ENERGY LABORATORY

MASSACHUSETTS INSTITUTE
OF TECHNOLOGY

A METHOD FOR ESTIMATING COMMON CAUSE FAILURE PROBABILITY AND MODEL PARAMETERS THE INVERSE STRESS-STRENGTH INTERFERENCE (ISSI) TECHNIQUE

by
Ching Ning Guey

Energy Laboratory Report No. MIT-EL 84-010

July 1984

A METHOD FOR ESTIMATING COMMON CAUSE FAILURE PROBABILITY AND MODEL PARAMETERS: THE INVERSE STRESS-STRENGTH INTERFERENCE (ISSI) TECHNIQUE

by

Ching Ning Guey

Principal Investigator
Prof. Carolyn Heising

Energy Laboratory
and
Department of Nuclear Engineering

Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Sponsored by:

Northeast Utilities Service Company
Pickard, Lowe and Garrick Incorporated

under the

MIT Energy Laboratory Electric Utility Program

MIT Energy Laboratory Report No. MIT-EL 84-010

July 1984

A METHOD FOR ESTIMATING COMMON CAUSE FAILURE PROBABILITY AND MODEL PARAMETERS: THE INVERSE STRESS-STRENGTH INTERFERENCE (ISSI) TECHNIQUE

by

CHING NING GUEY

ABSTRACT

In this study, an alternative for the analysis of common cause failures (CCFs) is investigated. The method studied consists of using the Licensee Event Report (LER) data to get single component failure probability and using stress and strength parameters to evaluate multiple component failure probabilities. Since an inversion of stress-strength interference (SSI) theory is involved, the approach is called the inverse stress-strength interference (ISSI) technique.

The ISSI approach is applied to standby systems in commercial nuclear power plants. At a component level, major pumps and valves are studied. Comparisons with other CCF analysis methods indicate that the medians based on the ISSI method are slightly higher because of the inclusion of potential failure causes. Applications to multiple-train systems show that the ISSI method agrees well with the beta factor method. In all cases studied, it appears that uncertainty intervals associated with the ISSI are smaller than other methods.

This study suggests that the ISSI method is a promising alternative to estimate CCF probabilities. The method will be particularly valuable when:

(1) Component-specific and system specific values are needed.
(2) Failure data are scarce.
(3) Level of redundancy is high.
(4) Uncertainty needs to be quantified.

Table of Contents

List of Figures

List of Tables

List of Tables (Continued)

ACKNOWLEDGEMENTS

I would like to take this opportunity to express sincere thanks and appreciation to my thesis advisor Prof. Carolyn D. Heising for her support, encouragement and patient guidance throughout the course of this work. It was she who originally suggested the use of the stress-strength interference approach to estimating common cause failure analysis parameters and the general framework of this thesis. I am also grateful to my thesis reader, Prof. Norman C. Rasmussen, who patiently struggled with me through evolutions of this study. Prof. John E. Meyer also gave me insightful comments on some important "trees-in-the-forest" of my major work. In addition, I am also indebted to his constant amiability during my studies at M.I.T.

I would also like to express my sincere appreciation of the help offered by the staff in the Scientific Writing Program, especially, Steve Strang, to make my thesis more readable.

Financial support provided by Northeast Utilities Service Company and Pickard, Lowe and Garrick Inc., via the M.I.T. Energy Laboratory throughout my study is highly appreciated.

Last but not least, I sincerely appreciate the time and effort my wife Su-Ju has devoted in taking good care of all members of my family so that I can complete the work in time.

Executive Summary

The objectives of this thesis have been twofold: the developmemt of a methodology for the evaluation of common cause failure probabilities of multiple-train systems; and the demonstration of the methodology through its application to standby safety systems in commercial nuclear power plants.

Methodology

One problem with the common cause failure analysis (CCFA) of safety systems originates from, among other things, the lack of an appropriate data base. This lack limits, in particular, the usefulness of conventional statistical methods to perform meaningful CCFA. Very few approaches have been developed which explicitly incorporate engineering considerations and quantify engineering judgment based on laboratory experiments.

Although the common load model provides a probabilistic framework for computing the multiple failure probability, it remains essentially a theoretical construction due to the difficulty of implementation. The ISSI technique proposed in this thesis represents the first attempt to combine engineering knowledge with operating experience to evaluate multiple failure probabilities. The basic idea is to decompose the failure occurrences into constituent causes.

For each cause, there are two ways to compute single failure probability. One is to use the SSI formalism. The other is to adopt statistical procedures in analyzing the LER data. To evaluate the multiple failure probability, we may apply the extension of the SSI formalism, the so-called common load model. A conventional practice is, where possible, to perform statistical analyses of data.

The key step in the ISSI technique is to recognize that the single failure probability estimates, obtained from conventional statistical evaluation of the LER data, is relatively more significant (by the virtue of a relatively larger sample size) than the multiple failure probabilty estimates. The ISSI technique consists of inverting the LER estimates of single failure probability to derive a constraint on the unknown stress and strength parameter. The engineering knowledge about each failure cause is then used to find the unknown parameter. One can then proceed to calculate the multiple failure probabilities by using the expressions derived via the common load model.

Four different models, encompassing common engineering interests, have been investigated. The normal model represents an engineering situation in which both the stress and the strength of a component are normally distributed. This is a useful approximation for components that have a good quality control. The lognormal model describes an engineering situation in which both the stress and the strength of a component are lognormally distributed. Two

types of mixed models have been studied. The first represents the normally distributed stress and the lognormally distributed strength, called the normal-lognormal model. The other describes the lognormally distributed stress and the normally distributed strength, called the lognormal-normal model. Numerical studies performed for typical engineering situations show that, for a given single component failure probability, the normal model gives the lowest multiple failure probabilities. The lognormal model, on the other hand, yields the highest CCF probabilities. The normal-lognormal model gives slightly higher CCF probability than the normal model, but lower than the lognormal-normal model. Thus, if an engineer is not certain about the stress-strength models underlying a particular situation, he can use the lognormal model as an upper bound. Similarly, he can use the normal model as a lower bound.

Three cases have been investigated:

Case 1: V_R and V_S Known

Case 2: V_S and M Known

Case 3: V_R and M Known

Here V_R, V_S represent the coefficient of variation of strength and stress respectively. M is safety factor, i.e. the ratio between the mean strength and the mean stress. The sensitivity of the multiple failure probability to changes in the stress-strength parameters has been explored. In

particular, case 1 has been studied to a greater depth than the other two. This is because that current engineering practices usually provide information as required for case 1, i.e. the variability of both the stress and the strength for each specific failure mode.

Numerical studies indicated that the multiple failure probability, for a given single failure probability, depends strongly on the ratio of V_R and V_S. The larger the loading roughness (defined as V_S/V_R), the larger the multiple failure probability. Furthermore, if the single failure probability is greater, other conditions being the same, the multiple failure probability increases. This agrees with common practices in which active components have a higher failure probability than passive ones. For example, it has been a 'rule-of- thumb' to assume that the beta factor is 0.2 for active components (e.g. pumps), and 0.1 for passive components (e.g. valves). The sensitivity studies also suggested that the larger the values of the V_R and V_S, the smaller the multiple failure probability.

The ISSI approach not only yields the multiple failure probabilities directly, but it also provides an alternative for estimating parameters in other advanced CCF models. In particular, expressions for multiple dependent failure fractions f_k in the MDFF method and β , γ , and δ in the MGLM have been derived.

Demonstration of The Methodology

An application of the ISSI technique to important mechanical components in commercial nuclear power plants has been performed. Major pumps and valves in the HPIS and the AFWS have been studied from the perspective of the ISSI approach.

Two failure modes stand out as major contributors to the LER occurrences. It is not unexpected that tribological causes have been identified as a category of special concern. Design engineers tend to regard friction, wear and lubrication as a major concern for operating and maintenace crew. The fact that the ASME code does not have specific requirements for the tribological aspects of pump and valve designs has made engineers think that wear-related failures are of secondary importance. It is unfortunate that after most traditional aspects of the design have been addressed in detail, the 'next' important failure cause, namely the tribologically induced, has become the dominant failure mode, because insufficient attention is devoted to it.

Another major failure contributor identified is foreign material contamination. This is not associated with the pump or valve per se, but with the related electrical parts that support the adequate function of the pump or valve. Circuit breakers, relays and switches are in this category.

The results of the application of the ISSI approach have indicated that it yields smaller uncertainty compared with other common statistical CCFA methods. Intuitively, this is related to the efficient use of engineering knowledge. It is

generally true that the uncertainty in most engineering studies of the material properties, for a particular well-defined failure mode, is usually less than 20%. If we decompose the field failure data into specific root causes and bring to bear related engineering principles and laws, we have a better grasp of the prediction than dealing with the field data directly. By analyzing each failure mode with higher confidence, and then synthesizing all pertinent failure modes into the overall failure, one expects to have a reduced uncertainty in the end results. This 'divide and conquer' mechanism is, in essence, the approach adopted in the ISSI technique.

The sensitivity of the final results to different sources at a system level is also illustrated. The variation in both the input data and the models is investigated.

An idealized AFWS is studied first. Results indicate that order-of-magnitude underestimates exist if the CCFs are not taken into account. Furthermore, the conventional beta factor method yields higher estimates for the multiple failure probability.

The HPIS is next evaluated. Two configurations have been addressed. For a typical Westinghouse three-loop plant, the charging pumps are used for the purpose of high pressure injection in addition to its normal function of chemical and volume control. This configuration contains a combination of doubly and quadruply redundant trains. The other HPIS design investigated typifies a Westinghouse four-loop plant.

In this design, two additional HPIS pumps are provided. This configuration is in essence a 1-out-of-4 system as far as four pumps are considered. Three cases are studied for this configuration. First, we assume that the charging pump trains and the HPIS trains are independent. This yields such a small probability of failure that the CCFs are not of concern. Second, if the HPIS and the charging pump trains are identical, the unavailability is approximately a thousand times larger. In actuality, the system unavailability is in-between. If one considers only those root causes that are common to the HPIS pumps and the charging pumps (instead of all root causes as in redundant case studied above), the unavailbility is approximately 2.9 x E-6. The results indicate that when CCFs are present, marginal improvements result from adopting a higher redundancy. Cost-benefit analysis is required to decide the choice of a proper configuration.

This study suggests that the ISSI method is a promising alternative to estimate CCF probabilities. The method will be particularly valuable when:

(1) Component-specific and system specific values are needed.

(2) Failure data are scarce.

(3) Level of redundancy is high.

(4) Uncertainty needs to be quantified.

Chapter 1

Introduction

1.1 Background

Since the draft Reactor Safety Study{1.1} report was published in 1974, there has been substantial discussion on the use of probabilistic risk assessment (PRA) in the nuclear regulatory process. One of the critical problems in risk analysis study is the adequate evaluation of dependent failures among important safety systems{1.2}. In particular, a subclass of dependent failures called common cause failure has been a controversial issue in PRA studies. In essence, difficulties associated with common cause failure analysis (CCFA) focus on :

(1). discrepancies in the definition of CCF,

(2). the modelling of CCF, and

(3) the estimate of parameters in CCFA models.

In order to have a meaningful PRA, the problems of CCFA have to be addressed satisfactorily. Risk analysis results are sometimes very sensitive to the way in which CCFs are dealt with. Order-of-magnitude difference may exist between various CCFA modeling methods. In addition, within each modelling approach, the procedure for estimating model parameters also affects results significantly. One of the reasons for this state of affairs stems from the lack of an appropriate data base. This difficulty is even more serious in the case of highly redundant systems.

Prevailing CCFA methods are based mainly on statistical analyses of historical data from operating plants. Since failure-related data are extremely scarce, the uncertainty of the results is thus often too large to make inferences significant. Moreover, the applicability of generic data to an individual plant is fairly difficult to judge without a substantial physical understanding of the component failures of interest. Under such a predicament, it is important for the engineer to get insight into the elements of CCF and to depend less on fuzzy statistical methods.

CCFs are not merely hypothetical events in PRA studies. For example, two incidents at the Salem 1 reactor sey in February, 1983 marked notoriously in the American nuclear program that the automatic scram system failed to function on an operating reactor. On both occasions, two Westinghouse DB-50 circuit breakers simutaneously failed to operate on signal because the UV trip attachments (relays) were dirty and worn{1.3,1.4}. This highlights the practical importance of eliminating or reducing the probability of CCF occurrences in commercial nuclear power plants. This paper contends that only through understanding the failure phenomena thoroughly and taking them into account during the components' entire life-cycle can an engineer achieve a reliable performance. The proposed approach sheds some light on how an engineer, involved in either design or

maintenance, can explicitly factor in some of the important elements that affect the probability of common cause failures.

1.2 Objectives

Inherently, reliablility data are hard to come by. In particular, the CCF data for multiple-train systems are even more difficult to obtain because of the low probability of such occurrences. The present study thus has the following objectives:

(1) providing a convenient framework in which CCFs are addressed(in particular, the approach used is aimed at multiple-train systems);

(2) presenting a method in which data requirements are relatively easy to satisfy; and

(3) demonstrating a procedure by which engineering considerations are quantified explicitly and the uncertainty of results reduced.

To accomplish these goals, the following tasks had to be performed:

(1). developing a method, called the inverse-stress-strength interference (ISSI) technique, in combination with common load models to evaluate multiple component failure probabilities;

(2). identifying failure causes that lead to component failures from licensee event reports (LERs);

(3). specifying and quantifying factors influencing failure causes identified in task 2;

(4). synthesizing factors affecting each failure cause to obtain parameters needed in the ISSI method; and

(5). combining mechanism-specific multiple component failure probabilities to derive overall multiple component failure probabilities.

It is useful to understand the assumptions under which these tasks were performed. In order to make the analysis compatible with the current available reliability data base such as the LERs, the present investigation focuses on the following:

(1) Internal events only

This limitation is intended for the purposes of considering enviromental conditions that the redundant components are normally subjected to. External events such as earthquakes, flooding, missiles, tornadoes, etc., important as they are, are not included. In the context of this study, internal events refer to common hardware failures due to the interaction of the mechanical component with its environmental conditions such as pressure, temperature, vibration, wear, etc.

(2) 'Normal' operating conditions

Although it is possible in principle to analyze component failure under accident conditions using the framework expounded in this thesis, the lack of data imposes a strict constraint to overcome. The 'normal' conditions refer to the operating status of the plants containing the components of interest. For the systems

studied in this thesis, the conditons under which the components are specified to operate remain essentially the same as in normal operating conditions. This is true in general for components not located in reactor containment.

(3) Standby systems

One of the concerns in the defense-in-depth philosophy of the safety system design is the low availability associated with engineered safety features. To limit the present study, such systems are thus chosen to illustrate the method proposed. However, the approach can certainly be used in other systems as well.

(4) Design, manufacture, installation, operation, and maintenance errors

CCFs are the aggregation of all possible failure-inducing conditions accumulated during entire life-cycle of a set of redundant components. Separating them into different stages may be useful for some purposes, but it renders the quantification of CCFs an incomplete endeavor. The common association between redundant components mainly comes from an identical design concept, from similar manufacturing processes, or from similar installation procedures, etc. The combination of all these commom elements makes the assumption of statistical independence invalid.

(5) Coupled failure only {1.5}

A useful idea of this CCF classification scheme is to consider CCF as two types, shown in Fig. 1.1. Cascade failures refer to multiple failures where the failure of a component is caused by that of another identical component. In a sense this kind of failure can be visualized as an avalanche leading to the propagation of component failures. In general, to evaluate the multiple failure probability of cascade failure requires more knowledge of the system. The present study thus focuses only on the coupled failure as described in (4).

1.3 Organization

The organization of this thesis is as follows.

Chapter 2 describes in a concise manner the general aspects of CCF. First, definitions of CCF that have been used are discussed to distill the essential elements and place the issue in proper context. Then previously available studies on the quantification of CCFs are briefly reviewed with emphasis on the principle, the disadvantages, and the advantages associated with different methods. The models reviewed include the beta factor method, the binomial failure rate model (BFR), and the coupling method. To conclude this chapter, a rigorous probabilistic framework is presented to provide a solid basis for the proposed approach.

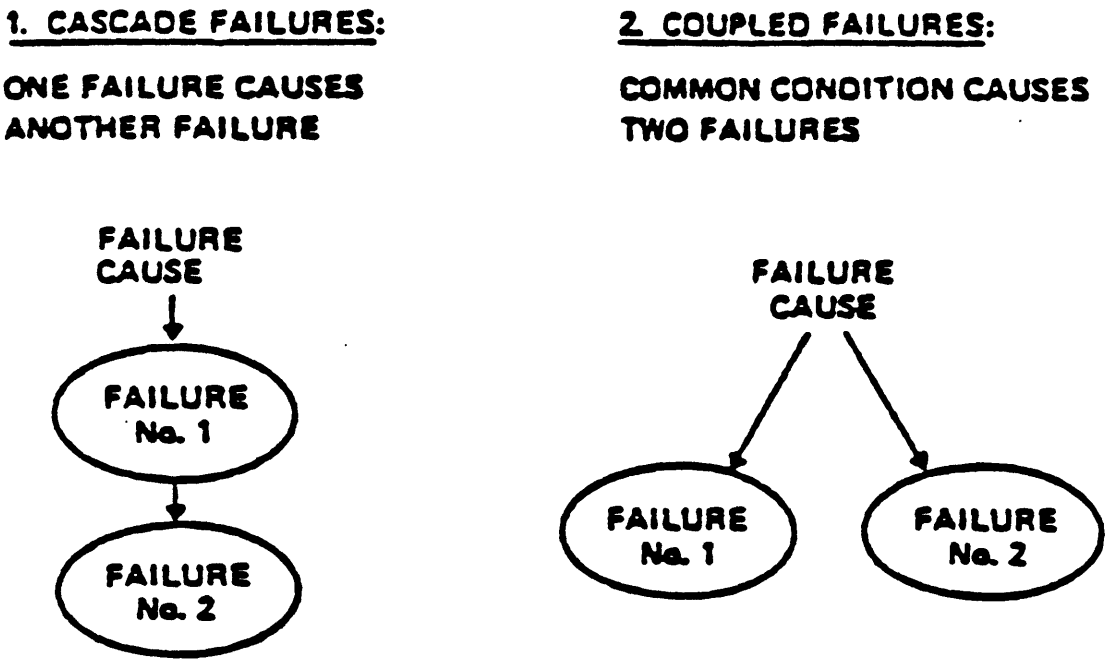


Figure 1.1 Common Cause Failure Types (Ref. 1.5)

Chapter 3 discusses recent developments in the CCFA of multiple-train systems. Two methods are briefly examined. The multiple dependent failure fraction (MDFF) method is first discussed. In particular, the generalization of this model to 1-out-of-4 systems is studied in detail. The multiple Greek letter method (MGLM) is next described. Both methods require more data than the beta factor method to statistically estimate model parameters. A simple relationship between the MDFF method and the MGLM is then derived to show that they are conceptually equivalent. Chapter 3 ends with a brief discussion of the difference between the beta factor method and the multiple-train method.

Chapter 4 starts with a description of the general nature of stress and strength. The different level of sophistication to model these two entities are outlined. Having set the stage, we then present the stress-strength interference (SSI) theory with useful expressions derived for some common engineering distributions. Then the concept of the SSI is generalized to systems with k redundant components to derive the commom load model. Useful expressions based on this model are then derived for both normal and lognormal distributions.

Chapter 5 presents an innovative approach to model CCFs. Recognizing the scarcity of multiple failure data, we describe a method which makes use of only single component failure data. Then, assuming an analyst can estimate any of

the three parameters - V_R (the coefficient of variation of strength), V_S (the coefficient of variation of stress), and M (the safety factor) - the ISSI technique is used to compute multiple failure probability. Three cases are studied:

Case 1. V_R, V_S given

Case 2. V_R, M given

Case 3. V_S, M given

Some qualitative results for each case are next presented to give a feel for the general behavior of multiple failure probability based on this ISSI method.

Chapter 6 presents an application of the method to safety-related pumps and valves in commercial nuclear power plants. General mechanical failure considerations are first studied to provide a foundation for the specific analysis of pumps and valves. Important categories of failure mechanisms are then identified from the LERs. The role of tribological failures and foreign material contamination is then discussed. A comparison is then made among the results obtained based on the different methods discussed in Chapter 2.

Chapter 7 demonstrates the application of the ISSI method to evaluate CCF probabilities of standby systems in pressurized water reactors (PWRs). An idealized auxiliary feedwater system (AFWS) is first analyzed. Then, a high pressure injection system is studied to demonstrate the

sensitivity of final results to different CCF modelling techniques.

Chapter 8 summarizes the overall study and makes recommendations for further research.

Chapter 2

Generalities Of Common Cause Failures

2.1 Introduction

Many factors make the analysis of potential dependent failures, in particular CCFs, a rather difficult task. In order to view the results of different CCFA approaches in the proper light, it is important to keep such factors as the following in mind:

(1) the controversial nature of the definition and classification of common cause failures;

(2) the scarcity of reliable data sources for CCFs; and

(3) the serious limitations associated with existing methods of quantifying CCF probabilities.

This chapter attempts to summarize previous developments in dealing with different aspects of CCFs.

Section 2.2 discusses the definition dilemma and elements of various classification schemes. As more information is exchanged between different researchers in the CCFA, a consistent unified definition will emerge. Since a consensus about a relevant definition of CCF is an important step in dependent failure analysis, a special effort is made to review currently available terminology.

Section 2.3 describes CCFA models that have been proposed up to this time. The advantages and disadvantages of various CCFA methods are discussed to provide insight into the state-of-the-art of CCFA. Since only the quantitative

method is the focus of this thesis, qualitative methods are not addressed.

Section 2.4 presents a probabilistic formulation of CCF. This provides a general framework to account for CCF in a more rigorous fashion.

2.2 Definition And Classification Of CCF

Common cause failures mean different things to different people. Recent CCF discussions, evaluations, and conclusions have led to confusion. To clarify the issues so that CCF questions can be analyzed from some reasonably agreed -upon perspective ., it is necessary to have a clear definition that is in common use. To facilitate reliable communication, it is necessary to know the definition the CCF analyst has in mind when discussing specific examples, reviewing statistics, estimating the frequency of CCF in a system, or evaluating preventive measures.

Smith and Watson {2.1} defined a CCF as:

" Inability of multiple, first-line items to perform as required in a defined critical period of time due to a single underlying defect or physical phenomenon such that the end effect is judged to be a loss of one or more systems. "

A slightly revised version of the definition is:

" Inability of multiple (first-in-line) items to perform as required in a defined critical period due to a

common underlying defect or physical phenomenon such that the end effect is critical. "

An examination of the definition reveals the following elements:

a. Inability to perform as required

This is simply the definition of failure, irrespective of CCF issue. The product or component specification usually defines required performance and is thus the basis for failure determination and its criticality. Note that a failure while in the standby mode (e.g. HPIS pumps) belongs to this category whether a challenge occurs or not.

b. Multiple

This appears to be a universally accepted requirement for CCF. However, redundancy per se is not an additional constraint. Indeed, redundant component failure is a special case of multiple component failure. It is noted the loss of redundancy is often the uppermost consideration when dealing with CCFs. Although multiple component failure is used, it is of pratical interest only to cope with multiple failures of redundant components. For example, the simultaneous failure of a valve and a pump in redundant trains is usually not likely and is thus ignored.

c. First-in-line

In the early definition, this is explicitly assumed to exclude those failures that cascade along one or more

paths. This exclusion of cascade failures is a point of controversy. It is better to include both first-in-line and cascade failures as CCFs.

d. In a defined critical period of time

This is a more general term than 'simultaneous'. The point is fundamental to the CCF issue. The critical period strongly depends on the mission requirement. It may vary from seconds to hours to days depending on the demand on the system.

e. Due to a single underlying defect or physical phenomonon

This is the heart of the CCF issue. This common thread of failure potential separates the CCF into a class by itself. There are two kinds of commonality of cause. One is referred to as intrinsic (defects or errors from within the system), the other is extrinsic (external events such as earthquakes, floods, etc.) This study focuses on intrinsic events only.

f. End effect

If multiple failures occur, they must lead to the disabling of some system or major elements of the product. It follows from the definition that partial failures (e.g. 2 failures in a 1-out-of-4 system) do not constitute CCF.

Rasmuson et.al., {2.3} also discussed important concepts involved in the CCF definition. In particular, a distinction between common mode failures and CCFs is made.

In WASH-1400, "common mode failures" was used as an all-inclusive term. Almost any multiple failures that are not independent are included as common mode failures. More recently, as detailed in Ref.2.3, analysts tend to set aside the ambiguous term " common mode failures " and increasingly adopt " common cause failures" to represent the general study of dependencies between components. Since redundant components by nature share many dependencies, an analyst restricted to such components will garner most of the significant dependencies. However, if thoroughness is desired, the scope of analysis must be broadened to search for common causes resulting in dependencies among all components and not just similar components.

Since large differences exist in the scope of CCF definition, Vaurio {2.5} suggested that each analyst select those attributes essential for his definition and explain under what titles other features are taken into account. Other salient points worth noting include:

a. Foreseen versus unforeseen failures

It is sometimes considered an essential feature of CCFs that they are unforeseen events. Adopting this viewpoint would make the definition not only subjective but also variable in time. Since past events can be foreseen for future plants and eliminated or analyzed explicitly, it would become impossible by definition to have any specific data for future CCFs. A more stable definition is required. Nevertheless, it is useful to identify for

each event whether or not it had been foreseen before its occurrence. This would facilitate demonstrating that the frequencies of both foreseen and unforeseen CCFs are diminishing.

b. Challenges

To estimate the unavailability of a standby system, it is necessary to include all multiple failures while in the standby mode, not only those few that were accompanied with a challenge (i.e.a true demand or an initiator). The failure experience data would be virtually impossible to obtain due to the low probability of both a challenge and the failure of component given challenge.

Hartung {2.6} defines CCFs as coexistent failures of two or more systems or components due to a single cause. The definition encompasses two types of CCFs as illustrated in Figure 1-1. They are called "cascade failures" and "coupled failures". Cascade failures can be visualized as a sequence of two or more failures in which each failure results from the preceding one. For example, the failure of an instrument can be caused by steam released from a ruptured steam line. Coupled failures occur when a common adverse condition causes two or more systems or components to fail concurrently. For example, failure of several components can be caused by common design, manufacturing, maintenance, or operational error or flaw. Table 2.1 from the PRA procedure guide summarizes the different types of dependent

Table 2.1 Dependent Failure Classification (Ref. 2.7)

Type 1	Common Cause Initiators (external events) These include external and internal events that have the potential for initiating a plant transient and increase the probability of failure in multiple plant systems. These events usually, but not always, result in severe environmental stresses on components and structures. Examples include fires, floods and earthquakes.
Type 2	Intersystem Dependencies These are events or failure causes that create interdependencies among the probabilities of failure of multiple systems. States another way, intersystem dependencies cause the conditional probability of failure of a given system along an accident sequence to be dependent on the success or failure of systems that precede it in the sequence. There are several subtypes of interest in risk analysis.
Type 2A	Functional Dependencies These are dependencies among systems that follow from the plant design philosophy, system capabilities and limitations, and design base. One example is a system that is not used or needed unless other systems have failed. Another is a system that is designed to function only in conjunction with the successful operation of other system.
Type 2B	Shared Equipment Dependencies These are dependencies of multiple systems on the same components, subsystems, or auxiliary equipment. Example are: 1) a collection of pumps and valves that provide a coolant injection and a coolant recirculation function when the functions appear as different events in the event tree, and 2) components in different systems fed from the same electrical bus.

Table 2.1 (Continued)

Type 2C	Physical Interactions These are failure mechanisms, similar to those in common cause initiators, that do not cause an initiating event but nonetheless increase the probability of multiple system failures occurring at the same time. Often they are associated with extremeenvironmental stresses created by the failure of one or more systems after an initiating event. For example, the failure of a set of sensors in one system can be caused by the excessive temperature resulting from the failure of a second system intended to cool the heat source.
Type 2D	Human Interaction Dependencies These are dependcies introduced by human actions, including errors of omission and commission. The persons involved can be anyone associated with a plant life cycle activity, including designers, manufacturers, constructors, inspectors, operators, and maintenance personnel. Such a failure occurs, for example, when an operator turns off a system after failing to correctly diagnose the plant condition.
Type 3	Intercomponent Dependencies These are events or failure causes that result in a dependence among the probabilities of failure of multiple components or subsystems. The multiple failures of interest in risk analysis are usually within the same system or the same minimal cutset that has been identified for a system or an entire accident sequence. Subtypes 3A, 3B, 3C and 3D are defined to correspond with subtypes 2A, 2B, 2C and 2D, respectively, except that the multiple failures occur at the subsystem and component level instead of at the system level.

failures identified. {2.7} The major type of CCF considered in this research belongs to the type 3D dependent failure. The other type of CCF, i.e. cascade failure, corresponds to type 3A and 3C.

More recently, a modified labelling scheme {2.8} of component unavailability based on proximate cause has been devised. A summary of this classification is shown in Table 2.2. As can be seen, six classes are defined in this scheme as follows:

1. Independent failure

   the failure of a single component due to a noncomponent cause (i.e., not the unavailability of another component)

2. Cascade failure

   the failure of a single component due to the unavailability of another component.

3. Functional unavailability

   the inability of a single component to perform its intended function because of the lack of proper input. The proximate cause can be either the unavailability of another support or noncomponent cause.

4. Conditionally independent failures

   two or more component failures due to the same noncomponent cause. Conditional independence indicates that the multiple failures, while statistically coupled, are not related to each other in any physical or engineering sense. This is the same as the coupled

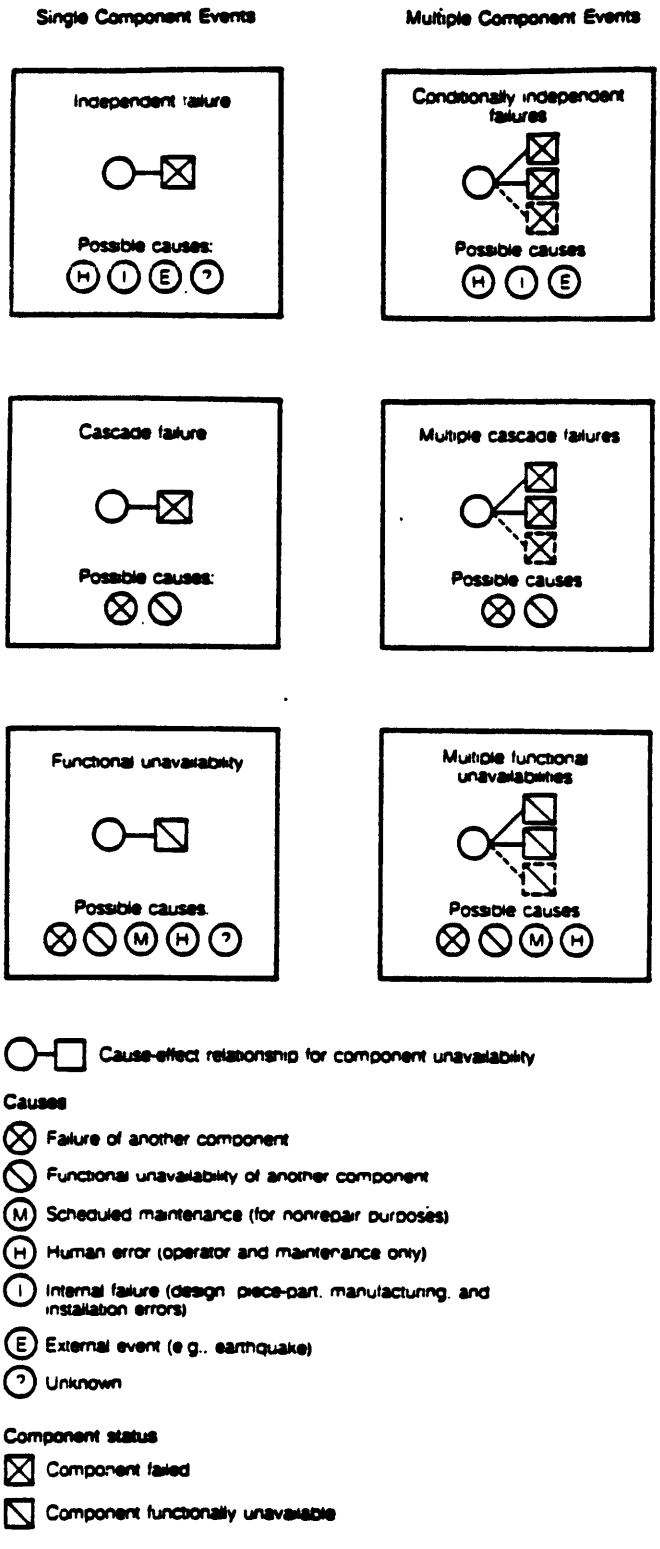


Table 2.2 Component Unavailability Event Classification
(Ref. 2.8)

failures defined earlier.

5. Multiple cascade failures

   two or more component failures directly caused by another single component.

6. Multiple functional unavailabilities

   the inability of two or more components to perform the function because of the lack of proper input. The proximate cause can be either the unavailability of another component or a noncomponent cause.

2.3 Previous Studies

A number of CCFAs are reviewed in Ref. 2.3. A more recent critical comparison is made by Hirshberg {2.9}. Since our major focus is on the quantitative aspects of CCF, only the beta factor method, the binomial failure rate (BFR) model and the coupling method will be discussed. Another method that is general but may become tedious as systems get more complicated is the Markovian analysis. In addition, the parameters required in the Markovian models are often difficult to obtain based solely on the analysis of historical data. For more information, interested readers can consult Ref. 2.10,2.11.

2.3.1 The Beta Factor Method

The beta factor method was introduced by Fleming in the AIPA study {2.12}. It is a generally applicable model and

easy to use.

In its simplest form, beta factor is defined to be

$$\beta = \frac{\lambda_2}{\lambda} \qquad (2.3.1)$$

where

$\lambda = \lambda_1 + \lambda_2$

λ_1 = independent failure rate

λ_2 = CCF rate

It then follows

$$\lambda_1 = (1-\beta)\lambda \qquad (2.3.2)$$

$$\lambda_2 = \beta\lambda \qquad (2.3.3)$$

By substituting the failure rate in terms of the beta factor into the Markov type of analysis, failure probability can be obtained for different level of redundancy.

A limiting feature of this method is the assumption of a complete coupling between redundant units. This means that the occurrence of a common cause will lead to total failure of all redundant units in a given system. This point will be discussed in more depth in section 3.4.

2.3.2 The Binomial Failure Rate Model

In an effort to obtain more detailed common cause assessments, Vesely [2.13] developed a statistical approach

for quantifying CCFs. The underlying model is based on the multivariate exponential distribution developed by Marshall and Olkin {2.14}. It is not intended here to give full description of the theory and analysis used in their work. Only a summary of key steps is discussed below.

For the quantification of CCF, it is assumed that common causes occur in accordance with a Poisson process. Thus the number of occurrences N_x of x components simultaneously failing in a population of m components in time period T is Poisson with parameter $\binom{m}{x}\lambda_x T$.

For the binomial failure rate case, the equation for λ_x is obtained by factoring the CCF rate into a total common cause rate and a detailed effect probability.

Let Λ be the sum of all the CCF rates for x_1 or more components simultaneously failing. Then,

$$\Lambda = \sum_{x=x_1}^{m} \binom{m}{x} \lambda_x \qquad (2.3.4)$$

where λ_x is the CCF rate for x specific components failing and all possible combinations are summed. Λ is the total CCF rate for the population. Assuming that when a CCF occurs, each component has a probability p of being affected by the common cause, the failure rate λ_x is given by :

$$\lambda_x = \frac{\Lambda}{C} p^x (1-p)^{m-x} \qquad (2.3.5)$$

where C is a normalization constant such that Eq. (2.3.4) is satisfied and is given by

$$C = \sum_{x=x_1}^{m} \binom{m}{x} p^x (1-p)^{m-x} \qquad (2.3.6)$$

The CCF rate λ_{i0} for i simultaneous failures, which are the failure rates used in reliability quantifications, are given by

$$\lambda_{i0} = \frac{\Lambda}{C} p^i \qquad (2.3.7)$$

The BFR model has been applied to the CCFA of valve leakages.{2.15} Other applications of the BFR to nuclear power plant components are reported in Ref. 2.14

2.3.3 Coupling Method {2.17}

It is assumed that the frequency of an event q is log-normally distributed, i.e.

$$q = m \exp (az) \qquad (2.3.8)$$

where z is a standard normal variate and m is the median of q. a is lognrmal standard deviation.

For parallel configuration, each with failure frequency q, one has the follwing expressions for system failure probabilities:

2-unit system $q^2 = m^2 \exp(2az)$

3-unit system $q^3 = m^3 \exp(3az)$

4-unit system $q^4 = m^4 \exp(4az)$ (2.3.9)

In most PRA studies, the failure frequency q is given in terms of a 90% interval estimate. Let the 95th percentile of q be q_{95}, and 5th percentile be q_{05} It can be readily shown that

$$a = (\ln q_{95} - \ln q_{05}) / 3.29 \qquad (2.3.10)$$

To obtain the upper and lower bound for a multiple failure case, the following expressions are useful:

2-unit system $q_{95} = m^2 \exp (3.29az)$

$q_{05} = m^2 \exp (-3.29az)$

3-unit system $q_{95} = m^3 \exp (4.94az)$

$q_{05} = m^3 \exp (-4.94az)$

4-unit system $q_{95} = m^4 \exp (6.58az)$

$q_{05} = m^4 \exp (-6.58az)$ (2.3.11)

Notice that if there is no coupling of q, the following expressions can be used instead:

2-unit system $q_{95} = m^2 \exp (1.41az)$

$q_{05} = m^2 \exp (-1.41az)$

3-unit system $q_{95} = m^3 \exp (1.73az)$

$q_{05} = m^3 \exp (-1.73az)$

4-unit system $q_{95} = m^4 \exp (2.00az)$

$q_{05} = m^4 \exp (-2.00az)$ (2.3.12)

Thus the interval for the coupled case is wider than the independent case. In chapter 6 multiple failure probability estimates based on this method will be compared with the ISSI method and the BFR method.

Table 2.3 Comparison of Quantitative Methods for CCF

Method	Advantages	Disadvantages
Beta Factor	1. Directness and flexibility 2. Only one parameter necessary 3. Easy to estimate	1. No allowance for partial failures 2. Simultaneous failures
Binomial Failure Rate	1. Much information can be extracted from scarce data 2. Distinction made between partial and total failures	1. Complicated estimation procedure 2. CCF causes assumed to have equal severity
Coupling	1. Simple to use 2. Only individual component failure data necessary	1. Lognormal not always valid 2. Considerable uncertainty 3. Low failure probability for systems with high redundancy.

2.4 Probabilistic Modelling of CCF

If a system is composed such that the occurrence of either of two events A or B will cause a failure (often called a series system) then

$$P_f = P(A) + P(B) - P(AB) \qquad (2.4.1)$$

where P_f represents failure probability of the system.

On the other hand, if a system is constructed such that the occurrence of both events A and B is necessary to cause the system failure (often called a parallel system) then

$$P_f = P(AB) \qquad (2.4.2)$$

In most engineering systems, $P(A)P(B) < P(AB) < P(A)$, where A and B are assumed to be equally likely events. If statistical independence is assumed, i.e., $P(AB) = P(A)P(B)$, it is easily seen that in the series case we overestimate the system failure probability, while in the parallel system we underestimate it. In order to have a rational basis of taking into consideration the degree of dependence, the probabilistic definition of independence will be pursued next

2.4.1 Mathematical Definition Of Statistical Independence

In general,the following expression

$$P(AB) = P(A)P(B|A) = P(B)P(A|B) \qquad (2.4.3)$$

is valid. The events A and B are defined as statistically independent if

$$P(B|A) = P(B),$$
$$P(A|B) = P(A),$$
$$P(AB) = P(A)P(B). \qquad (2.4.4)$$

In many applications of engineering analyses the assumption of statistical independence is often made. But how does one decide when two events are statistically independent? Eq. (2.4.4) thus serves as a criterion to make such judgment.

2.4.2 Mathematical Definition Of Physical Independence

Suppose that events A and B are always accompanied by some other events $E_i (i=1,2,...N)$ which we call an environmental profile. Let these subsets E_i be exhaustive, mutually exclusive, and distinct. Subsets are mutually exclusive if the occurrence of any one precludes the occurrence of all the others. Subsets are exhaustive if it is known that at least one of them must occur. The subsets E_i are distinct if there is no E_j and E_k such that the following is true:

$$P(A|E_j) = P(A|E_k),$$
or $$P(B|E_j) = P(B|E_k),$$
$$P(AB|E_j) = P(AB|E_k), \qquad (2.4.5)$$

Then we can define A and B to be physically independent under E_i if and only if they are statistically independent under E_i,

$$P(AB|E_i) = P(A|E_i)P(B|E_i) \qquad (2.4.6)$$

It is emphasized that physical independence differs from statistical independence in that the former has the environmental profile specified.

Consider two system components a and b. Let A represent the failure of component a, B the failure of component b. Suppose they are physically independent for all E_i with N > 1. The proper formula to combine failure probability to calculate P(AB) is

$$P(AB) = \sum_i P(A|E_i)P(B|E_i)P(E_i) \qquad (2.4.7)$$

It is shown {2.18} that for events with low failure probabilities, it is impossible to have statistical independence. The failure of a and b are physically independent (i.e. the failure of one in no way causes the failure of the other), but they are not statistically independent. The 'dependence' is caused by the severe environmental profiles of low probability.

Easterling {2.21} discusses a more general framework in which he considers conditions under which the components have to operate. In this fashion he shows that CCF comes about naturally.

Let C_{A1}, C_{A2}, ... denote the conditions under which component A may be asked to operate and let C_{B1}, C_{B2}, ... be similarly defined for component B. The term 'condition' is used broadly to include such things as designer, manufacturer, and environmemt. There may be a spectrum of conditions and identifying them may be a difficult task. For an engineering component such as a pump or a valve, this relies largely on engineering knowledge and lessons learned from failures. The constraint placed on each of the conditions is that they be mutually exclusive and exhaustive.

Let $P(C_{Ai}\ C_{Bj})$ denote the joint probability of conditions C_{Ai} and C_{Bj} occuring. Then the unconditional probability of A and B failing is given by

$$P(AB) = \sum_{i,j} P(AB|C_{Ai}\ C_{Bj})\ P(C_{Ai}\ C_{Bj}) \qquad (2.4.8)$$

Consider now the unconditional probability of A failing. With similar notation, this is given by

$$P(A) = \sum_{i} P(A|C_{Ai})\ P(C_{Ai}) \qquad (2.4.9)$$

assuming

$$P(A|C_{Ai}\ C_{Bj}) = P(A|C_{Ai}) \qquad (2.4.10)$$

Similarly, the unconditional probability of B failing is given by

$$P(B) = \sum_j P(B|C_{Bj}) \, P(C_{Bj}) \qquad (2.4.11)$$

assuming

$$P(B|C_{Ai} \, C_{Bj}) = P(B|C_{Bj}) \qquad (2.4.12)$$

The dependent failure of concern in common PRA studies is represented by

$$P(AB) > P(A) \, P(B) \qquad (2.4.13)$$

It is obvious that the common assumption of P(AB) = P(A) P(B) is optimistic for redundant system as described earlier.

To pursue further the conditions when Eq. (2.4.13) holds, consider the following two properties D1 and D2:

D1. Failure of A and B are conditionally statistically independent events. In other words, for all i and j,

$$P(AB|C_{Ai} \, C_{Bj}) = P(A|C_{Ai}) \, P(B|C_{Bj}). \qquad (2.4.14)$$

D2. The occurrence of C_{Ai} and C_{Bj} are statistically independent events, meaning

$$P(C_{Ai} C_{Bj}) = P(C_{Ai}) P(C_{Bj}), \text{ for all i and j.} \quad (2.4.15)$$

If D1 and D2 hold, it can be shown that

$$P(AB) = P(A) P(B) \quad (2.4.16)$$

Suppose D1 does not hold. Then this is the situation where failure events are dependent and one does not obtain Eq. (2.4.16). An example is the failure of A increases the failure probability of B, which is exactly what we call cascade failure earlier.

Suppose D2 does not hold. Then, for at least one (i,j)

$$P(C_{Bj} | C_{Ai}) \neq P(C_{Bj}) \quad (2.4.17)$$

It can be shown that again Eq. (2.4.16) does not hold. This is the so-called coupled failure described earlier.

A particular case of interest is where A and B are subject only to common causes. In terms of the probabilistic definition, conditions C_{Ai} and C_{Bj} are identical and

$$\begin{aligned} P(C_{Bj} | C_{Ai}) &= 0 \quad \text{if } i \neq j \\ P(C_{Bj} | C_{Ai}) &= 1 \quad \text{if } i = j \end{aligned} \quad (2.4.18)$$

For redundant components, such an assumption might apply if they are situated so that they are subject to the same environmemt.

Suppose further that A and B are identical and physically independent. In other words, they are conditionally statistically independent

$$P(AB|C_i) = P(A|C_i)\, P(B|C_i) \tag{2.4.19}$$

where C_i refers to the common conditions A and B are subjected to. Then

$$\begin{aligned} P(AB) &= \sum_{i,j} P(AB|C_{Ai}C_{Bj})\, P(C_{Ai}C_{Bj}) \\ &= \sum_{i,j} P(AB|C_{Ai}C_{Bj})\, P(C_{Bj}|C_{Ai})\, P(C_{Ai}) \\ &= \sum_{i} P(A|C_{Ai}C_{Bj})\, P(B|C_{Ai}C_{Bj})\, P(C_{Ai}) \\ &= \sum_{i} P(A|C_{Ai})\, P(A|C_{Ai})\, P(C_{Ai}) \end{aligned} \tag{2.4.20}$$

In most applications, we have only partial association between components, i.e. not all the conditions are identical for A and B. Suppose we have n common causes and m independent causes. Then

$$P(AB) = \sum_{i=1}^{n} P(A|C_{Ai})^2\, P(C_{Ai}) + \sum_{j=1}^{m} [P(A|C_{Aj})\, P(C_{Aj})]^2 \tag{2.4.21}$$

The derivation given above can be readily extended to k-component systems. If k components are identical, we have

$$P(A_1 A_2 \ldots A_k) = \sum_{i=1}^{n} P(A_1|C_{Ai})^k P(C_{Ai}) + \sum_{j=1}^{m} [P(A_1|C_{Aj})P(C_{Aj})]^k \tag{2.4.22}$$

where A_i i=1,2,...k, represents identical components. If the k components are not identical, we have

$$P(A_1A_2\ldots A_k) = \sum_{i}^{n}\prod_{1}^{k} P(A_1|C_{Ai})P(C_{Ai}) + \sum_{j1}^{mk}\prod P(A_1|C_{Aj})P(C_{Aj}) \quad (2.4.23)$$

where

$$\prod_{1}^{k} P(A_1|C_{Ai}) = P(A_1|C_{Ai})P(A_2|C_{Ai})\ldots P(A_k|C_{Ai})$$

It is also worth noting that in most applications, the probability of conditions such as $P(C_{Ai})$ may be a random variable. Then, $P(C_{Ai})$ is itself a probability distribution.

The above formulation provides a very general framework for calculating the multiple failure probability and serves as a basis for later applications.

Chapter 3

Existing Methods for Multiple-Train Systems

3.1 Introduction

In the U.S. single failure criterion has served as one of the design guidelines for safety systems in nuclear power plants. Redundant subsystems have often been used to assure the fulfillment of single failure requirement. This is deemed necessary for another reason. The extremely small failure probability required to maintain both the incidence of accidents and the unavailability of safety systems at an acceptably low level may not be realistically achieved if a single component or subsystem failure can cause a failure of the total system. In addition to satisfying the single failure criterion, redudancy may increase the reliability by allowing testing and repair of redundant components while the reactor is on-line.

In most European plants, a N-2 criterion is introduced. The additional redundancy is to assure that during the test even if a component fails the system can still function as intended. For the N-2 criterion, redundancy higher than 2 is inevitable. It is then important to recognize that common causes may not lead to failure of all redundant components within the period of interest. It is of interest to quantify the probability associated with different multiplicity of failures.

The presentation of the rest of this chapter is as follows. Section 3.2 describes an approach to distinguish

between multiple failures. This is the multiple dependent failure fraction (MDFF) method. First, 1-out-of-3 system is reviewed. Then an extension of the derivation to 1-out- of-4 system is described. Section 3.3 presents a similar approach to analyze multiple-train system. This is the so- called multiple greek letter method (MGLM). Section 3.4 compares three different methods of dealing with CCFs. These are beta factor method, MDFF method and MGLM. It is shown that MDFF method and MGLM give identical results. In addition, the relationship between them is presented.

3.2 The MDFF Method

In most CCFA models of redundant systems, no distinction is made between different levels of failure due to a common cause. Little effort has been made to obtain estimates for the probability of failing three, four, or more identical trains. Instead, the failure contribution due to different levels of component multiplicity is aggregated into a single value (the beta factor). Reasons for this include:

1. previous studies have focused mostly on two-unit redundant systems.
2. little experience data is available on CCFs so that consideration of different levels of system is not easily done.

However, to treat the partial failures, one needs to factor in appropriate parameter describing them into the Markovian analysis of the redundant system.

It can be shown that for a 1-out-of-n system excluding repair that:

$$\frac{dP_i(t)}{dt} = -Z_i P_i(t) + \sum_{\substack{j=0 \\ j<0}}^{n} Z_{ji} P_j(t) \qquad (3.2.1)$$

where $P_i(t)$ is the probability at time t, the system has exactly i failed components (i = 1,2,...N); Z_{ji} is transition rate from initial state j to final state i assuming no repair (i.e. j < i); and Z_i is transition rate from state i to any other possible states.

3.2.1 1-out-of-3 system

The set of uncoupled differential equations that result from making use of Eq. (3.2.1) with i=1, 2, and 3 is: {3.1}

$$\frac{dP_0}{dt} = -Z_0 P_0(t) \qquad (3.2.2)$$

$$\frac{dP_1}{dt} = -Z_1 P_1(t) + Z_{01} P_0(t) \qquad (3.2.3)$$

$$\frac{dP_2}{dt} = -Z_2 P_2(t) + Z_{02} P_0(t) + Z_{12} P_1(t) \qquad (3.2.4)$$

$$\frac{dP_3}{dt} = Z_{03} P_0(t) + Z_{13} P_1(t) + Z_2 P_2(t) \qquad (3.2.5)$$

where

$$Z_0 = Z_{01} + Z_{02} + Z_{03} \qquad (3.2.6)$$

$$Z_1 = Z_{12} + Z_{13} \qquad (3.2.7)$$

These equations can be solved to obtain the following expression for the system unavailability, Q:

$$Q = 1-e^{-Z_o t}(1 + A_1 + A_2) + e^{-Z_1 t}(A_1+A_3) + e^{-Z_2 t}(A_2-A_3) \quad (3.2.8)$$

where

$$A_1 = Z_{01}/(Z_1-Z_o), \quad (3.2.9)$$

$$A_2 = (Z_{02} + Z_{12}A_1)/Z_2-Z_o), \quad (3.2.10)$$

$$A_3 = (Z_{12}A_1/Z_2-Z_1). \quad (3.2.11)$$

Following the treatment of the beta factor method described earlier, we can define the system failure rate as λ consisting of a random failure component, λ_r, and a common cause component λ_c. Then we can extend this definition for the term λ_c making use of failure fractions f_n such that:

$$\lambda = \lambda_r + \lambda_c \equiv \lambda_r + \lambda \sum_{n=2}^{N} f_n = \lambda_r + f\lambda \quad (3.2.12)$$

where f_n is fraction of n-tuple failures (n= 2,...N) and f is fraction of common cause failures (analogous to the beta factor defined before). If we assume the following:

$$Z_{01} = 3(1-f)\lambda = 3(1-\beta)\lambda;\ Z_{02} = 0;\ Z_{03} = f_3\lambda = \beta\lambda$$
$$Z_{12} = 2(1-f)\lambda = 2(1-\beta)\lambda;\ Z_{13} = f_2\lambda = \beta\lambda;\ Z_{23} = \lambda \quad (3.2.13)$$

then the unavailability expression reduces to that for the beta factor method. Thus it is obvious that beta factor method is a special case of the MDFF method.

3.2.2 1-out-of-4 system

Similarly, for a 1-out-of-4 system, the Markov model yields the following set of differential equations:

$$\frac{dP_0}{dt} = -Z_0 P_0(t) \tag{3.2.14}$$

$$\frac{dP_1}{dt} = -Z_1 P_1(t) + Z_{01} P_0(t) \tag{3.2.15}$$

$$\frac{dP_2}{dt} = -Z_2 P_2(t) + Z_{12} P_1(t) + Z_{02} P_0(t) \tag{3.2.16}$$

$$\frac{dP_3}{dt} = -Z_{34} P_3(t) + Z_{13} P_1(t) + Z_{23} P_2(t) + Z_{03} P_0(t) \tag{3.2.17}$$

$$\frac{dP_4}{dt} = Z_{04} P_0(t) + Z_{14} P_1(t) + Z_{24} P_2(t) + Z_{34} P_3(t) \tag{3.2.18}$$

where the transition rates Z_{ij} must satisfy the relations:

$$Z_0 = Z_{01} + Z_{02} + Z_{03} + Z_{04}$$

$$Z_1 = Z_{12} + Z_{13} + Z_{14}$$

$$Z_2 = Z_{23} + Z_{24}$$

$$Z_3 = Z_{34} \tag{3.2.19}$$

Solving the above set of equations renders the following unavailability expression:

$$Q = 1 - e^{-Z_0 t}(1 + A_1 + A_2 + A_4) + e^{-Z_1 t}(A_1 + A_3 + A_5)$$
$$+ e^{-Z_2 t}(A_2 - A_3 - A_6) - e^{-Z_3 t}(A_5 - A_4 - A_6)$$

(3.2.20)

where

$$A_1 \equiv (Z_{01}/(Z_1 - Z_0),$$

$$A_2 = (Z_2 - Z_0)^{-1}(Z_{02} + Z_{12}A_1)$$

$$A_3 = (Z_{12}A_1)/(Z_2 - Z_1)$$

$$A_4 = (Z_3 - Z_0)^{-1}(Z_{03} + Z_{13}A_1 + Z_{23}A_2)$$
$$A_5 = (Z_3 - Z_1)^{-1}(Z_{23}A_3 + Z_{13}A_1)$$
$$A_6 = (Z_3 - Z_2)^{-1}Z_{23}(A_3 - A_2) \qquad (3.2.21)$$

As in the case of the 1-out-of-3 system, it can be shown that the transition rates Z_{ij} for the beta factor method reduce to the following:

$$Z_{01} = 4(1 - \beta)\lambda; \quad Z_{02} = 0; \quad Z_{03} = 0; \quad Z_{04} = \beta\lambda$$

$$Z_0 = (4 - 3\beta)\lambda; \quad Z_{12} = 3(1 - \beta)\lambda; \quad Z_{13} = 0; \quad Z_{14} = \beta\lambda$$

$$Z_1 = (3 - 2\beta)\lambda;$$

$$Z_{23} = 2(1 - \beta)\lambda;\ Z_{24} = \beta\lambda;\ Z_2 = (2 - \beta)\lambda;\ Z_3 = \lambda \qquad (3.2.22)$$

Then, it can be shown that the system unavailability Q is given as:

$$Q = 1 - 4e^{-\lambda t} + 6e^{-(2-\beta)\lambda t} - 4e^{-(3-2\beta)\lambda t} + e^{-(4-3\beta)\lambda t} \qquad (3.2.23)$$

3.3 The Multiple Greek Letter Method

The idea behind the multiple Greek letter method (MGLM) {3.2} is essentially similar to that of the MDFF method. This approach provides a systematic way of quantifying failure probabilities of different system multiplicity by introducing conditional probabilities. In addition, the method is structured such that the work involved in the original beta factor method does not have to be redone.

3.3.1 Three-Unit System

The following definitions are used :

β = conditional probability of a CCF affecting at least two units given failure of each unit.

γ = conditional probability of a three-unit CCF given that a CCF involves at least two units.

For a 1-out-of-3 system,

Q_3 = likelihood of failure on demand for all the units due to a common cause.

Q = total failure on demand probability for each unit

It is then easily derived that

$$Q_3 = \gamma\beta Q$$

3.3.2 Four-Unit System

Similarly, the following definitions are made in the so-called MGLM:

β = conditional probability of a CCF affecting at least two units given failure of each unit.

γ = conditional probability of three or more failures given a CCF involves at least two units.

δ = conditional probability of four-unit failures given a CCF involves at least three units.

Q = total failure probability

Q_4 = probability of failure on demand for all four units due to a common cause.

It is then easily derived that

$$Q_4 = \delta\gamma\beta\, Q$$

It is noted that in the derivation, failure probability on demand is used. It is also possible to use the failure rate per hour, multiplied by the period of time of interest, in the formulation.

The above definition of a set of Greek letters has been illustrated for various configurations involving different cut sets. Table 3.1 summarizes expressions derived for the application. For more detail, Ref. 3.2 may be consulted.

3.4 Comparison of the Beta Factor, MDFF and MGLM Methods

In this section the commonly used beta factor is compared with MDFF first. Then the relationship between MDFF and MGLM is established to show that they are essentially the same. The question of how to estimate the parameters in

Table 3.1 Summary of Results Based on MGLM (Ref. 3.2)

Model	Redundancy Level	Success Criteria	Approximate* Formula for System Unavailability (second order in Q and β)
I	3 x 50%	2/3	$Q_S = 3Q^2 + \frac{3}{2}(1-\gamma)\beta Q + \gamma\beta Q$
II	3 x 100%	1/3	$Q_S = \gamma\beta Q$
III	4 x 33%	3/4	$Q_S = 6Q^2 + \beta Q\left[2 - \frac{\gamma}{3}(2+\delta)\right]$
IV	4 x 50%	2/4	$Q_S = \frac{\beta Q\gamma}{3}(4-\delta)$
V	4 x 100%	1/4	$Q_S = \delta\gamma\beta Q$

*Should only be used when $Q \leq 10^{-1}$ and $\beta \leq 10^{-1}$.

these multiple-train models are then addressed to motivate the approach used in the thesis.

3.4.1 Beta Factor vs MDFF Methods {3.3}

For a 1-out-of-n system, the failure probability for the beta factor, Q_{BF}, and for the MDFF method, Q_{MDFFM}, are given by (to first order approximation):

$$Q_{BF} = \beta\lambda t \tag{3-4.1}$$

$$Q_{MDFFM} = f_n\lambda t \tag{3-4.2}$$

Since $\beta > f_n$, the beta factor method yields higher system unreliability estimates than does the MDFF method. For a second order approximation,

$$Q_{BF} = \beta\lambda t + n(1-\beta)\lambda t\beta\lambda t \tag{3-4.3}$$

$$Q_{MDFFM} = f_n\lambda t + nf_{n-1}(\lambda t)^2 + \sum_{k=1}^{n-2} \binom{n}{k} f_k\lambda t\, f_{n-k}\lambda t \tag{3-4.4}$$

It can be shown {3.3} that if

$$\lambda t < \frac{\sum_{k=1}^{n-2}}{(n-1)\left[\beta^2 \sum_{k=1}^{n-2} \binom{n}{k} + n\beta - (1-\beta)\beta\right]} \tag{3-4.5}$$

the MDFF method yields lower estimates than does the beta factor method. For typical situations, Eq. (3-4.5) is valid. Thus we have shown that Beta factor method yields higher failure probability than the MDFF method.

3.4.2 MDFF vs MGLM

As described in 3.2, the MDFF approach is based on defining the multiple failure rate as a fraction of the single component failure rate. The MGLM, on the other hand, defines the multiple failure probability conditioned on the aggregate of various multiplicity of failure probabilities. Table 3.2 provides a set of expression relating different parameters in the two formulations of CCFA.

3.4.3 Estimating Parameters in the MDFF and MGLM Methods

It is an important task now to develop estimates of the parameters f_k in the MDFF and Greek letters β, γ and δ in the MGLM. The conventional approach based on historical data proves frustrating based on the following observations:

1. Scarcity of Data

   Since most of the systems and components of interest in the PRA studies are highly reliable, failure occurrences are rare. It is even more so for multiple failure occurrences.

2. Inadequacy of Assumptions Underlying the Method

   In the conventional statistical approach, many assumptions are made mainly for the mathematical conveniences. For example, in the BFR model, the common cause is assumed to have equal impact on identical components. Although this justifies the binomial distribution, it by no means represents realities.

Table 3.2 Relationship Between MDFF and MGLM

MDFF

$f_k \equiv$ fraction of time failure is due to k component failure, k=2,3,4

$$f_k = \frac{p_f^k}{p_f}$$

p_f = single component failure probability

MGLM

four-unit system

$$\beta = \frac{3p_f^2 + 3p_f^3 + p_f^4}{p_f + 3p_f^2 + 3p_f^3 + p_f^4} = \frac{3f_2 + 3f_3 + f_4}{1 + 3f_2 + 3f_3 + f_4}$$

$$\gamma = \frac{3p_f^3 + p_f^4}{3p_f^2 + 3p_f^3 + p_f^4} = \frac{3f_3 + f_4}{3f_2 + 3f_3 + f_4}$$

$$\delta = \frac{p_f^3}{3p_f^3 + p_f^4} = \frac{f_4}{3f_3 + f_4}$$

three-unit system

$$\beta = \frac{p_f^2 + p_f^3}{p_f} = f_2 + f_3$$

$$\gamma = \frac{p_f^3}{p_f^2 + p_f^3} = \frac{f_3}{f_2 + f_3}$$

3. Relevance of Data Collected.

Since reliability data collected are usually difficult to interpret, the analyst may fall into the trap of misconceiving the data such that it bears no resemblance to the true state of affairs. Engineering judgement which is not explicit or scrutable can hide the irrevelance of the data used in analysis.

For these reasons, it is desirable to have a method which addresses the above concerns and provide a rational basis for quantification of the parameters in the CCF models described in this chapter.

The approach used in this study is based on stress-strength interference theory and the common load model. A special variation of this technique is developed, called the inverse stress-strength interference (ISSI) approach, furnishing a framework to take engineering considerations into account and alleviate the difficulties of using historical data alone for estimation purposes. Chapter 4 discusses the fundamentals of SSI theory and the common load model to set the stage for the introduction of the ISSI technique, discussed further in Chapter 5.

Chapter 4

Stress-Strength Interference Theory and the Common Load Model

4.1 Introduction

To determine the reliability of electronic and electrical components {4.1} the concept of the failure rate is used. The failure rate is defined as the number of failures which occur per unit time at a specific age of the component, and frequently it is expressed in terms of failures per million hours of operation. The relationship between this failure rate and the age of a component is shown in Fig. 4.1 (the so-called bath-tub curve). For electronic components in particular, there is a relatively long period during which the failure rate is the lowest and constant in magnitude. This is called the useful life period. During this period the component's reliability R(T), for an operating period T, is evaluated from

$$R(T) = \exp(- \lambda T) \qquad (4\text{-}1.1)$$

where

λ = constant,useful life period failure rate in failures per hour

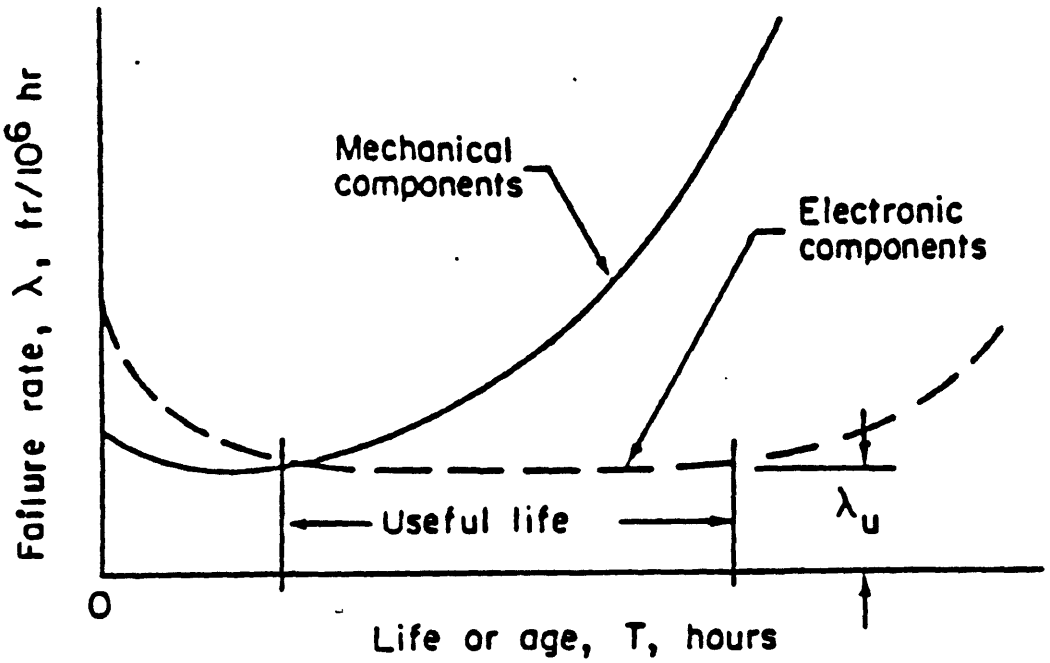


Figure 4.1 Reliability Bath-tub Curves for Electrical and Mechnical Components (Ref. 4.1)

T = operating period or mission time in hours

For mechanical components and structural members subjected to quasistatic, dynamic, fatigue, wear and corrosion environments, there is usually no such long constant failure period as also indicated in Fig. 4.1. Consequently, Eq. (4-1.1) should be used discriminately to evaluate the reliaility of such components.

In general, there are three approaches to determine the reliability of mechanical components such as pumps and valves. One approach is to establish a representative failure rate. This could be the average failure rate ,$\bar{\lambda}$, for the desired function period, obtained from

$$\bar{\lambda} = \frac{1}{T_2-T_1}\int_{T_1}^{T_2} \lambda(T)\,dT \qquad (4\text{-}1.2)$$

where

$\bar{\lambda}$ = average failure rate in life period T_1 to T_2

$\lambda(T)$ = time dependent failure rate in life period T_1 to T_2

T_1 = age of the component at the beginning of the period

T_2 = component age at the end of the period

These quantities are identified in Fig. 4.2.

The component reliability can then be calculated from

$$R(T_1 \rightarrow T_2) = \text{EXP}\ (\ -\bar{\lambda}(T_2-T_1)\ ) \qquad (4\text{-}1.3)$$

The values of $\bar{\lambda}$ may be obtained from several sources {4.2,4.3,4.4}. Ref.{4.4} reviewed 30 different data banks

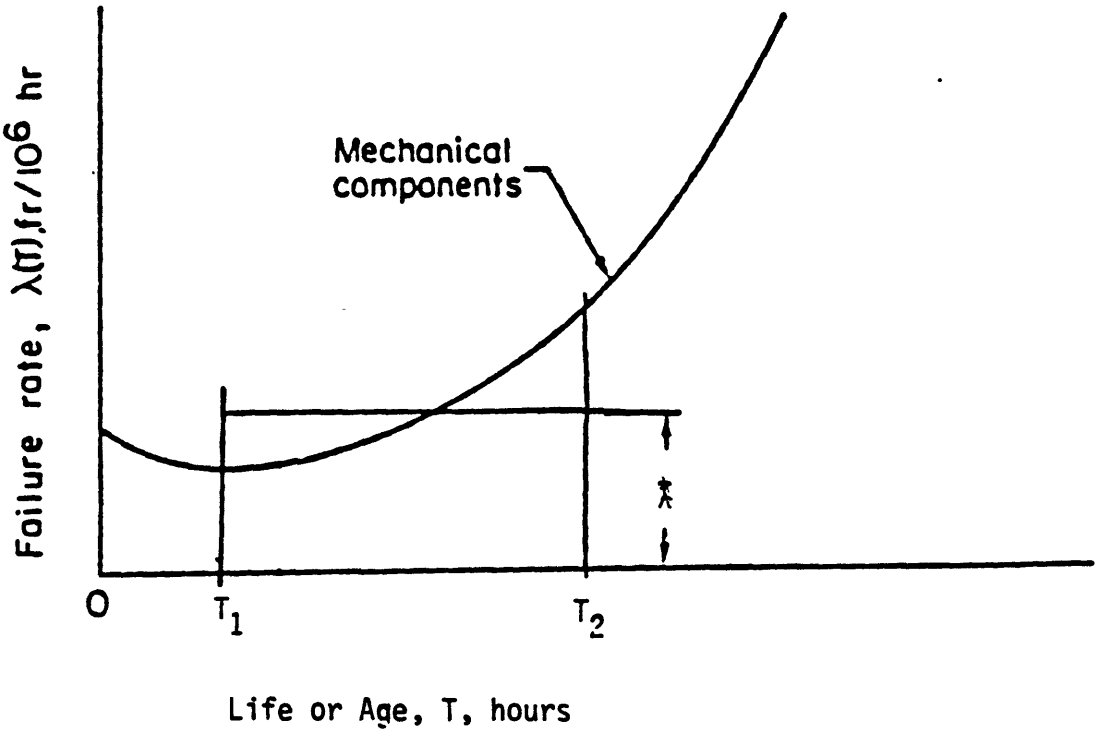


Figure 4.2 Average Failure Rate for Mechanical Components. (Ref. 4.1)

to provide upper and lower bounds as well as an assessment median for most of mechanical and eletrical components used in nuclear power plants. However, such estimates are based on a wide range of conditions under which the components are designed, manufactured, and operated. Deviations from these conditions, as would be most often the case, would invalidate such estimates if not corrected for or would not give any indication as to where within the wide range the failure rate of a specific application would lie. Furthermore, the ratio of the maximum to the minimum predicted component failure rate is usually in excess of 5 to 1. An engineer would like to to know his system reliability more precisely than this so that he can optimize the system design. This leads to the need of the second approach. The goal is to design a specified reliability into a component, the so-called probabilistic design approach.{4.5,4.6} Other names have been used including stress-strength overlap, mechanical reliability, stress-strength interference theory (SSI), the probabilistic design for reliability, and the design-by-reliability approach. Section 4.3 describes this in more detail.

The third approach is based on life-testing procedures assuming general three-parameter Weibull time-to-failure distribution. Three parameters are then used to evaluate the component reliability as follows.

$$R(T_1 \rightarrow T_2) = \exp\left\{ -\left[\left(\frac{T_2-\gamma}{\eta}\right)^{\beta} - \left(\frac{T_1-\gamma}{\eta}\right)^{\beta}\right] \right\} \quad (4\text{-}1.4)$$

where

γ = location parameter of the Weibull time-to-failure distribution

η = scale parameter of the Weibull time-to-failure distribution

β = shape parameter of the Weibull time-to-failure distribution

More research still needs to be conducted to compile a handbook of such Weibull distribution parameters for commonly used mechanical components and structural members. Then Eq. (4-1.4) can be used to compute reliability.

Section 4.2 presents a general discussion on the nature of " stress " and " strength ". The interpretation of " stress " and " strength " used in different disciplines is briefly described.

Section 4.3 discusses the stress-strength interference theory and derives useful expressions for the probability of failure based on some commonly used engineering distributions.

Section 4.4 describes the common load model as an extension of the SSI and derives useful expressions of multiple component failure probability in terms of stress and strength distribution parameters. This can then be used to evaluate the parameters in multiple failure models discussed in Chapter 3.

4.2 Definition of Stress and Strength

Before we embark on a definition of stress and strength, it is useful to understand some concepts that arise in the modelling of random phenomena. The most general description of any uncertain physical quantity is in terms of random fields, a collection of indexed random variables x(t). In n-dimensional space, vector $\underline{t} = (t_1, t_2, \ldots, t_n)$ has elements t_1, t_2, $\ldots t_n$, each representing either the coordinates or parameters.{4.7} In the special case where t is the time, a stochastic process (or random process) x(t) is defined.

The notion of a stochastic process x(t) provides a generalizing concept for the modelling of stress and strength. However, it usually requires considerable observations to completely characterize a stochastic process. Analysis is simplified and data requirement reduced if a stochastic process is stationary. A stationary process is a special stochastic process whose across-the-ensemble probability distributions are invariant during a shift in time axis. This property implies that for a given process, the probability density is universally independent of time. For example, the distribution of static ultimate strength is essentially independent of time. As a consequence, all statistical parameters based on the probability distribution underlying such a process (e.g. the mean and variance) are independent of time. Under the assumption of stationarity,

therefore, it is reasonable to describe a process in terms of a random variable.

In physical situations, it is often more convenient to characterize a process based on a sample function (i.e. a single observation of one realization of the process). This requires the following properties to hold:

(1) the process is a stationary process

(2) the ensemble statistics and the statistics of all sample functions are identical in the limit of very large observations.

As an example, consider a geometric feature, say the dimension, of a typical mechanical product. Production processes that employ cutting tools (e.g. as in drilling, milling, turning) are subject to change over time. The same is true of rolling and forging processes. Any dimension such as distance between hole centers, distance between parallel faces, thickness, and length modified by tool wear results in a geometric random process that is nonstaionary. If corrections for tool wear are made periodically, the dimensional values retain the properties of random variables, but the time trend is minimized and it is possible to consider the random process as approximately ergodic.

Fig. 4.3 illustrates the stochastic behavior of a typical stress and strength, with the resulting time-dependent reliability.{4.8} At each particular instant of time, however, stress and strength can be regarded as a

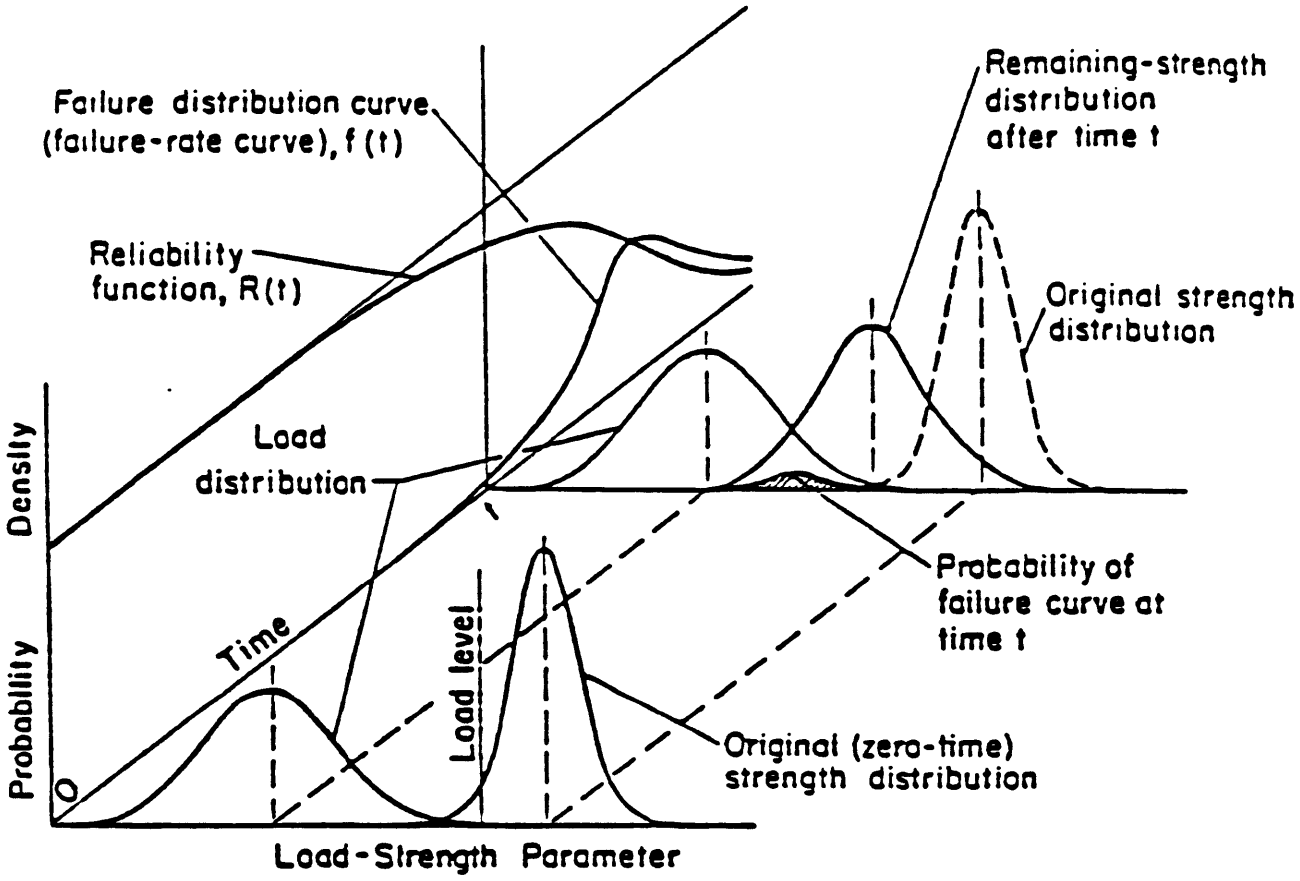


Figure 4.3 Time-Dependent Load and Strength Distributions {6.8}

random variable. It is noted that, under usual circumstances, the strength distribution becomes broader as time evolves. In addition, the reliability decreases due to a reduction of mean strength as evidenced in the figure.

The concept of random process is useful in developing the strength behavioral model of a specific material produced by a number of different companies.{4.9} It is well known that the statistical characteristics of a material produced to the same specification will vary from company to company. Therefore, if the sample of test results from each company is treated as a discrete sample function S(x), the samples from a number of sources will make up a finite ensemble of finite length records. The sample distributions will vary randomly, but the ensemble distributions at any two x values will approach identity as the ensemble length increases, that is, reflect a discrete stationary process.

It may be postulated that the strength is very likely ergodic. Since for an ergodic process, a single sample record is sufficient to define the process, the use of the distributional statistics determined from a single sample of strength of data is justified. There are, however, several significant exceptions to the adequacy of stationarity or ergodicity of stress or strength. For example, fatigue strength, is a continuous nonstationary random process. In such situations, to model fatigue strength as a random variable would necessiate picking up distribution at such a time that conservatism is included. For example, fatigue

strength at the very end of useful life may have to be used for design considerations.

Table 4.1 summarizes the different possible levels of modelling for stress and strength. In general, the more sophiscated a model is, the higher the accuracy of the result will be. On the other hand data requirement limits possible models for practical use. Therefore, a tradeoff between accuracy and practicality has to be made in most engineering situations.

The full meaning of the concept of stress and strength requires some elaboration. In most failure processes there is some 'parameter' with a limiting value that defines failure. The parameter may be a performance measure such as an efficiency, describing a particular device with a limiting value beyond which losses or temperature becomes excessive. As an example, consider an elastomeric seal, such as an "O" ring or chevron seal. A pertinent 'strength' would be defined as the ability to withstand pressure differentials across the seal with a certain probability of dimensional variations in view of a probability of initial compression. A corresponding stress would be the existing pressure differentials across the seal. The failure would occur whenever a preset leakage limit is exceeded. Resiliency loss and/or permanent seal deformation would be possible degration of strength factors.

In this study, because of limitation of information, the stress and strength will be modelled as a random variable.

Table 4.1 Levels of Stress and Strength Modeling

Models	Data Requirement and Sophistication	Assumptions and Ease
Stochastic	High	Low
Ergodic	↓	↓
Stationary	↓	↓
Random Variable	↓	↓
Second Moment Characterization	↓	↓
Deterministic	Low	High

Although this seems to be a strict assumption, it is the only approach that strikes a balance between oversimplification and overcomplication.

It is also useful to note that the stress and strength concept used in the context of this report is not as restricted as the name might appear. There are similar applications of the idea in other areas of engineering. For example, in the area of structural reliability, load and resistance are the counterparts of stress and strength in mechanical reliability.{4.10.4.11,4.12,4.13,4.14} In general, even at a system level, performance requirement represents a generalized stress, while performance achievement can be thought of as a generalized strength. In seismic risk analysis, seismicity and fragility correspond to the stress and strength concepts. Here, however, instead of a probability density function, seismicity is the complementary cumulative distribution function of stress, while fragility is the cumulative distribution function of strength.

In the most general case, one can consider stress as any failure-inducing demand on a component, while strength as any corresponding failure-resisting capacity of the component. Table 4.2 summarizes the stress and strength concepts used in different disciplines. With this perspective on the concepts of stress and strength, we are now in a position to discuss stress-strength interference theory.

Table 4.2 Comparison of Stress and Strength Concepts in Various Applications

Stress	Strength (Mechanical)
Load	Resistance (Civil)
Performance Requirement	Performance Achievement (Reliability)
Failure-Inducing Demand	Failure-Resisting Strength
Generalized Stress	Generalized Strength
Seismicity	Fragility

4.3 Stress-Strength Interference Theory

In its most elementary form a stress-strength mode of relationship arises as a natural model for describing the ability of a rope having a random breaking strength to withstand a load of an uncertain magnitude. More generally, a stress-strength model of reliability applies to the situation where a piece of equipment or component accomplishes its intended function provided it is strong enough to overcome the opposing forces of the operating environment which interfere with its performance. The operating strength is essentially determined by such factors of the manufaturing process as the quality of imputed materials, the mechanics of the process and the precision of assembly of parts, etc. The intrinsic variability in these factors makes it necessary to model the strength of the equipment in terms of a random variable rather than a deterministic constant. By the same token, the interfering force or stress in the operating environment may also vary in intensity on different occasions so that it should be described using probability distribution.

A promising technique for predicting mechanical reliability prior to the availability of the field data is the concept of interfering stress-strength probability density distribution {4.15}. Stress-Strength interference (SSI) theory is concerned with the problem of determining the probability of a part which is subjected to a stress S and which has a strength R.

It is assumed that both S and R are random variables with known probability density functions $f_S(x)$ and $f_R(x)$ respectively. One says failure occurs whenever stress exceeds strength. Hence the probability that failure occurs is equivalent to the probability that stress exceeds strength. In symbols,

$$\Pr(\text{ failure }) = \Pr(S > R) \qquad (4\text{-}3.1)$$

To determine the probability of failure one needs to explore the probability that the stress exceeds the strength. Suppose that the stress and the strength are independent of each other. One can fix attention on some particular value of the stress (S) and determine the probability that the strength (R) does not exceed this fixed value , say x, a particular stress level. The probability that R does not exceed x is written as

$$\Pr(R < x) \qquad (4\text{-}3.2)$$

In terms of probability density function this is equivalent to

$$F_R(x) = \int_{-\infty}^{x} dy\, f_R(y) \qquad (4\text{-}3.3)$$

where the "$-\infty$" is symbolic only, representing the actual lower limit for physical stress; and the F_R and f_R represent corresponding cumulative distribution function and probability density function respectively. The probability that R<S is given by

$$Pr(\ R<S\ ) = \int_{-\infty}^{\infty} f_S(x)\, dx\, F_R(x) \qquad (4\text{-}3.4)$$

An equivalent representation by the same kind of procedure gives

$$Pr(\ R<S\ ) = \int_{-\infty}^{\infty} f_R(x)[1-F_S(x)]dx \qquad (4\text{-}3.5)$$

where $F_R(x)$ is the cumulative distribution function of the random variable S, i.e. stress.

As described in section 4.2, the 'stress-strength' have other connotations in other engineering areas. However, Eqs. (4-3.4) or (4-3.5) provides a point of departure for the reliability investigations in all these areas. It is mainly in the interpretation and assumption of underlying stress and strenth distributions that various disciplines differs.

It is useful to consider some common distributions as engineering approximations of stress and strength and derive expressions for the probability of failure.

4.3.1 Normal Model

It is well known that if stress(S) and strength(R) are normally distributed random variables, with mean values μ_S and μ_R and variances σ_S^2 and σ_R^2, then the random variable defined by $Z = R - S$ is also normally distributed. The mean of Z is $\mu_R - \mu_S$, and the variance of Z is $\sigma_R^2 + \sigma_S^2$. Consequently, the probability of failure, P, will be given by the area under the normal probability curve whose mean and variance are μ_Z and σ_Z respectively.{4.15}

$$P = Pr(R < S) = \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi}\,\sigma_Z} e^{-\frac{1}{2}\left(\frac{x-\mu_Z}{\sigma_Z}\right)^2}$$

$$= \int_{-\infty}^{-\frac{\mu_Z}{\sigma_Z}} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2} dx$$

$$= \Phi\left(-\frac{\mu_R - \mu_S}{\sqrt{\sigma_R^2 + \sigma_S^2}}\right) \qquad (4\text{-}3.6)$$

where Φ represents cumulative distribution function of a standardized normal variable. For high reliability situations, it is usually not possible to look up a value in normal table with only probability greater than, say, 0.99999 . It is then necessary to perform numerical integration using the follwing expression,

$$P_f = \int_{-\infty}^{\infty} dz \frac{1}{\sqrt{2\pi}\,\sigma_S} e^{\left[-\frac{1}{2}\left(\frac{z-\mu_S}{\sigma}\right)^2\right]} \left[\Phi\left(\frac{z-\mu_R}{\sigma_R}\right)\right] \qquad (4\text{-}3.7)$$

It is sometimes more convenient to use coefficient of variation than standard deviation. Eq. (4-3.6) can then be recast into the following,

$$P_f = \Phi\left(-\frac{M}{\sqrt{M^2 V_R^2 + V_S^2}}\right) \qquad (4\text{-}3.8)$$

where $M = \dfrac{\mu_R}{\mu_S}$ = safety factor

$V_R = \dfrac{\sigma_R}{\mu_R}$ = coefficient of variation of strength

$V_S = \dfrac{\sigma_S}{\mu_S}$ = coefficient of variation of stress (4-3.9)

It is seen that in this framework, only three parameters are required to determine the failure probability of a component or a structure. These are safety factor, the coefficient of variation of stress and strength. The argument that appears in Eq. (4-3.6), without minus sign, has a special meaning in the SSI theory. It is called safety margin or reliability index. The larger the safety margin, the less the failure probability. It is noted that the safety margin as defined here includes consideration of the uncertanties associated with both stress and strength. This is more general than the traditional 'safety margin' that takes into account only the difference between the mean of strength and stress. The conventional design methodology based on safety factors or

safety margins has succeeded to date, because with the safety factors used today most designs end up with very high reliabilities. But this has been often achieved at the expense of frequently unnecessary overdesign. It is apparent that to achieve the same degree of reliability while not incurring economic penalties, the SSI seems to be a very useful tool.

There are several advantages of using the coefficient of variation instead of the standard deviation. Among these are :

1. It is dimensionless and thus allows easy addition of the coefficient of variation of different quantities with different units.
2. In cases of lognormal distribution, it comes about in a naturual way mathematically, as can be seen in later derivations.
3. It is less sensitive to the exact form different variables exist in various physical models. For example, consider u = x * x, v = x * y. The coefficients of variation of u and v are the same if x and y have the same coefficient of variation.
4. It is in line with most expert judgment or statement of accuracy in physical and engineering testing and investigations.

It is of interest to observe that the result obtained by probabilistic approach reduces to that of deterministic

approach if V_R and V_S are both zero. For example, from Eq. (4-3.8),

$$P_f = 1, \qquad \text{if } M < 1.$$

$$P_f = 0, \qquad \text{if } M > 1.$$

It is noted in the probabilistic framework, even if $M > 1$, there is some failure probability as long as V_R or V_S is not equal to zero. In fact, the safety factor used in traditional engineering design is an attempt to account for inherent uncertainties associated with either the stress (e.g., unexpected or uncontrollable external forces) or strength (e.g., material degradation). The above formulation thus provides a unique way to quantify 'how safe ' the safety factor is.

4.3.2 Lognormal Model

In this case, it is convenient to consider that failure occurs when the ratio between stress and strength is greater than 1. In other words, failure probability is

$$P_f = \Pr\left(\frac{R}{S} < 1\right) \qquad (4\text{-}3.10)$$

Since stress and strength are both lognormally distributed, a random variable Z (defined such that $\ln Z = \ln R - \ln S$) is also lognormally distributed. The probability of failure is then, {4.5}

$$P_f = \int_0^1 \frac{1}{\sqrt{2\pi}\,\sigma_z z} \exp\left[- \frac{1}{2\sigma^2} (\ln z - \mu)^2 \right] dz$$

$$= \int_{-\infty}^{-\frac{\mu_z}{\sigma_z}} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{1}{2} z'^2\right) dz'$$

$$= \Phi\left(-\frac{\mu_z}{\sigma_z}\right) \qquad (4.3.11)$$

Another derivation also gives the same result. Consider a lognormally distributed random variable y. Its probability density function is

$$f(y) = \frac{1}{\sqrt{2\pi}\sigma y} \exp\left[- \frac{1}{2\sigma^2} (\ln y - \mu)^2\right] \qquad (4\text{-}3.12)$$

It follows from Eq. (4-3.4) that

$$P_f = \int_0^\infty \frac{1}{\sqrt{2\pi}\,\sigma_s y} \exp\left[- \frac{1}{2}\left(\frac{\ln y - \mu_s}{\sigma_s}\right)^2\right] \Phi\left(\frac{\ln y - \mu_R}{\sigma_R}\right) dy$$

Now let $y' = \ln y$. Then, we have the following expression for failure probability,

$$P_f = \int_{-\infty}^\infty \frac{1}{\sqrt{2\pi}\,\sigma_s} \exp\left[- \frac{1}{2}\left(\frac{y' - \mu_s}{\sigma_s}\right)^2\right] \Phi\left(\frac{y' - \mu_R}{\sigma_R}\right) dy' \qquad (4\text{-}3.13)$$

This is similar in form to Eq. (4-3.7), hence identical to

$$P_f = \Phi \left(- \frac{\mu_R - \mu_S}{\sqrt{\sigma_R^2 + \sigma_S^2}} \right)$$

where

μ_S, μ_R = central parameters of stress and strength distribution

σ_S, σ_R = dispersion parameters of stress and strength distribution

Eq. (4-3.13) is identical to Eq. (4-3.11). It is necessary to express these in terms of the median and coefficient of variation of stress and strength distribution. This can facilitate future applications, because in engineering studies one usually know about the mean (or median) and coefficient of variations. The following relationships are useful:

$$\mu_y = \exp \left(\mu + \frac{1}{2} \sigma^2 \right) \qquad (4\text{-}3.14)$$

$$\sigma_y^2 = \exp \left(2\mu + \sigma^2 \right) \qquad (4\text{-}3.15)$$

where

μ_y = mean of a lognormally distributed random variable y

σ_y = standard deviation of a lognormally distributed random variable y

It is then possible to find μ and σ in terms of μ_y and σ_y. It can be shown

$$\mu = \ln \mu_y, \qquad (4\text{-}3.16a)$$

where

$$\mu_y = \text{median of } y$$

$$\sigma^2 = \ln \left(\frac{\sigma_y^2}{\mu_y^2} + 1 \right)$$

$$\sigma = \sqrt{\ln \left(1 + \frac{\sigma_y^2}{\mu_y^2} \right)}$$

By taking the first term of the Taylor series expansion of the above expression, we obtain

$$\sigma = V_y \qquad (4\text{-}3.16b)$$

Substituting Eqs. (4-3.16) and (4-3.17) into Eq. (4-3.13) gives

$$P_f = \Phi \left(- \frac{\ln \hat{\mu}_R / \hat{\mu}_S}{\sqrt{V_R^2 + V_S^2}} \right) \qquad (4\text{-}3.17)$$

or

$$P_f = \Phi \left(- \frac{M'}{\sqrt{V_R^2 + V_S^2}} \right) \qquad (4\text{-}3.18)$$

where

$\hat{\mu}_S$ = median of stress

$\hat{\mu}_R$ = median of strength

$$M' = \ln\left(\frac{\hat{\mu}_R}{\hat{\mu}_S}\right)$$

In the case where numerical integration is required (e.g., as mentioned before when the failure probability is outside the range of normal table), the following expression for failure probability is more convenient to use

$$P_f = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\, V_S} \exp\left[-\frac{1}{2}\left(\frac{x}{V_S}\right)^2\right] \left[\Phi\left(\frac{x-M'}{V_R}\right)\right]^k dx \qquad (4\text{-}3.19)$$

4.3.3 Rectangular Model

In order to obtain some physical insight into the operation of the SSI theory, a simpler distribution for stress and strength is studied. As in the previous two cases, it is assumed stress is invariant with time. However, unlike previous cases, the cyclic loading is assumed to apply n times. The basic model assumes that both the stress and strength could be represented by rectangular distributions. Figure 4.4 compares the normal model with rectangular model.{4.16}

With rectangular distributions the limiting stress s_1, s_2, s_3, s_4 will be given by

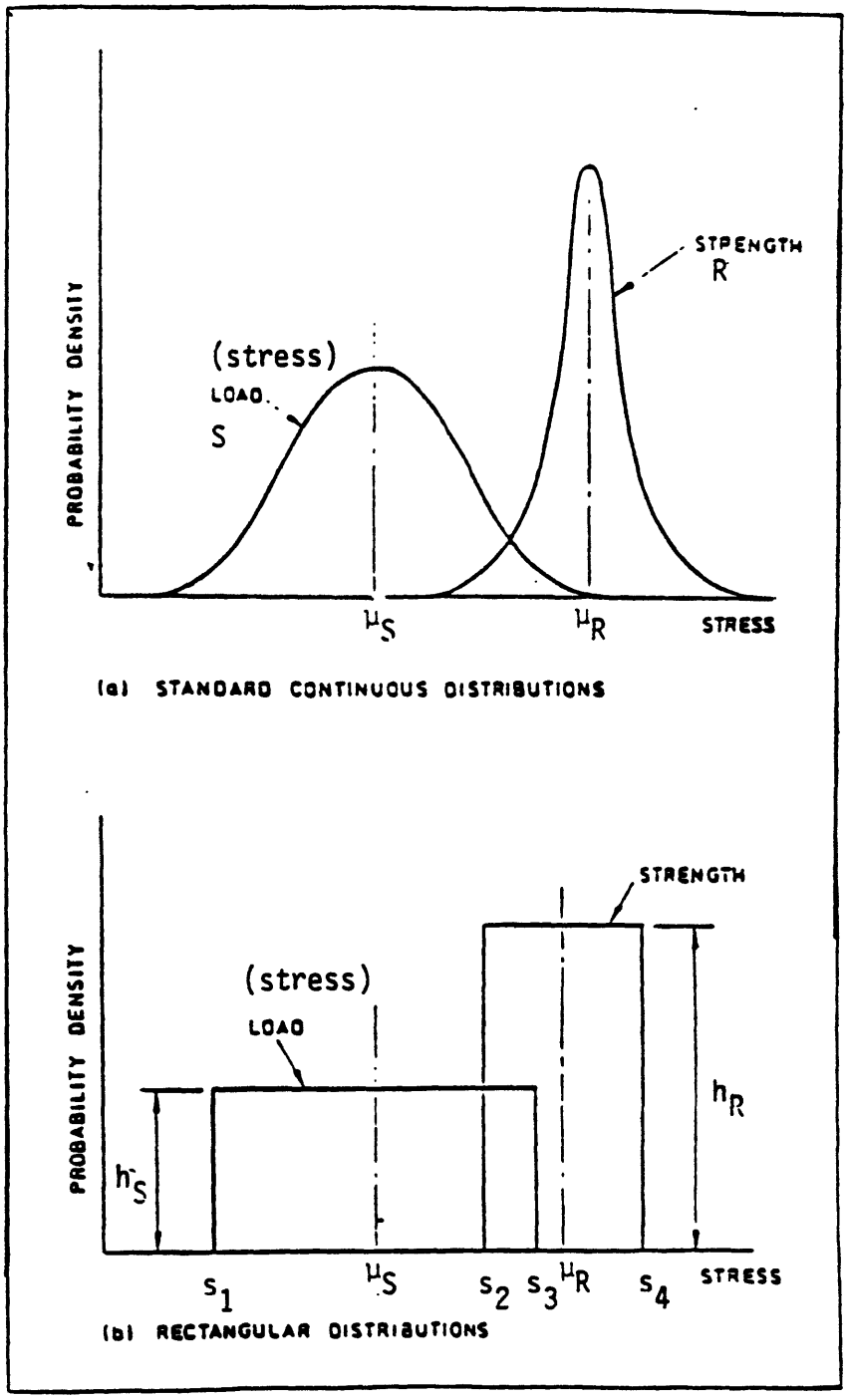


Figure 4.4 Distributions of Load and Strength (Ref. 4.16)

$$s_1 = \mu_S - \sqrt{3}\,\sigma_S$$

$$s_2 = \mu_R - \sqrt{3}\,\sigma_R$$

$$s_3 = \mu_S + \sqrt{3}\,\sigma_S$$

$$s_4 = \mu_R + \sqrt{3}\,\sigma_R \qquad (4\text{-}3.20)$$

where

s_1 = lower limit of rectangular stress distribution

s_2 = lower limit of rectangular strength distribution

s_3 = upper limit of rectangular stress distribution

s_4 = upper limit of rectangular strength distribution

$\mu_S \mu_R$ = mean values of stress and strength respectively

$\sigma_S \sigma_R$ = standard deviation of stress and strength respectively

The probability density function , S(s) and R(r), of stress and strength will be given by

$$S(s) = 0 \qquad s < s_1$$

$$S(s) = \frac{1}{2\sqrt{3}\sigma_S} = h_S \qquad s_1 < s < s_3$$

$$S(s) = 0 \qquad s > s_3 \qquad (4\text{-}3.21)$$

$$R(r) = 0 \qquad r < s_2$$

$$R(r) = \frac{1}{2\sqrt{3}\,\sigma_R} = h_R \qquad s_2 < r < s_4$$

$$R(r) = 0 \qquad r > s_4 \qquad (4\text{-}3.22)$$

Using Eq. (4-3.4) with the above distribution, the failure probability is

$$P_f = 1 - \left[\frac{h_R}{n+1} \frac{\{1-(h_S s_2 - h_S s_1)^{n+1}\}}{h_S} + h_S(s_4 - s_3) \right] \qquad (4\text{-}3.23)$$

For large values of n,

$$\bar{P}_f = 1 - h_R (s_4 - s_3) = h_R (s_3 - s_2) \qquad (4\text{-}3.24)$$

It is immediately obvious that with very large values of n, all items whose strength is less than the maximun stress must fail.

It is then clear why the reliability in a smooth-loading situation (i.e., $\sigma_R/\sigma_S >> 1$) must ultimately always be higher than that in a rough loading situation (i.e. $\sigma_R/\sigma_S << 1$) of the same safety factor. This can be understood from the following considerations.

Failures can only occur in the overlap region of the two distributions, i.e., between s_2 and s_3, and within this region are in proportion to h_R. For smooth loading h_S is high and h_R is small. It follows that the number of failures is low and the reliability high with this type of loading. The reverse is true with rough loading.

4.3.4 Extended Rectangular Model

The basic model studied in 4.3.3 is unrepresentative inasmuch as a very dramatic cutoff is postulated at both the upper and lower limits of both the stress and strength distribution. In realities both distributions must have some form of tail. A small rectangular tail is added to the model in section 4.3.3 as shown in Fig. 4.6. Three subcases are studied.

4.3.4.1 Tail Associated With Stress

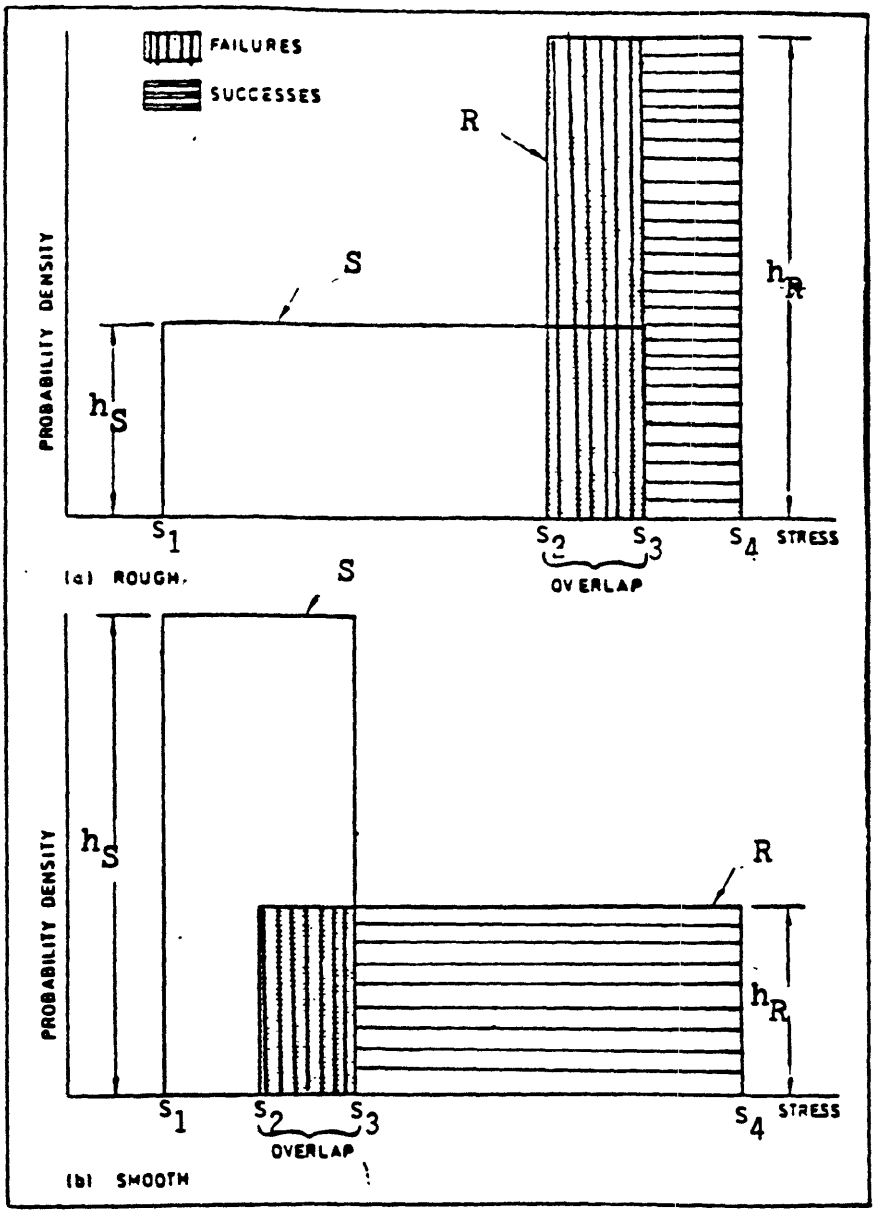


Fig. 4.5 Comparison of Distributions for Rough And Smooth Loading (Ref. 4.16)

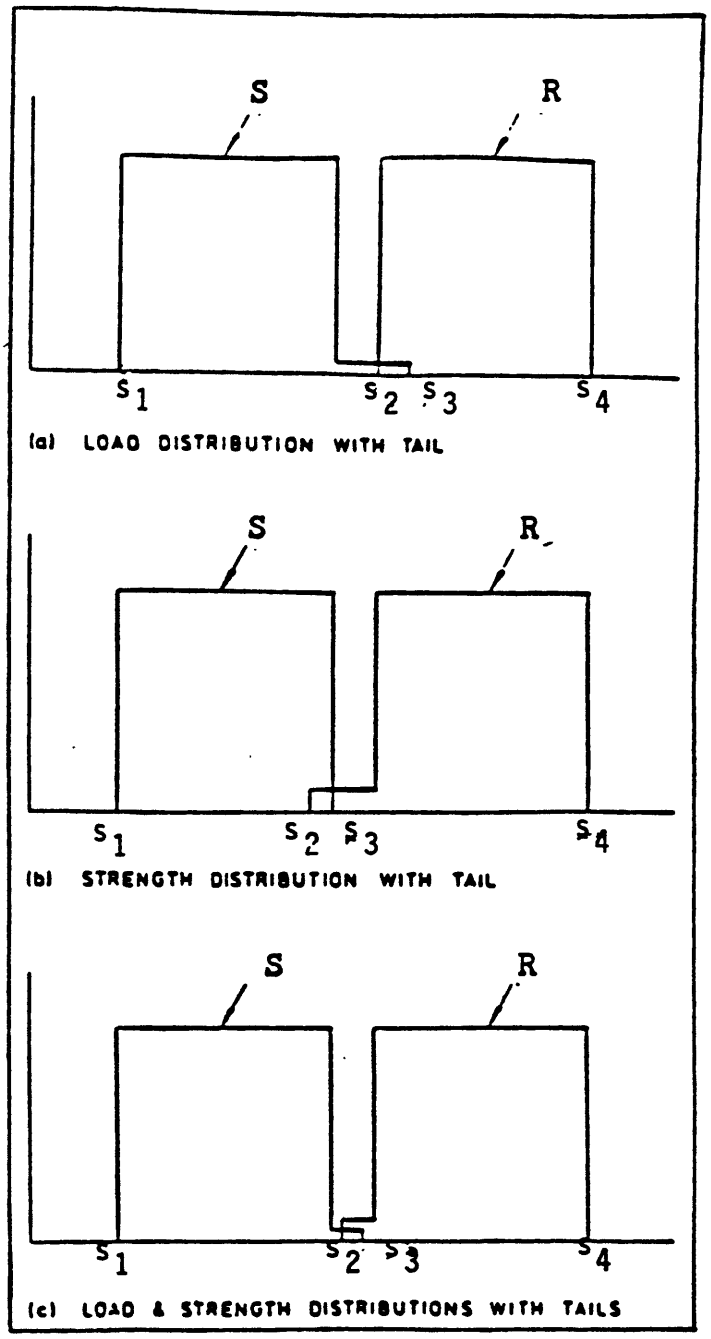


Fig. 4.6 Rectangular Distributions with Tails (Ref. 4.16)

It is shown, by applying Eq. (4-3.4), that the probability of failure in general is given by

$$P_f = 1 - [h_R (s_3 - s_2)\{1 - \frac{n\varepsilon_s(s_3 - s_2)}{2}\} + h_S (s_4 - s_3)] \quad (4\text{-}3.25)$$

If n is large,

$$\bar{P}_f = h_R (s_3 - s_2) \quad (4\text{-}3.26)$$

where

ε_s = tail height of stress distribution

4.3.4.2 Tail Associated With Strength

The failure probability in this case can be obtained from the expression

$$P_f = \varepsilon_R (s_3 - s_2) - \frac{\varepsilon_R}{n+1}\left[\frac{1-(h_S s_2 - h_S s_1)^{n+1}}{h_S}\right] \quad (4\text{-}3.27)$$

For large n,

$$P_f = \varepsilon_R (s_3 - s_2) \quad (4\text{-}3.28)$$

where

ε_R = tail height associated with strength

4.3.4.3 Tails Associated With Both Stress And Strength

In general this is most often the best representation of engineering situations. The following expression gives the failure probability.

$$P_f = \varepsilon_s(s_3-s_2)-\varepsilon_R(s_3-s_2)\left[1- \frac{n\varepsilon_s(s_3-s_2)}{2}\right] \qquad (4\text{-}3.29)$$

If n is large,

$$P_f = \varepsilon_s(s_3-s_2) \qquad (4\text{-}3.30)$$

where ε_s and ε_R are tails associated with stress and strength distribution respectively. In this case it is important to note that the tail of the stress distribution effectively dominates the situation as can be seen from Eq. (4-3.30).

From the study of above three cases one should keep in mind that tails of distribution play an essential role in determining the reliability or failure rate of a component. The tail of the stress distribution is the most significant parameter responsible for reliability.

Another important insight that can be obtained is with regard to the general trend in results of assuming different stress and strength distributions. Irrespective of a particular distribution chosen, the behavior of failure probability with respect to the stress-strength parameters have similar characteristics. As the ratio between the coefficient of variation of stress and that of strength increases, the failure probability increases. On the other hand, if this ratio decreases the failure probability decreases. This provides a very convenient basis for judgment if one is only interested in qualitative aspects of failure. One can proceed with simple distribution to avoid mathematical difficulties while the results so obtained are still correct qualitatively.

However, if one is to obtain more accurate quantitative results, some knowledge of the genesis of distributions often encountered in enginnering applications is required. Table 4.3 provides a concise description of relationships between mathematical models, process description, and resultant statiscal distribution. This should be of significant aid in the choice of a model when one does not have a great amount of data but does have some insight from

Mathematical Operation	Mathematical Model	Process Description	Example	Resultant Statistical Distribution
Counting	$p = \frac{c}{n}$	Enumeration or Classification	Inspection Sorting	Binomial
Addition	$f(y) = \sum_{i}^{n} (x_i)$	Linear Additive	Addition or subtraction of materials; i.e., cutting, weighing, etc., also mechanical assembly.	Normal
Multiplication	$f(y) = \prod_{i}^{n} (x_i)$	Rate-Dependent Proportional Response	Simple chemical processes; i.e., etching, corrosion, gaseous diffusion. Simple biological processes; i.e., growth rate. Simple economic processes; i.e., distribution of income.	Log-Normal
Simple Exponentiation *or* Addition of Transcendental Terms	$f(y) = ax_0 + bx_1 + cx_2^2$ *or* $f(y) = e^{x_0} + e^{x_1} + e^{x_2}$	Algebraic Polynomial Solutions of Linear Differential Equations with Constant Coefficients.	Complex processes involving the combined effects of a number of independent causes each with a different operational form; i.e., breaking strengths, meteorological and geophysical phenomena, electronic and chemical measurements, financial data.	Extreme Value
Counting of Time Duration to an Event	$f(x; n, \lambda) = \frac{\lambda^n}{\Gamma(n)} x^{(n-1)} e^{-\lambda x}$	Waiting Time	Time required for an event(s) to occur or to obtain some service.	Gamma
Addition of Squared Normalized Vectors	$f(y) = \sum_{i}^{n} \left(\frac{x_i}{\sigma_i}\right)^2$	Vector Sums	Resultant value in a system of n-fold vector spaces from physics, space-time, and probability applications.	Chi-Square
Multiplication of Transcendental Terms	$f(y) = e^{(x_0 \cdot x_1 \cdot x_{n-1})}$ $f(y) = e^{(x_0/x_1)(x_2/x_3)}$	Solutions of General Differential Equations Particle Sizing	Complex exponential processes involving the interdependent effects of independent causes; i.e., breakage of particulate materials, solid state diffusion, chemical kinetics.	Log-Extreme Value
Sums, Products, and Powers of Exponents of Transcendental Terms	$f(y) = e^{\left(\frac{x-\varepsilon}{\omega-\varepsilon}\right)^{\beta}}$	Solutions of Differential Equations with Boundary Conditions "Upper-Limit" Distributions	Processes involving limits and maxima-minima; i.e., life/failure distributions, bounded particle size distributions, and general potential, gradient, and field problems.	Weibull

Table 4.3. Genesis of Common Statistical Models (Ref. 4.17)

engineering considerations about the physical quantities of interest.

The normal distribution, which forms the basic model for the present study, has a very nice property of invariance under additive operations. Since many well controlled laboratary experiments usually can be modelled in terms of linear combinations of certain physical quantities, it appears that this distribution provides a reasonable approximation for the analysis of such data.

The lognomal distribution, which forms an alternate model in the present study, possesses a very nice property of invariance under multiplicative operations. Indeed, any product or division of lognormally distributed variables is still a lognormal variable. This is also useful when a physical quantity is the product of several factors each of which obeys lognormal distribution.

Other distributions listed in Table 4.3 may be useful for different applications. Since we are most concerned with stress and strength in this study no effort is made to explore them due to their different nature.

4.3.5 Other Distributions

In the literature surveyed, the above-mentioned models have been used to arrive at various expressions for probability of failure. In simple cases closed form solutions are available. In more complicated situations,

numerical integrations or Monte-Carlo simulations have to be used to come up with numbers. References 4.15,4.18,4.19,4.20,and 4.21 derive useful expressions based on various combinations of stress and strength distributions. These include common statistical models used in engineering such as exponential, gamma, Weibull, extreme-valued, Rayleigh,chi-squared etc. It is noted most of the distributions that have been investigated are those existing in diverse disciplines for different applications. For example, in earthquake engineering, extreme value type I distribution has often been used to model the nonexceedance frequency of earthquake acceleration, the so-called seismicity as mentioned in section 4-2. In the case of fatigue investigations, Weibull distribution has often been used as a model to fit the life-time to failure of ball bearing. In statistical testing for validity of certain model hypothesized, chi-squared distributions are often used.

Some observations on the studies made previously are described as follows:

1. The results obtained from these analytical investigations are mainly of academic interest at present stage. No concrete examples have been presented to demonstrate the application. It remains merely as an exercise of mathematical nature unless practical implications can be illustrated.

2. Statistical analyses or physical considerations concerning the adequacy of presented models have not been indicated. This is indeed an area that needs to be pursued further if applications are to be meaningful.

3. There are more models than data warrant. It is important to use physical and statistical techniques to design and analyze data so that adequate model is chosen realistically.

4. There is a strong need to come up with a method that can relax data requirement and incorporate engineering considerations explicitly. Indeed, this is the very objective of this research.

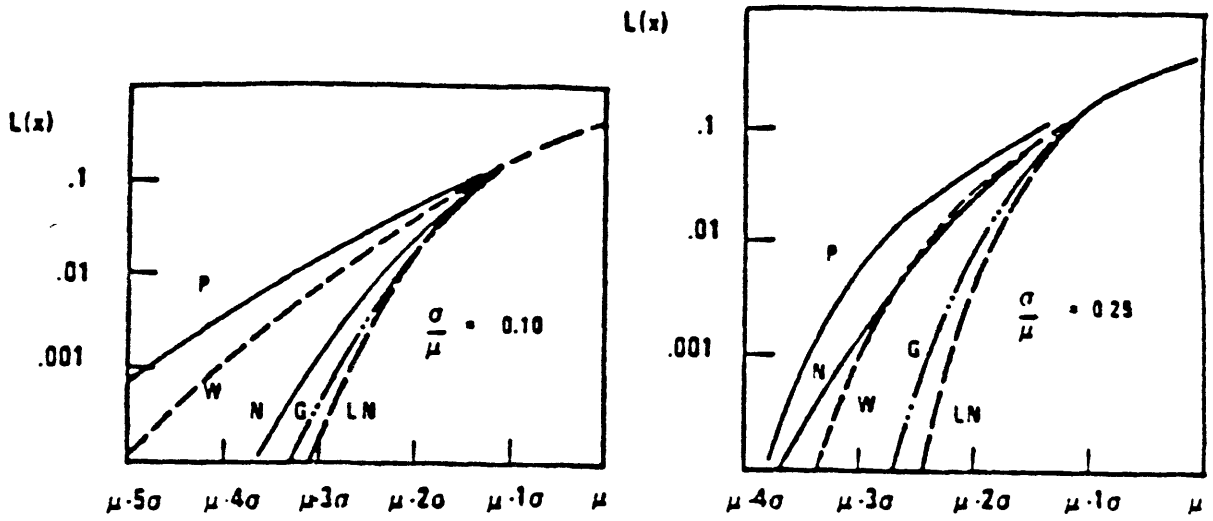
It is of special importance to note that the data required for SSI applications are different in nature from those for common statistical life-time type of analysis mentioned at the beginning of this chapter. In the latter, one generally needs failure time data so that statistical procedures coupled with accompanying assumptions can be used to estimate failure rate. The data required for SSI, however, are stress and strength distributions. They can be easily gleaned if effort is conscientiously made. This difference in the nature of the data should be kept in mind to view the stress-strength interference theory in a proper light.

Before proceeding to discuss an extension of the SSI theory, let's look at the problems associated with tails of different distributions more closely. Since we have confined

our attention to two-parameter characterization of distributions, there are many possible distributions with a given mean and coefficient of variation. It is mainly the upper tails of the stress distributions and lower tails of the strength distributions that are important in determining the probability of failure. For high reliability situations probabilities of failure are even more sensitive to the tails. Considerations to cope with the tail-sensitivity are outlined as follows.

1) Sensitivity studies may be performed to indicate the range in which the failure probability is expected to lie. Fig. 4.7 shows lower tail probabilities for commom statistical models. {4.22,4.23} Looking at the Figure, when uncertain and to be conservative, one should choose strength distribuions with higher lower-tail probability. This means it is more likely that the strength stays in lower range than the stress distribution, yielding higher probability of failure. Thus using a normal strength distribution is more conservative than using a lognormal one, other conditions being equal.

Fig. 4.8 gives upper tail probabilities for the same statistical models. It is immediately obvious that the lognormal distribution has higher upper tail probabilities than the normal one. To be conservative, it is necessary to use the lognormal distribution for stress modelling when insufficient information is available.



NOMENCLATURE

PROBABILITY DENSITY FUNCTIONS, F(x):

N - NORMAL W - WEIBULL P - POWER
LN - LOGNORMAL G - GAMMA

μ - MEAN σ - STANDARD DEVIATION

LOWER TAIL AREA:

$$L(x) = \int_{-\infty}^{x} F(s)ds$$

Fig. 4.7. Lower Tail Probabilities for Common Statistical Models (Ref. 4.22)

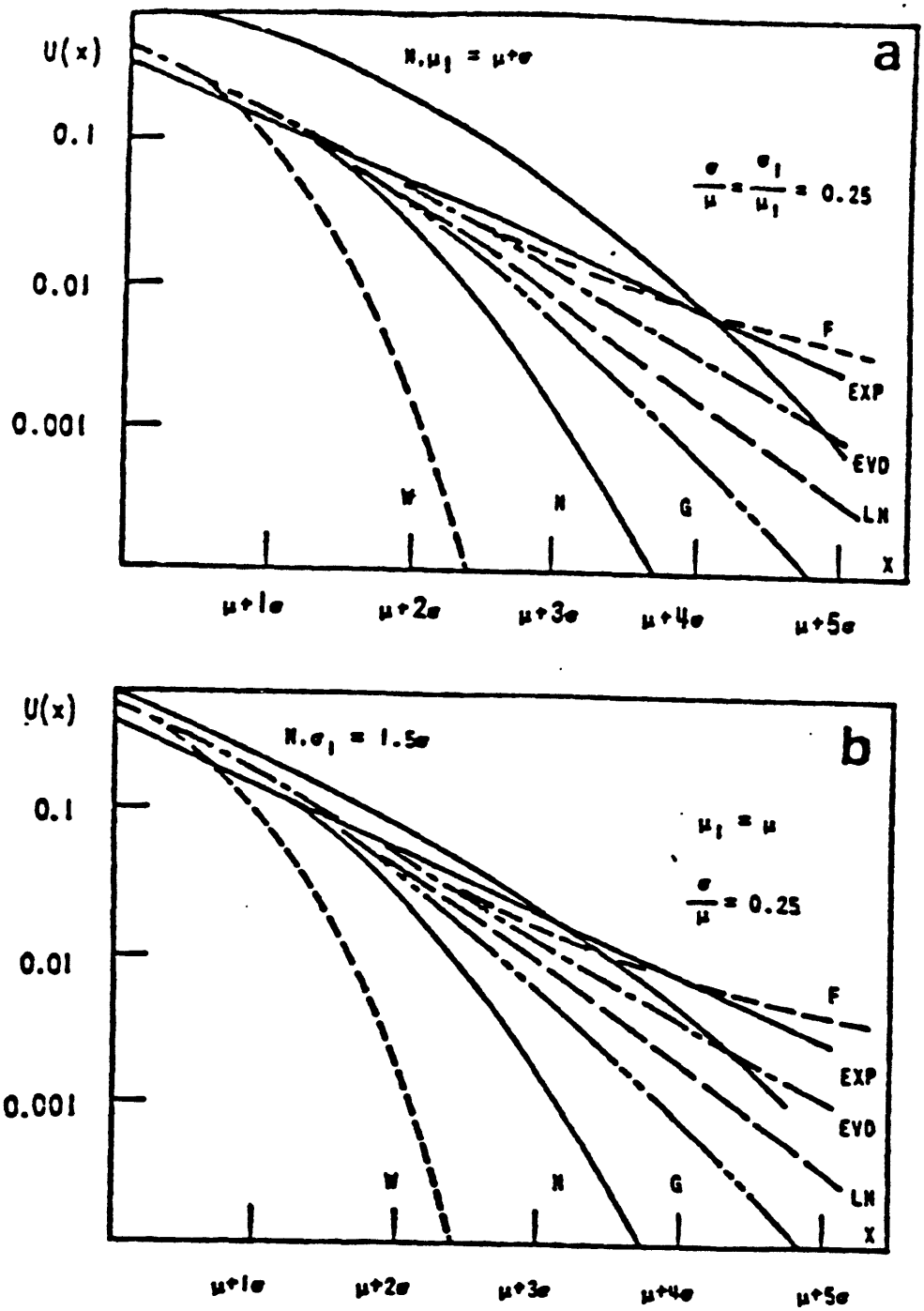


Fig. 4.8. Upper Tail Probabilities for Common Models

(a).Compared with Normal Distribution with Increased Mean

(b).Compared with Normal Distribution with Increased Standard Deviation (Ref. 4.22)

2). If available data are not sufficient to perform meaningful statistical analysis, physical considerations play an even more important role in selecting a particular model for stress and strength distributions.

3).If only qualitative results are of interest, it appears whichever common statistical models with given mean and coefficient of variation will give the same trend, as discussed before.

4.4 Common Load Model {4.26,4.27}

The common load model originated from an attempt to justify the " square root " approach for evaluating dependent failure probabilities used in WASH-1400. In essence, it is an extension of the SSI theory for single component to a system consisting of N identical components. It is used in this research to provide a rational basis for quantifying multiple dependent failure fractions and parameters in MGLM discussed in Chapter 3.

The basic mathematical model developed is based on the assumption that the loading of the components concerned is described by a single parameter, for example, a particular stress. In addition, the following assumptions are made :

1). N identical components, each has an identical resistance to stress, which is treated as a random variable with the probability density function $f_R(x)$ and with the cumulative distribution function denoted by

$$F_R(x) = \int_{-\infty}^{x} dy.f_R(y) \qquad (4\text{-}4.1)$$

The physical interpretation of $F_R(x)$ is that if stress has a single value x, $F_R(x)$ is the corresponding failure probability.

2). When N items are loaded in parallel, the multiple failure due to a common cause dictates that the stress distribution $f_s(x)$ be the same for each item. But different values of $F_R(x)$ may be at presence although the same functional form of $F_R(x)$ is assumed for each item. The probability of precisely k components out of N failing is given by

$$P_{k/N} = \int_{-\infty}^{\infty} dx . f_S(x) \; [F_R(x)]^k [1 - F_R(x)]^{N-k} \binom{N}{k} \qquad (4\text{-}4.2)$$

The probability of at least k components out of N failing is given by

$$P_{>k/N} = \sum_{i=k}^{N} P_{i/N} \qquad (4\text{-}4.3)$$

In particular, if we are interested in 1 out of k system, i.e., all components have to fail, the probability of failure is given by

$$P_{k/k} = \int_{-\infty}^{\infty} dx \; f_S(x)[F_R(x)]^k = P_f^k \qquad (4\text{-}4.4)$$

where P_f^k stands for k-component failure probability.
If k=1, the model reduces to the single component stress-strength model assumed in the previous section.

Let's now generalize the above formulation to practical engineering situations where there are n common causes operating on identical k components. Since in highly redundant systems, independent failures are negligible compared with CCF, we focus the present discussion on CCFs only. As described in section 2.3, the probabilistic modelling of CCF is in principle easier than it appears. The key lies in identifying all the common conditions which may impose common stresses for all the redundant components. The probability of k-component failure due to CCF, P_f^k, is

obtained by summing over all the conditional failure probabilities. Thus,

$$P_f^k = P^k(A| C_{Ai}) P (C_{Ai}) \qquad (4\text{-}4.5)$$

where

$$P^k(A| C_{Ai}) = P (A| C_{Ai})$$

$P(A|C_{Ai})$ = Failure probability of component A due to condition C_{Ai}

$P(C_{Ai})$ = Probability of condition C_{Ai}

It follows, by putting in probabilistic formulations used previously,

$$P_f^k = \sum_{i=1}^{n} \int_{-\infty}^{\infty} f_{S_i}(x)[F_{R_i}(x)]^k \, dx \qquad (4\text{-}4.6)$$

Similarly, for a single component, the probability of failure is given by

$$P_f = \sum_{i=1}^{n} \int_{-\infty}^{\infty} f_{S_i}(x)[F_{R_i}(x)] \, dx \qquad (4\text{-}4.7)$$

It can be seen that the data requirement for computing multiple failure probability is identical to that for the single component failure case.

It is again useful to consider two special cases, the normal and the lognormal models.

4.4.1. Normal Model

The expression is essentially the same as Eq. (4-3.7), except the strength term is raised to the kth power as explained above. Thus,we have

$$P_f^k = \sum_{i=1}^{n} \int_{-\infty}^{\infty} dz \frac{1}{\sqrt{2\pi}\,\sigma_{S_i}} e^{\left[-\frac{1}{2}\left(\frac{z-\mu_{Si}}{\sigma_{Si}}\right)\right]} \left[\Phi\left(\frac{z-\mu_{Ri}}{\sigma_{R_i}}\right)\right]^k \qquad (4\text{-}4.8)$$

or

$$P_f^k = \sum_{i=1}^{n} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\,V_{Si}} \exp\left[-\frac{1}{2}\left(\frac{z-1}{V_{Si}}\right)^2\right] \left[\Phi\left(\frac{z-M_i}{V_{R_i}}\right)\right]^k dz \qquad (4\text{-}4.9)$$

where i designates a particular cause i.

4.4.2 Lognormal Model

The expression is essentially the same as Eq. (4-3.19), except the strength term is raised to the kth power as in the normal case.

$$P_f^k = \sum_{i=1}^{n} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\,V_{S_i}} \exp\left[-\frac{1}{2}\left(\frac{z}{V_{S_i}}\right)^2\right] \left[\Phi\left(\frac{z-M_i'}{V_{Ri}}\right)\right]^k dz \qquad (4.4.10)$$

It can be seen from Eq. (4-4.9) and (4-4.10) that once numerical values regarding the paremeters of stress and strength distributions are obtained by some means, the calculation of multiple component failure probability is a straightforward numerical integration. A small computer program used for this purpose is described in Appendix A.

It has been our goal in this research to study coupled failures. However, it is worth noting that studies on cascade failures have been performed for redundant structures.{4.13,4.25} Traditional stress analysis is used to assess additional stresses to be carried by residual intact members when one or more structural members fail. Then expressions similar to Eq. (4-4.2) are used to derive failure probability of the whole structure. Future research effort is needed if a similar approach is to be used for redundant components in nuclear safety systems.

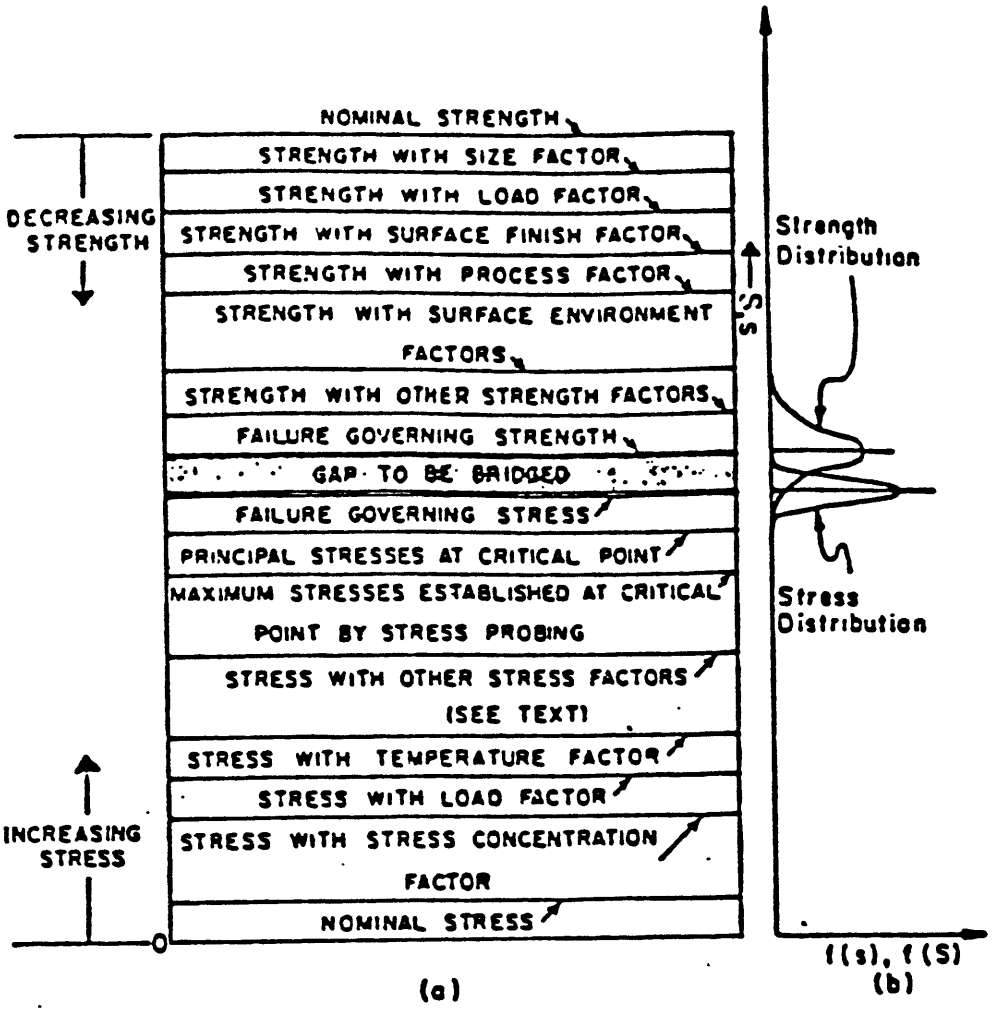
Chapter 5

The Inverse Stress-Strength Interference Technique

5.1 An Alternative Approach to Estimating Multiple Failure Parameters

In Chapter 4 the stress-strength interference theory was explored in some depth for commonly used statistical models in engineering situations. The basic data requirement consists of two parameters characterizing the stress distributions, and another two parameters describing the strength distributions. The procedure for arriving at the failure governing stress distribution of mechanical components {5.1}, as illustrated in Fig. 5.1, is as follows:

1. Identify all significant failure modes.
2. If fracture is one of the significant failure modes, perform stress probing to determine the locations where the combination of stresses acting are most likely to fail a component
3. Calculate the nominal stress components at these locations.
4. Determine the maximum value of each stress component with the use of proper stress modifying factors.
5. Combine these stresses into the failure governing stress at each location in accordance with the failure governing criterion involved in the failure mode being considered. The location with the highest failure governing stress is the one where



(a). Sfress increase and strength decrease resulting from the application of the respective stress and strength factors.

(b). Failure governing stress and strength distributions

Figure 5.1 Determination of Failure-governing Stress and Strength Distributions (Ref. 5.1)

the component will have the highest probability of failure.

6. Determine the distribution of each nominal stress, and stress modifying factor and parameter, in the equation for the failure governing stress.

   The following factors may have to be included for different situations:

   a. stress concentration factors.
   b. load factors such as static, quasistatic, dynamic, impact, shock, and energy load factors.
   c. temperature stress factors.
   d. forming/manufacturing stress factors.
   e. surface treatment stress factors.
   f. heat treatment stress factors.
   g. assembly stress factors.
   h. corrosion stress factors.
   i. direct surface environmemt stress factors.
   j. notch sensitivity factors.

   Unfortunately, relatively little statistical information is available for these factors presently. Much research needs to be conducted to determine this information.

7. Synthesize these distributions into the failure governing stress distribution.
8. Repeat the previous steps for each one of the significant failure modes.

Some failure governing criteria are:

1. Maximum normal stress.
2. Maximum shear stress.
3. Maximum distortion energy.
4. Maximum strain energy
5. Maximum strain.
6. Maximum deflection.
7. Combination of the mean and alternating stresses into the maximum shear or distortion energy in case of fatigue.
8. Maximum total strain gauge in case of fatigue.
9. Maximum allowable corrosion.
10. Maximum allowable vibration amplitude.
11. Maximum allowable creep.
12. Others depending on the nature of the significant failure mode.

The failure governing stress is the stress at failure. The procedure for determining the failure governing strength distribution, as illustrated in Fig. 5.1, is as follows:

1. Establish the applicable failure governing strength criterion. This criterion should be the same as that used for the failure governing stress involved and failure mode being considered.
2. Determine the nominal strength.
3. Modify the nominal strength with appropriate strength factors to convert the nominal strength

determined under an idealized and standardized test be exhibited by environmemt it is designed for.

4. Determine the distribution of the nominal strength, and of each strength modifying factor and parameter in the failure governing strength equation.
5. Synthesize these distributions into the failure governing strength distribution.

There is also little data for the determination of the failure governing strength. There have been increasing efforts during the last ten years to generate such data; nevertheless, the pace of such efforts must increase to give the SSI theory the impetus it deserves.

As described above, the calculation of reliability in general requires distributional strength data, including static, yielding and ultimate strength data, cycles-to-failure and stress-to-failure data in fatigue, creep data, Young's modulus data, Poisson's ratio, thermal conductivity, thermal coefficient of expansion etc., for different operating environments. In addition, distributions for dimensions, loads, temperatures, pressures, etc., are needed to determine the failure governing stress distributions. As alluded to above, there are relatively few sources for the latter, and much effort needs to be conducted to generate such distributional data. It is worth pointing out that the kind of data required in the SSI framework differs from life-testing situations. What one

needs for the latter usually takes a long time to accumulate and is usually more expensive to collect. To make use of the ISSI, one requires the strength properties and stress acting on the component. These are less expensive to obtain but require some knowledge of statistical methods to extract more useful information from laboratory measurements. The experimental data statistically analyzed can thus be of direct use for SSI applications. Furthermore, if the design of experiments to measure certain material stress or strength effects is aided by statistical considerations beforehand, more powerful results can be gleaned within the usual engineering constraints, either technically or economically.

To alleiviate the problems just cited in applying the common load model to analyze common cause failure, we make use of available LER data to estimate single component failure probability. Once we come up with an appropriate value for single component failure probability, we make use of this important piece of information relating the stress-strength parameters. By inverting the expressions obtained from SSI theory, a relationship between these parameters can be established. At the same time, engineering considerations based on past operating experience and laboratory tests can provide us with numerical values on either the variations of stress or strength, or safety factor, depending on circumstances. These are then combined to come up with multiple failure

probability by making use of common load model. Several major advantages are worth noting.

First, this process not only allows an analyst to quantify the parameters needed, but also provides a designer an opportunity to recognize the area of improvement. Secondly, the engineering judgment is made explicit by quantifying various coefficient of variations and safety factors for possible failure modes. Thirdly, LER data provides a data base most relevant to nuclear power plant conditions, and should be used as much as possible. The single component failure data to be used is the most statistically significant because of a larger number of occurrences compared with multiple occurences reported in the LER. The inverse stress-strength method thus capitalizes on it. Fourthly, in the process of using only single component failure data, the bias involved in the interpretation of some vague CCF reporting statements in the LER is avoided. Most other approaches based solely on statistical analyses of LER data such as binomial failure rate models are susceptible to the bias just mentioned. Last but not least, current methods for estimating multiple failure parameters rely heavily on statistical procedures. The sparcity of multiple failure data introduces tremendous variability in the results that few meaningful conclusions can be drawn for engineering decision purposes.

Section 5.2 discusses the inverse stress-strength interference (ISSI) method when the underlying stress and

strength distributions are both normal. It can be seen in this framework, flexibility is incorporated to accomodate different availability of data.

Section 5.3 presents the ISSI method when the underlying stress and strength distributions are lognormal. The expressions derived in this case are identical in form to the normal case, only interpretations of terms are slightly different.

Section 5.4 describes some qualitative results obtained in applying ISSI method. The discussion gives some salient features of the significance of various parameters in stress and strength distributions.

5.2 Normal Model

There are various reasons for the assumption of normal distribution. Physically, most random phenomena, especailly those carried out in laboratory under well-controlled conditions, are subject to a large number of factors which exert more or less influence microscopically. For engineering interests, one is usually dealing with macroscopic quantities which are manifestations of total effect of those large number of influencing factors. If all these factors play an equally important role, the macroscopic quantity of interest can be reasonably approximated by the virtue of central limit theorem.

Mathematically, any linear combination of a normal random variable is still normally distributed. In engineering applications, the system or component behavior can usually be approximated by a linear model. Thus, it is worthwhile to discuss the inverse SSI method based on normal distributions.

As derived in Sec. 4.3,

$$P_f = \Phi\left(-\frac{M-1}{\sqrt{M^2V_R^2+V_S^2}}\right)$$

gives a simple formula for calculating P_f. On the other hand, we have a reasonable estimate of P_f from LER data. The inverse SSI method makes use of this estimate to get a relationship between the three parameters that completely specify multiple failure probability. By inverting the expression obtained from the SSI theory,

$$-\Phi^{-1}(P_f) = \alpha = \frac{M-1}{\sqrt{V_S^2+V_R^2M^2}} \qquad (5\text{-}2.1)$$

where α is the safety margin or reliability index defined previously. Three cases are possible, depending on the data available on stress and strength distribution parameters.

5.2.1 V_R, V_S Given

It is generally much easier in engineering situations to estimate the variability of a random quantity than estimating the whole distribution. Actually, it is even

easier to come up with the coefficient of variation from a sample of experimental data. Any elementary statistical description of data can give indication of the coefficient of variation. Suppose we have obtained the coefficient of variation for both stress and strength based on engineering considerations. By taking the inverse of Eq. (4-3.8) and solving M in terms of V_R and V_S,

$$M = \frac{-1 - \sqrt{1 - (\alpha^2 V_S^2 - 1)(\alpha^2 V_R^2 - 1)}}{\alpha^2 V_R^2 - 1} \qquad (5\text{-}2.2)$$

where α is defined as above.

By directly substituting M, V_R, and V_S into the following equation

$$p_f^k = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\, V_S} \exp\left[-\frac{1}{2}\left(\frac{x-1}{V_S}\right)^2\right] \left[\Phi\left(\frac{x-M}{V_R M}\right)\right]^k dx \qquad (5\text{-}2.3)$$

one can compute multiple-component failure probability readily.

5.2.2 V_R, M Given

In some cases, based on previous experience, a design based on safety factor M can be specified. The coefficient of variation of material strength can again be estimated from tests performed in laboratory. It is then straightforward to solve for V_S, making use of Eq. (5-2.1) to obtain

$$V_S^2 = \left(\frac{M-1}{\alpha}\right)^2 - V_R^2 M^2 \qquad (5\text{-}2.4)$$

Then substituting back into Eq. (5-2.3), it is easy to obtain multiple-component failure probability.

5.2.3 V_S, M Given

In other cases, it may happen that the analyst is more confident about values of V_S and M. Then by making use of LER data one can solve for V_R from Eq. (5-2.1) to obtain

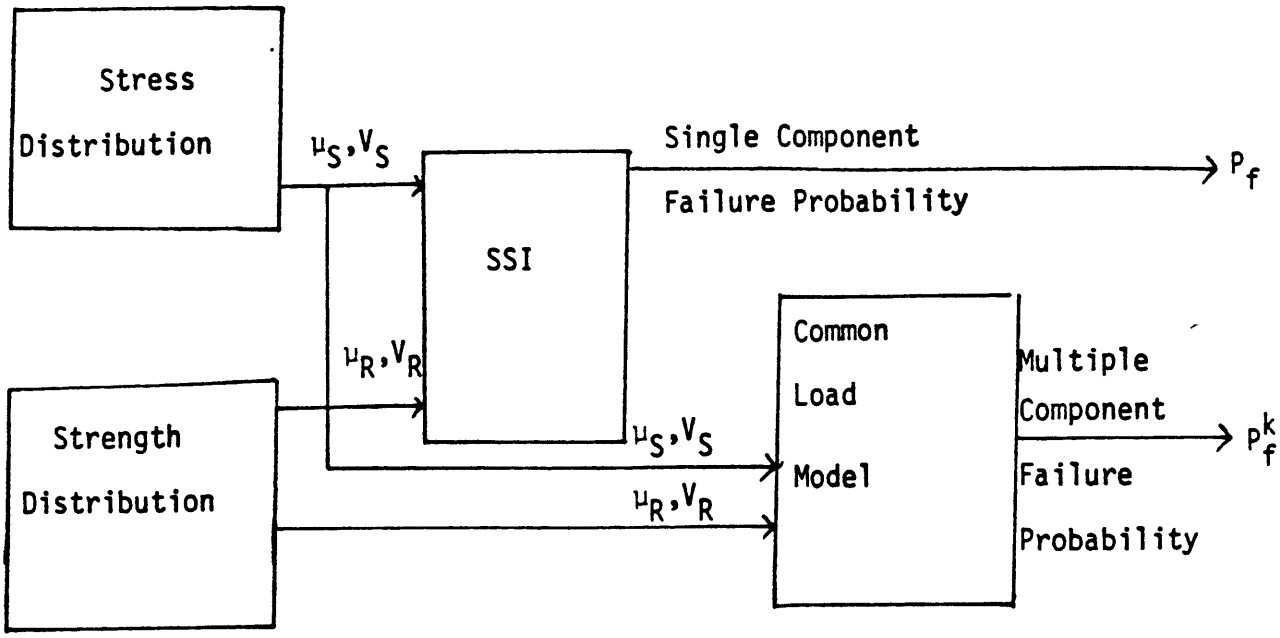
$$V_R^2 = \left(\frac{M-1}{\alpha M}\right)^2 - \left(\frac{V_S}{M}\right)^2 \qquad (5\text{-}2.5)$$

Then substituting back into Eq. (5-2.3), one obtains multiple-component failure probability readily. The information flow for the ideal case where all distributional data are available is shown in Fig. 5.2. In the same figure three cases of the inverse stress-strength method just described are also summarized. As an example, if one can estimate the coefficient of variation of stress and strength associated with the component of interest, the following procedure provides a convenient way to compute multiple failure probability:

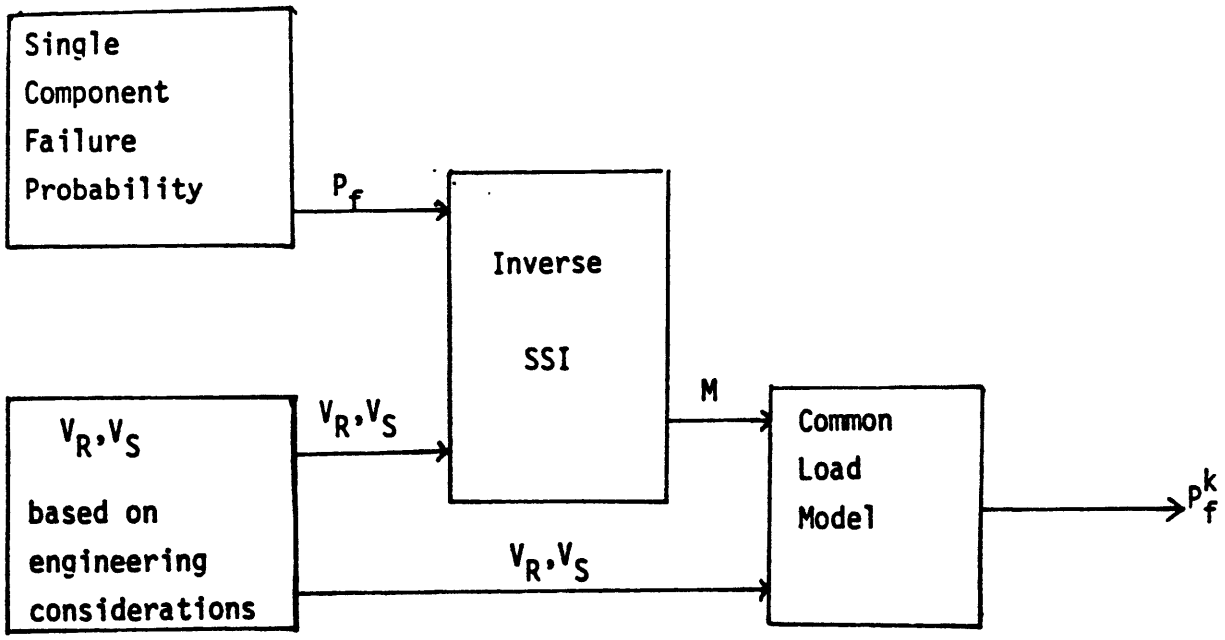
1. Estimate V_S and V_R based on pertinent laboratory test data or other engineering considerations.

2. From LER data for components of interest, estimate failure probability of single component, P_f.

Figure 5.2 Information Flow in Failure Analysis: Normal Model



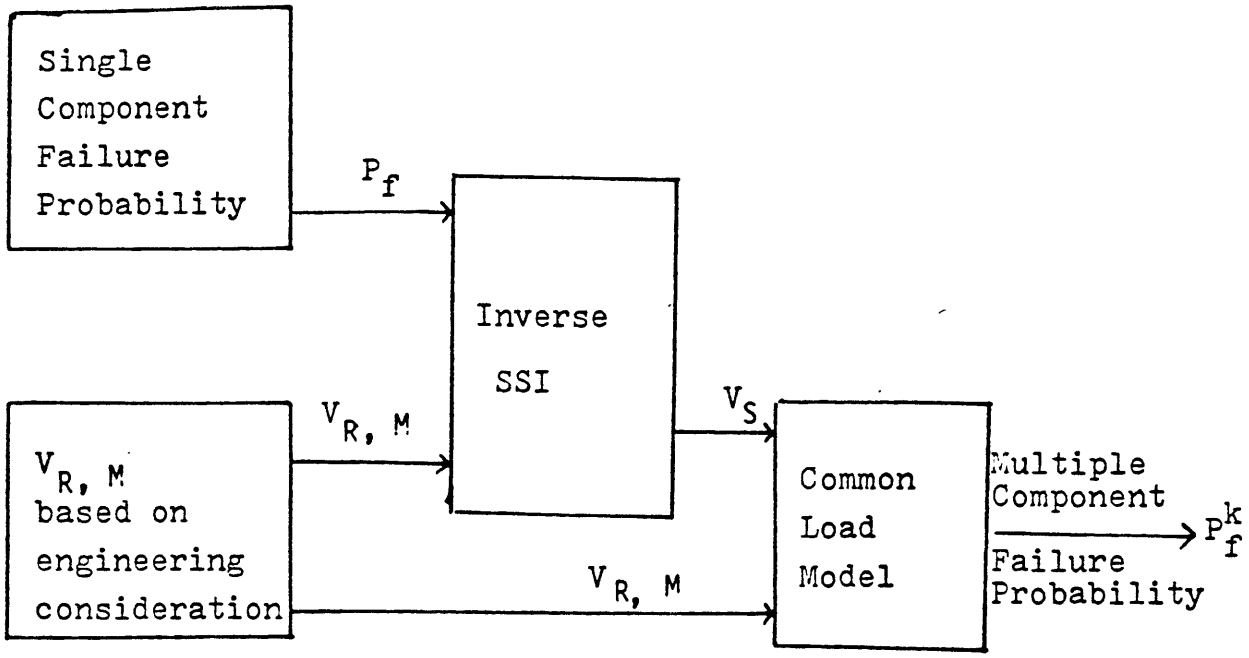
Ideal Situation



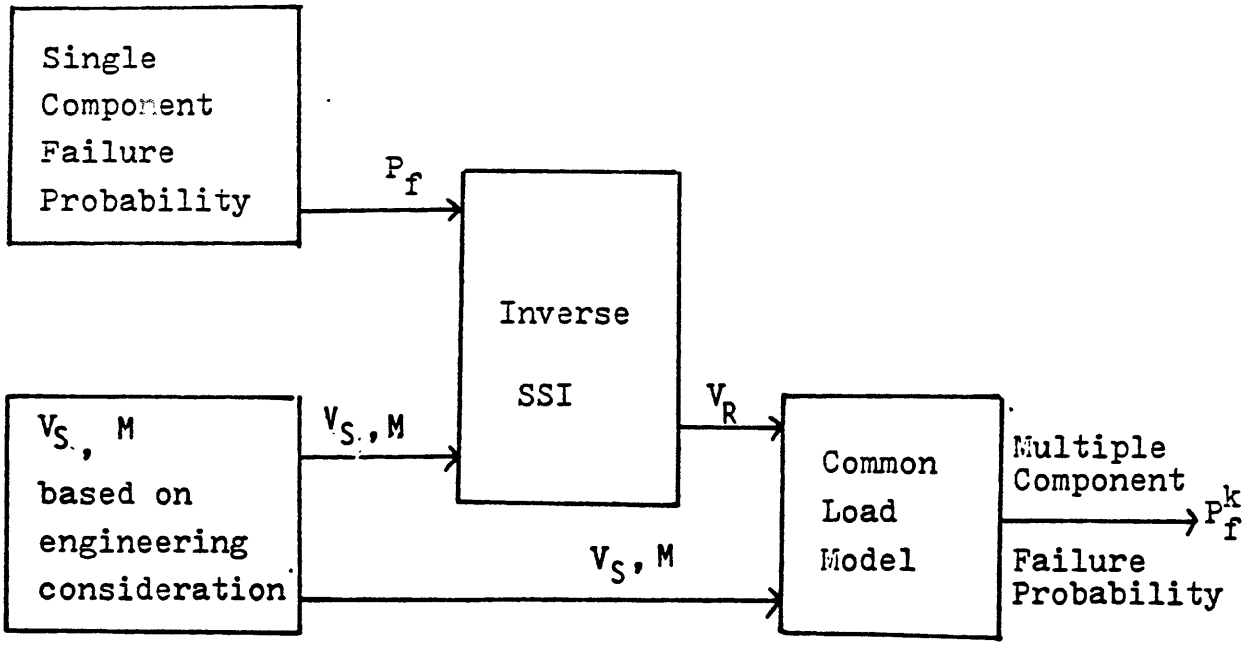
Inverse SSI, Case 1. V_R, V_S Given

Figure 5.2 (Continued)

Case 2. V_R, M given



Case 3. V_S, M given



3. Find the inverse of $\Phi(-\alpha) = P_f$, where

$$\alpha = -\Phi^{-1}(P_f) = \frac{M-1}{\sqrt{V_S^2+V_R^2M^2}}$$

4. Find safety factor M from the expression

$$M = \frac{-1 - \sqrt{1 - (\alpha^2V_S^2-1)(\alpha^2V_R^2-1)}}{\alpha^2V_R^2 - 1}$$

5. Substitute V_R, V_S, and M into the expression

$$P_f^k = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\,V_S} \exp[-\frac{1}{2}(\frac{x-1}{V_S})^2]\ [\Phi(\frac{x-M}{V_RM})]^k\ dx$$

The procedure is illustrated in Fig. 5.2, case 1. Similar procedures apply to other situations where data availability dictates different approaches.

In actual applications, to be discussed in next chapter, one is often faced with a number of common causes operating together, as indicated in section 4.4. To obtain reliability index making use of LER data, i.e., Eq. (5-2.1), one has to decompose data into distinct causes. Some of them are not contributing much to multiple failure probability and hence can be ignored. Others may be lethal in nature (i.e. leading to complete failure of redundant components) and do not need to utilize the method discussed in this work. Most personnel errors are in this category. Chapter 6 demonstrates the above procedure by applying the inverse

stress-strength method to pumps and valves in commercial nuclear power plants. Failure to recognize that most LER data are aggregation of different causes, each with different coupling capability, is one of the reasons why CCFA has not reached consensus in both the structures and the parameters used in different modeling effort.

5.3 Lognormal Model

In principle, the procedure adopted under this assumption is identical to that of the normal case. One starts off by inverting Eq. (4-3.18),

$$\alpha = -\Phi^{-1}(P_f) = \frac{M'}{\sqrt{V_S^2+V_R^2}}$$

where α is the usual safety margin or reliability index. Again three cases can be identified.

5.3.1 V_R, V_S Given

By solving for M' from Eq. (5-3.1), one obtains

$$M' = \alpha \sqrt{V_R^2 + V_S^2} \qquad (5\text{-}3.2)$$

Then substituting V_R, V_S and M' into the expression

$$P_f^k = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\, V_S} \exp\left[-\frac{1}{2}\left(\frac{x}{V_S}\right)^2\right] \left[\Phi\left(\frac{x-M}{V_R}\right)\right]^k dx \qquad (5\text{-}3.3)$$

the failure probability of multiple components can be obtained. It is noted that Eq. (5-3.3) is identical in form to Eq. (5-2.3). Thus the numerical calculation of the integral can be performed by slightly modifying the program used in the normal case. Appendix A discusses this in more detail.

5.3.2 V_R And M' Given

Again, by solving for V_S from Eq. (5-3.1), the following expression is obtained

$$V_S^2 = \frac{M'}{\alpha^2} - V_R^2 \qquad (5\text{-}3.4)$$

Substituting V_R, V_S and M' into Eq. (5-3.1), the probability for multiple component failure is obtained.

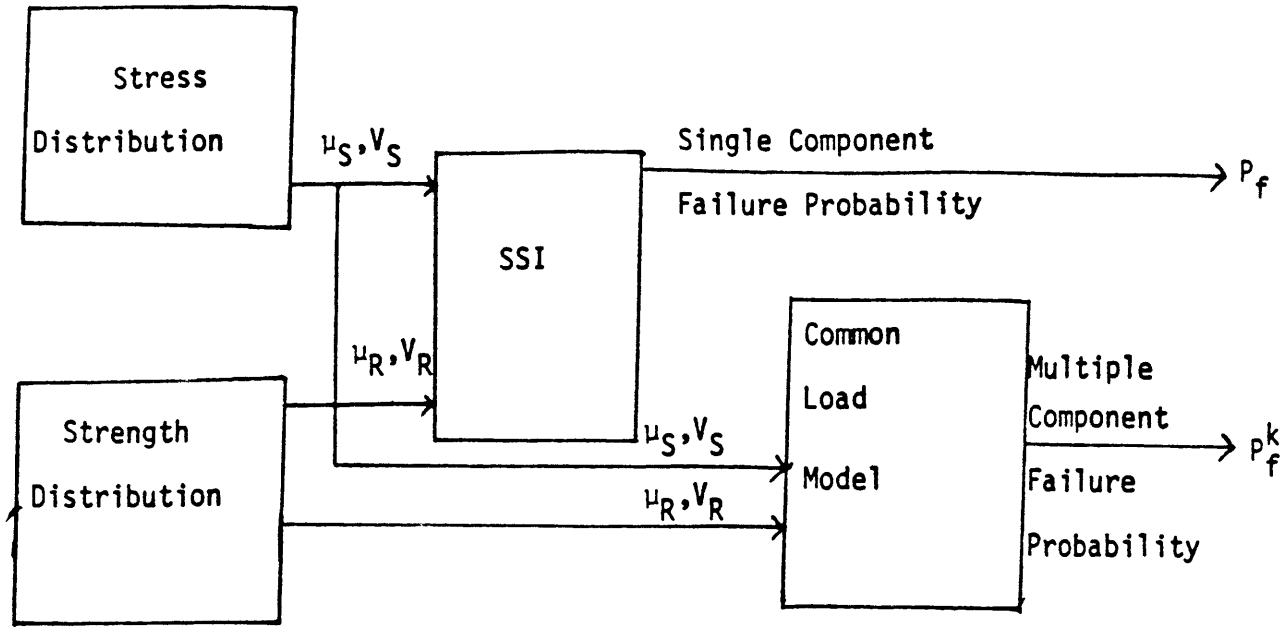
5.3.3 V_S And M' Given

Again, by solving for V_R from Eq. (5-3.1), one obtains

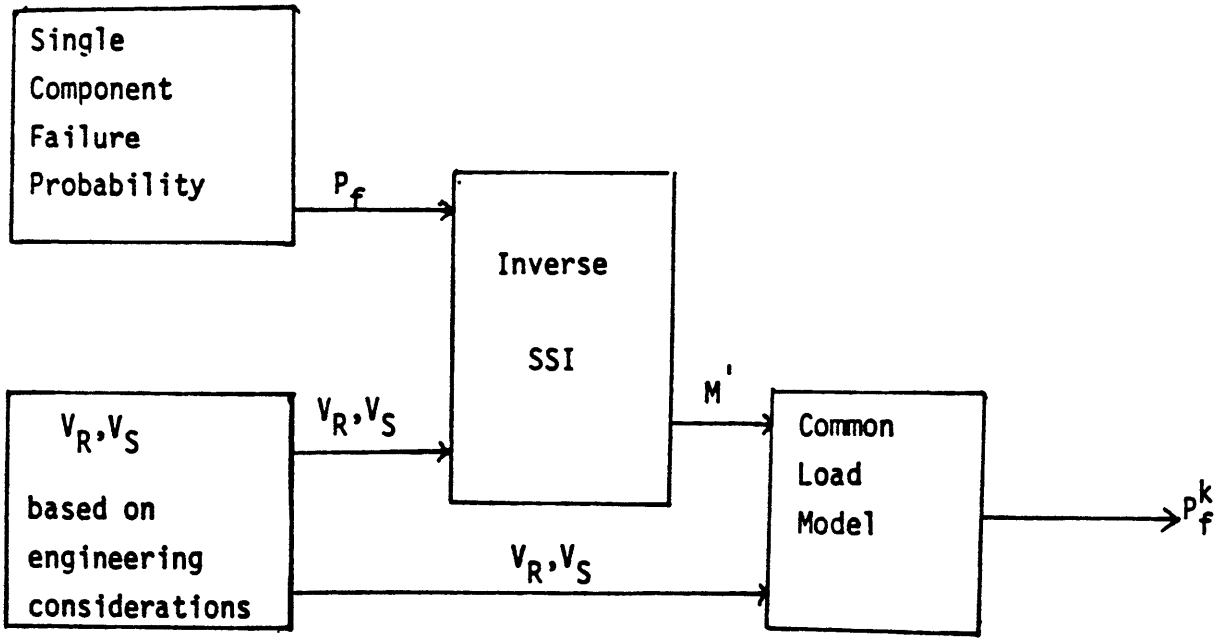
$$V_R^2 = \frac{M'}{\alpha^2} - V_S^2 \qquad (5\text{-}3.5)$$

By substituting V_S, M', and V_R into Eq. (5-3.3), one can compute multiple failure probability readily. Figure 5.3 summarizes the information flow for the lognormal model just discussed. It is seen by comparing Fig. 5.2 and 5.3 that the structure of the approach to compute multiple failure probability is identical in both cases. Although different

Figure 5.3 Information Flow in Failure Analysis:
Lognormal Model



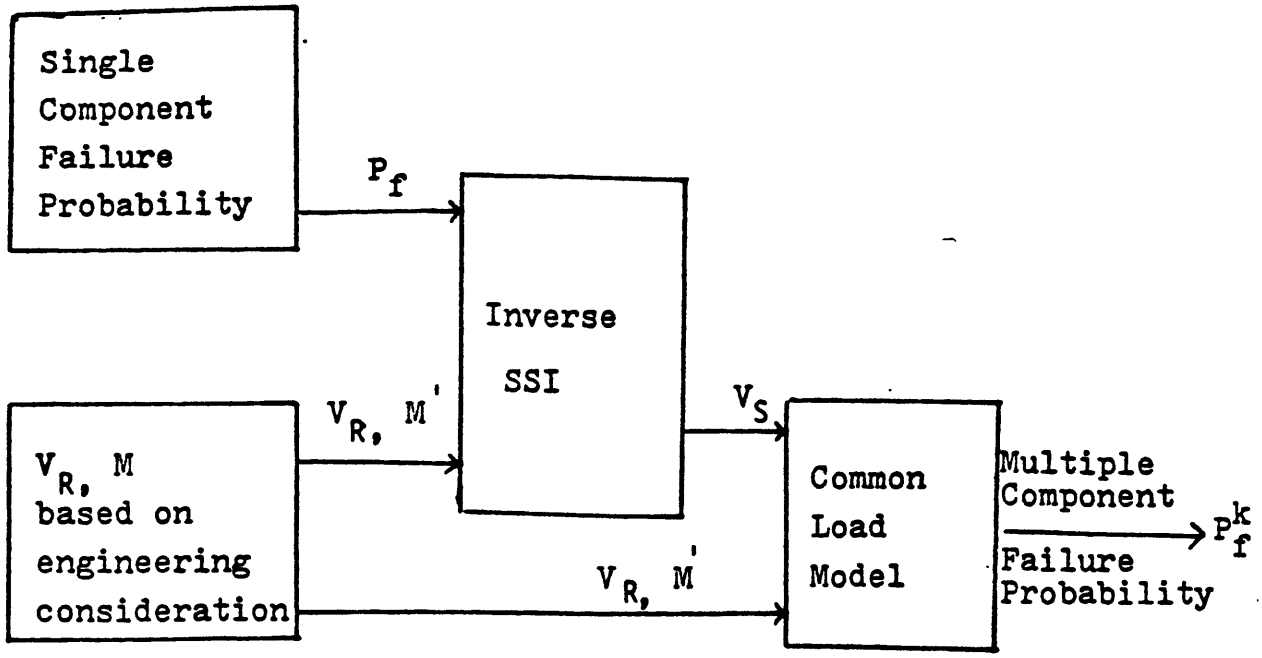
Ideal Situation



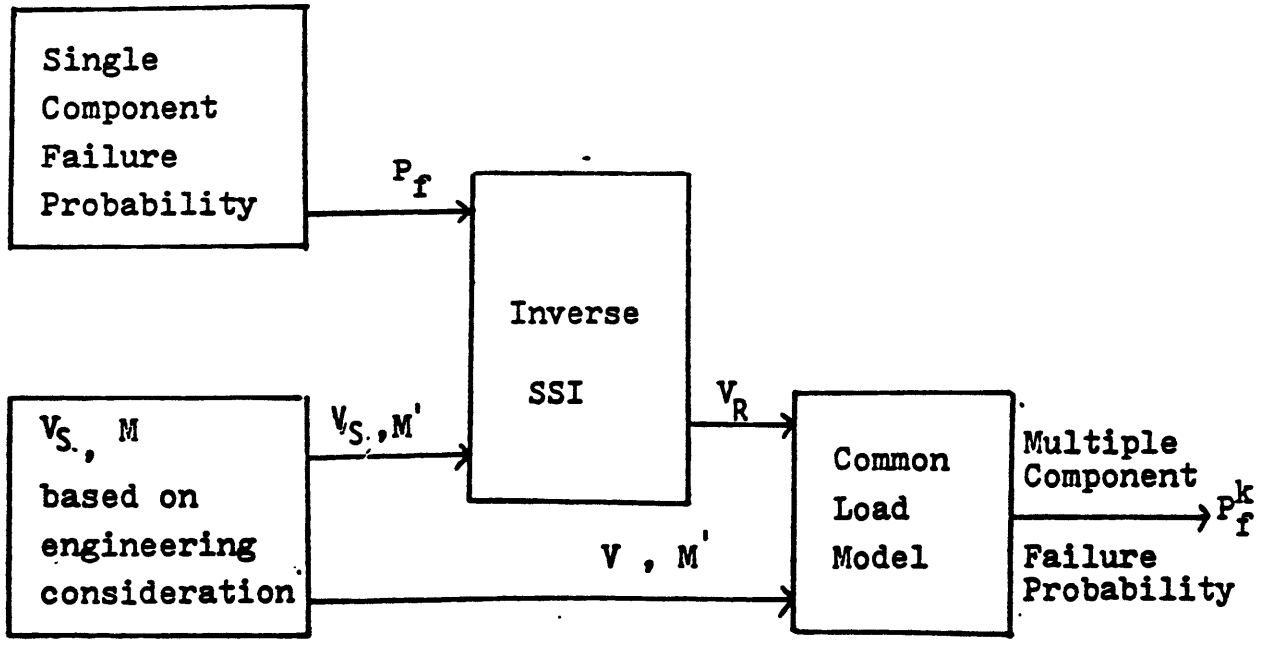
Inverse SSI, Case 1. V_R, V_S Given

Figure 5.3 (Continued)

Case 2. V_R, M' given



Case 3. V_S, M' given



parameters are involved in the information flow of two models, the ISSI method is applicable equally well. This can be said for other models not investigated in this work as well. If one can have a way to invert the SSI result for single component failure probability, it is then a straightforward matter to use common load model to compute multiple-component failure probability.

5.4 Mixed Models

It is of interest to study the in-between situations where stress is normally distributed and strength lognomally distributed or vice versa.

5.4.1 Normal-Lognormal Model

Suppose the stress is normally distributed and strength is lognormally distributed. By following the procedure used to derive normal model, one obtains the expression for multiple failure probability

$$P_f^k = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\, V_S} \exp\left[-\frac{1}{2}\left(\frac{x-1}{V_S}\right)^2\right] \left[\Phi\left(\frac{\ln x - M'}{V_R}\right)\right]^k dx \qquad (5.4.1)$$

where

$$M' = \ln \frac{\hat{\mu}_R}{\hat{\mu}_S}$$

By iterating the following expression, with known parameters and P_f substituted in,

$$P_f = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\, V_S} \exp\left[-\frac{1}{2}\left(\frac{x-1}{V_S}\right)^2\right] \left[\Phi\left(\frac{\ln x - M'}{V_R}\right)\right] dx \qquad (5.4.2)$$

one can find the unknown parameter. Then it is straightforward to use Eq. (5.4.1) to compute multiple failure probability. Since the steps are essentially the same as those in the normal model, with the addition of iteration, no further discussion is offered. A computer program is written to facilitate the procedure. Appendix A presents a listing of the program.

5.4.2 Lognormal-Normal Model

In this case, we assume that the stress is lognormally distributed, while the strength is normally distributed. By applying the procedure used to derive the normal model, one obtains the expression for multiple failure probability

$$P_f^k = \int_0^\infty \frac{1}{\sqrt{2\pi}\, V_S} \exp\left[-\frac{1}{2}\left(\frac{\ln x}{V_S}\right)^2\right] \left[\Phi\left(\frac{x-M}{V_R}\right)\right]^k dx \qquad (5.4.3)$$

where

$$M = \mu_R/\mu_S$$

By iterating the following expression, with known parameters and P_f substituted in,

$$P_f = \int_0^\infty \frac{1}{\sqrt{2\pi}\, V_S} \exp\left[-\frac{1}{2}\left(\frac{\ln x}{V_S}\right)^2\right] \left[\Phi\left(\frac{x-M}{V_R}\right)\right] dx \qquad (5.4.4)$$

one can find the unknown parameter. Then it is straightforward to use Eq. (5-4.3) to compute the multiple failure probability.

Since the steps are essentially the same as those in the normal model, with the addition of iteration, no further discussion is offered. A computer program is written to facilitate the procedure. Appendix A presents a listing of the program.

5.5 Some Qualitative Results

Since the expressions to compute multiple component failure probability are similar for both the normal and lognormal models, it is useful to discuss the results for normal model in detail. The trend observed in the normal model thus serves as a convenient framework for understanding the qualitative characteristics of other models.

5.5.1 Normal Model

5.5.1.1 V_R, V_S Given

A very interesting case arises when safety factor is approximately equal to one. This corresponds to a situation where a great deal of experience has been accumulated for similar designs of the the component so that large safety factor is unnecessary. In fact, it is engineer's desire to have as small safety factor as possible due to economic penalty considerations. When safety factor is close to one (e.g. say within 5 % or less), Eq. (4-3.8) reduces to

$$P_f = \Phi\left(-\frac{M-1}{\sqrt{V_R^2+V_S^2}}\right) \qquad (5\text{-}5.1)$$

Eq. (5-2.3) reduces to

$$P_f^k = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\, V_S} \exp\left[-\frac{1}{2}\left(\frac{x-1}{V_S}\right)^2\right] \left[\Phi\left(\frac{x-M}{V_R}\right)\right]^k dx \qquad (5\text{-}5.2)$$

By taking the inverse of Eq. (5-4.1), the expression for safety margin reduces to

$$\alpha = \frac{M-1}{\sqrt{V_S^2+V_R^2}} \qquad (5\text{-}5.3)$$

$$M = \alpha \sqrt{V_R^2 + V_S^2} + 1 \qquad (5\text{-}5.4)$$

Numerical studies on Eq. (5-4.2) indicates that the multiple failure probability, for a given single failure probability, depends strongly only on the ratio of V_R and V_S, not on individual values of V_R or V_S. This is shown in Table 5.1 and agrees with the results in Ref. 5.2.

As indicated in section 4.3, the larger the loading roughness (defined as V_S/V_R), the larger the multiple failure probability. Figures 5.4, 5.5, and 5.6 illustrate probabilty for double failure, triple failure, and quadruple failure respectively. If the single failure probability is larger, other conditions being the same, the multiple failure probability increases. This is consistent with common practices where active components have higher failure probability than passive ones. For example, it has been a 'rule-of- thumb' type usage to assume beta factor of 0.2 for

Table 5.1 Multiple Failure Probability for Safety Factor Close to 1

Single Failure Probability	c	V_S	MDFF k=2	MDFF k=3	MDFF k=4
P_f=1.0E-3	0.2	=1.0	6.4E-1	5.1E-1	4.4E-1
		=0.1	6.4E-1	5.1E-1	4.4E-1
		=0.01	6.4E-1	5.1E-1	4.4E-1
		=0.001	6.4E-1	5.1E-1	4.4E-1
	2.0	=1.0	6.9E-3	1.5E-4	7.0E-6
		=0.1	6.9E-3	1.5E-4	7.0E-6
		=0.01	6.9E-3	1.5E-4	7.0E-6
		=0.001	6.9E-3	1.5E-4	7.0E-6
P_f=1.0E-4	1.0	=1.0	2.3E-2	2.5E-3	5.5E-4
		=0.1	2.3E-2	2.5E-3	5.5E-4
		=0.01	2.3E-2	2.5E-3	5.5E-4
		=0.001	2.3E-2	2.6E-3	5.6E-4
	0.1	=1.0	7.8E-1	6.9E-1	6.4E-1
		=0.1	7.8E-1	6.9E-1	6.4E-1
		=0.01	7.8E-1	6.9E-1	6.4E-1
		=0.001	7.8E-1	6.9E-1	6.4E-1
P_f=1.0E-6	2.0	=1.0	6.2E-5	4.3E-8	1.4E-10
		=0.1	6.2E-5	4.3E-8	1.4E-10
		=0.01	6.2E-5	4.3E-8	1.4E-10
		=0.001	6.2E-5	4.3E-8	1.4E-10
	0.2	=1.0	4.9E-1	3.5E-1	2.8E-1
		=0.1	4.9E-1	3.5E-1	2.8E-1
		=0.01	4.9E-1	3.5E-1	2.8E-1
		=0.001	4.9E-1	3.5E-1	2.8E-1

MDFF= Multiple Dependent Failure Fraction

P_f : single component failure probability

V_S : coefficient of variation of stress

c : V_R/V_S

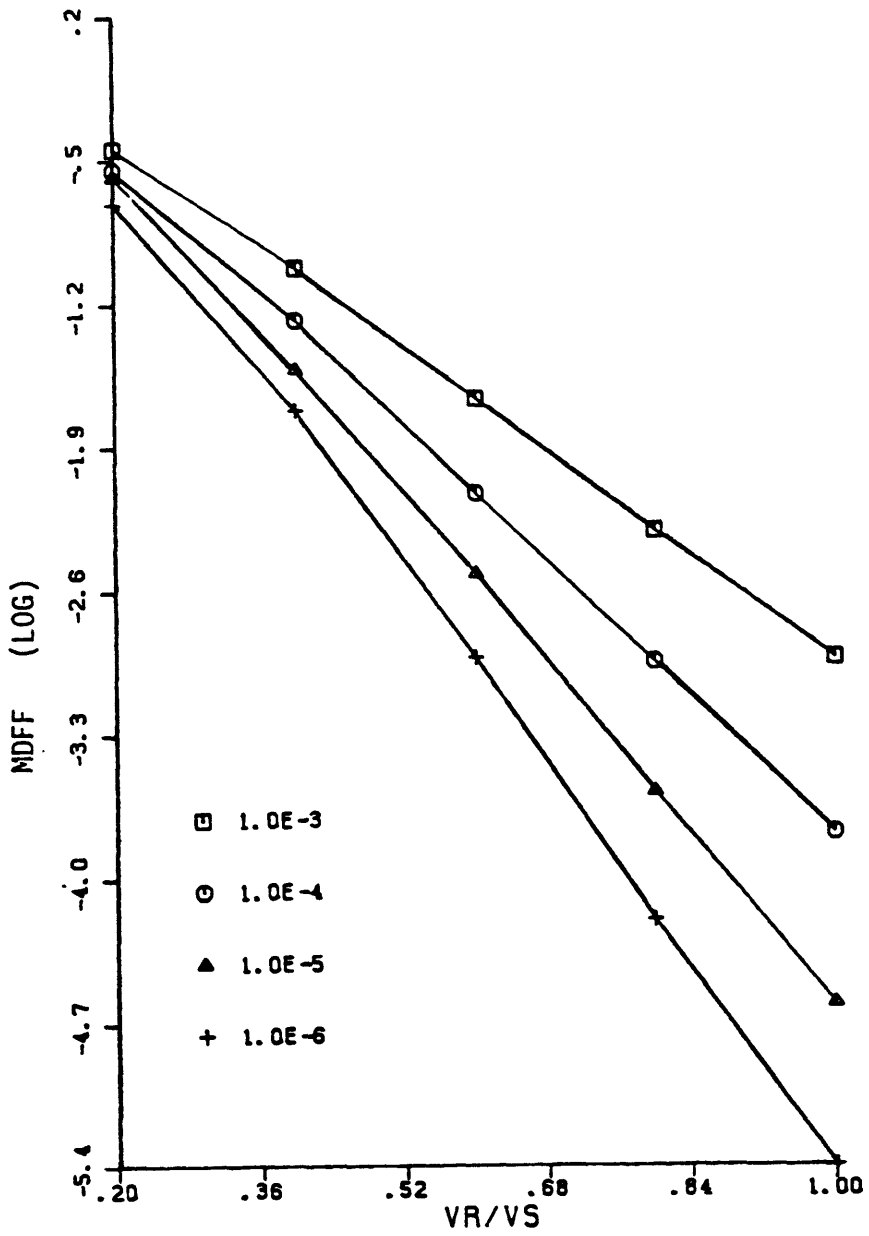


Figure 5.4 MDFF(k=2) Based on the ISSI Technique (Approximate) for Various Single Failure Probabilities

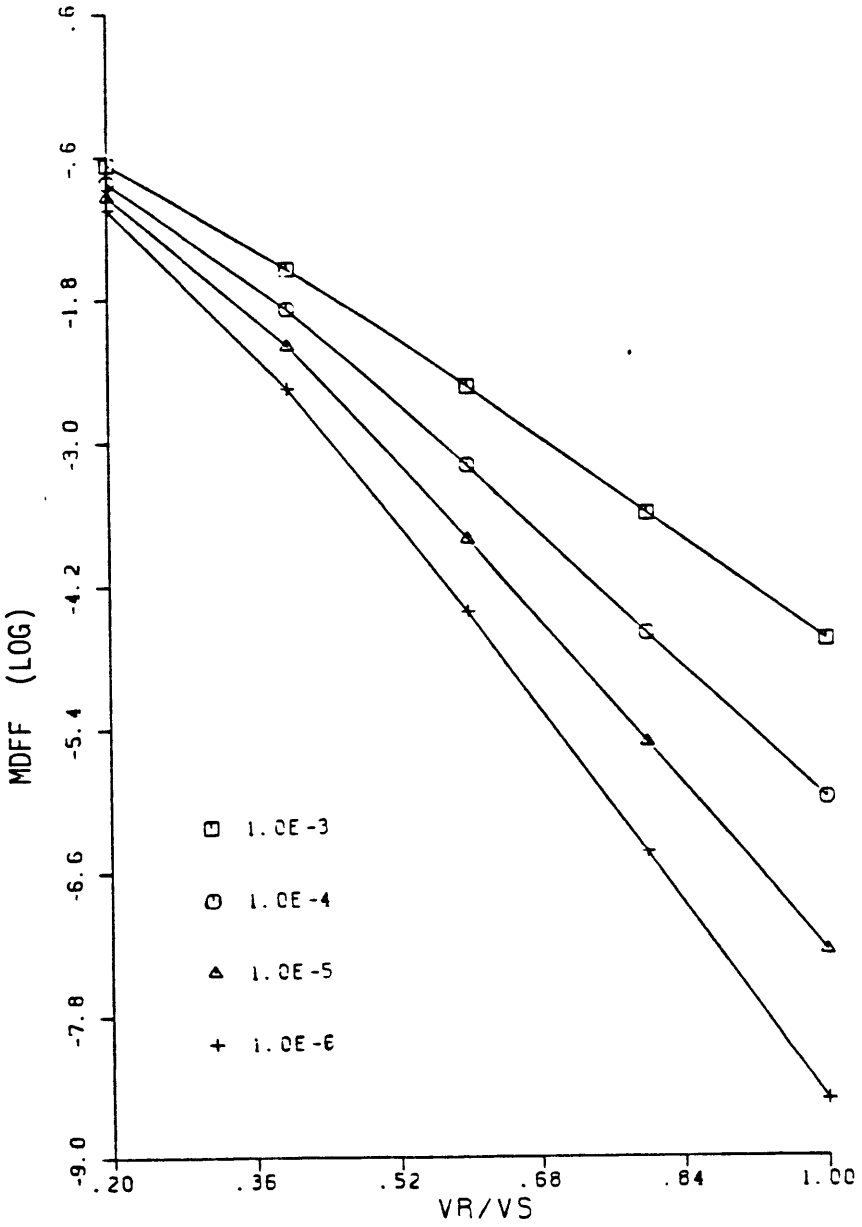


Figure 5.5 MDFF(k=3) Based on the ISSI Technique (Approximate) for Various Single Failure Probabilities

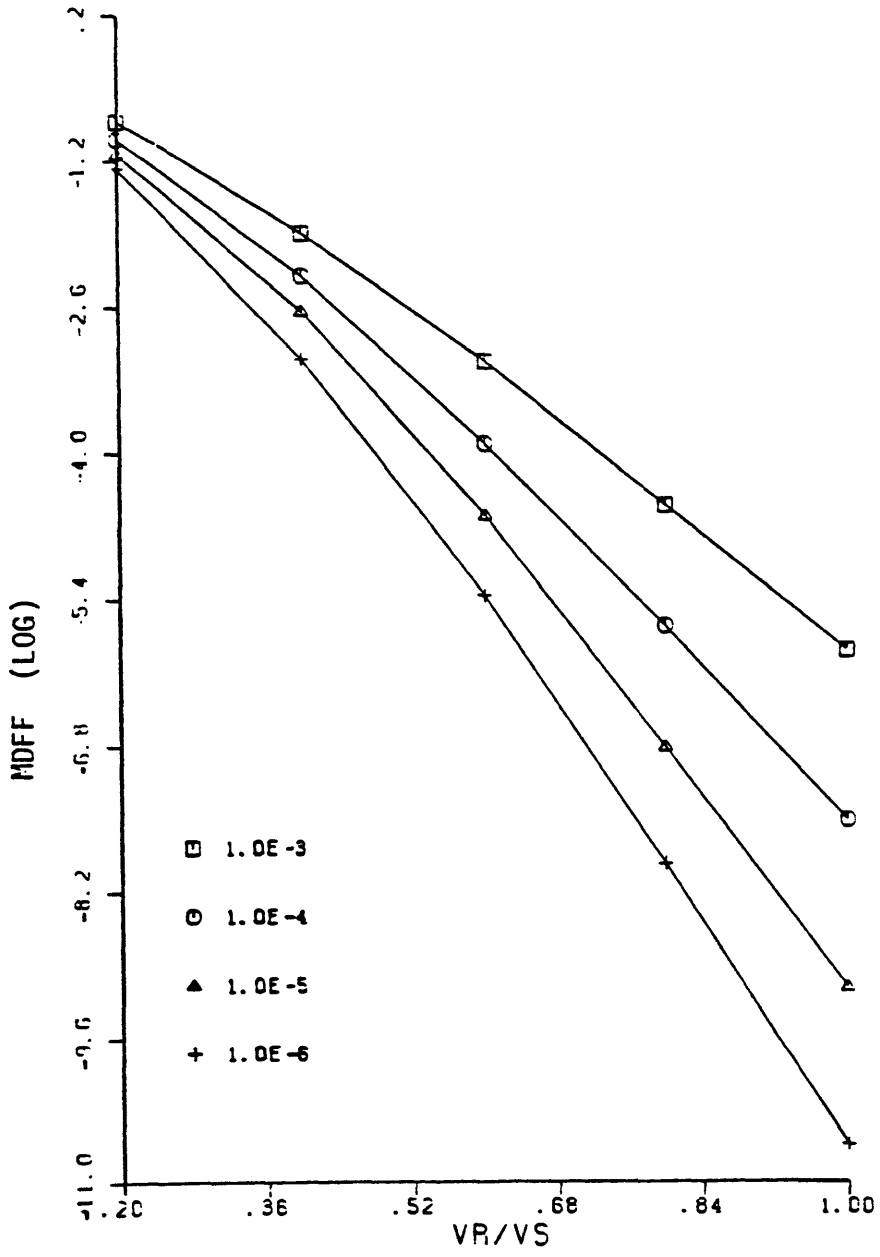


Figure 5.6 MDFF(k=4) Based on the ISSI Technique (Approximate) for Various Single Failure Probabilities

active components (e.g. pumps), and 0.1 for passive components (e.g. valves). In the general case where safety factor is not assumed to be close to one, the similar trend for the ratio of V_R and V_S still holds. However, the larger the values of the V_R and V_S, the smaller the multiple failure probability. Figures 5.7, 5.8 and 5.9 illustrate multiple failure probability for the cases of K=2, 3, and 4 respectively. It is noted that Figures 5.4-5.9 are based on the value of V_R equal to 0.03, a typical engineering situation. Studies for other values of V_R indicate similar trend. This shows that the above qualitative characteristics are generally valid.

5.5.1.2 V_R, M Given

To get some insight into the behavior of multiple failure probabilities, the qualitative trends outlined below are useful to keep in mind:

1. For a given safety factor and single failure probability, the larger the coefficient of variation of strength, the smaller the coefficient of variation of stress. This follows readily from Eq. (5-2.4). Since multiple failure probabilities are smaller, when V_R/V_S is larger, one gets smaller failure probabilities for this case. For example, as shown in Table 5.2, the multiple failure probabilities associated with V_R equal to 0.05 are smaller than those associated with V_R equal to 0.035.

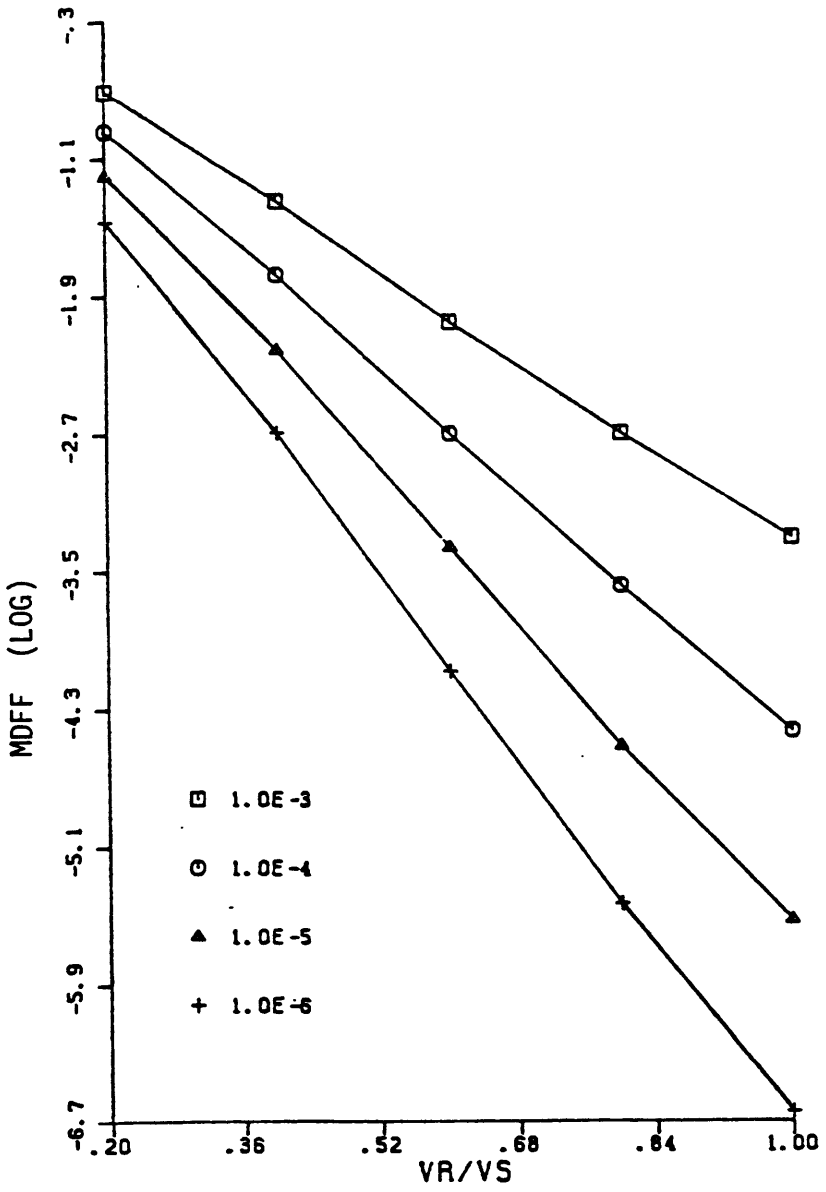


Figure 5.7 ISSI Results: V_R, V_S Given k equal to 2

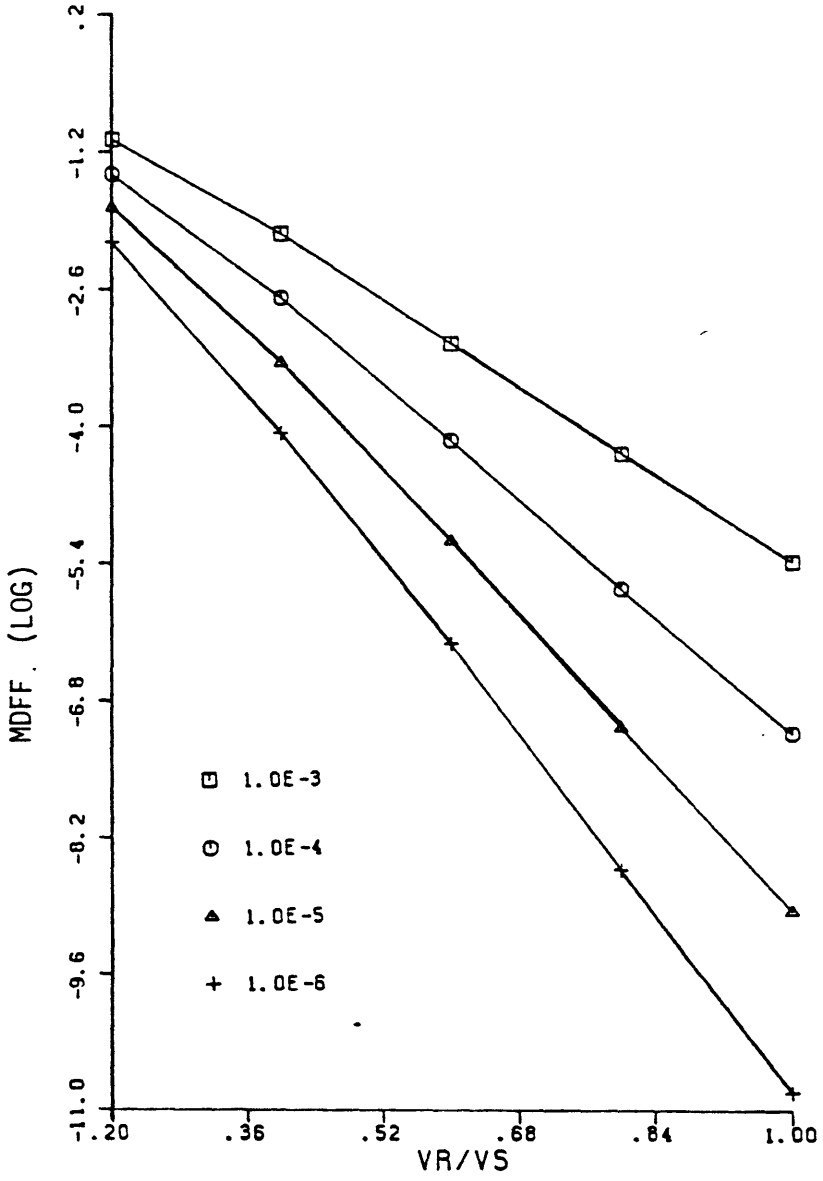


Figure 5.8 ISSI Results: V_R, V_S Given k equal to 3

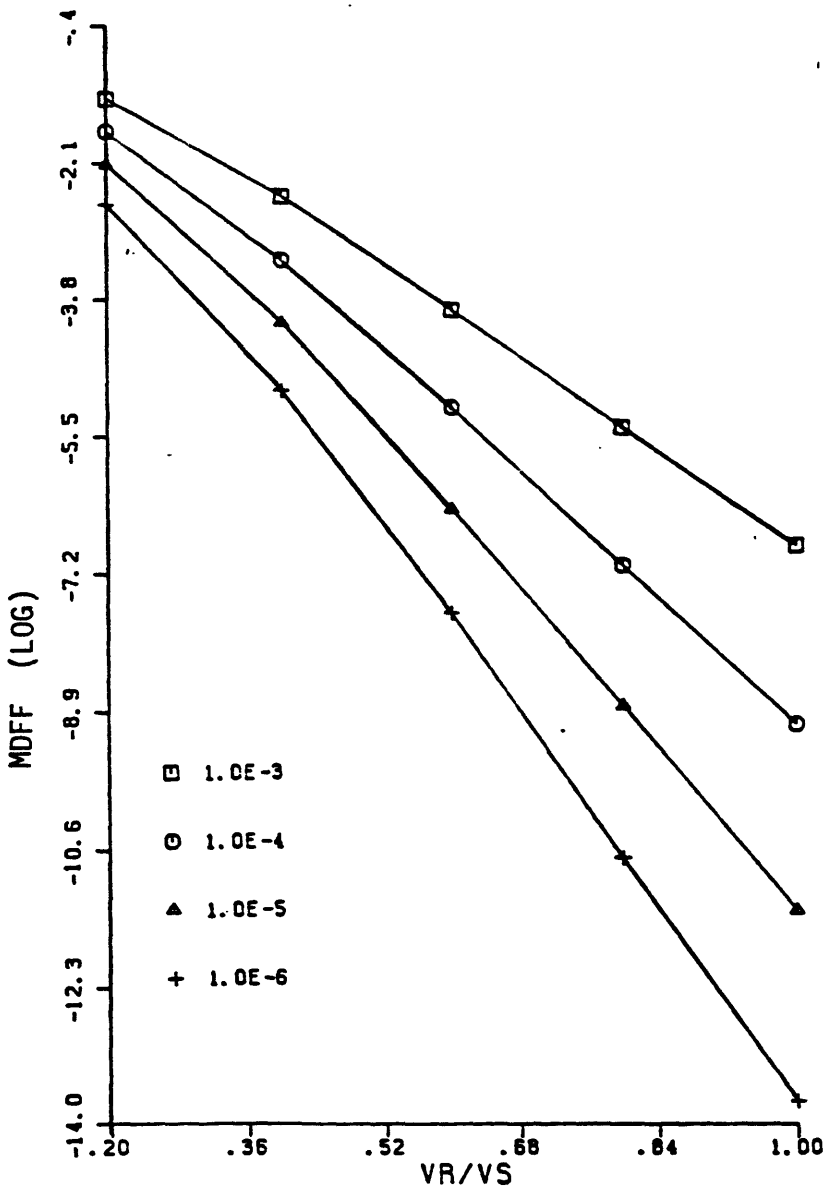


Figure 5.9 ISSI Results: V_R, V_S Given k equal to 4

Table 5.2 ISSI Calculation, V_R And M Known

Parameter Values	Multiple Failure Probability		
P_f, M, V_R	k=2	k=3	k=4
P_f = 1.0E-5			
M=2.0 V_R=0.05	1.6E-6	6.3E-7	3.5E-7
M=2.0 V_R=0.035	3.3E-6	1.9E-6	1.4E-6
M=3.0 V_R=0.05	3.0E-6	1.6E-6	1.1E-6
M=3.0 V_R=0.035	4.4E-6	3.0E-6	2.3E-6
P_f = 1.0E-3			
M=2.0 V_R=0.05	4.5E-4	3.0E-4	2.3E-4
M=2.0 V_R=0.035	5.8E-4	4.4E-4	3.7E-4
M=3.0 V_R=0.05	5.1E-4	3.7E-4	3.0E-4
M=3.0 V_R=0.035	5.2E-4	4.1E-4	3.4E-4

2. For a given V_R and single failure probability, the larger the safety factor, the larger the multiple failure probabilities. For example, in Table 5.2, for V_R = 0.05, multiple failure probabilities associated with safety factor of 3 are larger than those for safety factor of 2.

3. For a given V_R and safety factor, the larger the single failure probability, the larger the multiple failure probabilities. In addition, the MDFFs are also larger accordingly. In Table 5.2, f_2=0.45 for P_f =1.0E-3 is larger than f_2=0.16 for P_f =1.0E-5, with safety factor of 2 and V_R = 0.05 in both cases.

5.5.1.3 V_S, M Given

The following general trends summarize the calculation based on the ISSI method:

1. For a given safety factor and single failure probability, the larger the coefficient of variation of stress, the smaller the coefficient of variation of strength. This follows readily from Eq. (5-2.5). When is larger, the associated multiple failure probabilities are larger. In all cases shown in Table 5.3 this trend is evidenced.

2. For a given V_S and single failure probability, the larger the safety factor the smaller the multiple failure probabilities. This is just the opposite to the trend observed in case 2. For example, in Table 5.3, for V_S = 0.05, multiple failure probabilities associated with safety

Table 5.3 ISSI Calculation, V_S And M Known

Parameter Values	Multiple Failure Probability		
P_f, M, V_S	k=2	k=3	k=4
P_f = 1.0E-5			
M=1.3 V_S=0.06	7.6E-7	2.0E-7	8.5E-8
M=1.3 V_S=0.05	1.0E-7	7.7E-9	1.3E-9
M=1.4 V_S=0.06	4.0E-8	1.3E-9	1.2E-10
M=1.4 V_S=0.05	9.2E-9	7.4E-6	2.0E-7
M=2.0 V_S=0.20	7.6E-7	2.0E-7	8.5E-8
M=2.0 V_S=0.15	4.0E-8	1.3E-9	1.2E-10
P_f = 1.0E-6			
M=2.0 V_S=0.20	2.7E-7	1.4E-7	9.3E-8
M=2.0 V_S=0.15	5.0E-9	2.4E-10	3.0E-11

factor of 1.4 are smaller than those for safety factor of 1.3.

3. For a given V_S and safety factor, the larger the single failure probability the larger the multiple failure probabilities. However, unlike case 2, the MDFFs are smaller due to increased value of V_R/V_S. This comes about because in Eq. (5-2.5), α is smaller for larger P_f. Consequently, V_R is larger and MDFFs are smaller. In Table 5.3,

f_2 = 4.0E-3, for P_f = 1.0E-5

f_2 = 5.0E-3, for P_f = 1.0E-6

with M = 2, V_S = 0.15 in both cases.

5.5.2 Lognomal Models

As described previously in sections 5.3 and 4.3, the equations to compute multiple failure probability is essentially the same as those for the normal model. The qualitative behavior of the final results is thus expected to be similar in both cases. However, one major difference is worth noting. Other conditions being the same, the lognomal model yields a slightly higher value of multiple failure probability. The multiple failure probability for a typical calculation for normal and lognormal models is showm in Table 5.4. Although the scoping studies are by no means exhaustive, they do indicate a consistent trend within the ranges studied. The results suggests that the normal and lognormal models differ within a factor of ten in the multiple failure probability. For stronger dependence

Table 5.4 Typical ISSI Results for Normal and Lognormal Models

Stress	Strength	k=2	k=3	k=4
Normal	Normal			
	V_R/V_S =1.0	1.2E-6	8.0E-8	1.1E-8
	=0.8	2.8E-6	3.5E-7	8.5E-8
	=0.6	6.7E-6	1.6E-6	6.3E-7
	=0.4	1.6E-5	7.2E-6	4.2E-6
	=0.2	3.9E-5	2.4E-5	1.8E-5
Lognormal	Lognormal			
	V_R/V_S =1.0	2.3E-6	2.6E-7	6.3E-8
	=0.8	5.3E-6	1.0E-6	3.5E-7
	=0.6	1.2E-5	4.1E-6	2.0E-6
	=0.4	2.8E-5	1.5E-5	9.9E-6
	=0.2	5.8E-5	4.4E-5	3.7E-5

$V_R = 0.03$, $P_f = 1.0E-4$

between identical components, the difference is smaller. On the other hand, if the redundancy is high, the results show a larger difference.

5.5.3 Mixed Models

In the real world, it is also likely that the true state-of-affairs lies in betwwen the normal and lognormal models. It is thus of interest to study the mixed model to see what the implications of different models.

5.5.3.1 Normal-Lognormal Model

This refers to a situation where the stress is normally distributed while the strength is lognormally distributed. There is no simple inversion formula for this case. This stems from the fact that algebraic combination of normal and lognormal random variables are not normal or lognormal. To apply the ISSI technique, an iteration is needed to find the relatioship between stress-strength parameters. For typical engineering situations, the sensitivity studies performed indicate the multiple failure probability based on this model is between that based on normal and lognormal models described previously.

5.5.3.2 Lognormal-Normal Model

In this case the stress is lognomally distributed, while the strength is normally distributed. As in the normal-lognormal model, an iteration is required to invert the single component failure probability. Sensitivity

studies performed show that this model gives lower values for multiple failure probability than lognomal models but higher values than normal and normal-lognormal models. Figures 5.10,5.11 and 5.12 compares the multiple failure probability(for k=2, 3 and 4 respectively) based on different combinations of normal and lognormal models as stress and strength distributions.

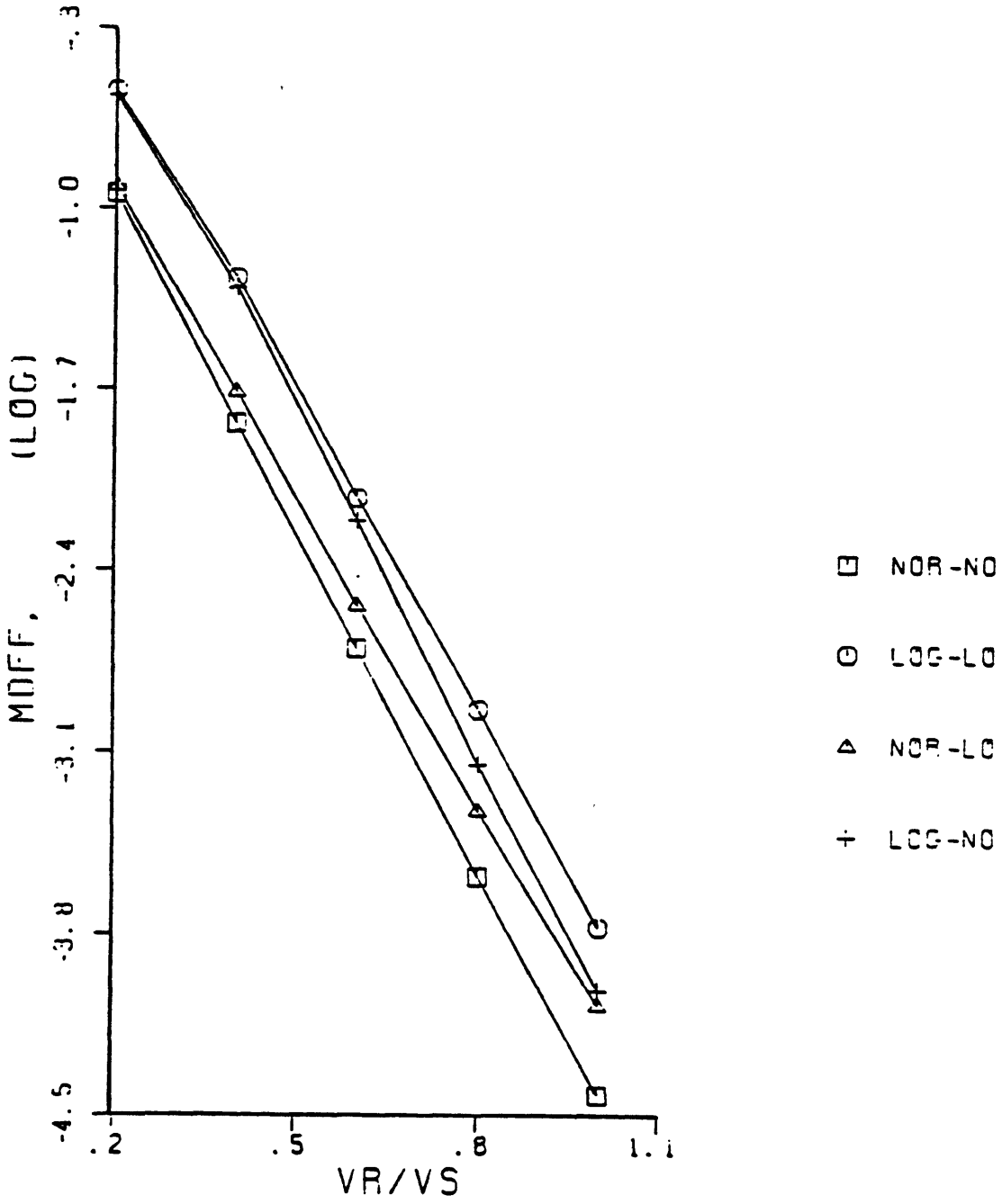


Figure 5.10 Comparison of MDFF for Different Models
(k Equal to 2)

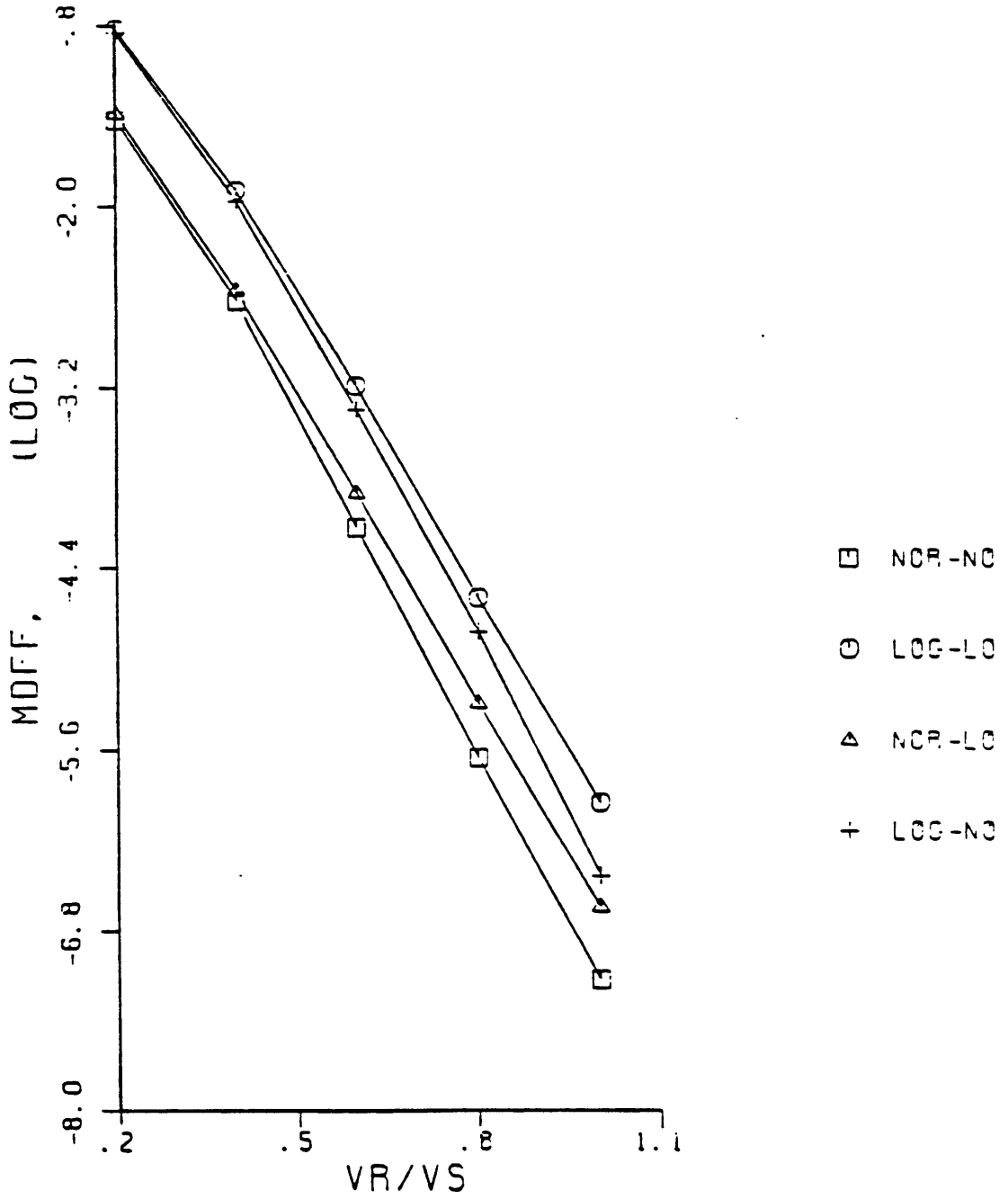


Figure 5.11 Comparison of MDFF for Different Models
(k Equal to 3)

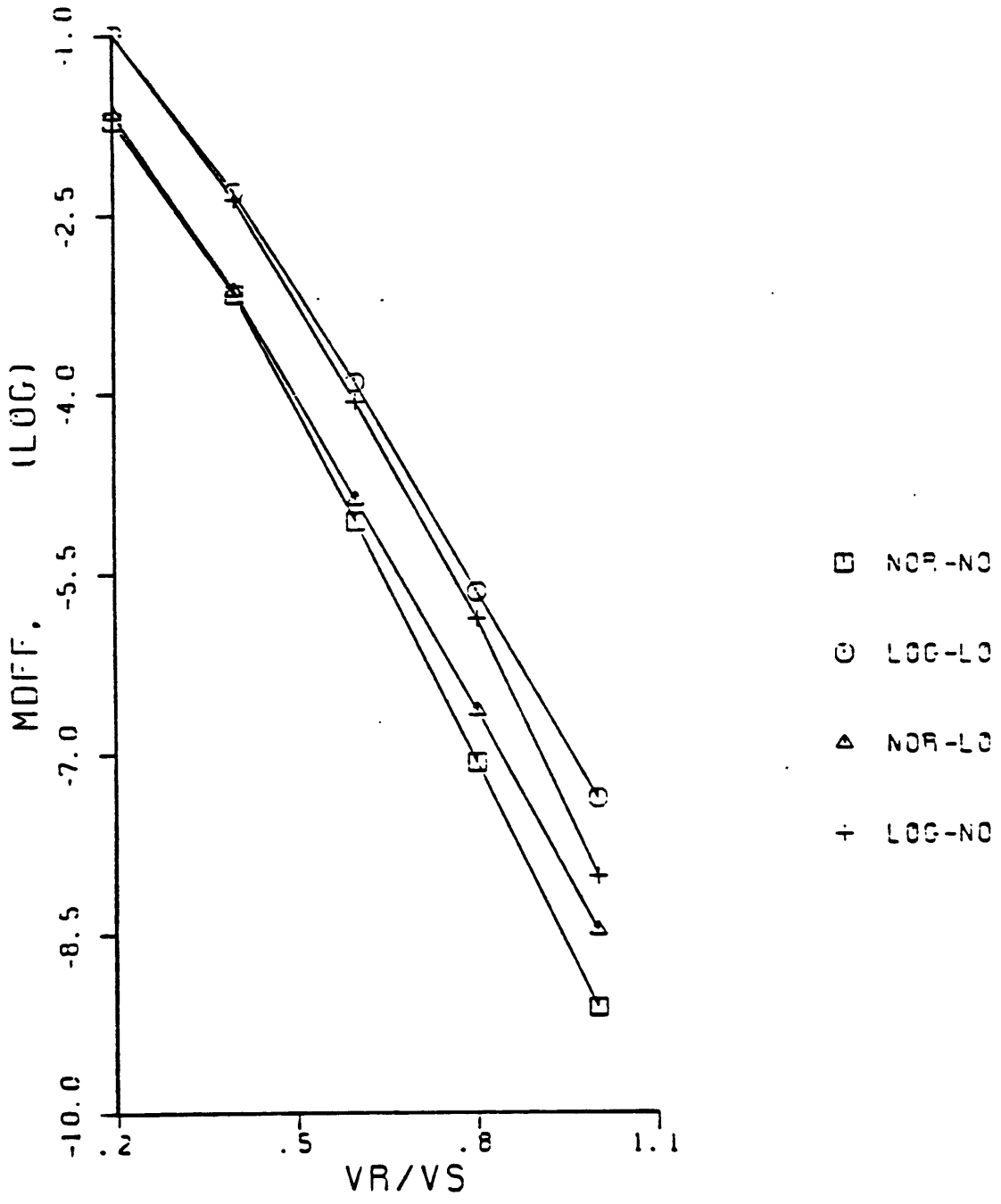


Figure 5.12 Comparison of MDFF for Different Models
(k Equal to 4)

5.6 Estimating CCF Parameters with the ISSI Method

It has been illustrated the ISSI method provides a way to estimate CCF probabilities within a mission time. In addition, it also can be used to estimate parameters in the other CCF modelling such as MDFF and MGLM.

It was pointed out in Chapter 3 that more study is required to obtain the parameters in either MDFF model or MGLM. Since three or more parameters are to be estimated, it is hardly possible to collect sufficient data within the useful life of the component for statistical analysis to be significant. In addition, the new changes and improvements in design tends to make historical data obsolete. Only the ISSI method seems less susceptible to these difficulties. It partially overcomes these barriers by providing a framework such that explicit engineering considerations are embedded.

The relationship between the results of the ISSI approach (i.e. common load model fortified with the inversion of SSI formalism), the parameters in both MDFF method and MGLM are shown in Table 5.5 By following the procedure of the ISSI method, multiple failure probability can be computed. It is then straightforward to use the expressions derived in Table 5.5 to evaluate f_k for MDFF, and β, γ and δ for MGLM. The time-dependent multiple failure probability can then be calculated based on Markov models as derived in chapter 3.

Table 5.5 Relationship Between ISSI Results, MDFF And MGLM

a. ISSI Results

V_R, V_S, or M quantified by engineering considerations

$$p_f^k = \int_{-\infty}^{\infty} f_s(x)[F_R(x)]^k \, dx$$

p_f^k = simulaneous k-component failure probability, k=2,3,4

b. MDFF

$f_k \equiv$ fraction of time failure is due to k component failure, k=2,3,4

$$f_k = \frac{p_f^k}{p_f}$$

p_f = single component failure probability

c. MGLM

four-unit system

$$\beta = \frac{3p_f^2 + 3p_f^3 + p_f^4}{p_f + 3p_f^2 + 3p_f^3 + p_f^4} = \frac{3f_2 + 3f_3 + f_4}{1 + 3f_2 + 3f_3 + f_4}$$

$$\gamma = \frac{3p_f^3 + p_f^4}{3p_f^2 + 3p_f^3 + p_f^4} = \frac{3f_3 + f_4}{3f_2 + 3f_3 + f_4}$$

$$\delta = \frac{p_f^3}{3p_f^3 + p_f^4} = \frac{f_4}{3f_3 + f_4}$$

three-unit system

$$\beta = \frac{p_f^2 + p_f^3}{p_f} = f_2 + f_3$$

$$\gamma = \frac{p_f^3}{p_f^2 + p_f^3} = \frac{f_3}{f_2 + f_3}$$

Chapter 6

Application of the ISSI Method to Pumps and Valves in Nuclear Power Plants

6.1 Introduction

In this chapter, the quantification of multiple dependent failure fractions of common pumps and valves in nuclear power plants is performed to illustrate an application of the ISSI method discussed in Chapter 5. To avoid confusion, the following set of definitions is adopted throughout the following discussion.

Failure Mode

This is used to describe the manner in which a component ceases to perform its intended function. The term is also loosely used to describe certain failure phenomenon. If more than one components fails in the same mode, one might say common mode failures occur.

Failure Cause

This is used to describe an identified condition, event, or cause that prevented the component from performing its intended function. The term usually covers a broad range of situations. Its definite meaning depends on the perspectives of the analyst.

Failure Mechanism

This refers to any physical modelling of a failure mode or a failure cause. In the framework of SSI theory, the failure model says that if the "stress"

associated with the failure exceeds the "strength" failure will occur. For example, the failure mechanism associated with tribological causes is the force existing between surfaces in relative motion and the corresponding resistance of the material to withstand this surface stress.

In essence, the procedure to compute multiple failure probability consists of the following steps:

1. Identification Of Failure Causes

   LER is used to select applicable failure causes. The failure causes thus selected are treated as the potential common causes. This approach is different from the usual statistical analysis of historical data where only actual occurences of multiple failures are considered. The potential failure causes are implicitly ignored since LER does not record such occurences. This is unrealistic and gives an incomplete analysis of CCF. The ISSI method provides a handy vehicle to account for potential failure causes.

2. Identification Of Failure Mode

   Since the failure causes classified from LERs are not in an appropriate form to apply ISSI method, a study of LER one-line description of events is necessary to identify failure modes for a particular failure cause. In addition, the failure cause identified in LER in step 1 is sometimes too broad. It is useful under such circumstances to resolve the broad classification into

more specific causes to allow for physical analysis.

3. Aggregation Of Failure Modes

   The failure modes identified in step 2 usually have underlying failure phenomena associated with them. It is important to aggregate those failure causes having similar physical processes into a group.

   For each aggregation, a set of "stress" and "strength" parameter is identified from engineering knowledge.

4. Selection and Quantification of "Stress" and "Strength"

   It is assumed that for each aggregation there is a set of material property (i.e. "strength" and "stress") that describes the behavior of failure mechanism as stated in the previous step. The selection and quantification of these parameters requires knowledge from laboratory testing of material performance to simulate field behavior.

5. Computation of CCF Probabilities by the ISSI Method

   The formalism discussed in Chapter 5 is then used to calculate the failure probabilities of different multiplicity.

Section 6.2 surveys general mechanical failure modes and indicates sailient features of some of the important and pertinent underlying mechanisms.

Section 6.3 describes the application to pumps in HPIS and AFWS. The LER classification of failure is first discussed. Then interpretation based on the study of one-line event description is presented. The procedure described previously

is illustrated in more detail.

Section 6.4 presents the application to motor-operated valves in both HPIS and AFWS. In addition, check valves are also analyzed in a similar fashion. It is found that the failure behavior of pumps and valves are similar, except that pumps have higher failure probability for all levels of multiplicity. This is in agreement with the fact that pumps have more moving parts than valves.

Section 6.5 compares the results of estimates of CCF probability based on different approaches. Both the point values and the uncertainty bounds are presented. It seems that the ISSI method generally yields slightly higher failure probability than BFR and coupling method. Also, the uncertainty bounds are tightest for the results of ISSI method. Possible explanations are discussed to shed insight on the difference between the statistical approach and that incorporating engineering knowledge.

6.2 General Discussion Of Mechanical Failures

Mechanical failures may be defined as any change in size, shape or material properties of a machine, or machine part that renders it incapable of satisfactorily performing its intended function. With this definition, one might define failure mode as the physical process or processes that take place or combine their effects to produce failure.

A systematic classification has been devised by which all possible failure modes could be predicted {6.13}. Such a

classification is based on defining three categories:

(1) Manifestations of failure

(2) Failure-inducing agent

(3) Locations of failure

Each specific failure mode is then identified as a combination of one or more manifestations of failure together with one or more failure-inducing agents and a failure location.

The four manifestations of failure, some with subcategories are:

1. Elastic deformation
2. Plastic deformation
3. Rupture or fracture
4. Material change
   a. Metallugical
   b. Chemical
   c. Nuclear

The four failure-inducing agents, each with subcatogories, are:

1. Force
   a. Steady
   b. Transient
   C. Cyclic
   d. Random
2. Time
   a. Very short
   b. Short
   c. Long

3. Temperature
   a. Low
   b. Room
   c. Elevated
   d. Steady
   e. Transient
   f. Cyclic
   g. Random
4. Reactive Environmemt
   a. Chemical
   b. Nuclear

The two failure locations are:

1. Body type
2. Surface type

To be precise in describing a specific mode of failure, it is necessary to select appropriate categories for the above list without omitting any of the three major categories.

Table 6.1 lists some of the failure modes that have been identified as most frequently observed in common mechanical components. It serves as a guideline in the design, analysis or prevention against potential failure modes in mechanical components. Note that not all failure modes listed in Table 6.1 are mutually exclusive. Several failure modes are combinations of two or more modes. {6.1}

A brief glossary {6.1,6.2,6.3} describing those failure modes that are relevant for the present application is

Table 6.1 Common Failure Modes for Mechanical Components (Ref. 6.1)

1. Elastic deformation
2. Yielding
3. Brinelling
4. Ductile failure
5. Brittle fracture
6. Fatigue
   a. High-cycle fatigue
   b. Low-cycle fatigue
   c. Thermal fatigue
   d. Surface fatigue
   e. Impact fatigue
   f. Corrosion fatigue
   g. Fretting fatigue
7. Corrosion
   a. Direct chemical attack
   b. Galvanic corrosion
   c. Crevice corrosion
   d. Pitting corrosion
   e. Intergranular corrosion
   f. Selective leaching
   g. Erosion-corrosion
   h. Cavitation
   i. Hydrogen damage
   j. Biological corrosion
   k. Stress corrosion
8. Wear
   a. Adhesive wear
   b. Abrasive wear
   c. Corrosive wear
   d. Surface fatigue wear
   e. Deformation wear
   f. Impact wear
   g. Fretting wear
9. Impact
   a. Impact fracture
   b. Impact deformation
   c. Impact wear
   d. Impact fretting
   e. Impact fatigue
10. Fretting
    a. Fretting fatigue
    b. Fretting wear
    c. Fretting corrosion
11. Galling and seizure
12. Scoring
13. Creep
14. Stress rupture
15. Thermal shock
16. Thermal relaxation
17. Combined creep and fatigue
18. Buckling
19. Creep buckling
20. Oxidation
21. Radiation damage
22. Bonding failure
23. Delamination
24. Erosion

presented below. For a more complete discussion on these failure modes, Ref. 6.1 is a good source of information.

1. Elastic deformation

   For a component or part subject to force and/or temperature related loads, within the elastic range of the material property, the elastic deformation occurs. If the deformation becomes great enough to interfere with the ability of the machine satisfactorily performing its intended function, failure occurs.

2. Yielding

   When the plastic (unrecoverable) deformation in a ductile machine member, brought about by the imposed operational loads or motions, becomes great enough to interfere with the ability of the machine to perform its intended function, failure occurs. Common design based on the American Soceity of Mechanical Engineers (ASME) codes takes both elastic deformation and yielding into account.

3. Brinneling

   This refers to the permanent surface discontinuity of significant size produced by the static forces between two curved surfaces in contact which result in local yielding of one or both mating members. For example, if a ball bearing is statically loaded so that a ball is forced to permanently indent the race through local plastic flow, the race is brinelled.

Subsequent operation of the bearing might result in intolerably increased vibration, noise and heating.

4. Fatigue

This is a general term given to the sudden and catastrophic separation of a machine part into two or more pieces as a result of the application of fluctuating loads or deformation over a period of time. Variables that are found to affect the fatigue life {6.3} include the effects of stress or strain amplitude, mean stress, combined stress, various stress histories, the speed of testing, hardness, metallurgical structure, level and distribution of impurities, the surface condition, and environmental variables such as temperature, humidity, or special combination. It is noted that fatigue data obtained with poorly controlled geometry and finishes on the specimen can be very misleading. By the same token, real applications, with their lack of laboratory control, can exhibit very wide variations in life. Many types of fatigue exist as shown in Table 6.1.

5. Corrosion

The term describes undesired deterioration of the material as a result of chemical or electrochemical interaction with the environment. Corrosion often interacts with other failure modes such as wear or fatigue. As in the case of fatigue, many forms of corrosion exist as shown in Table 6.1.

6. Wear

Surface interactions give rise to a number of important macroscopic phenomena, the main ones being friction and wear. Wear is the undesired cumulative change in dimensions brought about by the gradual removal of discrete particles from contacting surfaces in motion predominantly as a result of mechanical action. Wear is not a single process, but a number of different processes that can take place independently or in combination, resulting in material removal from contacting surfaces through a complex combination of local shearing, plowing, gouging, welding, tearing, and others. Wear rates are proportional to the load, the distance slid, and inversely proportional to the hardness.

From the standpoint of CCFA, the above failure modes represent common cause candidates to be screened from LER.

Evaluation of either failures or abnormal occurrences in light water reactor (LWR) coolant systems indicate that valves and pumps are significant contributors {6.4}. The next two sections of chapter 6 present the application of ISSI method to pumps and valves.

6.3 Application To Pumps

Since the present study focuses on PRA applications, safety systems are of major interest. The HPIS and AFWS are examples of important safety systems and are analyzed in this section.

6.3.1 HPIS pumps

In applying the ISSI technique to evaluate CCF probabilities, the first step is to estimate single failure probability. The approach used is to take the estimates from the LER based on the BFR model.

Median values are used. Doubtlessly, there is uncertainty associated with median values. The robustness of medians with respect to outliers does not introduce large error in ignoring the variation of median.

The next step involves identifying failure causes as coded in one-line description of LERs. Table 6.2 lists a classification scheme used in LER {6.6} for Westinghouse designed plants. There are several weaknesses associated with the coding used in Table 6.2. These include:

1. The decomposition is useful to get a feel for general behavior for different parts, but tends to be vague. It does not recognize the nature of failure.
2. Some of the failure causes are not mutually exclusive. For example, it is obvious that bearing or seal failures belong to the category of failed internals too.
3. The classification is not in the appropriate form for

Table 6.2 LER HPIS Pump Failure Classification

Failure Cause	Number of Failures
Unknown	3
Personnel (Operation)	1
Personnel (Maintenance)	3
Personnel (Testing)	1
Design Error	1
Improper Clearances	1
Extreme Environment	3
Bearing	1
Mechanical Control Parts Failures	13
Failed Internals	4
Foreign Material Contamination	1
Loss Of Pressure Boundary	1
TOTAL	33

the application of SSI theory.

Upon further investigations into one-line LER description of each occurrence, it is possible to identify four major categories of causes that underlie all failure occurrences. This is shown in Table 6.3.

It can be seen that tribological causes contributes most to the HPIS pump failures. Seal leakage, bearing failures, failed internals, shaft breakage, improper clearances and air leakages are included in this category. The rationale behind this classification is the following :

1. Tribology is the least attended and most uncertain area of technology for design engineers. In the design of mechanical components, engineers have so far focused on the traditional stress analysis of components. The ASME pressure vessel and boiler code addresses only the structural integrity and does not take wear into account. In a sense, wear is thus 'designed' into the mechanical components or systems by this negligence.
2. Seals, bearing, shafts and other pump internals are the parts in constant rubbing motion. Their most likely failure mode is thus wear. Improper clearance or lubrication affects the wear behavior strongly. Thus they are in the same group of tribology-related causes.

Foreign material contamination refers to undesirable dust or sticky material on parts that are left in a place without attention to cleanliness. Electrical and electronic parts

Table 6.3 HPIS Pump Failure Reclassification

Failure Cause	Number of Failures
I. Tribological Failures	10
Seal	1
Bearing	1
Shaft	1
Failed Internals	4
Mechanical Binding	1
Improper Clearances	1
Air Leakage	1
II. Foreign Material Contamination	7
Stuck Relays	1
Dirty Contacts	2
Dirty Breakers	4
III. Personnel-Related	4
IV. Unknown And Miscellaneous	12
TOTAL	33

are especially vulnerable to this failure cause. For example, greasy relays, sticky breakers, and dirty contacts are included in this category.

Some of personnel errors during operation, maintenance and testing can fail redundant components simultaneously. Other personnel errors are not likely to involve multiple component failures and are treated as independent events.

Miscellaneous and unknown causes refer to those that are either independent or without a specified failure cause due to insufficient information. As a first approximation, the unknown occurrences are treated as independent.

To calculate multiple failure probability, the following conditional probability formulas described in section 2.4 are used.

Case 1. Two-component failure probability

$$P(AB|C_i,\ i=1,2,3,4) = \sum_{i=1}^{4} P(AB|C_i)$$

$$= \sum_{i=1}^{2} P^2(A|C_i)P(C_i) + P(A|C_3) + P(A|C_4)P(B|C_4)\ ,$$

for 1-out-of-2 system

$$= \sum_{i=1}^{2} P^2(A|C_i)P(C_i) + P(A|C_4)P(B|C_4)$$

for 1-out-of-3 and 1-out-of-4 system

Case 2. Three-component failure probability

$$P(ABC|C_i, i=1,2,3,4) = \sum_{i=1}^{4} P(ABC|C_i)$$

$$= \sum_{i=1}^{2} P^3(A|C_i)P(C_i) + P(A|C_3) + P(A|C_4)P(B|C_4)P(C|C_4)$$

for 1-out-of-3 system

$$= \sum_{i=1}^{2} P^3(A|C_i)P(C_i) + P(A|C_4)P(B|C_4)P(C|C_4)$$

for 1-out-of-4 system

Case 3. Four-component failure probability

$$P(ABCD|C_i, i=1,2,3,4) = \sum_{i=1}^{4} P(ABCD|C_i)$$

$$= \sum_{i=1}^{2} P(A|C_i)\,P(C_i) + P(A|C_3) + P(A|C_4)\,P(B|C_4)\,P(C|C_4)\,P(D|C_4),$$

for 1-out-of-4 system

where

$P(AB|C_i, i=1,2,3,4)$ = failure of component A and B under conditions 1, 2, 3 and 4

$P(ABC|C_i, i=1,2,3,4)$ = failure of component A, B and C under conditions 1, 2, 3 and 4

$P(ABCD|C_i, i=1,2,3,4)$ = failure of component A, B, C and D under conditions 1, 2, 3 and 4

i = 1; refers to tribological failures

i = 2; refers to foreign material contamination

i = 3; refers to personnel error

i = 4; refers to independent failures

Because roughly equal research effort has been made in different aspects of each failure cause, it is plausible to assume that no single factor dominates the behavior of the failure cause. Accordingly, the central limit theorem suggests that the normal model for the stress and strength parameters is reasonable.

To identify the parameters characterizing the 'stress' and 'strength' for the two important failure causes, a basic understanding of the physics of these causes are necessary.

1. Wear models {6.7}

   In spite of the potential usefulness of wear models, there are relatively few good wear models and there are no universal models. However, for the purpose of applying the ISSI technique, one does not require an exact wear model for a particular service. Instead, the uncertainty associated with the material wear resistance and the stresses exisiting on wearing surface provides sufficient data requirements. By reviewing the expressions proposed by various authors to model wear, one can identify {6.7} the material hardness as a common variable that plays a decisive role in all these models. Thus one can regard the material hardness as a proper ' strength ' in all wear related failures. Similarly, as discussed in Ref. 6.8, one can identify the surface energy as the proper ' stress ' characterizing tribologically related failure causes.

2. Foreign material contamination

In the study of contacts for electrical control of any component, one recognizes that junction sizes have a dominant effect on the electrical resistance. Further investigations into the distribution of junction size {6.9} reveals that it is again related to the hardness of the material used. If foreign material contamination is a prevailing failure cause for switching devices, then an appropriate ' strength ' to use is the junction size of the contact. If enough junctions in the contact are contaminated by dirt or foreign particles, failure is expected. It is thus appropriate to regard the particle size existing in a particular environment as the ' stress ' acting on the switching devices such as relays, breakers etc.

With the above understanding of the failure mechanism, it is now necessary to quantify the ' stress ' and ' strength ' parameters thus identified. Studies to model adhesive wear {6.10} suggests that the coefficient of variation of stress at rubbing surface is bwtween 0.2 and 0.5 for common engineering situations. Fig. 6.1 {6.11} shows a typical result obtained for hardness measurement. It appears that normal distribution fits the data quite well. This is generally the case for other measurements where individual phenomenon is isolated and variables are relatively under better control. The coefficient of variation for the ' strength ' of wear-related failures used in the study is between 0.03 and 0.06.

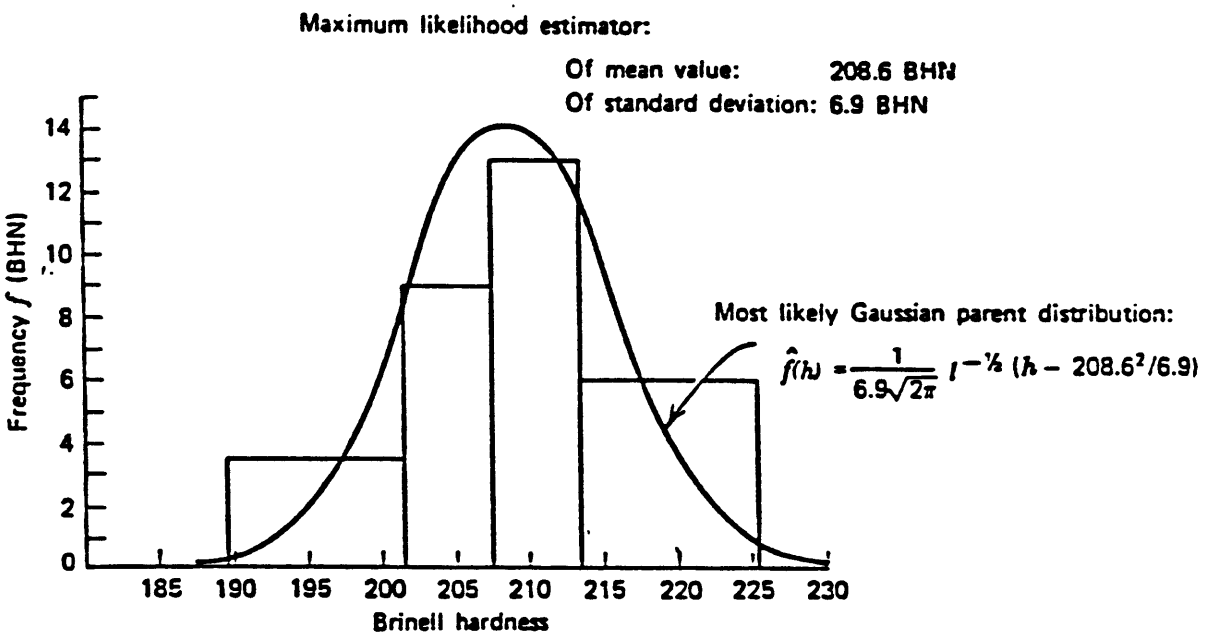


Figure 6.1 Sample Distribution of Brinnel Hardness (Ref. 6.11)

Similarly, the coefficient of variation for junction size distribution used in the study is between 0.03 and 0.06. The particle size distribution in common engineering situation {6.12,6.13} has the coefficient of variation of between 0.2 and 0.5. It is noted although these values are the same as for the tribological failures, they are analyzed separately due to their different nature.

Table 6.4 presents the results by the ISSI technique for different configurations of interest. The results obtained for BFR and coupling method are also shown for comparison. It is apparent that the uncertainty is smallest in the case of the ISSI approach. The failure probabilties for different multiplicity are also slightly higher with the ISSI method. Other trends are similar to those described in chapter 5.

Table 6.5 shows the multiple dependent failure fraction corresponding to the cases presented in Table 6.4.

6.3.2 AFWS Pumps

There are generally three kinds of pumps in AFWS. Motor-driven pumps are largest in number, followed by turbine-driven and then diesel-driven pumps. To illustrate the ISSI procedure, only motor-driven pumps are considered.

By adopting the same procedure, identical failure causes are identified for AFWS pumps as for HIPS pumps. The same corresponding 'stress' and 'strength' parameters are also used. The only difference lies in the single component failure probability for each category. In addition, electrical failures are identified in AFWS pumps. Examples in

Table 6.4 CCF Results for Various Methods: HPIS Pumps

Configuration	ISSI	BFR	COUPLING
2-unit system			
k=2	upper lower 1.5E-4 6.7E-5 median 1.0E-04	upper lower 4.0E-4 2.6E-6 median 3.2E-05	upper lower 9.7E-7 8.7E-8 median 2.9E-07
3-unit system			
k=2	upper lower 1.1E-4 4.8E-5 median 7.3E-05	upper lower 3.6E-4 1.9E-6 median 2.6E-05	upper lower 7.6E-7 6.4E-8 median 2.2E-07
k=3	upper lower 7.9E-5 2.2E-5 median 4.2E-05	upper lower 3.3E-4 6.5E-7 median 1.5E-05	upper lower 6.4E-10 1.6E-11 median 1.0E-10
4-unit system			
k=2	upper lower 9.6E-5 4.1E-5 median 6.3E-05	upper lower 3.6E-4 1.6E-6 median 2.4E-05	upper lower 6.3E-7 5.2E-8 median 1.8E-07
k=3	upper lower 6.9E-5 1.9E-5 median 3.6E-05	upper lower 3.3E-4 6.1E-7 median 1.4E-05	upper lower 5.2E-10 1.2E-12 median 8.0E-11
k=4	upper lower 5.5E-5 1.1E-5 median 2.9E-05	upper lower 3.2E-4 4.3E-7 median 1.2E-05	upper lower 4.1E-14 2.8E-16 median 3.4E-15

Table 6.5 MDFF for Various Methods: HPIS Pumps

Configuration	ISSI	BFR	COUPLING
2-unit system			
k=2	upper lower 2.8E-1 1.2E-1 median 1.9E-01	upper lower 7.4E-1 4.8E-3 median 5.9E-02	upper lower 1.8E-3 1.6E-4 median 5.4E-04
3-unit system			
k=2	upper lower 2.3E-1 1.0E-1 median 1.6E-01	upper lower 7.7E-1 4.0E-3 median 5.5E-02	upper lower 1.4E-3 1.4E-4 median 4.7E-04
k=3	upper lower 1.7E-1 4.7E-2 median 8.9E-02	upper lower 7.0E-1 1.4E-3 median 3.2E-02	upper lower 1.4E-06 3.4E-08 median 2.1E-07
4-unit system			
k=2	upper lower 2.3E-1 9.5E-2 median 1.5E-01	upper lower 8.4E-1 3.7E-3 median 5.6E-02	upper lower 1.5E-3 1.2E-4 median 4.2E-04
k=3	upper lower 1.6E-1 4.4E-2 median 8.4E-02	upper lower 7.7E-1 1.4E-3 median 3.3E-02	upper lower 1.2E-06 2.8E-09 median 1.9E-07
k=4	upper lower 1.3E-1 2.6E-2 median 6.7E-02	upper lower 7.4E-1 1.0E-3 median 2.8E-02	upper lower 9.5E-11 6.5E-13 median 7.9E-12

this category include loose wires, broken connectors etc. To be conservative, they are considered as potential common cause failures. It turns out that they are not significant contributors to the overall multiple failure probability.

Table 6.6 shows the failure classification according to the LER coding. As in the case of HPIS pumps, the scheme is not of direct usefulness for applying the ISSI method.

Table 6.7 presents the appropriate failure mechanisms for the application of the ISSI method. It is worth noting that in AFWS, more failures associated with electrical parts are identified. This may be due to more control functions present in AFWS pumps.

Table 6.8 presents multiple failure probabilities for different configurations based on various methods. One can readily recognize that the ISSI approach gives slightly higher values than other methods. Also, as in the case of HPIS pumps, the uncertainty seems reduced relative to the statistical approaches.

Table 6.9 presents MDFF based on the median values of single component failure probability.

6.4 Application To Valves

Valves are major contributors to failures or abnormal occurences in nuclear power plant systems. Two kinds of valves are studied as an application of the ISSI technique. Motor-operated valves (MOVs) provide important functions in many of the standby systems to be discussed in chapter 7.

Table 6.6 LER AFWS Pump Failure Classification

Failure Cause	Number of Failures
Unknown	8
Personnel (Operation)	5
Personnel (Maintenance)	7
Personnel (Testing)	2
Design Error	7
Procedural Discrepancies	5
Extreme Environment	9
Bearing	3
Mechanical Control Parts Failures	44
Failed Internals	2
Foreign Material Contamination	11
Normal Wear	1
Shaft/Coupling Failure	2
Drive Train Failure	4
Seal/Packing Failure	1
Misalignment	1
TOTAL	112

Table 6.7 AFWS Pump Failure Reclassification

Failure Cause	Number of Failures
I. Tribological Failures	13
Seal	1
Bearing	3
Shaft	2
Failed Internals	2
Mechanical Binding	2
Linkage Misalignment	1
II. Foreign Material Contamination	24
Stuck Relays	6
Dirty Contacts	3
Dirty Breakers	11
Strainer Clogged	4
III. Electrical Failures	19
IV. Personnel-Related	8
V. Unknown And Miscellaneous	58
TOTAL	112

Table 6.8 CCF Results for Various Methods: AFWS Pumps

Configuration	ISSI	BFR	COUPLING
2-unit system			
k=2	upper lower 3.5E-4 1.6E-4 median 2.4E-04	upper lower 8.6E-4 4.0E-5 median 1.9E-04	upper lower 1.1E-5 1.5E-6 median 4.0E-06
3-unit system			
k=2	upper lower 3.1E-4 1.3E-4 median 2.0E-04	upper lower 8.3E-4 2.7E-5 median 1.5E-04	upper lower 9.0E-6 1.1E-6 median 3.2E-06
k=3	upper lower 2.4E-4 6.2E-5 median 1.2E-04	upper lower 6.8E-4 6.1E-6 median 6.4E-05	upper lower 2.7E-08 1.2E-09 median 5.8E-09

Table 6.9 MDFF for Various Methods: AFWS Pumps

Configuration	ISSI	BFR	COUPLING
2-unit system			
k=2	upper lower 1.8E-1 8.0E-2 median 1.2E-01	upper lower 4.3E-1 2.0E-2 median 9.5E-02	upper lower 5.5E-3 7.5E-4 median 2.0E-03
3-unit system			
k=2	upper lower 1.7E-1 7.0E-2 median 1.1E-01	upper lower 4.6E-1 1.5E-2 median 8.3E-02	upper lower 5.0E-3 6.1E-4 median 1.8E-03
k=3	upper lower 1.3E-1 3.0E-2 median 6.7E-02	upper lower 3.8E-1 3.4E-3 median 3.6E-02	upper lower 1.5E-05 6.7E-07 median 3.2E-06

Check valves, on the other hand, are used to direct flow in only one direction. The investigation in this thesis focuses only on the reliability aspects of valves. No attention is given to the hydraulic characteristics of these components.

In essence, we use the same procedure applied in the analysis of pumps to evaluate the CCF probabilities of the valves. To recapitulate, the following steps represent how one proceeds to apply the ISSI technique:

1. Define failure causes as identified in the LER
2. Reclassify the failure causes into root causes
3. For each root cause, quantify the pertinent 'stress' and 'strength' parameters. In this study, we find it easier to work with the coefficient of variations and leave the safety factor an unknown parameter.
4. Invert the LER estimates of the single failure probability to obtain the value of reliability index.
5. Find the unknown parameter (in this study, it is the safety factor). Now, all the required stress-strength parameters have been estimated.
6. Use the common load model to compute the multiple failure probability.
7. Combine the multiple failure probability obtained for each failure cause to get the final CCF probabilities due to common causes.

After careful application of the above procedure, we observe the following:

1. Pumps generally involve more sophiscated moving parts, which leads to a higher failure probability than valves. According to the insight discussed in section 5.5, valves should have lower multiple failure probabilities. This indeed agrees with the results.
2. In the AFWS MOVs, electrical failures represent a significant fraction of the failure cause. However, with regard to CCF probability, electrical-related causes do not play an important role as tribological causes.

Table 6.10 summarizes the LER coding scheme for HPIS MOVs. As described previously, this scheme is useful for a general discussion on reliability. To pursue further the CCF issue, one needs to identify root causes. Table 6.11 shows the reclassification of causes for HPIS MOVs. Table 6.12 compares the multiple failure probabilities calculated on the basis of different methods. Specifically, this table compares the ISSI, the BFR and the coupling method.

Table 6.13 lists the LER coding scheme for AFWS MOV failures. Table 6.14 represents the root causes identified for AFWS MOVs. As indicated above, electrical failures contribute significantly in the failure statistics. The loading rougness (an indication of the variability of the stress to strength) is small due to a relatively better control and advanced knoweldge in the area of electric

Table 6.10 LER HPIS MOV Failure Classification

Failure Cause	Number of Failures
Unknown	3
Personnel (Operation)	3
Personnel (Maintenance)	1
Mechanical Control Parts Failures	2
Packing Failures	1
Electrical Input Failures	7
Lack Of Lubrication	1
Electrical Motor Operator Failures	2
Torque Switch Failures	1
Limit Switch Failures	1
TOTAL	22

Table 6.11 HPIS MOV Failure Reclassification

Failure Cause	Number of Failures
I. Tribological Failures	5
Packing	1
Valve Stem	2
Shaft	1
Screw Holding Lever	1
II. Foreign Material Contamination	6
Stuck Contacts	3
Dirty Contacts	1
Dirty Breakers	1
Limit Switches	1
III. Personnel-Related	4
IV. Unknown And Miscellaneous	7
TOTAL	22

Table 6.12 CCF Results for Various Methods: HPIS MOVs

Configuration	ISSI	BFR	COUPLING
2-unit system			
k=2	upper lower 3.8E-4 1.8E-4 median 2.6E-04	upper lower 4.5E-4 1.7E-7 median 8.7E-06	upper lower 2.7E-4 1.9E-8 median 2.3E-06
3-unit system			
k=2	upper lower 3.5E-4 1.6E-4 median 2.4E-04	upper lower 3.9E-4 4.1E-7 median 1.3E-05	upper lower 2.0E-4 2.0E-8 median 2.0E-06
k=3	upper lower 2.7E-4 8.0E-5 median 1.5E-04	upper lower 2.9E-4 3.2E-7 median 9.6E-06	upper lower 2.8E-06 2.8E-12 median 2.8E-09
4-unit system			
k=2	upper lower 3.5E-4 1.6E-4 median 2.4E-04	upper lower 3.6E-4 5.4E-7 median 1.4E-05	upper lower 2.0E-4 2.0E-8 median 2.0E-06
k=3	upper lower 2.7E-4 8.0E-5 median 1.5E-04	upper lower 2.9E-4 3.2E-7 median 9.6E-06	upper lower 2.8E-06 2.8E-12 median 2.8E-09
k=4	upper lower 2.2E-4 5.0E-5 median 1.0E-04	upper lower 2.9E-4 3.0E-7 median 9.3E-06	upper lower 3.8E-08 3.8E-16 median 3.8E-12

Table 6.13 LER AFWS MOV Failure Classification

Failure Cause	Number of Failures
Unknown	1
Personnel (Maintenance)	1
Fabrication/Construction/Q.C.	1
Mechanical Control Parts Failures	1
Excessive Vibration	1
Electrical Input Failures	7
Electrical Motor Operator Failures	8
Torque Switch Failures	1
TOTAL	21

Table 6.14 AFWS MOV Failure Reclassification

Failure Cause	Number of Failures
I. Tribological Failures	2
Worn Ring	1
Valve Seating	1
II. Electrical Failures	10
Broken Wires	3
Loose Connections	3
Setpoint Drift	1
Relay Failures	1
Operator Failure	2
III. Personnel-Related	2
IV. Unknown And Miscellaneous	7
TOTAL	21

parts. Table 6.15 presents the ISSI results with those based on the BFR and the coupling method.

Table 6.16 summarizes the failure causes according to the LER coding scheme for check valves. It is noted that no distinction is made between 'failure to open' and 'failure to close'. This is because of the lack of specific information available to make the judgment. It is, however, reasonable to assume that both failure modes have the same root causes as identified in Table 6.17. Whether closing or opening, the root causes potentially exist to fail the check valves. On the other hand, opening check valves presents a lower failure probability than closing them according to the LER. Tables 6.18 and 6.19 summarize the results for these two types of failures. The results based on the BFR and the coupling methods are also compared in these tables.

6.5 Comparison with the BFR and the Coupling Method

As noted earlier, current methods to model CCFs are primarily statistical approaches. In order to check the adequacy of the proposed approach, the ISSI technique, one has to compare the CCF estimates based on various modelling methods. The BFR and the coupling methods are studied.

The BFR represents a possible statistical approach, while the coupling method designates a practical heuristic procedure to analyze CCFs.

The comparison made between the ISSI, the BFR and the coupling method is based on the following assumptions:

Table 6.15 CCF Results for Various Methods: AFWS MOVs

Configuration	ISSI	BFR	COUPLING
2-unit system			
k=2	upper lower 8.8E-5 5.6E-5 median 7.0E-05	upper lower 4.5E-4 1.7E-7 median 8.7E-06	upper lower 2.7E-4 1.9E-8 median 2.3E-06
3-unit system			
k=2	upper lower 7.8E-5 4.8E-5 median 6.1E-05	upper lower 3.9E-4 4.1E-7 median 1.3E-05	upper lower 2.0E-4 2.0E-8 median 2.0E-06
k=3	upper lower 3.8E-5 1.7E-5 median 2.5E-05	upper lower 2.9E-4 3.2E-7 median 9.6E-06	upper lower 2.8E-06 2.8E-12 median 2.8E-09
4-unit system			
k=2	upper lower 7.8E-5 4.8E-5 median 6.1E-05	upper lower 3.6E-4 5.4E-7 median 1.4E-05	upper lower 2.0E-4 2.0E-8 median 2.0E-06
k=3	upper lower 3.8E-5 1.7E-5 median 2.5E-05	upper lower 2.9E-4 3.2E-7 median 9.6E-06	upper lower 2.8E-06 2.8E-12 median 2.8E-09
k=4	upper lower 2.6E-5 9.8E-6 median 1.6E-05	upper lower 2.9E-4 3.0E-7 median 9.3E-06	upper lower 3.8E-08 3.8E-16 median 3.8E-12

Table 6.16 LER Check Valve Failure Classification

Failure Cause	Number of Failures
Unknown	23
Personnel (Operation)	1
Personnel (Maintenance)	2
Design Error	2
Mechanical Control Parts Failures	7
Fabrication/Construction/Q.C.	5
Procedural Discrepancies	2
Normal Wear	2
Excessive Wear	1
Corrosion	1
Foreign Material Contamination	9
Seat/Disc Failure	5
TOTAL	60

Table 6.17 Check Valve Failure Reclassification

Failure Cause	Number of Failures
I. Tribological Failures	10
Leakage	4
Disk	1
Seat Surface	3
Wear Of Internal	1
II. Foreign Material Contamination	9
Sand On Seat Surface	4
Dirt On Seat Surface	5
III. Personnel-Related	9
IV. Unknown And Miscellaneous	32
TOTAL	60

Table 6.18 CCF Results for Various Methods: Check Valves

Failure to Remain Open

Configuration	ISSI	BFR	COUPLING
2-unit system			
k=2	upper lower 2.2E-5 7.6E-6 median 1.3E-05	upper lower 3.2E-4 2.5E-6 median 2.8E-05	upper lower 2.7E-7 3.1E-9 median 2.9E-08
3-unit system			
k=2	upper lower 1.8E-5 6.0E-6 median 1.0E-05	upper lower 3.2E-4 1.7E-6 median 2.3E-05	upper lower 2.5E-7 2.0E-9 median 2.0E-08
k=3	upper lower 1.3E-5 2.2E-6 median 5.3E-06	upper lower 3.0E-4 5.7E-7 median 1.3E-05	upper lower 9.2E-11 8.6E-14 median 2.8E-12
4-unit system			
k=2	upper lower 1.7E-5 5.5E-6 median 9.7E-06	upper lower 3.1E-4 1.4E-6 median 2.1E-05	upper lower 1.8E-7 1.6E-9 median 1.7E-08
k=3	upper lower 1.2E-5 2.1E-6 median 5.0E-06	upper lower 3.0E-4 5.3E-7 median 1.3E-05	upper lower 7.8E-11 6.2E-14 median 2.2E-12
k=4	upper lower 9.2E-6 1.1E-6 median 3.2E-06	upper lower 2.9E-4 3.8E-7 median 1.0E-05	upper lower 3.3E-11 2.5E-18 median 9.1E-15

Table 6.19 CCF Results for Various Methods: Check Valves

Failure to Close

Configuration	ISSI	BFR	COUPLING
2-unit system			
k=2	upper lower 7.1E-5 2.7E-5 median 4.4E-05	upper lower 3.3E-4 1.5E-6 median 2.2E-05	upper lower 6.1E-6 9.4E-9 median 2.4E-07
3-unit system			
k=2	upper lower 6.4E-5 2.5E-5 median 4.0E-05	upper lower 3.2E-4 1.2E-6 median 2.0E-05	upper lower 6.2E-6 6.5E-9 median 2.0E-07
k=3	upper lower 4.6E-5 1.1E-5 median 2.2E-05	upper lower 3.0E-4 5.5E-7 median 1.3E-05	upper lower 1.6E-08 5.3E-13 median 9.1E-11
4-unit system			
k=2	upper lower 6.0E-5 2.3E-5 median 3.7E-05	upper lower 3.2E-4 1.0E-6 median 1.8E-05	upper lower 6.2E-6 5.1E-9 median 1.8E-07
k=3	upper lower 4.3E-5 9.6E-6 median 2.0E-05	upper lower 3.0E-4 5.3E-7 median 1.3E-05	upper lower 1.5E-08 3.5E-13 median 7.4E-11
k=4	upper lower 3.4E-5 5.5E-6 median 1.4E-05	upper lower 3.0E-4 4.1E-7 median 1.1E-05	upper lower 3.8E-11 2.5E-17 median 3.1E-14

1. Single component failure probability is identical in three methods investigated. It is based on the LER estimates.
2. The failure probability over a certain test interval is compared. The test interval is chosen to be one month for pumps and three months for valves, which is roughly the industry practice.
3. On-demand failure probability is not considered. This is consistent with the previous assumption.
4. For the BFR method, the results are directly taken from the LER estimates. (Ref. 6.5 and 6.14)
5. For the AFWS pumps, the failure rate used is that for a 3-unit configuration. For the HPIS pumps, the failiure rate used is the one applicable to a 2-unit configuration.
6. The range used in the rest of discussion denotes a 90% interval of the estimated failure probability. For each component, the 95th percentile, the median and the 5th percentile indicate the magnitude of uncertainty.
7. For the ISSI method, the 95th percentile is obtained based on the stress coefficient of variation of 0.5 and strength coefficient of variation of 0.03. The 5th percentile is obtained based on the stress coefficient of variation of 0.2 and strength coefficient of variation of 0.06. These are values judged to be the bounds for stress and strength from

engineering considerations as described in sections 6.3 and 6.4.

Figures 6.2, 6.3 and 6.4 present the range for the HPIS pump, with k=2, 3 and 4 respectively. Here, as elsewhere, k stands for the number of redundancy.

Figures 6.5 and 6.6 show the range for the AFWS pump, with k=2 and 3.

Figures 6.7, 6.8 and 6.9 present the range for the HPIS MOV, with k=2, 3 and 4 respectively.

Figures 6.10, 6.11 and 6.12 show the range for the AFWS MOV, with k=2, 3 and 4 respectively.

Figures 6.13, 6.14 and 6.15 illustrate the range for the check valves(fail to open), with k=2, 3 and 4 respectively.

Finally, Figures 6.16, 6.17 and 6.18 present the range for the check valves (fail to close), with k=2, 3 and 4 respectively.

It is cautioned that the ordinates of these figures are in logarithmic scale. In addition, the scale is different in each case to account for the range for multiple failure probabilities under different redundancies and various single failure probabilities. Tables 6.4, 6.8, 6.12, 6.15, and 6.19 provide specific numerical values for Figures 6.2 through 6.19.

By studying these figures closely, one finds the following qualitative characteristics:

1. The ISSI approach as illustrated in this study yields

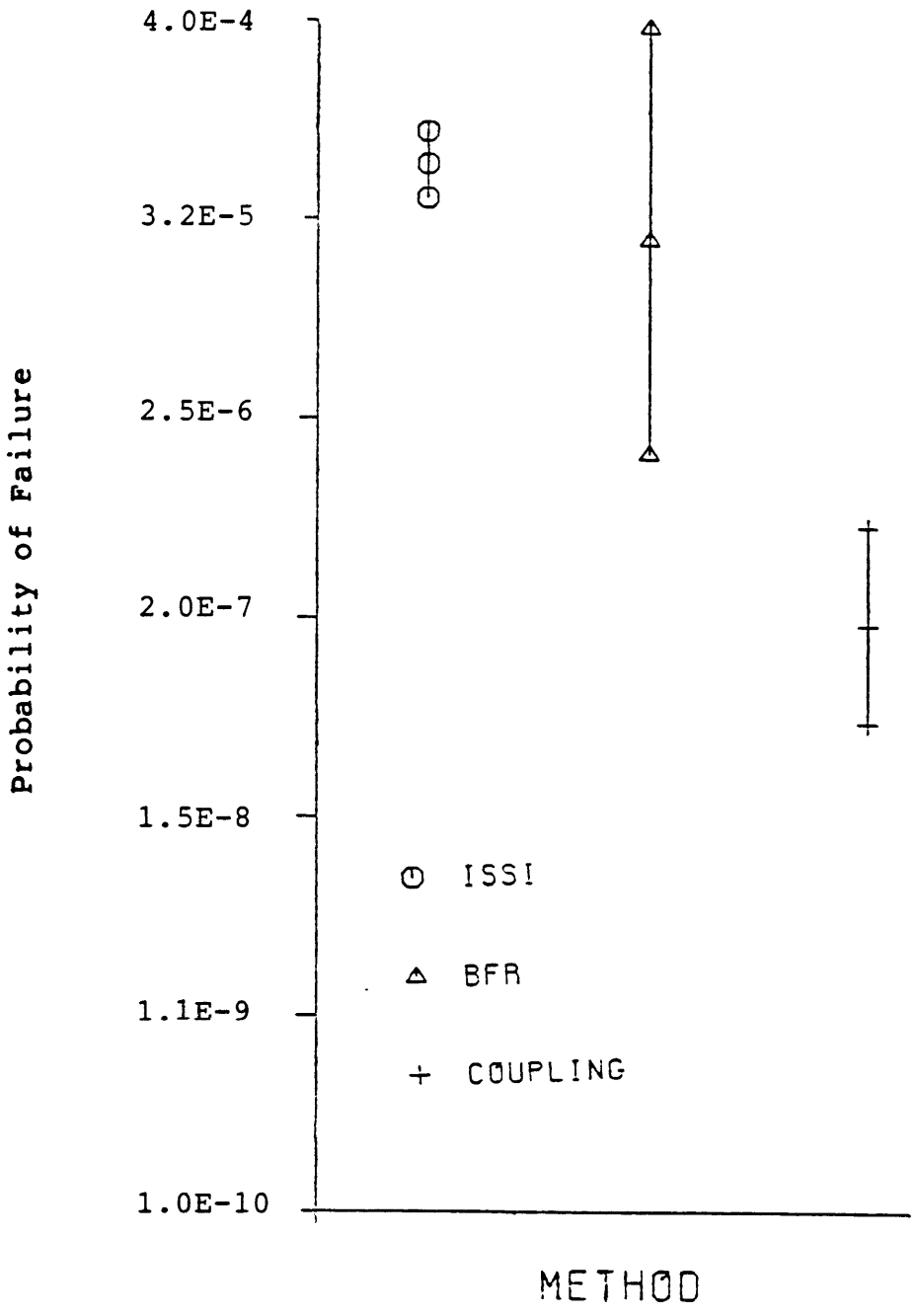


Figure 6.2 CCF Range Estimates: HPIS Pump, k Equal to 2

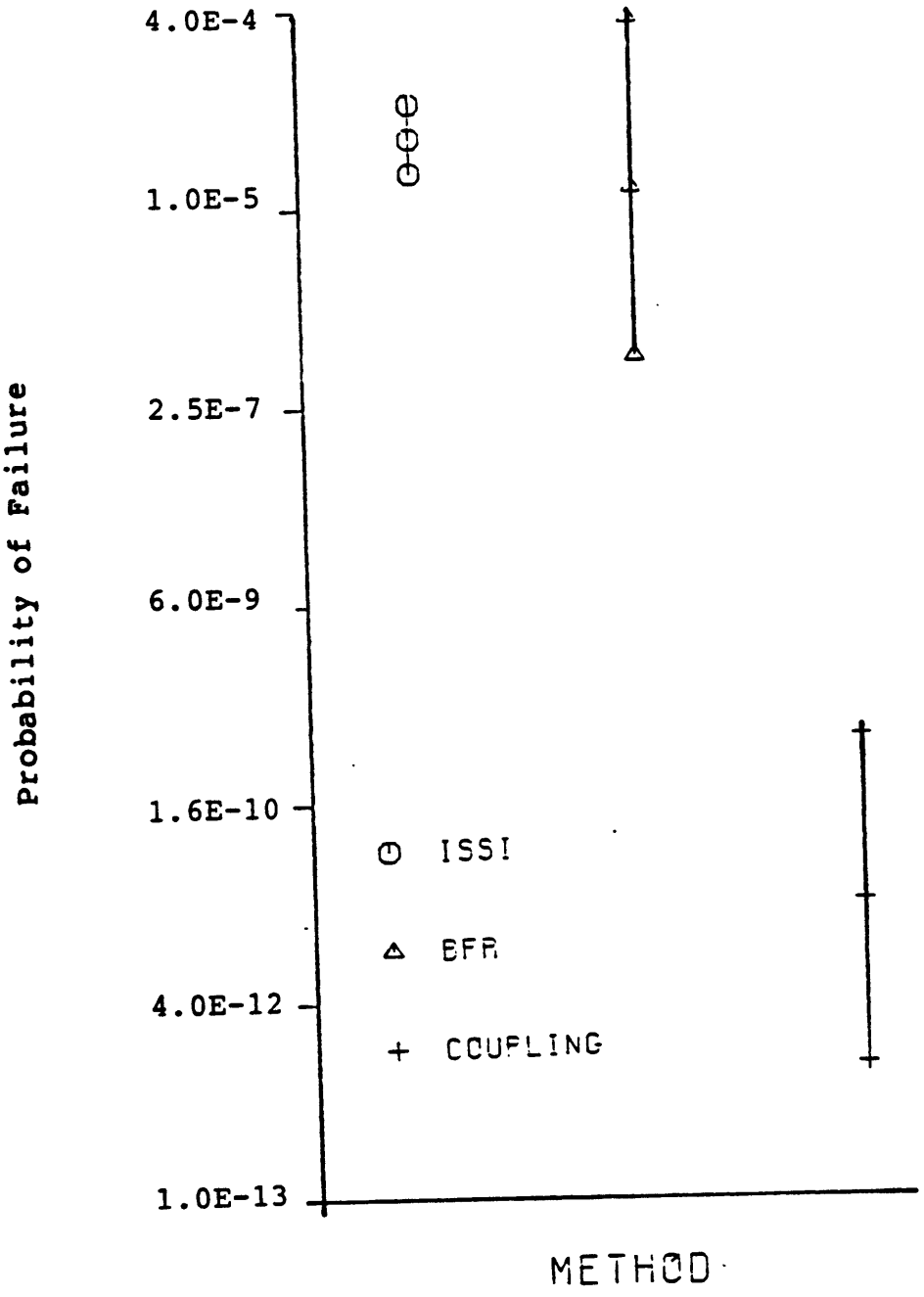


Figure 6.3 CCF Range Estimates: HPIS Pump, k Equal to 3

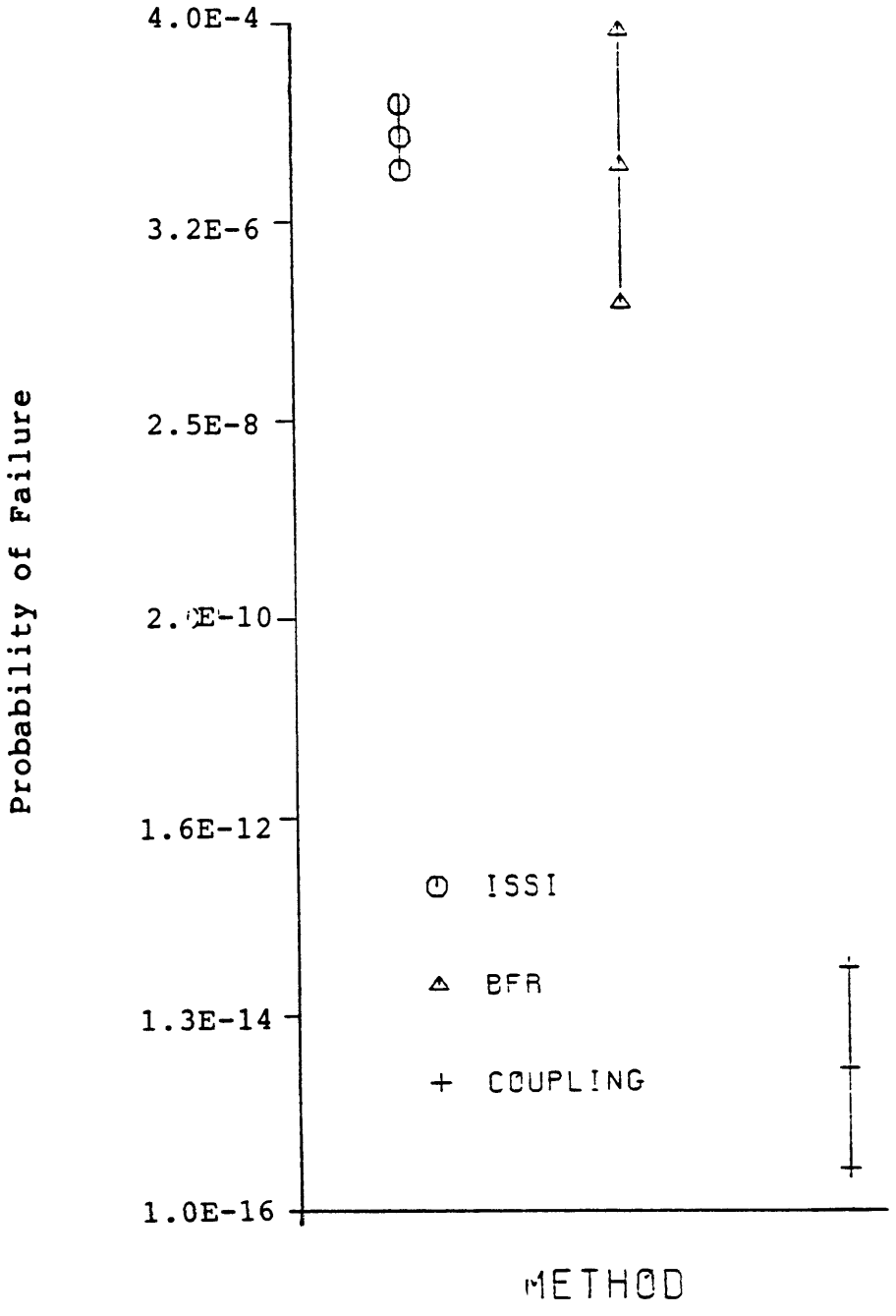


Figure 6.4 CCF Range Estimates: HPIS Pump, k Equal to 4

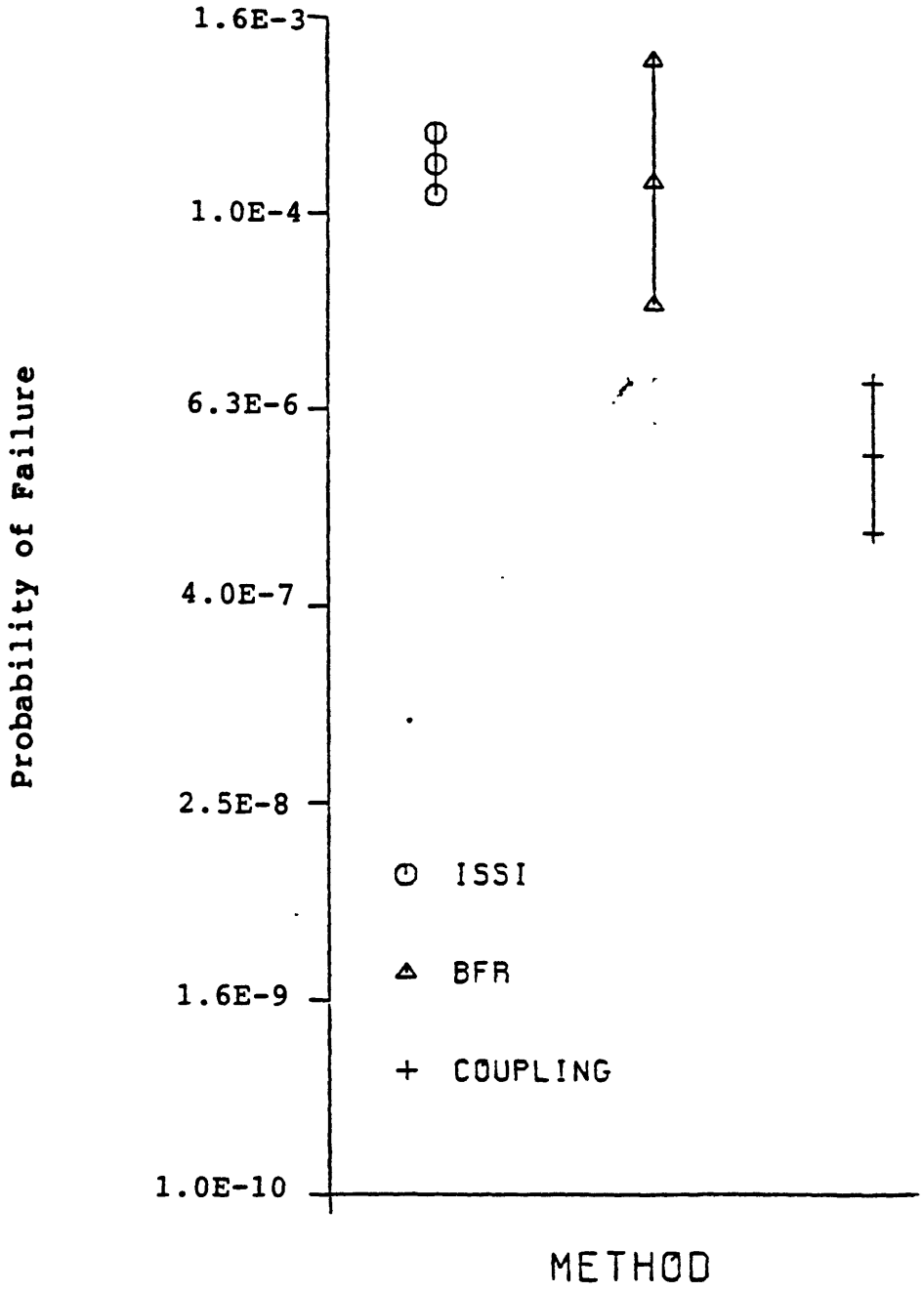


Figure 6.5 CCF Range Estimates: AFWS Pump, k Equal to 2

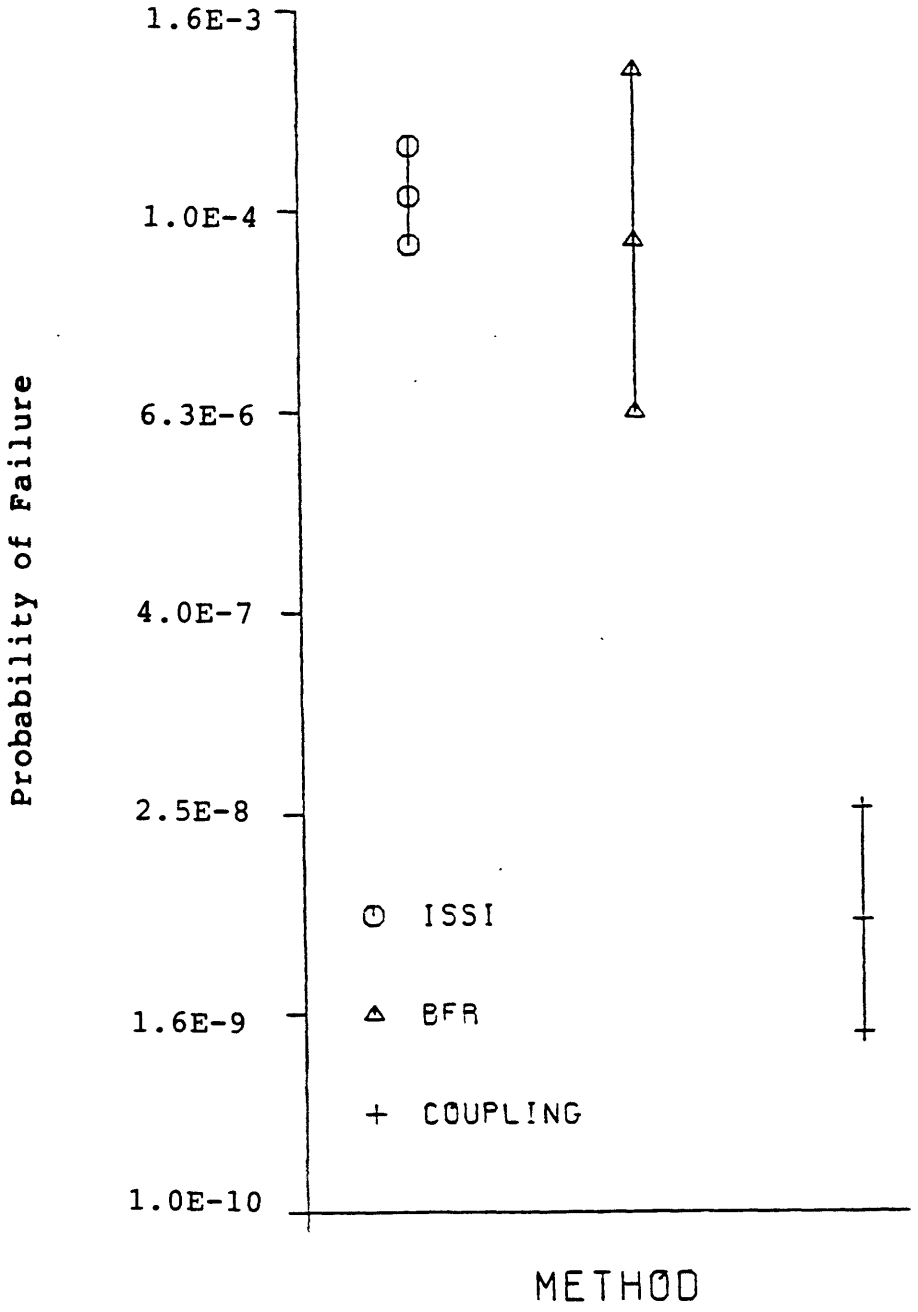


Figure 6.6 CCF Range Estimates: AFWS Pump, k Equal to 3

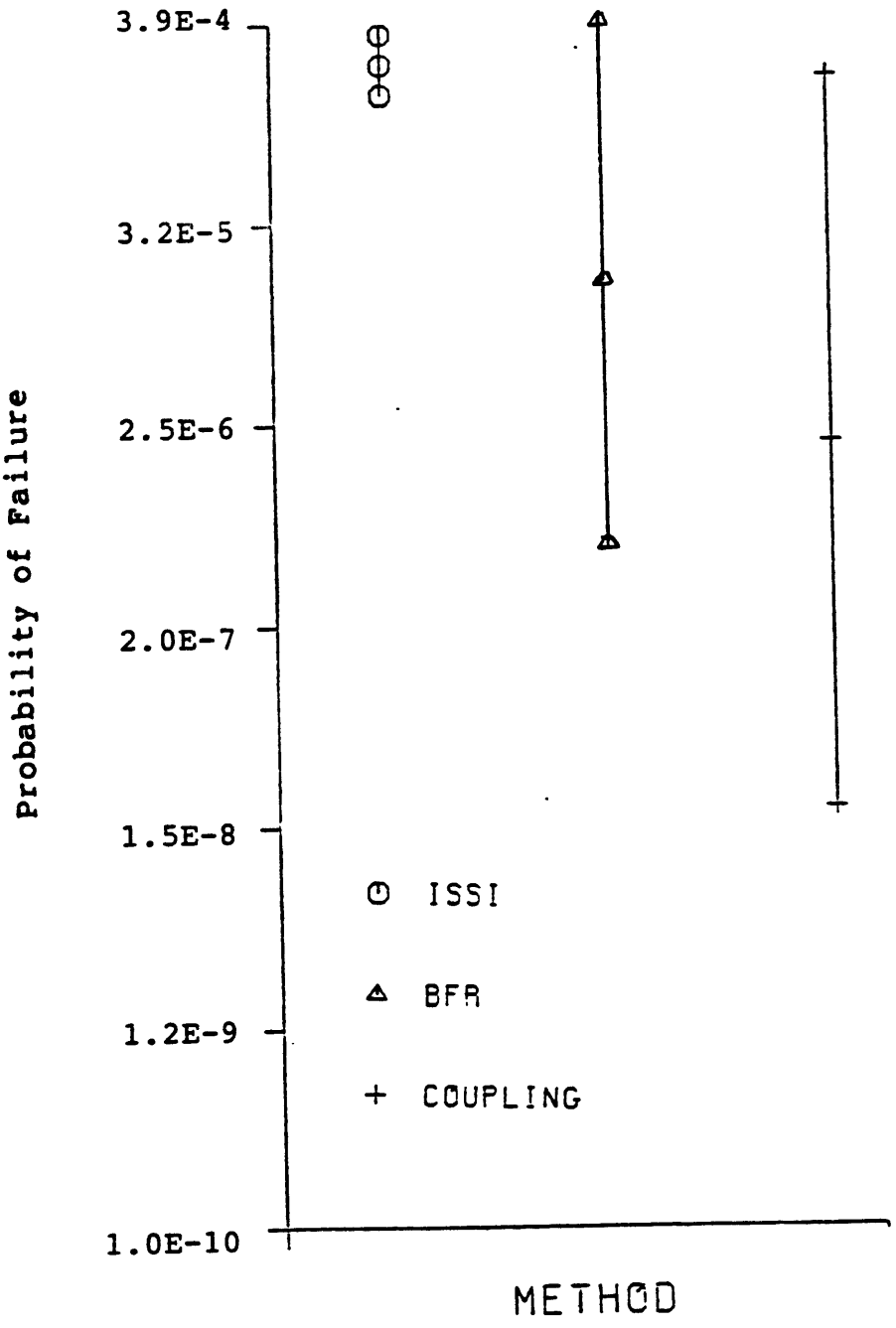


Figure 6.7 CCF Range Estimates: HPIS MOV, k Equal to 2

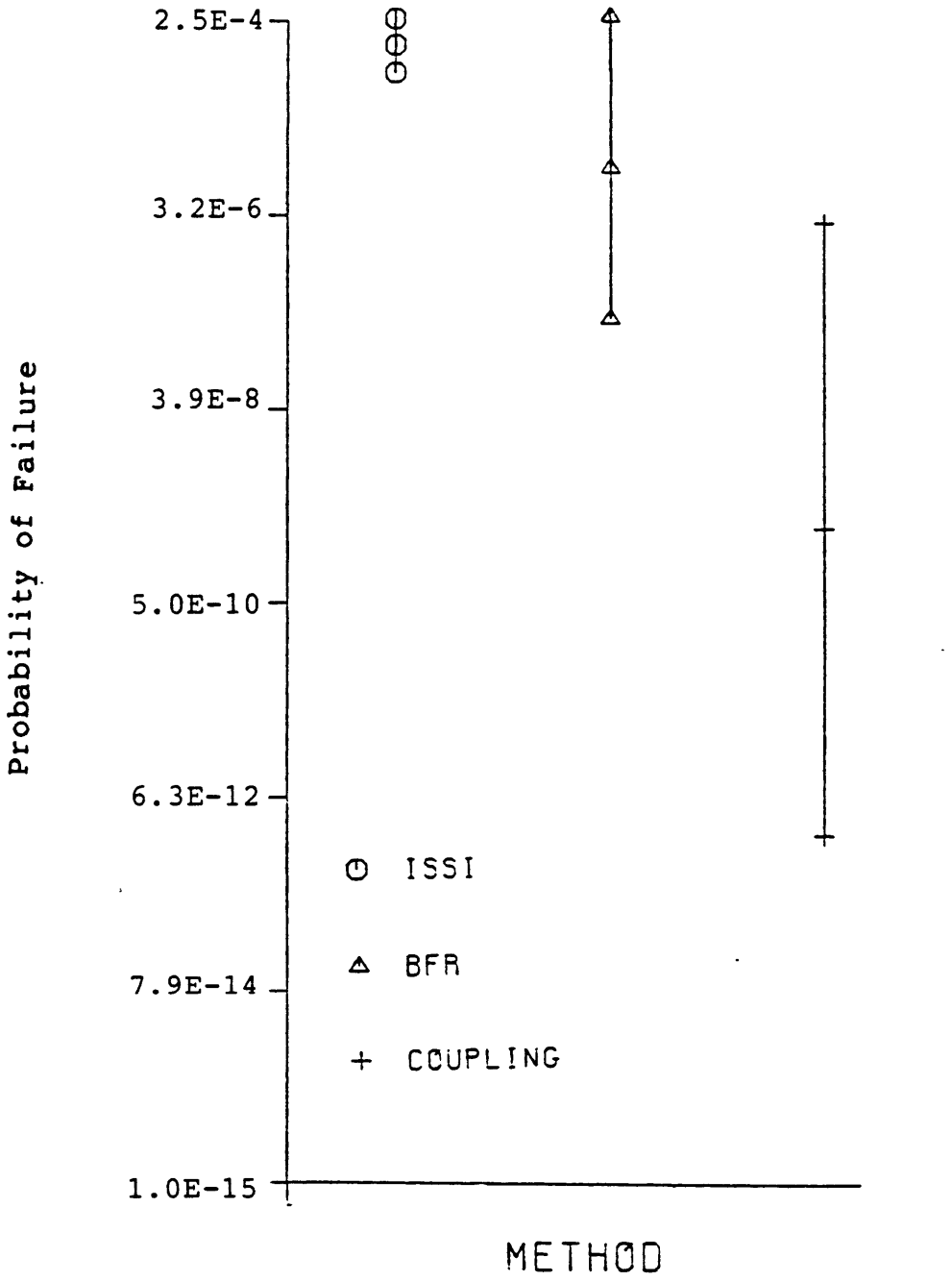


Figure 6.8 CCF Range Estimates: HPIS MOV, k Equal to 3

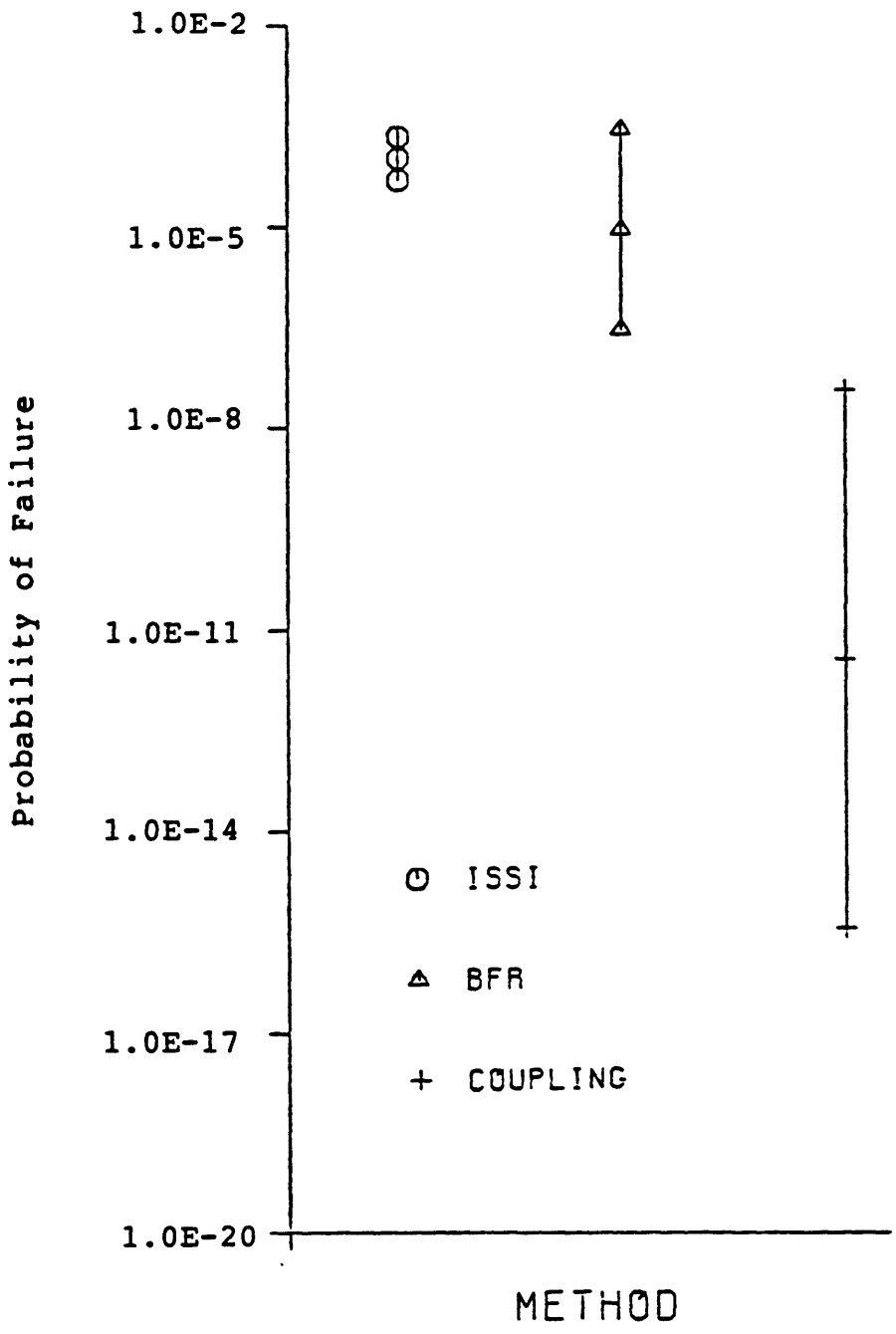


Figure 6.9 CCF Range Estimates: HPIS MOV, k Equal to 4

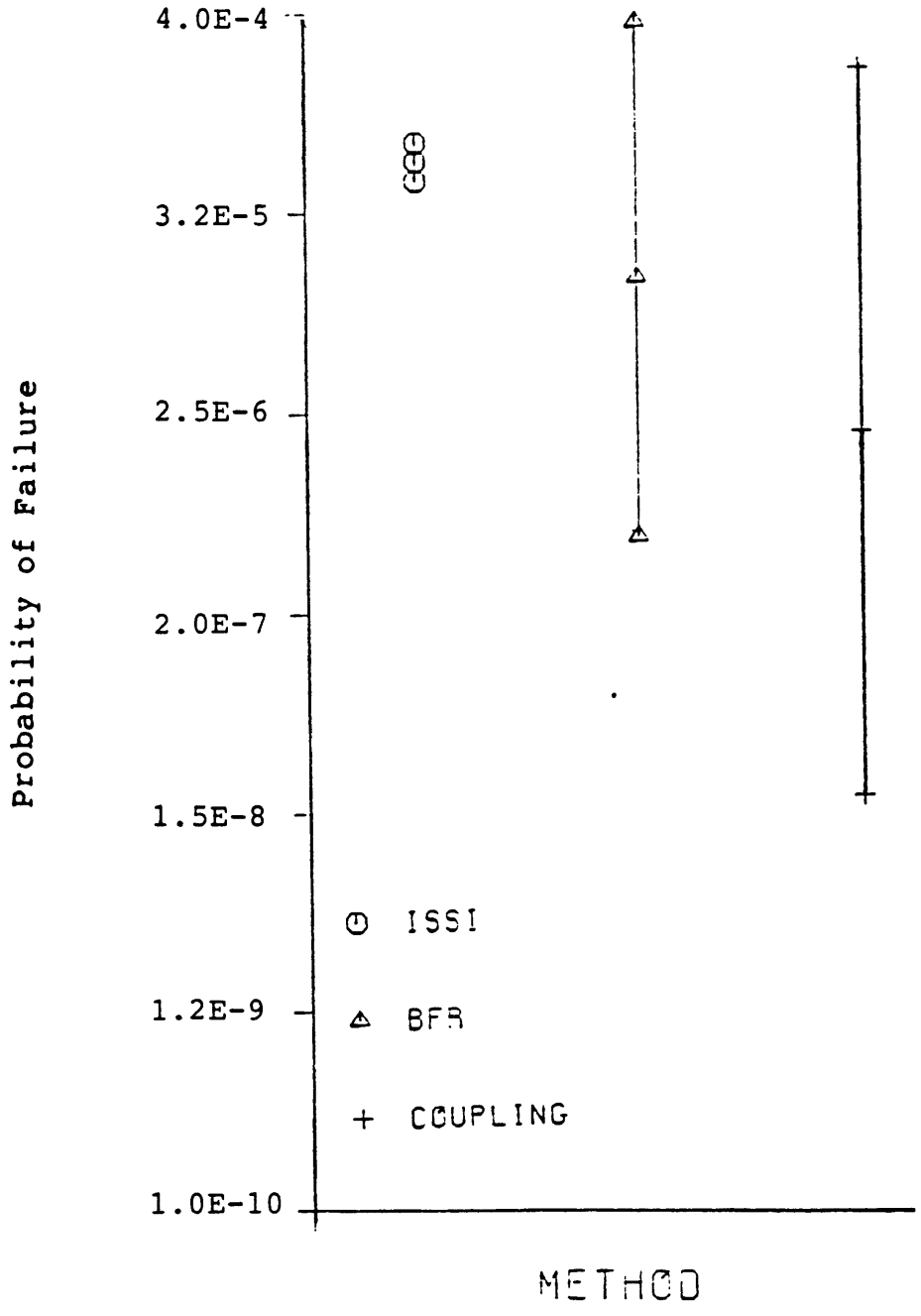


Figure 6.10 CCF Range Estimates: AFWS MOV, k Equal to 2

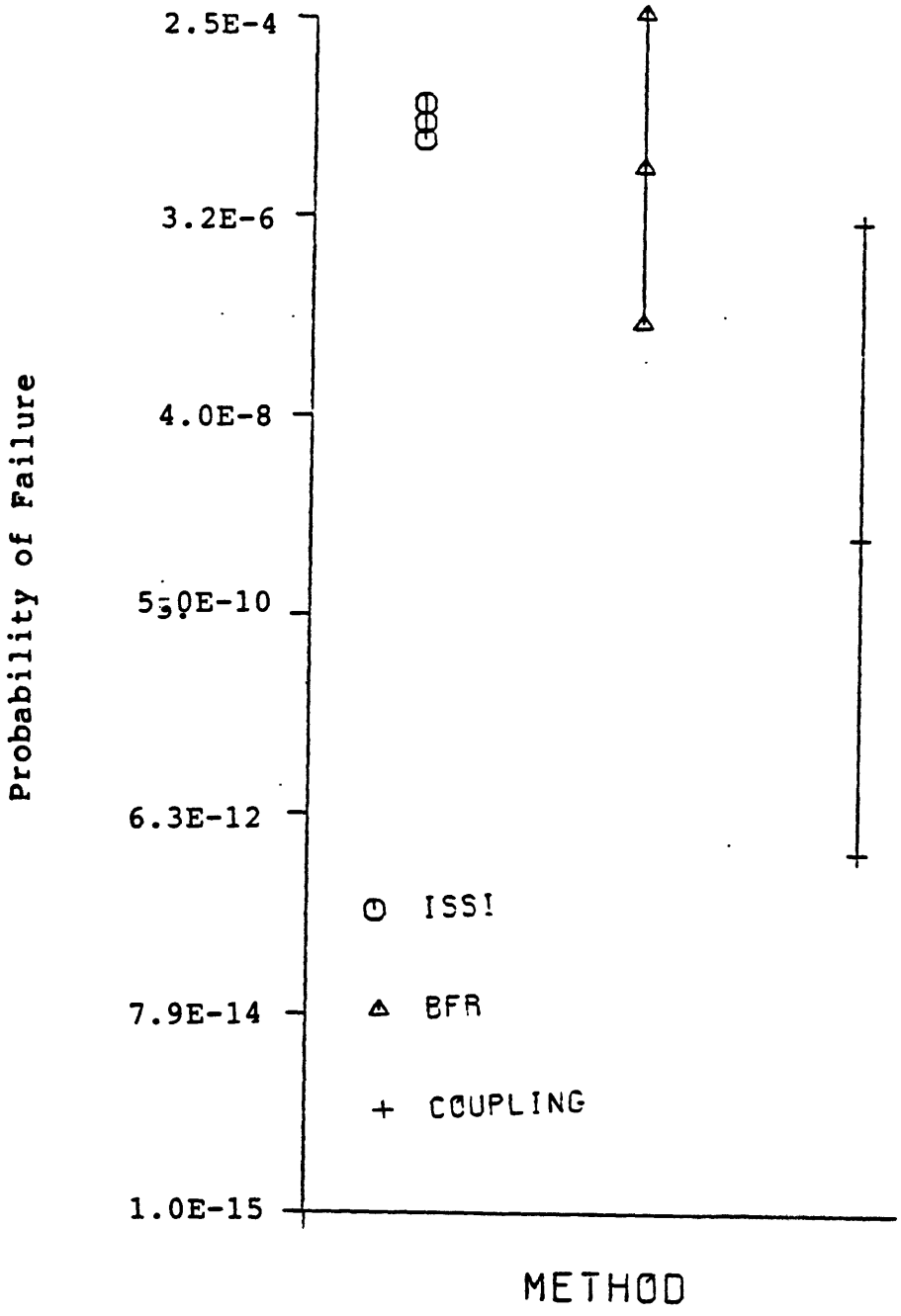


Figure 6.11 CCF Range Estimates: AFWS MOV, k Equal to 3

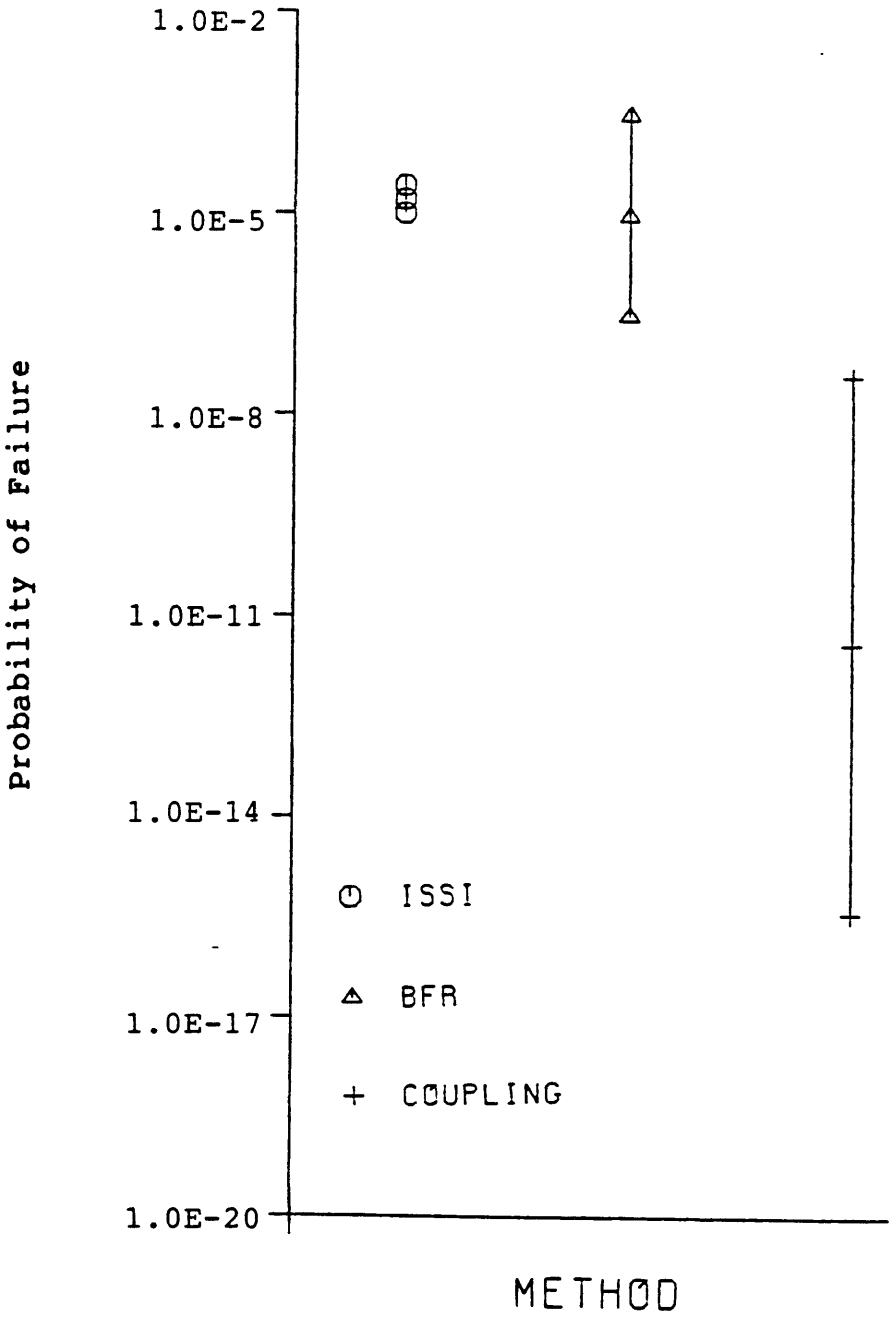


Figure 6.12 CCF Range Estimates: AFWS MOV, k Equal to 4

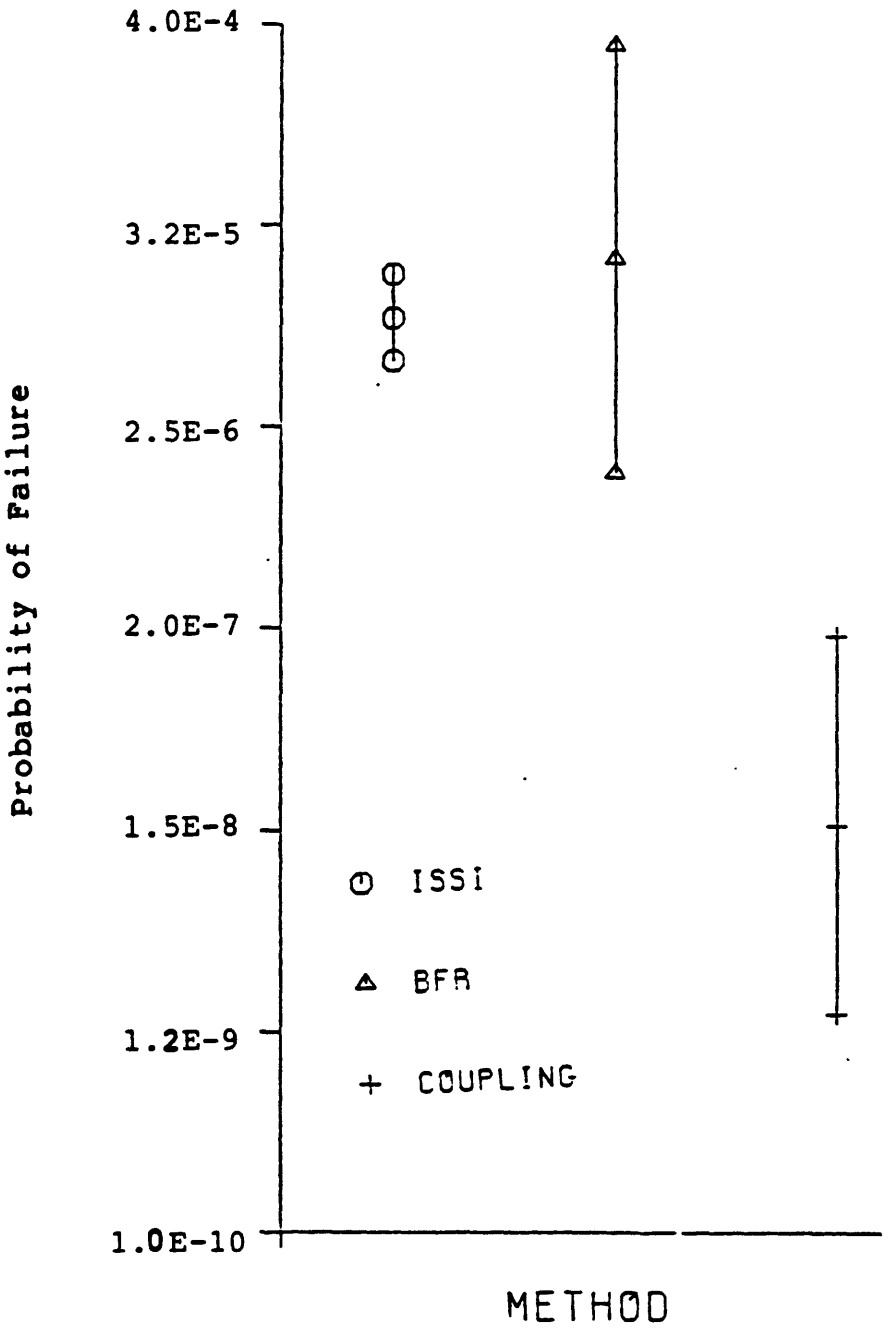


Figure 6.13 CCF Range Estimates: Check Valve, k Equal to 2 (Fail to Open)

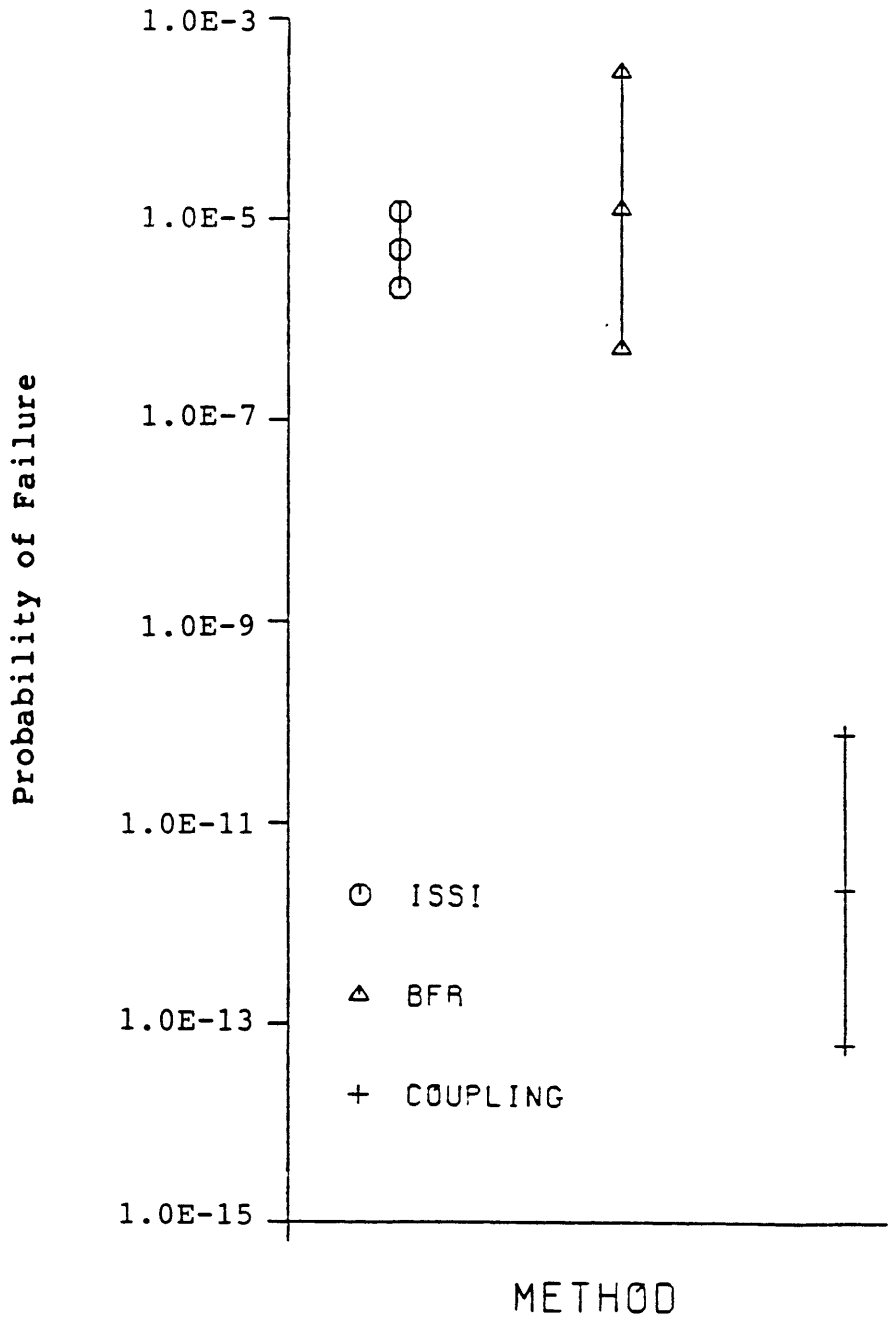


Figure 6.14 CCF Range Estimates: Check Valve, k Equal to 3 (Fail to Open)

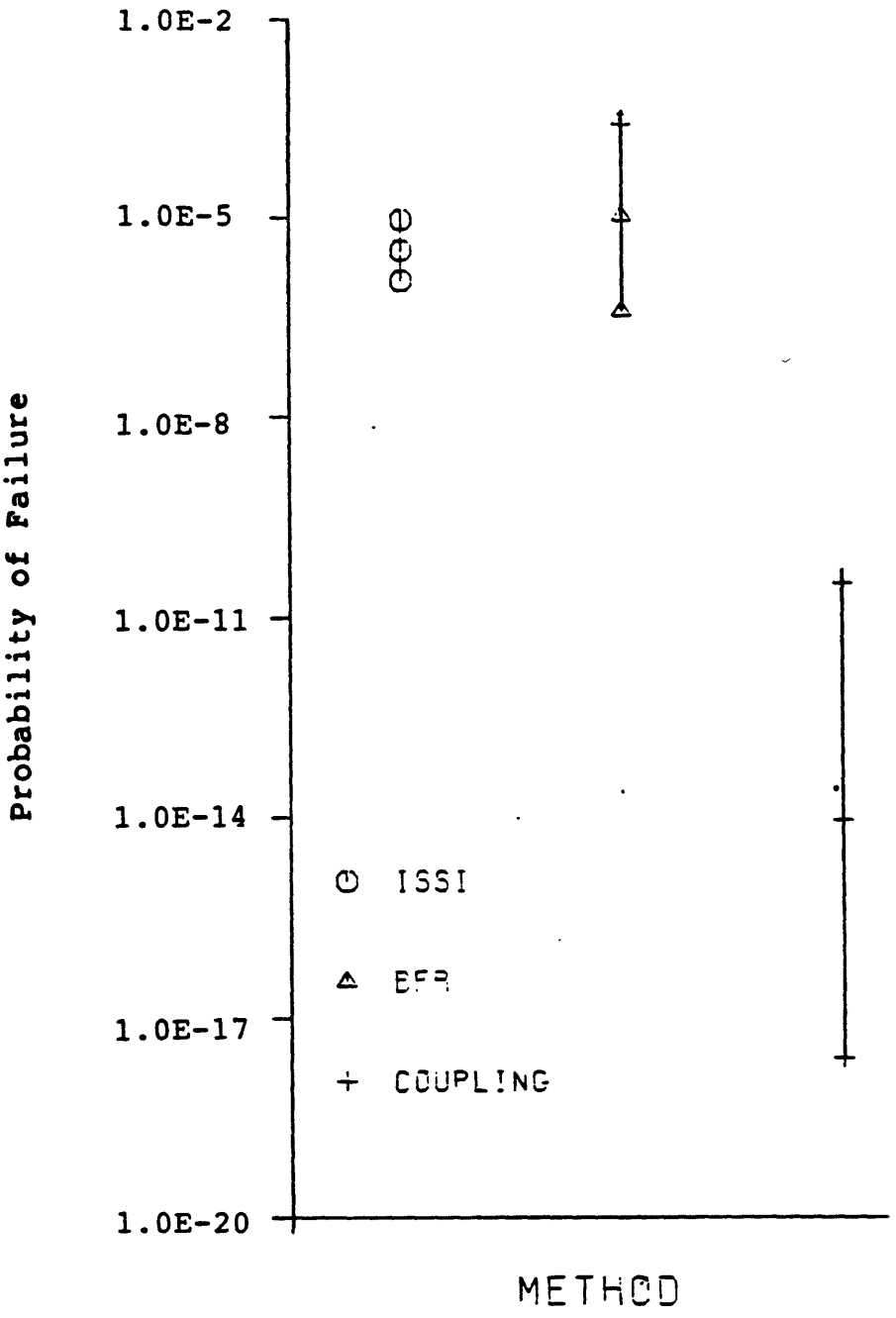


Figure 6.15 CCF Range Estimates: Check Valve, k Equal to 4 (Fail to Open)

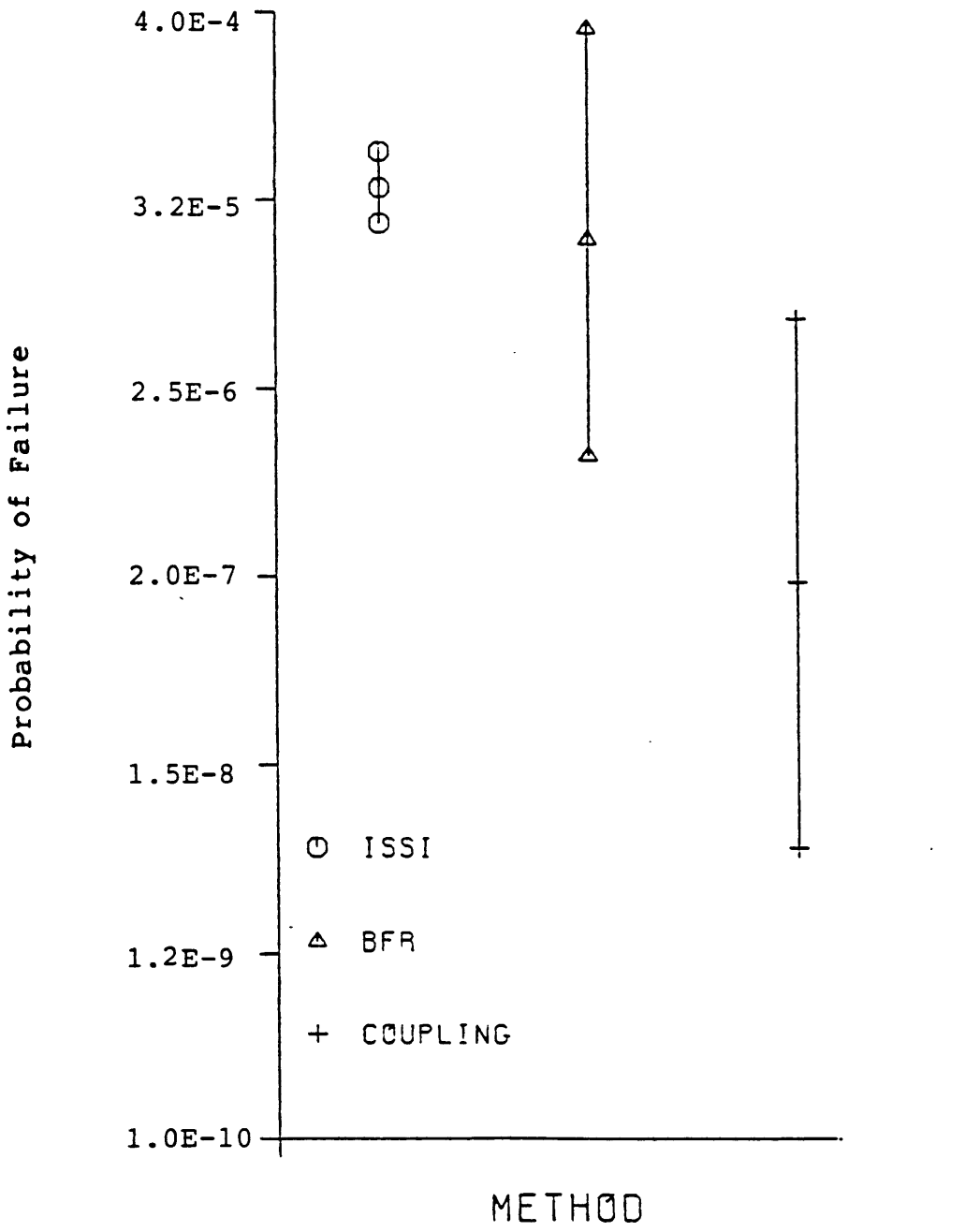


Figure 6.16 CCF Range Estimates: Check Valve, k Equal to 2 (Fail to Close)

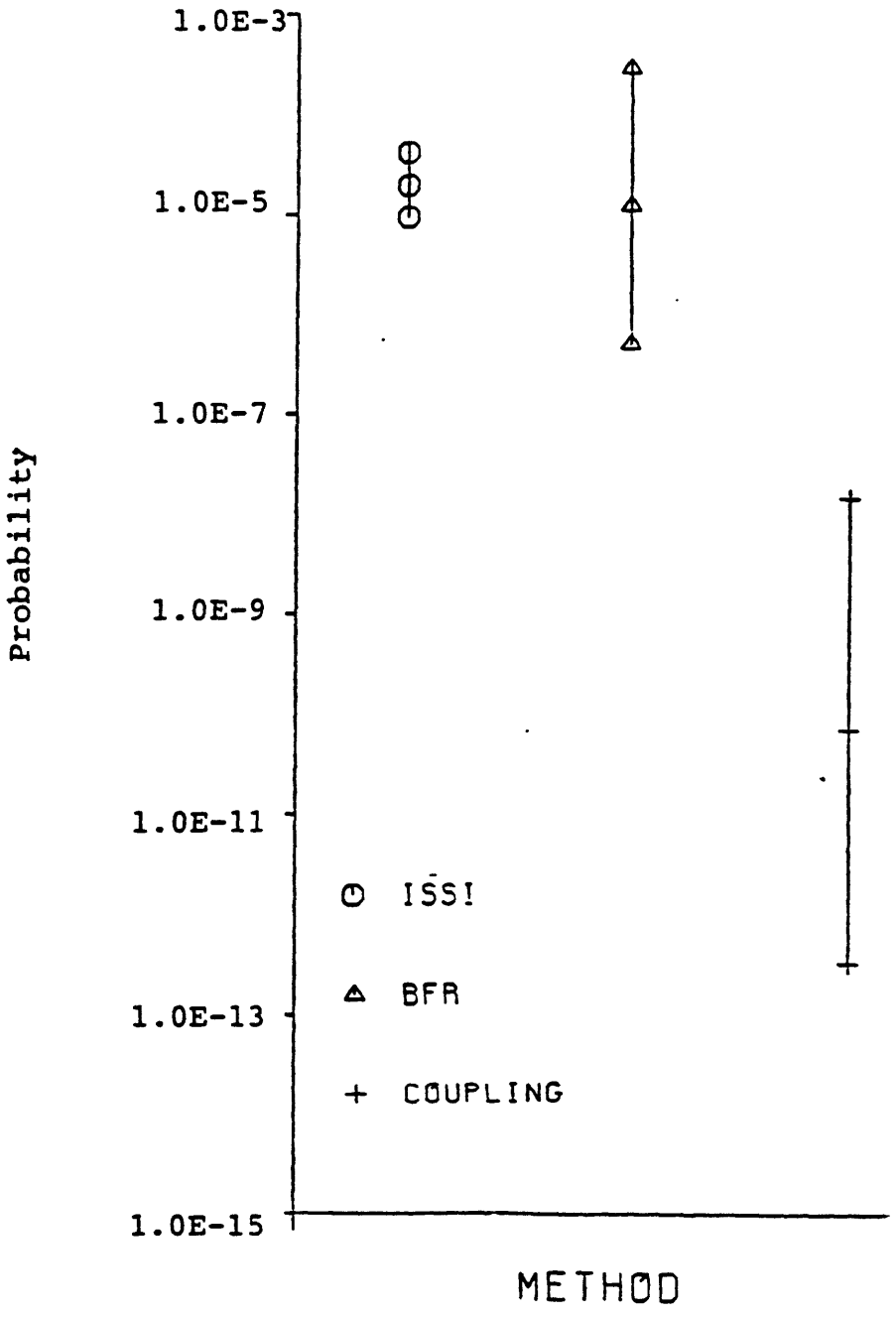


Figure 6.17 CCF Range Estimates: Check Valve, k Equal to 3 (Fail to Close)

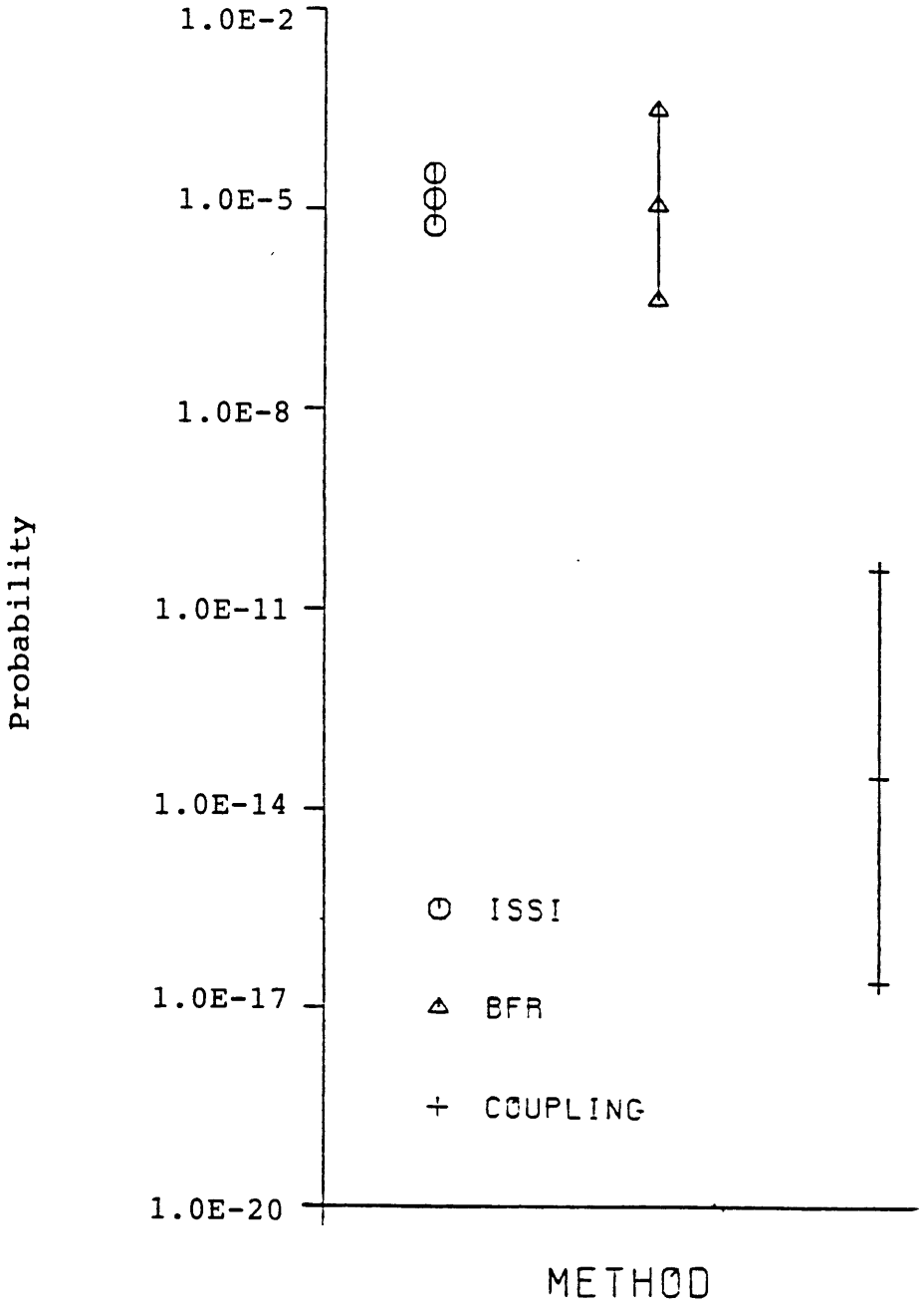


Figure 6.18 CCF Range Estimates: Check Valve, k Equal to 4 (Fail to Close)

higher multiple failure probabilities than either the BFR or the coupling methods. This is because that the ISSI technique includes potential failure causes. The BFR method takes into account only those multiple failures that have been reported to exist. The coupling method assumes that the failure probability is independent. Only the knowledge on the failure probability is coupled. This explains why the coupling method yields wide uncertainty intervals and low median values (same as the median values of the independent case).

2. In general, any approach which is based on more specific knowledge of the process yields a smaller range than an approach with little basis. Since the ISSI approach incorporates essential engineering considerations in the identification of the CCF root causes and the quantification of the stress-strength parameters, a smaller uncertainty is expected to be associated with it. Indeed this is manifested in all the cases studied as shown in Figs. 6.2 through 6.18.
3. The smaller the single failure probability, the greater the uncertainty. This agrees with intuition. Inherently, a rare event gives a very small sample size for statistical inferences. CCF is a rare event. It is thus expected the above trend is obeyed in the results of CCFA models. This is evident in Figs. 6.2 through 6.18. For example, compare Fig. 6.2 with Fig.

6.10. Both the BFR and the coupling methods show a larger uncertainty range for valves than for pumps. However, for the ISSI approach, this trend is less obvious. The statistical nature is hidden one level down in the quantification of the stress-strength parameters. If more data are available, the range on the variability of the stress and strength narrows. This will reduce the range of the mutiple failure probability.

4. The higher the redundancy, the larger the range of the estimates. This follows from the same argument presented above. For higher redundancy, multiple failures are less likely. The sample size to draw inference is then smaller than the case of lower redundancy. Thus one can expect to obtain a wider range of estimated failure probabilities, say, for quadruply than for triply or doubly redundant cases. As an evidence, one can compare Figures 6.2, 6.3 and 6.4. Note the different logarithmic scale in these figures tends to make the effect less apparent; it is still notable, however.

Chapter 7

Application To PWR Standby Safety Systems

7.1 Introduction

The ISSI technique has been illustrated at the component level through the application to pumps and valves in the HPIS and AFWS in commercial nuclear power plants in the previous chapter. This chapter will further demonstrate the same technique at a system level. The demonstration will indicate the significance of various CCF models in affecting the unavailability results.

The sensitivity studies include different levels of complexity in system configuration. Two types of systems are studied. First, a system with 'pure' redundancy is studied. Next, we investigate a combination of various redundancy levels in the system. The former is typified by an idealized AFWS, while the latter is exemplified by a HPIS.

7.2 Idealized AFWS

The AFWS is designed to provide a supply of feedwater to the steam generators during startup operations, during the reactor system initial cooldown period for removal of decay heat from the reactor core and during emergency decay heat removal operations following loss of offsite power. For a complete loss of offsite power, the AFWS performs the vital function of providing flow to the steam generators to remove

any decay heat generated by the core. Each auxiliary feedwater pump is sized on the basis of meeting this condition.

7.2.1 System Description

A typical scematic diagram for AFWS is shown on Fig. 7.1 {7.1}. The AFWS shown consists of two motor-driven, full-capacity auxiliary feedwater pumps and one full-capacity turbine-driven auxiliary feedwater pump, with piping, valves, and associated instrumentation and controls.

For the purpose of this analysis, consider an idealized three-train AFWS. A schematic diagram is shown on Fig. 7.2. The idealized system has three identical trains. Each is composed of a motor-operated valve at the suction and the discharge ends of a motor-operated driven pump.

Studies were performed to check the sensitivity of the system unavailability with respect to:

1. data base
2. CCFA models

7.2.2 Data Base

Although specific data for pumps and valves are not easy to quantify precisely, for the purpose of this study three typical sets of data are used. One other difficulty in the study needs to be noted. This is related to the basis of definition and interpretation with a given set of failure

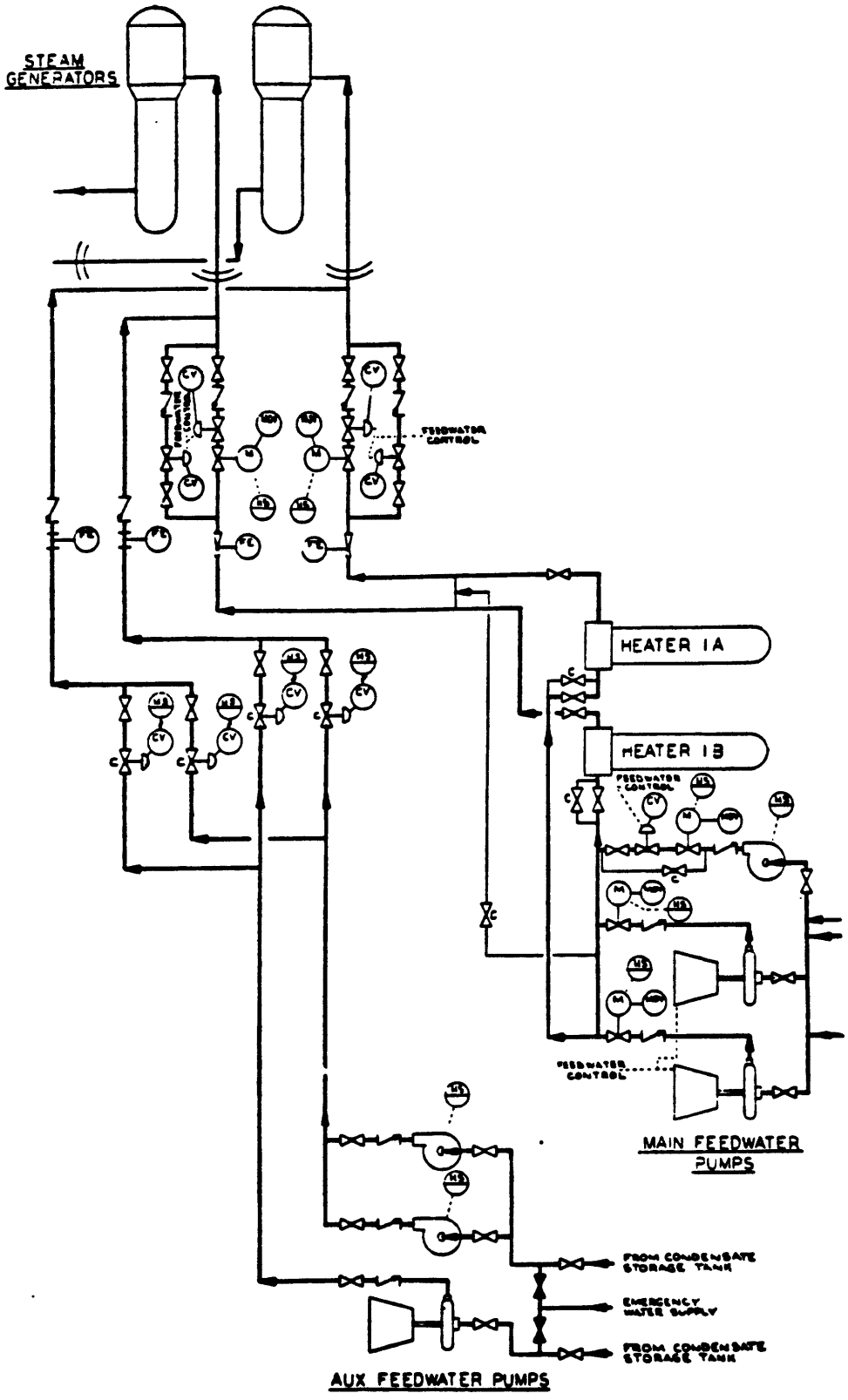


Figure 7.1 A Typical AFWS Schematic Diagram

data. One thus should make sure that the comparison of different data is conducted on an approximately equal basis.

Table 7.1 presents the data used for the AFWS unavailability study. The first set is modified from the Reactor Safety Study (RSS) {7.2}. In the RSS, for standby conditions, no values are given for the failure rates. The approach used in the RSS attributes the failure to demand related mechanisms. In the German Risk Study {7.3}, all the failures are assumed to be due to standby failures instead. The modified RSS data presented in Table 7.1 adopts the failure per demand from the RSS and uses the failure to run for standby failure. The second set of data is taken from a PLG study {7.4}. An additional data set based solely on the failure rate is selected from the LER {7.5,7.6}. It is noted that the main requirement for the choice is that the data base is representative. The results based on these sets of data are thus able to illustrate the general behavior of the realistic system unavailability. For a specific plant analysis, the data may have to be refined to reflect particular features of the plant.

7.2.3 CCF Modelling Techniques Studied

Four CCF methods have been investigated in this study. These are the BFR method, the coupling method, the ISSI technique and the beta factor method. For the ISSI technique, both the normal and the lognormal models are included in the sensitivity analysis. For the beta factor

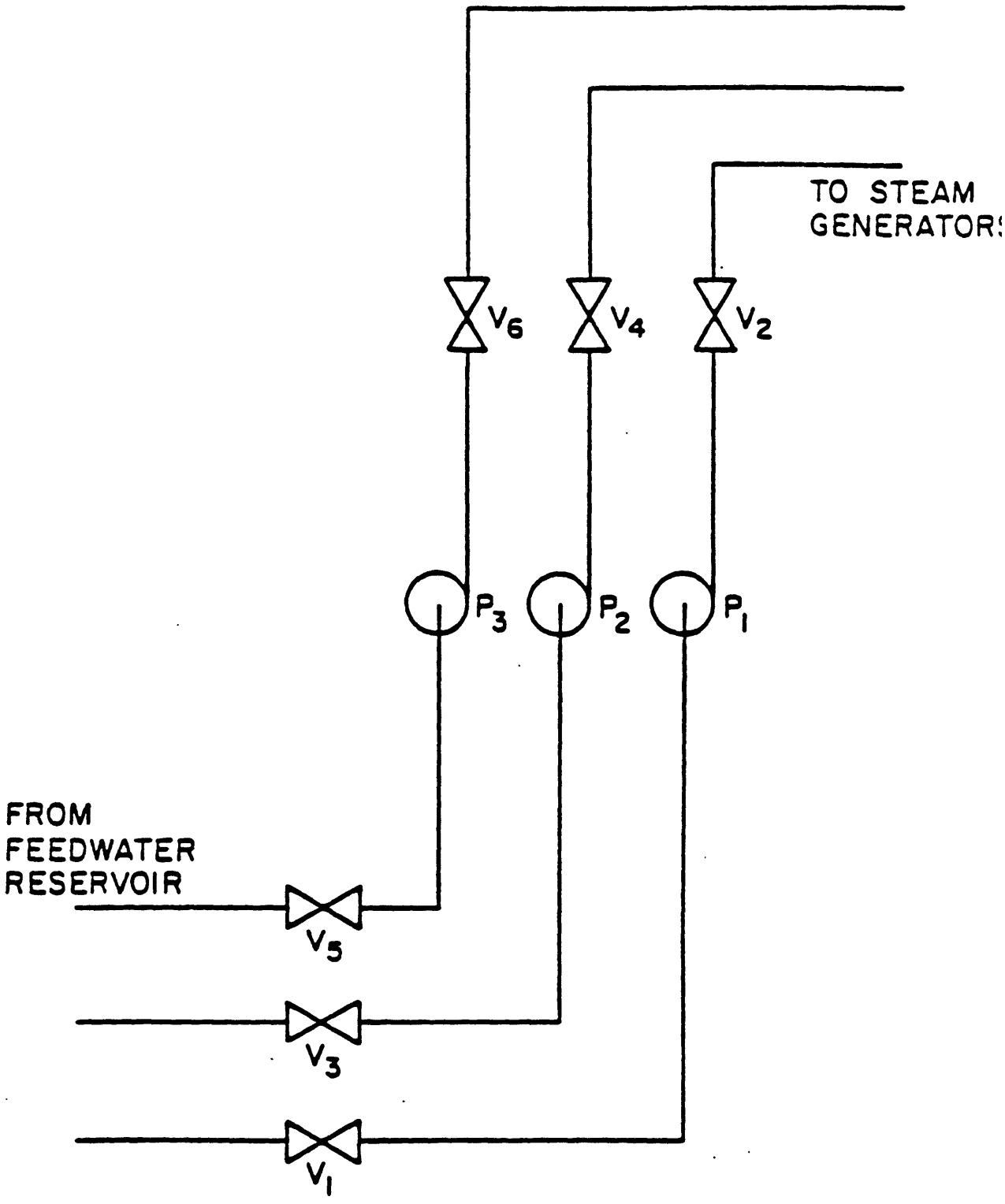


Figure 7.2 An Idealized AFWS Diagram

Table 7.1 Data Base for AFWS Study

Component	Data Type	RSS	PLG	LER
Pump	Failure per Demand			
	Upper	3.0E-3	5.1E-3	0.0
	Lower	3.0E-4	5.8E-4	0.0
	Median	1.0E-3	1.7E-3	0.0
	Failure Rate (/hr)			
	Upper	3.0E-4	5.1E-5	8.5E-6
	Lower	3.0E-6	1.1E-5	3.0E-6
	Median	3.0E-5	2.3E-5	5.5E-6
MOV	Failure per Demand			
	Upper	3.0E-3	5.8E-3	0.0
	Lower	3.0E-4	6.6E-4	0.0
	Median	1.0E-3	2.0E-3	0.0
	Failure Rate (/hr)			
	Upper	1.0E-7	2.4E-7	1.3E-5
	Lower	1.0E-9	8.1E-8	1.3E-7
	Median	1.0E-8	1.4E-7	3.6E-6

method, two cases are considered. One is the conventional practice which takes the beta factor as 0.2 for active components and 0.1 for passive components. The other assumes that the beta factor is obtained via the ISSI approach. These methods are chosen because of their popular use in current PRA studies. The MDFF method and the MGLM are not pursued because there is not a satisfying way of quantifying the parameters in these methods. In fact, it is one of the objectives of this thesis is to obtain an estimate of these parameters.

7.2.4 Uncertainty Analysis

The approach used to perform an uncertainty analysis is identical to that adopted in chapter 6. In this framework, the uncertainty for the estimates of the multiple failure probability of components stems from the uncertainty in the stress and the strength. In particular, the coefficent of variations for the stress and the strength represents a major source of the uncertainty. The uncertainty at the component level then 'propagates' to yield the uncertainty in the final system unavailability.

Two sets of data for the coefficient of the variations of the stress and the strength are used. The upper bound is 0.3 and 0.03, while the lower bound is 0.2 and 0.06. It is expected that as more experts take part in the failure analysis, the range of these stress and strength parameters

can be reduced. The uncertainty in the system unavailability can then be reduced accordingly.

For other approaches, the uncertainty for the system unavailability mainly results from the uncertainty for the single component failure probability. Table 7.2 summarizes the major sources of uncertainty for the CCF modelling techniques studied. Table 7.3 presents the data base used for the uncertainty calculation according to the BFR method. Table 7.4 summarizes the stress and the strength parameters that yield the upper and lower bounds of the system unavailability. It is noted the upper and lower bound is only an indication of the 95th percentile and the 5th percentile of the system unavailability. Since insufficient data exists, it is beyond the scope of this thesis to perform more rigorous uncertainty analysis based on advanced statistical methods.

7.2.5 Results

By applying the expressions for multiple failure probability derived in the preceding chapters and using the combinatorial analysis, the system unavailability is readily computed. It is noted that the idealized AFWS analyzed is simple enough that no sophisticated fault tree analysis computer programs are required. Instead, the combinatorial analysis which identifies major combinations of pumps and valves to cause failure is used.

Table 7.2 Summary of Sources of Uncertainty

Method	Source of Uncertainty Considered
Independent	Variation of Single Failure Probability
BFR	Variation Due to Sample Size
Coupling	Variation of Single Failure Probability
ISSI	Uncertainty in Stress and Strength Model (a) Form of the Distribution (b) Parameter Values
Beta Factor Conventional	Variation in Single Failure Probability
Based on ISSI	Same as ISSI

Table 7.3 Data for Uncertainty Analysis: BFR Method

Multiplicity (k)	Pump (/hr)			Valve (/hr)		
	Upper	Median	Lower	Upper	Median	Lower
k=1	8.5E-6	5.5E-6	3.0E-6	1.3E-5	3.6E-6	1.3E-7
k=2	2.3E-6	8.9E-7	7.5E-8	3.3E-7	8.8E-8	5.0E-10
k=3	1.9E-6	6.4E-7	1.7E-8	2.7E-7	7.2E-8	3.0E-10

Table 7.4 Data for Uncertainty Analysis: ISSI Method

Parameter	Upper	Lower
Coefficient of Variation (Stress)	0.3	0.2
Coefficient of Variation (Strength)	0.03	0.06

Figure 7.3 shows the time-dependent AFWS unavailability based on three methods: the ISSI, the square root, and the beta factor. The beta factor used in this case is based on that derived from the ISSI technique. It can be seen that the beta factor method gives higher values than ISSI method. Since the MDFF method and the MGLM yield the same system unavailability as the ISSI technique, the beta factor method gives higher failure probability than these methods. This illustrates the proposition discussed in chapter 3 that the beta factor method results in higher failure probability than the multiple-train approaches. The square root method, indicated in the Figure as SRT, yields the lowest (probably underestimates) system unavailability.

Figure 7.4 shows similar results as Figure 7.3, except that the former is based on the lognormal model while the latter on the normal model. As discussed before, the lognormal model yields a higher failure probability than the normal model.

Figure 7.5 presents the time-dependent beta factor for the AFWS pumps and valves. The decomposition of the failure data into a standby failure rate and a failure probability per demand affects the magnitude of the beta factor. In the case of valves, since the standby failure rate used is small, on-demand failure probability dominates. This gives rise to an essentially constant beta factor. For pumps, since the standby failure rate used is relatively large, the beta factor is time-dependent.

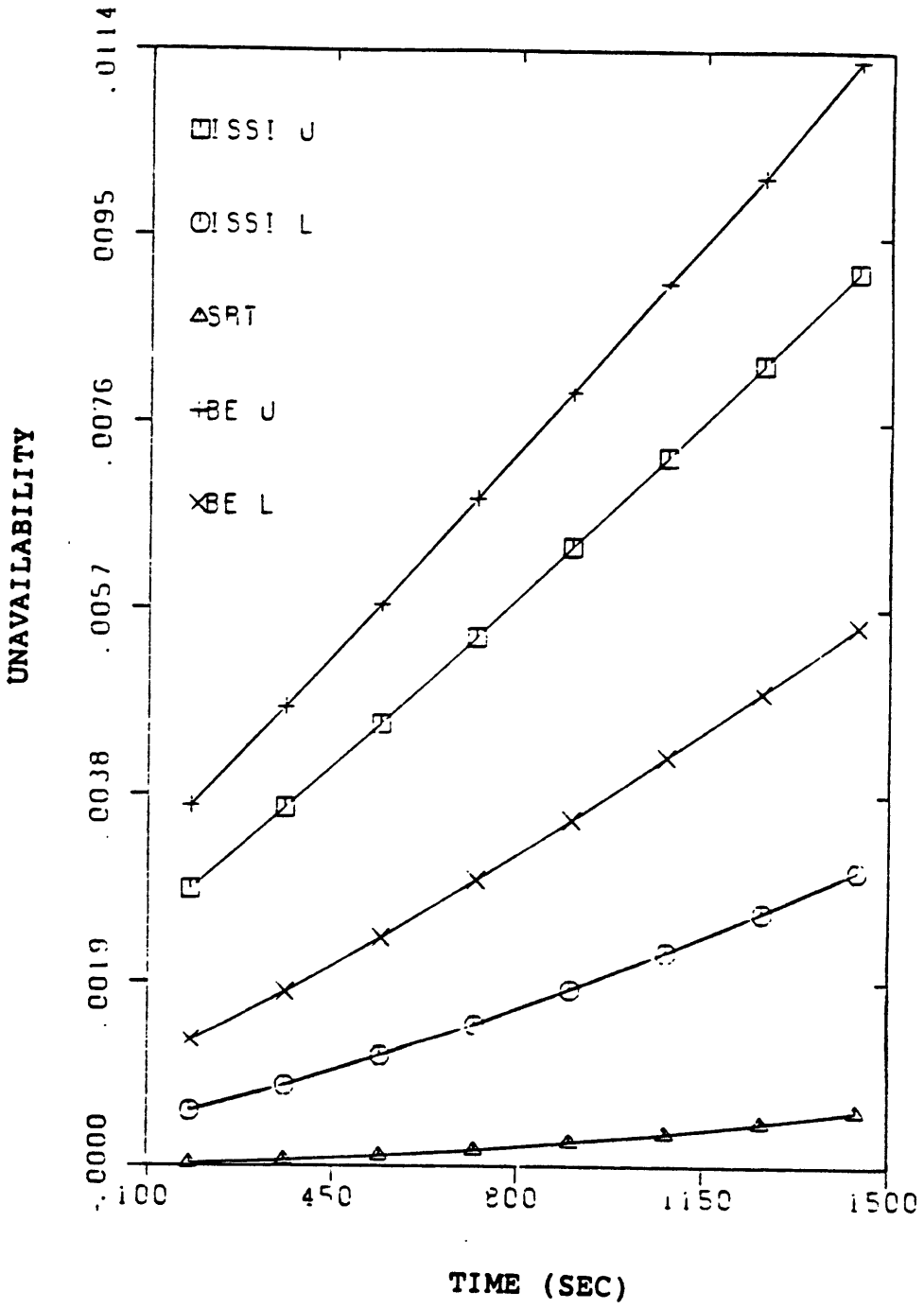


Figure 7.3 Time-dependent AFWS Unavailability: Normal Model

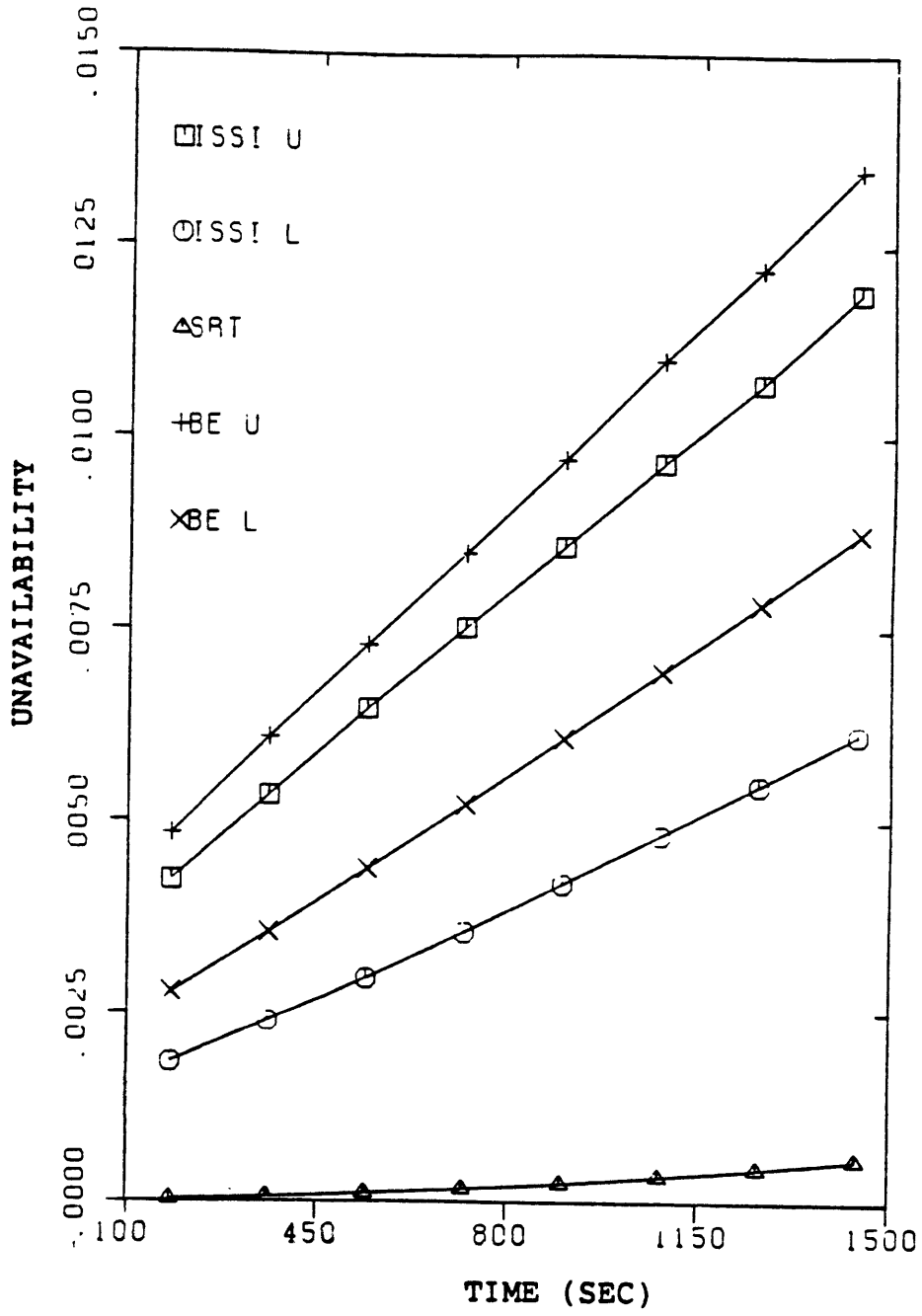


Figure 7.4 Time-dependent AFWS Unavailability: Lognormal Model

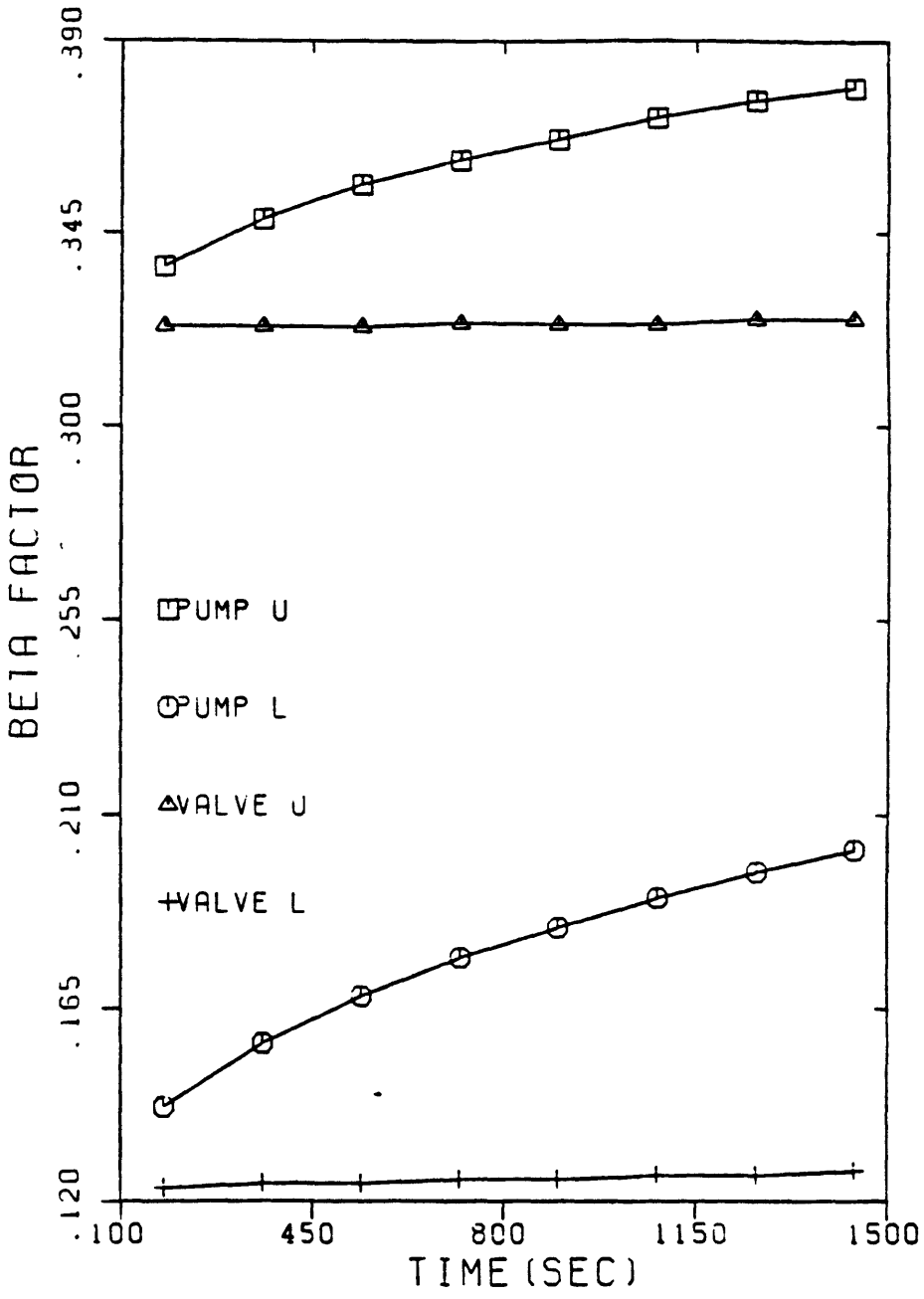


Figure 7.5 Time-dependent Beta Factor for AFWS Pumps and Valves

Table 7.5 illustrates the effect of input data variation on the AFWS unavailability. The unavailability based on the LER is initially smaller than that based on the modified RSS data. This is because of the lower demand failure probability associated with the LER. However, as time evolves, the higher standby failure rate associated with the LER data yields a higher system unavailability.

Table 7.6 illustrates a similar trend for the beta factor associated with pumps. This is again due to the nature of the standby and on-demand failure data as discussed above. For valves, shown in Table 7.7, the beta factor does not change with time for both the PLG and the modified RSS data.

Table 7.8 summarizes the AFWS unavailability based on different CCFA methods. As can be seen, a factor of 5000 may result due to the different approach used. For the case assuming independence, the results can be a factor of 10 different due to the variation of input data used. For the cases including CCF, the difference in results due to the modelling techniques can be a factor of 50 or larger. In addition, the difference between the upper and lower estimates vary with the methods used. In the case of the BFR method and the coupling method a factor of 100 and larger is observed. In the case of the ISSI approach, the uncertainty range is only a factor of 10 or less.

Table 7.5 Time-dependent AFWS Unavailabilities

Time(Sec)	PLG	RSS	LER
180.0	6.24E-3	2.88E-3	1.88E-3
360.0	7.09E-3	3.66E-3	4.05E-3
540.0	7.96E-3	4.52E-3	6.35E-3
720.0	8.86E-3	5.40E-3	8.72E-3
1440.0	1.26E-2	9.15E-3	1.88E-2

Table 7.6 Time-dependent Beta Factor Via ISSI: AFWS Pumps

Time (Sec)	PLG	RSS
180.0	0.142	0.136
360.0	0.157	0.154
540.0	0.168	0.167
720.0	0.177	0.177
900.0	0.184	0.186
1080.0	0.191	0.193
1260.0	0.197	0.199
1440.0	0.202	0.205

Table 7.7 Time-dependent Beta Factor Via ISSI: AFWS MOVs

Time (Sec)	PLG	RSS
180.0	0.123	0.099
360.0	0.124	0.099
540.0	0.124	0.099
720.0	0.125	0.099
900.0	0.125	0.099
1080.0	0.126	0.100
1260.0	0.126	0.100
1440.0	0.127	0.100

Table 7.8 AFWS Unavailabilities Via Various Methods

Method	Upper	Median	Lower	Data Source
Independent	4.5E-5	3.1E-6	2.2E-7	PLG
	3.0E-5	2.7E-7	2.5E-9	LER
BFR	3.4E-3	1.7E-4	8.8E-6	LER
Coupling	1.1E-3	1.7E-4	2.8E-5	PLG
	1.3E-2	1.9E-4	2.8E-6	RSS
ISSI(Normal)	8.9E-3	4.6E-3	2.4E-3	PLG
	5.4E-3	2.4E-3	1.1E-3	RSS
ISSI(Lognor)	1.2E-2	8.3E-3	5.8E-3	PLG
	7.5E-3	5.2E-3	3.6E-3	RSS
Beta Factor				
(0.2,0.1)	9.9E-3	3.9E-3	1.5E-3	PLG
	2.6E-2	3.7E-3	5.2E-4	RSS
ISSI(Nor)	1.1E-2	7.2E-3	4.7E-3	PLG
	6.8E-3	4.5E-3	3.0E-3	RSS
ISSI(Logn)	1.4E-2	1.1E-2	8.5E-3	PLG
	8.5E-3	6.6E-3	5.2E-3	RSS

The general characteristics of different CCF modelling techniques as exemplified in the AFWS study is summarized as follows:

1. In the case of assuming independence between identical components, the variation in input data affects the system unavailability significantly. While for the cases accounting for CCFs, this variation does not have as strong effect as the difference in various CCFA models.
2. The BFR method yields lowest system unavailability among all CCF modelling techniques studied.
3. The coupling method yields a largest range of system unavailability.
4. The ISSI method results in smallest range of system unavailability.
5. In the ISSI approach, the normal model yields a lower system unavailability than the lognormal model.
6. The conventional beta factor method yields system unavailability estimates within a factor of two smaller than the ISSI method.
7. The beta factor derived from the ISSI method gives greater system unavailability than the ISSI method. This is expected because the beta factor does not take into account partial failures.

7.3. Two-train High Pressure Injection System

The AFWS analyzed in the previous section represents one of the most important standby systems in a nuclear power plant. Another important standby system is the HPIS which is a part of the engineered safeguards. In this section, the HPIS that typifies a three-loop plant designed by Westinghouse is studied.

7.3.1 System Description

The two-train HPIS utilizes the pumps and a portion of the piping of the makeup and purification system to provide cooling water from borated water storage tank (BWST) to the reactor coolant system. A simplified schematic diagram for important components is shown in Figure 7.6.

The following assumptions are made in the analysis:

1. A minimum of two injection lines is assumed to be sufficient to pass full flow for the analyzed state.
2. All the HPIS support systems are available and an actuation signal is applied to both trains from the emergency core cooling actuating system.
3. No credit is taken for operator to recover failed equipment or to provide flow from alternate sources over the period of this analysis.
4. The mission time for the HPIS is 24 hours and the test interval is two months for pumps, 18 months for valves.
5. Human errors during the maintenance and testing is not considered.

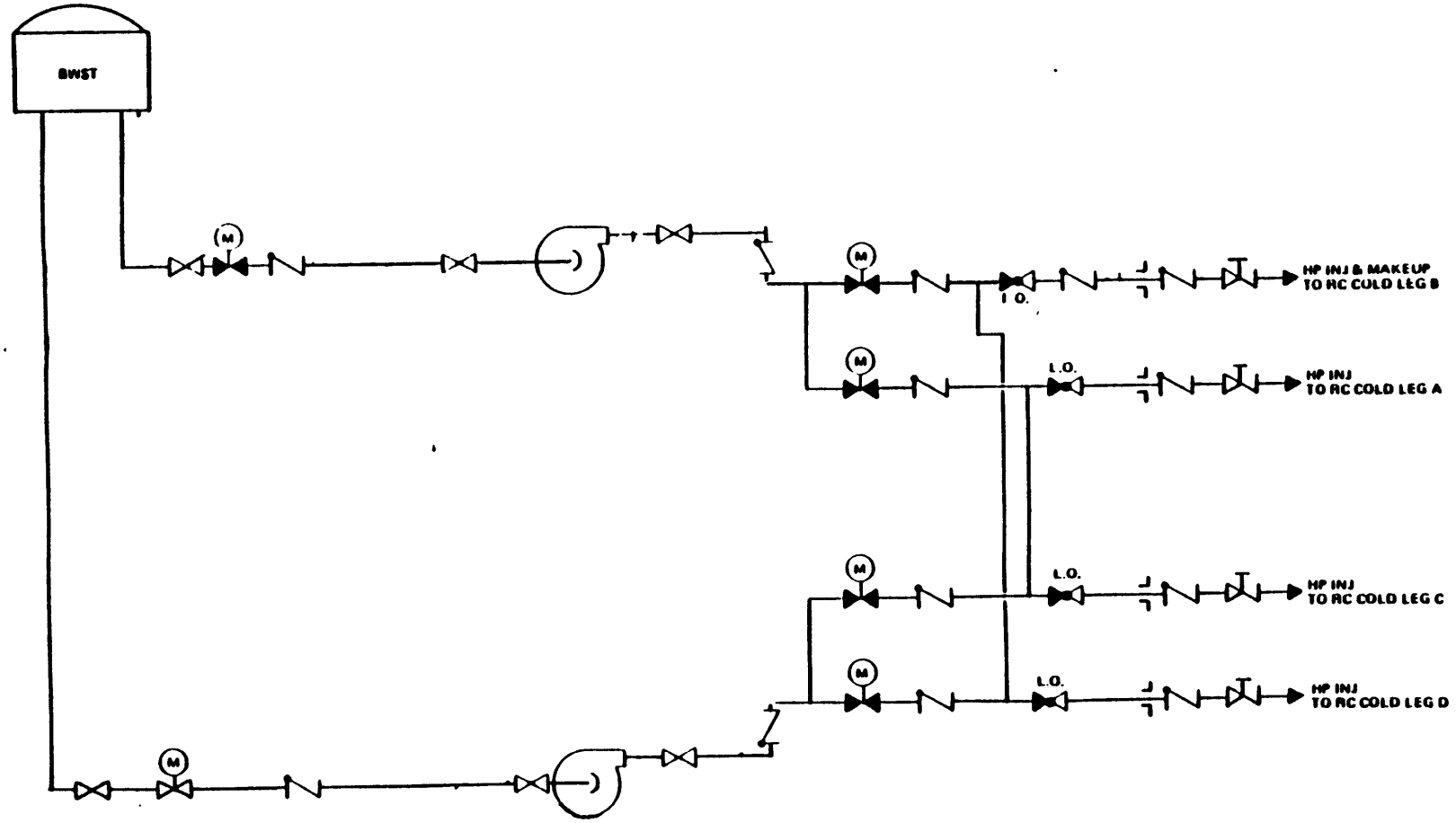


Figure 7.6 A Typical Two-train HPIS Schematic Diagram

For the calculation of the HPIS unavailability, the following expression is used:

$$F_s = Q_{od} + \lambda_h \tau_t + \lambda_{h'} \tau_0 \qquad (7.3.1)$$

where

Q_{od} = unavailability on demand of a subsystem or a component

τ_t = test interval divided by two

τ_0 = system mission time

λ_h = subsystem or component standby failure rate

$\lambda_{h'}$ = subsystem or component running failure rate

The component unavailability is then input into the system equivalent fault tree or a reliability expression to obtain the total system unavailability. Figure 7.7 shows a simplified reliability block diagram for the two-train HPIS. By an application of combinatorial principle or fault tree analysis, the total HPIS unavailability expression Q is:

$$Q = (S1 + PA)\,(S2 + PB) + (S1 + PA)\,(C \times D) + C(B1 + D1) + (D(A1 + C1) + (S2 + PB)\,(A \times B) + A(B1 + D1) + B(A1 + C1) + Q_3 + Q_4, \qquad (7.3.2)$$

where

$$Q_3 = (A \times C)\,(B1 + D1) + (B \times D)\,(A1 + C1) + (A1 \times B1 \times C1) + (A1 \times B1 \times D1) + (A1 \times C1 \times D1) + (B1 \times C1 \times D1)$$

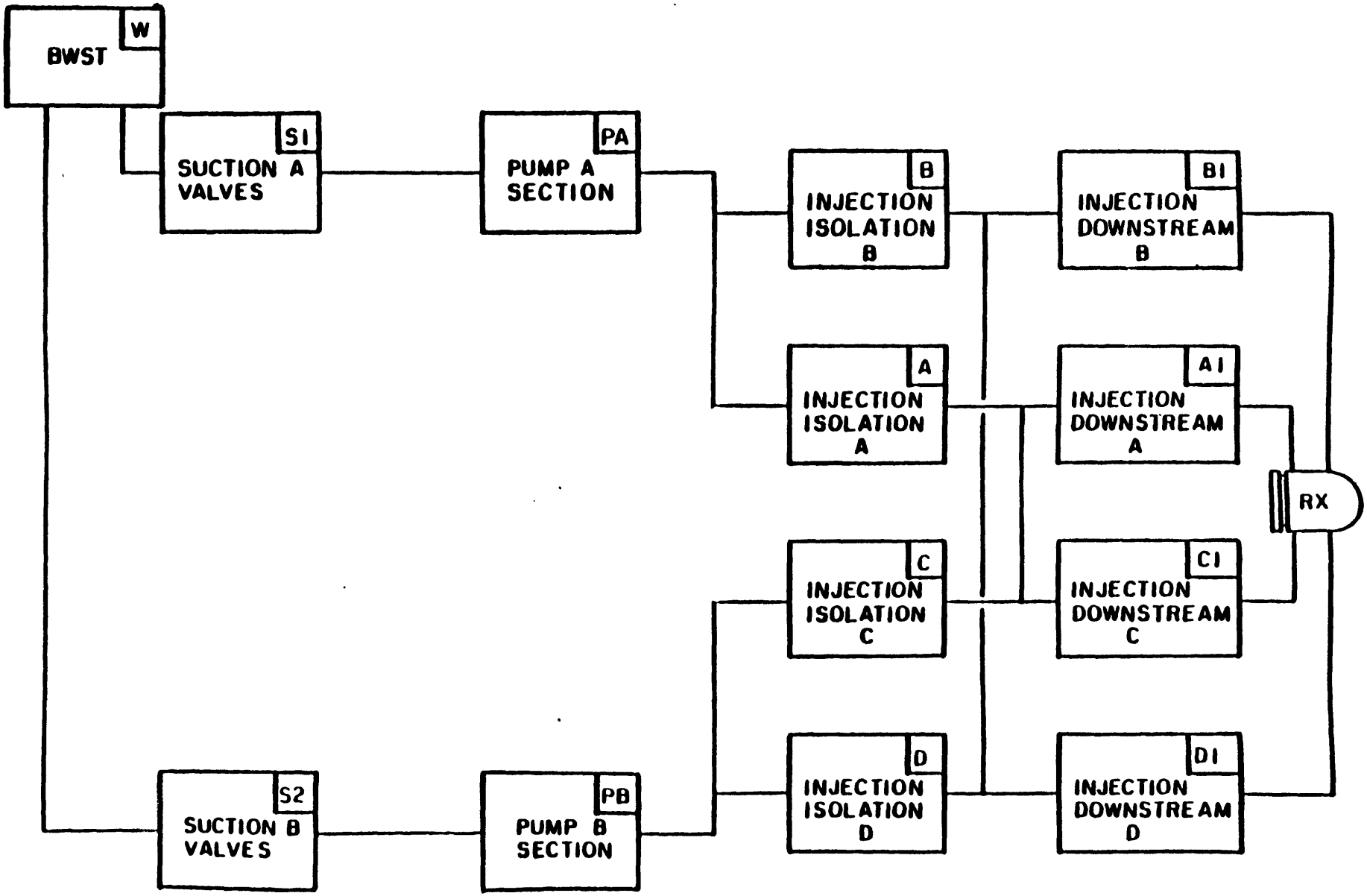


Figure 7.7 Two-train HPIS Reliability Block Diagram

and

$$Q_4 = (A \times C)\ (B1 \times D1) + (B \times D)\ (A1 \times C1) + (A \times Bx\ Cx\ D) + (A1 \times B1 \times C1 \times D1).$$

The subsystems shown in Figure 7.7 can be decomposed into several 1-out-of-n configurations, shown in Figure 7.8.

7.3.2 Data Base

The failure data used for the two-train HPIS is shown in Table 7.9. The RSS and PLG data do not distinguish components in different systems. Thus the pump and the MOV data are identical to those used in the AFWS study. The LER data, however, recognizes the system and the configuration to which the components belong. Thus, the data for pumps and valves in the HPIS are differnt from those in the AFWS.

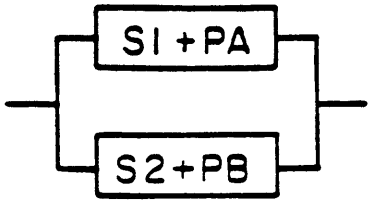
7.3.3 CCF Modelling Techniques Studied

Four different CCFA methods are applied. These are the same methods used for the AFWS study.

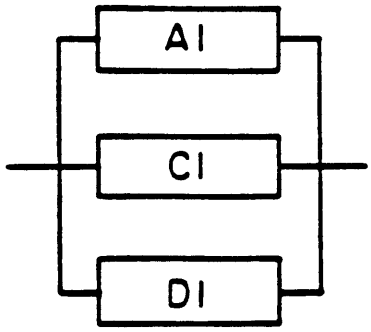
7.3.4 Uncertainty Bounds

The same approach for computing the upper and lower system unavailability used for the AFWS is adopted in this study. The minor modifications stems from the stress-strength parameters for the pumps. Since the LER recognizes the difference in the system to in which the pumps reside, a different fraction of the total failure

(a) 1 OUT OF 2 UNIT SYSTEM



(b) 1 OUT OF 3 UNIT SYSTEM



(c) 1 OUT OF 4 UNIT SYSTEM

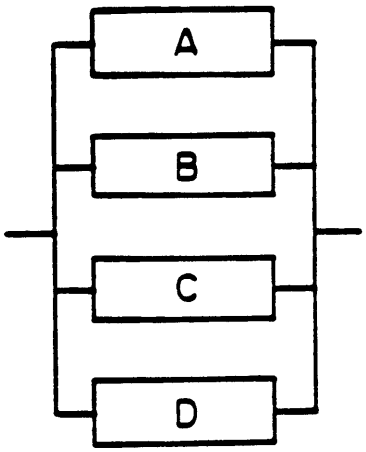


Figure 7.8 Abbreviated Subsystem Configurations for the HPIS

Table 7.9 Data Base for 2-train HPIS Study

Component	Data Type	RSS	PLG	LER
Pump	Failure per Demand			
	Upper	3.0E-3	5.1E-3	0.0
	Lower	3.0E-4	5.8E-4	0.0
	Median	1.0E-3	1.7E-3	0.0
	Failure Rate (/hr)			
	Upper	3.0E-4	5.1E-5	8.5E-6
	Lower	3.0E-6	1.1E-5	3.0E-6
	Median	3.0E-5	2.3E-5	5.5E-6
MOV	Failure per Demand			
	Upper	3.0E-3	5.8E-3	0.0
	Lower	3.0E-4	6.6E-4	0.0
	Median	1.0E-3	2.0E-3	0.0
	Failure Rate (/hr)			
	Upper	1.0E-7	2.4E-7	1.3E-5
	Lower	1.0E-9	8.1E-8	1.3E-7
	Median	1.0E-8	1.4E-7	3.6E-6
CKV	Failure per Demand			
	Upper	3.0E-4	7.2E-4	0.0
	Lower	3.0E-5	7.7E-5	0.0
	Median	3.0E-3	2.4E-4	0.0
	Failure Rate (/hr)			
	Upper	1.0E-7	2.4E-6	4.0E-7
	Lower	1.0E-9	2.5E-8	3.7E-8
	Median	1.0E-8	2.4E-7	1.2E-7

probability is attributed to the various causes as discussed in Chapter 6.

7.3.5 Results

Figure 7.9 presents time-dependent unavailability for the HPIS based on three different CCF modelling techniques. The beta factor used in this case is that derived on the basis of the ISSI approach. It is evident that the beta factor yields a higher value for the system unavailability. The SRT method gives a factor of ten or so lower estimate of the unavailability.

Figure 7.10 presents results similar to Figure 7.9. The former, however, is based on the lognormal model, while the latter is based on the normal model. The results indicate that the lognomal model yields a higher failure probability, consistent with the obsevation made in Chapter 6.

Table 7.10 summarizes the HPIS unavailability based on various methods. Several features can be noted:

1. The difference between the independent case and the cases including CCFs is not as strong as for the AFWS study. This is because the HPIS is essentially a doubly redundant system, while the AFWS is a triply redundant configuration.
2. The BFR method gives the highest uncertainty range. This is an exemplification that the statistical procedures give little information in the case of small sample size.

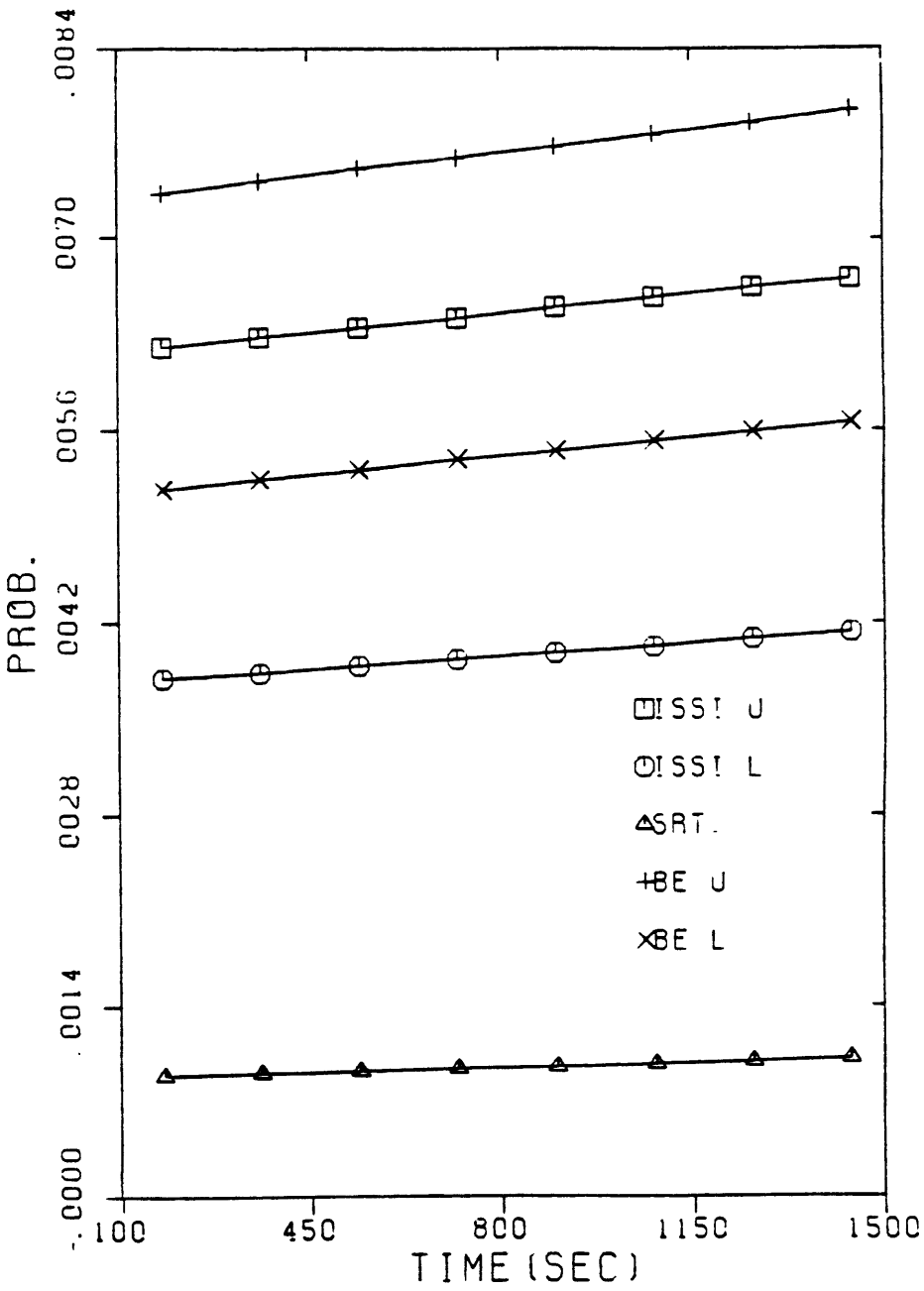


Figure 7.9 Time-dependent HPIS Unavailability: Normal Model

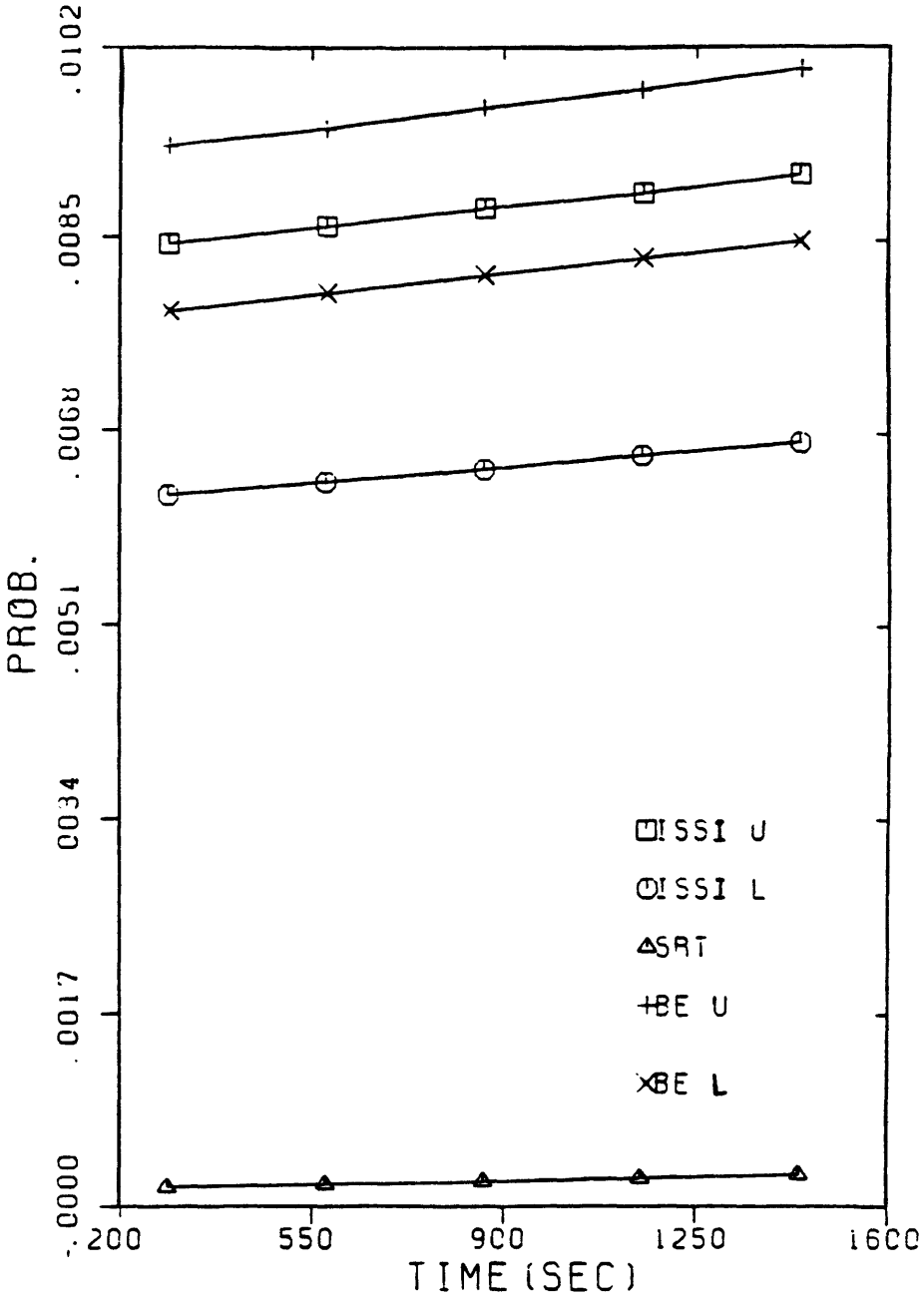


Figure 7.10 Time-dependent HPIS Unavailability:
Lognormal Model

Table 7.10 2-train HPIS Unavailabilities Via Various Methods

Method	Upper	Median	Lower	Data Source
Independent	3.5E-4	6.2E-5	1.1E-5	PLG
	2.2E-4	1.3E-5	7.2E-7	RSS
BFR	8.7E-2	2.0E-3	4.7E-5	LER
Coupling	1.7E-3	4.3E-4	1.1E-4	PLG
	1.5E-3	1.9E-4	2.5E-5	RSS
ISSI(Normal)	6.7E-3	5.2E-3	4.1E-3	PLG
	2.4E-3	1.4E-3	7.6E-4	RSS
ISSI(Lognor)	9.1E-3	7.8E-3	6.7E-3	PLG
	3.4E-3	2.5E-3	1.8E-3	RSS
Beta Factor				
(0.2,0.1)	5.3E-3	2.2E-3	8.8E-4	PLG
	3.9E-3	9.5E-4	2.3E-4	RSS
ISSI(Nor)	7.9E-3	6.7E-3	5.7E-3	PLG
	2.8E-3	1.6E-3	9.7E-4	RSS
ISSI(Logn)	1.0E-2	9.2E-3	8.5E-3	PLG
	3.6E-3	2.7E-3	2.1E-3	RSS

3. The coupling method seems to yield lower values than other CCFA methods. For higher redundancies, to be discussed in section 7.4, this effect is even stronger.
4. The ISSI approach seems to give somewhat higher values than the BFR. This may stem from the consideration of all the failure causes and not just the events that have actually occurred, as considered in the BFR. In addition, the uncertainty interval associated with the ISSI is the narrowest among all CCFA methods. This is likely due to the engineering considerations that have been incorporated as demonstrated in the previous chapter.
5. The ISSI method can be used to estimate beta factors. The factor so calculated are compared to normally used values of the beta factor. It is interesting to note that in this 2-train case the values from the different methods are within a factor of 2.

7.4 Four-train High Pressure Safety Injection System

The major difference between the HPIS studied in section 7.3 and the 4-train HPSI system is the addition of two HPSI pump trains. The design typifies a four-loop plant designed by Westinghouse.

7.4.1 System Description

The major components of the 4-train high pressure safety injection (HPSI) system are the charging and HPSI pumps, along with the associated piping, valves and control circuitry.

Two of the three charging pumps are normally used for the chemical and volume control system. These two pumps are rotated on a monthly basis so that one pump is always operating. When the safeguards actuation signal is received, the injection mode of operation is automatically initiated. The non-operating charging pump is started and both it and the running pump are realigned to take suction from the refueling water storage tank (RWST), discharging into the reactor coolant system (RCS) cold legs (one in each of the four RCS loops). As a simplification, the analysis only models two of the three charging pumps.

During the normal operation, the two HPSI pumps are not in operation but are prealigned to the RWST. When the safeguards actuation signal is received, both pumps start, taking suction from the RWST and discharging to the RCS cold legs.

A simplified diagram of the HPSI system appears in Figure 7.11. The results of the two-train HPIS studied in the previous section indicate that the dominant contributors to the system unavailability come from the pumps and valves upstream of the injection header, not from the injection trains. In this analysis, we analyze the system including only the components upstream of the injection header. Since

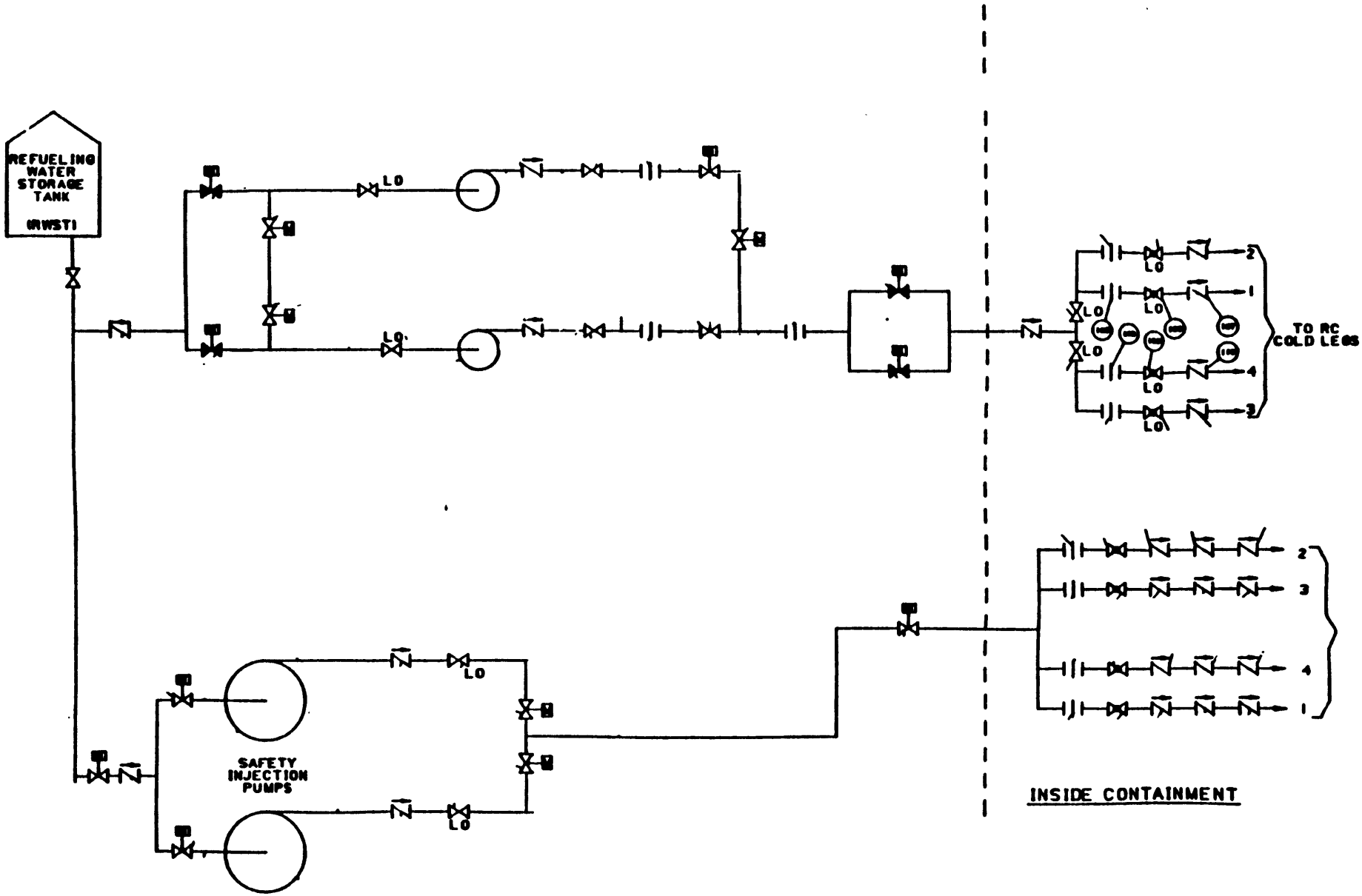


Figure 7.11 A Typical Four-train HPIS Schematic Diagram

the MOVs in the HPSI pump trains are prealigned to the RWST and are normally open, they are ignored in the unavailabilitycalculation. The HPSI system thus essentially reduces to a four-train system. Figure 7.12 shows the reliability block diagram for this system.

Two cases are analyzed. The first assumes that the charging pumps and the HPSI pumps are independent, denoted as a diverse case. The other considers that the charging pumps and the HPSI pumps are identical, denoted as redundant case.

7.4.2 Data Base

Table 7.11 summarizes the failure data used for the four-train HPSI system. The components S1 and S2 refer to the suction valves upstream of the charging pumps. D1 and D2 refer to the discharge valves downstream of the charging pumps. P1 and P2 refer to the charging pumps. P3 and P4 refer to the HPSI pumps. The results of the two-train HPIS analysis suggest that these are the only significant contributors. The data presented in Table 7.11 is thus sufficient to calculate the system unavailability.

7.4.3 CCF Modelling Techniques Considered

For both the diverse and redundant cases, the four methods studied in the previous sections are included. These are the BFR, the coupling, the ISSI and the beta factor methods.

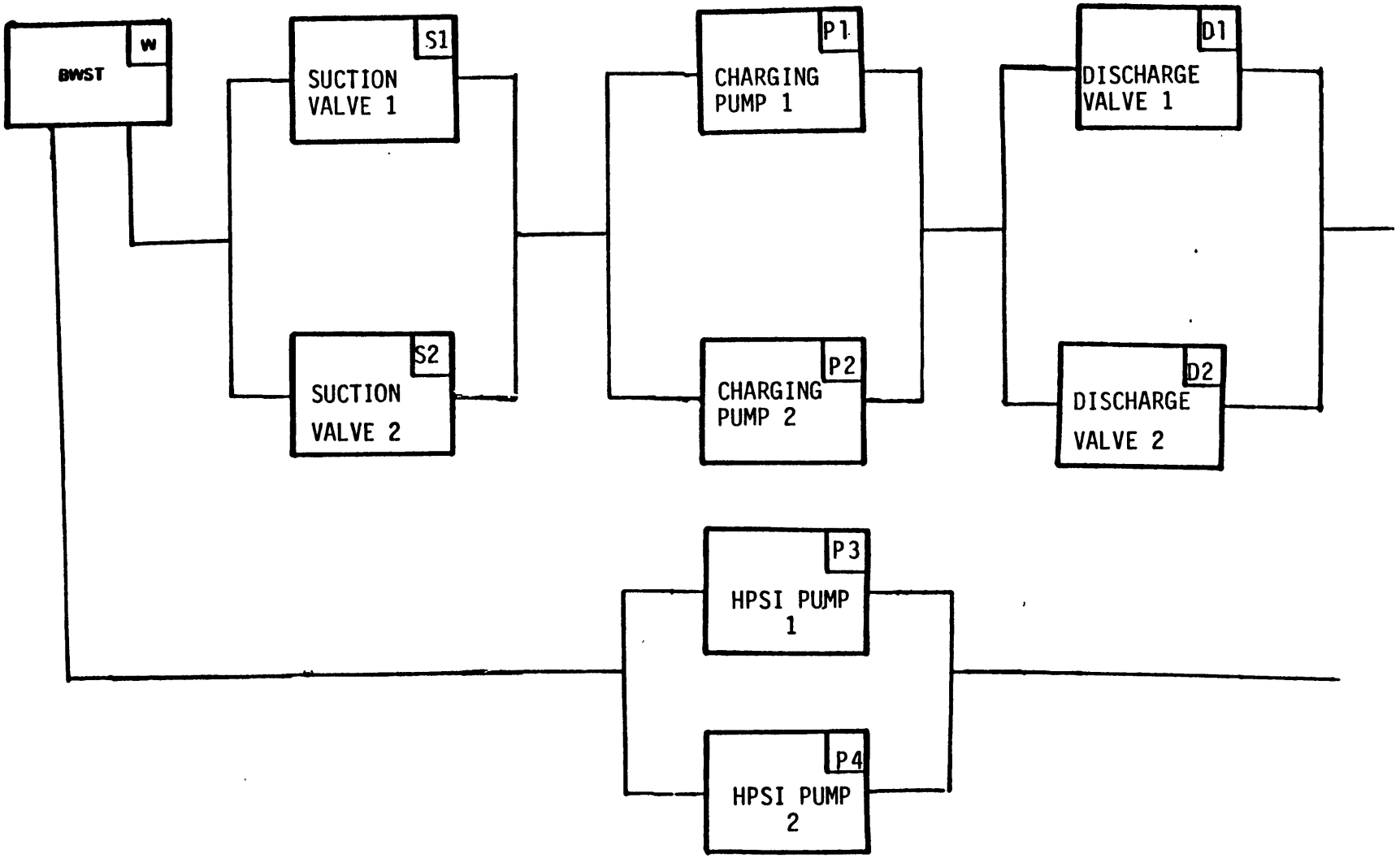


Figure 7.12 Four-train HPIS Reliability Block Diagram

7.4.4 Uncertainty Analysis

The approach adopted in the uncertainty bound calculation is identical to that used in previous sections. For the ISSI technique, the same set of the stress-strength parameters is used. For other approaches, the upper and lower values of failure probability presented in Table 7.11 are used.

7.4.5 Results

Table 7.12 and Table 7.13 summarize the system unavailability obtained by adopting various methods for the diverse and the redundant case, respectively. It is of interest to compare the 4-train and 2-train HPIS.

Results indicate that a drastic reduction, for the diverse case, in the system unavailability for all the CCFA methods except the coupling method. This suggests that the coupling method seems to underestimate the unavailability by almost a factor of 10,000.

The general trend observed previously still holds:

1. The ISSI technique yields a smallest uncertainty interval estimates for the system unavailability.
2. The beta factor, given the same information as the ISSI, gives most conservative estimates.
3. The BFR method consistently produces smaller system unavailability than the ISSI approach and the beta factor method. In addition, the uncertainty associated with the BFR method is larger than the

Table 7.11 Data Base for 4-train HPIS Study

Component	Upper	Median	Lower
S1	7.0E-4	5.7E-4	4.6E-4
S2	7.0E-4	5.7E-4	4.6E-4
D1	9.7E-3	1.1E-3	1.3E-4
D2	9.7E-3	1.1E-3	1.3E-4
P1	2.9E-3	1.3E-3	5.8E-4
P2	2.9E-3	1.3E-3	5.8E-4
P3	6.9E-3	2.1E-3	6.4E-4
P4	6.9E-3	2.1E-3	6.4E-4

Table 7.12 4-train HPIS Unavailabilities
Via Various Methods: Diverse Case

Method	Upper	Median	Lower	Data Source
Independent	4.9E-9	1.1E-11	2.3E-14	Table 7.11
BFR	5.1E-7	1.5E-9	4.3E-12	LER
Coupling	6.4E-7	1.6E-8	4.1E-10	Table 7.11
ISSI(Normal)	6.4E-7	2.2E-7	7.5E-8	Table 7.11
ISSI(Lognor)	1.1E-6	6.4E-7	3.7E-7	Table 7.11
Beta Factor				
(0.2,0.1)	2.4E-6	4.9E-7	1.0E-7	Table 7.11
ISSI(Nor)	6.4E-7	2.2E-7	7.5E-8	Table 7.11
ISSI(Lognor)	1.1E-6	6.4E-7	3.7E-7	Table 7.11

Table 7.13 4-train HPIS Unavailabilities
Via Various Methods: Redundant Case

Method	Upper	Median	Lower	Data Source
Independent	4.9E-9	1.1E-11	2.3E-14	Table 7.11
BFR	3.2E-4	1.2E-6	4.3E-7	LER
Coupling	1.0E-6	9.1E-8	8.2E-9	Table 7.11
ISSI(Normal)	2.6E-4	9.4E-5	3.4E-5	Table 7.11
ISSI(Lognor)	4.4E-4	2.6E-4	1.5E-4	Table 7.11
Beta Factor				
(0.2,0.1)	1.6E-3	5.4E-4	1.8E-4	Table 7.11
ISSI(Nor)	6.9E-4	4.2E-4	2.6E-4	Table 7.11
ISSI(Logn)	8.9E-4	5.3E-4	3.1E-4	Table 7.11

ISSI method or the beta factor method.

4. The coupling method yields the smallest system unavailability and the largest uncertainty compared with other methods.

5. The ISSI method can be used to estimate beta factors. The factor so calculated are compared to conventional values of the beta factor. It is interesting to note that in this 4-train case the median for the conventional method is even closer to those based on the ISSI methods.

Chapter 8

Conclusions And Recommendations

8.1 Conclusions

We have established that the difficulties associated with the CCFA arise from i) discrepancies in the definition, ii) the lack of an appropriate data base, and iii) the choice of adequate modelling techniques. The scarcity of the CCF occurrences due to the highly reliable performance of the nuclear safety systems makes the statistical approaches inefficient. The discrepancies of the CCF definition impede the progress of the CCFA. The choice of adequate CCF modelling techniques baffles reliability analysts since no single technique can cover every aspect of the CCFs. Furthermore, because of the sparseness of data, no useful criterion can serve as a measure of the adequacy of a particular model.

The conventional beta factor method does not take into account partial failures. For multiple-train (i.e. three or more trains) systems, the more realistic approach would be either the MDFF method or MGLM. However, there is a serious lack of adequate data to determine the parameters in these methods.

The ISSI technique proposed in this thesis represents a step forward in modelling the failures due to association of identical components during their entire life cycle, a

special kind of CCF. The data requirement is inherently different from that of statistical approaches. Instead of making use of life-time data, the stress and the strength corresponding to root causes are identified and quantified. This approach thus combines the engineering knowledge and statistical procedures to quantify the multiple failure probabilities. The parameters in the MDFF method and the MGLM can then be evaluated by converting the multiple failure probability based on the ISSI method.

Based on the LER coding scheme for failure occurrences, we have identified tribological mechanisms and foreign material contamination as two major failure contributors. The coefficient of variation used for the calculation of CCF probabilities were obtained from wear-related literature. The engineering considerations indicate that the value of the coefficient of variation for the stress is 0.2 - 0.5, while that for the strength is 0.03 -0.06.

Applications to the pumps and valves in nuclear power plants also indicate that the uncertainty in the unavailability estimates of the components seems greatly reduced. This in turn leads to the narrowing of the range of the unavailability estimates for systems that are composed of redundant pumps and valves.

For multiple-train systems, this study showed that CCFs reduce drastically the system availability that is based on the assumption of independent failures. The coupling method yields an unresonably low value of multiple failure

probability. The BFR method takes into account partial failures, but possesses large uncertainty. The ISSI approach gives results with least uncertainty, although the median values for multiple failure probability so obtained are slightly higher.

This study suggests that the ISSI method is a promising alternative to estimate CCF probabilities. The method will be particularly valuable when:

(1) Component-specific and system specific values are needed.

(2) Failure data are scarce.

(3) Level of redundancy is high.

(4) Uncertainty needs to be quantified.

8.2 Recommendations

The recommendations based on the present investigation pertain to three areas:

1. CCF Modelling

- Use the ISSI techniques more widely

The results of this study suggest that the ISSI technique captures the essence of the coupled failures. In addition, by incorporating the engineering knowledge, one not only reduces the uncertainty but also obtains substantial insights into the significant factors that control the failures. It is thus recommended that the ISSI techniques be more widely used to evaluate CCFs for highly reliable systems.

2. Engineering Practices

- Devote more attention to tribology and cleanliness

We have identified tribological and foreign material contamination as two major contributors for CCFs. It is recommended that more research effort be dedicated to the consideration of these failure causes to reduce the probability of failures. The CCF probability will then be reduced accordingly.

- Include uncertainty statements in engineering studies

By its very nature, every engineering process exhibits statistical fluctuations. This variation with respect to space and time is mainly due to hidden conditions or causes beyond our control. In order to get a feel for the degree of confidence for a given experiment or analysis, it is useful

to state the uncertainty associated with the endeavor. This uncertainty statement can then be used in the ISSI framework to facilitate the CCFA. Additionally, by conscientiously quantifying the uncertainty, one can identify where to spend the time and effort most effectively.

- Develop more cooperation between engineers and statisticians

Based on the illustration described in Chapter 6, one recognizes that engineers play an important role in interpreting, identifying and quantifying the failure causes. On the other hand, statisticians provide efficient tools to determine the single component failure probability. It is thus important to coordinate the perspectives of the engineers and those of statisticians to obtain realistic results efficiently. It appears that the prevailing practice is that once the LER have been codified, the engineer seems not to participate in the data analysis.

3. Future Work

- Extend the ISSI approach to cascade failures

Throughout this study, we have focused attention only on the coupled failures. The cascade failures have been neglected due to the limitation of information. To model cascade failures, as indicated previously, require a substantial advancement in our understanding about the stresses imposed on the intact by the failed components. Few studies have addressed this subject.

- Extend the ISSI approach to accident conditions

An example of accident condition is the loss of service water. This would give rise to a severe environmental condition for the HPIS pumps and the charging pumps, because of the loss of lube oil cooling. Additional research in this area would be useful for the equipment qualification under severe conditions.

- Extend the ISSI approach to human errors

It has been recognized that human errors play a crucial role in the performance of the standby safety systems. If managerial procedures would not eliminate human error at all, it would be of interest to understand and evaluate the factors that influence the performance of operators in various tasks. The CCF probability could then be assessed by adopting the ISSI approach. A great deal of knowledge needs to be improved before this can be achieved, however.

REFERENCES

Chapter 1

1.1 WASH-1400

"Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix III, Failure Data", U.S. Atomic Commission, Washington D.C., September 1974

1.2 H.W.Lewis., et.al.

"Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commision", NUREG/CP-1400, September, 1978

1.3 "Automatic Scram Fails At Salem", Nuclear Engineering International, May 1983, p3

1.4 "Lessons Learned From Salem", Nuclear Engineering International, June 1983, pp.13-14

1.5 J.A.Hartung

"A Statistical Correlation Model And Proposed General Statement of Theory for Common Cause Failure", PRA Meeting, Portchester, N.Y., 1981, pp.640-648

Chapter 2

2.1 A.M. Smith and I.A. Watson

"Common Cause Failures- A Dilemma in Perspective", 1980 Proceedings of Annual Reliability and Maintainability Symposium, pp.332-339

2.2 I.A. Watson

"The Rare Event Dilemma and Common Cause Failures", 1982 Proceedings of Annual Reliability and Maintainability Symposium, pp.5-10

2.3 D.M. Rasmuson, G.R. Burdick, and J.R. Wilson
"Common Cause Failure Analysis Techniques: A Review and Comparative Evaluation", TREE-1349, September,1979

2.4 WASH-1400
"Reactor Safety Study: An Assessment of Accident Risks in Commercial Nuclear Power Plants", NUREG-75/104, October, 1975

2.6 J.A. Hartung
"A Statistical Correlation Model And Proposed General Statement of Theory for Common Cause Failure", PRA Meeting, Portchester, N.Y., 1981, pp.640-648

2.5 J.K. Vaurio
"Structures for Common Cause Failure Analysis", PRA Meeting, Portchester, N.Y., 1981, pp.676-685

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

2.8 David Worledge
"Common Cause Failures", EPRI Journal, July/August 1983 pp.62-64

2.9 S.Hirshberg
"Limitations And Critical Comparison of Methods for Quantitative Analysis of Common Cause Failures", Workshop on Dependent Failure Analysis, Vasteras, 27-28 April,1983

2.10 M.L. Shooman
"Probabilistic Reliability: An Engineering Approach", McGraw-Hill, 1968

2.11 I.A. Papazoglou

"Markovian Reliability Analysis Under Uncertainty With An Application of The Shutdown System of The Clinch River Breeder Reactor", Ph.D. Dissertation, November 1977, Department of Nuclear Engineering, Massachusetts Institute of Technology

2.12 K.N. Fleming et.al.

"HTGR Accident Initiation Progression Analysis Status Report ", Vol.II, General Atomic Report GA-13617, October, 1975

2.13 W.E. Vesely

"Estimating Common Cause Failure Probability in Reliability and Risk Analysis : Marshall-Olkin Specialization", Proceedings, International Conference on Nuclear Systems Reliability Engineering and Risk Assessment, Gatlinburg, Tennesse, June,1977

2.14 A.W. Marshall and I. Olkin

"A Multivariate Exponential Distribution", JASA, 62 1967, pp.30-44

2.15 J.W. Johnson and W.E. Vesely

"Common Mode Analysis of Valve Leakages", ANS Topical Meeting on Probabilistic Analysis of Nuclear Power Plants, Newport Beach, Calif, May 1978,

2.16 J.A. Steverson and C.L. Atwood

"Common Cause Failure Rates Estimates for Diesel Generators in Nuclear Power Plant", 1981 PRA Meeting, Portchester, N.Y.

2.17 G. Apostolakis and S. Kaplan
"Pitfalls in Risk Calculations", Reliability Engineering, 2 (1981), pp.135-145

2.18 R.A. Evans
"Statistical Independence in Calculating the Reliability of Redundant Systems", ASQC Journal of The Electronics Division, pp.14-19, January 1966

2.19 A.M. Breipohl
"Statistical Independence in Reliability Equations", Proceedings of the Eighth National Symposium on Reliability and Quality Control, January 1962 pp.1-6

2.20 R.A. Evans
"Problems in Probability", Proceedings of Symposium on Reliability, 1965, pp.347-353

2.21 R.G. Eastering
"Probabilistic Analysis of Common Mode Failures" ANS Topical Meeting on Probabilistic Analysis of Nuclear Power Plants, Newport Beach, Calif, May 1978
Probabilistic Risk Assessment Meeting, Portchester, N.Y., 1981

Chapter 3

3.1 M.G. Stametalatos
"Improved Method for Evaluating Common Cause Failure Probabilities", p.474, Transactions of ANS Winter Meeting, Nov. 14-18, 1982

3.2 K.N. Fleming, and A.M. Kalinowski
"An Extension of the Beta Factor Method for Systems

with High Levels of Redundancy", PLG-0289, August 1983

3.3 Carolyn D. Heising and Ching N. Guey
"A Comparison of Methods for Calculating System Unavailability Due to CCFs: The Beta Factor and MDFF Methods", Reliability Engineering, 8 (1984), pp.1-16

Chapter 4

4.1 D.Kececioglu
"Mechanical Reliability Research Needs", in Reliability, Stress Analysis and Failure Prevention Methods in Mechanical Design, .W.D.Milestone, Edited, pp.153-167

4.2 RADC/RBRAC
"Nonelectronic Parts Reliability Data", Reliability Analysis Center (RAC), Griffiss Air Force Base, N.Y., 13441, 1978

4.3 Green,A.E., and Bourne, A.J.
"Reliability Technology", John Wiley and Sons, Inc., New York, 1972

4.4 WASH-1400
"Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix III, Failure Data.", U.S. Atomic Commision, Washington D.C., October, 1975

4.5 D.Kececioglu, and D.Cormier
"Designing a Specified Reliability into a Component", Proceedings of The Third Annual SAE-ASME-AIAA Aerospace Reliability and Maintainability Conferrence,

Washington D.C., 1964, pp. 546-565

4.6 D.Kececioglu

"Reliability Analysis of Mechanical Components and Systems", Nuc. Eng. and Des., 19, (1972), pp. 259-290

4.7 E.Vanmarcke

"Random Fields Analysis and Synthesis", M.I.T. Press, 1983

4.8 A.M.Freudenthal et.al.

"The Analysis of Structural Safety", Journal of Structural Division, Proceedings of The A.S.C.E., February, 1966, pp.267-325

4.9 E.B.Haugen

"Probabilistic Mechanical Design", John Wiley and Sons, 1980

4.10 A.A.Mittenbergs

"The Material Problems in Structural Reliability", Annals of Reliability and Maintainability, 1966

4.11 J.M.Hudson, and J.H.Wiggins

"Common Mode Failures in Nuclear Power Plants", Proceedings Annual Reliability and Maintainability, 1981

4.12 R.P. Kennedy, et.al.

"Probabilistic Seismic Safety Study of an Existing Nuclear Power Plant", Nuc. Eng. and Des., 59, (1980), pp. 315-338

4.13 S. Kaplan, et.al.

"A Methodology for Seismic Risk Analysis of Nuclear

Power Plants ", NUREG/CP-0027, Vol. 1, 1982

4.14 C.A. Cornell, and N.M. Newmark
"On the Seismic Reliability of Nuclear Power Plants", ANS Topical Meeting on Probabilistic Analysis of Nuclear Power Plants, Newport Beach, California, 1978

4.15 Kapur, K.C., and Lamberson, L.R.
"Reliability in Engineering Design", John Wiley and Sons, New York, 1977

4.16 A.D.S. Carter,
"The Interaction Between Some Simple Load And Strength Distributions", Jnl. Instn. Qual. Assurance, 1979, 5, pp.3-8

4.17 J.R. King
"Probability Charts for Decision Making", Industrial Press Inc., 1972

4.18 B.S. Dhillon
"Mechanical Component Reliability Under Environmental Stress ", Microelectronics and Reliability Vol.20, 1980, pp.153-160

4.19 B.S. Dhillon
"Mechanical Reliability : Interference Theory Models", Proceedings Annual Reliability and Maitainability Symposium, 1980, pp. 462-467

4.20 B.S. Dhillon, C.L. Proctor and E.A.R. Elsayed
"Stress-Strength Reliability Analysis of A Redundant System", Reliability Stress Analysis, and Failure Prevention Methods in Mechanical Design,

edited by W.D.Milestone, pp.9-11

4.21 W.K. Chung

"Some Stress-Strength Reliability Models", Microelectronics and Reliability, Vol.22, No.2, 1982, pp.277-280

4.22 R.P. Zemanick, and F.J. Witt

"An Engineering Assessment of Probabilistic Structural Reliability Analysis", Nuc. Eng. Des., 50, (1978), pp.173-183

4.23 P.H. Wirshing

"On The Behavior of Statitical Models Used For Design ", ASME paper 75 WA/DE28

4.24 M. Shinozuka, et.al.

"On the Reliability of Redundant Structures", Proceedings of 6th Int. Symp. on Space Technology and Science, 1965, Tokyo

4.25 M. Shinozuka, et.al.

"On the Reliability of Redundant Structures", Annals of Reliability and Maintainability, 1966

4.26 T. Mankamo

"Common Cause Failure of Reactor Pressure Components", Proceedings of a Symposium, Vienna 10-13, October 1977, Reliability Problems of Reactor Pressure Components

4.27 G.K. Bhattacharyya, and R.A. Johnson,

"Stress-Strength Models for System Reliability", Reliability and Fault Tree Analysis, SIAM, 1975, pp.509-532

Chapter 5

5.1 D.Kececioglu

" Reliability Analysis of Mechanical Components and Systems ", Nuc. Eng. and Des., 19, (1972), pp. 259-290

5.2 T.Mankamo

" Common Cause Failure of Reactor Pressure Components ", Proceedings of a Symposium, Vienna 10-13, October 1977, Reliability Problems of Reactor Pressure Components

Chapter 6

6.1 J.A. Collins

"Failure of Materials in Mechanical Design", John Wiley and Sons, 1981

6.2 G.E. Dieter

"Engineering Design, A Materials and Processing Approach", McGraw-Hill, Inc., 1983

6.3 F.A. McClintock and A.S. Argon

"Mechanical Behavior of Materials", Addison-Wesley, 1966

6.4 D.D. Reiff

"NRC Activities Related to Pump and Valve Operability", ASME paper 80-c2/PVP-31, 1980

6.5 C.L. Atwood

"Common Cause Fault Rates for Pumps", NUREG/CR-2098, February, 1983

6.6 M. Trojovsky

"Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants", NUREG/CR-1205, Revision 1, January, 1982

6.7 K.C. Ludema

"A Perspective on Wear Models", ASTM Standardization News, September 1974, pp.13-17

6.8 E. Rabinowicz

"The Physics and Chemistry of Surfaces", ASTM Standardization News, September 1974, pp.18-21

6.9 E. Rabinowicz

"Friction and Wear of Materials", Wiley, New York, 1965

6.10 E. Rabinowicz

"An Adhesive Wear Model Based on Variations in Strength Values", Wear, 63 (1980), pp. 175-181

6.11 E.B. Haugen

"Probabilistic Mechanical Design", John Wiley and Sons, 1980

6.12 R.J. Akers and J.I.T. Stenhouse

"A Theoretical and Experimental Study of Particle Sampling from Hydraulic Systems", C92/76, Instn. Mech. Eng. Conference Publications, 1976

6.13 R.Rimmer

"On the Prediction of the Reliability of Fluid Control System Components Subject to Particulate Contamination", C88/76, ibid.

6.14 J.A Steverson and C.L. Atwood

"Common Cause Fault Rates for Valves", EGG-EA-5485, Revision 1, September 1982

6.15 C.F. Miller et.al.

"Data Summaries of Licensee Event Reports of Valves at

U.S. Commercial Nuclear Power Plants", October, 1982

Chapter 7

7.1 Millstone Nuclear Power Station Unit 2 PSAR, Vol.1, Section 10

7.2 WASH-1400
"Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix III, Failure Data", U.S. Atomic Commission, Washington D.C., October 1975

7.3 A.W. Barsell, and I.B. Wall
"German Risk Study", EPRI-NP-1804-SR, April 1981

7.4 Midland PRA Studies, PLG Report

7.5 C.L. Atwood
"Common Cause Fault Rates for Pumps", NUREG/CR-2098, February, 1983

7.6 J.A Steverson and C.L. Atwood
"Common Cause Fault Rates for Valves", EGG-EA-5485, Revision 1, September 1982

Appendix A

Compuatational Aspects of the ISSI Method

A.1 Introduction

The approach used in this thesis is based on the ISSI method. The method includes two important steps in which numerical calculations are involved. The first is concerned with the inversion of a single failure probability for the component. The other is related to the evaluation of integrals for the multiple failure probability.

The components in commercial nuclear power plants usually are designed to have lower failure rate. Typically, the failure rate is on the order of 1.0E-6/hr or less. The common normal table generally only gives values as small as 1.0E-4, leaving somthing to be desired. Several computer programs have been developed to facilitate the nemerical computation.

A.2 The Normal Distribution

As discussed previously, the expressions for both simple and multiple failure probabilities have been derived for different underlying stress and strength models. However, for the models studied, the expressions are similar in form. It suffices to discuss the normal models. For all other models, the same procedure applies.

Use is made of the error function

$$\mathrm{erf}(y) = (2\pi)^{-\frac{1}{2}} \int_0^y \exp(-t^2)dt \qquad \text{(A-1)}$$

to compute the cumulative distribution function of standardized normal random variables. In the expressions for failure probabilities on the basis of the SSI, the follwing is involved:

$$\Phi(x)= (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{x} dt \exp(-\tfrac{1}{2}t^2) \qquad \text{(A-2)}$$

A simple algebraic manipulation gives

$$\Phi(x)= [1+\text{sign}(x)\text{erf}(|x|/\sqrt{2})]/2 \qquad \text{(A-3)}$$

To numerically integrate any functions, the well-known Simpson's rule was used. The follwing formula represents this numerical scheme:

$$\int_{x_j}^{x_{j+2}} dx\ f(x) = \tfrac{h}{3}[\ f_j+4f_{j+1}+f_{j+2}] \qquad \text{(A-4)}$$

A-3 The Inversion of Single Failure Probability

One of the key steps in the ISSI method is to find the inverse of a single failure probability. The following discussion indicates the approach used in this study.

To solve the equation $P = \Phi(x)$ for x when P is given, $0 < p < 1$, let $f(x) = \Phi(x) - P$ and compute by Newton-Ralphson iteration {2}.

$$x_i = x_{i-1} - f(x_{i-1}) \ / \ f'(x_{i-1}), \quad (i=1,...m) \qquad \text{(A-5)}$$

where

$$f'(x) = (2\pi)^{-\frac{1}{2}} \exp(-0.5\, y^2)$$

and

x_0 is some suitably chosen starting approximation.

If m=2, x_0 is given by the rational approximation

$$x_0 = t - \frac{a+bt+ct^2}{1+dt+et^2+ft^3}, \quad t = \sqrt{\ln(1/Q^2)}, \quad 0<Q=1-P<0.5 \qquad (A\text{-}6)$$

If $P_0 < P < 1-P_0$ and $P_0=10^{-s}$, then as a rule of thumb the error is smaller than $10^{-(11-s)}$ for $1 \leq s \leq 9$. This degree of accuracy should be adequate for our purposes. The constants used above are:{3}

$$a = 2.515517,\ b = 0.802853,\ c = 0.010328$$
$$d = 1.432788,\ e = 0.189269,\ f = 0.001308 \qquad (A\text{-}7)$$

Seven computer programs have been developed to facilitate the numerical evaluations of multiple failure probabilities. These are:

1. For Normal Model
   a. COM1: when safety factor is approximately one
   b. COM2: when V_S and M are known
   c. COM3: when V_R and V_S are known
   d. COM4: when V_R and M are known

2. For Lognomal Model

   a. COM3L: when V_R and V_S are known

3. For Normal-Lognormal Model

   a. COM3A1: when V_R and V_S are known

4. For Lognormal-Normal Model

   a. COM3A2: when V_R and V_S are known

The listings of these programs are presented in the follwing pages.

References

1. M. Clark, Jr., and K.F. Hansen
"Numerical Methods for Reactor Analysis", Academic Press, New York, 1964, pp.89

2. R.C. Milton and R. Hotchkiss
"Computer Evaluation of the Normal and Inverse Normal Distribution Function", Technometrics, Vol.11, No.4, Nov, 1969, pp.817-822

3. C. Hastings, Jr., "Approximation for Digital Computers", Princeton University Press, 1955

```
* File com1 fortran
  301 READ(5,100)B,P,S,N
  100 FORMAT(3E13.5,I5)
      K=1
      AKA=-CDFNI(P)
      R=B*S
      P=CDFN(-AKA)
      WRITE(6,3)AKA
    3 FORMAT(10X,'AKA=',E13.6)
      UR=AKA*SQRT(B*B+1.)*S+1.0
      WRITE(6,4)R,P
    4 FORMAT(10X,'R=',E12.5,'P=',E12.5)
      IF(R.LE.0)STOP
      WRITE(6,7)UR,S
    7 FORMAT(10X,'UR=',E12.5,'S=',E12.5)
      IF(UR.LT.0.OR.S.LT.0.)STOP
      US=1.0
      A1=0.398942280/S
    5 TOT=0.
      XL=US-8.*S
      XU=UR+8.*S
      CON=0.000001
      IF(P.LT.CON)XL=US-12.*S
      IF(P.LT.CON)XU=UR+12.*S
      H=(XU-XL)/N
      DO 10 I=1,N,2
      X1=XL+(I-1)*H
      X2=X1+H
      X3=X2+H
      XX=(X1-US)/S
      XX1=-.5*XX*XX
      IF(XX1.LT.-20.) GO TO 15
      EXX1=A1*EXP(XX1)
      YY=(X1-UR)/R
      IF(K.EQ.1)F1=EXX1*CDFN(YY)
      IF(K.EQ.2)F1=EXX1*CDFN(YY)*CDFN(YY)
      IF(K.EQ.3)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)
      IF(K.EQ.4)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)*CDFN(YY)
      GO TO 16
   15 F1=0.0
   16 AXX=(X2-US)/S
      AXX1=-.5*AXX*AXX
      AEXX1=A1*EXP(AXX1)
      AYY=(X2-UR)/R
      BXX=(X3-US)/S
      IF(K.EQ.1)F2=AEXX1*CDFN(AYY)
      IF(K.EQ.2)F2=AEXX1*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.3)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.4)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      BXX1=-.5*BXX*BXX
      BEXX1=A1*EXP(BXX1)
      BYY=(X3-UR)/R
      IF(K.EQ.1)F3=BEXX1*CDFN(BYY)
      IF(K.EQ.2)F3=BEXX1*CDFN(BYY)*CDFN(BYY)
```

```
      IF(K.EQ.3)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.4)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      GO TO 10

   10 TOT=TOT+H*(F1+4.*F2+F3)/3.0
C     WRITE(6,74)TOT,H
C 74  FORMAT(10X,'TOT=',F12.8,'H=',F12.8)
      WRITE(6,311)TOT
  311 FORMAT(5X,T10,'FAILURE PROBABILITY',1PG12.5)
C     WRITE(6,312)
C 312 FORMAT(10X,'INPUT DATA KK I5 =0 MEANS STOP')
      READ(5,101)KK
  101 FORMAT(I5)
      K=KK
      IF(KK.EQ.0)GO TO 9
      IF(KK.EQ.6)GO TO 301
      GO TO 5
    9 STOP
      END
```

```
* File com2 fortran
  301 READ(5,100)SM,S,P,N,US
  100 FORMAT(3E10.5,I5,E10.5)
      K=1
      AKA=-CDFNI(P)
      RR=((SM-1.)/(AKA*SM))**2-(S/SM)**2
      IF(RR.LT.0.)STOP
      R=SQRT(RR)
      P=CDFN(-AKA)
      WRITE(6,3)AKA
    3 FORMAT(10X,'AKA=',E13.6)
      WRITE(6,4)R,P
      UR=SM
    4 FORMAT(10X,'R=',E12.5,'P=',E12.5)
      IF(R.LE.0)STOP
      WRITE(6,7)UR,S
    7  FORMAT(10X,'UR=',E12.5,'S=',E12.5)
      IF(UR.LT.0.OR.S.LT.0.)STOP
      A1=0.398942280/S
    5 TOT=0.
      XL=1.-8.*S
      XU=UR+8.*R
      CON=0.000001
      IF(P.LT.CON)XL=1.-12.*S
      IF(P.LT.CON)XU=UR+12.*R
      H=(XU-XL)/N
      DO 10 I=1,N,2
      X1=XL+(I-1)*H
      X2=X1+H
      X3=X2+H
      XX=(X1-1.)/S
      XX1=-.5*XX*XX
      IF(XX1.LT.-20.) GO TO 15
      EXX1=A1*EXP(XX1)
      YY=(X1-UR)/(SM*R)
      IF(K.EQ.1)F1=EXX1*CDFN(YY)
      IF(K.EQ.2)F1=EXX1*CDFN(YY)*CDFN(YY)
      IF(K.EQ.3)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)
      IF(K.EQ.4)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)*CDFN(YY)
      GO TO 16
  15  F1=0.0
  16  AXX=(X2-1.)/S
      AXX1=-.5*AXX*AXX
      IF(AXX1.LT.-20.) GO TO 17
      AEXX1=A1*EXP(AXX1)
      AYY=(X2-UR)/(SM*R)
      BXX=(X3-1.)/S
      IF(K.EQ.1)F2=AEXX1*CDFN(AYY)
      IF(K.EQ.2)F2=AEXX1*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.3)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.4)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      GO TO 28
  17  F2=0.0
  28  BXX1=-.5*BXX*BXX
```

```
      IF(BXX1.LT.-20.) GO TO 18
      BEXX1=A1*EXP(BXX1)
      BYY=(X3-UR)/(SM*R)
      IF(K.EQ.1)F3=BEXX1*CDFN(BYY)
      IF(K.EQ.2)F3=BEXX1*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.3)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.4)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      GO TO 10
   18 F3=0.0
   10 TOT=TOT+H*(F1+4.*F2+F3)/3.0
C     WRITE(6,74)TOT,H
C 74  FORMAT(10X,'TOT=',F12.8,'H=',F12.8)
      WRITE(6,311)TOT
  311 FORMAT(5X,T10,'FAILURE PROBABILITY',1PG12.5)
C     WRITE(6,312)
C 312 FORMAT(10X,'INPUT DATA KK I5 =0 MEANS STOP')
      READ(5,101)KK
  101 FORMAT(I5)
      K=KK
      IF(KK.EQ.0)GO TO 9
      IF(KK.EQ.6)GO TO 301
      GO TO 5
    9 STOP
      END
```

```
* file com3 fortran
  301 READ(5,100)R,S,P,N
  100 FORMAT(3E10.5,I5)
      K=1
      AKA=-CDFNI(P)
      P=CDFN(-AKA)
      WRITE(6,3)AKA
    3 FORMAT(10X,'AKA=',E13.6)
      WRITE(6,4)R,P
      DD1=AKA**2*S**2-1.
      DD2=AKA**2*R**2-1.
      UR=(-1.-SQRT(1.-DD1*DD2))/DD2
    4 FORMAT(10X,'R=',E12.5,'P=',E12.5)
      IF(R.LE.0)STOP
      WRITE(6,7)UR,S
    7 FORMAT(10X,'UR=',E12.5,'S=',E12.5)
      IF(UR.LT.0.OR.S.LT.0.)STOP
      SM=UR
      US=1.0
      A1=0.398942280/S
    5 TOT=0.
      XL=US-12.*S
      XU=UR+12.*S
      H=(XU-XL)/N
      DO 10 I=1,N,2
      X1=XL+(I-1)*H
      X2=X1+H
      X3=X2+H
      XX=(X1-US)/S
      XX1=-.5*XX*XX
      IF(XX1.LT.-20.) GO TO 15
      EXX1=A1*EXP(XX1)
      YY=(X1-SM)/(R*SM)
      IF(K.EQ.1)F1=EXX1*CDFN(YY)
      IF(K.EQ.2)F1=EXX1*CDFN(YY)*CDFN(YY)
      IF(K.EQ.3)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)
      IF(K.EQ.4)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)*CDFN(YY)
      GO TO 16
   15 F1=0.0
   16 AXX=(X2-US)/S
      AXX1=-.5*AXX*AXX
      IF(AXX1.LT.-20.) GO TO 17
      AEXX1=A1*EXP(AXX1)
      AYY=(X2-SM)/(SM*R)
      BXX=(X3-US)/S
      IF(K.EQ.1)F2=AEXX1*CDFN(AYY)
      IF(K.EQ.2)F2=AEXX1*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.3)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.4)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      GO TO 18
   17 F2=0.0
   18 BXX1=-.5*BXX*BXX
      IF(BXX1.LT.-20.) GO TO 19
      BEXX1=A1*EXP(BXX1)
```

```
      BYY=(X3-SM)/(SM*R)
      IF(K.EQ.1)F3=BEXX1*CDFN(BYY)
      IF(K.EQ.2)F3=BEXX1*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.3)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.4)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      GO TO 10
   19 F3=0.0
   10 TOT=TOT+H*(F1+4.*F2+F3)/3.0
      TOTL=ALOG(TOT)
C     WRITE(6,74)TOT,H
C 74  FORMAT(10X,'TOT=',F12.8,'H=',F12.8)
      WRITE(6,311)TOT,TOTL
  311 FORMAT(5X,T10,'FAILURE PROB.',1PG12.5,5X,E13.6)
C     WRITE(6,312)
C 312 FORMAT(10X,'INPUT DATA KK I5 =0 MEANS STOP')
      READ(5,101)KK
  101 FORMAT(I5)
      K=KK
      IF(KK.EQ.0)GO TO 9
      IF(KK.EQ.6)GO TO 301
      GO TO 5
    9 STOP
      END
      FUNCTION CDFNI(P)
      DOUBLE PRECISION Q,A,X,R,T,DCON,P,CDFN
      R=P
      NN=1
      Q=1.-P
      IF(R)1,3,4
    1 PRINT 2,P
    2 FORMAT(30H ILLEGAL ARGUMENT IN CDFNI  P=,E20.10)
      STOP
    3 CDFNI=-7.
      RETURN
    4 IF(1.-R)1,5,6
    5 CDFNI=7.
      RETURN
    6 IF(R-.5)9,7,8
    7 CDFNI=0.
      RETURN
    8 R=1.-R
      NN=2
      Q=P
    9 IF(R-1.E-10)10,11,11
   10 X=6.41
      GO TO 14
   11 T=SQRT(DLOG(1./(R*R)))
      X=T-((.010328*T+.802853)*T+2.515517)/(((.001308*T+.189269)*T
     1 +1.432788)*T+1.)
      LL=1
   12 DO 13 I=1,2
      LL=LL+1
      DCON=.3989422804*DEXP(-.5*X*X)
      X=X-((CDFN(X)-Q)/DCON)
```

```
      A=CDFN(X)-Q
  500 FORMAT(10X,'X=',E17.11,'A=',E17.11)
  13  CONTINUE
   14 GO TO (15,16),NN
   15 CDFNI=-X
      RETURN
   16 CDFNI=X
      WRITE(6,17)
   17 FORMAT('LEAVE CDFNI')
      RETURN
      END
      FUNCTION CDFN(X)
      DOUBLE PRECISION Y,X,CDFN
      Y=X*0.70710678119
      SGNY=1.
      IF(Y)2,1,3
    1 CDFN=.5
      RETURN
    2 SGNY=-1.
      Y=-Y
    3 CDFN=.5+SGNY*0.5*DERF(Y)
      RETURN
      END
```

```
* File com4 fortran
      READ(5,100)SM,R,P,N
  100 FORMAT(3E10.5,I5)
      K=1
      AKA=-CDFNI(P)
      SS=((SM-1.)/(AKA))**2-R**2*SM**2
      IF(SS.LT.0.)STOP
      S=SQRT(SS)
      P=CDFN(-AKA)
      WRITE(6,3)AKA
    3 FORMAT(10X,'AKA=',E13.6)
      WRITE(6,4)R,P
      UR=SM
    4 FORMAT(10X,'R=',E12.5,'P=',E12.5)
      IF(R.LE.0)STOP
      WRITE(6,7)UR,S
    7  FORMAT(10X,'UR=',E12.5,'S=',E12.5)
      IF(UR.LT.0.OR.S.LT.0.)STOP
      US=1.0
      A1=0.398942280/S
    5 TOT=0.
      XL=US-8.*S
      XU=UR+8.*R
      CON=0.000001
      IF(P.LT.CON)XL=US-12.*S
      IF(P.LT.CON)XU=UR+12.*R
      H=(XU-XL)/N
      DO 10 I=1,N,2
      X1=XL+(I-1)*H
      X2=X1+H
      X3=X2+H
      XX=(X1-US)/S
      XX1=-.5*XX*XX
      IF(XX1.LT.-20.) GO TO 15
      EXX1=A1*EXP(XX1)
      YY=(X1-UR)/(SM*R)
      IF(K.EQ.1)F1=EXX1*CDFN(YY)
      IF(K.EQ.2)F1=EXX1*CDFN(YY)*CDFN(YY)
      IF(K.EQ.3)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)
      IF(K.EQ.4)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)*CDFN(YY)
      GO TO 16
   15 F1=0.0
   16 AXX=(X2-US)/S
      AXX1=-.5*AXX*AXX
      AEXX1=A1*EXP(AXX1)
      AYY=(X2-UR)/(SM*R)
      BXX=(X3-US)/S
      IF(K.EQ.1)F2=AEXX1*CDFN(AYY)
      IF(K.EQ.2)F2=AEXX1*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.3)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.4)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      BXX1=-.5*BXX*BXX
      BEXX1=A1*EXP(BXX1)
      BYY=(X3-UR)/(SM*R)
```

```
      IF(K.EQ.1)F3=BEXX1*CDFN(BYY)
      IF(K.EQ.2)F3=BEXX1*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.3)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.4)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      GO TO 10

   10 TOT=TOT+H*(F1+4.*F2+F3)/3.0
C     WRITE(6,74)TOT,H
C  74 FORMAT(10X,'TOT=',F12.8,'H=',F12.8)
      WRITE(6,311)TOT
  311 FORMAT(5X,T10,'FAILURE PROBABILITY',1PG12.5)
C     WRITE(6,312)
C  312 FORMAT(10X,'INPUT DATA KK I5 =0 MEANS STOP')
      READ(5,101)KK
  101 FORMAT(I5)
      K=KK
      IF(KK.EQ.0)GO TO 9
      GO TO 5
    9 STOP
      END
```

```
* com31 fortran
  301 READ(5,100)R,S,P,N
  100 FORMAT(3E10.5,I5)
      K=1
      AKA=-CDFNI(P)
      P=CDFN(-AKA)
      WRITE(6,3)AKA,P
    3 FORMAT(10X,'AKA=',E13.6,'P=',E13.6)
      WRITE(6,7)R,S
    7 FORMAT(10X,'R=',E12.5,'S=',E12.5)
      DD1=S**2
      DD2=R**2
      UR=AKA*SQRT(DD1+DD2)
      SM=UR
      IF(R.LE.0)STOP
      IF(UR.LT.0.OR.S.LT.0.)STOP
      US=1.0
      A1=0.398942280/S
    5 TOT=0.
      XL=US-12.*S
      XU=UR+12.*S
      IF(UR.LT.US)XL=UR-12.*S
      IF(UR.LT.US)XU=US+12.*S
      H=(XU-XL)/N
      IF(H.LT.0.0)STOP
      DO 10 I=1,N,2
      X1=XL+(I-1)*H
      X2=X1+H
      X3=X2+H
      XX=X1/S
      XX1=-.5*XX*XX
      IF(XX1.LT.-20.) GO TO 15
      EXX1=A1*EXP(XX1)
      YY=(X1-UR)/R
      IF(K.EQ.1)F1=EXX1*CDFN(YY)
      IF(K.EQ.2)F1=EXX1*CDFN(YY)*CDFN(YY)
      IF(K.EQ.3)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)
      IF(K.EQ.4)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)*CDFN(YY)
      GO TO 16
   15 F1=0.0
   16 AXX=X2/S
      AXX1=-.5*AXX*AXX
      IF(AXX1.LT.-20.) GO TO 17
      AEXX1=A1*EXP(AXX1)
      AYY=(X2-UR)/R
      BXX=X3/S
      IF(K.EQ.1)F2=AEXX1*CDFN(AYY)
      IF(K.EQ.2)F2=AEXX1*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.3)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.4)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      GO TO 18
   17 F2=0.0
   18 BXX1=-.5*BXX*BXX
      IF(BXX1.LT.-20.) GO TO 19
```

```
      BEXX1=A1*EXP(BXX1)
      BYY=(X3-UR)/R
      IF(K.EQ.1)F3=BEXX1*CDFN(BYY)
      IF(K.EQ.2)F3=BEXX1*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.3)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.4)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      GO TO 10
   19 F3=0.0
   10 TOT=TOT+H*(F1+4.*F2+F3)/3.0
      IF(TOT.LE.0.)STOP
      TOTL=ALOG(TOT)
C     WRITE(6,74)TOT,H
C 74  FORMAT(10X,'TOT=',F12.8,'H=',F12.8)
      WRITE(6,311)TOT,TOTL
  311 FORMAT(5X,T10,'FAILURE PROB.',1PG12.5,5X,E13.6)
C     WRITE(6,312)
C 312 FORMAT(10X,'INPUT DATA KK I5 =0 MEANS STOP')
      READ(5,101)KK
  101 FORMAT(I5)
      K=KK
      IF(KK.EQ.0)GO TO 9
      IF(KK.EQ.6)GO TO 301
      GO TO 5
    9 STOP
      END
```

```
* File com3a1 fortran
  301 READ(5,100)R,S,P,N,US
  100 FORMAT(3E10.5,I5,E10.5)
      K=1
      ITER=0
      AKA=-CDFNI(P)
      P=CDFN(-AKA)
      WRITE(6,3)AKA
    3 FORMAT(10X,'AKA=',E13.6)
      WRITE(6,4)R,P
      DD1=AKA**2*S**2-1.
      DD2=AKA**2*R**2-1.
      UR=(-1.-SQRT(1.-DD1*DD2))/DD2
      CC1=S**2
      CC2=R**2
      URP=AKA*SQRT(CC1+CC2)
    4 FORMAT(10X,'R=',E12.5,'P=',E12.5)
      IF(R.LE.0)STOP
   20 WRITE(6,7)UR,S,URP
    7 FORMAT(10X,'UR=',E12.5,'S=',E12.5,'URP=',E12.5)
      IF(UR.LT.0.OR.S.LT.0.)STOP
      IF(URP.LT.0)STOP
      SM=UR
      A1=0.398942280/S
    5 TOT=0.
      XL=US-12.*S
      XU=UR+12.*S
      IF(UR.LT.US)XL=UR-12.*S
      IF(UR.LT.US)XU=US+12.*S
      H=(XU-XL)/N
      IF(H.LT.0.0)STOP
      IF(XL.LT.0.0)XL=H
      DO 10 I=1,N,2
      X1=XL+(I-1)*H
      X2=X1+H
      X3=X2+H
      XX=(X1-1.)/S
      XX1=-.5*XX*XX
      IF(XX1.LT.-20.) GO TO 15
      EXX1=A1*EXP(XX1)
      IF(X1.LE.0.)STOP
      YY=(ALOG(X1)-SM)/R
      IF(K.EQ.1)F1=EXX1*CDFN(YY)
      IF(K.EQ.2)F1=EXX1*CDFN(YY)*CDFN(YY)
      IF(K.EQ.3)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)
      IF(K.EQ.4)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)*CDFN(YY)
      GO TO 16
   15 F1=0.0
   16 AXX=(X2-1.)/S
      AXX1=-.5*AXX*AXX
      IF(AXX1.LE.-20.)GO TO 17
      AEXX1=A1*EXP(AXX1)
      IF(X2.LE.0.0)STOP
      AYY=(ALOG(X2)-SM)/R
```

```
C       AYY=(X2-SM-ALOG(US))/R
C       IF(AYY.LE.-7.0)GO TO 17
        BXX=(X3-1.)/S
        IF(K.EQ.1)F2=AEXX1*CDFN(AYY)
        IF(K.EQ.2)F2=AEXX1*CDFN(AYY)*CDFN(AYY)
        IF(K.EQ.3)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
        IF(K.EQ.4)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
        GO TO 18
   17   F2=0.0
   18   BXX1=-.5*BXX*BXX
        IF(BXX1.LE.-20.)GO TO 29
        BEXX1=A1*EXP(BXX1)
        IF(X3.LE.0.0)STOP
        BYY=(ALOG(X3)-SM)/R
C       BYY=(X3-SM-ALOG(US))/R
C       IF(BYY.LE.-7.0)GO TO 29
        IF(K.EQ.1)F3=BEXX1*CDFN(BYY)
        IF(K.EQ.2)F3=BEXX1*CDFN(BYY)*CDFN(BYY)
        IF(K.EQ.3)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
        IF(K.EQ.4)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
        GO TO 10
   29   F3=0.0
   10   TOT=TOT+H*(F1+4.*F2+F3)/3.0
        WRITE(6,310)TOT
  310   FORMAT(5X,T10,'FAILURE PROB.',1PG12.5)
        IF(TOT.LT.0.OR.TOT.GT.1.)STOP
        IF(KK.GE.2.AND.KK.NE.6)GO TO 70
        ESP=TOT-P
        CRI=0.05*P
        IF(ABS(ESP).LE.CRI)GO TO 70
        IF(ESP.LT.0.)LL=1
        IF(ESP.GT.0.)LL=2
        ERR=ESP*SM/TOT
        IF(LL.EQ.1)SM=SM+ERR*0.08
        IF(LL.EQ.2)SM=SM+ERR*0.08
        ITER=ITER+1
        IF(ITER.GT.10.)STOP
        GO TO 5
   70   IF(TOT.LT.0.)STOP
        TOTL=ALOG(TOT)
        WRITE(6,311)TOT,TOTL
  311   FORMAT(5X,T10,'FAILURE PROB.',1PG12.5,5X,1PG12.5)
        READ(5,101)KK
  101   FORMAT(I5)
        K=KK
        IF(KK.EQ.0)GO TO 9
        IF(KK.EQ.6)GO TO 301
        GO TO 5
      9 STOP
        END
```

```
* File com3a2 fortran
  301 READ(5,100)R,S,P,N,US
  100 FORMAT(3E10.5,I5,E10.5)
      K=1
      ITER=0
      AKA=-CDFNI(P)
      P=CDFN(-AKA)
      WRITE(6,3)AKA
    3 FORMAT(10X,'AKA=',E13.6)
      WRITE(6,4)R,P
      DD1=AKA**2*S**2-1.
      DD2=AKA**2*R**2-1.
      UR=(-1.-SQRT(1.-DD1*DD2))/DD2
      CC1=S**2
      CC2=R**2
      URP=AKA*SQRT(CC1+CC2)
    4 FORMAT(10X,'R=',E12.5,'P=',E12.5)
      IF(R.LE.0)STOP
   20 WRITE(6,7)UR,S,URP
    7 FORMAT(10X,'UR=',E12.5,'S=',E12.5,'URP=',E12.5)
      IF(UR.LT.0.OR.S.LT.0.)STOP
      IF(URP.LT.0)STOP
      SM=UR
      A1=0.398942280/S
    5 TOT=0.
      XL=US-12.*S
      XU=UR+12.*S
      IF(UR.LT.US)XL=UR-12.*S
      IF(UR.LT.US)XU=US+12.*S
      IF(XL.LT.0.)XL=0.10
      H=(XU-XL)/N
      IF(H.LT.0.0)STOP
      DO 10 I=1,N,2
      X1=XL+(I-1)*H
      X2=X1+H
      X3=X2+H
      XX=ALOG(X1)/S
      XX1=-.5*XX*XX
      IF(XX1.LT.-20.) GO TO 15
      EXX1=A1*EXP(XX1)
      IF(X1.LE.0.)STOP
      YY=(X1-SM)/(SM*R)
      IF(K.EQ.1)F1=EXX1*CDFN(YY)
      IF(K.EQ.2)F1=EXX1*CDFN(YY)*CDFN(YY)
      IF(K.EQ.3)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)
      IF(K.EQ.4)F1=EXX1*CDFN(YY)*CDFN(YY)*CDFN(YY)*CDFN(YY)
      GO TO 16
   15 F1=0.0
   16 AXX=ALOG(X2)/S
      AXX1=-.5*AXX*AXX
      IF(AXX1.LE.-20.)GO TO 17
      AEXX1=A1*EXP(AXX1)
      IF(X2.LE.0.0)STOP
      AYY=(X2-SM)/(SM*R)
```

```
      BXX=ALOG(X3)/S
      IF(K.EQ.1)F2=AEXX1*CDFN(AYY)
      IF(K.EQ.2)F2=AEXX1*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.3)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      IF(K.EQ.4)F2=AEXX1*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)*CDFN(AYY)
      GO TO 18
   17 F2=0.0
   18 BXX1=-.5*BXX*BXX
      IF(BXX1.LE.-20.)GO TO 29
      BEXX1=A1*EXP(BXX1)
      IF(X3.LE.0.0)STOP
      BYY=(X3-SM)/(SM*R)
      IF(K.EQ.1)F3=BEXX1*CDFN(BYY)
      IF(K.EQ.2)F3=BEXX1*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.3)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      IF(K.EQ.4)F3=BEXX1*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)*CDFN(BYY)
      GO TO 10
   29 F3=0.0
   10 TOT=TOT+H*(F1+4.*F2+F3)/3.0
      WRITE(6,310)TOT
  310 FORMAT(5X,T10,'FAILURE PROB.',1PG12.5)
      IF(TOT.LE.0.OR.TOT.GE.1.)STOP
      IF(KK.GE.2.AND.KK.NE.6)GO TO 70
      ESP=TOT-P
      CRI=0.005*P
      IF(ABS(ESP).LE.CRI)GO TO 70
      IF(ESP.LT.0.)LL=1
      IF(ESP.GT.0.)LL=2
      ERR=ESP*SM/TOT
      IF(LL.EQ.1)SM=SM+ERR*0.01
      IF(LL.EQ.2)SM=SM+ERR*0.01
      ITER=ITER+1
      IF(ITER.GT.50.)STOP
      GO TO 5
   70 TOTL=ALOG(TOT)
      WRITE(6,311)TOT,TOTL,SM
  311 FORMAT(5X,T10,'FAILURE PROB.',1PG12.5,5X,1PG12.5,5X,1PG12.5)
      READ(5,101)KK
  101 FORMAT(I5)
      K=KK
      IF(KK.EQ.0)GO TO 9
      IF(KK.EQ.6)GO TO 301
      GO TO 5
    9 STOP
      END
```