RECEIVED BY TIC MAR 26 1973

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Atomic Energy Commission, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

THE FAULT TREE AS A SAFETY OPTIMIZATION DESIGN TOOL *

Charles W. Griffin

Atomics International, A Division of Rockwell International
Canoga Park, California

ABSTRACT

Fault tree, after a very encouraging start nearly six years ago in nuclear reactor development, appeared to decline into very limited use. Some work on the Heavy Water Organic Cooled Reactor was quite successful in defining the relative safety of two containment concepts. The technique was applied to evaluation of added risk for the general public due to construction of a large sodium test facility. These two studies are discussed in detail. The techniques developed are then applied to construction of a fault tree for evaluation of both on-site and off-site risk to the owner of accident consequences in operating a large test facility complex. Recently suggested criteria are applied.

DISCUSSION

Fault Tree evolved in the early 1960's and was expanded into a very effective tool for coordinating design, reliability and safety efforts of ten major sub-contractors functioning under the overall management of Boeing in the development of the Minute Man missile. In 1965-1966, fault tree was introduced to the nuclear power development industry as a potential tool for instilling better logic and coordination in the safety design optimization and cost reduction for the design of new nuclear power facilities. However, the results fell far short of expectations as compared to its success in missile development. Inexperience in handling this tool, as demonstrated by reactor design engineers through the very poor and unreliable results emanating from these studies, caused backers to become quite skeptical of fault tree methods. The skepticism was accelerated by too early an attempt to develop and apply super-sophisticated numerical techniques to fault tree event probability evaluation before even the poorest statistical data on nuclear facility component failure expectation was available. Thus, after a very encouraging start by most of the reactor developers and some of the national laboratories, its application appeared to decline into very limited use by only its dedicated proponents. In watching its progress, I tended to sympathize with those persons who were expressing extreme skepticism as to validity of results. Too many people were attempting to apply these very poor statistical data to very complex systems and endeavoring to make management believe the results in spite of inapplicability of both the data and the assumptions made. During these early days it was not at all unusual to hear the fault tree proponents referred to as the four nine's boys or to hear their technical presentations referred to as being extremely impractical.

Until this year very little practical fault tree work in the nuclear field has been reported either as publications or technical papers for the last four or five years. At the recent International Joint Conference of the ANS/AIF in Washington, I was pleasantly surprised to hear fault tree referred to at least once in every session that I attended. There seems to be a strongly rejuvenated

*Work sponsored by the U.S. Atomic Energy Commission under contract with Rockwell International Corporation.

interest in fault tree applications and the associated concept of risk evaluation. It was obvious from listening to the papers that some very excellent, as yet unpublished, work was being done. Also, renewed academic interest was demonstrated by the existence of several student papers. Overall evaluation of presentations, however, substantiated the conclusion that today, just as yesterday, very few people know how to use the fault tree as a practical visual aid to decision making.

My intent in this presentation is to illustrate simple techniques which have been used in applying fault tree to speed up, simplify, and verify safety optimization in the design of new nuclear power plant concepts and to demonstrate its applicability to resolution of the relative risk involvement. Three basic applications are illustrated: (1) comparison of relative safety of two similar containment systems; (2) comparative risk increase to the public given a source of toxicological release; and (3) an example of fundamentals in setting up the fault tree for analysis of the environmental risk of a potential incident in an industrial complex.

COMPARISON OF THE RELATIVE PROTECTION AFFORDED THE GENERAL PUBLIC BY THE CONTAINMENT CAPABILITY OF TWO SIMILAR CONTAINMENT SYSTEMS

Fault Tree was applied¹ to fundamental optimization studies of protective systems and to the safety analysis of the heat transfer and containment systems for the Heavy Water Organic Cooled Reactor (HWOCR). Since this reactor was never built there was no opportunity to present these findings to ACRS or to subsequently defend these findings. In the preliminary studies reported in Reference 1, the inherent visibility which makes fault tree such an excellent empirical tool was used rather than numerical methodology. Having properly selected his undesirable event, a good fault tree engineer must learn to make use of all the expertise at his disposal to optimize and improve the protective aspects of his fault tree through empirical application of the good engineering judgment of experts in the various disciplines available to him. Numerical analysis, if any, should be deferred until all empirical avenues of technical judgment have been exploited to the fullest extent. Fault tree was used exclusively and very effectively throughout the entire preliminary design work of this reactor. Application of technical judgment in the placement of inhibitor "and" gates within the respective fault trees made it unnecessary with one exception, to resort to numerical analysis in order to select between one protective design concept and another as being the most effective method of preventing a given undesirable event. The exception was related to the necessity of establishing the most reliable containment criteria. Two options were proposed. One would place the steam generators within the containment vessel, and the other would place the steam generators outside the containment vessel in an auxiliary containment building. The problem was to determine by some method which concept afforded the public the greater protection irrespective of cost. The basic fault tree had already been developed in empirical studies. It became painfully evident from the onset that it was going to be very difficult to develop a numerical method of evaluating the relative advantages or relative protective aspects of the two concepts. First, almost no formal data had been recorded on the expected reliability of containment components in reactor facilities. Fortunately, Holmes & Narver had just completed some preliminary studies on containment penetration, component failures, and maintenance frequencies at Dresden, Indian Point and Yankee. Holmes & Narver was very cooperative in affording a preliminary draft of their publication² on this work. The numerical data therein, weighted and adjusted for this study, constituted at least half of the component failure data applied. Second, the necessity immediately evolved of obtaining good unbiased design counsel as to what changes really have to take place when you expanded one containment concept to probably twice its size. That is, if you doubled the size of the vessel and the heat input to its ventilation system, you must at least double the ventilation system. Does this mean that you put in twice as many penetrations of the same size with the same reliability as the smaller system penetrations or do you enlarge the capacity of the single system? If the latter, can you apply the same expectation of failure to the larger ventilation system isolation valves as you had applied to those of the smaller

systems? This particular question was resolved by saying that we would go to the larger system as long as the size of the isolation valves did not exceed those which could be readily obtained from normal sources. Given similar experience in industry there should be approximately a similar expectation of failure. Many other more localized technical judgment type problems developed and had to be resolved by some empirical methods as the analysis progressed. Some of these are touched on as we follow through the example. The problem of interest was to analytically determine the relative probability of the undesirable event "Excessive" Radiological Release to the Environs," given a design base accident. Analysis of this undesirable event focused on evaluation of the relative integrity of containment penetrations in the two containment concepts.

Certain assumptions were made in order to establish rules for comparison during the safety studies, 1) the fundamental design of containment for both cases is the same, 2) acts of God (sabotage or missiles are ignored as equally probable for both), 3) similar components have identical maintenance, inspection, and failure expectation, 4) the λT method of fault tree analysis is applicable and 5) maximum duration of the DBA is 30 days.

Development of the fault tree was no simple matter. It required availability of highly qualified personnel experienced in both fault tree development, statistical analysis, and particularly knowledgeable with respect to heat transfer systems. They also had to have had actual power plant operation experience and understand the fundamentals of system and reactor protection. Implementation of safety and reliability through protective inhibitors and optimization of inspection periods are the tools by which the fault tree is manipulated. If you have all "or" gates you have no protection. The analyst must have the knowledge to implement "and" gates, through use of practical design methods and conventional hardware, in order to inhibit the propagation of the "undesirable event." Figures 1 and 2, from Reference 1, show schematics of the relative differences in containment penetrations. These figures also demonstrate the required level of complexity which, while simple, yet afford almost complete visibility in identifying potential problem areas. These fault trees were constructed through use of empirical analysis, considering specific failure modes and protection devices. Additional fault trees are developed in Reference 1 for the three undeveloped rectangles of Figure 1. One of the hardest tasks for the novice to accomplish in fault tree development is that of selecting, to head each sub-branch, a specific "undesirable event" such that it is amenable to ready system analysis. Development of a slightly different undesirable event could lead to excessive frustration and fruitless effort in the fault tree construction.

One numerical problem is establishment of failure rates for standby safety equipment which, hopefully, will never be required for use, and has a limited inspection period. A failure discovered by inspection affords little information of actual time of failure. If checked often and a failure is observed, much better information on life expectancy is observed. Reference 2 indicated that containment vessel standby equipment inspection periods varied in frequency from months to annually. Some method of weighting the data was required. A search of the literature revealed a paper by B. Epstein and M. Sabel³, which gives a mathematical expression and a table for evaluating life expectancy given r failures out of a sample of n for both the case of no replacement (no repair) and constant replacement (repair) based on an assumed exponential distribution of life. Extensive use was made of this approach.

Data sources have improved very little since this work was done, and the methods applied six years ago appear equally applicable to present situations. It is to be hoped that new data collection systems just getting underway by such institutions as EEI and others will, over the years, begin to alleviate this problem. Yet, as will be seen, good judgment and a little data can go a long way in many applications. For this study, the DBA was defined as gross fuel damage within the core coincident with a breach of the primary coolant system and subsequent release of radioactivity to the containment vessel atmosphere. The modified fault tree networks used in the analysis were developed to highlight these fault

7680-15200

Figure 1. Excessive Radiological Release to Environs

Figure 2. Failure of Containment Structure

sequences which were specifically applicable to the study. As examples of this simplification: 1) the branches of the general fault tree involving fires, earthquakes, etc., have been deleted (because of lower probability levels; and 2) the lower components on some branches such as wear and minor malfunctions have been combined into a higher level composite failure rate for the total subsystem or component because available failure rate data does not identify failure mechanisms to this level of detail. Many of these composite subsystem failure rates are obtained from EEI publications.⁴ Many innovations were used to arrive at reasonable values for expected failure rates due to the lack of good failure data sources. The one most consistently used was that of comparison of components having unknown failure rates with similar components having known failure rates. This method evolved early in fault tree development and in particular for mechanical components for which very little data have been collected. The classical method was to set an expert or experts before a blackboard and sketch a graph in ascending order of components with known failure rates. The component with unknown failure rate was then introduced and an attempt made to use the knowledge and experience of the experts to place the unknown on the graph. It was surprising how well this method worked. In our case we said that if the unknown component was quite similar in performance, general construction and in environmental operational function, then the failure expectancy of that component should be no greater than the known component. This was a somewhat more conservative approach than used in the described technique. The failure rates of some of the components were readily seen to be so small by comparison with known components within a system that the failure rate could essentially be set equal to zero in a particular branch of the fault tree. As a typical example of numerical development, one critical branch of a major fault tree in Figure 2 has been selected in order to show specific details of the analysis, and the application of very limited and questionable failure rate data. One of the most critical sub-branches of the fault tree, in the comparison analysis, was that associated with "Air Lock System Failure," as the local undesirable event. The expanded fault tree for the subsystem undesirable event "Air Lock System Failure" is shown in Figure 3. Most of the numerical values were obtained from the Dresden portion of the data in Reference 2.

Reference 3's method of weighting, coupled to the 'percent time failure method'² assumption that, if a failure is observed in time T, it has equal probability of having failed at any period since the last inspection, thus a conservative assumption is that it failed at time = T/2, (i.e., it is highly probable that twice the inspections would have discovered no more failures) permits weighting of such data as that obtained by H&N for standby protective equipment.

Epstein and Sabel give the weighting factor for r failures out of a sample of n as

$$\alpha_{r,n} = \frac{E(X_{r,n})}{E(X_{r,r})}$$

where $E(X_{r,n})$ is the expected time to observe r failure of n events. If constant repair is assumed, the numerator becomes:

$$E(X_{r,n}) = \theta r/n$$

where θ is the true life expectation. The best evaluation of life expectation is obtained by permitting r failures to occur on a sample of r, with no repair, and measuring the total time, $E(X_{r,r})$. This is given by

$$E(X_{r,r}) = \theta \left[\sum_{j=1}^r \frac{1}{r-j+1} \right]$$

- A. 2 DOORS OPEN BY OPERATOR ERROR
- B. INTERLOCK FAILURE
- C. EQUALIZER VALVE LEAKS
- D. 1 DOOR LEFT OPEN (OPPOSITE DOOR FROM EQUALIZED VALVE)
- E. DOOR HAS LEAKY GASKET (OPPOSITE DOOR FROM EQUALIZED VALVE)
- F. ELECTRICAL PENETRATION LEAK

*SUBSCRIPTS IMPLY VALUES $E_1 \neq E_2$, $C_1 \neq C_2$

LMEC90021

Figure 3. Air Lock System Failure

Then, for constant repair

$$\alpha_{r,n} = \frac{\theta \cdot r/n}{\theta \sum_{j=1}^r \frac{1}{r-j+1}}$$

At Dresden, an observation of ventilation valves functioning properly showed that of 43 tests at intervals of about 36 days, 2 failures were observed in the 4 systems. Using the "percent time failed method," the probability of failure at any one test if tested every 36 days is:

$$Q = \frac{r}{43m \times 2} \quad \begin{matrix} r = 2 \\ m = 4 \end{matrix}$$

(actual $n = 43 \times m$ but the $T/2$ assumption gives $n = 43 \times m \times 2$).

$$Q = \frac{2}{43 \times 4} \times \frac{1}{2} = \frac{1.16 \cdot 10^{-2}}{2} = 5.8 \times 10^{-3}$$

$$\lambda = \frac{Q}{\tau} = \frac{5.8 \times 10^{-3}}{36 \times 24} = \frac{5.8 \times 10^{-3}}{864} = \underline{6.7 \cdot 10^{-6}/hr}$$

where $\tau = T = 36$ days,

or, $\lambda = 6.7 \times 10^{-6} \times 2 = 1.3 \times 10^{-5}/hr$

assuming $\tau = \frac{T}{2} = 18$ days.

Applying the weighting function method

with $\tau = T = 36$ days

$$\frac{r}{n} = Q = 5.8 \times 10^{-3}$$

$$\sum_{j=1}^2 \frac{1}{2-j+1} = \frac{1}{2} + 1 = 1.5$$

$$\alpha_{r,n} = 3.87 \times 10^{-3}, \quad \theta = \frac{\tau}{\alpha_{r,n}}$$

$$\lambda = \frac{1}{\theta} = \frac{\alpha_{r,n}}{\tau} = \frac{3.87 \times 10^{-3}}{864} = \underline{4.48 \times 10^{-6}/hr}$$

Dresden's data on air locks

Initial preparation test March 1958

Subsequent tests

Jan	1961
Oct	1961
March	1963
Oct	1963
May	1964

Total time 6 years 2 months = 54,050 hours

Hours per inspection 10,810

Failures which could have caused loss of integrity

	<u>Personnel (2)</u>	<u>Airlock Equip.(1)</u>	<u>Emerg.(1)</u>
Door gaskets	3	1	0
Equalizing valves	1	1	1
Electrical & pipe penetrations	0	1	1

Evaluation

Personnel Air Lock

$$r = 3$$

$$n = 4 \text{ (gasket)} \times 5 \text{ (tests)} \times 2 = 40$$

$$\frac{r}{n} = \frac{3}{40} = 0.075$$

$$\sum_{j=1}^3 \frac{1}{3 - j + 1} = \frac{1}{3} + \frac{1}{2} + 1 = 1.83$$

$$\alpha_{3,40} = \frac{0.075}{1.83} = 4.1 \times 10^{-2}$$

$$\lambda = \frac{1}{\theta} = \frac{\alpha_{3,40}}{\tau} = \frac{4.1 \times 10^{-2}}{10,810} = \underline{3.8 \times 10^{-6}/\text{hr}}$$

Equalizing values

$$r = 1$$

$$n = 40$$

$$\frac{r}{n} = 0.025$$

$$\sum_{j=1}^1 \frac{1}{1 - j + 1} = 1$$

$$\alpha_{1,40} = 0.025$$

$$\lambda = \frac{2.5 \times 10^{-2}}{10,810} = \underline{2.3 \times 10^{-6}/\text{hr}}$$

Electrical or pipe penetration failures of this type on the other less used doors indicate an expectancy of at least 1 even though no actual failures were observed. Therefore,

$$\lambda = \underline{2.3 \times 10^{-6}/\text{hr}}$$

Equipment air lock

Door gaskets

$$r = 1$$

$$n = 2 \times 5 \times 2 = 20$$

$$\frac{r}{n} = 0.05$$

$$\alpha_{1,20} = 0.05$$

$$\lambda = \frac{0.05}{10,810} = \underline{4.6 \times 10^{-6}/\text{hr}}$$

Valves

$$r = 1$$

$$n = 20$$

$$\lambda = \underline{4.6 \times 10^{-6}/\text{hr}}$$

Penetration (same)

$$\lambda = \underline{4.6 \times 10^{-6}/\text{hr}}$$

Emergency air lock

(Essentially no failures)

For the air locks the optimum test period appeared to settle down to about 8 months or

$$\tau = \underline{5840 \text{ hrs.}}$$

Yankee Air Locks

No normal access (emergency and inspection only during power operation).
Average about 1 entry per week.

1 personnel access gasket failed due to icing in a period from Jan 61 to Feb 65 with approximately annual inspections.

$$n = 1$$

$$m = 4 \times 4 \times 2 = 32$$

$$n/m = 0.03$$

$$\alpha_{1,32} = 0.03$$

$$\tau = 8760$$

$$\lambda = \frac{0.03}{8760} = \underline{3.5 \times 10^{-6}}$$

Indian Point (March '62 to November '64 - 31 months)

Continues leak rate monitors
No access during operation

Total access ports

- 2 personnel
- 3 equipment
- 1 maintenance
- 6 emergency

In 31 months, 2 small leaks but within tolerance, found in 80 inspections.

Fuel handling lock failed to close once

Indian Point data generally not applicable due to lack of air lock usage.

The λr method is then applied to analysis of the fault tree for each containment configuration. The differences in the configuration for this example, would be only the number of access ports of each type that would be considered necessary. From this study it is seen that with a little innovation, ingenuity, and application of standard techniques, very exacting information can be obtained for comparative optimization and safety evaluation even when the statistical data available for use is both poor and of non-existence statistical quality.

Techniques which have been employed in other studies, not this one, in an attempt to obtain a better fix on the expectation of failure of components are: the bull session with experts (previously discussed), and the application of Bayesian statistical methods. LMEC evaluated EBR-1 component failure rate histories, by the bull session method since there was no written record. The personnel at Argonne National Laboratories, who had worked and operated the EBR-1, were called together at a large conference for three days and asked to remember all of the experiences that they could think of related to the sodium components and their problems. The reason for pulling the people together at the same time was to avoid the possibility that each would remember something in a different manner and that the conclusion obtained from individual's knowledge would be that two different events had occurred rather than one. Bayesian statistics is a completely different approach. In this case there is a certain amount of information on the expected failure of a class of components. However, the information may or may not be directly applicable to the expected use or environmental condition in which the new system will be applied. In this case, additional tests for information under expected environmental conditions are planned using the knowledge previously obtained as an apriori value. To date very little has been done with Bayesian statistical application to mechanical systems, but it has a good potential.

RISK - AS A LIMITING BASIS

I would now like to explore the concept of risk. Since my first exposure to nuclear reactor safety and the concept of the Maximum Credible Accident, safety engineers, managers, and reliability experts have attempted to apply the concept of expectation of an accident vs. associated risk to the general public, to operations personnel, and to other facilities. We, as individuals, apply this type of thinking to our every day activities by the level of risk exposure we are willing to accept in going about our daily work, wherein some risk of both accident and death are always present. However, it has been known to be very difficult to deliberately set up a potential accident and ask the general public to accept this additional risk unless it can be proven that the substantial benefits claimed are in truth existent and worth the risk. Risk has been an increasingly popular subject at each of the ANS sessions for the last year or more. The last session presented several excellent papers on the subject. I will briefly review some of these and show how these concepts have been used in the past and how they can be practically utilized in your own studies. In the Joint ANS/AIF session on How Safe is Safe Enough - and Why, two papers were of particular interest. One by Dr. Chauncy Starr formerly with UCLA and the other by Dr. Herbert Ley, Medical Consultant to the Food and Drug Administration. Dr. Starr expanded the fact that a study of the public acceptance of mortality risk arising from involuntary exposure to sociotechnical systems indicates that our society has accepted a rather broad range of risk exposure as a normal aspect of our normal life. His gross analysis indicated that, for a benefit per capita exceeding only a few hundred dollars, a natural hazard annual mortality risk of one per million people was readily acceptable. That for a per capita benefit of 10,000 to \$100,000 the mortality risk of 1,000 to 10,000/per million might be acceptable, but any risk greater than this might not be acceptable irrespective of the magnitude of the benefit. The latter magnitude of mortality risk is that presently associated with death due to disease. Dr. Ley in his presentation pointed to the extreme difficulty the public is encountering in attempting to assess the potential risk associated with the obvious benefits accrued through food processing. Fundamental to the difficulty the public has in individual assessment of risk, is the consistently conflicting advice on potential risk released by the food processing/protective

officials vs. that which is obtained by technical hypothesis. He reiterated the need expressed over the recent years by many others for a "Supreme Court" of science for public safety. Such a court, it is hoped, would be independent of public pressure and thus would avoid the natural biases that are inherent with public officials or special purpose organizations active in exerting political pressure to attain their special ends.

This general concept of comparing relative risk known to be acceptable to the public with that which may be additionally imposed on the public due to a new construction was applied by one organization in 1970. The relative additional risk that might be incurred by the public due to the construction of a large sodium test facility planned for construction at a field laboratory was evaluated. The reference accident considered for the safety analysis report was a large sodium fire following a sodium spill. Its magnitude and potential toxicant effects upon operations personnel and the closest center to the facility were the subjects of evaluation.

The classic approach of the DBA is not readily applicable to this type of study in that there is no radiological release nor is there the extremely low leakage type of containment required for radiological safety. The mechanism of toxicological release is from a pool of sodium, burning at a predictable burning rate and releasing toxic sodium oxides to the environs. Therefore, a new reference base had to be initiated and applied while maintaining the political expedients of reference to a design base accident. The method selected was to limit the probability of toxic release and of its transportation to the nearest population center to a risk level that was at least an order of magnitude less than that which the general public accepts on a routine basis.

A simple fault tree was constructed in order to readily visualize the potential for a fire, the potential for release, and the options for inhibiting each (Fig.4). in the process of analysis of the fault tree, the size of a fire that could be tolerated, under the worst meteorological conditions, and still limit the toxic concentration at the population center to that permissible by state regulation was determined. By concentrating the assumed sodium spill in a grid catch pan arrangement with an area of 150 square feet or less the effluent from a fire would be limited to within both long and short-term tolerance limits. A considerable amount of meteorological analysis and on-site topographic measurement went into this study.

Many of the events illustrated in Figure 4 obviously have a probability of one; such as the "sodium ignition temperature", and "adequate oxygen" for the normal air atmosphere of the building under study. Nevertheless, these are important to good thinking in fault tree construction and should be included. It is these events who's high or unit probability may be reduced by expensive facility design changes if, in the process of analysis, it becomes impossible to prohibit the undesirable event by any reasonable means. In fact, during this study, such ideas as automatic building isolation and self-smothering of the fire due to building oxygen depletion were considered. It is obvious from the fault tree that the probability of a sodium spill must be evaluated for the specific sodium system, and that reasonable failure rates of other sodium facilities operating under similar operating conditions must be obtained. The engineer who prepared this fault tree had to know sodium systems, sodium fires and meteorology. He, therefore, knew from previous studies of sodium fires that one of the best methods of controlling the magnitude of a sodium fire is to limit the burning area and if possible the burning rate per unit area. Therefore, the spilled area must be limited to some acceptable value and must be deep enough to contain an order of magnitude larger spill than that positively determined acceptable. Exact meteorological conditions must be studied. The probability of oxide effluent reaching the populated area, and the acceptable risk known to be acceptable to the general public must be determined.

A complete surveillance⁵ was made of all major sodium components for which leaks have been recorded from six sodium facilities. Applying the probability of a leak of a given magnitude as evidenced by this study to the actual SPTF components and their design life expectancy, a distribution function was constructed which indicated the probability of a spill of given magnitude or greater occurring.

LWF 1.90022

Figure 4. Excessive Risk to General Public

If the volume of spill containment of the catch pan area is such as to contain any reasonably expected volume of sodium leaking from a system and the expectation of occurrence and propagation to a populated area is of very low magnitude compared to normally accepted risk by the general public, then the risk associated with its occurrence should also be acceptable to the general public and to a formal safety review authority.

The approach used to determine the magnitude of risk accepted by the general public was first to attempt to isolate categories of risk. In every day activities, excluding those risks associated with employment, the general public accepts certain levels of risk with regard to the potential for bodily injury or death. These may be divided into two classes: 1) that class wherein the public voluntarily exposes itself with full awareness of the level of risk involved. These include transporting oneself or being transported from one place to another, doing chores or do-it-yourself tasks, deliberately resideing in a high risk industrial area, or soliciting employment in a high risk or dangerous field. This class does not consider employment risk per se. The second class are those risks which the public accepts but has no personal control over. These include exposure to accidents such as: explosions; poison, toxic or radiological release from transport or storage vessels, and invasion of the home by missiles or violent persons. Obtaining this information required a considerable amount of digging but once the sources^{6,7,8,9,10} were located, a reasonable picture of exposure risk could be put together. In this study, it was found that for the class of "Voluntary Risk:"

1. If a passenger takes one commercial flight per year, the probability of death is about 0.8×10^{-5} .
2. Motor vehicles for 1968 disabling injury = $1000/10^{-5}$ people
3. All means of commercial transportation 8.2×10^{-5} fatalities/passenger year.
4. Home: $14.2 \text{ deaths}/10^5 \text{ people}$, $2.2 \times 10^3 \text{ disabling injuries}/10^5 \text{ people}$.
5. Pedestrians: $80 \text{ deaths or injuries}/10^5 \text{ people}$, with deaths₃ 1 out of 40.
6. General public activity, $10.2 \text{ deaths}/10^5 \text{ persons}$, $1.3 \times 10^3 \text{ disabling injuries}/10^5 \text{ persons}$.

Total exposure is then about:

1. Fifty deaths/ 10^5 persons/year or about 1 chance in 30 that during his lifetime he will be accidentally killed due to deliberately exposing himself,₃ and₅
2. $4.6 \times 10^3/10^5$ person per year of disabling injuries.

A similar analysis for the class of exposure without personal control gives an expectation of about $0.14 \text{ deaths or injuries}/10^5 \text{ persons/year}$ for the estimated 25% of the population which lives within reasonable proximity to industries or transportation lanes where such accidents occur.

Based on this study, it was determined that, to afford no greater exposure potential to the public then presently exists, control of the DBA should assure containment of all sodium leaks of 455 lbs or less in an area no greater than 175 square feet. The actual design will be capable of containing 7800 pounds of sodium in an area of 150 square feet and is several orders of magnitude safer than the least conservative estimates of accepted public exposure of 10^{-3} deaths or injuries/ 10^5 people per year (based on observed 10^{-1} to 5×10^{-3}). This level of conservatism was considered necessary in order to allow for the difference between the operations environment and the six facilities which were the sources of the component leak data.

Of the references on accidental death and injury used in this study, only reference seven has been updated by a 1972 edition. While this issue has broader coverages and additional categories of information, the basic accident rates have changed very little from those in the 1969 edition.

RISK CRITERIA APPLIED TO A TEST FACILITY COMPLEX

The previous study was an excellent example of using fault tree as a guidance tool to the initial exploration of a problem and to define the areas of uncertainty which must be explored. It also illustrated the use of risk analysis as a safety criterion in which additional risks to the general public as a result of a proposed

action shall be negligible as compared to that already incurred by the public. Over the years there have been many such criteria proposed in an attempt to justify the application of the concept of risk as compared to that of the design base accident. Some of these concepts have been assembled in a very excellent, logical, and practical manner by Dr. Stig O. W. Bergstrom, of the Studsvik Nuclear Research Center in Sweden in a paper "Principles of Reactor Siting" presented at the recent ANS/AIF Conference. He was kind enough to send me a copy of his complete paper. I would like to review the fundamentals of his criteria and logic and apply them to a hypothetical study. Quote from Dr. Bergstrom's paper:

"The influence upon the environmental risk situation from a certain plant-size combination must be acceptably judged after three kinds of more or less well established criteria:

- Normal operation^x shall not create effects in the environment that exceed recommended limits for radiological doses, temperature increases in water recipients, etc.
- The frequency and consequences of accidents should not be greater - average over long periods of time - than, and that their total effects are small compared with those considered permissible from the normal operations of the plant.
- The largest conceivable accident of significant probability should not cause consequences greater than those from other risk types which might be influenced by man and which already exist at that probability level.

It is common that siting analyses are made without any consideration of the effects upon plant and personnel from the operations and accidents studies. As these are mainly independent of the site they do not influence the relative merits of a site. However, when making an absolute evaluation of the costs and benefits of nuclear power safety these aspects must be included. Even though it is very difficult to convince intervenors and nuclear power opposition in general about this, it seems most probable to the author that concern for the plant personnel and the invested capital will place more stringent safety requirements upon design and operation of nuclear plant than environmental criteria."

In referring to the first of these criteria on environmental effects, he said that: "To start with it seems most probable that if human health is not harmed, then all other organisms and vegetation should also be safe from serious injury," and that "radioactivity releases under normal operation (as defined earlier) to air and water, and other possible radiation exposures must be controlled so that neither doses to individuals in the immediate environment nor the integral population dose exceed the ICRP or corresponding criteria".

With respect to his second criteria he stated "The criterion that the long time average of consequences from nuclear accidents should be small compared with those permissible from normal operation can be used to formulate a design target for tolerable accident probability". "For example, an earthquake that happens in a non-seismic area or reaches an exceptional magnitude where one has designed for more moderate effects, could both cause a containment break and a major fission product release. The probability for this event must then be compared with the combined probabilities for long sequences of unlikely faults and other unfavorable conditions. Interest up to now has been concentrated upon safeguarding against seismic effects in areas where they are most frequent, and to avoid sites close to active earthquake faults. It seems like, though, that it would pay off to use design criteria which aim at the limitation of moderate seismic effects even at other sites."

In analyzing his third criteria he refers to maxident considerations. Maxident means maximum conceivable accident. Several quotes have been taken from his

^xNormal operation is not an easily defined fairly constant state, but is part of a spectrum ranging from undisturbed to accidental conditions. The only practically useful definition of this state seems to be "any situation when the plant can be operated as desired, without restrictions of a practical or a formal nature."

text to assist in understanding his thoughts associated with this criteria.

"There may be a minimum probability which one is ready to consider as significant. In a similar way there might exist an accident consequence so large that we do not dare to introduce it as a possibility even at a very low probability. How large an accident society is willing to risk as a maximum is difficult to decide and is, of course, dependent upon the benefit that accompanies such risks".---

"The coexistence of jumbo jets and large busy airports indicate that the consequence limit lies well above 1000 dead and 10,000 injured individuals. The largest indoor auditoriums give further evidence that similar or even higher numbers lie inside the limit". -- "One may wonder if a total risk of 100,000 dead and injured people is not acceptable when large populations are located in areas notorious for earthquakes, floods, hurricanes or ocean waves." An excellent example of this latter can be seen in the response of people to the near collapse of the Van Norman Dam during the February 1971 earthquake in the San Fernando Valley. The collapse of this dam could have wiped out housing in a stretch a mile wide and 10 to 15 miles long. When in 1972 it was proposed to rebuild this dam, very few of the people living within this path had interest enough in preventing its reconstruction to attend a public hearing. Dr. Bergstrom also observed that maximum late health effects due to delayed radiation health effects due to delayed radiation health damage will never limit the choice of a reactor site; and that, while slower releases from distant sites can be met with countermeasures such as evacuation and the distribution of pills with stable iodine to reduce thyroid doses, urban areas and large fractions of the public cannot be informed until after several hours, and may require for large population an establishment of practice drills.

As an application of Dr. Bergstrom's criteria, this last example of fault tree application demonstrates an approach to overall evaluation of a test facility complex in which both nuclear and non-nuclear facilities exist. The overall safety evaluation would quantify the serious off-site and on-site consequences of relatively high probability accidents. The purpose of this evaluation is to quantify the current risks the owner is assuming, where risk is the product of probability and consequences of an accident. It will provide a basis for recognizing operational changes or modifications to each facility that may be necessary to assure that there is no undue risk to the public, employees, or the environment, and will make it possible to properly establish priorities for changes, modifications, and for developing complete individual facility safety evaluations later. Some basic constraints include:

1. All facilities containing sufficient quantities of radioactive, toxic, flammable, and/or explosive materials should be considered.
2. Off-site and on-site consequences of accidents were to be evaluated.
3. Low probability accidents such as tornadoes may be excluded.
4. Higher probability accidents such as fire, earthquake, operator error etc., should be evaluated.
5. It should be assumed that accident prevention efforts fail, and
6. Itemize existing and recommended accident consequence limiting features evolving from this study.

From these constraints it is obvious that a certain amount of information must be obtained in order to identify those facilities for which a safety evaluation must be made. First, we are constrained that only some facilities require this evaluation, and second the quantity of dangerous materials must be sufficient to cause a problem. Obviously these two constraints may eliminate several facilities from consideration. However, this is of very little importance to getting started with construction of the fault tree logic. The simplest approach is to set up the fault tree such that it will be applicable to the analysis of any and all of the facilities. It is also easier to start with those things that we know must be evaluated as the basic roots of the analysis. One of the basics which we know must be evaluated is accidents. A list of general types of accidents previously studied for these facilities would include as a minimum:

1. Sodium Fires
2. Radioactive materials fires
3. Criticality incidents
4. Reactor excursions
5. Explosions
6. Incidents involving other toxic materials

Ground level fault trees for each of these accidents will be constructed for later insertion into the overall evaluation of risk fault tree. Since we have already developed the sodium fires fault tree, let us review Figure 4 again to see if we have met the prescribed constraints. We see that, for sodium fires: accident prevention efforts fail; accident sequence limiting features are considered; and both operator's error and the probability of breach of the sodium system boundary has been evaluated on the basis of historical failure of similar components. Thus, it would appear that, except for the fact that we have not specifically evaluated the effects of earthquakes and faults as peculiar to, say the Santa Susana facilities, this branch fault tree is satisfactory. In addition, we have not included radioactive sodium fires, per se, since we were studying a non-nuclear facility. Thus, with the addition of these two factors, Figure 4 should be adequate for this study. This branch of the three is now given a symbol AA to differentiate it from as yet undeveloped branch fault trees for the other classes of accidents. An expert in each of the other classes of accidents should be selected to prepare a simple fault tree similar to that in Figure 4. One factor, however, which this person should keep in mind is that each of these fault trees should have a constraint at its top, similar to that for sodium fire surface area, which would state that the quantity of available dangerous material is sufficient to have the potential of exceeding allowable limits. Assuming these fault trees are being developed, our fault tree expert will now go on to the next stage of analysis. He must investigate the consequences of these accidents both off-site and on-site. Since the two consequences are considerably different, it is better to keep them separated. Thus, let us first examine off-site consequences for already developed sodium fires insofar as the general public is concerned at the nearest population center, Brandeis Camp. The concentrations at this Camp must not exceed to 2 mg/m^3 of sodium oxide or radiological concentrations in excess of 10CFR100 limits. However, since we are analyzing total incurred risk by the owner, we must keep in mind that part of this investigation may require evaluation of financial risk incurred due to potential damage to cattle or range personnel which might be caught in the path of the effluent cloud. Radioactive material fires, criticality accidents, reactor excursions and accidents involving other types of toxic materials must also be limited by 10CFR100 or other government regulatory constraints. Explosions, however, at such as the Santa Susana facilities will have no off-site effects unless they are secondary in nature and release toxicological or radioactive substances which would then fall under the same criteria as the other accidents.

In order to exceed the regulatory concentration limits, the toxicological or radiological effluent must be carried to the population site by some physical means. In order to evaluate the probability of this occurring, it is necessary to carefully analyze the meteorological conditions of the site, the hydrological conditions of the site and any other means by which transportation may be enhanced. Other site information which must be obtained and applied to the study are location of faults, seismological magnitude expectations as a result of activity by major off-site faults, and geological considerations which permit access to subterranean water contamination must be considered in the probability that the results of an accident may reach a population center.

Now consider the concept of risk. Risk has been defined as the product of the probability and consequences of an accident. However, consequences are difficult to predict as a quantitative value.

There are several aspects of risk which must be considered in the case of off-site risk. One must consider risk to the general public of death, accident,

of inconvenience and of financial loss. All are popular subjects of liability suits. In addition, California has been flooded of recent by suits associated with effects on environment. This is another area which must be considered legally when initiating a new facility and from the standpoint of potential liability considering the weaknesses of existing facilities. It is now time to take another look at Dr. Bergstrom's three basic criteria.

For our purposes I would like to repeat these criteria in simpler phraseology.

1. For normal operation, defined as all operations short of an accident, we are controlled by legal limits (Criterion 1 would then not apply to off-site risk except at the site boundary.)
2. Deleterious effects over a long period of time shall be small compared to deleterious effects from normal operation. (Again for this site in our consideration of off-site consequences, this criterion does not apply since we have no normal operation off-site deleterious effects.)
3. The consequences of the worst accident, we feel worthy of consideration, should be no greater than the consequences of a normal risk event which the public is willing to accept and which has the same probability of occurrence as the accident which we are considering. (This criterion definitely applies to off-site risk analysis).

The difficulty with application of criterion 3 is the ascertainment of the probability of occurrence for the accident; and the identification of a normal risk accident of similar probability that the general public has shown willingness to accept. Thus, if we are going to have any chance of succeeding with any regulatory authority, we must voluntarily insert some level of conservatism in the application of this criterion. Experience has generally indicated that for most accidents, it is possible to determine the probability of occurrence within half an order of magnitude, or on rare occasions, only within an order of magnitude. The expert who is constructing the fault tree for a given accident, in evaluating the probability of it's occurrence should have some feeling of the level of confidence he has in his numerical values. He and he alone should select the degree of conservatism which must be placed on criterion 3. One specific advantage of criterion 3 that we can readily see for the case of death or injury is that it relieves the analyst of having to define exactly the numerical value of consequences in order to arrive at a numerical concept of risk. Since we have already studied acceptable accidents to the public and the probability of occurrence in our second example, it is highly probable that the same sources or similar sources will provide us with the answer to the correlating acceptable accident which meets this criterion. We are now ready to complete the fault tree for off-site consequences. This is shown in Figure 5 as qualified by the notes.

The undesirable event is "Excessive off-site risk to the owner." The fault tree itself is quite simple and direct. Yet, as can be seen, it affords an excellent tool for: identifying those areas which need additional research; making assignments to personnel; identifying cost and funding requirements; and scheduling and following work progress. Now that the easy job is well underway, let us examine what is required to evaluate on-site consequences. Going back to Dr. Bergstrom's criteria, both criterion 1 and 2 are now applicable. Property damage and death for which off-site consequences could immediately be seen to be extremely low, if not zero, have much higher potential on-site. Also, disabling injury potential has increased. How does this effect the basic plan of action and the construction of the fault tree? Actually very little, even though the problem is far more complex and difficult to resolve.

Obviously the undesirable event must be changed to include on-site. Second, release limits - both radiological and toxological must include specific on-site limits. These are usually higher limits since control of area access and evacuation to prescribed areas is taken credit for. Third, the values for maximum allowable property damage multiplied by the probability of occurrence to determine the risk factor must be weighed against the cost of prevention (the weighting factor has yet to be determined). Fourth, employee inconvenience is not a factor, neither is

Figure 5. Risk Analysis for Test Facility Complex

environmental considerations. Applicable toxicological and 10CFR20 limits, under the restricted access criteria, would be applied for criterion 1. In applying criterion 2 the on-site consequences of each accident must be evaluated by some means and the productive risk determined. As an example, a weighted integrated dose related to 10CFR20 might be applied to the risk of disability injury in the case of an accident for short time occupancy of an hour or less. Criterion 3 still permits comparison of acceptable risk with respect to death or disabling injury since the individual should not be expected to accept greater risk at work than at home.

The suggested alterations are shown in Figure 5 by the elimination of those areas enclosed by dotted lines and by including alternate limitation on dosage in order to permit on-site risk evaluations. Additional clarification is given in the notes.

It is now possible to evaluate for both cases the existing accident consequence limiting features as originally requested. It is also now possible to decrease the potential of risk by recommending additional accident consequence limiting feature modifications to the specific facility under study. In the latter case, the fault tree affords an excellent overview of problem areas by pointing to critical paths which may be open to specific consequence limiting feature improvement alterations. With the completion and addition of each of the sub-branch accident type probability fault trees, the overall off-site and on-site risk to the owner may be evaluated provided the extensive amount of leg work in obtaining the probabilities associated with each event has been completed. This fault tree was developed purely as a theoretical exercise for this paper. The logic approach outlined, however, is exactly the approach which I plan to use when and if funding becomes available for this type of study.

In conclusion, I hope that these three examples of simple and logical application of fault trees to optimization studies of nuclear reactor power plant safety analysis and associated design modifications will be of help in encouraging you to make greater use of fault tree as a graphic tool. I also hope that they have demonstrated a means to ease of thinking logic and of presenting the basis of this logic to responsible management in a readily understandable visible form.

REFERENCES

1. Heavy Water Organic Cooled Reactor, AI-CE-MEMO-25 (Mar. 29, 1966).
2. B. J. Garrick, et al., "An Analysis of Nuclear Power Plant Operating and Safety Experience," HN-185, Vol. 1 and 2 (Dec. 15, 1966).
3. B. Epstein and M. Sabel, Journal of American Statistical Association 48 485-502 (1953)
4. EEI Publication No. 63-42, Edison Electric Institute, N.Y. 17.
5. Failure Data Handbook, LMEC Memo-69-7, Vol. 1, Rev.1 (Sept. 22, 1970).
6. C. S. Bartholemew, Boeing Company, "Some Economic Implications of Reliability/Maintainability and Safety in Transport Systems," Seventh Reliability and Maintainability Conference (1968).
7. Accident Facts, 1969 Edition, National Safety Council.
8. Engineering and Safety Department, American Insurance Association Police Investigation Bulletin, Bulletin No. 1 (February 1966).
9. Suggested Guide for State Action on Safety on Fire, Explosion, and Health Hazards, Highway Transportation of Extra Hazard Commodities, American Insurance Association (AIA) (1966).
10. E&S Department, AIA, Highway Emergency Training Bulletin, Bulletins Nos. 4, 7, 8, 9, 10 (1966).