Available online at www.sciencedirect.com
ScienceDirect
Reliability Engineering and System Safety 93 (2008) 922–932
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

RADYBAN: A tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks

S. Montani, L. Portinale*, A. Bobbio, D. Codetta-Raiteri

Dipartimento di Informatica, Università del Piemonte Orientale, Via Bellini 25g, 15100 Alessandria, Italy

Available online 19 March 2007

Abstract

In this paper, we present RADYBAN (Reliability Analysis with DYnamic BAyesian Networks), a software tool which allows to analyze a dynamic fault tree relying on its conversion into a dynamic Bayesian network. The tool implements a modular algorithm for automatically translating a dynamic fault tree into the corresponding dynamic Bayesian network and exploits classical algorithms for the inference on dynamic Bayesian networks, in order to compute reliability measures. After having described the basic features of the tool, we show how it operates on a real world example and we compare the unreliability results it generates with those returned by other methodologies, in order to verify the correctness and the consistency of the results obtained.

1. Introduction

The modeling possibilities offered by *fault trees* (FT), one of the most popular techniques for dependability analysis of large, safety critical systems, can be extended by relying on *Bayesian networks* (BN) [1–5]. This formalism allows to relax some constraints which are typical of FTs. In addition, BNs allow to represent local dependencies and to perform both predictive and diagnostic reasoning.

In [6], we have shown how BNs can provide a unified framework in which also *dynamic fault trees* (DFT) [7], a rather recent extension to FTs able to treat several types of dependencies, can be represented.

In particular, DFTs introduce four basic (dynamic) gates: the warm spare (WSP), the sequence enforcing (SEQ), the functional dependency (FDEP) and the priority AND (PAND). A WSP dynamic gate models one primary component that can be substituted by one or more backups (spares), with the same functionality (see Fig. 1(a), where spares are identified by "circle-headed" arcs). The WSP gate fails if its primary fails and all of its spares have failed or are unavailable (a spare is unavailable if it is shared and being used by another spare gate). Spares can fail even while they are dormant, but the failure rate of an unpowered (i.e. dormant) spare is lower than the failure rate of the corresponding powered one. More precisely, being λ the failure rate of a powered spare, the failure rate of the unpowered spare is $\alpha\lambda$, with $0 \leqslant \alpha \leqslant 1$ called the dormancy factor. Spares are more properly called "hot" if $\alpha = 1$ and "cold" if $\alpha = 0$.

A SEQ gate forces its inputs to fail in a particular order: when a SEQ is found in a DFT, it never happens that the failure sequence takes place in different orders. SEQ gates can be modeled as a special case of a cold spare [8], so they will not be considered any more in the following.[1]

In the FDEP gate (Fig. 1(b)), one trigger event T (connected with a dashed arc in the figure) causes other dependent components to become unusable or inaccessible. In particular, when the trigger event occurs, the dependent components fail with $p_d = 1$; the separate failure of a dependent component, on the other hand, has no effect on the trigger event. FDEP has also a non-dependent output, that simply reflects the status of the trigger event and is called dummy output (i.e. not used in the analysis).

We have generalized the FDEP by defining a new gate, called probabilistic dependency (PDEP). In the PDEP, the

*Corresponding author. Tel.: +39 0131 360 184; fax: +39 0131 360 198.
E-mail addresses: stefania@mfn.unipmn.it (S. Montani), portinal@mfn.unipmn.it (L. Portinale), bobbio@mfn.unipmn.it (A. Bobbio), raiteri@mfn.unipmn.it (D. Codetta-Raiteri).

[1] The conceptual difference between the two kinds of gates is that the inputs to a SEQ do not need to be a component and its set of spares, but can be components covering any kind of function in the FT.

0951-8320/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2007.03.013

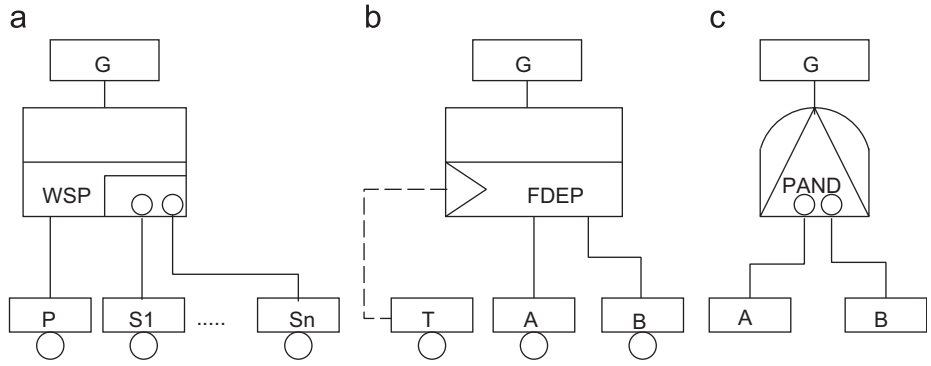

Fig. 1. Dynamic gates in a DFT.

probability of failure of dependent components, given that the trigger has failed, is $p_d \leqslant 1$.

Finally, the PAND gate reaches a failure state if and only if all of its input components have failed in a preassigned order (from left to right in graphical notation). While the SEQ gate allows the events to occur only in a preassigned order and states that a different failure sequence can never take place, the PAND does not force such a strong assumption: it simply detects the failure order and fails just in one case (in Fig. 1(c) a failure occurs iff A fails before B, but B may fail before A without producing a failure in G).

The quantitative analysis of DFTs typically requires to expand the model in its state space, and to solve the corresponding continuous time Markov chain (CTMC) [7]. Through a process known as modularization [9], it is possible to identify the independent sub-trees with dynamic gates, and to use a different Markov model (much smaller than the model corresponding to the entire DFT) for each one of them. Nevertheless, there still exists the problem of state explosion.

In order to alleviate this limitation, as stated above, we have proposed a translation of the DFT into a *dynamic Bayesian network* (DBN). With respect to CTMC, the use of a DBN allows one to take advantage of the factorization in the temporal probability model. As a matter of fact, the conditional independence assumptions implicit in a DBN enable a compact representation of the probabilistic model, allowing the system designer or analyst to avoid the complexity of specifying and using a global-state model (like a standard Markov Chain); this is particularly important when the dynamic module of the considered DFT is significantly large.

In this paper, we describe RADYBAN (Reliability Analysis with DYnamic BAyesian Networks), a tool we have implemented able to realize an automatic translation of a DFT into the corresponding DBN. The tool allows the reliability engineer to access the modeling constructs of an enhanced version of the DFT formalism for the construction of the suitable reliability model; the resulting model is then compiled in the corresponding DBN and the analysis is performed in a transparent way to user, who has just to specify the desired type of analysis algorithm.

The rest of the paper is organized as follows: In Section 2 we briefly review the basic framework of DBNs, in Section 3 we describe the main functionalities of RADYBAN, by taking into consideration in particular the translation from a DFT to a DBN for the computation of reliability measures, and finally in Section 4, we show an application of the tool features to a real world example taken from [2], concerning an active heat reaction system. Conclusions and future works are then reported in Section 5.

2. Dynamic Bayesian networks

DBNs [10] extend the BNs formalism by providing an explicit discrete temporal dimension. They represent a probability distribution over the possible histories of a time-invariant process; the advantage with respect to a classical probabilistic temporal model like Markov chains is that a DBN is a stochastic transition model factored over a number of random variables, over which a set of conditional dependency assumptions is defined.

Time invariance ensures that the dependency model of the variables is the same at any point in time. While a DBN can in general represent semi-Markovian stochastic processes of order $k-1$, providing the modeling for k time slices, the term DBN is usually adopted when $k=2$ (i.e. only two time slices are considered in order to model the system temporal evolution; for this reason such models are also called 2-TBN or 2-*time-slice temporal Bayesian network*).

Given a set of time-dependent state variables $X_1 \ldots X_n$ and given a BN N defined on such variables, a DBN is essentially a replication of N over two time slices t and $t+\Delta$ (Δ being the so-called discretization step usually assumed to be 1), with the addition of a set of arcs representing the transition model. Letting X_i^t denote the copy of variable X_i at time slice t, the transition model is defined through a distribution $P[X_i^{t+\Delta}|X_i^t, Y^t, Y^{t+\Delta}]$ where Y^t is any set of variables at slice t other than X_i (possibly the empty set), while $Y^{t+\Delta}$ is any set of variables at slice $t+\Delta$ other than X_i ($Y^{t+\Delta}$ is non-empty only in the case of the PDEP gate conversion). Arcs interconnecting nodes at different slices are called inter-slice edges, while arcs interconnecting nodes at the same slice are called intra-