DOCUMENT RESUME

ED 245 343 EA 016 886

AUTHOR	Barker, Bruce O.; Petersen, Paul D.
TITLE	Fault Tree Analysis: An Operations Research Tool for Identifying and Reducing Undesired Events in Training.
PUB DATE	Apr 84
NOTE	16p.; Paper presented at the Annual Meeting of the National Society for Performance and Instruction (22nd, Atlanta, GA, April 23-26, 1984).
PUB TYPE	Information Analyses (070) -- Speeches/Conference Papers (150)
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	Critical Path Method; Decision Making; Diagrams; Evaluation Methods; *Management Information Systems; *Methods; *Models; *Operations Research; Organizational Communication; Problem Solving; Research Tools; *Search Strategies; *Systems Analysis

ABSTRACT

This paper explores the fault-tree analysis approach to isolating failure modes within a system. Fault tree investigates potentially undesirable events and then looks for failures in sequence that would lead to their occurring. Relationships among these events are symbolized by AND or OR logic gates, AND used when single events must coexist to produce the more general event. Other fault-tree symbols represent input or output types or failure-oriented events, and are classified by their nature. The circle, for instance, points to a failure event in which further development is not required. In constructing the tree, decision-makers should develop each failure event so that cause and effect relationships can be identified, and thus recommendations leading to better communications or resource allocations made. (KS)

FAULT TREE ANALYSIS: AN OPERATIONS RESEARCH TOOL FOR IDENTIFYING AND REDUCING UNDESIRED EVENTS IN TRAINING

A paper presented at the 22nd Annual Conference of the National Society for Performance and Instruction. Atlanta, Georgia. April 23-26, 1984.

by

Bruce O. Barker
Assistant Professor of Education
Texas Tech University
Lubbock, Texas 79409

and

Paul D. Petersen
Program Administrator
Division of Continuing Education
Brigham Young University
Provo, Utah 84602

FAULT TREE ANALYSIS: AN OPERATIONS RESEARCH TOOL FOR IDENTIFYING AND REDUCING UNDESIRED EVENTS IN TRAINING

Introduction

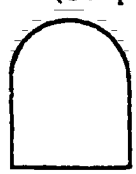
Analysis of a system, in relation to accomplishment of previously established objectives, can be viewed in terms of two basic approaches: (1) analysis in terms of success or accomplishment of a system's purpose -- that is, what must or should be done in order to achieve desired results; or (2) analysis in terms of failure or non-accomplishment of a system's purpose. The general procedure of both the past and the present seems to be to look at success factors. Yet, it seems much more difficult and time comsuming to predict or determine what promotes success in a system than it does to isolate those factors which cause failure. (Stephens, 1973). If decision makers can systematically isolate and avoid failure modes within a system, the probability for success will be enhanced. The purpose of this paper is to explore and suggest a systematic approach to analysis of factors contributing to possible failure of a system, in order that decision makers will be better informed and able to plan for mission success.

Fault Tree Analysis

One approach to isolating failure modes within a system is fault tree analysis. The fault tree method of analysis takes the approach of looking at and analyzing the most undesirable events which could occur within a system and then searching for and analyzing failures in sequence which would lead to these undesirable events. The name "fault tree" is derived in the fact that the graphic portrayal of a functional system which has undergone the process of a fault tree analysis utilizes a branching process similar in outline to a coniferous tree.

The process of fault tree construction starts with a statement of a critical undesired event which one wants to prevent from happening. The fault tree is then constructed according to a series of logic steps, showing precisely how a given failure event could occur. (Failure, as used here, means the inability of a system or portion of a system to perform its expected function). Once identified, potential failure modes can be easily ranked against each other and weighted in terms of probable occurrence, resulting in the identification of a critical or strategic failure path(s). Failure sequence priorities can then be established, allowing decision makers to know what should be avoided first, second, third, etc. The idea is to identify, then plan strategies to avoid potential failure events thereby increasing the probability of success.

Fault Tree Construction

The fault tree is constructed by showing the relationship between various kinds of events which could cause failure of the system. These relationships are symbolized by logic gates. Two principle kinds of logic gates exist, the AND gate and the OR gate (Stephens, et al, 1979). Graphically, the AND gate is depicted by the symbol  , and is used when two or more events must coexist in order to produce the more general event. Figure 1 depicts the portrayal of events related by an AND gate as they would appear in a fault tree. The use of the AND gate(s) occurs much less frequently (in most cases not at all) in behavioral systems than in hardware systems (Stephens, et al, 1979). The tree in Figure 1 would read: "Events B and C must coexist in order to produce Event A; or the output A can occur only if the inputs B and C coexist."

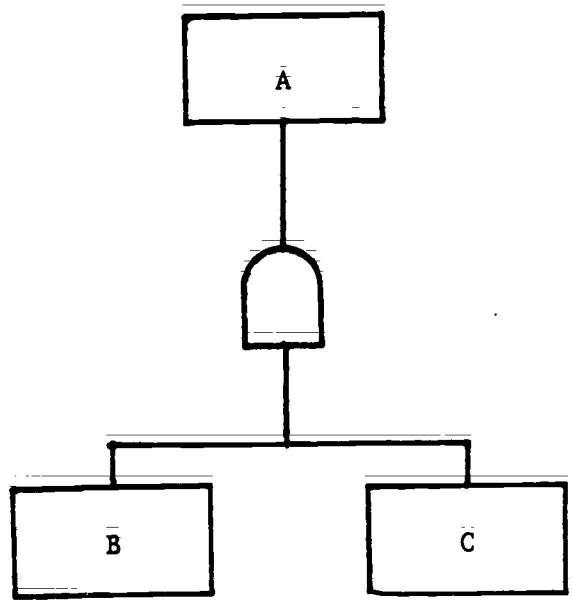
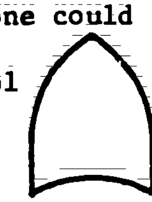


FIGURE 1. THE <u>AND</u> GATE.

The OR logic gate occurs most commonly in behavioral systems. It is used when, of two or more possible inputs to an event, any one alone could produce the output. The OR gate is depicted graphically by the symbol . Figure 2 depicts the portrayal of events related by an OR gate as they would appear in a fault tree. The tree in Figure 2 would read: "The occurence of either Event B or Event C alone will produce Event A."

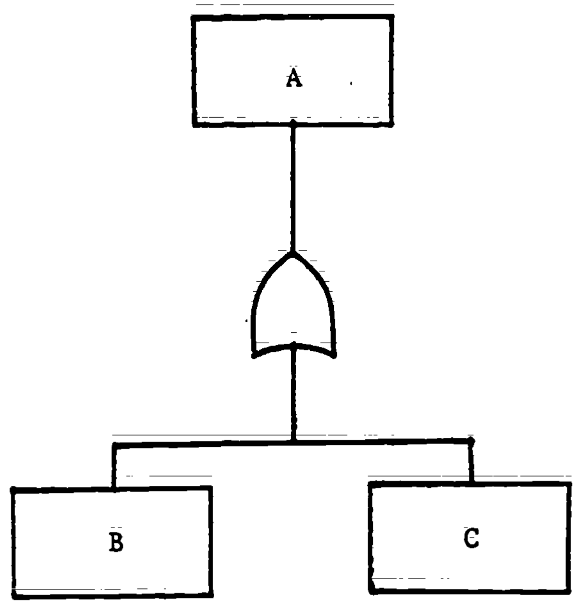
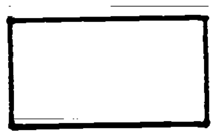
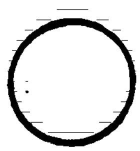


FIGURE 2. THE OR GATE

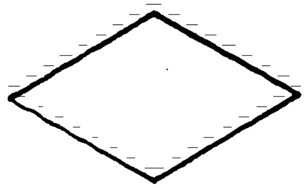
Symbols Used in Fault Tree Construction

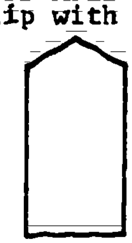
In addition to logic gates, other symbols are used in drawing a fault tree. These symbols depict the types of inputs and outputs or events which could lead to failure, and are classed according to their nature (Stephens, et al, 1979). Symbols most commonly used for fault trees include:

1. Rectangle:  Identifies an event that results from a combination of less general fault events through an associated logic gate. All events symbolized by rectangles have additional development or analysis in the fault tree.

2. Circle:  Identifies a basic failure event in which no further development is required. The decision regarding whether the event is

a basic one or not depends largely on the perspective of the analyst. A basic failure event occurs when the definition of an event is sufficiently explicit to satisfy the purpose of the analysis. It is a failure inherent within the unit of analysis.

3. Rhombus:  Identifies an event which is not developed further because of (a) insufficient information, (b) very remote likelihood of occurrence, or (c) due to other constraints (eg. time, money, etc.) which preclude further analysis. If at a later date, however, constraints are removed and it is desired to analyze the rhombus in greater depth, then it can be changed to a rectangle in which case it could be developed and analyzed further. The rhombus has no relationship with the diamond used as a decision point in flow charting.

4. House:  Identifies an event which, under normal conditions, is expected to occur in the system defined and by itself may not cause a failure event. The importance of noting it, however, is that when combined with other events it might contribute to a failure event.

A rudimentary fault tree branch is portrayed in Figure 3. The botton of the tree, for any fault tree branch, should always have events depicted by the circle, rhombus, or house. These signify the end of development. In the example portrayed in Figure 3, there are two branches of the tree and three levels of development or analysis. The tree would read: "Event A can be produced <u>either</u> by Event B <u>or</u> Event C or both. Event B can be produced only by the coexistence of Events D <u>and</u> E. Event C can be produced either by Event F <u>or</u> Event G or both. Event E is viewed as a primary or a basic failure event. And Event F is an event which is normally expected to occur within the system, but which can contribute to Event C. Events, D, E, F, and G -- at the bottom of the tree -- require no further analysis or development."

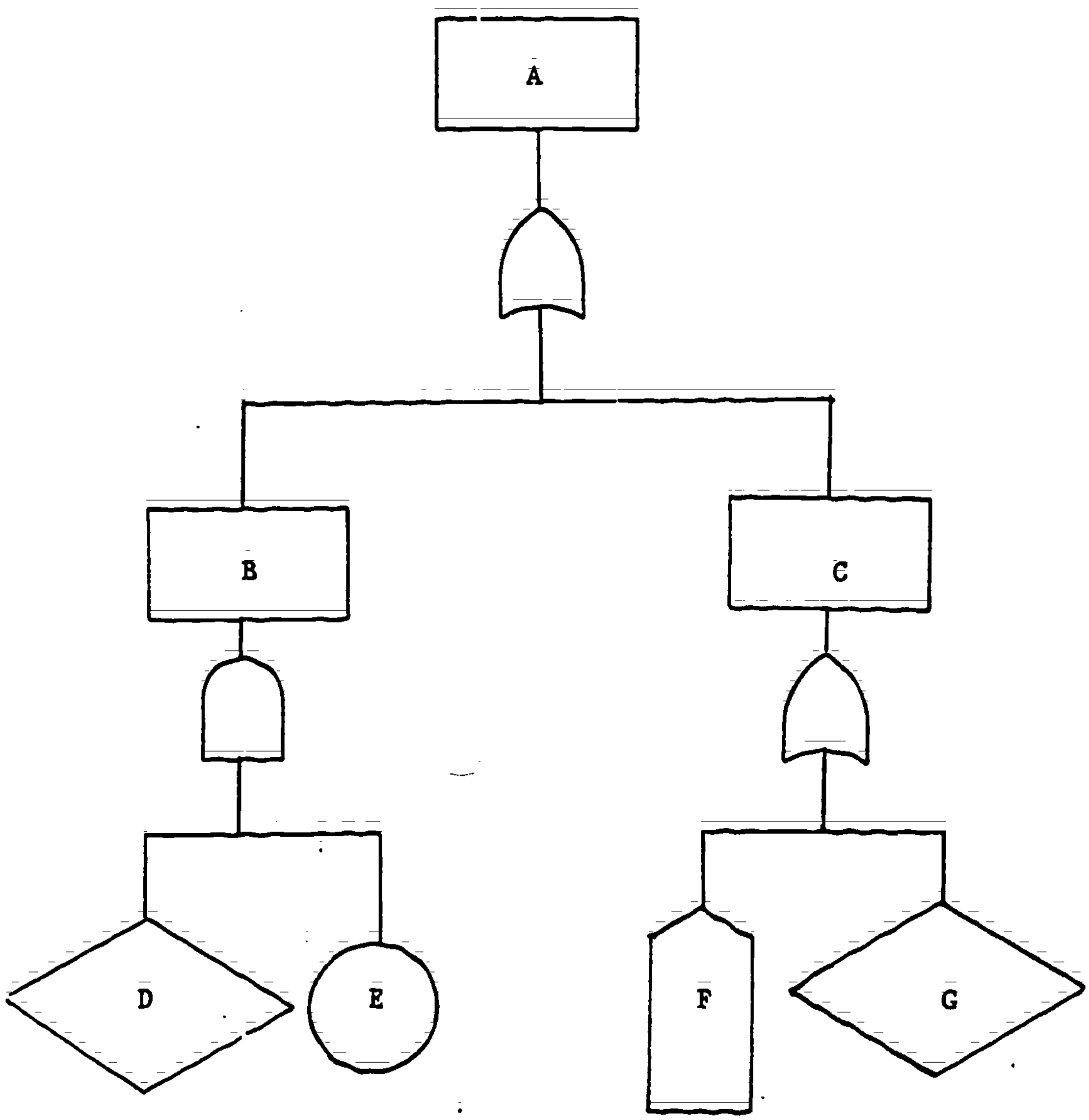


FIGURE 3. ILLUSTRATION OF A FAULT TREE BRANCH.

Drawing the Fault Tree

The purpose of fault tree analysis is not to analyze all the possible failure modes which could occur in a system, just the major ones. To help insure that no important events are omitted, it is wise to conduct a thorough mission analysis (see Figure 4) before attempting the graphical construction of the fault tree.

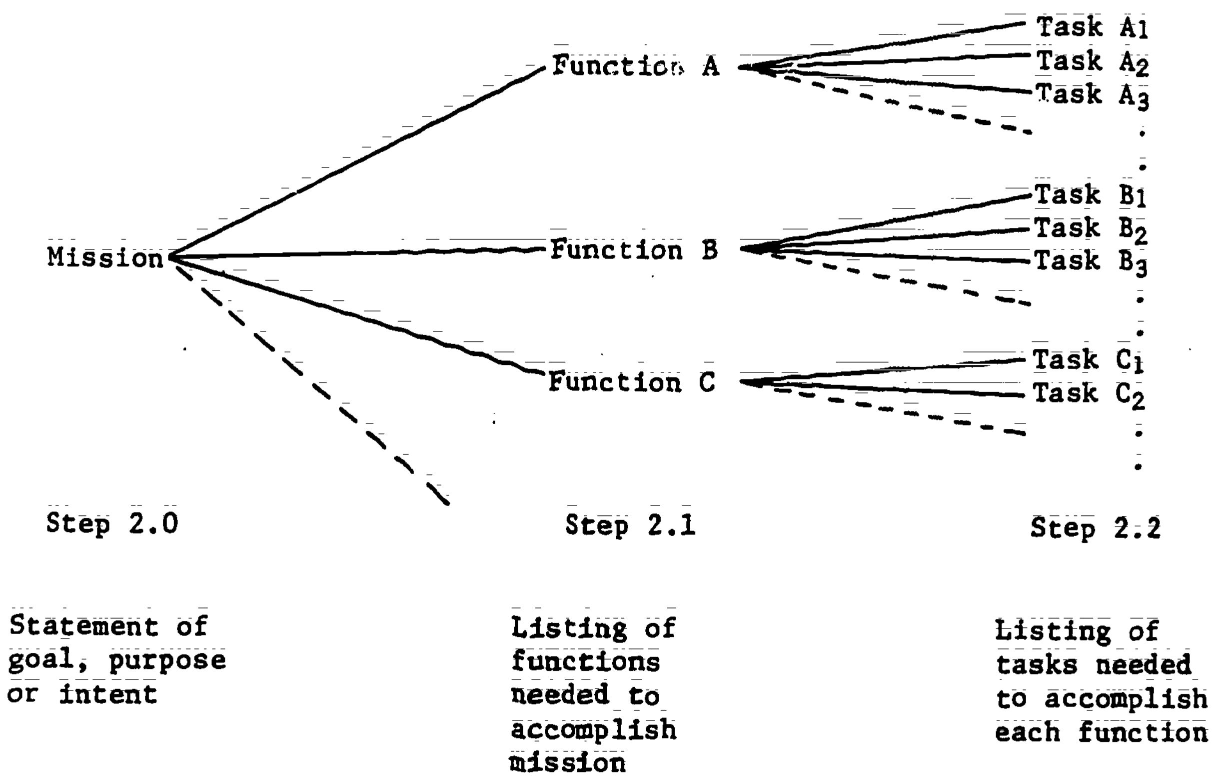
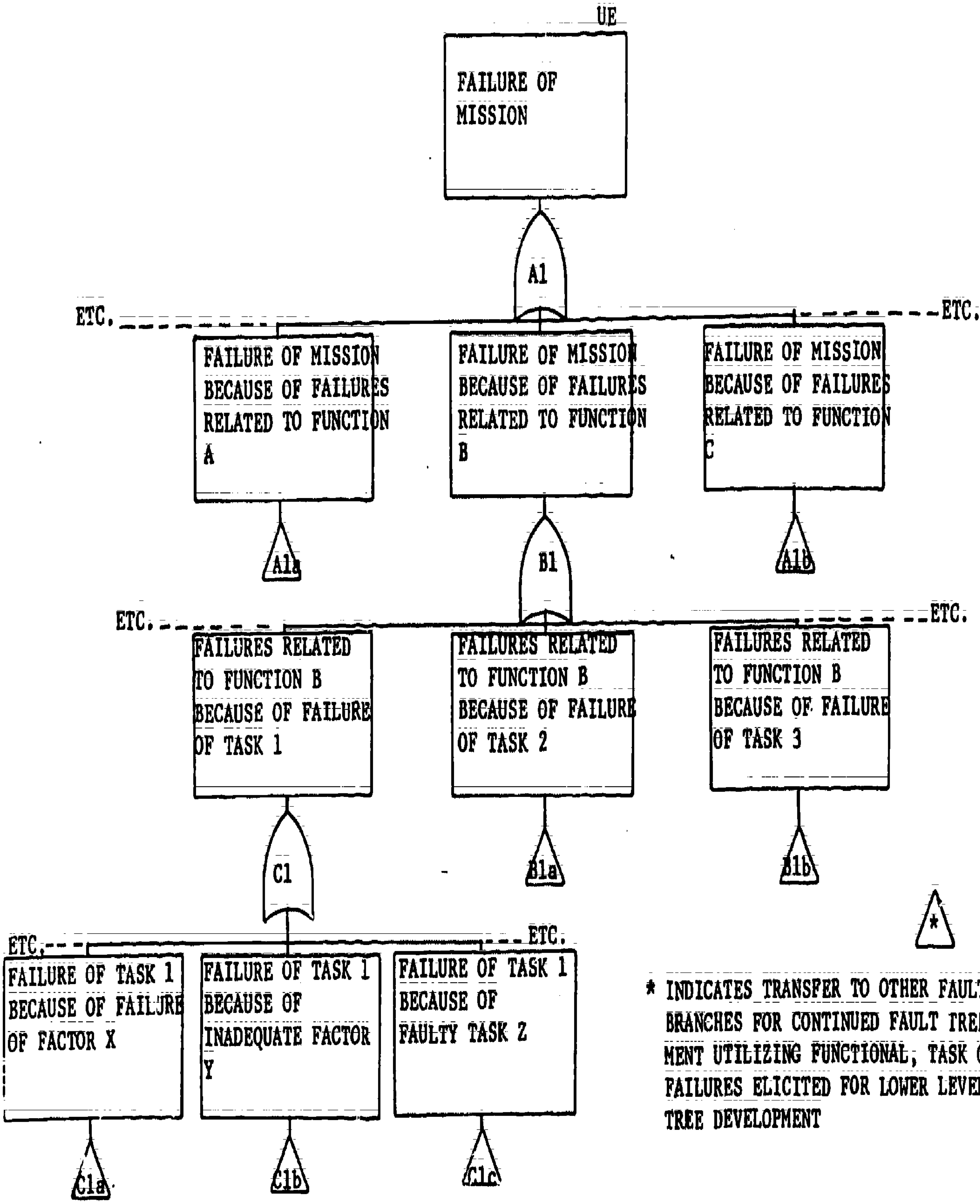


FIGURE 4. SCHEMATIC SHOWING MAJOR STEPS IN MISSION ANALYSIS.

The mission analysis is derived by systematically considering the major functions necessary to accomplish the mission and those important tasks which must be accomplished within each function. Mission analysis enables the analyst to see the system under study in a broad perspective, at the same time identify specific areas that might undergo failure analysis.

Actual fault tree construction begins with the selection of a top or most general undesired event (UE). The UE may be stated in terms of failure of the entire mission, or a failure identified with some function or task crucial to the success of the mission. Regardless, it stands at the top of the tree and analysis proceeds downward and outward. Inputs to the UE, in turn, become contributory failure events in a perceived cause and effect relationship. The analyst drawing the fault tree, should have a good working knowledge of the system under analysis, or immediate access to experts who do.

In generating the tree, the basic question seems to be: "Given a specified UE, what sequences of events may possibly take place to result in the actual occurrence of the UE?" Drawing the tree is a deductive process. The general methodology is to identify predecessor events from the top of the tree successively down to initiating or primal failure events. Once constructed -- and in the process of construction -- the tree is read from the top down, noting at each level whether events are inputs to AND gates or OR gates. In an effort to help insure proper diagnosis of each failure event, the analyst should be very specific in formulating failure statements. Each failure statement should contain four vital words: "Failure of ... because of ..." or a suitable euphemism for them (see Figure 5).



* INDICATES TRANSFER TO OTHER FAULT TREE BRANCHES FOR CONTINUED FAULT TREE DEVELOPMENT UTILIZING FUNCTIONAL, TASK OR OTHER FAILURES ELICITED FOR LOWER LEVEL FAULT TREE DEVELOPMENT

FIGURE 5. GENERAL FORMAT FOR DESCRIBING FAILURE EVENTS IN A FAULT TREE.

As the analysis proceeds, it will be found that very similar events, or even identical ones, will often show up in different branches of the tree. This is a signal to the analyst to examine them in more detail, particularly if it is felt that the likelihood of their occurence is high.

The analysis will be more accurate and efficient if it is done horizontally rather than vertically — that is, if all the inputs to an undesired event are generated at one level before proceeding to the next level. The analysis need not proceed any further than the analyst desires. Some events may be represented by twelve levels, whereas others may be developed to only two. The general rule is that each failure event should be developed to a point where cause and effect relationships may be identified, and from which rectification or treatment can be applied. The bottom of the tree, for any branch, will always have terminal events.

Formulating Recommendations

Once the tree has been completely drawn, events can be subjectively ranked against each other at each level to determine the strategic path(s) of possible failure occurence. In addition, Stephens (1979) has designed a computer program which calculates the relative probability of occurence for each event. Discussion of the computer program and its application is beyond the scope of this paper. For small trees (less than 300 events) much information, including the ranking of events, may be gained by simply inspecting the tree without necessarily quantifying events in the tree via a computer program.

The final step in conducting a fault tree analysis is to make recommendations to promote success of a system based on the identification of a strategic failure path(s) and terminal failure events. One of the great values of fault tree analysis, as it relates to the formulation of recommendations is that emphasis is focused not only on the strategic path(s) but also on the bottom levels or terminal events of the tree. If each bottom event is avoided or rectified, then logically the entire sequence of failure events above it would likewise not occur. Hence, in formulating recommendations, not only is the strategic path(s) investigated closely, but also each terminal event of interest.

In the drawing of the tree and its inspection, an individual or team of experts can easily identify areas in which special care should be given within a system to help insure its success. If the analysis is made during the design of a new program, the decisions based on it could confirm original feelings or lead to design changes. Recommendations based on the completed tree and identification of the strategic path may lead to reallocation of resources, installments of back-up systems, monitoring of paths with high failure potential, provisions for improved communications, or the taking of corrective action. Furthermore, visually displaying the completed fault tree and discussing the strategic paths with personnel at various levels of the organization often results in the formation of excellent suggestions for improvements and creates an appreciation for the entire system seen as a whole.

Conclusion

By examining failure modes, the fault tree process generates questions about a system which would not occur under the usual conditions of success analysis. In generating failure inputs, the fault tree method focuses thinking on specifics. In addition, such analysis focuses attention on aspects that might otherwise be overlooked by considering such questions as, "If this event were to happen because of such and such causes, what measures can we fall back on?" Furthermore, the methodology elicits answers to the question "why?" That is, "why does a system fail, or why might it fail?"

In summary, fault tree analysis has great, but relatively untested potential for use under the following conditions:

1. Whenever undesired events or concerns and factors contributing to such can be identified.
2. Whenever involvement of the members of an organization needs structure and systemizing.
3. Whenever a defensible approach to resource allocation within a complex system is needed.
4. Whenever consensus as to what constitutes success within a system is difficult to obtain.

References

Kent Stephens. _Fault tree Analysis: A Management Science Technique for Educational Planning and Evaluation._ Technical Report Number 2. Alameda County School Department, Hayward, California, 1973.

Kent Stephens. "A Fault Tree Approach to Needs Assessment -- An Overview." Paper Presented at Needs Assessment Conference. Oakland, California. April 8, 1976.

Kent Stephens, Ken Wood, and Bruce Barker. "Fault Tree Analysis: An Emerging Methodology for Instructional Science." _Instructional Science_, Volume 8, Number 1, January 1979.