
CHAPTER 3.5

RELIABLE SYSTEM DESIGN AND MODELING

Ronald T. Anderson, Richard L. Doyle, Stanislaw Kus,
Henry C. Rickers, S. Sugihara, James W. Wilbur

SYSTEM DESIGN

System reliability can be enhanced in several ways. A primary technique is through the application of *redundancy*. Other methods include *design simplification*, *degradation analysis*, *worst-case design*, *overstress analysis*, and *transient analysis*.

Redundancy

Depending on the specific applications a number of approaches are available to improve reliability through redundant design. They can be classified on the basis of how the redundant elements are introduced into the circuit to provide a parallel signal path. There are two major classes of redundancy.

In *active redundancy* external components are not required to perform the function of detection, decision, or switching when an element or path in the structure fails. In *standby redundancy* external elements are required to detect, make a decision, and switch to another element or path as a replacement for a failed element or path.

Techniques related to each of these two classes are depicted in the simplified tree structure of Fig. 3.5.1 Table 3.5.1 further defines each of the eight techniques.

Redundancy does not lend itself to categorization exclusively by element complexity. Although certain of the configurations in Table 3.5.1 are more applicable at the part or circuit level than at the equipment level, this occurs not because of inherent limitations of the particular configuration but because of such factors as cost, weight, and complexity.

Another form of redundancy can exist within normal nonredundant design configurations. Parallel paths within a network often are capable of carrying an added load when elements fail. This can result in a degraded but tolerable output. The allowable degree of degradation depends on the number of alternate paths available. Where a mission can still be accomplished using an equipment whose output is degraded, the definition of failure can be relaxed to accommodate degradation. Limiting values of degradation must be included in the new definition of failure. This slow approach to failure, *graceful degradation*, is exemplified by an array of elements configured to an antenna or an array of detectors configured to a receiver. In either case, individual elements may fail, reducing resolution, but if a minimum number operate, resolution remains good enough to identify a target.

The decision to use redundant design techniques must be based on a careful analysis of the tradeoffs involved. Redundancy may prove the only available method when other techniques of improving reliability have been exhausted or when methods of part improvement are shown to be more costly than duplications. Its use may offer an advantage when preventive maintenance is planned. The existence of a redundant element can

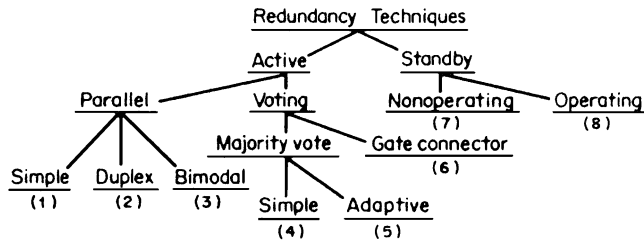


FIGURE 3.5.1 Redundancy techniques.

allow for repair with no system downtime. Occasionally, situations exist in which equipment cannot be maintained, e.g., spacecraft. In such cases, redundant elements may prolong operating time significantly.

The application of redundancy is not without penalties. It increases weight, space, complexity, design, cost, time to design, and maintenance cost. The increase in complexity results in an increase of unscheduled maintenance actions; safety and mission reliability is gained at the expense of logistics mean time between failures (MTBF).

In general, the reliability gain may be minimal for additional redundant elements beyond a few parallel elements. As illustrated in Fig. 3.5.2 for simple parallel redundancy, there is a diminishing gain in reliability and MTBF as the number of redundant elements is increased. As seen for the simple parallel case, the greatest gain, achieved through addition of the first redundant element, is equivalent to a 50 percent or more increase in the system MTBF. In addition to maintenance-cost increases because of the additional elements, reliability of certain redundant configurations may actually be less. This is a result of the serial reliability of switching or other peripheral devices needed to implement the particular redundancy configuration (see Table 3.5.1).

The effectiveness of certain redundancy techniques, especially standby redundancy, can be enhanced by repair. Standby redundancy allows repair of the failed unit (while operation of the unfailed unit continues uninterrupted) by virtue of the switching function built into the standby redundant configuration. The switchover function can also provide an indication that failure has occurred and that operation is continuing on the alternate channel. With a positive failure indication, delays in repair are minimized. A further advantage of switching is related to built-in test (BIT) objectives. Built-in test can be readily incorporated into a sensing and switchover network. Also, the hot swapping of redundant boards or modules minimizes system downtime.

An illustration of the enhancement of redundancy with repair is shown in Fig 3.5.3. The achievement of increased reliability through redundancy depends on effective isolation of redundant elements. Isolation is necessary to prevent failures from affecting other parts of the redundant network. The susceptibility of a particular design to failure propagation can be assessed by application of failure-mode-effects analysis.

Interdependence is most successfully achieved through standby redundancy, as represented by configurations classified as *decision with switching*, where the redundant element is disconnected until a failure is sensed. However, design based on such techniques must provide protection against switching transients and must consider the effects of switching interruptions on system performance.

Furthermore, care must be exercised to ensure that reliability gains from redundancy are not offset by increased failure rates because of switching devices, error detectors, and other peripheral devices needed to implement the redundancy configurations.

Design Simplification

Many complex electronic systems have subsystems or assemblies that operate serially. Many of their parts and circuits are in series so that only one need fail to stop the system. This characteristic, along with the increasing trend of complexity in new designs, tends to add more and more links to the chain, thus greatly increasing the statistical probability of failure.

Therefore, one of the steps in achieving reliability is to simplify the system and its circuits as much as possible without sacrificing performance. However, because of the general tendency to increase the loads on the components that remain, there is a limiting point to circuit simplification. This limit is the value of electrical stress that must not be exceeded for a given type of electrical component. Limit values can be established for

TABLE 3.5.1 Redundancy Techniques

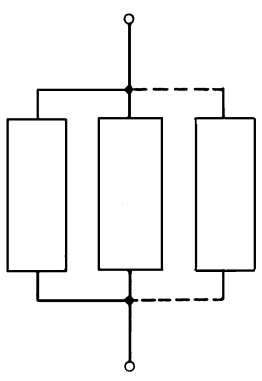
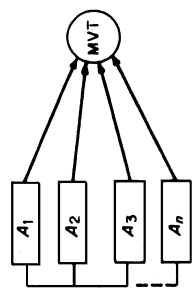
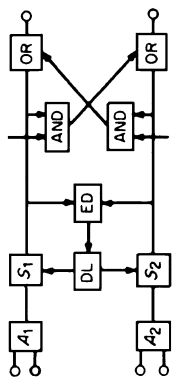
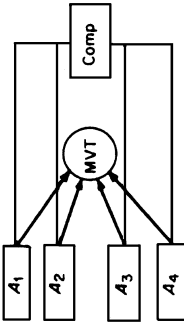
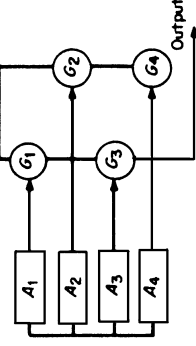
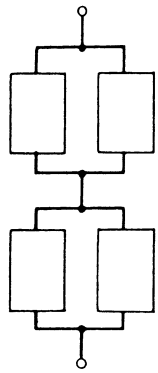
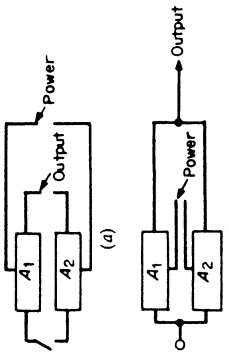
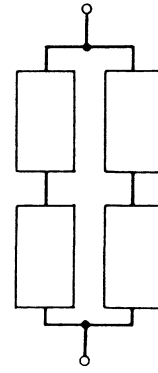
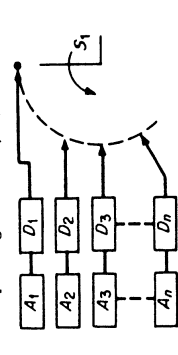
<p>Simple parallel redundancy</p>  <p>In its simplest form, redundancy consists of a simple parallel combination of elements; if any element fails open, identical paths exist through parallel redundant elements</p>	<p>Majority-voting redundancy</p>  <p>Decision can be built into the basic parallel redundant model by inputting signals from parallel elements into a voter to compare each signal with remaining signals; valid decisions are made only if the number of useful elements exceeds the failed elements</p>
<p>Duplex redundancy</p>  <p>This technique is applied to redundant logic sections, such as A_1 and A_2, operating in parallel; it is primarily used in computer applications where A_1 and A_2 can be used in duplex or active redundant modes or as a separate element; an error detector at the output of each logic section detects noncoincident outputs and starts a diagnostic routine to determine and disable the faulty element</p>	<p>Adaptive-majority logic</p>  <p>This technique exemplifies the majority logic configuration with a comparator and switching network to switch out or inhibit failed redundant elements</p>
<p>Gate-connector redundancy</p>  <p>Similar to majority voting; redundant elements are generally binary circuits; outputs of the binary elements are fed to switchlike gates, which perform the voting function; the gates contain no components whose failure would cause the redundant circuit to fail; any failures in the gate connector act as though the binary element were at fault</p>	<p>(Continued)</p>

TABLE 3.5.1 Redundancy Techniques (Continued)

<p>Bimodal parallel-series redundancy</p>  <p>(a)</p>	<p>A series connection of parallel redundant elements provides protection against shorts and opens; direct short across the network because of a single element's shorting is prevented by a redundant element in series; an open across the network is prevented by the parallel element; network (a) is useful when the primary element-failure mode is open; network (b) is useful when the primary element-failure mode is short</p>	<p>Standby redundancy</p>  <p>(a)</p> <p>(b)</p>	<p>A particular redundant element of a parallel configuration can be switched into an active circuit by connecting outputs of each element to switch poles; two switching configurations are possible: (a) the element may be isolated by the switch until switching is completed and power applied to the element in the switching operation; (b) all redundant elements are continuously connected to the circuit and a single redundant element activated by switching power to it</p>
<p>Bimodal series-parallel redundancy</p>  <p>(a)</p>		<p>Operating redundancy</p> 	<p>In this application, all redundant units operate simultaneously; a sensor on each unit detects failures; when a unit fails, a switch at the output transfers to the next unit and remains there until failure</p>

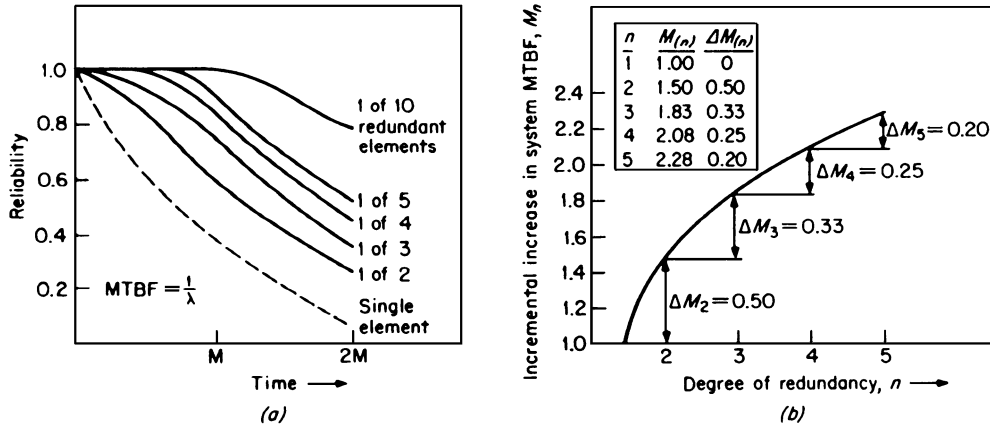


FIGURE 3.5.2 Decreasing gain in reliability as number of active elements increases: (a) simple active redundancy for one of n elements required and (b) incremental increase in system MTBF for n active elements.

various types of components as determined by their failure rates. In addition, it is also clear that the simplified circuit must meet performance criteria under application conditions, e.g., worst-case conditions.

Design simplification and substitution involves several techniques: the use of proved circuits with known reliability, the substitution of highly reliable digital circuitry where feasible, the use of high-reliability integrated circuits to replace discrete lumped-constant circuitry, the use of highly reliable components wherever individual discrete components are called for, and the use of designs that minimize the effects of catastrophic failure modes.

The most obvious way to eliminate the failure modes and mechanisms of a part is to eliminate the part itself. For instance, a digital design may incorporate extraneous logic elements. Minimization techniques, e.g., boolean reduction, are well established and can be powerful tools for incorporating reliability in a design through simplification. Simplification can also include the identification and removal of items that have no functional significance.

In addition, efforts should also be directed toward the reduction of the critical effects of component failures. The aim here is to reduce the result of catastrophic failures until a degradation in performance occurs. As an example, consider Fig. 3.5.4, which illustrates the design of filter circuits. A low-pass design, shown in

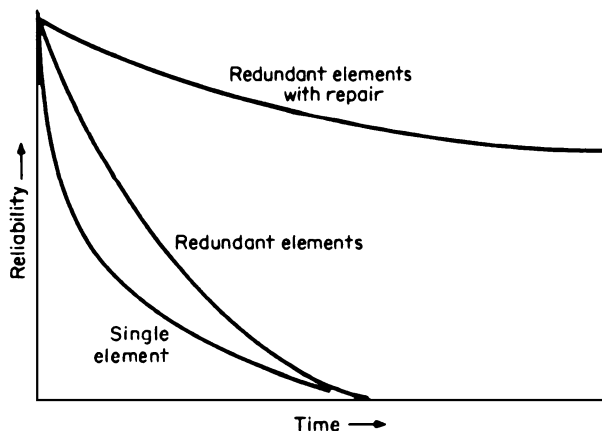


FIGURE 3.5.3 Reliability gain for repair of simple parallel redundant elements on failure.

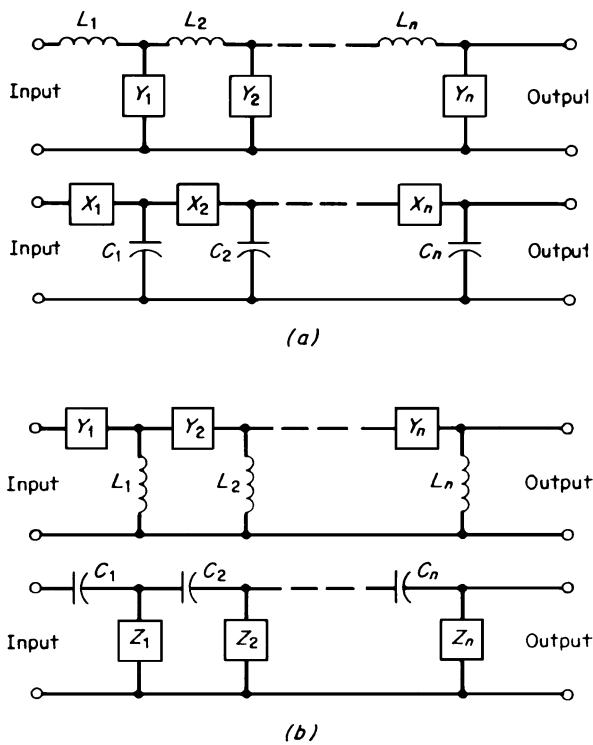


FIGURE 3.5.4 Alternative filter designs: (a) low-pass, (b) high-pass.

Fig. 3.5.4a, can involve either series inductances or shunt capacitances. The latter are to be avoided if shorting is the predominant failure mode peculiar to the applicable capacitor types, e.g., solid tantalum, since a catastrophic failure of the filter could result. Similarly, in the high-pass filter of Fig. 3.5.4b, using a shunt inductor is superior to using a series ceramic capacitor, for which an open is the expected failure mode. Here, the solid-tantalum capacitor, if applicable to the electrical design, could be the better risk, since its failure would result only in noise and incorrect frequency, not a complete loss of signal.

Degradation Analysis

There are basically two approaches to reduce part variation because of aging: control of device changes to hold them within limits for a specified time under stipulated conditions and the use of tolerant circuit design to accommodate drifts and degradation time. In the first category, a standard technique is to precondition the component by burn-in. In addition, there is detailed testing and control of the materials going into the part, along with strict control of fabrication processes.

In the second category, the objective is to design circuits that are inherently tolerant to part parameter change. Two different techniques are the use of feedback to compensate electrically for parameter variations and thus provide for performance stability and the design of circuits that provide the minimum required performance, even though the performance may vary somewhat because of aging. The latter approach makes use of analyses procedures such as worst-case analysis, parameter variation, statistical design, transient design, and stability analysis.

In the design of electronic circuits there are two ways to proceed. One is to view the overall circuit specification as a fixed requirement and to determine the allowable limits of each part parameter variation. Each part is then selected accordingly. The alternative approach is to examine the amount of parameter variation

expected in each part (including the input) and to determine the output under worst-case combination, or other types of combination, e.g., rms or average deviation. The result can be appraised with regard to determining the probability of surviving degradation for some specified period of time. Optimization programs are helpful in both types of design approach.

Worst-Case Analysis

In worst-case analysis, direct physical dependence must be taken into account. For example, if a voltage bus feeds several different points, the voltages at each of the several points should not be treated as variables independent of each other. Likewise, if temperature coefficients are taken into account, one part of the system should not be assumed to be at the hot limit and the other at the cold limit simultaneously unless it is physically reasonable for this condition to occur. A general boundary condition for the analysis is that the circuit or system should be constructed according to its specifications and that the analysis proceeds from there.

In the *absolute worst-case analysis*, the limits for each independent parameter are set without regard to other parameters or to its importance to the system. The position of the limits is usually set by engineering judgment or circuit analysis. In some cases, the designer may perform several analysis with different limits for each case to assess the result before fixing the limits.

Modified worst-case analyses are less pessimistic than absolute worst-case analysis. Typically, the method for setting the limits is to give limits to critical items as in absolute worst-case analysis and to give the rest of the items limits of the purchase tolerance.

In any worst-case analysis, the values of the parameters are adjusted (within the limits) so that circuit performance is as high as possible and then readjusted so it is as low as possible. The values of the parameters are not necessarily set at the limits; the criterion for their values is to drive the circuit performance to either extreme. The probability of this occurring in practice depends on the limits selected by the engineer at the outset, on the probability functions of the parameters, and on the complexity of the system being considered.

Computer Analyses. Computer routines are available for performing these analyses on electronic circuits. Generally speaking, the curve of circuit performance versus each independent parameter is assumed to be monotonic, and a numerical differentiation is performed at the nominal values to see in which direction the parameter should be moved to make circuit performance higher or lower. It is also assumed that this direction is independent of the values of any of the other parameters as long as they are within their limits. If these assumptions are not true, a much more detailed analysis of the equations is necessary before worst-case analysis can be performed. This involves generation of a response surface for the circuit performance which accounts for all circuit parameters.

Overstress and Transient Analysis

Semiconductor circuit malfunctions generally arise from two sources: *transient circuit disturbances* and *component burnout*. Transient upsets are generally overriding because they can occur at much lower energy levels.

Transient Malfunctions. Transients in circuits may prove troublesome in many ways. Flip-flops and Schmitt triggers may be triggered inadvertently, counters may change count, memory may be altered owing to driving current or direct magnetic field effect, one-shot multivibrators may pulse, the transient may be amplified and interpreted as a control signal, switches may change state, and semi-conductors may latch-up in undesired conducting states and require reset. The effect may be caused by transients at the input, output, or supply terminals or combination of these. Transient upset effects can be generally characterized as follows:

1. Circuit threshold regions for upset are very narrow; i.e., there is a very small voltage-amplitude difference between the largest signals which have no probability of causing upset and the smallest signals that will certainly cause upset.
2. The dc threshold for response to a very slow input swing is calculable from the basic circuit schematic. This can establish an accurate bound for transients that exceed the dc threshold for times longer than the circuit propagation delay (a manufacturer's specification).

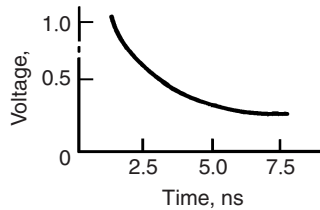


FIGURE 3.5.5 Square-pulse trigger voltage for typical low-level integrated circuit.

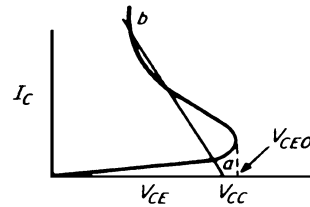


FIGURE 3.5.6 Latch-up response.

3. Transient upsets are remarkably independent in the exact waveshape, depending largely on the peak value of the transient and the length of time over which the transient exceeds the dc threshold. This waveform independence allows relatively easy experimental determination of circuit behavior with simple waveforms such as a square pulse.
4. The input leads or signal reference leads are generally the ones most susceptible to transient upset.

Standard circuit handbook data can often be used to gauge transient upset susceptibility. For example, square-pulse triggering voltage is sometimes given as a function of pulse duration. A typical plot for a low-level integrated circuit is shown in Fig 3.5.5.

Latch-up. There are various ways in which semiconductors may latch-up in undesired conducting states that require reset (power removal). One common situation is shown in Fig. 3.5.6, which shows an open-base transistor circuit with collector current as a function of collector-emitter voltage and the load line for a particular collector resistance. The collector current is normally low (operating point *a*), but a transient can move the operating level to point *b*, where the circuit becomes latched up at a high current level. The signal required to cause this event can be determined by noting that the collector-emitter voltage must be driven above the V_{CEO} (collector-emitter breakdown) voltage.

Another mode of latch-up can occur when a transistor is grown in a semiconductor substrate, e.g., an *npn* transistor in a doped *p*-substrate. Under usual voltage or gamma-radiation stress, the device can act like an SCR device, latching into conduction.

Transient Overstress. Although various system components are susceptible to stress damage, the most sensitive tend to be semiconductor components.

Transient Suppression. There are many techniques available for transient suppression; however, most involve zener diode clamps. Others include some of transistors, SCRs, CMOS, ITL, and diode protection. These techniques are representative of generally applicable methods and are not intended as an exhaustive list.

SYSTEM MODELING

The probability of survival or the reliability function denoted by $R(t)$ is the probability that no failures occur during the time interval $(0, t)$. The most commonly used reliability function is the exponential given by

$$R(t) = e^{-\lambda t} \quad \begin{array}{l} \lambda > 0 \\ t \geq 0 \end{array} \quad (1)$$

The failure density is the negative of the reliability function. For the exponential case the failure density is

$$f(t) = -R'(t) = \lambda e^{-\lambda t} \quad \begin{array}{l} \lambda > 0 \\ t \geq 0 \end{array} \quad (2)$$

The cumulative distribution $F(t)$ is the probability of failure up to time t and is simply given by $1 - R(T)$. For the exponential case where the density exists we have

$$F(t) = 1 - R(t) = \int_0^t f(z) dz = 1 - e^{-\lambda t} \quad \begin{array}{l} \lambda > 0 \\ t \geq 0 \end{array} \quad (3)$$

Thus for the exponential case we have the unique property of having a constant failure function.

In describing the reliability of a complex system the exponential function is rarely appropriate. The reliability function is generally nonexponential because (1) the system is composed of redundant elements (even if each element were itself exponential, the system is no longer exponential), and (2) the system experiences burn-in and wearout properties so that the failure rate is nonconstant. During burn-in the hazard function generally decreases, and during wearout the hazard function generally increases.

For systems formulated as (1), one is given the element reliabilities so that the system reliability can be obtained as a function of them. The particular function obtained depends on the type of redundancy used.

For systems formulated as (2), one is given the hazard function so that reliability is obtained as the solution of the linear differential equation

$$R(t) = -h(t)R(t) \quad \begin{array}{l} R(0) = 1 \\ t \geq 0 \end{array} \quad (4)$$

The solution of Eq. (4) is

$$R(t) = \exp\left(-\int_0^t h(z) dz\right) \quad t \geq 0 \quad (5)$$

In general, $h(t)$ need only be piecewise continuous. If failure time is truncated at $t = L$, then $R(t)$ is continuous in the half-open interval $(0, L)$ and the hazard function is not defined at $t = L$.

Reliability for a system is defined here as the product of individual module or branch reliabilities, where each module or branch reliability is made up of reliability functions described in categories (1) and/or (2).

Module-Reliability Models

This section describes various reliability models currently available. The models are developed at the module level, and the system reliability is the product of these module and branch reliabilities. Branch reliabilities are described later. The set of module reliabilities is not exhaustive; others may be developed.

Model 1: Active Exponential Redundant Reliability. There are n elements in parallel, each element is active with an identical exponential reliability. The module reliability is then

$$R(t) = 1 - (1 - e^{-\lambda t})^n \quad (6)$$

Equation 6 is simply 1 minus the probability that all n elements fail. The symbol λ is the failure rate of the exponential reliability model and is used in the models that follow whenever the exponential reliability model is assumed.

Model 2: Standby Exponential Redundant Reliability. There are n elements in parallel, each element in standby until called upon to operate. Each element has an identical exponential reliability and does not experience any degradation while on standby. The module reliability is then

$$R(t) = \sum_{x=0}^{n-1} \frac{e^{-\lambda t} (\lambda t)^x}{x!} \quad (7)$$

Model 3: Binomial Exponential (Active) Redundancy Reliability. There are n elements of which c are required to function properly for the module. Each element is assumed active with an identical exponential reliability. The module reliability is given by the binomial sum

$$R(t) = \sum_{x=c}^n \binom{n}{x} (e^{-\lambda t})^x (1 - e^{-\lambda t})^{n-x} \tag{8}$$

In Eq. (8) the variable x is interpreted as the number of successes. If we define N ($N = c, c + 1, \dots$) as the number of trials until c successes occur, we have the negative binomial sum for module reliability

$$R(t) = \sum_{N=c}^n \binom{N-1}{c-1} (e^{-\lambda t})^c (1 - e^{-\lambda t})^{N-c} \tag{9}$$

If we further define $y = N - c$ ($y = 0, 1, 2, \dots$) as the number of failures until c successes occur, we have an alternate form of the negative binomial sum for module reliability

$$R(t) = \sum_{y=0}^{n-c} \binom{c+y-1}{y} (e^{-\lambda t})^c (1 - e^{-\lambda t})^y \tag{10}$$

Model 4: Standby Exponential Redundant Reliability with Exponential Standby Failure. There are n elements in parallel standby as in model 2, but it is further assumed that the elements in standby have an exponential standby reliability with failure rate λ . Thus, each element has in addition to an identical exponential operational reliability an identical exponential standby reliability. The module reliability is then

$$R(t) = e^{-\lambda t} \sum_{x=1}^n \frac{(1 - e^{-\mu t})^{x-1} \Gamma(\beta + x - 1)}{\Gamma(x)\Gamma(\beta)} \tag{11}$$

where $\beta = \lambda/\mu$.

The special case for $\mu = 0$ (no standby failure) given as Eq. (7) is obtained from Eq. (11) by taking its limit as $1/\beta \rightarrow 0$.

Model 5: Open-Close Failure-Mode Exponential Redundant Reliability. There are n elements in series in each of m parallel lines, as shown in Fig 3.5.7. The reliability of the module illustrated is

$$R(t) = (1 - Q_b^m)^n - (1 - R_a^m)^n \tag{12}$$

where

$$Q_b = (1 - R_b) = q_b(1 - e^{-\rho t}) \quad Q_a = (1 - R_a) = q_a(1 - e^{-\rho t})$$

and where q_b = conditional probability of failure to close (valve) or failure to open (switch) given system failure = μ/ρ , q_a = conditional probability of failure to open (valve) or failure to close (switch) given system failure = λ/ρ , and $\rho = \lambda + \mu$. There is a total of nm elements in the module A configuration dual to the module illustrated in Fig. 3.5.7 is the “bridged” module, which is the same as that in Fig. 3.5.7 except that the dashed vertical lines are now made solid so that the module units are bridged. For this dual module the reliability is

$$R(t) = (1 - Q_a^m)^n - (1 - R_b^m)^n \quad R_b \geq Q_a \tag{13}$$

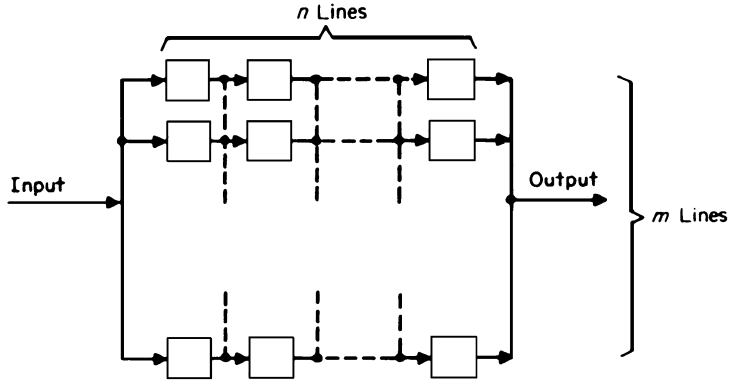


FIGURE 3.5.7 General open-close failure system.

Model 6: Gaussian Redundant Reliability. There are n identical Gaussian elements in standby redundancy, so that if t_i is the failure time of the i th elements, the module failure time is

$$t = \sum_{i=1}^n t_i \tag{14}$$

The individual elements are independent Gaussian with mean μ_0 and variance σ_0^2 . The module then is also Gaussian with mean and variance

$$\mu = n\mu_0 \quad \sigma^2 = n\sigma_0^2$$

The module reliability is therefore given by

$$R(t) = \frac{c}{\sqrt{2\pi\sigma}} \int_t^\infty e^{-(1/2)\sigma^2(x-\mu)^2} dx \quad t \geq 0 \tag{15}$$

where $c = 1/R(0)$

Model 7: Bayes Reliability for Inverted Gamma Function. The module reliability for a single standby element is given by

$$R(t) = R_1(t) + \int_0^t f_1(t_1)R_2(t-t_1)R_{2s}(t_1)dt_1 \tag{16}$$

- where $R_i(t)$ = reliability of i th element, $i = 1, 2$
- t_1 = failure time of first element ($i = 1$)
- $f_1(t)$ = failure density of first element [$= -R_1'(t)$]
- $R_{2s}(t)$ = reliability of second element in standby mode

Equation (16) is a general formulation of the two-element standby reliability in the sense that the element reliabilities are general. In particular, for the case where the reliabilities are exponential, Eq. (16) reduces to Eq. (11) for $n = 2$. For the case considered here it is assumed that the reliabilities are Bayesian estimates of

3.84 RELIABILITY

reliability where the mean-time-to-failure parameter of the exponential has an inverted gamma density. The reliabilities are given by

$$R_j(t) = \left(1 + \frac{t}{T + \mu}\right)^{-(r+v)} \quad j = 1, 2 \quad (17)$$

and

$$R_{2s}(t) = \left(1 + \frac{t}{T + \mu'}\right)^{-(r+v')} \quad (18)$$

where T = test time

r = number of failures in time T

μ , v , μ' , and v' = inverted gamma parameters

It is noted in Eqs. (17) and (18) that both elements have the same active reliability. In the application of this model the parameters are modeled as follows:

$$\mu = K\theta_A \left(1 + \frac{1}{W^2}\right) \quad v = \left(2 + \frac{1}{W^2}\right) \quad \text{or} \quad \mu' = \mu/K_1 \quad v' = v \quad (19)$$

where K and W are the scale factors on the mean and standard deviation of the a priori mean time to failure (inverted-gamma) variable and K_1 is the ratio between the means for the active and standby reliabilities. when $K = 1$, the mean is equal to θ_A , and when $W = 1$, the standard deviation is equal to $K\theta_A$. The relations of Eqs. (17) and (18) define a specific application of Eq. (16).

Model 8: Reliability Model for Weibull Distribution. The Weibull reliability model is presented in Chap. 3.3 (see "Failure Time Distributions"). Also related to the Weibull distribution is "Specific Hazard Rate Model," also in Chap. 3.3.

Model 9: Accelerated Life Model for all Distribution. The accelerated life model is presented in Chap. 3.3. This model is a function of temperature and time.

Model 10: Reliability Model for Hazard Function Compound of Three Piecewise Continuous Functions. The general reliability model considered here is for the hazard function described in Chap. 3.3.

$$\lambda(t) = \begin{cases} h_1(t) & 0 \leq t < t_1 \\ h_2(t) & t_1 \leq t < t_2 \\ h_3(t) & t_2 \leq t < \infty \end{cases} \quad (20)$$

The particular case considered here is where h_1 and h_3 are Weibull hazard functions and h_2 is the exponential hazard function. Further, it is assumed that the hazard function is continuous at the transit t_1 and t_2 so that we have

$$\begin{aligned} h_1(t) &= \alpha_1 \lambda_1 t^{\alpha_1 - 1} & 0 \leq t < t_1 \\ h_2(t) &= \lambda & t_1 \leq t < t_2 \\ h_3(t) &= \lambda_2 \lambda_2 t^{\alpha_2 - 1} & t_2 \leq t < \infty \end{aligned} \quad (21)$$

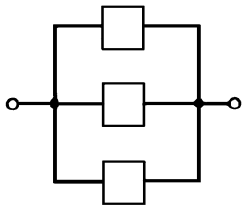


FIGURE 3.5.8 Branch system *a* consisting of a model 3 module.

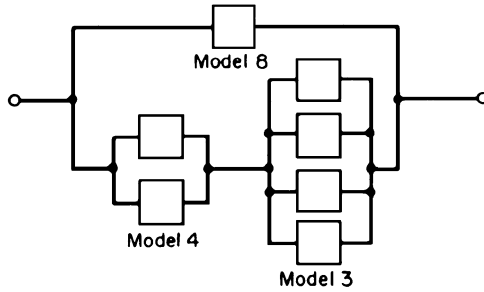


FIGURE 3.5.9 Branch system *b* consisting of models 3, 4, and 8.

where

$\alpha_1, \alpha_2, t_1, t_2,$ and λ are input parameters

$$\lambda_i = \frac{\lambda}{\alpha_i t_i^{\alpha_i - 1}} \quad i = 1, 2$$

Model 11: Tabular Reliability Model. An arbitrary reliability function can be evaluated as an input table of reliability versus time. For each output time, reliability is obtained by interpolation of the input table. This capability is useful as an approximation to a complex reliability model and is also useful in evaluating a reliability function that is available as a plot or a table for which no mathematical model is available.

Model 12: Active Exponential Redundant Reliability with Different Redundant Failure Rate. There are n elements in parallel. The original c elements are exponential each with failure rate λ . The $n - c$ remaining exponential elements in active parallel with the original elements each have failure rate μ . The module reliability is

$$R_s(t) = 1 - (1 - e^{-\lambda t})^c (1 - e^{-\mu t})^{n-c} \tag{22}$$

Branch-Reliability Models

A branch-reliability model is a model that evaluates reliability (at each instant in time) for a set of modules arranged in branches. Each branch individually consists of a set of modules. In particular, a branch may be a module itself. Some typical branches are shown in Figs. 3.5.8 to 3.5.10 and are identified as branches *a*, *b*, and *c*, respectively.

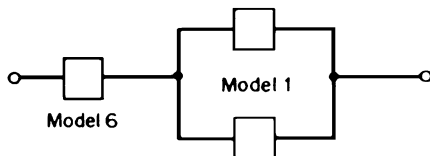


FIGURE 3.5.10 Branch system *c* consisting of models 1 and 6.

Branch system *a* is simply a module. Branch system *c* is a branch consisting of two modules in series and can be evaluated as two separate modules. Branch system *b* is made up of two subbranches in parallel.

A more complex branch system consisting of subbranch systems *a*, *b*, and *c* is shown in Fig. 3.5.11. Branches *a* and *b* are in series in active redundancy to branch system *c*.

Although the reliability functions for particular branch models are not developed here, clearly it is possible, and a generalized computer program based on both module and branch models can be developed.

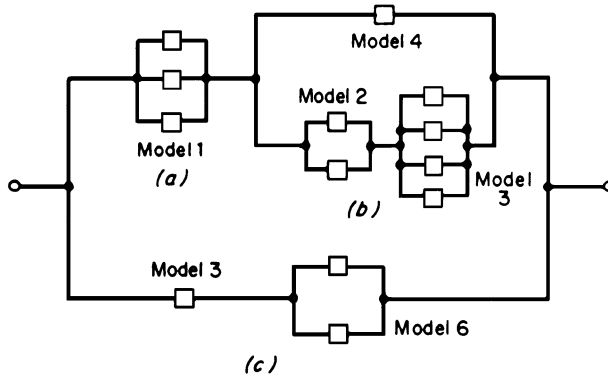


FIGURE 3.5.11 System consisting of branch systems shown in Figs.

The Systems Model

The system reliability model is obtained as the product of the individual branch reliabilities. In addition, the branch reliabilities are multiplied by a system exponential reliability factor and a constant factor; thus

$$R_s(t) = P_0 e^{-\lambda_s t} \prod_{i=1}^{K'} R_i(t) \tag{23}$$

where λ_s = exponential hazard function for system elements not included in branches

- P_0 = system reliability factor
- $R_i(t)$ = i th branch reliability, $i = 1, 2, \dots, K'$
- K' = number of branches in series

BIBLIOGRAPHY

Brombacher, A. C., "Reliability by Design: CAE Techniques for Electronic Components and Systems," Wiley, 1992.
 Choi, M., N. Park, and F. Lombardi, "Hardware-Software Co-reliability in Field Reconfigurable Multiprocessor Memory Systems," IPDPS, 2000.
 "Fault-Tree Analysis Application Guide," *FTA, RAC*.
 Rao, S. S., "Reliability-Based Design," McGraw-Hill, 1992.
 "Testability Design and Assessment Tools," *TEST, RAC*.
 "Thermal Guide for Reliability Engineers," *RADC-TR-82-172, AD118839, NTIS*.
 "Worst-Case Circuit Analysis Guidelines," *WCCA, RAC*.