Available online at www.sciencedirect.com
ScienceDirect
Reliability Engineering and System Safety 92 (2007) 351–359
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

Reliability analysis of hierarchical computer-based systems subject to common-cause failures

Liudong Xing[a,*], Leila Meshkat[b], Susan K. Donohue[c]

[a]Electrical and Computer Engineering Department, University of Massachusetts-Dartmouth, 285 Old Westport Road, North Dartmouth, MA 02747, USA
[b]Jet Propulsion Laboratory, California Institute of Technology, MS 301-180, Pasadena, CA 91109, USA
[c]Department of Systems and Information Engineering, University of Virginia, 151 Engineers Way, P.O. Box 400747, Charlottesville, VA 22904, USA

Available online 26 May 2006

Abstract

The results from reliability modeling and analysis are key contributors to design and tuning activities for computer-based systems. Each architecture style, however, poses different challenges for which analytical approaches must be developed or modified. The challenge we address in this paper is the reliability analysis of hierarchical computer-based systems (HS) with common-cause failures (CCF). The dependencies among components introduced by CCF complicate the reliability analysis of HS, especially when components affected by a common cause exist on different hierarchical levels. We propose an efficient decomposition and aggregation (EDA) approach for incorporating CCF into the reliability evaluation of HS. Our approach is to decompose an original HS reliability analysis problem with CCF into a number of reduced reliability problems freed from the CCF concerns. The approach is represented in a dynamic fault tree by a proposed CCF gate modeled after the functional dependency gate. We present the basics of the EDA approach by working through a hypothetical analysis of a HS subject to CCF and show how it can be extended to an analysis of a hierarchical phased-mission system subject to different CCF depending on mission phases.

Keywords: Common-cause failures; Dynamic fault trees; Hierarchical systems; Reliability analysis

1. Introduction

A preferred architecture for large and complex computer systems is a hierarchical system (HS) model. The HS model is characterized by multiple layers of modules and components. When performing reliability analysis of a HS, we must consider component failures both on the same level and on different layers. The analysis becomes even more complicated when considering components subject to common-cause failures (CCF).

CCF are multiple dependent component failures within a system that are a direct result of a shared root cause such as sabotage, flood, earthquake, power outage, or human errors. It has been shown by many reliability studies that CCF tend to increase a system's joint failure probabilities and thus contribute significantly to the overall unreliability of systems subject to CCF [1]. Therefore, failure to consider CCF in the reliability analysis of such systems leads to overestimated system reliability measures. Considerable research efforts have been expended in the study of CCF for reliability modeling and analysis of computer-based systems; see, for example, [1–16]. However, the existing CCF models are mainly applicable to non-HS. They also have various limitations, such as being concerned with a specific system structure (see, for example, [4,11,12,16]); applicable only to systems with exponential time-to-failure distributions (see, for example, [3,5,8]); being subject to combinatorial explosion as the redundancy level of the system increases (see, for example, [6,7]); limiting analysis to components belonging to at most a single common-cause group (CCG) [1,13]; having a single common cause (CC) that affects all components of a system (see, for example, [2,11]); or defining CC as being statistically independent or mutually exclusive (see, for example, [14]).

*Corresponding author. Fax: +1 508 999 8489.
E-mail addresses: lxing@umassd.edu (L. Xing), Leila.Meshkat@jpl.nasa.gov (L. Meshkat), SusanD@virginia.edu (S.K. Donohue).

0951-8320/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2006.04.010

We seek to address some of these limitations in developing a model for the reliability analysis of HS subject to CCF by allowing for multiple CC that can affect different subsets of system components, and which can occur statistically dependently. Our recent work [17] extended the current CCF models by breaking these restrictions in the reliability analysis of computer network systems. In this paper, we utilize the generalized CCF model of [17] and incorporate this CCF model into dynamic fault trees (DFT) through the use of a new dynamic gate. (For background on DFT see, for example, [18–20].) In addition, we propose an efficient decomposition and aggregation (EDA) approach for incorporating CCF into the reliability analysis of HS.

The remainder of the paper is organized as follows: Section 2 presents an example of a HS subject to CCF to help make tangible the type of system for which this approach is meant as well as the analytical challenge we address in this paper. Section 3 presents the reliability modeling of HS using DFT. Section 4 presents an example of the EDA approach using a hypothetical HS subject to CCF. The extension of this approach to the analysis of a hierarchical phased-mission system subject to different CCF depending on mission phases is presented in Section 5. In the last section, we present our conclusions as well as directions for future work.

The following acronyms are used in the paper[1]:

ACS	attitude control system
CC	common cause
CCE	common-cause event
CCF	common-cause failure
CCG	common-cause group
CDS	command and data handling system
CM	computing module
CPUC	CPU chip
DFT	dynamic fault tree
EDA	efficient decomposition and aggregation
FDEP	functional dependency
HGA	high-gain antenna
HS	hierarchical computer-based system
IC	interface chip
MC	memory chip
MM	memory module
MOI	Mars orbit insertion
PTC	port chip
SA	solar array
s-	implies statistical(ly)

2. An illustrative example

To illustrate the application and advantages of the proposed approach, we consider a hierarchical computer system adapted from [21]. Fig. 1 is an illustration of the

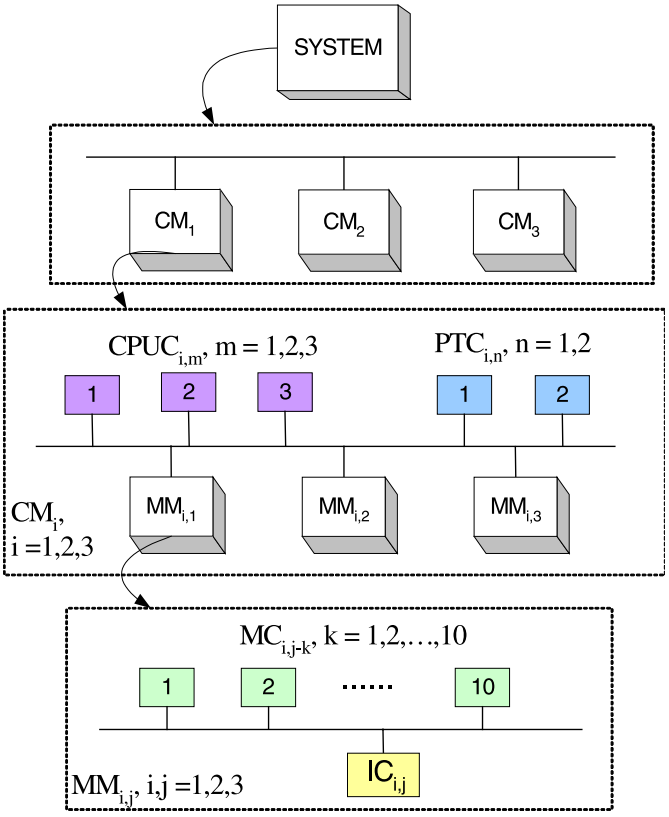

Fig. 1. An example HS.

system's three-level architecture. The top or system layer is composed of three computing modules (CM_i) residing in three different sites. Each computing module CM_i includes three memory modules ($MM_{i,j}$), three identical CPU chips ($CPUC_{i,m}$), and two identical port chips ($PTC_{i,n}$). This middle or second layer is called the module layer. Each $MM_{i,j}$ is made up of 10 identical memory chips ($MC_{i,j-k}$) and one interface chip ($IC_{i,j}$). This bottom layer is called the component layer. The HS is decomposed by resolving the system layer into modules, and then resolving each successive module layer into components. The following conditions must hold for the example system to be operational:

- at least eight of MC and one IC have to be unfailed for the MM to be operational,
- at least two MM, two CPUC and one PTC must be operational to make each CM operational,
- at least two CM must be operational for the whole system to be operational.

In order to demonstrate the effects of CCF on the reliability analysis of this example HS, we propose the following hypothetical scenario about CCF: the system is subject to CCF from two independent CC, earthquakes (denoted by CC_1) and power outages (denoted by CC_2). An earthquake of sufficient intensity would cause $MC_{1,3-8}$, $MC_{1,3-9}$, $MC_{1,3-10}$, $PTC_{1,2}$, $CPUC_{2,1}$, $MC_{2,1-1}$, $MC_{2,1-2}$, $MC_{2,1-3}$, and $MC_{2,1-4}$ to fail; a power failure would cause

[1]The singular and plural of an acronym are the same.