

SAND93-1822
Unlimited Release
Printed October 1993

Distribution
Category UC-706

Algorithms for Treating Redundancy in Repairable and Non-Repairable Systems

James E. Campbell
Manufacturing Systems Reliability
Sandia Laboratories
Albuquerque, NM 87185
Dennis E. Longsine¹
Joel Atkins²

Abstract

This report presents equations and computational algorithms for analyzing reliability of several forms of redundancy in repairable and non-repairable systems. For repairable systems, active, standby, and R of N redundancy with and without repair are treated. For non-repairable systems, active, standby, and R of N redundancy are addressed. These equations can be used to calculate mean time between failures, mean time to repair, and reliability for complex systems involving redundancy.

October 1993

MASTER

¹Intera, Inc., Albuquerque, NM

²Statistics Department, University of California, Berkeley, CA

CONTENTS

Chapter 1	1
Introduction.....	1
Chapter 2	5
Active with Repair.....	5
Two Parallel Components - Active with Repair.....	5
Three Parallel Components - Active with Repair	8
N Parallel Components - Active with Repair.....	10
Chapter 3	13
Active without Repair.....	13
Two Parallel Components - Active without Repair.....	13
Three Parallel Components - Active without Repair	15
N Parallel Components - Active without Repair.....	17
Active Redundancy in Non-Repairable Systems	18
Chapter 4	21
Standby with Repair	21
Notation	22
Two Components in Parallel - Standby with Repair	22
Three Components in Parallel - Standby with Repair.....	27
Chapter 5	33
Standby without Repair	33
Standby Redundancy in Non-Repairable Systems.....	35
One Active and One Standby Component.....	35
One Active and Two Standby Components	38
One Active and N - 1 Standby Components	40
Chapter 6	45
R of N Redundancy with Repair	45
Chapter 7	49
R of N Redundancy without Repair	49
Three Parallel Components, Two Required, without Repair.....	49
Four Parallel Components, Two Required, without Repair.....	52
N Parallel Components, R Required, without Repair.....	55
R of N Redundancy in Non-Repairable Systems.....	58
Chapter 8	59
Conclusions.....	59

References	63
Appendix A.....	65
Algorithm for Standby with Repair.....	65
Appendix B.....	73

FIGURES

Figure 2.1 Two Components in Parallel	6
Figure 2.2 Three Components in Parallel	8
Figure 3.1 Reliability of a Parallel System as a Function of the Number of Components.....	19
Figure 6.1 4 Components in Parallel, 3 Required for Success	45
Figure 6.2 3 of 4 Redundancy as a Series Arrangement.....	45
Figure 8.1 MTBF for Parallel Components with Different Redundancy Treatments.....	61
Figure A.1 Flowchart of the Algorithm.....	68
Figure A.2 Subchart A.....	69
Figure A.3 Subchart B.....	70
Figure A.4 Subchart C.....	71
Figure A.5 Subchart D.....	72

TABLES

Table 2.1	Comparison for Two Components in Parallel, Active with Repair	8
Table 2.2	Comparison for Three Components in Parallel, Active with Repair	10
Table 2.3	Comparison for Five Components in Parallel, Active with Repair	11
Table 3.1	Comparison for Two Components in Parallel, Active without Repair	15
Table 3.2	Comparison for Three Components in Parallel, Active without Repair.	17
Table 3.3	Comparison for Five Components in Parallel, Active without Repair	18
Table 4.1.	States and Transition Probabilities for a 2 Component System.....	22
Table 4.2	States and Transition Probabilities for a 2 Component System.....	24
Table 4.3	Comparison for Two Components in Parallel, Standby with Repair.	26
Table 4.4	States and Transition Probabilities for a 3 Component System.....	27
Table 4.5	States and Transition Probabilities for a 3 Component System.....	28
Table 4.6	States and Transition Probabilities for a 3 Component System.....	29
Table 4.7	States and Transition Probabilities for a 3 Component System.....	31
Table 4.8	States and Transition Probabilities for a 3 Component System.....	32
Table 4.9	Comparison for Three Components in Parallel, Standby with Repair.	32
Table 5.1	Comparison for Two Components in Parallel, Standby without Repair.	34
Table 5.2	Comparison for Three Components in Parallel, Standby without Repair.	35
Table 6.1	Comparison for Two of Three Redundancy with Repair	46
Table 6.2	Comparison for Three of Four Redundancy with Repair.....	47
Table 7.1	Comparison for Two of Three Redundancy without Repair	52
Table 7.2	Comparison for Three of Four Redundancy without Repair.....	58

Table 8.1 MTBF of Parallel Components with Different Redundancy Treatments.....	61
--	----

Chapter 1

INTRODUCTION

Parallelism or redundancy is routinely used to achieve high reliability in systems where high levels of safety must be assured (e.g., aircraft, nuclear reactors, space and defense systems). Other factors that might drive the use of redundancy are unacceptability of down time (e.g., defense radar systems) or high down time cost. For example, fault tolerant computers have been used for several years. However, ordinary microcomputers are commonly used to control manufacturing equipment and processes. Because down time can be quite expensive for manufacturing equipment, microcomputers that achieve high reliability using redundancy are increasingly available.

The typical treatment of redundancy in reliability analysis of mission-oriented applications is, in most cases, relatively straightforward [3]. In such applications, one is concerned with the probability of successful operation over some defined mission time. The probability of successful operation of the parallel system is just the probability that at least one of the parallel components does not fail. In analysis of repairable systems, treatment of redundancy becomes more complex [4]. In this case, system performance measures such as mean time between failures, availability, and system mean time to repair are of interest. The analysis is further complicated by the possibility that failed components can be repaired while the system continues to operate on other parallel components.

In this report, we develop equations for several redundancy options for both repairable and non-repairable systems. For all configurations in this report, we will assume that individual components have a constant failure rate. For repairable systems, we consider the following six redundancy treatments:

Active with Repair All parallel components are active with only one needed for success. A failed component can be repaired while the system continues to operate on other parallel components.

Active without Repair All parallel components are active with only one needed for success. Failed components are not repaired until all parallel components have failed. Then all are repaired.

Standby with Repair Only one of the redundant components is active with others held in standby. In case the active component fails, a standby component can be switched on either manually or automatically. The failed component is repaired while the system operates using a standby component.

Standby without Repair Only one of the redundant components is active with others held in standby. In case the active component fails, a standby component can be switched on either manually or automatically. The failed component is not repaired until all redundant components have failed.

R of N with Repair The system consists of N components of which R ($1 < R < N$) are required for success. Failed components are repaired while the system operates.

R of N without Repair The system consists of N components of which R ($1 < R < N$) are required for success. Failed components are not repaired until more than $N - R$ have failed and the system cannot operate. For an example of R of N redundancy without repair, consider a car wheel with 5 lug nuts. If 4 are considered necessary for safe operation, the lug nuts provide 4 of 5 redundancy.

While there are a multitude of ways to design redundancy, the six options treated in this document provide good coverage of the range of effectiveness of redundancy in repairable systems. In each case, the intent is to find an equivalent failure rate and repair time for the redundant components. Even though we assume that failure rates of individual components are constant, the equivalent failure rates for parallel components are generally not constant for any of the redundancy options. The possible exceptions are the standby redundancy options which have at least piece-wise constant failure rates since only one component is active at any time. For the redundancy options that involve repair while the parallel system remains active, we calculate the mean time between failures (MTBF). For redundancy options that do not involve repair

of failed components until the parallel system fails, we calculate the mean time to fail (MTTF). In both cases, we treat the reciprocal ($1/\text{MTBF}$ or $1/\text{MTTF}$) as the average failure rate of the parallel components that are part of a larger repairable system.

Chapters 2 through 7 develop equations and algorithms for the above six redundancy options in repairable systems.

For non-repairable systems, we consider three redundancy treatments:

Active All parallel components are active with only one needed for success. The redundant system fails only when all parallel components fail.

Standby Only one of the redundant components is active with others held in standby. In case the active component fails, a standby component can be switched on either manually or automatically. The redundant system fails only when all parallel components fail.

R of N The system consists of N components of which R ($1 < R < N$) are required for success. The redundant system fails only when less than R components are operable (i.e., when $N - R + 1$ components have failed).

For redundancy in non-repairable systems, our interest is in calculating the reliability of the redundant arrangement. The reliability of the above three redundancy treatments in non-repairable systems is addressed in Chapters 3, 5, and 7.

All redundancy options listed are being implemented in the Reliability Analysis and Modeling (RAMP) software. Version 1 of RAMP ([1], [2]) treated active with repair for uniform repair times for all components in the system. Version 2 of RAMP incorporates all of the options listed above with component-specific repair times and failure rates, and will be released in 1993.

Chapter 2

ACTIVE WITH REPAIR

In the active with repair redundancy option, we assume that two or more components are active and only one component is necessary for successful operation. In case a component fails, it is repaired while another active component performs the required function. The parallel system fails only if all parallel components are down at the same time. In the following discussion, we take the mean time to repair as the total down time, that is, the time period beginning when a component or the system fails and ending when the component or system returns to operation.

Two Parallel Components - Active with Repair

Consider two components in parallel as shown in Figure 2.1 below. The mean time between failures and the mean time to repair (MTTR) are

$$\begin{aligned} \text{MTBF}_A &= T_{FA} & \text{MTTR}_A &= T_{RA} = \frac{1}{\mu_A} \\ \text{MTBF}_B &= T_{FB} & \text{MTTR}_B &= T_{RB} = \frac{1}{\mu_B} \end{aligned} \quad (2.1)$$

Implicit in Equations (2.1) is that times to failure and times to repair follow an exponential distribution. That is

$$Q_{FA} = 1 - e^{-t/T_{FA}} \quad Q_{RA} = 1 - e^{-t/T_{RA}} \quad (2.2)$$

where Q_{FA} is the probability that component A fails during time t . Similarly, Q_{RA} is the probability that component A, having failed, is repaired during time t .

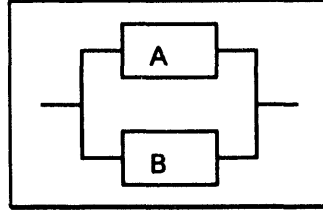


Figure 2.1 Two Components in Parallel

If either component A or B fails, the system does not fail unless the second component fails before the first can be repaired. Then the fraction of time that component A is down is

$$F_A = \frac{T_{RA}}{T_{FA} + T_{RA}}. \quad (2.3)$$

Similarly, the down time fraction for component B is

$$F_B = \frac{T_{RB}}{T_{FB} + T_{RB}}. \quad (2.4)$$

The system is down only if both A and B fail. Since both components are assumed to have a constant failure rate and failures occur randomly, the down time fraction for the system is

$$F_S = F_A F_B = \frac{T_{RA}}{T_{FA} + T_{RA}} \frac{T_{RB}}{T_{FB} + T_{RB}}. \quad (2.5)$$

We now need to calculate the average down time when the system fails. For the system to fail, both A and B must fail. The average time to repair the system is the average time before either A or B is repaired. Recalling Equation (2.2) and setting $\mu_A = 1/T_{RA}$, the probability that A is not repaired during time t is $e^{-\mu_A t}$. Similarly, the probability that B is not repaired during time t is $e^{-\mu_B t}$. The average time over which neither A nor B are repaired can be found from

$$T_{RS} = \int_0^{\infty} t e^{-\mu_A t} e^{-\mu_B t} dt / \int_0^{\infty} e^{-\mu_A t} e^{-\mu_B t} dt. \quad (2.6)$$

Performing the integrals we get

$$T_{RS} = (\mu_A + \mu_B) \left[\frac{e^{-(\mu_A + \mu_B)t}}{(\mu_A + \mu_B)^2} \{ -(\mu_A + \mu_B)t - 1 \} \right]_0^\infty$$

$$T_{RS} = \frac{1}{\mu_A + \mu_B} = \frac{T_{RA} T_{RB}}{T_{RA} + T_{RB}} \quad (2.7)$$

T_{RS} is the average down time when the system (both A and B) fails. Then, the expected number of failures per hour of the system is the system down time fraction divided by the mean time to repair the system. That is

$$\frac{F_s}{T_{RS}} = \frac{(T_{RA} + T_{RB})}{(T_{FA} + T_{RA})(T_{FB} + T_{RB})} \quad (2.8)$$

and the system MTBF is

$$T_{FS} = \frac{1 - F_s}{\left(\frac{F_s}{T_{RS}} \right)} = \frac{\left[1 - \frac{T_{RA} T_{RB}}{(T_{FA} + T_{RA})(T_{FB} + T_{RB})} \right]}{\frac{(T_{RA} + T_{RB})}{(T_{FA} + T_{RA})(T_{FB} + T_{RB})}} \quad (2.9)$$

$$T_{FS} = \frac{(T_{FA} + T_{RA})(T_{FB} + T_{RB}) - T_{RA} T_{RB}}{T_{RA} + T_{RB}} \quad (2.10)$$

Availability is given by

$$\text{Availability} = A = \frac{T_{FS}}{T_{FS} + T_{RS}} \quad (2.11)$$

As a numerical example, let

$$\begin{array}{ll} T_{FA} = 50 \text{ hr} & T_{RA} = 3 \text{ hr} \\ T_{FB} = 100 \text{ hr} & T_{RB} = 5 \text{ hr} \end{array}$$

This problem was analyzed by Markov analysis and using the equations developed above. Comparison of Markov analysis results with results obtained using Equations (2.7), (2.10), and (2.11) is shown in Table 2.1.

	Calculated	Markov Analysis
Availability	0.9973	0.9973
MTBF (T_{FS})	694 hr	694 hr
MTTR (T_{RS})	1.88 hr	1.88 hr

Table 2.1 Comparison for Two Components in Parallel, Active with Repair

The results in Table 2.1 show excellent agreement between the equations developed above and the Markov analysis.

Three Parallel Components - Active with Repair

Consider 3 components in parallel as shown in Figure 2.2.

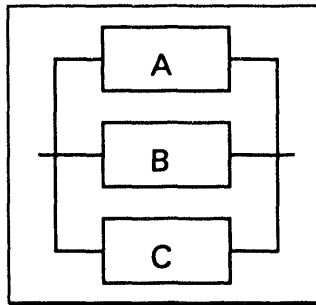


Figure 2.2 Three Components in Parallel

As before,

$$\begin{aligned}
 F_A &= \frac{T_{RA}}{T_{FA} + T_{RA}} \\
 F_B &= \frac{T_{RB}}{T_{FB} + T_{RB}} \\
 F_C &= \frac{T_{RC}}{T_{FC} + T_{RC}}
 \end{aligned}
 \tag{2.12}$$

$$F_s = F_A F_B F_C = \frac{T_{RA} T_{RB} T_{RC}}{(T_{FA} + T_{RA})(T_{FB} + T_{RB})(T_{FC} + T_{RC})}. \quad (2.13)$$

We have shown earlier (Eq. 2.7) that the average down time for components A and B is

$$T_{RAB} = \frac{T_{RA} T_{RB}}{T_{RA} + T_{RB}}. \quad (2.14)$$

By a similar argument, we can show that the average down time overlap between AB and C is

$$T_{RS} = \frac{T_{RAB} T_{RC}}{T_{RAB} + T_{RC}} = \frac{1}{\frac{1}{T_{RAB}} + \frac{1}{T_{RC}}}. \quad (2.15)$$

Therefore, the average system down time (MTTR) is

$$T_{RS} = \frac{1}{\frac{T_{RA} + T_{RB}}{T_{RA} T_{RB}} + \frac{1}{T_{RC}}} = \frac{1}{\frac{1}{T_{RA}} + \frac{1}{T_{RB}} + \frac{1}{T_{RC}}}. \quad (2.16)$$

The average system down time per failure is

$$\frac{F_s}{T_{RS}} = \frac{(T_{RA} T_{RB} + T_{RA} T_{RC} + T_{RB} T_{RC})}{(T_{FA} + T_{RA})(T_{FB} + T_{RB})(T_{FC} + T_{RC})}. \quad (2.17)$$

Then, the system MTBF is the fraction of time the system is operating divided by the number of system failures per hour. That is

$$T_{FS} = \frac{1 - F_s}{\left(\frac{F_s}{T_{RS}}\right)} = \frac{\left(1 - \frac{T_{RA} T_{RB} T_{RC}}{(T_{FA} + T_{RA})(T_{FB} + T_{RB})(T_{FC} + T_{RC})}\right)}{\left(\frac{T_{RA} T_{RB} + T_{RA} T_{RC} + T_{RB} T_{RC}}{(T_{FA} + T_{RA})(T_{FB} + T_{RB})(T_{FC} + T_{RC})}\right)} \quad (2.18)$$

$$T_{FS} = \frac{(T_{FA} + T_{RA})(T_{FB} + T_{RB})(T_{FC} + T_{RC}) - T_{RA}T_{RB}T_{RC}}{T_{RA}T_{RB} + T_{RA}T_{RC} + T_{RB}T_{RC}} \quad (2.19)$$

Results obtained using Equations (2.16) and (2.19) were compared with a Markov calculation for three components in parallel having the following MTBF's and MTTR's:

$$\begin{array}{ll} T_{FA} = 100 \text{ hr} & T_{RA} = 5 \text{ hr} \\ T_{FB} = 50 \text{ hr} & T_{RB} = 3 \text{ hr} \\ T_{FC} = 25 \text{ hr} & T_{RC} = 2 \text{ hr} \end{array}$$

The comparisons are shown in Table 2.2.

	Calculated	Markov Analysis
Availability	0.9998	0.9998
System MTBF (T_{FS})	4846 hr	4846 hr
System MTTR(T_{RS})	0.968 hr	0.968 hr

Table 2.2 Comparison for Three Components in Parallel, Active with Repair

N Parallel Components - Active with Repair

The key results from the previous sections can now be generalized. Assume n components in parallel (active with repair). Let their MTBFs and MTTRs be

$$\begin{array}{ll} \text{MTBF for component } i = T_{Fi} \text{ (hr)} & \text{MTTR for component } i = T_{Ri} \text{ (hr)} \\ \text{MTBF for the system} = T_{Fs} \text{ (hr)} & \text{MTTR for the system} = T_{Rs} \text{ (hr)} \end{array}$$

Then for N components in parallel,

$$T_{FS} = \frac{\prod_{i=1,N} (T_{Fi} + T_{Ri}) - \prod_{i=1,N} T_{Ri}}{\sum_{k=1,N} \left(\prod_{i=1,N, i \neq k} T_{Ri} \right)}, \quad (2.20)$$

and

$$T_{RS} = \frac{1}{\sum_{i=1,N} \left(\frac{1}{T_{Ri}} \right)}. \quad (2.21)$$

Equations (2.20) and (2.21) were compared with Markov analysis results for the following case of 5 components in parallel.

$$\begin{array}{ll} T_{F1} = 10 \text{ hr} & T_{R1} = 2 \text{ hr} \\ T_{F2} = 15 \text{ hr} & T_{R2} = 3 \text{ hr} \\ T_{F3} = 12 \text{ hr} & T_{R3} = 4 \text{ hr} \\ T_{F4} = 8 \text{ hr} & T_{R4} = 2 \text{ hr} \\ T_{F5} = 20 \text{ hr} & T_{R5} = 5 \text{ hr} \end{array}$$

The results of this comparison for 5 parallel components are shown in Table 2.3.

	Calculated	Markov Analysis
Availability	0.99972	0.99972
System MTBF (T_{FS})	2018 hr	2018 hr
System MTTR(T_{RS})	0.56 hr	0.56 hr

Table 2.3 Comparison for Five Components in Parallel, Active with Repair

As before, the comparisons between the equations developed above and Markov analysis are excellent.

The results given by Equation (2.20) can be used to calculate an average failure rate as

$$\lambda = \frac{1}{T_{FS}}.$$

Chapter 3

ACTIVE WITHOUT REPAIR

With this redundancy option, as in the active with repair option, all parallel components are active but only one component is needed for success. However, in a repairable system, failed components are repaired only after all parallel components have failed. This is one of the least effective uses of redundancy in terms of improving system reliability.

Two Parallel Components - Active without Repair

We begin again with two components in parallel as shown in Figure 2.1. Suppose both A and B are active but the system requires only one of them for successful operation. Let W_A (W_B) be the event that A (B) fails. Then the failure probability for the simple parallel system of Figure 2.1 is

$$P(W_s) = P(W_A \cap W_B) \quad (3.1)$$

That is, the combination of A and B in parallel fails if both A and B fail. If these events are independent, that is, if the failure or success of either component does not influence the failure or success of the other, then

$$Q_s = Q_A Q_B \quad (3.2)$$

Recall that Q is used to denote probability of failure (unreliability). If R_A and R_B are the reliabilities of A and B, then the probability of system failure is

$$Q_s = (1 - R_A)(1 - R_B) \quad (3.3)$$

The system reliability is given by

$$R_s = 1 - Q_s = 1 - (1 - R_A)(1 - R_B) \quad (3.4)$$

That is, the probability of successful operation of the parallel system over time t is 1 minus the probability that both components fail during t . We will calculate the mean life of the system (mean time to system failure). For a repairable system where the repaired system is as good as new, the mean life is the same as the MTBF. The mean life of the system is given by

$$T_{FS} = \int_0^{\infty} R_S(t) dt = \int_0^{\infty} [1 - Q_{FA}(t)Q_{FB}(t)] dt \quad (3.5)$$

If we assume that components A and B have a constant failure rate given by λ_A and λ_B , then

$$T_{FS} = \int_0^{\infty} [1 - \{(1 - e^{-\lambda_A t})(1 - e^{-\lambda_B t})\}] dt \quad (3.6)$$

and

$$T_{FS} = \frac{1}{\lambda_A} + \frac{1}{\lambda_B} - \frac{1}{\lambda_A + \lambda_B} = T_{FA} + T_{FB} - \left(\frac{1}{T_{FA}} + \frac{1}{T_{FB}} \right)^{-1} \quad (3.7)$$

To calculate the mean time to repair for the two parallel components, first recognize that both must be repaired before the parallel system is considered repaired. Thus, in analogy to Equation (3.5), the mean time to repair is given by

$$T_{RS} = \int_0^{\infty} [1 - Q_{RA}(t)Q_{RB}(t)] dt \quad (3.8)$$

where $Q_{RA}(t)$ is the probability that A is repaired in time interval t and $Q_{RB}(t)$ is defined similarly. In words, the mean time to repair the parallel components is the integral over time of the probability that at least one component is not repaired. Assuming a constant repair rate (let μ be the repair rate), then

$$T_{RS} = \int_0^{\infty} [1 - \{(1 - e^{-\mu_A t})(1 - e^{-\mu_B t})\}] dt \quad (3.9)$$

$$T_{RS} = \frac{1}{\mu_A} + \frac{1}{\mu_B} - \frac{1}{\mu_A + \mu_B} = T_{RA} + T_{RB} - \left(\frac{1}{T_{RA}} + \frac{1}{T_{RB}} \right)^{-1} \quad (3.10)$$

Given MTTR and MTTF, availability can be calculated as

$$\text{Availability} = A = \frac{T_{FS}}{T_{FS} + T_{RS}} \quad (3.11)$$

Comparison of results calculated using Equations (3.7) and (3.10) with numerical simulation results are shown in Table 3.1 for the following case:

$$\begin{array}{ll} T_{FA} = 50 \text{ hr} & T_{RA} = 1 \text{ hr} \\ T_{FB} = 50 \text{ hr} & T_{RB} = 2 \text{ hr} \end{array}$$

	Calculated	Markov Analysis
Availability	0.9698	0.9698
System MTTF (T_{FS})	75 hr	75 hr
System MTTR (T_{RS})	2.3 hr	2.3 hr

Table 3.1 Comparison for Two Components in Parallel, Active without Repair

Three Parallel Components - Active without Repair

For three components in parallel (Figure 2.2),

$$T_{FS} = \int_0^{\infty} R_s(t) dt = \int_0^{\infty} [1 - Q_{FA}(t)Q_{FB}(t)Q_{FC}(t)] dt \quad (3.12)$$

Again assuming constant failure rates,

$$T_{FS} = \int_0^{\infty} \left[1 - \left\{ (1 - e^{-\lambda_A t})(1 - e^{-\lambda_B t})(1 - e^{-\lambda_C t}) \right\} \right] dt \quad (3.13)$$

Expanding the integrand,

$$T_{FS} = \int_0^{\infty} \left(e^{-\lambda_A t} + e^{-\lambda_B t} + e^{-\lambda_C t} - e^{-(\lambda_A + \lambda_B)t} - e^{-(\lambda_A + \lambda_C)t} - e^{-(\lambda_B + \lambda_C)t} + e^{-(\lambda_A + \lambda_B + \lambda_C)t} \right) dt$$

So,

$$T_{FS} = \frac{1}{\lambda_A} + \frac{1}{\lambda_B} + \frac{1}{\lambda_C} - \frac{1}{\lambda_A + \lambda_B} - \frac{1}{\lambda_A + \lambda_C} - \frac{1}{\lambda_B + \lambda_C} + \frac{1}{\lambda_A + \lambda_B + \lambda_C} \quad (3.14)$$

In terms of component MTBF's,

$$T_{FS} = T_{FA} + T_{FB} + T_{FC} - \left[\frac{1}{T_{FA}} + \frac{1}{T_{FB}} \right]^{-1} - \left[\frac{1}{T_{FA}} + \frac{1}{T_{FC}} \right]^{-1} - \left[\frac{1}{T_{FB}} + \frac{1}{T_{FC}} \right]^{-1} + \left[\frac{1}{T_{FA}} + \frac{1}{T_{FB}} + \frac{1}{T_{FC}} \right]^{-1} \quad (3.15)$$

Calculation of system MTTR follows the same steps. That is,

$$T_{RS} = \frac{1}{\mu_A} + \frac{1}{\mu_B} + \frac{1}{\mu_C} - \frac{1}{\mu_A + \mu_B} - \frac{1}{\mu_A + \mu_C} - \frac{1}{\mu_B + \mu_C} + \frac{1}{\mu_A + \mu_B + \mu_C} \quad (3.16)$$

In terms of component MTTR's,

$$T_{RS} = T_{RA} + T_{RB} + T_{RC} - \left[\frac{1}{T_{RA}} + \frac{1}{T_{RB}} \right]^{-1} - \left[\frac{1}{T_{RA}} + \frac{1}{T_{RC}} \right]^{-1} - \left[\frac{1}{T_{RB}} + \frac{1}{T_{RC}} \right]^{-1} + \left[\frac{1}{T_{RA}} + \frac{1}{T_{RB}} + \frac{1}{T_{RC}} \right]^{-1} \quad (3.17)$$

Comparison of results calculated using Equations (3.15) and (3.17) with Markov analysis results are shown in Table 3.2 for the following case:

$T_{FA} = 50$ hr	$T_{RA} = 3$ hr
$T_{FB} = 100$ hr	$T_{RB} = 5$ hr
$T_{FC} = 200$ hr	$T_{RC} = 4$ hr

	Calculated	Markov Analysis
Availability	0.9697	0.9697
System MTTF (T_{FS})	238.6 hr	238.6 hr
System MTTR(T_{RS})	7.47 hr	7.47 hr

Table 3.2 Comparison for Three Components in Parallel, Active without Repair.

N Parallel Components - Active without Repair

Equations (3.15) and (3.17) can be generalized to N components in parallel as follows:

Let CS be the set of all components in the parallel arrangement. Subsets of CS are indicated as $K \subseteq CS$. For example, if A, B, and C are in parallel, CS is {A,B,C} and subsets are {A}, {B}, {C}, {A,B}, {A,C}, {B,C}, and {A,B,C}. Of course, the null set ϕ is also a subset. The number of elements in a set is called its order and is indicated by $|K|$. We generalize the equations for MTTF and MTTR in terms of failure rates and repair rates as in Equations (3.14) and (3.16).

$$T_{FS} = \sum_{\substack{K \subseteq CS \\ K \neq \phi}} \left[(-1)^{(|K|-1)} \frac{1}{\sum_{i \in K} \lambda_i} \right] \quad (3.18)$$

and

$$T_{RS} = \sum_{\substack{K \subseteq CS \\ K \neq \phi}} \left[(-1)^{(|K|-1)} \frac{1}{\sum_{i \in K} \mu_i} \right] \quad (3.19)$$

Comparison of results calculated using Equations (3.18) and (3.19) with Markov analysis are shown in Table 3.3 for the following case:

$T_{F1} = 50 \text{ hr}$	$T_{R1} = 3 \text{ hr}$
$T_{F2} = 100 \text{ hr}$	$T_{R2} = 5 \text{ hr}$
$T_{F3} = 200 \text{ hr}$	$T_{R3} = 4 \text{ hr}$
$T_{F4} = 40 \text{ hr}$	$T_{R4} = 2 \text{ hr}$
$T_{F5} = 30 \text{ hr}$	$T_{R5} = 3 \text{ hr}$

	Calculated	Markov Analysis
Availability	0.9674	0.9674
System MTTF (T_{FS})	242 hr	242 hr
System MTTR(T_{RS})	8.2 hr	8.2 hr

Table 3.3 Comparison for Five Components in Parallel, Active without Repair

Active Redundancy in Non-Repairable Systems

In this case, we are interested in the reliability of active, parallel components when the system cannot be repaired. From Equation (3.4) for two parallel active components,

$$R_s = 1 - Q_s = 1 - (1 - R_A)(1 - R_B) \quad (3.20)$$

For the general case of N components in parallel, we can easily write an equation for the reliability of the parallel assembly. That is

$$R_p = 1 - \prod_{i=1}^N (1 - R_i) \quad (3.21)$$

The implicit assumption in Equation (3.21) is that all parallel components are active with only one required for success. It is clear that parallel system reliability increases as the number of parallel components increases. However, the incremental increase in reliability diminishes with each additional parallel component. Figure 3.1 shows the reliability of parallel systems as a function of the number of identical components for several fixed component reliabilities.

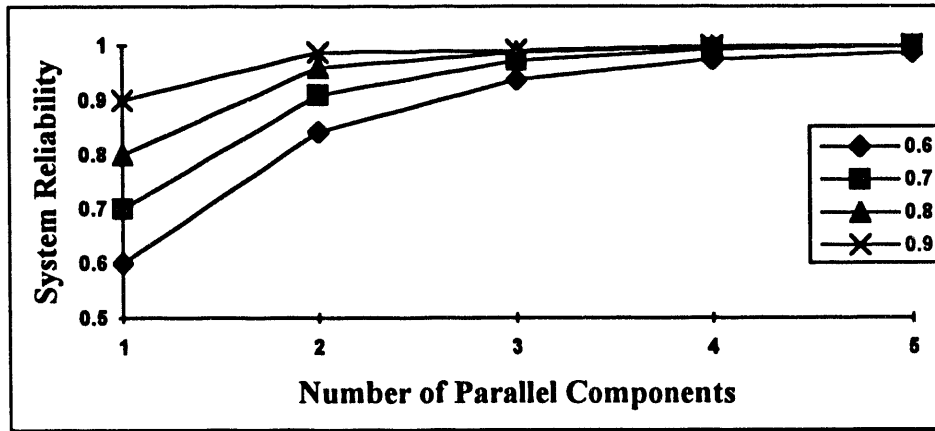


Figure 3.1 Reliability of a Parallel System as a Function of the Number of Components

The number of components needed to achieve high reliability depends on the reliability of the individual components.

Chapter 4

STANDBY WITH REPAIR

Standby redundancy can be designed in a virtually endless variety of forms. The following discussion describes the assumptions used in the treatment presented here.

For standby redundancy, only one component will be active at any time. When that component fails, a standby component can be switched on, either manually or automatically. This standby component will begin working if its switch works. Switch failures are treated as discrete events with known probability of failure (p). In the event of a switch failure, the system will go to the next standby component. Components which are not operable can be repaired at any time. If all of the components are operable at some point, then the first component will begin working again, and the component which was working will resume its role as a standby component. In the event of a system failure, we assume the system remains down until all of the components are operable and the system can return to its initial state.

As an example of this treatment, consider a system with four components. Once the first component fails, we will try to switch to the second component. If the second component's switch fails, then we will try to switch to the third component. If its switch works, then the third component will be working. If the third component fails before the first component is repaired, then the system will try to switch to the fourth component. If its switch works, the fourth component will be working, the second will be operable, and the first and third will both be inoperable. If the first and third components are both repaired before the fourth component fails, then the first component will be the active component again. If the fourth component fails before both the first and the third components are repaired, then the system will fail.

For this redundancy treatment, we have not derived closed form equations. Rather, we will describe an algorithm that can be programmed to produce

accurate results for the assumptions described above. The algorithm presented here traces the system through all of the possible paths by which it can fail. We will first go through the algorithm on systems with 2 and 3 components to show how it works.

Notation

We will let T_{Fi} denote the MTBF for component i , T_{Ri} denote the mean time to repair component i , and p_i be the probability that the switch to component i fails. Assume that T_{Fi} and T_{Ri} are expressed in hours.

To describe a state, we will put a one in the location of components that are operable, and underline the component that is working, e.g., 011 corresponds to the first component being down, the second and third components being operable, and the third component working. If no component is underlined (or working) then the system is down, i.e., 01 corresponds to the second component being operable and the system being down. For the discussion of three components in parallel, we will use superscripts to denote which step or iteration we have just finished.

Two Components in Parallel - Standby with Repair

The system will start with both components operable and the first working (this state is written as 11). When the first component fails, the second component will still be operable but the system may or may not stay up. Thus, the system will go to either 011 or 01 depending on whether the switch for the second component works. Thus, for each of the states we have the transition probabilities in Table 4.1.

State	Probability	Expected hours to reach that state
011	$1 - p_2$	T_{F1}
01	p_2	T_{F1}

Table 4.1. States and Transition Probabilities for a 2 Component System

At state 01, the system has already failed. Thus, we are interested in where the system can go from 01. From 01, the system can go to either 00 or 11 depending on which occurs first - failure of the second component or repair of the first. The probability that the second component fails before the first is repaired is:

$$\begin{aligned}
 & \int_{t=0}^{\infty} P(1 \text{ is not repaired by time } t) P(2 \text{ fails at time } t) dt = \\
 & \int_{t=0}^{\infty} (e^{-\mu_1 t}) (e^{-\lambda_2 t} \lambda_2 dt) = \int_{t=0}^{\infty} \lambda_2 e^{-(\mu_1 + \lambda_2)t} dt = \frac{\lambda_2}{\mu_1 + \lambda_2} \\
 & = \frac{(T_{F2})^{-1}}{(T_{R1})^{-1} + (T_{F2})^{-1}} = \frac{T_{R1}}{T_{R1} + T_{F2}}. \tag{4.1}
 \end{aligned}$$

Similarly, the probability that the first component is repaired before the second fails is

$$\frac{T_{F2}}{T_{R1} + T_{F2}}. \tag{4.2}$$

The expected time until either the second component fails or the first component is repaired is

$$\int_0^{\infty} t e^{-\lambda_2 t} e^{-\mu_1 t} dt / \int_0^{\infty} e^{-\lambda_2 t} e^{-\mu_1 t} dt = \frac{1}{\lambda_2 + \mu_1} = \frac{T_{R1} T_{F2}}{T_{R1} + T_{F2}}. \tag{4.3}$$

This gives us the states and transition probabilities in Table 4.2. Since reaching the state 11 means that the system is reset to the state where it started, the probability of being in state 01 when the system fails is $q_{01}/(q_{00} + q_{01})$ and the probability of being in state 00 when the system fails is $q_{00}/(q_{00} + q_{01})$.

State	Probability	Hours to Reach that State
01	$q_{01} = p_2$	$t_{01} = T_{F1}$
00	$q_{00} = (1 - p_2) \frac{T_{R1}}{T_{R1} + T_{F2}}$	$t_{00} = T_{F1} + \frac{T_{R1} T_{F2}}{T_{R1} + T_{F2}}$
<u>11</u>	$q_{11} = (1 - p_2) \frac{T_{F2}}{T_{R1} + T_{F2}}$	$t_{11} = T_{F1} + \frac{T_{R1} T_{F2}}{T_{R1} + T_{F2}}$

Table 4.2 States and Transition Probabilities for a 2 Component System

The system will return to 11 some number of times before it fails. We will expect it to take a certain amount of time each time the system goes from 11 to 01 and then returns to 11. The more times that the system goes through this cycle, the more time will elapse before the system fails. So, if we let B_i be the event that system goes back to the state 11 i times (we do not count the system's starting there as a time that it goes there) and then fails to state 01, then all of the B_i 's are disjoint, and their union is the event that the system fails to state 01. Then the expected time for the system to fail via state 01 is

$$\begin{aligned}
 E(\text{time to fail} \mid \text{fail to 01}) &= \frac{\sum_{i=0}^{\infty} P(B_i) P(01|B_i) E(\text{time until 01}|B_i)}{\sum_{i=0}^{\infty} P(B_i) P(01|B_i)} \\
 &= \frac{\sum_{i=0}^{\infty} (q_{11}^i q_{01}) (i t_{11} + t_{01})}{\sum_{i=0}^{\infty} (q_{11}^i q_{01})} \\
 E(\text{time to fail} \mid \text{fail to 01}) &= \frac{q_{01} \left[\frac{1}{(1 - q_{11})^2} - \frac{1}{1 - q_{11}} \right] t_{11} + q_{01} \left[\frac{1}{1 - q_{11}} \right] t_{01}}{\frac{q_{01}}{1 - q_{11}}}
 \end{aligned}$$

$$E(\text{time to fail} \mid \text{fail to } 01) = \left(\frac{1}{1 - q_{11}} - 1 \right) t_{11} + t_{01} \quad (4.4)$$

Similarly, if the system is in state 00 when it fails, then the expected time until it fails is

$$\begin{aligned} E(\text{time to fail} \mid \text{fail to } 00) &= \frac{\sum_{i=0}^{\infty} P(B_i) P(00 \mid B_i) E(\text{time until } 00 \mid B_i)}{\sum_{i=0}^{\infty} P(B_i) P(00 \mid B_i)} \\ &= \frac{\sum_{i=0}^{\infty} (q_{11}^i q_{00}) (i t_{11} + t_{00})}{\sum_{i=0}^{\infty} (q_{11}^i q_{00})} \\ &= \frac{q_{00} \left[\frac{1}{(1 - q_{11})^2} - \frac{1}{1 - q_{11}} \right] t_{11} + q_{00} \left[\frac{1}{1 - q_{11}} \right] t_{00}}{\frac{q_{00}}{1 - q_{11}}} \end{aligned}$$

$$E(\text{time to fail} \mid \text{fail to } 00) = \left(\frac{1}{1 - q_{11}} - 1 \right) t_{11} + t_{00} \quad (4.5)$$

Now, since we know the probability of being in each state when the system fails, and the expected time for the system to fail conditioned on it failing to each state, we can find the expected time until the system fails. In this case, it would be

$$T_{FS} = \frac{q_{00} \left[\left(\frac{1}{1 - q_{11}} - 1 \right) t_{11} + t_{00} \right] + q_{01} \left[\left(\frac{1}{1 - q_{11}} - 1 \right) t_{11} + t_{01} \right]}{q_{00} + q_{01}}$$

$$T_{FS} = \left[\frac{1}{1 - q_{11}} - 1 \right] t_{11} + \frac{q_{00}t_{00} + q_{01}t_{01}}{q_{00} + q_{01}} \quad (4.6)$$

We stated earlier that the ratios $q_{01}/(q_{00} + q_{01})$ and $q_{00}/(q_{00} + q_{01})$ are the probabilities of being in state 01 and 00, respectively, when the system fails. These are conditional probabilities: given the system fails, these are the probabilities of being in state 01 and 00. The conditional probabilities were used in Equation (4.6) to find the expected time to system failure. They are also used to find the expected time to repair the system.

If the system fails to 01, then only the first component requires repair. If it fails to 00, then both components must be repaired. Thus, the expected repair time is

$$T_{RS} = \frac{q_{01}}{q_{00} + q_{01}} T_{R1} + \frac{q_{00}}{q_{00} + q_{01}} T_{R(12)} \quad (4.7)$$

where $T_{R(12)}$ can be found from Equation (3.10), or in its more general form, Equation (3.19).

Comparison of results calculated using Equations (4.6) and (4.7) with Markov analysis results are shown in Table 4.3 for the following case:

$$\begin{array}{lll} T_{FA} = 200 \text{ hr} & T_{RA} = 10 \text{ hr} & \\ T_{FB} = 500 \text{ hr} & T_{RB} = 20 \text{ hr} & p_B = 0.01 \end{array}$$

	Calculated	Markov Analysis
Availability	0.9974	0.9974
System MTBF (T_{FS})	7130 hr	7130 hr
System MTTR (T_{RS})	18.8 hr	18.8 hr

Table 4.3 Comparison for Two Components in Parallel, Standby with Repair.

For the case of two parallel components shown in Table 4.3, the comparison of Equations (4.6) and (4.7) with Markov analysis is excellent.

Three Components in Parallel - Standby with Repair

The approach for three components is similar to that presented in the previous section for two components. When the first component fails, the system can go to any of three states: $0\bar{1}1$, $01\bar{1}$, or 011 . For these states, we have the results shown in Table 4.4.

State	Probability	Hours to Reach that State
$0\bar{1}1$	$q_{0\bar{1}1} = 1 - p_2$	$t_{0\bar{1}1} = T_{F1}$
$01\bar{1}$	$q_{01\bar{1}} = p_2(1 - p_3)$	$t_{01\bar{1}} = T_{F1}$
011	$q_{011} = p_2 p_3$	$t_{011} = T_{F1}$

Table 4.4 States and Transition Probabilities for a 3 Component System

If the system is in state $0\bar{1}1$, and the first component is repaired before the second component fails, then the system is reset to $\bar{1}11$. If we consider Equation 4.2, then we see that the probability of this is:

$$\frac{\mu_1}{\mu_1 + \lambda_2} = \frac{T_{F2}}{T_{R1} + T_{F2}}. \quad (4.8)$$

If the second component fails before the first component is repaired (see Equation (4.1), then the system will go to state $00\bar{1}$ or state 001 , with probabilities

$$P_{00\bar{1}} = \frac{T_{R1}}{T_{R1} + T_{F2}} (1 - p_3) \quad (4.9)$$

$$P_{001} = \frac{T_{R1}}{T_{R1} + T_{F2}} p_3 \quad (4.10)$$

If we consider Equation (4.3), then we realize that the time required to reach one of these three states from 011 is

$$\frac{T_{R1}T_{F2}}{T_{R1} + T_{F2}}. \quad (4.11)$$

Thus if we wait until the first component has failed, and either the first component has been repaired or the second component is not working (because it has failed or its switch failed) then the possible states are shown in Table 4.5.

State	Probability	Hours to Reach that State
<u>111</u>	$q_{111}^2 = q_{011}^1 \frac{T_{F2}}{T_{R1} + T_{F2}}$	$t_{111}^2 = T_{F1} + \frac{T_{R1}T_{F2}}{T_{R1} + T_{F2}}$
00 <u>1</u>	$q_{001}^2 = q_{011}^1 \frac{T_{R1}}{T_{R1} + T_{F2}} (1 - p_3)$	$t_{001}^2 = T_{F1} + \frac{T_{R1}T_{F2}}{T_{R1} + T_{F2}}$
001	$q_{001}^2 = q_{011}^1 \frac{T_{R1}}{T_{R1} + T_{F2}} p_3$	$t_{001}^2 = T_{F1} + \frac{T_{R1}T_{F2}}{T_{R1} + T_{F2}}$
01 <u>1</u>	$q_{011}^2 = q_{011}^1$	$t_{011}^2 = T_{F1}$
011	$q_{011}^2 = q_{011}^1$	$t_{011}^2 = T_{F1}$

Table 4.5 States and Transition Probabilities for a 3 Component System

We are interested in the system failing, so we want to know whether the system will get to 001, 001, 011, or 011 first, and how long it will take to get there. Recall our assumption that when the system fails, we require that all failed components be repaired before the system is placed back in operation. Since going to 111 means that the system is reset to the state which it started in, it is possible to find both the probabilities and expected time to reach these states. To find the probabilities that the system hits one of those states before the other three, we will divide the probability of that state by the sum of the probabilities of all four states. To find the expected time to reach that state, we will do calculations analogous to those leading to Equation 4.4. This will give us the results in Table 4.6.

001 and 011 are the only states in the table where the system has not already failed. Thus, we are interested in where the system can go from those two states. From 001, the system can go to 111, 100, 010, 000, with probabilities:

State	Probability	Hours to Reach that State
00 <u>1</u>	$q_{001}^3 = \frac{q_{001}^2}{1 - q_{111}^2}$	$t_{001}^3 = \left[\frac{1}{1 - q_{111}^2} - 1 \right] t_{111}^2 + t_{001}^2$
001	$q_{001}^3 = \frac{q_{001}^2}{1 - q_{111}^2}$	$t_{001}^3 = \left[\frac{1}{1 - q_{111}^2} - 1 \right] t_{111}^2 + t_{001}^2$
01 <u>1</u>	$q_{011}^3 = \frac{q_{011}^2}{1 - q_{111}^2}$	$t_{011}^3 = \left[\frac{1}{1 - q_{111}^2} - 1 \right] t_{111}^2 + t_{011}^2$
011	$q_{011}^3 = \frac{q_{011}^2}{1 - q_{111}^2}$	$t_{011}^3 = \left[\frac{1}{1 - q_{111}^2} - 1 \right] t_{111}^2 + t_{011}^2$

Table 4.6 States and Transition Probabilities for a 3 Component System

$$\begin{aligned}
 P_{111|001} &= P_{111 \text{ through } 011|001} + P_{111 \text{ through } 101|001} \\
 &= \frac{T_{R1} T_{F3}}{T_{R1} T_{F3} + T_{R2} T_{F3} + T_{R1} T_{R2}} \frac{T_{F3}}{T_{R1} + T_{F3}} \\
 &\quad + \frac{T_{R2} T_{F3}}{T_{R1} T_{F3} + T_{R2} T_{F3} + T_{R1} T_{R2}} \frac{T_{F3}}{T_{R2} + T_{F3}}
 \end{aligned} \tag{4.12a}$$

$$P_{100|001} = \frac{T_{R2} T_{F3}}{T_{R1} T_{F3} + T_{R2} T_{F3} + T_{R1} T_{R2}} \frac{T_{R2}}{T_{R2} + T_{F3}} \tag{4.12b}$$

$$P_{010|001} = \frac{T_{R1} T_{F3}}{T_{R1} T_{F3} + T_{R2} T_{F3} + T_{R1} T_{R2}} \frac{T_{R1}}{T_{R1} + T_{F3}} \tag{4.12c}$$

$$P_{000|001} = \frac{T_{R1}T_{R2}}{T_{R1}T_{F3} + T_{R2}T_{F3} + T_{R1}T_{R2}} \quad (4.12d)$$

From 011 the system can go to 111 or 010 with probabilities:

$$P_{111|011} = \frac{T_{F3}}{T_{F3} + T_{R1}} \quad (4.13)$$

and

$$P_{010|011} = \frac{T_{R1}}{T_{F3} + T_{R1}} \quad (4.14)$$

Thus, if we wait until the either the third component has failed or its switch has failed, then the possible states are as shown in Table 4.7.

When the system fails, it can be in 000, 001, 010, 011, or 100. For these five possible states, we have the transition probabilities shown in Table 4.8.

Now, the expected time until the system fails will be

$$T_{FS} = q_{000}^5 t_{000}^5 + q_{001}^5 t_{001}^5 + q_{010}^5 t_{010}^5 + q_{011}^5 t_{011}^5 + q_{100}^5 t_{100}^5 \quad (4.15)$$

From each of these 5 states we can calculate the average repair time to go from the failed state to state 111 using Equation (3.19). Given that the system fails, the probability of being in each of these 5 states is the conditional probability for the state. For example, q_{000}^5 is the probability of being in state 000 when the system fails, given that it fails. The expected time to repair the system is then the sum of the five products of conditional probability and average repair time.

Comparison of results calculated using the approach above with Markov analysis results are shown in Table 4.9 for the following case:

$T_{FA} = 300 \text{ hr}$	$T_{RA} = 15 \text{ hr}$	
$T_{FB} = 1000 \text{ hr}$	$T_{RB} = 20 \text{ hr}$	$p_B = 0.01$
$T_{FC} = 700 \text{ hr}$	$T_{RC} = 5 \text{ hr}$	$p_C = 0.05$

State	Probability	Hours to Reach that State
000	$q_{000}^4 = p_{000 001} q_{001}^3$	$t_{000}^4 = t_{001}^3 + \frac{T_{R1} T_{R2} T_{F3}}{T_{R1} T_{R2} + T_{R1} T_{F3} + T_{R2} T_{F3}}$
001	$q_{001}^4 = q_{001}^3$	$t_{001}^4 = t_{001}^3$
010	$q_{010}^4 = p_{010 011} q_{011}^3 + p_{010 001} q_{001}^3$	$t_{010}^4 = \frac{p_{010 011} q_{011}^3}{q_{010}^4} \left[t_{011}^3 + \frac{T_{R1} T_{F3}}{T_{R1} + T_{F3}} \right] + \frac{p_{010 001} q_{001}^3}{q_{010}^4} \times \left[t_{001}^3 + \frac{T_{R1} T_{R2} T_{F3}}{T_{R1} T_{R2} + T_{R1} T_{F3} + T_{R2} T_{F3}} + \frac{T_{R1} T_{F3}}{T_{R1} + T_{F3}} \right]$
011	$q_{011}^4 = q_{011}^3$	$t_{011}^4 = t_{011}^3$
100	$q_{100}^4 = p_{100 001} q_{001}^3$	$t_{100}^4 = t_{001}^3 + \frac{T_{R1} T_{R2} T_{F3}}{T_{R1} T_{R2} + T_{R1} T_{F3} + T_{R2} T_{F3}} + \frac{T_{R2} T_{F3}}{T_{R2} + T_{F3}}$
111	$q_{111}^4 = p_{111 001} q_{001}^3 + p_{111 011} q_{011}^3$	$t_{111}^4 = \frac{p_{111 011} q_{011}^3}{q_{111}^4} \left[t_{011}^3 + \frac{T_{R1} T_{F3}}{T_{R1} + T_{F3}} \right] + \frac{p_{111 \text{ through } 011 001} q_{001}^3}{q_{111}^4} \left[t_{001}^3 + \frac{T_{R1} T_{R2} T_{F3}}{T_{R1} T_{F3} + T_{R2} T_{F3} + T_{R1} T_{R2}} + \frac{T_{R1} T_{F3}}{T_{R1} + T_{F3}} \right] + \frac{p_{111 \text{ through } 101 001} q_{001}^3}{q_{111}^4} \left[t_{001}^3 + \frac{T_{R1} T_{R2} T_{F3}}{T_{R1} T_{F3} + T_{R2} T_{F3} + T_{R1} T_{R2}} + \frac{T_{R2} T_{F3}}{T_{R2} + T_{F3}} \right]$

Table 4.7 States and Transition Probabilities for a 3 Component System

State	Probability	Hours to Reach that State
000	$q_{000}^5 = \frac{q_{000}^4}{1 - q_{111}^4}$	$t_{000}^5 = \left[\frac{1}{1 - q_{111}^4} - 1 \right] t_{111}^4 + t_{000}^4$
001	$q_{001}^5 = \frac{q_{001}^4}{1 - q_{111}^4}$	$t_{001}^5 = \left[\frac{1}{1 - q_{111}^4} - 1 \right] t_{111}^4 + t_{001}^4$
010	$q_{010}^5 = \frac{q_{010}^4}{1 - q_{111}^4}$	$t_{010}^5 = \left[\frac{1}{1 - q_{111}^4} - 1 \right] t_{111}^4 + t_{010}^4$
011	$q_{011}^5 = \frac{q_{011}^4}{1 - q_{111}^4}$	$t_{011}^5 = \left[\frac{1}{1 - q_{111}^4} - 1 \right] t_{111}^4 + t_{011}^4$
100	$q_{100}^5 = \frac{q_{100}^4}{1 - q_{111}^4}$	$t_{100}^5 = \left[\frac{1}{1 - q_{111}^4} - 1 \right] t_{111}^4 + t_{100}^4$

Table 4.8 States and Transition Probabilities for a 3 Component System

	Calculated	Markov Analysis
Availability	0.99987	0.99987
System MTBF (T_{FS})	162406 hr	162406 hr
System MTTR (T_{RS})	21.2 hr	21.2 hr

Table 4.9 Comparison for Three Components in Parallel, Standby with Repair.

As in the case of two components, standby with repair, the case of 3 components shows excellent comparison with Markov analysis.

We have only presented the algorithm for standby with repair for the cases of two and three components in parallel. However, a general algorithm for standby with repair has been developed and is described in Appendix A.

Chapter 5

STANDBY WITHOUT REPAIR

In this treatment of redundancy, only one of the redundant components is assumed to be active with others held in standby. In case the active component fails, a standby component can be switched on either manually or automatically. Failed components are not repaired until all have failed and the system is down.

The MTTF of the system of 1 component active with $N - 1$ standby without repair is just the sum of the individual MTBF's of the components accounting for the probability of switch failure. That is

$$T_{FS} = T_1 + \sum_{i=2}^N (1 - p_i) T_{Fi} \quad (5.1)$$

No repairs are performed until all standby components or their switches have failed. Therefore, the MTTR for the system is calculated similarly as for N active without repair. Let $P_1(t)$ be the probability that component 1 is repaired (not failed) at time t and $P_2(t)$ is defined similarly. Then from Equation (3.8),

$$T_{RS} = \int_0^{\infty} [1 - Q_{R1}(t) Q_{R2}(t)] dt. \quad (5.2)$$

In words, the mean time to repair the parallel components is the integral over time of the probability that at least one component is not repaired. Recall that if a component is not operable, it could be because the component itself failed or its switch failed. If the component is unavailable because of switch failure, then the component doesn't need to be repaired. Assuming a constant repair rate (let μ denote repair rate), then

$$T_{RS} = \int_0^{\infty} \left\{ 1 - \left[p_1 + (1 - p_1) \left(1 - e^{-\mu t} \right) \right] \left[p_2 + (1 - p_2) \left(1 - e^{-\mu t} \right) \right] \right\} dt \quad (5.3)$$

where p_1 and p_2 are the probabilities of switch failure to components 1 and 2. Note that ($p_1 = 0$). Equation 5.3 can be rewritten as

$$T_{RS} = \int_0^{\infty} \left[1 - \left\{ 1 - (1 - p_1)e^{-\mu_1 t} \right\} \left[1 - (1 - p_2)e^{-\mu_2 t} \right] \right] dt. \quad (5.4)$$

From Equation (3.10), we see that the solution to Equation (5.4) is

$$T_{RS} = \frac{(1 - p_1)}{\mu_1} + \frac{(1 - p_2)}{\mu_2} - \frac{(1 - p_1)(1 - p_2)}{\mu_1 + \mu_2}. \quad (5.5)$$

By the same arguments that lead to Equation (3.19), we can show that

$$T_{RS} = \sum_{\substack{K \subseteq CS \\ K \neq \phi}} \left[(-1)^{(|K|-1)} \frac{\prod_i (1 - p_i)}{\sum_{i \in K} \mu_i} \right] \quad (5.6)$$

where $p_1 = 0$.

The comparison calculations that were performed earlier for standby with repair are repeated here for standby without repair. The case for two components follows.

$$\begin{array}{lll} T_{FA} = 200 \text{ hr} & T_{RA} = 10 \text{ hr} & \\ T_{FB} = 500 \text{ hr} & T_{RB} = 20 \text{ hr} & p_B = 0.01 \end{array}$$

	Calculated	Markov Analysis
Availability	0.9677	0.9677
System MTBF (T_{FS})	695 hr	695 hr
System MTTR (T_{RS})	23.2 hr	23.2 hr

Table 5.1 Comparison for Two Components in Parallel, Standby without Repair.

Table 5.2 shows comparison results for 3 in parallel, standby without repair, with the following properties

$$\begin{array}{lll}
 T_{FA} = 300 \text{ hr} & T_{RA} = 15 \text{ hr} & \\
 T_{FB} = 1000 \text{ hr} & T_{RB} = 20 \text{ hr} & p_B = 0.01 \\
 T_{FC} = 700 \text{ hr} & T_{RC} = 5 \text{ hr} & p_C = 0.05
 \end{array}$$

	Calculated	Markov Analysis
Availability	0.9865	0.9865
System MTBF (T_{FS})	1955 hr	1955 hr
System MTTR (T_{RS})	26.7 hr	26.7 hr

Table 5.2 Comparison for Three Components in Parallel, Standby without Repair.

For both cases, the Equations (5.1) and (5.6) provide excellent agreement with Markov analysis results.

Standby Redundancy in Non-Repairable Systems

With standby redundancy, we consider a single active component with 1 or more (not necessarily identical) components available in standby. In case the active component fails, the system switches either manually or automatically to a standby component. In general, there is a non-zero probability that the switching mechanism will not be successful in activating the standby component. If there is more than one standby component available, component failure (either the component itself or its activation mechanism) will cause the system to switch to the next available standby component. Standby redundancy is fairly common in electrical and electronic systems. For example, many home security systems have a standby battery available in case of failure of the external power supply.

One Active and One Standby Component

We begin by considering a system consisting of one active component with one component in standby ready to be activated if the active component fails. Let p_2 be the probability that the standby component fails to activate on demand. Assume that the two components have constant failure rates λ_1 and λ_2 . The probability of successful operation over some mission time T for the system is the sum of the probabilities of two mutually exclusive events. That is

R_S = Probability that component 1 operates successfully over time T

+ Probability that component 1 fails before T and component 2 operates successfully for the remainder of T

$$R_S = R_1 + \int_0^T e^{-\lambda_1 t} \lambda_1 (1 - p_2) e^{-\lambda_2 (T-t)} dt \quad (5.7)$$

where

R_1 is the probability of successful operation of component 1 over the mission time T,

$e^{-\lambda_1 t} \lambda_1 dt$ is the probability that component 1 survives to time t ($e^{-\lambda_1 t}$) then fails during interval dt ($\lambda_1 dt$),

$1 - p_2$ is the probability that component 2 is successfully activated, and

$e^{-\lambda_2 (T-t)}$ is the probability that component 2 operates successfully from t until T.

Then

$$R_S = R_1 + \lambda_1 (1 - p_2) e^{-\lambda_2 T} \int_0^T e^{(\lambda_2 - \lambda_1)t} dt \quad (5.8)$$

Performing the integral in Equation (5.8) gives

$$R_S = R_1 + \frac{\lambda_1}{\lambda_2 - \lambda_1} (1 - p_2) e^{-\lambda_2 T} (e^{(\lambda_2 - \lambda_1)T} - 1)$$

$$R_S = R_1 + \frac{\lambda_1}{\lambda_2 - \lambda_1} (1 - p_2) (R_1 - R_2), \quad \lambda_1 \neq \lambda_2 \quad (5.9)$$

For the case of perfect switching ($p_2 = 0$),

$$R_S = \frac{\lambda_2 R_1}{\lambda_2 - \lambda_1} + \frac{\lambda_1 R_2}{\lambda_1 - \lambda_2}, \quad \lambda_1 \neq \lambda_2, \quad p_2 = 0 \quad (5.10)$$

where $R_1 = e^{-\lambda_1 T}$.

Equation (5.10) is clearly only valid if $\lambda_1 \neq \lambda_2$. Using Equation (3.5), we can calculate the mean time to failure as

$$\begin{aligned}
 T_F &= \int_0^{\infty} R(t) dt \\
 T_F &= \int_0^{\infty} \left\{ e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_2 - \lambda_1} (1 - p_2) (e^{-\lambda_1 t} - e^{-\lambda_2 t}) \right\} dt \\
 T_F &= \frac{1}{\lambda_1} + \frac{\lambda_1}{\lambda_2 - \lambda_1} (1 - p_2) \left(\frac{1}{\lambda_1} - \frac{1}{\lambda_2} \right) \\
 T_F &= \frac{1}{\lambda_1} + \frac{1 - p_2}{\lambda_2}, \quad \lambda_1 \neq \lambda_2
 \end{aligned} \tag{5.11}$$

Equation (5.11) is the same as Equation (5.1) applied to two components and is easily interpreted. The mean time to first failure of the redundant system consisting of component 1 with component 2 in standby is the MTTF of component 1 plus the MTTF of component 2 weighted by the probability of component 2 being successfully activated.

In case the two components have the same failure rates, we need to return to Equation (5.8) to determine the reliability. Let $\lambda_1 = \lambda_2 = \lambda$. Then

$$\begin{aligned}
 R_s &= e^{-\lambda T} + \lambda(1 - p_2) \int_0^T dt \\
 R_s &= e^{-\lambda T} [1 + \lambda T(1 - p_2)], \quad \lambda_1 = \lambda_2 = \lambda
 \end{aligned} \tag{5.12}$$

In this case the mean time to failure is

$$T_F = \int_0^{\infty} e^{-\lambda T} [1 + \lambda T(1 - p_2)] dt \tag{5.13}$$

$$T_F = \frac{1}{\lambda} + \lambda(1 - p_2) \frac{1}{\lambda^2} \tag{5.14}$$

$$T_F = \frac{2 - p_2}{\lambda}, \quad \lambda_1 = \lambda_2 = \lambda \quad (5.15)$$

One Active and Two Standby Components

We now consider the case of one active component with two in standby. If component 1 fails, component 2 is switched on. If component 2 fails, component 3 is switched on. The probabilities of failing to successfully activate components 2 and 3 are p_2 and p_3 . We begin with the case $\lambda_1 \neq \lambda_2 \neq \lambda_3$. The reliability of the system is the sum of the probabilities of the following 4 mutually exclusive events:

1. Component 1 operates successfully for the entire mission time T .
2. Component 1 fails at $t < T$, component 2 is successfully activated and operates for the remainder of the mission time.
3. Component 1 fails at $t < T$, component 2 fails to activate, component 3 is successfully activated and operates for the remainder of the mission time.
4. Component 1 fails at $t' < T$, component 2 is successfully activated and operates until time t ($t' < t < T$), component 3 is successfully activated and operates for the remainder of the mission time.

In equation form,

$$\begin{aligned} R_s = & e^{-\lambda_1 T} + \int_0^T e^{-\lambda_1 t} \lambda_1 (1 - p_2) e^{-\lambda_2 (T-t)} dt \\ & + \int_0^T e^{-\lambda_1 t} \lambda_1 p_2 (1 - p_3) e^{-\lambda_3 (T-t)} dt \\ & + \int_0^T \int_{t'}^T e^{-\lambda_1 t'} \lambda_1 (1 - p_2) e^{-\lambda_2 (t-t')} \lambda_2 (1 - p_3) e^{-\lambda_3 (T-t)} dt dt' \end{aligned} \quad (5.16)$$

Rearranging terms and performing integrals, we get

$$\begin{aligned}
 R_s = & e^{-\lambda_1 T} + \lambda_1(1-p_2)e^{-\lambda_2 T} \left(\frac{e^{-(\lambda_2-\lambda_1)T} - 1}{\lambda_2 - \lambda_1} \right) \\
 & + \lambda_1 p_2(1-p_3)e^{-\lambda_3 T} \left(\frac{e^{-(\lambda_3-\lambda_1)T} - 1}{\lambda_3 - \lambda_1} \right) \\
 & + \lambda_1(1-p_2)\lambda_2(1-p_3)e^{-\lambda_3 T} \int_0^T e^{-(\lambda_2-\lambda_1)t'} \frac{(e^{-(\lambda_3-\lambda_2)T} - e^{-(\lambda_3-\lambda_2)t'})}{\lambda_3 - \lambda_2} dt
 \end{aligned} \tag{5.17}$$

Finally,

$$\begin{aligned}
 R_s = & R_1 + \lambda_1(1-p_2) \left(\frac{R_1 - R_2}{\lambda_2 - \lambda_1} \right) \\
 & + \lambda_1 p_2(1-p_3) \left(\frac{R_1 - R_3}{\lambda_3 - \lambda_1} \right) \\
 & + \frac{\lambda_1 \lambda_2 (1-p_2)(1-p_3)}{\lambda_3 - \lambda_2} \left(\frac{R_1 - R_2}{\lambda_2 - \lambda_1} - \frac{R_1 - R_3}{\lambda_3 - \lambda_1} \right), \lambda_1 \neq \lambda_2 \neq \lambda_3
 \end{aligned} \tag{5.18}$$

For perfect switching ($p_2 = p_3 = 0$), Equation (5.18) becomes

$$\begin{aligned}
 R_s = & \frac{\lambda_2 \lambda_3 R_1}{(\lambda_2 - \lambda_1)(\lambda_3 - \lambda_1)} + \frac{\lambda_1 \lambda_3 R_2}{(\lambda_1 - \lambda_2)(\lambda_3 - \lambda_2)} \\
 & + \frac{\lambda_1 \lambda_2 R_3}{(\lambda_1 - \lambda_3)(\lambda_2 - \lambda_3)}, \lambda_1 \neq \lambda_2 \neq \lambda_3
 \end{aligned} \tag{5.19}$$

where $R_i = e^{-\lambda_i T}$.

In case two or more of the parallel components have the same failure rates, we can readily derive equations for the system reliability beginning with Equation (5.16). Equations for the various combinations of equal failure rates are given below.

$\lambda_1 = \lambda_2 \equiv \lambda_{1,2} \neq \lambda_3$ $R_1 = R_2 \equiv R_{1,2}$	$R_s = R_{1,2} + \lambda_{1,2} T R_{1,2} (1 - p_2) + \lambda_{1,2} p_2 (1 - p_3) \frac{R_{1,2} - R_3}{\lambda_3 - \lambda_{1,2}}$ $+ \frac{\lambda_{1,2}^2 (1 - p_2)(1 - p_3)}{\lambda_3 - \lambda_{1,2}} \left[R_{1,2} T - \frac{R_{1,2} - R_3}{\lambda_3 - \lambda_{1,2}} \right]$	(5.20)
$\lambda_1 = \lambda_3 \equiv \lambda_{1,3} \neq \lambda_2$ $R_1 = R_3 \equiv R_{1,3}$	$R_s = R_{1,3} + \lambda_{1,3} (1 - p_2) \left[\frac{R_{1,3} - R_2}{\lambda_2 - \lambda_{1,3}} \right] + \lambda_{1,3} p_2 (1 - p_3) R_{1,3} T$ $+ \frac{\lambda_{1,3} \lambda_2 (1 - p_2)(1 - p_3)}{\lambda_{1,3} - \lambda_2} \left[\frac{R_{1,3} - R_2}{\lambda_2 - \lambda_{1,3}} - R_{1,3} T \right]$	(5.21)
$\lambda_1 \neq \lambda_2 = \lambda_3 \equiv \lambda_{2,3}$ $R_2 = R_3 \equiv R_{2,3}$	$R_s = R_1 + \lambda_1 (1 - p_2) \left[\frac{R_1 - R_{2,3}}{\lambda_{2,3} - \lambda_1} \right] + \lambda_1 p_2 (1 - p_3) \left[\frac{R_1 - R_{2,3}}{\lambda_{2,3} - \lambda_1} \right]$ $+ \frac{\lambda_1 \lambda_{2,3} (1 - p_2)(1 - p_3)}{\lambda_{2,3} - \lambda_1} \lambda_{2,3} T$	(5.22)
$\lambda_1 = \lambda_2 = \lambda_3 \equiv \lambda$ $R_1 = R_2 = R_3 \equiv R$	$R_s = R + \lambda (1 - p_2) R T + \lambda p_2 (1 - p_3) R T$ $+ \frac{\lambda^2 T^2}{2} (1 - p_2)(1 - p_3)$	(5.23)

One Active and N - 1 Standby Components

We can now develop the general case (1 active component and N-1 in standby) for unequal failure rates. Initially component 1 (C_1) is active and C_2, C_3, \dots, C_N are on sequential standby. Let

p_i = probability that the switch to component C_i fails, $p_1 = 0$

λ_i = the (constant) failure rate for component C_i , and

T = the mission time.

Find the reliability over time T .

There are several ways the configuration can survive over T . For example, C_1 can survive the entire mission time. Or C_1 can fail prior to T , the switch to the C_2 can fail, the switch to C_3 can operate, and C_3 survives the remainder of the

mission time T . We will determine all possible ways the configuration can survive, find the probability of each, and find the sum of all the probabilities.

Let S be the union of the set $\{C_1\}$ and any subset of $\{C_2, C_3, \dots, C_N\}$ and let L be the index of the last component in S (the component with the largest index). Given the following interpretation of S , S represents a combination of occurrences that enables the configuration to survive to time T ;

- Each component C_j in S , $j < L$, is sequentially accessed and then fails during time T
- Component C_L is accessed last and survives the time remaining to T .

A natural outcome of this formulation is that the switch to component C_j operates for each C_j in S , $j > 1$. If there are components with index less than L that are not in the set S , they were not accessed, so we conclude that their switches failed.

The probability (P_s) that the configuration survives to time T through the path defined by set S , is found for each possible set S . Since all paths defined by the sets S are mutually exclusive, the reliability of the configuration, R , is then found by summing over all possible sets S .

$$R = \sum_s P_s \quad (5.24)$$

The remaining problem is to find P_s . Define any sequence of times

$$0 = t_0 < t_1 < \dots < t_n = T$$

where n is the number of components in S . Suppose that component S_1 survived from t_0 to t_1 , S_2 survived from t_1 to t_2 , ..., and S_n survived from t_{n-1} to t_n , where S_k is used to denote component k of set S . Since the failure rate for each component is assumed to be constant, the probability that component k survives over time interval $t_k - t_{k-1}$ and then fails during infinitesimal time dt_k about t_k is

$$e^{-\lambda_k(t_k - t_{k-1})} \lambda_k dt_k \quad (5.25)$$

Note that for $k = n$, the factor $\lambda_k dt_k$ does not appear since the last component does not fail prior to time T . The probability of S can be found by summing over all possible time sequences. That is, form the nested integral of the product of the above factors and integrate sequentially over $(0, t_2)$, $(0, t_3)$, ..., $(0, T)$.

From the integrand we can factor out the failure rates and combine their product with the appropriate product of switch failure probabilities. The resulting factor appears outside the integral and has the form

$$\prod_{\substack{i \in S \\ i < L}} \lambda_i \prod_{j \in S} (1 - p_j) \prod_{\substack{k \notin S \\ k < L}} p_k \quad (5.26)$$

The first product is over all components in S except that $i < L$ (the largest component index in S). The second product is over all components in S indicating that, by definition, there is no switch failure for components in the set. The third product is over all components not in S with index $< L$ indicating that these components are assumed not in S because of switch failure.

The integral can be solved analytically. The only complication is the potential for singularities. Factoring out $e^{-\lambda_n T} \equiv R_n$, we are left with the product

$$e^{-(\lambda_1 - \lambda_2)t_1} dt_1 e^{-(\lambda_2 - \lambda_3)t_2} dt_2 \dots e^{-(\lambda_{n-1} - \lambda_n)t_{n-1}} dt_{n-1} \quad (5.27)$$

If all the λ_i are distinct, then integrating the above expression over $(0, t_2)$, $(0, t_3)$, ..., $(0, T)$ yields

$$\sum_{j \in S} \frac{R_j}{\prod_{\substack{k \in S \\ k \neq j}} (\lambda_k - \lambda_j)} \quad (5.28)$$

Finally,

$$P_S = \prod_{\substack{i \in S \\ i < L}} \lambda_i \prod_{j \in S} (1 - p_j) \prod_{\substack{k \notin S \\ k < L}} p_k \left(\sum_{\substack{i \in S \\ m \in S \\ m \neq i}} \frac{R_i}{\prod_{m \in S} (\lambda_m - \lambda_i)} \right) \quad (5.29)$$

From Equations (5.24) and (5.29), we can now write the equation for the reliability of a system consisting of 1 active component with N - 1 in standby. That is

$$R = \sum_s P_s = \sum_s \left(\prod_{\substack{l \in S \\ l < L}} \lambda_l \prod_{j \in S} (1 - p_j) \prod_{\substack{k \in S \\ k < L}} p_k \left(\sum_{\substack{l \in S \\ m \in S \\ m \neq l}} \frac{R_l}{\prod_{m \in S} (\lambda_m - \lambda_l)} \right) \right) \quad (5.30)$$

For the case of different failure rates and perfect switching we can write the general equation beginning with Equations (5.10) and (5.19),

$$R_s = \sum_{i=1}^N \frac{R_i \left(\prod_{\substack{j=1 \\ j \neq i}}^N \lambda_j \right)}{\prod_{\substack{k=1 \\ k \neq i}}^N (\lambda_k - \lambda_i)}, \quad \lambda_i \neq \lambda_k, \quad p_i = 0 \quad (5.31)$$

Finally, we consider the case of perfect switching with all failure rates equal for one active component and N-1 components in standby. In this case, the probability of successful operation over a mission time T is the sum of the probability of N mutually exclusive events.

1. Component 1 operates successfully for the entire mission time T.
2. Component 1 fails at $t < T$, component 2 operates for the remainder of the mission time.
3. Component 1 fails at $t' < T$, component 2 operates from t' until t then fails ($0 \leq t' \leq t \leq T$), component 3 is activated and operates for the remainder of the mission time.

•
•
•

We can write the equation for these events as follows

$$\begin{aligned}
 R_s = & e^{-\lambda T} + \int_0^T e^{-\lambda t} \lambda e^{-\lambda(T-t)} dt + \int_0^T \int_{t'}^T e^{-\lambda t} \lambda e^{-\lambda(t-t')} \lambda e^{-\lambda(T-t)} dt dt' + \\
 & + \int_0^T \int_{t''}^T \int_{t'}^T e^{-\lambda t} \lambda e^{-\lambda(t-t'')} \lambda e^{-\lambda(t-t')} \lambda e^{-\lambda(T-t)} dt dt' dt'' + \dots
 \end{aligned} \tag{5.32}$$

$$R_s = R \sum_{i=1}^N \frac{\lambda^{i-1} T^{i-1}}{(i-1)!} \tag{5.33}$$

where $0! \equiv 1$.

Chapter 6

R OF N REDUNDANCY WITH REPAIR

In this redundancy treatment, the system has N components in parallel with R ($1 < R < N$) required for success. If a component fails, we assume it is repaired while the remaining $N - 1$ continue to operate. First, consider a simple example of 3 of 4 redundancy (Figure 6.1).

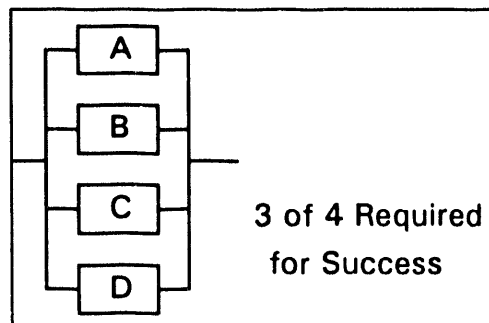


Figure 6.1 4 Components in Parallel, 3 Required for Success

Since three components are required for success, failure of any two components will cause the system to fail. Therefore, the cut sets are

AB, AC, AD, BC, BD, CD.

Thus, the system can be treated as shown in Figure 6.2.

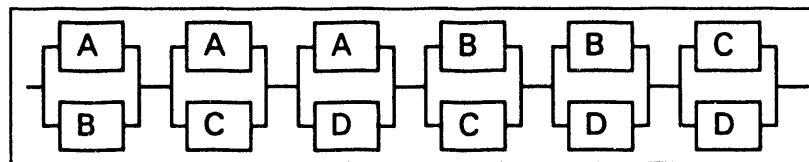


Figure 6.2 3 of 4 Redundancy as a Series Arrangement

In effect, 3 of 4 redundancy becomes a series system consisting of all possible combinations of 2 components in parallel. Failure of any 2 components causes

the system to fail. In general, R of N redundancy (active with repair) can be treated as $N!/[(N-R+1)!(R-1)!]$ cut sets representing all possible combinations of (N-R+1) terms. The failure rate (1/MTBF) for each cut set can be calculated using Equation (2.23). Failure rates can then be added for all cut sets to get a total failure rate for the parallel system. The MTBF for the parallel system is then the inverse of the system failure rate. MTTR for each cut set can be calculated using Equation (2.24). The MTTR for the parallel system is calculated using the following equation

$$T_{RS} = \frac{\sum_{i=1}^{N_C} \lambda_{C_i} T_{RC_i}}{\sum_{i=1}^{N_C} \lambda_{C_i}} \quad (6.1)$$

where N_C is the number of cut sets, λ_{C_i} is the failure rate for the i^{th} cut set, and T_{RC_i} is the MTTR for cut set i . Whereas the other redundancy treatments are exact when compared to Markov analysis for comparable assumptions, the approach presented here for R of N with repair is an approximation. It can be shown that this approximation is accurate so long as the repair time is small compared to the MTBF for individual components in the parallel arrangement. Specifically, if $T_{Ri} < 0.1 \times T_{Fi}$, the results predicted Equation (6.1) for R of N redundancy with repair should be accurate to 10% or better.

Comparisons between Equation (6.1) for R of N redundancy with repair and Markov analysis were performed for 2 of 3 and 2 of 4 redundancy. The 2 of 3 case had the following component properties:

$$\begin{array}{ll} T_{FA} = 500 \text{ hr} & T_{RA} = 20 \text{ hr} \\ T_{FB} = 1500 \text{ hr} & T_{RB} = 10 \text{ hr} \\ T_{FC} = 1000 \text{ hr} & T_{RC} = 15 \text{ hr} \end{array}$$

Results of the comparison are shown in Table 6.1.

	Calculated	Markov Analysis
Availability	.9991	.9991
System MTBF (T_{FS})	8273 hr	8382 hr
System MTTR (T_{RS})	7.62 hr	7.63 hr

Table 6.1 Comparison for Two of Three Redundancy with Repair

For both the MTBF and MTTR, the accuracy of the approximation is quite acceptable.

The 3 of 4 case used the following component properties:

$T_{FA} = 500$ hr	$T_{RA} = 20$ hr
$T_{FB} = 1500$ hr	$T_{RB} = 10$ hr
$T_{FC} = 1000$ hr	$T_{RC} = 15$ hr
$T_{FD} = 2000$ hr	$T_{RD} = 30$ hr

Results of the comparison are shown in Table 6.2.

	Calculated	Markov Analysis
Availability	.99998	.99998
System MTBF (T_{FS})	3.27E5 hr	3.32E5 hr
System MTTR (T_{RS})	5.7 hr	5.7 hr

Table 6.2 Comparison for Three of Four Redundancy with Repair

The calculated MTBF for 3 of 4 redundancy is accurate to 1.5% and the MTTR is accurate to two significant digits.

Chapter 7

R OF N REDUNDANCY WITHOUT REPAIR

For this case, the system will have N components. R of those components must be working for the system to be operable. Once there are less than R components working, the system will no longer be operable. Then it will be turned off until all of the components have been repaired.

Three Parallel Components, Two Required, without Repair

Since the case $R = 1$ has been accounted for in Chapter 3, two of three redundancy is the simplest example of R of N redundancy. The approach to finding mean time to failure is comprised of two steps. First, develop an expression for the probability that the system survives to an arbitrary time t . Second, since that expression is equivalent to the cumulative probability that the time to fail the system (T_F) exceeds t , integrate the expression from zero to infinity to find the mean time to fail the system (MTTF or T_F).

For this example, the system survives to time t if at least two components are operable at time t . There are four possible combinations of components working and not working that have at least two operating components. It is helpful to represent these combinations as subsets of the set $\{A, B, C\}$. If a component is in the subset, the component is working. Thus, of the eight possible subsets, subsets $\{A, B\}$, $\{A, C\}$, $\{B, C\}$, and $\{A, B, C\}$ represent the system working.

The probabilities for each subset are found from

$$P\{A, B\} = e^{-\lambda_A t} e^{-\lambda_B t} (1 - e^{-\lambda_C t})$$

$$P\{A, C\} = e^{-\lambda_A t} e^{-\lambda_C t} (1 - e^{-\lambda_B t})$$

$$P\{B, C\} = e^{-\lambda_B t} e^{-\lambda_C t} (1 - e^{-\lambda_A t})$$

$$P\{A, B, C\} = e^{-\lambda_A t} e^{-\lambda_B t} e^{-\lambda_C t}$$

Combining terms gives

$$P(T_F > t) = e^{-\lambda_A t} e^{-\lambda_B t} + e^{-\lambda_A t} e^{-\lambda_C t} + e^{-\lambda_B t} e^{-\lambda_C t} - 2e^{-\lambda_A t} e^{-\lambda_B t} e^{-\lambda_C t}. \quad (7.1)$$

Integrating $P(T_F > t)$ on t from zero to infinity gives the mean time to fail the system.

$$T_F = \frac{1}{\lambda_A + \lambda_B} + \frac{1}{\lambda_A + \lambda_C} + \frac{1}{\lambda_B + \lambda_C} - \frac{2}{\lambda_A + \lambda_B + \lambda_C}. \quad (7.2)$$

The mean time to repair the system (T_R) depends on which components require repair and their repair times. If we know the combination of component failures that caused the system to fail, the resulting average repair time for the combination can be found using Equation (3.19). Suppose that the redundant arrangement fails because A and B fail. Then, let $J = \{C\}$ be the subset of components that operated successfully. The complement of J ($J^c = \{A, B\}$) is the failed subset. Denote T_{RS} of Equation (3.19) as $E(T_R | J^c)$, the expected repair time of the components that have failed. We find T_R as the expected time to repair the system:

$$T_R = \sum_{\substack{J \subseteq \{A, B, C\} \\ |J|=1}} E(T_R | J^c) P(J) \quad (7.3)$$

where the sum is over all subsets J of $\{A, B, C\}$ such that failure of J^c causes the system to fail and $|J|$ is the number of components in the subset. For two of three redundancy, the subsets of interest are those having one component, i. e., cases where two components have failed. Note that we do not include the case where all three fail since the system goes down as soon as two fail and the probability of two or three failing simultaneously is vanishingly small.

The subset {A} represents the event where A is operating but both B and C have failed at time t. $P(\{A\})$ is found as the sum of probabilities of two mutually exclusive events determined from which component failed last:

1. A is operating at t, B failed prior to t, C fails at t, and
2. A is operating at t, B fails at t, C failed prior to t.

The first event has probability

$$\int_0^{\infty} e^{-\lambda_A t} (1 - e^{-\lambda_B t}) e^{-\lambda_C t} \lambda_C dt$$

The second event has probability

$$\int_0^{\infty} e^{-\lambda_A t} (1 - e^{-\lambda_C t}) e^{-\lambda_B t} \lambda_B dt$$

Integrating and adding the probabilities yields,

$$P(\{A\}) = \frac{\lambda_B}{\lambda_A + \lambda_B} + \frac{\lambda_C}{\lambda_A + \lambda_C} - \frac{\lambda_B + \lambda_C}{\lambda_A + \lambda_B + \lambda_C} \quad (7.4)$$

By similar arguments, we get

$$P(\{B\}) = \frac{\lambda_A}{\lambda_B + \lambda_A} + \frac{\lambda_C}{\lambda_B + \lambda_C} - \frac{\lambda_A + \lambda_C}{\lambda_B + \lambda_A + \lambda_C} \quad (7.5)$$

$$P(\{C\}) = \frac{\lambda_A}{\lambda_C + \lambda_A} + \frac{\lambda_B}{\lambda_C + \lambda_B} - \frac{\lambda_A + \lambda_B}{\lambda_C + \lambda_A + \lambda_B} \quad (7.6)$$

Note that in Equations (7.4) - (7.6) the failure rate for the surviving component appears in each term in the denominator. The numerators, and the other failure rates in the denominators, are represented by all nonempty subsets of the set of failed components. The sign of each term depends on the size of the subset; if the size is odd, the sign is positive and vice versa.

Comparisons between the above treatment of R of N redundancy without repair (Equations 7.2 and 7.3) and Markov analysis were performed for 2 of 3 redundancy. The 2 of 3 case had the following component properties:

$$\begin{array}{ll} T_{FA} = 500 \text{ hr} & T_{RA} = 20 \text{ hr} \\ T_{FB} = 1500 \text{ hr} & T_{RB} = 10 \text{ hr} \\ T_{FC} = 1000 \text{ hr} & T_{RC} = 15 \text{ hr} \end{array}$$

Results of the comparison are shown in Table 7.1.

	Calculated	Markov Analysis
Availability	.9690	.9690
System MTBF (T_{FS})	763 hr	763 hr
System MTTR (T_{RS})	24.4 hr	24.4 hr

Table 7.1 Comparison for Two of Three Redundancy without Repair

Four Parallel Components, Two Required, without Repair

Before generalizing the treatment of R of N redundancy, it is useful to do another special case. Consider a parallel system consisting of the four active components {A, B, C, D} with two required for successful operation. Then the probability that the configuration operates successfully to time t (the reliability of the system over time t) is the sum of the probabilities of the following 11 mutually exclusive events:

1. Components A and B fail before t and components C and D operate successfully for the entire time t.
2. Components A and C fail before t and components B and D operate successfully for the entire time t.
3. Components A and D fail before t and components B and C operate successfully for the entire time t.
4. Components B and C fail before t and components A and D operate successfully for the entire time t.

5. Components B and D fail before t and components A and C operate successfully for the entire time t.
6. Components C and D fail before t and components A and B operate successfully for the entire time t.
7. Component A fails before t and components B, C and D operate successfully for the entire time t.
8. Component B fails before t and components A, C, and D operate successfully for the entire time t.
9. Component C fails before t and components A, B, and D operate successfully for the entire time t.
10. Component D fails before t and components A, B, and C operate successfully for the entire time t.
11. All four components operate successfully over time t.

Thus, the equation for the reliability over time t of the redundant system, R_S , can be written in terms of the reliabilities ($R_i = e^{-\lambda_i t}$) and unreliabilities ($1 - R_i$) over time t for each component $i \in \{A, B, C, D\}$.

$$\begin{aligned}
 R_S = & (1 - R_A)(1 - R_B)R_C R_D + (1 - R_A)R_B(1 - R_C)R_D \\
 & + (1 - R_A)R_B R_C(1 - R_D) + R_A(1 - R_B)(1 - R_C)R_D \\
 & + R_A(1 - R_B)R_C(1 - R_D) + R_A R_B(1 - R_C)(1 - R_D) \\
 & + (1 - R_A)R_B R_C R_D + R_A(1 - R_B)R_C R_D + R_A R_B(1 - R_C)R_D \\
 & + R_A R_B R_C(1 - R_D) + R_A R_B R_C R_D
 \end{aligned} \tag{7.7}$$

Expanding the products and combining terms yields,

$$\begin{aligned}
 R_S = & R_A R_B + R_A R_C + R_A R_D + R_B R_C + R_B R_D + R_C R_D \\
 & - 2R_A R_B R_C - 2R_A R_B R_D - 2R_A R_C R_D - 2R_B R_C R_D \\
 & + 3R_A R_B R_C R_D
 \end{aligned} \tag{7.8}$$

Integrating R_S on t from zero to infinity gives the mean time to fail the system.

$$T_F = \frac{1}{\lambda_A + \lambda_B} + \frac{1}{\lambda_A + \lambda_C} + \frac{1}{\lambda_A + \lambda_D} + \frac{1}{\lambda_B + \lambda_C} + \frac{1}{\lambda_B + \lambda_D} + \frac{1}{\lambda_C + \lambda_D} \quad (7.9)$$

$$- \frac{2}{\lambda_A + \lambda_B + \lambda_C} - \frac{2}{\lambda_A + \lambda_B + \lambda_D} - \frac{2}{\lambda_A + \lambda_C + \lambda_D} - \frac{2}{\lambda_B + \lambda_C + \lambda_D}$$

$$+ \frac{3}{\lambda_A + \lambda_B + \lambda_C + \lambda_D}$$

Failure rates are added for each subset of $\{A, B, C, D\}$ of size $k \geq R = 2$ in the denominators of Equation (7.9) and the sign of each term depends on k ; if k is even, the sign is positive and vice versa. The coefficient of each term is the combination of $k - 1$ taken $k - R$ at a time.

The mean time to repair the system (T_R) depends on which components require repair and their repair times. For each combination of component failures that cause the system to fail, we use Equation (3.19) to find the resulting average repair time. We need only to weight the repair times by the probability that the combination causes the system to fail. Consider the event $\{D\}$. In the terminology used in the 2 of 3 case, $\{D\}$ is the event that component D survives to time t , whereas the components in the complement of $\{D\}$ ($\{A, B, C\}$) all fail, causing the system to fail. Recalling the approach to Equations (7.4) - (7.6), we find the probability for the three cases in which components A , B , and C are the last to fail, and combine results. We can write:

$$P\{D\} = \frac{\lambda_A}{\lambda_A + \lambda_D} + \frac{\lambda_B}{\lambda_B + \lambda_D} + \frac{\lambda_C}{\lambda_C + \lambda_D} \quad (7.10)$$

$$- \frac{\lambda_A + \lambda_B}{\lambda_A + \lambda_B + \lambda_D} - \frac{\lambda_A + \lambda_C}{\lambda_A + \lambda_C + \lambda_D} - \frac{\lambda_B + \lambda_C}{\lambda_B + \lambda_C + \lambda_D}$$

$$+ \frac{\lambda_A + \lambda_B + \lambda_C}{\lambda_A + \lambda_B + \lambda_C + \lambda_D}$$

Note that in Equation (7.10) the failure rate for the surviving component $\{D\}$ appears in each term in the denominator. The numerators, and the other failure rates in the denominators, are represented by all nonempty subsets of the set of

failed components {A, B, C}. The sign of each term depends on the size of the subset; if the size is odd, the sign is positive and vice versa.

Each of the other 3 events where three components fail and the other survives have probabilities identical in form to that of Equation (7.10). Moreover, those are the only events that need be considered when finding repair times. That is, as soon as three fail, the system is shut down. The probability that two or more components fail simultaneously is vanishingly small and need not be treated.

N Parallel Components, R Required, without Repair

For the general case, the probability that the system is operable at time t is the sum of the probabilities of each state which has at least R components working at time t . That is

$$P_s(t) = \sum_{k=R}^N \sum_{J, |J|=k} P(J) P(J^c) \quad (7.11)$$

where $|J|$ is the number of components in the set J (thus the second summation is over all sets of k components), $P(J)$ is the probability that the k components of J are all operable at time t , and $P(J^c)$ probability that the $N - k$ components not in J have all failed by time t .

$P(J)$ is the product of the reliabilities over time t ($e^{-\lambda_i t}$) of components i in set J and $P(J^c)$ is the product of the unreliabilities over time t ($1 - e^{-\lambda_i t}$) for the components i not in J . Thus, Equation (7.11) can be easily implemented in its current form to calculate the reliability of the R of N configuration over time t . However, Equation (7.11) must be integrated on t to find the mean time to fail. To do the integration, the product defining $P(J^c)$ in the integrand must be expanded. As in the 2 of 3 and 2 of 4 cases above, we do the expansion and collect like terms *a priori*. The collected terms can be counted using a simple combination, and Equation (7.11) can be written in the form:

$$P_s(t) = P(T_F > t) = \sum_{k=R}^N \sum_{J: |J|=k} (-1)^{(k-R)} \binom{k-1}{k-R} e^{-\sum_{i=1}^k \lambda_{J_i} t}. \quad (7.12)$$

Proof of the form for Equation (7.12) for general R and N can be found in Appendix B. Since T_F is non-negative, the mean time to fail is found by integrating over all non-negative t .

$$\begin{aligned} \text{MTTF} &= \int_{t=0}^{\infty} P(T_F \geq t) dt \\ \text{MTTF} &= \int_{t=0}^{\infty} \left[\sum_{k=R}^N \sum_{J: |J|=k} (-1)^{(k-R)} \binom{k-1}{k-R} e^{-\sum_{i=1}^k \lambda_{J_i} t} \right] dt \\ \text{MTTF} &= \sum_{k=R}^N \sum_{J: |J|=k} (-1)^{(k-R)} \binom{k-1}{k-R} \frac{1}{\sum_{i=1}^k \lambda_{J_i}}. \end{aligned} \quad (7.13)$$

The system is repaired as soon as it fails, as soon as there are less than R components working. If we let $D = N - R + 1$, this is equivalent to waiting until D components are down, and then repairing those D components. Let E_J be the event that the components in J are the first D components to fail, then

$$\text{MTTR} = \sum_{J: |J|=D} E(T_R | E_J) P(E_J). \quad (7.14)$$

$E(T_R | E_J)$ can be calculated using the appropriate form of Equation (3.19) since all failed components are repaired. $P(E_J)$ is the probability that the components in J are the first D components to fail. To find $P(E_J)$ take the sum as i goes through the components in J of the probability that i is the last component in J to fail and that i fails before any component which is not in J . This is

$$P(E_J) = \sum_{i=1}^D \left\{ \int_{t=0}^{\infty} \left[\prod_{\substack{k=1 \\ k \neq i}}^D (1 - e^{-\lambda_k t}) \prod_{m \in J} e^{-\lambda_m t} \right] e^{-\lambda_i t} \lambda_i dt \right\} \quad (7.15)$$

The first product in the integrand is the probability that all components in J (except i) have failed prior to time t . The second product is the probability that those components not in J are still operable at time t . The last factor is the probability that component i fails at time t . Once the first product is expanded, the integration is straightforward.

We expand the first product and integrate, then sum over all components i of J . In doing so, several terms that have the same denominator are combined. To write down the final result, we introduce the following notation. Let a be a nonempty subset of J of size $|a|$ and let λ_{ak} denote the failure rate for component k in subset a . Then

$$P(E_J) = \sum_{\substack{a \subset J \\ a \neq \emptyset}} (-1)^{|a|-1} \frac{\sum_{k=1}^{|a|} \lambda_{a_k}}{\left(\sum_{k=1}^{|a|} \lambda_{a_k} + \sum_{m \in J} \lambda_m \right)} \quad (7.16)$$

Equation (7.16) follows the pattern established in the 2 of 3 case and in the 2 of 4 case, see Equations (7.4)-(7.6) and (7.10) above. That is, failure rates for the surviving components appear in each denominator. Each numerator and the rest of each denominator are represented by the nonempty subsets of the set of failed components. The sign of each ratio depends on the size of the subset; if $|a|$ is odd, the sign is positive, and vice versa.

Comparisons between the RAMP treatment of R of N redundancy without repair (Equations (7.13) and (7.14)) and Markov analysis were performed for 2 of 4 redundancy. This case used the following component properties:

$T_{FA} = 500$ hr	$T_{RA} = 20$ hr
$T_{FB} = 1500$ hr	$T_{RB} = 10$ hr
$T_{FC} = 1000$ hr	$T_{RC} = 15$ hr
$T_{FD} = 2000$ hr	$T_{RD} = 30$ hr

Results of the comparison are shown in Table 7.2.

	Calculated	Markov Analysis
Availability	.9735	.9735
System MTBF (T_{FS})	1280 hr	1280 hr
System MTTR (T_{RS})	34.8 hr	34.8 hr

Table 7.2 Comparison for Three of Four Redundancy without Repair

The agreement between the RAMP treatment and Markov analysis is exact.

R of N Redundancy in Non-Repairable Systems

The reliability over some mission time T of an R of N redundancy configuration in a non-repairable system is found by substituting T for t in Equation (7.12) above. We also note that the exponential term in Equation (7.12) is the product of component reliabilities over time T . We therefore write:

$$R_s = \sum_{k=R}^N \sum_{j_1, j_2, \dots, j_k} (-1)^{(k-R)} \binom{k-1}{k-R} \prod_{i=1}^k R_{j_i}. \quad (7.17)$$

Chapter 8

CONCLUSIONS

In this report, we have developed equations for the equivalent (average) failure rates and repair times of the following six redundancy treatments:

Active with Repair All parallel components are active with only one needed for success. A failed component can be repaired while the system continues to operate on other parallel components.

Active without Repair All parallel components are active with only one needed for success. Failed components are not repaired until all parallel components have failed. Then all are repaired.

Standby with Repair Only one of the redundant components is active with others held in standby. In case the active component fails, a standby component can be switched on either manually or automatically. The failed component is repaired while the system operates using a standby component.

Standby without Repair Only one of the redundant components is active with others held in standby. In case the active component fails, a standby component can be switched on either manually or automatically. The failed component is not repaired until all redundant components have failed.

R of N with Repair The system consists of N components of which R ($1 < R < N$) are required for success. For example, if a car wheel has 5 lug nuts and 4 are considered necessary for safe operation, the lug nuts provide 4 of 5 redundancy. Failed components are repaired while the system operates.

R of N without Repair The system consists of N components of which R ($1 < R < N$) are required for success. Failed components are not repaired until more than N - R have failed and the system cannot operate.

These options are currently being implemented in RAMP 2.0 which will be released in 1993.

A Markov analysis program was developed for the above redundancy options prior to development of the equations presented in Chapters 2 through 7. While the Markov code proved too expensive for use in RAMP in terms of computer memory and processing time, it did provide an independent basis for evaluating the accuracy of the redundancy equations. A few comparison calculations have been presented in this report. For active with and without repair, standby with and without repair, and R of N without repair, the comparisons between the equations developed here and Markov analysis was exact. The treatment of R of N with repair is an approximation that compares with Markov analysis to 10% or better so long as component repair times are no larger than about one tenth of component mean times between failures. In addition, an extensive suite of test calculations has been performed with similar results to those presented in this document.

While the purpose of this document is to present the theoretical basis for the redundancy analysis in RAMP 2.0 rather than offering design guidance on appropriate redundancy treatments, it is interesting to compare active and standby redundancy options. To generate these, we considered two components in parallel with equal MTBFs and repair times. In each case, the repair time for each component was assumed to be 10 hours while the MTBF was varied from 0 to 400 hours. Figure 8.1 shows that standby redundancy with repair is most effective for this simple case in terms of the MTBF of the parallel system whereas active without repair is the least effective. The results shown graphically in Figure 8.1 are also presented in Table 8.1.

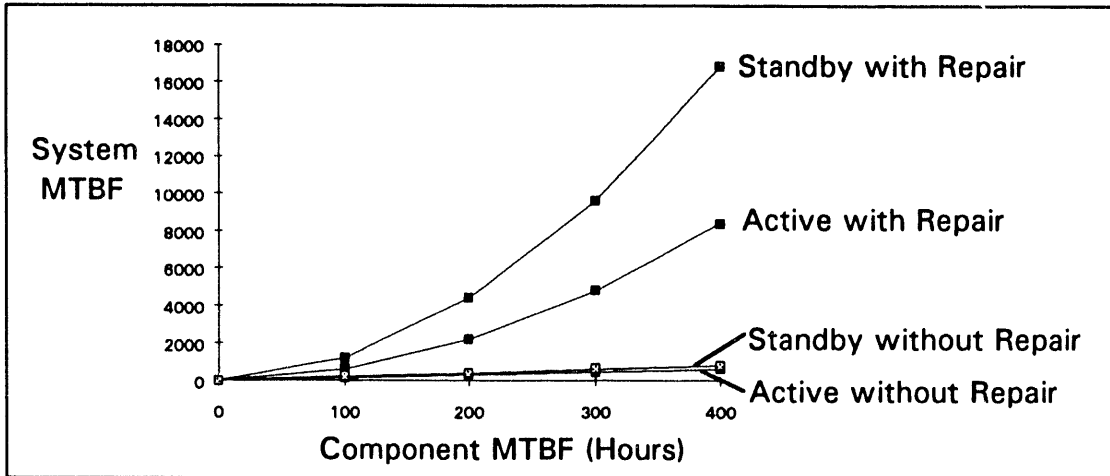


Figure 8.1 MTBF for Parallel Components with Different Redundancy Treatments

Component MTBF	Active With Repair	Active Without Repair	Standby With Repair	Standby Without Repair
100	600	150	1200	200
200	2200	300	4400	400
300	4800	450	9600	600
400	8400	600	16800	800

Table 8.1 MTBF of Parallel Components with Different Redundancy Treatments

It is clear that redundancy can, in some circumstances, provide considerable improvements in system reliability, particularly if the equipment can be designed to allow repair of a failed redundant component while the system remains operable. With RAMP 2.0, the design engineer will be able to evaluate such options easily.

References

1. Campbell, R.L. Iman, D.E. Longsine, and B.M. Thompson, "A Tutorial on Reliability Modeling Using RAMP," SETEC Report, SETEC91-030, December, 1991.
2. Campbell, B.M. Thompson, D.E. Longsine, P.A. O'Connell, and R.L. Iman, "RAMP User's Reference Manual," SETEC Report, SETEC91-031, December, 1991.
3. Doty, Leonard A., "Reliability for the Technologies, Second Edition," Industrial Press, Inc., New York, 1989.
4. RADC-TR-77-287, "A Redundancy Notebook," Systems Reliability and Engineering Division, Rome Air Development Center, Griffiss Air Force Base, New York.
5. Ryser, Herbert John, "Combinatorial Mathematics," Mathematical Association of America, 1963.

Appendix A

ALGORITHM FOR STANDBY WITH REPAIR

A state of the standby-with-repair parallel system is determined by the following:

- Which components are operable. Note that a component can be operable but not actually operating.
- Whether the system is up or down.
- If the system is up, which component is working.

We will refer to the state where all of the components are operable, the system is up, and the first component is working as the beginning state.

We will order the states so that from any state, the system can only go to later states or the beginning state. This can be done by making sure that the ordering satisfies the following two conditions:

1. If $i < j$, then any state in which component i is working will come before any state in which component j is working.
2. If the same component is working in two states, and a different number of components are operable in each of the two states, then the state with fewer operable components will come first.

Any order which satisfies both of these conditions will serve our purposes. Thus, in the flowchart and the psuedo-code, we do not specify one. In the actual code, we use a convenient, but otherwise arbitrary order which satisfies both conditions.

The system will start in the beginning state. Once the first component fails, the system will go to one of the states where all of the other components are

operable. We will calculate the probability of the system going to each of these states and the expected amount of time that will transpire before the first component fails and the system makes the transition. We will then work our way through all of the other possible states. As we go through each state, we will consider where the system can go from that state and how long it will take to get there. Eventually, we will go through all of the sets where the system is up, and we will know the probability of being in each down state when the system fails and how long we would expect it to take for the system to get there.

Let i go from 2 to the number of components in the parallel system. Then, for each value of i , we will let j go from 0 to $(i-2)$. We will consider all of the states in which component i is working and j of the components before component i are operable.

We will look at where the system can go from these states and how long it will take for the system to go to these places. Once we have done this for one value of j , we will have exhausted all of the ways that the system can go to a state in which $(j+1)$ of the components before component i are operable. Thus, we can now consider the next value of j , and consider where those states will go.

The last value of j was $(i-2)$. From the corresponding states, the system could go to the beginning state. Thus, when we have exhausted all of the states in which component i was working, there will be some probability that the system returned to the beginning state. (We will let p refer to $1 -$ the probability of the system returning to the beginning state.) If this had happened, the system would have started over and continued starting over until it found some other state at this point. Thus, we will divide the probability of being in each other possible state by p . Since going to the beginning state and starting over will take time, we will add $(1/p - 1)$ to the time to reach the beginning state to the times to reach each of the other states.

We will now have, conditioned on the event that the system is in the first state where none of the first i components are working, the probability of being in each possible state and the expected time for the system to reach that state. We will now use the next value of i , and consider all of the states where that component is working.

After we have gone through all of the possible states where the system is up, we will have, conditioned on the system being in the first state where the system is down, the probabilities of the system being in each possible (down) state. We also know the expected time for the system to reach each of these down states, conditioned on that state being the first down state which the system has reached.

We can use this information to find the expected time until the system is in its first down state (or fails). We can also calculate the time to repair the system from each down state, and thus find the expected time to repair the system once it fails.

Flow charts for this algorithm follow.

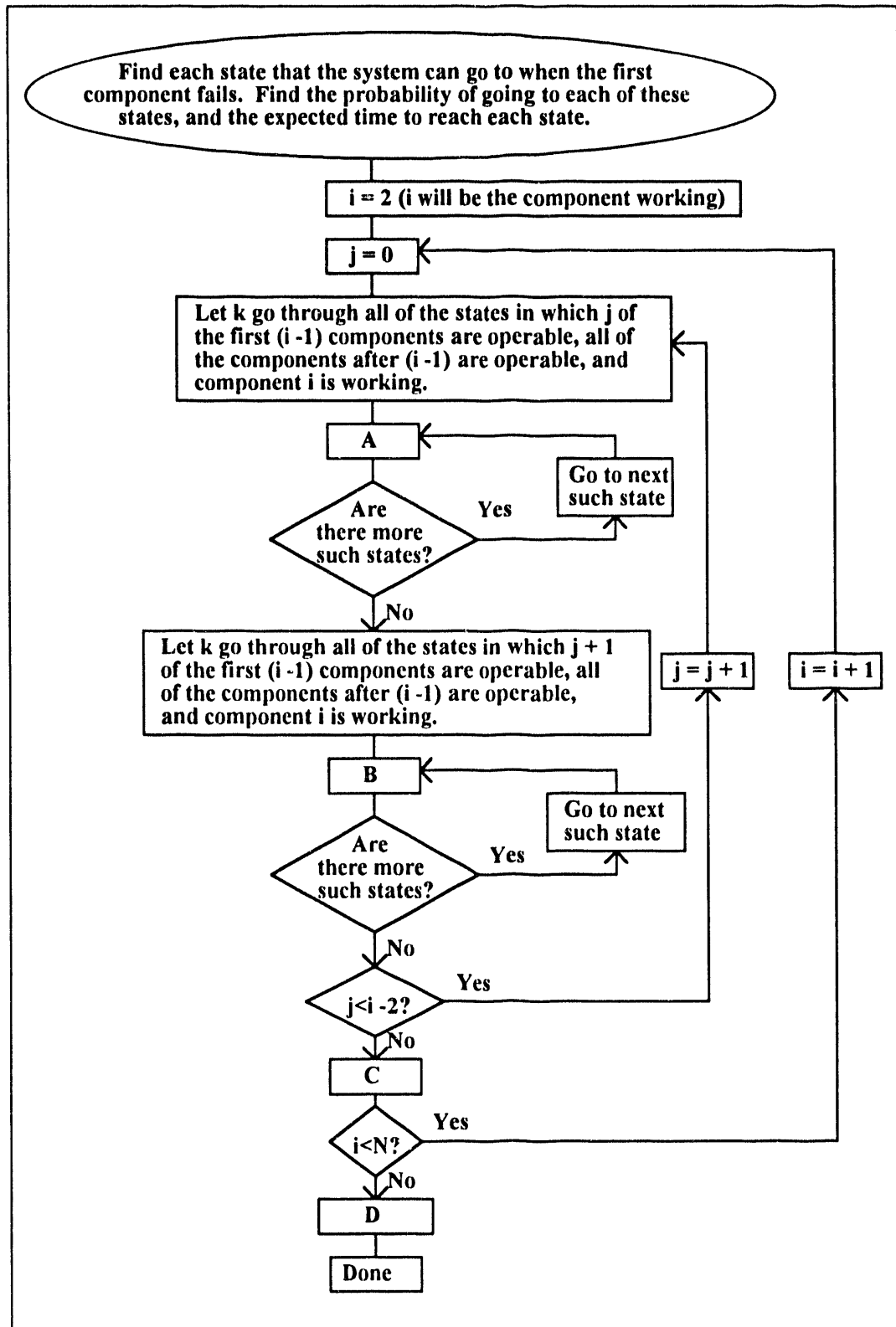


Figure A.1 Flowchart of the Algorithm

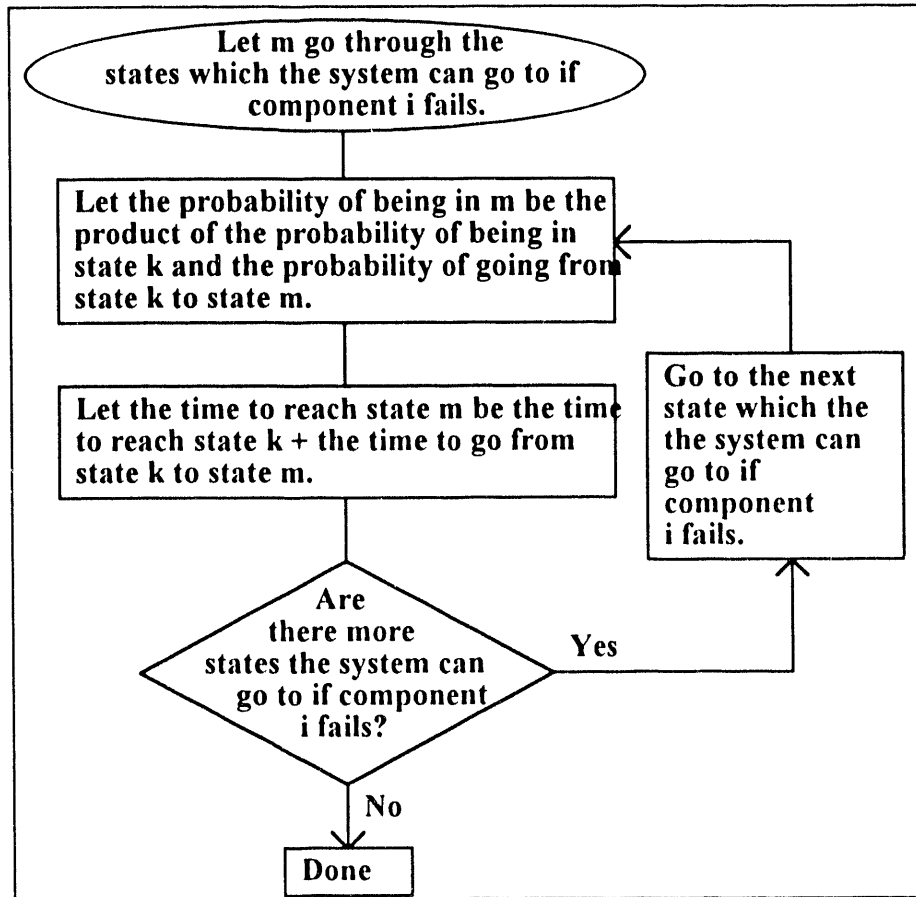


Figure A.2 Subchart A

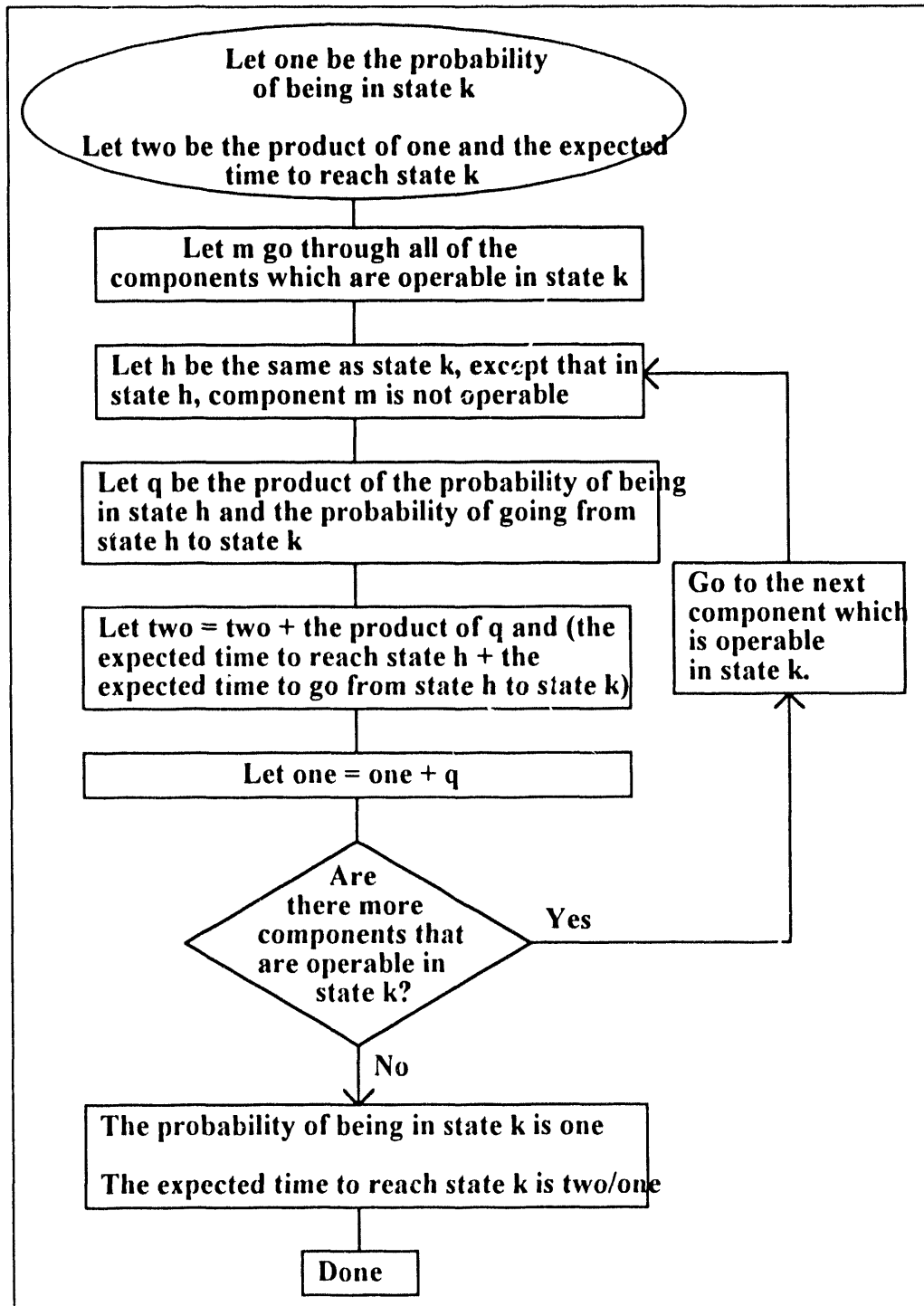


Figure A.3 Subchart B

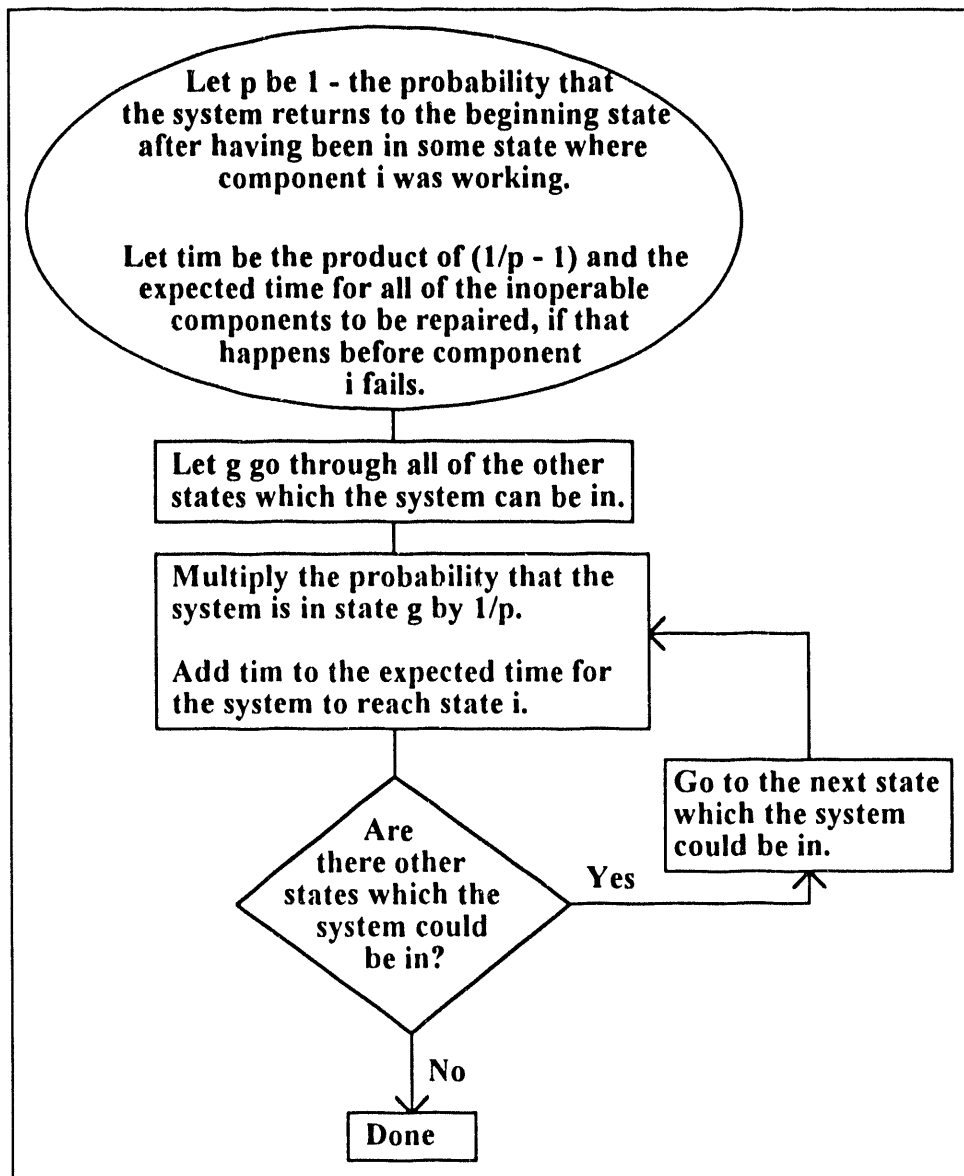


Figure A.4 Subchart C

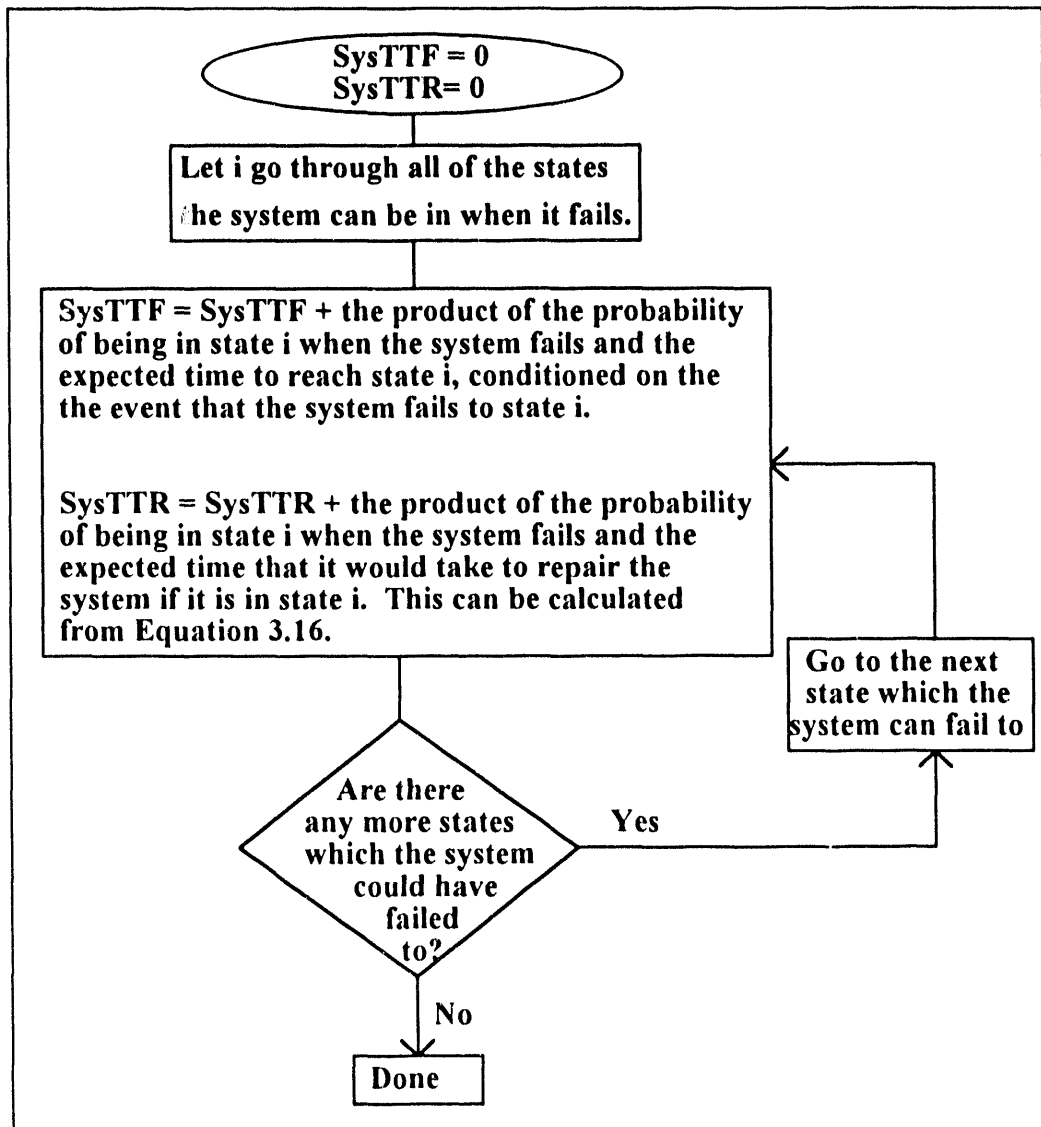


Figure A.5 Subchart D

Appendix B

In Chapter 7 there are two formulas presented for finding reliability over time t , $P_s(t)$, for a general R of N configuration. The first formula is derived in the text and takes the form:

$$P_s(t) = \sum_{k=R}^N \sum_{J:|J|=k} P(J) P(J^c) \quad (B.1)$$

where J is a subset of the N components of size $|J|$ and J^c is the complement of J . The second form is inferred from the 2 of 3 and 2 of 4 examples,

$$P_s(t) = \sum_{k=R}^N \sum_{J:|J|=k} (-1)^{(k-R)} \binom{k-1}{k-R} P(J). \quad (B.2)$$

To show they are the same, first note that [5]

$$\sum_{k=R}^N \sum_{J:|J|=k} P(J) P(J^c) = \sum_{k=R}^N \sum_{s=k}^N (-1)^{(s-k)} \binom{s}{k} \sum_{J:|J|=s} P(J).$$

Thus, we want to prove that

$$\sum_{k=R}^N \sum_{s=k}^N (-1)^{(s-k)} \binom{s}{k} \sum_{J:|J|=s} P(J) = \sum_{k=R}^N \sum_{J:|J|=k} (-1)^{(k-R)} \binom{k-1}{k-R} P(J). \quad (B.3)$$

Using s as the index on the right, instead of k , and changing the order of summation on the left, gives us:

$$\sum_{s=R}^N \sum_{k=R}^s (-1)^{(s-k)} \binom{s}{k} \sum_{J:|J|=s} P(J) = \sum_{s=R}^N \sum_{J:|J|=s} (-1)^{(s-R)} \binom{s-1}{s-R} P(J). \quad (B.4)$$

From inspection, Equation (B.4) is true if:

$$\sum_{k=R}^s (-1)^{(s-k)} \binom{s}{k} = (-1)^{(s-R)} \binom{s-1}{s-R}. \quad (B.5)$$

Thus the formulations for $P_s(t)$ are the same if Equation (B-5) is valid. We prove Equation (B-5) using the formula [5],

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}. \quad (\text{B-6})$$

Start with the left hand side of Equation (B-5); split off the $k = s$ term (which equals +1) and use Equation (B-6) to write

$$\sum_{k=R}^s (-1)^{(s-k)} \binom{s}{k} = \sum_{k=R}^{s-1} (-1)^{(s-k)} \binom{s-1}{k} + \sum_{k=R}^{s-1} (-1)^{(s-k)} \binom{s-1}{k-1} + 1. \quad (\text{B-7})$$

Note that the + 1 term can be treated as the $k = s$ term for the second summation on the right. We incorporate that term to run the sum to s and change the index of summation ($j = k - 1$). Factor out (-1) from the first summation on the right and rewrite Equation (B-7) as,

$$\sum_{k=R}^s (-1)^{(s-k)} \binom{s}{k} = (-1) \sum_{k=R}^{s-1} (-1)^{(s-k)} \binom{s-1}{k} + \sum_{j=R-1}^{s-1} (-1)^{(s-j-1)} \binom{s-1}{j}. \quad (\text{B-8})$$

We see that the two summations cancel in Equation (B-8) except for the $j = R - 1$ term. Thus,

$$\sum_{k=R}^s (-1)^{(s-k)} \binom{s}{k} = (-1)^{(s-R)} \binom{s-1}{R-1}. \quad (\text{B-9})$$

The combinations on the right hand sides of Equations (B-5) and (B-9) are the same by definition, and we are done.

DISTRIBUTION

SEMATECH (2)
Attn: Paul Tobias
Mario Villacourt
2706 Montopolis Drive
Austin, TX 78741-6499

Joel Atkins
Statistics Department
367 Evans Hall
University of California
Berkeley, CA 94720

Applied Materials
Attn: Ralph Dudley
M/S 0906
2696 Augustine Drive
Santa Clara, CA 95954

Internal

GENUS Corp.
Attn: Sam Becktel
1139 Karlstad Drive
Sunnyvale, CA 94089

0335 Janet Sjulín
0335 Donald Wright
2314 Everett Saverino
2571 Roger Roberts
8 Gary Ferguson

LAM Research Corp.
Attn: Mark Meisner
4650 Cushing Parkway
Fremont, CA 94358-6401

.2 Allen Camp
6412 Sharon Daniels
6412 Susan Dingman
6412 Greg Wyss

INTERA, Inc. (2)
Attn: Bruce Thompson
Pat O'Connell
1650 University Blvd., NE, Suite 300
Albuquerque, NM 87102

6613 Maria Armendariz
6613 James Campbell (9)
6613 Robert Cranwell
6613 Eric Tomlin
7141 Technical Library (5)
7151 Technical Publications (1)
7613-2 Document Processing for

INTERA, Inc. (3)
Attn: Dennis Longsine
6850 Austin Center Blvd., Suite 300
Austin, TX 78731

DOE/OSTI (10)
8116 Rene L. Bierbaum
8523-2 Central Technical Files (1)

**DATE
FILMED**

2 / 10 / 94

END

