Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 192 (2017) 10 – 15

Procedia Engineering

www.elsevier.com/locate/procedia

TRANSCOM 2017: International scientific conference on sustainable, modern and safe transport

Modelling of transition of system with standby redundancy into failed state

Jozef Balák[a]*, Peter Ždánsky[a]

[a]*Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia*

Abstract

An extension of a system by redundancy is a method of system modification which can be used for failure detection, failure masking or recovery after a failure. Dependability system features (availability) and safety system features (safety integrity) can be improved in a desired manner by an application of redundancy. The resulting influence of redundancy on the system depends on used forms of redundancy and its application methods. The paper deals with a calculation of a failed state probability of the system with standby redundancy and it points out the importance of choosing of a suitable method for an analysis of a monitored system feature.

Peer-review under responsibility of the scientific committee of TRANSCOM 2017: International scientific conference on sustainable, modern and safe transport

Keywords: reliability; redundancy; standby redundancy; failed state probability; failure rate; FTA; CTMC

1. Introduction

System modification based on system expansion by redundant parts can be used for failure detection, failure masking or recovery after a failure. Redundant parts are used for achieve required reliability and safety in safety related communication systems, too. If redundant parts are used only for improvement of dependability measures, redundant parts are called redundancy. Redundancy can operate as active or standby redundancy [1,2,3,6].

* Corresponding author. Tel.: +421-41-513-3306.
E-mail address: jozef.balak@fel.uniza.sk

Peer-review under responsibility of the scientific committee of TRANSCOM 2017: International scientific conference on sustainable, modern and safe transport
doi:10.1016/j.proeng.2017.06.002

At active redundancy, a basic item and all redundant items perform a control function at the same time. If only a part of all items which perform the required function is active and the rest of the items is inactive (they are waiting to put into the active state if one of the active items fails), this system is called a system with standby redundancy. A configuration when the system performs the required function until at least one item is functional is very often. Increasing the system availability is a positive benefit of standby redundancy [1,2,3].

The redundant item of standby redundancy can be in a passive functional state, active functional state or failed state. In the passive functional state, the basic item performs the required function and the redundant item is without the failure, but doesn't perform any function and waits to be put into the active functional state. The redundant item is in the active functional state, if the basic item fails and the redundant item is without the failure and takes over the function of the basic item. If redundant item has got the random failure, it is in the failed state [1,2,3].

If the random failures occurrence of the redundant item follows the exponential distribution, then the derating degree of redundancy is expressed by the so-called redundancy derating factor α [1,2,3]

$$\alpha = \frac{\lambda_{RP}}{\lambda_{RA}} \tag{1}$$

where λ_{RP} is a random failure rate of the redundant item in the passive functional state and λ_{RA} is a random failure rate of the redundant item in the active functional state. If the redundant item is hardware identical with the basic item, then $\lambda_{RA} = \lambda$, where λ is a random failure rate of the basic item.

These values of redundancy derating factor are characteristic for the redundant item in the passive functional state:

- $\alpha = 0$ (cold standby redundancy); it is assumed that the random failure of the redundant item cannot occur in this operation mode (an idealized idea) and therefore it is considered that $\lambda_{RP} = 0$ (in reality $\lambda_{RP} \ll \lambda$ and $\alpha \rightarrow 0$); the redundant item is disconnected from the power source,
- $0 < \alpha < 1$ (warm standby redundancy); $0 < \lambda_{RP} < \lambda$; only some parts of the item are connected to the power source,
- $\alpha = 1$ (hot standby redundancy); $\lambda_{RP} = \lambda$; the whole redundant item is connected to the power source.

In the active functional state, the whole redundant item is connected to the power source.

The most commonly used methods for a reliability analysis or fault analysis of non-repaired items are Reliability Block Diagram (RBD) and Fault Tree Analysis (FTA). During the system reliability analysis, also an influence of a possible change of reliability parameters of the redundant item have to be respected [5].

2. Analysis of system with standby redundancy by FTA

Let the system with standby redundancy contains a basic item A, a redundant item B and a switch P (Fig. 1. (a)). The switch is a critical element of the system with standby redundancy because it determines which item will be connected to the process. From a dependability point of view, it is required that the failure rate of a switch is significantly smaller than failure rates of other items. Fig. 1.(b) shows a fault tree which describes a failure of the system in Fig. 1.(a) (a top event N) depending on failures of individual items of this system (basic events A, B, P) [4]. This fault tree can be described by a logic (Boolean) function

$$N = P + A(B+P) + B(A+P) = P + AB \tag{3}$$

If the item B operates as hot standby redundancy and the occurrence of random failures of the items A, B, P follows the exponential distribution, then the occurrence probability of the top event N (a probability of the failure of the system in Fig. 1.(a)) is defined by:

$$p_N(t) = 1 - e^{-(\lambda_A+\lambda_P)t} - e^{-(\lambda_B+\lambda_P)t} + e^{-(\lambda_A+\lambda_B+\lambda_P)t} \tag{4}$$