NUREG/CR-2211
BNL-NUREG-51411

Modeling of Multiple Sequential Failures During Testing, Maintenance and Calibration

Prepared by P. K. Samanta, S. P. Mitra

Brookhaven National Laboratory

Prepared for
U.S. Nuclear Regulatory
Commission

Available from

GPO Sales Program
Division of Technical Information and Document Control
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Printed copy price: $4.75

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-2211
BNL-NUREG-51411
RX

Modeling of Multiple Sequential Failures During Testing, Maintenance and Calibration

Manuscript Completed: October 1981
Date Published: December 1981

Prepared by
P. K. Samanta, S. P. Mitra

Brookhaven National Laboratory
Upton, NY 11973

Prepared for
Division of Facility Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN A3219

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission,
   Washington, DC 20555
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the NRC/GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, transactions, and codes and standards. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

ABSTRACT

In this report the nature of dependence among human failures in a multiple sequential action is analyzed and distinguished from other types of multiple failures. Human error causes selective failure of components depending on when the failure started. Two models are developed for quantifying the failure probability in a multiple sequential action. The first is very general in nature and does not require any dependent failure data. The failure probability obtained from this model is a conservative one with associated uncertainty The uncertainty is calculated considering many possible sources such as data, coupling and modeling. In the second model, details of the process in multiple sequential failures are taken into account. The model increments the conditional failure probabilities by a certain amount from their lower bounds (independent failure probability). This approach provides important insights into the influence of dependence between failures on system reliability. The model can be used effectively to choose an optimum system considering the individual failure probability, dependence factor and the amount of redundancy in a system. It was observed that in many cases it may be better to reduce the individual failure probability and to use a different type of system, rather than trying to decrease the dependence between the failures.

CONTENTS

TABLES

FIGURES

1. INTRODUCTION

Dependent failures (also called common mode or common cause failures) and their quantitative description have received wide attention in nuclear safety analysis in recent years. Since redundancy was first used in an attempt to achieve high reliability in systems, the recognition that the redundant components can fail simultaneously because of some characteristics common to all the components has been an important consideration in system design. The Reactor Safety Study[1] termed such dependent failures common mode failures, and defined them as "multiple failures which occur because of a single initiating or influencing cause. The single cause or mechanism serves as a common input to the failures affected. If this mechanism or cause occurs all the failures are triggered simultaneously and a common mode failure occurs."

The treatment of these dependent failures is extremely important in the reliability assessment of any complex system that must be highly reliable. When a system is built of redundant subsystems, dependent failures may become the determining factor in the assessment of system reliability (or unreliability). In certain situations, the potential advantages of applying redundancy may be defeated by the dependent failures introduced.

The analysis of dependent failures is an intricate problem, and many techniques have been proposed. It is usually approached qualitatively, to identify major sources of failure, and then quantitatively to determine their impact on system reliability.[2]

In this study, a particular type of dependent failure is analyzed, and modeling is attempted to quantify the probability of such a failure. The failure addressed is dependent human failure during testing, maintenance, and calibration, which originates with a failure in one of the components caused by the operator. Since, during testing and maintenance, an operator performs his job sequentially, this type of failure is termed a multiple sequential failure (msf) during testing and maintenance.

In Section 2 the nature of msfs during testing and maintenance is analyzed and compared with other types of msfs. Examples of such failures and their importance in PWR safety analysis are provided. The available models for the treatment of msfs during testing and maintenance are briefly presented, and their applicability is analyzed.

In Section 3 various distributions are applied to the bounds obtained using bounding technique, and a central estimate is obtained using Chebyshev's inequality. The propogation of error in such an analysis is also calculated.

In Section 4 a model is developed by increasing the probability of dependent failures by a certain amount over the random failure probability, and the parameters of the model are estimated from available data. Section 5 provides some general conclusions about dependent failure probability based on the models developed in this study.

2. DEPENDENT FAILURES--OPERATOR ERRORS

2.1 Classification of Dependent Failures

Epler[3] wrote the first article concerning dependent failures. He concluded on the basis of some simple calculations, which included dependent failures, that there are "serious doubts as to the usefulness of a reliability calculation that considers random events only, when common mode failures may be dominant by as much as 10^{-5}." Since then the various types of dependent failures have received significant attention.

Dependent failures can be classified in many ways, and they have been assigned to broad categories on the basis of their causes, [1,4] which may be any of the following:

1. Design defects.
2. Manufacturing, fabrication, and quality control errors.
3. Test, maintenance, and repair errors.
4. Environmental variations.
5. Failure and degradation due to an initiating failure.
6. External initiation of failure.

Various measures have been recommended to reduce the probability of dependent failures,[1,4,5] such as the use of different types of equipment, the use of different procedures for testing or monitoring the state of a system, the presence of more than one operator to review personnel actions, and the physical separation of various redundant components.

It is unlikely that a single model will be suitable for quantitative analysis of all the different types of dependent failures, since the ways in which the different types of dependent failures occur are different. According to Mankamo,[6] the failure of a group of components can occur in three basic ways:

1. The failure is caused by an event outside the group but common to the components.
2. A failure within the group, e.g., a single component failure, results in the failure of all components concerned.
3. The components all fail randomly.

Dependent failures of the first type should be called "common cause failures" and those of the second type are usually called "cascade failures" or "multiple failures." The term "dependent failure" covers all kinds of failure dependencies and includes the first and second types of failures and also their combination. In this report, this terminology will be used.

Cascade or multiple failures (originating from failure of a single component within the group) that are due to human errors in testing and maintenance differ from those due to a single hardware failure. Since humans perform their tasks in a sequence, in a case of human error the state of the system depends on which component failed first, whereas in a case of hardware failure the final state of the system is likely to be independent of which component failed first. Figure 1 shows various failure states for a three-unit system. An operator error in the component A influences the probability of error in both components B and C, but an error in component B influences only component C, because of the procedure followed. Once an operator has correctly performed an operation on component A and moved on to component B, he has no reason to go back to component A, and, if he does go back to check, the action will usually be a correct one. Thus, a failure he causes in component B can result in only two component failures, and an error in component C will cause a single component failure. The situation is different for hardware failure, where failure of any one component can result in failure of all: not only can failure of A cause failure of B and C, out failure of B can cause failure of both A and C, and failure of C can cause failure of B and A.

In determining the probability of dependent failures, this distinction between two types of multiple or cascade failures is not taken into account in any of the present models, but use of the same model for both types will be erroneous. Dependent failures should be divided into at least three general classes, each requiring a different model:

1. Multiple sequential failure (msf) during testing and maintenance.
2. Multiple component failure due to single hardware failure within the group.
3. Failures caused by common events outside the group, i.e., common cause failures.

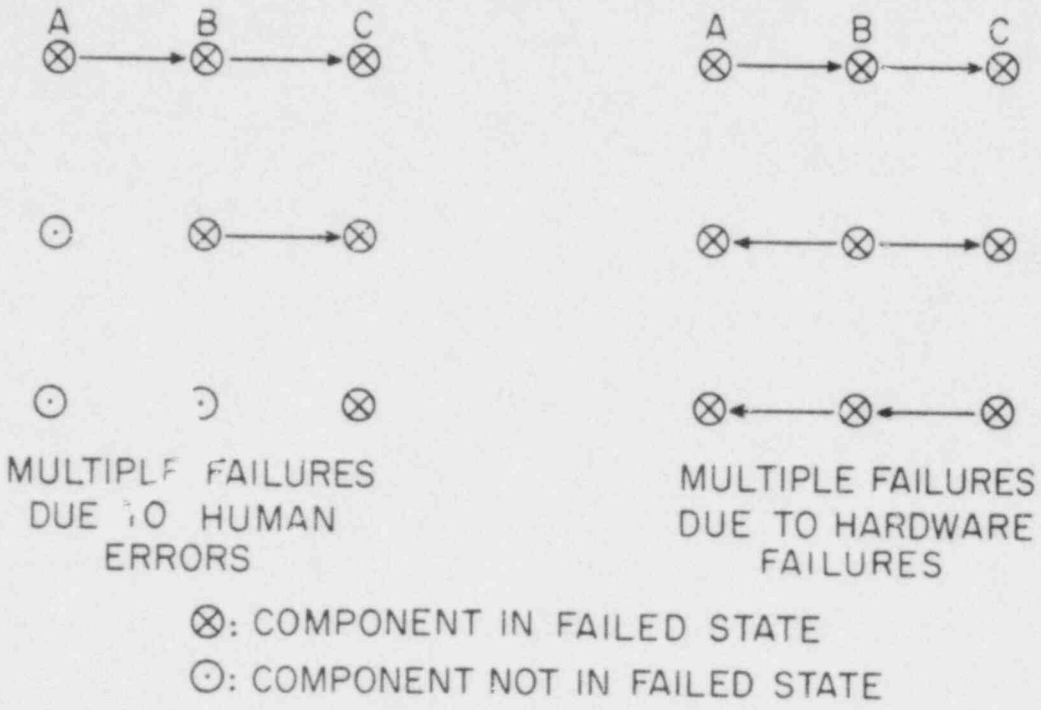

Figure 1. Different failure states resulting from human failures during testing and maintenance and those originating from a single hardware failure.

Modeling techniques described in the literature have addressed the second and third types; this study deals with the first type, msfs during testing and maintenance.

2.2 Situations of Multiple Sequential Failures in the Reactor Safety Study for a PWR

Multiple sequential component failures during testing, maintenance, and calibration play a significant role in the determination of system unavailability. In many PWR safety systems, this type of error is the dominant contributor to system unavailability. Samanta et al.,[7] applying an importance measure to human errors, showed this type to be among the most important ones. In many situations, given a particular type of accident, many of these errors could cause a core melt. Such errors in PWRs[1] include the following:

1. The possibility of repetitive human errors when calibrating three sets of comparators or bistable amplifiers in reactor protection system (RPS). These comparators are tested and calibrated at about the same time, although

the procedures for all of them may take several days. This error was found to be the most important one in terms of reliability importance to core melt probability. Also, given a small-small LOCA, with this error and no other intervention, the probability of core melt is 1.

2. The operator leaves each of the three pairs of pump discharge valves in auxiliary feedwater system (AFWS) closed following monthly tests. Since three pump tests are done sequentially as part of the same general procedure, these faults are coupled. Given a transient event, this error was found to be the most important one in terms of reliability importance to core melt probability. Also, given a small-small LOCA, with this error and no other intervention by the operator, the probability of core melt is 1.

3. Failure to close manual valves of two containment spray injection system (CSIS) pumps after monthly tests. Although the test procedure requires opening of one valve at a time, because one system is tested immediately after the other there is a dependence between the faults. Given this error, along with a small-small LOCA and no other operator intervention, the core melt probability is 1.

4. Operator error in calibration that causes failure of at least two of the three pressurizer low pressure comparators or of at least two of the three pressurizer low level comparators, and also of at least two of the four containment high pressure comparators. This error affects three systems: SICS, HPIS, and LPIS. It is among the important errors in terms of reliability importance to core melt probability and also in terms of structural importance to core melt.

5. Operator incorrectly calibrates at least two of the four sensor loops in CLCS HI train 1A or 1B. The same four sensors are used in both trains. Given a small-small LOCA with this error and no other operator intervention, the core melt probability is 1.

2.3 Modeling of Dependent (Common Mode) Failures

Various models have been proposed for estimating the probability of dependent failures. Some of these models are designed for specific types of dependent failures and others are general.

Lack of supporting data has been the major problem in validating such models. Since dependent failures are important only in highly reliable systems, and recognition of the problem has been rather recent, data will remain sparse for some time to come. Progress has been made, however, in the realization that treatment of dependent failures should differ from conventional reliability analysis in which the reliability of the system almost reaches unity if sufficient redundancy is added. The models used in reactor safety studies have generally been the "geometric mean" model and the "β-factor" model. The geometric mean model was developed by the RSS[1] and was used in assessing accident risks in U.S. commercial nuclear power plants. The β-factor model[8] was developed at Gulf General Atomics and was used in analyzing HTGR accident initiation and progression. Both these models are general in nature and are attractive for their simplicity. A third model was developed by Vesely[9] using the multivariate exponential distribution of Marshall-Olkin as the basis for common cause analysis. Most other available models assume the occurrence of a "shock" and are not applicable to the type of problem of interest here. The first two models mentioned above have been used to quantify multiple sequential failures in testing and maintenance, and the third one may be applied because of its attractive features. The general characteristics of these three models are discussed below.

2.3.1 Geometric Mean Model

The Reactor Safety Study[1] applied a bounding technique known as the geometric mean in the assessment of dependent failures. The model first determined the bounds within which the failure probability lies and then used judgement to estimate the value of the probability within the defined range. In general cases, defined as "loose coupling," the geometric mean of the upper and lower bounds was used to estimate the failure probability. This approach utilizes no dependent failure data; it relies on judgement to determine the degree of dependence. Also, it does not distinguish among different types of dependent failures. The model is very simple to use, but as pointed out by Lewis et al.,[13] is arbitrary in its use of the geometric mean in the estimation of failure probability.

Consider the example of two valves erroneously left closed by the operator after maintenance. The failure to leave the second valve open is dependent on the first action, i.e., whether the first valve was left open or closed. Let

the symbols H_1 and H_2 respectively represent failure to keep the first and the second valve open, and let H_1H_2 represent failure to keep both open.

$P(H_1)$: probability of the first error,

$P(H_2)$: probability of the second error,

$P(H_1H_2)$: probability of making both errors.

The expression $P(H_1H_2)$, called the combination probability, is totally general and does not imply anything about the dependence or independence of the errors H_1 and H_2.

If the events are completely independent,

$$P(H_1H_2) = P(H_1)P(H_2) .$$

This value of $P(H_1H_2)$ is defined as its lower bound, $P_L(H_1H_2)$.

If the events are dependent, the above expression is not valid. However, even in the dependent case, in order for H_1H_2 to happen, both H_1 and H_2 must happen. Accordingly,

$$P(H_1H_2) \leq P(H_1) ,$$

$$P(H_1H_2) \leq P(H_2) .$$

Since both of these are valid,

$$P(H_1H_2) \leq \text{MIN } [P(H_1), P(H_2)] ,$$

which is the upper bound, $P_U(H_1H_2)$, of the value of $P(H_1H_2)$.

The boundary values define the range in which the failure probability lies. Such ranges can be defined for other types of systems, and the technique is discussed in more detail in Section 3.2. The RSS assumed a lognormal distribution for the range of possible values and, to obtain the best estimate, used the median of the lognormal distribution, which is the geometric mean of the range:

$$P_M(H_1H_2) = \sqrt{P_U(H_1H_2) \cdot P_L(H_1H_2)} .$$

For identical acts,

$$P(H_1) = P(H_2) = p, \quad P_L(H_1H_2) = p^2, \quad P_U(H_1H_2) = p, \quad \text{and} \quad P_M(H_1H_2) = p^{3/2} .$$

2.3.2 β-Factor Model

Fleming[8] developed the β-factor model for the quantification of dependent failures in HTGR risk assessment. The name is derived from the use of a factor, β, relating the dependent failure rate to the total failure rate for one channel. Let

λ : total failure rate of one channel,

λ_i : independent failure rate of the channel,

λ_{cm} : dependent (common mode) failure rate of the channel.

The model assumes that the total failure rate of each unit can be expanded into its independent and dependent rates:

$$\lambda = \lambda_i + \lambda_{cm} .$$

It also defines the parameter β as the fraction of the total failure rate attributable to dependent failure:

$$\beta = \frac{\lambda_{cm}}{\lambda_i + \lambda_{cm}} = \frac{\lambda_{cm}}{\lambda} .$$

Assuming exponential distribution for both independent and dependent failures, the system failure probability for a 1 out of 2:G type* of system is obtained as

$$F(t) = 1 - 2e^{-\lambda t} + e^{-(2-\beta)\lambda t}$$

$$\approx \tfrac{1}{2}(2 - 4\beta + \beta^2)(\lambda t)^2 + \beta\lambda t .$$

The value of β lies between 0 and 1, with $\beta = 1$ implying that all failures are dependent (common mode), and $\beta = 0$ that all failures are independent. Fleming and Raabe[10] obtained estimates of β for six different component types from reliability experience data. They found that β tends to have values very closely clustered in the range from 0.1 to 0.2.

---

*k out of n:G logic configuration signifies that the system of n components is good i.f.f. at least k components are good.

The basic steps used to develop the reliability prediction for 1 out of 2:G type systems can be applied to larger systems and higher levels of redundancy. The reliability predictions for 1 out of 3:G systems and 2 out of 3:G systems by the β-factor model are given by Fleming.[8]

2.3.3 Marshall-Olkin Specialized Model

Vesely[9] used the multivariate exponential distribution of Marshall and Olkin for the treatment of common cause failures. The basic multivariate model was specialized for the estimation of model parameters and was made capable of direct quantification of common cause failure probabilities. All failures are assumed to occur at the same time, and this is taken as an approximation in cases of dependent failures occurring within short intervals.

The model considers an arbitrary group of m components which fail from various causes. For m components, the total number of possible failure causes is 2^{m-1}, and each is described by a unique vector $\bar{x}$. For example, for two components, m = 2, the vector (1,0) or (0,1) describes an independent cause affecting only component 1 or component 2, and the vector (1,1) describes a common cause simultaneously failing both the components.

In the model, the probability distribution associated with each failure cause is described by an exponential distribution from its time of occurrence,

$$f_{\bar{x}}(t) = \lambda_{\bar{x}} \exp(-\lambda_{\bar{x}} t) ,$$

where $\lambda_{\bar{x}}$ is the failure rate associated with cause $\bar{x}$.

All the failure causes are assumed to be competing, and the observed failure is determined by the cause that occurs first. A multivariate exponential distribution describes the observed component failure times. For two identical components, the probability that neither component will fail in time t, $\bar{F}(t)$, is given by

$$\bar{F}(t) = \exp(-\lambda_1 t - \lambda_1 t - \lambda_2 t) ,$$

where λ_1 is the individual component failure rate for the vector (1,0) or (0,1) and λ_2 is the common cause failure rate described by the vector (1,1).

Smith et al.[11] have shown that for a two component system the system failure probability, F(t), to second order is given by,

$$F(t) = \tfrac{1}{2}(2\lambda_1^2 - \lambda_2^2)t^2 + \lambda_2 t .$$

Vesely provided a technique for estimating the parameters λ_1, λ_2, or $\lambda_{\bar{x}}$ based on Poisson statistical methods considering the number of failures observed in a specified time interval. This technique reduces the number of parameters to be estimated by assuming that the failure rates depend on the number of components failed, i.e., $\lambda_{\bar{x}} = \lambda_x$ where x is the total number of components simultaneously failed by the cause. This specialized model is called the homogeneous model. Both constant failure rate (CFR) and binomial failure rate (BFR) assumptions within the homogeneous model were analyzed for estimation.

In CFR, common cause failure rates are independent of the failure number:

$$\lambda_x = \lambda, \quad x \geq x_1 ,$$

where the equality is assumed only for numbers of failures greater than or equal to x_1.

In BFR, the equation for λ_x is obtained by factoring the common cause failure rate into an overall occurrence rate and a detailed effect probability. The quantity λ_x is obtained from the expression

$$\Lambda = \sum_{x=x_1}^{m} \binom{m}{x} \lambda_x$$

where Λ is the sum of all the common cause failure rates for $x \geq x_1$.

2.4 Applicability of the Available Dependent Failure Models

Other models besides the three described above have been proposed for the quantification of dependent failures. They are either shock or common load types of models. Shock models[12] are applicable where the failures are assumed to be due to a fatal "shock," defined as an event imposing abnormal stresses on the components leading to their failure. The common load model[6] is useful when the load and resistance distributions are well known. For the analysis of msf in testing and maintenance, such models are not applicable because the specific cause of the dependent failure is of a different nature.

The geometric mean model was applied by the Reactor Safety Study[1] for all types of dependent failures without regard to the specific cause of the dependence between the failures. The bounding technique applied by the model may be plausible for msfs, even though its use may be questioned for dependent failures resulting from external shocks. It also may be used very effectively for judging the importance of dependent failures with respect to random failures. But, as pointed out in the Lewis report,[13] use of the geometric mean of the bounds is totally arbitrary, and in many situations such an approach results in a lower bound that is absurdly low. The assumption that the central estimate lies symmetrically between the upper and lower bounds results in an estimate that is strongly influenced by a low lower bound which in many cases is viewed with little confidence. This results in increasing underestimation of the dependent failure probability with decreasing independent failure probability as the lower bound becomes very low.

The β-factor model has been used in HTGR risk assessment at Gulf General Atomics.[14] Because of its simplicity, it is attractive, but also it is questioned with regard to its applicability to all types of multiple failures. Its authors claim that human operator and maintenance errors "are accurately treated by the β-factor approach, since a design error or an operator error that leads to an equipment failure would most likely be symmetrically applied to any identical redundant equipment and would result in simultaneous or near simultaneous, multiple failures." But the model fails to distinguish between msfs during testing and maintenance and msfs due to other causes, as explained in Figure 1. Also, in the estimation of β, the counting procedure followed for the number of multiple failures could result in erroneous answers. For example, in 2 out of 3:G type systems, whether 2 of the units or 3 of the units simultaneously fail, both cases are counted as a multiple failure and given the same weight in estimating β.

Fleming and Raabe[10] have shown that the β-factor model is based on the Markov model of the system. The β-factor model also specifies that failure must be exponential and repair, if present, must also be exponential, i.e., the failure data must be expressed as rates. As correctly pointed out by Apostolakis,[15] because of the limits of the Markov model, which imposes the

requirement on the β-factor model that the failure data must be expressed as rates, the β-factor model cannot be applied to failure on demand and dependent maintenance errors.

Fleming and Raabe assert that observations "that β estimates for entirely different types of components exhibit such little variation suggest that β may be a more fundamental yardstick for measuring and predicting common cause failure susceptibility than, say, the common cause failure rate." Such apparent stability of β values cannot be used to justify application of the β-factor model in multiple failures due to testing and maintenance. Apostolakis[15] argues in general that the above assertion is "not acceptable."

Edwards and Watson[2] have also questioned the very basis of the definition of β. They argue that, since the similarity of the natures of dependent and independent failures has not been demonstrated, there is not much justification for taking the ratio of dependent failure rate to total failure rate.

The Marshall-Olkin specialized model of Vesely has been applied only in the estimation of multiple rod failure probabilities in the BWR. The model has desirable characteristics; by considering the failure cause as a vector $\bar{x}$, all states of the system can be distinctly identified. But estimation of the parameters of the model at that general level becomes extremely difficult.

The model is well suited for common cause types of failures, where the basic assumption of Marshall and Olkin[16] that all the failure causes are equally competing is applicable. In the situation of interest here, in which failure of one component can result in the failure of another component, that assumption is not strictly valid.

In this study, first a model was investigated by assuming various distributions with the bounds obtained by use of a bounding technique, as described in Section 3. The model is very general and does not use any dependent failure data. As described in Section 4, a more detailed model was then formulated by analyzing the process involved in msfs during testing and maintenance and other types of msfs (as explained in Figure 1) was accounted for. However, assumptions had to be made to avoid complexity in the model.

3. QUANTIFICATION OF DEPENDENT FAILURE PROBABILITY USING VARIOUS DISTRIBUTIONS

3.1 Bounding Technique and Use of Various Distributions

The bounding technique of the Reactor Safety Study[1] properly defines the bounds within which multiple component failure probability lies. The problem is to obtain an estimate for the failure probability within that range. The RSS's use of a lognormal distribution within the bounds is without proper justification and has been criticized, but the lack of data makes the choice of any other distribution equally unjustifiable. The choice of any distribution will generate criticism whenever there is insufficient available data to adequately back it up. However, Lewis et al.[13] point out that "most models will not give wildly different answers. The choice of one model over another generates an uncertainty, but within that uncertainty the use of the model is justified, provided the uncertainty is estimated and indicated." Therefore, modeling that includes modeling uncertainty could be attempted by considering a number of distributions. The estimate obtained from such a model along with the uncertainty associated with it (including data and modeling uncertainty) will be more defensible than that obtained with a model based on any arbitrary chosen distribution.

Modeling was attempted, as described below, by applying various well-known distributions within the bounds defined by the bounding technique. The use of various distributions provides different estimates and establishes a range of values for the dependent failure probability. It is argued that the uncertainty generated from this range is the modeling uncertainty. A final estimate for the dependent failure probability within this range was obtained by using Chebyshev's inequality. The uncertainty associated with the estimate, comprised of data uncertainty, coupling uncertainty, and modeling uncertainty, was calculated by using error propagation technique. The estimate obtained from this model, along with the uncertainty, is considered to be more suitable for use when little or no data are available, than an estimate obtained with any particular distribution.

3.2 Bounding Technique

The bounding technique establishes the bounds within which dependent failure probability should lie. The upper bound is the maximum value, with the assumption of total dependence between the failures, and the lower bound is the value with failures considered to be random, i.e., with no dependence among them.

Consider a system consisting of n components, where the symbols H_1, H_2, ..., H_n represent failure of the respective components. The expression $H_1H_2...H_m$ represents failure of components 1 through m. For example, $H_1H_2H_3$ represents the failure of components 1, 2 and 3. Let the individual failure probability of the n^{th} component be represented by $P(H_n)$, and the probability of the combination failure $H_1H_2...H_m$ by $P(H_1H_2...H_m)$.

The upper bound can be obtained by considering a single failure combination. This is suitable for the situation in which the failures are totally dependent. In order for the combination of components to fail, each of the components must fail individually; therefore,

$$P(H_1H_2...H_n) \leq P(H_1)$$

$$P(H_1H_2...H_n) \leq P(H_2)$$

$$\vdots \qquad\qquad \vdots$$

$$P(H_1H_2...H_n) \leq P(H_n) \ .$$

Since all of the above inequalities are true, the upper bound is the minimum of the individual failure probabilities:

$$P(H_1H_2...H_n) \leq \text{MIN}\ [P(H_1), P(H_2), ..., P(H_n)] \ .$$

Consider the situation in which all the acts are identical, i.e.,

$$P(H_1) = P(H_2) = ... = P(H_n) = p \ ;$$

the upper bound is given by

$$P_U(H_1H_2...H_n) = p \ .$$

The lower bound is obtained by considering totally random failures. In general, for m out of n:G type systems,

$$_mp_n = \binom{n}{r} p^r \ ,$$

where $_mP_n$ is the probability that at least m out of the n components fail, and r is given by

$$r = n - m + 1 .$$

From the above formula the lower bound of n repetitive failures is obtained as

$$P_L(H_1H_2...H_n) = p^n .$$

The bounds of different m out of n:G type systems, i.e., the type such that the system is good i.f.f. at least m components are good, are presented in Table 1.

Table 1

Bounds of System Failure Probability of Different Systems for Same Individual Failure Probability

Type of G System	Upper Bound, P_U	Lower Bound, P_L
1 out of 2	p	p^2
1 out of 3	p	p^3
2 out of 3	p	$3p^2$
1 out of 4	p	p^4
2 out of 4	p	$4p^3$
3 out of 4	p	$6p^2$

3.3 Choice of Various Distributions

The bounding technique establishes the bounds of the dependent failure probability. It is resonable to assume, with high confidence, that the failure probability lies within the bounds, but the appropriate distribution for describing dependent failures is not known. A choice of one distribution over the others cannot be rigorously justified. It can be argued, however,

that the appropriate distribution, even though not known, is unlikely to be very different from the well-known distributions followed by other known natural processes. Therefore, by applying various well-known distributions, a range that includes central estimates of all of them can be established. It is then reasonable to assume that the dependent failure probability lies within this range.

The central estimates of various distributions were obtained by assuming the lower bound (P_L) and the upper bound (P_U) of the dependent failure probability as 5% and 95% confidence limits of the distribution. The distributions considered applicable for this analysis are the following:

(1) Normal,
(2) Cauchy,
(3) Gamma,
(4) Weibull,
(5) Lognormal,
(6) Log Cauchy.

The following presentation provides the probability density function (pdf) of the distributions and the calculation of their central estimates in terms of the upper and lower bounds of the dependent failure probability (the 5% and 95% confidence limits).

(1) Normal Distribution:

The pdf of normal distribution is given by

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp[-(x - \mu)^2/2\sigma^2] , \qquad -\infty < x < \infty , \tag{3-1}$$

$$\text{Mean} = \bar{X} = = \frac{X_L + X_U}{2} ,$$

$$\text{Median} = X_{0.5} = \frac{X_L + X_U}{2} ,$$

Standard deviation = σ ,

where X_L and X_U are the lower and upper bounds respectively.

The standard deviation, σ, associated with μ is obtained from tables of the standard normal distribution function, $\phi(z)$:

$$\phi(z) = \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du = P(Z \leq z).$$

The normal variate, X, in our case, is related to Z by the expression

$$Z = \frac{X - \mu}{\sigma} .$$

Hence,

$$P(\frac{X - \mu}{\sigma} \leq z) = \phi(z) .$$

Taking $\phi(z)$ for corresponding z from the standard normal distribution function table,[20] we can obtain σ for corresponding μ and X.

(2) Cauchy Distribution:

The pdf of Cauchy distribution is given by

$$f(x) = \frac{b}{\pi[b^2 + (x - a)^2]} , \qquad -\infty < x < \infty . \tag{3-2}$$

The cumulative distribution fuction (cdf) is given by

$$F(x) = \frac{1}{2} + \frac{1}{\pi} \tan^{-1}(\frac{x - a}{b}) ; \qquad -\infty < x < \infty.$$

For 5% and 95% confidence limits we obtain

$$F(X_L) = 0.05 = \frac{1}{2} + \frac{1}{\pi} \tan^{-1} (\frac{X_L - a}{b}) ,$$

$$F(X_U) = 0.95 = \frac{1}{2} + \frac{1}{\pi} \tan^{-1} (\frac{X_U - a}{b}) .$$

Solution of the above equations gives

$$a = \frac{X_L + X_U}{2} \quad \text{and} \quad b = \frac{(X_U - X_L)}{2\tan(0.45\pi)} \ .$$

$$\text{Median} = X_{0.5} = a = \left(\frac{X_L + X_U}{2}\right) \ .$$

The results show that for our analysis with the lower and upper bounds the median for the Cauchy distribution is the same as that obtained with normal distribution. This is expected since the plot of the Cauchy density resembles that of the normal density except that its tail tends toward zero much more slowly as $|x| \to \infty$. Since use of both the normal and the Cauchy distribution will not provide additional information, a choice between them had to be made and normal distribution was chosen over Cauchy for estimating dependent failure probability.

(3) Gamma Distribution:

The pdf of gamma distribution is given by

$$f(x) = \frac{x^{\alpha-1}\exp(-x/\beta)}{\beta^{\alpha}\Gamma(\alpha)} \ , \quad x > 0 \ . \tag{3-3}$$

Since the median of the gamma distribution cannot be expressed analytically in terms of the bounds, the parameters α, β of the distribution and the corresponding median were obtained from tables and graphs of gamma distribution.[21] Hence, the median estimate of the gamma distribution used in this study is an approximate one.

(4) Weibull Distribution:

The pdf of the Weibull distribution is given by

$$f(x) = \frac{\beta x^{\beta-1}}{\lambda^{\beta}} \exp[(-x/\lambda)^{\beta}], \qquad x \geq 0, \ \beta < 0, \ \lambda > 0. \tag{3-4}$$

The cdf of the distribution is

$$F(x) = \int_0^x f(x)dx = 1 - \exp[-(x/\lambda)^{\beta}] .$$

For 5% and 95% confidence limits,

$$F(X_L) = 0.05 = 1 - \exp[-(X_L/\lambda)^{\beta}] ,$$

$$F(X_U) = 0.95 = 1 - \exp[-(X_U/\lambda)^{\beta}] .$$

Solving for β and λ gives

$$\beta = (4.067)/\ln(X_U/X_L) ,$$

$$\ln\lambda = \ln X_U + 0.27 \ln(X_U/X_L) , \qquad (3\text{-}5)$$

and

$$\text{Median} = X_{0.5} = \lambda e^{-0.36/\beta}$$

where λ and β are given by Eq. (3.5).

(5) Lognormal Distribution:

The pdf of lognormal distribution is given by

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}x} \exp[-(\ln x - \mu)^2/2\sigma^2] , \quad x > 0 , \qquad (3\text{-}6)$$

$$\text{Median} = X_{0.5} = e^{\mu} ,$$

$$\text{Mean} = \bar{X} = \exp[\mu + (\sigma^2/2)] .$$

$$\text{Second moment about median*} = \exp(2\mu)[\exp(2\sigma^2) - 2\exp(\sigma^2/2) + 1] . \qquad (3\text{-}7)$$

The deviation associated with the median needed for working with the median is obtained by taking the square root of the second moment about the median as given by Eq. (3-7). The parameters, μ and σ, are obtained from the following equations:

$$e^{\mu} = \sqrt{X_L X_U} , \qquad (3\text{-}8)$$

$$P\left(\frac{\ln X - \mu}{\sigma} \leq z\right) = \phi(z) . \qquad (3\text{-}9)$$

*See Appendix for derivation.

For lognormal distribution of X, lnX is normally distributed, and z corresponding to $\Phi(z)$ is obtained from standard normal distribution function tables.[20] σ is obtained as

$$\sigma = \frac{\ln X - \mu}{z} .$$

(6) Log Cauchy Distribution:

The pdf of log Cauchy distribution is given by

$$f(x) = \frac{b}{\pi[b^2 + (\ln x - a)^2]}, \qquad x > 0 . \tag{3-10}$$

The cdf is given by

$$F(x) = \frac{1}{2} + \frac{1}{\pi} \tan^{-1}\left(\frac{\ln x - a}{b}\right) ,$$

$$\text{Median} = X_{0.5} = \sqrt{X_L X_U} .$$

The median obtained is the same as that of the lognormal distribution. As in the case of the normal and the Cauchy distributions, discussed above, a choice had to be made, and the lognormal was chosen over the log Cauchy distribution for estimating dependent failure probability.

3.3.1 Range of Central Estimate

By applying the above distributions, the various central estimates (mean or median) are obtained. For a particular individual failure probability, these central estimates are ordered, and two extreme values provide the upper and lower limits of the range. The question then, is which central estimate to use, the mean or the median. It is interesting that normal distribution consistently provided the upper limit and lognormal the lower limit. Since for a normal distribution the mean and the median are the same, and for a lognormal, the median is always lower than the mean, the use of medians will provide a range that envelops all the central estimates. Following our previous argument that the distribution obeyed by the dependent failure is probably close to one of the discussed distributions, it is plausible to assume that the dependent failure probability lies within the range established.

The median values obtained by the use of various distributions for the dependent failure probability for 1 out of 2:G type systems are presented in Table 2 and plotted in Figure 2. The shaded portion of the figure is the range within which the dependent failure probability is expected to lie. Similar ranges can be established for other types of systems.

Table 2

Median Value of $P(H_1H_2)$ for Various Distributions Considered with Given $P(H_1)$

Type of Distribution	Dependent Failure Probability $P(H_1H_2)$ with $P(H_1)$						
	10^{-1}	5×10^{-2}	10^{-2}	5×10^{-3}	10^{-3}	5×10^{-4}	10^{-4}
Normal	5.5×10^{-2}	2.63×10^{-2}	5.05×10^{-3}	2.51×10^{-3}	5.01×10^{-4}	2.5×10^{-4}	5×10^{-5}
Gamma	3.8×10^{-2}	1.52×10^{-2}	2.0×10^{-3}	8.2×10^{-4}	1.1×10^{-4}		
Weibull	4.39×10^{-2}	1.71×10^{-2}	1.92×10^{-3}	7.51×10^{-4}	8.90×10^{-5}	3.29×10^{-5}	3.7×10^{-6}
Lognormal	3.16×10^{-2}	1.12×10^{-2}	1×10^{-3}	3.54×10^{-4}	3.16×10^{-5}	1.12×10^{-6}	1×10^{-6}

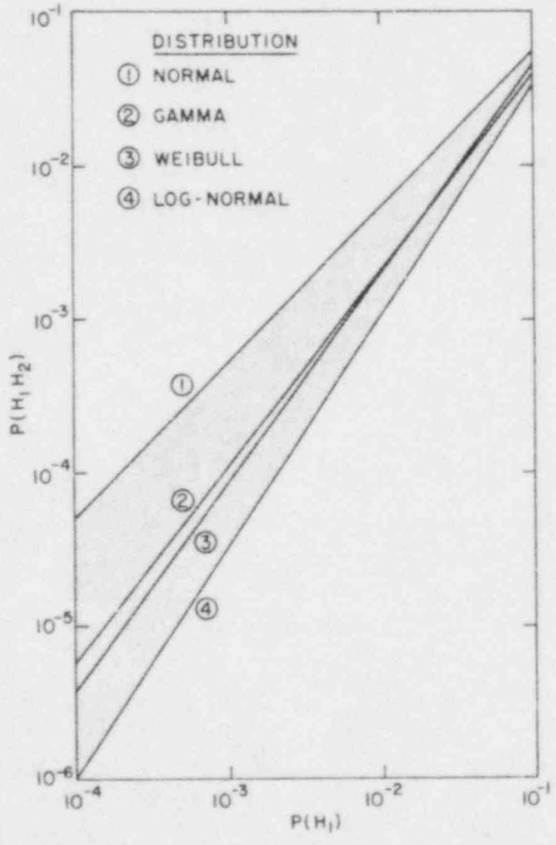

Figure 2. Median values (point estimates) of $P(H_1H_2)$ for different types of distributions considered with given $P(H_1)$ for a 1 out of 2:G type system.

3.4 Application of Chebyshev's Inequality

The next step is to obtain a value of the dependent failure probability within the defined range. We assume a 90% confidence that the dependent failure probability lies within the range. Stated mathematically,

$$P[X \leq \mu_{m,1}] = 0.05 , \qquad P[X \leq \mu_{m,n}] = 0.95 .$$

Hence,

$$P[\mu_{m,1} \leq X \leq \mu_{m,n}] = 0.9 , \tag{3-11}$$

where $\mu_{m,1}$ is the median value from loynormal distribution and $\mu_{m,n}$ is that from normal distribution.

With only the knowledge of bounds we cannot construct the probability distribution, but with the knowledge of mean and variance we can obtain bounds to such probabilities by using Chebyshev's inequality. Since we know the bounds, we use Chebyshev's inequality to obtain the mean and variance of the dependent failure probability.

3.4.1 Chebyshev's Inequality

Let X be a random variable with $E(X) = \mu_C$ and let c be any real number. Then, if $E(X - c)^2$ is finite and ε is any positive number, Chebyshev's inequality states[17]

$$P[|X - c| \geq \varepsilon] \leq \frac{1}{\varepsilon^2} E(X - c)^2 .$$

Choosing $c = \mu_C$ and $\varepsilon = k\sigma$, where $\sigma^2 = \text{Var } X > 0$, we obtain

$$P[|X - \mu_C| \geq k\sigma] \leq 1/k^2$$

or

$$1 - P[|X - \mu_C| < k\sigma] \leq 1/k^2$$

or

$$P[\mu_C - k\sigma < X < \mu_C + k\sigma] \geq 1 - 1/k^2 .$$

Conservatively,

$$P[\mu_C - k\sigma < X < \mu_C + k\sigma] = 1 - 1/k^2 . \tag{3-12}$$

Comparing Eqs. (3-11) and 3-12), we obtain

$$1 - 1/k^2 = 0.9 \quad \text{or} \quad k = 3.162 .$$

Also, $\mu_C = \dfrac{\mu_{m,1} + \mu_{m,n}}{2}$ and $\sigma = \dfrac{\mu_{m,n} + \mu_{m,1}}{6.324}$

where μ_C is the value given to the dependent failure probability by this type of analysis. Table 3 provides μ_C for 1 out of 2:G type systems given different individual failure probabilities. Figures 3, 4, and 5 show the estimates of dependent failure probability, μ_C, for 2-, 3-, and 4-unit systems.

Table 3

Estimate for $P(H_1H_2)$, μ_C, Applying Chebyshev's Inequality

$P(H_1)$	$\mu_{m,1}$	$\mu_{m,n}$	μ_C	$\sigma_{\mu,m,ch}$
10^{-1}	3.16×10^{-2}	5.5×10^{-2}	4.33×10^{-2}	3.7×10^{-3}
5×10^{-2}	1.12×10^{-2}	2.63×10^{-2}	1.875×10^{-2}	1.39×10^{-3}
3×10^{-2}	5.2×10^{-3}	1.55×10^{-3}	1.03×10^{-2}	1.63×10^{-3}
10^{-2}	1×10^{-3}	5.05×10^{-3}	3.03×10^{-3}	6.4×10^{-4}
5×10^{-3}	3.54×10^{-4}	2.51×10^{-3}	1.43×10^{-3}	3.41×10^{-4}
3×10^{-3}	1.65×10^{-4}	1.51×10^{-3}	8.34×10^{-4}	2.13×10^{-4}
10^{-3}	3.16×10^{-5}	5.005×10^{-4}	2.66×10^{-4}	7.41×10^{-5}
5×10^{-4}	1.12×10^{-5}	2.5×10^{-4}	1.31×10^{-4}	3.78×10^{-5}
1×10^{-4}	1×10^{-6}	5×10^{-5}	1.55×10^{-5}	7.74×10^{-6}

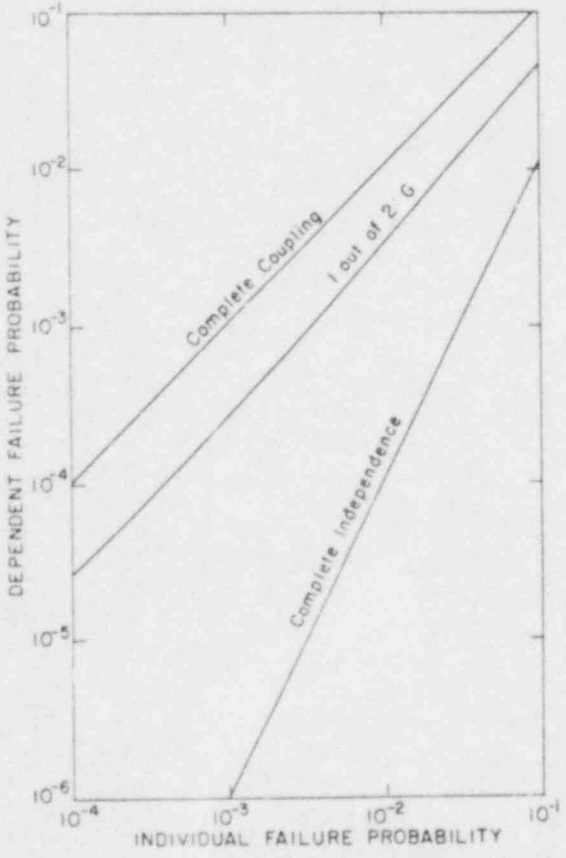

Figure 3. Estimate for dependent failure probability using Chebyshev's inequality for a 2-unit system.

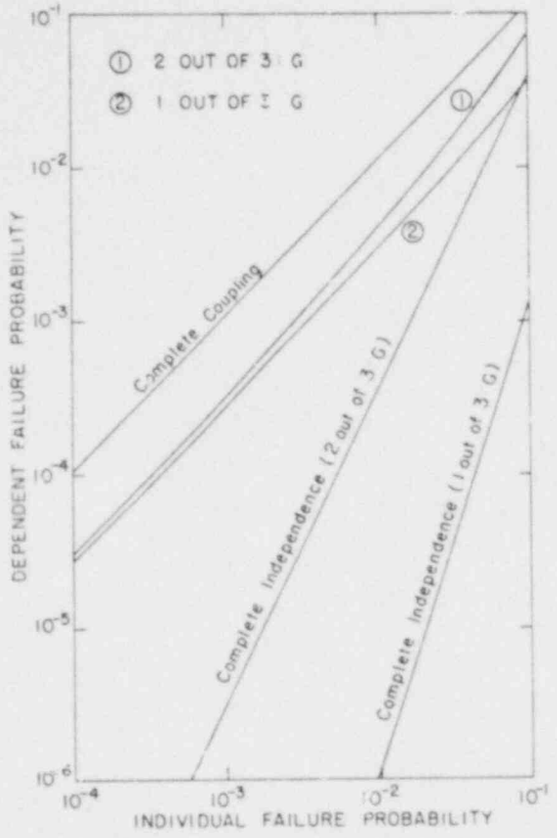

Figure 4. Estimate of dependent failure probability using Chebyshev's inequality for a 3-unit system.

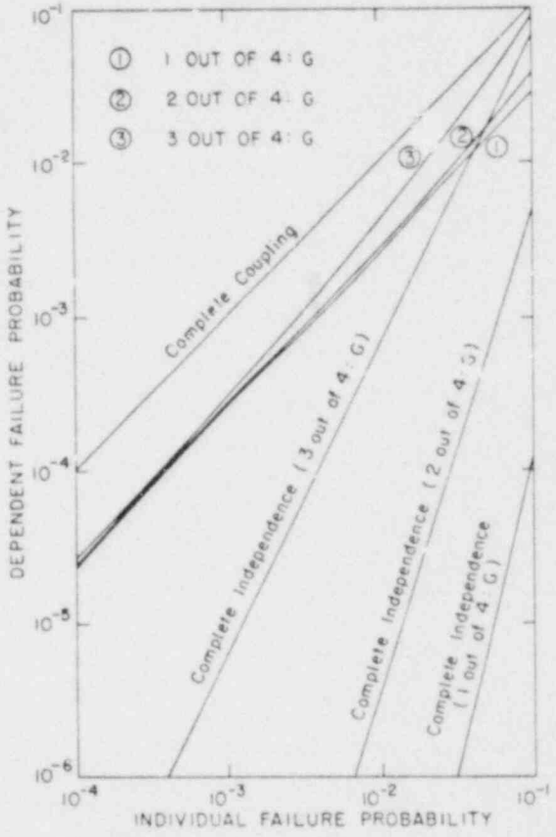

Figure 5. Estimate of dependent failure probability using Chebyshev's inequality for a 4-unit system.

3.5 Uncertainty in the Estimation of Dependent Failure Probability

3.5.1 Sources of Uncertainty in the Dependent Failure Probability Estimations

The estimation of any parameter or quantity always has an uncertainty associated with it particularly when the estimate of the parameter in question is too small, e.g., in the region of 10^{-2} to 10^{-5}. The sources of uncertainty in the estimation of the parameter may be many. In this section many possible sources of uncertainty in the final estimate of the dependent failure probability are discussed and defined.

The estimation process starts with the bounds defined from the individual failure probability, which is obtained from experimental data. The data base provides the failure rate in the form of an assigned median value and an associated error factor. The error factor denotes the amount of variation

(i.e., the range) in the failure probability. The data, in this case the failure rates, are treated as random variables and not as constant values. In essence, the random variable, representing a range of values, gives the possible values that the data may assume in various applications. A probability distribution is assigned to this range, which gives the probability associated with the particular assumed values. The error spreads are interpretable as uncertainties of the data. These uncertainties are due to data variability from component to component and with differing environmental conditions. The uncertainty also represents the basically random nature of the data, i.e., the data may assume various possible values given various possible applications. These uncertainties are termed as "data uncertainty" in this analysis. The probability distribution believed to represent the range of the individual failure probability, the random variable in question, is the lognormal distribution.

Given the individual failure probability, we obtain the bounds within which the dependent failure probability lies. The point value, which represents the dependent failure probability within the range, depends on the degree of dependence between the actions. The degree of dependence among the human actions is also referred to as the amount of coupling of human actions. In terms of the bounds, the upper bound represents complete coupling (i.e., complete dependence) and the lower bound represents no coupling (complete independence). The amount of coupling for the situations being modeled is said to be "loose," i.e., somewhere between complete and no coupling. We assumed various distributions between the bounds and claimed that the central estimate of the assumed distribution expresses the loose coupling. Given that bounds are perfectly defined, i.e., they are of constant values and the distribution assumed for the dependent failure probability is correctly known, there is some uncertainty in the coupled or dependent failure probability obtained from the central estimate of the distribution. This uncertainty can be attributed to two factors. First, looseness of coupling is random in nature, i.e., given the same two human actions defined to be loosely coupled, the coupled or dependent failure probability will be different for different sets of experiments. Second, there is no basis for claiming that the central estimate of the distribution perfectly determines the loosely coupled probability. It is then asserted that the central estimate associated with the error

spreads given by the distribution defines the range within which the dependent failure probability lies. The uncertainty expressed by this error spread is termed "coupling uncertainty."

Because of the data uncertainty, the bounds of the dependent failure probability are not defined to be of constant value. They lie within a range. Along with the coupling uncertainty, the data uncertainty also introduces an uncertainty in the coupled or dependent failure probability. By sampling the respective ranges of the bounds, we obtain different bounds for each sample. The median and the associated error spread due to coupling uncertainty from one set of bounds will be different from those from another. Thus, the net uncertainty at this point of the calculation will be a combination of the propagated data uncertainty and the coupling uncertainty.

The probability distribution followed by the dependent failure probability was varied. Each distribution considered defined a central estimate and the associated net error spread. A final estimate of the dependent failure probability was obtained by using Chebyshev's inequality as applied to the end points of the range of central estimates. If the bounds of the dependent failure probability are perfectly defined to a constant value and the loose coupling is perfectly defined and represented by the central estimate of the distribution chosen, a range will be obtained for the dependent failure probability due to the use of various distributions, i.e., due to different modeling approaches. The uncertainty in the central estimate obtained from this range expresses the "modeling uncertainty" in the final estimate. In our analysis the standard deviation obtained by the use of Chebyshev's inequality expresses this modeling uncertainty.

Along with the modeling uncertainty in the final estimate there will be uncertainty due to the variation of the bounds obtained from the individual failure probability and due to variance in the amount of coupling. The coupling and data uncertainties are propagated to the final estimate. The combination of these two uncertainties with the modeling uncertainties provides the total uncertainty in the final estimate of the dependent failure probability.

The discussion of various sources of uncertainty in the estimation of dependent failure probability can be summarized by saying that the uncertainty originates from three sources:

(1) Data uncertainty - this is due to the variability of the individual failure probability and arises from the data base of the individual failure probability.

(2) Coupling uncertainty - this expresses the variability in the amount of coupling.

(3) Modeling uncertainty - this is associated with the estimate of dependent failure probability and is due to the assumption of different models in the estimation process. In this case it is due to the choice of various distributions.

In the following section, the above three types of uncertainties are all accounted for in calculating the uncertainty in the estimate of dependent failure probability.

3.5.2 Calculation of Uncertainty in the Estimation of Dependent Failure Probability

The uncertainty in the dependent failure probability for a 1 out of 2:G type of system is calculated as follows.

The individual failure probability, $P(H_1)$, in the mode' is estimated from the data base and is the source of basic data uncertainty. The available data are in the form of a failure probability (median value) and the associated error factor, EF.

The error factor denotes the amount of variation (i.e., the range) in the failure probability. The median value is the reference point value. Accordingly, $P(H_1)/EF$ is the lower bound and $P(H_1) \cdot EF$ is the upper bound. We assume that the data are lognormally distributed with the lower bound as the 5% and the upper bound as the 95% confidence limit.

$P(H_1)$ is the median of the distribution. If we were working with the mean of the distribution, the second moment about the mean (the variance) would provide a measure of the uncertainty of the distribution. The square

root of the variance, the standard deviation, is usually used in the propagation of uncertainty calculations. However, since we are working with the median of the distribution, the appropriate measure of uncertainty is the second moment about the median. The square root of this measure is used for the propagation of uncertainty calculation.

σ_{d_1} : "data uncertainty" associated with $P(H_1)$.

$\sigma_{d_2} = 2\sigma_{d_1}P(H_1)$: "data uncertainty" associated with $P(H_1)^2$

where $P(H_1)^2$ is the lower bound in 1 out of 2:G type systems with the same individual failure probability for both the units. Note that $P(H_1) << 1$ and therefore $\sigma_{d_2} < \sigma_{d_1}$, but $\sigma_{d_2}/P(H_1)$, the coefficient of variation for $P(H_1)^2$ is twice as large as $\sigma_{d_1}/P(H_1)$, the coefficient of variation for $P(H_1)$. Table 4 provides σ_{d_1} and σ_{d_2} for different values of $P(H_1)$.

Table 4

Estimating σ_{d_1} and σ_{d_2} for Different Individual Failure Probabilities, $P(H_1)$, and Associated Error Factor (EF)

$P(H_1)$	Error Factor (EF)	U = $P(H_1).EF$	L = $P(H_1)/EF$	μ = $\ln P(H_1)$	σ = $\frac{\ln(U/L)}{3.284}$	Second moment wrt median σ_{d_1}*	σ_{d_2} = $2\sigma_{d_1}P(H_1)$
10^{-1}	3	3×10^{-1}	3.33×10^{-2}	-2.303	0.669	9.72×10^{-2}	1.94×10^{-2}
3×10^{-2}	3	9×10^{-2}	10^{-2}	-3.507	0.669	2.92×10^{-2}	1.75×10^{-3}
10^{-2}	3	3×10^{-2}	3.33×10^{-3}	-4.605	0.669	9.72×10^{-3}	1.94×10^{-4}
10^{-2}	10	10^{-1}	10^{-3}	-4.605	1.40	6.79×10^{-2}	1.36×10^{-3}
3×10^{-3}	3	9×10^{-3}	10^{-3}	-5.809	0.669	2.92×10^{-3}	1.75×10^{-5}
3×10^{-3}	10	3×10^{-2}	3×10^{-4}	-5.809	1.40	2.04×10^{-2}	1.22×10^{-4}
10^{-3}	3	3×10^{-3}	3.33×10^{-4}	-6.908	0.669	9.73×10^{-4}	1.95×10^{-6}
10^{-3}	10	10^{-2}	10^{-4}	-6.908	1.40	6.79×10^{-3}	1.36×10^{-5}

*$\sigma_{d_1} = e^{\mu}(e^{2\sigma^2} - 2e^{\sigma^2/2} + 1)^{1/2}$

For each type of distribution considered to describe the dependent failure probability, we have a central measure asscciated with an error spread. This error spread gives a measure of the coupling uncertainty. We define $\sigma_{c,a}$ as the "coupling uncertainty" due to the choice of "a" distribution, where

$$a = \begin{cases} \text{n: normal distribution} \\ \text{w: Weibull distribution} \\ \text{l: lognormal distribution} \\ \cdot \\ \cdot \\ \cdot \end{cases}$$

Values of $\sigma_{c,a}$ are obtained by calculating the square root of the second moment with respect to the central estimate, in this case, the median.

In obtaining the distribution, the two bounds considered could be anywhere within the range of uncertainties of these bounds. By choosing the bounds randomly within the respective ranges we obtain a slightly different distribution each time and the corresponding value of $\sigma_{c,a}$ changes. Thus, the effective uncertainty associated with the central estimate will be some combination of propagated data uncertainty and coupling uncertainty, which in reality is an integral representation involving $\sigma_{c,a}$. But here an approximation is made with the assumption that the uncertainty is composed of two separate parts: (i) the "coupling uncertainty" obtained from the distribution with the choice of the respective central points in the intervals as bounds, $\sigma_{c,a}$, and (ii) the uncertainty due to the propagation of the data uncertainty in the calculation of the central estimate, $\sigma_{d,a}$.

It is further assumed that the effective uncertainty, $\sigma_{\mu,a}$, associated with the central estimate, $\mu_{m,a}$, for the choice of the distribution "a" is the root mean square of the above two uncertainties:

$$\sigma_{\mu,a} = (\sigma_{c,a}^2 + \sigma_{d,a}^2)^{\frac{1}{2}} .$$

Values for $\sigma_{d,a}$ are obtained by using the propagation of error equation,

$$\sigma^2_{d,a} = \sigma^2_{d_1} \left[\frac{\partial f[P(H_1),\ P(H_1)^2]}{\partial [P(H_1)]} \right]^2$$

For normal distribution,

$$\mu_{m,n} = f[P(H_1),\ P(H_1)^2] = \frac{P(H_1) + P(H_1)^2}{2} ,$$

and

$$\sigma_{d,n} = \frac{\sigma_{d_1}}{2} \sqrt{[1 + 4P(H_1) + 4P(H_1)^2]}$$

For lognormal distribution,

$$\mu_{m,l} = P(H_1)^{3/2} ,$$

and

$$\sigma_{d,l} = \frac{3}{2} \sigma_{d_1} P(H_1)^{\frac{1}{2}} .$$

Finally, the dependent failure probability, μ_C, was estimated by using Chebyshev's inequality, and the corresponding uncertainty obtained ($\sigma_{\mu,m,ch}$) denotes the uncertainty due to the choice of various distributions and is termed the "modeling uncertainty." The effective uncertainty associated with μ_C is the combination of the "modeling uncertainty" and the uncertainty propagated in the calculation of μ_C.

Here, again, it is assumed that the total uncertainty associated with the estimate, μ_C, is the root mean square of the two separate uncertainties contributing to the total uncertainty: (i) modeling uncertainties obtained by using Chebyshev's inequality and (ii) propagated data and coupling uncertainty. Let σ_{μ_C} be the total uncertainty associated with μ_C, given by

$$\sigma_{\mu_C} = (\sigma^2_{\mu,d,ch} + \sigma^2_{\mu,m,ch})^{\frac{1}{2}} ,$$

where $\sigma_{\mu,m,ch}$ is the standard deviation obtained by using Chebyshev's inequality signifying the "modeling uncertainty," and $\sigma_{\mu,d,ch}$ is the uncertainty obtained in the calculation of μ_c by propagating both the basic "data uncertainty" and the "coupling uncertainty" and given by

$$\sigma_{\mu,d,ch} = (\sigma^2_{\mu,n} + \sigma^2_{\mu,1})^{1/2}/2 \ .$$

Figure 6 provides the graphical representation of various types of uncertainties considered and Table 5 provides the numerical estimates of the uncertainties for different $P(H_1)$.

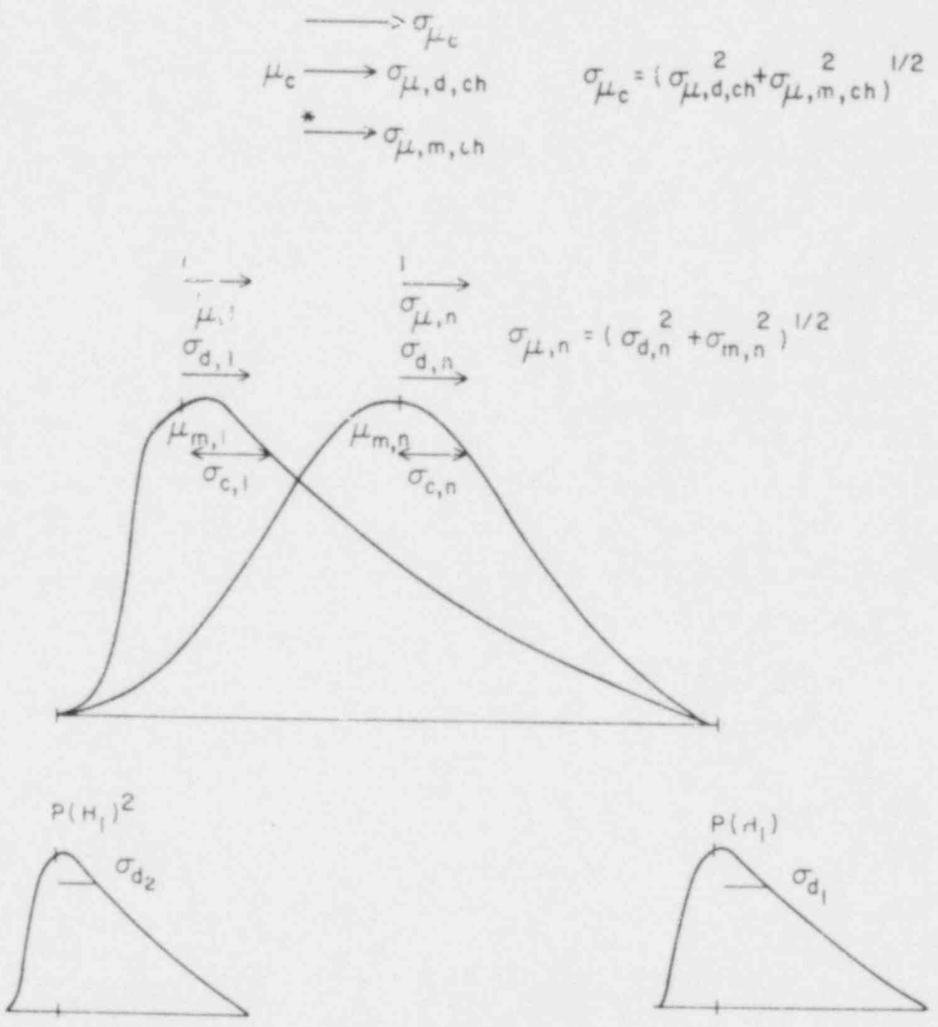

Figure 6. Propagation of error in the determination of central estimate.

TABLE 5

Estimating the Total Uncertainty $\sigma_{\mu C}$, Associated With
The Estimation of μ_c for 1 out of 2:G Type System

$P(H_1)$	EF	σ_{d_1}	$\sigma_{d,l}$	$\sigma_{c,l}$	$\sigma_{d,n}$	$\sigma_{c,n}$	$\sigma_{\mu,l}$	$\sigma_{\mu,n}$	$\sigma_{\mu,d,ch}$	$\sigma_{\mu,m,ch}$	σ_{μ_c}
10^{-1}	3	9.72×10^{-2}	4.61×10^{-2}	3.35×10^{-2}	5.83×10^{-2}	2.74×10^{-2}	5.70×10^{-2}	6.44×10^{-2}	4.3×10^{-2}	3.7×10^{-3}	4.32×10^{-2}
3×10^{-2}	3	2.92×10^{-2}	7.59×10^{-3}	1.37×10^{-2}	1.55×10^{-2}	8.86×10^{-3}	1.56×10^{-2}	1.79×10^{-2}	1.19×10^{-2}	1.63×10^{-3}	1.69×10^{-2}
10^{-2}	3	9.72×10^{-3}	2.92×10^{-3}	6.78×10^{-3}	4.96×10^{-3}	3.02×10^{-3}	7.38×10^{-3}	5.81×10^{-3}	4.70×10^{-3}	6.4×10^{-4}	4.74×10^{-3}
10^{-2}	10	6.79×10^{-2}	1.02×10^{-2}	6.78×10^{-3}	3.46×10^{-2}	3.02×10^{-3}	1.23×10^{-2}	3.47×10^{-2}	1.84×10^{-2}	6.4×10^{-4}	1.84×10^{-2}
3×10^{-3}	3	2.92×10^{-3}	2.40×10^{-4}	3.75×10^{-3}	1.47×10^{-3}	9.11×10^{-4}	3.76×10^{-3}	1.73×10^{-3}	2.07×10^{-3}	2.13×10^{-4}	2.08×10^{-3}
3×10^{-3}	10	2.04×10^{-2}	1.68×10^{-3}	3.75×10^{-3}	1.03×10^{-2}	9.11×10^{-4}	4.11×10^{-3}	1.03×10^{-3}	5.55×10^{-3}	2.13×10^{-4}	5.55×10^{-3}
10^{-3}	3	9.73×10^{-4}	4.62×10^{-5}	2.60×10^{-3}	4.88×10^{-4}	3.04×10^{-4}	2.60×10^{-3}	5.75×10^{-4}	1.33×10^{-3}	7.41×10^{-5}	1.33×10^{-3}
10^{-3}	10	6.79×10^{-3}	3.22×10^{-4}	2.60×10^{-3}	3.40×10^{-3}	3.04×10^{-4}	2.62×10^{-3}	3.41×10^{-3}	2.15×10^{-3}	7.41×10^{-5}	2.15×10^{-3}

3.6 Discussion of Results

The dependent failure probability obtained by the use of various distributions is more conservative than those obtained by using the geometric mean model or the β-factor model (Figure 7). In reality, whether the dependent failure failure probability is more closely approximated by this approach than by some other modeling approach can be determined only by an adequate data base on dependent failures. But, in the absence of a data base, such an approach seems to be more appropriate than the use of any particular distribution or β-factor model with a particular value of β. When knowledge is limited, being conservative in safety analysis is probably the proper course.

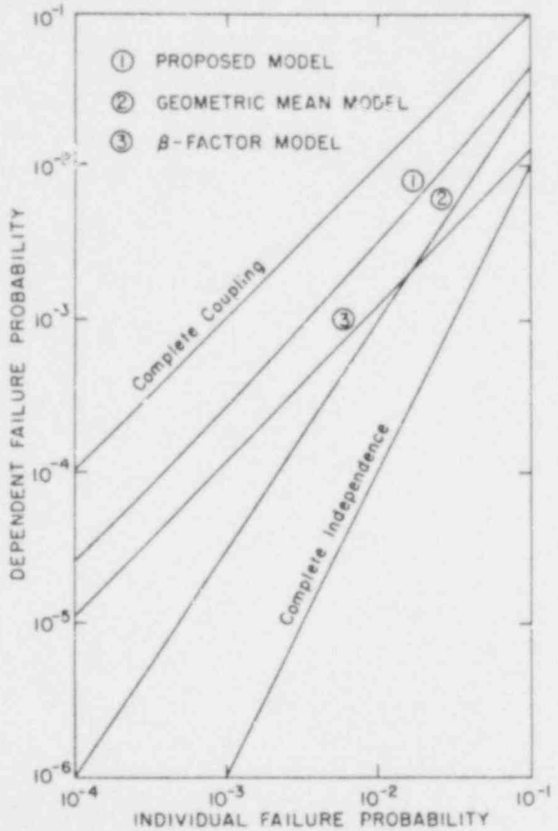

Figure 7. Comparison of the results of the proposed model with the geometric mean and the β-factor model for a 1 out of 2:G system.

One interesting property of the result is its changing dependence on the lower bound of the dependent failure probability. When the lower bound is significant, it influences the final estimate of the dependent failure probability; but, as the lower bound (denoting complete independence) decreases in magnitude, its influence also decreases so that the dependent failure probability becomes more and more dependent on the upper bound. Such a characteristic is justified because the lower bound becomes too small in magnitude, as the independent failure probability decreases, to have any significant influence. The geometric mean model is thought to underestimate the dependent failure probability as the individual failure probability decreases because of its strong dependence on the lower bound.

Our approach also provides the basis for incorporating many possible kinds of uncertainties including modeling uncertainties. The uncertainties in the estimate of the dependent failure probability for a 1 out of 2:G type system are significant, as shown in Table 5. This is expected and reflects our state of knowledge. The data uncertainty in the individual failure probability plays a significant role. With the improvement of our knowledge of individual failure rates, that uncertainty will decrease. Also, as more data become available on dependent failures, the distributions applicable to such failures could also be limited and thus the uncertainty due to modeling might be reduced. Overall, such an approach, an estimate of dependent failure probability with an associated uncertainty considering various distributions, is attractive when data are non-existent or very limited.

4. MODELING OF MULTIPLE SEQUENTIAL FAILURES

4.1 Basis of the Model

In this section a multiple sequential failure (msf) during testing and maintenance is modeled by taking into account the processes involved in such a failure. Dependence between two successive failures is accounted for by increasing the probability of the dependent failure by a certain amount over its independent or random failure probability. Modeling is carried out at a level sufficiently detailed to distinguish between msfs during testing and maintenance and those due to hardware failures, as discussed in Section 2.1. In that sense this approach is distinct from other dependence failure modeling approaches and is directly applicable to an msf during testing and maintenance.

The physical processes considered in this modeling approach may be explained as follows. Given two sequential actions, the second action, given failure in the first action, is no longer independent; accordingly, the probability of failure in the second action will be larger than its independent failure probability. Given three sequential actions, the third action, given failure in the first two, is not independent, and its dependence on previous failure is expected to be stronger than the dependence of the second action on the first action. The probability of failure in the third action, given failure in the first two, should exceed its independent failure probability by an amount greater than that in the case of second failure, given the first failure. Similarly, the probability of failure in the fourth action, given failure in the first three, should exceed its independent failure probability by an amount greater than that in the case of third failure, given first two failures, and so on. It is argued that in multiple sequential failures the probability of failure in the third action is more dependent on the probability of failure in the second action, given the first failure, than on the independent failure probability of the third action, unless the independent failure probability of the third action is larger. Thus, the range of the probability of failure in the third action is shrunk by increasing its lower bound from its independent failure probability to the probability of second failure, given the first failure. For similar dependent actions the probability of second failure, given the first failure, is always greater than the independent failure probability of the third action. In this way the ranges of probability of

higher and higher actions are shrunk, and the respective probabilities are increased because of the change in the lower bound of the respective shrunken ranges. To some extent, this approach automatically takes into account the increased dependence for any action compared with the preceding action in a multiple sequential action. That is, such increased dependence is built into the model.

Let us consider n sequential actions and let the symbols H_1, H_2, ..., H_n represent failure in the respective actions. The expression $H_1H_2 \cdots H_m$ represents repetitive failures in actions 1 through m.

In reliability analysis, the probability of n sequential failures is given by

$$P(H_1H_2 \cdots H_n) = P(H_1)\, P(H_2/H_1) P(H_3/H_1H_2) \cdots P(H_n/H_1H_2 \cdots H_{n-1}),$$

where the bounds of the conditional probabilities are given by

$$\begin{aligned}
P(H_2) \leq P(H_2/H_1) &\leq 1 \\
P(H_3) \leq P(H_3/H_1H_2) &\leq 1 \\
&\vdots \\
P(H_n) \leq P(H_n/H_1H_2 \cdots H_{n-1}) &\leq 1 .
\end{aligned} \tag{4-1}$$

The lower bound represents total independence between the failures, whereas the upper bound represents total dependence between the failures. It is the determination of the conditional failure probability that makes the problem difficult. Following is the method applied in this model for calculating such conditional failure probabilities.

The probability of failure in the second action, given failure in the first action, is assumed to be larger than its independent failure probability, and it is expressed as the sum of the independent failure probability, $P(H_2)$, and a dependent failure probability (P_{df}). The dependent failure probability is assumed to be a fraction of the total range of the conditional failure probability. From Figure 8,

$$\begin{aligned}
P(H_2/H_1) &= DB = DC + CB \\
&= P(H_2) + P(df_2)
\end{aligned}$$

where $P(df_2)$ is given by

$$P(df_2) = [1 - P(H_2)]\, k_1$$

and k_1 is the dependence factor.

The probability of failure in the third action, given failure in the first two, is given by

$$P(H_3/H_1H_2) = \text{Max}[P(H_3),\ P(H_2/H_1)] + \{1 - \text{Max}[P(H_3),\ P(H_2/H_1)]\}k_2 .$$

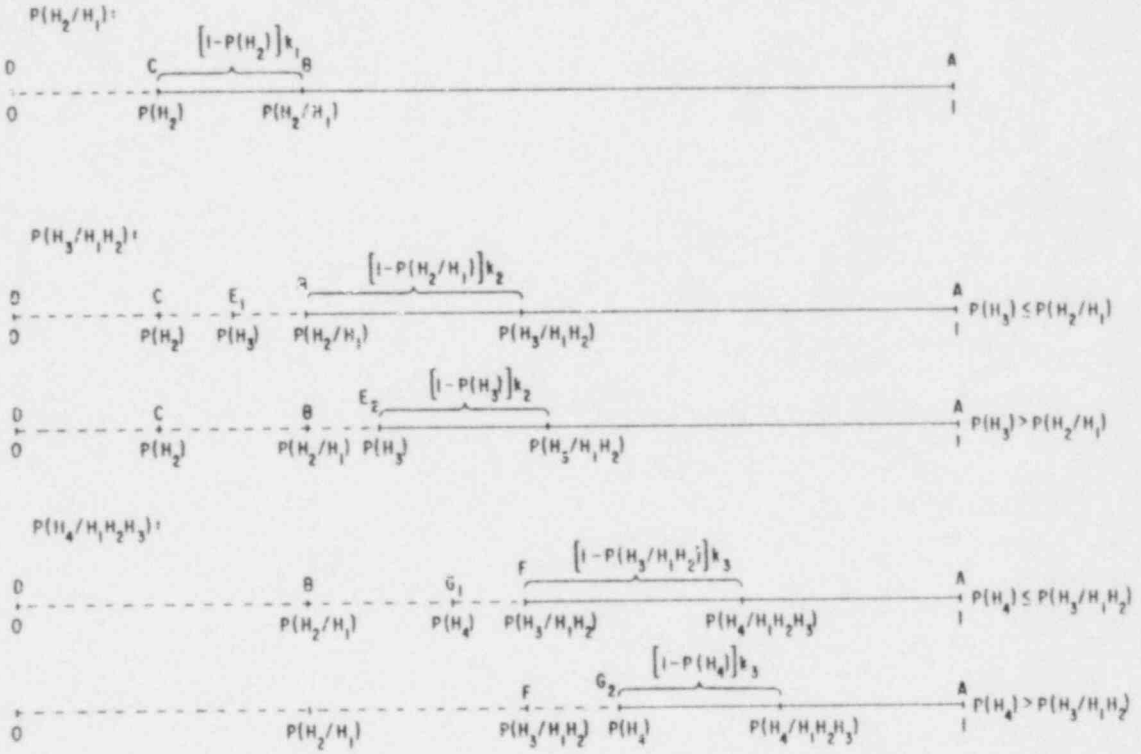

Figure 8. Representation of the conditional failure probabilities in a probability diagram.

In a multiple sequential action, the previous action is usually the determining factor in the probability of the present action because of the dependence among the actions. That is, the probability of failure in the third

action, given failure in the first two, is expected to depend more on the probability of failure in the second action, given failure in the first, than on the independent failure probability of the third action, unless the latter is larger. Thus the lower bound of $P(H_3/H_1H_2)$ is the larger of $P(H_3)$ and $P(H_2/H_1)$, and its probability is determined by adding a certain amount to this lower bound.

The reason for using the maximum, or larger value, of $P(H_3)$ and $P(H_2/H_1)$ is also clear from Figure 8. Given the dependence among the failures, the probability of failure in the third action, given failures in the first two, is expected to be greater than the probability of failure in the second action, given failure in the first; i.e., $P(H_3/H_1H_2) > P(H_2/H_1)$. Thus, when $P(H_3) < P(H_2/H_1)$, the range of the conditional probability $P(H_3/H_1H_2)$ is BA and not E_1A. But when $P(H_3) > P(H_2/H_1)$, the range of the conditional probability is E_2A. That is,

$$\text{Max}\,[P(H_3),\ P(H_2/H_1)] \leq P(H_3/H_1H_2) \leq 1 .$$

Even though certain amounts of increase in the dependence are accounted for by appropriately shrinking the range of the failure probabilities, strictly speaking the factor by which the failure probability is increased from the lower bound should be different for different actions, as the dependence between different sets of actions changes.

The dependence factor (k_2) used in the case of $P(H_3/H_1H_2)$ is different from that (k_1) used in the case of $P(H_2/H_1)$ because the dependence between third and second failure is expected to differ from that between second and first failure by more than the amount accounted for by shrinking the range of $P(H_3/H_1H_2)$.

Similarly, the probability of failure in a fourth sequential action, given failure in the first three, is given by

$$P(H_4/H_1H_2H_3) = \text{Max}[P(H_4),\ P(H_3/H_1H_2)] + \{1 - \text{Max}[P(H_4),\ P(H_3/H_1H_2)]\}\, k_3 .$$

In many practical situations, all the actions are similar in type, and their independent failure probabilities are usually the same:

$$P(H_1) = P(H_2) = \ldots = p .$$

Because estimating separate dependence factors with the available data is almost impossible--although a very general model must consider the dependence factors to be different--the dependence factor is assumed to be constant in order to simplify the estimation process:

$$k_1 = k_2 = \ldots = k \ .$$

Even with this assumption, a certain amount of increase in the dependence is accounted for in the model by the built-in process of appropriately shrinking the ranges of the failure probabilities.

With the above assumptions, the expressions for the conditional probabilities can be written as

$$P(H_2/H_1) = p + (1 - p)k$$

$$P(H_3/H_1H_2) = P(H_2/H_1) + [1 - P(H_2/H_1)]k$$

$$= p + (1 - p)k + \{1 - [p + (1 - p)k]\}k \ .$$

. .
. .
. .

For $k = 1$,

$$P(H_2/H_1) = 1$$

$$P(H_3/H_1H_2) = 1$$

. .
. .
. .

i.e., all the conditional probabilities reduce to 1, signifying complete dependence between the actions.

For $k = 0$,

$$P(H_2/H_1) = p$$

$$P(H_3/H_1H_2) = p$$

. .
. .
. .

i.e., all the conditional probabilities reduce to random failure probabilities signifying total independence between the actions.

Therefore, k must lie between 0 and 1, and its value determines the degree of dependence between the actions, which increases as the value of k approaches 1.

4.2 Multiple Sequential Failure Probability

For identical actions, with the above modeling approach, multiple sequential failure probability can be expressed in terms of two parameters: the independent failure probability, p, and the dependence factor, k.

Let P_n be defined as the probability of n sequential failures, i.e., repetition of the error for the n^{th} time. For similar actions, the conditional failure probability is always larger than the individual failure probability, for example, $P(H_2/H_1) > P(H_2) = P(H_3)$, and P_n can be written as

$$
\begin{aligned}
P_1 &= P(H_1) && = p \\
P_2 &= P(H_1)P(H_2/H_1) && = P_1\{P(H_2) + [1 - P(H_2)]\,k\} \\
P_3 &= P_2 P(H_3/H_1H_2) && = P_2\{P(H_2/H_1) + [1 - P(H_2/H_1)]\,k\} \\
&\vdots && \vdots \\
P_{n-1} &= P_{n-2}P(H_{n-1}/H_1H_2\cdots H_{n-2}) && = P_{n-2}\{P(H_{n-2}/H_1H_2\cdots H_{n-3}) \\
& && \quad + [1 - P(H_{n-2}/H_1H_2\cdots H_{n-3})]\,k\} \\
P_n &= P_{n-1}P(H_n/H_1H_2\cdots H_{n-1}) && = P_{n-1}\{P(H_{n-1}/H_1H_2\cdots H_{n-2}) \\
& && \quad + [1 - P(H_{n-1}/H_1H_2\cdots H_{n-2})]\,k\}\,. \qquad (4\text{-}2)
\end{aligned}
$$

With the conditional probabilities expressed in terms of p and k, some algebraic manipulation gives

$$
\begin{aligned}
P_1 &= p \\
P_2 &= P_1\{p + (1 - p)[1 - (1 - k)]\} \\
P_3 &= P_2\{p + (1 - p)[1 - (1 - k)^2]\} \\
&\vdots \\
P_{n-1} &= P_{n-2}\{p + (1 - p)[1 - (1 - k)^{n-2}]\} \\
P_n &= P_{n-1}\{p + (1 - p)[1 - (1 - k)^{n-1}]\}\,. \qquad (4\text{-}3)
\end{aligned}
$$

Finally, after some more algebra, P_n can be expressed as

$$P_n = \prod_{i=0}^{n-1} [1 - (1 - p)(1 - k)^i]$$

4.2.1 2-Unit System

For a 2-unit system, we give below the probabilities of the following different states of the system resulting from human failures:

none of the units is failed: (0,0);

one of the units is failed: (0,1) and (1,0);

both the units are failed: (1,1).

The vector (0,1) denotes no failure in unit 1, but failure in unit 2 of the system. Also, P(m/n) denotes the probability that m out of n of the units are failed.

P(0/2) = probability that none of the units is failed by human error

$$= [1 - P(H_1)][1 - P(H_2/\bar{H}_1)]$$

$$= (1 - p)^2 .$$

since $P(H_2/\bar{H}_1)$ is the probability of a second failure, given that the first failure did not occur,

$$P(H_2/\bar{H}_1) = P(H_2) = p .$$

P(1/2) = probability that one of the units is failed by human error

$$= P(H_1)[1 - P(H_2/H_1)] + [1 - P(H_1)]P(H_2/\bar{H}_1)$$

$$= p\{1 - [p + (1 - p)k]\} + (1 - p)p$$

$$= 2p(1 - p) - kp(1 - p) . \qquad (4\text{-}5)$$

P(2/2) = P_2 = probability that both units are failed by human error

$$= P(H_1)P(H_2/H_1)$$

$$= p[1 - (1 - p)(1 - k)]$$

$$= p^2 - kp^2 + kp . \qquad (4\text{-}6)$$

As expected,

$$P(0/2) + P(1/2) + P(2/2) = 1.$$

For a 1 out of 2:G logic type of system, the failure probability is given by

$$1_{P_2} = P(2/2) = p^2 - kp^2 + kp \tag{4-7}$$

where mp_n indicates the probability of system failure for a system of the out of n:G type.

4.2.2 3-Unit System

For a 3-unit system, we give below the probabilities of the following different states resulting from human errors:

none of the units is failed: (0,0,0);

one of the units is failed: (1,0,0), (0,1,0), (0,0,1);

two of the units are failed: (1,1,0), (0,1,1), (1,0,1);

all three units are failed: (1,1,1).

Assumption: The probability of failure in a particular action, given no failure in the preceding action, is assumed to be the independent or random failure probability of that action. For example, $P(H_3/H_1\bar{H}_2)$, i.e., the probability of failure in the third sequential action, given that failure has occurred in the first but not in the second, is the independent failure probability, $P(H_3)$. This assumption is plausible because, as soon as a correct action is performed following a failure, the dependence on that failure is assumed to be lost. That is, following a success or correct action, the probability of success or failure of the next action is treated as though it were an action in the first unit.

$P(0/3)$ = probability that none of the units is failed by human error

$$= [1 - P(H_1)][1 - P(H_2/H_1)][1 - P(H_3/H_1H_2)]$$

$$= (1 - p)^3 . \tag{4-8}$$

$P(1/3)$ = probability that one of the units is failed by human error

$$= P(H_1)[1 - P(H_2/H_1)][1 - P(H_3/H_1\bar{H}_2)]$$
$$+ [1 - P(H_1)]P(H_2/\bar{H}_1)[1 - P(H_3/\bar{H}_1H_2)]$$
$$+ [1 - P(H_1)][1 - P(H_2/\bar{H}_1)]P(H_3/\bar{H}_1\bar{H}_2)$$
$$= P_1(1 - P_2/P_1)(1 - P_1) + (1 - P_1)P_1(1 - P_2/P_1) + (1 - P_1)^2P_1$$
$$= 2p(1 - p)[1 - 1 + (1 - p)(1 - k)] + p(1 - p)^2$$
$$= 2p(1 - p)^2(1 - k) + p(1 - p)^2 . \qquad (4\text{-}9)$$

$P(2/3)$ = probability that two of the units are failed by human error

$$= P(H_1)P(H_2/H_1)[1 - P(H_3/H_1H_2)]$$
$$+ P(H_1)[1 - P(H_2/H_1)]P(H_3/H_1\bar{H}_2) + [1 - P(H_1)]P(H_2/\bar{H}_1)P(H_3/\bar{H}_1H_2)$$
$$= P_2(1 - P_3/P_2) + P_1(1 - P_2/P_1)P_1 + (1 - P_1)P_2$$
$$= p[1 - (1 - p)(1 - k)][1 - 1 - (1 - p)(1 - k)^2]$$
$$+ p^2[1 - 1 + (1 - p)(1 - k)] + p(1 - p)[1 - (1 - p)(1 - k)]$$
$$= p(1 - p) - p(1 - p)(1 - 2p)(1 - k)$$
$$+ p(1 - p)(1 - k)^2 - p(1 - p)^2(1 - k)^3 . \qquad (4\text{-}10)$$

$P(3/3)$ = probability that all three units are failed by human error

$$= P(H_1)P(H_2/H_1)P(H_3/H_1H_2)$$
$$= P_3$$
$$= p[1 - (1 - p)(1 - k)][1 - (1 - p)(1 - k)^2]$$
$$= p - p(1 - p)(1 - k) - p(1 - p)(1 - k)^2$$
$$+ p(1 - p)^2(1 - k)^3 . \qquad (4\text{-}11)$$

As expected,

$$P(0/3) + P(1/3) + P(2/3) + P(3/3) = 1 .$$

For a 1 out of 3:G logic type of system, the failure probability is given by

$$1p_3 = P(3/3)$$
$$= p - p(1 - p)(1 - k) - p(1 - p)(1 - k)^2 + p(1 - p)^2(1 - k)^3 . \qquad (4\text{-}12)$$

For a 2 out of 3:G logic type of system, the failure probability is given by

$$
\begin{aligned}
2p_3 &= P(2/3) + P(3/3) \\
&= p(1-p) - p(1-p)(1-2p)(1-k) + p(1-p)(1-k)^2 \\
&\quad - p(1-p)^2(1-k)^3 + p - p(1-p)(1-k) - p(1-p)(1-k)^2 \\
&\quad + p(1-p)^2(1-k)^3 \\
&= p(2-p) - 2p(1-p)^2(1-k) \; . \qquad (4\text{-}13)
\end{aligned}
$$

4.2.3 4-Unit System

For a 4-unit system, the different states of the system resulting from human failures are as follows:

none of the units is failed: (0,0,0,0);
one of the units is failed: (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1);
two of the units are failed: (1,1,0,0), (1,0,1,0), (1,0,0,1), (0,1,1,0), (0,1,0,1), (0,0,1,1);
three of the units are failed: (1,1,1,0), (1,0,1,1), (1,1,0,1), (0,1,1,1);
all four units are failed: (1,1,1,1).

The probabilities of these different states are given by the following:

P(0/4) = probability that none of the units is failed by human error

$$
\begin{aligned}
&= [1 - P(H_1)][1 - P(H_2/\overline{H}_1)][1 - P(H_3/\overline{H}_1\overline{H}_2)][1 - P(H_4/\overline{H}_1\overline{H}_2\overline{H}_3)] \\
&= (1-p)^4 \; . \qquad (4\text{-}14)
\end{aligned}
$$

P(1/4) = probability that one of the units is failed by human error

$$
\begin{aligned}
&= P(H_1)[1 - P(H_2/H_1)][1 - P(H_3/H_1\overline{H}_2)][1 - P(H_4/H_1\overline{H}_2\overline{H}_3)] \\
&\quad + [1 - P(H_1)]P(H_2/\overline{H}_1)[1 - P(H_3/\overline{H}_1H_2)][1 - P(H_4/\overline{H}_1H_2H_3)] \\
&\quad + [1 - P(H_1)][1 - P(H_2/\overline{H}_1)]P(H_3/\overline{H}_1\overline{H}_2)[1 - P(H_4/\overline{H}_1\overline{H}_2H_3)] \\
&\quad + [1 - P(H_1)][1 - P(H_2/\overline{H}_1)][1 - P(H_3/\overline{H}_1\overline{H}_2)]P(H_4/\overline{H}_1\overline{H}_2\overline{H}_3) \\
&= 3(1-P_1)^2(P_1 - P_2) + P(1-P_1)^3 \\
&= p(1-p)^3 + 3(1-p)^2p(1-p)(1-k) \\
&= p(1-p)^3 + 3p(1-p)^3(1-k) \; . \qquad (4\text{-}15)
\end{aligned}
$$

$P(2/4)$ = probability that two of the units are failed by human error

$$
\begin{aligned}
&= P(H_1)P(H_2/H_1)[1 - P(H_3/H_1H_2)][1 - P(H_4/H_1H_2\bar{H}_3)] \\
&+ P(H_1)[1 - P(H_2/H_1)]P(H_3/H_1\bar{H}_2)[1 - P(H_4/H_1\bar{H}_2H_3)] \\
&+ P(H_1)[1 - P(H_2/H_1)][1 - P(H_3/H_1\bar{H}_2)]P(H_4/H_1\bar{H}_2\bar{H}_3) \\
&+ [1 - P(H_1)]P(H_2/\bar{H}_1)P(H_3/\bar{H}_1H_2)[1 - P(H_4/\bar{H}_1H_2H_3)] \\
&+ [1 - P(H_1)]P(H_2/\bar{H}_1)[1 - P(H_3/\bar{H}_1H_2)]P(H_4/\bar{H}_1H_2\bar{H}_3) \\
&+ [1 - P(H_1)][1 - P(H_2/\bar{H}_1)]P(H_3/\bar{H}_1\bar{H}_2)P(H_4/\bar{H}_1\bar{H}_2H_3) \\
&= 2(1 - P_1)(P_2 - P_3) + 2P_1(P_1 - P_2)(1 - P_1) + (P_1 - P_2)^2 \\
&+ P_2(1 - P_1)^2 \\
&= 2(1 - p)(1 - p)(1 - k)^2p[1 - (1 - p)(1 - k)] \\
&+ 2p(1 - p)p(1 - p)(1 - k) + [p(1 - p)(1 - k)]^2 \\
&+ (1 - p)^2p[1 - (1 - p)(1 - k)] \\
&= p(1 - p)^2 + [2p^2(1 - p)^2 - p(1 - p)^3](1 - k) \\
&+ p(1 - p)^2(2 + p)(1 - k)^2 - 2p(1 - p)^3(1 - k)^3 .
\end{aligned}
\tag{4-16}
$$

$P(3/4)$ = probability that three of the units are failed by human error

$$
\begin{aligned}
&= P(H_1)P(H_2/H_1)P(H_3/H_1H_2)[1 - P(H_4/H_1H_2H_3)] \\
&+ P(H_1)P(H_2/H_1)[1 - P(H_3/H_1H_2)]P(H_4/H_1H_2\bar{H}_3) \\
&+ P(H_1)[1 - P(H_2/H_1)]P(H_3/H_1\bar{H}_2)P(H_4/H_1\bar{H}_2H_3) \\
&+ [1 - P(H_1)]P(H_2/\bar{H}_1)P(H_3/\bar{H}_1H_2)P(H_4/\bar{H}_1H_2H_3) \\
&= (1 - p)(1 - k)^3p[1 - (1 - p)(1 - k)][1 - (1 - p)(1 - k)^2] \\
&+ p(1 - p)(1 - k)^2p[1 - (1 - p)(1 - k)] \\
&+ p[1 - (1 - p)(1 - k)]p(1 - p)(1 - k) \\
&+ (1 - p)p[1 - (1 - p)(1 - k)][1 - (1 - p)(1 - k)]^2 \\
&= p(1 - p) + p(1 - p)(2p - 1)(1 - k) \\
&+ [p^2(1 - p) - p^2(1 - p)^2 - p(1 - p)^2](1 - k)^2 \\
&+ [p(1 - p)^3 + p(1 - p) - p^2(1 - p)^2](1 - k)^3 - p(1 - p)^2(1 - k)^4 \\
&- p(1 - p)^2(1 - k)^5 + p(1 - p)^3(1 - k)^6 .
\end{aligned}
\tag{4-17}
$$

$P(4/4)$ = probability that all four units are failed by human error

$$= P(H_1)P(H_2/H_1)P(H_3/H_1H_2)P(H_4/H_1H_2H_3)$$

$$= P_4$$

$$= p[1 - (1 - p)(1 - k)][1 - (1 - p)(1 - k)^2][1 - (1 - p)(1 - k)^3]$$

$$= p - p(1 - p)(1 - k) - p(1 - p)(1 - k)^2 - p^2(1 - p)(1 - k)^3$$

$$+ p(1 - p)^2(1 - k)^4 + p(1 - p)^2(1 - k)^5 - p(1 - p)^3(1 - k)^6 . \quad (4\text{-}18)$$

As expected,

$$P(0/4) + P(1/4) + P(2/4) + P(3/4) + P(4/4) = 1 .$$

For a 1 out of 4:G logic type of system, the system failure probability is given by

$$1p_4 = P(4/4) = P_4 ,$$

which is obtained from Eq. (4-18).

For a 2 out of 4:G logic type of system, the system failure probability is given by

$$2p_4 = P(3/4) + P(4/4)$$

$$= p(2 - p) - 2p(1 - p)^2(1 - k)$$

$$+ p(1 - p)(p^2 + p - 2)(1 - k)^2 + 2p(1 - p)^3(1 - k)^3 . \quad (4\text{-}19)$$

For a 3 out of 4:G logic type of system, the system failure probability is given by

$$3p_4 = P(2/4) + P(3/4) + P(4/4)$$

$$= (3 - 3p + p^2)p - 3p(1 - p)^3(1 - k) . \quad (4\text{-}20)$$

4.3 Investigation of the Influence of the Dependence Factor on System Failure Probability

The impact of the dependence between failures is that it reduces the gain in system reliability achieved by the use of redundant units. The degree of dependence between failures is the determining factor in such reliability reduction and its detrmination is the most important part of the problem. If the individual failure probability (p) and the degree of dependence among the

various failures (the dependence factor, k) are known, the optimum system can be chosen. Two types of systems with the same random failure probability are seen to have different failure probabilities when the dependence between failures is taken into account. The advantage of using one system rather than another may be altered when the degree of dependence between failures is increased or decreased. Often the reduction of dependence between failures receives too much attention, when it might be better to reduce the individual failure probability and use a different type of system, the reason being that the degree of dependence would have to be reduced to an unachievably low value to achieve the same reliability. Therefore, choice of an optimum system requires consideration of the individual failure probability (p), the degree of dependence (k), and the type of system. With the help of the model described above, the influence of these three parameters on system reliability is analyzed here.

Figure 9 shows the variation in failure probability due to changes in degree of dependence between failures, for a fixed individual failure probability ($p = 10^{-2}$), for redundant systems of the m out of n:G logic type (i.e., the system of n components is good i.f.f. at least m components are good) including a 1 out of 2:G, a 1 out of 3:G, and a 1 out of 4:G system. The random failure probabilities of these systems differ by at least two orders of magnitude but any significant gain in system reliability due to redundancy is largely wiped out when the degree of dependence (k) between the failures reaches about 0.3. For $k \geq 0.3$, the advantage of using redundancy beyond 2 is almost nil. When the failures due to different actions are totally dependent on each other ($k = 1$), the advantage of using extra redundancy is totally lost, as shown by the convergence of the curves at that point.

Figure 10 shows the relation between system failure probability and degree of dependence between failures for the same three systems, but with individual failure probabilities adjusted so as to make the random failure probability the same for all three systems. The individual failure probability (p) is then 1×10^{-3}, 1×10^{-2}, and 3.16×10^{-2} for a 1 out of 2:G, 1 out of 3:G, and 1 out of 4:G system respectively. In this case the curves for a 1 out of 2:G and a 1 out of 3:G system intersect at $k = 0.032$. That is, a 1 out of 2:G system with $p = 10^{-3}$ is the better choice for $k > 0.032$, but not for $k < 0.032$.

Table 6

Multiple Failure Probabilities Due to
Human Error for Different G-Logic Types of Systems

Type of G-Logic System	System Failure Probability
1 out of 2	$kp + p^2(1 - k)$
1 out of 3	$p - p(1 - p)(1 - k) - p(1 - p)(1 - k)^2 + p(1 - p)^2(1 - k)^3$
2 out of 3	$p(2 - p) - 2p(1 - p)^2(1 - k)$
1 out of 4	$\prod_{i=0}^{3} [1 - (1 - p)(1 - k)^i]$
2 out of 4	$p(2 - p) - 2p(1 - p)^2(1 - k) + p(1 - p)(p^2 + p - 2)(1 - k)^2 + 2p(1 - p)^3(1 - k)^3$
3 out of 4	$(3 - 3p + p^2)p - 3p(1 - p)^3(1 - k)$

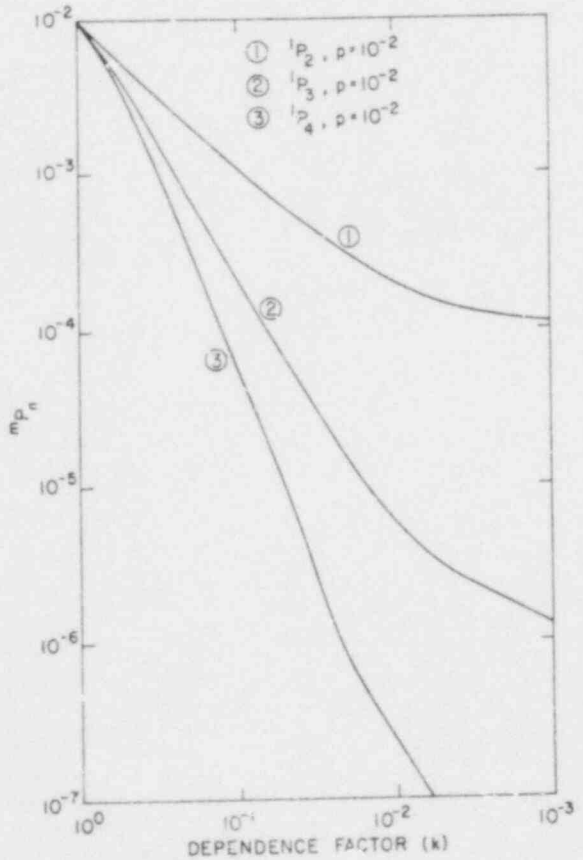

Figure 9. Relation between different 1 out of n:G type system failure probabilities and dependence factor for a fixed individual failure probability.

Similarly, for the choice between a 1 out of 2:G and a 1 out of 4:G system the determining value of k is 0.046. Thus, for k values > 0.046, as they usually are, it appears more beneficial to reduce the individual failure probability rather than to increase the redundancy of the system.

The results of a similar analysis of a 2 out of 3:G and a 2 out of 4:G system are presented in Figure 11. For k > 0.033, the failure probability was found to be much lower for a 2 out of 3:G system with $p = 10^{-3}$ than for a 2 out of 4:G system with $p = 10^{-2}$.

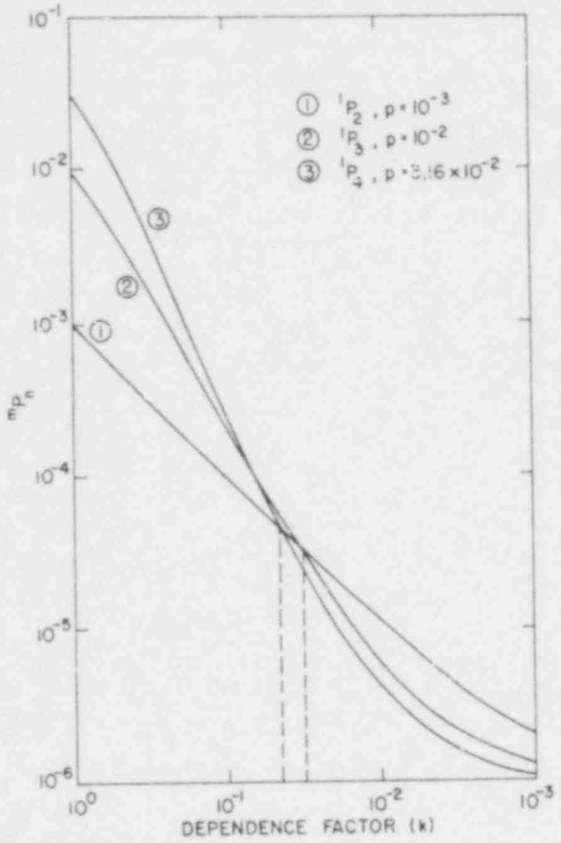

Figure 10. Relation between different 1 out of n:G system failure probabilities (with some random system failure probabilities) and dependence factor.

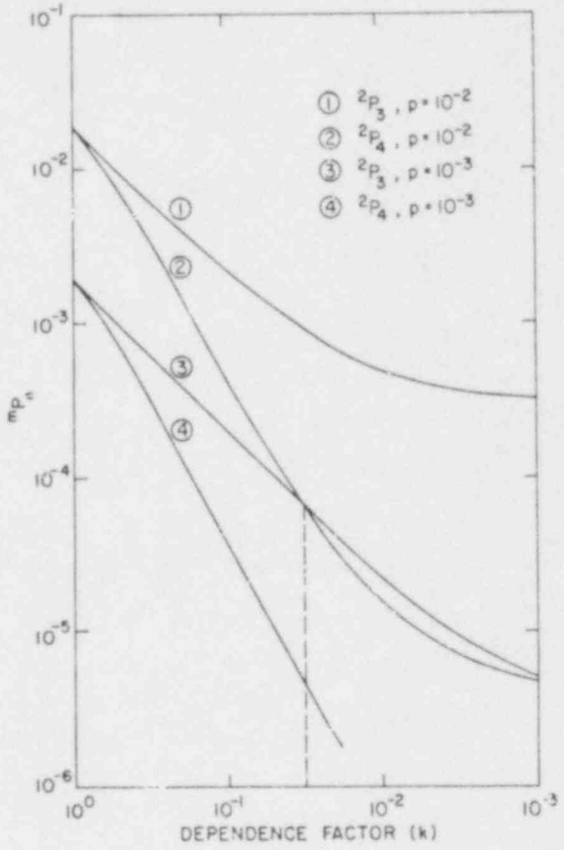

Figure 11. Relation between different m out of n:G type system failure probabilities and dependence factor.

4.4 Estimation of the Parameters of the Model

The parameters of the model were estimated from the available data. The two parameters needed are the individual failure probability (p) and the dependence factor (k). Since p is largely known, k is the parameter that it is important to estimate.

The estimation procedure used was the moment estimation technique, which provides point estimates for the parameters. This is not as flexible as the maximum likelihood estimation technique, but it leads to much simpler equations. For our case, even for three-unit systems, the maximum likelihood estimation procedure leads to very complicated fifth-order simultaneous equations that would require sophisticated computer programs for solution. Since at this stage an understanding of where the value of the dependence factor lies is of interest, moment estimates are considered suitable. For more accurate results, these estimates can be used as the initial value (seed) in an iterative computer program to obtain a maximum likelihood estimate.

The general technique of moment estimation is to match the moments of the data to the moments of the hypothesized distribution.[18] If the numbers $x_1, x_2, \ldots, x_n$ represent a set of data, then an unbiased estimator of the k^{th} origin moment of the data is

$$m_k = \frac{1}{n} \sum_{i=1}^{n} x_i^k \ .$$

The moments of the distribution are given by

$$\mu_k = \int_0^\infty t^k f(t)dt \ .$$

In our case,

$$\mu_k = \sum_{i=1}^{n} i^k P(i/n) \ ,$$

where $P(i/n)$ is the probability that i out of n components of the system fail.

If the hypothesized distribution has n parameters, n equations are obtained by equating m_1 to μ_1, m_2 to μ_2, ..., and m_n to μ_n. For our case with two unknown parameters, m_1 is equated to μ_1 and m_2 to μ_2, and the solution of the resulting equations provides estimates of the parameters.

The data required for such an analysis are scarce. The model developed requires data on the number of occurrences, each, of 1, 2, ..., n failures in an n-unit system. Rasmussen[19] reviewed Licensee Event Reports as a source of human error data and judged 111 reported errors to be in the category "calibration, setting, and testing." These are the only available data on such failures and are presented in Table 7. Rasmussen points out that "the reports do not give information on the actual frequency of errors committed but rather on the frequency of errors which are immediately corrected by the operator. This means that the error frequencies found in the reports are heavily biased by opportunities for self monitoring and error correction in the specific task." But, since the probability of system failure due to human errors rather than the specific human error rates is of interest here, these data are suitable for our analysis. Also, since the model developed does not take into account possible feedback alerting the operator to the commission of successive errors, (recovery factor), the failure data obtained after the operator's error correction due to feedback are appropriate for use.

As evident from Table 7, the total number of opportunities for such failures is usually not available, i.e., the problem is lack of "denominator data." The purpose of this study is not the development of human error rates, but rather the determination of the dependence between human failures. Therefore, based on RSS,[1] the assumption is made that failure to return a manually operated test valve to its proper configuration after maintenance has a rate of 10^{-2}, i.e., $p = 10^{-2}$. Based on this and the available data, a determination of the total number of opportunities for failure can be made, as follows.

The data indicating failures in 17 channels are neglected because this happened only once and no simultaneous failures in 5 to 16 channels have been recorded, and its incorporation would involve unnecessary complications. This leaves data for a 4-unit system.

Let x_0 be the number of times none of the units was affected by human error. Then

$$(x_0 + 96 + 11 + 2 + 2) = (x_0 + 111)$$

is the total number of opportunities for human error, and $(1 - p)^4$, the

probability that none of the channels is affected by human error, is

$$(1 - p)^4 = \frac{x_c}{x_o + 111} .$$

For $p = 10^{-2}$,

$x_o = 2706$ and $N = x_o + 111 = 2817$.

By using a similar technique and data for the first three units, the total number of opportunities for failure can be estimated for three units; these data are used for the analysis of the 3-unit system in the next section.

Table 7

Human Errors in Test and Calibration

Number of Channels Affected by Operator		Number of Cases
1	x_1	95
2	x_2	11
3	x_3	2
4	x_4	2
17	x_{17}	1

Table 8

Derived Data for Human Errors in Test and Calibration

Number of Channels Affected by Operator		Number of Cases
0	x_0	2706
1	x_1	95
2	x_2	11
3	x_3	2
4	x_4	2
		N = 2817

3-Unit System

The moment estimation technique and the available data were used to determine the dependence factor (k) and the individual failure probability (p). Since p was assumed to be 10^{-2} in developing the derived data, the estimated value of p is expected to be around 10^{-2}. Application of the technique used above for a 4-unit system in a 3-unit system gave the total number of opportunities for failure for a 3-unit system, listed in Table 9.

Table 9

Derived Data for Human Errors in Test and Calibration for a 3-Unit System

Number of Channels Affected by Operator	Number of Cases	
0	x_0	3528
1	x_1	95
2	x_2	11
3	x_3	2
	N =	3636

The moments equations for a 3-unit system are

$$P(1/3) + 2P(2/3) + 3P(3/3) = \frac{1}{N}(x_1 + 2x_2 + 3x_3) ,$$

$$P(1/3) + 4P(2/3) + 9P(3/3) = \frac{1}{N}(x_1 + 4x_2 + 9x_3) . \qquad (4\text{-}21)$$

Use of P(i/n)'s in the form presented in Section 4.2 gives very complicated simultaneous equations. These are avoided by using approximations neglecting the higher-order terms:

The expression

$$P(1/3) = 2p(1 - p)^2(1 - k) + p(1 - p)^2$$

$$= 3p - 2pk - 6p^2 + 4p^2k$$

becomes, with the p^2k term neglected,

$$P(1/3) \simeq 3p - 6p^2 - 2pk .$$

For the expression

$$P(2/3) = p(1 - p)[1 - (1 - 2p)(1 - k) + (1 - k)^2 - (1 - p)(1 - k)^3]$$

$$= 2pk + 3p^2 - 7p^2k - 2k^2p + k^3p - 3p^3 - 5p^3k - 2k^2p^2 - k^3p^2,$$

since k is expected to be about an order of magnitude greater than p, the terms containing up to third orders of k were kept whereas higher orders of

p were neglected. Neglecting p^2k, p^3, p^3k, k^2p^2, and k^3p^2 terms gives

$$P(2/3) \simeq 2kp + 3p^2 - 2k^2p + k^3p .$$

The expression

$$P(3/3) = p - p(1 - p)(1 - k) - p(1 - p)(1 - k)^2 + p(1 - p)^2(1 - k)^3$$
$$= p^3 + 3p^2k + 2pk^2 - 5k^2p^2 - k^3p$$

becomes, with the k^2p^2 term neglected,

$$P(3/3) \simeq p^3 + 3p^2k + 2pk^2 - k^3p .$$

Use of the approximate expressions for P(i/n)'s in the moments equations and the data in Table 9 gives

$$3p + 2pk + 2k^2p + 3p^3 - 4k^3p + 9p^2k = 0.0342,$$

and

$$3p + 6p^2 + 9p^3 + 6pk + 10k^2p - 5k^3p + 27p^2k = 0.0436 . \quad (4\text{-}22)$$

Again, neglecting the higher-order terms reduces the equations to the form

$$3p + 2pk + 2k^2p = 0.0342 , \quad (4\text{-}23)$$

$$3p + 6p^2 + 6pk + 10k^2p = 0.0436 . \quad (4\text{-}24)$$

From Eq. (4-23),

$$p = 0.0342/(3 + 2k + 2k^2) .$$

Use of this value of p in Eq. (4-24) gives an equation for k:

$$0.5096k^4 + 0.7456k^3 + 0.944k^2 + 0.296k - 0.205 = 0 .$$

This equation was solved in a programmable calculator, which gave the following results:

$$k = 0.301 \quad \text{and} \quad p = 9.04 \times 10^{-3} . \quad (4\text{-}25)$$

The model was tested with two hypothetical data sets representing extreme situations -- (1) complete independence and (2) complete dependence between failures. The first data set was created by simulating almost binomial data, with the p value maintained at 10^{-2}, and is shown in Table 10.

The moments equations for this data set are

$$3p + 2pk + 2k^2p = 0.03147,$$

$$3p + 6p^2 + 6pk + 10k^2p = 0.03475 ,$$

and their solution is

$$k = 0.0603 . \qquad (4\text{-}26)$$

This is justified because a low value of k, approaching zero, is expected for random failures, and binomial failure data represent such a situation. A perfect binomial data will result in k = 0. Thus, the model properly interprets data representing random failures. This is borne out by the fact that the probability expressions in Section 4.2 represent binomial distribution for k = 0.

The second data set, also with p maintained at 10^{-2}, is shown in Table 11.

Table 10

Example Data Set Representing Complete Independence Between Failures for Human Errors in Test and Calibration for a 3-Unit System

Number of Channels Affected by Operator		Number of Cases
0	x_0	3267
1	x_1	95
2	x_2	3
3	x_3	1
	N =	3366

Table 11

Example Data Set Representing Complete Dependence Between Failures for Human Errors in Test and Calibration for a 3-Unit System

Number of Channels Affected by Operator		Number of Cases
0	x_0	1164
1	x_1	10
2	x_2	2
3	x_3	24
	N =	1200

The moments equations for this data set are

$$3p + 2pk + 2k^2p = 0.07167,$$

$$3p + 6p^2 + 6pk + 10k^2p = 0.19500,$$

and their solution is

$$k = 0.988 . \qquad (4\text{-}27)$$

This data set shows strong dependence between failures because the failure data are dominated by the failure of all three units. Other combinations also can result in $k > 1$, and these are interpreted as totally dependent situations.

4-Unit System

The value of k for a 4-unit system was determined from the data in Table 8 The approximations for P(i/n)'s for a 4-unit system are as follows:

$$P(0/4) = 1 - 4p ,$$

$$P(1/4) = 4p - 12p^2 - 3pk ,$$

$$P(2/4) = 3pk + 6p^2 - 4pk^2 ,$$

$$P(3/4) = 8p^2k + (4p - 26p^2)k^2 - (8p - 37p^2)k^3 + 9pk^4 - 5pk^5 ,$$

$$P(4/4) = 13p^2k^2 + (6p - 31p^2)k^3 - 9pk^4 + 6pk^5 . \qquad (4\text{-}28)$$

The moments equations for a 4-unit system are

$$P(1/4) + 2P(2/4) + 3P(3/4) + 4P(4/4) = \frac{1}{N}(x_1 + 2x_2 + 3x_3 + 4x_4) = c_1 ,$$

$$P(1/4) + 4P(2/4) + 9P(3/4) + 16P(4/4) = \frac{1}{N}(x_1 + 4x_2 + 9x_3 + 16x_4) = c_2 .$$

Use of P(i/n)'s from Eq. (4-28) in moments equations, neglecting some of the higher-order terms, gives

$$p(4 + 3k + 4k^2 - 9k^4 + 9k^5) + p^2(24k - 26k^2) = c_1 ,$$

$$p(4 + 9k + 20k^2 + 24k^3 - 53k^4) + p^2(12 + 72k - 26k^2) = c_2 .$$

Use of the data from Table 8 gives

$$c_1 = 0.04878 \quad \text{and} \quad c_2 = 0.07021.$$

With some algebraic manipulation, these values result in

$$p = \frac{0.585 + 3.392k + 0.558k^2 - 8.098k^3}{48 + 228k + 48k^2 - 436k^3 + 1432k^4}$$

Replacing p by the above expression provides an equation for k:

$$0.05 + 4.44k + 12.46k^2 - 17.148k^3 - 95.98k^4 - 36.82k^5 + 25.51k^6 + 77.9k^7 = 0 .$$

The solution for k is

$$k = 0.403 . \qquad (4\text{-}29)$$

2-Unit System

The moments equations for a 2-unit system are

$$P(1/2) + 2P(2/2) = \frac{1}{N}(x_1 + 2x_2) ,$$

$$P(1/2) + 4P(2/2) = \frac{1}{N}(x_1 + 4x_2) .$$

Replacing the P(i/n)'s gives

$$2p + kp(1 - p) + \frac{1}{N}(x_1 + 2x_2),$$

$$2p + 2p^2 + 3kp(1 - p) = \frac{1}{N}(x_1 + 2x_2) . \qquad (4\text{-}30)$$

Use of data up to 2 units from the original data set, and maintaining $p = 10^{-2}$ gives the data set shown in Table 12. Solving Eq. (4-30) with these data results in

$$k = 0.199 . \qquad (4\text{-}31)$$

Table 12

Derived Data for Human Error in Test and Calibration for a 2-Unit System

Number of Channels Affected by Operator	Number of Cases	
0	x_0	5270
1	x_1	95
2	x_2	11
	N =	5376

4.5 Discussion of Results

Significant liberties had to be taken in manipulating the data base because of the scarcity of available data. Strictly speaking, in analyzing an n-unit system, only data from an n-unit system should be used. That is, data from a 4-unit system should be used only for determining the dependence factor in a 4-unit system and should not be manipulated for use with a 3-unit or 2-unit system. However, even though such manipulations were performed in the study, and the moment estimation technique used was simpler than superior ones such as the maximum likelihood estimation technique, the results obtained provide interesting insights into dependent failure probability.

The dependence factors obtained for 2-unit, 3-unit, and 4-unit systems are 0.199, 0.301, and 0.403 respectively. These factors imply that the contribution of dependent failure probability is much larger than the commonly accepted estimate that such a contribution is 10% of the individual failure probability, which was based on data for hardware failures only. The comparable β-value in a β-factor model for the same failure probability is > 0.1. The values of dependence factor obtained indicate that dependence is much stronger among human failures than among failures due to other causes.

These limited data also suggest that the dependence among failures increases as the number of components in the system increases. If this is so, it will offset the gain in system reliability due to added redundancy. Since increased redundancy and increased dependence among failures have a competing influence on system failure probability, an optimum choice regarding the amount of redundancy can be made from the point of view of human failures. The results in Table 13 show that in going from a 1 out of 2:G to a 1 out of 3:G system, the failure probability decreases even though the dependence factor increases from 0.199 to 0.301 because the increase in dependence does not fully offset the gain due to added redundancy. In going from a 1 out of 3:G to a 1 out of 4:G system, however, the dependence factor increases from 0.301 to 0.403, and this raises the system failure probability from 1.59×10^{-3} to 2.1×10^{-3}, fully offsetting the gain due to added redundancy. These limited data indicate that, with respect to human failures, a 1 out of 3:G system is the most reliable one of the 1 out of n:G type. This is consistent with the observation in Section 4.3 that any significant gain in system

reliability in 1 out of n:G type systems due to redundancy > 3 is largely wiped out when the degree of dependence between failures reaches about 0.3. As more data become available, it will be possible to use this model to choose the most reliable system for application when dependent failures play a significant role.

Table 13

System Failure Probabilities Due to Human Error for Different G Type Systems

Type of G-Logic System	p	k	System Failure Probability
1 out of 2	10^{-2}	0.199	2.07×10^{-3}
1 out of 3	10^{-2}	0.301	1.59×10^{-3}
2 out of 3	10^{-2}	0.301	5.20×10^{-3}
1 out of 4	10^{-2}	0.403	2.1×10^{-3}
2 out of 4	10^{-2}	0.403	5.31×10^{-3}
3 out of 4	10^{-2}	0.403	1.23×10^{-2}

5. SUMMARY AND CONCLUSIONS

In analyzing the nature of dependence among human failures in a multiple sequential action, the way human error causes failure of the components of a system was found to differ from the way a single hardware failure causes failure of all the components. Human error causes selective failure of components depending on when the failure started. This type of dependent failure was distinguished from other types of dependent failures in which all the components failed, and it was termed multiple sequential failure (msf).

Available models for dependent failures were analyzed with regard to their applicability to msfs and were found to be lacking. These models do not distinguish among various types of dependent failures, and the same quantification technique has been applied regardless of the basic nature of the dependent failures. In our opinion it is erroneous to apply the same dependent failure model to different types of dependent failures, and therefore dependent failures were separated into three broad categories, each requiring a different model for quantification.

This study addressed the type of dependent failure categorized as multiple sequential failure during testing, maintenance, and calibration. Two models were develped. The first is very general in nature and does not require any dependent failure data. Various well-known distributions were used to describe the dependent failure in this model. The final estimate obtained with this model is a conservative one with associated uncertainty. The uncertainty was calculated considering many possible sources--data, coupling, and modeling. Such a method of estimation seems to be appropriate when no data on dependent failures are available.

In the second model developed, details of the process in msfs were taken into account. The model includes two parameters-- dependent failure probability and the dependence factor between failures. This model provided interesting insights into the influence of dependence between failures on system reliability. The results indicated that for a 1 out of n:G system the advantage of using redundance > 3 units is almost completely lost when the dependence factor between failures is $\geq$ 0.3. Also, use of the limited data available suggested that dependence among the failures due to human error is much stronger than that among those due to hardware failures. The dependence fac-

tors obtained for 2-unit, 3-unit, and 4-unit systems are 0.19, 0.30, and 0.40 respectively. For hardware failure, the comparable dependence factor is about 0.1. Also, the dependence factor appears to increase as the number of components in the system increases. Since the dependence actor and the redundancy ina system have competing influences, this model can be effectively used to choose an optimum system from the point of view of reliability.

APPENDIX

SECOND MOMENT ABOUT THE MEDIAN OF A LOGNORMAL DISTRIBUTION

The lognormal distribution is defined by its probability density function (pdf),

$$f(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp[-(\ln x - \mu)^2/2\sigma^2] \quad , \quad x > 0 \ ,$$

where μ and σ are the standard lognormal parameters;

$$\text{median} = e^{\mu} \ .$$

The second moment about the median is

$$\int_{-\infty}^{\infty} (x - e^{\mu})^2 f(x)dx$$

$$= \int_{-\infty}^{\infty} (x^2 - 2xe^{\mu} + e^{2\mu}) \frac{1}{\sigma\sqrt{2\pi}} \frac{1}{x} \exp[-(\ln x - \mu)^2/2\sigma^2]dx$$

$$= \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} xe^{-\frac{(\ln x-\mu)^2}{2\sigma^2}} dx - \frac{2e^{\mu}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(\ln x-\mu)^2}{2\sigma^2}} dx$$

$$+ \frac{e^{2\mu}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} \frac{1}{x} e^{-\frac{(\ln x-\mu)^2}{2\sigma^2}} dx \ .$$

Make change of variables:

$$\ln x = t \quad \text{or} \quad dx = e^t dt$$

and

$$e^t = x \ .$$

The equation for the second moment about the median is transformed into

$$\frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{t} e^{-\frac{(t-\mu)^2}{2\sigma^2}}\, dt - \frac{2e^{\mu}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(t-\mu)^2}{2\sigma^2}}\, e^{t} dt + \frac{e^{2\mu}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(t-\mu)^2}{2\sigma^2}}\, dt$$

$$= \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma^2} t^2 + 2t + \frac{\mu}{\sigma^2} t - \frac{\mu^2}{2\sigma^2}}\, dt - \frac{2e^{\mu}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma^2} t^2 + t + \frac{\mu t}{\sigma^2} - \frac{\mu^2}{2\sigma^2}}\, dt$$

$$+ \frac{e^{2\mu}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma^2} t^2 + \frac{\mu}{\sigma^2} t - \frac{\mu^2}{2\sigma^2}}\, dt$$

$$= \frac{e^{-\mu^2/2\sigma^2}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma^2} t^2 + \frac{2\sigma^2+\mu}{\sigma^2} t}\, dt$$

$$- \frac{2e^{\mu - \mu^2/2\sigma^2}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma^2} t^2 + \frac{\mu+\sigma^2}{\sigma^2} t}\, dt$$

$$+ \frac{e^{2\mu - \mu^2/2\sigma^2}}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma^2} t^2 + \frac{\mu}{\sigma^2} t}\, dt .$$

Use of the standard integral,

$$\int_{-\infty}^{\infty} e^{-p^2x^2+qx}\, dx = e^{q^2/4p^2} \frac{\sqrt{\pi}}{p} ,$$

gives

$$\frac{e^{-\mu^2/2\sigma^2}}{\sigma\sqrt{2\pi}} \cdot e^{2\mu+2\sigma^2+\mu^2/2\sigma^2}\sigma\sqrt{2\pi}$$

$$+ \frac{2e^{\mu-\mu^2/2\sigma^2}}{\sigma\sqrt{2\pi}} e^{\mu^2/2\sigma^2 + \mu+\sigma^2/2}\sigma\sqrt{2\pi} + \frac{e^{2\mu-\mu^2/2\sigma^2}}{\sigma\sqrt{2\pi}} e^{\mu^2/2\sigma^2}\sigma\sqrt{2\pi}$$

$$= e^{2\mu+2\sigma^2} - 2e^{2\mu+\sigma^2/2} + e^{2\mu}$$

$$= e^{2\mu}(e^{2\sigma^2} - 2e^{\sigma^2/2} + 1)$$

LIST OF ACRONYMS

BWR	Boiling Water Reactor
CLCS-HI	Consequence Limiting Control System - Hi
CSIS	Containment Spray Injection System
HPIS	High Pressure Injection system
HTGR	High Temperature Gas Cooled Reactor
i.f.f.	if and only if
LOCA	Loss of Coolant Accident
LPIS	Low Pressure Iniection System
msf	Multiple Sequert'al Failure
PWR	Pressurized Water Reactor
RPS	Reactor Protection System
SICS	Safety Injection Control System

ACKNOWLEDGEMENTS

The authors wish to thank Mr. Robert E. Hall of Brookhaven National Laboratory for his constant encouragement and support throughout this project and Professor William Kerr of the University of Michigan for many useful discussions. Thanks are also due to Ms. Margaret Dienes for her technical editing of the report and to Ms. Susan Monteleone for her help in typing and preparing the manuscript.

REFERENCES

1. Reactor Safety Study (RSS), An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400; NUREG 75/014, 1975.

2. G.T. Edwards and I.A. Watson, A Study of Common Mode Failures, Safety and Reliability Directorate, UKAEA, July 1979.

3. E.P. Epler, Common mode failure considerations in the design of systems for protection and control, Nuclear Safety, 10(1), 38-45 (1969).

4. W.C. Gangloff, An Evaluation of Anticipated Operational Transients in Westinghouse Pressurized Water Reactor, WCAP-7486, May 1971.

5. I.M. Jacobs, The common mode failure study discipline, IEEE Trans. Nucl. Sci. NS-17, 594-8 (1977).

6. T. Mankamo, Common Cause Failures of Reactor Pressure Components, IAEA-SM-218/5, 125-137, 1977.

7. P.K. Samanta, A.L. Swoboda, and R.E. Hall, Sensitivity of Risk Parameters to Human Errors in Reactor Safety Study for a PWR, NUREG/CR-1879, BNL-NUREG-51322, Jan. 1981.

8. K.N. Fleming, A Reliability Model for Common Mode Failures in Redundant Safety Systems, GA-A13284, April 1975.

9. W.E. Vesely, Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specialization, in Nuclear Systems Reliability Engineering and Risk Assessment, J.B. Fussel and G.R. Burdick, Eds., SIAM, Philadelphia, 1977.

10. K.N. Fleming and P.H. Raabe, A Comparison of Three Methods for the Quantitative Analysis of Common Cause Failures, GA-A14568, May 1978.

11. T.H. Smith et al., A Risk Base Fault Tree Analysis Method for Identification, Preliminary Evaluation, and Screening of Potential Accident Release Sequences in Nuclear Fuel Cycle Operations, BNWL-1959, Jan. 1976.

12. G.E. Apostolakis, Effect of certain class of potential common mode failures on the reliability of redundant systems, Nuclear Engineering and Design 36 (1), 123-133 (1976).

13. H.W. Lewis et al., Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission, NUREG/CR-0400, Sept. 1978.

14. K.N. Fleming et al., HTGR Accident Initiation and Progressing Analysis Status Report, Vol. II, GA-A13617, Vol. II, Oct. 1975.

15. G.E. Apostolakis et al., Methodology and Application of Probabilistic Evaluation to Thermal Reactor Safety, EPRI NP-1443, Project 297-1, July 1980.

16. A.W. Marshall and I. Olkin, A multivariate exponential distribution, JASA 62, 30-44 (1967).

17. P.L. Meyer, Introductory Probability and Statistical Applications, Addison-Wesley, Reading, MA, 1970.

18. M.L. Shooman, Probabilistic Reliability: An Engineering Approach, McGraw-Hill, New York, 1968.

19. J. Rasmussen, Operator/Technician Errors in Calibration, Setting and Testing Nuclear Power Plant Equipment, Working Paper, March 1978.

20. B.W. Lindgren and G.W. McElrath, Introduction to Probability and Statistics, 2nd ed., Macmillan, Riverside, NJ, 1959.

21. R.A. Waller, M.M. Johnson, M.S. Waterman, and H.F. Martz Jr., Gamma prior distribution selection for Bayesian analysis of failure rate and reliability, in Nuclear System Reliability Engineering and Risk Assessment, J.B. Fussel and G.R. Burdick, Eds., SIAM, Philadelphia, 1977.

NRC FORM 335 (7.77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG/CR-2211
BNL-NUREG-51411

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
Modeling of Multiple Sequential Failures During Testing, Maintenance, and calibration

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
P. K. Samanta and S. P. Mitra

5. DATE REPORT COMPLETED
MONTH: October YEAR: 1981

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Brookhaven National Laboratory
Upton, New York 11973

DATE REPORT ISSUED
MONTH: December YEAR: 1981

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Facility Operations
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
FIN A3219

13. TYPE OF REPORT
Final

PERIOD COVERED (Inclusive dates)

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

In this report the nature of dependence among human failures in a sequential action is analyzed and distinguished from other types of multiple failures. Human error causes selective failure of components depending on when the failure started. Two models are developed for quantifying the failure probability in a multiple sequential action. The first is very general in nature and does not require any dependent failure data. The failure probability obtained from this model is a conservative one with associated uncertainty. The uncertainty is calculated considering many possible sources such as data, coupling and modeling. In the second model, details of the process in multiple sequential failures are taken into account. The model increments the conditional failure probabilities by a certain amount from their lower bounds (independent failure probability). This approach provides important insights into the influence of dependence between failures on system reliability. The model can be used effectively to choose an optimum system considering the individual failure probability, dependence factor and the amount of redundancy in a system.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

Human Error
Dependent Failures
Common Mode Failures

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS (This report)
Unclassified

21. NO. OF PAGES

20. SECURITY CLASS (This page)
Unclassified

22. PRICE
$

NRC FORM 335 (7.77)

NUREG/CR-2211

MODELING OF MULTIPLE SEQUENTIAL FAILURES DURING TESTING, MAINTENANCE AND CALIBRATION

DECEMBER 1981