Assessing System Reliability Through Binary Decision Diagrams Using Bayesian Techniques

John Andrews[1], Jake Ansell[2], Pingchuan Ma[2] and Michael Phillips[3]

[1]Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, LE11 3TU, UK

[2]School of Management, University of Edinburgh, Edinburgh, EH8 9JY, UK.

[3]Department of Mathematics, University of Leicester, Leicester, LE1 7RH, UK

Abstract

Binary Decision Diagrams (BDDs) have been shown to be efficient for the numerical evaluation of the reliability of complex systems. They achieve exact results where Fault Tree Analysis could generally produce only bounds. In this paper the approach to systems evaluation using a Bayesian method in conjunction with BDDs is explored. The advantages of the approach are discussed with respect to both efficiency and the ability to deal with dependency within the system in a natural manner. As an illustration a simple pump configuration is considered which features a dependency. The results demonstrate both the flexibility of the approach and the ease of dealing with the additional complexity of dependency.

Introduction

The use of Binary Decision Diagrams (BDDs) have many advantages for the analysis of complex reliability structures over Fault Tree Analysis, see Andrews (2001) and Beeson and Andrews (2003). In section two there is a brief review of the major features of BDDs. A particular strength of using a BDD is the estimation of the failure probability of a system since BDDs provide exact calculation methods whereas in the past Fault Tree Analysis (FTA) has generally only allowed bounds. Another aspect of the BDD is its ability to explore dependency within the system such as that existing due to standby redundancy.

This paper explores the use of the BDD model in a Bayesian evaluation of the system. Whilst there are many issues to address, the main aspect will be the approach to the analysis of a system's reliability on the assumption that there already exists data on the specific component's failure times and elicited information on prior beliefs about these elements. The third section of the paper will explore the general concepts. These will include the use of BDDs to explore dependency within the system, both at a component level but also through the data.

To provide greater insight into the approach taken a simple example will be considered of a pump system with associated pressure relief valves. Obviously some will appreciate that the model chosen has resonance within safety critical systems. It will be assumed that information regarding the failure time distribution for the valves used is well established but that there is relatively little known about the pumps involved. The specific system will be described along with the data available for analysis.

The data and system structure will be then used to run a series of experiments. This will illustrate how we can use the model dynamically to provide insight into the context of the dependency. The last section will provide a summary of results and discussion of further research.

Modelling of Systems Reliability Using BDD

Fault tree analysis is frequently employed to study the performance of systems, especially safety critical systems, see Henley and Kumamoto (1981). An acyclic graph is derived to describe the relationship between a specific failure mode for the system and the constituent elements of the system. Figure 1 presents a diagram, which will be subsequently used in the example.

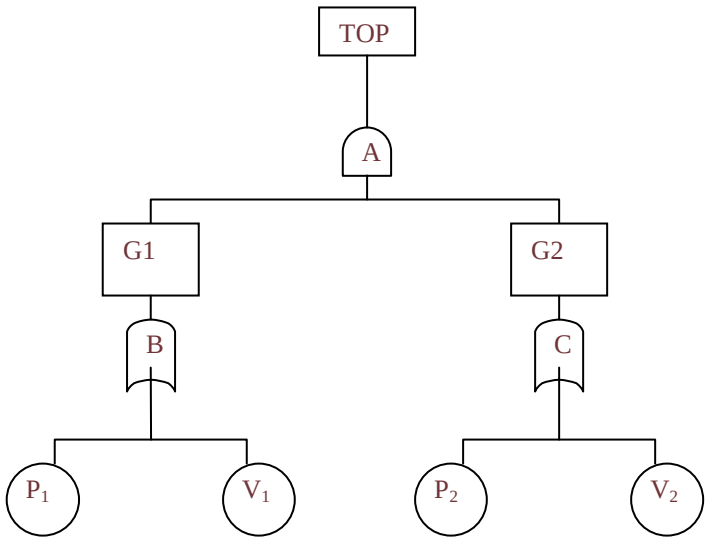

Figure 1 Fault Tree of Pump System

In Figure 1 the top event is connected to intermediate gate events, G1 and G2 by an AND gate, gate A. G1 is connected to P1 and V1 by an OR gate, gate B, and G2 is connected to P2 and V2 by an OR gate, gate C. The logic equation for the system is

$$TOP = (P1 \cup V1) \cap (P2 \cup V2) \quad (1)$$

The Binary Decision Diagram (BDD) is an alternative representation of the fault tree structure for the top event logic function. It uses Shannon's description of the system behaviour in terms of a structure function $\phi(\mathbf{x})$ where $\mathbf{x}$ represents a vector of component states. $\phi(\mathbf{x})$ takes the value 0 if system works and 1 if systems is failed, and $\mathbf{x}$ comprises component state indicator variables **xi** with the component working (0) or failed (1). The BDD represents the failure logic of the system and is usually derived by conversion from the fault tree. The basic events are put in an ordering. The BDD is based on an if-then-else, **ite**, architecture, so every basic node will be represented as X = ite(X,1,0).
For each gate with inputs J = ite(X,f1,f2) and H = ite(Y,g1,g2) then:

$$\text{If } X < Y \qquad J \oplus H = \text{ite}(X, f1 \oplus H, f2 \oplus H); \quad (2)$$

$$\text{If } X = Y \qquad J \oplus H = \text{ite}(X, f1 \oplus g1, f2 \oplus g2) \tag{3}$$

where $\oplus$ is the logic gate (AND/OR). The outcome of the conversion of the fault tree shown in Figure 1 is presented in Figure 2.

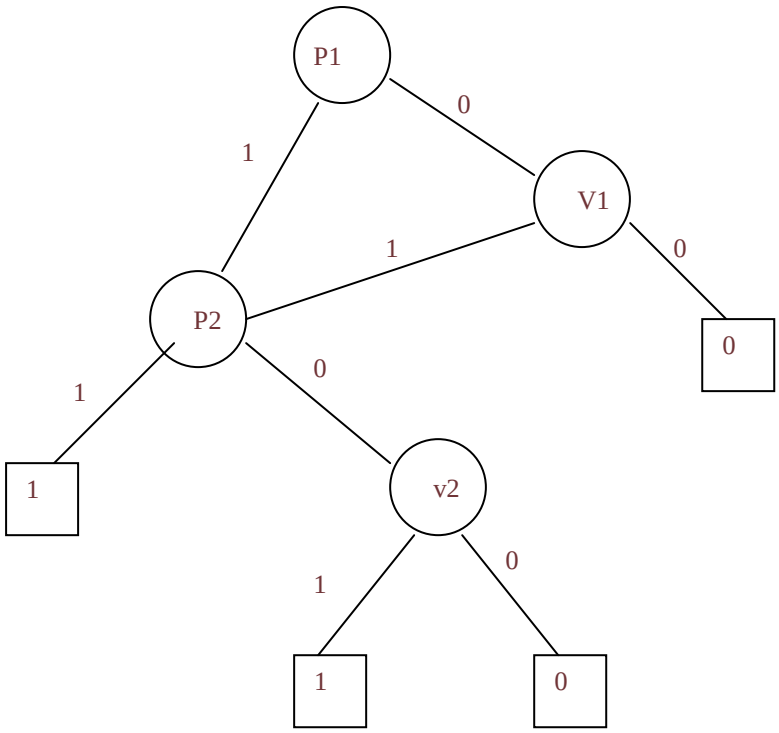

Figure 2: BDD for Fault Tree in Figure 1

Each path through the BDD from root vertex to a terminal 1 node represents a system failure mode and so represents a cut set. The set of cuts sets can be obtained by tracing each path through the BDD, which ends in a failure node. Obviously of most interest is the minimum cut set, the minimum set of component failures that will lead to the failure of the system. Rauzy (1993) produced an algorithm to derive the minimum cut sets from the BDD. For the system represented in Figures 1 and 2 the minimum cut sets are: $\{P_1,P_2\}$, $\{P_1,V_2\}$, $\{V_1,V_2\}$ and $\{V_1,P_2\}$. In conventional fault tree analysis, the minimum cut sets can be used to derive the probability of system failure given the basic event failure probabilities.

The main advantage of the BDD is however that the system failure probability can be obtained without the need to evaluate the minimal cut sets. It can be obtained directly from the disjoint paths which yield a failed system state. Each disjoint path leading to system failure considers the set of events that lead to a terminal one state and include both working and failed component conditions. Since these are disjoint the system failure probability is obtained by summing the likelihood of each disjoint path on the BDD. For the BDD shown in figure 2 the four disjoint paths are:

1	$P1.P2$
2	$P1.\overline{P2}.V2$
3	$\overline{P1}.V1.P2$
4	$\overline{P1}.V1.\overline{P2}.V2$

The system failure probability, Q_{sys} is then given by:

$$Q_{SYS} = q_{P1}q_{P2} + q_{P1}(1-q_{P2})q_{V2} + (1-q_{P1})q_{V1}.q_{V2} + (1-q_{P1})q_{V1}(1-q_{P2})q_{V2} \qquad (4)$$

For a small example such as this the system reliability expression can be checked by use of the inclusion-exclusion expansion, Henley and Kumamoto (1981).

$$Q_{sys} = \Sigma_i P(Ci) - \Sigma_{ij} P(C_i \cap C_j) + \Sigma_{ijk} P(C_i \cap C_j \cap C_k) - ...$$

where C_i for i=1, ..., n is the minimum cut sets. The form for Q_{sys} for system given earlier would be

$$Q_{sys} = P\{P_1.P_2\} + P\{P_1.V_2\} + P\{V_1.V_2\} + P\{V_1.P_2\} - P\{P_1.P_2.V_2\} - P\{P_1.P_2.V_1\} - P\{P_1.V_1.V_2\} - P\{P_2.V_1.V_2\} + P\{P_1.P_2.V_1.V_2\} \qquad (5)$$

General Concepts of Bayesian Analysis using BDDs

A brief description of the BDD was given in the previous section, in this section the aim is to discuss the use of BDDs in the context of a Bayesian Analysis. The specific goal that will be undertaken is the estimation of the reliability of the overall system based on the assumption that the model of the system is correct and that information about the components, in the form of prior beliefs about their performance and data on their performance, is available. Obviously it is possible to consider a more general problem which might be to predict the reliability of the system without assuming the model of system is correct. However, this is regarded simply as an extension of the current model considering all possible combinations of the components.

The objective of the study is to ascertain the reliability of the system given the information about the components. This can be immediately interpreted in terms of the structure function, $\phi(\mathbf{x})$, as $E_{\mathbf{X}}[\phi(\mathbf{x})]$. This means that there is a natural interpretation of the reliability in terms of the BDD.

Therefore using the BDD will provide a mechanism for evaluating the system reliability distribution. The speed of calculation offered by the BDD makes it an efficient way to assess the reliability and the methodology can be easily extended to include dependencies. Given the representation, in terms of the **ite** structure, it is rapid to implement a Bayesian methodology. The computational efficiency in using Monte Carlo Markov Chain based techniques is clear, see Gilks et al (1996).

Dependency within the system arises from structural aspects, interaction between components, and from the component failure time data used. In the case of structural

dependency, the design and operation of the system means that there are interactions between component failures, for example a piece of equipment might be in cold standby and so will only be used if other equipment fails to operate. Since the standby element will be assumed perfectly reliable whilst in backup mode it only has a non-zero failure probability if the primary component fails. Hence the dependency between the components where failure of one will influence the likelihood of failure of another component. Other causes of dependency may be the increase in strain or stress resulting from the primary failure event. This type of dependency would, of course, need modelling of the specific form of dependency and is currently outside the scope of this paper. Finally the data used for analysis can lead to dependency. Often data in reliability studies is pooled assuming homogeneity to provide better estimates of the performance. This may not be appropriate and may lead to an underestimate or an overestimate of performance.

Pumping System

The fault tree and the BDD for the pumping system were introduced in earlier sections. A little further information is required about the system, and how dependencies can exist in the system. Flow is normally through stream 1 that includes pump, P_1, and over-pressure protection valve, V_1. If either P_1 or V_1 fail, the flow is switched to stream 2 comprising of duplicate components P_2 in cold standby (cannot fail when not operational) and over-pressure valve V_2. The failure of components P_1, V_1 and V_2 are independent. The potential failure of P_2, though, only can occur if the flow is switched to stream 2, when either P_1 or V_1 have failed. Hence failure of P_2 is conditional on P_1 or V_1 failure. The system has been analysed on the basis of both independence (hot standby) and dependency (cold standby) for P_2. From equation 4 it is possible to derive the expression for Q_{sys} as

$$Q_{sys} = [q_{p2|x} + (1 - q_{p2|x})q_{v2}][1 - (1- q_{v1})(1- q_{p1})], \quad (6)$$

Where q_{p1}, q_{v1} and q_{p2} are the failure probabilities of P_1, V_1 and V_2 respectively and $q_{p2|x}$ is the failure probability of P_2 conditional on either P_1 or V_1 failing.

The focus of the analysis will be on the impact the pumps have on the overall reliability estimate and it will be assumed that sufficient is known about the valves that there is no uncertainty about the lifetime distribution. The data is obtained from water pumps at two different sites and the data are presented in Table 1.

Site	Time Between Failures (days)
1	131,9,1,33,39,23,99,36,51,350,2,28,105
2	1,6,1,1,1,2,2,2,3,1,2,4,3,1,2,3,3,2,2,4,4,5,4,3,7,1,5,4,5,6,4, 3,4,12,4,3,16,5,11,2,6,2,6,22,106,17,121,63,115,43,96

Table 1 Pump Data

It is assumed that the failure times for the pumps are given by the two-parameter Weibull distribution**.** Hence there are two parameters to estimate the scale (λ) and the shape (β). The Weibull plots of the data are presented in Figure 3. The limited amount of data available for Site 1 is possibly insufficient to judge whether the

underlying population is Weibull or not. For Site 2 it appears more likely that the data is from a Weibull distribution.

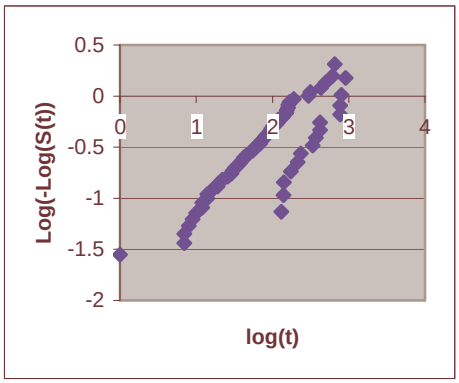

Figure 3 Weibull Plots for the two Sites

Analysis

The aim of the analysis is to demonstrate the use of the BDD to estimate the reliability of the system using a Bayesian methodology. Obviously the aim is not to carry out a full Bayesian analysis but illustrate those parts where the BDD can be used effectively in assessing the reliability. For this purpose it was decided to use gamma priors for the Weibull, since there is a requirement for the parameters to be positive. It is also the case that it was decided to use the same priors for both Sites and for the combination.

The priors selected for both λ and β are gamma $(1.0,10^{-3})$. This could be regarded as unrealistic but for the purpose of the study is adequate. It is assumed in the analysis as indicated before that the valves have the same failure time distribution, also a Weibull with $\lambda = 0.005$ and $\beta = 1.5$.

It was decided to explore the estimates achieved from each site and assuming the data from sites were homogeneous. This will show the effect of the site data on the analysis. The posterior distributions are summarised and drawn in Figures 4, 5 and 6 for Site 1 Pump, Site 2 Pump and Combined Site 1 and 2 Pump.

Using Site1 data only to estimate P1 and P2 parameters

node	mean	sd	MC error	2.5%	median	97.5%	start	sample
P1.lamda	0.07889	0.05778	5.751E-4	0.01258	0.06407	0.229	100000	100001
P1.r	0.6972	0.1515	0.001677	0.4263	0.6886	1.017	100000	100001
P2.lamda	0.07711	0.05637	5.946E-4	0.01226	0.06247	0.2233	100000	100001
P2.r	0.7017	0.1512	0.001747	0.4307	0.6938	1.021	100000	100001

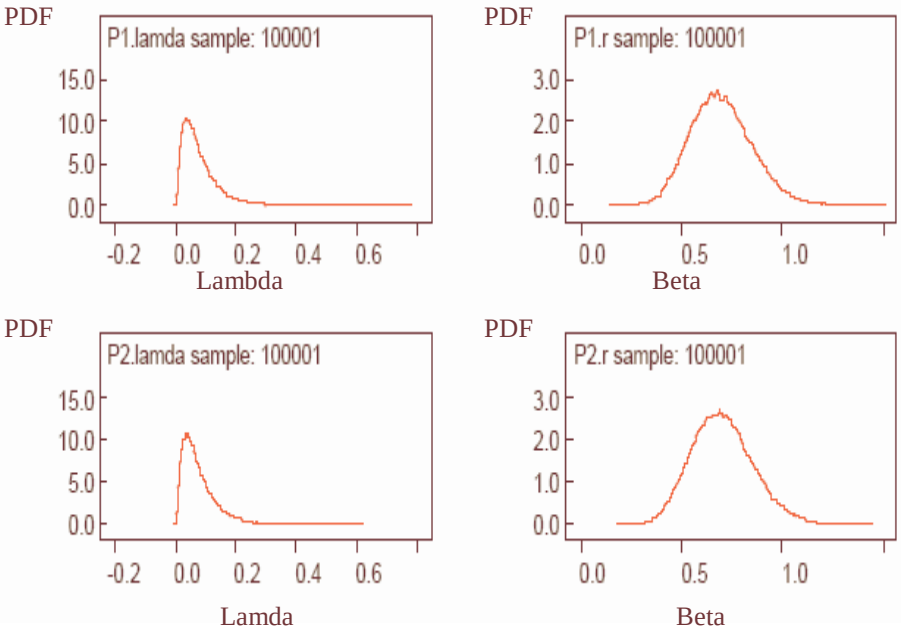

Figure 4 Analysis for Site 1

The exploration of the effect of dependency was studied by considering whether the pump, P2, was on hot or cold standby. It is assumed in this case that hot standby represents case of independence and cold standby illustrates structural dependency in the system. Figure 7 provides the graph of the mean reliabilities over 100 days. Clearly, as expected, there is an ordering of the results with the Reliability for Site 1 higher than the Combined Site reliability which is higher than the Site 2 failure probability. Also Cold standby will produce a higher mean than hot standby in this context where there is no assumption of starting difficulties.

Summary and Discussion

The objective of this paper is to illustrate the use of the BDD to estimate the reliability of systems using Bayesian methods. The approach taken shows that such an analysis can be carried out effectively for very small system examples. Obviously scaling the system up will encounter the difficulties found with any systems analysis. However the utilisation of the BDD should facilitate the scale-up to systems of greater complexity.

Using Site2 data to estimate paramerts

node	mean	sd	MC error	2.5%	median	97.5%	start	sample
P1.lamda	0.2332	0.05557	3.762E-4	0.1385	0.2284	0.3553	100001	100000
P1.r	0.6538	0.06337	4.386E-4	0.5329	0.6527	0.7812	100001	100000
P2.lamda	0.2331	0.05552	3.81E-4	0.1389	0.2282	0.3558	100001	100000
P2.r	0.654	0.0633	4.321E-4	0.5334	0.6527	0.7816	100001	100000

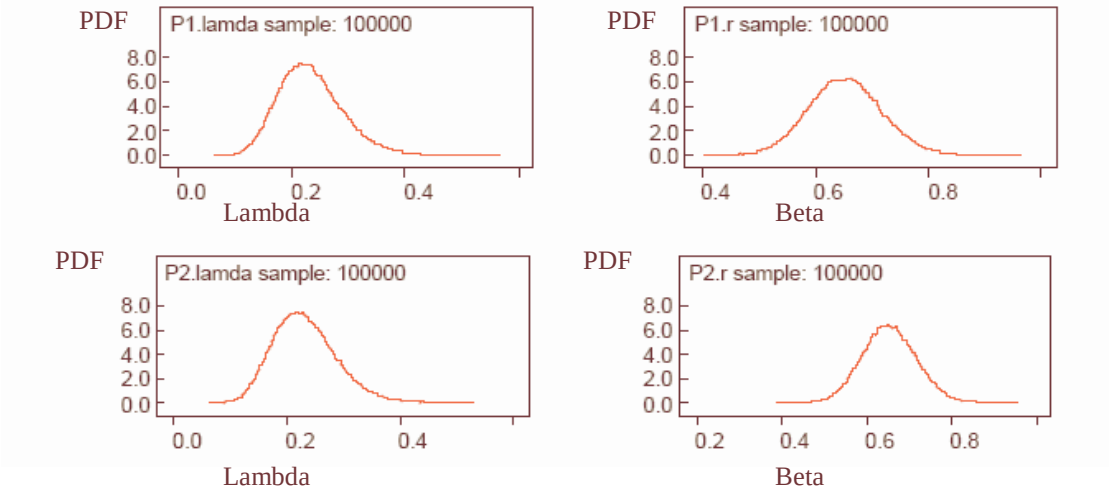

Figure 5 Analysis for Site 2

Using Site1 and Site2 data to estimated

node	mean	sd	MC error	2.5%	median	97.5%	start	sample
P1.lamda	0.1966	0.04516	3.316E-4	0.1202	0.1924	0.2961	100001	100000
P1.r	0.6021	0.05403	3.929E-4	0.4992	0.601	0.7104	100001	100000
P2.lamda	0.1968	0.04511	3.284E-4	0.1201	0.1927	0.2959	100001	100000
P2.r	0.6018	0.05413	4.003E-4	0.4981	0.6007	0.7105	100001	100000

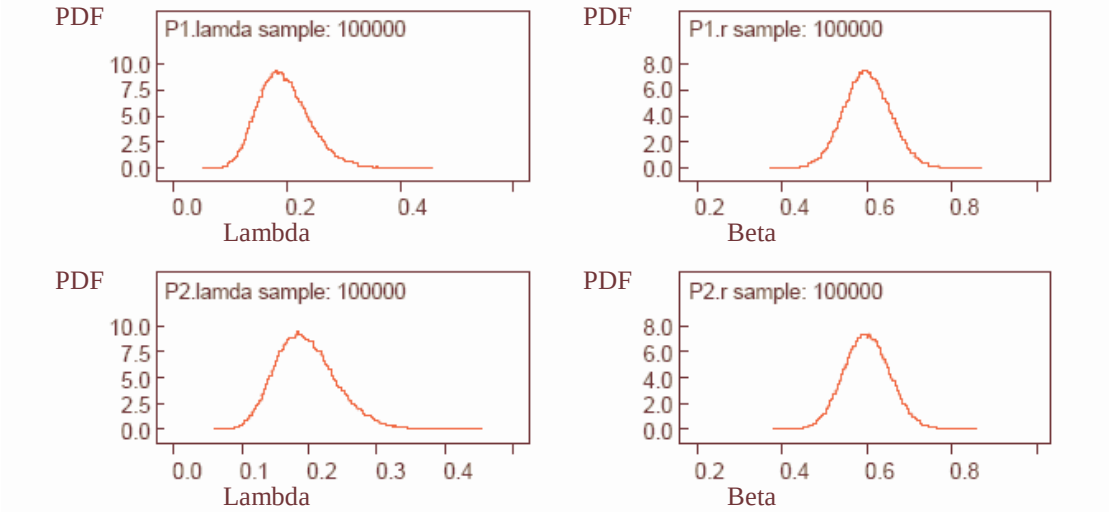

Figure 6 Analysis for Combined Site

Obviously in this paper only structural and data dependency has been considered. As stated earlier if other forms of dependency are pursued then both the form and the nature of estimation will have to be explored. It is likely, though, they could be effectively implemented using BDD approach.

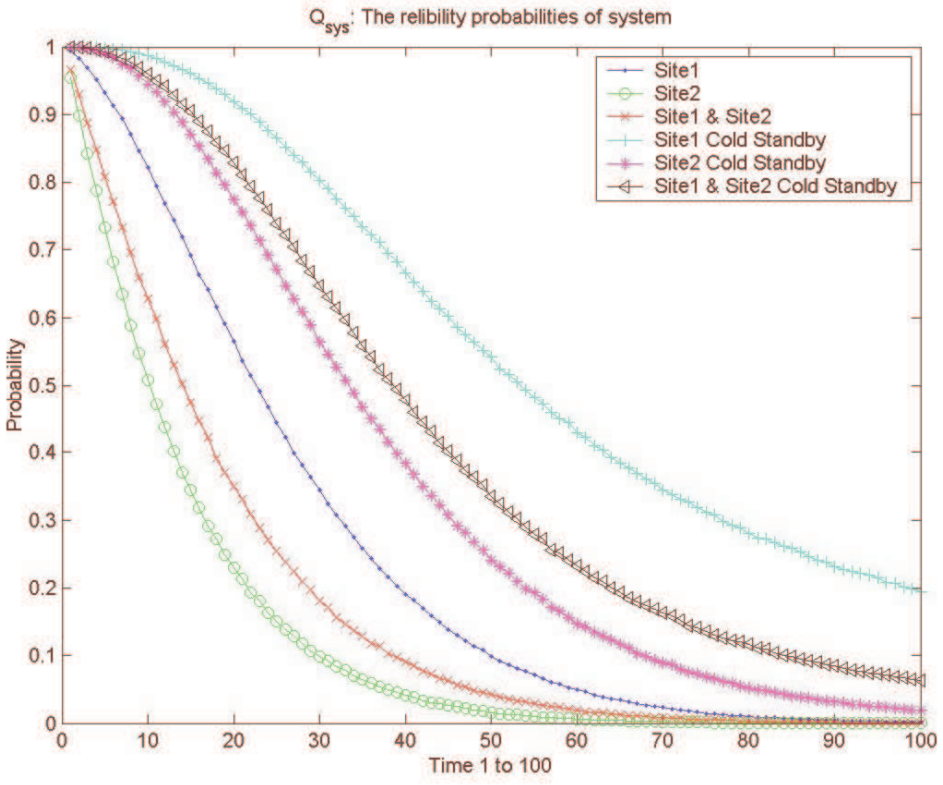

Figure 7 Mean Reliabilities over 100 days for hot and cold standby for Site 1, Site 2 and Combined Sites.

References

1. Andrews, J.D., *Quality and Reliability Eng Intern*, 17, 143-150, (2001).
2. Beeson, S., and Andrews, J.D., *IEEE Trans Reliability*, (2003).
3. Gilks, W.R., Richardson, S., and Spiegelhalter, D.J., *Markov Chain Monte Carlo in Practice*, Chapman & Hall, (1996).
4. Henley, E.J., and Kumamoto, H., *Reliability Engineering and Risk Assessment*, Prentice-Hall, (1981).
5. Rauzy, A., *Reliability Eng & Safety Sys*, **40**, 203-211, (1993).