NUCLEAR SCIENCE AND ENGINEERING: 73, 1-18 (1980)

Markovian Reliability Analysis Under Uncertainty with an Application on the Shutdown System of the Clinch River Breeder Reactor

Ioannis A. Papazoglou and Elias P. Gyftopoulos

Massachusetts Institute of Technology, Nuclear Engineering Department
Cambridge, Massachusetts 02139

Received May 15, 1979
Accepted August 14, 1979

A methodology for the assessment of uncertainties about reliability of nuclear reactor systems described by Markov models is developed, and the uncertainties about the failure probability of the shutdown system of the Clinch River Breeder Reactor (CRBR) are assessed.

Failure and repair rates and all other inputs of reliability analysis are taken as random variables with known probability distribution functions (pdf's). The pdf of reliability is calculated by both a Monte Carlo simulation and a Taylor series expansion approximation. Three techniques are developed to reduce the computational effort: (a) ordering of system states, (b) merging of Markov processes, and (c) judicious choice of time steps.

A Markov model has been used for reliability analysis under uncertainty of the shutdown system of the CRBR. It accounts for common-cause failures, interdependences between unavailability of the system and occurrence of transients, and inspection and maintenance procedures that depend on the state of the system and that include possibility of human errors. Under these conditions, the failure probability of the shutdown system differs significantly from that computed without common-cause failures, human errors, and input uncertainties.

I. INTRODUCTION

The objectives of this paper are (a) the development of a methodology for the calculation of uncertainty about reliability[1] of a large nuclear reactor system described by a Markov model, and (b) the assessment of uncertainty about the failure probability of the shutdown system of the Clinch River Breeder Reactor (CRBR).

Markov models are used in reliability analyses whenever statistical dependences among either failures or repairs or both must be considered.[2-8] For large systems with many states, however, existing

[1]The term reliability refers to any probabilistic measure of performance of a system such as failure probability, availability, etc.

[2]I. A. PAPAZOGLOU and E. P. GYFTOPOULOS, "Markovian Reliability Analysis Under Uncertainty with an Application on the Shutdown System of the Clinch River Breeder Reactor," NUREG/CR-0405 or BNL-NUREG-50864, Brookhaven National Laboratory (1978).

[3]R. BARLOW and F. PROCHAN, *Mathematical Theory of Reliability*, John Wiley and Sons, Inc., New York (1965).

[4]G. H. SANDLER, *System Reliability Engineering*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey (1963).

[5]M. L. SHOOMAN, *Probabilistic Reliability: An Engineering Approach*, McGraw Hill Book Company, New York (1969).

[6]R. BILLINTON, R. J. RINGLEE, and A. J. WOOD, *Power-System Reliability Calculations*, M.I.T. Press, Cambridge, Massachusetts (1973).

[7]A. E. GREEN and A. J. BOURNE, *Reliability Technology*, Wiley-Interscience, New York (1972).

[8]J. A. BUZACOTT, *IEEE Trans. Reliab.*, **19**, 128 (1970).

0029-5639/80/0001-0001$02.00/0

methods are not practical because of numerical difficulties.[9,10] In addition, failure and repair rates of the components of a system may not be known with certainty, either because our knowledge of these rates is incomplete or because they are inherently uncertain. This is especially true for newly designed systems, such as the liquid-metal fast breeder reactor, the high-temperature gas-cooled reactor, and the gas-cooled fast breeder reactor. We conclude that reliability of such systems is uncertain, i.e., it has a range of values and a probability associated with each of these values.

In this paper, we present two techniques for reducing the numerical complexity of Markov chains describing large reactor systems, and also present a methodology for calculating uncertainty about reliability of a system described by a Markov chain, given the uncertainties about the reliability of its components.

As a numerical illustration of the methodology, we calculate the uncertainty about the failure probability of the shutdown system of the CRBR. Specifically, we calculate the uncertainties associated with the probability of loss of core coolable geometry due to failure to scram on transients. We use a Markov model that includes:

1. "common-cause failures" due to interdependences among the failure rates and the states of the components and the system
2. interdependences between the unavailability of the shutdown system and the occurrence of transients
3. inspection and maintenance procedures that depend on the state of the system and the possibility of human errors.

The inclusion in the model of interdependences and uncertainties about the characteristics of the components results in values of the failure probabilities significantly different from those found without consideration of interdependences and uncertainties.

The paper is divided into two parts. Part one describes the methodology. The basics of Markovian reliability analysis and three techniques for reducing the numerical complexity of the analysis of large systems are presented in Sec. II, and the problem of Markovian reliability analysis under uncertainty is given in Sec. III. The second part demonstrates the methodology developed in part one by assessing the uncertainties about the probability of loss of core coolable geometry of the CRBR. The description of the shutdown system is given in Sec. IV.A, the system mission and model in Sec. IV.B, the data base and assumed uncertainties about the reliability of various components in Sec. IV.C, results in Sec. IV.D, and conclusions in Sec. V.

II. MARKOVIAN RELIABILITY ANALYSIS OF LARGE SYSTEMS

First, we consider a Markovian system with failure and repair rates that are certain. It can be shown[2,11] that the computation of reliability involves the solution of the first-order difference equation,

$$\boldsymbol{\pi}(n+1) = \boldsymbol{\pi}(n) \cdot \mathbf{P} \quad , \tag{1}$$

where $\boldsymbol{\pi}(n)$ is the state probability vector at time n, and $\mathbf{P}$ is the transition probability matrix of the Markov process that describes the system. The transition rate of each component at time n depends on the state of the system, namely, on the states of other components. So, the model can account for common-cause failures. For example, the common-cause failure of two components can be modeled by assuming one failure rate when both components are operating and another when only one component is operating.

We can solve Eq. (1) with the aid of a computer. But, when the number of states of the system is large, the necessary computer storage and computer time are prohibitive because of the large size of the transition probability matrix $\mathbf{P}$. For example, for a system consisting of ten two-state components, $\mathbf{P}$ has more than 10^6 elements. In general, the computational effort associated with the solution of Eq. (1) depends on three factors: (a) structure of $\mathbf{P}$, (b) dimensions of $\mathbf{P}$, and (c) number of time steps.

We have developed techniques that address each of these factors. By ordering the states, we simplify the structure of $\mathbf{P}$ (Sec. II.A); by merging states into superstates, we reduce the dimensions of $\mathbf{P}$ (Sec. II.B); by introducing an approximation that permits the use of large time steps, we reduce their number (Sec. II.C).

II.A. Ordering of States

We classify the states of the system in a special order. First, if Z is the set of all possible states, we partition it into two subsets X and Y such that (a) X contains all the states in which the system is operating successfully—the subset of operating states, and (b) Y contains all the states in which the system is not operating—the subset of failed states. Correspondingly, we partition $\boldsymbol{\pi}(n)$ into subvectors $\boldsymbol{\pi}(n,X)$ and $\boldsymbol{\pi}(n,Y)$, and $\mathbf{P}$ into submatrices $\mathbf{P}(X,X)$, $\mathbf{P}(X,Y)$, $\mathbf{P}(Y,X)$, and $\mathbf{P}(Y,Y)$ so that Eq. (1) has the form

[9]G. SINGH and R. BILLINTON, *IEEE Trans. Reliab.*, **24**, 31 (1975).

[10]B. P. ZELENTSOV, *IÈEE Trans. Reliab.*, **19**, 132 (1970).

[11]R. HOWARD, *Dynamic Probabilistic Systems*, Vols. I and II, John Wiley and Sons, Inc., New York (1971).

$$[\boldsymbol{\pi}(n+1,X),\boldsymbol{\pi}(n+1,Y)] = [\boldsymbol{\pi}(n,X),\boldsymbol{\pi}(n,Y)]\cdot\begin{bmatrix}\mathbf{P}(X,X) & \mathbf{P}(X,Y)\\ \mathbf{P}(Y,X) & \mathbf{P}(Y,Y)\end{bmatrix} . \quad (2)$$

The vector $\boldsymbol{\pi}(n)$ contains the information for calculating reliability. For example, the probability that the system will occupy operating state i at time n is $\pi_i(n,X)$. Hence, the probability that the system will be operating at n—the availability $A(n)$— is given by the relation

$$A(n) = \sum_{i\in X} \pi_i(n,X) . \quad (3)$$

Again, the probability that the system will not leave the subset of operating states X during the time period from 0 to n inclusive—the reliability $R^*(n)$—is the probability that the system will be in X at n, given that transitions from Y back to X are not possible. Hence, $R^*(n)$ is given by the relation

$$R^*(n) = \sum_{i\in X} \pi_i^*(n,X) , \quad (4)$$

where $\boldsymbol{\pi}^*(n,X)$ is the solution of Eq. (2) with $\mathbf{P}(Y,X) = \mathbf{0}$.

Next, we partition X and Y into subsets $X(I)$, for $I = 0, 1, \ldots, M$, and $Y(K)$, for $K = 1, 2, \ldots, N$, respectively, where either I or K denotes the number of failed components of the system, M is the maximum number of failed components with which the system can still be operating, and N is the total number of components of the system. Correspondingly, we partition $\boldsymbol{\pi}(n,X)$ and $\boldsymbol{\pi}(n,Y)$ into subvectors, and $\mathbf{P}(X,X)$, $\mathbf{P}(X,Y)$, $\mathbf{P}(Y,X)$, and $\mathbf{P}(Y,Y)$ into submatrices in the ascending orders determined by I and K. Thus, Eq. (2) becomes

$$[\boldsymbol{\pi}^0(n+1,X),\ldots,\boldsymbol{\pi}^N(n+1,Y)] = [\boldsymbol{\pi}^0(n,X),\ldots,\boldsymbol{\pi}^N(n,Y)]\cdot\begin{bmatrix}[\mathbf{P}^{IJ}]_{XX} & [\mathbf{P}^{IL}]_{XY}\\ [\mathbf{P}^{KJ}]_{YX} & [\mathbf{P}^{KL}]_{YY}\end{bmatrix} , \quad (5)$$

where X and Y are the unions

$$X = X(0)UX(1)\ldots UX(M) , \quad (6a)$$

$$Y = Y(1)UY(2)\ldots UY(M)\ldots UY(N) , \quad (6b)$$

$I, J = 0, 1, \ldots, M$, and $K, L = 1, 2, \ldots, N$. The number of subvectors $\boldsymbol{\pi}^Q(n,R)$ is $M + N + 1$. Since each subvector consists of more than one state probability $\pi_i(n)$, $M + N + 1$ is smaller than the number of state probabilities (system states) Z.

Finally, in general, we can use a time step such that transition probabilities among system states differing in the states of two or more components are negligible. Then, the submatrices of $\mathbf{P}$ in Eq. (5) are of the form

$$\mathbf{P} = \left[\begin{array}{cccc|cccc}
\mathbf{P}^{00} & \mathbf{P}^{01} & 0 & \ldots 0 & \mathbf{P}^{01} & 0 & 0 & \ldots 0 \\
\mathbf{P}^{10} & \mathbf{P}^{11} & \mathbf{P}^{12} & \ldots 0 & 0 & \mathbf{P}^{12} & 0 & \ldots 0 \\
\vdots & \ddots & \ddots & & \vdots & \ddots & \ddots & \\
0 & \ldots & & \mathbf{P}^{MM} & 0 & \ldots & & \mathbf{P}^{M,M+1} \\
\hline
\mathbf{P}^{10} & 0 & 0 & \ldots 0 & \mathbf{P}^{11} & \mathbf{P}^{12} & 0 & \ldots 0 \\
0 & \mathbf{P}^{21} & 0 & \ldots 0 & \mathbf{P}^{21} & \mathbf{P}^{22} & \mathbf{P}^{23} & \ldots 0 \\
\vdots & \ddots & \ddots & & \vdots & \ddots & \ddots & \\
0 & \ldots & & \mathbf{P}^{M+1,M} & 0 & \ldots & & \mathbf{P}^{M+1,M+1} \\
\vdots & & & & \vdots & & & \\
0 & \ldots & & 0 & 0 & \ldots & & \mathbf{P}^{NN}
\end{array}\right] , \quad (7)$$

where, for convenience, the dependences of the submatrices on X and Y have been omitted.

We see from Eqs. (5) and (7) that the ordering of states reduces the numerical complexity of the problem in a systematic manner. For example, the structure of submatrix $\mathbf{P}(X,Y)$ in Eq. (7) indicates that transitions from an operating state with I failed components to a failed state with L failed components is not possible if (a) $|I - L| > 1$, namely, if more than one component-state transitions must occur, and (b) $I = L + 1$, namely, if a failed component is repaired, since such a repair in an operating state cannot

bring the system into a failed state. Again, Eq. (7) indicates that only $5M + 3N + 1$ submatrices of the ordered **P** need be stored instead of the $(M+N+1)^2$ submatrices of the unordered **P**. Moreover, the ordering results in computing time savings because solving Eq. (2) is much faster when **P** is ordered than when it is not.

The generation and ordering of possible states of a system, the formation of the ordered **P** matrix, and the solution of Eq. (1) have been computerized.

II.B. Mergeable Markov Processes

Equations (3) and (4) show that reliability of a system can be calculated either if all $\pi_i(n)$'s or partial sums of $\pi_i(n)$'s are known. A partial sum of state probabilities is equal to the probability that the system will be in any of the individual states included in the partial sum.

If a new process can be formed such that its states—superstates—and transition probabilities are groups of the original states and depend only on the transition probabilities of the original process, respectively, then we say that the original process is mergeable, and calculate reliability in terms of the state probabilities of the merged process. Because the number of superstates is smaller than the number of states, the dimensions of the state probability vector and the transition probability matrix of a merged process are much smaller than those of the original process. Hence, reliability analysis of a merged process is easier than that of the original process.

A grouping of states into superstates corresponds to a Markov process if and only if the transition probabilities of the original process satisfy the mergeability criterion.[2,8,9,11-14] In general, creating all possible groupings of the states of a Markov process and testing for the satisfaction of the mergeability criterion are practically impossible. We have shown, however, that Markov processes describing systems exhibiting certain symmetries are mergeable. These symmetries are almost always encountered in the highly redundant safety systems of nuclear reactors and are defined as follows:

1. *Symmetries at the component level*: Two components of a system are symmetrical if and only if

   a. each component can be in the same number of states as the other

   b. each component has the same conditional failure rates and conditional repair rates as the other

   c. for any operating (failed) system state, interchanging only the states of the two components results in an operating (failed) system state.

2. *Symmetries at the subsystem level*: Any partial collection of components of a system forms a subsystem. A subsystem state is defined whenever the states of the components that belong to the subsystem are defined. Two subsystems are symmetrical if and only if

   a. there is a one-to-one correspondence between the components of the two subsystems such that two corresponding components can be in the same number of states and have the same failure and repair rates

   b. for any operating (failed) system state, interchanging only the states of the corresponding components of the two subsystems results in an operating (failed) system state.

A Markov process of a system exhibiting any of the symmetries just cited is proved to be mergeable in Refs. 2 and 12.

For systems with symmetries, the generation of the superstates of the merged process and its transition probability matrix have been computerized. For large systems, the reductions in the dimensions of **P** and in the number of elements that need be stored, resulting from ordering and merging, are of decisive practical importance. This assertion is confirmed by the numerical results listed in Table I.

II.C. Choice of the Time Step

If Δt is the size of the time step, and T the time horizon of the problem, then the number of time steps—the number of times the multiplication in the right side of Eq. (1) must be repeated—is $T/\Delta t$. The choice of the appropriate time step is of particular importance for the Monte Carlo simulation (see Sec. III.A). A detailed discussion of this assertion is given in the Appendix and in Ref. 2.

III. MARKOVIAN RELIABILITY ANALYSIS UNDER UNCERTAINTY

The reliability of a nuclear reactor system is uncertain because both the failure and repair rates of components and other quantities that characterize the behavior of the system are uncertain. To quantify these uncertainties, we assume that transition rates and probabilities are random variables distributed according to given probability density functions

[12] I. A. PAPAZOGLOU and E. P. GYFTOPOULOS, "Automated Merging of Markov Processes of Large Reactor Systems," *Proc. Topl. Mtg. Probabilistic Analysis of Nuclear Reactor Safety*, Los Angeles, California, May 8-11, 1978, IJBN 89448-1011, 3, VIII.3-1, American Nuclear Society (1978).

[13] G. C. BACON, *Inf. Control*, 7, 320 (1964).

[14] J. G. KEMENY and J. L. SNELL, *Finite Markov Chains*, D. Van Nostrand Company, New York (1960).

TABLE I

Savings in Computer Storage Requirements Resulting from Ordering and Merging of States of the Shutdown Subsystems of the CRBR

Subsystem	Markov Process	Number			Storage Savings Factor	
		States	Elements of Matrix P	Elements Needing Storage	Ordering	Overall
Mechanical	Original Merged	4096 105	16 777 216 11 025	2 499 240 1 227	7 9	10^4
Primary output logic	Original Merged	256 20	65 536 400	11 248 285	6 2	10^2
Electrical systems	Original Merged	1728 113	2 985 984 12 769	582 339 2 314	5 6	10^3

(pdf's). Hence, reliability will also be a random variable. The problem then is "given the pdf's of the input data, find the pdf of reliability." For Markovian systems, this problem is equivalent to "given the pdf's of the transition probabilities of the process, find the pdf of the state probability vector $\boldsymbol{\pi}(n)$."

For large systems, we show that it is not possible to find an explicit analytical solution for the pdf of $\boldsymbol{\pi}(n)$. For $\mathbf{P}$ independent of n, from Eq. (1) we see that the state probability vector $\pi(n)$ at time n is given by the relation

$$\boldsymbol{\pi}(n) = \boldsymbol{\pi}(0) \cdot \mathbf{P}^n \tag{8a}$$

or

$$\pi_i(n) = \sum_{j=1}^{z} \pi_j(0) p_{ji}^{(n)} \quad , \tag{8b}$$

where $p_{ij}^{(n)}$ denotes the ij element of the n'th power $\mathbf{P}^n$ of random matrix $\mathbf{P}$, and $\boldsymbol{\pi}(0)$ is the initial value of the state probability random vector.[15] Given $\boldsymbol{\pi}(0)$ and the pdf's of z^2 random variables p_{ij}, we would find the pdf of $\boldsymbol{\pi}(n)$ if we could calculate the pdf's of the z^2 random variables $p_{ij}^{(n)}$. Equivalently, given $\boldsymbol{\pi}(0)$ and the pdf $g(\mathbf{P})$ of the $z \times z$ random matrix $\mathbf{P}$, we would find the pdf of $\boldsymbol{\pi}(n)$ if we could calculate the pdf $h(\mathbf{P}^n)$ of the $z \times z$ random matrix $\mathbf{P}^n$.

Because the $p_{ij}^{(n)}$'s are functions of the p_{ij}'s, it can be shown that

$$h(\mathbf{P}^n) = \overline{g(\mathbf{P})} \cdot |J| \quad ,$$

where $\overline{g(\mathbf{P})}$ denotes the pdf g expressed in terms of the elements of $\mathbf{P}^n$, i.e., the elements p_{ij} in $g(\mathbf{P})$ are replaced by their expressions in terms of the $p_{ij}^{(n)}$'s, and $|J|$ is the Jacobian of the transformation from the $p_{ij}^{(n)}$'s to the p_{ij}'s. But expressing the p_{ij}'s in terms of the $p_{ij}^{(n)}$'s is a very difficult task. To the best of our knowledge, the difficulty can be overcome only when (a) the dimensionality of $\mathbf{P}$ is small (e.g., $z = 2$), and (b) the structure of $\mathbf{P}$ is very simple (e.g., diagonal, tridiagonal).

To avoid this difficulty, we have used the moment matching technique.[16-18] Here, this technique consists in calculating the first four moments of reliability and in approximating its pdf by a two-parameter distribution that has the same four moments. The first two moments determine the parameters of the distribution and the other two the shape (skewness and kurtosis). We calculate moments of reliability by using either a Monte Carlo simulation or a Taylor series expansion.

III.A. Monte Carlo Simulation

For m input variables, the Monte Carlo simulation consists in randomly generating a sample of N m-tuples $\{x_{ij}\}$ for $i = 1, 2, \ldots, m$, and $j = 1, 2, \ldots, N$, where x_{ij} denotes the j'th random value of the i'th input variable, and in solving the Markov model N times—once for each m-tuple $\{x_{ij}\}$. The resulting random sample of N values of reliability is then used to estimate the values of the required moments. It is noteworthy that we use the Monte Carlo simulation to generate a random sample of N reliability values and not a specific value of reliability. Hence, the sample size need not be large. From the experience gained during our research, we feel that $\sim 10^3$ trials

[15] By definition, the elements of a random vector (matrix) are random variables. The pdf of an $l \times z$ random vector ($z \times z$ random matrix) is the joint pdf of the $z(z^2)$ elements of the vector (matrix).

[16] H. L. ROYDEN, *Ann. Math. Stat.*, **24**, 361 (1953).

[17] G. J. HAHN and S. S. SHAPIRO, *Statistical Models in Engineering*, John Wiley and Sons, Inc., New York (1967).

[18] G. E. APOSTOLAKIS and Y. T. LEE, *Nucl. Eng. Des.*, **41**, 411 (1977).

are adequate for most practical problems. A systematic procedure for determining the size of the time step for each trial as well as an approximation that allows the use of large time steps is discussed in Ref. 2.

III.B. Taylor Series Expansion

The Taylor series expansion[17-23] consists in representing a reliability function by a truncated Taylor series around the means of the independent variables and using the series for the direct calculation of the moments. For Markovian systems, we calculate the expansion coefficients of the Taylor series as follows.

Reliability is a function of the transition rates of the components of the system. If the number of transition rates in m, and x_i, for $i = 1, 2, \ldots, m$, denotes the i'th rate, then reliability R of the system at time n is given by a function of the form

$$R = R(x_1, x_2, \ldots, x_m) \text{ at time } n \ . \tag{9}$$

For complicated systems, a closed form for R is not available. But we can obtain an approximate closed form at each time n by representing R by a truncated Taylor series around the expectation values, $\bar{x}_i$'s, of x_i's. Truncating after terms of fourth order, we find

$$\begin{aligned} R(x_1, \ldots, x_m) = R(\bar{x}_1, \ldots, \bar{x}_m) &+ \sum_i \frac{\partial R}{\partial x_i}(x_i - \bar{x}_i) + \frac{1}{2!}\sum_i \sum_j \frac{\partial^2 R}{\partial x_i \partial x_j}(x_i - \bar{x}_i)(x_j - \bar{x}_j) \\ &+ \frac{1}{3!}\sum_i \sum_j \sum_k \frac{\partial^3 R}{\partial x_i \partial x_j \partial x_k}(x_i - \bar{x}_i)(x_j - \bar{x}_j)(x_k - \bar{x}_k) \\ &+ \frac{1}{4!}\sum_i \sum_j \sum_k \sum_r \frac{\partial^4 R}{\partial x_i \partial x_j \partial x_k \partial x_r}(x_i - \bar{x}_i)(x_j - \bar{x}_j)(x_k - \bar{x}_k)(x_r - \bar{x}_r) \ , \end{aligned} \tag{10}$$

where the partial derivatives are evaluated at the point $(\bar{x}_1, \ldots, \bar{x}_m)$, and all summations extend from 1 to m.

Equation (10) can be used to determine any moment of R about the origin or about the mean. If $E(R)$ denotes the mean value of R, and $\mu_k(R)$ and μ_k^i the k'th central moment of R and x_i, respectively, then it can be shown that

$$E(R) = R(\bar{x}_1, \ldots, \bar{x}_m) + \frac{1}{2}\sum_{i=1}^{m} \frac{\partial^2 R}{\partial x_i^2}\mu_2^i + \frac{1}{6}\sum_{i=1}^{m} \frac{\partial^3 R}{\partial x_i^3}\mu_3^i + \frac{1}{24}\sum_{i=1}^{m} \frac{\partial^4 R}{\partial x_i^4}\mu_4^i + \frac{1}{24}\sum_{i=1}^{m-1}\sum_{j=i+1}^{m} \frac{\partial^4 R}{\partial x_i^2 \partial x_j^2}(\mu_2^i)(\mu_2^j) \ , \tag{11}$$

$$\mu_2(R) = \sum_{i=1}^{m}\left(\frac{\partial R}{\partial x_i}\right)^2 \mu_2^i + \sum_{i=1}^{m} \frac{\partial R}{\partial x_i}\cdot\frac{\partial^2 R}{\partial x_i^2}\mu_3^i + \frac{1}{3}\sum_{i=1}^{m} \frac{\partial R}{\partial x_i}\cdot\frac{\partial^3 R}{\partial x_i^3}\mu_4^i + \frac{1}{4}\sum_{i=1}^{m}\left(\frac{\partial^2 R}{\partial x_i^2}\right)^2 [\mu_4^i - (\mu_2^i)^2] \ , \tag{12}$$

$$\mu_3(R) = \sum_{i=1}^{m}\left(\frac{\partial R}{\partial x_i}\right)^3 \mu_3^i + \frac{3}{2}\sum_{i=1}^{m}\left(\frac{\partial R}{\partial x_i}\right)^2 \cdot \frac{\partial^2 R}{\partial x_i^2}[\mu_4^i - (\mu_2^i)^2] \ , \tag{13}$$

$$\mu_4(R) = \sum_{i=1}^{m}\left(\frac{\partial R}{\partial x_i}\right)^4 [\mu_4^i - 3(\mu_2^i)^2] + 3[\mu_2(R)]^2 \ , \tag{14}$$

where we have assumed that x_i's are uncorrelated and, therefore, that averages of products of order $(x_i - \bar{x}_i)(x_j - \bar{x}_j)$ and higher vanish. These results are also presented in Refs. 19, 20, 21, and 23, while results for correlated x_i's are presented in Refs. 19, 20, 21, and, including up to second-order terms, in Ref. 17. By virtue of Eqs. (11) through (14), we see that the problem of estimating the first four moments of reliability reduces to that of calculating derivatives of R.

The derivatives of R can be evaluated with the help of a set of recurrence formulas. By virtue of Eqs. (3), (4), and (8), at time n we have

[19] J. W. TUKEY, "Propagation of Errors, Fluctuations and Tolerances, No. 1: Basic Generalized Formulas," Technical Report No. 10, Statistical Techniques Research Group, Princeton University, Princeton, New Jersey (1957).

[20] J. W. TUKEY, "Propagation of Errors, Fluctuations and Tolerances, No. 2: Supplementary Formulas," Technical Report No. 11, Statistical Techniques Research Group, Princeton University, Princeton, New Jersey (1957).

[21] J. W. TUKEY, "Propagation of Errors, Fluctuations and Tolerances, No. 3: Exercise in Differentiation," Technical Report No. 12, Statistical Techniques Research Group, Princeton University, Princeton, New Jersey (1957).

[22] N. D. COX and J. O. CERMAC, *Energy Sources*, 1, 339 (1974).

[23] D. H. EVANS, *J. Quality Technol.*, 7, 1 (1975).

$$\frac{\partial^k R}{\partial x_i^k} = \sum_{i\epsilon X} \sum_{j=1} \pi_j(0) \frac{\partial^k p_{ji}^{(n)}}{\partial x_i^k}$$

$$= \sum_{i\epsilon X} \bar{\boldsymbol{\pi}}(0) \cdot \mathbf{D}_{k;i}^{(n)}$$

$$= \sum_{i\epsilon X} \boldsymbol{d}_{k;i}^{(n)} \quad , \tag{15}$$

where matrix $\mathbf{D}_{k;i}^{(n)}$ and vector $\boldsymbol{d}_{k;i}^{(n)}$ are defined by the identities

$$\mathbf{D}_{k;i}^{(n)} \equiv \frac{\partial^k \mathbf{P}^n}{\partial x_i^k} \qquad \text{and} \qquad \boldsymbol{d}_{k;i}^{(n)} \equiv \frac{\partial^k \bar{\boldsymbol{\pi}}(n)}{\partial x_i^k} \tag{16}$$

and $\bar{\boldsymbol{\pi}}(0)$ is assumed constant—not a function of the x_i's. Moreover, writing the n'th power $\mathbf{P}^n$ of matrix $\mathbf{P}$ in the form $\mathbf{P}^{n-1} \cdot \mathbf{P}$, we find

$$\frac{\partial \mathbf{P}}{\partial x_i} = \frac{\partial \mathbf{P}^{n-1}}{\partial x_i} \cdot \mathbf{P} + \mathbf{P}^{n-1} \cdot \frac{\partial \mathbf{P}}{\partial x_i} \quad , \tag{17a}$$

or, equivalently,

$$\mathbf{D}_{1;i}^{(n)} = \mathbf{D}_{1;i}^{(n-1)} \cdot \mathbf{D}_{0;i}^{(1)} + \mathbf{D}_{0;i}^{(n-1)} \cdot \mathbf{D}_{1;i}^{(1)} \quad . \tag{17b}$$

Differentiating Eq. (17) repeatedly and premultiplying each result by $\bar{\boldsymbol{\pi}}(0)$, we obtain, respectively,

$$\mathbf{D}_{k;i}^{(n)} = \sum_{\nu=0}^{k} \binom{k}{\nu} \mathbf{D}_{k-\nu;i}^{(n-1)} \cdot \mathbf{D}_{\nu;i}^{(1)} \tag{18}$$

and

$$\boldsymbol{d}_{k;i}^{(n)} = \sum_{\nu=0} \binom{k}{\nu} \boldsymbol{d}_{k-\nu;i}^{(n-1)} \cdot \mathbf{D}_{\nu;i}^{(1)} \quad . \tag{19}$$

But the elements of $\mathbf{P}$ are linear functions of the x_i's and, therefore,

$$\mathbf{D}_{\nu;i}^{(1)} = \begin{cases} \mathbf{P} & \text{for} \quad \nu = 0 \\ \dfrac{\partial \mathbf{P}}{\partial x_i} & \text{for} \quad \nu = 1 \\ \mathbf{0} & \text{for} \quad \nu \geqslant 2 \end{cases} , \tag{20}$$

$$\boldsymbol{d}_{\nu;i}^{(1)} = \bar{\boldsymbol{\pi}}(0) \cdot \mathbf{D}_{\nu;i}^{(1)} = \begin{cases} \bar{\boldsymbol{\pi}}(1) & \text{for} \quad \nu = 0 \\ \bar{\boldsymbol{\pi}}(0) \cdot \dfrac{\partial \mathbf{P}}{\partial x_i} & \text{for} \quad \nu = 1 \\ \mathbf{0} & \text{for} \quad \nu \geqslant 2 \end{cases} . \tag{21}$$

By virtue of Eqs. (19), (20), and (21), it follows that

$$\boldsymbol{d}_{1;i}^{(n)} = \boldsymbol{d}_{1;i}^{(n-1)} \cdot \mathbf{P} + \bar{\boldsymbol{\pi}}(n-1) \cdot \mathbf{D}_{1;i}^{(1)} \quad , \tag{22a}$$

$$\boldsymbol{d}_{2;i}^{(n)} = \boldsymbol{d}_{2;i}^{(n-1)} \cdot \mathbf{P} + 2\boldsymbol{d}_{1;i}^{(n-1)} \cdot \mathbf{D}_{1;i}^{(1)} \quad , \tag{22b}$$

$$\boldsymbol{d}_{3;i}^{(n)} = \boldsymbol{d}_{3;i}^{(n-1)} \cdot \mathbf{P} + 3\boldsymbol{d}_{2;i}^{(n-1)} \cdot \mathbf{D}_{1;i}^{(1)} \quad , \tag{22c}$$

$$\boldsymbol{d}_{4;i}^{(n)} = \boldsymbol{d}_{4;i}^{(n-1)} \cdot \mathbf{P} + 4\boldsymbol{d}_{3;i}^{(n-1)} \cdot \mathbf{D}_{1;i}^{(1)} \quad . \tag{22d}$$

We see that Eqs. (21) and (22) provide the recurrence formulas for the calculation of the derivatives of R—last relation of Eq. (15)—and, therefore, the moments specified by Eqs. (11) through (14).

It can be readily verified that the method just cited can be used also for the calculation of the moments of any function of R.

The entire procedure for the calculation of derivatives of the state vector $\boldsymbol{d}_{\nu;i}^{(n)}$ and moments of R has been computerized.

The smaller the deviations of the independent variables from the point around which a function is expanded, the more accurate the Taylor series representation of that function. Therefore, the smaller the probability that the x_i's will simultaneously take values "far" from their respective means, the more accurate the estimation of the moments. The Taylor series method provides also a tool for performing sensitivity analyses. Indeed, once the accuracy of the method has been checked at a certain level of the mean values of the x_i's (perhaps with a Monte Carlo calculation), the higher moments of the x_i's can be varied, and the changes in the reliability moments can be calculated.

IV. ASSESSMENT OF THE CRBR SHUTDOWN SYSTEM RELIABILITY UNDER UNCERTAINTY

To illustrate the methodology developed in Secs. II and III, we assess the uncertainties about the failure probability of the design of the shutdown system of the CRBR described in Refs. 24 and 25.

IV.A. System Description

The reactor shutdown system (RSS) of the CRBR consists of two independent systems: the primary and the secondary. Each shutdown system is designed to independently terminate the effects of the anticipated and unlikely fault events, without exceeding specified core damage limits.

A simplified logic block diagram illustrating the interconnections of the various subsystems is shown in Fig. 1. The primary shutdown system (PSS) can be divided into three subsystems:

1. the primary protective function (PPF)
2. the primary output logic (POL)
3. the primary mechanical subsystem (PMS).

The secondary shutdown system (SSS) can be divided into two subsystems:

[24]"Reliability Assessment of CRBR Reactor Shutdown System," WARD-D-0118, Westinghouse Electric Corporation (1975).

[25]Preliminary Safety Analysis Report, Clinch River Breeder Reactor Project.

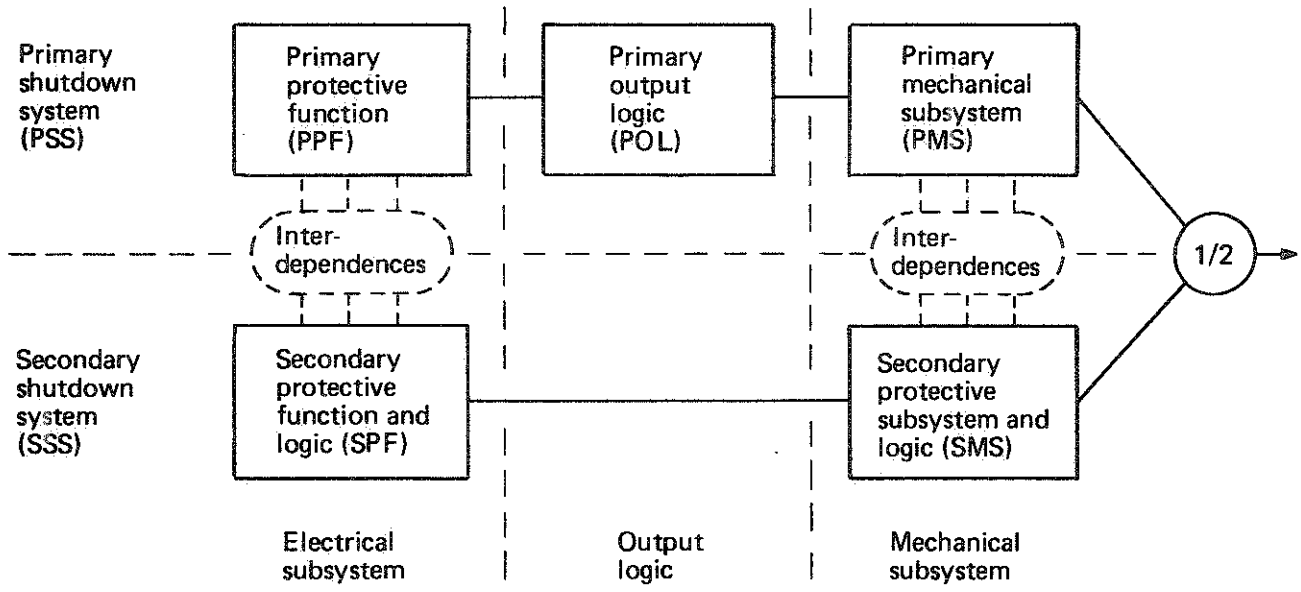

Fig. 1. Simplified logic block diagram of the CRBR shutdown system.

1. the secondary protective function (SPF), containing part of the secondary logic
2. the secondary mechanical subsystem (SMS), containing the rest of the secondary output logic.

If a transient occurs, either protective function can sense it and can signal the corresponding mechanical subsystem to insert the necessary negative reactivity to control the transient. Successful operation of either the PSS or the SSS guarantees successful operation of the RSS.

A detailed description of the RSS is given in Refs. 24 and 25. A brief description of the subsystems follows.

The electrical design of the primary shutdown system has the potential to include up to 24 protective functions arranged in a local coincidence logic configuration. Each protective function consists of three redundant channels, each of which feeds into three redundant logic trains, as shown in Fig. 2. A typical protective function channel is made up of sensors, signal conditioning, a calculation unit, and a comparator. Whenever it senses the need for a shutdown, a protective function channel changes from a reset to a trip state. If more than one of the three channels is in a trip state, a trip signal is applied to each of the three logic trains. When more than one of the three logic trains provides trip signals to its respective scram breaker, the proper combination of scram breakers opens, causing all power to the 15 primary control rods to be removed and, thus, activating the unlatching mechanisms. If a failure is detected in a channel, the operator manually trips the channel. Then, the usual two-out-of-three logic configurations of the protective function channels will have one tripped input (reconfigured to an effective one-out-of-two logic configuration) until repair of the failed channel is completed and the channel is returned to service.

The electrical design of the secondary shutdown system has the potential to include up to 16 protective functions arranged in a general coincidence logic configuration. Each protective function consists of three redundant channels, each channel separately feeding a logic train, as shown in Fig. 2. Thus, there is separation between redundant protective function channels throughout the secondary electrical subsystems. A typical SPF channel is similar to the PPF channel. The coupling between the protective function network and the logic train is, however, optical in the primary and magnetic in the secondary. Whenever more than one of the three logic trains propagates a trip signal to the four two-out-of-three valve configurations, the rods are unlatched and fall to their shutdown position. The manual tripping of the SPF channels is completely analogous to that of the primary channels.

The PMS consists of 15 primary control rod systems, and provides a startup, reactivity (power) control, burnup compensation, and primary shutdown capabilities for the reactor. The SMS consists of four secondary control rod systems, and provides secondary (redundant) shutdown capabilities for the reactor.

IV.B. System Mission and Model

The mission of and the model for the reactor shutdown system are as follows:

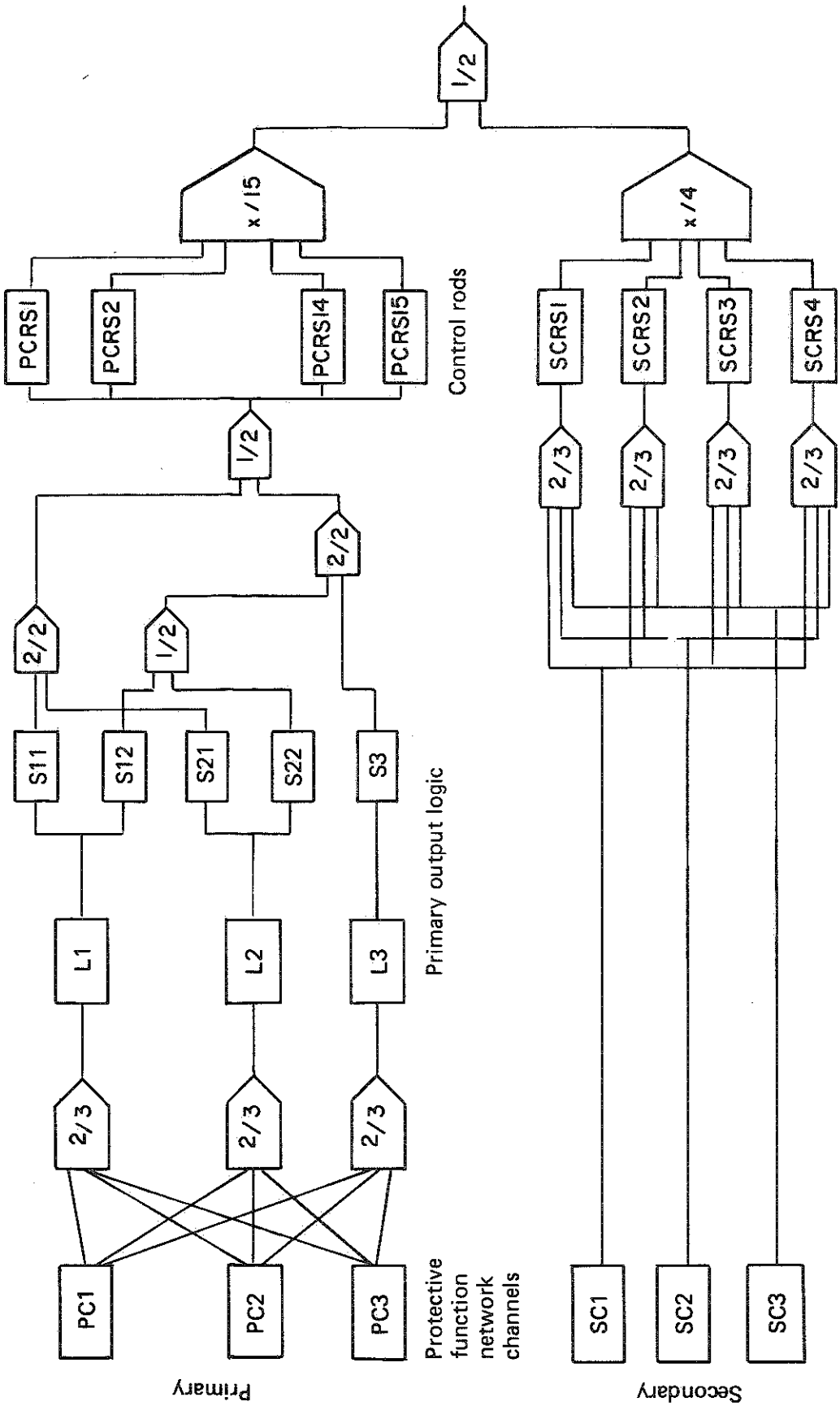

Fig. 2. Logic block of the CRBR shutdown system. The success combination for the control rods depends on the transient and the particular rods available.

1. During operation, the mission of the shutdown system is to successfully respond to the following three types of transients.[24]

a. *Reactivity transients* that result in an overpower condition (power/flow > 1.0). To control them, the RSS must insert negative reactivity sufficiently fast to prevent hot-channel sodium boiling (1700°F). Sufficient margin is provided to ensure an in-vessel bulk sodium outlet temperature below 1250°F. A total of 5 dollars of negative reactivity is required.

b. *Major flow transients* (reduction in coolant flow) that may damage the core. To control them, the RSS should perform as for reactivity transients except that no compensation is required for reactivity changes associated with the initiating event. A total of 2.5 dollars of negative reactivity is required.

c. *Limited response transients* that do not require a rapid response from the shutdown system. A grace period of 10 min is available before the insertion of 2.5 dollars of negative reactivity becomes necessary to avoid core damage.

2. Transients occur randomly and arrive according to a Poisson random process.

3. If a transient occurs, the system can either respond successfully or fail.

4. Electrical response is required only for reactivity and major flow transients. For limited response transients, we assume that the plant operator will initiate a manual scram with probability equal to unity.

5. If the RSS responds successfully to a transient, the system is renewed instantly.

6. While the reactor is shut down, no transients occur and therefore no failures.

7. All component failures are random, and the times-to-failure are exponentially distributed. We assume that the failure rates may depend on the states of other components. Specifically,

a. The failure rates of a component of the PPF or SPF depend on the states of other components in these two subsystems.

b. The failure rates of a component of the primary output logic depend on the states of other components in this subsystem.

c. The failure rates of a component of the secondary output logic depend on the states of other components in this subsystem.

d. The failure rates of a component of the PMS or of the SMS depend on the states of other components in these two subsystems.

These assumptions enable us to consider common-cause failures in the electrical subsystems, the output logic, and the mechanical subsystems.

8. For a given transient, the protective function that monitors the dynamic plant parameters affected by the transient constitutes the protective function network for each electrical subsystem.

9. For both electrical and mechanical systems, we assume worst-case configurations. This means that the PPF (SPF) network is taken always to be the one out of the 24 (16) that includes the components with the highest failure rates, and that the mechanical subsystem is always at its beginning-of-equilibrium cycle configuration.

10. The primary protective function network (PPFN) consists of three components, i.e., the three channels connected in a two-out-of-three logic. Each channel of the PPFN can be in three states: operating, trip, and failed undetected state U. Here, we assume that the detection of a detectable failure, and the subsequent tripping of a channel, is instantaneous. This assumption is valid because the mean time to detect a failure and trip a channel is much smaller than the mean-time-to-detectable failure.

11. The secondary electrical subsystem (SES) consists of three components, the three secondary channels connected in a two-out-of-three logic. Each channel of the SES can be in four states: operating, trip, failed undetected state U (containing failures of the protective function part of the channel), and failed undetected state $U1$ (containing failure of the secondary logic).

Detection of detectable failures and tripping is instantaneous.

12. Interdependences among the components of the two electrical subsystems are described by the following relations:

a. If λ_{Ti}^{*} denotes the transition rate from the operating state of a channel to the trip state, and i the number of tripped channels in both subsystems, then

$$\lambda_{Ti}^{*} = k_{Ti}\lambda_T$$

for $i = 1, 2$ and $k_{T0} = 1$.

Each k is called a dependence coefficient.

b. If λ_{Ui}^{*} denotes the transition rate from the operating state of a channel to the failed state U, and i the number of failed channels in both subsystems, then

$\lambda^*_{Ui} = k_{Ui} \cdot \lambda_U$

for $i = 0, 1, 2, 3, 4, 5$ and $k_{U0} = 1$.

c. If λ^*_{U1i} denotes the transition rate from the operating state of a channel of the SES to the failed state $U1$, and i the number of failed secondary logic trains, then

$\lambda^*_{U1i} = k_{U1i}\lambda_{U1}$

for $i = 0, 1, 2$ and $k_{U10} = 1$.

13. The logic trains and scram breakers of the primary output logic can be in two states: operating and failed. Their interdependences are as follows:

a. If λ^*_{Li} denotes the failure rate of the logic trains when i have already failed, then

$\lambda^*_{Li} = k_{Li}\lambda_L$

for $i = 0, 1, 2$, and $k_{L0} = 1$.

b. If λ^*_{Bi} denotes the failure rate of the scram breakers when i have already failed, then

$\lambda^*_{Bi} = k_{Bi}\lambda_B$

for $i = 0, 1, 2, 3, 4$ and $k_{B0} = 1$.

14. In its worst-case configuration, the PMS consists of eight fully withdrawn rods[24]: two row 4 startup rods each worth 2 dollars, and six row 7 corner rods each worth 1 dollar.

15. In its worst-case configuration, the SMS consists[24] of the four row 4 safety rods, each worth 2.5 dollars.

16. Each control rod constitutes a component that can be in two states: operating (in which the rod can insert its reactivity into the core on time) and failed (in which the rod cannot insert its reactivity).

17. The times-to-failure for the control rods are exponentially distributed, and have the following interdependences. If λ^*_{Ci} denotes the failure rate of the rods when i have already failed, then

$\lambda^*_{Ci} = k_{Ci}\lambda_C$ for $i = 0, 1, 2, \ldots, 11$ and $k_{C0} = 1$.

In models 12, 13, and 17, each dependence coefficient k_{pq} is a random variable taking values in the interval $[1, \infty)$ and being statistically independent of the corresponding λ_p. Thus, we guarantee that each interdependence results in a rate larger than that in the absence of the interdependence ($\lambda^* > \lambda$), and reduce the numerical complexity of the problem.[2]

18. Inspection of the electrical subsystems at predetermined intervals is possible and has the following features:

a. The inspection is instantaneous. This is a conservative assumption. A channel under inspection is put into a tripped state until the inspection is completed. This results into a one-out-of-two reconfiguration of the two-out-of-three logic. Thus, even though a reactor shutdown might result from the tripping or a spurious signaling of one of the two remaining channels, an unsafe failure of the system because of the "unavailability" of the channel under inspection cannot happen.

b. The testing of components belonging to the same subsystem is simultaneous. Testing of different subsystems is, however, staggered, i.e., done at different times.

c. The inspection is not perfect. An inspection error is defined to be a failure that has not been detected or a failure that has been caused by the inspection.

d. The failure rates of the components are not affected by the inspection.

e. An inspection of a protective function network (PFN) with one channel in a tripped state means a reactor shutdown. For this reason, we consider two policies:

Policy 1. If at the time of inspection of a PFN one of its channels is in a tripped state, the reactor is shut down.

Policy 2. If at the time of inspection of a PFN one of its channels is in a tripped state, the inspection is not performed unless the other PFN has also a trippped channel.

In general, policy 1 results in a lower failure probability for the RSS but in a higher reactor unavailability than policy 2. In choosing between policies 1 and 2, we need to establish a value trade-off between failure probability and reactor unavailability.

19. The time horizon of the problem is 48 weeks. For the remaining four weeks of a year, the reactor is assumed to be shut down for refueling and maintenance. During the refueling period, a complete overhaul of the shutdown system takes place, and at the beginning of the following year, the RSS is assumed to be completely renewed.

20. Failed system states are absorbing, i.e., the system cannot recover from a failure. The set of all possible system states can be divided into the following six subsets:

a. Subset AR—containing all the system states in which the reactor is on-line (a transient can occur), and the RSS is able to respond to any type of transient.

b. Subset AMF—containing all the system states in which the reactor is on-line, and the RSS is able to respond only to major flow and limited response transients.

c. Subset ALR—containing all the system states in which the reactor is on-line and the RSS is able to respond only to limited response transients.

d. Subset AF—containing all the system states in which the reactor is on-line but the RSS is not able to respond to any transient.

e. Subset S—containing all the system states in which the reactor is shut down. No transients can occur if the system is in a state of S.

f. Subset F—containing all the failed states.

The six subsets of states along with the possible transients are shown in Fig. 3. The system has failed if it enters subset F. Its transitions from state to state are random, and its probabilistic behavior is simulated by a Markov process.

IV.C. Data Base

For the quantitative evaluation of the RSS failure probability, F, we have used the following data. The failure rates, transient arrival rates, and repair rate are random variables, each having a range $[0,\infty]$ and distributed according to a gamma pdf (Refs. 2 and 17). The dependence coefficients are random variables, each having a range $[1,\infty]$ and distributed according to a gamma pdf. The probability of detecting a protective function channel failure as well as the probabilities of inspection errors are random variables, each having a range $[0,1]$ and distributed according to a beta pdf (Refs. 2 and 17). Each pdf is determined by two parameters.

One "objective set" of data is given in Ref. 24. It consists of "failure rates and failure probabilities which are evaluated using expected test conditions and analyses to produce an objective reliability which will be demonstrated by a combination of tests and analyses." Here, we assume that these "objective values" are the most probable values of the corresponding random variables. Thus, we can determine one of the two parameters of each pdf. To determine the second parameter, we assume that the 0.95 percentile is one order of magnitude higher than the 0.05 percentile which, in turn, is of the same order of magnitude as the most probable value.

For the failure rates, the numerical values of the parameters of the pdf's and the 0.05 and 0.95 percentiles are listed in Table II. For the dependence coefficients, the parameters of the pdf's and the 0.05 and 0.95 percentiles are listed in Table III. Here, the parameters are assessed subjectively. The effects of the dependence coefficients on the pdf's of some transition rates are shown in Fig. 4.

The most probable value of the reactor repair rate is assumed to be 10^{-3} h^{-1}. This corresponds to a conditional mean time-to-repair of 1000 h. The times-to-repair are assumed to be of that order of magnitude

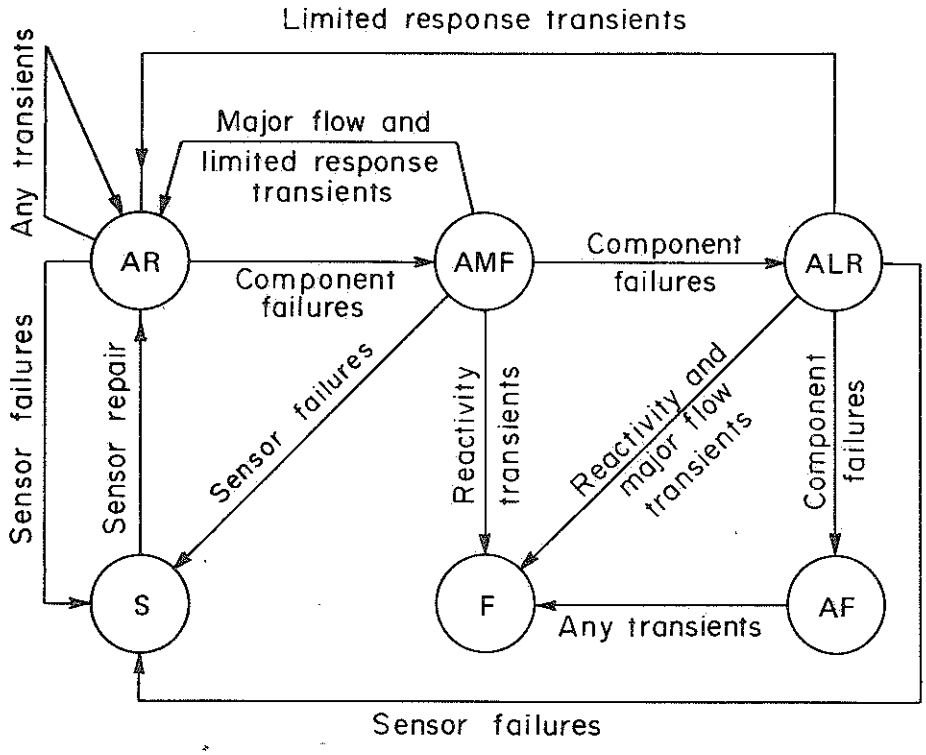

Fig. 3. State flow chart for the CRBR shutdown system.

TABLE II

Values of Parameters of pdf's and Other Characteristics of Failure Rates of Components of Primary and Secondary Protective Function Networks of Shutdown System of CRBR*

Component	Parameter		Value (10^{-6} h^{-1})			
	r	y	Most Probable	Mean	0.05 Percentile	0.95 Percentile
Primary flux sensor	2	20 000	5.0	10.0	1.8	23.6
Primary pressure sensor	2	50 000	2.0	4.0	0.7	9.5
Primary flux electronics	2	5 000	20.0	40.0	7.0	94.5
Primary pressure electronics	2	12 500	8.0	16.0	2.8	37.8
Primary calculation unit	2	34 483	2.9	5.8	1.0	13.7
Primary comparator	2	34 483	2.9	5.8	1.0	13.7
Secondary flux sensor	2	20 000	5.0	10.0	1.8	23.6
Secondary flow sensor	2	50 000	2.0	4.0	0.7	9.5
Secondary flux electronics	2	5 000	20.0	40.0	7.0	94.5
Secondary flow electronics	2	12 500	8.0	16.0	2.8	37.8
Secondary calculation unit	2	34 483	2.9	5.8	1.0	13.7
Secondary comparator	2	24 390	4.1	8.2	1.4	19.4
Secondary logic train	2	25 000	4.0	8.0	1.4	19.9
Primary logic train L1	2	35 714	2.8	5.6	0.98	13.23
Primary logic train L2 or L3	2	35 714	2.8	5.6	0.98	13.23
Primary breaker S1	2	80 000	1.25	2.5	0.44	5.90
Primary breaker S22 or S32	2	80 000	1.25	2.5	0.44	5.90
Primary breaker S21, S31	2	80 000	1.25	2.5	0.44	5.90
Control rod	2	100 000	1.00	2.0	0.35	4.72

*Gamma pdf $= \dfrac{\exp(-yx)(yx)^{r-1}}{\Gamma(r)}\, y$; $\Gamma(r) = \int_0^\infty x^{r-1}\exp(-x)dx$.

TABLE III

Values of Parameters of pdf's and Other Characteristics of Dependence Coefficients of the Shutdown System of the CRBR*

Subsystem	Parameter		Value			
	r	y	Most Probable	Mean	0.05 Percentile	0.95 Percentile
Electrical subsystem						
One channel down	2	0.20	6.00	11.00	2.75	24.62
Two channels down	2	0.10	11.00	21.00	4.50	48.23
Three or more channels down	2	21.00	41.00	81.00	8.00	95.46
Primary logic						
One or more trains or breaker down	2	0.20	6.00	11.00	2.75	24.62
One control rod down	2	0.50	3.00	5.00	1.70	10.46
Two control rods down	2	0.25	5.00	9.00	2.40	19.89
Three control rods down	2	0.17	7.00	13.00	3.10	29.34
Four control rods down	2	0.13	9.00	17.00	3.80	38.78
Five control rods down	2	0.10	11.00	21.00	4.50	48.23
Six or more control rods down	2	0.05	21.00	41.00	8.00	95.46

*Gamma pdf $= \dfrac{\exp[-y(x-1)][y(x-1)]^{r-1}}{\Gamma(r)}\, y$; $\Gamma(r) = \int_0^\infty x^{r-1}\exp(-x)dx$.

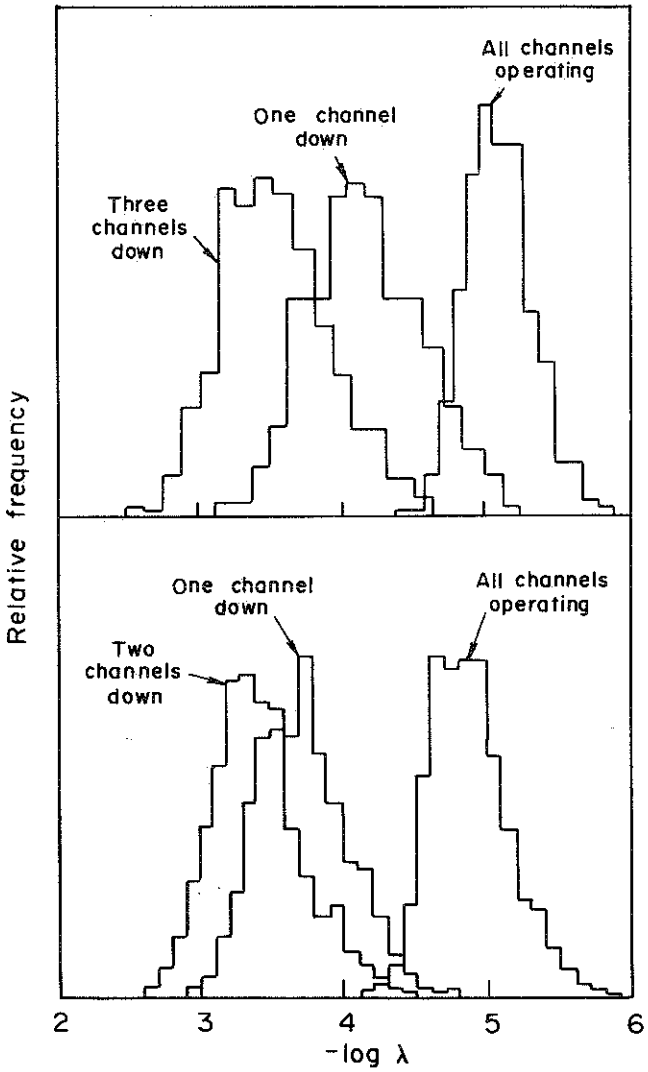

Fig. 4. Histograms of transition rates of components of the shutdown system: from the operating state to the failed state (top), and from the operating state to the trip state (bottom).

because each repair involves in-vessel components (sensors).

Objective values for the transient arrival rates are given in Ref. 24. They are such that the number of expected transients per year (arriving according to a Poisson random process) is less than that of the design duty cycle with a probability of 0.95. Here, we assume that these objective values are the most probable values of the corresponding random variables. Using our rules, we find the parameters of the pdf's and the 0.05 and 0.95 percentiles of the reactor repair rate and the transient arrival rates listed in Table IV. Finally, the parameters and percentiles for the probability of failure detection and the probabilities of inspection errors are listed in Table V.

In Ref. 24, the inspection of the electrical subsystem is considered as perfect. Here, we assume that human errors during an inspection are possible. The mean value of the probability of making an error in inspecting the first channel of a subsystem is set equal to 10^{-3}, the mean value of conditional probability of an error in the second channel given an error in the first is 3×10^{-1}, and the mean value of the conditional probability of a third error, given the first two is 7×10^{-1}. Using these mean values as point estimates of the corresponding probabilities, we find a joint probability of three errors of 2.1×10^{-4}. For an average of ten inspections per subsystem per year, and for a 30-yr plant life, the chance of having one triple error during the plant lifetime is approximately one in ten ($\simeq 2.1 \times 10^{-4} \times 2 \times 10 \times 30$). In the *Reactor Safety Study*[26] (Appendix III, "Human Reliability"), it has been assumed that the probability of a first error in inspecting the RSS of a light water reactor (LWR) is 10^{-2}, that of a second error, given the first, is 10^{-1}, and that of a third, given that two have occurred, is

[26]*Reactor Safety Study*, WASH-1400, U.S. Nuclear Regulatory Commission (1975).

TABLE IV

Values of Parameters and Other Characteristics of Reactor Repair Rate and Transient Arrival Rates of the Shutdown System of the CRBR*

Event	Parameter		Value (10^{-6} h^{-1})			
	r	y	Most Probable	Mean	0.05 Percentile	0.95 Percentile
Reactor repair	2	1 000	1000	2000	350.00	4723
Reactivity transient	2	10 752	93	186	32.55	439.24
Major flow transient	2	24 390	41	82	14.35	193.64
Limited response	2	804	1244	2488	435.40	5875.40

*Gamma pdf $= \dfrac{\exp(-yx)(yx)^{r-1}}{\Gamma(r)}\, y$; $\Gamma(r) = \int_0^\infty x^{r-1}\exp(-x)dx$.

TABLE V

Values of Parameters and Other Characteristics of Failure Detection Probability and Inspection Error Probabilities of the Shutdown System of the CRBR*

Probability	Parameter		Value			
	p	q	Most Probable	Mean	0.05 Percentile	0.95 Percentile
Failure detection	98	2	0.99	0.98	0.95	0.99
One inspection error	5	4995	8×10^{-4}	10^{-3}	3.7×10^{-4}	1.85×10^{-3}
Two inspection errors given one	3	7	0.25	0.30	0.09	0.55
Three inspection errors given two	5	2	0.80	0.70	0.42	0.94

*Beta pdf $= \frac{\Gamma(p+q)}{\Gamma(p)\Gamma(q)} x^{p-1}(1-x)^{q-1}$; $\Gamma(r) = \int_0^\infty x^{r-1}\exp(-x)dx$.

unity. Because inspections of the primary and secondary subsystems of CRBR take place at different times, each inspection may be compared with the inspection of the shutdown system of an LWR (LWRs have only one shutdown system). The CRBR is, however, an experimental demonstration plant. For this reason, we have assumed values for the inspection probabilities different from those in a typical LWR (Ref. 27).

IV.D. Results

We calculated the pdf of the failure probability, F, by the moment matching technique. We found the moments of the failure probability by both Monte Carlo and Taylor series methods (see Secs. III.A and III.B).

For the Monte Carlo calculation, we generated 37 random samples (one for each input variable) each containing 1200 values, and solved the Markov model 1200 times. Thus, we obtained a sample of 1200 values of the failure probability at each point in time. For each sample, we estimated the first four central moments, and from them the corresponding pdf by the moment matching method. We also estimated the first four central moments of the negative common logarithm of the failure probability with the Taylor series expansion method.

For both methods, the calculated values of the median, and 0.95 and 0.05 percentiles of the RSS failure probability at various times, are listed in Table VI and graphed in Fig. 5. At each point in time,

[27]G. E. APOSTOLAKIS and P. P. BANSAL, *IEEE Trans. Reliab.*, **26** (1977).

TABLE VI

Median and 0.05 and 0.95 Percentiles of the Failure Probability at Various Times for the Shutdown System of the CRBR

Time (week)	Median		0.05 Percentile		0.95 Percentile	
	Monte Carlo	Taylor Series	Monte Carlo	Taylor Series	Monte Carlo	Taylor Series
4	3.1×10^{-8}	1.7×10^{-8}	2.0×10^{-9}	2.5×10^{-9}	6.2×10^{-7}	1.5×10^{-7}
8	2.7×10^{-7}	1.6×10^{-7}	2.9×10^{-8}	2.1×10^{-8}	4.0×10^{-6}	1.2×10^{-6}
12	5.1×10^{-7}	3.2×10^{-7}	4.8×10^{-8}	4.0×10^{-8}	7.4×10^{-6}	2.5×10^{-6}
16	7.8×10^{-7}	4.8×10^{-7}	7.1×10^{-8}	5.8×10^{-8}	1.1×10^{-5}	4.0×10^{-6}
20	1.0×10^{-6}	6.6×10^{-7}	9.8×10^{-8}	7.6×10^{-8}	1.5×10^{-5}	5.6×10^{-6}
24	1.3×10^{-6}	8.3×10^{-7}	1.2×10^{-7}	9.5×10^{-8}	1.9×10^{-5}	7.3×10^{-6}
28	1.6×10^{-6}	1.0×10^{-6}	1.5×10^{-7}	1.1×10^{-7}	2.2×10^{-5}	9.1×10^{-6}
32	1.9×10^{-6}	1.3×10^{-6}	1.7×10^{-7}	1.3×10^{-7}	2.7×10^{-5}	1.1×10^{-5}
36	2.2×10^{-6}	1.4×10^{-6}	2.0×10^{-7}	1.5×10^{-7}	3.3×10^{-5}	1.3×10^{-5}
40	2.5×10^{-6}	1.6×10^{-6}	2.2×10^{-7}	1.7×10^{-7}	3.7×10^{-5}	1.4×10^{-5}
44	2.8×10^{-6}	1.7×10^{-6}	2.5×10^{-7}	1.9×10^{-7}	4.4×10^{-5}	1.6×10^{-5}
48	3.1×10^{-6}	1.9×10^{-6}	2.7×10^{-7}	2.1×10^{-7}	4.5×10^{-5}	1.8×10^{-5}

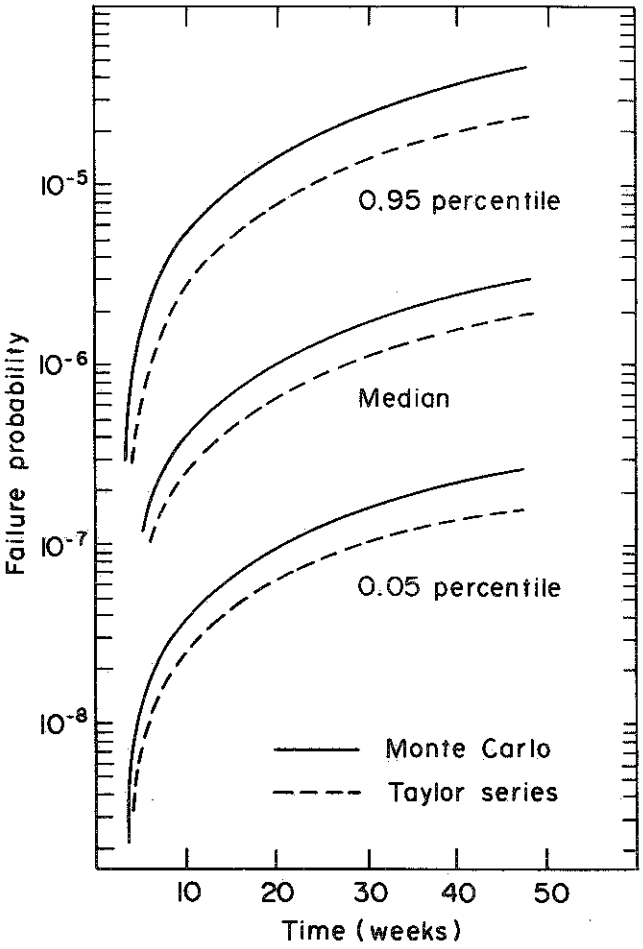

Fig. 5. Characteristic values of the failure probability of the shutdown system.

we found that the failure probability distribution is approximately lognormal. The expected value, the variance, and the coefficients[2,17] of skewness (β_1) and kurtosis (β_2) of the pdf of the negative common logarithm of the failure probability are listed in Table VII. We see from this table that the pairs (β_1, β_2) at various times are very close to the pair (0, 3) corresponding to the normal pdf, and that the results of the Taylor series expansion method and the Monte Carlo simulation are in very good agreement.

At the end of the 48th week, the Taylor series approximation and the histogram of the Monte Carlo simulation for the pdf of the negative common logarithm of the failure probability, F, are graphed in Fig. 6. This failure probability has a median of 2×10^{-6} and 0.95 and 0.05 percentiles of 2×10^{-5} and 2×10^{-7}, respectively. It differs considerably from the 1×10^{-9} point estimate found when interdependences are excluded, the inspection is perfect, and the input variables are certain.[24,25]

Our results parallel those obtained from analyses of and experience with LWRs in which human errors during test and maintenance activities and common-cause failures are major contributors to system unavailability and, therefore, to the failure probability.[26,27]

To assess the sensitivity of the RSS failure probability to interdependences and human errors, we have examined four special cases: (a) the failure rates of the components are completely independent and the inspection is perfect, i.e., every four weeks the electrical subsystems are completely renewed; (b) the failure rates and the states of the components are completely independent, and the inspection is perfect;

TABLE VII

Mean, Variance, and Coefficients of Skewness (β_1) and Kurtosis (β_2) of the Negative Common Logarithm of the Failure Probability at Various Times for the Shutdown System of the CRBR

(For the normal pdf, $\beta_1 = 0$ and $\beta_2 = 3$.)

Time (week)	Mean		Variance		Skewness (β_1)		Kurtosis (β_2)	
	Monte Carlo	Taylor Series	Monte Carlo	Taylor Series	Monte Carlo	Taylor Series	Monte Carlo	Taylor Series
4	7.5	7.8	0.53	0.29	0.108	0.075	3.21	3.30
8	6.6	6.8	0.44	0.28	0.114	0.042	3.25	3.26
12	6.3	6.5	0.44	0.30	0.091	0.032	3.22	3.30
16	6.1	6.3	0.44	0.31	0.078	0.020	3.20	3.30
20	6.0	6.2	0.44	0.32	0.071	0.014	3.18	3.30
24	5.9	6.1	0.44	0.33	0.068	0.010	3.16	3.30
28	5.8	6.0	0.45	0.34	0.066	0.009	3.15	3.29
32	5.7	5.9	0.45	0.34	0.068	0.007	3.14	3.29
36	5.6	5.9	0.46	0.35	0.072	0.007	3.14	3.29
40	5.6	5.8	0.46	0.35	0.078	0.006	3.16	3.29
44	5.5	5.8	0.47	0.35	0.086	0.005	3.18	3.28
48	5.5	5.7	0.47	0.35	0.096	0.005	3.22	3.28

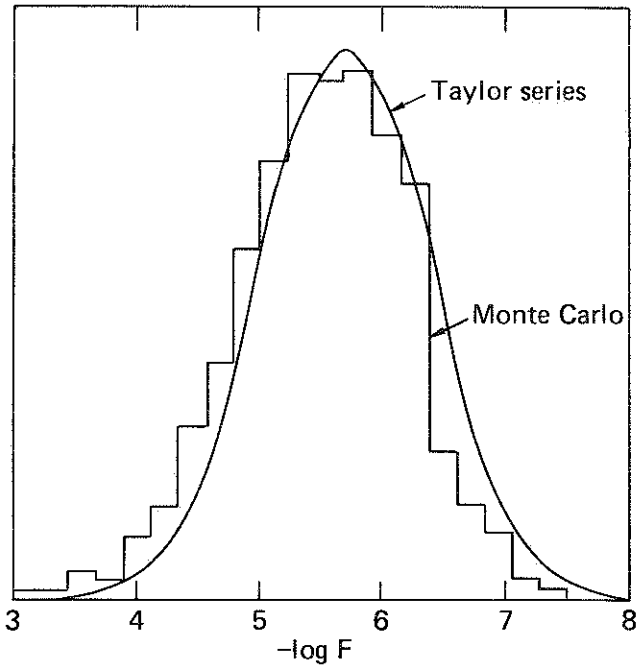

Fig. 6. The pdf of the logarithm of the failure probability of the shutdown system.

(c) the failure rates of the components are completely independent, but inspection is imperfect, i.e., human errors are possible; and (d) interdependences exist, and the inspection is imperfect.

For these cases, medians, 90% probability bands, and point estimates of the RSS failure probability per year are listed in Table VIII. In addition, the table includes the objective value of the failure probability obtained in Ref. 24. This objective value differs from the point estimate of case (a) because, in our study, we used a more detailed model for the electrical subsystem than in Ref. 24. Specifically, we assumed that successful responses to limited response transients result in the renewal of the electrical subsystem, and that the repair of the sensors (with the reactor shut down) is not instantaneous.

We see from Table VIII that (a) uncertainties about the input variables [case (a)] result in a 90% failure probability band that spans three orders of magnitude (4×10^{-11} to 2×10^{-8}); (b) uncertainties and interdependences [case (b)] result in a 90% failure probability band of the same size as in case (a) but shifted by two orders of magnitude from 1×10^{-9} to 6×10^{-6}; (c) uncertainties and human errors [case (c)] result in a 90% failure probability band shifted by two orders of magnitude but narrower than that of case (a) (1×10^{-8} to 5×10^{-6}); and (d) uncertainties, interdependences, and human errors [case (d)] result in a 90% failure probability band shifted by three orders of magnitude but narrower than that of case (a) (2×10^{-7} to 2×10^{-5}).

The results of the Taylor series calculations provide a means for classifying the input variables according to their contribution to the uncertainties of the failure probability. We have performed such a classification for the RSS failure probability at the end of one year. Each variable is classified according to two "importance indexes." Index 1 gives the percentage the variable contributes to deviation D of the expected value of the negative common logarithm of the failure probability from the value obtained when all input variables are fixed at their means.[28] Index 2 gives the percentage the variable contributes to the variance of the negative common logarithm of the failure probability [see Eq. (12)]. The relative importances of the variables are listed in Table IX. For example, if the arrival rate of the limited response transients were fixed at its mean value, deviation D would have increased by 69.6%, and the variance of

[28]The deviation D is defined by $D \equiv E(u) - u(x_1, \ldots, \bar{x}_m)$, where $u = -\log F$ [see Eq. (11)].

TABLE VIII

Point Estimate, Median, and 90% Probability Band of the Failure Probability per Year Under Various Assumptions for the Shutdown System of the CRBR

(Point estimate is the value of the failure probability obtained when the input variables are assumed to be fixed at their means.)

Case	Assumption	Failure Probability			
		Point Estimate	Median	0.05 Percentile	0.95 Percentile
0	WARD-D-0118 "Objective"	1.5×10^{-9}	---	---	---
a	No dependences, perfect inspection	8×10^{-10}	1×10^{-9}	4×10^{-11}	2×10^{-8}
b	Dependences, perfect inspection	2×10^{-7}	8×10^{-8}	1×10^{-9}	6×10^{-6}
c	No dependences, perfect inspection	4×10^{-7}	2×10^{-7}	1×10^{-8}	5×10^{-6}
d	Dependences, imperfect inspection	2×10^{-6}	2×10^{-6}	2×10^{-7}	2×10^{-5}

TABLE IX

Classification of Input Variables According to Their Contribution to the Uncertainties of the Failure Probability

Input Variable	Importance Index 1	Importance Index 2
Limited response transients	−69.6	25.6
Reactivity transient	59.7	18.0
Probability of one inspection error	36.3	15.6
Conditional probability of second inspection error	33.6	9.2
Dependence coefficient (three or more channels down)	22.3	7.8
Major flow transient	8.6	2.0
Dependence coefficient (one channel down)	7.8	1.1
Dependence coefficient (two channels down)	5.4	1.6
Secondary logic train	−4.6	1.8
Secondary comparator	3.9	10.9
Primary comparator	−3.6	2.2
Reactor repair rate	3.0	Negligible

the negative logarithm would have decreased by 25.6%. It is noteworthy that the importance of the limited response transient arrival rate is due to the renewal effect that successful responses have on the shutdown system and not to the failures that these transients might cause. This means that limited response transients are equivalent to complete, perfect repairs of the system, occurring randomly in time. Again, from Table IX we see that the uncertainty about the failure probability is due primarily to uncertainties about the arrival rates of transients and human errors during the inspection of the electrical subsystems.

V. CONCLUSIONS

We have developed a methodology for the calculation of uncertainties about the reliability of Markovian systems, including three techniques for the reduction of the computational effort associated with Markovian reliability analyses of large reactor systems. All the calculations necessary for the implementation of the methodology have been computerized.

As an illustration of the methodology, we have assessed the uncertainties about the failure probability of the shutdown system of the CRBR. Uncertainty of one order of magnitude about various input variables results in two orders of magnitude uncertainty about the failure probability.

Either tests or further analyses or both can reduce the uncertainty about the input variables and, hence, the uncertainty about the probability of loss of core coolable geometry of CRBR due to shutdown system failures. More information about failure rates can be obtained by testing and analysis of individual components. However, information about interdependence (hardware common-cause failures), human errors, and transient arrival rates can be obtained only by observing real systems in operation and not from tests of individual components. For this reason, we believe that experience gained from prototype systems, such as the Fast Flux Test Facility and the CRBR, is of major importance to the safety assessment of breeder reactors.

APPENDIX

CHOICE OF TIME STEP

For a Markovian process, the probability p_{ij} that the system will transit from state i to state j during an interval Δt is given by the relation

$$p_{ij} = 1 - \exp(-h_{ij}\Delta t) \ , \qquad \text{(A.1)}$$

where h_{ij} is the transition rate (failure or repair) between states i and j. For discrete time steps, we assume that the transition occurs at the end of Δt and select it such that

$$p_{ij} \approx h_{ij}\Delta t \qquad \text{for all } i \text{ and } j \ . \qquad \text{(A.2)}$$

For the Monte Carlo simulation, we choose randomly a set $\{h_{ij}\}$, and a Δt that allows the use of approximation (A.2). Because they are random variables unbounded from above, the transition rates can be very large (albeit with small probability) and the time step very small. A small time may result in an expensive simulation if the number of time steps is large.

If all or most of the h_{ij}'s are large, the number of time steps is small because the system reaches a steady state after a reasonable number of transitions.

If one transition rate is much larger than the others, the number of time steps can be prohibitively large because the system may not reach a steady state after a reasonable number of transitions. The reason is that the size of the time step, dictated by the fast change of state of a particular component, is much smaller than that required by the slower change of state of the system. To avoid this problem, we proceed as follows. If in the set $\{h_{ij}\}$ the rate h_{ir} is much larger than the others, we choose a large Δt such that

$$p_{ij} \cong h_{ij}\Delta t \quad \text{for all } i \text{ and } j \neq r, \text{ and } p_{ir} \approx 1 \ . \qquad \text{(A.3)}$$

Details about this approach, its accuracy, and its limitations are given in Ref. 2.

ACKNOWLEDGMENT

This work was performed under the auspices of the U.S. Nuclear Regulatory Commission, while the first author (I.A.P.) was at Brookhaven National Laboratory, Department of Applied Science, Fast Reactor Safety Division.