Reliability of Systems with Multiple Failure Modes

Hoang Pham

Chapter 2

2.1 Introduction

A component is subject to failure in either open or closed modes. Networks of relays, fuse systems for warheads, diode circuits, fluid flow valves, *etc.* are a few examples of such components. Redundancy can be used to enhance the reliability of a system without any change in the reliability of the individual components that form the system. However, in a two-failure mode problem, redundancy may either increase or decrease the system's reliability. For example, a network consisting of n relays in series has the property that an open-circuit failure of any one of the relays would cause an open-mode failure of the system and a closed-mode failure of the system. (The designations "closed mode" and "short mode" both appear in this chapter, and we will use the two terms interchangeably.) On the other hand, if the n relays were arranged in parallel, a closed-mode failure of any one relay would cause a system closed-mode failure, and an open-mode failure of all n relays would cause an open-mode failure of the system. Therefore, adding components in the system may decrease the system reliability. Diodes and transistors also exhibit open-mode and short-mode failure behavior.

For instance, in an electrical system having components connected in series, if a short circuit occurs in one of the components, then the short-circuited component will not operate but will permit flow of current through the remaining components so that they continue to operate. However, an open-circuit failure of any of the components will cause an open-circuit failure of the system. As an example, suppose we have a number of 5 W bulbs that remain operative in satisfactory conditions at voltages ranging between 3 V and 6 V. Obviously, on using the well-known formula in physics, if these bulbs are arranged in a series network to form a two-failure mode system, then the maximum and the minimum number of bulbs at these voltages are $n = 80$ and $k = 40$, respectively, in a situation when the system is operative at 240 V. In this case, any of the bulbs may fail either in closed or in open mode till the system is operative with 40 bulbs. Here, it is clear that, after each failure in closed mode, the rate of failure of a bulb in open mode increases due to the fact that the voltage passing through each bulb increases as the number of bulbs in the series decreases.

System reliability where components have various failure modes is covered in References [1–11]. Barlow *et al.* [1] studied series–parallel and parallel–series systems, where the size of each subsystem was fixed, but the number of subsystems was varied to maximize reliability. Ben-Dov [2] determined a value of k that maximizes the reliability of k-out-of-n systems. Jenney and Sherwin [4] considered systems in which the components are i.i.d. and subject to mutually exclusive open and short failures. Page and Perry [7] discussed the problem of designing the most reliable structure of a given number of i.i.d. components and proposed an alternative algorithm for selecting near-optimal configurations for large systems. Sah and Stiglitz [10] obtained a necessary and sufficient condition for determining a threshold value that maximizes the mean profit of k-out-of-n systems. Pham and Pham [9] further studied the effect of system parameters on the optimal k or n and showed that there does not exist a (k, n) maximizing the mean system profit.

This chapter discusses in detail the aspects of the reliability optimization of systems subject to two types of failure. It is assumed that the system component states are statistically independent and identically distributed, and that no constraints are imposed on the number of components to be used. Reliability optimization of series, parallel, parallel–series, series–parallel, and k-out-of-n systems subject to two types of failure will be discussed next.

In general, the formula for computing the reliability of a system subject to two kinds of failure is [6]:

$$\begin{aligned}\text{System reliability} &= \Pr\{\text{system works in both modes}\}\\ &= \Pr\{\text{system works in open mode}\}\\ &\quad - \Pr\{\text{system fails in closed mode}\}\\ &\quad + \Pr\{\text{system fails in both modes}\}\end{aligned} \tag{2.1}$$

When the open- and closed-mode failure structures are dual of one another, *i.e.* Pr{system fails in both modes} $= 0$, then the system reliability given by Equation 2.1 becomes

$$\begin{aligned}\text{System reliability} &= 1 - \Pr\{\text{system fails in open mode}\}\\ &\quad - \Pr\{\text{system fails in closed mode}\}\end{aligned} \tag{2.2}$$

We adopt the following notation:

- q_o the open-mode failure probability of each component ($p_o = 1 - q_o$)
- q_s the short-mode failure probability of each component ($p_s = 1 - q_s$)
- $\bar{\Phi}$ implies $1 - \Phi$ for any Φ
- $\lfloor x \rfloor$ the largest integer not exceeding x
- $*$ implies an optimal value.

2.2 The Series System

Consider a series system consisting of n components. In this series system, any one component failing in an open mode causes system failure, whereas all components of the system must malfunction in short mode for the system to fail.

The probabilities of system fails in open mode and fails in short mode are

$$F_o(n) = 1 - (1 - q_o)^n$$

and

$$F_s(n) = q_s^n$$

respectively. From Equation 2.2, the system reliability is:

$$R_s(n) = (1 - q_o)^n - q_s^n \tag{2.3}$$

where n is the number of identical and independent components. In a series arrangement, reliability with respect to closed system failure increases with the number of components, whereas reliability with respect to open system failure falls. There exists an optimum number of components, say n^*, that maximizes the system reliability. If we define

$$n_0 = \frac{\log\left(\dfrac{q_o}{1-q_s}\right)}{\log\left(\dfrac{q_s}{1-q_o}\right)}$$

then the system reliability, $R_s(n^*)$, is maximum for

$$n^* = \begin{cases} \lfloor n_0 \rfloor + 1 & \text{if } n_0 \text{ is not an integer} \\ n_0 \text{ or } n_0 + 1 & \text{if } n_0 \text{ is an integer} \end{cases} \tag{2.4}$$

Example 1. A switch has two failure modes: fail-open and fail-short. The probability of switch open-circuit failure and short-circuit failure are 0.1 and 0.2 respectively. A system consists of n switches wired in series. That is, given $q_o = 0.1$ and $q_s = 0.2$. From Equation 2.4

$$n_0 = \frac{\log\left(\dfrac{0.1}{1-0.2}\right)}{\log\left(\dfrac{0.2}{1-0.1}\right)} = 1.4$$

Thus, $n^* = \lfloor 1.4 \rfloor + 1 = 2$. Therefore, when $n^* = 2$ the system reliability $R_s(n) = 0.77$ is maximized.

2.3 The Parallel System

Consider a parallel system consisting of n components. For a parallel configuration, all the components must fail in open mode or at least one component must malfunction in short mode to cause the system to fail completely.

The system reliability is

$$R_p(n) = (1 - q_s)^n - q_o^n \tag{2.5}$$

where n is the number of components connected in parallel. In this case, $(1 - q_s)^n$ represents the probability that no components fail in short mode, and q_o^n represents the probability that all components fail in open mode. If we define

$$n_0 = \frac{\log\left(\dfrac{q_s}{1-q_o}\right)}{\log\left(\dfrac{q_o}{1-q_s}\right)} \tag{2.6}$$

then the system reliability $R_p(n^*)$ is maximum for

$$n^* = \begin{cases} \lfloor n_0 \rfloor + 1 & \text{if } n_0 \text{ is not an integer} \\ n_0 \text{ or } n_0 + 1 & \text{if } n_0 \text{ is an integer} \end{cases} \tag{2.7}$$

It is observed that, for any range of q_o and q_s, the optimal number of parallel components that maximizes the system reliability is one, if $q_s > q_o$. For most other practical values of q_o and q_s, the optimal number turns out to be two. In general, the optimal value of parallel components can be easily obtained using Equation 2.6.

2.3.1 Cost Optimization

Suppose that each component costs d dollars and system failure costs c dollars of revenue. We now wish to determine the optimal system size n that minimizes the average system cost given that the costs of system failure in open and short modes are known. Let T_n be a total of the system. The average system cost is given by

$$E[T_n] = dn + c[1 - R_p(n)]$$

where $R_p(n)$ is defined as in Equation 2.5. For given q_o, q_s, c, and d, we can obtain a value of n, say n^*, minimizing the average system cost.

Theorem 1. *Fix q_o, q_s, c, and d. There exists a unique value n^* that minimizes the average system cost, and*

$$n^* = \inf\left\{ n \le n_1 : (1 - q_o)q_o^n - q_s(1 - q_s)^n < \frac{d}{c} \right\} \tag{2.8}$$

where $n_1 = \lfloor n_0 \rfloor + 1$ and n_0 is given in Equation 2.6.

The proof is straightforward and left for an exercise. It was assumed that the cost of system failure in either open mode or short mode was the same. We are now interested in how the cost of system failure in open mode may be different from that in short mode.

Suppose that each component costs d dollars and system failure in open mode and short mode costs c_1 and c_2 dollars of revenue respectively. Then the average system cost is given by

$$E[T_n] = dn + c_1 q_o^n + c_2[1 - (1 - q_s)^n] \qquad (2.9)$$

In other words, the average system cost of system size n is the cost incurred when the system has failed in either open mode or short mode plus the cost of all components in the system. We can determine the optimal value of n, say n^*, which minimizes the average system cost as shown in the following theorem [5].

Theorem 2. *Fix q_o, q_s, c_1, c_2, and d. There exists a unique value n^* that minimizes the average system cost, and*

$$n^* = \begin{cases} 1 & \text{if } n_a \le 0 \\ n_0 & \text{otherwise} \end{cases}$$

where

$$n_0 = \inf\left\{ n \le n_a : h(n) \le \frac{d}{c_2 q_s} \right\}$$

and

$$h(n) = q_o^n \left[\frac{1 - q_o}{q_s} \frac{c_1}{c_2} - \left(\frac{1 - q_s}{q_o} \right)^n \right]$$

$$n_a = \frac{\log\left(\dfrac{1 - q_o}{q_s} \dfrac{c_1}{c_2} \right)}{\log\left(\dfrac{1 - q_s}{q_o} \right)}$$

Example 2. Suppose $d = 10$, $c_1 = 1500$, $c_2 = 300$, $q_s = 0.1$, $q_o = 0.3$. Then

$$\frac{d}{c_2 q_s} = 0.333$$

From Table 2.1, $h(3) = 0.216 < 0.333$; therefore, the optimal value of n is $n^* = 3$. That is, when $n^* = 3$ the average system cost (151.8) is minimized.

Table 2.1. The function $h(n)$ vs n

n	$h(n)$	$R_p(n)$	$E[T_n]$
1	9.6	0.6	490.0
2	2.34	0.72	212.0
3	0.216	0.702	151.8
4	−0.373	0.648	155.3
5	−0.504	0.588	176.5
6	−0.506	0.531	201.7

2.4 The Parallel–Series System

Consider a system of components arranged so that there are m subsystems operating in parallel, each subsystem consisting of n identical components in series. Such an arrangement is called a parallel–series arrangement. The components could be a logic gate, a fluid-flow valve, or an electronic diode, and they are subject to two types of failure: failure in open mode and failure in short mode. Applications of the parallel–series systems can be found in the areas of communication, networks, and nuclear power systems. For example, consider a digital circuit module designed to process the incoming message in a communication system. Suppose that there are, at most, m ways of getting a message through the system, depending on which of the branches with n modules are operable. Such a system is subject to two failure modes: (1) a failure in open circuit of a single component in each subsystem would render the system unresponsive; or (2) a failure in short circuit of all the components in any subsystem would render the entire system unresponsive.

We adopt the following notation:

- m — number of subsystems in a system (or subsystem size)
- n — number of components in each subsystem
- $F_o(m)$ — probability of system failure in open mode
- $F_s(m)$ — probability of system failure in short mode.

The systems are characterized by the following properties.

1. The system consists of m subsystems, each subsystem containing n i.i.d. components.
2. A component is either good, failed open, or failed short. Failed components can never become good, and there are no transitions between the open and short failure modes.
3. The system can be (a) good, (b) failed open (at least one component in each subsystem fails open), or (c) failed short (all the components in any subsystem fail short).
4. The unconditional probabilities of component failure in open and short modes are known and are constrained: $q_o, q_s > 0; q_o + q_s < 1$.

The probabilities of a system failing in open mode and failing in short mode are given by

$$F_o(m) = [1 - (1 - q_o)^n]^m \tag{2.10}$$

and

$$F_s(m) = 1 - (1 - q_s^m)^m \tag{2.11}$$

respectively. The system reliability is

$$R_{ps}(n, m) = (1 - q_s^n)^m - [1 - (1 - q_o)^n]^m \tag{2.12}$$

where m is the number of identical subsystems in parallel and n is the number of identical components in each series subsystem. The term $(1 - q_s^n)^m$ represents the probability that none of the subsystems has failed in closed mode. Similarly, $[1 - (1 - q_o)^n]^m$ represents the probability that all the subsystems have failed in open mode.

An interesting example in Ref. [1] shows that there exists no pair n, m maximizing system reliability, since R_{ps} can be made arbitrarily close to one by appropriate choice of m and n. To see this, let

$$a = \frac{\log q_s - \log(1 - q_o)}{\log q_s + \log(1 - q_o)}$$
$$M_n = q_s^{-n/(1+a)} \qquad m_n = \lfloor M_n \rfloor$$

For given n, take $m = m_n$; then one can rewrite Equation 2.12 as:

$$R_{ps}(n,\ m_n) = (1 - q_s^n)^{m_n} - [1 - (1 - q_o)^n]^{m_n}$$

A straightforward computation yields

$$\begin{aligned}\lim_{n\to\infty} R_{ps}(n, m_n) &= \lim_{n\to\infty} \{(1 - q_s^n)^{m_n} - [1 - (1 - q_o)^n]^{m_n}\} \\ &= 1\end{aligned}$$

For fixed n, q_o, and q_s, one can determine the value of m that maximizes R_{ps}, and this is given below [8].

Theorem 3. *Let n, q_o, and q_s be fixed. The maximum value of $R_{ps}(m)$ is attained at $m^* = \lfloor m_0 \rfloor + 1$, where*

$$m_0 = \frac{n(\log p_o - \log q_s)}{\log(1 - q_s^n) - \log(1 - p_o^n)} \tag{2.13}$$

If m_0 is an integer, then m_0 and $m_0 + 1$ both maximize $R_{ps}(m)$.

2.4.1 The Profit Maximization Problem

We now wish to determine the optimal subsystem size m that maximizes the average system profit. We study how the optimal subsystem size m depends on the system parameters. We also show that there does not exist a pair (m, n) maximizing the average system profit.

We adopt the following notation:

$A(m)$	average system profit
β	conditional probability that the system is in open mode
$1 - \beta$	conditional probability that the system is in short mode
c_1, c_3	gain from system success in open, short mode
c_2, c_4	gain from system failure in open, short mode; $c_1 > c_2, c_3 > c_4$.

The average system profit is given by

$$\begin{aligned}A(m) &= \beta\{c_1[1 - F_o(m)] + c_2 F_o(m)\} \\ &\quad + (1 - \beta)\{c_3[1 - F_s(m)] + c_4 F_s(m)\}\end{aligned} \tag{2.14}$$

Define

$$a = \frac{\beta(c_1 - c_2)}{(1 - \beta)(c_3 - c_4)}$$

and

$$b = \beta c_1 + (1-\beta)c_4 \tag{2.15}$$

We can rewrite Equation 2.14 as

$$A(m) = (1-\beta)(c_3 - c_4) \times \{[1 - F_s(m)] - aF_o(m)\} + b \tag{2.16}$$

When the costs of the two kinds of system failure are identical, and the system is in the two modes with equal probability, then the optimization criterion becomes the same as maximizing the system reliability. Here, the following analysis deals with cases that need not satisfy these special restrictions.

For a given value of n, one wishes to find the optimal number of subsystems m (m^*) that maximizes the average system profit. Of course, we would expect the optimal value of m to depend on the values of both q_o and q_s. Define

$$m_0 = \frac{\ln a + n \ln\left(\dfrac{1-q_o}{q_s}\right)}{\ln\left[\dfrac{1-q_s^n}{1-(1-q_o)^n}\right]} \tag{2.17}$$

Theorem 4. *Fix β, n, q_o, q_s, and c_i for $i = 1, 2, 3, 4$. The maximum value of $A(m)$ is attained at*

$$m^* = \begin{cases} 1 & \text{if } m_0 < 0 \\ \lfloor m_0 \rfloor + 1 & \text{if } m_0 \ge 0 \end{cases} \tag{2.18}$$

If m_0 is a non-negative integer, both m_0 and $m_0 + 1$ maximize $A(m)$.

The proof is straightforward. When m_0 is a non-negative integer, the lower value will provide the more economical optimal configuration for the system. It is of interest to study how the optimal subsystem size m^* depends on the various parameters q_o and q_s.

Theorem 5. *For fixed n, c_1, c_2, c_3, and c_4.*

(*a*) *If $a \ge 1$, then the optimal subsystem size m^* is an increasing function of q_o.*
(*b*) *If $a \le 1$, then the optimal subsystem size m^* is a decreasing function of q_s.*
(*c*) *The optimal subsystem size m^* is an increasing function of β.*

The proof is left for an exercise. It is worth noting that we cannot find a pair (m, n) maximizing average system-profit $A(m)$. Let

$$x = \frac{\ln q_s - \ln p_o}{\ln q_s + \ln p_o} \qquad M_n = q_s^{-n/l+x} \qquad m_n = \lfloor M_n \rfloor \tag{2.19}$$

For given n, take $m = m_n$. From Equation 2.14, the average system profit can be rewritten as

$$A(m_n) = (1-\beta)(c_3 - c_4) \times \{[1 - F_s(m_n)] - aF_o(m_n)\} + b \tag{2.20}$$

Theorem 6. *For fixed q_o and q_s*

$$\lim_{n\to\infty} A(m_n) = \beta c_1 + (1-\beta)c_3 \tag{2.21}$$

The proof is left for an exercise. This result shows that we cannot seek a pair (m, n) maximizing the average system profit $A(m_n)$, since $A(m_n)$ can be made arbitrarily close to $\beta c_1 + (1-\beta)c_3$.

2.4.2 Optimization Problem

We show how design policies can be chosen when the objective is to minimize the average total system cost given that the costs of system failure in open mode and short mode may not necessarily be the same.

The following notation is adopted:

d	cost of each component
c_1	cost when system failure in open
c_2	cost when system failure in short
$T(m)$	total system cost
$E[T(m)]$	average total system cost.

Suppose that each component costs d dollars, and system failure in open mode and short mode costs c_1 and c_2 dollars of revenue, respectively. The average total system cost is

$$E[T(m)] = dnm + c_1F_o(m) + c_2F_s(m) \tag{2.22}$$

In other words, the average system cost is the cost incurred when the system has failed in either the open mode or the short mode plus the cost of all components in the system. Define

$$h(m) = [1 - (p_o)^n]^m \left[c_1 p_o^n - c_2 q_s^n \left(\frac{1 - q_s^n}{1 - p_o^n} \right)^m \right] \tag{2.23}$$

$$m_1 = \inf\{m < m_2 : h(m) < dn\}$$

and

$$m_2 = \left\lfloor \frac{\ln \left[\frac{c_1}{c_2} \left(\frac{p_o}{q_s} \right)^n \right]}{\ln \left(\frac{1 - q_s^n}{1 - p_o^n} \right)} \right\rfloor + 1 \tag{2.24}$$

From Equation 2.23, $h(m) > 0$ if and only if

$$c_1 p_o^n > c_2 q_s^n \left(\frac{1 - q_s^n}{1 - p_o^n} \right)^m$$

or equivalently, that $m < m_2$. Thus, the function $h(m)$ is decreasing in m for all $m < m_2$. For fixed n, we determine the optimal value of m, m^*, that minimizes the expected system cost, as shown in the following theorem [11].

Theorem 7. *Fix q_o, q_s, d, c_1, and c_2. There exists a unique value m^* such that the system minimizes the expected cost, and*

(*a*) *if $m_2 > 0$ then*

$$m^* = \begin{cases} m_1 & \text{if } E[T(m_1)] \le E[T(m_2)] \\ m_2 & \text{if } E[T(m_1)] > E[T(m_2)] \end{cases} \tag{2.25}$$

(*b*) *if $m_2 \le 0$ then $m^* = 1$.*

The proof is straightforward. Since the function $h(m)$ is decreasing in m for $m < m_2$, again the resulting optimization problem in Equation 2.25 is easily solved in practice.

Example 3. Suppose $n = 5, d = 10, c_1 = 500, c_2 = 700$, $q_s = 0.1$, and $q_o = 0.2$. From Equation 2.25, we obtain $m_2 = 26$. Since $m_2 > 0$, we determine the optimal value of m by using Theorem 7(a).

The subsystem size m, $h(m)$, and the expected system cost $E[T(m)]$ are listed in Table 2.2; from this table, we have

$$m_1 = \inf\{m < 26 : h(m) < 50\} = 3$$

Table 2.2. The data for Example 3

m	$h(m)$	$E[T(m)]$
1	110.146	386.17
2	74.051	326.02
3	49.784	301.97
4	33.469	302.19
5	22.499	318.71
6	15.124	346.22
7	10.166	381.10
8	6.832	420.93
9	4.591	464.10
10	3.085	509.50

and

$$E[T(m_1)] = 301.97$$

For $m_2 = 26$, $E[T(m_2)] = 1300.20$. From Theorem 7(a), the optimal value of m required to minimize the expected total system cost is 3, and the expected total system cost corresponding to this value is 301.97.

2.5 The Series–Parallel System

The series–parallel structure is the dual of the parallel–series structure in Section 2.4. We study a system of components arranged so that there are m subsystems operating in series, each subsystem consisting of n identical components in parallel. Such an arrangement is called a series–parallel arrangement. Applications of such systems can be found in the areas of communication, networks, and nuclear power systems. For example, consider a digital communication system consisting of m substations in series. A message is initially sent to substation 1, is then relayed to substation 2, *etc.*, until the message passes through substation m and is received. The message consists of a sequence of 0's and 1's and each digit is sent separately through the series of m substations. Unfortunately, the substations are not perfect and can transmit as output a different digit than that received as input. Such a system is subject to two failure modes: errors in digital transmission occur in such a manner that either (1) a one appears instead of a zero, or (2) a zero appears instead of a one.

Failure in open mode of all the components in any subsystem makes the system unresponsive. Failure in closed (short) mode of a single component in each subsystem also makes the system unresponsive. The probabilities of system failure in open and short mode are given by

$$F_o(m) = 1 - (1 - q_o^n)^m \tag{2.26}$$

and

$$F_s(m) = [1 - (1 - q_s)^n]^m \tag{2.27}$$

respectively. The system reliability is

$$R(m) = (1 - q_o^n)^m - [1 - (1 - q_s)^n]^m \tag{2.28}$$

where m is the number of identical subsystems in series and n is the number of identical components in each parallel subsystem.

Barlow *et al.* [1] show that there exists no pair (m, n) maximizing system reliability. For fixed m, q_o, and q_s, however, one can determine the value of n that maximizes the system reliability.

Theorem 8. *Let n, q_o, and q_s be fixed. The maximum value of $R(m)$ is attained at $m^* = \lfloor m_0 \rfloor + 1$, where*

$$m_0 = \frac{n(\log p_s - \log q_o)}{\log(1 - q_o^n) - \log(1 - p_s^n)} \tag{2.29}$$

If m_0 is an integer, then m_0 and $m_0 + 1$ both maximize $R(m)$.

2.5.1 Maximizing the Average System Profit

The effect of the system parameters on the optimal m is now studied. We also determine the optimal subsystem size that maximizes the average system profit subject to a restricted type I (system failure in open mode) design error.

The following notation is adopted:

- β — conditional probability (given system failure) that the system is in open mode
- $1 - \beta$ — conditional probability (given system failure) that the system is in short mode
- c_1 — gain from system success in open mode
- c_2 — gain from system failure in open mode $(c_1 > c_2)$
- c_3 — gain from system success in short mode
- c_4 — gain from system failure in short mode $(c_3 > c_4)$.

The average system-profit, $P(m)$, is given by

$$P(m) = \beta\{c_1[1 - F_o(m)] + c_2 F_o(m)\} + (1 - \beta)\{c_3[1 - F_s(m)] + c_4 F_s(m)\} \tag{2.30}$$

where $F_o(m)$ and $F_s(m)$ are defined as in Equations 2.26 and 2.27 respectively. Let

$$a = \frac{\beta(c_1 - c_2)}{(1 - \beta)(c_3 - c_4)}$$

and

$$b = \beta c_1 + (1 - \beta)c_4$$

We can rewrite Equation 2.30 as

$$P(m) = (1 - \beta)(c_3 - c_4) \times [1 - F_s(m) - a F_o(m)] + b \tag{2.31}$$

For a given value of n, one wishes to find the optimal number of subsystems m, say m^*, that maximizes the average system-profit. We would anticipate that m^* depends on the values of both q_o and q_s. Let

$$m_0 = \frac{n \ln\left(\dfrac{1 - q_s}{q_o}\right) - \ln a}{\ln\left[\dfrac{1 - q_o^n}{1 - (1 - q_s)^n}\right]} \tag{2.32}$$

Theorem 9. *Fix β, n, q_o, q_s, and c_i for $i = 1, 2, 3, 4$. The maximum value of $P(m)$ is attained at*

$$m^* = \begin{cases} 1 & \text{if } m_0 < 0 \\ \lfloor m_0 \rfloor + 1 & \text{if } m_0 \geq 0 \end{cases}$$

If $m_0 \geq 0$ and m_0 is an integer, both m_0 and $m_0 + 1$ maximize $P(m)$.

The proof is straightforward and left as an exercise. When both m_0 and $m_0 + 1$ maximize the average system profit, the lower of the two values costs less. It is of interest to study how m^* depends on the various parameters q_o and q_s.

Theorem 10. *For fixed n, c_i for $i = 1, 2, 3, 4$.*

(*a*) *If $a \geq 1$, then the optimal subsystem size m^* is a decreasing function of q_o.*
(*b*) *If $a \leq 1$, the optimal subsystem size m^* is an increasing function of q_s.*

This theorem states that when q_o increases, it is desirable to reduce m as close to one as is feasible. On the other hand, when q_s increases, the average system-profit increases with the number of subsystems.

2.5.2 Consideration of Type I Design Error

The solution provided by Theorem 9 is optimal in terms of the average system profit. Such an optimal configuration, when adopted, leads to a type I design error (system failure in open mode), which may not be acceptable at the design stage. It should be noted that the more subsystems we add to the system the greater is the chance of system failure by opening ($F_o(m)$, Equation 2.26)); however, we do make the probability of system failure in short mode smaller by placing additional subsystems in series. Therefore, given β, n, q_o, q_s and c_i for $i = 1, 2, \ldots, 4$, we wish to determine the optimal subsystem size m^* in order to maximize the average system profit $P(m)$ in such a way that the probability of system type I design error (*i.e.* the probability of system failure in open mode) is at most α.

Theorem 9 remains unchanged if m^* obtained from Theorem 9 is kept within the tolerableα level, namely $F_o(m) \leq \alpha$. Otherwise, modifications are needed to determine the optimal system size. This is stated in the following result.

Corollary 1. *For given values of β, n, q_o, q_s, and c_i for $i = 1, 2, \ldots, 4$, the optimal value of m, say m^*, that maximizes the average system profit subject to a restricted type I design error α is attained at*

$$m^* = \begin{cases} 1 & \textit{if } \min\{\lfloor m_0 \rfloor, \lfloor m_1 \rfloor\} \\ \min\{\lfloor m_0 \rfloor + 1, \lfloor m_1 \rfloor\} & \\ & \textit{otherwise} \end{cases}$$

where $\lfloor m_0 \rfloor + 1$ is the solution obtained from Theorem 9 and

$$m_1 = \frac{\ln(1 - a)}{\ln(1 - q_o^n)}$$

2.6 The k-out-of-n Systems

Consider a model in which a k-out-of-n system is composed of n identical and independent components that can be either good or failed. The components are subject to two types of failure: failure in open mode and failure in closed mode. The system can fail when k or more components fail in closed mode or when $(n - k + 1)$ or more components fail in open mode. Applications of k-out-of-n systems can be found in the areas of target detection, communication, and safety monitoring systems, and, particularly, in the area of human organizations. The following is an example in the area of human organizations. Consider a committee with n members who must decide to accept or reject innovation-oriented projects. The projects are of two types: "good" and "bad". It is assumed that the communication among the members is limited, and each member will make a yes–no decision on each project. A committee member can make two types of error: the error of accepting a bad project and the error of rejecting a good project. The committee will accept a project when k or more members accept it, and will reject a project when $(n - k + 1)$ or more members reject it. Thus, the two types of potential error of the committee are: (1) the acceptance of a bad project (which occurs when k or more members make the error of accepting a bad project); (2) the rejection of a good project (which occurs when $(n - k + 1)$ or more members make the error of rejecting a good project). This section determines the:

- optimal k that minimizes the expected total system cost;
- optimal n that minimizes the expected total system cost;
- optimal k and n that minimizes the expected total system cost.

We also study the effect of the system's parameters on the optimal k or n. The system fails in closed mode if and only if at least k of its n components fail in closed mode, and we obtain

$$F_s(k,n) = \sum_{i=k}^{n} \binom{n}{i} q_s^i p_s^{n-i} = 1 - \sum_{i=0}^{k-1} \binom{n}{i} q_s^i p_s^{n-i} \tag{2.33}$$

The system fails in open mode if and only if at least $n-k+1$ of its n components fail in open mode, that is:

$$F_o(k,n) = \sum_{i=n-k+1}^{n} \binom{n}{i} q_o^i p_o^{n-i} = \sum_{i=0}^{k-1} \binom{n}{i} p_o^i q_o^{n-i} \tag{2.34}$$

Hence, the system reliability is given by

$$\begin{aligned} R(k,n) &= 1 - F_o(k,n) - F_s(k,n) \\ &= \sum_{i=0}^{k-1} \binom{n}{i} q_s^i p_s^{n-i} - \sum_{i=0}^{k-1} \binom{n}{i} p_o^i q_o^{n-i} \end{aligned} \tag{2.35}$$

Let

$$b(k;\, p, n) = \binom{n}{k} p^k (1-p)^{n-k}$$

and

$$b\inf(k;\, p, n) = \sum_{i=0}^{k} b(i;\, p, n)$$

We can rewrite Equations 2.33–2.35 as

$$\begin{aligned} F_s(k,n) &= 1 - b\inf(k-1;\, q_s, n) \\ F_o(k,n) &= b\inf(k-1;\, p_o, n) \\ R(k,n) &= 1 - b\inf(k-1;\, q_s, n) \\ &\quad - b\inf(k-1;\, p_o, n) \end{aligned}$$

respectively. For a given k, we can find the optimum value of n, say n^*, that maximizes the system reliability.

Theorem 11. *For fixed k, q_o, and q_s, the maximum value of $R(k,n)$ is attained at $n^* = \lfloor n_0 \rfloor$ where*

$$n_0 = k\left[1 + \frac{\log\left(\dfrac{1-q_o}{q_s}\right)}{\log\left(\dfrac{1-q_s}{q_o}\right)}\right]$$

If n_0 is an integer, both n_0 and n_0+1 maximize $R(k,n)$.

This result shows that when n_0 is an integer, both n^*-1 and n^* maximize the system reliability $R(k,n)$. In such cases, the lower value will provide the more economical optimal configuration for the system. If $q_o = q_s$, the system reliability $R(k,n)$ is maximized when $n = 2k$ or $2k-1$. In this case, the optimum value of n does not depend on the value of q_o and q_s, and the best choice for a decision voter is a majority voter; this system is also called a majority system [12].

From the above Theorem 11 we understand that the optimal system size n^* depends on the various parameters q_o and q_s. It can be shown the optimal value n^* is an increasing function of q_o and a decreasing function of q_s. Intuitively, these results state that when q_s increases it is desirable to reduce the number of components in the system as close to the value of threshold level k as possible. On the other hand, when q_o increases, the system reliability will be improved if the number of components increases.

For fixed n, q_o, and q_s, it is straightforward to see that the maximum value of $R(k,n)$ is attained at $k^* = \lfloor k_0 \rfloor + 1$, where

$$k_0 = n\frac{\log\left(\dfrac{q_o}{p_s}\right)}{\log\left(\dfrac{q_s q_o}{p_s p_o}\right)}$$

If k_0 is an integer, both k_0 and k_0+1 maximize $R(k,n)$.

We now discuss how these two values, k^* and n^*, are related to one another. Define α by

$$\alpha = \frac{\log\left(\dfrac{q_o}{p_s}\right)}{\log\left(\dfrac{q_s q_o}{p_s p_o}\right)}$$

then, for a given n, the optimal threshold k is given by $k^* = \lceil n\alpha \rceil$, and for a given k the optimal n is $n^* = \lfloor k/\alpha \rfloor$. For any given q_o and q_s, we can easily show that

$$q_s < \alpha < p_o$$

Therefore, we can obtain the following bounds for the optimal value of the threshold k:

$$nq_s < k^* < np_o$$

This result shows that for given values of q_o and q_s, an upper bound for the optimal threshold k^* is the expected number of components working in open mode, and a lower bound for the optimal threshold k^* is the expected number of components failing in closed mode.

2.6.1 Minimizing the Average System Cost

We adopt the following notation:

d each component cost
c_1 cost when system failure is in open mode
c_2 cost when system failure is in short mode

$$b\,\mathrm{inf}(k;\, q_s, n) = 1 - b\,\mathrm{inf}(k-1;\, q_s, n)$$

The average total system cost $E[T(k,n)]$ is

$$E[T(k,n)] = dn + [c_1 F_o(k,n) + c_2 F_s(k,n)] \tag{2.36}$$

In other words, the average total system cost is the cost of all components in the system (dn), plus the average cost of system failure in the open mode ($c_1 F_o(k,n)$) and the average cost of system failure in the short mode ($c_2 F_s(k,n)$).

We now study the problem of how design policies can be chosen when the objective is to minimize the average total system cost when the cost of components, the costs of system failure in the open, and short modes are given. We wish to find the:

- optimal k (k^*) that minimizes the average system cost for a given n;
- optimal n (n^*) that minimizes the average system cost for a given k;
- optimal k and n (k^*, n^*) that minimize the average system cost.

Define

$$k_0 = \frac{\log\left(\dfrac{c_2}{c_1}\right) + n\log\left(\dfrac{p_s}{q_o}\right)}{\log\left(\dfrac{p_o p_s}{q_o q_s}\right)} \tag{2.37}$$

Theorem 12. *Fix n, q_o, q_s, c_1, c_2, and d. The minimum value of $E[T(k,n)]$ is attained at*

$$k^* = \begin{cases} \max\{1, \lfloor k_0 \rfloor + 1\} & \text{if } k_0 < n \\ n & \text{if } k_0 \geq n \end{cases}$$

If k_0 is a positive integer, both k_0 and $k_0 + 1$ minimize $E[T(k,n)]$.

It is of interest to study how the optimal value of k, k^*, depends on the probabilities of component failure in the open mode (q_o) and in the short mode (q_s).

Corollary 2. *Fix n,*

1. *if $c_1 \geq c_2$, then k^* is decreasing in q_o;*
2. *if $c_1 \leq c_2$, then k^* is increasing in q_s.*

Intuitively, this result states that if the cost of system failure in the open mode is greater than or equal to the cost of system failure in the short mode, then, as q_o increases, it is desirable to reduce the threshold level k as close to one as is feasible. Similarly, if the cost of system failure in the open mode is less than or equal to the cost of system failure in the short mode, then, as q_s increases, it is desirable to increase k as close to n as is feasible. Define

$$a = \frac{c_1}{c_2}$$

$$n_0 = \left\lfloor \frac{\log a + k\log\left(\dfrac{p_o P_s}{q_o q_s}\right)}{\log\left(\dfrac{p_s}{q_o}\right)} - 1 \right\rfloor$$

$$n_1 = \left\lceil \frac{k-1}{1-q_o} - 1 \right\rceil$$

$$f(n) = \left(\frac{p_s}{q_o}\right)^n \frac{(n+1)q_s - (k-1)}{(n+1)p_o - (k-1)}$$

$$B = a\left(\frac{p_o p_s}{q_o q_s}\right)^k \frac{q_o}{p_s}$$

and

$$n_2 = f^{-1}(B) \quad \text{for } k \leq n_2 \leq n_1$$

Let

$$n_3 = \inf\left\{ n \in [n_2,\ n_0] : h(n) < \frac{d}{c_2} \right\}$$

where

$$h(n) = \binom{n}{k-1} p_o^k q_o^{n-k+1} \times \left[a - \left(\frac{q_o q_s}{p_s p_o}\right)^k \left(\frac{p_s}{q_o}\right)^{n+1} \right] \quad (2.38)$$

It is easy to show that the function $h(n)$ is positive for all $k \le n \le n_0$, and is increasing in n for $n \in [k, n_2)$ and is decreasing in n for $n \in [n_2, n_0]$. This result shows that the function $h(n)$ is unimodal and achieves a maximum value at $n = n_2$. Since $n_2 \le n_1$, and when the probability of component failure in the open mode q_o is quite small, then $n_1 \approx k$; so $n_2 \approx k$. On the other hand, for a given arbitrary q_o, one can find a value n_2 between the values of k and n_1 by using a binary search technique.

Theorem 13. *Fix q_o, q_s, k, d, c_1, and c_2. The optimal value of n, say n^*, such that the system minimizes the expected total cost is $n^* = k$ if $n_0 \le k$. Suppose $n_0 > k$. Then:*

1. *if $h(n_2) < d/c_2$, then $n^* = k$;*
2. *if $h(n_2) \ge d/c_2$ and $h(k) \ge d/c_2$ then $n^* = n_3$;*
3. *if $h(n_2) \ge d/c_2$ and $h(k) < d/c_2$, then*

$$n^* = \begin{cases} k & \text{if } E[T(k,k)] \le E[T(k,n_3)] \\ n_3 & \text{if } E[T(k,k)] > E[T(k,n_3)] \end{cases} \quad (2.39)$$

Proof. Let $\Delta E[T(n)] = E[T(k, n+1)] - E[T(k,n)]$. From Equation 2.36, we obtain

$$\Delta E[T(n)] = d - c_1 \binom{n}{k-1} p_o^k q_o^{n-k+1} + c_2 \binom{n}{k-1} q_s^k p_s^{n-k+1} \quad (2.40)$$

Substituting $c_1 = ac_2$ into Equation 2.40, and after simplification, we obtain

$$\Delta E[T(n)] = d - c_2 \binom{n}{k-1} p_o^k q_o^{n-k+1} \times \left[a - \left(\frac{q_o q_s}{p_o p_s}\right)^k \left(\frac{p_s}{q_o}\right)^{n+1} \right] = d - c_2 h(n)$$

The system of size $n+1$ is better than the system of size n if, and only if, $h(n) \ge d/c_2$. If $n_0 \le k$, then $h(n) \le 0$ for all $n \ge k$, so that $E[T(k,n)]$ is increasing in n for all $n \ge k$. Thus $n^* = k$ minimizes the expected total system cost. Suppose $n_0 > k$. Since the function $h(n)$ is decreasing in n for $n_2 \le n \le n_0$, there exists an n such that $h(n) < d/c_2$ on the interval $n_2 \le n \le n_0$. Let n_3 denote the smallest such n. Because $h(n)$ is decreasing on the interval $[n_2, n_0]$ where the function $h(n)$ is positive, we have $h(n) \ge d/c_2$ for $n_2 \le n \le n_3$ and $h(n) < d/c_2$ for $n > n_3$. Let n^* be an optimal value of n such that $E[T(k,n)]$ is minimized.

(a) If $h(n_2) < d/c_2$, then $n_3 = n_2$ and $h(k) < h(n_2) < d/c_2$, since $h(n)$ is increasing in $[k, n_2)$ and is decreasing in $[n_2, n_0]$. Note that incrementing the system size reduces the expected system cost only when $h(n) \ge d/c_2$. This implies that $n^* = k$ such that $E[T(k,n)]$ is minimized.

(b) Assume $h(n_2) \ge d/c_2$ and $h(k) \ge d/c_2$. Then $h(n) \ge d/c_2$ for $k \le n < n_2$, since $h(n)$ is increasing in n for $k < n < n_2$. This implies that $E[T(k, n+1)] \le E[T(k,n)]$ for $k \le n < n_2$. Since $h(n_2) \ge d/c_2$, then $h(n) \ge d/c_2$ for $n_2 < n < n_3$ and $h(n) < d/c_2$ for $n > n_3$. This shows that $n^* = n_3$ such that $E[T(k,n)]$ is minimized.

(c) Similarly, assume that $h(n_2) \ge d/c_2$ and $h(k) < d/c_2$. Then, either $n = k$ or $n^* = n_3$ is the optimal solution for n. Thus, $n^* = k$ if $E[T(k,k)] \le E[T(k,n_3)]$; on the other hand, $n^* = n_3$ if $E[T(k,k)] > E[T(k,n_3)]$. □

In practical applications, the probability of component failure in the open mode q_o is often quite small, and so the value of n_1 is close to k. Therefore, the number of computations for finding a value of n_2 is quite small. Hence, the result of the Theorem 13 is easily applied in practice.

In the remaining section, we assume that the two system parameters k and n are unknown. It is of interest to determine the optimum values of (k, n), say (k^*, n^*), that minimize the expected total system cost when the cost of components and the costs of system failures are known. Define

$$\alpha = \frac{\log(p_s/q_o)}{\log(p_o p_s/q_o q_s)} \qquad \beta = \frac{\log(c_2/c_1)}{\log(p_o p_s/q_o q_s)} \quad (2.41)$$

We need the following lemma.

Lemma 1. *For* $0 \le m \le n$ *and* $0 \le p \le 1$*:*

$$\sum_{i=0}^{m} \binom{n}{i} p^i (1-p)^{n-i} < \sqrt{\frac{n}{2\pi m(n-m)}}$$

Proof. See [5], Lemma 3.16, for a detailed proof. □

Theorem 14. *Fix* q_o, q_s, d, c_1, *and* c_2. *There exists an optimal pair of values* (k_n, n), *say* (k_{n^*}, n^*), *such that average total system cost is minimized at* (k_{n^*}, n^*), *and*

$$k_{n^*} = \lfloor n^* \alpha \rfloor$$

and

$$n^* \le \frac{\frac{(1-q_o-q_s)}{2\pi}\left(\frac{c_1}{d}\right)^2 + 1 + \beta}{\alpha(1-\alpha)} \tag{2.42}$$

Proof. Define $\Delta E[T(n)] = E[T(k_{n+1}, n+1)] - E[T(k_n, n)]$. From Equation 2.36, we obtain

$$\begin{aligned}\Delta E[T(n)] = d + c_1[&b\inf(k_{n+1}-1;\ p_o, n+1)\\ &- b\inf(k_n-1;\ p_o, n)]\\ &- c_2[b\inf(k_{n+1}-1;\ q_s, n+1)\\ &- b\inf(k_n-1;\ q_s, n)]\end{aligned}$$

Let $r = c_2/c_1$, then

$$\begin{aligned}\Delta E[T(n)] &= d - c_1 g(n)\\ g(n) &= r[b\inf(k_{n+1}-1;\ q_s, n+1)\\ &\quad - b\inf(k_n-1;\ q_s, n)]\\ &\quad - [b\inf(k_{n+1}-1;\ p_o, n+1)\\ &\quad - b\inf(k_n-1;\ p_o, n)]\end{aligned} \tag{2.43}$$

Case 1. Assume $k_{n+1} = k_n + 1$. We have

$$g(n) = \binom{n}{k_n} p_o^{k_n} q_o^{n-k_n+1} \times \left[r\left(\frac{q_o q_s}{p_o p_s}\right)^{k_n}\left(\frac{p_s}{q_o}\right)^{n+1} - 1\right]$$

Recall that

$$\left(\frac{p_o p_s}{q_o q_s}\right)^{\beta} = r$$

then

$$\left(\frac{q_o q_s}{p_o p_s}\right)^{n\alpha+\beta}\left(\frac{p_s}{q_o}\right)^{n+1} = \frac{1}{r}\frac{p_s}{q_o} \tag{2.44}$$

since $n\alpha + \beta \le k_n \le (n+1)\alpha + \beta$, we obtain

$$\begin{aligned}r\left(\frac{q_o q_s}{p_s p_s}\right)^{k_n}\left(\frac{p_s}{q_o}\right)^{n+1} &\le r\left(\frac{q_o q_s}{p_o p_s}\right)^{n\alpha+\beta}\left(\frac{p_s}{q_o}\right)^{n+1}\\ &= \frac{p_s}{q_o}\end{aligned}$$

Thus

$$\begin{aligned}g(n) &\le \binom{n}{k_n} p_o^{k_n} q_o^{n-k_n+1}\left(\frac{p_s}{q_o} - 1\right)\\ &= \binom{n}{k_n} p_o^{k_n} q_o^{n-k_n}(p_s - q_o)\end{aligned}$$

From Lemma 1, and $n\alpha + \beta \le k_n \le (n+1)\alpha + \beta$, we obtain

$$\begin{aligned}g(n) &\le (p_s - q_o)\left[2\pi n\frac{k_n}{n}\left(1 - \frac{k_n}{n}\right)\right]^{-1/2}\\ &\le (p_s - q_o)\left\{2\pi n\left(\alpha + \frac{\beta}{n}\right)\right.\\ &\quad \times \left.\left[1 - \alpha\left(\frac{n+1}{n}\right) - \frac{\beta}{n}\right]\right\}^{-1/2}\\ &\le (1 - q_s - q_s)\\ &\quad \times \{2\pi n[n\alpha(1-\alpha) - \alpha(\alpha+\beta)]\}^{-1/2}\end{aligned} \tag{2.45}$$

Case 2. Similarly, if $k_{n+1} = k_n$ then from Equation 2.43, we have

$$g(n) = \binom{n}{k_n - 1} q_s^{k_n} p_s^{n-k_n+1} \times \left[\left(\frac{p_o p_s}{q_o q_s}\right)^{k_n}\left(\frac{q_o}{p_s}\right)^{n+1} - r\right]$$

since $k_n = \lceil n\alpha + \beta \rceil \leq n\alpha + \beta + 1$, and from Equation 2.44 and Lemma 1, we have

$$\begin{aligned}
g(n) &\leq q_s \binom{n}{k_n - 1} q_s^{k_n-1} p_s^{n-k_n+1} \\
&\quad \times \left[\left(\frac{p_o p_s}{q_o q_s}\right)^{n\alpha+\beta+1} \left(\frac{q_o}{p_s}\right)^{n+1} - r \right] \\
&\leq q_s \sqrt{\frac{n}{2\pi(k_n-1)[n-(k_n-1)]}} \\
&\quad \times \left[\left(\frac{p_o p_s}{q_o q_s}\right)^{n\alpha+\beta} \left(\frac{q_o}{p_s}\right)^{n+1} \left(\frac{p_o p_s}{q_o q_s}\right) - r \right] \\
&\leq q_s \sqrt{\frac{n}{2\pi(k_n-1)[n-(k_n-1)]}} \\
&\quad \times \left[r \left(\frac{q_o}{p_s}\right) \left(\frac{p_o p_s}{q_o q_s}\right) - r \right] \\
&\leq \sqrt{\frac{n}{2\pi(k_n-1)[n-(k_n-1)]}} (1 - q_o - q_s)
\end{aligned}$$

Note that $k_{n+1} = k_n$, then $n\alpha - (1 - \alpha - \beta) \leq k_n - 1 \leq n\alpha + \beta$. After simplifications, we have

$$\begin{aligned}
g(n) &\leq (1 - q_o - q_s) \\
&\quad \times \left[2\pi n \left(\frac{k_n - 1}{n}\right) \left(1 - \frac{k_n - 1}{n}\right) \right]^{-1/2} \\
&\leq (1 - q_o - q_s) \\
&\quad \times \left[2\pi n \left(\alpha - \frac{1 - \alpha - \beta}{n}\right) \right. \\
&\qquad \left. \times \left(1 - \alpha - \frac{\beta}{n}\right) \right]^{-1/2} \\
&\leq \frac{1 - q_o - q_s}{\sqrt{2\pi[n\alpha(1-\alpha) - (1-\alpha)^2 - (1-\alpha)\beta]}}
\end{aligned} \tag{2.46}$$

From the inequalities in Equations 2.45 and 2.46, set

$$(1 - q_s - q_o) \frac{1}{\sqrt{2\pi[n\alpha(1-\alpha) - \alpha(\alpha+\beta)]}} \leq \frac{d}{c_1}$$

and

$$\frac{1 - q_o - q_s}{\sqrt{2\pi[n\alpha(1-\alpha) - (1-\alpha)^2 - \alpha(\alpha+\beta)]}} \leq \frac{d}{c_1}$$

we obtain

$$\begin{aligned}
&(1 - q_o - q_s)^2 \left(\frac{c_1}{d}\right)^2 \frac{1}{2\pi} \\
&\quad \leq \min\{n\alpha(1-\alpha) - \alpha(\alpha+\beta),\, n\alpha(1-\alpha) \\
&\qquad - (1-\alpha)^2 - (1-\alpha)\beta\}
\end{aligned}$$

$$\Delta E[T(n)] \geq 0$$

when

$$n \geq \frac{\frac{(1-q_o-q_s)^2}{2\pi}\left(\frac{c_1}{d}\right) + 1 + \beta}{\alpha(1-\alpha)}$$

Hence

$$n^* \leq \frac{\frac{(1-q_o-q_s)^2}{2\pi}\left(\frac{c_1}{d}\right) + 1 + \beta}{\alpha(1-\alpha)} \qquad \square$$

The result in Equation 2.42 provides an upper bound for the optimal system size.

2.7 Fault-tolerant Systems

In many critical applications of digital systems, fault tolerance has been an essential architectural attribute for achieving high reliability. It is universally accepted that computers cannot achieve the intended reliability in operating systems, application programs, control programs, or commercial systems, such as in the space shuttle, nuclear power plant control, *etc.*, without employing redundancy. Several techniques can achieve fault tolerance using redundant hardware [12] or software [13]. Typical forms of redundant hardware structures for fault-tolerant systems are of two types: fault masking and standby. Masking redundancy is achieved by implementing the functions so that they are inherently error correcting, *e.g.* triple-modular redundancy (TMR), N-modular redundancy (NMR), and self-purging redundancy. In standby redundancy, spare units are switched into the system when working units break down. Mathur and De Sousa [12] have analyzed, in detail, hardware redundancy in the design of fault-tolerant digital systems. Redundant software structures for fault-tolerant systems based on the acceptance tests have been proposed by Horning *et al.* [13].

This section presents a fault-tolerant architecture to increase the reliability of a special class of digital systems in communication [14]. In this system, a monitor and a switch are associated with each redundant unit. The switches and monitors can fail. The monitors have two failure modes: failure to accept a correct result, and failure to reject an incorrect result. The scheme can be used in communication systems to improve their reliability.

Consider a digital circuit module designed to process the incoming messages in a communication system. This module consists of two units: a converter to process the messages, and a monitor to analyze the messages for their accuracy. For example, the converter could be decoding or unpacking circuitry, whereas the monitor could be checker circuitry [12]. To guarantee a high reliability of operation at the receiver end, n converters are arranged in "parallel". All, except converter n, have a monitor to determine if the output of the converter is correct. If the output of a converter is not correct, the output is cancelled and a switch is changed so that the original input message is sent to the next converter. The architecture of such a system has been proposed by Pham and Upadhyaya [14]. Systems of this kind have useful application in communication and network control systems and in the analysis of fault-tolerant software systems.

We assume that a switch is never connected to the next converter without a signal from the monitor, and the probability that it is connected when a signal arrives is p_{s}. We next present a general expression for the reliability of the system consisting of n non-identical converters arranged in "parallel". An optimization problem is formulated and solved for the minimum average system cost. Let us define the following notation, events, and assumptions.

The notation is as follows:

p_i^{c}	Pr{converter i works}
p_i^{s}	Pr{switch i is connected to converter $(i+1)$ when a signal arrives}
p_i^{m1}	Pr{monitor i works when converter i works} = Pr{not sending a signal to the switch when converter i works}
p_i^{m2}	Pr{i monitor works when converter i has failed} = Pr{sending a signal to the switch when converter i has failed}
R_{n-k}^k	reliability of the remaining system of size $n-k$ given that the first k switches work
R_n	reliability of the system consisting of n converters.

The events are:

C_i^{w}, C_i^{f}	converter i works, fails
M_i^{w}, M_i^{f}	monitor i works, fails
S_i^{w}, S_i^{f}	switch i works, fails
W	system works.

The assumptions are:

1. the system, the switches, and the converters are two-state: good or failed;
2. the module (converter, monitor, or switch) states are mutually statistical independent;
3. the monitors have three states: good, failed in mode 1, failed in mode 2;
4. the modules are not identical.

2.7.1 Reliability Evaluation

The reliability of the system is defined as the probability of obtaining the correctly processed message at the output. To derive a general expression for the reliability of the system, we use an adapted form of the total probability theorem as translated into the language of reliability. Let A denote the event that a system performs as desired. Let X_i and X_j be the event that a component X (*e.g.* converter, monitor, or switch) is good or failed respectively. Then

$$\begin{aligned}&\Pr\{\text{system works}\}\\&\quad=\Pr\{\text{system works when unit } X \text{ is good}\}\\&\qquad\times\Pr\{\text{unit } X \text{ is good}\}\\&\qquad+\Pr\{\text{system works when unit } X \text{ fails}\}\\&\qquad\times\Pr\{\text{unit } X \text{ is failed}\}\end{aligned}$$

The above equation provides a convenient way of calculating the reliability of complex systems. Notice that $R_1 = p_i^{c}$, and for $n \geq 2$, the reliability of the system can be calculated as follows:

$$\begin{aligned}R_n &= \Pr\{W \mid C_1^{w} \text{ and } M_1^{w}\} \Pr\{C_1^{w} \text{ and } M_1^{w}\}\\ &\quad + \Pr\{W \mid C_1^{w} \text{ and } M_1^{f}\} \Pr\{C_1^{w} \text{ and } M_1^{f}\}\\ &\quad + \Pr\{W \mid C_1^{f} \text{ and } M_1^{w}\} \Pr\{C_1^{f} \text{ and } M_1^{w}\}\\ &\quad + \Pr\{W \mid C_1^{f} \text{ and } M_1^{f}\} \Pr\{C_1^{f} \text{ and } M_1^{f}\}\end{aligned}$$

In order for the system to operate when the first converter works and the first monitor fails, the first switch must work and the remaining system of size $n-1$ must work:

$$\Pr\{W \mid C_1^{w} \text{ and } M_1^{f}\} = p_1^{s} R_{n-1}^{1}$$

Similarly:

$$\Pr\{W \mid C_1^{f} \text{ and } M_1^{w}\} = p_1^{s} R_{n-1}^{1}$$

then

$$R_n p_1^{c} p_1^{m1} + [p_1^{c}(1-p_1^{m1}) + (1-p_1^{c})p_1^{m2}] p_1^{s} R_{n-1}^{1}$$

The reliability of the system consisting of n non-identical converters can be easily obtained:

$$R_n = \sum_{i=1}^{n-1} p_i^{c} p_i^{m1} \pi_{i-1} + \pi_{n-1} p_n^{c} \qquad \text{for } n > 1 \tag{2.47}$$

and

$$R_1 = p_1^{c}$$

where

$$\pi_k^{j} = \prod_{i=j}^{k} A_i \qquad \text{for } k \geq 1$$

$$\pi_k = \pi_k^{1} \qquad \text{for all } k, \text{ and } \pi_0 = 1$$

and

$$A_i \equiv [p_i^{c}(1-p_i^{m1}) + (1-p_i^{c})p_i^{m2}]$$

for all $i = 1, 2, \ldots, n$. Assume that all the converters, monitors, and switches have the same reliability, that is:

$$p_i^{c} = p^{c}, \quad p_i^{m1} = p^{m1}, \quad p_i^{m2} = p^{m2}, \quad p_i^{s} = p^{s}$$

for all i, then we obtain a closed form expression for the reliability of system as follows:

$$R_n = \frac{p^{c} p^{m1}}{1-A}(1-A^{n-1}) + p^{c} A^{n-1} \tag{2.48}$$

where

$$A = [p^{c}(1-p^{m1}) + (1-p^{c})p^{m2}] p^{s}$$

2.7.2 Redundancy Optimization

Assume that the system failure costs d units of revenue, and that each converter, monitor, and switch module costs a, b, and c units respectively. Let T_n be system cost for a system of size n. The average system cost for size n, $E[T_n]$, is the cost incurred when the system has failed, plus the cost of all n converters, $n-1$ monitors, and $n-1$ switches. Therefore:

$$E[T_n] = an + (b+c)(n-1) + d(1-R_n)$$

where R_n is given in Equation 2.48. The minimum value of $E[T_n]$ is attained at

$$n^* = \begin{cases} 1 & \text{if } A \leq 1 - p^{m1} \\ \lfloor n_0 \rfloor & \text{otherwise} \end{cases}$$

where

$$n_0 = \frac{\ln(a+b+c) - \ln[dp^{c}(A + p^{m1} - 1)]}{\ln A} + 1$$

Example 4. [14] Given a system with $p^{c} = 0.8$, $p^{m1} = 0.90$, $p^{m2} = 0.95$, $p^{s} = 0.90$, and $a = 2.5$, $b = 2.0$, $c = 1.5$, $d = 1200$. The optimal system size is $n^* = 4$, and the corresponding average cost (81.8) is minimized.

2.8 Weighted Systems with Three Failure Modes

In many applications, ranging from target detection to pattern recognition, including safety-monitoring protection, undersea communication, and human organization systems, a decision has to be made on whether or not to accept the hypothesis based on the given information so that the probability of making a correct decision is maximized. In safety-monitoring protection systems, *e.g.* in a nuclear power plant, where the system state is monitored by a multi-channel sensor system, various core groups of sensors monitor the status of neutron flux density, coolant temperature at the reaction core exit (outlet temperature), coolant temperature at the core entrance (inlet temperature), coolant flow rate, coolant level in pressurizer, on–off status of coolant pumps. Hazard-preventive actions should be performed when an unsafe state is detected by the sensor system. Similarly, in the case of chlorination of a hydrocarbon gas in a gas-lined reactor, the possibility of an exothermic, runway reaction occurs whenever the Cl_2/hydrocarbon gas ratio is too high, in which case a detonation occurs, since a source of ignition is always present. Therefore, there are three unsafe phenomena: a high chlorine flow y_1, a low hydrocarbon gas flow y_2, and a high chlorine-to-gas ratio in the reactor y_3. The chlorine flow must be shut off when an unsafe state is detected by the sensor system. In this application, each channel monitors a different phenomenon and has different failure probabilities in each mode; the outputs of each channel will have different weights in the decision (output). Similarly, in each channel, there are distinct number of sensors and each sensor might have different capabilities, depending upon its physical position. Therefore, each sensor in a particular channel might have different failure probabilities; thereby, each sensor will have different weights on the channel output. This application can be considered as a two-level weighted threshold voting protection systems.

In undersea communication and decision-making systems, the system consists of n electronic sensors each scanning for an underwater enemy target [16]. Some electronic sensors, however, might falsely detect a target when none is approaching. Therefore, it is important to determine a threshold level that maximizes the probability of making a correct decision.

All these applications have the following working principles in common. (1) System units make individual decisions; thereafter, the system as an entity makes a decision based on the information from the system units. (2) The individual decisions of the system units need not be consistent and can even be contradictory; for any system, rules must be made on how to incorporate all information into a final decision. System units and their outputs are, in general, subject to different errors, which in turn affects the reliability of the system decision.

This chapter has detailed the problem of optimizing the reliability of systems with two failure modes. Some interesting results concerning the behavior of the system reliability function have also been discussed. Several cost optimization problems are also presented. This chapter also presents a brief summary of recent studies in reliability analysis of systems with three failure modes [17–19]. Pham [17] studied dynamic redundant system with three failure modes. Each unit is subject to stuck-at-0, stuck-at-1 and stuck-at-x failures. The system outcome is either good or failed. Focusing on the dynamic majority and k-out-of-n systems, Pham derived optimal design policies for maximizing the system reliability. Nordmann and Pham [18] have presented a simple algorithm to evaluate the reliability of weighted dynamic-threshold voting systems, and they recently presented [19] a general analytic method for evaluating the reliability of weighted-threshold voting systems. It is worth considering the reliability of weighted voting systems with time-dependency.

References

[1] Barlow RE, Hunter LC, Proschan F. Optimum redundancy when components are subject to two kinds of failure. J Soc Ind Appl Math 1963;11(1):64–73.

[2] Ben-Dov Y. Optimal reliability design of k-out-of-n systems subject to two kinds of failure. J Opt Res Soc 1980;31:743–8.

[3] Dhillon BS, Rayapati SN. A complex system reliability evaluation method. Reliab Eng 1986;16:163–77.

[4] Jenney BW, Sherwin DJ. Open and short circuit reliability of systems of identical items. IEEE Trans Reliab 1986;R-35:532–8.

[5] Pham H. Optimal designs of systems with competing failure modes. PhD Dissertation, State University of New York, Buffalo, February 1989 (unpublished).

[6] Malon DM. On a common error in open and short circuit reliability computation. IEEE Trans Reliab 1989;38: 275–6.

[7] Page LB, Perry JE. Optimal series–parallel networks of 3-stage devices. IEEE Trans Reliab 1988;37:388–94.

[8] Pham H. Optimal design of systems subject to two kinds of failure. Proceedings Annual Reliability and Maintainability Symposium, 1990. p.149–52.

[9] Pham H, Pham M. Optimal designs of $\{k, n-k+1\}$ out-of-n: F systems (subject to 2 failure modes). IEEE Trans Reliab 1991;40:559–62.

[10] Sah RK, Stiglitz JE. Qualitative properties of profit making k-out-of-n systems subject to two kinds of failures. IEEE Trans Reliab 1988;37:515–20.

[11] Pham H, Malon DM. Optimal designs of systems with competing failure modes. IEEE Trans Reliab 1994;43: 251–4.

[12] Mathur FP, De Sousa PT. Reliability modeling and analysis of general modular redundant systems. IEEE Trans Reliab 1975;24:296–9.

[13] Horning JJ, Lauer HC, Melliar-Smith PM, Randell B. A program structure for error detection and recovery. Lecture Notes in Computer Science, vol. 16. Springer; 1974. p.177–93.

[14] Pham H, Upadhyaya SJ. Reliability analysis of a class of fault-tolerant systems. IEEE Trans Reliab 1989;38:333–7.

[15] Pham H, editor. Fault-tolerant software systems: techniques and applications. Los Alamitos (CA): IEEE Computer Society Press; 1992.

[16] Pham H. Reliability analysis of digital communication systems with imperfect voters. Math Comput Model J 1997;26:103–12.

[17] Pham H. Reliability analysis of dynamic configurations of systems with three failure modes. Reliab Eng Syst Saf 1999;63:13–23.

[18] Nordmann L, Pham H. Weighted voting human-organization systems. IEEE Trans Syst Man Cybernet Pt A 1997;30(1):543–9.

[19] Nordmann L, Pham H. Weighted voting systems. IEEE Trans Reliab 1999;48:42–9.