Reliability Engineering and System Safety 94 (2009) 872–883

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment

K. Durga Rao [a,*], V. Gopika [a], V.V.S. Sanyasi Rao [a], H.S. Kushwaha [a], A.K. Verma [b], A. Srividya [b]

[a] Bhabha Atomic Research Centre, Mumbai, India
[b] Indian Institute of Technology Bombay, Mumbai, India

ARTICLE INFO

Article history:
Received 21 July 2007
Received in revised form
22 September 2008
Accepted 24 September 2008
Available online 11 October 2008

Keywords:
Dynamic fault trees
Markov models
Monte Carlo simulation
Probabilistic safety assessment
Reactor regulation system

ABSTRACT

Traditional fault tree (FT) analysis is widely used for reliability and safety assessment of complex and critical engineering systems. The behavior of components of complex systems and their interactions such as sequence- and functional-dependent failures, spares and dynamic redundancy management, and priority of failure events cannot be adequately captured by traditional FTs. Dynamic fault tree (DFT) extend traditional FT by defining additional gates called dynamic gates to model these complex interactions. Markov models are used in solving dynamic gates. However, state space becomes too large for calculation with Markov models when the number of gate inputs increases. In addition, Markov model is applicable for only exponential failure and repair distributions. Modeling test and maintenance information on spare components is also very difficult. To address these difficulties, Monte Carlo simulation-based approach is used in this work to solve dynamic gates. The approach is first applied to a problem available in the literature which is having non-repairable components. The obtained results are in good agreement with those in literature. The approach is later applied to a simplified scheme of electrical power supply system of nuclear power plant (NPP), which is a complex repairable system having tested and maintained spares. The results obtained using this approach are in good agreement with those obtained using analytical approach. In addition to point estimates of reliability measures, failure time, and repair time distributions are also obtained from simulation. Finally a case study on reactor regulation system (RRS) of NPP is carried out to demonstrate the application of simulation-based DFT approach to large-scale problems.

1. Introduction

Fault tree (FT) analysis has gained wide spread acceptance for the quantitative reliability and safety analysis. FT is graphical representation of various combinations of basic failures that lead to the occurrence of undesirable top event. Starting with the top event all possible ways for this event to occur are systematically deduced. The methodology is based on three assumptions: (i) events are binary events, (ii) events are statistically independent, and (iii) relationship between events are represented by means of logical Boolean gates (AND, OR, and Voting). The analysis is carried out in two steps: a qualitative step in which the logical expression of the top event is derived in terms of prime implicants (the minimal cut-sets); a quantitative step in which on the basis of the probabilities assigned to the failure events of the basic components, the probability of occurrence of the top event is calculated.

The traditional static fault trees with AND, OR, and Voting gates cannot capture the dynamic behavior of system failure mechanisms such as sequence-dependent events, spares and dynamic redundancy management, and priorities of failure events. In order to overcome this difficulty, the concept of dynamic FTs is introduced by adding sequential notion to the traditional FT approach. System failures can then depend on component failure order as well as combination [1]. This is done by introducing dynamic gates into FTs. With the help of dynamic gates, system sequence-dependent failure behavior can be specified using dynamic FTs that are compact and easily understood. The modeling power of dynamic FTs has gained the attention of many reliability engineers working on safety critical systems [2].

Several researchers [1–3] proposed methods to solve dynamic FTs. Dugan et al. [1,4,5], has shown through a process known as modularization, it is possible to identify the independent sub-trees with dynamic gates and to use different Markov model for each of them. It was applied to computer-based fault tolerant systems successfully. But, with the increase in the number of basic elements, there is problem state space explosion. To reduce state space and minimize the computational time, an improved

[*] Corresponding author.
E-mail address: durga_k_rao@yahoo.com (K. Durga Rao).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.09.007

decomposition scheme where the dynamic sub-tree can be further modularized (if there exist some independent sub-trees in it) is proposed by Huang and Chang [6]. Amari et al. [2], proposed a numerical integration technique for solving dynamic gates. Though, this method is solving the state-space problem, it cannot be easily applied for repairable systems. Bobbio et al. [3,7], proposed Bayesian network-based method to further reduce the problem of solving dynamic FTs with state-space approach. Keeping the importance of sophisticated modeling for engineering systems in dynamic environment, several researches [8–11] contributed significantly to the development and application of dynamic FTs.

However, state-space approach for solving dynamic gates becomes too large for calculation with Markov models when the number of gate input increases. This is the case especially with probabilistic safety assessment (PSA) of nuclear power plant (NPP) where there is large number of cut sets. In addition, Markov model is applicable for exponential failure and repair distributions and also modeling test, maintenance information on spare components is difficult. Many of the methods to solve dynamic FTs are problem specific and it may be difficult to generalize for all the scenarios. In order to address some of these limitations of the above-mentioned methods, Monte Carlo simulation approach is attempted here to implement dynamic gates. Scenarios which may often be difficult to solve with analytical solutions are easily tackled with the Monte Carlo simulation approach. Monte Carlo simulation-based reliability approach, due to its inherent capability in simulating the actual process and random behavior of the system, can eliminate uncertainty in reliability modeling [12,13]. A software tool, Dynamic Reliability with SIMulation (DRSIM) is developed to do comprehensive dynamic FT analysis. Two reliability problems are solved with the tool and found that results are exactly matching with the analytical approaches. After validation of the approach, it is extended to a case study on RRS of NPP.

2. Dynamic fault tree analysis: dynamic gates

Dynamic fault trees (DFTs) introduces four basic (dynamic) gates: the priority AND (PAND), the sequence enforcing (SEQ), the standby or spare (SPARE), and the functional dependency (FDEP) [1]. They are discussed here briefly.

The PAND gate reaches a failure state if all of its input components have failed in a pre-assigned order (from left to right in graphical notation). A SEQ gate forces its inputs to fail in a particular order: when a SEQ gate is found in a DFT, it never happens that the failure sequence takes place in different orders. While the SEQ gate allows the events to occur only in a pre-assigned order and states that a different failure sequence can never take place, the PAND gate does not force such a strong assumption: it simply detects the failure order and fails just in one case (in Fig. 1—PAND: failure occurs if A fails before B, but B may fail before A without producing a failure in G).

SPARE gates are dynamic gates modeling one or more principal components that can be substituted by one or more backups (spares), with the same functionality (Fig. 1). The SPARE gate fails when the number of operational powered spares and/or principal components is less than the minimum required. Spares can fail even while they are dormant, but the failure rate of an unpowered spare is lower than the failure rate of the corresponding powered one. More precisely, λ being the failure rate of a powered spare, the failure rate of the unpowered spare is $\alpha\lambda$, where $0\leqslant\alpha\leqslant 1$ is the dormancy factor. Spares are more properly called “hot” if $\alpha=1$ and “cold” if $\alpha=0$.

In the FDEP gate (Fig. 1), there will be one trigger-input (either a basic event or the output of another gate in the tree) and one or more dependent events. The dependent events are functionally dependent on the trigger event. When the trigger event occurs, the dependent basic events are forced to occur. In the Markov-chain generation, when a state is generated in which the trigger event is satisfied, all the associated dependent events are marked as having occurred. The separate occurrence of any of the dependent basic events has no effect on the trigger event.

3. Monte Carlo simulation-based approach for dynamic gates

Monte Carlo simulation is a very valuable method which is widely used in the solution of real engineering problems in many fields. Lately the utilization of this method is growing for the assessment of availability of complex systems and the monetary value of plant operations and maintenances [12–15]. The complexity of the modern engineering systems besides the need for realistic considerations when modeling their availability/reliability renders analytical methods very difficult to be used. Analyses that involve repairable systems with multiple additional events and/or other maintainability information are very difficult to solve analytically (dynamic FTs through state space, numerical integration, Bayesian network approaches). Dynamic FT through simulation approach can incorporate these complexities and can give wide range of output parameters.

Simulation technique estimates the reliability indices by simulating the actual process and random behavior of the system in a computer model in order to create a realistic lifetime scenario of the system. This method treats the problem as a series of real experiments conducted in a simulated time. It estimates the probability and other indices by counting the number of times an event occurs in simulated time. The required information for the analysis is: probability density functions (PDF) for time to failure and repair of all basic components with the parameter values; maintenance policies; interval and duration of tests and preventive maintenance.

Components are simulated for a specified mission time for depicting the duration of available (up) and unavailable (down) states. Up and down states will come alternatively, as these states are changing with time they are called state time diagrams. Down state can be due to unexpected failure and its recovery will

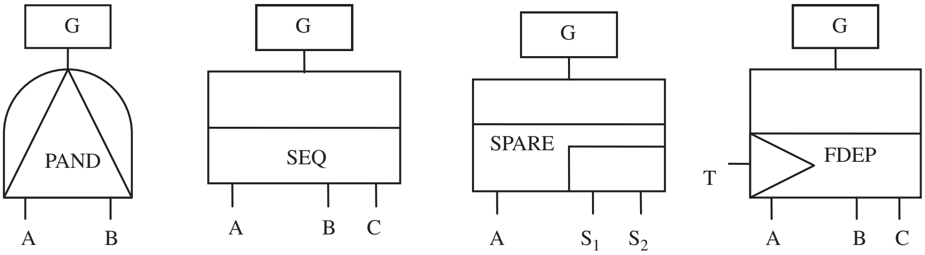

Fig. 1. Dynamic gates.