point for deriving formulations for A under more simplified conditions. For instance, by assuming

1) perfect testing, i.e., $\theta=1$

2) no false alarm, $\alpha=0$

3) $P_c=1$; $\beta=0$

Eq. (3.1) reduces to

$$A = \frac{1-e^{-\lambda T}}{\lambda(T+T_c) + \lambda T_R[1-e^{-\lambda T}]} \qquad (3.2)$$

From the above sketch, it follows that

$$T_2 = T + T_c + T_R$$

from which

$$T = T_2 - (T_c + T_R)$$

This, together with

$$\bar{A} = 1 - A$$

for the unavailability, leads to the following formula

$$\bar{A} = 1- \frac{1-e^{-\lambda T}}{\lambda(T_2-T_R e^{-\lambda T})} \qquad (3.3)$$

In order to find the optimum test interval, T_2, which minimizes Eq. (3.3) for the D.G. unit, a graphical procedure will be applied. For the base case, the following data are selected.

$$T_c = 1.5 \text{ hrs}$$

$$T_R = 21 \text{ hrs}$$

$$\lambda = 3 \times 10^{-5} \text{hr}^{-1}$$

Table 3.1 shows the behavior of $\bar{A}$ as a function of T_2, and Figure 3.1 displays this in a graphical form. The minimum is found at

$$T_{2_{opt}} = 14 \text{ days where } \bar{A}_{min} = 1.0045 \times 10^{-2}$$

For T_2 = 52 days, the unavailability is $\bar{A} = 1.9965 \times 10^{-2}$.

TABLE 3.1

D.G. Unavailability $\bar{A}$ as Function of the Test Interval, T_2, for T_c=1.5 hr.; T_R=21 hr. and $\lambda=3x10^{-5}hr^{-1}$

T_2 days	$\bar{A}x10^2$ -
5	1.7199
10	1.0699
15	1.0066
20	1.0694
25	1.1747
30	1.3127
35	1.4584
40	1.6117
50	1.9313
250	8.53

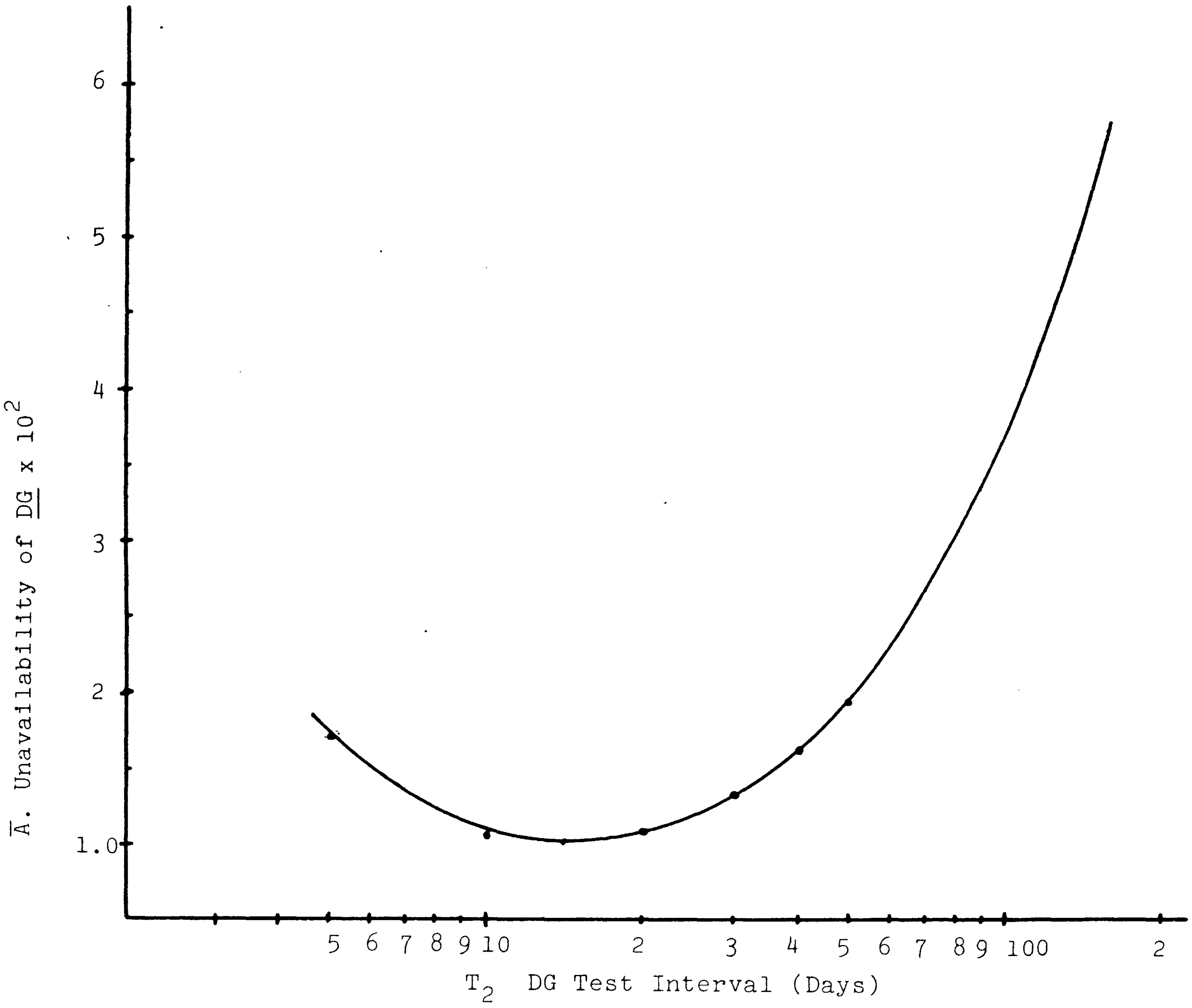


Figure 3.1: Variation of the Unavailability of DG as Function of T_2 for Perfect Testing

3.2.1 Effect of the Failure Rate on the Optimum Test Interval

In this section, the effect of the failure rate, λ, of the D.G. on the optimum test interval, $T_{2_{opt}}$, is studied parametrically and shown in Table 3.2. This is the result of a series of studies as described at the end of the foregoing section. As can be seen from this table, a decrease in the constant failure rate, λ, results in an increase in $T_{2_{opt}}$ and a decrease in the associated unavailability.

3.2.2 Effect of Test Caused Failure on the Optimum Test Interval

In this section, the additional effects of test caused failures on T_2 are studied, i.e., the assumptions of setting p=0 and P_c=1 are now relaxed. If, for instance, the following data are chosen for these two parameters

$$\beta = 10^{-2}$$

$$P_c = 0.75$$

and substituted into Eq. (3.1), the following expression results for the unavailability, $\bar{A}$, under the assumptions that still

1) $\theta = 1$

2) $\alpha = 0$

$$\bar{A} = 1- \frac{1-e^{-\lambda T}}{\lambda(T+T_c)[1+10^{-2}(0.25)e^{-\lambda T}] + \lambda T_R[1-0.999e^{-\lambda T}]} \qquad (3.4)$$

which can be further rewritten as

$$\bar{A} = 1- \frac{1-e^{-\lambda T}}{\lambda T_2+[\lambda(T_2-T_R)x2.5x10^{-3} - 0.99\lambda T_R]e^{-\lambda T}} \qquad (3.5)$$

TABLE 3.2

Effect of the D.G. Failure Rate on the Optimum Test Interval and Associated Unavailability (T_c = 1.5 hr; T_R = 21 hr)

$\lambda \times 10^6$	$T_{2_{opt}}$	$\bar{A}_{min} \times 10^2$
hr^{-1}	days	-
1	75	0.175
5	35	0.3973
10	24	0.566
30	14	1.0045
42	12	1.2003
60	10	1.4257
100	8	1.915

Table 3.3 shows the behavior of $\bar{A}$ as a function of T_2 for the data previously selected for the base case. A direct comparison with the results summarized in Table 3.1 reveals that by additionally accounting for test caused failures, the unavailability increases for a given test interval. As a net result, the optimum test interval, $T_{2_{opt}}$ and the associated unavailability, $\bar{A}_{min}$ change to

$$T_{2_{opt}} = 15 \text{ days with } \bar{A}_{min} = 1.311 \times 10^{-2}$$

$$T_2 = 44 \text{ days with } \bar{A} = 1.9946 \times 10^{-2}$$

3.2. 3 Effect of Imperfect Testing

In this section, the assumption of perfect testing made in the foregoing sections will be removed, i.e., θ will be changed from unity to $\theta=0.95$ for the purpose of this study. The other parameters are kept the same. Still, the assumption of no false alarm is kept, i.e., $\alpha=0$. Table 3.4 shows the additional impact of imperfect testing results in higher unavailabilities than by assuming perfect testing. The optimum test interval and its associated unavailability are

$$T_{2_{opt}} = 14 \text{ days} \qquad \bar{A}_{min} = 1.4201 \times 10^{-2}$$

If an unavailability goal of $\bar{A}=2\text{x}10^{-2}$ should be maintained, a test interval of $T_2 \leq 38$ days ($\bar{A} = 2.009 \times 10^{-2}$) must be chosen. This must be compared to the 44 days which were found under the perfect testing assumption in the foregoing section in order to see that imperfect testing necessitates shorter test intervals for any given unavailability goal.

TABLE 3.3

Effect of Test Caused Failure on the Test Interval and Associated Unavailability

(λ=3x10^{-5} hr^{-1}; T_c=1.5 hr; T_R=21 hr; β=10^{-2}; P_c=0.75; α=0; θ=1)

T_2	$\bar{A} \times 10^2$
days	-
5	2.1704
10	1.4085
15	1.3111
20	1.357
25	1.4567
30	1.5825
35	1.7226
40	1.8714
50	2.184
250	8.7225

TABLE 3.4

Effect of Imperfect Testing on the Test Interval and Associated Unavailability

($\lambda=3\text{x}10^{-5}\text{hr}^{-1}$; $T_c=1.5$ hr; $T_R=21$ hr; $\beta=10^{-2}$; $P_c=0.75$; $\theta=0.95$; $\alpha=0$)

T_2 days	$\bar{A}$ x 10^2 -
5	2.25
10	1.50
15	1.4208
20	1.4389
25	1.6012
30	1.7444
35	1.9020
40	2.0681
50	2.4151
250	9.5445

3.2.4 Effect of Changing the Probability for Failure During the Test Period

In the foregoing sections, it was assumed that β is equal to $\beta=10^{-2}$. In this section, how the results change when β is increased will be examined. Table 3.5 shows the results for the unavailabilities as function of the test interval when β is increased by a factor of five to $\beta=5\text{x}10^{-2}$, and when perfect testing, $\theta=1$, is assumed. Under these circumstances, the optimum test interval and its associated minimum unavailability increase to

$$T_{2_{opt}} = 18 \text{ days} \quad \text{and} \quad \bar{A}_{min} = 2.4854 \times 10^{-2}$$

As can be seen from this table, there is no way to keep the unavailability goal of $\bar{A}=2\text{x}10^{-2}$ because all values of $\bar{A}$ are larger indeed.

The situation even worsens if the test is imperfect ($\theta=0.95$) as can be seen from Table 3.6. Although the optimum test interval is longer, the minimum unavailability is even higher, i.e.,

$$T_{2_{opt}} = 20 \text{ days} \quad \text{and} \quad \bar{A}_{min} = 2.822 \times 10^{-2}$$

A comparison with Table 3.4 for which θ was also assumed to be $\theta=0.95$ reveals that an increase in β has a remarkable effect on the unavailabilities. If β is even further increased, the unavailability increases even more drastically.

Table 3.7 shows this very clearly where $\beta=10^{-1}$. Although again perfect testing ($\theta=1.0$) is assumed, the larger β results in

TABLE 3.5

Effect of a Change in β
($\lambda=3x10^{-5}$; $T_c=1.5$ hr; $T_R=21$ hr;
$\beta=5x10^{-2}$; $P_c=0.75$; $\theta=1$; $\alpha=0$)

T_2 days	$\bar{A} \times 10^2$ -
5	3.9318
10	2.740
15	2.511
20	2.491
25	2.5497
30	2.6468
35	2.7652
40	2.8966
50	3.182
250	9.4876

TABLE 3.6

Effects of a Change in β and Imperfect Testing
(λ=3x10^{-5}hr^{-1}; T_c=1.5 hr; T_R=21 hr;
β=5x10^{-2}; P_c=0.75; θ=0.95; α=0)

T_2 days	$\bar{A}$ x 10^2 -
5	4.268
10	3.0487
15	2.8293
20	2.822
25	2.8958
30	3.008
35	3.1417
40	3.2885
50	3.6047
250	10.451

TABLE 3.7

Effect of a Change in β and Perfect Testing
($\lambda=3x10^{-5}hr^{-1}$; $T_c=1.5$ hr; $T_R=21$ hr;
$\beta=10^{-1}$; $P_c=0.75$; $\theta=1$; $\alpha=0$)

T_2 days	$\overline{A}$ x 10^2 -
5	6.045
10	4.357
15	3.9702
20	3.8719
25	3.887
30	3.9454
35	4.0378
40	4.1484
50	4.401
250	10.43

much higher unavailabilities than those summarized in Tables 3.5 and 3.6. For this case, the optimum test interval increases to

$$T_{2_{opt}} = 22 \text{ days}$$

and the associated unavailability becomes

$$\bar{A}_{min} = 3.8673 \times 10^{-2}$$

The results of the study concerning the impact of the probability of failure during testing are summarized in Figure 3.2 for perfect testing. It can be clearly seen from the curves in this figure that the value of β plays a major role. In fact, if β increases, a given unavailability goal may not be reached anymore no matter what test interval is chosen.

It becomes apparent from both Figures 3.1 and 3.2 that for any given availability goal $\bar{A} \neq \bar{A}_{min}$ but $\bar{A}>\bar{A}_{min}$ there exist two test intervals, one which is shorter than $T_{2_{opt}}$ whereas the other is longer. Due to the fact that costs, manpower and services are required for performing these tests and all of these quantities certainly increase with the test frequency, there seems to be a strong economic incentive to select the longer test interval as long as the availability goal is met for all possible conditions in nuclear plant life. Only if it is absolutely mandatory to achieve the lowest unavailability possible is it important to determine the optimum test interval.

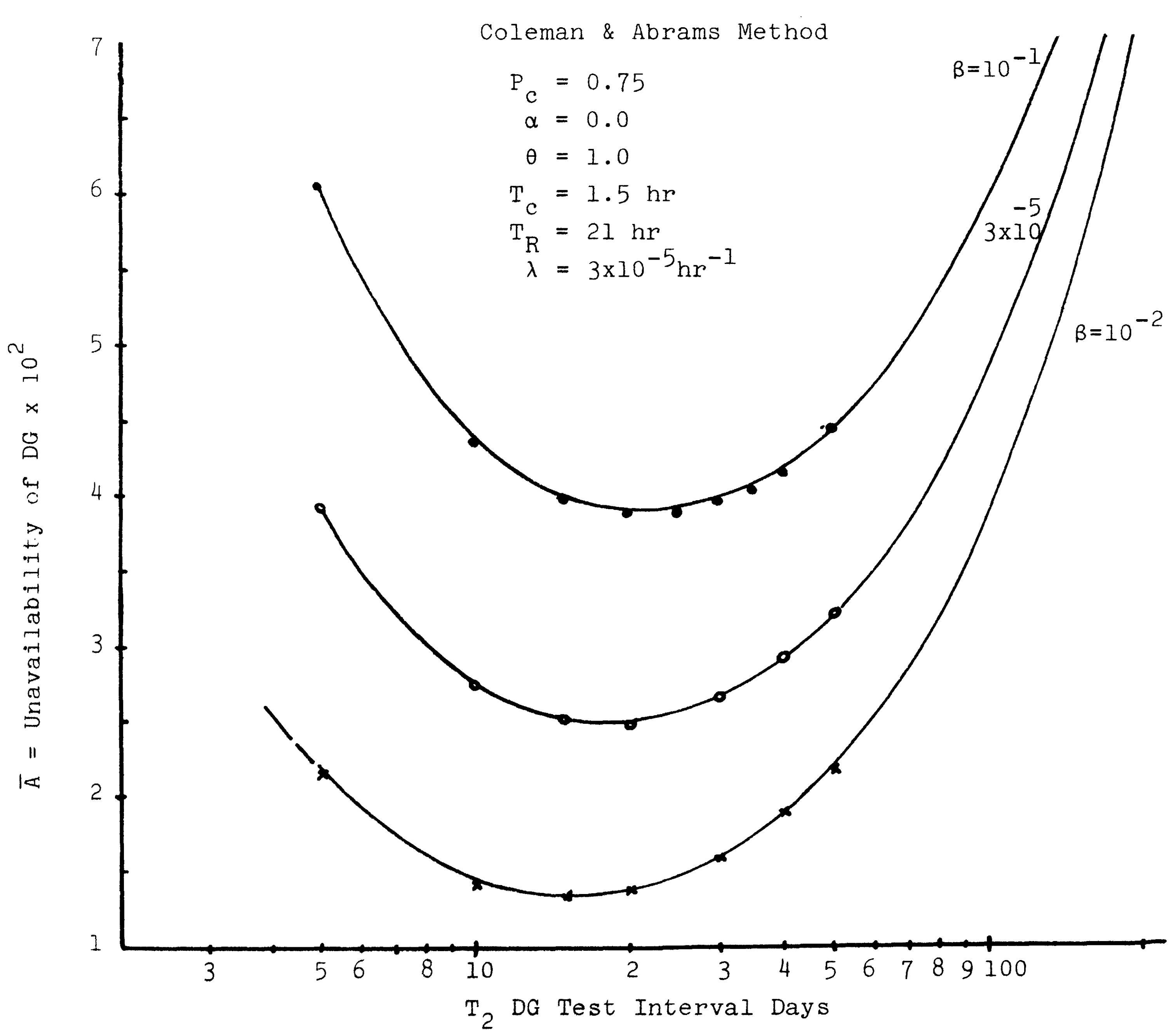


Figure 3.2: Variation of the Unavailability as Function of T_2 for Different Values of the Parameter β

3.2.5 Fixed Availability Goal

For the diesel generator unit, an unavailability goal of $\bar{A}=2x10^{-2}$ is selected. This is the result from the survey that has been performed on D.G. failures in U.S. nuclear power plants during this research. Appendix A summarizes the findings which generally agree with the review reported in [27].

It should be noticed that our results are obtained by averaging over all different kinds of D.G. units by applying point estimates. By using the exponential failure density function, the mean availability was found to be A=0.9726, with standard deviation of 0.0214. Therefore, the unavailability goal of $\bar{A}=2x10^{-2}$ seems to be reasonable.

Table 3.8 shows the test interval which would assure keeping the goal of $\bar{A}=2x10^{-2}$ as a function of the failure rate, λ. As can be seen, the test interval can be substantially increased if the failure rate can be reduced. The data of Table 3.8 are graphically represented in Figure 3.3.

From the discussions in the foregoing sections, the following data were obtained for the test intervals which would maintain a given unavailability goal of $\bar{A}=2x10^{-2}$.

a) $\lambda=3x10^{-5}hr^{-1}$; $T_c=1.5$ hr; $T_R=21$ hr

1) $\theta = 1$

2) $\alpha = 0$

3) $P_c = 1 \quad \beta = 0$

$T_2 = 52$ days $\qquad \bar{A} = 1.9965 \times 10^{-2}$

TABLE 3.8

Effect of Failure Rate on Test Interval to Assure A Given Unavailability of $\bar{A} = 2 \times 10^{-2}$

$\lambda \times 10^6$	T_2	$\bar{A} \times 10^2$
hr^{-1}	days	-
1	>365	2.00
5	335	2.0063
10	165	2.0007
30	52	1.9965
42	36	2.0061
60	23.5	2.0000
100	11	2.0098

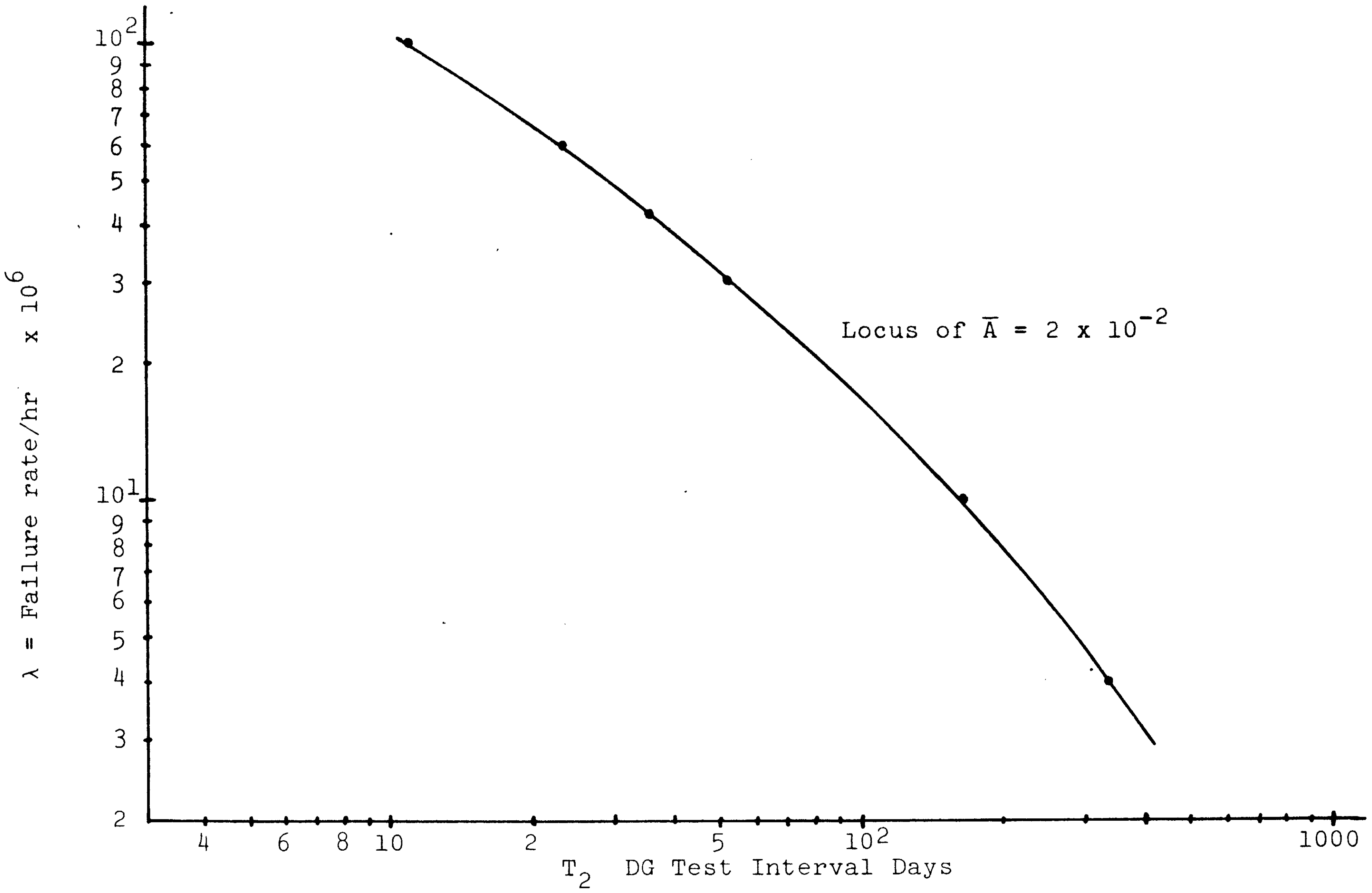


Figure 3.3: Variation of T_2 as Function of λ for a Constant Unavailability Goal of 2×10^{-2}

b) $\lambda=3\text{x}10^{-5}\text{hr}^{-1}$; $T_c=1.5$ hr; $T_R=21$ hr; $\beta=10^{-2}$; $P_c=0.75$

1) $\theta = 1$

2) $\alpha = 0$

$T_2 = 44$ days $\bar{A}=1.9946 \times 10^{-2}$

c) $\lambda=3\text{x}10^{-5}\text{hr}^{-1}$; $T_c=1.5$ hr; $T_R=21$ hr; $\beta=10^{-2}$; $P_c=0.75$; $\theta=0.95$

1) $\alpha = 0$

$T_2 = 38$ days $\bar{A} = 2.0009 \times 10^{-2}$

An increase in β leads to unavailabilities which are larger than $2\text{x}10^{-2}$. Therefore, under these conditions the unavailability goal cannot be kept.

3.3 Optimum Test Interval Prediction Following Jacobs' Method

By assuming that the time it will take to test and repair or renew the system is on the average T_c and that no failure can occur during testing, Jacobs showed that the optimum test interval can be approximately calculated from

$$T_{2_{opt}} = \sqrt{\frac{2T_c}{\lambda}} \quad \text{when } \lambda T_2 \leq 0.1 \qquad (3.6)$$

as was demonstrated in the derivation presented in Chapter 2.4.

Table 3.9 summarizes the values for $T_{2_{opt}}$ obtained from Eq. (3.6) for $T_c=1.5$ hr for various failure rates. It should be noticed that the data given for $T_{2_{opt}}$ are rounded to the nearest whole day since testing will be performed on this basis.

TABLE 3.9

Optimum Test Interval Derived from Jacobs' Formula as Function of the Failure Rate

$(T_c = 1.5 \text{ hr})$

$\lambda \times 10^6$	T_{2opt}	$\bar{A}_{min} \times 10^2$
hr^{-1}	days	-
1	72	0.173
5	32	0.386
10	23	0.545
30	13	0.943
42	11	1.114
60	9	1.33
100	7	1.713

By comparing these results with those given in Table 3.2 for the Coleman and Abrams Method, one can conclude that Eq. (3.6) is indeed quite adequate for finding the optimum test interval for straight base cases, although the neglection of the repair time contribution by Jacobs leads to somewhat shorter test intervals and lower minimum unavailabilities.

However, it should be noticed that Jacobs' results deviate substantially when imperfect testing, long repair times, failure during testing, etc., must be considered. However, for perfect testing and $T_R=0$, Jacobs' equation is a special case of Coleman and Abrams' more general question.

3.4 Optimum Test Interval Prediction Following Hirsch's Method

Hirsch [2] developed a methodology for determining the maximum allowable test duration and the required test interval as a function of the availability design goal. He started out by noticing that the availability design goal of a system which actually expresses the probability that the system will be available when needed is at the same time also a measure of the allowable downtime permitted. Since a portion of the unavailability is due to the test duration and another contribution is associated with the predicted probable failures, the assigned unavailability goal is the sum of both contributions, i.e.,

$$G = \bar{A}_F + \bar{A}_T \qquad (3.7)$$

where

$\bar{A}_F$: unavailability due to failures during the active part of the interval

$\bar{A}_T$: unavailability during test with part of the system bypassed

In accordance with Section 4.11 of IEEE-279 [28], the system unavailability during bypass must be commensurate with the unavailability of the system for the entire interval if no bypass were applied. Therefore, Hirsch set

$$\bar{A}_F = \bar{A}_T \tag{3.8}$$

and then developed formulas for the "one-out-of-two" logic and the "one-out-of-two, twice" logic. In addition, the procedure was extended to cover the "two-out-of-three" and "two-out-of-four" logic configurations.

Here, the analysis is continued for a single component. With

$$\bar{A}_T = \frac{T_c}{T_2} \tag{3.9}$$

and

$$\bar{A}_F = \lambda(T_2 - T_c) \tag{3.10}$$

one gets

$$\lambda(T_2 - T_c) = \frac{T_c}{T_2}$$

from which the optimum test interval follows as

$$T_{2_{opt}} = \frac{1}{2}[T_c + \sqrt{T_c^2 + \frac{4T_c}{\lambda}}] \tag{3.11}$$

With T_c chosen to be T_c=1.5 hr, Table 3.10 summarizes the results for $T_{2_{opt}}$ and their related minimum availabilities for different failure rates, λ. A comparison with the previous data indicates that the results obtained by Hirsch's method when applied to a single component system differ substantially from those obtained by using the Coleman and Abrams or Jacobs methodologies. The main reason for this is thought to lie in the fact that Hirsch developed his method for redundant systems whereas it was applied to a single component here.

3.5 Optimum Test Interval Following Vesely's Method Implemented into the FRANTIC-code

Because the FRANTIC code will be used extensively in the next chapter for the analysis of the optimum test intervals of redundant, multi-component systems, it seems to be appropriate to see what method it uses and how it compares to the approaches previously discussed for a single component system.

FRANTIC uses the common approximation to the exponential function

$$e^{-x} \approx 1-x$$

to arrive at the unavailability of a component between the tests

$$\bar{A} = \lambda(T_2 - T_c)$$

where T_c is understood as the average on-line test time. Due to the fact that the FRANTIC code considers both test as well as

TABLE 3.10

Optimum Test Interval Derived from Hirsch's Method as Function of the Failure Rate

(T_c = 1.5 hr)

$\lambda \times 10^6$	$T_{2_{opt}}$	$\bar{A}_{min} \times 10^2$
hr^{-1}	days	-
1	51	0.1224
5	23	0.273
10	16	0.386
30	9	0.694
42	8	0.781
60	7	0.893
100	6	1.04

repair contributions to the unavailabilities, two separate expressions are used in the code, namely

for the unavailability during test time T_c:

$$q_1 = P_f + (1-P_f)q_o + (1-P_f)(1-q_o)\bar{A} \qquad (3.12)$$

for the unavailability during repair time T_R

$$q_2 = P_f + (1-P_f)\bar{A} + \frac{1}{2}(1-P_f)(1-\bar{A})\lambda T_R \qquad (3.13)$$

where

P_f: probability of test caused failure

q_o: test override unavailability

The average unavailability of the component over a period of one test interval is

$$\bar{q} = \frac{1}{2}\lambda T_2 + q_1 \frac{T_c}{T_2} + q_2 \frac{T_R}{T_2} \qquad (3.14)$$

by using the results for q_1 and q_2 from Eqs. (3.12) and (3.13). The optimum value of T_2 is found by using Eqs. (3.12) through (3.14) and performing

$$\left(\frac{\partial \bar{q}}{\partial T_2}\right)_{q_1} = 0 \qquad (3.15)$$

which leads to

$$T_{2_{opt}} = \sqrt{\frac{2T_c q_1}{\lambda} + 2(1-P_f)T_R} \qquad (3.16)$$

In this derivation, q_1 is assumed to be independent of T_2. Moreover, a term by term comparison of the two terms under the square root reveals that the second term is negligible for all practical purposes unless the failure rate is abnormally high. Therefore, by assuming $P_f=1$ and $q_o=1$, one obtains

$$T_{2_{opt}} = \sqrt{\frac{2T_c}{\lambda}} \qquad (3.17)$$

because $q_1=1$. Eq. (3.17) shows that Vesely obtains the same formula as Coleman and Abrams as well as Jacobs for the condition stated above. Therefore, it seems to be unnecessary to perform a great deal of additional calculations for Vesely's method. The optimum test interval for the data of the base case is

$$T_{2_{opt}} = 13 \text{ days}$$

and follows from Eq. (3.17) as well as Eq. (3.6). This compares favorably with the value of 14 days obtained by using the Coleman and Abrams approach as shown in Table 3.2.

3.6 Comparison of Different Methods for the Prediction of the Optimum Test Interval

Figure 3.4 summarizes graphically the findings of this chapter by comparing the optimum test interval as function of the failure rate for the following three methods: Coleman and Abrams, Jacobs, and Hirsch. In this context, it should be remembered that the method by Vesely gives the same values as presented by the line generated by Jacobs' method if $q_o=1$ and perfect testing is assumed.

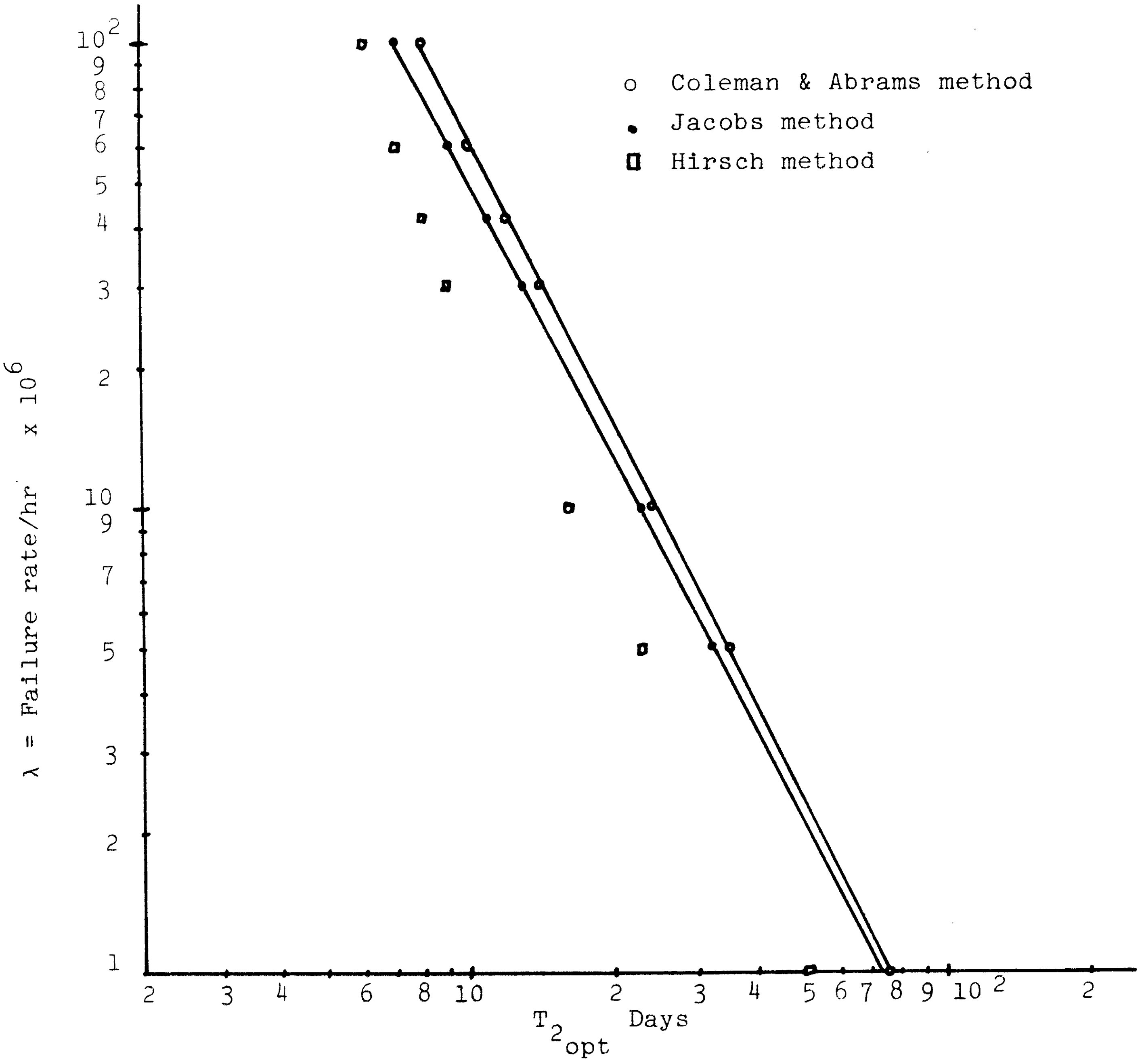


Figure 3.4: Comparison of Three Different Methods for the Determination of the Optimum Test Interval as Function of λ

Figure 3.4 shows that the results by Coleman and Abrams and those by Jacobs are very close to each other. The results obtained from Hirsch's method deviate from the other two by giving two short optimum test intervals as compared to the other methods.

For the data selected for the base case, $\lambda=3x10^{-5}$ hr^{-1}, $T_c=1.5$ hr, and $T_R=21$ hr, the optimum test interval found in this study ranges from 13 to 15 days depending on the method applied. This results in a minimum unavailability of $1.00x10^{-2}$.

On the other hand, by selecting the unavailability goal of $2x10^{-2}$, the test interval will increase to between 38 and 52 days depending on the perfectness of the test.

Finally, it can be concluded that for most practical purposes Jacobs' method gives reliable results for $T_{2_{opt}}$ as long as the circumstances validate its underlying assumptions. The expression given by Coleman and Abrams offers the highest flexibility when additional effects are to be studied and more accurate results about the repair time effect are desired.

4. STUDY OF THE OPTIMUM TEST INTERVAL FOR MULTICOMPONENT SYSTEMS --EXAMPLE: AUXILIARY FEEDWATER SYSTEM

4.1 Introduction and Aux-Feed-System Description

It was shown in the foregoing chapters that analytical procedures for estimating the optimum test interval only exist for single component systems. Although at least Hirsch's methodology [2] allows consideration of redundant situations, his formulas were developed only for redundant systems consisting of identical components. Therefore, the expressions given by Hirsch are only of limited usefulness for systems such as the Aux-Feed-System which, in its most primitive representation is shown in Figure 4.1, would consist of 2 D.G.s and a pump in parallel. This system can be described as a one-out-of-three system, i.e., functioning of any one of the three paths leads to system success. As Figure 4.1 shows, two paths require that one of the diesel generators functions while the third mandates that both valves and the pump are operational because they are in series.

From the very simple system configuration shown in Figure 4.1, it is an easy task to develop the fault tree of the Aux-Feed-System as depicted in Figure 4.2. The numbers in the fault tree correspond to the component numbers of Figure 4.1. From the fault tree the system logic function can be easily determined by inspection. This function is needed as input to the FRANTIC code because it does not have fault tree analysis capability. In terms of the FRANTIC nomenclature, the system logic function is given by

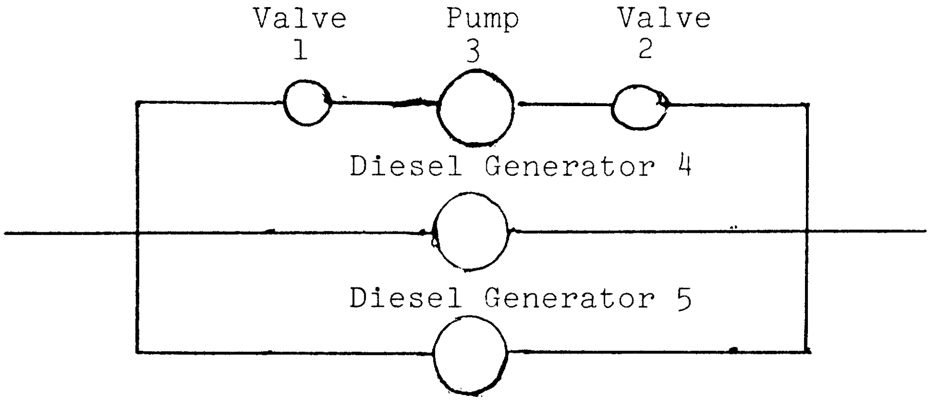


Figure 4.1: Simplified Aux-Feed System

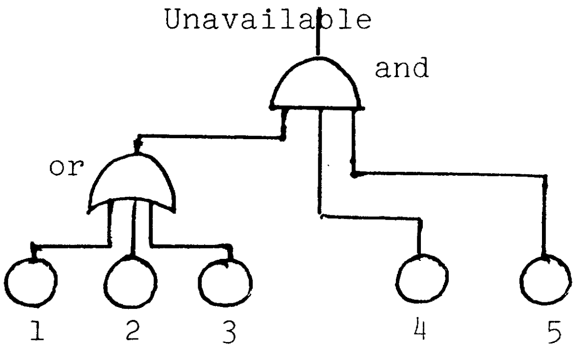


Figure 4.2: Fault Tree for the Simplified Aux-Feed System

$$QS = \{1.0-[1.0 - QC(1)] * [1.0 - QC(2)] * [1 - QC(3)]\} * [QC(4)] * [QC(5)] \qquad (4.1)$$

where QS = system unavailability
$QC(i)$ = unavailability of the i^{th} component

NOTE: The numbers in parentheses correspond to the component numbers in Figure 4.1.

It must be noticed that the unavailability of the i-th component QC(i) is a function of many parameters, not only of the component itself but also of the type of testing, effectiveness of the test, and the probability of test caused failure. Table 4.1 summarizes the input data to the FRANTIC code which are kept constant during this study. Only the test interval and the staggering times are varied.

Whereas most of the quantities in Table 4.1, such as failure rate, average test time, and probability of a test caused failure are self-explanatory, a few others need more clarification. For example, the override unavailability refers to the probability that the component, while being tested, cannot be switched back to its safeguard function. A value of $q_o=1$ means that the component cannot be used for its designed function while it is being tested. The detection inefficiency is the probability for a failure of a component's not being detected during the test. In the FRANTIC code, this situation is treated by considering the undetected failure rate as the product of the component

TABLE 4.1

Symbols and Typical Values Which Are Used in FRANTIC Code

λ -	component failure rate (x 10^{-6} hr^{-1})	= .3
T_2 -	component test interval (days)	= 38 days
T_1 -	initial component test interval used for staggering purpose (days)	=
T_c -	testing time (hrs)	= 1.5
T_R -	repair time (hrs)	= 7.0
q_o -	override unavailability	= 1.0
P_t -	probability of test induced failure	
p -	undetermined failure rate (10^{-6} hr^{-1})	
q_d -	residual unavailability	

TOTAL UMEAN - Aux-Feed-System mean unavailability for 1-year period failure rate, λ, and the detection inefficiency, i.e.,

$$\lambda_\mu = \lambda \cdot p \qquad (4.2)$$

where

λ_μ : undetected failure rate

λ : component failure rate

p : detection inefficiency

The objective of this study is to optimize the availability, i.e., minimize the unavailability of the Aux-Feed-System by finding the optimum test intervals while keeping the other components and testing characteristics constant as shown in Table 4.1.

4.2 Strategies for the Optimization of Test Intervals

Procedures for determining the optimum test interval for simple systems such as a single-component system or a two-component parallel system were already discussed and used in Chapter 3. As has been already indicated there, no analytical methods exist at present which allow explicit determination of the optimum test interval for large and complex systems. Therefore, the methods of Hirsch, Jacobs, and Coleman and Abrams are used again, this time to find the test intervals of the components, while the resulting system mean unavailability is determined by the FRANTIC code by using these test intervals as input. These results will the be compared to those resulting from an iterative search for the optimum test interval.

The basis of all comparisons presented in what follows is the system mean unavailability with due consideration given to the peak unavailability during the period of interest which is one year. Although it is acknowledged that the selection of test intervals should be related to risk and consequences, the present study is solely based on the mean and peak system unavailabilities.

4.3 Optimum Test Interval Determination for Components

4.3.1 Hirsch's Methodology

By using the availability design goals of the standard IEEE-279 [28], Hirsch developed a method for determining test intervals and allowable bypass time for several simple system configurations as already discussed in Chapter 3. For the purpose of the present study, the bypass (testing) time is considered predetermined and only the testing interval needs to be calculated. According to IEEE-279, the system unavailability due to testing must be commensurate to the system unavailability and is the sum of these two components as stated by Eq. (3.7). When the bypass time is considered variable, both the bypass time and the test interval are determined by the system configuration (for example, one-out-of-two), component failure rates, and the design goal. When the bypass time is given along with the system configuration and component failure rates, the test interval and system unavailability are determined.

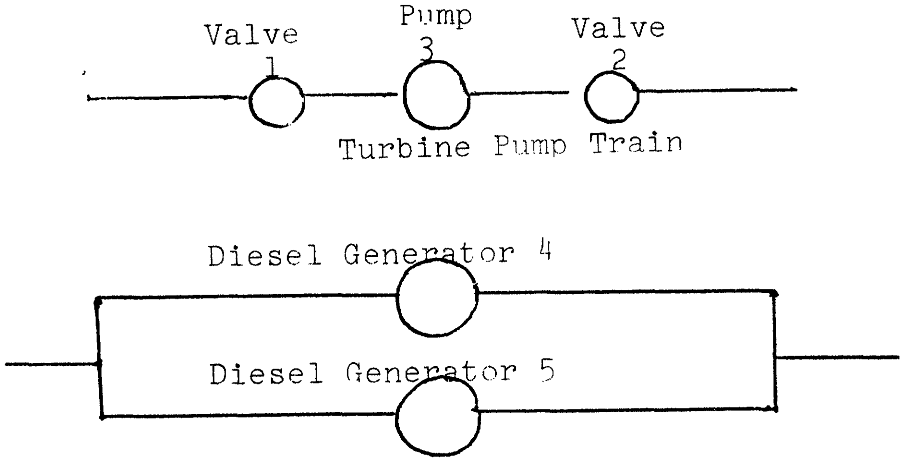


Figure 4.3: Subsystems of the Simplified Aux-Feed System

Unfortunately, Hirsch did not develop an expression for the one-out-of-three type of configuration which is the main characteristic of the Aux-Feed-System. However, in order to be able to apply Hirsch's methodology despite the nonexistence of a special expression for the one-out-of-three system, the Aux-Feed-System is being broken down into two subsystems as shown in Figure 4.3. One subsystem is the one-out-of-two diesel generator subsystem; the other is the turbine pump chain. The analytical method is applied as follows.

For the turbine pump chain, the system can be partitioned to an equivalent subsystem describing this series. Since an exponentially distributed failure has been assumed throughout this analysis, the failure rate, λ, for this series system is the sum of its component failure rates, i.e.,

$$\begin{aligned}\lambda_E &= \lambda_{v_1} + \lambda_{v_2} + \lambda_p \\ &= (0.3 + 0.3 + 3.0) \times 10^{-6}\ \text{hr}^{-1} \\ &= 3.6 \times 10^{-6}\ \text{hr}^{-1} \qquad (4.3)\end{aligned}$$

The testing time, T_c, is assumed to be the same for all components, i.e.,

$$T_c = T_{c_{v_1}} = T_{c_{v_2}} = T_{c_p} = 1.5\ \text{hr} \qquad (4.4)$$

Following the Hirsch method, T_2 is found as

$$T_{2_{opt}} = \frac{\lambda_E T_c - \sqrt{(\lambda_E T_c)^2 + 4\lambda_E T_c}}{2\lambda_E} \qquad (4.5)$$

With the data given above, T_2 follows as

$$T_{2_{opt}} = 646.25 \text{ hr} = 27 \text{ days} \qquad (4.6)$$

For the diesel generator subsystem (one-out-of-two), one can either consult the graphs supplied by Hirsch in [2] for the determination of $T_{2_{opt}}$ or use the following exact expressions for perfect staggered testing among the diesel generators.

With

$$\bar{A}_F = (\tfrac{5}{24})(\lambda T_2)^2 \qquad (4.7)$$

$$\bar{A}_T = \lambda T_c \qquad (4.8)$$

By satisfying Hirsch's requirement

$$\bar{A}_F = \bar{A}_T$$

one can solve for T_2 which follows as

$$T_2 = \frac{1}{\lambda}\sqrt{\frac{24}{5}\lambda T_c} \qquad (4.9)$$

With the data for the diesel generators taken as

$$\begin{aligned} \lambda &= 42 \times 10^{-6} \text{ hr}^{-1} \\ T_c &= 1.5 \text{ hr} \end{aligned} \qquad (4.10)$$

one obtains

$$T_2 = 414.04 \text{ hr} = 17 \text{ days} \tag{4.11}$$

The testing of the diesel generators according to the perfect staggered testing is shown on the time scale shown in Figure 4.4. It should be noticed that the testing time of 1.5 hr is not shown on this scale.

4.3.2 Jacobs' Methodology

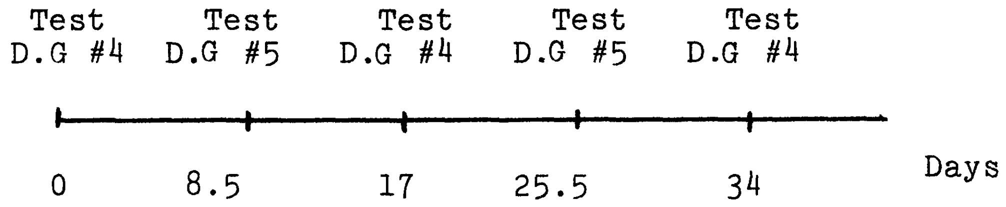
For a single component, Jacobs has determined the optimum test interval as a function of the failure rate, λ, and testing time, T_c. This test interval results in a minimum mean unavailability for the component. It will later be shown as for the other cases, that this test interval for the component differs from the test interval for the component when it is considered part of the system which is minimized.

The equation below can be solved to find the optimum single component test interval when both the failure rate and testing time are given.

$$\frac{1}{\lambda T_2^2}\,[e^{-\lambda(T_2-T_c)}(1+\lambda T_2)] - \frac{1}{\lambda T_2^2} = 0 \tag{4.12}$$

This function is transcendental and is not quickly solved without computer aid. Therefore, it is simplified according to the assumption that,

$$\lambda T_c \ll 1$$



NOTE: Testing time is 1.5 Hrs. and is not shown on time scale.

Figure 4.4: Time Scale for Staggered Test Procedure

to yield,

$$T_2 = \sqrt{\frac{2T_c}{\lambda}} \tag{4.13}$$

This formula is quite simple in nature since it does not account for the effects of repair time, test inefficiency, and other contributors to the components' unavailability.

Using Eq. (4.13), the test intervals for the Aux-Feed-System components are determined. It should be recalled that the valves and pump of the system must be tested simultaneously and, therefore, the equivalent failure rate, λ_E, is used for this part of the Aux-Feed-System. Table 4.2 below summarizes the results.

TABLE 4.2: TEST INTERVAL CALCULATED USING JACOBS' METHODOLOGY

Component	$\lambda(10^{-6}\ hr^{-1})$	T_c (hrs)	T_2 (days)
Diesel Generator 4	42	1.5	11
Diesel Generator 5	42	1.5	11
Pump Valve Chain	3.6	1.5	38

NOTE: The test interval, T_2, is rounded off to the nearest whole day since testing will be on this basis.

4.3.3 Coleman and Abrams Methodology

As discussed already in Chapter 3, these authors developed the most comprehensive expression for the component availability. For the present study, the following assumptions are made

$\beta = 0$, i.e., system does not fail during test

$\alpha = 0$, i.e., no false alarm

$\theta = 1$, i.e., perfect testing

which simplify Eq. (3.1) to the following expression for the availability

$$A = \frac{1-e^{-\lambda T_2}}{\lambda[T_2+T_c+T_R(1-e^{-\lambda T_2})]} \qquad (4.14)$$

$$\bar{A} = 1 - A$$

By using Eq. (4.14), the unavailability $\bar{A}$ is calculated for each component of the Aux-Feed-System.

Table 4.3 summarizes the results of these calculations for all components for a series of test intervals. These unavailabilities are plotted versus T_2 in Figure 4.5 for the pump, valves, and pump-valve chain, whereas Figure 4.6 shows $\bar{A}$ vs. T_2 for the diesel generators. By noticing where the minima occur, the test intervals for the diesels and the pump-valve chain are determined. The pump-valve chain is used rather than the individual components since they must be tested coincidentally. Table 4.4 summarizes the resultant test intervals.

TABLE 4.3

AUX-FEED-SYSTEM COMPONENT UNAVAILABILITIES AS A FUNCTION OF TEST INTERVAL

Component Test Interval (Days)	Pump (10^{-3})	Valve (10^{-3})	Unavailability Pump Valve Chain (10^{-3})	Diesel Generator (10^{-3})
7	--	--	--	1.32
10	--	--	--	1.2
12	--	--	--	1.2
14	--	--	--	1.2
15	--	--	4.9	1.25
20	3.9	--	4.0	1.4
25	3.4	--	3.6	1.6
30	3.2	2.2	3.4	1.8
35	3.1	1.9	3.35	--
40	3.1	1.7	3.34	--
45	3.1	1.6	3.4	--
50	3.1	1.4	3.5	--
60	3.3	1.3	3.7	--
80	3.7	1.1	4.3	--
100	4.3	.99	--	--
120	--	.95	--	--

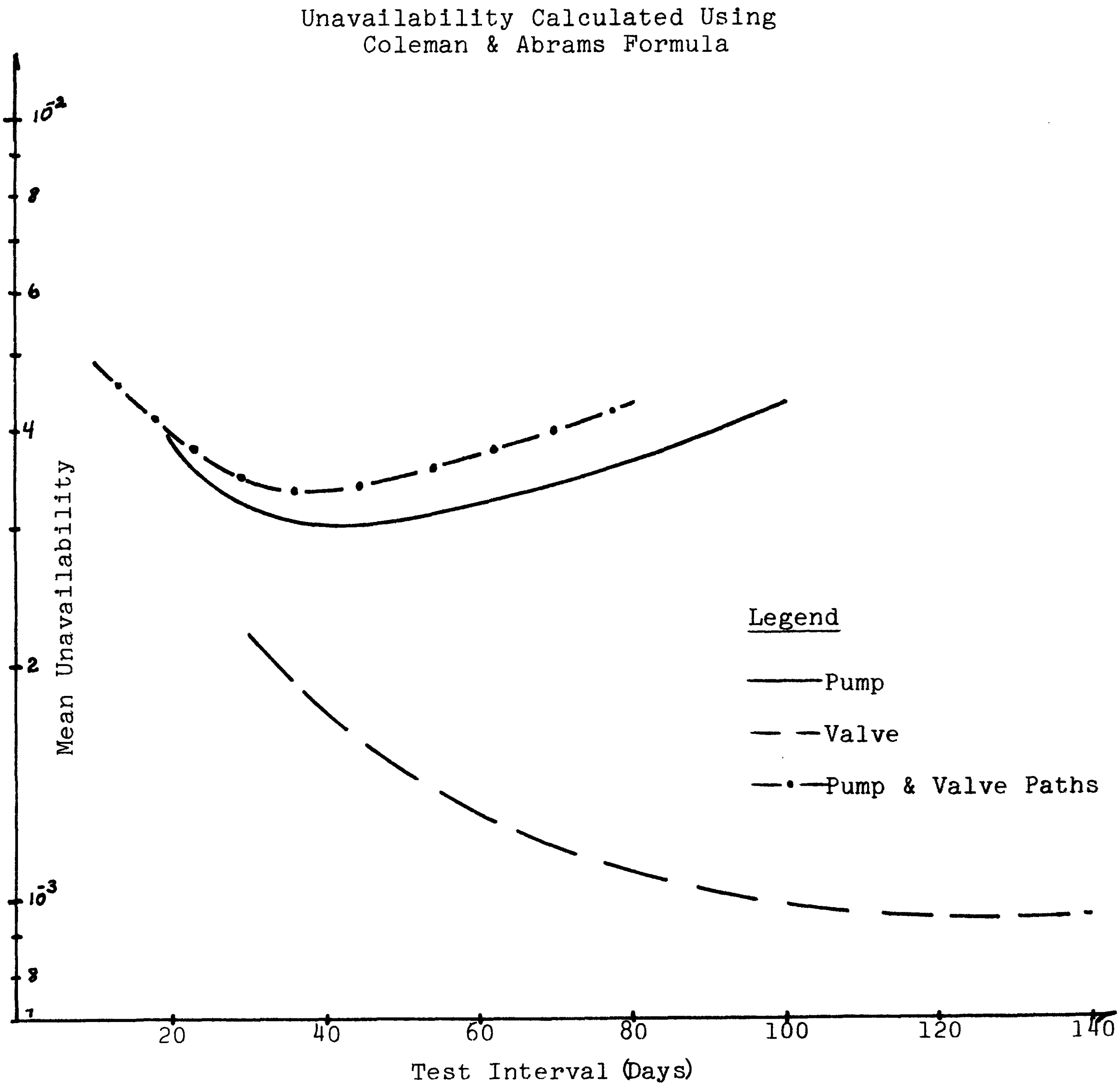


Figure 4.5: Aux-Feed-System--Unavailability for Individual Components as a Function of Test Interval

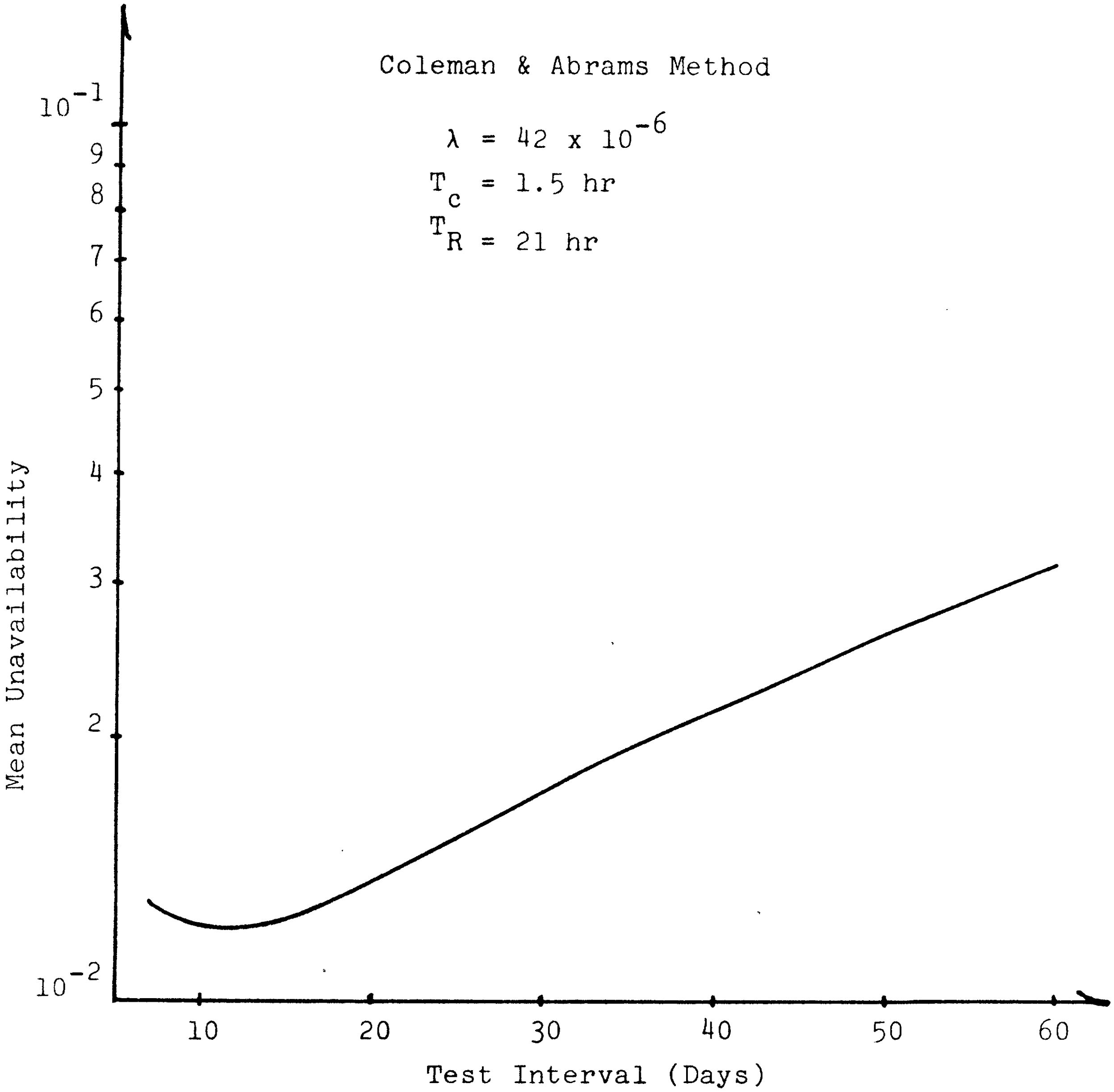


Figure 4.6: Aux-Feed-System -- Diesel Generator Unavailability as a Function of Test Interval

TABLE 4.4

OPTIMUM TEST INTERVALS CALCULATED USING
COLEMAN AND ABRAMS METHODOLOGY

Component	$(10^{-6}\ hr^{-1})$	T_c	T_R	T_2
Diesel Generator	42	1.5	21	12
Pump-Valve Chain	3.6	1.5	17	38

The resultant test intervals for the components as computed by using the methods of Hirsch, Jacobs, and Coleman and Abrams are summarized below in Table 4.5.

TABLE 4.5

OPTIMUM COMPONENT TEST INTERVALS (DAYS)

Method Component	Hirsch	Jacobs	Coleman and Abrams
Diesel Generator	17	11	12
Pump-Valve Chain	27	38	38

The methods of Jacobs and Coleman and Abrams agree quite closely since the objective of these two methods is to optimize the test interval versus the method of Hirsch which has as its objective to meet an unavailability goal for the system. Hirsch's method also uses the IEEE-279 requirement that unavailability due to testing be equal to the unavailability due to failure.

4.4 Determination of the System Unavailability by FRANTIC

The next step is to input these test intervals along with the component and testing characteristics in to the FRANTIC code and to calculate the resultant Aux-Feed-System unavailability. The FRANTIC code does not compute or determine optimum test intervals but rather determines the system unavailability due to test intervals.

For redundant systems, staggering is used to prevent testing the total system at one time, which results in the unavailability being unity. The actual method of staggering itself can have great effects on the system unavailability. Two methods of staggering are used here to show the upper and lower bounds of the Aux-Feed-System unavailability for each of the three methods used to calculate test intervals. In FRANTIC, staggering is handled by the input value of T_1. T_1 represents the first test interval for that component while T_2 is the test interval which was calculated using the methods previously cited.

The first type of staggering used is the simultaneous method. Since the diesels are tested on the same test basis, one diesel should be tested before the other to avoid large unavailabilities due to coincident testing. Therefore, simultaneous testing is used. Simultaneous testing means that after one diesel has been fully tested, the other diesel is tested immediately. To avoid testing either diesel at the same time as the pump and valves, the diesels must be staggered relative to the pump tests also. Because of this, T_1 for diesel #4 is 0.063 days (1.5 hrs = T_c) and T_1 for diesel #5 is 0.13 days (3.0 hrs = $2T_c$). Simultaneous testing yields an upper bound for system unavailability.

To determine the lower bound for the Aux-Feed-System unavailability, the method of perfect staggering is used. Since the test intervals,T_2, of the diesels are equal but are different from the test interval of the pump and valves, perfect staggering is applied to the diesels only. In perfect staggering, the first test interval, T_1, for one diesel is set equal to the actual test interval, T_2, divided by 2 since there are two diesel generators. The resultant initial test interval, T_1, for the methods of Jacobs and Hirsch are not whole numbers but have been rounded off to the nearest whole number of days. Again, to alleviate any possibility of coincidentally testing either diesel with the pump and valves, T_1 for each diesel has been offset by 0.063 days (T_c = 1.5 hrs).

Tables 4.6 and 4.7 show the results of the FRANTIC calculation,along with the inputs, for each of the three methods of test interval determination. Table 4.6 gives the results for simultaneous testing while Table 4.7 gives the results for perfect staggering.

The nomenclature used in these tables is explained below:

$\bar{A}_F$: mean system unavailability due to failure

$\bar{A}_T$: mean system unavailability due to testing

$\bar{A}_R$: mean system unavailability due to repair

$\bar{A}_{Total}$: total mean system unavailability

TABLE 4.6

Unavailability Calculations by Using the FRANTIC Code for the Aux-Feed-System, Simultaneous Testing (q_o=1; P_f=0; p=0; q_d=0)

HIRSCH METHOD

Component #		$\lambda x10^6 hr^{-1}$	T_2 day	T_1 day	T_c hr	T_R hr
1	Valve	0.3	27		1.5	7
2	Valve	0.3	27		1.5	7
3	Pump	3.0	27		1.5	19
4	Diesel	42	17	0.063	1.5	21
5	Diesel	42	17	0.13	1.5	21

$\bar{A}_{Total}$	$\bar{A}_F$	% of $\bar{A}_{Total}$	$\bar{A}_T$	% of $\bar{A}_{Total}$	$\bar{A}_R$	% of $\bar{A}_{Total}$
$1.928x10^{-6}$	$1.813x10^{-7}$	9.4	$1.724x10^{-6}$	89.44	$2.223x10^{-8}$	1.15

$\bar{A}_{peak}$	Time	Time between peaks
$2.253x10^{-3}$	323 d	varies

JACOBS METHOD

Component #		$\lambda x10^6 hr^{-1}$	T_2 day	T_1 day	T_c hr	T_R hr
1	Valve	0.3	38		1.5	7
2	Valve	0.3	38		1.5	7
3	Pump	3.0	38		1.5	19
4	Diesel	42	11	0.063	1.5	21
5	Diesel	42	11	0.13	1.5	21

$\bar{A}_{Total}$	$\bar{A}_F$	% of $\bar{A}_{Total}$	$\bar{A}_T$	% of $\bar{A}_{Total}$	$\bar{A}_R$	% of $\bar{A}_{Total}$
$3.408x10^{-6}$	$9.915x10^{-8}$	2.91	$3.29x10^{-6}$	96.56	$1.816x10^{-8}$	0.53

$\bar{A}_{peak}$	Time	Time between peaks
$3.203x10^{-3}$	341 d	67 d 1st 4 peaks

COLEMAN AND ABRAMS METHOD

Component #		$\lambda x10^6 hr^{-1}$	T_2 day	T_1 day	T_c hr	T_R hr
1	Valve	0.3	38		1.5	7
2	Valve	0.3	38		1.5	7
3	Pump	3.0	38		1.5	19
4	Diesel	42	12	0.063	1.5	21
5	Diesel	42	12	0.13	1.5	21

$\bar{A}_{Total}$	$\bar{A}_F$	% of $\bar{A}_{Total}$	$\bar{A}_T$	% of $\bar{A}_{Total}$	$\bar{A}_R$	% of $\bar{A}_{Total}$
$3.34x10^{-6}$	$1.182x10^{-7}$	3.54	$3.198x10^{-6}$	95.84	$2.066x10^{-8}$	0.62

$\bar{A}_{peak}$	Time	Time between peaks
$3.307x10^{-3}$	228 d	varies

TABLE 4.7

Unavailability Calculations by Using the FRANTIC Code for the Aux-Feed-System, Perfect Staggered Testing
(q_o=1; P_f=0; p=0; q_d=0)

HIRSCH METHOD

Component #		λ x10^6hr^{-1}	T_2 day	T_1 day	T_c hr	T_R hr
1	Valve	0.3	27		1.5	7
2	Valve	0.3	27		1.5	7
3	Pump	3.0	27		1.5	19
4	Diesel	42	17	0.083	1.5	21
5	Diesel	42	17	8.080	1.5	21

$\bar{A}_{Total}$	$\bar{A}_F$	% of $\bar{A}_{Total}$	$\bar{A}_T$	% of $\bar{A}_{Total}$	$\bar{A}_R$	% of $\bar{A}_{Total}$
3.327x10^{-7}	8.88x10^{-8}	26.72	2.226x10^{-7}	66.92	2.115x10^{-8}	6.36

$\bar{A}_{peak}$	Time	Time between peaks
1.743x10^{-4}	324 d	varies

JACOBS METHOD

Component #		λx10^6hr^{-1}	T_2 day	T_1 day	T_c hr	T_R hr
1	Valve	0.3	38		1.5	7
2	Valve	0.3	38		1.5	7
3	Pump	3.0	38		1.5	19
4	Diesel	42	11	0.083	1.5	21
5	Diesel	42	11	5.080	1.5	21

$\bar{A}_{Total}$	$\bar{A}_F$	% of $\bar{A}_{Total}$	$\bar{A}_T$	% of $\bar{A}_{Total}$	$\bar{A}_R$	% of $\bar{A}_{Total}$
2.159x10^{-7}	4.675x10^{-8}	21.66	1.502x10^{-7}	69.57	1.895x10^{-8}	8.78

$\bar{A}_{peak}$	Time	Time between peaks
7.943x10^{-5}	342 d	38 d for peaks 2 through 7

COLEMAN AND ABRAMS METHOD

Component #		λx10^6hr^{-1}	T_2 day	T_1 day	T_c hr	T_R hr
1	Valve	0.3	38		1.5	7
2	Valve	0.3	38		1.5	7
3	Pump	3.0	38		1.5	19
4	Diesel	42	12	0.063	1.5	21
5	Diesel	42	12	6.060	1.5	21

$\bar{A}_{Total}$	$\bar{A}_F$	% of $\bar{A}_{Total}$	$\bar{A}_T$	% of $\bar{A}_{Total}$	$\bar{A}_R$	% of $\bar{A}_{Total}$
2.463x10-7	5.605x10^{-8}	22.75	1.693x10^{-7}	68.75	2.092x10^{-8}	8.49

$\bar{A}_{peak}$	Time	Time between peaks
7.164x10^{-5}	114 d	114 d 1st 3 peaks

From Tables 4.6 and 4.7 it is obvious that using the optimum test interval as determined by the Jacobs method for perfect staggered test results in the lowest total mean system unavailability of all three methods applied. However, it will be shown in the next section that this unavailability of $\bar{A}_{Total} = 2.159x10^{-7}$ is in fact not a minimum for the Aux-Feed-System. Therefore, it must be concluded that optimum test intervals stemming from single component expressions do not necessarily result in a minimum system unavailability. Hence, these test intervals are not truly optimum with respect to the system as a whole.

Another observation which can be made by comparing these tables is that perfectly staggered testing leads to mean and peak unavailabilities which are by at least an order of magnitude lower than those resulting from simultaneous tests.

4.5 Optimization of the Test Interval by Iteration with FRANTIC

The FRANTIC code does not calculate the optimum test interval for components of a system but rather calculates the system and component mean unavailabilities for a given set of component test intervals. Therefore, in searching for optimum test intervals, various sets of test intervals for each component of the system are systematically input, and FRANTIC outputs the unavailabilities. By observing the output of FRANTIC, the "best" test intervals are determined. These test intervals are those which yield the smallest system unavailability. It is possible that these "best" test intervals are not optimum since at this point there is no analytic means of checking.

In addition, there may be differences between the optimum test interval and those test intervals which are implemented at the plant itself due to scheduling problems. For example, it would be rather difficult to schedule a six-day test interval. Probably this test interval could be changed to a weekly basis without great effect upon the system unavailability. Therefore, the results of two different types of testing are included in this section. The first is a result of testing on a basis without consideration to ease of scheduling, i.e., a test interval of 13 days could result. The second set of test intervals are those which could be scheduled relatively easily, i.e., weekly, biweekly, etc. The results are shown graphically with explanation.

To find the optimum test interval, all components were tested with equal test intervals on a perfect staggering basis. In this case, the staggering dates were not rounded off to the nearest whole day. Since there are three trains and all are tested on an equal interval, the staggering time is:

$$T_2/3 = T_1$$

The first diesel is tested after T_1 days and the second diesel is tested after $2T_1$ days for the first test interval only. The pump is tested with an initial interval of T_2 days. After the first testing of all components, the test intervals are all set to T_2 days, thus perfect staggering. The diesels are tested first since it has been shown that the components with the greatest failure rate should be tested prior to components with smaller testing intervals. This results in smaller unavailabilities.

Figure 4.7 is a plot of the Aux-Feed-System unavailability versus test interval T_2 using perfect staggering. From this graph, it is obvious that there is no "best" test interval because the curve obviously continues to decrease. Attempts were made to test the system's components every 2 days, but the FRANTIC code broke down. It should also be noted that already for the 3-day test interval the code was beginning to have underflow problems, but these were handled by the computer fixup routine.

Figure 4.8 shows a plot of the Aux-Feed-System unavailability versus the pump test interval. In this case, the diesels were tested every 4 days (held constant) and the pump test interval was varied to see its effects. The points plotted are for pump test intervals of integer multiples of the diesel test interval. The test intervals of 10 and 30 days are also included to see this effect, but due to staggering problems these unavailabilities did not lie on the curve. It is possible to lower these unavailabilities using appropriate staggering methods. From this figure, it is apparent that testing the diesels every 4 days according to perfect staggering and the pump every 8 days results in a minimum unavailability of approximately $5x10^{-8}$ which is a considerable improvement over the

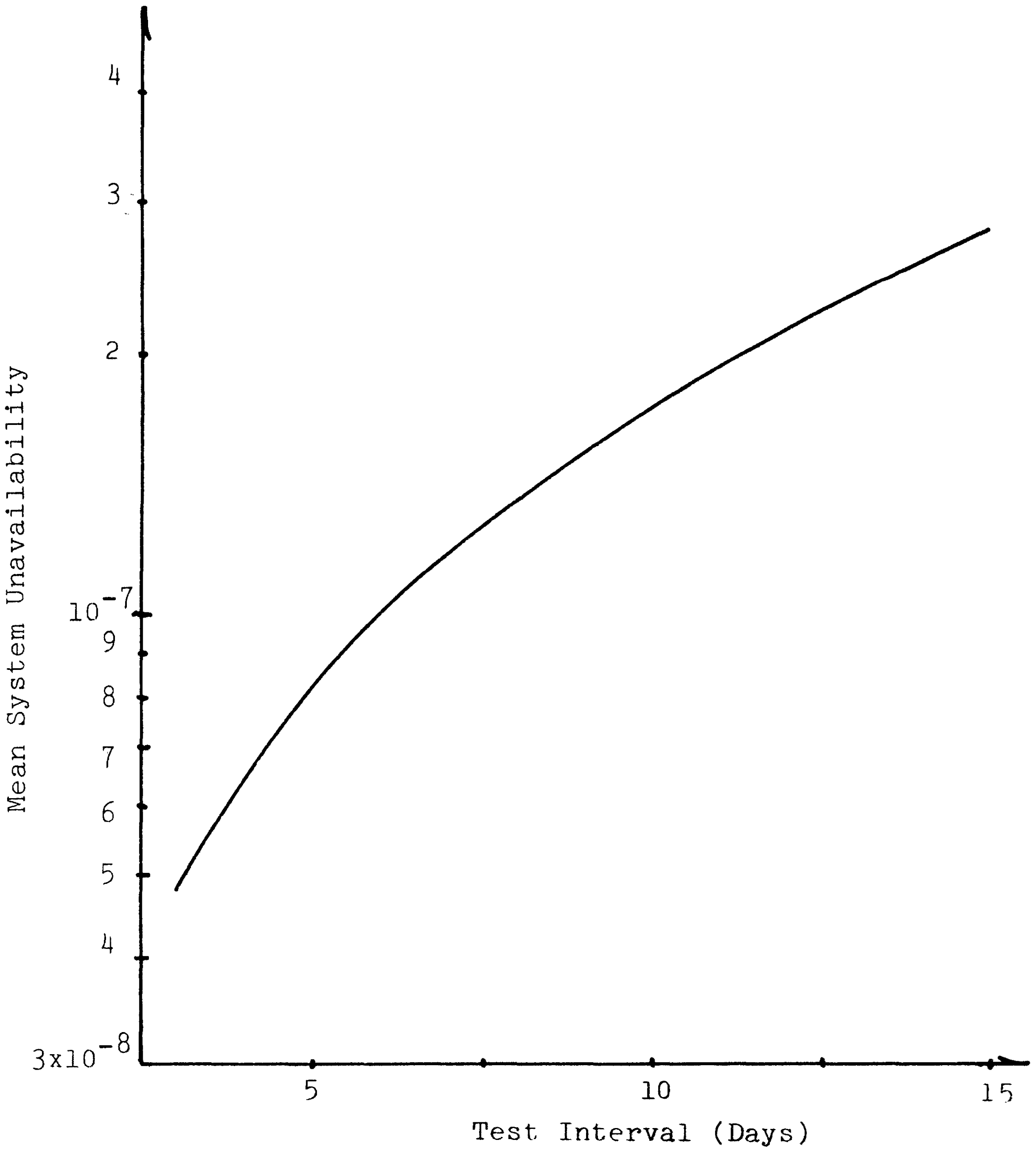


Figure 4.7: Aux-Feed-System -- Unavailability as Function of the Test Interval (All components tested at the same test interval; staggered.)

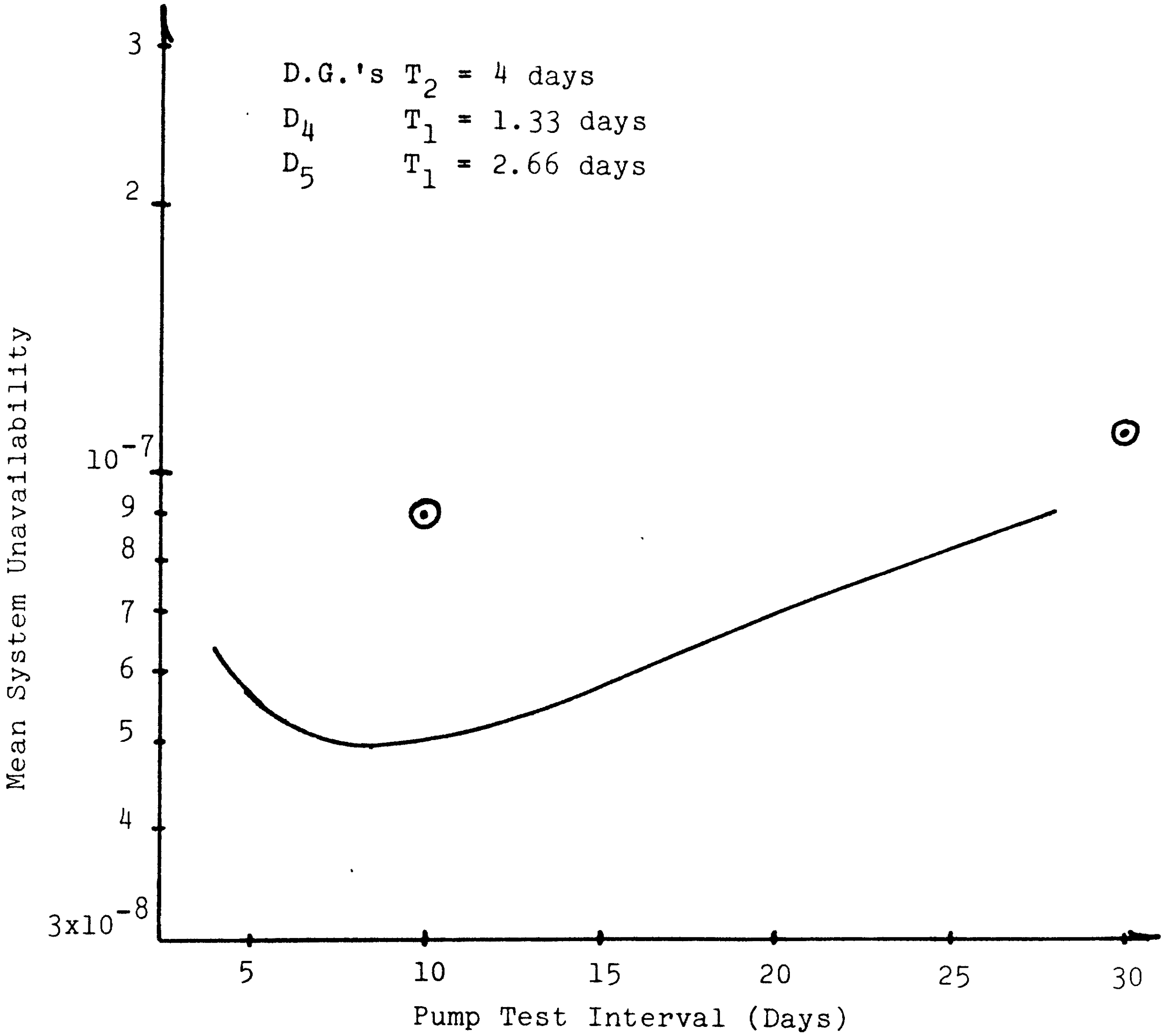


Figure 4.8: Aux-Feed-System -- Unavailability vs. Pump Test Interval

values found by the Jacobs method in Section 4.4 which was $\bar{A}_{Total}=2.159x10^{-7}$. Therefore, it can be concluded that the methods discussed in Section 4.4 do not yield optimum test intervals. In any case, it should be carefully noticed that neither result for the test intervals is implemented at the plant site.

By fully recognizing this difficulty, a study was initiated to investigate test intervals which could be practically scheduled on site. Since the diesel failure rate is not equal to that of the pump-valve train, tests were not only done on an equal test basis for all components but the pump test was also varied holding the diesel test interval constant. The basic test intervals, T_2, for the diesels were selected as 7, 10, 14, 15 days because it was deemed that these could relatively easily be scheduled on site.

With respect to staggered tests, the diesel tests were staggered on as nearly a perfect basis as possible, i.e., since there are two diesel trains, the interval between diesel tests equals one half the diesel test interval. This interval was rounded off to the nearest day. In the course of using the FRANTIC code to determine the "best" test intervals, it was found that testing a diesel on the day prior to testing the pump resulted in the lowest unavailabilities. This was obtained by still following the perfect staggered pattern for the diesel. For example, the time scale shown below displays the testing of the diesels every 7 days and the pump every 14 days using the method described above.

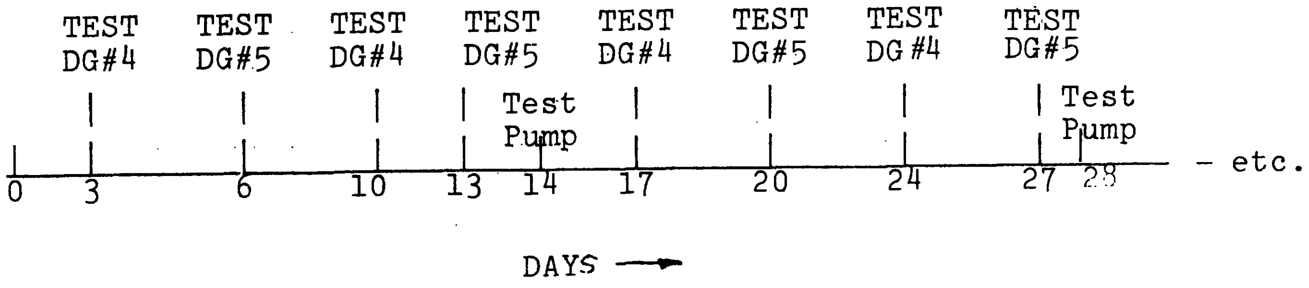


Figure 4.9 shows the results of testing the diesels for the aforementioned 4 different test intervals along with the varying pump test interval. From this figure, it is apparent that the "best" practical test intervals for the diesels and the pump are 7 days, respectively, because these test intervals result in the lowest unavailability of the Aux-Feed-System. By referring back to Figure 4.7 , the unavailability for testing the system components every 4 days using perfect staggering between all components is approximately $6.5x10^{-8}$. As can be seen from Figure 4.9 , the testing of the components every 7 days results in about the same unavailability, which is the combined result of the different staggering methods employed.

It is worth mentioning that the doubling of the pump test interval from 7 to 14 days does not significantly increase the unavailability of the Aux-Feed-System. (Note, the diesel test interval is still kept at 7 days. However, doubling the diesel test from 7 to 14 days results in a substantial increase in system unavailability. This is due to the fact that there are two diesel trains and that the diesel failure rate is by an order of magnitude higher than that of the pump.

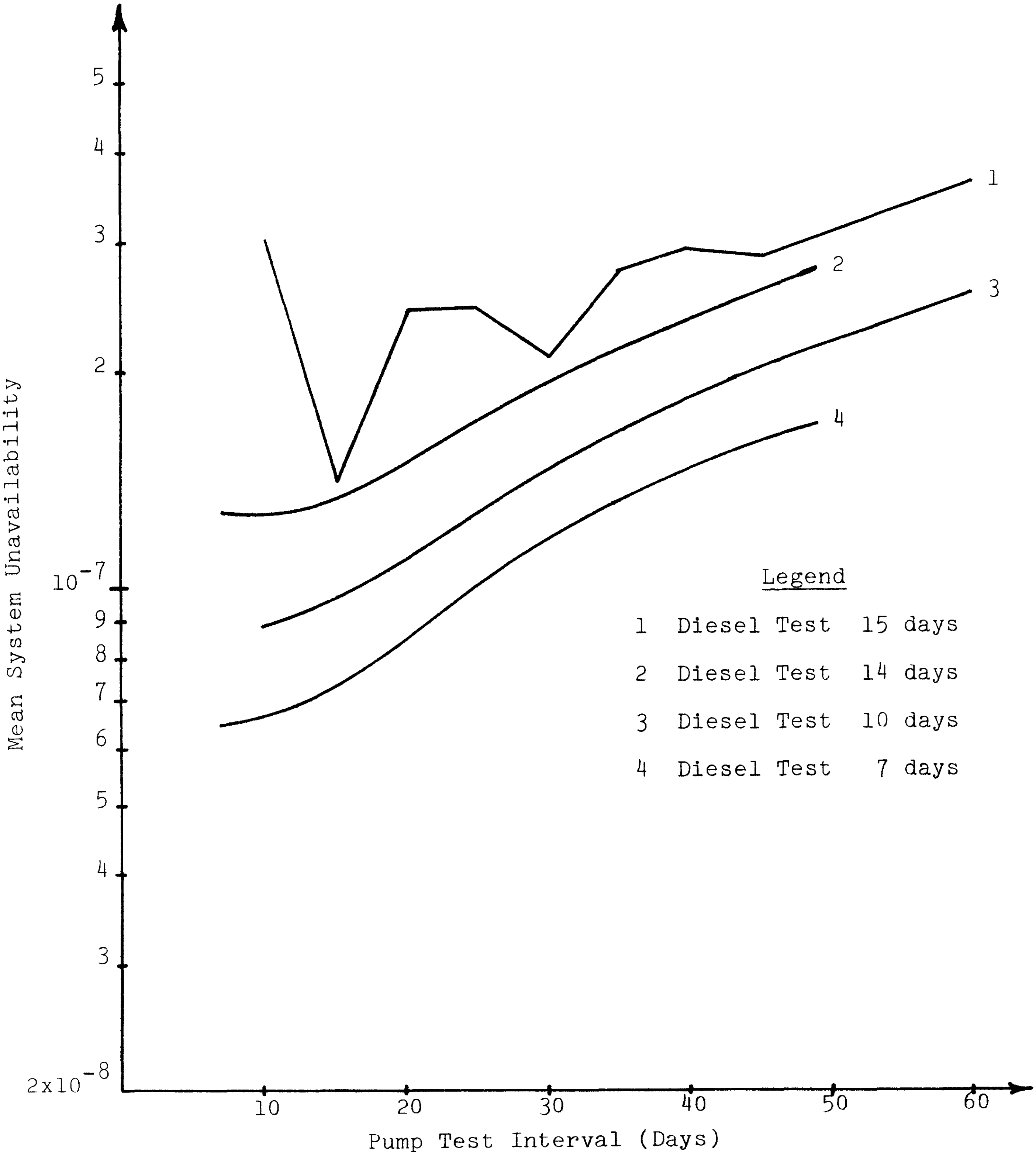


Figure 4.9: Aux-Feed-System -- Effect of Pump Test Interval on the Mean System Unavailability

A final note should be addressed to the presentation of the curves in Figure 4.9. The data generated by FRANTIC represent actually discrete unavailabilities. These were connected by continuous lines to display the effect of increasing test intervals. The actual system unavailability for pump test intervals other than those used for the plots is unknown.

4.6 Conclusions and Recommendations

In the search for optimum test intervals, it has been shown that one cannot solve for the optimum test interval of single components and expect these test intervals to result in a minimum mean unavailability for the system as a whole. Note that the best result for the method of Section 4.4, the Jacobs method, combined with perfect staggering yields a mean unavailability of $2.159\text{x}10^{-7}$ versus a mean unavailability of $4.815\text{x}10^{-8}$ using test intervals of 3 days and perfect staggering (trial and error method) of Section 4.5 . While this unavailability has not beenshown to be a minimum for the system since FRANTIC breaks down for intervals less than 3 days, this unavailability is a reduction of a factor of 4.5 over that obtained by the Jacobs method. In addition, it is shown in Figure 4.9 that by using more practical test intervals the unavailability can be reduced to less than what has been obtained by the Jacobs method. Therefore, it is concluded that the system unavailability, while being determined by individual component unavailabilities is not optimized by utilizing test intervals that are determined as optimum for the individual components.

By increasing the redundancy of a system, the optimum test intervals of the component decrease from their optimum test interval when a component is considered individually. This occurs because while one component is being tested, the other redundant components are available to provide the required function. Therefore, for identical trains, the test interval for a one-out-of-two system is smaller than the test interval for a one-out-of-one while a one-out-of-three system would allow for smaller optimum test intervals than a one-out-of-two system.

The results shown in this chapter are for components where only failure rate, testing time, repair time, test interval and test procedure are considered. More complexity can be brought into the picture by including the additional effects of override unavailability, test induced failure, and test inefficiency. However, it cannot be overemphasized enough that the main problem with implementing these last three parameters is the lack of real plant data. For this reason, the results for very small test intervals should be taken with caution because they do not reflect the possible degrading effects of too frequent testing.

5. Test Interval Optimization Study for the Emergency Power System

5.1 Introduction

Upon agreement of the sponsors, the Emergency Power System of the Maine Yankee power plant was chosen for this study. The one-line diagram of the emergency busses as shown in Figure 5.1 has been extracted from the more elaborate electrical system diagram.

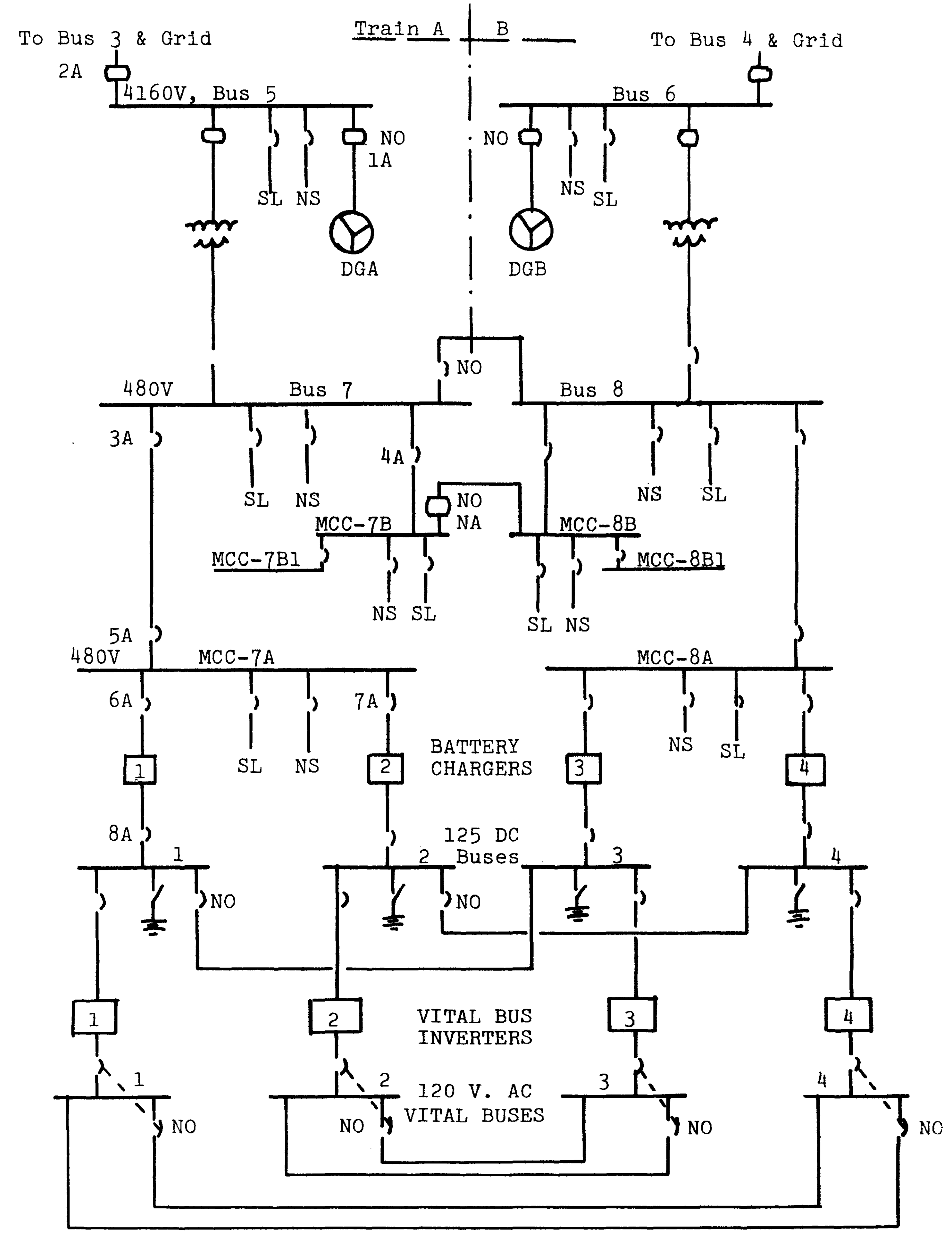
The Emergency Power System (EPS) consists of:

1. Two sources of off-site AC power.
2. Two sources of on-site AC power consisting of two diesel generator sets called DGA and DGB in Figure 5.1 and in what follows.
3. Four sources of DC power.
4. Auxiliary equipment including transformers, busses and cables for the distribution of power to the Engineered Safety Features (ESF) loads.

The principal function of the EPS is to provide power to the ESF systems in case of accidents and loss of off-site AC power.

The undesirable event for the development of the fault tree has been defined as "Insufficient Power to Engineered Safety Features", and is used in the following sections. This definition of the top event includes all states of the EPS which inhibit perfect operation of the Engineered Safety Features (ESF). Insufficient power is, in general, the coincident loss of two mutually redundant bus trains.

Figure 5.1: One Line Diagram of Maine Yankee Emergency Buses



ALL THE CCT BKR's ARE NORMALLY CLOSED (N.C.) UNLESS OTHERWISE NOTED

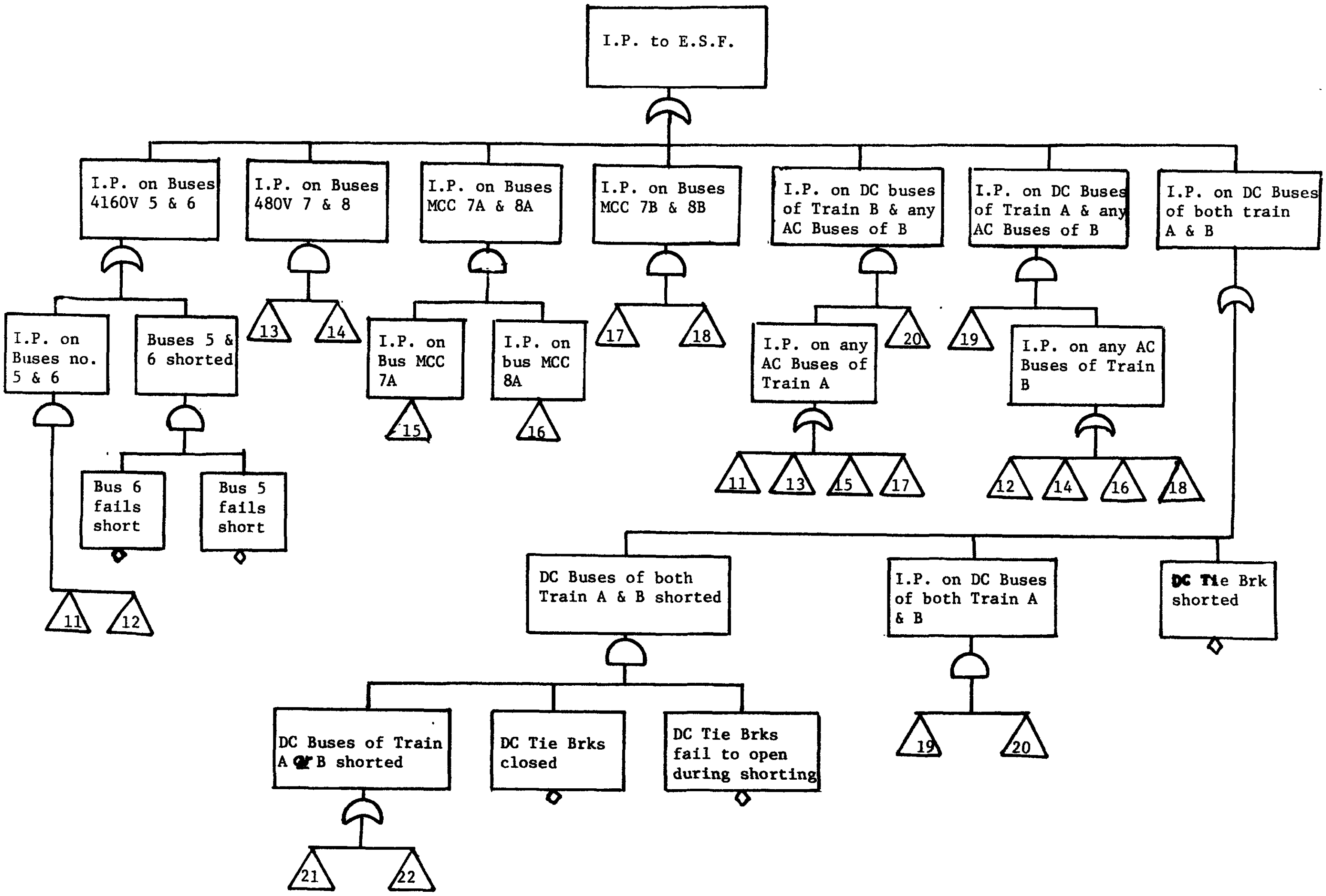
The EPS, as studied in the following, originates at the high voltage substation and terminates at the distribution busses which serve the ESF levels.

Each of the two redundant trains consists of five different busses which lead to 25 different combinations resulting in the top event. Figure 5.2 shows the major failure events which contribute to the top event. The complexity of the tree is quite apparent from this figure. Fortunately, it is sufficient to evaluate only one train for the analysis of the tree, because of the redundancy in each of the available components.

5.2 Collection and Analysis of Diesel Generator Failure Data

A literature survey on operational data of D.G. and related systems turned up 96 failures in the United States with respect to start and assuming power of the minimum number of 3208 starts over the three-year period 1975 to 1977 . These data and their analysis are summarized in Appendix A and the results of this study for failure rate and unavailability per demand were already used in Chapter 3.

The results of the literature survey are compared to the values used in the Reactor Safety Study [7] in Table 5.1. The RSS had obviously used data available up to 1973 [27]. As can be seen from Table 5.1, the differences between both data sources are negligible for most cases. For the present study, the most conservative data as resulting from both data sources are displayed in the last column of this table and are used for the following fault tree evaluation.


I.P. to E.S.F.
I.P. on Buses 4160V 5 & 6
I.P. on Buses 480V 7 & 8
I.P. on Buses MCC 7A & 8A
I.P. on Buses MCC 7B & 8B
I.P. on DC buses of Train B & any AC Buses of B
I.P. on DC Buses of Train A & any AC Buses of B
I.P. on DC Buses of both train A & B
I.P. on Buses no. 5 & 6
Buses 5 & 6 shorted
13
14
I.P. on Bus MCC 7A
I.P. on bus MCC 8A
17
18
I.P. on any AC Buses of Train A
20
19
I.P. on any AC Buses of Train B
15
16
Bus 6 fails short
Bus 5 fails short
11
13
15
17
12
14
16
18
11
12
DC Buses of both Train A & B shorted
I.P. on DC Buses of both Train A & B
DC Tie Brk shorted
DC Buses of Train A or B shorted
DC Tie Brks closed
DC Tie Brks fail to open during shorting
19
20
21
22

Odd No. refer to Emergency train related to Bus 5
Even No. refer to Emergency train related to Bus 6.

Figure 5.2 Maine Yankee Emergency Power System Fault Tree

Component		Symbols	Literature Survey	WASH 1400	Recommended Conservative
D.G.	fail to start, and assume power	$\lambda_S(EDG)$	3×10^{-5}	3×10^{-5}	3×10^{-5}
	unavail. upon demand	$Q_d(EDG)$	2×10^{-2}	3×10^{-2}	3×10^{-2}
BAT.	failure rate (degraded)	$\lambda(BAT)$	1.14×10^{-5}	10^{-6}	1.14×10^{-5}
	unavailability upon demand	$Q_d(BAT)$	1.14×10^{-4}	10^{-3}	10^{-3}
Net	failure rate	$\lambda(net)$	1×10^{-5}	2×10^{-5}	2×10^{-5}
	unavail. upon demand	$Q_d(net)$	2×10^{-4}	10^{-3}	10^{-3}

Table 5.1: Comparison of the results of a literature survey (1975-1977) with results used in WASH 1400

It should be noticed that the gathering of data as described above faces several difficulties. This is especially due to the fact that the D.G. units examined differ substantially with respect to design and power rating. Thus, each category should be analyzed separately and would certainly result in different failure rates. However, there are not enough data available which would allow the consistent analysis described above. Therefore, despite recognition of the special need for more consistency, it has been decided to use the overall failure frequency for the analysis of the literature survey. This seems to be a conservative assumption, especially in light of the fact that no malfunctioning has been reported for Maine Yankee thus far.

All other component data needed to complete the fault tree evaluation were taken from WASH-1400. In cases where no data were available, conservative estimates have been made with respect to the failure rates and repair times.

5.3 Unavailability Calculation of the 4160V Emergency Busses

5.3.1 Fault Tree Reduction

The availability of the power to the Engineered Safety Features is governed by the availability of the 4160V busses because the loss of these busses, 5 and 6, would immediately result in the loss of AC power to the ESF. Therefore, the analysis of the unavailability of the 4160V bus has been selected as being the most important issue for this study.

Figure 5.3 shows the fault tree diagram of Bus 5. This tree can be equally applied for Bus 6 if the manual circuit breaker 5R, which connects to Bus 5 from the reserve station transformer X-16, is neglected.

By using well-known principles of fault tree analysis, the fault tree diagram as shown in Figure 5.3 can be further reduced as depicted in Figure 5.4. This reduction is deemed to have no major impact upon the evaluation of the probability of occurrence of the top event. It is desirable from the point of view of a parametric study, and it is necessary in order to come up with a reasonably simple system whose system function, needed as input to FRANTIC, can be found without great difficulty.

Table 5.2 summarizes the data used for the primary events in this study.

5.3.2 Results

Figures 5.5 and 5.6 show the results of the study as obtained by the FRANTIC code for the point unavailability and the mean and peak unavailabilities of the system, respectively.

Figure 5.5 displays the point unavailability of Bus 5 over one full period, whereas Mean $\bar{A}$ and Max $\bar{A}$ are shown in Figure 5.6 as function of D.G. test interval.

As Figure 5.5 shows, for $\lambda(\text{EDG})=3\text{x}10^{-5}\text{hr}^{-1}$, the point unavailability displays the familiar characteristics, namely that during the test itself the unavailability increases, drops to a low level at repair and decreases further after repair beyond which it starts to increase again due to random failure.

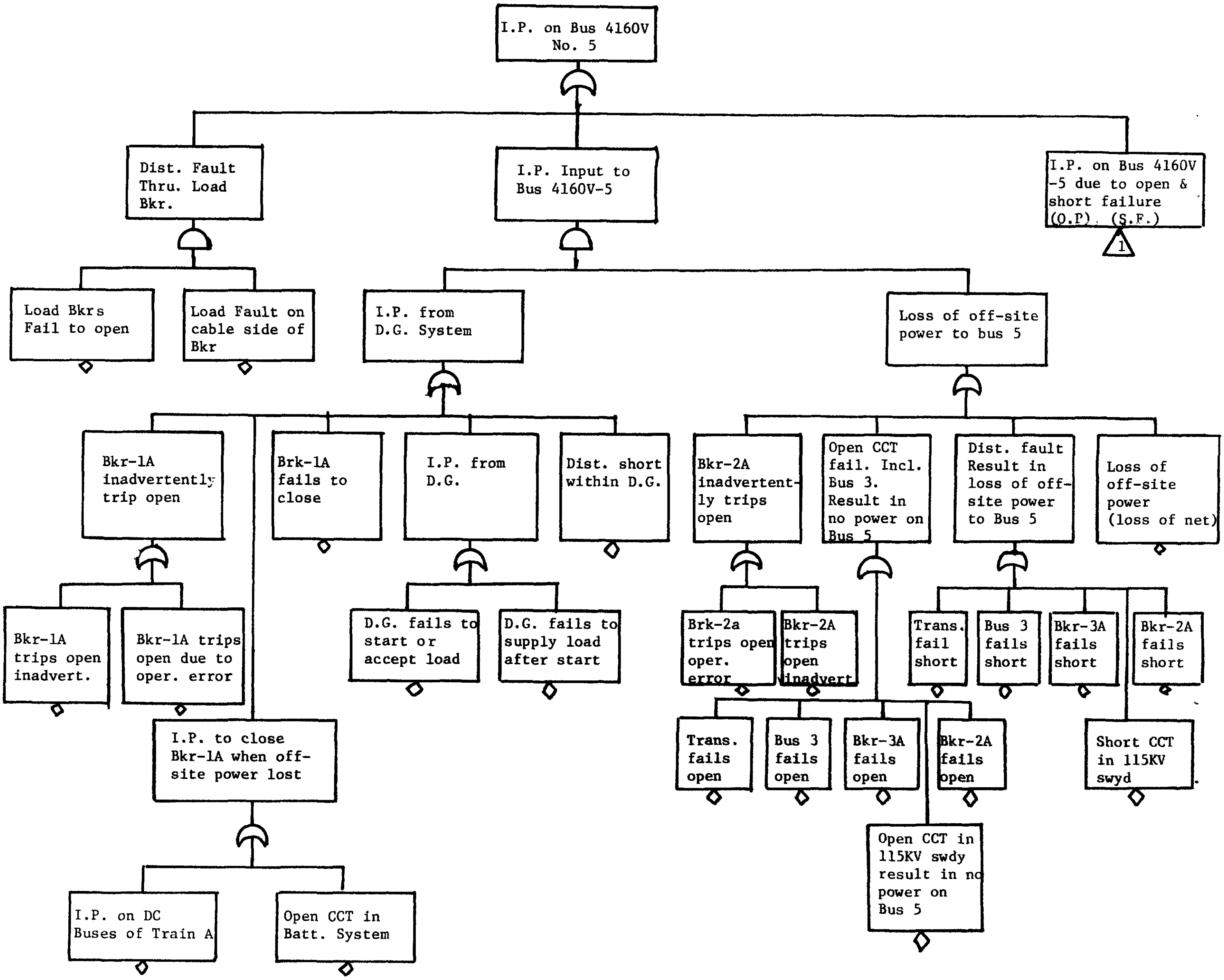

I.P. on Bus 4160V No. 5
Dist. Fault Thru. Load Bkr.
I.P. Input to Bus 4160V-5
I.P. on Bus 4160V -5 due to open & short failure (O.P). (S.F.)
1
Load Bkrs Fail to open
Load Fault on cable side of Bkr
I.P. from D.G. System
Loss of off-site power to bus 5
Bkr-1A inadvertently trip open
Brk-1A fails to close
I.P. from D.G.
Dist. short within D.G.
Bkr-2A inadvertently trips open
Open CCT fail. Incl. Bus 3. Result in no power on Bus 5
Dist. fault Result in loss of off-site power to Bus 5
Loss of off-site power (loss of net)
Bkr-1A trips open inadvert.
Bkr-1A trips open due to oper. error
D.G. fails to start or accept load
D.G. fails to supply load after start
Brk-2a trips open oper. error
Bkr-2A trips open inadvert
Trans. fail short
Bus 3 fails short
Bkr-3A fails short
Bkr-2A fails short
I.P. to close Bkr-1A when off-site power lost
Trans. fails open
Bus 3 fails open
Bkr-3A fails open
Bkr-2A fails open
Short CCT in 115KV swyd
Open CCT in 115KV swdy result in no power on Bus 5
I.P. on DC Buses of Train A
Open CCT in Batt. System

Figure 5.3 Bus 5 Fault Tree Diagram

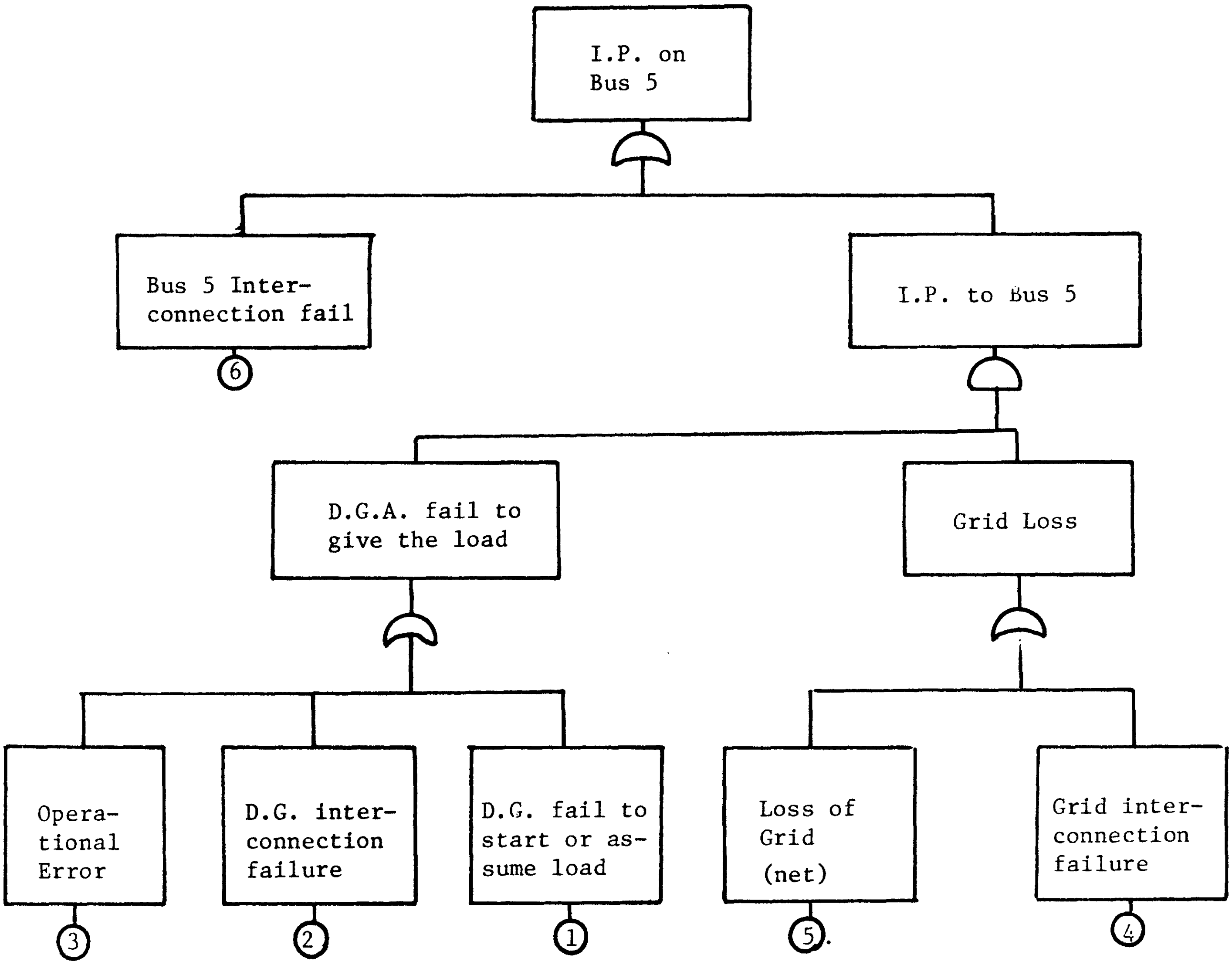

I.P. on Bus 5
Bus 5 Interconnection fail
6
I.P. to Bus 5
D.G.A. fail to give the load
Grid Loss
Operational Error
3
D.G. interconnection failure
2
D.G. fail to start or assume load
1
Loss of Grid (net)
5
Grid interconnection failure
4

Figure 5.4: Reduced Fault Tree for 4160V Bus 5

Table 5.2: Component and Event Data Used in this Study

Component	λ	T_2	T_1	T_C	T_R	P_f	Q_D
	$hr^{-1} \times 10^6$	days	days	hour	hour		
1. D.G.	30(3000)*	50^+	25^+	1.5	21	10^{-4}	0
2. D.G.I. Con.	250	--	--	--	1.0	--	--
3. Oper. Error	--	--	--	--	--	--	10^{-4}
4. Net Con.	11	--	--	--	1.0	--	--
5. Net	30	--	--	--	3.0	--	--
6. B. 5 LBF	2	--	--	--	1.0	--	--

*No. in parentheses represents the λ(EDG) for conservative run.

$^+T_2$ and T_1 vary from 50 and 25, to 25 and 12 days.

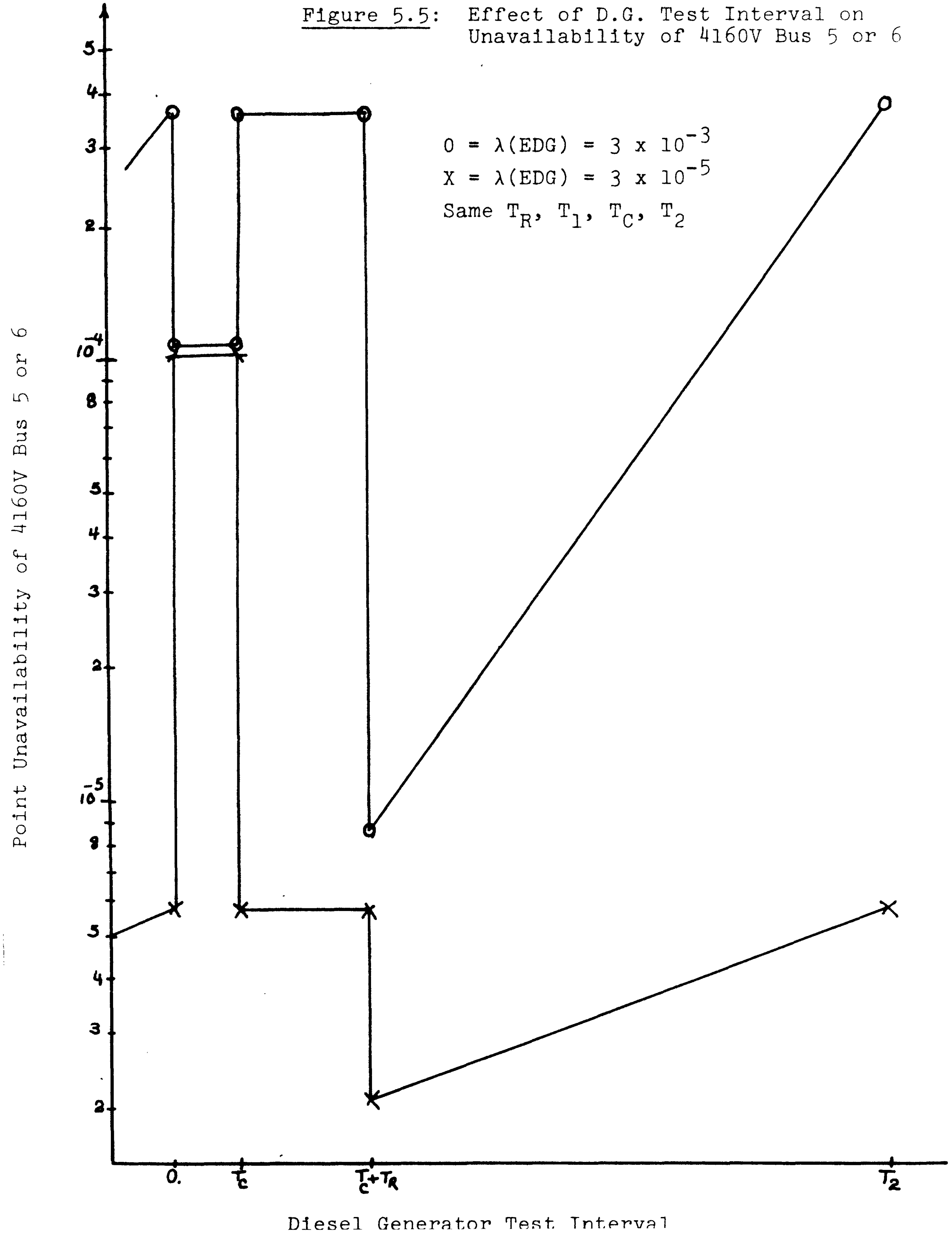
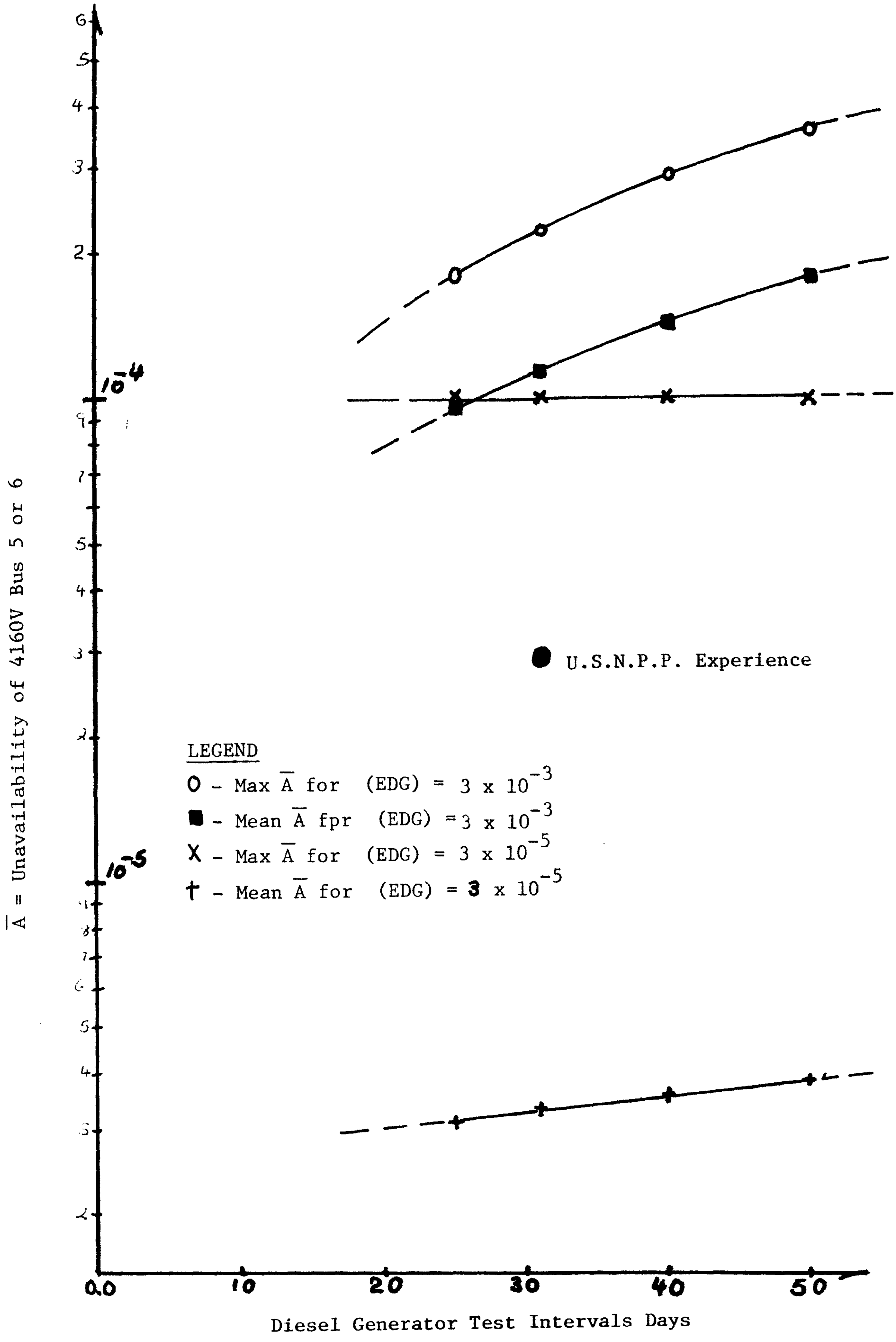


Figure 5.5: Effect of D.G. Test Interval on Unavailability of 4160V Bus 5 or 6

Figure 5.6: Effect of D.G. Test Interval on Unavailability of 4160V



By increasing the failure rate to $\lambda(EDG)=3x10^{-3}hr^{-1}$, Figure 5.5 shows a different point unavailability behavior, where obviously the contribution due to the test results in a lower unavailability than what is contributed by repair and random failure. This is certainly wrong and shows the inherent limitations of the FRANTIC code as a result of the various approximations employed. At this point, it should be recalled that for $\lambda T > 0.01$ the FRANTIC results become more and more questionable. Moreover, it should be noticed that the unavailability of the system for the very conservative estimate of $\lambda(EDG)=3x10^{-3}hr^{-1}$ is primarily the result of the contribution of the loss of off-site power, because for a 50-day test interval the D.G. is already in the failed state. This can be clearly demonstrated by examining the approximation for the unavailability as applied in FRANTIC, i.e.,

$$\overline{q} = \frac{1}{2}\lambda T_2 + q_1 \frac{T_c}{T_2} + q_2 \frac{T_R}{T_2}$$

By neglecting the two last terms, the D.G. unavailability becomes $\overline{q}=1.8$ and is thus already unrealistically larger than unity for $T_2=50d$. In fact, the calculations show that for the data chosen, the D.G. fails after 26.5 days.

The foregoing example clearly demonstrates that results generated by codes such as FRANTIC have to be taken with care. This is especially important because as Figure 5.6 reveals, nothing peculiar can be noticed from the curves for Mean $\overline{A}$ and Max $\overline{A}$.

As can be seen from Figure 5.6, the mean unavailability of the system ranges from $3.24\text{x}10^{-6}$ to $3.92\text{x}10^{-6}$ when the test interval of the D.G.s is changed from 25 to 50 days for the case of $\lambda(\text{EDG})=3\text{x}10^{-5}\text{hr}^{-1}$. The maximum unavailability, i.e., the value of $\bar{A}$ during test, stays constant at a value of $1.03\text{x}10^{-4}$ over the whole range.

At this point it should be remembered that these results are generated for a set of failure rates which must be considered conservative when compared to actual experience.

When the D.G. failure rate would assume the overly conservative value of $\lambda(\text{EDG})=3\text{x}10^{-3}\text{hr}^{-1}$, the mean unavailability increases by an order of magnitude and changes from $9.7\text{x}10^{-5}$ to $1.79\text{x}10^{-4}$ whereas the maximum unavailability changes from $1.84\text{x}10^{-4}$ to $3.65\text{x}10^{-4}$ over the range of test intervals from 25 days to 50 days.

5.3.3 Discussion and Conclusion

From the results presented in the foregoing section, it becomes apparent that the lack of reliable data forces the analyst to make conservative and possibly nonrealistic assumptions which may lead to results which are in fact not representative for the system under consideration. Hence, a consistent and realistic analysis is only possible to the extent to which reliable data are available.

The results of Figures 5.5 and 5.6 suggest that the failure rate of the D.G. should not be higher than 10^{-4}hr^{-1} according to the following arguments. As depicted by the individual point in

Figure 5.6 characterized as U.S.N.P.P., the U.S. nuclear power plant experience indicates an unavailability of both on-site and off-site AC power at the same time not greater than $9x10^{-10}$. For the assumption of $\lambda(EDG)=3x10^{-5}hr^{-1}$ and simultaneous D.G. test, the maximum unavailability is 10^{-8}, whereas this is reduced to $4x10^{-10}$ for a perfect staggered test procedure.

5.4 Study of the Additional Effect of D.G. Unavailability per Demand Upon the Unavailability of Bus 5

In order to study the additional effect of variations in the component data, the single bus failure has been reexamined by assuming that the D.G. not only fails randomly as was assumed in the previous section, but that it is characterized by a constant unavailability per demand in addition.

Table 5.3 summarizes the input data for this study which used the same reduced fault tree as shown in Figure 5.3. Two cases were studied with these data. The first one considered the D.G. as being perfectly available, i.e., $q_D=0$, whereas the second one assumed $q_D=10^{-2}$/demand.

Figure 5.7 shows the results for both cases as a function of D.G. test interval. As can be seen, the additional impact of a constant unavailability per demand is to increase the mean unavailability of the bus by about a factor of two, whereas the peak unavailability remains unaffected.

Table 5.3: Input Data for Single Bus Failure Study with Additional D.G. Unavailability (See Figure 5.3 for the underlying fault tree)

Component	λ hr^{-1}	T_c hr	T_R hr	q_0 --	q_D --
1. D.G.	3×10^{-5}	1.5	21	1.0	2×10^{-2}
2. D.G. Intercon.	2.5×10^{-4}	--	1.0	--	--
3. Operator	--	--	--	--	1×10^{-4}
4. G.N.C.	1.1×10^{-5}	--	1.0	--	--
5. Net	3×10^{-5}	--	3.0	--	--
6. Single bus	2.4×10^{-6}	--	1.0	--	--

T_2 changes from 50 to 20 days

T_1 changes from 25 to 10 days

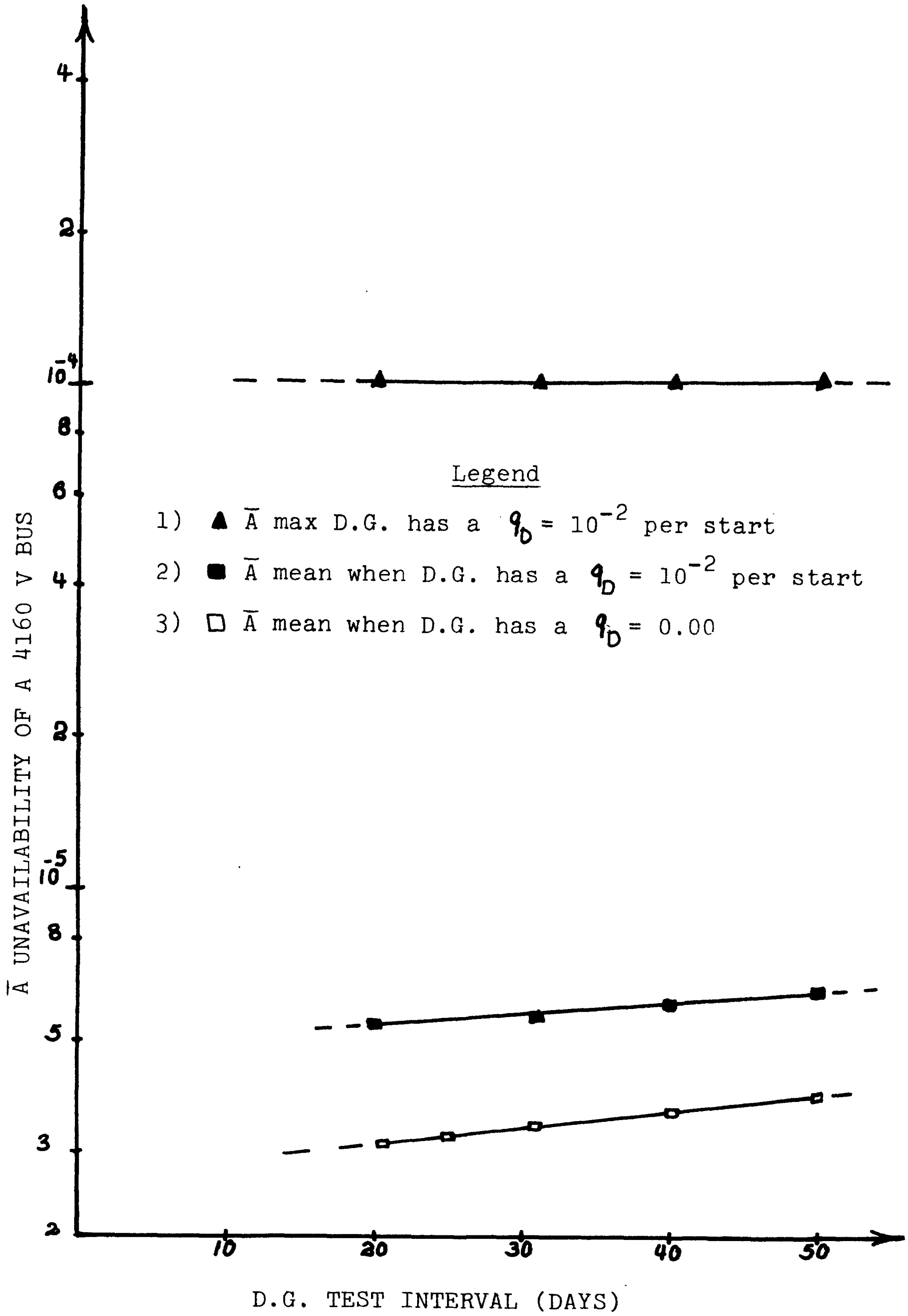


Figure 5.7: Effect of D.G. Unavailability Upon Demand on Bus 5 Mean and Peak Unavailability (See Table 5.3 for Input Data)

5.5 Station Blackout Study

5.5.1 Introduction

For illustrative purposes, a station blackout study was performed. The reasoning underlying this effort is as follows. In case, that Buses 5 and 6 and their respective prior interconnections as well as grid transmission lines can be considered as perfectly independent, the unavailability of both buses would be just the square of the unavailabilities reported in the previous chapters, i.e. it would fall in the range of about $10^{-8} > \bar{A} > 10^{-10}$. However, a closer look at the system reveals that both buses are connected to the same grid. Thus it is deemed to be more appropriate to reconstruct the fault tree for the top event "Insufficient Power on Both Buses 5 and 6" by considering the loss of the grid due to a common mode of event such as forest fire, snow storm, icing, or the like. As a result, it is expected that the unavailability of station power will increase compared to the value which is obtained with the assumption of complete independence.

5.5.2 Fault Tree and Data

Fig. 5.8 shows the fault tree for the analysis of station blackout whereas Table 5.4 summarizes the data which are used in this study. In order to comprehend the differences introduced into the blackout prediction, the reader is urged to compare Figs. 5.4 and 5.8.

As with respect to the data, two cases are examined. In

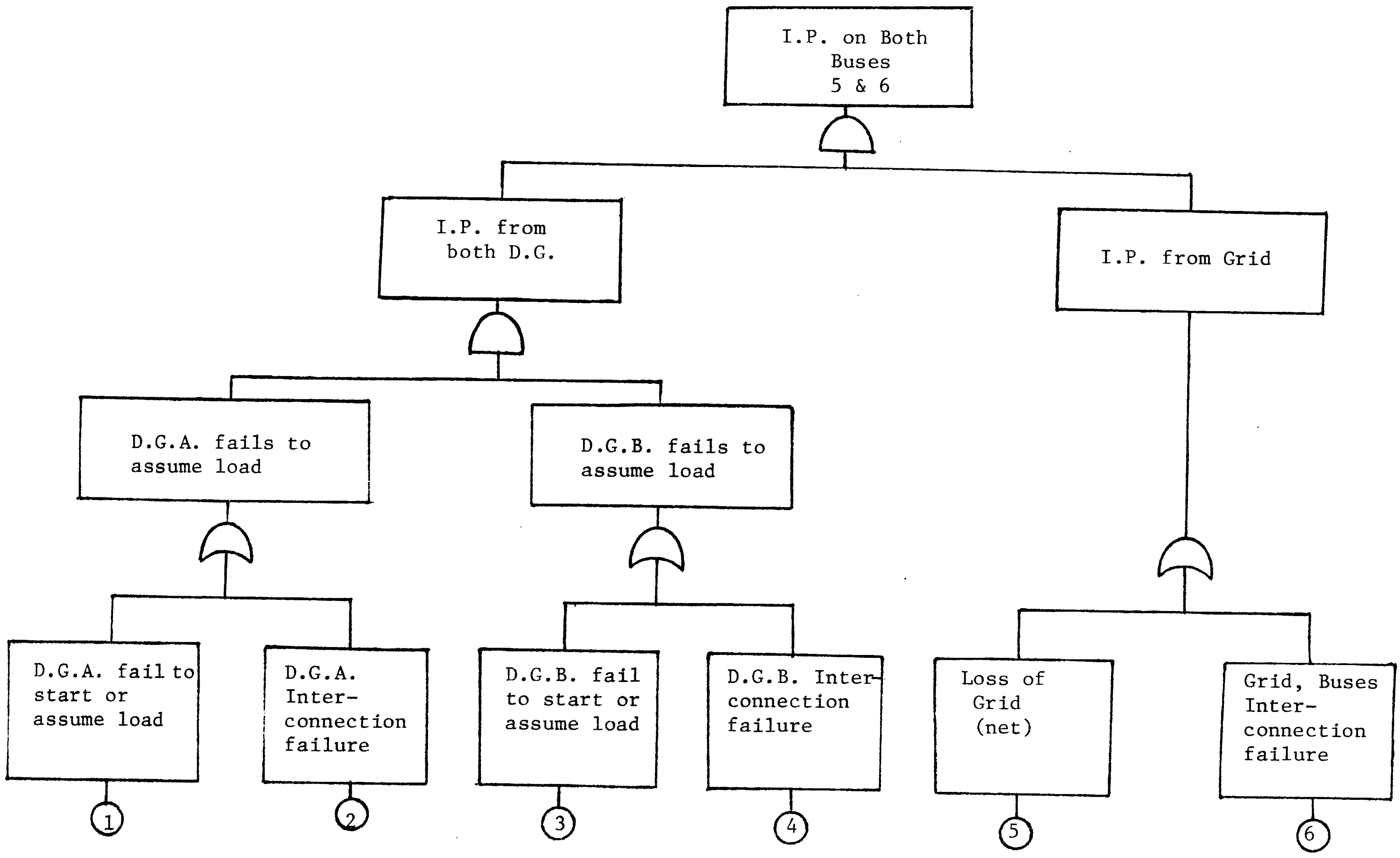

I.P. on Both Buses 5 & 6
I.P. from both D.G.
I.P. from Grid
D.G.A. fails to assume load
D.G.B. fails to assume load
D.G.A. fail to start or assume load
D.G.A. Inter-connection failure
D.G.B. fail to start or assume load
D.G.B. Inter-connection failure
Loss of Grid (net)
Grid, Buses Inter-connection failure
1
2
3
4
5
6

Fig. 5.8: Fault Tree for Station Blackout Study

Table 5.4:

Data for Station Blackout Study
(Perfect Staggered Testing of D.G.s)

Component	λ	T_r	q_o	P_f	q_d	
	hr^{-1}	hr	-	-	-	
1. D.G.A.	3×10^{-5}	21	1	10^{-4}	2×10^{-2} 0	(Case 1) (Case 2)
2. D.G.A. Conn.	2.6×10^{-4}	1	0	0	0	
3. D.G.B.	3×10^{-5}	21	1	10^{-4}	2×10^{-2} 0	(Case 1) (Case 2)
4. D.G.B. Conn.	2.6×10^{-4}	1	0	0	0	
5. Net	3×10^{-5}	3	0	0	0	
6. Net Conn.	1.1×10^{-5}	1	0	0	0	

Test Interval, T_2:	50 days to 20 days
First Test, T_1:	25 days to 10 days
Test Time, T_c:	1.5 hr for D.G.A. and D.G.B.

the first case (Case 1), it is assumed that the diesel generators do not only fail randomly but that they are also subject to a constant unavailability per demand (2×10^{-2}). In the second case (Case 2), it is assumed that the diesel-generators are perfectly available upon demand (q_D=0). All other data are kept the same. It should be noticed that only the case of perfect staggered testing is examined.

5.5.3 Results and Discussion

Again, the impact of the D.G. test interval on the unavailability of both buses has been studied and the results for the two cases discussed above are displayed in Fig. 5.9. As can be seen from this figure the mean and peak unavailabilities are rather strongly affected by the assumptions made for the diesel-generator failure. Thus, if only random failures are considered, $\bar{A}$ mean ranges from 8×10^{-9} to 4×10^{-8} for the range of test intervals considered. If in addition, a constant unavailability upon demand is accounted for, $\bar{A}_{mean}$ increases from 8×10^{-8} to 1.5×10^{-7}, i.e. an increase by a factor of 10 or 4, at the end points of the spectrum for the test interval, respectively. The same trend is apparent for the peak unavailabilities, $\bar{A}_{max}$ with the only difference that these values are by one to two orders of magnitude higher than the mean unavailabilities. A comparison of the respective pairs of curves for $\bar{A}_{mean}$ and $\bar{A}_{max}$ reveals that for increasing test intervals the differences in the unavailabilities decreases which is the result of the fact that with an increased test interval the effect of random failures increases.

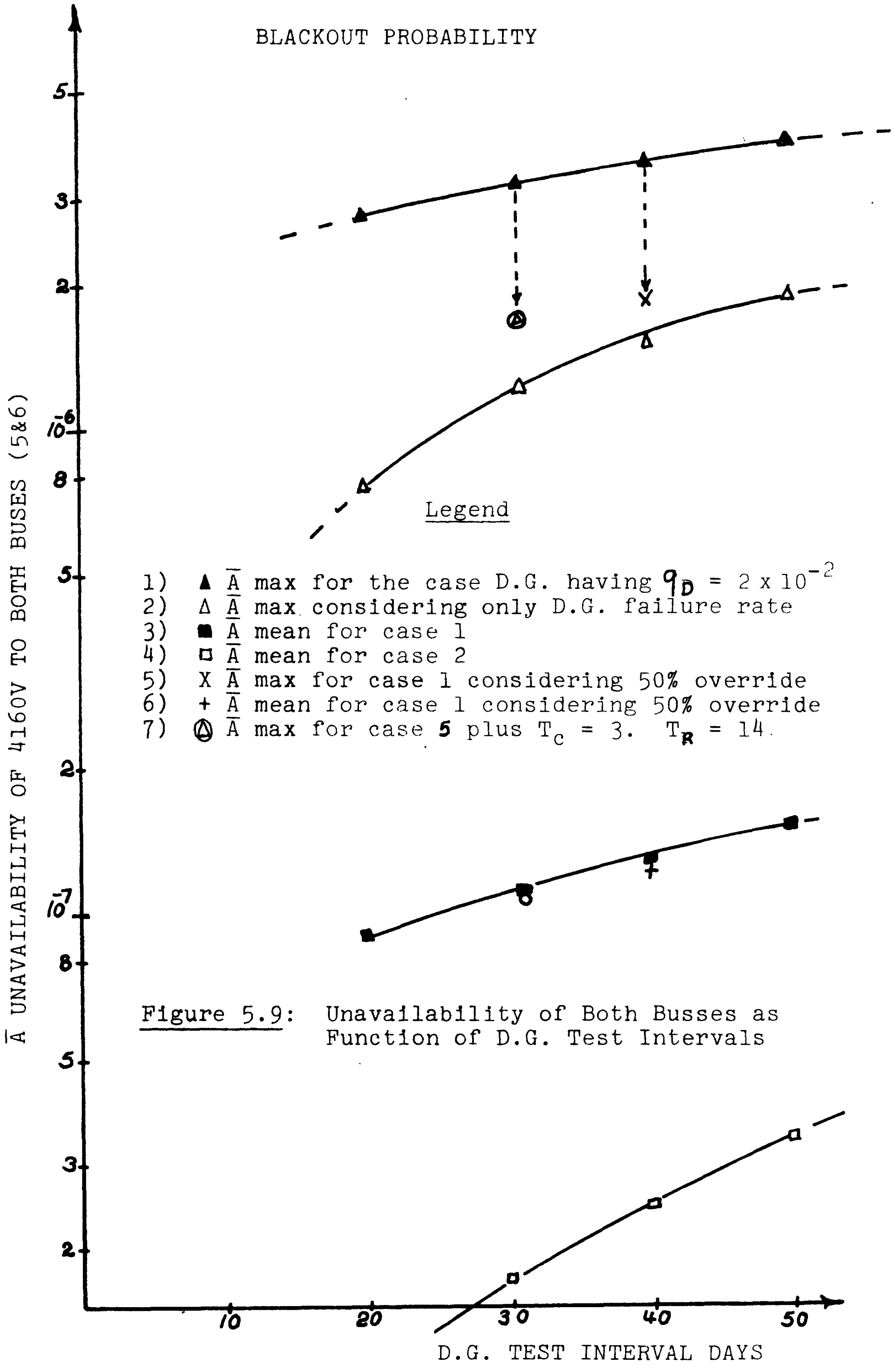


Figure 5.9: Unavailability of Both Busses as Function of D.G. Test Intervals

It is interesting to compare the predictions of the blackout study with the squares of the previously obtained unavailabilities of one bus (see Chapters 5.3.3 and 5.4). Naturally, as indicated before, the latter values are only valid for perfectly independent buses including the grid. With this assumption and the data shown in Fig. 5.7 $\bar{A}_{mean}$ would result as about 2.5 x 10^{-11} for both buses being unavailable at the same time for Case 1, whereas for Case 2 $\bar{A}_{mean}$ would be even smaller, namely $\bar{A}_{mean} \approx 9 \times 10^{-12}$. The respective values for the modified fault tree are about 10^{-7} and 10^{-8} respectively and show, as Fig. 5.9 reveals, a much higher sensitivity with respect to the test interval. The differences are not as pronounced for the peak unavailabilities, which become ~ 10^{-8} for independent buses and are 10^{-6} for the modified tree.

In addition to the main part of this study, two individual cases were run whose results are also displayed in Fig. 5.9 as individual points in order to demonstrate at least the trend of these effects. The first of the additional cases considers the effect of a 50% probability for override during test. As can be seen from the figure, $\bar{A}_{mean}$ remains nearly unaffected, where $\bar{A}_{max}$ can be reduced by a factor of 3 by this option, thereby nearly offsetting the impact of constant unavailability upon demand. The second additional case includes a reduction in repair time down to 14 hours from 21 hours originally and an increase in test time to 3 hours up from originally 1.5 hours. Again, $\bar{A}_{mean}$ is unaffected, whereas $\bar{A}_{max}$ can be reduced by a factor of 3 by these measures. The last example demonstrates clearly that the repair time is obviously of more importance to $\bar{A}_{max}$ than the test time, at least within the limits studied here.

6. STUDY OF TEST CAUSED FAILURES AND DETECTION INEFFICIENCY

6.1 Introduction

All of the previous examples were evaluated under the assumptions that the tests performed on components of the system as well as the detection of faults are perfect. However, it is a well-known fact that these actions are certainly not free of errors either induced by human failure or test actions. Unfortunately, FRANTIC is not able to simulate these effects by detailed models. In fact, models of these kind are even not available for general use. What remains then is to study test caused failures and detection inefficiencies on a parametric basis. For this purpose the FRANTIC code contains the two parameters, P_f and P where the former is the probability for test caused failures and the latter the probability for detection inefficiencies.

In what follows, a parametric study is presented for the unavailability of both D.G.s at the same time.

6.2 Fault Tree and Data

Fig. 6.1 shows the simplified fault tree used in this study. As can be seen from this tree, an event called operational error has been introduced which is connected to both D.G. failure gates in order to account for imperfect testing procedure and/or inefficient maintenance. The data which are held constant during this study are summarized in Table 6.1.

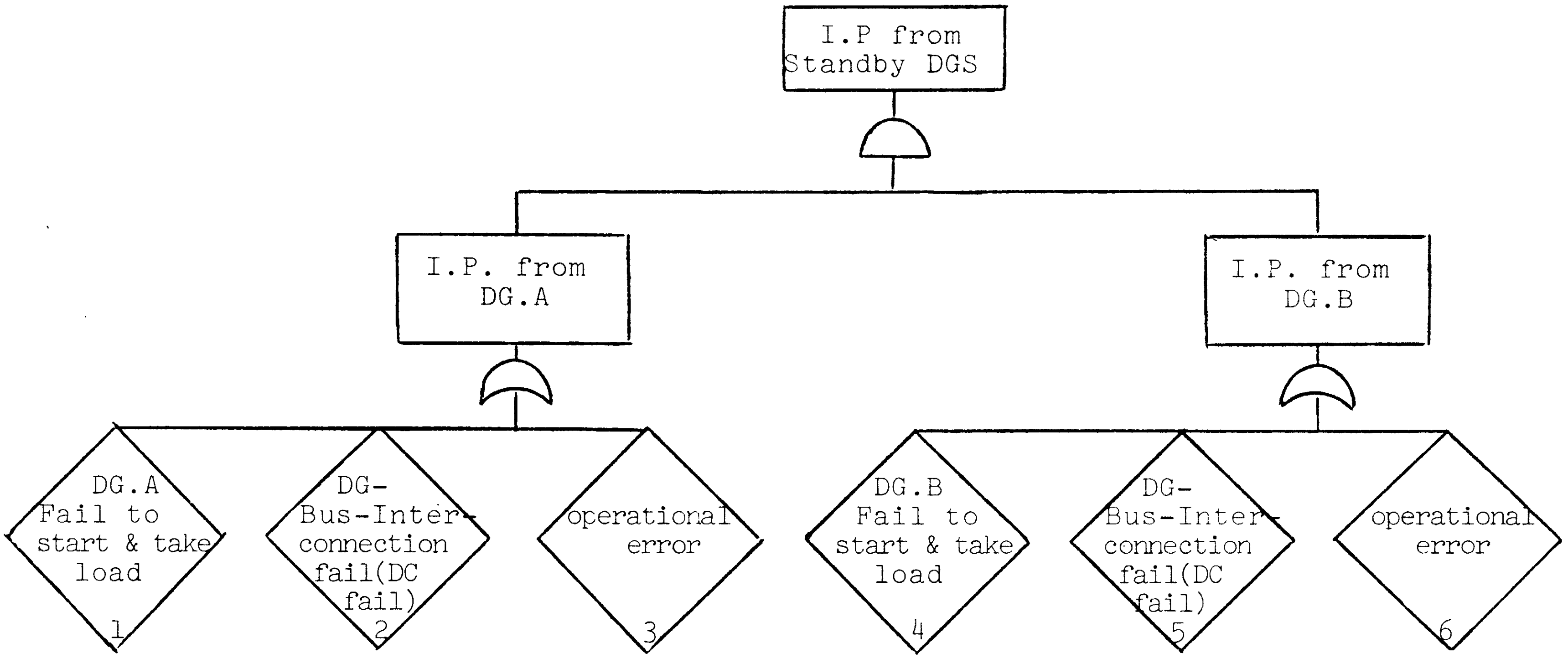

I.P from Standby DGS
I.P. from DG.A
I.P. from DG.B
DG.A Fail to start & take load
1
DG-Bus-Interconnection fail(DC fail)
2
operational error
3
DG.B Fail to start & take load
4
DG-Bus-Interconnection fail(DC fail)
5
operational error
6

Fig. 6.1: Fault Tree for the Parametric Study of Test Caused Failures and Detection Inefficiencies

TABLE 6.1

Component Data

Component	λ hr^{-1}	T_c hr	T_R hr	q_D -
1 D.G.	3×10^{-5}	1.5	21	-
2 DC Conn.				10^{-4}

These data are the same for events 4 and 5.

6.3 Study of Test Caused Failures

It is assumed that both D.G.'s are tested on a perfect staggered basis. The contribution by operational errors is specified as being constant for a given test interval. This constant, q_D, is increased with increased test frequency in order to account for the fact that increased testing may lead to a higher contribution by operational errors. For each test interval, T_2, and associated constant operator unavailability, q_D, the probability of test caused failures, P_f, changed parametrically as shown in Table 6.2. This table also summarizes the results for peak and mean unavailabilities. As can be seen from these results, the peak unavailability, $\bar{A}_{max}$, remains completely unaffected by changes in P_f. The mean unavailability, $\bar{A}_{mean}$, slightly increases with an increase of P_f at constant T_2, These trends are summarized in Fig. 6.2.

6.4 Study of Detection Inefficiency

The effect of the inefficiency in the detection of failures is studied for the same test intervals. Table 6.3 summarizes the variations of the parameters considered in this analysis as well as the results for the mean and peak unavailabilities. For a given test interval, the probability for test caused failures is held constant. This constant decreases with increased test interval. The probability for detection inefficiency as well as q_D are changed parametrically for each T_2. Again, for increased test interval, q_D has been chosen to decrease.

TABLE 6.2

Data and Results of the Parametric Study of Test Caused Failures (Perfect Staggered Testing)

T_2 days	q_D -	P_f	$\bar{A}_{mean}$	$\bar{A}_{max}$
10	5×10^{-3}	10^{-4}	1.914×10^{-4}	8.74×10^{-3}
		5×10^{-3}	1.99×10^{-4}	8.74×10^{-3}
		5×10^{-2}	2.686×10^{-4}	8.74×10^{-3}
20	5×10^{-4}	10^{-4}	1.145×10^{-4}	7.856×10^{-3}
		5×10^{-4}	1.148×10^{-4}	7.856×10^{-3}
		10^{-3}	1.151×10^{-4}	7.856×10^{-3}
		5×10^{-2}	1.490×10^{-4}	7.856×10^{-3}
30	10^{-4}	10^{-4}	1.615×10^{-4}	1.106×10^{-2}
		10^{-3}	1.620×10^{-4}	1.106×10^{-2}
		5×10^{-3}	1.646×10^{-4}	1.106×10^{-2}
		10^{-2}	1.678×10^{-4}	1.106×10^{-2}

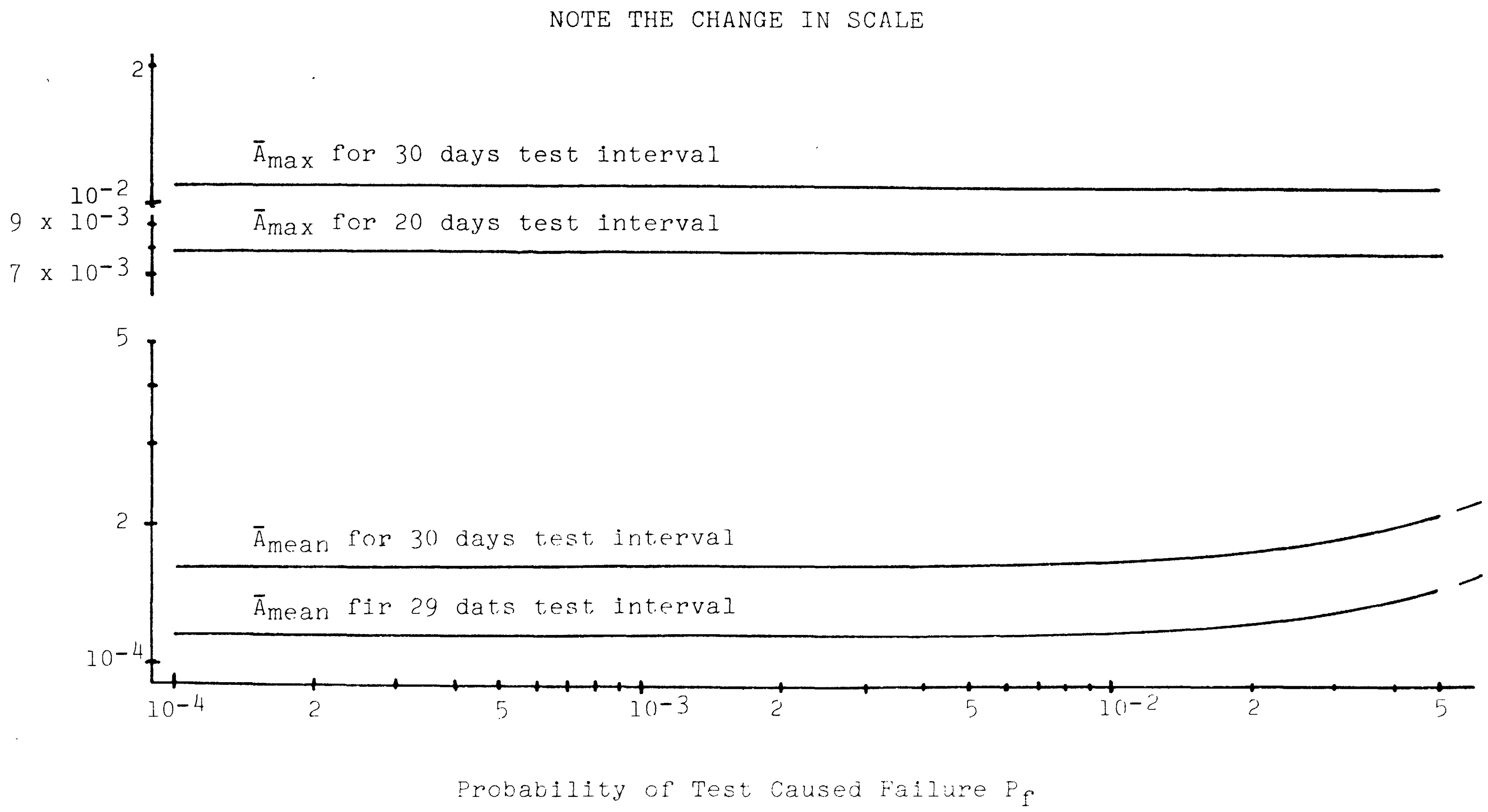


Fig. 6.2: The Effect of the Probability of Test Caused Failure on the Unavailability of Two D.G.s.

TABLE 6.3

Data and Results of the Parametric Study
of Detection Inefficiencies
(Perfect Staggered Testing)

T_2 days	q_D -	P_f -	P -	$\bar{A}_{mean}$ -	$\bar{A}_{max}$ -
10	5×10^{-3}	10^{-3}	5×10^{-3}	2.136×10^{-4}	1.004×10^{-2}
	5×10^{-3}	10^{-3}	10^{-3}	1.968×10^{-4}	8.99×10^{-3}
	10^{-2}	10^{-3}	5×10^{-3}	3.977×10^{-4}	1.5×10^{-3}
20	5×10^{-4}	5×10^{-4}	10^{-3}	1.177×10^{-4}	8.11×10^{-3}
	5×10^{-4}	5×10^{-4}	5×10^{-3}	1.296×10^{-4}	9.127×10^{-3}
	5×10^{-4}	5×10^{-4}	10^{-2}	1.45×10^{-4}	1.04×10^{-2}
	5×10^{-3}	5×10^{-4}	5×10^{-3}	2.567×10^{-4}	1.36×10^{-2}
30	10^{-4}	10^{-4}	10^{-3}	1.31×10^{-2}	1.65×10^{-4}
	10^{-4}	10^{-4}	10^{-2}	1.357×10^{-2}	1.968×10^{-4}
	10^{-4}	10^{-4}	5×10^{-2}	2.378×10^{-2}	3.78×10^{-4}
	10^{-4}	10^{-4}		1.106×10^{-2}	1.615×10^{-4}

The various trends observed in the results of Table 6.3 are more easily displayed in graphs. For example, Fig. 6.3 shows the effect of detection inefficiency upon $\bar{A}_{mean}$ and $\bar{A}_{max}$ for T_2 = 20 days, $P_f = 5 \times 10^{-4}$ and $q_D = 5 \times 10^{-4}$. Both unavailabilities increase slightly when P is changed by an order of magnitude from 10^{-3} to 10^{-2}. When q_D is increased by a factor of 10 both unavailabilities increase by about 3 and 1.5 respectively for $P = 5 \times 10^{-3}$.

The same trends can be observed in Fig. 6.4 for T_2 = 30 days, $P_f = 10^{-4}$ and $q_D = 10^{-4}$.

6.5 Conclusion and Discussion

As a result of both studies the following conclusions can be drawn.

- For large test intervals and their associated lower operational errors the effect of P_f is rather negligible.
- The peak unavailability remains unaffected by P_f in the range of values considered in this study.
- If P is smaller than 10^{-3}, its effect upon the unavailability is negligible.
- If P is in the order of 10/0, i.e. 10^{-2} its effect becomes more pronounced.

It should be noticed that although this study revealed certain trends it does not claim that the data selected for q_D, P_f and P are by any means realistic. As already briefly mentioned in the introduction of this chapter, no models exist which would allow consistent calculations of human reliability and wear out charac-

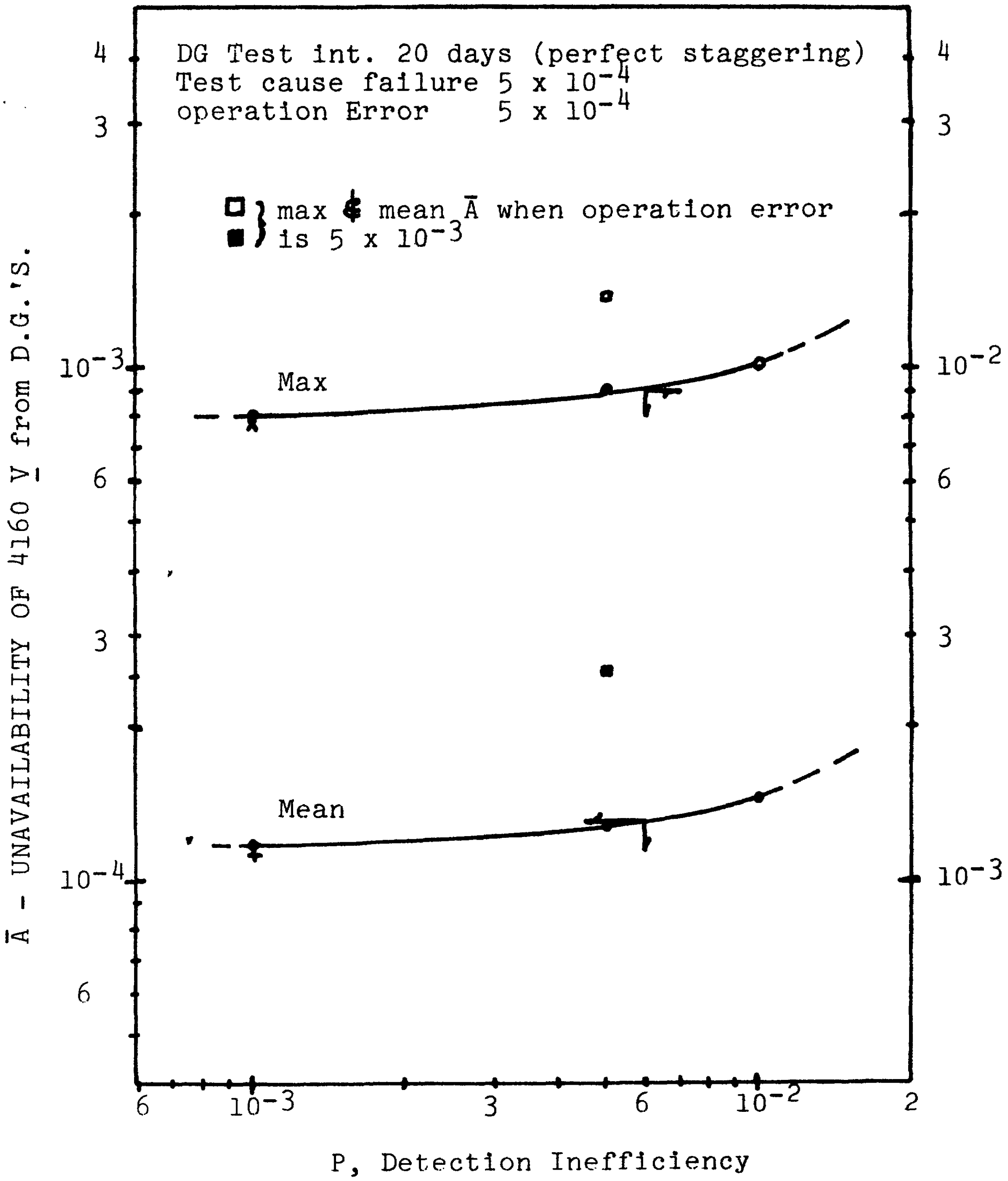


Fig. 6.3: The Effect of Detection Inefficiency

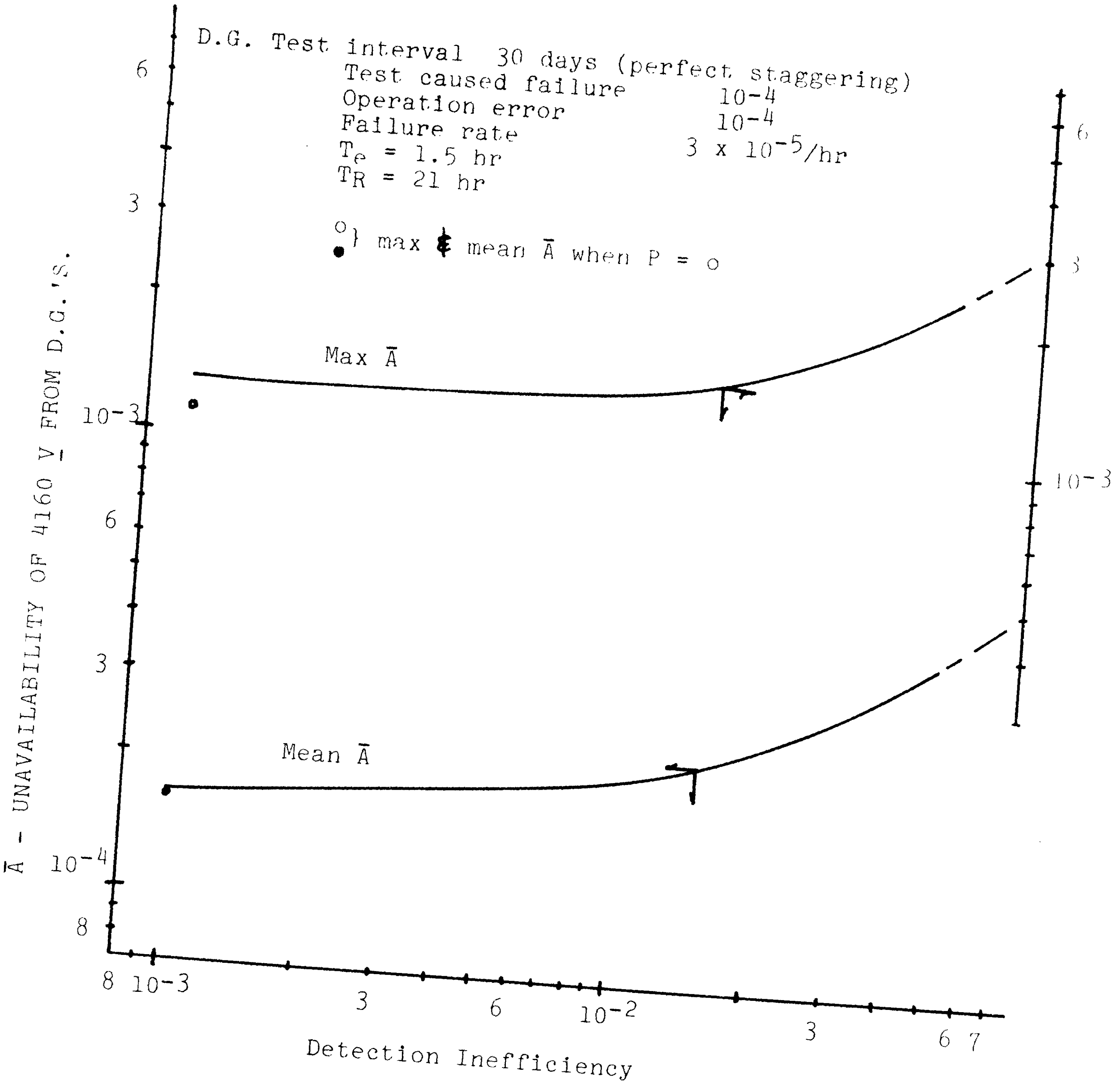


Fig. 6.4: Variation of Unavailability due to Detection Inefficiency

teristics of too frequent tests. Therefore, parametric studies of the kind used in this chapter remain the only option to assess the effect of test caused failures and the probability of undetected failures.

It is quite obvious, that in these areas much work remains to be done. In the meantime, engineering judgement is the only way to overcome the apparent lack of models.

7. CONCLUSIONS AND RECOMMENDATIONS

The following conclusions can be drawn from the results of this study.

Analytical methods are available which allow the explicit determination of optimum test intervals for single component systems and k-out-of-n systems. Their applications to systems of technical interest are limited however. Despite these short comings, the analytical methods offer a comprehensible way to study major effects and parameters which influence the system unavailability. For this reason, they are recommended as a starting point for test interval optimization studies. Jacob's methodology seems to be the easiest method. The formulation by Colemand and Abrams offers the highest flexibility in terms of additional parameters considered. However, by accounting for these parameters, such as detection inefficiency, imperfect test,and the like, the optimum test interval can be only obtained implicitly by iterative methods.

The only reliable method for determining optimum test intervals for complex technical systems is by computer code. For this purpose, the code FRANTIC has been implemented and benchmarked at MIT against analytical methods as well as other more sophisticated codes such as PL-MODT. The results of these studies clearly show that FRANTIC can be recommended for practical engineering day-to-day work. All of the approximations employed in the code render it conservative compared to more elaborate methods.

Several simplified engineered safety systems have been studied with FRANTIC. These studies indicated the importance of the test strategies for redundant systems as well as the need for the determination of point unavailabilities which are provided by FRANTIC.

The comparison of optimum test intervals determined by analytic means and those derived from FRANTIC showed that the former do not provide the minimum unavailabilities for more complex systems. Due to the existence of several components in those systems which are tested at different times and for different periods the functional dependence of the system unavailability versus the test interval of one component, say the D.G., of this system does not necessarily display the unique curve which is obtained for a single component. One additional reason for this is the lack of appropriate wearout models in codes like FRANTIC.

Despite the successful application of FRANTIC for the small systems studied during this research, some of its shortcomings are worth mentioning. These are summarized below.

- The reason that only small systems were analyzed lies in the inconvenience for the user to derive the system unavailability function for input into FRANTIC. This function is difficult to obtain for complex systems. In order to avoid the derivation and possible errors which may occur during this process, FRANTIC should be coupled to a code which automatically determines the minimal cut sets.

- The code does not account for wearout and its impact upon failure rates.

- No reliable information is available for detection inefficiency. This problem is closely related to human reliability which is an area not well understood thus far.

- There exists a substantial uncertainty in most of the input data. However, FRANTIC does not allow the propagation of these uncertainties to the top event. It is recommended therefore, that FRANTIC should be coupled to a Monte-Carlo simulation package which allows for a broad spectrum of possible distributions.

Notwithstanding the aforementioned drawbacks, it is thought that the methodology developed during this research project provides a good basis for the technical assessment of optimum test interval. Continued efforts in this field are strongly recommended because reliability and availability allocations will certainly be integral parts of system design in the near future.

APPENDIX A

Collection and Analysis of
Diesel Generator Performance Data
and Related Equipment

A literature survey on operational data of diesel generators and related equipment turned up 96 failures in the U.S. with respect to start and assuming load over the minimum number of 3208 starts in the three years period from 1975-1977. Table A-1 summarizes the whole data set. These data were the basis from which failure rate and unavailability per demand were derived. It is worth mentioning here that the diesel generators covered in the review differ substantially with respect to design and power rating. Therefore, each category would result in different failure rates. Despite of recognizing this fundamental difference, it has been decided to use the overall failures for the analysis. This seems to be a conservative assumption although it should be realized that larger sized units may be subject to more failures especially when those units are newly introduced on themarket. Another conservatism has been introduced into the analysis by considering both PWR and BWR systems. The data have been analyzed in accordance with the formulation used in the Reactor Safety Study. Thus, the failure rate follows from

$$\lambda = \frac{n_f}{N_P N_c T}$$

where:

n_f : number of failures observed

N_P : number of plants

N_c : average number of components per plant

T : observed (standby) time period (8760 hrs)

TABLE A-1

Diesel Generator Failure Data for the Period
1975-1977 U.S. Nuclear Power Plants

Plants	Units	Min. No. of starts	Diesel Generator Category A	Failure Category B
Calvert Cliffs 1	2	31		
Calvert Cliffs 2	1	8	2	
Pilgrim 1	2	72		2
Conn. Yankee	2	72		
Indian Point 1	-			2
Indian Point 2	3	108		1(F.T.C.)
Indian Point 3	-			
Beaver Valley	2	16	3	1(F.T.C.)
Oyster Creck	2	72		
Maine Yankee	2	72		
Three Mile Island	2	72	1	
Nine Mile Island	2	72		
Fitzpatrick	2	48	1	1
Millstone 1	1	36	3	
Millstone 2	2	216		1 (Fire)
Peach Bottom 2	2	72		1 (F.T.C.)
Peach Bottom 3	1	36		
Ginna	2	72		
Vermont Yankee 2	2	72		
Dresden 1	1	36		
Dresden 2	2	72	7	1(F.T.C.)
Dresden 3	1	36		
Zion 1	3	188	2	1
Zion 2	2	72		
Quad Cities 1	2	72		
Quad Cities 2	1	36		
Cook 1	2	72		
Arnold	2	72		2,1 (F.T.C.)
Cooper	3	108	1	2
Monticello	2	72	1	
Prairie Island 1	2	72	1	
Prairie Island 2	-			
Fort Calboun	2	72	2	1 (F.T.C.)
Point Beach 1	2	72		
Point Beach 2	-	-		
Kewannee	2	72	1	
Arkansas	2	72	1	
Brunswick 2	2	56		1
Turkey Point 3	2	72		
Turkey Point 4	-		1	1 (F.T.C.)
St. Lucie	2	24	3	
Crystal River	2	18	1	
Hatch 1	2	48	3	
Browns Ferry 1	3	84		
Browns Ferry 2	3	63		
Browns Ferry 3	-			
Surry 1	2	72		

			Diesel Generator	Failure
Plants	Units	Min. No. of starts	Category A	Category B
Surry 2	1	36		
Humbolt Bay	1	36		
Trojan	2	38		
Rondo Seco	2	64	3	
San Onofre 1	2	72		
Yankee Rowe	3	108		
Big Rock Point	1	36	2	
Palisades	2	72	1	
La Crosse	1	36		
Total	95	3208	42	26

Notation: Category A: Diesel Generator failed to start

Category B: Diesel Generator failed to run continuously

F.T.C.: Diesel Generator Circuit Breaker failed to close

From Table A-1 the following value result for the parameters n_f and $N_P N_c$,

$$n_f = 42 + 26 = 68$$

$$N_P N_c = 95$$

Thus,

$$\lambda = \frac{68}{95 \text{ x } 3\text{yr} \text{ x } 8760 \frac{\text{hr}}{\text{yr}}} = 3 \text{ x } 10^{-5}\text{hr}^{-1}$$

The formula for the unavailability per demand from the RSS reads

$$Q_d = \frac{n_f}{N_P N_c N_T}$$

where:

N_P : number of plants

N_c : average number of components per plant

N_T : average number of tests (demands) performed per component per year

From Table A-1 the following values result for the parameters n_f and $N_P N_c N_T$

$$n_f = 68$$

$$N_P N_c N_T = 3208$$

Thus,

$$Q_d = \frac{68}{3208} = 2 \text{ x } 10^{-2}$$

As the Table A-1 indicates the diesel generator circuit breaker failed to close 8 times. thus,

$$\lambda(\text{CCT BKR}) = \frac{8}{68} \text{ x } \lambda = 3.2 \text{ x } 10^{-6}\text{hr}^{-1}$$

It is interesting to note that if only diesel generator failures of category A, i.e., failure to start are considered, Q_d decreases to the following value

$$Q_d = \frac{42}{3208} = 1.3 \times 10^{-2}$$

which is more than a factor 2 lower than the value used by the RSS.

The result of the literature survey is compared to the values used in the RSS [7] which had obviously employed data available up to 1973. Table A-2 summarizes the comparison. As can be seen from the table, the differences between both data sources are negligible for most cases. A set of recommended conservative values is included in the last column of Table A-2 which summarizes the most conservative ones from each of the data sources.

TABLE A-2

Comparison of Results of a Literature Survey for the Period 1975-77 with the Results Used in WASH-1400

Component	Quantity	Literature Survey	WASH-1400	Recommended Conservative Valve
D.G. fail to start and assume power	λ(EDG)	$3x10^{-5}$ hr^{-1}	$3x10^{-5}$ hr^{-1}	$3x10^{-5}$
unavailability upon demand	Qd(EDG)	$2x10^{-2}$/d	$3x10^{-2}$/d	$3x10^{-2}$/d
BAT. failure rate (degraded)	λ(BAT)	$1.14x10^{-5}$ hr^{-1}	10^{-6} hr^{-1}	$1.14x10^{-5}$ hr^{-1}
unavailability upon demand	Qd(BAT)	$1.14x10^{-4}$/d	10^{-3}/d	10^{-3}/d
NET failure rate	λ(NET)	$1x10^{-5}$ hr^{-1}	$2x10^{-5}$ hr^{-1}	$2x10^{-5}$ hr^{-1}
unavailability upon demand	Qd(NET)	$2x10^{-4}$/d	10^{-3}/d	10^{-3}/d

APPENDIX B

Statistical Analysis of Maine Yankee Experience with Diesel Generators

This appendix discusses the estimation of parameters and the confidence intervals placed on those parameters. A confidence interval is defined as being a range of values to include the particular values of the parameters being estimated with a pre-assigned degree of confidence. Such an exercise will normally define a range of values within which the true value is believed to lie for a particular 'confidence level.' The estimated range or interval for the parameter is termed the confidence interval and the end points of the interval are called confidence limits. It is a well-known fact [29] that the best way of finding these confidence level estimates is to use the χ^2 distribution test. For an exponential probability density function of

$$f(t) = \theta e^{-\theta t}$$

where θ is the true failure rate per unit time.

t is the time range

the true failure rate, θ, can be found from the estimated failure rate, $\hat{\theta}$, from the sample population within the confidence level of p by the following expression [29].

$$\frac{\hat{\theta}\chi^2_{2,1}}{f} \leq \theta \leq \frac{\hat{\theta}\chi^2_{2,2}}{f}$$

where,

$f = 2(n)$ degrees of freedom

n = NO of failure during the testing period T

$\hat{\theta} = \frac{n}{T}$

$\chi^2_{2,1}$ = lower confidence limit of χ^2 test with probability of $\frac{1-p}{2}$ and degrees of freedom of f

$\chi^2_{2,2}$ = upper confidence limit of χ^2 test with probability of $\frac{1+p}{2}$ and degrees of freedom of f.

NOTE: For the case of no failure during the testing period T, obviously, the straightforward estimate of the mean failure rate would be zero. However, there is always a possibility that the last failure will not occur before the termination of the testing period. Therefore, in practice, one failure will be considered for the test.

In our situation, Main Yankee, there was no failure after five years of operation. Therefore

$T = 5 \times 8760 = 4380$ hr

$n = 1$

$f = 2$

and considering three diferent confidence levels of 50, 90, and 99%, the true failure rates will have the following ranges:

confidence level%	50	90	99
upper limit	1.58	6.84	12.1
θ (1 hr) x 10^5			
lower limit	1.58	0.1175	0.0114

$$\text{lower limit} \leqslant \theta \leqslant \text{upper limit}$$

Comparison of the above results and the results from the Appendix A suggests that our analysis with $\theta = 3 \times 10^{-5}$ is quite consistent with that of Main Yankee with 90% confidence. It is also worth mentioning that with the aforementioned confidence level the mean unavailability will be

$$Q = \frac{\theta . t}{2} \qquad t = 720\text{hr (one month)}$$

$$4.23 \times 10^{-4} \leqslant \theta \leqslant 2.46 \times 10^{-2}$$

which is again consistent with our goal unavailability which was discussed in the text of the report.

APPENDIX C

Description of the Remainder of the Fault Tree Appearing in Fig. 5.2

For complete drawing of the Fig. 5.2, a thorough knowledge of the emergency power system was required, and since we were only interested in the 4160 V emergency buses the expanded fault tree of these buses, 5 and 6, which in fact are the same was given in Fig. 5.3. For the rest of the numbers referred to in Fig. 5.2 the top event failures are given here only.

Numbers	Failure Events
11 & 12	I.P. on Buses (4160 V) 5 and 6
13 & 14	I.P. on Buses (480 V) 7 and 8
15 & 16	I.P. on Buses (480 V) MCC-7A & 8A
17 & 18	I.P. on Buses (480 V) MCC-7B & 8B
19 & 20	I.P. on Buses (125 VDC) DC-A & DC-B
21 & 22	DC Buses of Train A or B Shorted

I.P. is Insufficient Power

REFERENCES

[1] Institute of Electrical and Electronic Engineers- Inc., "Trial-Use Guide: General Principles for Reliability Analysis of Nuclear Power Generating Station Protection Systems," IEEE Std. 352-1972.

[2] Hirsch, M.M.: Setting Test Intervals and Allowable Bypass Times as a Function of Protection System Goals, IEEE Trans. Nucl. Sci. N-18 (1971), 488-494.

[3] Coleman, J. and Abrams, J.: Mathematical Model for Operation Readiness, J. Oper. Res. Soc. 10 (1962), 126.

[4] Jacobs, I.M.: Reliability of Engineering Safety Features as a Function of Testing Frequency, Nuclear Safety, 9 (1968),4.

[5] Vesely, W.E. and Goldberg, F.F.: FRANTIC-A Computer Code for Time Dependent Unavailability Analysis, NUREG-0193

[6] Vesely, W.E.: Reliability Quantification Techniques Used in the Rasmussen Study, In Reliability and Fault Tree Analysis, R.E. Barlow et al., eds., SIAM, (1975), 775-803.

[7] Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, Oct. 1975.

[8] Hirsch, M.M.: Methods for Calculating Safe Test Intervals and Allowable Repair Times for Engineering Safeguard Systems, NEDO-10739, 1973.

[9] Green, A.E. and Bourne, A.J.: Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors, AHSB(S) R117, 1966.

[10] Weiss, G.M.: A Survey of Some mathematical Models in the Theory of Reliability, In: Statistical Theory of Reliability, M. Zelen, Ed., The University of Wisconsin Press, Madison, Wis., 1963.

[11] Hunter, L.C.: Optimum Checking Procedures, In: Statistical Theory of Reliability, M. Zelen, Ed., The University of Wisconsin Press, Madison, Wis., 1963.

[12] Felhinger, B.J.: A Markovian Model for the Analysis of the Effects of Marginal Testing on System Reliability, Ann. Math. Stat. 33(1962), 754.

[13] Apostolakis, G.E. and Bansal, P.P.: The Effect of Human Error on the Availability of Periodically Inspected Redundant Systems, UCLA-ENG-7650, 1976.

[14] Young, D. and Conradi, L.L.: Including the Potential for Human Error in Fault Tree Analysis of Nuclear POwer Systems, Proc. 2nd Int. System Safety Conf., San Diego, 1975.

[15] Dressler, E., Spindler, H.: The Effect of Test and Repair Strategies on Reactor Safety, IAEA-SM-195/20, 551-556.

[16] Dressler, E., Spindler, M.: The Unavailability of Standby Systems as Function of Test Strategy and Repair Time (in German), MRR-144, 1975.

[17] Kontoleon, N. et al.: The Throw-Away-Maintenance Philosophy versus Repair, IAEA-SM-195/21, 1975, 679-687.

[18] Mastran, D.V.: A BAyesian Scheme for Sequentially Testing A Multi-Component System, IEEE Trans. on Reliability R-25 (1976), 270-272.

[19] Vesely, W.E.: Analysis of Fault Tree and Kinetic Tree Theory, IN-1330.

[20] Wolf, L.: REBIT - Reliability and Unavailability Analysis by Bit-Handling, Unpublished Report, Dept. Nucl. Eng., MIT, 1975.

[21] Modarres, M. and Wolf, L.: PL-MODT: A Modular Fault Tree Analysis and Transient Evaluation Code, Trans. Am. Nucl. Soc., 28 (1978), 510.

[22] Modarres, M. and Wolf, L.: Reliability and Availability Analysis of Complex Technical Systems Using the Fault Tree Modularization Technique, unpublished report, Dept. Nucl. Eng., MIT, Nov. 1978.

[23] Olmos, J. and Wolf, L.: A Modular Approach to Fault Tree Analysis and Reliability Analysis, NE-209, Dept. Nucl. Eng., MIT, Aug. 1977.

[24] Vesely, W.E.: A Time-Dependent Methodology for Fault Tree Evaluation, Nucl. Eng. Design 13 (1970, 337.

[25] Lambert, H.E.: Fault Tree for Decision Making in System Analysis, UCRL-51829, Oct. 1975.

[26] S. Levine: The Role of Risk Assessment in the Nuclear Regulatory Process, Nuclear Safety, vol. 19-5, 556-564.

[27] Cooks, J.L. and Vissing; G.S.: Diesel Generator Operating Experience at Nuclear Power Plant, OOE-002, June 1974.

[28] IEEE STandard 279: Criteria for Protection Systems for Nuclear Power Generating Station, 1971.

[29] Bourne, A.J. and Green, A.E.: "Reliability Technology", Wiley-Interscience, a division of John Wiley & Sons, Limited, London, New York, Published 1972.