Reliability Engineering and System Safety 164 (2017) 24–33

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Competing failure analysis in phased-mission systems with multiple functional dependence groups

Chaonan Wang[a], Liudong Xing[b,*], Rui Peng[c], Zhusheng Pan[d]

[a] College of Information Science and Technology, Jinan University, Guangzhou, Guangdong 510632, China
[b] Department of Electrical and Computer Engineering, University of Massachusetts, Dartmouth, MA 02747, USA
[c] Donlinks School of Economics and Management, University of Science and Technology Beijing, Beijing 100083, China
[d] Department of Computer Science and Technology, Zhejiang Normal University, Jinhua 321004, China

ARTICLE INFO

Keywords:
Competing failures
Failure isolation
Functional dependence
Markov chain
Phased-mission system
Propagated failure
Reliability analysis

ABSTRACT

A phased-mission system (PMS) involves multiple, consecutive, non-overlapping phases of operation. The system structure function and component failure behavior in a PMS can change from phase to phase, posing big challenges to the system reliability analysis. Further complicating the problem is the functional dependence (FDEP) behavior where the failure of certain component(s) causes other component(s) to become unusable or inaccessible or isolated. Previous studies have shown that FDEP can cause competitions between failure propagation and failure isolation in the time domain. While such competing failure effects have been well addressed in single-phase systems, only little work has focused on PMSs with a restrictive assumption that a single FDEP group exists in one phase of the mission. Many practical systems (e.g., computer systems and networks), however may involve multiple FDEP groups during the mission. Moreover, different FDEP groups can be dependent due to sharing some common components; they may appear in a single phase or multiple phases. This paper makes new contributions by modeling and analyzing reliability of PMSs subject to multiple FDEP groups through a Markov chain-based methodology. Propagated failures with both global and selective effects are considered. Four case studies are presented to demonstrate application of the proposed method.

1. Introduction

According to different effects imposed on other system components, two types of component failures can be identified: local failure (LF) and propagated failure (PF). An LF only causes an outage to the component itself; has no effect on other system components. A PF not only fails the component itself but also causes failures of other system components [1]. According to the scope of affected components, a PF can be further classified into two types: PF with global effect (PFGE) that propagates through the entire system and thus leads to the overall system failure, and PF with selective effect (PFSE) that only affects a subset of system components [2]. Refer to Section 4.4 for a detailed example of PFGE and PFSE.

However, it is not always the case that a PF can affect other system components; the global or selective propagation effect of a PF could be isolated in systems with functional dependence (FDEP) behavior, where the failure of certain component(s) (referred to as a trigger) causes other system component(s) (each referred to as a dependent component) to become unusable or inaccessible [3,4]. In particular, if the trigger component fails before the occurrence of any PF from dependent components, the propagation effects of the PF are isolated. In other words, the failure isolation effect takes place. However, if any PF from a dependent component happens before the trigger fails, the failure propagation effect takes place affecting other system components. Such competition between the failure propagation and failure isolation events in the time domain is referred to as competing failures in this work [5].

Consider an example of a local area network (LAN) where computers access the internet through routers. Since the router failure makes the connected computers inaccessible, each router is considered as a trigger component and the corresponding connected computers are components that are functionally dependent on the router. A PF (e.g. virus) occurring in a connected computer would propagate to other LANs through the router and thus crash the entire network. However, if the router has already failed before the PF happens to any connected computer (e.g., due to access to infected local files on a flash

Abbreviation: FDEP, Functional dependence; LAN, Local area network; LF, Local failure; PF, Propagated failure; PFGE, Propagated failure with global effect; PFSE, Propagated failure with selective effect; PMS, Phased-mission system

* Corresponding author.
E-mail addresses: c_wang@jnu.edu.cn (C. Wang), lxing@umassd.edu (L. Xing), pengrui1988@ustb.edu.cn (R. Peng), pan@zjnu.cn (Z. Pan).

http://dx.doi.org/10.1016/j.ress.2017.02.006
Received 9 October 2015; Received in revised form 23 February 2017; Accepted 26 February 2017
Available online 28 February 2017
0951-8320/

drive), the failure isolation effect occurs; computers of other LANs in the network are not affected by this PF.

Note that the type of competing failures considered in this work is different from those addressed in literature [6–10], which are mainly concerned with multiple failure or degradation processes. The competing failure addressed in this work is concerned with competition in the time domain between the failure isolation and failure propagation effects in systems with the FDEP behavior.

Considerable research efforts have been expended in the reliability analysis of single-phase systems subject to the considered competing failures [5,11–15]. However, many real-world systems, such as aerospace, nuclear power systems, air borne weapon systems and distributed computing systems, are phased-mission systems (PMSs) where the system mission involves several different tasks that have to be accomplished in consecutive phases [16–22]. Because a PMS may be subject to different stresses, environmental conditions and reliability requirements during different phases of the mission, system configuration, success criteria, and component behavior may vary from phase to phase. Consider the above mentioned computer network example where computers are working together to complete a computational task involving several sequential sub-tasks or phases. In some phases, only computers within an LAN are needed to complete the sub-tasks, that is, no FDEP behaviors are involved in these phases; whereas in other phases, external data or files are needed from outside the LAN, which can be accessible from the network through routers, and thus the FDEP behavior between the relevant computers and corresponding routers exist in these phases. The competition between virus propagation and router failures has to be addressed when analyzing reliability of such PMSs. Moreover, statistical dependencies exist across phases for a given component (the state of a component at the beginning of a new phase has to be identical to its state at the end of the previous phase). The dynamic behaviors in both component and system levels as well as the statistical dependencies bring unique challenges to competing failure analysis of PMSs [23].

Ref. [24] has recently studied effects of competing failures in the reliability analysis of PMSs. But the model of [24] is limited, assuming there is only a single FDEP group appearing in only one phase of the mission and any PF has the global effect (i.e., PFGE). In this work, we make new contributions by modeling PMSs with multiple FDEP groups that may appear in a single phase or multiple phases. Moreover, different FDEP groups are not necessarily independent; they may share the same trigger event or the same dependent component. For the computer network example, different groups of computers within the same LAN may be involved in different phases of the mission, which access internet through the same router. The common router makes the multiple FDEP groups dependent. Both PFGE and PFSE are addressed through case studies in this work.

The remainder of the paper is organized as follows. Section 2 introduces the system model studied. Section 3 presents a Markov-based method for reliability analysis of PMS subject to competing failures involving multiple independent or dependent FDEP groups. Section 4 presents four case studies. Conclusions and future work are given in Section 5.

2. System model

This paper considers non-repairable PMSs, in which both the system and its components are not maintained during the mission. All the system components are operational at the beginning of the mission. The phase durations are fixed and independent of the system state.

The LF and PF of any component are s-independent, that is, a component that has failed locally can still suffer PFs. This can happen in cases, for example, sensor nodes with both sensing and transmission functions. If LF is a sensing failure without damaging the transmission function, the node can still experience PF from jamming attacks [25].

Occurrence of a trigger component failure only makes the dependent components within the same FDEP group inaccessible in one phase; the dependent components are still functioning and can be used in other phases if they are accessed directly by the system function without involving the trigger component in these phases. Both PFGE and PFSE from the dependent component can be isolated by the failure of trigger component. An isolated PF including PFGE and PFSE only affects the component itself, i.e., causing LF to the component. The isolated PF in a previous phase can still propagate to other components in a later phase that does not possess the related FDEP group. For example, in the computer network example, a computer needs to access internet through a router to perform the function in one phase, while in a later phase only local function within the LAN is required. The PF (e.g., virus) isolated in the earlier phase due to failure of the router can still propagate to other components (e.g., computers within the same LAN) causing failure of the later phase hence failure of the entire mission.

Fault trees are used to represent the failure behavior of the system modeled in this work. In particular, a fault tree model consists of a top event (system failure) linked to some basic events(component failures) by logical gates, which express the interrelationships between the system failure and component failures [26]. The FDEP behavior considered in this work is modeled by an FDEP gate, which has a single trigger event and one or more dependent components. The occurrence of the trigger event would cause all the dependent components to become inaccessible or unusable [27]. Case studies in Section 4 illustrate the use of FDEP gates in the fault tree modeling.

3. Proposed Markov-based method

Markov chains have been widely applied to analyze reliability of both static and dynamic systems due to its flexibility in modeling various complicated behavior [28,29]. A Markov chain model is constructed based on system states; each state can be represented by a combination of all functioning and failed system components describing the system behavior at any given instant of time. The states are linked by state transitions; a transition between two different states is generally triggered or caused by the failure of a component. In the context of system reliability analysis, the construction of a Markov model starts from an initial state where all the system components are in good states. As the components fail one by one, the system goes from one state to another state until some absorbing state is reached, which typically represents the entire system failure. The exponential time-to-failure distribution is assumed for system components, i.e., failure rates of all the system components are constant.

A Markov-based method was proposed in [30] to analyze reliability of a PMS. But effects of FDEP behavior and competing failures have not been addressed at all in [30]. In this work we extend the Markov method of [30] by considering the competing failure effects in the reliability analysis of PMSs with multiple independent or dependent FDEP groups through new state definitions and special treatments in the phase mapping process. Both PFGE and PFSE are modeled. The extended Markov method can be summarized as a three-step procedure, detailed in the following subsections.

3.1. Step 1: Develop a separate Markov chain for each phase

Since LF, PFGE, and PFSE are assumed to be independent, each failure event can be modeled as an independent event. In the traditional Markov model, there is only one event for each component in each state representing the function or failure of the component. In the extended model, there are up to three events for each component in each state representing occurrence or non-occurrence of LF, PFGE, and PFSE of the components, respectively. The initial state in the proposed Markov chain is the state where all the component failure events do not