The Concept of Coverage and Its Effect on the Reliability Model of a Repairable System

THOMAS F. ARNOLD

Abstract—Duplication is a technique frequently employed to achieve high reliability for a repairable system. Although the philosophy of duplication is that it takes two faults to place a system out of service, there are generally some critical single faults that cause a system failure. This paper considers the effect of such a set of faults on a repairable system’s reliability. It is shown that even a small number of such faults may severely degrade the mean time to system failure and the expected downtime for an otherwise highly reliable system.

Index Terms—Coverage, fault tolerance, recovery, redundancy, reliability, reliability estimation.

INTRODUCTION

The design of highly reliable electronic systems generally incorporates spares for critical units. For example, an electronic telephone switching system may contain two central processors—one active and one standby [1], [2]. If the active unit develops a fault, then control is given to the standby unit in order to continue the normal processing functions. A system failure occurs if the spare unit (now active) develops a fault before the previously active unit has been repaired.

It is unfortunately true that a double fault (one in each of the mate units) is not a necessary condition for a system failure to occur. There are, in general, a small number of single faults from which a system with spares cannot recover automatically. The designer attempts to make this number as small as possible, but the number of such faults is rarely, if ever, brought down to zero.

This paper demonstrates the effect of such single faults on the reliability of a repairable system with spares. It is shown that if these faults constitute even a few tenths of a percent of all the possible system faults, the reliability of the system may be drastically reduced. The designer ignores this small number of faults at his own peril.

(Although this paper discusses system failure due to one or more faults, it is important to recognize that system failure may occur for other reasons. Common causes include manual error and software design errors. These two causes might be considered as members of a generalized class of faults. If one attempts to form such a class, the usual result is that the proportion of single faults that cause system failure is far higher than one would estimate on a purely hardware basis. Because such single faults drastically affect reliability, it follows that an accurate reliability estimate must take into account, to the extent possible, both manually caused failures and program caused failures.)

THE RELIABILITY MODEL OF A DUPLICATED REPAIRABLE SYSTEM AND THE CONCEPT OF COVERAGE

The important effects of the class of single faults that cause system failure in a replicated nonrepairable system are considered in Bouricius et al. [3], [7]. It is shown that these
faults can strongly affect the system mean time to failure, particularly if the number of spares is large. Informally, it would appear that this class of faults may also be very important to a duplicated repairable system, since such a system bears many of the characteristics of a nonrepairable system that contains a very large number of spares. It will be shown in what follows that this is indeed the case.

Consider a system composed of an active unit and a spare unit. Each of these units will be called a module. The following assumptions will be made concerning these modules.

**Assumption 1:** The failure rate of a module does not depend on whether the module is active or standby.

**Assumption 2:** The time to module failure is exponentially distributed.

**Assumption 3:** The time to repair a module is exponentially distributed.

Although the preceding assumptions may not always be true, they allow a simple demonstration of the importance of the class of single faults that cause system failure. Using these assumptions, a duplicated repairable system can be considered as a Markov process of three states [4] (Fig. 1).

**State 1:** Both system modules working.

**State 2:** One system module has failed, but the system is still working.

**State 3:** Both system modules have failed or a single fault has occurred from which the system did not recover; the system is down.

Once the system enters the third state, the system has failed. Transitions between the three states are dependent upon the following parameters.

\[ t_1 = 1/\lambda_1 \text{ Mean time to failure of a particular module.} \]
\[ t_2 = 1/\lambda_2 \text{ Mean time to repair for a failed module.} \]
\[ p \text{ Proportion of faults from which the system can automatically recover.} \]

The value on an arc from state \( i \) to state \( j \) is \((1/dt)\) times the probability that a transition occurs from \( i \) to \( j \) in the time interval \((t, t + dt)\), given that the system was in state \( i \) at time \( t \). These values are easily derived using the above definitions and the exponential assumptions.

**Definition:** The proportion of faults \( p \) from which a system automatically recovers is called the system’s coverage; the faults in this class are said to be covered by the recovery strategy.

**Mean Time to First Failure Calculations**

The model of Fig. 1 incorporates the coverage specifically in the transitions from State 1. Covered faults allow a transition into State 2, while noncovered faults cause a transition directly to State 3. The model may be used to determine the system’s mean time to first failure (MTTF), or the mean time required to make the first entry into State 3, given that the system starts in State 1. Let \( P_i(t) \) be the probability that the system is in state \( i \) at time \( t \), given that it was in State 1 at time 0.

Using the properties implied by Fig. 1, one may write

\[
\frac{dP_1(t)}{dt} = -2\lambda_1 P_1(t) + \lambda_2 P_2(t) \tag{1}
\]

\[
\frac{dP_2(t)}{dt} = 2\lambda_1 p P_1(t) - (\lambda_1 + \lambda_2) P_2(t) \tag{2}
\]

\[
\frac{dP_3(t)}{dt} = 2\lambda_1 (1-p) P_1(t) + \lambda_2 P_2(t) \tag{3}
\]

\[ P_1(0) + P_2(0) + P_3(0) = 1 \]

\[ P_1(0) = 1; P_2(0) = P_3(0) = 0. \tag{4} \]

These equations may be solved by standard techniques with the result that the MTTF is given by

\[
\text{MTTF} = \int_0^\infty t \dot{P}_3(t) \, dt = \frac{1 + \frac{\lambda_1}{\lambda_2} (5 - 3p)}{2\lambda_1 \lambda_2} \left[ \frac{1 + \frac{\lambda_2}{\lambda_1} (1 - p)}{5 - 3p} \right]. \tag{5} \]

Since typically \( \lambda_1 \ll \lambda_2 \), the second term of the numerator is always much smaller than 1 and can be ignored. The ideal MTTF when \( p = 1 \) is then very nearly

\[
\text{MTTF}_{p=1} \approx \frac{\lambda_2}{2\lambda_1^2}. \]

Thus, the effect of imperfect coverage is to reduce the MTTF by the quantity

\[
\frac{\text{MTTF}_{p=1}}{\text{MTTF}} \approx 1 + \frac{\lambda_2}{\lambda_1} (1 - p). \tag{6} \]

From the preceding, it can be seen that imperfect coverage becomes the dominant contributor to the failure rate of a duplicated repairable system when the proportion of noncovered faults \( 1 - p \) becomes as large as

\[
1 - p = \frac{\lambda_1}{\lambda_2}. \tag{7} \]

Typically, \( \lambda_1/\lambda_2 \) may be as small as 0.001 or smaller. For example, if a unit develops a fault, on the average, once every three months (2180 h), and if the fault can be repaired in an average of 2 h, then \( \lambda_1/\lambda_2 = 0.00092 \). Fig. 2 illustrates a set of MTTF curves for some typical values of \( p, \lambda_1, \) and \( \lambda_2 \). Notice that beyond a certain point, repair time has little to do with MTTF since the system is most likely to fail due to a noncovered fault. It should be clear from these curves that if noncovered faults amount to even a few tenths of one percent, the MTTF may be severely reduced.

**Expected Downtime Calculations**

In many cases it may be more valuable to estimate the proportion of time during which the system is in a failed state. This may be calculated for a duplicated, repairable system by
a refinement of the model of Fig. 1. It will be necessary to distinguish between two types of noncovered faults.

Type 1—Manually Recoverable Faults: Faults that are not covered by the automatic recovery strategy, but for which manual actions may recover a working system without repairing the fault.

Type 2—Nonrecoverable Faults: Faults that must be repaired before normal processing can be resumed. Noncovered faults of the first type may allow a rather rapid transition from the failed state into State 2, whereas noncovered faults of the second type generally require a long repair time resulting in a return to State 1. In addition to these two possibilities, a system failure due to a double fault would also generally require a long repair time, but with a return to State 2. In order to properly distinguish these cases, the model of Fig. 1 is refined into one containing five states, as shown in Fig. 3. The additional parameters are defined as follows.

\[ p' \] Proportion of all faults that are manually recoverable.

\[ t_3 = 1/\lambda_3 \] Average repair time of a fault in a system that has failed.

\[ t_4 = 1/\lambda_4 \] Average time to recover from a manually recoverable fault.

The expected downtime (EDT) is then the proportion of time that is spent in States 3, 4, and 5. The EDT can be found by writing the differential equations for the model of Fig. 3 and solving the equations in the steady-state \[ dp'(t)/dt = 0 \]. This results in (assuming \( \lambda_1 << \lambda_2, \lambda_3, \lambda_4 \))

\[
\text{EDT} = \frac{2\lambda_4^2}{\lambda_3 \lambda_4} \left[ p + p' + \frac{\lambda_2}{\lambda_1} (1 - p - p') + \frac{\lambda_2 \lambda_3}{\lambda_1 \lambda_4} p' \right].
\] (8)

In order to see how the EDT is affected by the parameters \( p \) and \( p' \), consider first the case where no faults are manually recoverable \((p' = 0)\). In this case, the EDT is dominated by noncovered faults when the coverage parameter becomes smaller than

\[
p = \frac{1}{1 + \frac{\lambda_1}{\lambda_2}} \approx 1 - \frac{\lambda_1}{\lambda_2}
\] (9)

as was the case for the MTFF. However, if all the faults are manually recoverable \((p' = 1 - p)\), then the EDT is not dominated by noncovered faults until \( p \) becomes smaller than

\[
p = 1 - \frac{\lambda_1}{\lambda_2} \cdot \frac{\lambda_4}{\lambda_3}.
\] (10)

Thus, if a system is designed to allow rapid manual recovery for noncovered faults, then a much higher proportion of noncovered faults can be tolerated for a given EDT. For example, if \( \lambda_1/\lambda_2 = 0.001 \), and if manual recovery is always possible (perhaps from a 24-h remote location), then \( \lambda_4/\lambda_3 \) might well achieve a value as high as 10 to 20. This would allow the proportion of noncovered faults to rise from 0.001 to perhaps 0.01 without significantly changing the EDT. To illustrate this, Fig. 4 has been prepared. This figure illustrates the EDT...
for a duplicated system with the same failure rate as used in Fig. 2, and it shows how the resulting EDT curve is improved if all faults are manually recoverable (i.e., \( p' = 1 - p \)) with \( \lambda_4/\lambda_3 = 10 \).

**MTFF AND EDT for \( n - 1 \) Active Units with One Spare**

A more general case than the duplication discussed above is one in which there are a total of \( n \) modules, of which \( n - 1 \) are necessary for processing. One module is available as a spare for any of the active modules. The models required to compute the MTFF and EDT for such a system are shown in Fig. 5. In Fig. 5(b), it is implicitly assumed that no additional failures occur while the system is in a failed state (States 3, 4, or 5). This assumption is required to keep the problem mathematically tractable, and has virtually no effect on the results.

The models of Fig. 5 are handled in the same way as those of Figs. 1 and 3. With \( \lambda_1 \ll \lambda_2, \lambda_3, \lambda_4 \), these models yield

\[
\text{MTFF} = \frac{\lambda_2}{n(n-1)\lambda_1^2 \left[ 1 + \frac{1-p}{n-1} \lambda_2 \right]}
\]

\[
\text{EDT} = \frac{n(n-1)\lambda_1^3 \left( (p+p') + \frac{1-p-p'}{n-1} \lambda_2 + \frac{p'}{n-1} \lambda_3 \right)}{\lambda_2 \lambda_3}
\]

If there are no manually recoverable faults (\( p' = 0 \)), then noncovered faults become important with respect to MTFF and EDT when the coverage becomes as low as

\[ p = 1 - (n-1) \frac{\lambda_1}{\lambda_2} . \]

If all faults are manually recoverable, the EDT is not significantly affected until \( p \) becomes as low as

\[ p = 1 - (n-1) \frac{\lambda_4}{\lambda_2} . \]

Note that the coverage factor becomes relatively less important as \( n \) increases. The reason for this is that the contribution to system failure rate when caused by two units failing increases with the square of \( n \), whereas the contribution caused by noncovered faults increases only linearly with \( n \). Thus, although the contribution to system failure rate caused by noncovered faults grows in absolute magnitude as the number of active units grows, this contribution may no longer be the dominant component for MTFF or EDT if \( n \) is large.

**Conclusions**

This paper has introduced the concept of covered faults in a repairable system. It has been shown that a very small proportion of noncovered faults may greatly reduce the reliability of a repairable system that includes one spare module. In the more general case, one might consider a system with more than one spare module. The model for this case is easily constructed, but the algebra required to solve the resulting equations becomes rather difficult. Nevertheless, the same general conclusions hold. In fact, one would expect that the presence of noncovered faults in each module would result in a limit to the number of spares that can be added to enhance a system's reliability.

**References**


---

Thomas F. Arnold was born in New York, N.Y., on September 23, 1943. He received the S.B. and S.M. degrees in electrical engineering from the Massachusetts Institute of Technology, Cambridge, in 1964 and 1965, respectively, and the D. Eng. Sc. degree in electrical engineering from Columbia University, New York, N.Y., in 1969.

In 1965 he joined the technical staff at Bell Telephone Laboratories, Inc., Holmdel, N.J., where he has participated in the development of electronic switching systems. He is presently engaged in hardware and software development for peripheral units and is especially concerned with the problems of highly reliable systems.

Dr. Arnold is a member of Tau Beta Pi, Eta Kappa Nu, and Sigma Xi.