LA-UR-81-2595

CONF-810905--5

TITLE: FAILURE MODE ANALYSIS USING STATE VARIABLES DERIVED FROM FAULT TREES WITH APPLICATION

AUTHOR(S): Robert J. Bartholomew

MASTER

SUBMITTED TO: International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
September 20-24, 1981
Port Chester, New York

University of California

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

LOS ALAMOS SCIENTIFIC LABORATORY
Post Office Box 1663 Los Alamos, New Mexico 87545
An Affirmative Action/Equal Opportunity Employer

Form No. 836 R3
St. No. 2629
12/78

UNITED STATES
DEPARTMENT OF ENERGY
CONTRACT W-7405-ENG. 36

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Failure-Mode Analysis Using State Variables Derived From Fault Trees with Application*

Robert J. Bartholomew

Los Alamos National Laboratory
Los Alamos, NM 87545

ABSTRACT

Fault Tree Analysis (FTA) is used extensively to assess both the qualitative and quantitative reliability of engineered nuclear power systems employing many subsystems and components. FTA is very useful, but the method is limited by its inability to account for failure mode rate-of-change interdependencies (coupling) of statistically independent failure modes. The state variable approach (using FTA-derived failure modes as states) overcomes these difficulties and is applied to the determination of the lifetime distribution function for a heat pipe-thermoelectric nuclear power subsystem. Analyses are made using both Monte Carlo and deterministic methods and compared with a Markov model of the same subsystem.

INTRODUCTION

The fault tree is widely used for qualitative and quantitative assessment of safety, reliability, and risk for many engineered systems.[1-4] The analytical methodology is called Fault Tree Analysis (FTA). FTA is helpful in designing engineered safety and reliability subsystems for nuclear power plants. However, one class of problems in reliability analysis is difficult, if not impossible, to handle with FTA alone. This class is one where FTA is used to identify failure modes leading to the top event, subsequently considering physical processes coupling two or more statistically independent failure modes. In this paper we formulate a model using FTA so that these coupling effects are studied.

The fault tree is a non-unique logic representation of failure. However, two different fault trees of the same problem must always yield identical minimal cut sets if both fault trees are correct. The state variable method of analysis has the mathematical structure wherein this non-uniqueness problem can be resolved.[5] This paper considers the input space as stochastic initiating events whose time-dependent properties we know. The state space we consider are the non-unique failure modes of the subsystem, and the

*This paper is a result of research by the author in partial fulfillment of Ph.D. dissertation requirements.

output space contains the top event(s). A practical example involves an electric power production module (subsystem) in a Space Power Advanced Reactor (SPAR).[6] Two state space models are formulated and compared: (1) a Markov model and (2) a failure mode state vector model. While these two models yield identical results for the top event lifetime distribution function for uncoupled models, the failure mode model possesses two distinct advantages over the Markov model: (1) The number of unknown states are considerably reduced, and (2) coupling effects between the time derivatives of the failure modes are easily studied. The failure mode model is studied from two different points of view: (1) a deterministic solution, and (2) a Monte Carlo simulation. This paper illustrates the advantages of the failure mode model over the Markov model.

MODEL FORMULATION

Physical Description of SPAR and Reliability-Fault Tree Models

The SPAR system consists of (1) a fast-reactor core with high power density, (2) core heat pipes for heat transport, (3) direct conversion of heat energy to electrical energy through thermoelectric modules at the core heat pipe condenser ends, (4) radiator heat pipes radiating waste heat to space, and (5) control drums for reactor safety and power level control. For the purpose of our analysis here we consider a subsystem power generation module for which we wish to examine the failure modes and coupling between (2) and (3), for SPAR goal constant failure rates. Figure 1 is an artist's conception of the complete SPAR system, and component details.

(a) (b)

(c) (d)

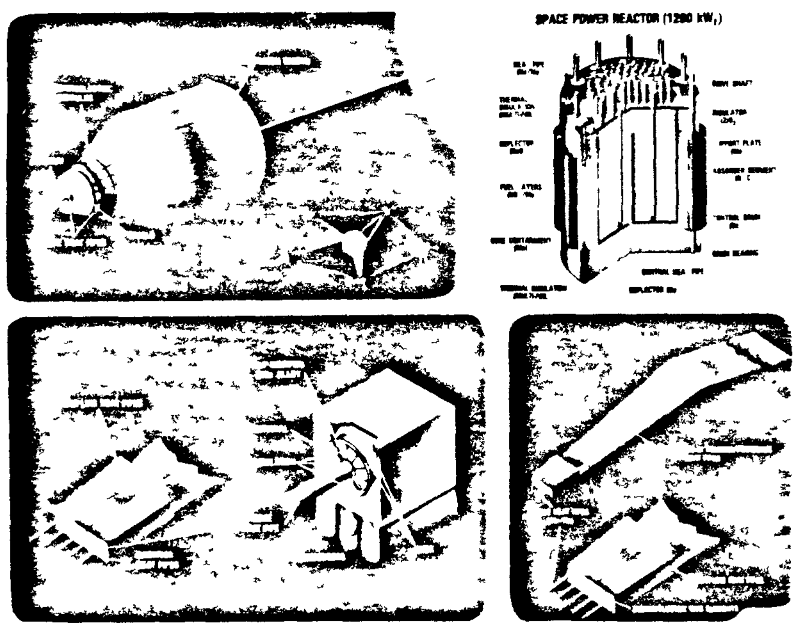


Fig. 1. (a) Complete SPAR system, (b) core details, (c) thermoelectric converter details, (d) radiator details.

In order to illustrate the advantages of the failure mode model over the Markov model, we consider the simplest three component case with a subsystem power generation module (Fig. 1) consisting of one core heat pipe, designated (1) and one thermoelectric converter unit, (2), consisting of two converters in parallel with the unit in series with respect to reliability as shown in Fig. 2.

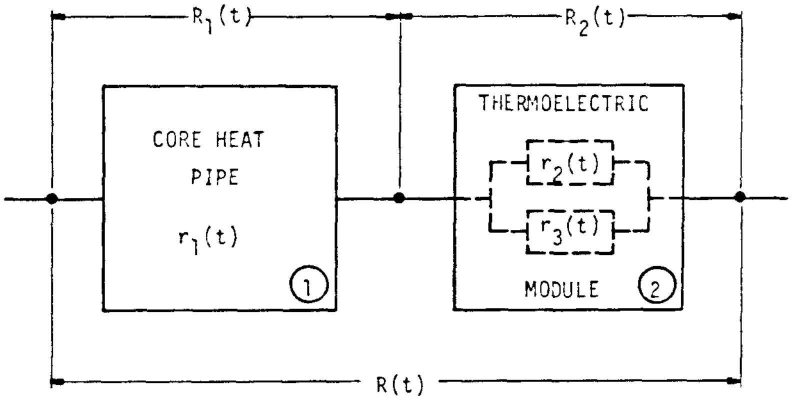


Fig. 2. Series reliability model for redundant thermoelectric converter subsystem power generation module.

With a Poisson process assumption for the stochastic behavior of failure mechanisms in this subsystem leading to exponential distributions of waiting time to failure,[7] we can express the component reliabilities as

$$R_1(t) = r_1(t) = e^{-\lambda_1 t} \quad , \quad r_2(t) = e^{-\lambda_2 t} \quad , \quad r_3(t) = e^{-\lambda_3 t} \tag{1}$$

and the series configuration with no cross coupling and stochastic independence assumptions gives the subsystem reliability

$$R(t) = R_1 \cdot R_2 \tag{2}$$

With stochastically independent components in the thermoelectric converter unit, the redundancy implied by the parallel reliability configuration results in

$$R_2(t) = r_2(t)+r_3(t) - r_2(t)\cdot r_3(t) = e^{-\lambda_2 t} + e^{-\lambda_3 t} - e^{-(\lambda_2+\lambda_3)t} \tag{3}$$

The corresponding lifetime cumulative distribution functions[8] (cdf's) associated with equations (1), (2), and (3) are

$$\left.\begin{aligned} F_1(t) &= u_1(t) = 1 - r_1(t) = 1 - e^{-\lambda_1 t} \\ F_2(t) &= 1-e^{-\lambda_2 t} - e^{-\lambda_3 t} + e^{-(\lambda_2+\lambda_3)t} \\ T(t) &= 1 - R(t) = 1-e^{-(\lambda_1+\lambda_2)t} - e^{-(\lambda_1+\lambda_3)t} + e^{-(\lambda_1+\lambda_2+\lambda_3)t} \end{aligned}\right\} \tag{4}$$

A simplified subsystem fault tree model was formulated consisting of a single core heat pipe to which two redundant thermoelectric modules are attached. We consider the following events: $\mathcal{T}$ = top event power output failure, which can happen if,

1) $\mathcal{F}_1 \triangleq$ the core heat pipe C_1 fails,

"OR"

2) $\mathcal{F}_2 \triangleq$ thermoelectric module C_2 fails

"AND" thermoelectric module C_3 fails.

The fault tree for this subsystem is shown in Fig. 3.

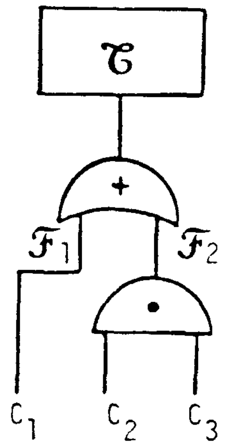


Fig. 3. Fault tree for SPAR example.

The top event equation for the fault tree of Fig. 3, using Boolean algebra (+),(·) reduction is

$$\mathcal{T} = C_1 + C_2C_3 \tag{5}$$

C_1 and C_2C_3 are the minimal cut sets for this system.

Assuming C_1, C_2, and C_3 to be initiator failures, Poisson distributed, with constant failure rates λ_1, λ_2, $\lambda_3 (yr^{-1})$, we can formulate the failure mode state variable model in differential equation form as:

$$\underbrace{\begin{bmatrix} \dot{F}_1 \\ \dot{F}_2 \end{bmatrix}}_{\dot{\underline{F}}} = \underbrace{\begin{bmatrix} -\lambda_1 & 0 \\ 0 & -(\lambda_2+\lambda_3) \end{bmatrix}}_{\underline{A}} \underbrace{\begin{bmatrix} F_1 \\ F_2 \end{bmatrix}}_{\underline{F}} + \underbrace{\begin{bmatrix} \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_3 & \lambda_2 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}}_{\underline{B}} \underline{U}(t) \tag{6}$$

with initial conditions

$$\underline{F}\ (0) = [0\ 0]^T\ ,\ \underline{U}\ (0) = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T \qquad (7)$$

and the top event equation

$$T = \underbrace{[1\ 1]}_{C}\ \underline{F} + [0\ \underbrace{-1\ -1\ -1\ 1\ 1\ 1\ -1}_{D}]\ \underline{U}(t) \qquad (8)$$

where

$$\underline{U} = \left[1\ \ 1-e^{-\lambda_1 t}\ \ 1-e^{-\lambda_2 t}\ \ 1-e^{-\lambda_3 t}\ \ 1-e^{-(\lambda_1+\lambda_2)t}\ \ 1-e^{-(\lambda_1+\lambda_3)t}\ \ 1-e^{-(\lambda_2+\lambda_3)t}\ \ 1-e^{-(\lambda_1+\lambda_2+\lambda_3)t}\right]^T \qquad (9)$$

In terms of reliability, we let $\overline{C}_1 \triangleq$ good state of heat pipe (1), $\overline{C}_2 \triangleq$ good state of TE module (2), and $\overline{C}_3 \triangleq$ good state of TE module (3).

The Markov model consists of eight states:

(1) S_0 = state $(\overline{C}_1\ \overline{C}_2\ \overline{C}_3)$, (2) S_1 = state $(\overline{C}_1\ \overline{C}_2\ C_3)$,

(3) S_2 = state $(\overline{C}_1\ C_2\ \overline{C}_3)$, (4) S_3 = state $(\overline{C}_1\ C_2\ C_3)$,

(5) S_4 = state $(C_1\ \overline{C}_2\ \overline{C}_3)$, (6) S_5 = state $(C_1\ \overline{C}_2\ C_3)$,

(7) S_6 = state $(C_1\ C_2\ \overline{C}_3)$, (8) S_7 = state $(C_1\ C_2\ C_3)$, where

C_i, i=1,2,3 is the bad state of the i^{th} component.

The class structure of the set of states $\{S_i,\ i=0,1,2,\ldots 7\}$ is illustrated in Fig. 4, where the Markov probability statement concerning one-step transitions is stated as

$$\Pr\{\text{remaining in or moving to } S_i \text{ at } t+\Delta t \mid \text{in } S_j \text{ at } t;\ i,j=0,1,2,\ldots 7\} \qquad (10)$$

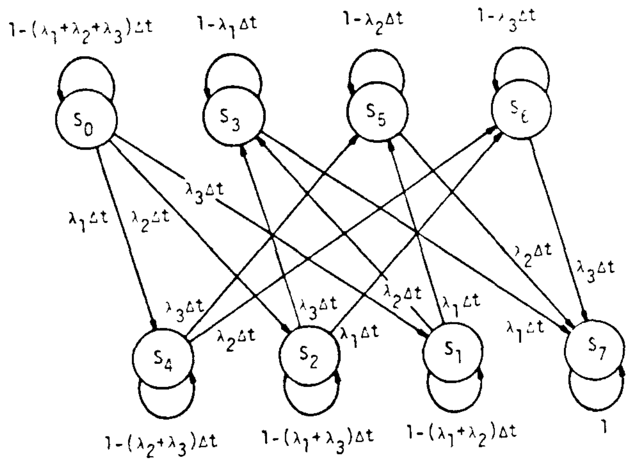


Fig. 4. Class structure and transitions for Markov model of redundant thermoelectric converter subsystem power generation model.

Using statement (10) and the Markov model postulates[7] from Fig. 4, we can write

$$\underbrace{\begin{bmatrix} P_0(t+\Delta t) \\ P_1(t+\Delta t) \\ P_2(t+\Delta t) \\ P_3(t+\Delta t) \\ P_4(t+\Delta t) \\ P_5(t+\Delta t) \\ P_6(t+\Delta t) \\ P_7(t+\Delta t) \end{bmatrix}}_{\underline{P}(t+\Delta t)} = \underbrace{\begin{bmatrix} 1-(\lambda_1+\lambda_2+\lambda_3)\Delta t & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_3\Delta t & 1-(\lambda_1+\lambda_2)\Delta t & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_2\Delta t & 0 & 1-(\lambda_1+\lambda_3)\Delta t & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_2\Delta t & \lambda_3\Delta t & 1-\lambda_1\Delta t & 0 & 0 & 0 & 0 \\ \lambda_1\Delta t & 0 & 0 & 0 & 1-(\lambda_2+\lambda_3)\Delta t & 0 & 0 & 0 \\ 0 & \lambda_1\Delta t & 0 & 0 & \lambda_3\Delta t & 1-\lambda_2\Delta t & 0 & 0 \\ 0 & 0 & \lambda_1\Delta t & 0 & \lambda_2\Delta t & 0 & 1-\lambda_3\Delta t & 0 \\ 0 & 0 & 0 & \lambda_1\Delta t & 0 & \lambda_2\Delta t & \lambda_3\Delta t & 1 \end{bmatrix}}_{\underline{P_{ij}}(\Delta t)} \underbrace{\begin{bmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \\ P_5(t) \\ P_6(t) \\ P_7(t) \end{bmatrix}}_{\underline{P}(t)} \qquad (11)$$

The vector $\underline{P}(t+\Delta t)$ is expressed as a forward (in time) recursion relation utilizing the transition matrix $\underline{P_{ij}}(\Delta t)$ and the vector $\underline{P}(t)$. $\underline{P_{ij}}(\Delta t)$ is obviously column stochastic as required by the Markov assumption, i.e., $\sum_{i=0}^{7} P_{ij}(\Delta t)=1$ for all $j=0,1,\ldots 7$, and $P_{ij}\geq 0$ for all i,j. Transposing $\underline{I}\ \underline{P}(t)$ to the left hand side, dividing by Δt and passing to the limit as $\Delta t\to 0$ gives eight differential equations of the form

$$\dot{\underline{P}}(t) = \underline{A}\ \underline{P}(t) \qquad (12)$$

with initial condition

$$\underline{P}(0) = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T. \qquad (13)$$

With no coupling the 8th order (eight state) Markov model involving $P_i(t)$, $i=0,1,7$ as given in Eqns (12) and (13), yields results identical with Eqns (4) for the "lumped" states

$$F_1(t) = \sum_{i=4}^{7} P_i(t) \quad , \; F_2(t) = P_3(t)+P_7(t), \text{ and } T(t) = \sum_{i=3}^{7} P_i(t).$$

Failure Mode Coupling

Let us now consider a possible cross coupling physical mechanism between the heat pipe and the compression fitted thermoelectric converter described as follows:

1. Molecular diffusion of constituent materials of the thermoelectric module due to high heat flux and high contact pressure through the hot leg contact with the heat pipe, causing changes in rate of fluid pumping in the heat pipe. We assume this coupling (a_{12}) is linear and is defined as the rate of change of heat pipe pumping life rate with respect to thermoelectric converter life.

2. Overheating and re-cooling of the heat pipe causes the thermoelectric converters to creep at the hot leg, losing contact pressure and resulting in loss of converter efficiency or, in the case of a bonded contact, the bond may be strengthened or weakened. We assume this coupling (a_{21}) is also linear and defined as the rate of change of thermoelectric converter life rate with respect to heat pipe life.

Mathematically, we describe coupling a_{12} and a_{21} as

$$\left.\begin{aligned}\dot{F}_1(t) &= \frac{\partial \dot{F}_1}{\partial F_1}F_1 + \frac{\partial \dot{F}_1}{\partial F_2}F_2 + \lambda_1 u_0(t) = -\lambda_1^{\star}F_1 + a_{12}F_2 + \lambda_1 \\ \dot{F}_2(t) &= \frac{\partial \dot{F}_2}{\partial F_1}F_1 + \frac{\partial \dot{F}_2}{\partial F_2}F_2 + \lambda_3 u_2(t) + \lambda_2 u_3(t) = a_{21}F_1 - \lambda_2^{\star}F_2 + \lambda_3(1-e^{-\lambda_2 t}) + \lambda_2(1-e^{-\lambda_3 t})\end{aligned}\right\} \quad (14)$$

The introduction of these couplings (a_{12}, a_{21}) implies probability constraints on the matrix $\underline{A}$ in order to ensure that $\lim_{t\to\infty} F_1(t) = \lim_{t\to\infty} F_2(t) = 1.0$.

The requirement of this constraint implies that $\lambda_1^{\star} = \lambda_1 + a_{12}$, and $\lambda_2^{\star} = \lambda_2 + \lambda_3 + a_{21}$.

In order that the resulting recursion matrix in reliability space has columns that sum to unity, we need an additional equation of the following form:

$$\begin{aligned}D(t+\Delta t) \triangleq\ &(\lambda_1 + a_{12} - a_{21})\Delta t\ R_1(t) + (\lambda_2 + \lambda_3 + a_{21} - a_{12})\Delta t\ R_2(t) \\ &+ (\lambda_2 - \lambda_3)\Delta t\ r_2(t) - (\lambda_2 - \lambda_3)\Delta t\ r_3(t) + D(t)\end{aligned} \quad (15)$$

The matrix of equations in incremental form is:

$$\underbrace{\begin{bmatrix} R_1(t+\Delta t) \\ R_2(t+\Delta t) \\ r_2(t+\Delta t) \\ r_3(t+\Delta t) \\ D(t+\Delta t) \end{bmatrix}}_{\underline{R}(t+\Delta t)} = \underbrace{\begin{bmatrix} 1-\lambda_1^{\star}\Delta t & a_{12}\Delta t & 0 & 0 & 0 \\ a_{21}\Delta t & 1-\lambda_2^{\star}\Delta t & \lambda_3\Delta t & \lambda_2\Delta t & 0 \\ 0 & 0 & 1-\lambda_2\Delta t & 0 & 0 \\ 0 & 0 & 0 & 1-\lambda_3\Delta t & 0 \\ (\lambda_1^{\star}-a_{21})\Delta t & (\lambda_2^{\star}-a_{12})\Delta t & (\lambda_2-\lambda_3)\Delta t & -(\lambda_2-\lambda_3)\Delta t & 1 \end{bmatrix}}_{\underline{P}_{R_{ij}}(\Delta t)} \underbrace{\begin{bmatrix} R_1(t) \\ R_2(t) \\ r_2(t) \\ r_3(t) \\ D(t) \end{bmatrix}}_{\underline{R}(t)} \quad (16)$$

For $\lambda_2 = \lambda_3$ (identical singly redundant thermoelectric converters), $\underline{P}_{R_{ij}}(\Delta t)$ is a column stochastic transition matrix with conditions

$$\left.\begin{array}{l} a_{12} > 0 \quad , \; a_{21} > 0 \\ -\lambda_1 \le a_{12} - a_{21} \le \lambda_2 + \lambda_3 = 2\lambda_2 \\ \lambda_1^{\star} = \lambda_1 + a_{12} \\ \lambda_2^{\star} = \lambda_2 + \lambda_3 + a_{21} = 2\lambda_2 + a_{21} \end{array}\right\} \qquad (17)$$

However, for $\lambda_2 \neq \lambda_3$, either the term $-(\lambda_2-\lambda_3)\Delta t$ with $\lambda_2 > \lambda_3$ or $(\lambda_2-\lambda_3)\Delta t$ with $\lambda_2 < \lambda_3$ is negative, which violates the condition for a stochastic matrix that all elements be positive or zero. (Note that this is true even for the uncoupled case $a_{12}=a_{21}=0$.) This causes difficulty only in the Monte Carlo simulation model; since we know that the failure mode state variable model gives the correct (equivalent to the Markov model) solutions for $F_1(t)$, $F_2(t)$, and $T(t)$ for $a_{12}=a_{21}=0$. We can obtain an approximate Monte Carlo simulation of system (16) if we realize that the redundancy of the thermoelectric converter module implies an intersection in the reliability space involving r_2 and r_3, and transitions to D from either r_2 or r_3. Thus the equation for $D(t+\Delta t)$ in (16) is a probability statement of events that are not mutually exclusive with respect to transitions from r_2 or r_3 to D. Since our main interest is not in Monte Carlo simulation but in establishing a state variable deterministic systems analysis procedure, we did not pursue further refinements in the simulation. The advantages of the deterministic state variable failure mode model over the more classical Markov model are clearly seen:

(1) We have reduced the 8th order Markov model to the 2nd order failure mode model.

(2) The failure mode model allows for the inclusion of rate couplings having a physical interpretation among the failure modes; whereas the Markov model does not.

Application and Results

The reliability goals for the SPAR power generation unit allow for failure on average of three heat pipes out of 90 for the 7-yr lifetime of the unit. The thermoelectric converter module is allowed one failure per 90 heat pipes on average for the 7-yr lifetime. These goals translate to average (constant) failure rates of

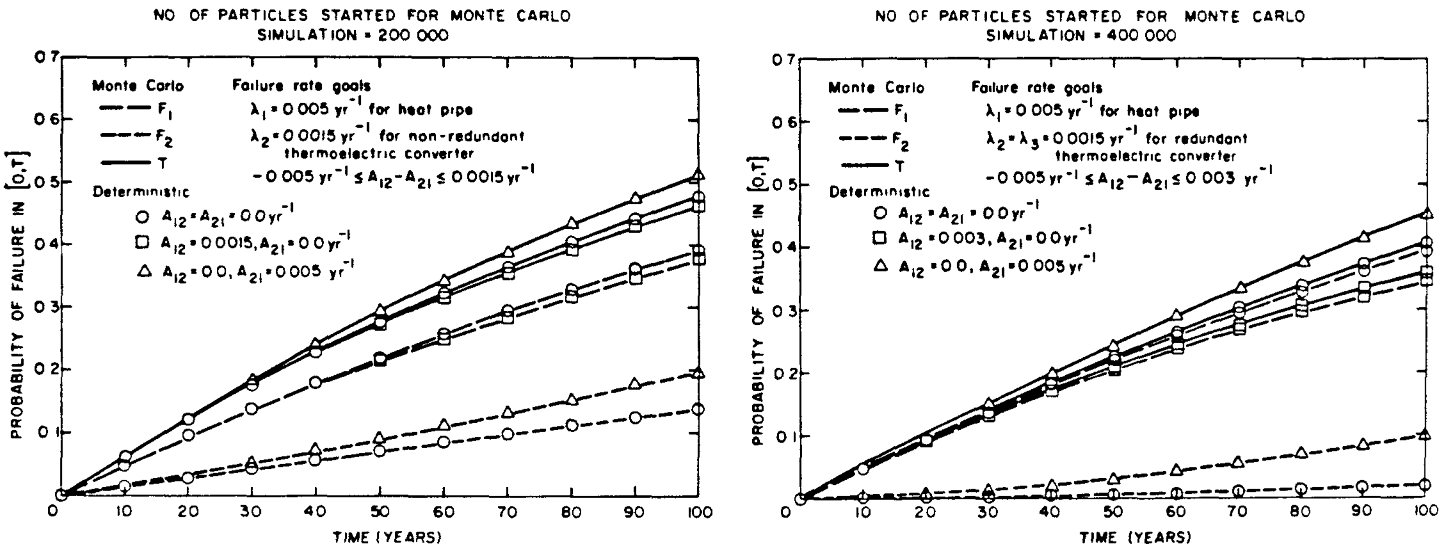
$\lambda_1 \simeq 5 \times 10^{-3} yr^{-1}$ for the heat pipes, and

$\lambda_2 \simeq 1.5 \times 10^{-3} yr^{-1}$ for the (non-redundant) thermoelectric converters.

For the single redundancy for thermoelectric converters we assume identical thermoelectric converters giving

$\lambda_3 \simeq = 1.5 \times 10^{-3} yr^{-1}$ for the redundant thermoelectric converters.

Using the coupling constraints, several lifetime distribution cases were calculated both deterministically and with a Monte Carlo simulation. Figures 4a and 4b show these coupling effects on F_1, F_2 and T for a 100 year period for the non-redundant and redundant systems, respectively. The implication of improvement in heat pipe reliability with positive a_{12} coupling is difficult to envision with respect to a physical mechanism. This situation implies that if degradation does occur due to a_{12} coupling, then a_{12} must be negative. This also infers that a_{21} could be negative also for some physical coupling situations. Since this violates our constraint conditions to ensure that the transition matrix is column stochastic, we cannot expect that $F_1(t)$, $F_2(t)$, and $T(t)$ are cdf's with respect to time. However, these functions, though they are not Markovian, can still have a probability interpretation since we have implied that $F_i(t+\Delta t)$ and $T(t+\Delta t)$ are the probabilities of the union of several events during Δt that are not mutually exclusive and, in fact, have an intersection implied by negative a_{12} and/or negative a_{21}.



(a) (b)

Fig. 4. Comparisons of lifetime distribution functions with failure mode coupling for a SPAR power generation module: (a) non-redundant thermoelectric converter system; (b) redundant thermoelectric converter system.

CONCLUSIONS

The major conclusions of this study are:

1) A state variable method of reliability analysis using the failure modes of fault trees as elements of a state vector is a practical method of reliability analysis.

2) A failure mode state variable reliability model has the distinct advantage over the classical Markov model in that the order of the system can be significantly reduced.

3) A second advantage of the failure mode state variable reliability model over the Markov model is that physical coupling effects between failure mechanisms that may have an alleviating or degrading effect on reliability can be easily included.

4) The reduced order failure mode state variable reliability model can be solved deterministically and the solutions checked with Monte Carlo simulations that have an analog correspondence; i.e., systems governed by a stochastic matrix.

FUTURE WORK

Future effort should be expended in establishing the failure mode state variable method of analysis for applications of a wider engineering scope. The expected lifetime distribution functions are obtained by this method, and it would be desirable to extend the method for systems that have a non-constant or even stochastic uncertainty with respect to failure rates. Experiments should be designed to give a failure rate data base on advanced technology components such as heat pipes, thermoelectric converters, structural materials under high temperature, high stress, and vacuum loading in a radiation environment.

REFERENCES

1. Reactor Safety Study, WASH-1400 (NUREG 75/014) October 1975, Appendix II, "Fault Trees."

2. W. E. Vesely and R. E. Narum, "PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree," IN-1349, August 1970.

3. R. B. Worrell and D. W. Stack, "A SETS User's Manual for the Fault Tree Analyst," (NUREG/CR-0465) SAND 77-2051, November 1978.

4. L. Caldarola and A. Wickenhäuser, "Recent Advancements in Fault Tree Methodology at Karlsruhe," in Nuclear Systems Reliability and Risk Assessment," J. B. Fussell and G. R. Burdick, Eds. (SIAM, 1977), pp. 518-542.

5. W. L. Brogan, Modern Control Theory (Quantum Publishers, Inc., NY, 1974), Chap. 9, pp. 148-170.

6. D. Buden, W. A. Ranken, D. R. Koenig, "Space Nuclear Reactor Power Plants," Los Alamos Scientific Laboratory report LA-8223-MS, January 1980.

7. S. Karlin and H. M. Taylor, A First Course in Stochastic Processes 2nd Edition (Academic Press, NY, 1975), Chap. 4, pp. 123-125.

8. P. W. Becker and F. Jensen, Design of Systems and Circuits (Polyteknik Forleg, Lyngby, Denmark, 1974), Chap. 2, pp. 19-20.