Probabilistic Fault Tree Analysis

S. Mohindra
Arthur D. Little, Inc.
Acorn Park, Cambridge, MA 02140, USA
Phone: (617) 498-5831
e-mail: mohindra.s@adlittle.com

ABSTRACT

Fault Tree analysis (FTA) is a system level deductive method for determining the various combinations of hardware failures, software failures, and human errors that could result in the occurrence of an undesired event (referred to as top event). The main purpose of fault tree analysis is to evaluate the probability or the frequency of the top event using quantitative information about the causal events (referred to as base events). FTA can provide useful information concerning the likelihood of a failure and the means by which such a failure could occur. Efforts to improve system safety and reliability can be focused and refined using the results of the FTA.

More often than not, deterministic inputs are often used for the frequencies and probabilities of base events. This masks the uncertainty of the result, and results in a loss of information such as the range and the distribution of top event probability or frequency. Consider the following scenario. John Mangler knows that on an average his widget has a life of between 18-24 months. He wants to use fault tree analysis to estimate the top event failure frequency. A dedicated engineer, he wants to bound the top event frequency by performing a scenario analysis for 18, 21, and 24 months. He quickly realizes that for his 12 base events, he would have to run a huge number of different fault tree scenarios, and then try to make sense of the various results. He gives up and uses the average numbers to come up with the average top event result. With 12 base events to consider, he no longer has a gut feel for the lower and upper bounds for the top event either. He does not know how the uncertainty in his failure estimates affects the quantification of the top event.

This paper presents a generic method for performing Fault Tree analysis using probability distributions for base events instead of single numbers. It relies on Monte-Carlo simulation to sample these base event distributions and then compute a probability distribution for the top event of the fault tree.