What Is a Fault Tree Analysis?

Use a general conclusion to determine specific causes of a system failure

by Simha Pilot

The fault tree analysis (FTA) was first introduced by Bell Laboratories and is one of the most widely used methods in system reliability, maintainability and safety analysis. It is a deductive procedure used to determine the various combinations of hardware and software failures and human errors that could cause undesired events (referred to as top events) at the system level.

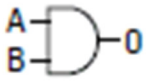
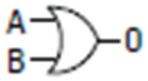
The deductive analysis begins with a general conclusion, then attempts to determine the specific causes of the conclusion by constructing a logic diagram called a fault tree. This is also known as taking a top-down approach.

The main purpose of the fault tree analysis is to help identify potential causes of system failures before the failures actually occur. It can also be used to evaluate the probability of the top event using analytical or statistical methods. These calculations involve system quantitative reliability and maintainability information, such as failure probability, failure rate and repair rate. After completing an FTA, you can focus your efforts on improving system safety and reliability.

FTA logic diagram

The basic symbols used in an FTA logic diagram are called logic gates and are similar to the symbols used by electronic circuit designers. Two kinds of gates, "and" and "or," are described in Table 1.

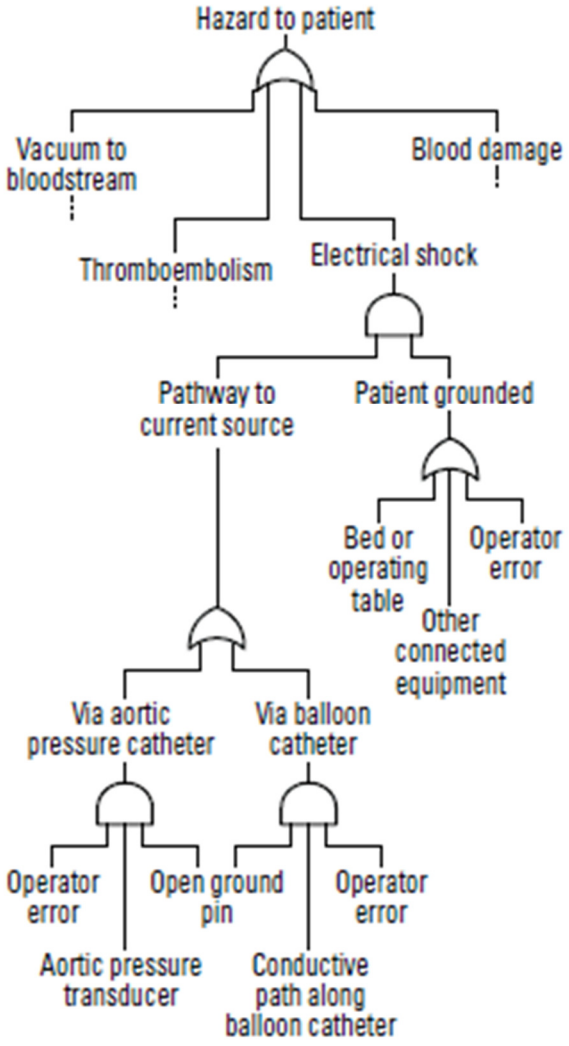
TABLE 1 Logic Gates

Description	Picture	Truth table		
The "and" gate indicates the output occurs if all the input events are present.		Input A	Input B	Output
		T	T	T
		T	F	F
		F	T	F
		F	F	F
The "or" gate indicates the output occurs if at least one of the input events is present.		Input A	Input B	Output
		T	T	T
		T	F	T
		F	T	T
		F	F	F

If a part or another factor is functioning correctly, the state is true (T). If the part or other factor is malfunctioning, the state is false (F). When a logic statement is true, it is assigned a Boolean logic value of one. When a logic statement is false, it is assigned a Boolean logic value of zero.

The partial FTA logic diagram in Figure 1 uses the "and" and "or" gates' symbols to analyze hazard to the patient. Inputs to the "or" gate at the top identify the four reasons this failure can occur. One of the reasons, electrical shock, is then broken down because it results from simultaneously grounding the patient and creating a pathway to a current source (an "and" gate). The analysis continues on, using the same technique, until the lowest levels such as operator error or open ground pin are identified.

FIGURE 1 Fault Tree Depicting The Root Causes of Hazard to Patients During Surgery



When you perform an FTA, you systematically determine what happens to the system when the status of a part or another factor changes. In some applications, the minimum criterion for success is that no single failure can cause injury or an undetected loss of control over the process. In others, where extreme hazards exist or when high value product is being processed, the criteria may be increased to require toleration of multiple failures.

Fault tree construction

To do a comprehensive FTA, follow these steps:

1. Define the fault condition, and write down the top level failure.
2. Using technical information and professional judgments, determine the possible reasons for the failure to occur. Remember, these are level two elements because they fall just below the top level failure in the tree.
3. Continue to break down each element with additional gates to lower levels. Consider the relationships between the elements to help you decide whether to use an "and" or an "or" logic gate.
4. Finalize and review the complete diagram. The chain can only be terminated in a basic fault: human, hardware or software.
5. If possible, evaluate the probability of occurrence for each of the lowest level elements and calculate the statistical probabilities from the bottom up.

Bibliography

Anderson, R.T., *Reliability Design Handbook* (Chicago: IIT Research Institute, 1976).

Evans, James R., and William M. Lindsay, *The Management and Control of Quality* (Mason, OH: South-Western Thomson Learning, 2001).

Juran, Joseph M., and Frank M. Gryna, *Quality Planning and Analysis* (New York: McGraw-Hill, 1991).

Michalsky, Walter J., *Top Tools for Manufacturers* (Portland, OR: Productivity Press, 1998).

Simha Pilot is a general manager at SPC Consultants in Israel. He received a master's degree in business administration from Tel Aviv University. Pilot is a member of ASQ and is an ASQ certified quality manager and quality systems lead auditor.