Improved Dynamic Fault Tree modelling using Bayesian Networks

David Marquez
Dep. of Computer Science
Queen Mary, University of London
marquezd@dcs.qmul.ac.uk

Martin Neil
Dep. of Computer Science
Queen Mary, University of London
martin@dcs.qmul.ac.uk

Norman Fenton
Dep. of Computer Science
Queen Mary, University of London
norman@dcs.qmul.ac.uk

1. Background

In modelling fault-tolerant systems, space state based approaches such as dynamic fault trees (DFTs) [4], have been shown to increase the power of traditional combinatorial models, like static fault trees (FTs) [9]. However, in practice, these approaches have severe limitations when dealing with the increasing complexity of component dependencies and failure behaviours of today's real-time fault-tolerant systems. Two major limitations are: 1) the problem of space state explosion and 2) the inability to handle non-exponential failure distributions for some dynamic constructs.

Bayesian Networks (BNs), and their extension for time-series modelling known as Dynamic Bayesian Networks (DBNs), [5], have shown to provide to a unified framework for reliability modelling and analysis of complex systems, [6]. In particular, the BN framework allows a compact representation of the temporal (and functional) dependencies among the system components and event-dependent failure behaviours characteristic of fault-tolerant systems, avoiding the state space explosion problem of the Markov Chain based approaches to DFT analysis, [3], [10].

In [8] we presented a new, effective and flexible event-based hybrid BN modelling method for Fault Tree analysis that scales up to large, complex dynamic systems. The new approach incorporates a recent powerful approximate inference algorithm for hybrid BNs, [7], based on a process of dynamic discretisation of the domain of all continuous variables in the BN, and the entropy error, as the basis for approximation. By combining the modelling capabilities of BNs with our dynamic discretisation inference algorithm we offer a unified technique for reliability analysis of large, safety critical systems, which overcomes most of the limitations of both space-state based reliability models and previous BN approaches. In our BN framework, continuous failure times with general parametric or empirical time-to-failure distributions occurring in practical applications, as well as discrete variables modelling the state of the system (or any subsystem) at a particular time instance, can be included in the model in a simple unified way. Approximated solutions for both static and dynamic constructs are obtained simultaneously, and so modularisation techniques, numerical integration and simulation methods are all unnecessary. Furthermore, Bayesian reliability data analysis can be easily carried out in our framework, allowing us to integrate information from multiple sources at different levels of granularity, as well as expert opinion.

The approach offers a powerful framework for analysts and decision makers to successfully perform robust reliability assessment. Sensitivity, uncertainty, diagnosis analysis, common cause failures, and warranty analysis can also be easily performed within this framework. All the example models in [8] were built and executed using the Bayesian Network tool AgenaRisk [1], in which the dynamic discretisation algorithm [7] is now implemented.

2. Applying the approach to an example of FT-like analysis

The example provided here is the redundant multiprocessor system, for which a detailed description is given in [2]. The BN model for this system is shown in Figure 1. It consists of a bus and two processing subsystems, each composed of a processor, a local memory bank, and a mirrored disk unit. Both subsystems have access through the bus to a shared memory bank, which will replace the local memory in case of a failure. Each mirrored unit is in turn a Hot Spare (HSP) redundancy configuration with one spare disk. For the whole system to be functional the bus and one of the subsystems must be functional.

In our BN reliability model, continuous root nodes represent the time-to-failure of the input components of a given construct. In this example, the failure distribution for all the components is assumed to be exponential: the failure rates for the disk units, the

processors, the memory units, and the bank are: $l_D = 8.0\times10^{-5}$, $l_P = 5.0\times10^{-7}$, $l_M = 3.0\times10^{-8}$, and $l_B = 2.0\times10^{-9}$, respectively. The time-to-failure of the fault tree constructs, connected in the model by means of incoming arcs to the components' time-to-failures, are defined as deterministic functions of the corresponding input components' time-to-failure. Once the BN structure and nodes probability distributions have been defined, FT-like analysis is carried out using our new approximate algorithm for performing inference in hybrid BNs. By running the model for 40 iterations, we obtain that the reliability of the system at a mission time t = 5000 h is $R(t) = 0.014$. This compares very well to the analytical results given in [2].

To appreciate the power and novelty of our approach, it is important to note that, in our framework, no analytical calculation needs to be performed and no tables need to be populated. Once we have defined the marginal time-to failure distributions for the basic components, the CPDs for the DFT constructs are automatically estimated by modelling them as an approximate mixture of Uniform distributions. The dynamic discretisation algorithm fits a histogram composed of Uniform distributions. Any form can be used for the failure distribution of the system's components. No closed-form solution for the system failure distribution is required. Therefore, we can easily estimate the failure distribution of the above system for any (non-exponential) time-to-failure of the input components. From the estimated failure distributions of the DFT constructs, we can obtain estimates for the reliability of any subsystem for a given mission time and other metrics of interest, like MTTF and warranty periods, for which analytical expressions might not be obtained.

References

[1] Agena Ltd. 2007, http://www.AgenaRisk.com/.

[2] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks", *Reliability Engineering and System Safety* 71 (3), 2001, pp. 249–260.

[3] H. Boudali and J.B. Dugan, "A Continuous-Time Bayesian Network Reliability Modeling and Analysis framework," *IEEE Transactions on Reliability*, vol 55, 2006, pp. 86-97.

[4] J.B. Dugan, S. J. Bavuso and M.A. Boyd, "Dynamic Fault Tree models for Fault Tolerant Computer Systems", *IEEE Trans. Reliability*, vol 41, Sept. 1992, pp. 363-377.

[5] Z. Ghahramani, "Learning Dynamic Bayesian Networks", In C.L. Giles and M. Gori (eds.), *Adaptive Processing of Sequences and Data Structures. Lecture Notes in Artificial Intelligence*, Berlin: Springer-Verlag, 1998, pp. 168-197.

[6] H. Langseth and L. Portinale, "Bayesian networks in reliability", *Reliability Engineering and System Safety*. (To appear), 2006.

[7] M. Neil, M. Tailor and D. Marquez, "Inference in Bayesian Networks using dynamic discretisation". *Accepted for publication in the Journal of Statistics and Computing*, 2006.

[8] M. Neil, M. Tailor, D. Marquez, N. Fenton and P. Hearty, "Modelling Dependable Systems using Hybrid Bayesian Networks". *Reliability Engineering and System Safety*, 2007 (to appear).

[9] W.G. Schneeweiss. *The Fault Tree Method*. LiLoLe Verlag, 1999.

[10] P. Weber, L. Jouffe, "Reliability modeling with Dynamic Bayesian Networks", *5th IFAC Sysmposium on Fault Detection, Supervision and Safety of Technical Processes*, Washington, D.C., USA, 2003.

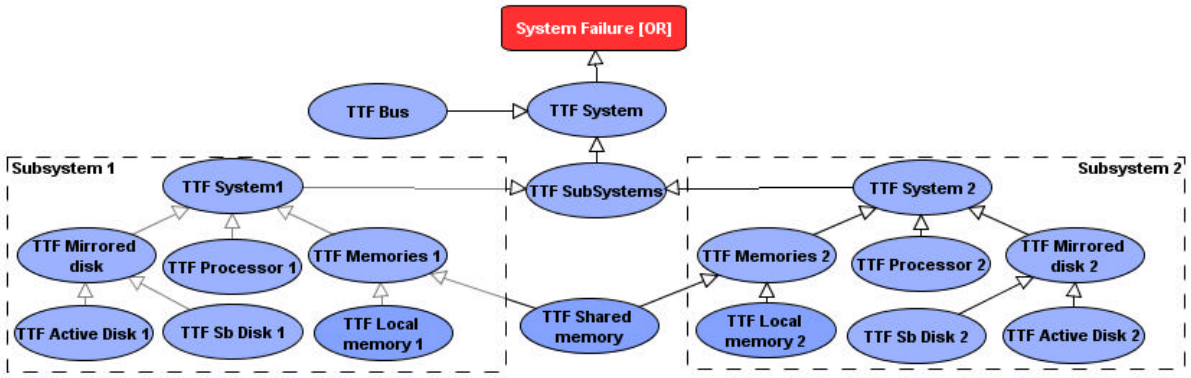

Figure 1