Chapter 16

Fault Tree Analysis (FTA) via Binary Diagram Decision (BDD) for Information Systems Design

Fausto Pedro García Márquez
University of Castilla-La Mancha, Spain

Alberto Pliego Mangurán
University of Castilla-La Mancha, Spain

Noor Zaman
King Faisal University, Saudi Arabia

ABSTRACT

A fault tree analysis (FTA) is presented as a qualitative method for studying the state of the WT as a system considering to its different sub-systems. The quantitative analysis of the FTA is done by Binary Diagram Decision (BDD). The size of the BDD generated by the transformation from FTA to BDD will depend on the ordering of the FTA events. This work employed the top-down-left-right, the level, and the “and” methods for listing the events. Finally, a classification of the events is done based on their importance measures. The importance measures has been calculated by the Birnbaum (1969), Critically and Structural heuristic methods. A comparative analysis is done, and the main results are presented.

INTRODUCTION

An FTA model is a graphical representation of logical relations between events (usually failure or fault events). Complex systems analysis may produce thousands of combinations of events (cut-sets) that can cause the system failure. The determination of these cut-sets can be a large and time-consuming process even on modern high speed digital computers. The determination of the exact top event probability also requires lengthy calculations if the fault tree has a great number of cut-sets.
Example

Figure 1 shows an example of a pumping station from the A reservoir to B reservoir. The system has three valves and two pump motors. The FTA associated to the system given in Figure 1 is shown in Figure 2.

Figure 1. Pumping station

Figure 2. FTA associated to the system shown in Figure 1

Nomenclature:
- \( V \): Valve
- \( P \): Pump
- \( \text{Top} \): Reservoir A does not receive water.
- \( g1 \): \( V3 \) does not receive water
- \( g2 \): \( V1 \) and \( P1 \) do not receive water
- \( g3 \): \( V2 \) and \( P2 \) do not receive water
- \( e1 \): Level in B is not enough
- \( e2 \): Fault in \( V3 \). Closed
- \( e3 \): Fault in \( P1 \)
- \( e4 \): Fault in \( V1 \). Closed
- \( e5 \): Fault in \( P2 \)
- \( e6 \): Fault in \( V2 \). Closed

For many complex fault trees this requirement may be beyond the capability of the available computers. As a consequence, approximation techniques have been introduced with a loss of accuracy. BDD provides a new alternative to the traditional cut-set based approach for FTA that leads to the determination of the output value of the function through the examination of the values of the inputs.

Binary Diagram Decisions

Binary Decision Diagrams (BDDs), as a data structure that represents the Boolean functions, were introduced by Lee (1959) and further popularised by Akers (1978), Moret (1982), and Bryant (1986).

A BDD is a directed acyclic graph \((V, N)\), with vertex set \( V \) and index set \( N \). Vertex set contains two types of vertices. On the one hand, a terminal vertex has as attribute a value: \( \text{value}(v) \in \{0, 1\} \), where a 1 state, that corresponds to system failure, or a 0 state which corresponds to a system success. All the paths that have 1 state provide the cut-sets of the fault tree. On the other hand, a non terminal vertex \( v \) has as attributes an argument index \((v) \in N \{0,1,...,n\} \) and two descendants, low\((v) \) and high\((v) \) \( \in V \), that are connected by a branch. Each