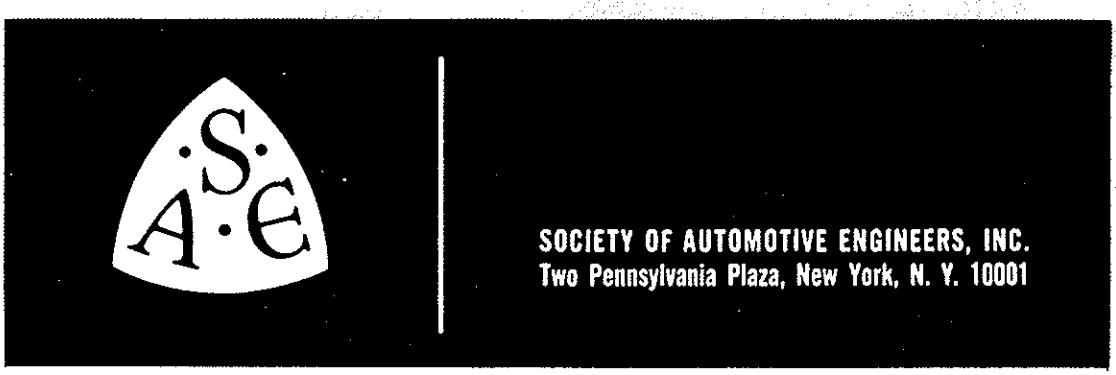

Introduction to Fault Tree Analysis

J. L. Recht
National Safety Council

SOCIETY OF AUTOMOTIVE ENGINEERS

Earthmoving Industry Conference
Central Illinois Section
Peoria, Illinois
April 23–24, 1974

740432

740432

ABSTRACT

This presentation includes a brief history of fault tree analysis, its relationship to systems safety analysis, and a description of how to do a fault tree analysis both on a simple and complex level. It will demonstrate how this analytical technique can give new insight into safety problems and thereby improve proposed answers or countermeasures. The application of this approach to management problems is also discussed.

Introduction to Fault Tree Analysis

J. L. Recht
National Safety Council

THE FAULT TREE METHOD of analysis is more than a decade old, but like most innovations its diffusion has been slow. It was successfully applied to some very knotty problems in the aerospace field and this success gained it acceptance, not only within the aerospace industry, but also by the Department of Defense, which made fault tree analysis a requirement in some of its contracts. However, the broad application of fault tree analysis seems to lie in the future. At the present time it is being used mainly for safety of missiles and aircraft by the design engineers in the design stages of these products.

In this article it is hoped that the potential for wider application of this relatively new technique can be shown. For example, the safety engineer (possibly with an assist from his own product engineers) can find uses for this analytical method, not only with respect to existing systems in his plant, but also for setting specifications on new or replacement equipment. Also, management can apply this method to gain additional insight in solving problems and making better decisions.

Fault tree analysis was first conceived in 1962 by H.A. Watson of Bell Telephone Laboratories in connection with an Air Force contract for study of the Minuteman launch-control system. Further development and refinement of the technique resulted from the combined efforts of the study team, which included A.B. Mearns. The problem of determining the likelihood of an inadvertent launch of a missile was successfully solved. The Boeing Company later modified the fault tree technique so that simulation with high-speed computers was possible. D.F. Haasl, R.J. Schroder, W.R. Jackson, and others contributed to this important development.

Because of this rapid growth in sophistication, it is possible to consider fault tree analysis on three different levels of complexity:

1. Simply draw a fault tree and examine it without performing any calculations.
2. Draw a fault tree and perform the calculations with a desk calculator or slide rule.
3. Draw a fault tree and devise a computer program for performing the calculations.

In this article, the first two levels will be discussed and the requirements for the third level will be indicated.

What is fault tree analysis? According to A.B. Mearns, the first fault tree analysis was made to study unlikely events in complex systems. This view can be expanded: a fault tree can be constructed for any event that can occur in a system. It is important to remember, however, that only one event is analyzed in a single fault tree.

To do a fault tree analysis, first an undesired event of sufficient importance is selected—this could be a catastrophic event (such as inadvertent launch of a missile) or an undesired event of smaller magnitude (such as failure of a power press interlock guard). Next it is necessary to reason backward from this event to visualize all the ways in which it could occur. These "causes" or contributing factors are, in turn, broken down into the events which lead to them, and so on. The events are diagrammed in the form of a tree with the undesired event at the top. The branches are continued until either "independent" events are reached or there is little reason to continue due to lack of information or insignificance of the contribution of additional breakdowns. An independent event is one which does not depend upon other components in the system for its occurrence.

MAKING THE TREE

A fault tree is really a logic diagram that traces all the events and combinations of events that can lead to the undesired event. For uniform representation of these events certain symbols are required.

One group of symbols, called "gates," indicates whether a single event or a combination is required to produce the next event higher up the tree. They also may indicate whether limiting conditions are involved, such as one event happening before another when both are required to pass through a gate.

Other symbols are needed for the events themselves to indicate whether they are "normal," "independent," or "insignificant."

The real strength of the fault tree symbolism lies in the fact that the symbols can readily be translated into algebraic terms so that the tree can be simplified. It can be mathematically reduced, so to speak, to its bare bones. All duplications can be eliminated and the most important independent events identified. If the frequency of occurrence (or probabilities) of the independent events is known or can be approximated, then the relative importance of the various independent events in producing the undesired event can be calculated.

A SAMPLE TREE

For the purpose of illustrating the fault tree method of analysis, we will use a home fire alarm system. As shown in Fig. 1, there are sensing devices on the first and second floors with wires connected to the alarm, which is powered by the ordinary 110 V commercial power supply. The undesired event selected for analysis is "a fire with no alarm."

Examining the tree (Fig. 2), it is seen that the undesired event can come about if there is a fire on the first floor with no alarm given or a fire on the second floor with no alarm.

A fire on the first floor with no alarm involves having a fire on the first floor and having the alarm unable to respond to the fire. (There is also an added condition that the alarm fails prior to the fire.) The alarm can fail to respond if the first-floor sensing device fails or the alarm is inoperative. The fire alarm will become inoperative if either the alarm itself fails or there is no power to the alarm system or the sensing lines fail. There will be no power if the power line fails or the commercial power is cut off at the source.

Similarly, the branch involving a fire on the second floor can be traced. The transfer symbol shown under "fire alarm inoperative" indicates that corresponding elements in the first-floor branch should be repeated beginning with the transfer symbol.

This represents the simplest level of fault tree analysis—drawing the tree and examining it. Since it requires precise and detailed knowledge of a system to draw a fault tree, completing the tree forces the analyst to learn more about the system.

For a complex system, it is often necessary to assign various branches of a tree to specialists to make sure that the event sequences are correctly portrayed.

There are important benefits to be gained from learning precisely what can go wrong and how this will affect the system. The analyst gains new insight and sees new possibilities; he can see what new data is needed for prevention purposes; and he will come up with better answers because they will be based on examination of the whole system rather than a single component.

INTRODUCING CALCULATIONS

The second level of complexity in fault tree analysis involves calculation. What is needed are the frequency of occurrence figures for the events symbolized with circles. These

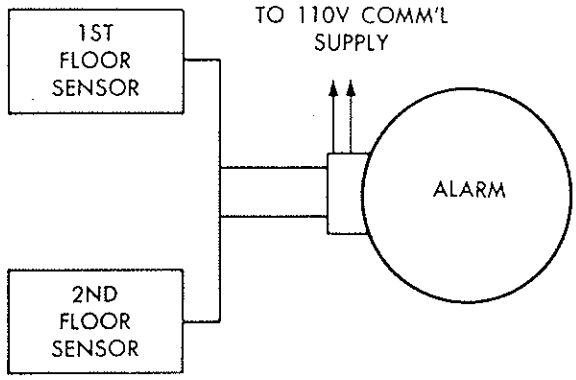

Fig. 1 - A sample home fire alarm system

frequency numbers are usually mean time between failures figures (MTBF), and they apply to the separate components. The sources for these numbers are varied—accident experience, test results from component manufacturers, comparisons with similar equipment, engineering data, judgment, and so on.

Next, the fault tree should be converted into algebraic terms using Boolean algebra. Boolean algebra sounds strange and possibly difficult until you realize that it is understood by any 7th or 8th grader who has studied the "new math" now taught in grade schools. They learn the algebra of sets, which is a form of Boolean algebra. Actually, all that is needed are about ten simple rules that can be learned thoroughly in a couple of hours.

The and relationships in the tree are represented by multiplication signs and the or relationships are represented by plus signs. Starting at the top of the fault tree, each of the events is written in algebraic form step by step until the entire tree has been expressed in terms of the "independent" events (those symbolized with circles or diamonds). The terms of this long algebraic expression can be greatly simplified using the Boolean rules. The MTBF figures or estimates of frequency of occurrence can then be substituted in this simplified expression and the relative importance of the various terms evaluated.

Typically, it will be found that some event sequences are thousands of times more likely to induce the undesired event than other event sequences. Thus, it is relatively easy to find the chief combinations of events that must be prevented to reduce the likelihood of the undesired event happening—even when the MTBF figures are not completely accurate.

The calculations enable the analyst to determine the overall likelihood of the undesired event, the combination of events most likely to lead to it, the single event that contributes most to this combination, the most likely paths through the tree to the top, and many other relationships. In addition, if the system is modified in any way, the fault tree can be changed to reflect the modification and new calculations performed to determine the effect of the innovation. In fact, numerous modifications can be made and the effects of all of them can be simultaneously evaluated.

In its original form, the fault tree was confined to faults or malfunctions of equipment. But there is no need to restrict the method in this manner. With sufficient information on

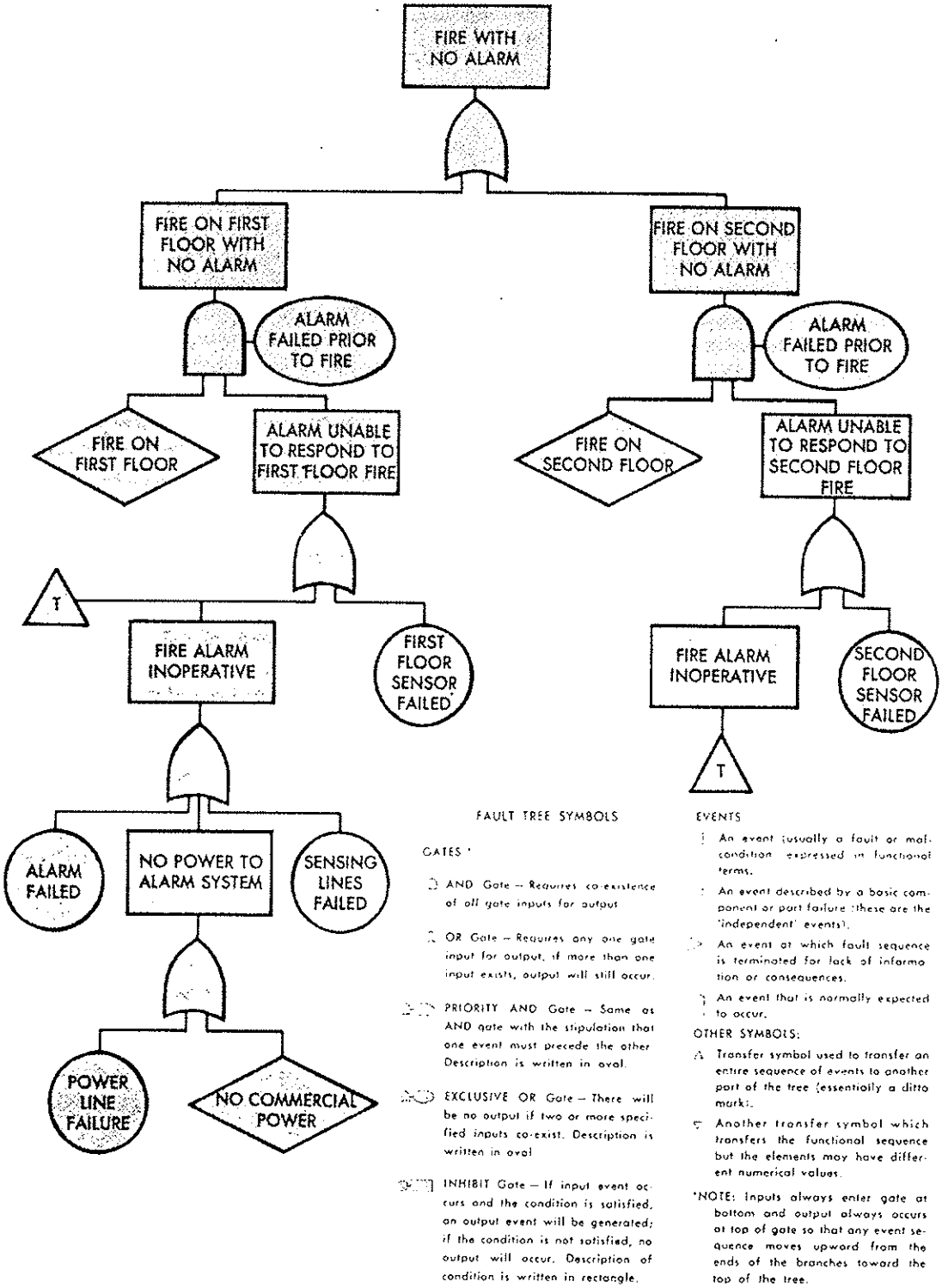

Fig. 2 - Fault tree analysis of the home fire alarm system

human error frequencies, human as well as mechanical malfunctions can be included in the fault tree.

Both the human errors and the mechanical malfunctions can be stated in probability terms and can, therefore, be combined with no logical difficulties. It should be noted, however, that much more information is available on equipment faults than on human errors and it may require considerable effort to quantify a fault tree having both kinds of malfunctions.

COMPUTER SIMULATION

It is clear that the fault tree method is a powerful and efficient technique for systems safety analysis. It is limited pri-

marily by the skill of the analyst and the availability of the basic numbers needed to indicate frequencies of certain events However, if the system being analyzed is quite complex, the calculations can be tedious and the lack of failure frequency data can become serious handicaps. To overcome both of these problems, the Boeing Company has developed ways of simulating fault trees on high-speed computers.

Briefly stated, this computer method requires that the fault tree be constructed as usual. Then either the MTBF figures or figures obtained by sophisticated sampling techniques applied to the frequency distributions for primary faults are used to designate time intervals in the life of the system during which a particular fault will occur. Coexisting faults will form event sequences that will ascend the tree and, in some cases, will reach the top of the tree. These combinations are recorded and after sufficient computer runs, the same sorts of information about the events will be obtained as they would be in the noncomputer calculations.

The computer format has an additional advantage, however, in permitting a more realistic situation to be used by allowing for repairs to be made to correct some faults. In the life of any system, repairs or maintenance activities are performed and this reduces the likelihood of specific undesired events happening. Introducing repair times into hand calculations offers no theoretical difficulties but it is much easier to incorporate in a computer program.

THE FAULT TREE IS A UNIQUE MODEL

Systems analysts and operations research technicians set up mathematical or logical models when solving problems. These models fall mainly into two classes: deterministic, that is, those showing causal relationships among the various parts of the model, and probabilistic, that is, those using probabilities to indicate the likely relations among the parts. The fault tree is a unique model because it combines both classes of model in one representation. When constructing the tree, the elements of the tree are developed as causal sequences showing what event can lead to others based upon knowledge that such happenings actually occur. Once probabilities have been assigned to the independent events, the model becomes a probabilistic one. The probabilities help to select not just relationships between variables, but to determine which causal chain is the most likely. Potentially, therefore, fault tree analysis is more powerful than traditional statistical techniques such as regression analysis, since it is on a new plane. It is choosing among causal sequences that are already known rather than merely linking elements. Of course, the power of this analysis method depends upon there being sufficient knowledge to draw the proper tree in the first place.

APPLICATIONS

The applications of fault tree analysis depend upon the ingenuity and knowledge of the persons using the method. But it might be helpful to indicate how a manager could gain insight by applying the method on the simplest level.

Suppose a plant manager decides that he would like to increase the gross income for his plant. He would start the tree with a rectangle at the top of the tree labeled "increase gross income." To increase the gross income he must either increase the prices for his present products sold or increase the amount of goods sold (at the present, higher, or slightly lower prices). On the tree this would be represented by an or gate and two branches—one for the higher prices and the other for the increased product sold. Looking just at the branch involving higher prices, he can reason that before prices can be increased, he must examine possible government regulations controlling prices, possible antitrust violations, current and future market conditions, the possibility of lower sales volume, and so on. Each item would be added in its proper place in the tree and further analyzed.

If the manager were to opt for increasing the amount of goods sold, he would now add items to the other main branch of the tree. He must examine the availability of additional raw material and additional manpower, more money for investment (perhaps through loans or stock sales) to finance the expansion, and follow these elements to other levels. Another subordinate branch might pursue the possibilities that increased sales might also be obtained by reducing inventories which could come about through lower prices or a better sales effort (more incentives for salesmen or better salesmen) or by improving the products sold. Improving products leads to examining the research facilities and the investment needed for this activity, and so on.

All of these elements are readily derived in a simple tree—once the process is started. When laid out in this form, the manager can determine the most likely sequence of events and make his decision based upon a better overall view of the processes involved. The process of drawing the tree in itself forces the analyst to view his problem more realistically and thereby generates added insight that can be very valuable in making his decision.

REFERENCES

1. A.B. Mearns, "The Study of Unlikely Events in Complex Systems." Bell Telephone Laboratories, Inc., Whippany, N.J.

2. R.J. Feutz and T.A. Waldeck, "The Application of Fault Tree Analysis to Dynamic Systems." Boeing Co., Seattle, Wash.

3. D.F. Haasl, "Advanced Concepts in Fault Tree Analysis." Boeing Co., Seattle, Wash.

Society of Automotive Engineers, Inc.
TWO PENNSYLVANIA PLAZA NEW YORK N Y 10001

8 page booklet. Printed in U.S.A.