Reliability Engineering and System Safety 180 (2018) 1–12

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Reliability analysis of a cold-standby system considering the development stages and accumulations of failure mechanisms

Ying Chen[a,b,*], Ze Wang[a], YingYi Li[a], Rui Kang[a], Ali Mosleh[b]

[a] Science and Technology on Reliability and Environmental Engineering Laboratory, School of Reliability and System Engineering, Beihang University, Beijing 100191, PR China

[b] B. John Garrick Institute for the Risk Sciences, Material Science Engineering, University of California, Los Angeles, United States

ARTICLE INFO

Keywords:
Cold-standby system
Development stage
Failure mechanism accumulation
E-type FMs

ABSTRACT

In this paper we classify failure mechanisms (FMs) into three types based on the triggering loads, including environmental load-triggered (E-type), operating load-triggered (O-type), and combined load-triggered (C-type) FMs. In a cold-standby component, E-type FMs develop when the component does not operate and may develop with different speeds due to changes in the environmental conditions at different stages. O-type FMs are triggered by operational loads. Environmental loads and operating loads are necessary for triggering C-type FMs. Previous studies have often assumed that cold-standby components are not subject to failures or degradation in the standby stage. However, E-type FMs can develop in cold-standby components at the standby stage and contribute to the degradation of the components. In this paper, we propose a hierarchical method based on the sequential binary decision diagram (SBDD) to analyze the reliability of a non-repairable cold-standby system while considering the correlation and development of FMs. In the case study, a reliability analysis is conducted for an example power supply subsystem equipped with an electronic control device, which comprises one primary unit and one cold-standby unit. The results show that the reliability of the cold-standby system is quite different when considering the development of E-type FMs in the cold-standby unit. In addition, the lifetime of the system will decrease when E-type FMs are considered in the simulation.

1. Introduction

In a cold-standby system, there are some online or operating modules and one or more standby modules that remain in a non-operating state and do not consume any power until the failed online component requires a replacement. Due to the structural redundancy, the cold-standby system has many particularities; in other words, it has many dependencies. Considerable efforts have been devoted to the modeling and analysis of a cold-standby system's reliability due to several problems that include standby element sequencing problems (SESP) [1,2], perfect or imperfect switching [3,4], imperfect backup [5], and failure propagation [6] with the aim of supporting optimal decisions making for the system's standby policy.

The cold-standby redundancy creates a sequential dependence between the online components and the standby components [7]. In particular, when the switch is perfect, a standby component can begin to operate and then fail only after the online component has failed. Thus, the occurrence of some failure events is frequently based on the occurrence of a trigger event, which usually refers to the failure event of the online component. Extensive studies have been carried out to analyze the reliability of cold-standby systems with sequential dependence and different modeling methods have been proposed including reliability block diagrams [8–10], fault tree analysis (FTA) [11,12], Markov-based methods [13–15], and binary-decision diagrams [7,16,17].

A traditional binary decision diagram (BDD) method can be used for analyzing static fault trees that represent the system failure in terms of logic AND/OR combinations of component failures [18]. A sequential binary decision diagram (SBDD) proposed by Xing et al. [7], an extended version of a traditional BDD, can model a dependent behavior and the failure sequence of the components, such as the pAND behavior or sequence dependence. Xing et al. [18] also explained in detail how to analyze a cold-standby system's reliability with the SBDD method and pointed out that the SBDD method has no limitation regarding the types of time-to-failure distributions for the system components. It does not need a priori knowledge of the minimal cut sets/sequences or an

---

* Corresponding author at: Science and Technology on Reliability and Environmental Engineering Laboratory, School of Reliability and System Engineering, Beihang University, Beijing 100191, PR China.

E-mail address: cheny@buaa.edu.cn (Y. Chen).

https://doi.org/10.1016/j.ress.2018.06.022
Received 12 September 2017; Received in revised form 11 June 2018; Accepted 27 June 2018

evaluation of an inclusion/exclusion (I/E) expression.

The standby components in cold-standby systems are not exposed to operating stresses, fail at low failure rates before working, and their lifetime data is time- and money-consuming to collect, which are the main reasons why it is often assumed that they are not subject to failures in the standby state [6,17,19]. Coit [20] studied the optimal design for non-repairable series-parallel systems with cold-standby redundancy. It is believed that the probability of failure for cold-standby components is very low and assumed to be zero until the component is required to operate as a substitute for a failed component. Levitin et al. [21] also assumed that the development speeds for failures in cold-standby components were zero during the standby state because they were shielded from the working stresses.

Most recent studies on cold-standby systems have focused on the redundancy allocation problem (RAP). Attar et al. proposed a simulation-based optimization method to handle a multi-objective joint availability-RAP and solved the optimization model by using two well-known multi-objective evolutionary computation algorithms, i.e., the non-dominated sorting genetic and strength Pareto evolutionary algorithms [22]. Levitin et al. first proposed a new numerical approach to evaluate the reliability and expected mission completion time for 1-out-of-N:G unrepairable cold-standby systems subject to imperfect backups [5]. Based on the proposed evaluation algorithm, the optimal backup frequency and initiation sequencing problem is formulated and solved for providing solutions that can maximize mission reliability or minimize the expected mission completion time depending on the design requirements. Kim considered the imperfect switches and optimal order into RAP with mixed components [23]. Under degradation performance, Nezakati and Razmkhah studied the reliability of k-out-of-n cold-standby systems consisting of n active components and one standby component [24]. A Gamma process is assumed for the degradation of the active and standby components and the effect of varying the shape and scale parameters on the system reliability is investigated. However, the degradation of the cold-standby component prior to the operation was not considered in their study. Several authors [25] have clearly stated the assumption that the cold-standby component did not degrade or fail prior to the operation, whereas in most studies, the default condition was assumed.

A special case of a cold-standby system is the standby safety equipment (SSE) [26,27] used in nuclear plants to prevent core damage and radiation leaks. This kind of standby system is used to terminate the nuclear physical reaction in a safe manner; this system differs from the traditional system in that the cold-standby component covers the failed active component and completes the function. Because of the temporary task of the SSE, related studies have focused on the availability during the failure of the main system. The degradation caused by the demand-related stress of the SSE prior to the operation was considered but other kinds of degradation, such as the parameter degradation and the exact failure mechanisms were not investigated.

Failure mechanisms (FMs) describe the causes or actions that occur in a physical or chemical domain during a failure. In our previous studies [28], FM dependencies were categorized as competition, trigger, acceleration, inhibition, and accumulation. However, no studies have been carried out on the FM dependencies and development in a cold-standby system and the degradation behavior of FMs in a standby state. In this paper, the dynamic behavior of the evolution of the FMs in a cold-standby system will be evaluated, taking into account the dependencies between the standby-state and the online-state.

The contributions of this paper are as follows: firstly, the concept of FMs is clarified and summarized and FMs are categorized into three types based on the triggered stress, which facilitates the determination of the FMs leading to the failure of components during a specific stress period. Secondly, different degrees of damages caused to the component are evaluated for those FMs that persisted throughout different stress periods. To describe the dependence between the damages, a model that considers multiple-stage developments and accumulation effects of FMs is proposed. Thirdly, an extended SBDD method for modeling a cold-standby system's reliability and describing the development of the FM is developed.

Based on the above description, the following assumptions are required:

(1) The system consists of two units. To begin with, one unit operates normally and the other one is in the cold-standby state. Upon the failure of the online unit, a perfect switch is used to switch the cold-standby unit into operation immediately.
(2) The FMs in the cold-standby system are categorized and distinguished based on different types of loads exerted on the corresponding components. It is considered that the environmental load-triggered FM of the system in the cold-standby stage is subject to a degradation effect.
(3) The system components are non-repairable; i.e., none of the mechanisms, elements, or products can recover from a failure or an unusable condition.
(4) The development speed of an FM under a constant stress level is invariable.
(5) Only two kinds of FM dependence are considered in this paper; they include accumulation and competition.

The remainder of this paper is organized as follows. Section 2 presents the evolution of the FMs in a cold-standby stage and an online stage. Section 3 proposes an extended SBDD method to model the FM relationships between these two stages. A flow diagram of this method, the general SBDD-based models and a flow diagram of the evaluation of the SBDD model are given in this section. Section 4 is a case study of an electronic control system. The differences in the reliability evolution speed for the different types of FMs in the case system and the component are evaluated. Finally, the conclusions of this paper and future planned studies are presented in Section 5.

2. Development of FMs in cold-standby systems

2.1. Different types of FMs

An FM is the physical, chemical, or other underlying cause of a failure of a component in a system. The development speeds of FMs change for different types of loads and environmental conditions.

Regardless of whether the component is an online or cold-standby component, FMs are affected by stress, material properties, and local structures. The factor that influences the development speed of an FM at a failure site is stress, which can be classified as working stress and environmental stress. These two types of stress may also influence each other. For example, due to a working stress such as electricity, a component may heat up, resulting in the rise of temperature of the surrounding environment. Considering the type of the trigger stress and its corresponding influence on FMs, this paper proposes to categorize FMs into three types, including FMs triggered by an operating load (operating load-triggered FMs), FMs triggered by environmental stress (environmental load-triggered FMs), and FMs triggered by a combination of both (combined load-triggered FMs), which are illustrated in Fig. 1.

(1) Environmental load-triggered FMs (E-type FMs)
As long as the trigger environmental stress exists, these types of FMs will develop at a certain speed related to the stress level; these are called E-type FMs. For example, some FMs develop under normal temperatures and result in the change in the material properties. Creep is a type of FM that is affected only by temperature. Under higher temperatures, it develops faster, while at lower temperatures, it develops at a very low speed. Thermal fatigue of the interconnection in electronic devices is another E-type FM. It occurs only if the device is maintained in a constant environment; otherwise, the temperature difference between day and night will trigger this type