Reliability Engineering and System Safety 165 (2017) 336–344

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Optimal backup in heterogeneous standby systems exposed to shocks

Gregory Levitin[a,b,*], Maxim Finkelstein[c,d]

[a] University of Electronic Science and Technology of China, Chengdu, China
[b] The Israel Electric Corporation, Haifa, Israel
[c] University of the Free State, Bloemfontein, South Africa
[d] ITMO University, St. Petersburg, Russia

ARTICLE INFO

Keywords:
Backup
Chocks
Warm standby
Mission success probability
Expected mission completion time
Optimization

ABSTRACT

The paper considers non-repairable 1-out-of-*N* heterogeneous warm standby computing systems with components exposed to internal failures and external shocks. To provide the data recovery in the case of operating component failure, the backup procedures are performed during the computational mission. The backups enable an activated standby component to take over the mission task from the point where the last backup has been completed without redoing the entire task from scratch. Both data backup and retrieval times depend on the amount of work performed. The system components are characterized by a different performance level, replacement time, time-to-internal failure distribution, and shocks survival probability. The shock processes also have different characteristics for different components. A numerical method is proposed to evaluate mission success probability for a given allowed mission time and expected mission completion time. The optimal backup scheduling problem is then formulated and solved for different optimization objectives and constraints.

1. Introduction

To enhance the system reliability, the standby sparing technique is widely applied in various application areas such as high performance computing [1], flight control [2], space missions [3], and power systems [4,5]. In a standby system part of components is in operation whereas other components serve as standby spares. When an operating component fails, a standby component is activated to take over the system task. Before being put into operation, standby components can exhibit different failure characteristics [6]: they can be unpowered, completely shielded from the working stresses, and thus have a zero constant failure function (cold standby); alternatively they can work in synchrony with the online components, being fully exposed to the working stresses, and thus having the same failure rate as online components (hot standby). A general model (warm standby) assumes that the standby components can be exposed to certain stresses, and their failure function be dominated by their corresponding full operational failure function [7,8]. The cold and hot standby can be considered as special cases of the general warm standby model.

To avoid redoing the mission task from scratch in the case of operating component failure, the backup technique is used in computing systems [9–11]. Each operating component usually performs a number of data backup procedures during its mission based on a predetermined schedule. These backup procedures are associated with additional mission time. The data backup time incurred in each backup action typically depends on the amount of work conducted since the last backup or since the beginning of the mission. When an operating component fails, a replacement procedure is initiated to activate a selected standby component, and to transfer the previously-saved data from the backup storage to the selected component. The activation can include powering and/or connecting, testing, warming up or synchronizing the standby element. The time of the activation/replacement procedure also contribute to the entire mission time. In addition, each activated standby component takes additional time for re-performing the part of task that was already done by the last active element since the previous successful backup.

To achieve the balance between the time needed for performing the backups and time needed to re-perform the part of the mission task by standby components in the case of failures, the optimal number of backups and backup schedule should be found. In [11] this task has been considered for 1-out-of-N heterogeneous warm standby systems with internal failures characterized by arbitrary time-to-failure distributions. However, besides internal failures, system components are usually exposed to external shocks as well. In order to achieve the

Acronyms and Abbreviations: cdf, cumulative distribution function; GA, genetic algorithm; WS, warm standby; HPP, homogeneous Poisson process; NHPP, non- homogeneous Poisson process; MSP, mission success probability; EMCT, expected mission completion time

[*] Corresponding author at: The Israel Electric Corporation, Haifa, Israel.

E-mail addresses: levitin@iec.co.il (G. Levitin), FinkelM@ufs.ac.za (M. Finkelstein).

http://dx.doi.org/10.1016/j.ress.2017.04.022
Received 29 May 2016; Received in revised form 28 February 2017; Accepted 9 April 2017
Available online 24 April 2017
0951-8320/ © 2017 Elsevier Ltd. All rights reserved.

Nomenclature

N number of system components

H number of backup procedures throughout the mission

M total number of operations to be performed during the mission (excluding backups)

R MSP

D EMCT

$b(x)$, $u(x)$ number of operations needed to save, retrieve data generated after performing fraction x of the entire mission task

B_h, δ_h number of operations, work portions needed for h-th backup procedure

U_h, μ_h number of operations, work portions needed to retrieve the data stored in h-th backup procedure

m number of work portions needed to accomplish the mission when no failures occur

τ minimal recognized time interval

Δ number of operations in each discrete portion of work

$T_{\max}$, $Y_{\max}$ maximum allowed mission time, number of time intervals in the mission

$Y_{\min}$ minimum possible number of time intervals in the mission

$\boldsymbol{\pi}$ backup distribution vector $\boldsymbol{\pi}=(\pi_1,...,\pi_H)$, where π_j is fraction of the entire mission task that should be performed between (j-1)-th and j-th backup procedures

γ_h number of work portions that should be completed between the (h-1)-th and h-th backup actions $\gamma_h=\pi_h M/\Delta$

α_h number of work portions that should be performed between the mission beginning and the end of the h-th backup procedure

$\varphi(i)$ integer number for which $\alpha_{\phi(i)} \le i < \alpha_{\phi(i)+1}$

$s(i)$ index of the component, which should be initiated, given it is still working, after components with indices $s(1)$,... $s(i$-1) have failed

$Q_j(h,Y)$ probability that the number of the last backup that was completed by the sequence of components $s(1)$, $s(2)$, ..., $s(j)$ is h and the number of the time interval when the last component from this sequence failed is Y

G_j, g_j performance (number of operations, work portions per time unit) of j-th component

λ_j replacement time of warm standby component j

d_j life-time deceleration factor for component j

$F_j(t)$ baseline time-to-internal-failure *cdf* for component j

r_j^{WS}, r_j^{OM} shock rates for component j in standby and operation modes

Ω_j initial shock resilience probability of component j

ω_j susceptibility to shocks factor for component j

$P_j^{\text{int}}(t_0, t)$ probability that component j that should be activated at time t_0 does not fail because of internal causes during time t

$P_j^{sh}(t_0, t)$ probability that component j that should be activated at time t_0 survives shocks during time t

$\Theta_j(t)$ shocks survival probability of component j

$\Phi_j(t_0, t)$ overall probability that component j that should be activated at time t_0 fails before time t

$[x]$ integer number closest to x

$\Psi(t)$ discretization function: $\Psi(t)=[t/\tau]$

adequate probabilistic description, the influence of shocks on the performance of systems should be taken into account and combined in a suitable way with inherent (internal) reliability characteristics. When systems are operating in a changing environment, neglecting this influence can lead to errors and misconceptions while analyzing their reliability characteristics. Therefore, in the current paper, we study the joint effect of internal failures and shocks on the performance of warm standby systems with backups. This joint effect in such type of systems has never been studied in literature.

Shock models are widely used in different reliability applications (see [12–16] among others). Traditionally, one distinguishes between two major types of shock models: cumulative shock models (systems fail because of some cumulative effect) and extreme shock models (systems fail due to one single shock). Some generalizations of traditional models have been considered in the literature (see, e.g., references [15–22]).

Most of the shock models in reliability have been developed under the assumption of the Poisson process of shocks (see, e.g., [15–17] and references therein). Poisson shock models are usually mathematically tractable and allow for rather compact expressions for the probabilities of interest. It is worth mentioning that shock models governed by the renewal processes, which have a simple probabilistic nature, are already more cumbersome and approximations and numerical methods should be used for dealing even with the simplest settings [18].

The influence of shocks on backup scheduling was not considered in the literature so far. Furthermore, the important and distinct from conventional shock models feature of our model is that the probability of a component's failure under a shock depends on the previously experienced shocks, which makes it more realistic in practice. For considered practical examples, we show how the shock rates and components' susceptibility to shocks affect the optimal backup schedule and suggest a tool for determining the most effective investment into the shock protection enhancement.

We assume that the considered two types of failure modes are independent, which is a reasonable assumption in practice especially for electronic systems that are characterized by 'sudden failures' as opposed to gradual failures, e.g., in mechanical or electro-mechanical systems. In the latter case, shocks usually influence degradation processes in the system and the assumption of independence is no longer valid.

The remainder of the paper is arranged as follows. Section 2 presents the system model. Section 3 derives the component shock survival probability for NHPP shock process. Section 4 describes the numerical algorithm for MSP and EMCT evaluation and briefly describes the optimization approach. Section 5 presents numerical examples and analysis results. Section 6 concludes the work.

2. The model

The system consists of N non-identical components. The components are exposed to both internal failures and random external shocks that constitute two failure modes for each component. Component j is characterized by a specific time-to-internal failure distribution with cumulative distribution function (*cdf*) $F_j(t)$, shock survival probability function that determines the shocks survival probability $\Theta_j(t)$ and performance (number of operations executed in a time unit) G_j. The computational complexity of the mission (total number of operations to be performed) is M. If no failures or backup procedures happen, then component j needs time M/G_j to complete the entire mission task. At any given time, only one component is in operation whereas the remaining components are in the warm standby (WS) mode.

In many practical systems the functionally equivalent standby components, such as onboard processors, are separated to enhance the system survivability and reduce the influence of common cause destructive factors. In addition, modern computing systems are often specially distributed by their nature. Consider for example local networks consisting of computers with different characteristics that can perform the same computational task. Depending on location, ambient

Download English Version:

https://daneshyari.com/en/article/5019331

Download Persian Version:

https://daneshyari.com/article/5019331

Daneshyari.com