

Optimal Cost-Effective Design of Standby Systems Subject to Imperfect Fault-Coverage

Giribabu G¹, Sarmistha Neogy², and Mita Nasipuri³

Jadavpur University, West Bengal, India-700032

¹babugiri71@yahoo.co.in

²sarmisthaneogy@computer.org

³mnasipuri@cse.jdvu.ac.in

Abstract—Fault tolerance is an important design attribute to achieve high reliability. Fault-coverage is a key factor used to account for the efficiency of fault tolerant designs. Systems subject to imperfect fault-coverage may fail even prior to the exhaustion of spares due to uncovered component failures. As a result, reliability of systems subject to imperfect fault coverage decreases after a certain level of active redundancy. Therefore, it is important to consider the effects of imperfect fault-coverage in design and analysis of these systems. It also creates the need to study alternative redundancy mechanisms. In this paper, we study the effects of imperfect fault-coverage in a cold standby system. We show that, unlike in active redundancy, the reliability of a cold standby system always increases with the additional redundancy. However, unlike in the perfect coverage models, there exists a maximum achievable reliability limit for the standby systems subject to imperfect fault-coverage. A closed-form solution to the maximum achievable reliability limit is provided. Further, an algorithm is provided to find the optimal cost-effective redundancy level that strikes a balance between system failure cost and the cost of spares. The results are demonstrated through numerical examples.

I. INTRODUCTION

In many critical applications of digital systems, fault tolerance has been an essential architectural attribute for achieving high reliability [14]. Fault-tolerant designs are particularly important for computer and communication systems that are used in life-critical applications such as flight control and space missions, where online/onboard manual intervention to repair or replace a failed component is difficult. Automatic recovery and reconfiguration mechanisms play a crucial role in implementing fault-tolerance because an uncovered fault may lead to a system failure even when adequate redundancy exists [7]. This is because if a faulty unit is not reconfigured out of the system, it can produce incorrect results that contaminate the non-faulty units. For example, in computing systems, an undetected fault may affect the subsequent calculations and functions and then operate on incorrect data, possibly leading to overall system failure [22]. Further, the effects of fault-coverage also play an important role in electrical power distribution, dangerous fluid transportation, and several standby redundancy applications [1]. The probability of successfully covering a fault (avoiding fault propagation) given that the fault has occurred is known as coverage-factor [7], [22]. Work in [4] shows that the reliability of systems subject to imperfect fault-coverage decreases after a certain level of active redundancy. Therefore, it is important to consider the effects of imperfect fault coverage in designing these systems. It also creates the need for studying alternative redundancy mechanisms.

In this paper, we study the effects of imperfect fault coverage in a cold standby system. We prove that, unlike in active redundancy, reliability of a cold standby system always increases with the additional redundancy. For the perfect coverage models, i.e., when coverage-factor is unity, we can achieve any desired system reliability with the addition of spares. However, it is not possible with imperfect fault-coverage. This means that there exists a maximum achievable reliability limit for the standby systems subject to imperfect fault-coverage. In this paper, we provide a closed form solution to the achievable maximum reliability limit. Hence, in order to improve system reliability, we should not only add additional redundancy but also improve the coverage-factor. The coverage-factor can be improved by using alternative fault-tolerant techniques that have better recovery and reconfiguration capabilities. In [20] various fault-tolerant techniques are discussed in detail and [10] discusses methods to estimate the coverage-factor.

The system failure cost decreases with additional spares because system reliability increases with additional spares. At the same time, the cost of system increases due to increase in the number of redundant components in the system. Thus, it is desirable to derive a cost-effective solution that strikes a balance between the reliability and cost of the system [16]. We also provide an algorithm to find the optimal cost effective redundancy level that strikes a balance between system failure cost and the cost of spares.

Section II presents the background and related work. Section III discusses the reliability evaluation and optimal design policies for a system with active redundancy. Section IV presents the reliability analysis and optimal design policies for a system with standby redundancy. Section V presents the summary of the results.

A. Acronyms & Notations used in present work:

SEA	simple and efficient algorithm [3]
n	number of components in the system
p	reliability of a component; for exponential failure distribution, $p = \exp\{-\lambda t\}$
q	unreliability of a component; $q = 1 - p$
c	coverage factor; $\Pr\{\text{system can recover} \mid \text{a fault occurs}\}$; see [7]
w	$\Pr\{\text{no uncovered failure of a component}\}$; $w = p + c.q$; see [3]
v	$\Pr\{\text{covered failure of a component}\}$; $v = c.q = w.Q$; see [3]
P	conditional reliability used in SEA; $P = p/w$

Q	conditional unreliability used in SEA; $Q = 1 - P = 1 - p/w = c.q/w$
R	reliability of the system; $R \equiv R(n)$
d_1	cost of each component
d_2	cost of system failure
T	average system cost; $T \equiv T(n)$
\bar{x}	compliment of x ; $\bar{x} \equiv 1 - x$
i.i.d	independent identically distributed
gilb(.)	greatest integer lower bound
inf(.)	infimum or greatest lower bound

II. BACKGROUND AND RELATED WORK

The seminal paper by Bouricius et al. [9] first defined coverage as a conditional probability to account for the efficiency of fault-tolerant mechanisms. This concept rapidly became widely recognized as a major concern in dependability evaluation studies. Since then, a large amount of work has been devoted to refining the notion of coverage [8], to the identification or estimation of relevant parameters [10], [18] and to developing associated system level models [12]. Coverage modeling introduces additional dependencies among system components. The landmark developments in solving these models include decomposition techniques (1983) [21], Markov chain-based solutions (1985-1995) [12], multi-state combinatorial techniques (1995) [11], and a separable method (1999) called the Simple and Efficient Algorithm (SEA) [3], which uses conditional probabilities. As its name suggests, SEA is simple and efficient compared to all other existing methods for solving imperfect fault-coverage models. Two main advantages of SEA are that (1) it can convert a fault coverage model into an equivalent perfect coverage model in linear time, and (2) it can produce simple closed-form solutions for all well-structured systems. As a result, the computational complexity of a fault-coverage model is reduced to its equivalent perfect coverage model, which in turn proves that it is impossible to find a better algorithm than SEA. The closed-form solutions help to study the system in detail and find efficient algorithms for optimal designs [4], [1].

Amari et al [4] proved that reliability of any system subject to imperfect fault-coverage decreases after a certain level of active redundancy. Therefore, there exists an optimal level of redundancy that maximizes the overall system reliability. These results coincide with the observations made in [12]. Specifically, [12] has shown that both reliability and mean time to failure (MTTF) of parallel systems subject to imperfect fault-coverage decreases with the increase in number of parallel components after reaching a certain limit. Initially, these observations seem counter intuitive. However, as explained in [12], the systems subject to imperfect fault-coverage can fail in two modes: covered failure and uncovered failure. Irrespective of the system structure function, the system behaves like a series system for the uncovered failure mode, which is a dominant failure mode for the systems with a large number of components. Therefore, system reliability decreases with an increase of redundant components after a certain limit. Several researchers have shown similar results for some special cases of k-out-of-n systems that include triple modular redundancy with spares [16], k-resilient protocols [19], and gracefully degradable systems [13]. [4] provides closed-form solutions for optimal

redundancy that maximize the reliability of various standard system models that include parallel system, series-parallel systems, parallel-series systems, N-tuple modular systems, and k-out-of-n systems. Similarly, using the concepts of SEA, the cost-effective design policies for parallel systems subject to imperfect fault-coverage are provided [2]. Works in [1] extended these results for complex systems composed of k-out-of-n subsystems and evaluated lower and upper bounds for optimal redundancy levels for both reliability optimization and cost minimization problems.

In all the previous studies, the aim is to (1) show the negative effects of imperfect fault-coverage, (2) emphasize the need for accurate analysis of coverage factor, and (3) emphasize the use of optimal redundancy (thereby discouraging the use of too much redundancy). In addition to this, [6] also discusses some alternative means for proving redundancy that include adding the redundancy in periodic intervals, use of standby redundancy, and adding the redundancy only when a certain predefined number of components have failed. In this paper, we consider the effects of imperfect fault-coverage on the cold standby redundancy policies. In order to compare the policies between standby redundancy and active redundancy, we also provide the results for active redundancy.

III. ACTIVE REDUNDANCY

In this section, we consider a parallel system with active redundancy.

A. Assumptions

- System consists of n i.i.d components.
- Reliability of each component is p .
- Coverage factor of each component is c .
- Cost of each component is d_1 .
- Cost of system failure is d_2 .

B. Reliability Evaluation and Optimization

Using SEA [3], reliability of the system can be expressed as:

$$R(n) = \frac{(w)^n \cdot [1 - Q^n]}{w^n - v^n} \quad (1)$$

From [4], the optimal n that maximizes $R(n)$ is n_1 .

$$n^* = n_1 \equiv \text{gilb} \left\{ \frac{\ln(\frac{v}{w})}{\ln(\frac{w}{v})} \right\} + 1 \quad (2)$$

Example 1: Given: $p = 0.9$ and $c = 0.95$.

Then, $w = 0.995$ and $v = 0.005025$. Therefore, from (2) $n^* = 3$ and $R(n^*) = 0.984$. ■

C. Cost Minimization

The average system cost, $T(n)$, is the cost incurred when the system has failed plus the cost of all components in the system.

$$T(n) = d_1 \cdot n + d_2 \cdot [1 - R(n)] \quad (3)$$

$R(n)$ is defined in (1).

From [2], the optimal n that minimizes $T(n)$ is n_2 .

$$n^* = n_2 \equiv \inf \left\{ n: f(n) < \frac{d_1}{d_2} \right\} \\ \equiv \inf \left\{ n \in [1, n_1]: f(n) < \frac{d_1}{d_2} \right\} \quad (4)$$

n_1 is defined in (2).

Example 2: Given: $p = 0.9, c = 0.95, d_1 = 1, d_2 = 1000$. Then, $d_1/d_2 = 0.001$. Therefore, from (4) $n^* = 3$ and $T(n^*) = 18.78$. ■

We can find the closed-form solution for the perfect coverage case, i.e., $c = 1$. From [6], the optimal n for this case is n_3 .

$$n^* = n_3 \equiv \text{glib} \left\{ \frac{\ln \left(\frac{d_1}{d_2 p} \right)}{\ln(q)} \right\} + 1 \quad (5)$$

Example 3: Given: $p = 0.9, d_1 = 1, d_2 = 1000$. Therefore, from (5) $n^* = 3$ and $T(n^*) = 4$. ■

IV. STANDBY REDUNDANCY

In this section, we consider a cold standby system subject to imperfect fault coverage.

A. Assumptions

- System consists of n i.i.d components.
- Initially only one component is in operation; remaining $(n - 1)$ components are in cold standby.
- Failure time of an operating component follows exponential distribution with failure rate λ .
- Components in standby mode cannot fail, i.e., failure rate in standby mode is zero.
- Coverage factor at failure of an operating component is c , i.e., when an operating component fails, it is replaced by standby component with probability c .
- System fails if all components fail in covered mode or any component fails in uncovered mode.
- Cost of each component is d_1 .
- Cost of system failure is d_2 .

B. Reliability Evaluation and Optimization

Standby redundancy introduces additional stochastic dependency among component failures. Therefore, we cannot use the SEA to find reliability of standby systems subject to imperfect fault-coverage. However, reliability of the system can be obtained using Markov chains. The state transition diagram of the underlying Markov process is shown in Figure 1.

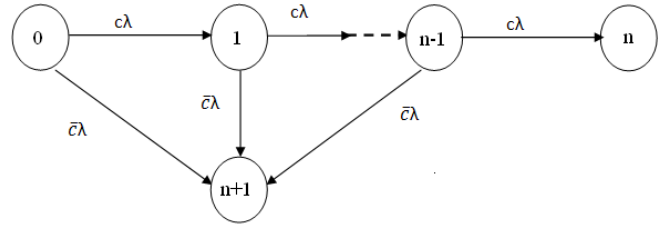


Fig. 1. State transition diagram of cold standby system subject to imperfect fault-coverage

State Description

- State i Represents number of failed components in system; $0 \leq i \leq n-1$; all these states are good states of system
- State n Represents covered failure state of system; this state is reached if spares are exhausted
- State $(n+1)$ Represents uncovered failure state of system ■

Solving the Markov chain shown in Figure 1, the reliability of the system at time t can be expressed as in (6).

$$R(n) = e^{-c\lambda t} \left[\sum_{i=0}^{n-1} \frac{(c\lambda t)^i}{i!} e^{-c\lambda t} \right] \\ = \sum_{i=0}^{n-1} \frac{(c\lambda t)^i}{i!} e^{-\lambda t} \quad (6)$$

Theorem 1: The reliability of a cold standby system subject to imperfect fault-coverage always increases with the number of standby components.

Proof: The reliability of the system can be expressed as a product of two functions $f_1(n)$ and $f_2(n)$.

$$R(n) = f_1(n) \cdot f_2(n) \\ f_1(n) = \sum_{i=0}^{n-1} \frac{(c\lambda t)^i}{i!} \\ f_2(n) = e^{-\lambda t} \quad (7)$$

Where $f_2(n)$ is independent of n and $f_1(n)$ is an increasing function in n . In fact, $f_1(n) \cdot e^{c\lambda t}$ is the reliability of a cold standby system with perfect coverage where the failure rate of each component is $c\lambda$. Therefore, the reliability of the system, $R(n)$, is an increasing function of n . ■

Therefore, unlike in active redundancy (hot standby system), the reliability of cold standby systems subject to imperfect coverage always increases with the number of redundant components in the system.

Lemma 1: When the cold standby system is subject to imperfect fault-coverage, the maximum achievable reliability of the system is $R(\infty) = e^{-c\lambda t}$. ■

Therefore, unlike the perfect fault-coverage case, we are not able to increase the reliability of a standby system with imperfect fault-coverage to unity.

Example 4: Given: $\lambda = 0.1, c = 0.95$, and $t = 1$.

Therefore, from lemma 1, maximum achievable reliability is 0.9950125. ■

C. Cost Minimization

The average system cost, $T(n)$, is the cost incurred when the system has failed plus the cost of all components in the system.

$$T(n) = d_1.n + d_2.[1 - R(n)] \quad (8)$$

$R(n)$ is defined in (6).

Lemma 2: Let us define

$$f(n) \equiv \Delta R(n) = R(n+1) - R(n) \\ = \frac{(c\lambda t)^n}{n!} e^{-\lambda t}$$

$$s_a \equiv \text{glib}\{c\lambda t - 1\} \\ s_0 \equiv \max\{1, s_a\} \\ t_0 \equiv \frac{1}{c\lambda} \quad (9)$$

- 1) For any given mission time of system, t ($0 < t < t_0$), $f(n)$ is decreasing in n for all $n \geq 1$.
- 2) For any given mission time of system, t ($t_0 < t \leq \infty$), $f(n)$: (i) is increasing in n for $1 \leq n < s_0$, (ii) is decreasing in n for $s_0 < n < \infty$, and (iii) is a stationary maximum at $s_0 + 1$.

Proof:

$$\Delta f(n) \equiv f(n+1) - f(n) \quad (10)$$

From (9)—

$$\Delta f(n) = \frac{(c\lambda t)^{n+1}}{(n+1)!} e^{-\lambda t} - \frac{(c\lambda t)^n}{n!} e^{-\lambda t} \\ = \frac{(c\lambda t)^n}{n!} e^{-\lambda t} \left[\frac{c\lambda t}{n+1} - 1 \right] \quad (11)$$

Therefore, $\Delta f(n) \geq 0$; iff –

$$c\lambda t \geq n + 1 \\ n \leq \text{glib}\{c\lambda t - 1\} \equiv s_a \quad (12)$$

Similarly, $\Delta f(n) \leq 0$ iff $n \geq s_a$. Let $t_0 = 1/c\lambda$, then, it follows that:

- 1) If $0 < t \leq t_0$, then $s_a < 0$. However, $n \geq 1$, then $\Delta f(n) \leq 0$ for all n . Thus, $f(n)$ is decreasing in n for all $n \geq 1$.
- 2) If $t > t_0$, then $s_0 = s_a \geq 0$. Thus, $f(n)$ is increasing in n for $1 \leq n < s_0 = s_a$, and is decreasing in n for $s_0 < n < \infty$.

Let—

$$s_1 \equiv \inf\{n : f(n) < c/d\} \\ s_2 \equiv \inf\{n \in [s_0, \infty) : f(n) < c/d\} \quad (13)$$

$f(n)$, s_0 are defined in lemma 2.

Determination of the optimal number of components, n^* , that minimizes the average system cost, $T(n)$, is summarized in theorem 2

Theorem 2: For fixed λ , c , t , d_1 , and d_2 , there exists an optimal value n^* such that the average system cost of the cold

standby system subject to imperfect fault-coverage, $T(n)$, is minimized.

- 1) If $t \leq t_0$, then $n^* = s_1$.
- 2) If $t > t_0$, then
if $f(s_0) < d_1/d_2$, then $n^* = 1$
else if $f(1) \geq d_1/d_2$, then $n^* = s_2$
else if $T(1) > T(n_2)$, then $n^* = s_2$
else $n^* = 1$.

Proof:

$$\Delta T(n) \equiv T(n+1) - T(n) \quad (14)$$

From (6) and (8)

$$\Delta T(n) \equiv d_1 - d_2 \cdot [R(n+1) - R(n)] \\ \equiv d_1 - d_2 \cdot f(n) \quad (15)$$

$f(n)$ is defined as in (9). Therefore, $\Delta T(n) \leq 0$ iff $f(n) \geq d_1/d_2$.

- 1) If $t \leq t_0$, then $s_a < 0$. Then $f(n)$ is decreasing in n for all $n \geq 1$ (from lemma 2).
- 2) If $t > t_0$, then $s_a = s_0$ is a non-negative integer.

Therefore, the rest of the proof is similar to the proof provided in [15]. ■

Example 5: Given: $\lambda = 0.1$, $c = 0.95$, $t = 1$, $d_1 = 1$, and $d_2 = 1000$.

Therefore, from theorem 2, $n^* = 3$ and $T(n^*) = 8.1199$. ■

V. CONCLUSIONS

This paper discusses the effects of imperfect fault-coverage in a cold standby system. It is shown that, unlike in active redundancy, reliability of a cold standby system always increases with the additional redundancy. However, unlike in the perfect coverage models, there exists a maximum achievable reliability limit for the standby system subject to imperfect fault-coverage. A closed-form solution to the maximum achievable reliability limit is provided. Further, a simple searching algorithm is provided to find the optimal cost-effective redundancy level that strikes a balance between system failure cost and the cost of spares.

REFERENCES

[1] S.V. Amari, H. Pham, G. Dill, "Optimal design of k-out-of-n:G subsystems subjected to imperfect fault-coverage", *IEEE Trans. On Reliability*, vol 53, pp. 567-575, December 2004.
 [2] S.V. Amari, L. McLaughlin, B. Yadlapati, "Optimal cost-effective design of parallel systems subject to imperfect fault-coverage", *Annual Proc. Reliability and Maintainability Symposium*, pp. 29-34, 2003.
 [3] S.V. Amari, J.B. Dugan, and R.B. Misra, "A separable method for incorporating imperfect fault-coverage into combinatorial models", *IEEE Trans. on Reliability*, vol. 48, pp. 267-274, Sep. 1999.
 [4] S.V. Amari, J.B. Dugan, and R.B. Misra, "Optimal reliability of systems subject to imperfect fault-coverage", *IEEE Trans. on Reliability*, vol. 48, pp. 275-284, Sep. 1999.
 [5] S.V. Amari, R.B. Misra, "Closed-form expressions for distribution of sum of exponential random variables", *IEEE Trans. Reliability*, vol. 46, pp. 519-522, 1997.

- [6] S.V. Amari, "Reliability, risk and fault-tolerance of complex systems", *PhD Dissertation*, Indian Institute of Technology, Kharagpur, 1997.
- [7] T. F. Arnold, "The concept of coverage and its effect on the reliability model of a repairable system", *IEEE Trans. on Computers*, vol. C-22, pp. 325-339, Mar. 1973.
- [8] A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", *IEEE Trans. On Dependable and Secure Computing*, vol. 1, pp 11-33, 2004.
- [9] W. G. Bouricius, W. C. Carter, P. R. Schneider, "Reliability modeling techniques for self-repairing computer systems," *Proc. 24th Ann. ACM., Nat'l Conf.*, pp 295-309, 1969.
- [10] M. Cukier, D. Powell, J. Arlat, "Coverage estimation methods for stratified fault-injection", *IEEE Trans. on Computers*, vol. 48, pp.707-723, July 1999.
- [11] S. A. Doyle, J. B. Dugan, F. A. Patterson-Hine, "A combinatorial approach to modeling imperfect coverage", *IEEE Trans. on Reliability*, vol. 44, pp. 87-94, Mar. 1995.
- [12] J. B. Dugan, K. S. Trivedi, "Coverage modeling for dependability analysis of fault-tolerant systems", *IEEE Trans. on Computers*, vol. 38, pp. 775-787, 1989.
- [13] W.A. Najjar and J. Gaudiot, "Scalability analysis in gracefully degradable large systems", *IEEE Trans. on Reliability*, vol. 40, pp. 189-197, Jun. 1991.
- [14] H. Pham and S.J. Upadhyaya, "Reliability analysis of a class of fault tolerant systems", *IEEE Trans. on Reliability*, vol. 38, pp. 333-337, Aug. 1989.
- [15] H. Pham, "On the optimal design of k-out-of-n:G subsystems", *IEEE Trans. on Reliability*, vol. 41, pp. 572-574, Dec. 1992.
- [16] H. Pham, "Optimal cost-effective design of triple-modular-redundancy with spares systems", *IEEE Trans. on Reliability*, vol. 42, pp. 369-374, Sep. 1993.
- [17] H. Pham and W. J. Galyean, "Reliability analysis of nuclear fail-safe redundancy", *Reliability Engineering and System Safety*, vol. 37, pp. 109-112, 1992.
- [18] D. Powell, E. Martins, J. Arlat, Y. Crouzet, "Estimators for fault tolerance coverage evaluation," *IEEE Trans. on Computers*, vol. 44, pp 261-274, 1995.
- [19] S. Rangarajan, Y. Huang, S. K. Tripathi, Computing reliability intervals for k-resilient protocols, *IEEE Trans. on Computers*, Vol. 44, pp. 462- 466, 1995.
- [20] M. L. Shooman, *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*, John Wiley & Sons, 2002.
- [21] K. S. Trivedi, R. Geist, "Decomposition in reliability analysis of fault tolerant systems", *IEEE Trans. on Reliability*, vol. R-32, pp 463-468, Dec. 1983.
- [22] W. Vesely, et al, *Fault Tree Handbook with Aerospace Applications*, Version 1.1, Aug. 2002.