Available online at www.sciencedirect.com

ScienceDirect

Reliability Engineering and System Safety 92 (2007) 144–155

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Analysis of on-line maintenance strategies for *k*-out-of-*n* standby safety systems

Lixuan Lu[a], Jin Jiang[b,*]

[a]School of Energy Systems and Nuclear Science, Faculty of Engineering and Applied Science, University of Ontario Institute of Technology, Oshawa, Ont., Canada L1H 7K4

[b]Department of Electrical and Computer Engineering, The University of Western Ontario, London, Ont., Canada N6A 5B9

Received 3 August 2005; received in revised form 4 October 2005; accepted 7 November 2005
Available online 19 January 2006

Abstract

The objective of this paper is to compare the performance of three on-line test and maintenance strategies (corrective maintenance, preventive maintenance and predictive maintenance) for standby *k*-out-of-*n* safety systems. Each channel of the *k*-out-of-*n* system is modelled by an age-dependent unavailability model to reflect the effect of maintenance on the aging process. The system unavailability, the probability of spurious operation and the overall cost under the above maintenance strategies are analyzed and compared to obtain the optimal maintenance strategy. Sensitivity analyses are performed to reveal the effect of different model parameters on the system performance. A standby safety system in Canadian Deuterium–Uranium (CANDU) Nuclear Power Plants (NPPs), the Shutdown System Number One (SDS1), is used to illustrate the proposed analysis and the procedure. It is concluded that maintenance should neither be performed too frequently nor too rarely. When the system deteriorates very slowly, the corrective maintenance is more preferable than the preventive and predictive maintenance. When the failure rate of the system is high, the preventive maintenance results in the best system performance.

Keywords: Unavailability; Safety; Spurious operation; Corrective maintenance; Preventive maintenance; Predictive maintenance; Dual-failure modes; Canadian Deuterium–Uranium (CANDU) Nuclear Power Plants

1. Introduction

For safety-critical control systems, such as those in Nuclear Power Plants (NPPs), chemical processes, and aerospace systems, it is important to have standby safety (shutdown) systems in addition to on-line regulation systems. During severe conditions, the standby system can take actions automatically to lead the system to a safe state and to prevent catastrophic consequences. However, standby safety systems may fail to operate on demand as well because of latent failures. Therefore, it is important to reveal and fix these problems through test and maintenance.

Normally, the test and maintenance are carried out following the recommendations from the system manufacturers, and they generally tend to be conservative. In safety-critical applications, the maintenance interval is often dictated by regulatory bodies. For example, in the field of NPPs, NRC[1] (US) and CNSC[2] (Canada) impose strict rules on the frequency of maintenance to keep the unreliability below a certain level. In general, more frequent tests can increase the likelihood of disclosing a failure. However, it may also deteriorate the system faster, incur unnecessary expenditure on resources, and can lead to a higher rate of spurious operations. Therefore, a reasonable and effective test and maintenance strategy is of considerable importance for standby safety systems.

*Corresponding author. Tel.: +1 519 661 2111x88320; fax: +1 519 850 2436.
E-mail addresses: lixuan.lu@uoit.ca (L. Lu), jjiang@eng.uwo.ca (J. Jiang).

0951-8320/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2005.11.012

[1]Nuclear Regulatory Commission.
[2]Canadian Nuclear Safety Commission.

The k-out-of-n systems are widely used in standby safety systems [1,2]. Basically, a k-out-of-n system consists of n parallel channels, as long as k of them are operational, the system will be able to perform its intended function. Each channel might have two failure modes: (1) channel unavailability, and (2) spurious operation. Channel unavailability means that the channel fails to function when there is a request. Spurious operation means that the channel takes action when there is actually no need. According to the logic of a k-out-of-n system, if more than n–k channels are unavailable, the k-out-of-n system will become unavailable. If k or more channels function spuriously, the system will function spuriously.

In this paper, a general procedure to determine the optimal test and maintenance strategy for a k-out-of-n system has been proposed. The ultimate goal is to determine the relationships among the unavailability, and the probability of spurious operation, and the overall cost of maintenance. In order to achieve this goal, the analysis of the unavailability, the probability of spurious operation and the overall cost for a k-out-of-n system under different test and maintenance strategies have to be performed. It is assumed that each channel in a k-out-of-n system can be modelled in terms of an age-dependent model as described in [3]. This model evaluates, in a quantitative manner, how test and maintenance affects the system performance and the overall cost. The model explicitly considers how maintenance affects the life of a component. Reliability parameters such as demand-failure probability, standby failure rate and aging rate have all been considered. Component unavailability as a function of test and maintenance interval is obtained analytically. The analysis has revealed the relations among system parameters and provided insights into system characteristics [4]. Based on the analysis results, the optimal test and maintenance strategy can be determined.

This paper is organized as follows: in Section 2, three test and maintenance strategies are introduced. Then, the age-dependent model for a single component is presented in Section 3. Based on this model, the system unavailability, the probability of spurious operation and the overall cost for a k-out-of-n system under the three test and maintenance strategies are analyzed in Section 4. Subsequently, the general procedure of maintenance decision making is presented. Following this, in Section 5, a standby safety system in Canadian Deuterium–Uranium (CANDU) NPPs [5,6], the Shutdown System Number One (SDS1), is used to illustrate how the proposed process of maintenance strategy is determined. Finally, in Section 6, sensitivity analyses are performed on several parameters to assess their effects on the optimal maintenance strategy.

2. Test and maintenance strategies

Test and maintenance methodology has evolved over the last several decades. In the beginning, maintenance is often performed whenever there is a component failure (corrective maintenance). Gradually, the plant availability, plant safety, equipment life, product quality, and overall operation cost are all incorporated into the maintenance planning process. Time-based preventive maintenance and condition-based predictive maintenance have been developed subsequently [7,8]. Fig. 1 illustrates the difference between corrective and preventive maintenance.

Three test and maintenance strategies have been considered for k-out-of-n systems in this paper:

Strategy 1—*Corrective maintenance*: Perform test and maintenance on each channel at pre-determined interval T. Repair the channel if a failure is detected. If the channel has not failed, return it back to service.

Strategy 2—*Time-based preventive maintenance*: Perform periodic preventive maintenance on each channel at each test and maintenance interval T. Then return the channel back to service.

Strategy 3—*Condition-based predictive maintenance*: Perform periodic inspection on each channel. The predictive maintenance evaluates the condition of the channel. If the degradation limit has been reached, a condition-based preventive maintenance will be carried out. Then, return the channel back to service.

It is assumed that these test and maintenance strategies are all carried out on-line, which means that the channel under test and maintenance has to be manually set in a tripped condition. The k-out-of-n system thus becomes a $(k-1)$-out-of-$(n-1)$ system during test and maintenance.

3. Age-dependent unavailability model

There exist several unavailability models in the literature [9,10] that can be used to quantify the unavailability of a component. A general model from [3] is adopted in the current work because it allows one to take into account of the effect of test and maintenance. This model was derived

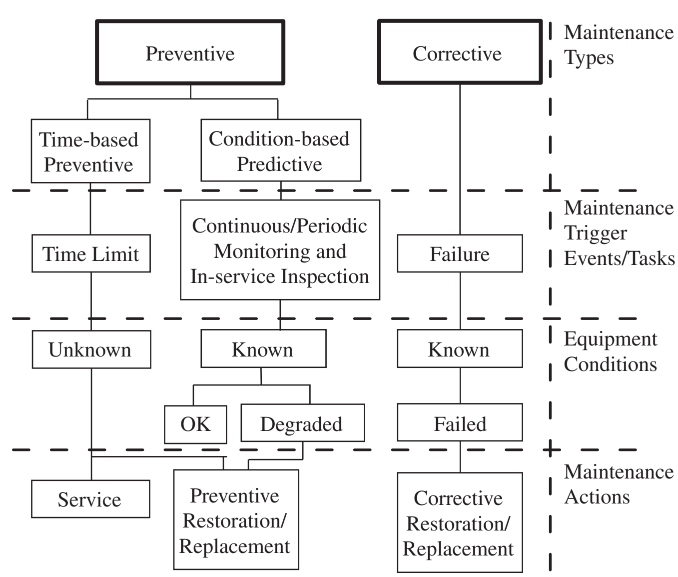

Fig. 1. Corrective maintenance vs. preventive maintenance.