PCS-5733

The Theory and Practice of Reliable System Design

DANIEL P. SIEWIOREK
ROBERT S. SWARZ

characterize and measure operational system unreliability due to software. There is a large gulf between the variables that can be easily measured in a running system and the number of bugs in its software. Instead, a cost-effective analysis should allow precise evaluation of software unreliability from variables easily measurable in an operational system, without knowing the details of how the software has been written.

MODELING TECHNIQUES

Redundant systems can be modeled under various operational assumptions, such as failure to exhaustion and failure with repair. Redundancy with failure to exhaustion is a simplistic and pessimistic model which assumes that all redundant modules fail before any repair. Failure with repair, on the other hand, models two separate but concurrent processes: the failure process and the repair process. Failure to exhaustion can be modeled by simple combinatorial probability, the first topic in this section. Failure with repair, which requires solutions of sets of differential equations, is the second main topic. Next, the impact on system availability of different assumptions concerning repair strategy is explored, followed by models built on the assumption that failures affect the performance of redundant systems.

Combinatorial Modeling

In combinatorial modeling, the system is divided into nonoverlapping modules. Each module is assigned either a probability of working, P_i, or a probability as a function of time, $R_i(t)$. The goal is to derive the probability, P_{sys}, or function, $R_{sys}(t)$, of correct system operation. The following assumptions are made:

1. Module failures are independent.
2. Once a module has failed, it is assumed always to yield incorrect results.
3. The system is considered failed if it does not satisfy the minimal set of functioning modules.
4. Once the system enters a failed state, subsequent failures cannot return the system to a functional state. This property, called coherency, is mathematically defined by Esary and Proschan [1962] in terms of a structure function $\varphi(x)$. x is a vector composed of elements $x_1, x_2, \ldots, x_n$, where each x_i is 1 if module i is functional, and 0 if module i is failed. A coherent system satisfies the following properties:
   a. $\varphi(1, 1, \ldots, 1) = 1$, when all modules function, the system must function;
   b. $\varphi(0, 0, \ldots, 0) = 0$, when all modules fail, the system fails; and
   c. $\varphi(x) \geq \varphi(y)$ whenever $x_i \geq y_i \, \forall i$, $i = 1, 2, \ldots, n$

Failure to exhaustion models typically enumerate all the states of the system (where a state is a pattern of failed and working modules) that meet or exceed the requirements of the minimal module set. Combinatorial counting techniques are used to simplify this enumeration. The following three subsections treat commonly used modeling techniques for series/parallel systems, M-of-N systems, and complex systems.

Series/Parallel Systems

Most frequently, reliability evaluation involves a series or parallel combination of independent systems. Figure 5-1 illustrates a serial string of modules, all of which must function for the system to function correctly. The modules could be resistors, fuel valves, computers, or any other components. If $R_i(t)$ is the reliability of module i and if the modules are assumed independent, then the overall system reliability is:

$$R_{series}(t) = \prod_{i=1}^{n} R_i(t) \tag{1}$$

Hence, the failure probability, denoted by Q, of a series system can be written as:

$$\begin{aligned} Q_{series}(t) &= 1 - R_{series}(t) = 1 - \prod_{i=1}^{n} R_i(t) \\ &= 1 - \prod_{i=1}^{n} (1 - Q_i(t)) \end{aligned} \tag{2}$$

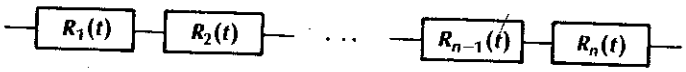


Figure 5–1. A series connection of n modules.

The parallel configuration in Figure 5-2 fails only if all the systems fail. The probability of failure is:

$$Q_{\text{parallel}}(t) = \prod_{i=1}^{n} Q_i(t) \tag{3}$$

The system reliability is:

$$R_{\text{parallel}}(t) = 1 - Q_{\text{parallel}}(t) = 1 - \prod_{i=1}^{n} Q_i(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t)) \tag{4}$$

Note the duality between R, Q; Equations 1 and 3; and Equations 2 and 4. For some systems it may be easier to work with failure probability than with reliability. Equations 1 through 4 can be applied recursively to complex series/parallel configurations to arrive at an overall reliability function. Figure 5-3 depicts two different interconnections of four components. These configurations have been used in aerospace systems for providing redundant transmission paths between terminals t_1 and t_2 where each working path has to contain at least one good component. The modules may be resistors or diodes (such as the component quadding used in OAO, the Orbital Astronomical Observatory) or valves controlling fuel flow to a rocket motor. The configuration in Figure 5-3a tolerates more patterns of shorted components (such as shorted resistors/diodes or stuck-at-open fuel valves) than does configuration (b). Both configurations tolerate all single shorts and double shorts (ac, bd). Configuration (a) also tolerates double shorts (ad, bc). In a dual manner, configuration (b) tolerates more patterns of open components (such as open resistors/diodes or stuck-at-closed fuel valves). In particular, configuration (b) tolerates the double-open failures of (ad, bc) for which configuration (a) fails.

Now consider the case where blocks (a, c) are processors and (b, d) are memories. For the system to operate, at least one processor-memory pair is required. Configuration (a) represents a

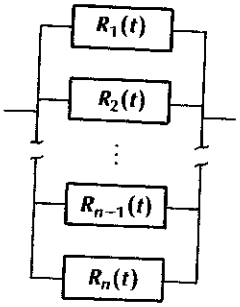
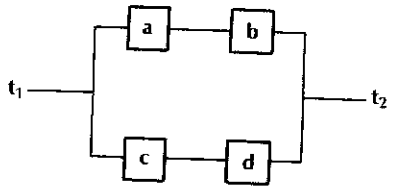


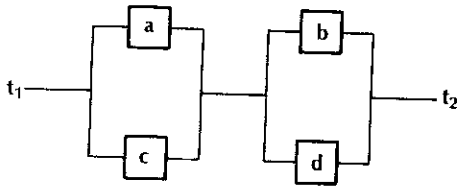
Figure 5–2. A parallel connection of n modules.



Shorts tolerated: a, b, c, d, ac, ad, bc, bd

Opens tolerated: a, b, c, d, ab, cd

a.



Shorts tolerated: a, b, c, d, ac, bd

Opens tolerated: a, b, c, d, ab, ad, bc, cd

b.

Figure 5–3. Two forms of series/parallel interconnection designed to tolerate a.) short and b.) open failures.

computer with a standby spare. Figure 5-4a illustrates the application of the series reliability equation. Now, applying the parallel reliability equation:

$$R_{\text{short}}(t) = 1 - (1 - R_a R_b)(1 - R_c R_d) \quad (5)$$

Note that the R_is may be either a single value such as a probability of success, or a function of time. In this text the function notation $R_i(t)$ is reserved for special cases. The reader may interpret R_i as either a single numbered probability or a function. Applying the parallel reliability equation to configuration (b) (Figure 5-4b) results in:

$$R_{\text{open}} = (1 - (1 - R_a)(1 - R_c)) \times (1 - (1 - R_b)(1 - R_d))$$

Letting $R_a = R_b = R_c = R_d = R_m$ yields

$$R_{\text{short}} = 2R_m^2 - R_m^4 \quad (6)$$

and

$$R_{\text{open}} = 4R_m^2 - 4R_m^3 + R_m^4$$

Because there are more combinations of working systems in configuration (b), it is obvious that

$$R_{\text{open}} > R_{\text{short}}$$

for all $t > 0$. Now consider the case of n modules in parallel, only one of which is required to function. The other $n - 1$ modules represent spares. The spares can be operating in parallel or, as is more usually the case, standing by to replace the operating module when it fails. The form of Equation 3 suggests that as n grows large, Q_{parallel} becomes close to perfection. For example, for R_{parallel} to be within ϵ of 1.0, choose n such that:

$$n = \frac{ln\,\epsilon}{ln\,Q} \quad (7)$$

for $\epsilon = 10^{-6}$ and $Q_m = 0.1$, $n = 6$.

Equations 3 and 4, however, assume that the detection of the failed operating module and the switchover of a standby spare occur flawlessly. This is not a valid asumption in complex systems, in which even failure detection is far from perfect (a typical diagnostic program, for example, may detect only 80–90 percent of possible faults). As a result, the concept of coverage [Wyle and Burnett, 1967; Bouricius, Carter, and Schneider, 1969a, 1969b] has been introduced. In this context, coverage is defined as the conditional probability that a system recovers, given there has been a failure. What constitutes proper recovery is a strong function of the intended application. It may mean merely establishing a workable hardware system configuration (such as telephone switching processors) or it may demand that no data are lost or corrupted (such as in transaction processing computers, used in banks). Let coverage be denoted by c. Then, for a system with two modules:

$$R_{\text{sys}} = R_1 + cR_2(1 - R_1) \quad (8)$$

The first term is the probability that the first module survives. The second term is the probability that the first module fails, the second is still functioning, and a successful switchover was accomplished. Note that if $c = 1$ and $R_1 = R_2 = R_m$, $R_{\text{sys}} = 2R_m - R_m^2 = 1 - (1 - R_m)^2$. If the modules are identical, then Equation 8 can be generalized to:

$$R_{\text{sys}} = R_m \sum_{i=0}^{n-1} c^i (1 - R_m)^i \quad (9)$$

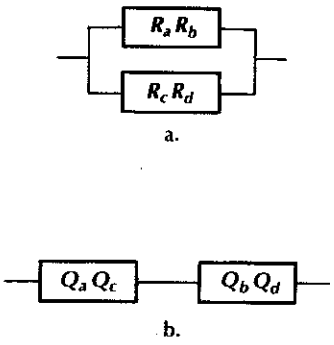


Figure 5-4. Applying a.) the series and b.) the parallel unreliability formula to Figure 5-3b.

This geometric progression can be evaluated by noting that:

$$\sum_{i=0}^{n} x^i = \frac{1 - x^{n+1}}{1 - x}$$

For $0 < x < 1$
Hence:

$$R_{sys} = R_m\left(\frac{1 - c^n(1 - R_m)^n}{1 - c(1 - R_m)}\right)$$

$$= R_m\left(\frac{1 - c^n Q_m^n}{1 - cQ_m}\right)$$

For R_{sys} to be within ϵ of 1.0, choose n such that:

$$n = \frac{ln\left[1 - \frac{(1 - \epsilon)(1 - cQ_m)}{R_m}\right]}{ln(cQ_m)} \quad (10)$$

Returning to the example where $R_{sys} = 1 - \epsilon$ for $\epsilon = 10^{-6}$, $R_m = 0.9$, and $c = 1.0$, it was shown that $n = 6$ was sufficient. Now assume a nonperfect, but still high coverage of $c = 0.99$. Even for $n = \infty$, R_{sys} from Equation 9 is only 0.99889. For a more conservative coverage of $c = 0.9$, the maximum value for R_{sys} with $n = \infty$ is 0.989.

Table 5-3 lists the values of system reliability expressed by Equation 9 as a function of module reliability (R_m), coverage (c), and number of modules (n). Two things should be noted from this table. First, as in all redundancy techniques, the initial application of redundancy produces a major decrease in system unreliability. Factors of 10 or more are not uncommon. In a comparison of R_m with R_{sys} for $n = 2$, the ratios of unreliability vary from a high of 9.09 to a low of 1.67. However, once n is increased to 4, the great majority of the system reliability improvement has been realized. Second, the single most important parameter is coverage. For high values of coverage (such as 0.99) and a moderate number of modules (say, four to six), system reliability is almost independent of module reliability over a wide range. Although coverage is a mathematically concise concept, it is often impossible to measure (or indeed even estimate) in practice because so many factors influence the final value of c.

The MTTF of a standby sparing system can be derived by integrating Equation 9.

$$\text{MTTF } (n \text{ modules}) = \int_0^\infty R_m \sum_{i=0}^{n-1} c^i(1 - R_m)^i\, dt$$

which can be rewritten for exponential reliability as:

$$\begin{aligned}\text{MTTF } (n \text{ modules}) &= \text{MTTF } (n - 1 \text{ modules}) \\ &\quad + \int_0^\infty R_m c^{n-1} \\ &\quad \times (1 - R_m)^{n-1}\, dt \\ &= \text{MTTF } (n - 1 \text{ modules}) \\ &\quad + \int_0^\infty e^{-\lambda t} c^{n-1} \\ &\quad \times (1 - e^{-\lambda t})^{n-1}\, dt \\ &= \text{MTTF } (n - 1 \text{ modules}) \\ &\quad + \frac{c^{n-1}}{n\lambda} \\ &= \frac{1}{\lambda c}\sum_{i=1}^{n} \frac{c^i}{i}\end{aligned} \quad (11)$$

The nth spare's contribution to MTTF is c^{n-1}/n times that of a single module. If c is not very close to 1.0, the added spare's contribution to MTTF is negligible.

The impact of improving coverage can also be demonstrated using mission time improvement. Setting Equation 4, with t replaced by It, equal to Equation 9, yields:

$$1 - Q_m(It)^n = R_m(t)\left(\frac{1 - c^n Q_m(t)^n}{1 - cQ_m(t)}\right)$$

Solving for I gives:

$$I = \frac{1}{\lambda t} ln\{1 - \{1 - R_m(t)\left(\frac{1 - c^n Q_m(t)^n}{1 - cQ_m(t)}\right)\}\} \quad (12)$$

Equation 12 is tabulated in Table 5-4 and plotted in Figure 5-5 for the value of $R_m(t) = 0.9$. Both

Table 5–3. Standby system reliability for various values of module reliability, coverage, and number of spares.

	Coverage								
n /	0.99			0.9			0.8		
R_m	2	4	∞	2	4	∞	2	4	∞
0.9	0.9891	0.9988	0.9989	0.9810	0.9889	0.9890	0.9720	0.9782	0.9783
0.8	0.9584	0.9960	0.9975	0.9440	0.9746	0.9756	0.9280	0.9518	0.9524
0.7	0.9079	0.9880	0.9957	0.8890	0.9538	0.9589	0.8680	0.9180	0.9211
0.6	0.8376	0.9689	0.9934	0.8160	0.9218	0.9375	0.7920	0.8731	0.8824
0.5	0.7475	0.9307	0.9901	0.7250	0.8718	0.9091	0.7000	0.8120	0.8333

illustrate the high sensitivity to the coverage parameter c.

M-of-N Systems

M-of-N systems are a generalization of the parallel model. However, instead of requiring only one of the N modules for the system to function, M modules are required. Consider triple modular redundancy (TMR), in which two of three must function in order for the system to function. Thus for module reliability R_m:

$$R_{\text{TMR}} = R_m^3 + \binom{3}{2} R_m^2(1 - R_m) \qquad (13)$$

Equation 13 enumerates all the working states. The R_m^3 term represents the state in which all three modules function. The $\binom{3}{2}R_m^2(1 - R_m)$ term represents the three states in which one module is failed and two are functional. Because the modules are assumed to be identical, all three states need not be enumerated. Any combination of two of the three modules is enumerated by the 3-take-2 combinatorial coefficient, denoted by $\binom{3}{2}$ where

$$\binom{N}{M} = \frac{N!}{(N - M)!\, M!}.$$

Table 5–4. Mission time improvement derived from increasing coverage from the indicated value to 1.0.

C	$n = 2$	$n = 4$
0.8	1.738	4.601
0.85	1.579	4.208
0.9	1.408	3.720
0.95	1.218	3.034
0.99	1.047	1.957

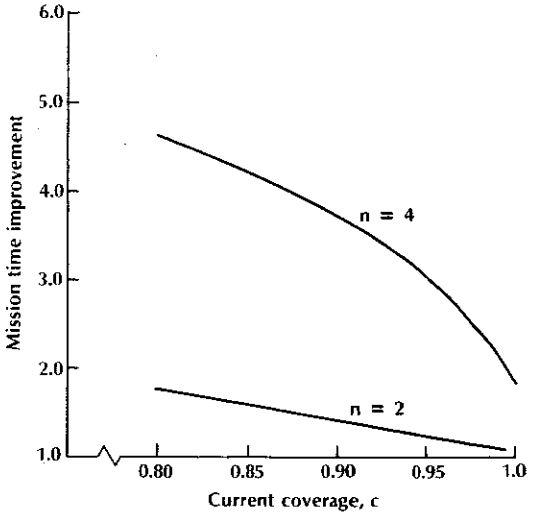


Figure 5–5. Potential mission time improvement with coverage increase from C to 1.0.

The M-of-N model can be generalized as: If there are N identical modules with the reliability of each module R_m (R_m may be a single number, such as a probability of success, or may be a function of time), and if a task requires k modules, the system can tolerate up to $N - k$ failures, and the reliability of such a system is:

$$R = \sum_{i=0}^{N-k} \binom{N}{i} R_m^{N-i}(1 - R_m)^i$$

We will use the M-of-N model to make several further points about system modeling, including incorrect conclusions drawn from single parameter summaries and the effect on redundant system reliability of extra logic (e.g., voters), more detailed modeling, more accurate modeling, and nonredundant components.

Single and Multiple Parameters. To compare different redundant systems, it is often desirable to summarize their models by a single parameter. The reliability may be an arbitrarily complex function of time and the selection of the wrong summary parameter could lead to incorrect conclusions. Consider, for example, TMR and MTTF. For the nonredundant system:

$$R_{\text{simplex}} = e^{-\lambda t}$$

$$\text{MTTF}_{\text{simplex}} = \frac{1}{\lambda}$$

For TMR with an exponential reliability function:

$$R_{\text{TMR}} = (e^{-\lambda t})^3 + \binom{3}{1}(e^{-\lambda t})^2(1 - e^{-\lambda t})$$

$$= 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

$$\text{MTTF}_{\text{TMR}} = \frac{3}{2\lambda} - \frac{2}{3\lambda}$$

$$= \frac{5}{6\lambda} < \frac{1}{\lambda} = \text{MTTF}_{\text{simplex}}$$

Thus, by the MTTF summary, TMR is worse than a simplex system.

Figure 5-6 plots the reliability functions for a simplex PDP-8 and a redundant PDP-8 (TMR

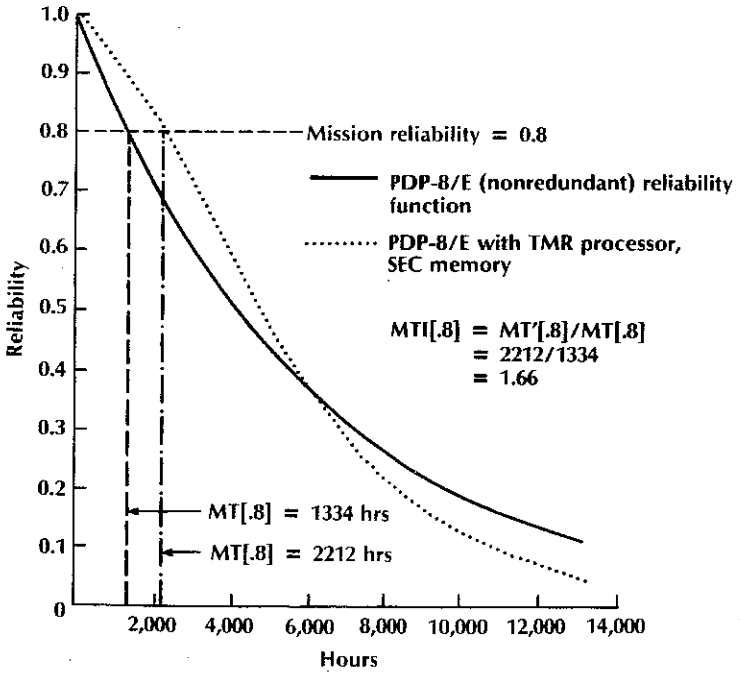


Figure 5–6. Relation of reliability function, mission time, and mission reliability.

processor and Hamming coded memory). Even though there is more area under the nonredundant curve (e.g., MTTF), the redundant system maintains a higher reliability for the first 6,000 hours of system life. Hence, comparison functions such as Mission Time Improvement (MTI) have been utilized to compare redundant systems in subregions of their operational life. The redundant PDP-8 in Figure 5-6 operates at or above a probability of success of 0.8, 66 percent longer than the simplex PDP-8. The S-shaped curve is typical of redundant systems; usually there is a well-defined knee. Above the knee, the redundant system has spare components that tolerate failures and keep the probability of system success high. Once the system has exhausted its redundancy, however, there is merely more hardware to fail (voters, switches, and other elements that support the redundancy) than in the nonredundant system. Thus, there is a sharper decrease in the redundant system's reliability function.

When modeling redundant systems with repair, single parameters such as MTTF may again be appropriate since the repair process replenishes the redundancy. There is no exhaustion phenomenon. This topic is discussed later in the chapter.

The Effect of Extra Logic in Redundant Systems.* In adding redundancy to a system, care must be taken that the extra logic to control the redundancy does not actually decrease the overall system reliability. Ingle and Siewiorek [1976] model various switches proposed for hybrid redundancy and show that the switch is a significant factor in determining the overall system reliability. A hybrid redundancy scheme with a TMR core may have a maximum attainable reliability for only one or two spares. Adding spares complicates the switch enough to cause the system reliability actually to decrease. There are conditions under which the switch becomes so complex that simple TMR would yield a better solution.

* This section is based on Ingle and Siewiorek [1976].

Consider the hybrid redundancy with a TMR voter described in Chapter 3. If only one of the three TMR core modules (those currently being voted on) is assumed to fail at a time, the system fails only if all the modules fail or if all but one module fails. The reliability of the hybrid system with a TMR core and $n - 3$ spares is:

$$R_{\text{hybrid}} = R_v \times R_{sw} \times \{1 - nR_m(1 - R_m)^{n-1} - (1 - R_m)^n\}$$

where R_v and R_{sw} are the voter and switch reliabilities, respectively. Subtracting the system reliability for n modules from that for $n + 1$ modules:

$$R_{sw} \times (1 - (n + 1) \times R_m(1 - R_m)^n - (1 - R_m)^{n+1})$$

$$-R_{sw} \times (1 - nR_m(1 - R_m)^{n-1} - (1 - R_m)^n)$$

$$= R_{sw} \times nR_m^2(1 - R_m)^{n-1}$$

This expression is positive for any $0 < R_m < 1$ and $n \geq 1$. Therefore, under the assumption that R_{sw} is independent of n, adding modules increases the system reliability. The switch typically becomes more complex as more modules are added, although the dependence of the switch complexity on n will be a function of the particular design. A reasonable assumption, however, is that switch complexity grows nearly linearly with n; that is, the addition of each module to the system increases switch complexity by a constant amount [Siewiorek and McCluskey, 1973]. Consequently, as a more realistic assumption we will consider the R_{sw} to be p^n, where p is the reliability of the switch component that must be added when a module is added. Further, let $p = R_m^\alpha$, where α is used to relate the relative complexities of the incremental switch component to the basic module. Hence, the system reliability is:

$$R_{\text{hybrid}} = R_m^{n\alpha}\{1 - nR_m(1 - R_m)^{n-1} - (1 - R_m)^n\}$$

standard SSI/MSI logic, Hamming code support circuitry has a failure rate several times that of the support circuitry for an equivalent nonredundant memory. Most current commercial designs use SSI/MSI support circuitry. Using more reliable LSI logic for ECC support would greatly improve the total ECC memory reliability.

Reduction of the Nonseries/Nonparallel Case

Sometimes a "success" diagram is used to describe the operational modes of a system. Figure 5-21a depicts a success diagram that is not directly reducible by application of the series/parallel formulas. Each path from terminal x to terminal y represents a configuration that leaves the system successfully operational. The exact reliability can be derived by expanding around a single module:

$$R_{sys} = R_m \times P(\text{system works} \mid m \text{ works}) + (1 - R_m) \times P(\text{system works} \mid m \text{ fails}) \quad (21)$$

where the notation $P(s|m)$ denotes the conditional probability "s given m has occurred."

Selecting module B to expand around, Equation 21 yields the two reduced diagrams in Figure 5-21b. In one, module B is replaced by a "short" (module B works); in the other, module B is replaced by an "open" (module B is failed and not available). Using the series/parallel reductions on the case where B is failed yields:

$$R_{sys} = R_B \times P(\text{system works} \mid B \text{ works}) + (1 - R_B)(R_D[1 - (1 - R_A R_E) \times (1 - R_F R_C)]) \quad (22)$$

The case for module B working has to be further reduced. Expanding around module C yields:

$$P(\text{system works} \mid B \text{ works}) = R_C[R_D(1 - (1 - R_A)(1 - R_F))] + (1 - R_C)[R_A R_D R_E]$$

Thus:

$$R_{sys} = R_B[R_C R_D(R_A + R_F - R_A R_F) + (1 - R_C)R_A R_D R_E] + (1 - R_B)[R_D(R_A R_E + R_F R_C - R_A R_C R_E R_F)]$$

Letting

$$R_A = R_B = R_C = R_D = R_E = R_F = R_m:$$

$$R_{sys} = R_m^6 - 3R_m^5 + R_m^4 + 2R_m^3$$

If the success diagram becomes too complex to evaluate exactly, upper- and lower-limit approximations on R_{sys} can be used. An upperbound on system reliability is [Essary and Proschan, 1962]:

$$R_{sys} \leqslant 1 - \Pi(1 - R_{\text{path } i}) \quad (23)$$

where $R_{\text{path } i}$ is the serial reliability of path i. Equation 23 calculates the system reliability as if all paths were in parallel. Placing the paths in parallel yields a Reliability Block Diagram (RBD). Figure 5-22 shows the RBD of Figure 5-21. Equation 23 is an upperbound because the paths are not independent; that is, the failure of a single module affects more than one path. Equation 23 is a close approximation when $R_{\text{path } i}$ is small.

Hence:

$$R_{sys} \leqslant 1 - (1 - R_A R_B R_C R_D)(1 - R_A R_E R_D) \times (1 - R_F R_C R_D) \quad (24)$$

Letting

$$R_A = R_B = R_C = R_D = R_E = R_F = R_m:$$

$$R_{sys} \leqslant 2R_m^3 + R_m^4 - R_m^6 - 2R_m^7 + R_m^{10}$$

The RBD method can be altered to yield an exact result.

Because the paths are not independent, perform the multiplication in Equation 23 by re-

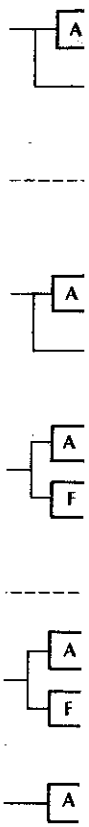


Figure 5–21 duced diag (working) a reduction v module C r

Figure 5–22 Figure 5-21.

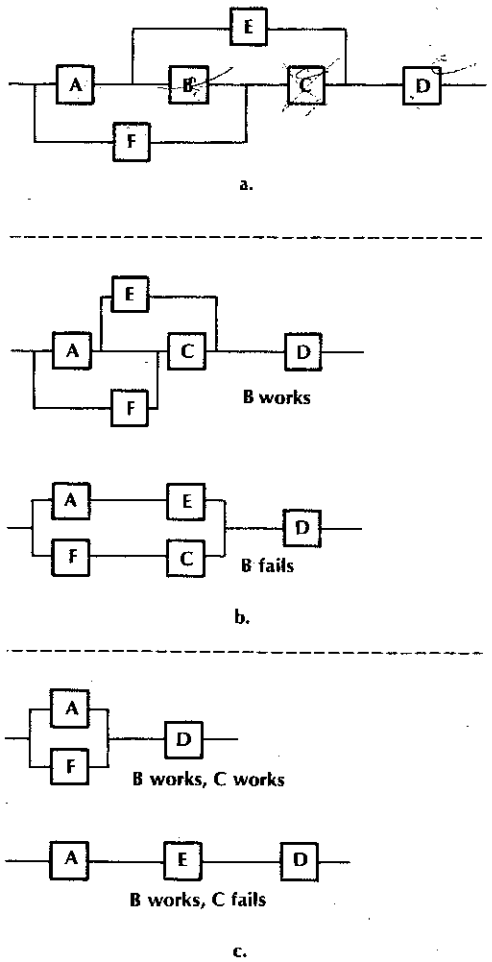


Figure 5–21. A system success diagram. a.) Reduced diagram replacing module B by a "short" (working) and an "open" (failed) b.) and further reduction with module B "shorted" (working) and module C replaced by an "open" and a "short" c.).

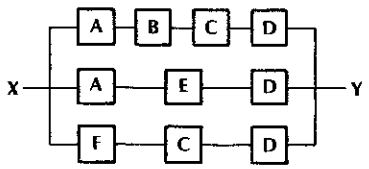


Figure 5–22. Reliability block diagram (RBD) of Figure 5-21.

placing R_m^i with R_m; that is, an individual module can only have its reliability raised to the first power.

$$\begin{aligned} R_{sys} = {} & R_A R_B R_C R_D + R_A R_E R_D \\ & - R_A R_B R_C R_D R_E \\ & + R_C R_D R_F - R_A R_C R_D R_E R_F \\ & - R_A R_B R_C R_D R_F \\ & + R_A R_B R_C R_D R_E R_F \end{aligned}$$

Letting

$$R_A = R_B = R_C = R_D = R_E = R_F = R_m:$$

$$R_{sys} = R_m^6 - 3R_m^5 + R_m^4 + 2R_m^3$$

which is the same result obtained from Equation 22. Setting all R_i's to R_m has to occur after the multiplication; otherwise, individual R_i's would be raised to higher than the first power and the result would be a lower bound. For obtaining exact reliability, the RBD approach is more suitable to noncomputerized calculations, because simplifying assumptions (such as $R_i = R_m$ for all i) can be made before algebraic expansion.

Essary and Proschan [1962] also define a lower bound in terms of the minimal cut sets of the system. Given that a minimal cut set is a list of components such that removal of any component from the list (by changing the component from operational to failed) will cause the system to change from operational to failed, a lower bound is given by:

$$R_{sys} \geq \Pi(1 - Q_{cut\ i}) \qquad (25)$$

where $Q_{cut\ i}$ is the probability that the minimal cut i does not occur. The minimal cut sets for Figure 5-21a are D, AC, AF, CE, and BEF. Hence assuming all modules are identical:

$$R_{sys} \geq R(1 - (1 - R)^2)^3(1 - (1 - R)^3)$$

and

$$R_{sys} \geq 24R^5 - 60R^6 + 62R^7 - 33R^8 + 9R^9 - R^{10}$$