Risk Analysis, Vol. 4, No. 3, 1984

Fault Trees vs. Event Trees in Reliability Analysis

M. Elisabeth Paté-Cornell[1]

Received May 27, 1981; revised December 12, 1983

Reliability analysis is the study of both the probability and the process of failure of a system. For that purpose, several tools are available, for example, fault trees, event trees, or the GO technique. These tools are often complementary and address different aspects of the questions. Experience shows that there is sometimes confusion between two of these methods: fault trees and event trees. Sometimes identified as equivalent, they, in fact, serve different purposes. Fault trees lay out relationships among events. Event trees lay out sequences of events linked by conditional probabilities. At least in theory, event trees can handle better notions of continuity (logical, temporal, and physical), whereas fault trees are most powerful in identifying and simplifying failure scenarios. Different characteristics of the system in question (e.g., a dam or a nuclear reactor) may guide the choice between fault trees, event trees, or a combination of the two. Some elements of this choice are examined, and observations are made about the relative capabilities of the two methods.

KEY WORDS: Reliability; fault trees; event trees; risk analysis.

1. INTRODUCTION

Risk analysis and reliability analysis are often based on identification and probabilistic evaluation of failure or accident scenarios. Ideally, one would like to identify all of them in a complete and systematic way. A failure scenario can be described by a sequence of events, some of them external (e.g., an earthquake) and some of them internal to the system (e.g., failure of a valve to open). These events can be displayed in different graphic forms. One convenient structure to encompass a family of scenarios is the structure of a tree (i.e., a graph without loops) representing a sequential progression of branching points at which several possibilities can be envisioned. Two particular structures of tree are of interest in reliability analysis: event trees and fault trees. It is proposed here to examine and compare their characteristics, the nature of the information that they provide in different cases, and the appropriateness of using one method or the other (or both) according to the characteristics of the considered system (time factor, continuity, nature of the initiating event, etc.).

An event tree is formed of a sequence of random variables (continuous or discrete) or event sets that can be associated with random variables (e.g., colors such as red, yellow, or blue that can be characterized as red = 0, yellow = 1, blue = 2, and a probability distribution defined over them). The branching point at which a new variable is introduced in the tree is called a node. Each node is followed by the possible realizations of this new variable, and its probability distribution conditional on values of previous random variables in the tree. The most common way of constructing an event tree is to use a deductive logic ("forward logic"); that is, starting with an initiating event, lay out all possible sequences of following events, and determine the outcome of each considered sequence. Because the probability of each event is displayed conditional on the occurrence of events that precede it in the tree, the joint probability of the

[1]Department of Industrial Engineering and Engineering Management, Stanford University, Stanford, California.

0272-4332/84/0900-0177$03.50/1

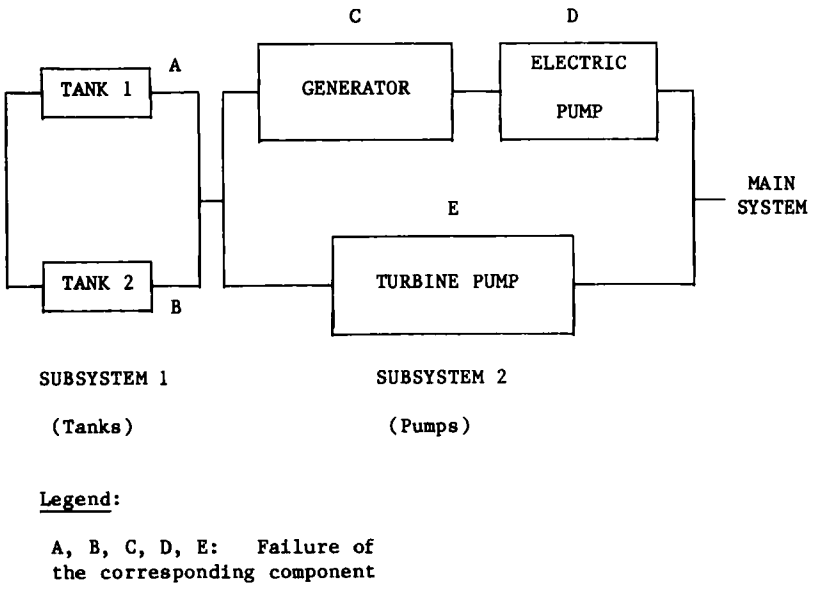

Fig. 1. Auxiliary feed water system: Block diagram.

intersection of events that constitute a sequence (or "scenario") is found by multiplication.

A fault tree is formed of events often described by binary (Boolean) variables (the event occurs or not) and related by logical functions, essentially OR and AND.[1] Graphically, these logical functions are represented by Boolean "gates" (see Fig. 1 and 2). The output of a gate (event represented immediately above the gate) is exactly equal to the Boolean function of the inputs of the gate (events represented immediately below). Each input event, in turn, can be the result of a logical function of a set of events, down to the point where all inputs are basic events that cannot be practically analyzed any further. One constructs fault trees by using inductive logic ("backward logic"), that is, by identifying a top event—failure of all or part of the system—and sequentially identifying unions or intersections of events that entirely describe each successive binary variable. Finally, what the fault tree allows one to obtain is a logical identity between the "top event" and a set of basic events. Then, on the basis of that identity, one can compute the probability of the top event as a function of the probabilities of the basic events. Phenomena that are not necessarily part of a failure scenario, but increase the probability of failure of the system, can be introduced at that stage. They may be external events, such as earthquake accelerations, or internal phenomena, such as a raise in temperature inside a system. The probability of the top event can then be computed conditional on the occurrence of these events at different "levels" if it is appropriate.

This difference, inductive vs. deductive logic, does not mean, however, that a fault tree is an "event tree backward." They have different structures and serve different purposes. A fault tree displays relationships among events. Consequently, the probability of the output of a logical gate is equal to the probability of the corresponding function of the inputs simply because they characterize the same event. Event trees, by contrast, display relationships among juxtaposed events on the basis of conditional probability. A chain of events ("path") in an event tree represents an intersection of even sets for the purpose of computing the probability of the joint event. A single path in a fault tree from the top event to one given basic event does not have, in general, any obvious meaning. By contrast with a path, a sub-tree in a fault tree represents the development of the logical function between the top event of that sub-tree and the basic inputs.

A characteristic of a system is its degree of continuity, its physical continuity, its temporal evolution, and the continuity of its failure states. Nuclear power plants have typically been modelled as discrete systems, that is, a combination of mechanical and electrical parts. When called into operation, each part can often be characterized by a binary state: it works or it does not. Multilevel or continuous states, when they appear, can be treated in the fault-tree methodology by extension of the simple logical gates men-

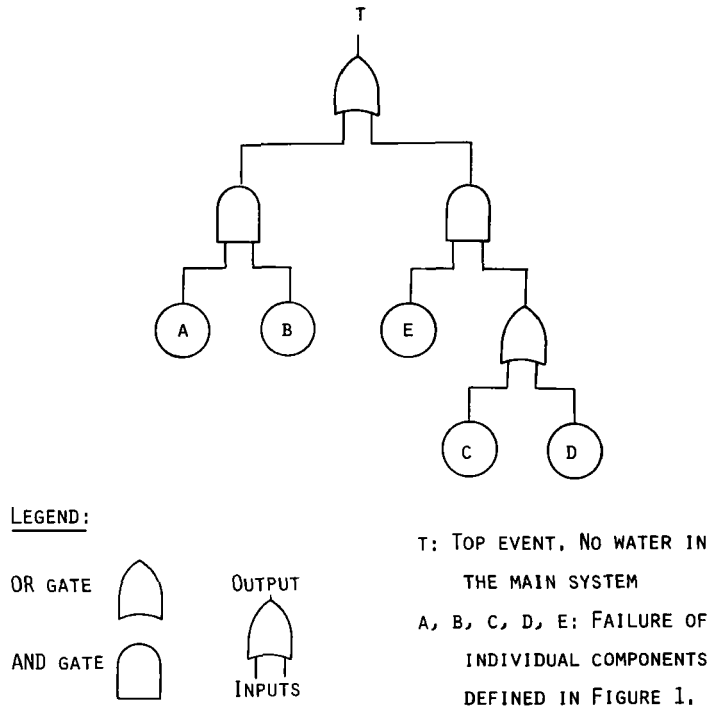

Fig. 2. Fault tree corresponding to the failure of the AFWS.

tioned above and by careful definition of functional failures.[2,3] Fault tree methodology is therefore quite adapted to this kind of mechanical system. Dams, by opposition, are constituted of continuous media (e.g., core, or embankments). Furthermore, failure modes, such as internal erosion in earth dams, are continuous processes in a continuous medium. Both fault trees and event trees are limited in their ability to approach physical continuity. Event trees, however, may give better insight into the contribution of different failure modes and external stimuli at different level of severity to the final failure probability of the dam. They can also better include probabilistic descriptions of the time of evolution, for example, the lead time between observation of deterioration signals and potential failure, and the probability that failure is avoided by appropriate actions.[4] It is interesting to observe the differences in the ability of the two methods to handle different characteristics of systems.

2. FAULT TREES

The easiest way to examine practical characteristics of fault trees is to start with a discrete system, then generalize to continuous systems.

Consider the block diagram in Fig. 1, a simplified representation of an "auxiliary feed water system" (AFWS) in a nuclear power plant.[5]

Step 1 — Construction of the Fault Tree

The top event being the failure to provide water, one can construct the fault tree as shown in Fig. 2. In this fault tree, each gate represents a logical function (OR, or AND). The output Boolean variable (i.e., event located just above the gate) is equal to the logical function of all input Boolean variables located just below the gate. This equality demands those and only those inputs that are necessary and sufficient to cause the output event.

Earthquakes, floodings, and other external events do not generally appear in the tree unless they are necessary elements of a failure mode. If they are not indispensable logical links in a failure mechanism, they may influence the failure probability of the components, but as will be shown below, they get eliminated from the tree by reduction of the Boolean polynomial.[2] (For a more formal definition of fault tree, see Barlow & Lambert.[6])

[2]No attempt is made in this paper to distinguish among what the literature calls "primary," and "control" failures.

Step 2 — Reduction of the Fault Tree

The object here is to reduce the expression of the top event into a standard form, namely, a union of simple intersections. Each such intersection is called "a min-cut set." A cut set is an intersection of events included in the top event, that is, an event of the type A AND B AND C...AND N, necessarily leading to the top event. A min-cut set is a cut set such that, if one event is removed from it, the occurrence of the remaining events no longer necessarily leads to the occurrence of the top event. To obtain the min-cut sets, one customarily uses Boolean algebra; each variable is zero or one, $\times$ means AND ($\cap$), $+$ means OR ($\cup$). Note that this is an inclusive OR, A OR B meaning A OR B OR both. The Boolean polynomial isomorphic to the tree is the following:

$$T = (A \times B) + E \times (C + D) \tag{1}$$

Using the property of distributivity of union over intersection, one obtains a Boolean polynomial of the form:

$$T = A \times B + E \times C + E \times D \tag{2}$$

One can sometimes reduce further this polynomial using laws of identity ($A \times A = A$, and $A + A = A$) and of absorption ($A + A \times B = A$). The form obtained after reduction displays the basic, irreducible failure modes (min-cut sets). Here, there is no further reduction of the polynomial and the min-cut sets are: A AND B (failure of both tanks), E AND C (failure of the turbine pump and the generator), and E AND D (failure of the turbine pump and the electric pump).[3]

Step 3 — Probability of the Top Event

Finally, probabilities are introduced. The probability of the top event calculated in terms of the sum of the probabilities of min-cut sets and their intersections is:

$p(T)$ = sum of probabilities of individual failure modes (e.g., $A \cap B$)
− prob. of "doubles" [2 failure modes at a time (e.g., $(A \cap B) \cap (E \cap C)$)]
+ prob. of the "triple" [the 3 failure modes at a time (e.g., $(A \cap B) \cap (E \cap C) \cap (E \cap D)$)]

$$p(T) = p(A \cap B) + p(C \cap E) + p(D \cap E) - p(A \cap B \cap C \cap E) - p(A \cap B \cap D \cap E) - p(C \cap D \cap E) + p(A \cap B \cap C \cap D \cap E) \tag{3}$$

In practice, in safety work, the probabilities of doubles, triples, etc., are typically smaller than the probabilities of basic failure modes, and the analysts may choose to truncate the calculation at singles, or doubles, or later. In the simplest case, when the component failures are independent events, the calculation of these probabilities is very easy.

2.1. Chronological Ordering of Failures in Fault Trees

The simple AND or OR gates defined above do not convey any notion of time ordering. The corresponding fault tree is a "snapshot" of the state of the system: that is, the basic components are in a failed state or not, and, as a result, the system is in a failed state or not. In other cases it is necessary to specify time spans and chronological order of events. Other types of gates allow some treatment of time in fault trees and in the tree reduction process, for example, "delay" gates and "inhibits".[7]

2.2. External Events

A fire that is a necessary step if the top event is defined to be "destruction of the system by fire," can appear in a fault tree. By contrast, an earthquake (which is neither a necessary nor sufficient contribution in cases in which the top event is simply "system's failure") may affect failure probabilities but does not enter the fault tree, which displays the mapping between the state of the components and the state of the system. That relationship does not depend upon the value of the "earthquake variable" should one even choose to define that variable to be included among the components.

For example, consider a simple system that depends upon the state of two parallel elements whose failures are noted A and B (see Fig. 3). Without

[3]All events which include system failure will have to include at least one of these three intersections.

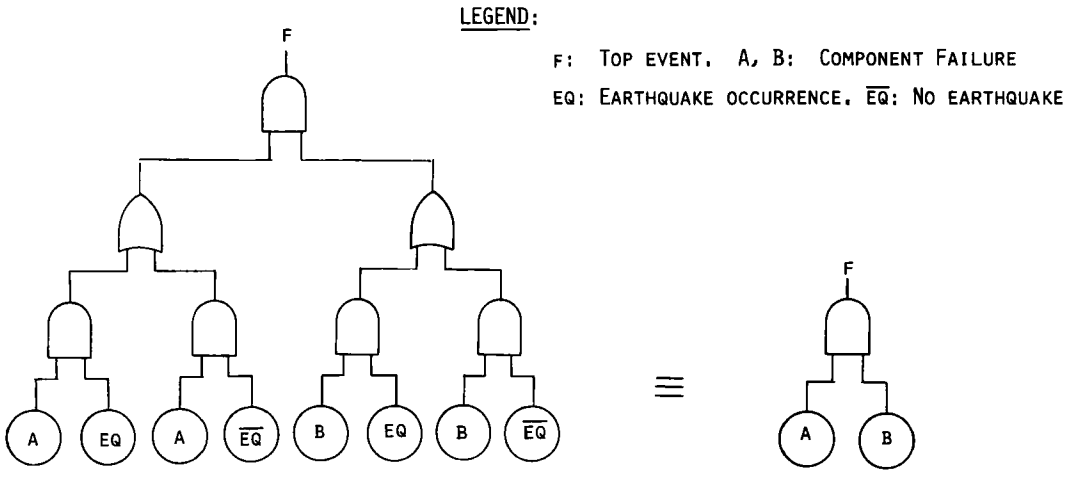

Fig. 3. Attempt to introduce earthquakes in the same fault trees.

introduction of earthquakes, F is equal to A AND B ($F = A \times B$). Failure A can occur with or without the earthquake. The same is true for failure B. Figure 3 shows the corresponding fault tree after introduction of events earthquake and no earthquake (EQ and $\overline{EQ}$). In the Boolean reduction, however, the variable EQ disappears from the logical relationship between F and the variables A, and B:

$$F = (A \times \overline{EQ} + A \times EQ) \times (B \times \overline{EQ} + B \times EQ)$$
$$= A \times B \tag{4}$$

The earthquake occurrence does enter the computation of the probability of the top event and constitutes a source of common mode (or common cause) failure. The probability of the top event and the probability of the basic events are conditional on the occurrence or not of the earthquake. In the case of the AFWS considered above, this can be written:

$$p(T) = p(T \text{ AND } EQ) + p(T \text{ AND } \overline{EQ})$$
$$= p(T|EQ) \times p(EQ) + p(T|\overline{EQ}) \times p(\overline{EQ}) \tag{5}$$

Considering only the first cut set A AND B one gets:

$$p(T) = p(A \text{ AND } B) + \ldots$$
$$= p(A \text{ AND } B|EQ) \times p(EQ) + \ldots$$
$$+ p(A \text{ AND } B|\overline{EQ}) \times p(\overline{EQ}) + \ldots \tag{6}$$

At that stage, one finds it sometimes convenient to use event trees to introduce the probability of fires, floods, earthquakes, and other external events in the computation of the total probability of the top event.

3. EVENT TREES

The construction and use of event trees is more straightforward. Considering the same auxiliary feed water system as before, the failure or not of each part can be considered sequentially (see Fig. 4) and constitutes the branches of the tree. External events, for example, earthquakes (EQ), can also be introduced directly in the tree. Each branch can be characterized by the probability of the considered event conditional on the occurrence of those that precede it in the tree. For example, the branches of the upper path of the event tree in Fig. 4 can be characterized successively by $p(EQ)$, $p(A|EQ)$, $p(B|A, EQ)$, $p(C|A, B, EQ)$, $p(D|A, B, C, EQ)$, and $p(E|A, B, C, D, EQ)$. The product of these six probabilities gives the joint probability of EQ, A, B, C, D, and E. The event tree enumerates all possible combinations of component states and external events. The analyst must then relate each of these component failure combinations to the state of the system (i.e., failure or no failure). It is important to note here that event trees are of no help in this task; that is, they do not indicate whether or not an intersection of events actually leads to system failure. Either the system is simple enough, as in the example above, and the mapping can be done

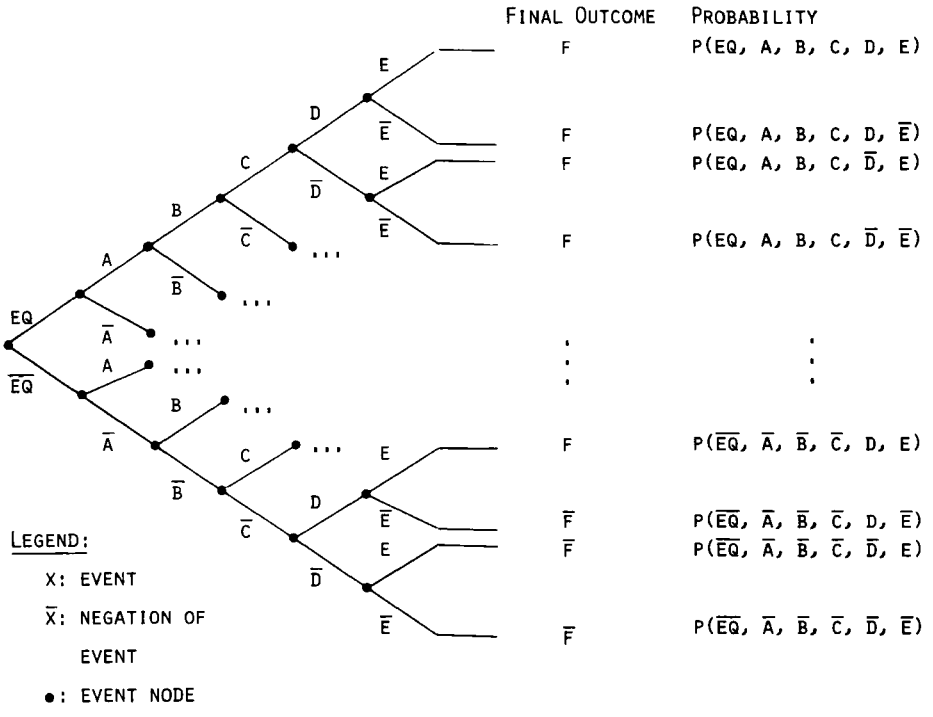

Fig. 4. Event tree (F: failure of the AFWS).

for each scenario without more formal analysis, or the system is more complex and fault trees have to be used to identify the failure modes. The probability of failure of the system (F) is then the sum of the probabilities of the sequences of events leading to F.

This method, however, can be cumbersome if it is not applied carefully. That is why, if the problem stops at the computation of the probability of system failure, one may prefer to use logical (fault) trees and to introduce external events in the probability computation. If the problem involves other random variables that affect failure consequences, event trees allow a more global approach to risk assessment. For example, an earthquake may slow down the evacuation process around a nuclear power plant and increase the human losses should a radioactive release occur at that time.

3.1. Continuity in Event Trees

The word "tree" conveys the idea of a finite number of branches at each node. There is no conceptual problem, however, in the introduction of a continuous random variable in an event tree.[8] Graphically, one represents the spectrum of possible values of the continuous variable by a fan originating at the event node. Instead of a discrete conditional probability distribution, one uses a continuous conditional probability density function and graphically develops the tree conditional on one particular value of the continuous variable. One then generally obtains continuous joint distributions as a result of the event tree analysis. Continuous random variables of this type can be, for example, the annual maximum 24-hour rainfall on a dam's watershed basin or the annual maximum peak ground acceleration in earthquakes at a given site. One can then compute the joint probability of system failure and a given level of rain (or peak ground acceleration), and, finally, the probability of system failure by integrating overall possible values of rain (or acceleration) levels. In practice, it may be more convenient for computational reasons to make discrete a continuous random variable, but theoretically at least it is not necessary.

3.2. Reordering of Event Trees

A natural way to construct an event tree is to place events in the chronological order in which they occur, if this order is unique and known. To facilitate

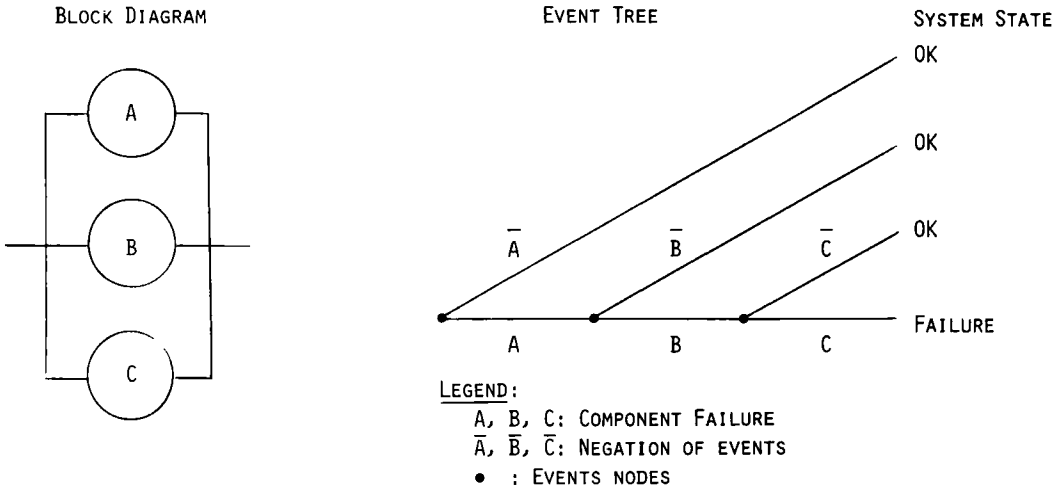

Fig. 5. Simplification of an event tree (by absorption law).

the probability calculation, however, another order may be preferable. The "best" order depends on the information available [e.g., $p(A|B)$ or $p(B|A)$]. The event tree structure requires only that each event be defined by its probability, conditional on the occurrence of the events that precede it *in the tree*, and not necessarily *in time*. In other terms, the selected structure of an event tree is not defined by event relationships ('AND's, 'OR's, etc.), but by (convenient) probabilistic conditionality (which may or may not reflect time). Certain component events or simple intersections (e.g., just an $A \cap B$) may imply system failure (or success) no matter what the outcome of other events. Then a convenient tree is formed by putting these events first in the line because the subsequent branching need not be developed in detail. In this case, relationships may affect tree construction (simplification). Examples can be found in WASH-1400[9] where some event trees have the type of structures shown in Fig. 5.

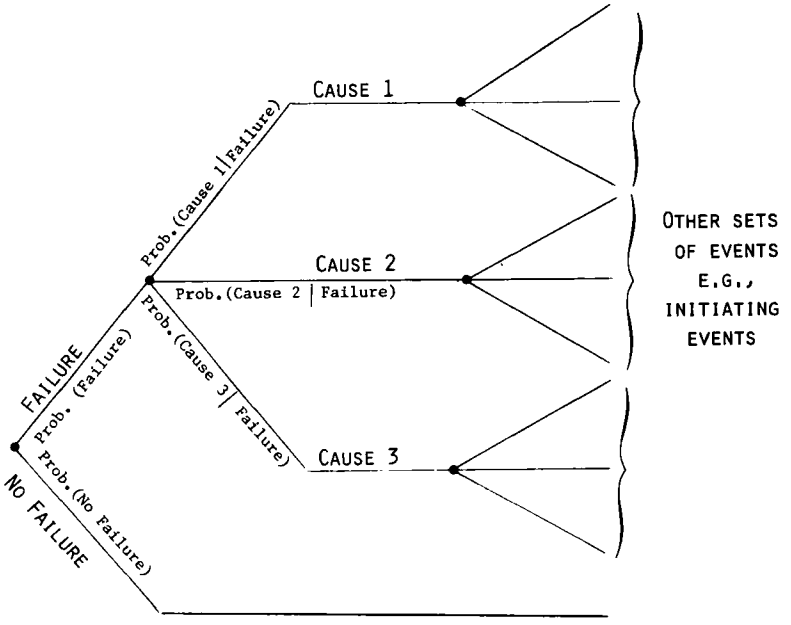

Fig. 6. Re-ordering of events in an event tree.

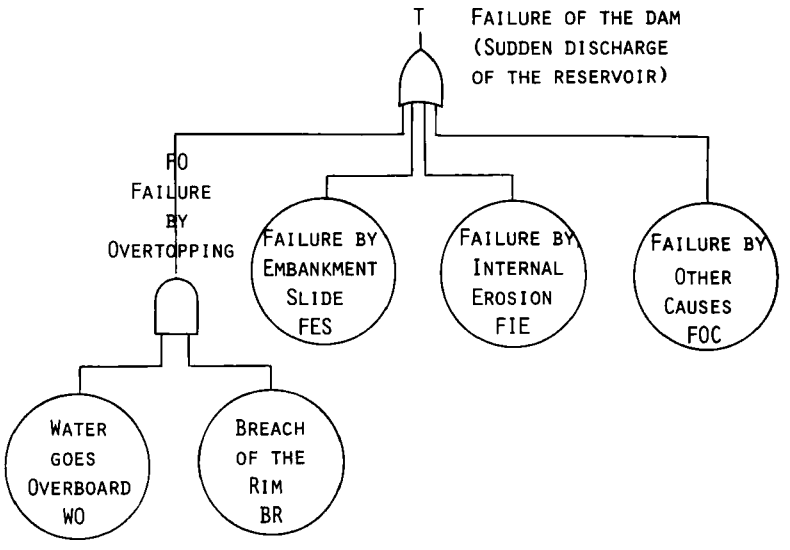

Fig. 7. Simple fault tree corresponding to the failure of a dam.

Another example of rearrangement of event trees can be found in a study of the risk of dam failure[4] where it was clear that a convenient order of events was, first, failure or not of the dam, and then the failure cause (for example, overtopping, internal erosion, or embankment slide; see Fig. 6). This is true simply because the probability of each cause conditional on failure can be easily derived from statistical observations reported in the literature.

Another example of reordering of event trees can be found in a study of earthquake prediction[10] where, for information reasons, predicted magnitudes were studied conditional on occurring magnitude (therefore reversing the chronological order of events). There is in fact a whole literature on the art of "trimming," and "rearranging" event trees (e.g., on "influence diagrams,"[3] and on "pruning" event trees[1]).

4. CONTINUOUS SYSTEMS, EXAMPLE: DAMS

To analyze dam failures one may attempt to use a fault tree technique, but there are two major limitations to the applicability of this method: the physical continuity of the dam medium and the poorly known nature of the failure mechanisms.

Figure 7 shows how the known failure modes for a dam simply become the basic events of the corresponding fault tree. Unless one knows (and wants to introduce) more about the internal failure mechanisms, this is all fault trees can give in this case. The basic failure modes, as identified here, simply become the basic logical elements.

The logical polynomial of the top events is:

$$T = WO \times BR + FES + FIE + FOC \tag{7}$$

In terms of probability, this leads to:

$$\begin{aligned} p(T) = {} & p(WO \text{ AND } BR) + p(FES) + p(FIE) \\ & + p(FOC) \\ & - p(\text{doubles}) + p(\text{triples}) - p(\text{quadruple}) \end{aligned} \tag{8}$$

If the analysis is concerned with seismically induced failures of the dam, one can introduce at this point the effect of earthquakes as external stimuli. The failure probability, conditional on an earthquake intensity of a given level, is the following (assuming that p(doubles), p(triples), and p(quadruple) are negligible):

$$\begin{aligned} p(T|EQ) = {} & p(WO \text{ AND } BR|EQ) + p(FES|EQ) \\ & + p(FIE|EQ) + p(FOC|EQ) \end{aligned} \tag{9}$$

The same is true for the occurrence of a rainstorm of given "intensity":

$$\begin{aligned} p(T|RS) = {} & p(WO \text{ AND } BR|RS) + p(FE|RS) \\ & + p(FIE|RS) + p(FOC|RS) \end{aligned} \tag{10}$$

Other probabilistic methods then have to be used to compute the probability of each failure mode, with and without the occurrence of external events; for example, one would have to do a continuous stochastic modelling of internal erosion and a continuous modelling of failure probability for different levels of seismic loads and different stages of piping. Indeed, neither fault trees nor event trees are sufficient in this case. Fault tree methodology only provides a relationship between probability of failure, probability of external events, and probability of the different failure modes. If one chooses to use event trees, it would have to be in conjunction with other techniques of stochastic modelling. Event trees, however, allow one to expand the scope of a reliability study to include, for instance, the effect on the overall safety of a dam of a given monitoring program. In this example, the observation of early signals of internal erosion (e.g., muddy springs at the bottom of the structure) with sufficient lead time can allow one to take appropriate measures, and perhaps avoid a failure which would have occurred otherwise.[4] Such scenarios, which can be analyzed in a similar way for discrete systems as well, are treated by event trees because the links among events can only be expressed by probabilistic conditionality (e.g., the lead time given signal observation).

5. CONCLUSION

Both event trees and fault trees are useful tools of reliability analysis. Fault trees can be used to identify the sets of events leading to system failure. Combined with techniques of Boolean algebra and probabilistic analysis, they can also be used to compute failure probabilities. Event trees can be directly used to compute probability distributions of various outcomes once the failure modes have been identified.

Event trees, in theory, appear to be more flexible than fault trees: for example, they allow one to introduce directly time factors, continuous random variables, and to use inductive as well as deductive logic. But they are much more cumbersome than fault trees because the number of branches may become very large. Logical functions in fault trees allow one to obtain a much more concise form of combination of events leading to failure of any subsystem.

For large mechanical systems, in which the different parts are easily identifiable, and in which each subsystem or element can be considered to be in a state of either failure or no failure, fault trees are appropriate. Difficulties may arise when "common cause failures" may occur.[11] One solution is then to use *both* fault tree and event tree techniques. That is what was done for the study of the safety of nuclear reactors (WASH-1400).[9] First, accident sequences were defined by event trees; then, fault trees were logically combined according to these sequences; the corresponding Boolean polynomials were established and simplified; finally, the probability of failure was computed for the desired accident sequence.

For continuous systems such as dams, neither fault trees nor event trees are easy to use in the present state of the art to improve the understanding of each failure mechanism. In all cases, however, external phenomena, human interventions and other events, when they are not essential elements of a failure mode but modify the failure probability of the different subsystems, are better handled by event trees.

ACKNOWLEDGMENT

This work was supported in part by the Center for Energy Policy Research, Massachusetts Institute of Technology, Cambridge, Massachusetts.

REFERENCES

1. E. J. Henley and H. Kumamoto, *Reliability Engineering and Risk Assessment* (Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1981).
2. M. N. Fardis and C. A. Cornell, "Analysis of Coherent Multistate Systems," *IEEE Transactions on Reliability* **R30**, 117–122 (June 1981).
3. Stanford Research Institute, Decision Analysis Group, "Development of Automated Aids for Decision Analysis," (ARPA Contract, 1976).
4. M. E. Paté, "Risk Benefit Analysis for Construction of New Dams: Sensitivity Study and Real Case Application," Research Report No. R81-26, (Department of Civil Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1981).
5. C. A. Cornell and N. M. Newmark, "On the Seismic Reliability of Nuclear Power Plants," *Proceedings of the Topical Meetings of the American Nuclear Society on Probabilistic Analysis of Nuclear Reactor Safety* Vol. 3, (Los Angeles, California, May 1978).
6. R. E. Barlow and H. E. Lambert, "Introduction to Fault Tree Analysis," *Reliability and Fault Tree Analysis* (SIAM) (United States Nuclear Regulatory Commission, 1975) pp. 7–35.
7. United States Nuclear Regulatory Commission, *The Fault Tree*

Handbook (NUREG/0492, 1980).
8. J. E. Matheson, "The Economic Value of Analysis and Computation," *IEEE Transactions on Systems Science and Cybernetics* **SSC-4**, 325–332 (September 1968).
9. United States Nuclear Regulatory Commission, "Reactor Safety Study, WASH-1400," (NUREG-75/014, Appendix II, Section 2, 1975).
10. M. E. Paté and H. C. Shah, "Public Policy Issues: Earthquake Prediction," *Bulletin of the Seismological Society of America* **69**, 1533–1547 (1979).
11. United States Nuclear Regulatory Commission, "PRA Procedures Guide," (NUREG/CR-2300, 1983).