CE-370 Safety and Reliability of Engineering Systems

Instructor: Eric M. Hernandez, PhD

SUMMARY OF LECTURE 12 - FAULT/EVENT TREE ANALYSIS

FAULT TREE

A fault tree is a top-down methodology to logically determine the potential causes of a fault, failure and(or) undesired event. Fault Tree Analysis (FTA) was originally developed in 1962 at Bell Laboratories by H.A. Watson and since then it has become an essential tool in reliability analysis. A fault tree is an inverse problem, in which one tries to answer the question: What are(were) the causes of a certain failure/fault/undesired event? This undesired event must be selected carefully in order not to make the task unmanageable, but at the same time, it can not be selected so narrowly that it proves insufficient to characterize the system behavior.

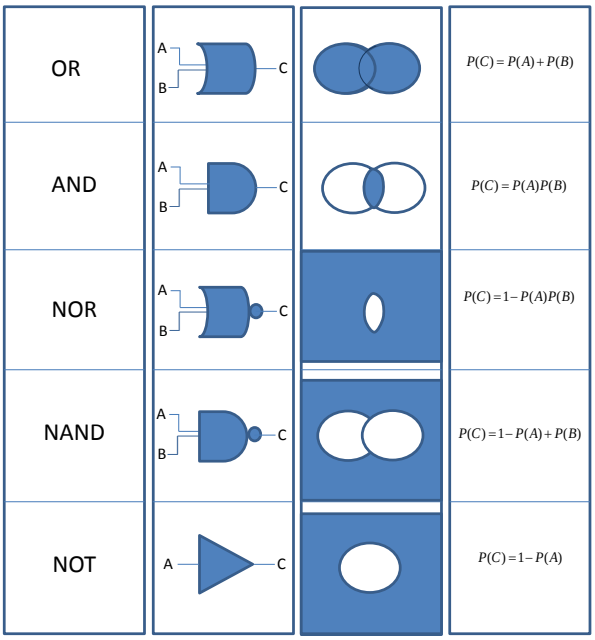
EVENT TREE

An event tree is an inductive bottom-up methodology to logically determine the potential effects of a fault or failure. In an event tree the main objective is to answer the question, *what if — happens?* An event tree can be considered as a lower bound method, because it will very likely have missing or unforseable consequences, hopefully these are of negligible importance. An event tree typically follows a fault tree analysis.

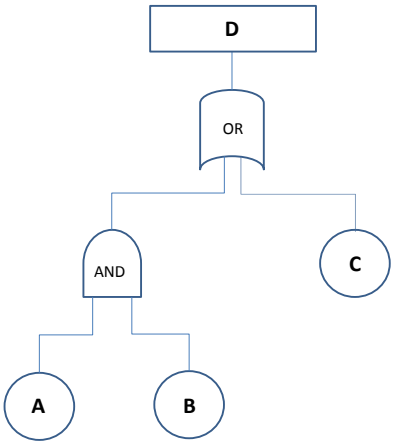
Fault and Event trees are composed of basic events, intermediate events and logic gates.

- **Basic Events**: Failure of component
- **Intermediate Event**: Used to indicate an important intermediate event or the failure of a sub-system
- **External Event**: Events that are expected to occur, but are not faults per se.
- **Logic Gates**: Describe the relationship between input and output events. The symbols are derived from Boolean logic symbols. These are OR, AND, NOR, NAND and NOT gates.

The following table describes the basic logic gates, their set properties and probabilistic interpretation.



Below an example of a simple fault tree. In this case if $p(A) = 1 \times 10^{-3}$, $p(B) = 2 \times 10^{-3}$, $p(C) = 3 \times 10^{-5}$, one can easily show that $p(D) = 3.2 \times 10^{-5}$



For futher reading on the subject see:

Fault Tree Handbook (NUREG-0492). U.S. Nuclear Regulatory Commission,1981.

Stewart, M. and Melchers, R., Probabilistic Risk Assessment of Engineering Systems, 1997, Chapman and Hall.