Reliability Engineering and System Safety 126 (2014) 65–71

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Optimal staggered testing strategies for heterogeneously redundant safety systems

Yiliu Liu

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

ARTICLE INFO

Article history:
Received 25 July 2013
Received in revised form
13 January 2014
Accepted 16 January 2014
Available online 24 January 2014

Keywords:
Safety instrumented system
Staggered testing
Optimal staggered time

ABSTRACT

Staggered testings are effective in improving the availability of redundant safety instrumented systems, and the optimal staggered time of testings for a system of two homogeneous components with the same testing interval has been proved as half of the testing interval. In this study, the impact of staggered time on the effectiveness of staggered testings for heterogeneous systems is examined, and the optimal staggered time is found still as half of the testing interval for systems with components different in failure rates but same in testing interval. In terms of systems with two components different in testing intervals, the optimal testing time is revealed as half of the shorter interval. Case studies of safety instrument systems present the same results. And then, Monte Carlo simulation based on Petri net models for these systems also confirms the conclusions obtained by numerical formulas. Such findings are helpful to effectively apply staggered testing strategies in more redundant systems.

1. Introduction

Redundancy is always introduced to improve the availability of safety instrumented systems (SISs). The redundant SISs have a parallel structure including two or more components. In the case of a SIS consist of two components, the system can be regarded as a 1-out-of-2 (1oo2) one if it is still able to perform the required safety instrumented function when only one of the components is functioning.

The unavailability of such systems is highly related with periodically proof testings [21,14,17,20], which can be classified into several types: simultaneous, sequential and staggered testings [2,14]. The so-called staggered testings refer to the proof testings which are performed on the two components at different times [19,12]. As shown in Fig. 1, we have two independent components in a 1oo2 SIS, and the probability of failure on demand (PFD) at time t is used to illustrate the instantaneous unavailability. Both PFDs of the two components and the system are dependent on time (the short dashed line denotes the changing of PFD of component 1 with time, the long dashed line is for component 2, while the solid line is for the system). Component 1 is tested at times $0, \tau, 2\tau\ldots$, while component 2 is tested at $t_0, \tau+t_0, 2\tau+t_0\ldots$. In this paper, τ is the testing interval, and the delay (t_0) from the test of component 1 to the test of component 2 is called staggered time. It should be noted that the time 0 here is not the time when the SIS is put into operation, but the start point that we observe the SIS while one testing is just finished. After each test, faults in a component will be removed, and the instantaneous PFD will be reduced to 0. The instantaneous PFD of the system is the multiplicity of those of the two components.

Usually, a 1oo2 SIS has two homogeneous components, meaning that they are the same in reliability and are tested with the same intervals. Previous studies [3] have verified that the average unavailability of such a system (PFD_{avg}) during a testing interval (e.g., from τ to 2τ) is lowest when the staggered time is half of τ. Given that the failure rate of the components is λ, PFD_{avg} of the SIS by staggered testings with the staggered time of $\tau/2$ has been calculated as $5(\lambda\tau)^2/24$, compared with $(\lambda\tau)^2/3$ by sequential (components are tested immediately one after another) or simultaneous (components are tested at the same time) testings with the same intervals [2,10].

However, two parallel operated components in a SIS are not necessarily the same in reliability, and they also have possibilities to be operated in different environments to perform the same safety function. For example, consider a pipeline with two shutdown valves installed physically in series. They are open during the normal operation, and the closure of one of them can stop the flow in the pipeline so as to act as a safety barrier. As a result, the two valves are parallel in function and consist of an 1oo2 system. But the upstream valve perhaps has more trips, and the downstream valve is only demanded when the former one is in fault. If the trip has the possibility to reduce the reliability of a valve, e.g., through aging the spring, wearing the seat, etc., the upstream valve may have a higher failure rate. In addition, the testing intervals of two components can be different. In this case, the testing interval for the downstream can be longer on the sake of

E-mail address: yiliu.liu@ntnu.no

0951-8320/$ - see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2014.01.013

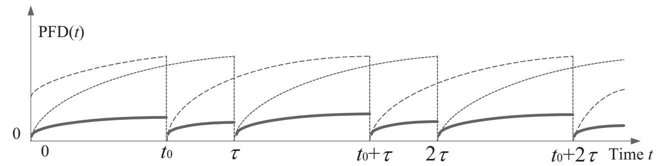

Fig. 1. PFD(t) of a SIS of two homogeneous components (the solid curve denotes PFD(t) of the whole system). It is plotted on the basis of the figure at page 435 of [9].

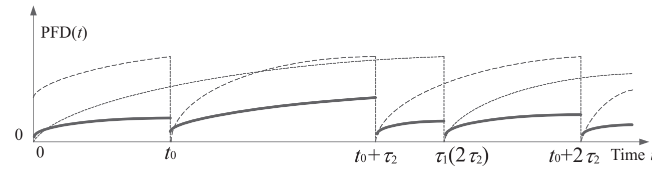

Fig. 2. PFD of a SIS of two components (same in failure rates but different in testing intervals).

testing cost, since it can be assumed to have a lower failure rate than the upstream one.

Not much attention has been paid on availability of these heterogeneous SISs with different components, and it is natural to suspect whether the optimal staggered testing strategy for the homogeneous systems can be applied in more systems. In this study, the testing strategies differentiate from each other by their staggered time. Therefore, the objective of this paper is to find the optimal staggered time t_0 for minimized unavailability when the reliability and testing intervals of components in a 1oo2 system are different.

The remainder of the paper is organized as follows: Section 2 presents the calculation of optimally staggered time for minimized unavailability in three heterogeneous contexts. And then, some cases will be studied for checking the calculation. In Section 4, Monte Carlo simulation based on Petri net models will be presented to examine the impact of staggered time on the effectiveness of staggered testings. Finally, conclusions and research perspectives occur at the end.

2. Optimal staggered time

Heterogeneousness in SISs comes from both structures and operations. In this study, the following three situations of 1oo2 SISs are taken into consideration:

1. Failure rates of the two components are the same, but testing intervals are different.
2. Testing intervals of the two components are the same, but failure rates are different.
3. Both failure rates and testing intervals of the two components are different.

In the following subsections, the optimal staggered time of testings will be explored in these three contexts. The average PFD in a certain period is adopted as the measure of the unavailability of a SIS, and a testing strategy with the optimal staggered time should ensure that PFD_{avg} of the system is the minimum.

Some assumptions in the analysis are necessary to be mentioned:

- The two components in a 1oo2 SIS are independent with constant failure rates.
- Only dangerous undetected (DU) failures occur in the components. In other words, safe failures and dangerous detected (DD) failures are ignored in this study, since they are not the main contributors of the unavailability of such a system. In fact, many types of failures can occur in SISs, and more details about the variety of types of failures in SISs can be found in [1,13,9].
- Common cause failures (CCFs) are ignorable although they are often considered in reliability assessment of redundant systems. Readers are recommended to find more information about CCFs in [15,16,18,4].
- Testing and repair times are rather short compared with testing intervals, so that they can be ignored.
- After testings, all faults in components can be found, and then the components are restored to the “as good as new” state.

2.1. Same failure rates, different testing intervals

For a 1oo2 SIS, we can assume without loss of generalization that the testing interval of component 1 (τ_1) is longer than that of component 2 (τ_2). Fig. 2 illustrates the effectiveness of staggered testings for a 1oo2 SIS, where $\tau_1 = 2\tau_2$. In the interval from 0 to τ_1, component 2 is tested firstly at time t_0 and then tested again at time $t_0+\tau_2$.

In this study, we set the ratio of τ_1 and τ_2 equal to n, and n is a positive integer (n=1, 2, 3,…). n_0 is used to describe testing times of component 2 in the interval of τ_1. At the point of $t_0+(n_0-1)\tau_2$, component 2 has been tested for n_0 times. And then, component 1 will be tested at the first time, so as

$$t_0+(n_0-1)\tau_2 \le \tau_1$$
$$t_0+(n_0-1)\tau_2 \le n\tau_2$$
$$(n_0-1)\tau_2 < n\tau_2$$
$$n_0 < n+1$$

On the other hand, since component 1 will be tested before component 2 after the time of $t_0+(n_0-1)\tau_2$, we have

$$\tau_1 - t_0 - (n_0-1)\tau_2 < \tau_2$$

Thus,

$$n_0\tau_2 + t_0 > \tau_1$$
$$(n_0+1)\tau_2 > \tau_1$$
$$(n_0+1)\tau_2 > n\tau_2$$
$$n_0 > n-1$$

Since n_0 is also an integer, n_0 is equal to n. In the following, we use n to denote the ratio of two testing intervals as well as the tested times of the component 2 during the period of two subsequent tests of component 1.

The symbol λ is used to denote the failure rate of the two components, and the unavailability of a component j is

$$q_j(t) = 1 - e^{-\lambda T_j}$$

where T_i is the operational time of the component j from the previous test.

It is noted that T_j is different from the total time of the component (t), and the latter one corresponds to the values of the x-axis in Fig. 2. For example in this case, if we measure the unavailability in the interval between 0 and τ_1, $T_1 = t$ for component 1, while for component 2, T_2 after the ith test is equal to $t-(i-1)\tau_2-t_0$.

The unavailability of the system (PFD(t)) at a time t can be obtained by $\text{PFD}(t) = q_1(t)\cdot q_2(t)$. Thus, for a testing interval of component 1 (0, τ_1], the average PFD can be calculated as

$$\text{PFD}_{\text{avg}} = \frac{q_S}{\tau_1} = \frac{1}{\tau_1}\left(\int_0^{t_0}(1-e^{-\lambda t})(1-e^{-\lambda(t+\tau_2-t_0)})\,dt\right.$$