Available online at www.sciencedirect.com
ScienceDirect
Reliability Engineering and System Safety 93 (2008) 1730–1739
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

Multi-state systems with multi-fault coverage

Gregory Levitin[a,*], Suprasad V. Amari[b]

[a]Israel Electric Corporation Ltd., P.O. Box 10, Haifa 31000, Israel
[b]Relex Software Corporation, 540 Pellis Road, Greensburg, PA 15601, USA

Received 29 November 2006; received in revised form 27 November 2007; accepted 2 December 2007
Available online 15 December 2007

Abstract

The paper introduces a new model of fault level coverage for multi-state systems in which the effectiveness of recovery mechanisms depends on the coexistence of multiple faults in related elements. Examples of this effect can be found in computing systems, electrical power distribution networks, pipelines carrying dangerous materials, etc. For evaluating reliability and performance indices of multi-state systems with imperfect multi-fault coverage, a modification of the generalized reliability block diagram (RBD) method is suggested. This method, based on a universal generating function technique, allows performance distribution of complex multi-state series–parallel system with multi-fault coverage to be obtained using a straightforward recursive procedure. Illustrative examples are presented.

Keywords: Multi-state system; Fault-tolerant system; Imperfect fault coverage; Reliability; Multi-fault coverage; Universal generating function

1. Introduction

Fault-tolerant system design is aimed at preventing the entire system failure even when some of its elements fail. Usually the fault tolerance is implemented by providing sufficient redundancy and using automatic recovery and reconfiguration mechanisms. However, some failures can remain undetected or uncovered, which can lead to the total failure of the entire system or its sub-systems. Examples of this effect of uncovered faults can be found in computing systems, electrical power distribution networks, pipelines carrying dangerous materials, etc. [1].

The systems with imperfect fault coverage have been intensively studied in [1–8]. It was shown that the system reliability can decrease with an increase in redundancy over some particular limit if the system is subjected to imperfect fault coverage [2]. As a result the system structure optimization problems arise. Some of these problems have been formulated and solved for parallel and k-out-of-n systems [4,5].

In many cases the system and its elements can function at different states characterized by different levels of performance. Such systems are referred to as multi-state systems (MSS). When applied to MSS, reliability is considered to be a measure of the ability of the system to provide a required performance level [11]. MSS can also be subjected to uncovered faults that lead to the total failure of the entire system or its subsystems [7,8,16].

1.1. Coverage models

The models that consider the effects of imperfect fault coverage are known as imperfect fault coverage models or simply fault coverage models or coverage models [2]. Depending on the type of fault-tolerant techniques used, the models are classified as [12]

- *Element level coverage* (ELC) *or single-fault models*: A particular fault coverage probability is associated with each element. This value is independent of the status of other elements.
- *Fault level coverage* (FLC) *or multi-fault models*: The fault coverage probability depends on the number of failed elements that belong to a specific group.

The ELC model is appropriate when the selection among the redundant elements is made on the basis of

*Corresponding author.
E-mail addresses: levitin@iec.co.il (G. Levitin), suprasad.amari@relex.com (S.V. Amari).

0951-8320/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2007.12.004

Nomenclature

RBD	reliability block diagram
FLC	fault level coverage
ELC	element level coverage
MSS	multi-state system
UGF, *u*-function	universal generating function
pmf	probability mass function
$\Pr\{e\}$	probability of event *e*
$E[X]$	expected value of *X*
$1(x)$	unity function: 1(TRUE) = 1, 1(FALSE) = 0
n	number of system elements
G_j	random performance of system element *j*
$\mathbf{g}_j$	set of possible realizations of G_j
g_{jh}	*h*th realization of G_j
x_j	performance of element (system) in a state of total failure
p_{jh}	$\Pr\{G_j = g_{jh}\}$
V	random system performance
v_i	*i*th realization of *V*
q_i	$\Pr\{V = v_i\}$
ϕ	system structure function: $V = \phi(G_1, \ldots, G_n)$
θ	system demand
$f(V, \theta)$	acceptability function
$R(\theta)$	system reliability: $\Pr\{f(V, \theta^*) = 1\}$
$W(\theta)$	conditional expected system performance
ω_k	set of elements affected by an uncovered failure (belonging to FLC group *k*)
$c_k(j)$	fault coverage probability in the case of exactly *j* failures in FLC group *k*
$r_k(j)$	probability that FLC group *k* continues functioning after failure of *j* elements
$u_j(z)$	*u*-function representing pmf of G_j
$\tilde{U}_\omega(z)$	*u*-function representing distribution of both performance and number of failed elements in subsystem consisting of elements belonging to set ω
$\tilde{u}_j(z)$	*u*-function representing distribution of both performance and state (number of failures) of element *j*
$U_\omega(z)$	*u*-function representing pmf of performance of subsystem consisting of elements belonging to set ω
$U(z)$	*u*-function representing pmf of *V*
$\otimes_\varphi$	composition operator over *u*-functions
$\varphi(G_i, G_j)$	function representing performance of pairs of elements

a self-diagnostic capability of the individual elements. Such systems typically contain a built-in test capability. The FLC model is appropriate for modeling systems in which the selection among available elements varies between initial and subsequent failures. In the ELC models, the effectiveness of recovery mechanisms depends on the occurrence of individual faults. A multi-element system with ELC can tolerate multiple coexisting single-faults. However, for any given fault, the success or failures of a recovery mechanism is independent of the status of other elements (or faults in the other elements). In the FLC models, the effectiveness of recovery mechanism depends on the occurrence of multiple faults within a recovery window. Ref. [12] compared the results of ELC and FLC models with that of perfect coverage models. The comparison indicates that the unreliability of a system for the ELC case is very high as compared with the FLC case. From this comparison, it is also apparent as to why systems requiring extremely low probabilities of failure use mid-value-select voting-based redundancy management (appropriately modeled with FLC), rather than a BIT-based approach (modeled with ELC). For more details on the comparison of ELC and FLC models and their applications, refer to [12].

Although the coverage models have been studied for several decades, the solutions to FLC models are still limited and require efficient methods [6]. In addition, several systems are accurately modeled using MSS and they can also be subjected to uncovered failures associated with the automatic recovery mechanisms. Recently, some authors studied the MSS using ELC models. In this paper, we model and solve the MSS using FLC models.

Consider for example a multi-channel data transmission system in which data packages are divided into sub-packages transmitted through different channels. This method allows the work to be shared among the channels, which results in accelerating the data transmission process. If some channels fail, an automatic data exchange management system is able to distribute the transmission task among the available channels. In this case the system performance (bandwidth) lowers, but the system remains operating. However, when a failure of any channel remains undetected, the management system cannot make the proper reconfiguration (cover the failure) and still assigns some sub-package to the unavailable channel. Therefore, some information is lost and the entire data transmission task fails.

If each channel has its individual fault detection and recovery mechanism, the channel failure detection/coverage probability does not depend on the number of available (failed) channels and the data transmission system can be represented by the ELS model. However, in many cases the fault detection and recovery is provided by a mechanism common for all the channels. The efficiency of this mechanism depends on the number of communication channels it monitors simultaneously. Therefore, the channel failure detection/coverage probability depends on the number of available channels. Such a situation corresponds to the FLC model.

Similarly, we can find the applications of FLC models in computer control systems used in aircraft applications