Reliability Engineering and System Safety 121 (2014) 18–25

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Reliability of demand-based phased-mission systems subject to fault level coverage

Rui Peng [a], Qingqing Zhai [b], Liudong Xing [c,*], Jun Yang [b]

[a] Dongling School of Economics and Management, University of Science and Technology Beijing, Beijing, China
[b] School of Reliability and Systems Engineering, Beihang University, Beijing, China
[c] University of Massachusetts, Dartmouth, MA, USA

A R T I C L E I N F O

Article history:
Received 19 March 2013
Received in revised form
21 July 2013
Accepted 27 July 2013
Available online 2 August 2013

Keywords:
Phased-mission system
Reliability evaluation
Multi-valued decision diagram
Mission demand
Fault level coverage

A B S T R A C T

In many real-world applications, a mission may consist of several different tasks or phases that have to be accomplished in sequence. Such systems are referred to as phased-mission systems (PMS). In this paper we consider the demand-based PMS with parallel structure, where the system components function in parallel with different capacities in each phase of the mission and the mission is successful if and only if the total system capacity meets the predetermined mission demand in each phase. The reliability of the demand-based PMS (DB-PMS) with parallel structure subject to fault-level coverage (FLC) is first studied using a multi-valued decision diagram (MDD) based technique. The traditional MDD is modified to accommodate the FLC mechanism and new MDD construction and evaluation procedures are proposed for DB-PMS. To reduce the size of the MDD, an alternative construction procedure applying the branching truncation method and new reduction rules are further proposed. An upwards algorithm is put forward to evaluate the reliability of DB-PMS subject to FLC. The proposed approaches are illustrated through examples.

1. Introduction

In many real-world applications, a mission may consist of several different tasks or phases which have to be accomplished in sequence [1]. For instance, an aircraft flight involves taxi, take-off, ascent, level-flight, descent and landing phases [2]. Such systems are referred to as phased-mission systems (PMS). During each phase, the system has to accomplish a specified task and may suffer different environment or stress conditions. Thus, the system configuration, success criteria, reliability requirements, and component behavior may vary from phase to phase [3–5]. For example, for a twin-engine aircraft, a single engine can ensure the function of the taxi phase whereas both engines are required during the take-off phase. Moreover, the engines usually suffer higher stress and are more likely to fail during the take-off phase than other phases.

Compared with single-phase systems, reliability analysis of PMS is more complex due to the above mentioned system dynamics as well as dependence across the phases (the state of a component at the beginning of a new phase should be identical to its state at the end of the previous phase) [6–8]. Generally, approaches to analyzing PMS can be classified into two classes: analytical methods and simulations [9]. The simulation methods are flexible and can be easily modified to adapt to different situations. However, they are computationally inefficient and require considerable numbers of runs to evaluate the system reliability. The analytical methods can explicitly reflect the system structure and the results might be used in further applications, e.g. optimization of the system design. The analytical methods can be further classified into state-space oriented models [10–12], combinatorial methods [1,3,13,14] and a phase modular solution [15] that combines the former two methods. The state-space oriented models (in particular Markov or Petri nets based methods) could handle both static and dynamic PMS. However they are difficult to be applied to large-scale systems due to the well-known state-space explosion problem. The combinatorial methods exploit the Boolean algebra and decision diagrams to reduce the computational complexity, which makes them applicable to handle larger-scale systems.

This paper focuses on the decision diagram based combinatorial methods. A general "demand-based" phased-mission system (DB-PMS) with parallel structure is considered. Similar to studies on capacitated networks [16,17] and weighted k-out-of-n systems [18–20], it is assumed that the system capacity is the sum of the capacities of the working components. In order to adapt to a wider range of applications, the component capacity is allowed to change from phase to phase. For example, the memory of chips can change when the heat or current changes; the capacity of solar panels can

* Corresponding author. Tel.: +1 508 999 8883; fax: +1 508 999 8489.
E-mail address: lxing@umassd.edu (L. Xing).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.07.013

Acronyms

MDD	multi-valued decision diagram
PMS	phased-mission system
DB-PMS	demand-based PMS
IFC	imperfect fault coverage
FLC	fault level coverage
ELC	element level coverage
CDF	cumulative distribution function
NONSN	number of the non-sink nodes

Notations

M	number of phases
$T_j(1 \le j \le M)$	duration of phase j
$d_j(1 \le j \le M)$	demand of phase j
$\mathbf{D}=(d_1,\ldots,d_M)$	demand vector of the mission
n	number of components in the system
$F_i(t)(1 \le i \le n)$	baseline lifetime distribution of component i
w_{ij}	capacity of component i in phase j
α_{ij}	acceleration factor for component i in phase j
q_{ij}	failure probability of component i in phase j
p_i	probability of component i surviving the mission
$c_i(1 \le i \le n)$	coverage factor for the ith component failure
Nu_{path}	number of failed components in a certain path in the MDD
$\mathbf{Ca}_{path}$	an M-tuple denoting the system capacity in M phases
$\Pr(path)$	occurrence probability of a certain path in the MDD without considering FLC
$R(path)$	occurrence probability of a certain path in the MDD considering FLC

also change according to the environment. The required demand for each phase of the mission is predetermined; the mission succeeds if and only if the system capacity exceeds the predetermined demand in all phases. For example, in a power system, each power plant has a nominal capacity and the total capacity of the working power plants determines the available electricity. The demand for the electricity varies in different periods of a day, and the power system is considered available if the demand is met during the whole day. To ensure the success and high reliability of the mission, redundancy has to be deployed especially for safety-critical or life-critical PMS; the redundancy is consumed with the failure of the component and the entire mission fails if the total capacity of the remaining components cannot meet the system demand in any phase.

For systems designed with redundancy, it may happen that a single uncovered component fault propagates through the system and leads to the overall system failure even when the remaining redundancy is still adequate [21,22]. Consider a scientific computation system where several processors are used simultaneously. If one processor fails without being detected or isolated, it may produce incorrect result which can lead to the corruption of the whole computation. This behavior is known as imperfect fault coverage (IFC) [2,23,24]. The system reliability may not increase unlimitedly with the increase of the system redundancy when IFC is considered [25–27]. According to the fault covering mechanism, two types of IFC models have been studied in the literature: element level coverage (ELC) and fault level coverage (FLC) [28]. In the ELC model, each component is supposed to fail with a specified coverage factor, that is, the failure of the component is covered with a probability c and not covered with probability $1-c$. In the FLC model, the first component failure has a probability c_1 of being covered, the second one has a probability c_2 of being covered, and so on. While most of the existing works on PMS analysis did not consider the IFC effect at all [3,5,8,12,14], some researchers studied the reliability of PMS subject to ELC [1,2,4,6]. FLC has been studied for single-phase systems [28,29], however, to the best of our knowledge, no work has been performed to consider the effect of FLC in the reliability analysis of PMS. In this paper, the DB-PMS subject to FLC is first analyzed and multi-valued decision diagram (MDD) is adapted to evaluate the system reliability.

The rest of the paper is organized as follows. Section 2 gives an overview of the problem to be solved including the system description and model assumptions. Section 3 presents the MDD based approach for the evaluation of the parallel DB-PMS reliability. Section 4 focuses on the complexity issues, including an alternative way to construct the MDD, the MDD reduction procedure, the upwards algorithm, and the computational complexity analysis. Examples are given in Section 5 to illustrate the proposed method. Conclusions are given in the end.

2. Problem statement

The DB-PMS with parallel structure subject to FLC is studied in this paper. The description and assumptions of the system are

(1) The system mission consists of M consecutive non-overlapping phases. The duration of each phase is deterministic.
(2) The system consists of n components which are statistically independent but not necessarily identical. Each component i in phase $j(1 \le j \le M)$ has a nominal capacity $w_{ij}(1 \le i \le n, 1 \le j \le M)$ and the system capacity in phase j is the summation of the capacities of the working components in phase j.
(3) The system demand may vary from phase to phase. To accomplish the mission successfully, the system has to meet the predetermined demand $d_j(1 \le j \le M)$ in each phase j.
(4) For each component, it may suffer different stresses or environment conditions in different phases, which lead to different failure behaviors in different phases. In this paper, the accelerated life time model [30,31] is utilized to model the components' failure behavior under different stresses. Suppose the baseline cumulative distribution function (CDF) of failure time for component i is $F_i(t)$ and the acceleration factor in phases j is α_{ij}, then the CDF of failure time for component i in phase j is $F_{ij}(t)=F_i(\sum_{k=1}^{j-1}\alpha_{ik}T_k+\alpha_{ij}(t-\sum_{k=1}^{j-1}T_k))$, where $\sum_{k=1}^{j-1}T_k < t \le \sum_{k=1}^{j}T_k$. The component failure time can follow arbitrary distributions.
(5) Both the system and its components are non-repairable during the mission. If a component fails during the mission, it will remain in the failed state for the rest of the mission. Moreover, the system state at the beginning of a new phase is identical to its state at the end of the last phase.

3. MDD-based approach

3.1. Traditional MDD

The MDD method provides an efficient and exact way to analyze static multi-state fault trees [32,33]. The traditional MDD