БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ . BULGARIAN ACADEMY OF SCIENCES

ПРОБЛЕМИ НА ТЕХНИЧЕСКАТА КИБЕРНЕТИКА И РОБОТИКАТА, 52
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS, 52

София . 2001 . Sofia

Application of Simple Approximate System Availability Analysis Tools

Bogomil Manchev, Boyka Nenkova***

**Risk Engineering Ltd., 34 Totleben Bulvd., 1606 Sofia, e-mail: bmanchev@bgnet.bg*
***Institute of Information Technologies – BAS, "Acad. G.Bonchev" Bl. 29a, 1113 Sofia*

1. Introduction

Markov models are the most frequently used tools for analyzing the reliability and availability of complex high reliable systems. The large number of components and possible system states often make detailed models of such systems large and unwieldy to the extent that they are understandable only by their developers or other experts after careful study, and frequently require special software to be solved. Fortunately, a set of simpler, "approximate", but nevertheless highly accurate models can be used for such systems.

The methods described in this report provide a set of simple, easily understood "approximate" models that are applicable to a large class of system architectures. A necessary requirement for their application is the systems to be repairable and the mean time to repair to be much smaller than the mean time to failure, a case most often met in the real practice.

Results of the "approximate" model application on a technological system of Kozloduy NPP are presented in this paper.

For comparison, values, calculated using other methods are also presented. The results obtained can be compared quite favorably.

2. Theoretical background

2.1. System model

The system model assumes that the system is a series combination of redundant subsystems. Individual units in the subsystem may fail, be repaired and returned to service without the subsystem failing. However, if too many units fail at the same time, the subsystem fails and the system fails. The number of units that can fail without the subsystem failing determines the subsystem structure [1].

The approximation model of the system is developed by constructing a Markov model of each redundant subsystem and finding its Mean Time To Failure (MTTF).

The state transition diagram for a 3-state Markov model of a redundant system with repair is shown on Fig 1. Let us assume that the units are identical with constant failure rateλ. When a unit fails it is repaired at a constant rate m. If more than one unit has failed the system fails. State S_2 is the state with all units working. We assume that S_2 is the initial state of the system. State S_1 is the state with one unit failed. This state does not distinguish which unit has failed since the system behavior is the same in all cases. State S_0 is the system failed state – it is entered if more than one unit has failed at the same time.

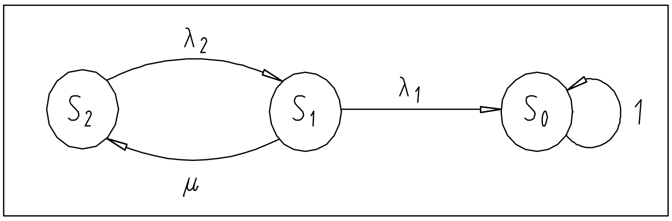


Fig. 1. 3-state Markov model of a parallel system with repair

With appropriate choices of the transition rates, the model in Fig. 1 can represent many system architectures. For the 2-unit parallel system both units are active and $\lambda_2 = 2\lambda$; for a standby system only one unit is active and we assume the standby unit does not fail, hence $\lambda_2 = \lambda$; $\lambda_1 = \lambda$ for both cases. A Triple Modular Redundant (TMR) system has three units and $\lambda_2 = 3\lambda$, $\lambda_1 = 2\lambda$. More generally, an $(n-1)$-out-of n system can be described by letting $\lambda_2 = n\lambda$ and $\lambda_1 = (n-1)\lambda$.

From this model it is not difficult to find an expression for the system reliability.

The result is:

(1) $$R(t) = 1 - P_0(t) = \frac{r_2}{r_2 - r_1} e^{-r_1 t} - \frac{r_1}{r_2 - r_1} e^{-r_2 t},$$

where

$$r_1,\ r_2 = \frac{(\lambda_1 + \lambda_2 + \mu) \pm \sqrt{\rho((\lambda_1 + \lambda_2 + \mu)^2 - 4\lambda_1\lambda_2}}{2}.$$

Integrating (1) from 0 to ∞ gives the subsystem MTTF:

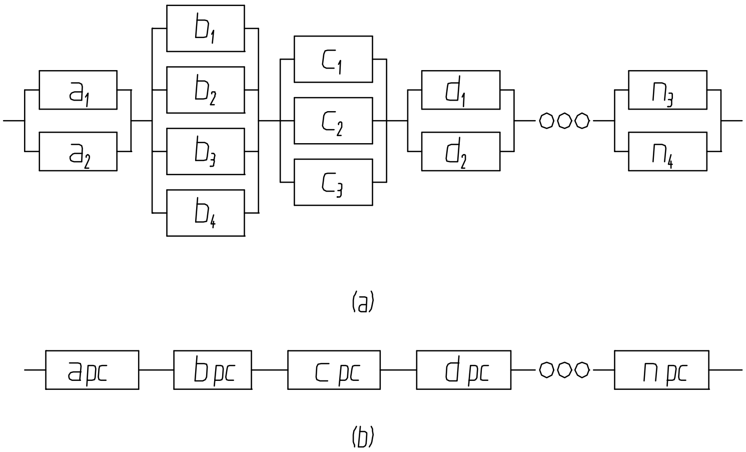
(2) $$M = 1/\lambda + \mu/(\lambda_1\lambda_2) + 1/\lambda_2 .$$

For $\mu >> \lambda_1, \lambda_2$, (i.e., MTTR<<MTTF), $M \approx \mu / \lambda_1 \lambda_2$, and

$$R(t) \approx \exp\left(-\frac{\lambda_1\lambda_2}{\mu} t\right).$$

This suggests approximating the reliability of the parallel subsystem by a pseudo-component having a constant failure rate $1/M$, and a reliability $R'(t) = \exp(-t/M)$, where M is the pseudo component MTTF. Using M from equation (2) gives the expressions in Table 1, and $M = m/\lambda_1\lambda_2$ gives those in Table 2, below.

Then the subsystem is replaced by a pseudo-component having a constant failure rate λ' equal to the inverse of the subsystem MTTF. The next step is to model the system as a series combination of these pseudo-components and its failure rate is the sum of the failure rates of the pseudo-components (Fig. 2a and 2b).



(a)

(b)

Fig.2. Reliability model of a redundant system (a) and its pseudo-component “approximation” (b)

Fig. 2a shows an example of a system consisting of redundant subsystems. In common case, for obtaining of necessary reliability it is possible for different subsystems different number of elements to be included in parallel. Fig. 2b shows the system model in Fig. 2a with each subsystem collapsed into a pseudo-component (designated by “pc”) [2, 3].

2.2. Approximation Formulas

Formulas for calculating the MTTF for various types of redundant subsystem are given in Table 1.

Table 1. MTTF and failure rate for pseudo-components representing a parallel subsystem, $m/\lambda>10$

System structure	BASIC APPROXIMATION*		WITH COVERAGE*		Relative error
	MTTF	λ’	MTTF	λ’	
2-unit standby $\lambda_1=\lambda$, $\lambda_2=\lambda$	$\frac{2}{\lambda}+\frac{\mu}{\lambda^2}$	$\frac{\lambda^2}{2\lambda+\mu}$	$\frac{\lambda+c\lambda+\mu}{\lambda^2+\lambda\mu(1-c)}$	$\frac{\lambda^2+\lambda\mu(1-c)}{\lambda+c\lambda+\mu}$	$\left(\frac{\lambda}{\mu}\right)^2$
2-unit parallel $\lambda_1=2\lambda$, $\lambda_2=\lambda$	$\frac{3}{2\lambda}+\frac{\mu}{2\lambda^2}$	$\frac{2\lambda^2}{3\lambda+\mu}$	$\frac{2c\lambda+\lambda+\mu}{2\lambda^2+2\lambda\mu(1-c)}$	$\frac{2\lambda^2+2\lambda\mu(1-c)}{2c\lambda+\lambda+\mu}$	$2\left(\frac{\lambda}{\mu}\right)^2$
3-unit TMR $\lambda_1=3\lambda$, $\lambda_2=2\lambda$	$\frac{5}{6\lambda}+\frac{\mu}{6\lambda^2}$	$\frac{6\lambda^2}{5\lambda+\mu}$	$\frac{3c\lambda+2\lambda+\mu}{6\lambda^2+3\lambda\mu(1-c)}$	$\frac{6\lambda^2+3\lambda\mu(1-c)}{3c\lambda+2\lambda+\mu}$	$6\left(\frac{\lambda}{\mu}\right)^2$
n-unit (n-1) -out-of-n:G $\lambda_1=n\lambda$, $\lambda_2=(n-1)\lambda$	$\frac{2n-1}{n(n-1)\lambda}+\frac{\mu}{n(n-1)\lambda^2}$	$\frac{n(n-1)\lambda^2}{(2n-1)\lambda+\mu}$	$\frac{cn\lambda+(n-1)\lambda^2+\mu}{n(n-1)\lambda^2+n\lambda\mu(1-c)}$	$\frac{n(n-1)\lambda^2+n\lambda\mu(1-c)}{cn\lambda+(n-1)\lambda+\mu}$	$n(n-1)\left(\frac{\lambda}{\mu}\right)^2$
n-unit k-out-of n:	See algorithm (3)				

The formulas given are for the most common types of subsystems used in commercial, transaction processing, computer and other kind of high reliable systems. In the formulas, λ is the unit failure rate and m is its repair rate. Columns 2 and 3 give the basic system formulas and columns 4 and 5 include a factor, *c*. This factor gives the probability that the unit failure is detected and the system survives the failure. The last column in Table 1 gives an expression for the maximum relative error in the approximation.

The formulas in Table 1 are quite accurate provided the unit MTTF and unit Mean Time to Repair (MTTR) have the ratio MTTF/ MTTR > 10. In case the ratio MTTF/ MTTR > 100, the simpler, but less accurate, approximations in Table 2 can be used.

For the general *k*-out-of *n* case (the subsystem is good if at least *k* out of *n* redundant units are working), a simple closed form expression does not exist for the subsystem MTTF but it can be calculated iteratively using expression (3):

$$M_1 = \begin{cases} 1/\lambda_r + (\mu_r/\lambda + 1)\, M_{r+1} & \text{for } r = 1,\ \dots,\ n-1,\ \dots,\ k \\ 1/\lambda_n & \text{for } r = n. \end{cases} \tag{3}$$

Table 2. Simplified expressions for MTTF and failure rates for pseudo component representing a parallel subsystem, μλ>100

System structure	BASIC APPROXIMATION*		WITH COVERAGE*	
	MTTF	λ′	MTTF	λ′
2-unit standby $\lambda_1=\lambda$, $\lambda_2=\lambda$	$\frac{\mu}{\lambda^2}$	$\frac{\lambda^2}{\mu}$	$\frac{\mu}{\lambda^2+\lambda\mu(1-c)}$	$\frac{\lambda^2}{\mu}+\lambda(1-c)$
2-unit parallel $\lambda_1=2\lambda$, $\lambda_2=\lambda$	$\frac{\mu}{2\lambda^2}$	$\frac{2\lambda^2}{\mu}$	$\frac{\mu}{2\lambda^2+2\lambda\mu(1-c)}$	$\frac{2\lambda^2}{\mu}+2\lambda(1-c)$
3-unit TMR $\lambda_1=3\lambda$, $\lambda_2=2\lambda$	$\frac{\mu}{6\lambda^2}$	$\frac{6\lambda}{\mu}$	$\frac{\mu}{6\lambda^2+3\lambda\mu(1-c)}$	$\frac{6\lambda^2}{\mu}+3\lambda(1-c)$
n-unit (*n*–1)-out-of-*n:G* $\lambda_1=n\lambda$, $\lambda_2=(n-1)\lambda$	$\frac{\mu}{n(n-1)\lambda^2}$	$\frac{n(n-1)\lambda^2}{\mu}$	$\frac{\mu}{n(n-1)\lambda^2+n\lambda\mu(1-c)}$	$\frac{n(n-1)\lambda^2}{\mu}+n\lambda(1-c)$
n-unit *k*-out-of-*n:G* $\lambda_1=i\lambda$,	$\frac{(k-1)!}{n!}\frac{1}{\lambda}\left[\frac{\mu}{\lambda}\right]^{n-k}$	$\frac{n!}{(k-1)}\lambda\left[\frac{\lambda}{\mu}\right]^{n-k}$		

* λ = unit failure rate, *c*=coverage factor.

The algorithm in equation (3), for the *k*-out-of-*n* system is derived by applying the approximation (2) iteratively to first the (*n*–1)-out-of-*n*, then the remaining the (*n*–2)-out-of-(*n*–1) system, etc. until the (*k*–1)-out-of-*k* system is reached. Note that this assumes that a repair operation restores the system to the fully working state regardless of how many units have failed (Fig. 3).

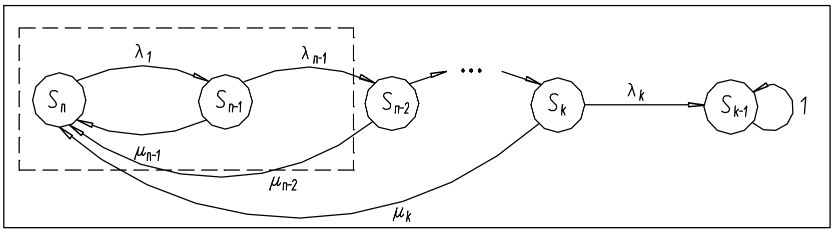


Fig. 3. Markov model of a *k*-out-of-*n*: system with bulk repairs

2.3. System and Subsystem Availability

When a redundant subsystem fails the entire system fails. Thus, there is an incentive to make the necessary repairs quicker than when making repairs to a single failed unit, which has not caused the entire system to fail. On the other hand, for the system considered here, a subsystem fails only when more than one of the redundant units has failed; thus more extensive repairs may be needed. Consequently, when a redundant subsystem fails, the repair rate will generally be different from the repair rate for an individual unit of the subsystem that is repaired while the subsystem remains operational. Let μ_{ss} denote this repair rate. Representing the subsystem as a pseudo component having the constant failure rate $\lambda'=1/\text{MTTF}$, the subsystem availability, $A(t)$, and its steady state availability, A, can be found by:

$$A(t) = \frac{\mu_{ss}}{\lambda'+\mu_{ss}} + \frac{\lambda'}{\lambda'+\mu_{ss}} e^{-(\lambda'+\mu_{ss})\,t}, \tag{4}$$

$$A(t) = \frac{\mu_{ss}}{\lambda'+\mu_{ss}}.$$

The overall system availability can be calculated as the product of the system availabilities obtained from the equations above given.

2.4. Error in the approximation

To use any approximation, it is important to have a good understanding of the error it introduces. The error in the subsystem approximation is defined as the relative error:

$$E(t) = \frac{R(t)-R'(t)}{R(t)} = 1 - \frac{R'(t)}{R(t)}, \tag{5}$$

where $R(t)$ is the true subsystem reliability at time t and $R'(t)$ is the pseudo-component reliability, ($R'(t)=\exp(\lambda' t)$). We note that since $R(t)\leq 1$, the relative error is always greater than or equal to the difference, $E(t) \geq R(t) - R'(t)$.

The error obtained by using the expressions given in the last column of Table 1 is generally on the order of the square of the ratio MTTR/MTTF. For most applications the formulas are sufficiently accurate for MTTF/MTTR>10. For many high reliable systems values of $1/\lambda$ often are greater than 10 000 hours and $1/\mu$ is often less than 50 hours. Hence, ratios $\mu/\lambda > 200$ are common and both approximations have very small errors. In some high reliable systems ratios of μ/λ may exceed 10 000.

For such systems the errors in both approximations are negligible. It is very important to note that without repair, the approximations given are not valid and the approach of replacing a parallel subsystem with a pseudo-component having a constant failure rate gives a very poor approximation. The errors obtained using the approximations in Table 2 are quite accurate for time periods of less than 5 times the unit MTTF. Thus, they are often good enough for practical work.

3. Example

As an example let us consider containment spray system –*TQn*1 [11, 21, 31] of unit 5 and 6 of the Kozloduy NPP consisting of three independent channels with three pumps [4]. If the seal of a pump fails, the pump can be taken off-line and repaired while the system remains operational. The pump MTTF is 1000 h, and the pump downtime including MTTR is up to 72 h. In case a pump does not work in a period of up to 72 h, the system is in standby position. If the downtime period continuous more than 72 h, the reactor is shutdown. If two pumps fail and it is necessary to be repaired, the reactor is also to be shutdown.

Assuming constant failure and repair rates and using the expression for the TMR system in Table 1 we have, λ=0.001 failures/hour, μ=0.014 repairs/hour; therefore M=3166.63h=131.94 days, and λ'=0.0076. Then the expression

$$F(t)=1-\exp(-\,0.0076\,t)$$

can be used as the failure distribution for the 3-pump system.

The downtime of this type of systems leads to losses caused by unproduction of electrical energy, (e.g. 1h = $21 000 losses). Hence, repairs are “expedited” when the system must be taken down. If the system repair time is only 2 days when the second pump fails, then m_{ss}=0.5, and we find from the equations (4) above:

$$A(t)=0.9850+0.01497\exp(-0.5076t),$$

$$A=0.9850.$$

Calculating the unavailability of the system we obtain:

$$Q_{sys}(t)=0.015.$$

For comparison, we show in Table 3 the values obtained using different procedures for calculation:

Table 3. Values obtained for *A* and *Q*

Procedure	WANO	According to Safety Analysis Report (SAR)	Operational data (!995-1996)	Approximation model
Availability (A)	0.992	0.96	0.972	0,985
Unavailability (Q)	0.008	0.04	0.028	0.015

4. Conclusions

Models of complex systems are really complex. As a result detailed models used to determine the availability and reliability of such systems are often too complex to be readily understood and a simpler, easily understood model is often more useful. In this paper we have described a set of relatively simple, “approximate”, but nevertheless, highly accurate models for such systems.The models as described above have rather simple representations and can be easily implemented with simple calculations.

References

1. Billinton, R., R. N. Allan. Reliability Evaluation of Engineering Systems. Concepts and Techniques. Pitman Advanced Publishing Program, 1982.
2. Bowles, J. B. Simple. Approximate system reliability and availability analysis techniques. – Reliability Review, Vol. 20, September 2000.
3. Reliability and Efficiency in Engineering. Handbook. Vol. 2: Mathematical Methods in Reliability and Efficiency Theory. B.V.Gnedenko (ed.). Moscow, Mashinostroenie, 1987 (in Russian).
4. GCR Ltd., Maintainability Program Optimization of Selected Systems of Units 1 - 6 at KNPP by the PM Optimizer Software. Report, 1997 (in Bulgarian).

Применение простых приблизительных методов для анализа надежности и готовности системы

Богомил Манчев, Бойка Ненкова***

**Риск Инженеринг ООД, бул. Тотлебен 34, 1606 София*

*** Институт по Информационни Технологии, 1113 София*

(Резюме)

В ряде случаев можно применять простые приблизительные модели системы на месте сложных, но “точных” моделей, которые очень трудоемкие и иногда трудно применимые.

Марковские модели являются самое частое средство для анализа надежности и эксплоатационной готовности сложных высоконадежных систем. Большое число елементов и многочисленные возможные состояния системы делают подробные модели таких систем тяжелые и трудные для применения так что они понимаемые только для их разработчиков или других экспертов, и часто требуют специального софтвера. Тогда для таких систем можно использовать набор более простых, “приблизительных”, но все таки с большой точностью моделей.

Методы, описаны в статье, представляют комплектом простых “приблизительных” моделей, применимых для большого класса системных структур.

Приблизительная модель создана путем построения Марковской модели каждой резервираной подсистемы и определения ее средной отработки до отказа. Результаты делают вычисления надежности и эксплоатационной готовности очень простые для системных инженеров. Другое преимущество что эти модели могут быть легко поняты лицами, которые не эксперты в этой области.

Представлены результаты применения “приблизительной” модели в технологической системе АЕЦ “Козлодуй”. Для сравнения представлены результаты, вычислены при помощи других методов. Полученые результаты демонстрируют хорошую сходимость.