Reliability Engineering and System Safety 119 (2013) 18–25

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Optimal structure of multi-state systems with multi-fault coverage

Rui Peng [a,*], Huadong Mo [b], Min Xie [b], Gregory Levitin [c]

[a] Dongling School of Economics and Management, University of Science and Technology Beijing, Beijing 100083, China
[b] Department of Systems Engineering and Engineering Management, City University of Hong Kong, Hong Kong
[c] The Israel Electric Corporation Ltd., Haifa, Israel

ARTICLE INFO

Article history:
Received 12 October 2012
Received in revised form
19 April 2013
Accepted 3 May 2013
Available online 16 May 2013

Keywords:
Genetic algorithm
Imperfect fault coverage
Reliability
Multi-fault coverage
Fault level coverage
Universal generating function

ABSTRACT

Due to imperfect fault coverage, the reliability of redundant systems cannot be enhanced unlimitedly with the increase of redundancy. Thus it is essential to study the optimal structure of redundant systems. This paper considers a multi-state series-parallel system with two types of parallelization: redundancy and work sharing. Different from existing works which consider single-fault coverage, multi-fault coverage is considered in order to adapt to a wider range of fault tolerant mechanisms. For multi-fault coverage, the coverage factor of an element failure in a work sharing group depends on the status of other elements. It is assumed that the uncovered failures in the elements belonging to the group of elements sharing the same task can cause failure of the entire group. The optimal trade-off between the two kinds of parallelization has been studied based on various settings of fault coverage factor. Examples of data transmission systems and task processing systems are presented to illustrate the applications of results.

1. Introduction

Fault tolerance is widely used to enhance system reliability, especially for systems with stringent reliability requirements, such as nuclear power controllers and flight control systems [12,8,22,20]. However, as the fault and error handling mechanisms (detection, location, and isolation) themselves can fail, some failures can remain undetected or uncovered, which can lead to total failure of the entire system or its sub-systems [17,26,13]. Examples of this effect of uncovered faults can be found in computing systems, electrical power distribution networks, phased mission systems etc [5,27,24].

The probability of successfully covering a fault (avoiding fault propagation) given that the fault has occurred is known as the coverage factor [4,1,2]. Due to the existence of different fault covering mechanisms, different coverage models have been studied in literatures [25,18,19]. Among these models, element level coverage (ELC) model and fault level coverage (FLC) model are the most important and widely studied. For ELC, the coverage probability of each system component is independent from the status of other components. ELC is typical for systems containing a built-in test (BIT) capability, where the selection among the redundant elements is made on the basis of a self-diagnostic capability of the individual elements. For FLC, the coverage probability of a system element depends on the number of failed elements. In other words, the selection among redundant elements varies between initial and subsequent failures. In the HARP terminology [3], ELC models are known as single-fault models, whereas FLC models are known as multi-fault models. Multi-fault models have the ability to model a wide range of fault tolerant mechanisms. An example is a majority voting system among the currently known working elements, see Myers and Rauzy [18].

Due to imperfect fault coverage, the system reliability can decrease with increase of redundancy over some particular limit [11,17]. As a result the system structure optimization problems arise. Some of these problems have been formulated and solved for parallel systems, k-out-of-n systems [1,2]. Levitin [10] presents a model of series-parallel multi-state systems (MSS) with two types of task parallelization: parallel task execution with work sharing, and redundant task execution. A framework to solve the optimal balance of the two kinds of parallelization which maximizes the system reliability is proposed based on the assumption that the ELC applies in each work sharing group. Considering the different types of fault handling mechanisms in practice, the ELC model alone cannot adapt to all the cases. Though Levitin and Amari [11] proposed a way to evaluate the reliability of MSS considering FLC, the system structure optimization problem was

Abbreviations: BIT, built-in test; ELC, element level coverage; FLC, fault level coverage; MSS, multi-state system; pmf, probability mass function; GA, genetic algorithm; WSG, work sharing group (group of elements affected by uncovered failures); UGF, universal generating function.

* Corresponding author. Tel.: +86 1305 154 0519.
E-mail addresses: pengrui1988@gmail.com, ruipeng@mail.ustc.edu.cn (R. Peng).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.05.007

Nomenclature

$1(x)$	unity function: 1(TRUE)=1, 1(FALSE)=0
θ^*	system demand
C^*	minimum allowed MSS capacity
T^*	maximum allowed MSS task execution time
E_m	number of parallel elements in subsystem m
$f(V, \theta^*)$	acceptability function
G_j	random performance of system element j
$\mathbf{g}_j$	set of possible realizations of G_j
g_{jh}	hth realization of G_j
M	number of subsystems connected in series
V	random system performance
v_i	ith realization of V
$c_m(\lvert\Phi_{mi}\rvert, j)$	the fault coverage probability in the case of jth failure in WSG i in subsystem m
$r_{mi}(k)$	the probability that WSG i in subsystem m does not fail after k failures have consecutively occurred
$u_j(z)$	UGF representing the pmf of G_j
$U_s(z)$	UGF representing the pmf of V
$U_{mi}(z)$	UGF representing the pmf of cumulative performance of WSG i in subsystem m
$U_m(z)$	UGF representing the pmf of cumulative performance of subsystem m
ϕ	system structure function: $V=\phi(G_1,\ldots,G_n)$
Φ_m	set of elements belonging to subsystem m
Φ_{mi}	set of elements belonging to the ith WSG of subsystem m

not studied. In Levitin [10], the incorporation of imperfect coverage is handled by using a special term to denote the case of uncovered failure in the universal generating function (UGF) of each element. After calculating the probability that the system fails due to uncovered element failure, the problem is reduced to the case where no uncovered failure exists. Incorporating FLC into the system structure optimization framework is much more complicated than incorporating ELC, especially for coding and programming, as not only the system performance but also the number of failed elements in each work sharing group need to be tracked. Besides, the consideration of FLC allows us to analyze the optimal system structure for different changing trends of the fault coverage factor with the number of failed elements. In order to provide a useful reference to the practitioners, this paper extends the problem of finding the optimal balance between the two kinds of parallelization to the case of FLC.

Section 2 presents the model. Section 3 describes the UGF based algorithm for evaluating the reliability of series-parallel MSS with FLC. Section 4 discusses the optimization procedures with the genetic algorithm technique. Numerical examples are shown in Section 5 to illustrate the applications of the framework in different situations.

2. Model description and problem formulation

Consider a system consisting of M subsystems connected in series. Each subsystem m contains E_m different elements connected in parallel. In each subsystem, the elements can be separated into several work sharing groups (WSG). In each WSG, the available elements share their work in an optimal way that maximizes the performance of the entire group. In case when some element fails in a WSG, the resource management system is able to redistribute the task among the available elements if the failure is covered. It is assumed that the states of all the elements are independent. In particular, the failure probability of each element is not influenced by whether other components in the same WSG have failed. However, an undetected failure of any element in a WSG causes the failure of the entire group.

The performance rate G_j of any system element j is assumed to have k_j+1 possible realizations, which are represented by the set $\mathbf{g}_j = g_{j0}, g_{j1}, \ldots, g_{jk_j}$. The state 0 corresponds to the total element failure, and the other k_j states correspond to the working states with full or partial performance. The probability associated with different values of G_j can be represented by the set $\mathbf{p}_j = p_{j0}, p_{j1}, \ldots, p_{jk_j}$ where $p_{jh} = \Pr(G_j = g_{jh})$ and $\sum_{h=0}^{k_j} p_{jh} = 1$.

Given the performance rates of the system elements, the performance rate of the entire system is determined by the system structure, that is, the distribution of elements among WSG in each subsystem. The mapping from the spaces of the elements' performance rates into the space of the system's performance rates is denoted by the system structure function $V=\phi\ (G_1,\ldots,G_n)$, where the system performance rate V is a random variable which takes values from the set $\{v_0,\ldots,v_K\}$.

In line with Levitin [10], the elements' distribution among WSG in each component m is considered as partitioning a set Φ_m of E_m items into E_m mutually disjoint subsets Φ_{mi}, i.e. such that

$$\bigcup_{i=1}^{E_m} \Phi_{mi} = \Phi_m \tag{1}$$

$$\Phi_{mi} \cap \Phi_{mj} = \varnothing\ , i \neq j \tag{2}$$

Each set can contain from 0 to E_m elements. The partition of the set Φ_m can be represented by the vector $\boldsymbol{\alpha}_m = \{\alpha_{mj}, 1 \leq j \leq E_m\}$, where α_{mj} is the index of the subset to which element j belongs.

For any given system structure $\boldsymbol{\alpha} = \{\boldsymbol{\alpha}_1,\ldots, \boldsymbol{\alpha}_M\}$, and given pmf of the system elements, one can obtain the pmf of the entire system performance V in the form

$$Q_i, v_i, 0 \leq i \leq K, \text{where} \quad Q_i = \Pr(V = v_i) \tag{3}$$

The MSS reliability is defined as the probability that the MSS satisfies the demand [9] as

$$R(\theta^*) = \sum_{i=0}^{K} Q_i f(v_i, \theta^*) \tag{4}$$

where the acceptability function $f(V,\theta^*)$ represents the desired relation between the system performance V and the system demand θ^* ($f(V,\theta^*)=1$ if the system performance is acceptable, and $f(V,\theta^*)=0$ otherwise). For example, in applications where the system performance is defined as a task execution time, and $\theta^*=T^*$ is the maximum allowed task execution time, $f(v_i, \theta^*)$ can be represented as $1(v_i < T^*)$. In applications where the system performance is defined as its productivity/capacity, and $\theta^*=C^*$ is the minimum allowed capacity, $f(v_i, \theta^*)$ can be represented as $1(v_i > C^*)$.

The MSS structure optimization problem is to find the optimal elements distribution $\boldsymbol{\alpha} = \{\boldsymbol{\alpha}_1,\ldots, \boldsymbol{\alpha}_M\}$, which maximizes MSS reliability $R(\theta^*)$ for a given demand θ^*,

$$\boldsymbol{\alpha} = \text{argmax}\{R(\boldsymbol{\alpha}, \theta^*)\}. \tag{5}$$