Available online at www.sciencedirect.com
ScienceDirect
IFAC Papers Online CONFERENCE PAPER ARCHIVE
IFAC-PapersOnLine 49-12 (2016) 139–144

Methods of reliability assessment of heterogeneous redundant systems

Elena Rogova*. Gabriel Lodewijks.*

** Department of Maritime and Transport Technology, Delft University of Technology, Mekelweg2, 2628CD Delft, The Netherlands (Tel: +31 015 27 82889; e-mail: E.S.Rogova@tudelft.nl, G.Lodewijks@tudelft.nl)*

Abstract: Reliability assessment is required for the determination of a safety integrity level (SIL) of safety systems in accordance to the functional safety approach. Functional safety standards suggest formulas for calculating PFD/PFH which numerical values are used for establishing correspondence to the SIL. However these formulas cannot be used for heterogeneous redundant systems with a combination of mechanical, electronic/electrical components and constant and non-constant failure rates. In this paper we present an overview of reliability assessment methods that are able to cope with these features of heterogeneous redundant systems, show their advantages, drawbacks and limitations in application.

Keywords: reliability analysis, redundancy, heterogeneous systems, non-constant failure rates, probability of failure on demand, safety integrity level.

1. INTRODUCTION

In the functional safety approach, safety instrumented systems (SIS) perform safety functions. Each safety function has a determined SIL (safety integrity level) from 1(minimum) till 4 (maximum). Correspondence of the SIS to the required SIL is a very important step in the design stage of a control system. Standards IEC 61508, 61511 and 62061 describe in details the procedure of reliability assessment of SIS for the determination of the corresponding SIL (IEC 61511-1, 2004; IEC 62061, 2005; IEC 61508-1, 2010). Analytical formulas for calculating PFD (Probability of failure on demand) and PFH (Dangerous Failure Frequency) for systems with M-out-of-N architecture are presented in book 6 of IEC 61508 (IEC 61508-6, 2010). However these formulas can be used only if the failure rates of a system are constant and channels are identical. For heterogeneous redundancy, that is defined as mixing of different types of components (Sharma et al. 2011) with different channels and combination of constant and non-constant failure rates, it is necessary to apply other methods.

A heterogeneous M-out-of-N redundancy architecture can be used in old mechanical safety systems when, instead of its full replacement, redundancy can be introduced by adding the required electrical/electronic components into the system. Due to the hardware diversity such redundancy significantly reduces common cause failures (CCF) and dramatically increases diagnostic coverage (DC) (IEC 62061, 2005; IEC 61508-6, 2010).

In this paper we will consider different methods that can be applied for the reliability assessment of different types of heterogeneous redundant systems. In addition we will show some possibilities to avoid excessive complexity and describe conditions when systems with non-constant failure rates can be considered as systems with constant failure rates and can be calculated by using conventional formulas presented in functional safety standards. Analytical formulas and algorithms suggested by the methods, considered in this paper, can be used in different control systems at the design stage to suit the required SIL. It is also important for the determination of a repair/maintenance policy.

The structure of the paper is as follows: in Section 2 we consider the main features of heterogeneous M-out-of-N redundant systems and the main issues in reliability assessment of such systems. Section 3 presents the difference between systems with constant and non-constant failure rates and describes conditions under which systems with degradation can be considered as systems with approximately constant failure rates. Reliability assessment methods divided into several groups are discussed in Section 4. Section 5 contains a description of the practical implementation of heterogeneous M-out-of-N redundancy architectures as a part of large engineering systems. In Section 6 we conclude.

2. HETEROGENEOUS REDUNDANT SYSTEMS

As was mentioned in Section 1, the main feature of heterogeneous redundant systems is the existence of different types of components. There are many different components that can be used in control systems from the level of sensors and detectors till the level of actuators and mechanisms. From the reliability point of view we separate these components based on three categories:

1) The first category is based on the nature of component: mechanical or electrical/electronic.

2) The second category is a sequence of the first one: constant (λ) or non-constant ($\lambda(t)$) failure rates.

3) The third category defines the difference or identity of channels in redundancy architecture:

Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2016.07.564

a. different components are located in the same channel, but all channels are identical;

b. channels are also different.

The choice of constant or non-constant failure rate in the second category depends on many parameters. First of all it depends on the available information for the specific component and approximation on the basis of a chosen model. Mechanical and electrical/electronic components have different physical principals. Many mechanical components have degradation of their reliability parameters that means non-constant failure rates. Electronic/electrical components also can have degradation. However the majority of them are assumed to have approximately constant failure rates.

Fig. 1 demonstrates different types of heterogeneous M-out-of-N architecture. Case a) is an M-out-of-N architecture with different channels and constant failure rates. The problem of reliability assessment of such architecture can be solved by using reliability block diagram (RBD) and all other methods that work with constant failure rates. Case b) looks like a homogeneous redundant system due to its identical channels. However heterogeneity of this system is in different types of components inside of each channel. For this case it is important to get a failure rate function for a channel based on failure rates of all components in a channel and use reliability assessment methods that are able to work with non-constant failure rates. Some methods (see Section 4) work only for systems with one component level redundancy and cannot be used for systems with several different components in one channel. Case d) is difficult for reliability assessment due to different channels and different non-constant failure rates. Case c) is even more difficult case because of different channels and a combination of constant and non-constant failure rates.

In general reliability assessment methods for heterogeneous redundant systems have two main issues: 1) non-identical channels and 2) non-constant failure rates. It is not difficult to find methods for each of these issues separately. But it is not easy to find a method that is able to cope with both of these issues simultaneously.

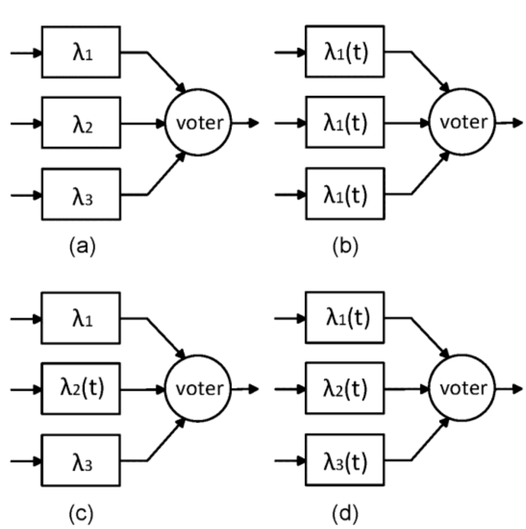

Fig. 1. Heterogeneous redundant systems.

3. CONSTANT OR NON-CONSTANT FAILURE RATES

As was discussed in Section 2, many mechanical components have degradation over time that means non-constant failure rates. However sometimes it is not easy to obtain a failure rate function and to find an appropriate reliability method. In some cases non-constant failure rates can be assumed as approximately constant under specific conditions. In this section we consider these conditions and discuss when it is reasonable to calculate the failure rate function instead of a failure rate.

Alfredsson and Waak (Alfredsson and Waak, 2001) compare constant and non-constant failure rates. The authors separate constant demand rates and constant components rates. They assume constant demand rates without assuming constant component failure rates. The reason of this assumption is that 'the demand process for a given item type at a given site is the result (in essence the superposition) of a number of component failure processes'. In this case, based on Drenick's theorem, the demand process can be approximated by a Poisson process, that means the demand rate is approximately constant (Alfredsson and Waak, 2001). Jones (Jones, 2001) considers a failure intensity analysis for estimation of system reliability using a non-constant failure rate model. He conducts an analysis of failure intensity curve of CMOS digital integrated circuits with 1000 hour intervals. The shape of the curve obtained by Jones is 'ample evidence that the constant failure rate assumption for this type of device is incorrect' (Jones, 2001). It is also important to notice that Jones considers only the first part of the bath-tube curve by using an example of CMOS digital devices. For mechanical components in general we are focused on the last region of the bath-tube curve that is related to the wear-out region.

For obtaining a failure rate function it is necessary to choose an appropriate distribution that can describe a degradation process. There are different distributions that can be chosen. However, many researchers and practitioners use a Weibull distribution for the mathematical description of the wear out failure characteristics (Chudoba, 2011; Kumar and Jackson, 2009; Keller and Giblin, 1985). A failure rate function of two-parameter Weibull distribution is demonstrated in (1):

$$\lambda(t) = \frac{\alpha \cdot t^{\alpha-1}}{\eta^{\alpha}} \quad (1)$$

where α – Weibull shape parameter; η – Weibull scale parameter.

Weibull shape and scale parameters can be obtained from real statistical data and also from Weibull databases where values of α and η are presented for typical components. These databases are very helpful if real statistical data is not available. However such data from databases should be used with caution because they give very approximate average values for components. The same components produced by different manufacturers can have very different Weibull parameters.

Constant failure rates can be applied as an approximate solution for components with non-constant failure rates if the following condition is met: the difference in values of the