"The Translation of Parametric Dynamic Fault Trees in Stochastic Well-formed Nets as a Case of Graph Transformation"

Daniele Codetta Raiteri, PhD student, *codetta@di.unito.it*
Dipartimento di Informatica, Università di Torino, Italy

Abstract

The Fault Tree (FT) is a stochastic model for the reliability analysis of complex and large system: it allows to model as a Direct Acyclic Graph (DAG) whose structure is similar to a tree, how combinations of component failure events determine the failure of subsystems or of the whole system; FT is a bipartite graph: its nodes can be event nodes or gates; event nodes model the occurrence of failure events, while gates propagate the failure towards the upper level event nodes if a particular logic condition is verified; the lowest level event nodes represent the failure of the basic components of the system, the internal event nodes represent the failure of subsystems, while the root node models the failure of the whole system.

FT can be easily analysed in a combinatorial way, so FT is a widespread model for the reliability analysis, but it suffers from some modeling limitations, such as the assumption of statistical indipendence among events; for this reason, an evolution of such model, called Dynamic FT (DFT) has been proposed with the aim of modeling event dependencies and more complicated failure propagation modes. The combinatorial analysis is not enough for DFT: it needs also the state space analysis; the generation of the state space of a DFT may be complicated, while the state space of a Stochastic Petri Net (SPN) can be generated in a direct way; so, an approach for the DFT analysis consists of translating a DFT in a SPN modeling the same failure propagation mode. In the case of Parametric DFT (PDFT), i. e. DFT where a unique parameterised subtree represents compactly the failure propagation mode of several identical subsystems, the translation result is a Coloured SPN in the form of Stochastic Well-formed Net (SWN).

The translation of PDFT in SWN can be performed by means of transformation rules: PDFT nodes can be events or gates, so for every kind of event or gate, a rule for its transformation to SWN is defined; the starting graph is a PDFT and at each step of the transformation, an event or a gate is replaced by the corresponding SWN applying the relative rule; when the transformation process ends, we obtain a SWN that models the failure propagation mode of the whole starting PDFT. Now, the state space analysis of the PDFT can be performed through the corresponding SWN.