DTU Library

Powering stochastic reliability models by discrete event simulation

Kozine, Igor; Wang, Xiaoyun

Published in:
International Conference on Statistical Models and Methods for Reliability and Survival Analysis and Their Validation

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

International Conference

On

Statistical Models and Methods for Reliability and Survival Analysis and Their Validation

4-6 July 2012, Bordeaux, France

University of Bordeaux

Mathematical Institute of Bordeaux

Powering stochastic reliability models by discrete event simulation

Igor Kozine
Department of Management Engineering
Technical University of Denmark
Kgs. Lyngby, Denmark
igko@dtu.dk

Xiaoyun Wang
Department of Mathematics and Physics
Tsinghua University
Beijing, P.R.China

***Abstract*-Markov reliability models are widely practiced tools for the analysis of repairable systems. Nevertheless, the assumptions of the Markov model may appear too restrictive to adequately model a real system and the explosion in the number of states as the size of the system increases may make it difficult to find a solution to the problem. The power of modern computers and recent developments in discrete-event simulation (DES) software enable to diminish some of the drawbacks of stochastic models. In this paper we describe the insights we have gained based on using both Markov and DES models for simple systems. By contrasting the results of the two models we illuminate their advantages and disadvantages as well as we conclude that it is a good way of model validation.**

Keywords-Markov reliability model, discrete event simulation

I. INTRODUCTION

Assessing the reliability of systems which are subject to certain inspection-repair-replacement policies is a complex task. At any instant in time the system can be in one of many possible states. The number of distinguished states depends on the number and function of the system equipment. To be able to model such a system and predict its reliability, the deterioration law of the system is usually assumed to be Markovian; that is, the future course of the system depends only on its state at present time and not on its past history. Given this assumption and that each component has approximately an exponential failure law and the reliability of it is fully restored after repair, the complete system can be described approximately by a Markov process. The models of this type are widely practiced by reliability analysts and, generally, they are regarded powerful tools in reliability, maintainability and safety engineering and commonly used to study the dependability of complex systems. The advantage of the Markov process is that it describes both the failure of an item and its subsequent repair and/or preventive maintenance and periodic testing. The Markov process can easily describe degraded states of operation, where the item has either partially failed or is in a degraded state where some functions are performed while other are not. (Markov models are extensively described in the literature, see, for example, [1])

All in all, a Markov model is a well-established and widely used method to solve stochastic event problems and is perhaps the most practiced analytical model of repairable systems and its appeal is in being able to derive reliability measures through analytical calculations. Nevertheless, as it often is, analytical solutions for complex systems are often based on assumptions the influence of which on the results may be underestimated and not well understood. For example, the Markovian property, which is the memoryless property of a stochastic process, cannot be regarded adequate in many reliability applications and should be employed consciously. Or one more point to think over: for the sake of mathematical convenience one often has to accept the governance of time between failures and repair times by exponential distributions, while available failure data may not strongly support such choice. It is clear that in this case the computed values may deviate significantly from the true probabilistic measures.

The usually stressed major drawback of the Markov method is the explosion in the number of states as the size of the system increases. The resulting diagrams for relatively complex systems are generally extremely large and complicated, difficult to construct and computationally extensive [2].

However, the rapid increase in computer power and the associated development of easy-to-use modelling tools promote the use of computer modelling and simulation as a standard tool for reliability and risk practitioner. Discrete Event Simulation (DES) models appear a competitive alternative to the conventional reliability analysis models and systems analysis methods [3]-[5]. Systems subjected to certain inspection-repair-replacement policies can also be modelled in DES environments. This way, the analyst is not confined to any specific assumptions that she is not confident to. For example, the assumptions of the Markov model can easily be discarded and a more adequate solution can be implemented. DES models give a great deal of flexibility when striving for adequate system presentation and, if properly developed, they become an effective system reliability analysis tool, in particular, for systems operated under certain inspection-repair-replacement policies.

In this paper we compare the Markov model and DES modeling approach in terms of the results they produce for different state probabilities. To do so, we have chosen a rather simple set of examples.

II. Example: Power Supply System

Consider a simple power supply system the layout of which is shown in Figure 1 [7] to see what kind of insights one can get by having a DES model. In case of normal operation all busbars are fed from the grid. If power supply from the grid fails, the main busbar and the emergency busbar are disconnected. The diesel generator starts and is switched to the emergency busbar. The following system states can be defined:

State 1: Grid is in operation (A) - Diesel generator is available (B)

State 2: Grid has failed and is under repair ($\underline{A}$) - Diesel generator is in operation (B)

State 3: Grid has failed and is under repair ($\underline{A}$) - Diesel generator has failed and is under repair ($\underline{B}$)

State 4: Grid has been restored (A) - Diesel generator is under repair ($\underline{B}$)

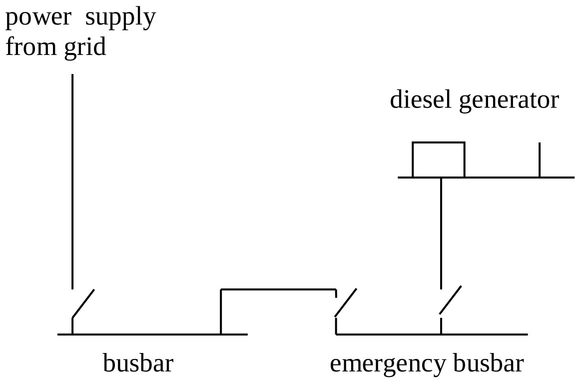

Figure 1. System layout of the power supply system

The corresponding state diagram is depicted in Figure 2. Special attention is called for the failure-to-start probability, Q_B, of the emergency diesel generator.

In state 1 both busbars are fed from the grid. The diesel generator is available but does not run. In state 2 power supply from grid is not available but the diesel generator has started and is in operation. In state 3 power supply from both the grid and the diesel generator is not available. The unavailability of the diesel generator can be a result of either a failure to start or a failure to run after a successful start. Two repair teams are at disposal to restore the subsystems concurrently in case they both fail. In state 4 power supply from the grid is restored, however the diesel generator is still under repair.

III. Markov Model of the Power Supply System

Assume that the failure and repair rates of the grid and diesel generator are constant, so the transition rates between the different systems states are homogeneous, which means that the failure process as well as the repair process is exponentially distributed. Then by constructing a transition matrix, we can get for each state steady-state solutions which are attained after having the system run for a long enough period of time.

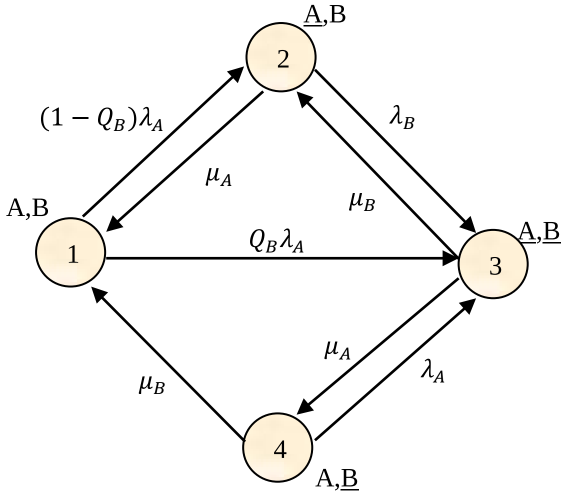

Figure 2. State diagram of the power supply system

Let λ_A and λ_B be the failure rates for the grid and diesel generator, respectively, while μ_A and μ_B be their repair rates. The probability of failure to start the diesel generator is denoted by Q_B. The transitions from state to state are shown in Figure 2, from which we can construct the transition matrix of the system and write Kolmogorov equations for computing the state probabilities P_1, P_2, P_3, and P_4:

$$\begin{bmatrix} \frac{dP_1}{dt} \\ \frac{dP_2}{dt} \\ \frac{dP_3}{dt} \\ \frac{dP_4}{dt} \end{bmatrix} = \begin{bmatrix} -Q_B\lambda_A-(1-Q_B)\lambda_A & \mu_A & 0 & \mu_B \\ (1-Q_B)\lambda_A & -\lambda_B-\mu_A & \mu_B & 0 \\ Q_B\lambda_A & \lambda_B & -\mu_A-\mu_B & \lambda_A \\ 0 & 0 & \mu_A & -\lambda_A-\mu_B \end{bmatrix} \cdot \begin{bmatrix} P_1 \\ P_2 \\ P_3 \\ P_4 \end{bmatrix}$$

It must also hold that

$$P_1+P_2+P_3+P_4=1.$$

For the steady-states, all derivatives $\frac{dP_i}{dt}$ are equalized to zero and, by doing this, the above system of equations becomes the system of algebraic equations that are rather easy to solve. With the help of MATLAB the following formulas were derived:

$$P_1 = \frac{\mu_A{\mu_B}^2 + {\mu_A}^2\mu_B + \lambda_A\mu_A\mu_B + \lambda_B\mu_A\mu_B}{A+B}, \qquad (1)$$

$$P_2 = \frac{\lambda_A{\mu_B}^2 + {\lambda_A}^2\mu_B + \lambda_A\mu_A\mu_B - \lambda_A\mu_A\mu_B Q_B}{A+B}, \qquad (2)$$

$$P_3 = \frac{{\lambda_A}^2\lambda_B + \lambda_A\lambda_B\mu_B + {\lambda_A}^2\mu_A Q_B + \lambda_A\mu_A\mu_B Q_B}{A+B}, \qquad (3)$$

$$P_4 = \frac{\lambda_A Q_B {\mu_A}^2 + \lambda_A \lambda_B \mu_A}{A + B} \quad (4)$$

where

$$A = Q_B {\lambda_A}^2 \mu_A + {\lambda_A}^2 \mu_B + \lambda_B {\lambda_A}^2 + Q_B \lambda_A {\mu_A}^2 + 2\lambda_A \mu_A \mu_B$$

$$B = \lambda_B \lambda_A \mu_A + \lambda_A {\mu_B}^2 + \lambda_B \lambda_A \mu_B + {\mu_A}^2 \mu_B + \mu_A {\mu_B}^2 + \lambda_B \mu_A \mu_B$$

It should be noted that formula (3) is different from that given in [7], as we did not neglect any terms, while the other formulas for state probabilities P_2, P_3, and P_4 were not provided at all in any form in [7].

IV. DES MODEL OF THE POWER SUPPLY

The appeal of models developed in a DES environment is that their logic follows the natural way the modelled system behaves. For example, the model of the power supply system works as follows. (See the logic of the model on the diagram given in Figure 3. This figure is a screen shot of the model buiolt in Arena.)

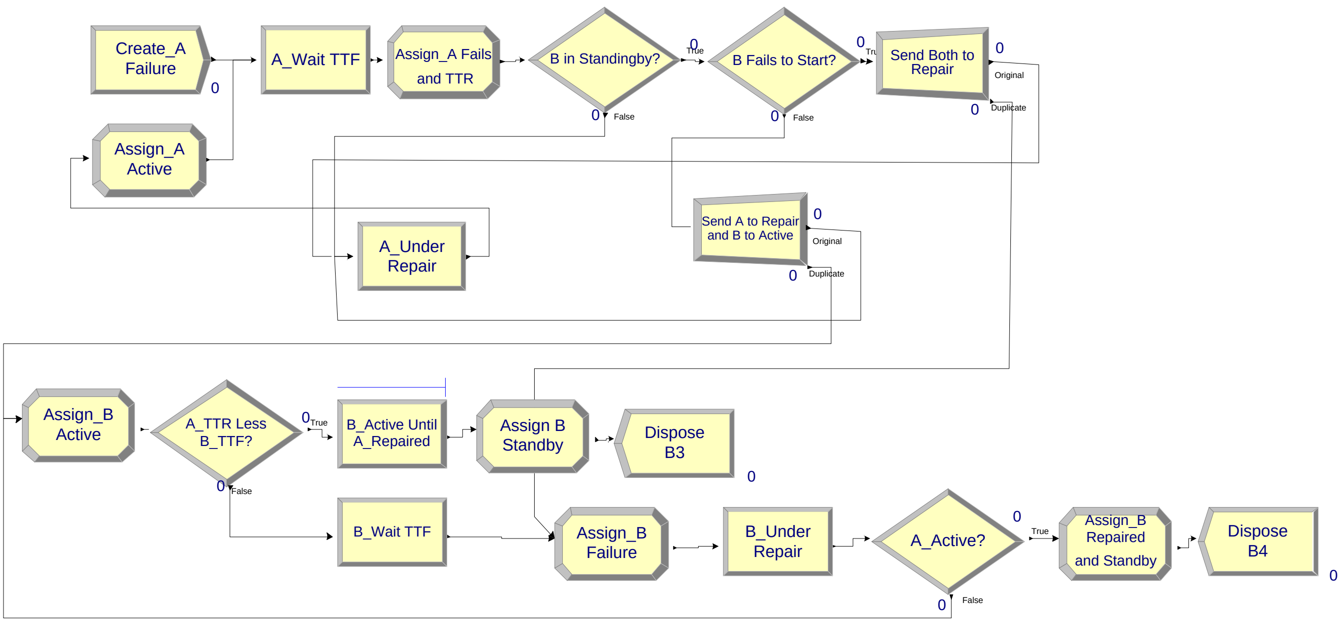

Figure 3. The diagram of the DES model of the power supply system as it appears in the Arena model window

At the instatnt of start running the model an entity is created in the "Create_A Failure" modul and sent further to the model. In the following modul, a time to failure governed by a specified probability distribution is generated and the entity is held in the "A_Wait TTF" modul for the the generated time. Then it moves to the Assign module, where the state of A is changed from "active" to "failure" and time to repair is generated according to a predefined probability distribution. Next, in the IF module it is checked whether the diesel generator, B, is in standby. If it is, then in the following IF module it is verified whether B fails to start. If it is, then from the following Separate module two entities are sent to the corresponding modules mimicking the repair of A and B. This is done in the modules "A_Under Repair" and "B_Under Repair" that simply delay the move of the entities for the specified times to repair of the both subsystems. The reader can further follow the logic and behaviour of the model on the diagram Figure 3. The model is run for a predefined period of time mimicking the system operation for thouzands of years. While the model is running, the times spent in the different states are accumulated and when the model run ends, the accumulated times are divided by the simulation time providing the state probabilities as an output.

The DES model of the power supply system was validated by comparing the values of the state probabilities obtained by simulation with those computed by formulas (1) – (4). A very high precision agreement was observed for the simulated and computed results. In this way, confidence to formulas (1) – (4) becomes higher as well. The two-way validation can be of utmost importance for the reliability analyst even for a simple system like that shown in Figure 2.

For example, let us take state probability P_3 as it is given in [7]:

$$P_3 \approx \frac{\lambda_A \times \lambda_B + \lambda_A \times \mu_A \times Q_B}{\mu_A(\mu_A + \mu_B)} \quad (5)$$

It may be not straightforward and easy to come to the conclusion that formula (5) is an approximation of (3). As well as it may be not obvious that (3) is correct. By running the simulation model exemplified in Figure 3 and comparing the results with those analytically computed the confidence to the both becomes definitely higher.

Another important point in support to mutual benefit for both Markov and DES model is a sensitivity or robustness analysis that can be rather easily conducted by DES. As soon as a DES model has been validated, one can drop the assumption of exponentially distributed time between failures and time to repair. The results obtained based on other distribution laws can be easily generated and by doing this the sensitivity of the model to the change of distributions can be numerically analysed.

Collecting representative samples of failure observations is a real problem reliability analysts face. The assessment of mean times between failures (MTBFs) and the variances based on a limited number of observations can rarely support the definitive conclusion that the times are exponentially distributed. Nonetheless, not having another tool except for the Markov model, the analyst is compelled to use the exponential distributions. How differently the results would be if TBFs were governed by other alternative distributions? Answering this question is often a requirement of reliability and risk analyses.

Besides the exponential distribution we have chosen three other (Rayleigh, log-normal and truncated normal) to see how the modeling results are sensitive to the change of the distribution. The parameters of the probability distributions were calculated based on a chosen fixed MTBFs and mean time to repair (MTTR). Surprisingly, the results of this exercise have demonstrated good model robustness.The highest spread in probability was for state 4. Although, even for a rather unrealistic ratio between MTBF and MTTR for the grid and generator (20 time units for MTBF: 1 time unit for MTTR) the range was not noticeably broad. More realistic ratios like 100:1 or 200:1 show more narrow uncertainty intervals for the state probabilities. A plot of the outputted results for the worst modeled case is presented in Figure 4. The differences in the probability are observed only in the third decimal.

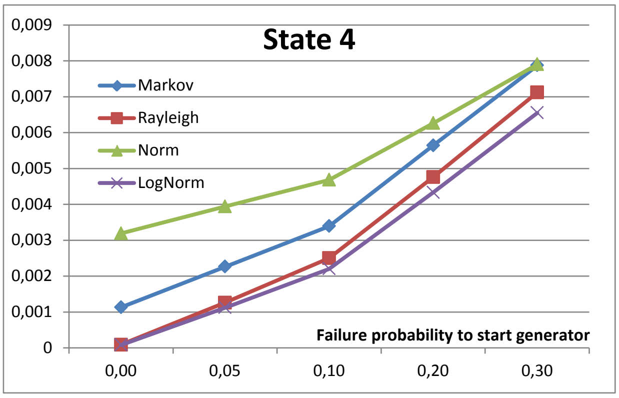

Figure 4. The probability of residing in State 4 obtained by simulation for the ration between MTBF and MTTR as 20:1

V. DES IN DEFENSE OF MARKOV MODEL

In this section we provide an example of fallacious in our opinion statements about some flaws of Markov models. To check the validity of the seemingly unquestionable statements, we computed the state probabilities by both the analytical approach and DES. By comparing the results, the conclusion was made in support to adequate modelling by the Markov process.

In [8] Markov models of multi-disk fault tolerant systems are briefly discussed. It is stated that the accuracy of Markov models and their utility decreases as the redundancy in the system increases. “For multi-disk fault tolerant systems, both rebuild models, the serial and concurrent (Figure 5), are incorrect. The rebuild transitions for states 2 through m are incorrect: they model the rebuild of the disk that failed most recently, whereas reliability is dominated by the rebuild of the disk that failed earliest. In essence, traditional Markov models reset the rebuild time for all disks being rebuilt whenever another disk fails. The traditional serial rebuild Markov model thus models a rebuild policy in which each subsequent disk failure changes which disk is being rebuilt, and “re-fails” the disk currently being rebuilt. The traditional concurrent rebuild Markov model thus models a rebuild policy in which each subsequent disk failure restarts the rebuild of all failed disks.” These assertions appeared to us logical until DES modeling proven their invalidity.

We have modelled a system consisting of five disks running in parallel and assumed that the system is operational until all five disks fail. Failure and repair rates were taken the same for the all disks. The both rebuild policies were subject to the modeling by the both methods.

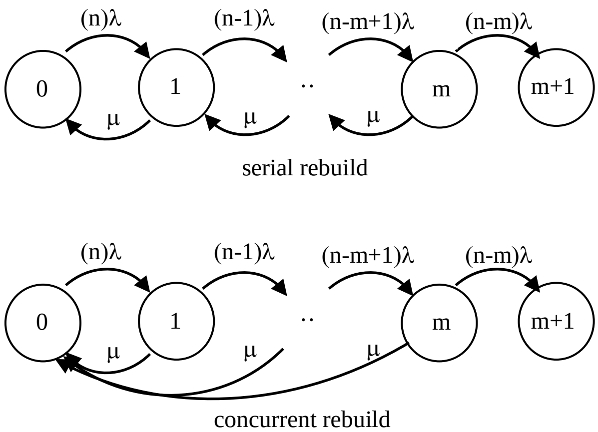

Figure 5. Traditional Markov models for rebuild policies

The analytical solutions for the state probabilities are given by the following formulas (see for example [9])

$$p_k = p_0 \prod_{i=1}^{k} \frac{\lambda_i}{\mu_i}, \quad p_0 = \frac{1}{1 + \sum_{k=1}^{n} \prod_{i=1}^{k} \frac{\lambda_i}{\mu_i}} \qquad (6)$$

The logics of the DES models are very simple. Figure 6 exemplifies the one for the concurrent rebuild policy.

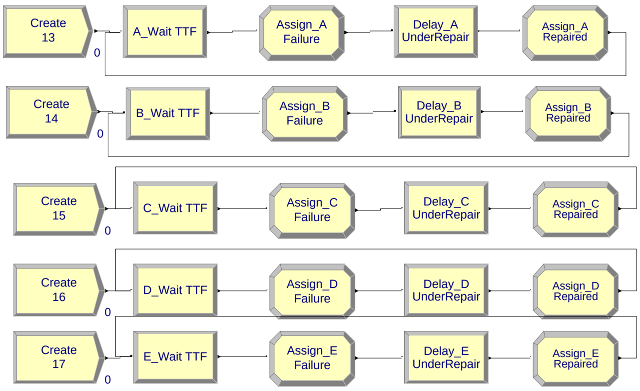

Figure 6. The outlook of the DES model made in Arena for the concurrent rebuild policy

The computed probabilities (6) of being in each of the six states and the results of the simulation have demonstrated very high agreement for all states. The expectation of having conservative reliability measures has not been supported by the modelling results.

VI. An Example of Explicit Advantage of DES

As stated in the introduction, the usually stressed major drawback of the Markov method is the explosion in the number of states as the size of the system increases. In fact, this drawback can be observed even for very simple systems like the ones depicted in Figure 5 with the only difference that each component (disk) has a distinctive failure rate. If this is the case, we have to enumerate all possible combinations of the components' failure each of which will represent a distinctive state. For a system of five components, the number of states will amount to 2^5 with numerous transition intersections on a state diagram. Assuming on top of that different repair rates for the all components results in a non-overviewable state diagram and a very-difficult-to-solve problem.

On contrary, the complexity of the DES model does not change at all when assigning different values to MTBFs and MTTRs, which enables to conduct nuanced analyses of the system

VII. Conclusion

The continuing increase of computer power and growing functionality of software tools supporting mathematical and reliability computations change the way the analysts tackle the problems they face. Analytical reliability models have undisputable advantages over numerical computations given they adequately count for important features of the system. Numerical models, including advanced Monte-Carlo simulation, can in turn be easily detached from restrictive assumptions of the analytical models, which gives the analyst a greater flexibility in building adequate models. In some cases, the two modeling approaches can be used to complement and validate each other.

Our experience in applying DES models shows one more their positive feature. As they simply mimic the behavior of the systems in time, they are easily understandable by domain experts that are not experienced in abstract mathematical modeling. This way the domain experts become collaborators in model development and contribute to model validation and greater confidence to the outputted results. That is to say, a frequently existing gap between the "black boxes" of complex mathematical models and a lack of confidence to them from the practitioners' side can be bridged by employing the alternative modeling approach.

The advantageous use of the DES models compared to Markov models has been stressed in the medical domain. As stated in [6], the DES model predicts the course of the HIV disease naturally, with few restrictions. This may give the model superior face validity with decision makers. Furthermore, this model automatically provides a probabilistic sensitivity analysis, which is cumbersome to perform with a Markov model. DES models allow inclusion of more variables without aggregation, which may improve model precision. The capacity of DES for additional data capture helps explain why this model consistently predicts better survival and thus greater savings than the Markov model. The DES model is better than the Markov model in isolating long-term implications of small but important differences in crucial input data.

A shortcoming of the use of DES consists in dependence on a specific simulation environment (software) in which the model is built and run. High costs of DES software and inability to run DES models in other environments, except for the one where they have been built, are the limitations against the analytical results obtained on Markov modelling.

References

[1] N.J. McCornick, Reliability and risk analysis. Academic Press, 1981.

[2] K.S. Trivedi and D. Selvamuthu, "Markov Modelling in Reliability" in Encyclopedia of Quantitative Risk Analysis and Assessment, vol. 3, E.L. Melnick and B.S. Everitt, Eds. Wiley, 2088, pp. 1045-1049.

[3] I. Kozine, F. Markert, and A. Alapetite; Discrete event simulation in support to hydrogen supply reliability, Paper 159, International Conference on Hydrogen Safety ICHS-3, Ajaccio, Corsica, France; September, 17th 2009

[4] I. Kozine, Discrete event simulation versus conventional system reliability analysis approaches, Reliability, Risk and Safety (2010), Eds. Ale, Papazoglou & Zio, Taylor & Francis Group London, ISBN 978-0-415-60427-7.

[5] I. Kozine, Simulation of human performance in time-pressured scenarios, Proc. IMechE Vol.221 Part O: J. Risk and Reliability (2007) 141-151

[6] K. N. Simpson, A. Strassburger, W.J. Jones, B. Dietz and R. Rajagopalan, Comparison of Markov Model and Discrete-Event Simulation Techniques for HIV. Pharmacoeconomics 27 (2), 2099, pp. 159-165.

[7] Shuller, J.C.H., et al. Methods for determining and processing probabilities. ‘Red Book’. Second edition. CPR 12E. VROM. The Hague, 1997

[8] K. Greenan and J. J.Wylie. Reliability Markov models are becoming unreliable (WIP submission). http://www.usenix.org/events/fast08/wips_posters/greenan-wip.pdf

[9] J. L. Hafner and K. Rao. Notes on reliability models for non-MDS erasure codes. Technical Report RJ– 10391, IBM, October 2006.