THE EFFECT OF THE CHECKER ON SYSTEM RELIABILITY

Daniel P. Siewiorek
Dileep P. Bhandarkar

Carnegie-Mellon University
Pittsburgh, Pa.

September, 1972

This work was supported by the Advanced Research Projects Agency of the Office of the Secretary of Defense (F44620-70-C-0107) and is monitored by the Air Force Office of Scientific Research. This document has been approved for public release and sale; its distribution is unlimited.

ABSTRACT

A new parameter is introduced for modeling the reliability of systems with standby spares. Dependability, d, is defined as the conditional probability that the checker reports a module as good given that the module is good. The trade-off between the number of spares and dependability then is examined.

Key words:

reliability, standby spares, checker, dependability, mission time

INTRODUCTION

New designs for reliable computers must be explored to meet the increasing demand for reliable computing systems. In order to select one design approach over another, a method of comparison must exist. One important method of comparison is the modeling of the system reliability.

It has been shown that system reliability is extremely sensitive to certain system design parameters [1]. Coverage is defined in [1] as the conditional probability that, given the existence of a failure, the system is able to recover. A new parameter will be introduced and its effect on the reliability of systems will be examined.

DEPENDABILITY

Consider a system with standby spares. A checking circuit detects faults in the active module. The checker initiates the replacement of the active module by a standby spare if it detects an error. Define dependability, d, as the conditional probability that the checker reports a module as good given that the module is good. At any given time the active module has not only a conceptual reliability R, but also a probability that it will be called good. Hence the effective module reliability (the module reliability as it appears to the system) is dR and the probability that a module is considered failed becomes (1-dR). Thus the overall effect of d is to decrease the conceptual module reliability from R to dR. For the case of a distributed checker (e.g., each module has some added circuitry which reports on the status of the module), d is simply the probability that the checker reports the faultless functioning of the module correctly. A checker failure could result in a non-failed module being called faulty.

Alternatively, the checker could be centralized such as often proposed for hybrid redundancy [2]. In this case d is not the probability that the entire checking circuit reports the condition of all modules correctly but rather that the proper condition of a given module is being reported.

A paper by Firstman and Gluss [3] defines a parameter which is the probability that a tester indicates a module is good given that it is good and uses this parameter to determine an optimum search routine for fault location. Most previous research efforts in the modeling of fault tolerant computing systems, however, have either ignored the effect of d or assumed the value of d is so close to 1.0 that it need not be considered. The next section demonstrates the importance of d.

THE EFFECT OF DEPENDABILITY

To see what effect d on predicted system reliability has we will use the parameter I, the mission time improvement [4]. I is a useful measure of reliability improvement in that it compares the time for which two systems are at or above a specified reliability. Assume $R = e^{-\lambda t}$. Let R_{sys} be the system reliability for d = 1.0 and mission time T':

$$R_{sys}(T') = 1 - (1-R(T'))^{S+1} \tag{4}$$

and let ${}_dR_{sys}$ be the system reliability for d < 1.0 and mission time T:

$${}_dR_{sys}(T) = 1 - (1-dR(T)^{S+1} \tag{5}$$

Define $I = T'/T$, then I is the gain in mission time for perfect d. Equating (4) and (5) yields the following solution for I:

$$I = -\frac{1}{\lambda T} \ell n[de^{-\lambda T}] \tag{6}$$

Figure 1 shows a plot of I vs. d for various values of λT. It is clear that when d is less than one a potential mission time improvement is possible if d can be made perfect. If the checker is distributed (adding components to each module to perform the checking) and made of the same components as the module, then the checker dependability d can be written as a function of the module reliability R. It seems reasonable to assume

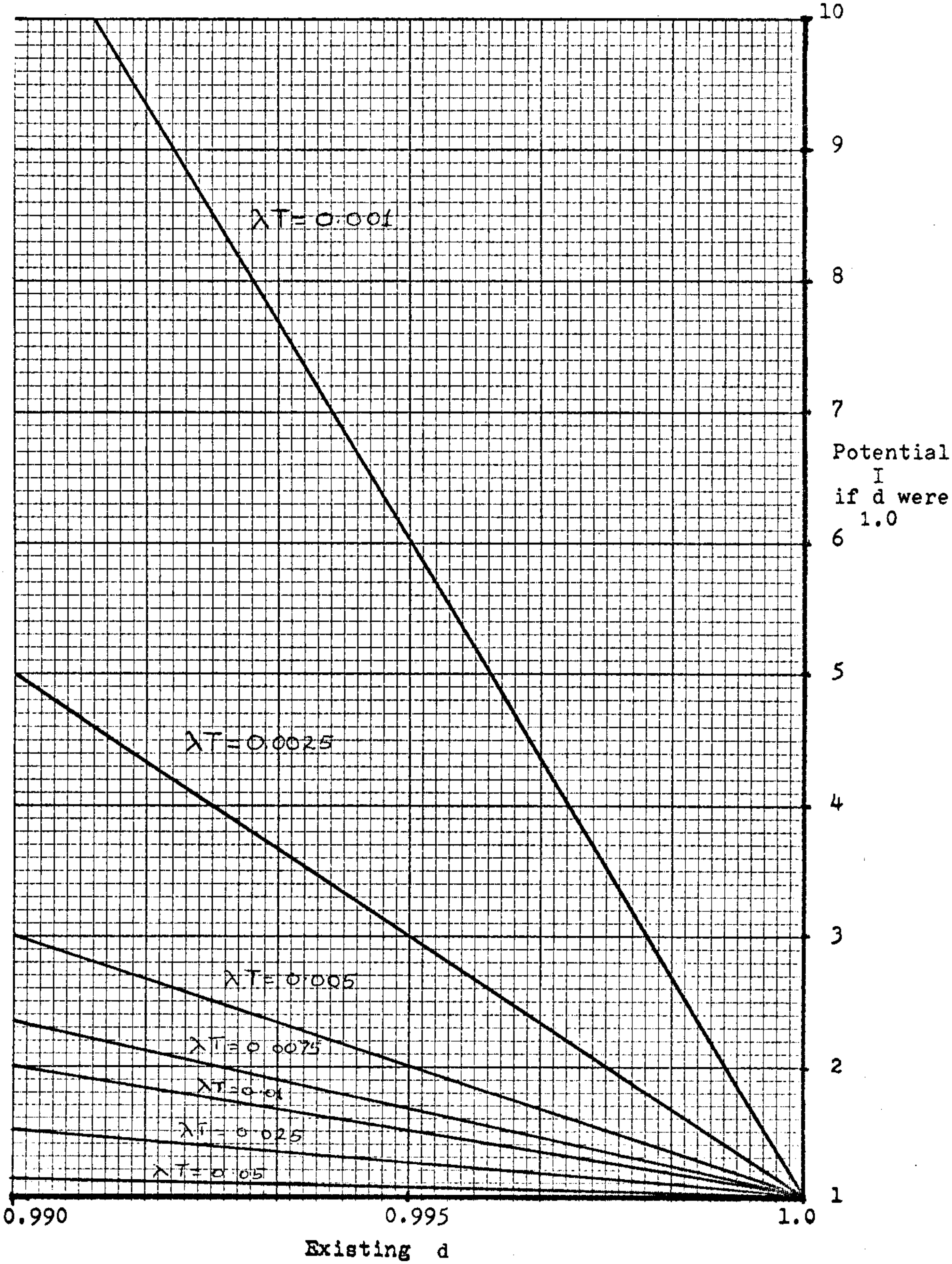
10
9
8
7
6
5
4
3
2
1
Potential I if d were 1.0
λT = 0.001
λT = 0.0025
λT = 0.005
λT = 0.0075
λT = 0.01
λT = 0.025
λT = 0.05
0.990
0.995
1.0
Existing d

Figure 1

that the checker is designed to be more reliable than the module. Let the dependability d equal R^i where i is less than unity. Table 1 depicts d for various values of R and i. With $d = R^i$, from equation (6), we see that the mission time improvement is 1+i for all values of λ.

R i	0.10	0.30	0.50	0.70	0.90
0.80000	0.97793	0.93525	0.89443	0.85539	0.81805
0.90000	0.98952	0.96889	0.94868	0.92890	0.90953
0.92000	0.99170	0.97530	0.95917	0.94330	0.92770
0.94000	0.99383	0.98161	0.96954	0.95761	0.94583
0.96000	0.99593	0.98783	0.97980	0.97183	0.96393
0.98000	0.99798	0.99396	0.98995	0.98596	0.98198

Table 1. $d = R^i$ for i ranging from 0.1 to 1.0

Equation 5 shows that there is a tradeoff between the number of spares s and the checker dependability d. Thus, a system designer at least has two independent ways of increasing the system reliability - either adding another spare or increasing the dependability of the checker. Let d' be the new dependability that achieves the same overall reliability as a system with an additional spare. Then,

$$1 - (1-d'R)^{S+1} = 1 - (1-dR)^{S+1+1} \tag{7}$$

and

$$d' = \frac{1 - (1-dR)^{\frac{S+2}{S+1}}}{R}$$

With $d = R^i$, (7) gives the new dependability:

$$d' = \frac{1 - (1 - R^{1+i})^{\frac{S+2}{S+1}}}{R}$$

Table 2 lists d' as a function of s, R and i. Since the value of d' is physically bounded by zero and one, those values listed in Table 2 calling for d' greater than one indicates that the addition of a spare is always superior to the increase of checker dependability. Note that for low values of s, i.e., $s = 1,2$, the addition of another spare is better in most cases. However, for low values of R and high values of i, increasing the checker dependability does provide a feasible alternative. Let $i^*(R,s)$ denote the critical values of i beyond which increase in dependability is a feasible alternative (i.e., $d' < 1.0$). Table 2 suggests that i^* becomes smaller as R decreases (mission time increases) and the number of spares, s, increases. Thus, for a system with three or more spares, and a long mission time, the number of spares can be traded for increased checker reliability. However, a factor that would determine the most effective alternative would be the relative cost of the two methods. The analysis presented here has ignored the inevitable increase in switch complexity resulting from increase in the number of spares.

NO. OF SPARES = 1

R i	0.10	0.30	0.50	0.70	0.90
0.80000	1.12307	1.09286	1.06036	1.02828	0.99608
0.90000	1.07089	1.06023	1.04901	1.03732	1.02525
0.92000	1.05876	1.05117	1.04314	1.03473	1.02600
0.94000	1.04587	1.04097	1.03576	1.03027	1.02453
0.96000	1.03208	1.02943	1.02659	1.02358	1.02043
0.98000	1.01708	1.01615	1.01515	1.01408	1.01295

NO. OF SPARES = 3

R i	0.10	0.30	0.50	0.70	0.90
0.80000	1.06417	1.02074	0.99032	0.95421	0.91882
0.90000	1.04118	1.02604	1.01068	0.99516	0.97955
0.92000	1.03513	1.02374	1.01213	1.00034	0.98843
0.94000	1.02838	1.02048	1.01238	1.00412	0.99574
0.96000	1.02073	1.01600	1.01112	1.00613	1.00103
0.98000	1.01177	1.00979	1.00775	1.00564	1.00348

Table 2. Checker dependability required to have the same effect as the addition of an extra spare. (continued on next page)

NO. OF SPARES = 5

i R	0.10	0.30	0.50	0.70	0.90
0.80000	1.03899	0.99988	0.96164	0.92438	0.88816
0.90000	1.02702	1.01014	0.99322	0.97631	0.95944
0.92000	1.02347	1.01054	0.99751	0.98443	0.97133
0.94000	1.01935	1.01017	1.00087	0.99148	0.98204
0.96000	1.01450	1.00881	1.00302	0.99715	0.99122
0.98000	1.00854	1.00602	1.00344	1.00082	0.99816

Table 2. (continued)

References

1. Bouricius, W. G., W. C. Carter and P. R. Schneider, "Reliability Modeling Techniques for Self-Repairing Computer Systems", ACM 1969 Annual Conference, p-69, pp. 295-309.

2. Siewiorek, D. P. and E. J. McCluskey, "An Iterative Cell Switch Design for Hybrid Redundancy", IEEE Transactions on Computers, to appear, March 1973.

3. Firstman, S. I. and B. Gluss, "Optimum Search Routines for Automatic Fault Location", Operations Research, Vol. 8, pp. 512-523, 1960.

4. Bouricius, W. G., W. C. Carter, D. C. Jessep, P. R. Schneider, and A. B. Wadia, "Reliability Modeling for Fault-Tolerant Computers", IEEE Transactions on Computers, Vol. C-20, No. 11, pp. 1306-1311, November 1971.