C_1, C_2 Complexity factors; functions of the number of gates on the chip and the number of pins in the package.

Further details can be found in *MIL-HDBK-217E*, which is a handbook produced by the U.S. Department of Defense.

Devices operating in space, which is replete with charged particles and can subject devices to severe temperature swings, can thus be expected to fail much more often than their counterparts in air-conditioned offices, so too can computers in automobiles (which suffer high temperatures and vibration) and industrial applications.

2.2 Failure Rate, Reliability, and Mean Time to Failure

In this section, we consider a single component of a more complex system, and show how reliability and Mean Time to Failure (MTTF) can be derived from the basic notion of failure rate. Consider a component that is operational at time $t = 0$ and remains operational until it is hit by a failure. Suppose now that all failures are permanent and irreparable. Let T denote the lifetime of the component (the time until it fails), and let $f(t)$ and $F(t)$ denote the probability density function of T and the cumulative distribution function of T, respectively. These functions are defined for $t \geqslant 0$ only (because the lifetime cannot be negative) and are related through

$$f(t) = \frac{\mathrm{d}F(t)}{\mathrm{d}t}, \qquad F(t) = \int_0^t f(\tau)\,\mathrm{d}\tau \tag{2.2}$$

$f(t)$ represents (but is not equal to) the momentary probability of failure at time t. To be exact, for a very small Δt, $f(t)\Delta t \approx \mathrm{Prob}\{t \leqslant T \leqslant t + \Delta t\}$. Being a density function, $f(t)$ must satisfy

$$f(t) \geqslant 0 \quad \text{for } t \geqslant 0 \quad \text{and} \quad \int_0^\infty f(t)\,\mathrm{d}t = 1$$

$F(t)$ is the probability that the component will fail at or before time t,

$$F(t) = \mathrm{Prob}\{T \leqslant t\}$$

$R(t)$, the reliability of a component (the probability that it will survive at least until time t), is given by

$$R(t) = \mathrm{Prob}\{T > t\} = 1 - F(t) \tag{2.3}$$

$f(t)$ represents the probability that a *new* component will fail at time t in the future. A more meaningful quantity is the probability that a good component of current age t will fail in the next instant of length $\mathrm{d}t$. This is a *conditional* probability, since

we know that the component survived at least until time t. This conditional probability is represented by the *failure rate* (also called the *hazard rate*) of a component at time t, denoted by $\lambda(t)$, which can be calculated as follows:

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \tag{2.4}$$

Since $\frac{dR(t)}{dt} = -f(t)$, we obtain

$$\lambda(t) = -\frac{1}{R(t)} \frac{dR(t)}{dt} \tag{2.5}$$

Certain types of components suffer no aging and have a failure rate that is constant over time, $\lambda(t) = \lambda$. In this case,

$$\frac{dR(t)}{dt} = -\lambda R(t)$$

and the solution of this differential equation (with $R(0) = 1$) is

$$R(t) = e^{-\lambda t} \tag{2.6}$$

Therefore, a constant failure rate implies that the lifetime T of the component has an exponential distribution, with a parameter that is equal to the constant failure rate λ

$$f(t) = \lambda e^{-\lambda t} \qquad F(t) = 1 - e^{-\lambda t} \qquad R(t) = e^{-\lambda t} \quad \text{for } t \geqslant 0$$

For an irreparable component, the MTTF is equal to its expected lifetime, $E[T]$ (where $E[\,]$ denotes the expectation or mean of a random variable)

$$\text{MTTF} = E[T] = \int_0^\infty t f(t)\, dt \tag{2.7}$$

Substituting $\frac{dR(t)}{dt} = -f(t)$ yields

$$\text{MTTF} = -\int_0^\infty t \frac{dR(t)}{dt}\, dt = -tR(t)\Big|_0^\infty + \int_0^\infty R(t)\, dt = \int_0^\infty R(t)\, dt \tag{2.8}$$

(the term $-tR(t)$ is equal to zero when $t = 0$ and when $t = \infty$, since $R(\infty) = 0$).

For the case of a constant failure rate for which $R(t) = e^{-\lambda t}$,

$$\text{MTTF} = \int_0^\infty e^{-\lambda t}\, dt = \frac{1}{\lambda}$$

Although a constant failure rate is used in most calculations of reliability (mainly owing to the simplified derivations), there are cases for which this simplifying

assumption is inappropriate, especially during the "infant mortality" and "wear-out" phases of a component's life (Figure 2.1). In such cases, the Weibull distribution is often used. This distribution has two parameters, λ and β, and has the following density function of the lifetime T of a component:

$$f(t) = \lambda\beta t^{\beta-1} e^{-\lambda t^{\beta}} \tag{2.9}$$

The corresponding failure rate is

$$\lambda(t) = \lambda\beta t^{\beta-1} \tag{2.10}$$

This failure rate is an increasing function of time for $\beta > 1$, is constant for $\beta = 1$, and is a decreasing function of time for $\beta < 1$. This makes it very flexible, and especially appropriate for the wear-out and infant mortality phases. The component reliability for a Weibull distribution is

$$R(t) = e^{-\lambda t^{\beta}} \tag{2.11}$$

and the MTTF of the component is

$$\text{MTTF} = \frac{\Gamma(\beta^{-1})}{\beta\lambda^{\beta^{-1}}} \tag{2.12}$$

where $\Gamma(x) = \int_0^{\infty} y^{x-1} e^{-y}\, dy$ is the Gamma function. The Gamma function is a generalization of the factorial function to real numbers, and satisfies

- $\Gamma(x) = (x-1)\Gamma(x-1)$ for $x > 1$;
- $\Gamma(0) = \Gamma(1) = 1$;
- $\Gamma(n) = (n-1)!$ for an integer n, $n = 1, 2, \ldots$.

Note that the Weibull distribution includes as a special case ($\beta = 1$) the exponential distribution with a constant failure rate λ.

With these preliminaries, we now turn to structures that consist of more than one component.

2.3 Canonical and Resilient Structures

In this section, we consider some canonical structures, out of which more complex structures can be constructed. We start with the basic series and parallel structures, continue with non-series/parallel ones, and then describe some of the many resilient structures that incorporate redundant components (next referred to as modules).

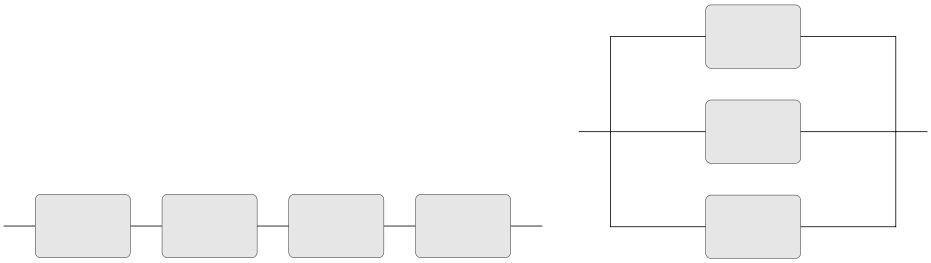

FIGURE 2.2 Series and parallel systems.

2.3.1 Series and Parallel Systems

The most basic structures are the series and parallel systems depicted in Figure 2.2. A *series system* is defined as a set of N modules connected together so that the failure of any one module causes the entire system to fail. Note that the diagram in Figure 2.2a is a reliability diagram and not always an electrical one; the output of the first module is not necessarily connected to the input of the second module. The four modules in this diagram can, for example, represent the instruction decode unit, execution unit, data cache, and instruction cache in a microprocessor. All four units must be fault-free for the microprocessor to function, although the way they are connected does not resemble a series system.

Assuming that the modules in Figure 2.2a fail independently of each other, the reliability of the entire series system is the product of the reliabilities of its N modules. Denoting by $R_i(t)$ the reliability of module i and by $R_s(t)$ the reliability of the whole system,

$$R_s(t) = \prod_{i=1}^{N} R_i(t) \tag{2.13}$$

If module i has a constant failure rate, denoted by λ_i, then, according to Equation 2.6, $R_i(t) = e^{-\lambda_i t}$, and consequently,

$$R_s(t) = e^{-\lambda_s t} \tag{2.14}$$

where $\lambda_s = \sum_{i=1}^{N} \lambda_i$. From Equation 2.14 we see that the series system has a constant failure rate equal to λ_s (the sum of the individual failure rates), and its MTTF is therefore $\text{MTTF}_s = \frac{1}{\lambda_s}$.

A *parallel system* is defined as a set of N modules connected together so that it requires the failure of all the modules for the system to fail. This leads to the

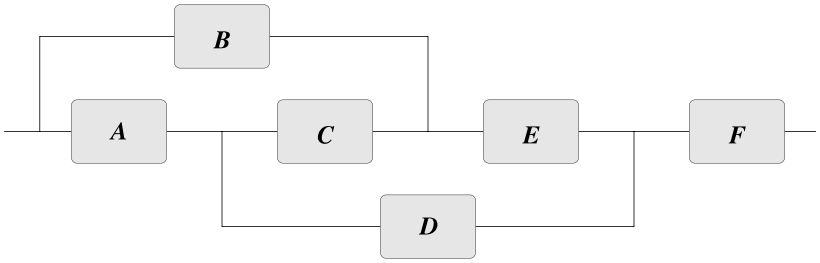

FIGURE 2.3 A non-series/parallel system.

following expression for the reliability of a parallel system, denoted by $R_p(t)$:

$$R_p(t) = 1 - \prod_{i=1}^{N} \left(1 - R_i(t)\right) \tag{2.15}$$

If module i has a constant failure rate λ_i, then

$$R_p(t) = 1 - \prod_{i=1}^{N} \left(1 - e^{-\lambda_i t}\right) \tag{2.16}$$

As an example, the reliability of a parallel system consisting of two modules with constant failure rates λ_1 and λ_2 is given by

$$R_p(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$$

Note that a parallel system does not have a constant failure rate; its failure rate decreases with each failure of a module. It can be shown that the MTTF of a parallel system with all its modules having the same failure rate λ is $\text{MTTF}_p = \sum_{k=1}^{N} \frac{1}{k\lambda}$.

2.3.2 Non-Series/Parallel Systems

Not all systems have a reliability diagram with a series/parallel structure. Figure 2.3 depicts a non-series/parallel system whose reliability cannot be calculated using either Equation 2.13 or 2.15. Each path in Figure 2.3 represents a configuration that allows the system to operate successfully. For example, the path *ADF* means that the system operates successfully if all three modules *A*, *D* and *F* are fault-free. A path in such reliability diagrams is valid only if all modules and edges are traversed from left to right. The path *BCDF* in Figure 2.3 is thus invalid. No graph transformations that may result in violations of this rule are allowed.

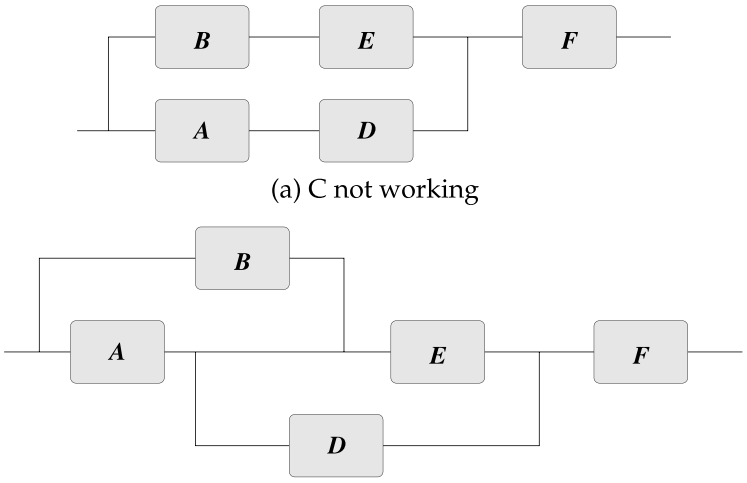

FIGURE 2.4 Expanding the diagram in Figure 2.3 about module *C*.

In the following analysis, the dependence of the reliability on the time t is omitted for simplicity of notation, although it is implied that all reliabilities are functions of t.

We calculate the reliability of the non-series/parallel system in Figure 2.3 by expanding about a single module i. That is, we condition on whether or not module i is functional, and use the Total Probability formula.

$$R_{\text{system}} = R_i \cdot \text{Prob}\{\text{System works}|i \text{ is fault-free}\} + (1 - R_i) \cdot \text{Prob}\{\text{System works}|i \text{ is faulty}\} \quad \textbf{(2.17)}$$

where, as before, R_i denotes the reliability of module i ($i = A, B, C, D, E, F$). We can now draw two new diagrams. In the first, module i will be assumed to be working, and in the second, module i will be faulty. Module i is selected so that the two new diagrams are as close as possible to simple series/parallel structures for which we can then use Equations 2.13 and 2.15. Selecting module C in Figure 2.3 results in the two diagrams in Figure 2.4. The process of expanding is then repeated until the resulting diagrams are of the series/parallel type. Figure 2.4a is already of the series/parallel type, whereas Figure 2.4b needs further expansion about E. Note that Figure 2.4b should not be viewed as a parallel connection of A and B, connected serially to D and E in parallel; such a diagram will have the path $BCDF$, which is not a valid path in Figure 2.3. Based on Figure 2.4 we can write, using Equation 2.17,

$$R_{\text{system}} = R_C \cdot \text{Prob}\{\text{System works}|C \text{ is fault-free}\} + (1 - R_C)R_F\big[1 - (1 - R_A R_D)(1 - R_B R_E)\big] \quad \textbf{(2.18)}$$

Expanding the diagram in Figure 2.4b about E yields

$$\begin{aligned}&\text{Prob\{System works}|C \text{ is fault-free}\}\\&= R_E R_F\big[1-(1-R_A)(1-R_B)\big]+(1-R_E)R_A R_D R_F\end{aligned}$$

Substituting this last expression in 2.18 results in

$$\begin{aligned}R_{\text{system}} = {} & R_C\big[R_E R_F(R_A+R_B-R_A R_B)+(1-R_E)R_A R_D R_F\big]\\&+(1-R_C)\big[R_F(R_A R_D+R_B R_E-R_A R_D R_B R_E)\big]\end{aligned} \tag{2.19}$$

If $R_A = R_B = R_C = R_D = R_E = R_F = R$, then

$$R_{\text{system}} = R^3\big(R^3-3R^2+R+2\big) \tag{2.20}$$

If the diagram of the non-series/parallel structure is too complicated to apply the above procedure, upper and lower bounds on R_{system} can be calculated instead.

An upper bound is given by

$$R_{\text{system}} \leqslant 1-\prod\big(1-R_{\text{path }i}\big) \tag{2.21}$$

where $R_{\text{path }i}$ is the reliability of the series connection of the modules along path i. The bound in Equation 2.21 assumes that all the paths are in parallel and that they are independent. In reality, two of these paths may have a module in common, and the failure of this module will result in both paths becoming faulty. That is why Equation 2.21 provides only an upper bound rather than an exact value. As an example, let us calculate the upper bound for Figure 2.3. The paths are ADF, BEF, and $ACEF$, resulting in

$$R_{\text{system}} \leqslant 1-(1-R_A R_D R_F)(1-R_B R_E R_F)(1-R_A R_C R_E R_F) \tag{2.22}$$

If $R_A = R_B = R_C = R_D = R_E = R_F = R$, then $R_{\text{system}} \leqslant R^3(R^7-2R^4-R^3+R+2)$, which is less accurate than the exact calculation in Equation 2.20.

The upper bound can be used to derive the exact reliability, by performing the multiplication in Equation 2.22 (or Equation 2.21 in the general case) and replacing every occurrence of R_i^k by R_i. Since each module is used only once, its reliability should not be raised to any power greater than 1. The reader is invited to verify that applying this rule to the upper bound in Equation 2.22 yields the same exact reliability as in Equation 2.19.

A lower bound can be calculated based on minimal cut sets of the system diagram, where a minimal cut set is a minimal list of modules such that the removal (due to faults) of all modules from the set will cause a working system to fail. The lower bound is obtained by

$$R_{\text{system}} \geqslant \prod\big(1-Q_{\text{cut }i}\big) \tag{2.23}$$

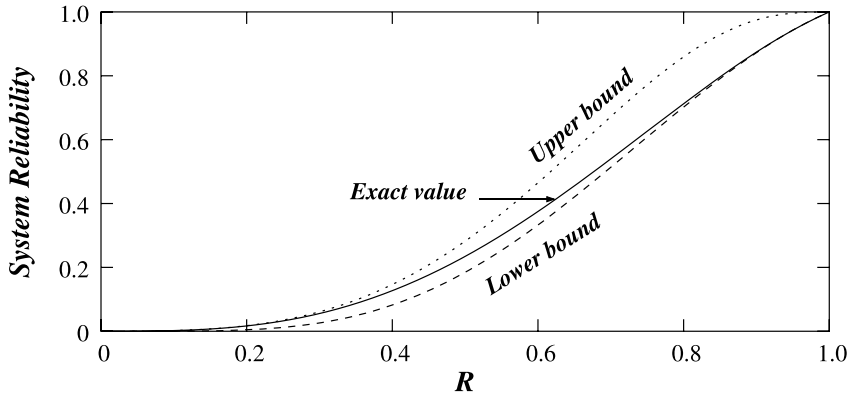

FIGURE 2.5 Comparing the exact reliability of the non-series/parallel system in Figure 2.3 to its upper and lower bounds.

where $Q_{\text{cut}\,i}$ is the probability that minimal cut i is faulty. In Figure 2.3, the minimal cut sets are F, AB, AE, DE, and BCD. Consequently,

$$R_{\text{system}} \geqslant R_F\big[1-(1-R_A)(1-R_B)\big]\big[1-(1-R_A)(1-R_E)\big]\big[1-(1-R_D)(1-R_E)\big] \times\big[1-(1-R_B)(1-R_C)(1-R_D)\big] \quad \textbf{(2.24)}$$

If $R_A = R_B = R_C = R_D = R_E = R_F = R$, then $R_{\text{system}} \geqslant R^5(24 - 60R + 62R^2 - 33R^3 + 9R^4 - R^5)$. Figure 2.5 compares the upper and lower bounds to the exact system reliability for the case in which all six modules have the same reliability R. Note that in this case, for the more likely high values of R, the lower bound provides a very good estimate for the system reliability.

2.3.3 *M*-of-*N* Systems

An M-of-N system is a system that consists of N modules and needs at least M of them for proper operation. Thus, the system fails when fewer than M modules are functional. The best-known example of this type of systems is the triplex, which consists of three identical modules whose outputs are voted on. This is a 2-of-3 system: so long as a majority (2 or 3) of the modules produce correct results, the system will be functional.

Let us now compute the reliability of an M-of-N system. We assume as before that the failures of the different modules are statistically independent and that there is no repair of failing modules. If $R(t)$ is the reliability of an individual module (the probability that the module is still operational at time t), the reliability of an M-of-N system is the probability that M or more modules are functional at