Operative Diagnosis of Graph-Based Systems with Multiple Faults

Stefano Chessa and Paolo Santi

Abstract

The problem of multiple faults diagnosis in safety-critical systems is considered. Error propagation between system components is modeled as a directed graph, with the assumption that errors propagate instantaneously along the edges of the graph. Some of the system components are equipped with alarms, which ring when abnormal conditions are detected. A diagnosis algorithm identifies the set of potential failure sources based on the set of ringing alarms.
This paper introduces the D-FAULTS algorithm, which diagnoses the system under the assumption that at most two nodes are faulty at the same time. The concept of sequential diagnosis is also introduced, to deal with an unbounded number of faults. Sequential diagnosis is aimed at locating a set of nodes containing at least one fault. With this approach, a faulty system can be restored to normal condition by executing repeatedly the diagnosis and repair phases. To this purpose, we introduce the sequential diagnosis algorithm S-DIAG of optimal time complexity.