Safety Corner

What is a Fault Tree?

A fault tree analysis (FTA) is a systematic, deductive, top-down method of analyzing system design and performance by addressing the causal relations between a given event, which is usually a system failure event or an undesirable outcome called the top event, and the events leading to it. It is deductive in the sense that a fault tree always starts from a defined top event sitting on the top most layer. The tree then unfolds the failure causes backward (or downward in the sense of a tree) to show the causes for the top event to occur down to the primary independent faults called the basic events at the bottom of the tree. The failure causes can be subsystem or component failures, natural phenomena, common mode failures, as well as human interactions.

Fault trees are built by linking the top event with the associated intermediate events and basic events through logic gates to show the failure logic between the events. There are, in practice, many other gates commonly used in the symbolic representation in additional to the conventional AND/OR gates in a fault tree analysis.

Fault trees can be used to qualitatively or quantitatively to evaluate system failures. The route between the top event and the basic events in the tree is called a Cutset. The shortest credible way through the tree from basic events to a top event is called a Minimal Cutset, which can be used to illustrate the unique failure logic of the top event and to quantify the failure probability or unavailability of the top event through boolean algebra. Without the analysis of minimal cutsets, the results of a fault tree analysis may not be meaningful. There are also techniques to analyse the relative importance of each basic event to the top event, and the uncertainties associated with the events.

==========

The Safety Corner is contributed by Ir Dr. Vincent Ho, who can be contacted at vsho.hkarms@gmail.com