NUCLEAR ENGINEERING AND DESIGN 13 (1970) 337–360. NORTH-HOLLAND PUBLISHING COMPANY

A TIME-DEPENDENT METHODOLOGY FOR FAULT TREE EVALUATION

W.E.VESELY
Idaho Nuclear Corporation,
Idaho Falls, Idaho 83401, USA

Received 22 April 1970

A methodology is developed by which exact and detailed probabilistic information is obtained for any fault tree. The methodology, called "Kinetic Tree Theory", is believed to be a major advancement in the field of reliability and safety analysis and is expected to have far-reaching ramifications.

The first assumption of Kinetic Tree Theory is that the primary failures, or components, of the fault tree are independent; one primary failure may occur at any number of places in the fault tree, but those primary failures which are unique are assumed independent. Inter-dependent primary failures can be handled by extension of the methods presented. The second and last assumption of Kinetic Tree Theory is that the mode failures (critical paths) of the fault tree are known. These are obtainable in a straightforward manner from the fault tree as is demonstrated.

Fault trees of any structure and of any complexity are handled. General failure and repair distributions are handled; there is no limitation to these distributions as in other methodologies. Complete probabilistic information is first obtained for each primary failure of the fault tree, then for each mode failure (critical path), and finally for the top failure itself. The information is obtained as a function of time, and hence, with regard to reliability and safety; complete kinetic behavior is obtained. The expressions developed are in a simple form, and as is shown, application to yield numerical results is both efficient and straightforward – with an average computer time on the order of one minute required for a 500 primary failure fault tree (on an IBM 360/75 computer).

1. Introduction

Any failure, whether it be of a reactor protective system, a rod drive system or the entire reactor power plant, can be depicted in terms of a fault tree. The fault tree is a logical diagram of the consequences of basic failures, called "primary failures", on the failure of interest, called the "top failure"*. The top failure is the final failure of predetermined designation while the primary failures are the fundamental failures which cause the top failure. The top failure, for example, may be the failure of a reactor protective system with the primary failures being failures of basic components of the reactor protective system. The fault tree traces the top failure to the primary failure causes; in this sense the fault tree represents a deductive method of analysis. The primary failures of the fault tree are failures whose respective causes are not of concern. The primary failures are thus "basic" failures, for which failure data is available, and represent the limit of resolution of the fault tree. The construction of fault trees and basic fault tree concepts are described by Haasl [1], Nagel [2], Mearns [3] and Headington et al. [4]. The purpose of this article is not the discussion of fault tree concepts and construction, of which the reader is assumed to have a basic knowledge. Instead, the evaluation of the constructed fault tree is the topic here, which is the subsequent step after construction.

The fault tree, having been constructed, is evaluated to first obtain the critical paths. A critical path, which we shall term a "mode failure", is a smallest set of primary failures such that if all these primary failures simultaneously exist, then the top failure exists **.

* In some references, "primary failure" is termed "component failure", and "top failure" the "system failure".

** In some nomenclatures, mode failures are termed "minimal cut sets".

A mode failure is thus a unique way, or mode, by which the top failure occurs. The (finite) collection of mode failures obtained from evaluating the fault tree are thus all the unique modes by which the top failure occurs. If a mode failure is defined to exist when all its member primary failures exist, then the top failure exists if one or more of the mode failures exist. The top failure can consequently be represented as the union of the mode failures of the fault tree; this union is the non-redundant expression of the fault tree. In terms of fault tree nomenclature, a mode failure consists of an "and gate" attached to which are the primary failures constituting this mode failure. The top failure can then be represented as an "or gate" attached to which are the mode failures (i.e., the and gates). Mode failures are discussed in more detail by Esary and Proschan [5]. The reader is assumed to have basic knowledge of the mode failure, or critical path, concepts.

In an actual evaluation, the mode failures of a fault tree can be obtained by a number of methods. The mode failures can be obtained by Boolean reduction, using simple rearrangement techniques or the minterm, maxterm approaches [6]. Testing of the fault tree can be used, where certain primary failures are assumed to occur and then the top failure is checked to determine if it has occurred. This deterministic testing is quite rapid if performed by a computer. Finally, Monte Carlo simulation can be used, with importance sampling employed to accelerate the Monte Carlo process. In general, the mode failures of a fault tree can be obtained in a straightforward and efficient manner.

With knowledge of the mode failures of the fault tree, the evaluation can then proceed to obtain the probabilistic characteristics of the primary failures, mode failures, and the top failure. Previously, the evaluation to obtain these probabilities has been done by Monte Carlo simulation or by Boolean deterministic methods. These evaluations were sometimes performed on the fault tree itself, in which case the mode failures were obtained concurrently with the probabilistic characteristics. In other cases, the evaluation was performed after the mode failures were obtained (i.e., the evaluation was performed on the non-redundant representation of the fault tree). The methodology which will be presented here is of the second type, where it is assumed that the mode failures have already been determined. (As stated, the obtainment of the mode failures is quite direct and actual methods of obtainment are demonstrated in the applications given later.)

Basically, the Monte Carlo approach is a procedure in which trials of the fault tree are simulated. In each trial, primary failures are made to occur and are repaired according to their failure and repair probabilities. The top failure is checked at various time points to determine whether it has occurred. For every top failure occurrence, a "success" is tallied in the appropriate tally counter. The average of the successes over many trials yields an estimate of the probability of the top failure occurring. The Monte Carlo simulation is applicable to systems of any complexity and can theoretically handle any prescribed failure and repair distributions. However, the Monte Carlo simulation requires a fairly large amount of computer time, and to obtain results in reasonable time, the failure and repair distributions assigned to the primary failures must be limited to simple forms. Further, the Monte Carlo simulation yields statistical estimates for results, and there is always a disturbing possibility that these estimates may be in considerable error, which is not shown by the accompanying error estimates. This is particularly so since the user must guess at forcing parameters which influence the estimates obtained.

The Boolean approach analyzes the fault tree in a Poisson manner by considering the various combinations of primary failure occurrences which are necessary for a top failure occurrence. The probabilities of these combinations are computed deterministically and are then tallied to obtain the probability of the top failure occurring. The Boolean approach has the advantage of yielding deterministic results without any associated statistical error. However, to yield results in a practical amount of time, the Boolean approach is limited to analysis of simpler trees, where there are a smaller number of the various primary failure combinations for which probabilities must be computed. The severest limitation of the Boolean approach is that methods have been derived to handle only very simple failure and repair distributions which can be assigned to the primary failures. General failure distributions, such as those which include burn-in and wear-out, and general repair distributions, such as a normal repair distribution, cannot be handled.

To incorporate the generality which is theoretically possible in the Monte Carlo approach and the deterministic results which are obtainable from the Boolean approach, the methodology presented here evaluates the fault tree by means of probability theory and differential calculus. The methodology, as stated, assumes the mode failures of the fault tree have been determined. The methodology also assumes the primary failures of the fault tree are independent; one primary failure may appear at any number of places on the fault tree, however, independence is assumed with regard to any two or more primary failures. Interdependent primary failures can be handled by a straightforward extension of the methods which will be developed here.

In the wedding of probability theory and differential calculus, the probabilities of the events considered are proportional to dt, a differential increment in time. Probabilities of intersections of these events are of order $(dt)^2$ and hence can be validly neglected (unlike the Boolean approach which must consider all intersections since "macroscopic" events are considered). Analysis of general, complex fault trees thus becomes significantly simplified. Further, general failure and repair distributions can be assigned to the primary failures; there is no restriction as to the distributions which can be used. The results obtained with this methodology are exact and are obtained as functions of time. Moreover, detailed, time-dependent probabilities are obtained not only for the top failure, but are obtained for every mode failure and for every primary failure of the fault tree. Thus, complete knowledge of the top failure, including the importance of particular mode failures and primary failures, is obtained for all time. Finally, as will be evident from the applications given, the methodology can be simply applied to yield numerical results in very little computer time. We shall call this methodology of using probability theory and differential calculus "Kinetic Tree Theory" since reliability and safety information is obtained for all time.

2. Primary failure information

Consider a single primary failure of the fault tree. Let

$\lambda(t)\,dt$ = the probability of the failure occurring in time t to $t + dt$ given the failure is not existing at time t, (1)

$\mu(t)\,dt$ = the probability of the failure being repaired in time t to $t + dt$ given the failure is existing at time t (2)

The quantities $\lambda(t)$ and $\mu(t)$ are basic data in terms of fault tree analysis or reliability theory and are dealt with extensively in the literature [7–9]. The quantity $\lambda(t)$ is termed the failure rate for the primary failure, while $\mu(t)$ is termed the repair rate for the primary failure. If the primary failure is the failure of a component, then $\lambda(t)$ and $\mu(t)$ are termed the component failure rate and component repair rate, respectively. For any reliability or fault tree study, the quantities $\lambda(t)$ and $\mu(t)$, or their equivalent, must be known for every primary failure of the fault tree. Extensive tabulations of $\lambda(t)$ and $\mu(t)$ have been obtained for a wide variety of failures [4, 7], and it will be assumed that $\lambda(t)$ and $\mu(t)$, or their equivalents, are known for every primary failure of the fault tree.

From $\lambda(t)$ and $\mu(t)$, other probabilistic quantities may be obtained which quantify, or characterize, the particular primary failure. The probability of the primary failure first occurring in time t to $t + dt$ given it is not existing at time t', $a(t', t)\,dt$, is

$$a(t', t)\,dt = \exp\left[-\int_{t'}^{t} \lambda(t'')\,dt''\right]\lambda(t)\,dt\,; \qquad t' \leqslant t\,. \tag{3}$$

From eq. (3), the probability that the primary failure does not occur from time t' to t, $f(t', t)$, is simply

$$f(t', t) = \exp\left(-\int_{t'}^{t} \lambda(t'')\,dt''\right); \quad t' \leqslant t\,. \tag{4}$$

With regard to repair, the probability that the primary failure is repaired at time t to $t + dt$, given it is existing at time t', $b(t', t)\,dt$, is

$$b(t', t)\,dt = \exp\left[-\int_{t'}^{t} \mu(t'')\,dt''\right] \mu(t)\,dt \;; \quad t' \leqslant t \,. \tag{5}$$

The quantities $a(t', t)$ and $b(t', t)$ are termed the first occurrence distribution (or first failure distribution) and the repair distribution, respectively. The term $f(t', t)$ is called the non-occurrence or non-failure probability. The quantities $\lambda(t)$ and $\mu(t)$, and the quantities $a(t', t)$, $b(t', t)$ and $f(t', t)$ which are directly derived from $\lambda(t)$ and $\mu(t)$ will all be termed primary failure data.

Besides the above, there are two other primary failure characteristics which are essential for any reliability study or fault tree evaluation. The first characteristic is the primary failure intensity $w(t)$, which is defined such that

$$w(t) = \text{the expected number of times the primary failure occurs at time } t \text{ per unit time.} \tag{6}$$

From the definition of $w(t)$, the expected number of times the primary failure occurs in any interval from t' to t, $w(t', t)$, is thus

$$w(t', t) = \int_{t'}^{t} w(t'')\,dt'' \,. \tag{7}$$

The quantity $w(t)\,dt$ is the expected number of times the failure occurs in time t to $t + dt$; the failure must not exist at time t and then must occur in the interval dt.

From hereon, assume the initial condition that at $t = 0$ the primary failure does not exist. An equation for $w(t)$ in terms of the data for the primary failure can then be readily obtained from balance considerations;

$$w(t) = a(0, t) + \int_{0}^{t} dt'' w(t'') \int_{t''}^{t} dt' b(t'', t')\, a(t', t). \tag{8}$$

The first term on the right hand side of eq. (8) is the contribution to $w(t)$ from the first occurrence of the primary failure. The second term is the contribution to $w(t)$ from the failure occurring at time t'', being repaired at t', and then reoccurring at time t.

For a specific first occurrence distribution $a(t', t)$ and repair distribution $b(t', t)$, eq. (8) thus determines the primary failure intensity $w(t)$. For the case of the failure being non-repairable, for example, $b(t', t) \equiv 0$ and eq. (8) becomes

$$w(t) = a(0, t) \;; \text{ non-repairable primary failure} \,. \tag{9}$$

In general, eq. (8) can be solved using Laplace transform techniques, or simple numerical integration techniques can be used.

The second primary failure characteristic of interest is the primary failure existence probability $q(t)$;

$$q(t) = \text{the probability of the primary failure existing at time } t. \tag{10}$$

The non-existence probability, or the probability of the primary failure not existing at time t is merely $1 - q(t)$. From the definition of $\lambda(t)$, eq. (1), and $w(t)$, eq. (6), it is apparent that

$$w(t) = [1 - q(t)]\ \lambda(t) \,, \tag{11}$$

or

$$q(t) = 1 - \frac{w(t)}{\lambda(t)} \,. \tag{12}$$

For a specific failure intensity $w(t)$ and failure rate $\lambda(t)$, $q(t)$ is simply obtainable from eq. (12).

The quantities $w(t)$ and $q(t)$, along with the basic data $\lambda(t)$, $\mu(t)$, $a(t', t)$, $b(t', t)$ and $f(t', t)$, are definitive functions which characterize the probabilistic behavior of the primary failure for all time. From the primary failure's basic data, $w(t)$ and $q(t)$ can be simply obtained for every primary failure of the fault tree. This merely requires using the pertinent data in eqs. (8) and (12) for each primary failure. The characteristics $w(t)$ and $q(t)$, obtained for every primary failure, are important in themselves since they show the effects of repair, maintenance, and changes in environment (phases) and show these effects as functions of time. Moreover, with $w(t)$ and $q(t)$ determined for all the primary failures of the fault tree, the probabilistic characteristics for the mode failures and for the top failure can be obtained.

3. Mode failure information

As stated previously, a mode failure, or critical path, is a smallest set of primary failures such that if all these primary failures exist at time t the mode failure (and top failure) exists at time t. Because a mode failure is simply a "compounded" type of failure, the same probability characteristics which were obtained for a primary failure can be obtained for the mode failure.

Consider a particular mode failure. Let it consist of n primary failures and let these constituent primary failures be designated with indices from 1 through n. Assume the primary failures are independent and at $t = 0$ they all do not exist. The first characteristic obtained for the mode failure will be the mode failure existence probability $Q(t)$;

$$Q(t) = \text{the probability that the mode failure exists at time } t. \tag{13}$$

Since the mode failure exists at time t if and only if all its primary failures exist at time t,

$$Q(t) = \prod_{j=1}^{n} q_j(t), \tag{14}$$

where $q_j(t)$ is the existence probability for the jth primary failure of the mode failure (eq. (12)). The mode failure non-existence probability, $P(t)$, is then just $1 - Q(t)$ and is the probability of the mode failure not existing at time t; in terms of the constituent primary failures, $P(t)$ is the probability of one or more of these primary failures not existing at time t. Equation (14) allows $Q(t)$, or $P(t)$, to be simply determined from the primary failure information.

The existence probability $Q(t)$ is of significance to the top failure to which the particular mode failure contributes. If the mode failure exists at time t then the top failure exists at time t. $Q(t)$ is consequently the probability that the top failure exists at time t by means of this particular mode failure existing at time t. Examination of the $Q(t)$ for all the mode failures (critical paths) of the fault tree will yield those critical mode failures by which the top failure is most likely to exist.

The mode failure rate $\Lambda(t)$ is defined in the same way as for a primary failure;

$$\Lambda(t)\,\mathrm{d}t = \text{the probability of the mode failure occurring in time } t \text{ to } t + \mathrm{d}t \text{ given the mode failure does not exist at time } t. \tag{15}$$

If

$$u_t \equiv \text{the event of the mode failure not existing at time } t \tag{16}$$

and

$$d_{t+\mathrm{d}t} \equiv \text{the event of the mode failure existing at time } t + \mathrm{d}t, \tag{17}$$

then

$$\Lambda(t)\,\mathrm{d}t = \mathcal{P}(d_{t+\mathrm{d}t}/u_t). \tag{18}$$

The symbol "$\mathcal{P}$" denotes the probability of an event and the symbol "/" denotes the probabilistic given condition. Eq. (18) merely states that, given it does not exist at time t, the mode failure occurs in t to $t + \mathrm{d}t$ if and only if it is existing at time $t + \mathrm{d}t$. From basic probability theory, eq. (18) may be written as

$$\Lambda(t)\,\mathrm{d}t = \frac{\mathcal{P}(d_{t+\mathrm{d}t}\,u_t)}{\mathcal{P}(u_t)}, \tag{19}$$

where a product of events denotes their intersection, or simultaneous occurrence.

For the event $d_{t+\mathrm{d}t}u_t$ to occur, one or more of the primary failures must not exist at time t and these primary failures not existing must all simultaneously occur between time t to $t + \mathrm{d}t$. Validly neglecting orders of $\mathrm{d}t$ greater than or equal to two, $\mathcal{P}(d_{t+\mathrm{d}t}u_t)$ is thus

$$\mathcal{P}(d_{t+\mathrm{d}t}u_t) = \sum_{j=1}^{n} w_j(t)\,\mathrm{d}t \prod_{\substack{l=1 \\ l\neq j}}^{n} q_l(t). \tag{20}$$

Each term in the above summation is the probability of the jth primary failure occurring in t to $t + \mathrm{d}t$ ($w_j(t)\,\mathrm{d}t$) with the remaining primary failures already existing at time t. Because primary failures occurring in a time interval $\mathrm{d}t$ are considered, only one primary failure can occur and combinations of more than one primary failure simultaneously occurring can be validly neglected.

The mode failure rate $\Lambda(t)$ is thus obtained since

$$\mathcal{P}(u_t) = 1 - Q(t)\,, \tag{21}$$

where $Q(t)$ is the mode existence probability. Eq. (19) therefore becomes

$$\Lambda(t)\,\mathrm{d}t = \frac{\sum_{j=1}^{n} w_j(t)\,\mathrm{d}t \prod_{\substack{l=1 \\ l\neq j}}^{n} q_l(t)}{1 - Q(t)} \tag{22}$$

or

$$\Lambda(t) = \frac{\sum_{j=1}^{n} w_j(t) \prod_{\substack{l=1 \\ l\neq j}}^{n} q_l(t)}{1 - Q(t)}\,. \tag{23}$$

By use of eq. (23) the mode failure rate is thus readily obtained from the constituent primary failure information.

From the mode failure rate $\Lambda(t)$, the first occurrence distribution for the mode failure, $A(t', t)$, can be expressed in an analogous manner as for a primary failure;

$$A(t', t) = \exp\left[-\int_{t'}^{t} \Lambda(t'')\,\mathrm{d}t''\right]\,\Lambda(t)\,; \quad t' \leqslant t\,. \tag{24}$$

$A(t', t)\,\mathrm{d}t$ is the probability that the mode failure first occurs at time t to $t + \mathrm{d}t$ given it is not existing at time t'. As for a primary failure, the non-occurrence probability for the mode failure $F(t', t)$ is

$$F(t', t) = \exp\left[-\int_{t'}^{t} \Lambda(t'')\,\mathrm{d}t''\right]\,; \quad t' \leqslant t\,, \tag{25}$$

and is the probability of the mode failure not occurring in the interval from t' to t. The probability that the mode failure occurs in this interval is simply $1 - F(t', t)$. $A(t', t)$ and $F(t', t)$ (or $1 - F(t', t)$) are important characteristics since they aid in determining the most critical mode failures, those which are most likely to occur and cause the top failure to occur.

The remaining quantity of interest characterizing the mode failure is termed the mode failure intensity $W(t)$;

$$W(t) = \text{the expected number of times the mode failure occurs at time } t \text{ per unit time.} \tag{26}$$

The integral of $W(t)$ over any time interval from t' to t is thus the expected number of times the mode failure occurs in this time interval. The mode failure intensity $W(t)$ is immediately determined from the definition of the existence probability $Q(t)$ and the failure rate $\Lambda(t)$;

$$W(t) = [1 - Q(t)]\,\Lambda(t)\,. \tag{27}$$

The mode failure can occur in t to $t + \mathrm{d}t$ only if it does not exist at time t and it then occurs in $\mathrm{d}t$. Substituting eq. (23) into eq. (27) yields $W(t)$ in terms of the constituent primary failure information,

$$W(t) = \sum_{j=1}^{n} w_j(t) \prod_{\substack{l=1 \\ l\neq j}}^{n} q_l(t)\,. \tag{28}$$

The quantities $Q(t)$, $\Lambda(t)$, and $W(t)$, which characterize the mode failure are thus all simply determinable from the characteristics $w(t)$ and $q(t)$ of the primary failures which comprise the mode failure. The probabilistic characteristics for the mode failure are important in themselves since they quantify each mode failure as functions of time. They show the effects of repair, maintenance and environmental conditions on the particular mode failure, or critical path. The characteristics can be simply determined for every mode failure of the fault tree by using in eqs. (14), (23) and (28), the appropriate primary failures which are members of each mode failure. In doing so, the critical mode failures, those which are most likely to cause the top failure to occur, will be determined, and any corrective action will consequently be directed toward these critical mode failures. Besides being important in themselves and yielding the critical mode failures, the mode failure characteristics are important since they lead to the determination of the characteristics of the top failure of the fault tree.

4. Top failure information

Before venturing into the evaluation of the probabilistic characteristics of the top failure of the fault tree, some general probability relationships must first be established. Let $\bigcup_{i=1}^{n} A_i$ denote the union of the n events A_i, and let $A_1, A_2, \ldots, A_m$ denote the intersection of the m events. Then, from basic probability theory [10],

$$\mathcal{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \mathcal{P}(A_i) - \sum_{i=2}^{n}\sum_{j=1}^{i-1} \mathcal{P}(A_i A_j) + \sum_{i=3}^{n}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} \mathcal{P}(A_i A_j A_k) - \ldots + (-1)^{n-1} \mathcal{P}(A_1 A_2 \ldots A_n), \tag{29}$$

where the symbol "$\mathcal{P}$" again denotes the probability of an event. As depicted in eq. (29), the probability of a union of events involves the probabilities of all the various combinations of the intersections of the events. It is also shown in basic probability theory that if these intersections are taken into account such that intersections of an increasing number of events are successively considered, then successive upper and lower bounds are obtained for $\mathcal{P}(\bigcup_{i=1}^{n} A_i)$ until, finally, its exact value is reached [10].

$$\mathcal{P}\left(\bigcup_{i=1}^{n} A_i\right) \leqslant \sum_{i=1}^{n} \mathcal{P}(A_i), \tag{30}$$

$$\mathcal{P}\left(\bigcup_{i=1}^{n} A_i\right) \geqslant \sum_{i=1}^{n} \mathcal{P}(A_i) - \sum_{i=2}^{n}\sum_{j=1}^{i-1} \mathcal{P}(A_i A_j), \tag{31}$$

$$\mathcal{P}\left(\bigcup_{i=1}^{n} A_i\right) \leqslant \sum_{i=1}^{n} \mathcal{P}(A_i) - \sum_{i=2}^{n}\sum_{j=1}^{i-1} \mathcal{P}(A_i A_j) + \sum_{i=3}^{n}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} \mathcal{P}(A_i A_j A_k)$$

$$\vdots$$

etc. (32)

Eq. (30) is generally the most useful for determining an upper bound for $\mathcal{P}(\bigcup_{i=1}^{n} A_i)$. If, however, the contributions from successively greater intersections become increasingly smaller, then the successive upper and lower bounds, eqs. (31), (32), etc., will approach each other, and the "bracketing" or "enveloping" of the true probability will become increasingly tighter. The upper bounds, eqs. (30), (32), etc., will become successively smaller in value and will approach the lower bounds, eqs. (31), etc., which successively grow in value. When applicable, this successive bracketing of $\mathcal{P}(\bigcup_{i=1}^{n} A_i)$ is a useful method of converging to its true value.

With these preliminary relationships established, the evaluation of the characteristics for the top failure may proceed. Assume the mode failures (critical paths) of the fault tree are known, and let there be N such mode failures. Let these mode failures be indexed from 1 to N. Assume also the initial condition that at $t = 0$ all the primary failures of the fault tree are non-existent. The top failure characteristic most simply obtained is the top failure existence probability $Q_0(t)$;

$$Q_0(t) = \text{the probability that the top failure exists at time } t. \tag{33}$$

The complement of this quantity, $1 - Q_0(t)$, is the probability that the top failure is not existing at time t and is sometimes termed the availability of the system.

Let

$$d_i = \text{the event that the } i\text{th mode failure exists at time } t. \tag{34}$$

From eq. (13),

$$\mathcal{P}(d_i) = Q_i(t), \tag{35}$$

where $Q_i(t)$ is the ith mode failure existence probability, which is simply determined from eq. (14), where the primary failures in this equation are those comprising the ith mode failure. Since the top failure exists if and only if one or more of the mode failures exist

$$Q_0(t) = \mathcal{P}\left(\bigcup_{i=1}^{N} d_i\right). \tag{36}$$

Using the expansion relationship, eq. (29), eq. (36) may be written as

$$Q_0(t) = \sum_{i=1}^{N} \mathcal{P}(d_i) - \sum_{i=2}^{N} \sum_{j=1}^{i-1} \mathcal{P}(d_i d_j)$$

$$+ \ldots + (-1)^{N-1} \mathcal{P}(d_1 d_2 \ldots d_N) . \quad (37)$$

Consider a general event $d_1 d_2 \ldots d_m$, i.e., the simultaneous existence of the m mode failures. Since the primary failures are assumed independent and since a mode failure exists if and only if all its primary failures exist,

$$\mathcal{P}(d_1 d_2 \ldots d_m) = \prod^{+1,\ldots,m} q(t) . \quad (38)$$

The product symbol is defined such that

$$\prod^{+1,\ldots,m} = \text{the product of unique primary failure quantities where the primary failure occurs in at least one of the mode failures } 1, \ldots, m. \quad (39)$$

A particular primary failure quantity thus occurs at most only once in the product and occurs only if the primary failure is a member of at least one of the mode failures denoted above the product symbol. Computation of $\mathcal{P}(d_1 \ldots d_m)$, eq. (38), therefore simply consists of collecting the unique primary failures which are members of one or more of the m mode failures (with indices $1, \ldots, m$) and then multiplying the existence probabilities $q(t)$ of these primary failures. From eq. (38), eq. (37) thus becomes

$$Q_0(t) = \sum_{i=1}^{N} Q_i(t) - \sum_{i=2}^{N} \sum_{j=1}^{i-1} \prod^{+i,j} q(t)$$

$$+ \ldots + (-1)^{N-1} \prod^{+1,\ldots,N} q(t) . \quad (40)$$

The exact value for $Q_0(t)$ can be straightforwardly determined by using eq. (40) since the products involved (eq. (38)) can be computed by a simple collection of the unique primary failures in the mode failures denoted above the product sign. Following this collection, a simple multiplication of the existence probabilities $q(t)$ is made. This is particularly rapid when programmed for a computer. For a fault tree with a smaller number of mode failures, or critical paths, eq. (40) will thus yield $Q_0(t)$ in a reasonable amount of time. Further, for a large class of primary failure data, the primary failure existence probabilities $q(t)$ and hence $Q_0(t)$ reach "steady state", constant values very quickly. Therefore, for these situations, $Q_0(t)$ need only be calculated as a function of time until it assumes its respective steady state value, or this steady state value can only be calculated using the steady state values for the $q(t)$ of the primary failures.

For primary failure existence probabilities, $q(t)$, much less than 1, which is generally the case, the bracketing procedure (eqs. (30), (31), (32), etc.) is a particularly efficient method of obtaining successively tighter envelopes for $Q_0(t)$. As the bracketing procedure is applied to eq. (40), $Q_0(t)$ is less than or equal to the first term on the right hand side, is greater than or equal to the first two terms, and so forth:

$$Q_0(t) \leqslant \sum_{i=1}^{N} Q_i(t) , \quad (41)$$

$$Q_0(t) \geqslant \sum_{i=1}^{N} Q_i(t) - \sum_{i=2}^{N} \sum_{j=1}^{i-1} \prod^{+i,j} q(t) , \quad (42)$$

$$\vdots$$

etc.

The contribution from each successive term involves a larger number of factors of $q(t)$ in the product. Therefore, for $q(t) \ll 1$, these successive terms become rapidly smaller and can be regarded as higher order correction terms. For fault trees with many mode failures, or critical paths, the bracketing can be carried out only as far as deemed necessary, giving tight envelopes for $Q_0(t)$ in a reasonable time; in fact, the first two brackets, eqs. (41) and (42), are usually within three significant figures of one another, giving a tight enough envelope for most computations.

For those situations in which a simple but accurate approximation is desired for $Q_0(t)$, use may be made of a relationship determined by Esary and Proschan [5]. In their paper, Esary and Proschan show that

$$\mathcal{P}(f_1=0, f_2=0, \ldots, f_m=0) \geq \prod_{i=1}^{m} \mathcal{P}(f_i=0) , \quad (43)$$

where the f_i consists of products of certain independent binary random variables (i.e., the random variables can only assume values of 1 or 0).

Let

$$u_i = \text{the event if the } i\text{th mode failure not existing at time } t, \quad (44)$$

where from the definition of the mode failure existence probability, eq. (13),

$$\mathcal{P}(u_i) = 1 - Q_i(t) . \quad (45)$$

Taking the complement of eq. (36),

$$1 - Q_0(t) = \mathcal{P}(u_1 u_2 \ldots u_N) ; \quad (46)$$

the top failure does not exist at time t if and only if no mode failure exists at time t. Assign binary random variables to each primary failure such that the variable equals 1 when the failure exists and equals 0 when it does not exist. The event u_i then corresponds to the event $f_i = 0$ where f_i is the product of the binary random variables of the primary failures which are members of the ith mode failure. Therefore, eq. (43) may be applied to the probability $\mathcal{P}(u_1 u_2 \ldots u_N)$ to obtain,

$$\mathcal{P}(u_1 u_2 \ldots u_N) \geq \prod_{i=1}^{N} \mathcal{P}(u_i) , \quad (47)$$

or

$$\mathcal{P}(u_1 u_1 \ldots u_N) \geq \prod_{i=1}^{N} (1 - Q_i(t)) . \quad (48)$$

Substitution of eq. (46) into eq. (48) results in the relationship desired;

$$Q_0(t) \leq 1 - \prod_{i=1}^{N} (1 - Q_i(t)) . \quad (49)$$

Eq. (49) gives an upper bound and hence a safe and conservative estimate for $Q_0(t)$. As the mode existence probabilities $Q_i(t)$ can be simply determined from eq. (14), this upper bound can be simply obtained for fault trees with any number of mode failures. Moreover, eq. (49) would be an exact equality if the mode failures had no primary failures in common, or equivalently if the events u_i were independent. If the mode existence probabilities $Q_i(t)$ are much less than 1, which is the usual case, then the events u_i are very nearly independent since the probabilities $\mathcal{P}(u_i) = 1 - Q_i(t)$, for all i, are approximately equal to 1. In fact, as the $Q_i(t)$ approach 0, the upper bound given by the right hand side of eq. (49) approaches the true value of $Q_0(t)$. In general, therefore, eq. (49) gives an accurate and also conservative approximation for $Q_0(t)$.

Having obtained $Q_0(t)$, the characteristic next determined is the top failure intensity, $W_0(t)$;

$$W_0(t) = \text{the expected number of times the top failure occurs at time } t \text{ per unit time.} \quad (50)$$

$W_0(t)\,\mathrm{d}t$ is the expected number of times the top failure occurs in t to $t + \mathrm{d}t$, and the integral of $W_0(t)$ from t_1 to t_2 is the expected number of times the top failure occurs in this particular interval of time. Let

$$\theta_i = \text{the event of the } i\text{th mode failure occurring in time } t \text{ to } t + \mathrm{d}t. \quad (51)$$

From eq. (26)

$$\mathcal{P}(\theta_i) = W_i(t)\,\mathrm{d}t , \quad (52)$$

where $W_i(t)$ is the ith mode failure intensity.

For the top failure to occur in t to $t + \mathrm{d}t$, all the mode failures must not exist at time t and then one or more of the mode failures must occur in t to $t + \mathrm{d}t$. Hence,

$$W_0(t)\,\mathrm{d}t = \mathcal{P}[A \cap \bigcup_{i=1}^{N} \theta_i] , \quad (53)$$

where $\bigcup_{i=1}^{N} \theta_i$ is the event of one or more of the θ_i occurring and A is the event of all the mode failures not existing at time t. From eq. (44),

$$A = u_1 u_2 \ldots u_N , \quad (54)$$

where u_i is the event of the ith mode failure not existing at time t. A product of events, as in eq. (54), again denotes their intersection (simultaneous occurrence). From basic probability theory,

$$\mathcal{P}[A \bigcup_{i=1}^{N} \theta_i] = \mathcal{P}[\bigcup_{i=1}^{N} \theta_i] - \mathcal{P}[B \bigcup_{i=1}^{N} \theta_i] , \quad (55)$$

where B is the event of one or more of the mode failures existing at time t;

$$B = \bigcup_{j=1}^{N} d_j . \quad (56)$$

The event d_j is the event of the jth mode failure existing at time t (eq. (34)). The expression for the top failure intensity $W_0(t)$ therefore becomes

$$W_0(t)\,\mathrm{d}t = \mathcal{P}[\bigcup_{i=1}^{N} \theta_i] - \mathcal{P}[B \bigcup_{i=1}^{N} \theta_i] . \quad (57)$$

Eq. (57) is readily understood from consideration of the individual terms on the right hand side. The first contribution to $W_0(t)\,\mathrm{d}t$, $\mathcal{P}[\bigcup_{i=1}^{N} \theta_i]$, is the contribution from one or more of the mode failures occurring. Whenever a mode failure occurs, the top failure occurs. However, the second term $\mathcal{P}[B \bigcup_{i=1}^{N} \theta_i]$ must be subtracted from $\mathcal{P}[\bigcup_{i=1}^{N} \theta_i]$. This term accounts for those cases in which one or more mode failures occur while other mode failures are already existing. The top failure cannot occur in these cases since it is already existing (i.e., has occurred at an earlier time and was not repaired).

Consider the first term on the right-hand side of eq. (57). Using the expansion relationship, eq. (29),

$$\mathcal{P}[\bigcup_{i=1}^{N} \theta_i] = \sum_{i=1}^{N} \mathcal{P}[\theta_i] - \sum_{i=2}^{N} \sum_{j=1}^{i-1} \mathcal{P}[\theta_i \theta_j] + \ldots + (-1)^{N-1} \mathcal{P}[\theta_1 \theta_2 \ldots \theta_N] . \quad (58)$$

The first term on the right hand side of this equation is simply the contribution from an individual mode failure occurring (eq. (52)). The second and proceeding terms involve the simultaneous occurrence of two or more mode failures; the mode failures considered in the particular combinations must all not exist at time t and then must all simultaneously occur in t to $t + \mathrm{d}t$.

The probability of one primary failure occurring in t to $t + \mathrm{d}t$ is equal to $w(t)\,\mathrm{d}t$ and hence is proportional to $\mathrm{d}t$. The simultaneous occurrence of two or more mode failures can thus only be caused by one primary failure occurring, and moreover this primary failure must be a common member of all those mode failures which must simultaneously occur. Consider the general event $\theta_1 \theta_2 \ldots \theta_m$, i.e., the simultaneous occurrence of the m mode failures. Let there be k unique primary failures which are common members to all of the m mode failures; each of these primary failures must be a member of every one of the mode failures $1, \ldots, m$. If k is zero, then the event $\theta_1 \theta_2 \ldots \theta_m$ cannot occur and its associated probability is zero. Assume, therefore, k is greater than zero.

If one of these k primary failures does not exist at t and then occurs in t to $t + \mathrm{d}t$, and all the other primary failures of the m mode failures exist at t (including the $k - 1$ common primary failures) then the event $\theta_1 \ldots \theta_m$ will occur. The probability of the event $\theta_1 \ldots \theta_m$ is thus seen to be

$$\mathcal{P}[\theta_1 \ldots \theta_m] = W(t; 1, \ldots, m)\,\mathrm{d}t \prod_{\cdot}^{+1,\ldots,m} q(t) . \quad (59)$$

The product symbol in eq. (59) is defined such that

$$\prod_{\cdot}^{+1,\ldots,m} = \text{the product of unique primary failure quantities where the primary failure occurs in at least one of the mode failures } 1, \ldots, m \text{ but is not a common member in all of them.} \quad (60)$$

The product in eq. (59) is therefore the product of the existence probabilities of those primary failures other than the k common primary failures. Also, a primary failure existence probability occurs only once in the product even though it is a member of two or more mode failures (it cannot be a member of all m mode failures since these are the k common primary failures).

The quantity $W(t; 1, \ldots, m)\,\mathrm{d}t$ accounts for the k

common primary failures and is defined such that

$W(t; 1, ..., m)$ = the failure intensity for a mode failure which has as its primary failures the primary failures which are common members to all the mode failures $1, ..., m$. (61)

If the m mode failures have no primary failures common to all of them, then $W(t; 1, ..., m)$ is defined to be identically zero;

$W(t; 1, ..., m) = 0$, no primary failures common to all m mode failures. (62)

Examination of the expression for a mode failure intensity, eq. (28), shows that the intensity consists of one primary failure occurring and the other primary failures already existing. This is precisely what is needed for the k common primary failures. Computation of $W(t; 1, ..., m)$ therefore consists of considering the k common primary failures as being members of a mode failure and using eq. (28) to calculate $W(t; 1, ..., m)$, the failure intensity for this "mode failure".

Computation of the probability of m mode failures simultaneously occurring, eq. (59), is therefore quite direct. The unique primary failures which are members of any of the m mode failures are first separated into two groups, those which are common to all m mode failures and those which are not common to all the mode failures. Those primary failures which are not common are those which do not appear in every mode failure. A particular primary failure thus occurs in only one group and occurs only once in this group. The common group is considered as a mode failure in itself and $W(t; 1, ..., m)$ is computed for this group directly from eq. (28). If there are no primary failures in this common group, then $W(t; 1, ..., m)$ is identically zero and computation need proceed no further ($\mathcal{P}[\theta_1 ... \theta_m] = 0$). For the non-common group, the product of the existence probabilities for the member primary failures is computed. This product and $W(t; 1, ..., m)$ are multiplied, and with the additional factor of dt, $\mathcal{P}[\theta_1 ... \theta_m]$ is obtained. As will be seen, the factor dt will "cancel out" in the final expression and will not be needed.

With the general term $\mathcal{P}[\theta_1 ... \theta_m]$ being determined, eq. (58) which gives the first term for $W_0(t)dt$ is subsequently determined.

$$\mathcal{P}[\bigcup_{i=1}^{N} \theta_i] = \sum_{i=1}^{N} W_i(t)\,dt - \sum_{i=2}^{N}\sum_{j=1}^{i-1} W(t; i, j)\,dt \times \prod_{\cdot}^{+i,j} q(t) + \sum_{i=3}^{N}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} W(t; i, j, k)\,dt \prod_{\cdot}^{+i,j,k} q(t) \cdot + (-1)^{N-1} W(t; 1, ..., N)\,dt \prod^{+1,...,N} q(t) . \quad (63)$$

The first term on the right hand side of this equation is simply the sum of the failure intensities of the individual mode failures. Each product in the remaining terms consists of separating the common and uncommon primary failures for the particular combination of mode failures and then performing the operations as described in the preceding paragraph. The operations can be rapidly performed by a computer. Moreover, each succeeding term on the right hand side of eq. (63) consists of combinations of a larger number of mode failures simultaneously occurring and in turn consists of a larger number of products of $q(t)$. Therefore, each succeeding term rapidly decreases in value, and as will be elaborated later, the bracketing procedure is extremely efficient when applied to eq. (63).

Eq. (63) consequently determines the first term for $W_0(t)\,dt$, eq. (57), and the second term $\mathcal{P}[B \bigcup_{i=1}^{N} \theta_i]$ must now be determined. Expanding this second term yields

$$\mathcal{P}[B \bigcup_{i=1}^{N} \theta_i] = \sum_{i=1}^{N} \mathcal{P}[\theta_i B] - \sum_{i=2}^{N}\sum_{j=1}^{i-1} \mathcal{P}[\theta_i \theta_j B] + ... + (-1)^{N-1} \mathcal{P}[\theta_1 \theta_2 ... \theta_N B] , \quad (64)$$

where again

$$B = \bigcup_{j=1}^{N} d_j . \quad (56)$$

Consider a general term in this expansion, $\mathcal{P}[\theta_1 ... \theta_m B]$

$\mathcal{P}[\theta_1 \ldots \theta_m B]$ is the probability of the m mode failures simultaneously occurring in t to $t + \mathrm{d}t$ with one or more of the other mode failures already existing at time t (event B). Let

$$W_B(t; 1, \ldots, m)\, \mathrm{d}t = \mathcal{P}[\theta_1 \ldots \theta_m B] \,, \tag{65}$$

where

$W_B(t; 1, \ldots, m)$ = the rate of occurrence of the m mode failures $1, \ldots, m$ simultaneously occurring at t with one or more of the other mode failures already existing at time t. (66)

The term "rate of occurrence" simply means "probability per unit time". The term $W_B(t; 1, \ldots, m)$ should not be confused with the term $W(t; 1, \ldots, m)$ of eq. (61). $W_B(t; 1, \ldots, m)$ is simply used for ease of notation and refers to the entire event $\theta_1 \ldots \theta_m B$ occurring while $W(t; 1, \ldots, m)$ refers to the common primary failures of the modes $1, \ldots, m$ occurring. With the notation of eq. (65), eq. (64) may be rewritten as

$$\mathcal{P}[B \bigcup_{i=1}^{N} \theta_i] = \sum_{i=1}^{N} W_B(t; i)\, \mathrm{d}t - \sum_{i=2}^{N} \sum_{j=1}^{i-1} W_B(t; i, j)\, \mathrm{d}t + \ldots + (-1)^{N-1} W_B(t; 1, \ldots, N)\, \mathrm{d}t. \tag{67}$$

Since the event B involves a union, the general term in eq. (67) may be expanded into the form

$$W_B(t; 1, \ldots, m)\, \mathrm{d}t = \sum_{i=1}^{N} \mathcal{P}[\theta_1, \ldots, \theta_m d_i] - \sum_{i=2}^{N} \sum_{j=1}^{i-1} \mathcal{P}[\theta_1 \ldots \theta_m d_i d_j] + \ldots + (-1)^{N-1} \mathcal{P}[\theta_1 \ldots \theta_m d_1 d_2 \ldots d_N] \,, \tag{68}$$

where d_i is the event of the ith mode failure existing at t. Consider now a general term in this expansion, $\mathcal{P}[\theta_1 \ldots \theta_m d_1 \ldots d_n]$. If this term is determined then $W_B(t; 1, \ldots, m)\, \mathrm{d}t$ will be determined and hence $\mathcal{P}[B \bigcup_{i=1}^{N} \theta_i]$ will be determined.

The event $\theta_1 \ldots \theta_m d_1 \ldots d_n$ is similar to the event $\theta_1 \ldots \theta_m$ previously analyzed with the exception that now the mode failures $1, \ldots, n$ must also exist at time t. If a mode failure exists at time t all its primary failures must exist at time t, and these primary failures cannot occur in t to $t + \mathrm{d}t$ since an occurrence calls for a non-existence at t and then an existence at $t + \mathrm{d}t$. The expression for $\mathcal{P}[\theta_1 \ldots \theta_m d_1 \ldots d_n]$ is therefore analogous to the previous expression for $\mathcal{P}[\theta_1 \ldots \theta_m]$ (eq. (59)) with one alteration. Those primary failures common to all the m mode failures $1, \ldots, m$, which are also in any of the n mode failures $1, \ldots, n$, cannot contribute to $W(t; 1, \ldots, m)$ since they must already exist at time t (for the event $d_1 \ldots d_n$). Hence, these primary failures, common to all m mode failures and also in any of the n mode failures, must be deleted from $W(t; 1, \ldots, m)$ and must be incorporated in the product of primary failure existence probabilities

$$\prod_{+1, \ldots, m} q(t) \,.$$

It is therefore seen that $\mathcal{P}[\theta_1 \ldots \theta_m d_1 \ldots d_n]$ can be expressed as

$$\mathcal{P}[\theta_1 \ldots \theta_m d_1 \ldots d_n] = W(t; 1, \ldots, m-1, \ldots, n)\, \mathrm{d}t \prod_{1, \ldots, m}^{1, \ldots, n} q(t) \,. \tag{69}$$

The failure intensity $W(t; 1, \ldots, m-1, \ldots, n)$ is defined such that

$W(t; 1, \ldots, m-1, \ldots, n)$

= the failure intensity for a mode failure which has as its primary failures the primary failures common to all m mode failures $1, \ldots, m$ deleted from which are those primary failures also in any of the mode failures $1, \ldots, n$. (70)

If there are no such primary failures, then $W(t; 1, ..., m-1, ..., n)$ is defined to be identically zero;

$$W(t; 1, ..., m-1, ..., n) = 0, \quad \text{no primary failures common to all the mode failures } 1, ..., m \text{ and also not in any of the mode failures } 1, ..., n. \tag{71}$$

The computation of $W(t; 1, ..., m-1, ..., n)$ is again straightforward. As before, the primary failures common to all m mode failures $1, ..., m$ are first obtained. From this group are deleted those primary failures also in any of the mode failures $1, ..., n$. This remaining group of primary failures, those in all m mode failures and not in any of the n mode failures, is considered a mode failure and eq. (28) is used to directly compute $W(t; 1, ..., m-1, ..., n)$ for this "mode failure".

The product symbol in eq. (69) is defined such that

$$\prod_{1, ..., m}^{1, ..., n} = \text{the product of unique primary failure quantities, where the primary failure is a member of any of the mode failures } 1, ..., n \text{ or is a member of the mode failures } 1, ..., m, \text{ but is not a common member of these } m \text{ mode failures.} \tag{72}$$

The product is simply a product of primary failure quantities for those primary failures which are members of any of the mode failures $1, ..., m$ or $1, ..., n$ deleted from which are those primary failures used for $W(t; 1, ..., m-1, ..., n)$. In case of eq. (69), the product involves primary failure existence probabilities.

The computation $\mathcal{P}[\theta_1 ... \theta_m d_1 ... d_n]$ is therefore straightforward. All the unique primary failures which are in any of these $m+n$ mode failures are first collected. If a primary failure occurs in more than one mode failure it still only appears once in this collection. From this collection are removed those primary failures used for $W(t; 1, ..., m-1, ..., n)$, i.e., those primary failures only in the m mode failures which are also common to all of them. If there are no such primary failures, then $W(t; 1, ..., m-1, ..., n)$ is identically zero and computation need proceed no further, ($\mathcal{P}[\theta_1 ... \theta_m d_1 ... d_n] = 0$). If there exists a group of such primary failures, then this group is considered a mode failure in itself and eq. (28) is used directly to calculate its failure intensity $W(t; 1, ..., m-1, ..., n)$. The existence probabilities of the remaining primary failures in the original collection are then simply multiplied together. This product is multiplied by $W(t; 1, ..., m-1, ..., n)$, and with an additional factor of dt, then gives $\mathcal{P}[\theta_1 ... \theta_m d_1 ... d_n]$. As will be seen the factor dt becomes unnecessary in the final computation. The computation can be rapidly performed by a computer, and as will be seen, is extremely efficient since the bracketing procedure can be used.

With the general term $\mathcal{P}[\theta_1 ... \theta_m d_1 ... d_n]$ determined, $W_B(t; 1, ..., m)\, dt$ of eq. (68) is consequently determined;

$$W_B(t; 1, ..., m)\, dt = \sum_{i'=1}^{N} W(t; 1, ..., m-i')\, dt \prod_{1, ..., m}^{i'} q(t) - \sum_{i'=2}^{N} \sum_{j'=1}^{i'-1} W(t; 1, ..., m-i', j')\, dt \prod_{1, ..., m}^{i', j'} q(t) + ... \tag{73}$$

Each term for $\mathcal{P}[B \cup_{i=1}^{N} \theta_i]$ in eq. (67) is thus determined and can be expressed as

$$W_B(t; i_1, ..., i_n) = \sum_{i'=1}^{N} W(t; i_1, ..., i_n - i') \prod_{i_1, ..., i_n}^{i'} q(t) - \sum_{i'=2}^{N} \sum_{j'=1}^{i'-1} W(t; i_1, ..., i_n - i', j') \prod_{i_1, ..., i_n}^{i', j'} q(t) + ..., \tag{74}$$

where for the first term on the right hand side of eq. (67), $i_1, ..., i_n$ becomes i, for the second $i_1, ..., i_n$ becomes i, j, and so forth. The computation of each term in eq. (74) follows the same procedure as was

described earlier for $\mathcal{P}[\theta_1 \ldots \theta_m d_1 \ldots d_n)$; for example, for the terms within the first summation sign, $i_1, \ldots, i_n$ become the mode failures $1, \ldots, m$ and i' becomes the mode failures $1, \ldots, n$ in the previous discussion.

The second term for $W_0(t)\,dt$ is determined with the use of eq. (74), and hence the top failure intensity $W_0(t)$ is finally determined. Summarizing the expressions obtained,

$$W_0(t) = W_0^{(1)}(t) - W_0^{(2)}(t)\,, \tag{75}$$

$$W_0^{(1)}(t) = \sum_{i=1}^{N} W_i(t) - \sum_{i=2}^{N}\sum_{j=1}^{i-1} W(t; i, j) \prod_{\cdot}^{+i,\,j} q(t)$$

$$+ \sum_{i=3}^{N}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} W(t; i, j, k) \prod_{\cdot}^{+i,\,j,\,k} q(t)$$

$$- \ldots\,, \tag{76}$$

$$W_0^{(2)}(t) = \sum_{i=1}^{N} W_B(t; i)$$

$$- \sum_{i=2}^{N}\sum_{j=1}^{i-1} W_B(t; i, j) + \ldots\,, \tag{77}$$

$$W_B(t; i_1, \ldots, i_n)$$

$$= \sum_{i'=1}^{N} W(t; i_1, \ldots, i_n - i') \prod_{i_1,\ldots,i_n}^{i'} q(t) \tag{78}$$

$$- \sum_{i'=2}^{N}\sum_{j'=1}^{i'-1} W(t; i_1 \ldots i_n - i', j') \prod_{i_1,\ldots,i_n}^{i',\,j'} q(t) + \ldots$$

The product symbols and failure intensities in the above equations are defined by eq. (60), (61), (70), and (72). The differential dt has "cancelled out" in the above equations, and the symbols $W_0^{(2)}(t)$ and $W_0^{(1)}(t)$ have replaced $\mathcal{P}[B \cup_{i=1}^{N} \theta_i]$ and $\mathcal{P}[\cup_{i=1}^{N} \theta_i]$, respectively (with the cancellation of dt).

For fault trees with a smaller number of mode failures, the above system of equations can be solved exactly to obtain $W_0(t)$. The operations needed to compute the individual terms, which were described earlier, are straightforward and can be rapidly performed by a computer. If the primary failure quantites used in the terms reach asymptotic, steady state values then $W_0(t)$ need only be computed as a function of time until its steady state value is reached. For a large class of problems the steady state values are reached quickly, simplifying the calculations.

For fault trees with a larger number of mode failures, the bracketing procedure is an extremely efficient method of obtaining as tight an enveloping as desired for $W_0(t)$. In eqs. (76) through (78), an upper bound can be obtained for $W_0^{(1)}(t)$, $W_0^{(2)}(t)$, or $W_B(t; i_1, \ldots, i_n)$ by considering just the first terms in the respective right hand expressions for these quantities. Lower bounds can be obtained by considering the first two terms, new upper bounds can be obtained by considering the first three terms, and so forth. Various combinations of these successive upper and lower bounds will give successive upper and lower bounds for $W_0(t)$.

As an example of the application of the bracketing procedure, a first (and simplest) upper bound for $W_0(t)$, $W_0(t)_{\max}$, is given by the relations

$$W_0(t)_{\max} = W_0^{(1)}(t)_{\max}\,, \tag{79}$$

where

$$W_0^{(1)}(t)_{\max} = \sum_{i=1}^{N} W_i(t)\,. \tag{80}$$

Hence, the first upper bound, $W_0(t) < W_0(t)_{\max}$, is simply the sum of the individual mode failure intensities. A first lower bound for $W_0(t)$, $W_0(t)_{\min}$, is given by the relations

$$W_0(t)_{\min} = W_0^{(1)}(t)_{\min} - W_0^{(2)}(t)_{\max}\,, \tag{81}$$

with

$$W_0^{(1)}(t)_{\min} = \sum_{i=1}^{N} W_i(t)$$

$$- \sum_{i=2}^{N}\sum_{j=1}^{i-1} W(t; i, j) \prod_{\cdot}^{i,\,j} q(t)\,, \tag{82}$$

$$W_0^{(2)}(t)_{\max} = \sum_{i=1}^{N} W_B(t; i)_{\max}, \tag{83}$$

$$W_B(t;i)_{\max} = \sum_{i'=1}^{N} W(t;i-i') \prod_{i}^{i'} q(t) . \quad (84)$$

This lower bound for $W_0(t)$, $W_0(t) \geqslant W_0(t)_{\min}$, only involves combinations of two mode failures. Considering more terms in the expressions given by eqs. (76)–(78), will yield other successive upper and lower bounds of $W_0(t)$.

Because the primary failure existence probabilities $q(t)$ are much less than unity, the successive upper and lower bounds will rapidly converge to one another. As an example, the first upper bound and lower bound, given by eqs. (79) and (81), will generally agree to within three significant figures, giving a tight enough envelope for most computations. For scoping calculations, and in fact for many calculations, the first upper bound (eq. (79)) is of sufficient accuracy for a determination of $W_0(t)$;

$$W_0(t) \leqslant \sum_{i=1}^{N} W_i(t) . \quad (86)$$

This approximation gives a conservative estimate of $W_0(t)$, which is desirable, can be simply computed from the mode failure intensities $W_i(t)$, and is usually within three significant figures of the true value of $W_0(t)$.

The top failure intensity $W_0(t)$ is thus determined, whether it be by computation of its exact value or by use of the bracketing procedure to obtain successive upper and lower bounds, one upper and lower bound, or merely an upper bound. With the failure intensity $W_0(t)$ and the existence probability $Q_0(t)$ determined, the remaining top failure characteristic, the top failure rate, is simply obtainable. The top failure rate $\Lambda_0(t)$ is defined in a completely analogous manner to the primary and mode failure rate;

$\Lambda_0(t)\,dt$ = the probability that the top failure occurs in time t to $t+dt$ given it is not existing at time t. (87)

Moreover, the top failure rate is applied in precisely the same way as the other failure rates. The quantity

$$\exp\left(-\int_0^t \Lambda_0(t')\,dt'\right) \Lambda_0(t)$$

is the first occurrence distribution for the top failure, the probability that the top failure first occurs at t per unit time. The quantity,

$$\exp\left(-\int_0^t \Lambda_0(t')\,dt'\right)$$

is the probability that the top failure does not occur during the interval from 0 to t and one minus this quantity is the probability that the top failure does occur in this interval.

From the definitions of the top failure existence probability $Q_0(t)$ (eqs. (33)) and the top failure intensity $W_0(t)$ (eq. (50)), it is apparent that

$$W_0(t)\,dt = [1 - Q_0(t)]\,\Lambda_0(t)\,dt . \quad (88)$$

For the top failure to occur in t to $t+dt$, $W_0(t)\,dt$, it must not exist at time t, $1 - Q_0(t)$, and given it does not exist at time t it must occur in t to $t+dt$, $\Lambda_0(t)\,dt$. Therefore, quite simply,

$$\Lambda_0(t) = \frac{W_0(t)}{1 - Q_0(t)} , \quad (89)$$

and with knowledge of $W_0(t)$ and $Q_0(t)$, $\Lambda_0(t)$ is therefore known.

Using the exact values in eq. (89), for $W_0(t)$ and $Q_0(t)$ will yield the exact value for $\Lambda_0(t)$. Using upper or lower bounds for both $W_0(t)$ and $Q_0(t)$, obtained from bracketing, will yield respective upper or lower bounds for $\Lambda_0(t)$. Obtaining envelopes for $W_0(t)$ and $Q_0(t)$ will thus yield envelopes for $\Lambda_0(t)$. The simplest upper bound for $\Lambda_0(t)$ is obtained by using the upper bound for $Q_0(t)$ from the Esary and Proschan relation, eq. (49) and the first upper bound for $W_0(t)$ given by eq. (79),

$$\Lambda_0(t) \leqslant \sum_{i=1}^{N} W_i(t) \Big/ \prod_{i=1}^{N} (1 - Q_i(t)) . \quad (90)$$

This first upper bound is directly obtained from the mode failure characteristics $W_i(t)$ and $Q_i(t)$ and moreover is also an excellent approximation to the true value of $\Lambda_0(t)$, generally agreeing to within three significant figures of the true value. This approximation is also desirable since it is conservative, being an upper bound. Using the simplest lower bounds for $W_0(t)$ and $Q_0(t)$ (eqs. (81) and (42)) will give the simplest

lower bound for $\Lambda_0(t)$ generally agreeing with eq. (90) to three significant figures.

The top failure rate $\Lambda_0(t)$ is thus determined, whether exactly or by enveloping. The top failure characteristics $Q_0(t)$, $W_0(t)$, and $\Lambda_0(t)$ are consequently all determined. These characteristics completely quantify the top failure for all time. The values of these characteristics quantitatively give the safety of the system with regard to the occurrence of the top failure. The response of these characteristics to design changes or particular repair and maintenance schemes quantitatively determines the effectiveness of such changes or schemes. Moreover, response of these characteristics to changes in environment or operation is immediately obtained. This response to system "phases" is an immediate by-product of the functional dependence of the characteristics on time. The top failure information obtained therefore encompasses general conditions incorporated in the fault tree, yielding detailed and complete knowledge for any specific situation. With the use of the bracketing or enveloping procedure, the information is furthermore obtained efficiently and in little time.

5. Applications

To apply the methodology described in the preceding sections, which we call Kinetic Tree Theory, three computer programs have been developed, PREP, KITT-1, and KITT-2. The codes are written in FORTRAN IV for the IBM 360/75 computer. As stated, the Kinetic Tree Theory methodology requires the mode failures, or critical paths, of the fault tree in order to obtain the top failure information. The code PREP, therefore, first obtains the mode failures from the fault tree. Having obtained the mode failures, KITT-1 or KITT-2 is then run to obtain the characteristics for the individual primary failures, mode failures, and top failure.

The fault tree, having been drawn, is first input in a coded form to the PREP program. The input to PREP is quite simple. Each unique primary failure on the fault tree is assigned an arbitrary unique name. Also, each unique logical gate is assigned an arbitrary name. Each gate is then described on an input card; the card gives the name of the gate, the type of gate ("AND" or "OR") and the names of the gates and/or primary failures attached to the gate. The gates may be input in any order, PREP determining the necessary logical sequence. Up to 2000 gates and up to 2000 primary failures (or inhibit conditions) can be handled by PREP.

From the input, PREP constructs the FORTRAN logical description of the fault tree and then obtains the unique mode failures (critical paths). The mode failures are determined either by Monte Carlo simulation or by deterministic testing. The Monte Carlo simulation uses the power method described by Nagel [2]. However, this technique is used only to obtain the mode failures and is therefore quite fast since it is not used to obtain quantitative information (the probability characteristics); for example, 500 mode failures can be found for a 400 primary failure fault tree on the order of 1 minute computer time. The power method has the feature that the most important mode failures, those most likely to occur, are found first. In the deterministic testing method, combinations of primary failures are made to occur and the top failure is then checked for its occurrence in order to obtain the mode failures. Each primary failure is made to occur singularly to obtain the mode failures consisting of one primary failure. Combinations of two primary failures are made to simultaneously occur to obtain the mode failures consisting of two primary failures, and so forth. The deterministic testing method ensures that all mode failures consisting of up to n primary failures are found, where n is set by the user. Since it is not the purpose of this paper to delve into the details of determining mode failures, the virtues of one technique over the other, or how to combine the two techniques most efficiently to obtain the mode failures, this will not be discussed. The PREP and KITT code manuals [11] describe the mechanics and use of the codes in detail, for the interested reader. It need only be said here that for a general, complex fault tree, the mode failures can be obtained in an efficient and complete manner.

Having obtained the mode failures, either KITT-1 or KITT-2 is then run to obtain the probability characteristics described in the preceding sections. The KITT codes are particular applications of the general Kinetic Tree Theory methodology presented earlier and hence the codes have certain restrictions. For the codes, the primary failures are restricted to having constant failure rates ($\lambda(t) = \lambda$). With regard to repair

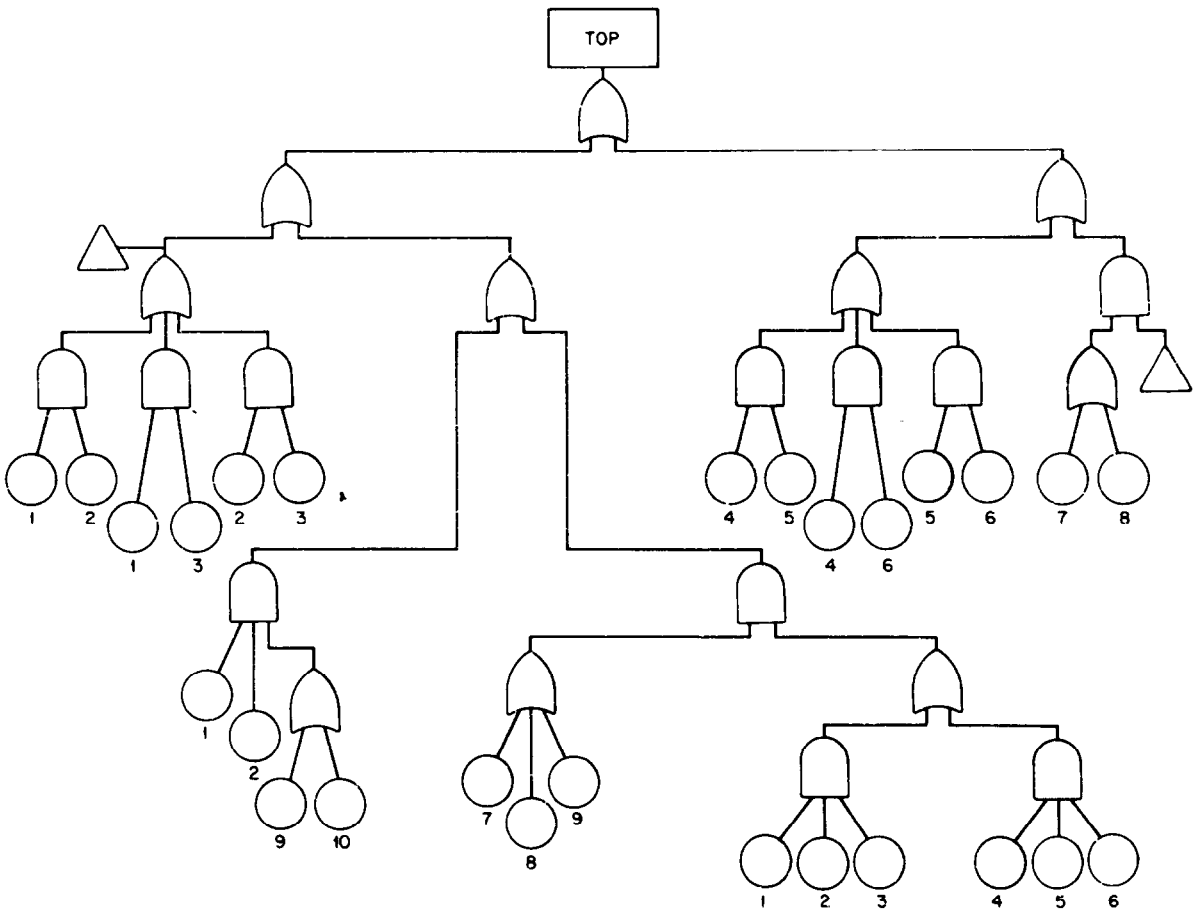


Fig. 1. Sample fault tree.

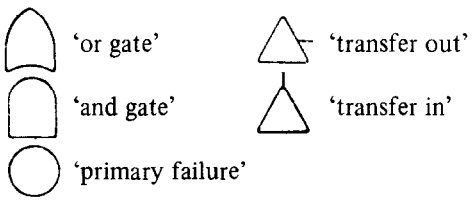
of the primary failure, constant repair times, constant repair rates ($\mu(t) = \mu$), and non-repairability can be handled. (For a constant repair time τ, the primary failure is repaired in exactly a time interval of τ from the time of its occurrence, where τ is the sum of the detection and actual repair time.) Any mixture of non-repairable and repairable primary failures can be handled. Also, any number of inhibit conditions can be treated *. As in the general methodology, all primary failures are assumed independent.

KITT-1 is a "single-phase" code; for a given primary failure, its failure rate and type of repair (or non-repairability) must remain the same for all time.

* An inhibit condition is a condition, or event, which must exist in addition to a primary failure in order to cause subsequent, or secondary, failures.

KITT-2 is a "multiphase" code in which the failure rate and type of repair must be constant in one time period (phase) but can change in an arbitrary manner from phase to phase; each primary failure may have up to 50 unique phases. The input to KITT-1 or KITT-2, besides the mode failures obtained from PREP, consists of the failure rates and repair data for the primary failures. If KITT-2 is used, the time boundaries of the phases, for each primary failure, must also be specified. The output from the KITT codes are the primary failure, mode failure, and top failure characteristics enumerated in the previous sections. These characteristics are obtained at arbitrary time points specified by the user. Since the mechanics of the codes is not of concern here, they will not be elaborated upon. The computer codes have been thoroughly checked, and their use and mechanics are described in their associated manuals [11].

As an illustration of the applications of the methodology developed, consider the sample fault tree depicted in fig. 1. The symbols, as described by Haasl [1], denote:



The phraseology describing failures caused as a consequence of primary failures has been deleted for brevity (these subsequent failures are usually described in rectangles). The primary failures have simply been given indices as their names; the indices associated with the corresponding primary failures are shown in fig. 1. Also, the top failure has simply been called "TOP".

The gates of this sample fault tree were arbitrarily named, and the fault tree was input to PREP. The deterministic testing method was used to obtain all the mode failures, or critical paths, of the fault tree. These mode failures obtained are shown in table 1. In this table, each unique mode failure was given a separate index to identify it and these indices are given in the first column. In the second column, the primary failures which are members of the particular mode failure are given. The indices of the primary failures are those used in fig. 1. For example, from table 1, primary failures 1 and 2 must both simultaneously exist for mode failure 1 to exist. Since a mode failure (critical path) is simply a mode by which the top failure exists, if primary failures 1 and 2 both exist, then the top failure exists. That these are all the unique mode failures of the fault tree can be verified by simple inspection of the tree. The total computer time needed by PREP was under 0.01 minutes.

Table 1
Mode failures of the sample fault tree

Mode failure	Primary failures constituting the mode failure
1	1, 2
2	1, 3
3	2, 3
4	4, 5
5	4, 6
6	5, 6

Having obtained the mode failures, KITT-1 was then used to obtain the characteristics for this fault tree. The failure rates assigned to the primary failures and input to KITT-1 are shown in table 2. All the primary failures were treated as being non-repairable for this first problem.

Table 2
Primary failure rates λ for the sample fault tree

Primary failure index	λ (hr^{-1})
1	2.60–06
2	2.60–06
3	2.60–06
4	3.50–05
5	3.50–05
6	3.50–05
7	5.00–06
8	5.00–06
9	8.00–06
10	8.00–06

(The nomenclature used in this paper is such that 2.60–06 means 2.60×10^{-6}.) The primary failure and mode failure characteristics obtained form KITT-1 are shown in table 3. The top failure characteristics obtained are shown in table 4. The characteristics were obtained for 11 points in time (t), equally spaced at 1000 hours, however only 7 of these time points are given in these tables.

The characteristics shown in table 3 for primary failure 1 are also those for primary failures 2 and 3 since these primary failures all have the same failure rates (2.60–06 hr^{-1}); in an analogous manner the characteristics shown for primary failure 4 are also those of primary failures 5 and 6. In table 3, the primary failure rates λ are merely those read in and are printed again for convenience. The characteristics for primary failures 7 through 10 are not given since these primary failures are not members of any of the mode failures and hence in no way affect the top failure. It can be simply shown from the preceding theoretical discussions that for a non-repairable primary failure;

Table 3
Primary failure and mode failure characteristics for the non-repairable sample tree

	Characteristics for primary failure 1			Characteristics for primary failure 4		
t ($\times 10^3$ hr)	$\lambda(t)$ (hr^{-1})	$w(t)$ (hr^{-1})	$q(t)$	$\lambda(t)$ (hr^{-1})	$w(t)$ (hr^{-1})	$q(t)$
0.0	2.60–06	2.60–06	0.0	3.50–05	3.50–05	0.0
1.0	2.60–06	2.59–06	2.60–03	3.50–05	3.38–05	3.44–02
2.0	2.60–06	2.59–06	5.19–03	3.50–05	3.26–05	6.76–02
3.0	2.60–06	2.58–06	7.77–03	3.50–05	3.15–05	9.97–02
4.0	2.60–06	2.57–06	1.03–02	3.50–05	3.04–05	1.31–01
5.0	2.60–06	2.57–06	1.29–02	3.50–05	2.94–05	1.61–01
10.0	2.60–06	2.53–06	2.57–02	3.50–05	2.47–05	2.95–01
	Characteristics for mode failure 1			Characteristics for mode failure 4		
t ($\times 10^3$ hr)	$\Lambda(t)$ (hr^{-1})	$W(t)$ (hr^{-1})	$Q(t)$	$\Lambda(t)$ (hr^{-1})	$W(t)$ (hr^{-1})	$Q(t)$
0.0	0.0	0.0	0.0	0.0	0.0	0.0
1.0	1.35–08	1.35–08	6.74–06	2.33–06	2.32–06	1.18–03
2.0	2.68–08	2.68–08	2.69–05	4.43–06	4.41–06	4.57–03
3.0	4.01–08	4.01–08	6.04–05	6.34–06	6.28–06	9.94–03
4.0	5.32–08	5.32–08	1.07–04	8.09–06	7.95–06	1.71–02
5.0	6.63–08	6.63–08	1.67–04	9.68–06	9.43–06	2.58–02
10.0	1.30–07	1.30–07	6.59–04	1.60–05	1.46–05	8.72–02

Table 4
The top failure characteristics for the non-repairable sample tree

	Exact results			Upper bounds			$Q_0(t)$ envelopes		MC $Q_0(t)$
t ($\times 10^3$ hr)	$\Lambda_0(t)$ (hr^{-1})	$W_0(t)$ (hr^{-1})	$Q_0(t)$	$\Lambda_0^u(t)$ (hr^{-1})	$W_0^u(t)$ (hr^{-1})	$Q_0^u(t)$	$Q_0(t)_{min}$	$Q_0(t)_{max}$	$Q_0(t)$
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1.0	6.80–06	6.77–06	3.49–03	7.04–06	7.01–06	3.56–03	3.45–03	3.57–03	3.47–03
2.0	1.26–05	1.24–05	1.32–02	1.35–05	1.33–05	1.37–02	1.29–02	1.38–02	1.30–02
3.0	1.76–05	1.71–05	2.80–02	1.95–05	1.90–05	2.97–02	2.70–02	3.00–02	2.85–02
4.0	2.19–05	2.09–05	4.70–02	2.53–05	2.40–05	5.06–02	4.48–02	5.15–02	4.68–02
5.0	2.57–05	2.39–05	6.95–02	3.08–05	2.85–05	7.58–02	6.54–02	7.78–02	6.90–02
10.0	3.94–05	3.10–05	2.12–01	5.81–05	4.41–05	2.41–01	1.86–01	2.64–01	2.08–01

$$q(t) = \int_0^t w(t')\,dt' , \tag{91}$$

$$q(t) = 1 - \exp(-\int_0^t \lambda(t')\,dt') . \tag{92}$$

Hence, $q(t)$ in table 3 is also equal to the expected number of times the primary failure will occur to time t (eq. (91)) and in addition is also equal to the probability that the primary failure will occur to time t (eq. (92)).

The characteristics for mode failure 1 in table 3 are also those for mode failures 2 and 3 since these mode failures are all composed of similar primary failures. Likewise, the characteristics for mode failure 4 are also those of mode failures 5 and 6. As for a non-repairable primary failure, for a mode failure consisting of non-repairable primary failures,

$$Q(t) = \int_0^t W(t')\,dt' \tag{93}$$

and

$$Q(t) = 1 - \exp(-\int_0^t \Lambda(t')\,dt') . \tag{94}$$

$Q(t)$ in table 3 thus equals the accumulated number of occurrences of the mode failure and also equals the occurrence probability for the mode failure.

In table 4, which gives the top failure characteristics, the upper bounds $\Lambda_0^u(t)$, $W_0^u(t)$, and $Q_0^u(t)$ are those given by eqs. (90), (86), and (49), respectively. It was stated that these bounds are excellent approximations for the respective true values when the primary failure existence probabilities are near zero, and in fact these bounds approach the true values as the existence probabilities approach zero. This is evident from the table since these upper bounds depart from the exact values as t increases. Even at $t = 10^4$ hr, when the maximum primary failure existence probability equals 2.95–01 (for primary failure 4) which indeed is not near zero, the upper bounds are still fairly good approximations. The $Q_0(t)$ envelopes in table 4, $Q_0(t)_{max}$ and $Q_0(t)_{min}$ are those given by eq. (41) and (42), respectively. The first two brackets for $W_0(t)$, eqs. (79) and (81) behaved in an analogous manner to the $Q_0(t)$ envelopes. As was discussed, the bracketing procedure gains in efficiency as the primary failure existence probabilities approach zero. However, even the first two brackets for $Q_0(t)$ are still fairly close to one another at $t = 10^4$ hr. Taking more brackets (considering more terms in eqs. (40), and (76)–(78)) would yield tighter envelopes; in fact, the exact values of table 4 were obtained by considering all terms in these equations.

Finally, in table 4, a Monte Carlo run was made to verify the results from the KITT code. The column MC $Q_0(t)$ gives these results; all the values obtained had errors (standard deviations) less than 1.5%. The Monte Carlo approach is quite time-consuming, but if run properly also gives the "exact" answers – within the statistical errors associated with a Monte Carlo result. The methodology presented here, of course, has the advantage of obtaining the exact answers with no statistical error and in little computer time. In a large number of problems, however, the Monte Carlo approach was used to verify this methodology. As exemplified in table 4, the Monte Carlo results always agreed with the results obtained by the KITT codes.

The output in tables 3 and 4 demonstrates the complete and detailed type of information yielded by the Kinetic Tree Theory methodology. Even though a "sample" fault tree was analyzed, the tree being quite simple in its logic, the same type of information will be obtained regardless of the complexity and size of the fault tree. Moreover, the information is self-explanatory and "physical" in nature. For example, for mode failure 1 of the sample fault tree (table 3),

$$1 - \exp(-\int_0^t \Lambda(t')\,dt')$$

which in this case equals $Q(t)$ simply gives the *probability* that the mode failure will occur at all to time t;

$$\int_0^t W(t')\,dt'$$

again in this case equalling $Q(t)$ simply gives the *number* of times the mode failure will occur; and $Q(t)$ simply gives the probability of the mode failure *existing* at time t. In addition, the characteristics $\Lambda(t)$ and $W(t)$ give the pointwise behavior of this mode failure. This same information is obtained for each primary failure, each mode failure or critical path, and finally for the top failure itself. Since the

Table 5
Primary failure and mode failure characteristics for the repairable sample tree

	Characteristics for primary failure 1				Characteristic for primary failure 4			
t ($\times 10^3$ hr)	$w(t)$ (hr^{-1})	$q(t)$	$w(0,t)$	$1-f(0,t)$	$w(t)$ (hr^{-1})	$q(t)$	$w(0,t)$	$1-f(0,t)$
0.0	2.60–06	0.0	0.0	0.0	3.50–05	0.0	0.0	0.0
0.003	2.60–06	7.80–06	7.80–06	7.80–06	3.50–05	1.05–04	1.05–04	1.05–04
0.006	2.60–06	1.56–05	1.56–05	1.56–05	3.50–05	2.10–04	2.10–04	2.10–04
0.024	2.60–06	6.24–05	6.24–05	6.24–05	3.50–05	2.10–04	8.40–04	8.40–04
1.0	2.60–06	6.24–05	2.60–03	2.60–03	3.50–05	2.10–04	3.50–02	3.44–02
2.0	2.60–06	6.24–05	5.20–03	5.19–03	3.50–05	2.10–04	7.00–02	6.76–02
10.0	2.60–06	6.24–05	2.60–02	2.57–02	3.50–05	2.10–04	3.50–01	2.95–01
	Characteristics for mode failure 1				Characteristic for mode failure 4			
t ($\times 10^3$ hr)	$W(t)$ (hr^{-1})	$Q(t)$	$W(0,t)$	$1-F(0,t)$	$W(t)$ (hr^{-1})	$Q(t)$	$W(0,t)$	$1-F(0,t)$
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.003	4.06–11	6.08–11	6.08–11	6.08–11	7.35–09	1.10–08	1.10–08	1.10–08
0.006	8.11–11	2.43–10	2.43–10	2.43–10	1.47–08	4.41–08	4.41–08	4.41–08
0.024	3.24–10	3.89–09	3.89–09	3.89–09	1.47–08	4.41–08	3.09–07	3.09–07
1.0	3.24–10	3.89–09	3.21–07	3.21–07	1.47–08	4.41–08	1.46–05	1.46–05
2.0	3.24–10	3.89–09	6.45–07	6.45–07	1.47–08	4.41–08	2.93–05	2.93–05
10.0	3.24–10	3.89–09	3.24–06	3.24–06	1.47–08	4.41–08	1.47–04	1.47–04

Table 6
The top failure characteristics for the repairable sample tree

t ($\times 10^3$ hr)	$\Lambda_0(t)$ (hr^{-1})	$W_0(t)$ (hr^{-1})	$Q_0(t)$	$W_0(0,t)$	$1-F_0(0,t)$
0.0	0.0	0.0	0.0	0.0	0.0
0.003	2.22–08	2.22–08	3.33–08	3.33–08	3.33–08
0.006	4.43–08	4.43–08	1.33–07	1.33–07	1.33–07
0.024	4.50–08	4.50–08	1.44–07	9.37–07	9.37–07
1.0	4.50–08	4.50–08	1.44–07	4.49–05	4.49–05
2.0	4.50–08	4.50–08	1.44–07	8.99–05	8.99–05
3.0	4.50–08	4.50–08	1.44–07	1.35–04	1.35–04
4.0	4.50–08	4.50–08	1.44–07	1.80–04	1.80–04
5.0	4.50–08	4.50–08	1.44–07	2.25–04	2.25–04
10.0	4.50–08	4.50–08	1.44–07	4.50–04	4.50–04

information is obtained as a function of time, the complete history of each type of failure is determined. This time dependency is quite important. For example, the importance of the mode failures may change in time – a particular mode failure may be of little importance at one time and yet, at a later time may become the most probable mode by which the top failure will occur.

The detailed quality of the information obtained makes it apparent for the sample fault tree that mode failures 4, 5 and 6 are the most probable modes by which the top failure will occur, being 100 times more probable than mode failures 1, 2 and 3. If the probability of the top failure occurring was deemed too high, then design modifications would be centered around these most probable mode failures. Also, if the top failure had occurred, the primary failures in these most probable mode failures should be those first checked as to the causes of the top failure – the information obtained thereby giving optimal repair schemes.

The information obtained also makes apparent the effect of repair with regard to the fault tree. For example, for the sample fault tree, if primary failures 1, 2, and 3 could be detected and repaired in 24 hours and primary failures 4, 5, and 6 could be detected and repaired in 6 hours then the sample fault tree would have the characteristics shown in tables 5 and 6. For these tables, the input to KITT-1 was the same as for the non-repairable tree (the same primary failure rates and mode failures were used) except that each primary failure was assigned a constant detection plus repair time as given above.

In table 5, $w(0, t)$ equals the accumulated number of times the primary failure occurs to time t

$$w(0, t) = \int_0^t w(t')\,\mathrm{d}t' \ .$$

Also, $1 - f(0,t)$ equals the probability that the primary failure will occur at all to time t

$$1 - f(0,t) = 1 - \exp\left(-\int_0^t \lambda(t')\,\mathrm{d}t'\right) \ .$$

Analogous nomenclature is used for the mode failures;

$$W(0,t) = \int_0^t W(t')\,\mathrm{d}t' \ ,$$

and

$$1 - F(0,t) = 1 - \exp\left(-\int_0^t \Lambda(t')\,\mathrm{d}t'\right) .$$

These quantities are no longer equal to the respective existence probabilities ($q(t)$ or $Q(t)$) since the primary failures are now repairable. The failure rates, $\lambda(t)$ for the primary failures and $\Lambda(t)$ for the mode failures, are not given in table 5 since they have the same value, to three significant figures, as the corresponding failure intensity ($w(t)$ or $W(t)$). Again, primary failures 1, 2, and 3 and primary failures 4, 5 and 6 have the same characteristics; also mode failures 1, 2, and 3 and mode failures 4, 5, and 6 have the same characteristics.

In table 6, $W_0(0,t)$ is the accumulated number of times the top failure occurs to t

$$W_0(0,t) = \int_0^t W_0(t')\,\mathrm{d}t' \ ,$$

and $1 - F_0(0,t)$ is the probability of the top failure occurring at all to time t

$$1 - F_0(0,t) = 1 - \exp\left(-\int_0^t \Lambda_0(t')\,\mathrm{d}t'\right) \ .$$

Since the characteristics have a different behavior when the primary failures are repairable, a number of different time points are given in table 6 (and table 5). It is noted that since the maximum repair time for a primary failure is 24 hours, the top characteristics $\Lambda_0(t)$, $W_0(t)$, and $Q_0(t)$ remain constant for $t > 24$ hr (i.e., assume their steady state, asymptotic values). This achievement of steady state is also exhibited by the analogous mode failure and primary failure characteristics (table 5). The upper bound approximations for $\Lambda_0(t)$, $W_0(t)$, and $Q_0(t)$ (eqs. (90), (86), and (49), respectively) are not given in table 6 since they agreed to four significant figures with the exact values given in the table. Similarly, the first two envelopes given by eqs. (41) and (42) or by eqs. (79) and (81) are not given since they agreed with each other, and with the respective exact value, to four significant figures. Because the primary failure existence probabilities are now near zero (table 5), and remain there for all time, the upper bounds and the bracketing procedure are extremely accurate and efficient – for all the time points. In general, regardless of the size and complexity of the fault tree, the simple upper bounds are accurate "scoping" approxi-

mations, and the bracketing procedure is an extremely efficient method of converging to the exact values.

From tables 5 and 6, and comparing with tables 3 and 4, the detailed effect of repair is immediately made obvious. How the primary failure characteristics respond, how the mode failures (critical paths) change in importance, and how the top failure characteristics change in value are all made evident. Different repair times could be assigned to determine their effect, or only certain primary failures could be repairable while others would remain non-repairable. Similar studies could be made by varying the primary failure rates (e.g., what is the effect of using more reliable components). In the KITT-2 code, where the primary failures may have phases, the effect of different environments could be analyzed. These comparative studies, or sensitivity studies, are now completely feasible because of the detailed results obtained and the small computer times needed. For the above two problems, the total computer time needed for the PREP and KITT codes was under 0.08 minutes. In general, for large fault trees (500 primary failures) the total time needed is on the order of 1 minute for each case studied (independent of the number of time points used).

The above sample studies serve to demonstrate the amount of information obtained for any fault tree from the "Kinetic Tree Theory" methodology developed here. The PREP and KITT codes are presently being used in a routine manner for the reliability and safety analyses performed at the National Reactor Testing Station. Fault trees consisting of up to 1800 primary failures and 1500 gates have been evaluated using the PREP and KITT codes. The information obtained for these fault trees was exactly the same as that obtained for the sample studies; time-dependent characteristics were obtained for each primary failure, for each mode failure and for the top failure. The fault trees consisted of various mixtures of non-repairable and repairable primary failures; failure rates used for the primary failures ranged from 1.0–10 hr^{-1} to 1.0–02 hr^{-1} and repair-plus-detection times ranged from one hour to 1.0+04 hr. For these fault trees, the primary failure, mode failure and top failure characteristics were obtained at up to 200 time points arbitrarily spaced, the spacing between time points ranging from 0.1 hr to 1.0+03 hr. In addition, multiphase fault trees have been routinely evaluated, with the number of phases, ranging from 2 to 45. The average total computer time needed to obtain the complete information described, for 100 time points, was on the order of one minute for a 500 primary failure tree.

Reactor scram systems, pressure reduction systems, and isolation containment systems are examples of the systems for which fault trees were evaluated. The evaluation of these fault trees was used to quantitatively determine the safety and reliability of the respective systems. Comparative studies were made to determine the effects of certain design changes, to determine optimal maintenance intervals, and to determine optimal monitoring and repair schemes. Because the methodology developed here readily lends itself to being automated, as exemplified by the PREP and KITT codes, these evaluations and comparative studies were extremely simple to carry out. Because of the speed and ease with which results are obtained, and because of the detailed, time-dependent information obtained, experience in applying the Kinetic Theory methodology has verified its value as an extremely useful and simple tool for evaluating any fault tree – regardless of its complexity, size, type of primary failure repair used, or the number of phases assigned for which the primary failure data differs.

6. Summary and conclusions

A methodology, termed "Kinetic Tree Theory", is presented by which any fault tree can be evaluated. The basic approach taken in Kinetic Tree Theory is that whether it be for a primary failure, a mode failure, or for the top failure, complete information is obtained from three characteristics – the existence probability, the failure rate, and the failure intensity. When these three characteristics are determined for a particular entity, that entity being a primary failure, a mode failure, or the top failure, then subsequent probabilistic information, both pointwise and cumulative, is obtained for all time for this entity.

In the Kinetic Tree Theory methodology, the probabilistic characteristics are determined by using probability analysis on events which occur at a general time t or which occur in a general increment of time, t to $t + dt$. Complete information is thus obtained for all time, and this information is obtained simply since numerous combinations involving orders

of $(dt)^2$ can be neglected. The primary failure characteristics which are not given as data are determined from balance considerations. The balance considerations incorporate general failure and repair distributions. The mode failure characteristics are then determined from the primary failure characteristics; this determination assumes knowledge of the primary failures constituting the mode failure and assumes independence of these primary failures. The top failure characteristics are finally determined from the mode failure information; this information involves knowledge of the mode failures constituting the top failure.

Thus, given the mode failures (critical paths) of the fault tree, complete, time-dependent information is obtained for the top failure by proceeding from the primary failures to the mode failures and finally to the top failure. In proceeding in this stepwise fashion, complete time-dependent information is also obtained for each primary failure and mode failure of the fault tree. In application of the Kinetic Tree Theory methodology, as exemplified by the PREP and KITT codes, the mode failures or critical paths are first determined by a deterministic testing method or by Monte Carlo simulation (the PREP code) and then the characteristics are determined according to the Kinetic Tree Theory approach (the KITT codes). In the application, the top failure characteristics are determined by use of the simple upper bound approximations or by use of the bracketing procedure. The bracketing procedure can be used to obtain two simple envelopes, can be carried further to obtain higher order envelopes, or can be carried to completion by which the exact top failure characteristics are obtained.

In application, the Kinetic Tree Theory methodology yields numerical results simply automatically, and in very little computer time. Because of this efficiency and because of the completeness of the information obtained, characteristics can not only be simply determined for complex fault trees by using one set of data, but comparative studies can be simply performed to obtain the effect of certain design changes, maintenance schemes, or repair schemes. For these comparative studies several sets of data would be used for the same fault tree or the fault tree itself would be modified. The speed by which numerical results are yielded, the completeness of information obtained, the versatility to handle a wide spectrum of fault trees, and the simplicity and automation of application make the Kinetic Tree Theory approach an extremely useful tool for evaluating fault trees.

Acknowledgements

Acknowledgement is given to D.F.Haasl, Institute of System Sciences, for his discussions both on the basic concepts of fault trees analysis and on the previous problems in fault tree evaluation which had to be circumvented. Acknowledgement is also given to R.E.Narum, Idaho Nuclear Corporation, who programmed parts of the computer codes developed.

References

[1] D.F.Haasl, Advanced concepts in fault tree analysis, System Safety Symposium, 8–9 June, 1965, Seattle: The Boeing Company (1965).
[2] P.M.Nagel, Importance sampling in systems simulation, Fifth Annual AIAA Conference on Reliability and Maintainability, 18–20 July 1966, New York City.
[3] A.B.Mearns, Fault tree analysis: the study of unlikely events in complex systems, System Safety Symposium, 8–9 June 1965, Seattle: The Boeing Company (1965).
[4] W.L.Headington et al., Fault Tree Analysis of the PBF Transient Rod Drive System, IDO-17274 (Nov. 1968).
[5] J.D.Esary and F.Proschan, Coherent structures of non-identical components, Technometrics 5 (1963) 191–209.
[6] N.H.Roberts, Mathematical methods in reliability engineering (McGraw-Hill, Inc., New York, 1961).
[7] A.M.Polovko, Fundamentals of Reliability Theory (Academic Press, Inc., New York, 1968).
[8] I.Bazovsky, Reliability Theory and Practice (Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1961).
[9] B.J.Garrick et al., Reliability Analysis of Nuclear Power Plant Protective Systems, NH-190 (May 1967).
[10] H.D.Brunk, An Introduction to Mathematical Statistics (Ginn and Company, Boston, 1960) p. 23.
[11] W.E.Vesely and R.E.Narum, The User's Manual for the PREP and KITT codes, IN-1349 (to be published).