Available online at www.sciencedirect.com
ScienceDirect
Reliability Engineering and System Safety 92 (2007) 1267–1273
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

A simple reliability block diagram method for safety integrity verification

Haitao Guo*, Xianhui Yang

Department of Automation, Tsinghua University, Beijing 100084, China

Received 27 June 2006; received in revised form 31 July 2006; accepted 8 August 2006
Available online 2 October 2006

Abstract

IEC 61508 requires safety integrity verification for safety related systems to be a necessary procedure in safety life cycle. PFD_{avg} must be calculated to verify the safety integrity level (SIL). Since IEC 61508-6 does not give detailed explanations of the definitions and PFD_{avg} calculations for its examples, it is difficult for common reliability or safety engineers to understand when they use the standard as guidance in practice. A method using reliability block diagram is investigated in this study in order to provide a clear and feasible way of PFD_{avg} calculation and help those who take IEC 61508-6 as their guidance. The method finds mean down times (MDTs) of both channel and voted group first and then PFD_{avg}. The calculated results of various voted groups are compared with those in IEC61508 part 6 and Ref. [Zhang T, Long W, Sato Y. Availability of systems with self-diagnostic components-applying Markov model to IEC 61508-6. Reliab Eng System Saf 2003;80(2):133–41]. An interesting outcome can be realized from the comparison. Furthermore, although differences in MDT of voted groups exist between IEC 61508-6 and this paper, PFD_{avg} of voted groups are comparatively close. With detailed description, the method of RBD presented can be applied to the quantitative SIL verification, showing a similarity of the method in IEC 61508-6.

Keywords: Safety related system; Reliability block diagram; Safety integrity level; Probability of failure on demand; IEC 61508

1. Introduction

IEC 61508 [1] published in 2000 has been adopted by many countries as their national standard and is being updated. Two significant concepts, safety life cycle and safety integrity level (SIL) [1–3], appeared in IEC 61508. A necessary procedure of safety life cycle is SIL verification, which verifies whether the average probability of failure on demand (PFD_{avg}) of designed safety related systems (SRS) meets the required failure measure. If not, retrofit or modification must be taken to reduce the PFD_{avg} of safety related system till safety goal is satisfied. Besides PFD_{avg} verification, architectural constraints defined in IEC 61508 must be also considered during SIL verification process [17]. This study focuses on PFD_{avg} calculation.

Since IEC 61508 is a performance based standard, the verification can be done through a number of probabilistic analysis techniques. There are many techniques in published literature, such as fault tree analysis (FTA) [4,5], reliability block diagram (RBD) [6], Markov Analysis (MA) [5,7,8,13], simplified equations [9,10] and hybrid method [11]. Rouvroye and Brombacher [12] compared those techniques and outlined their advantages and disadvantages. Bukowski [13] compared MA and simplified equations and provided an overview of their advantages and disadvantages. Andrews and Ericson II [14] analyzed various design complexities using FTA and MA respectively and they concluded that both FTA and MA can provide satisfactory accuracy of calculation, but FTA model is more intuitive and easier to create for large and complex systems. What can also be seen is that the outcomes of FTA and MA are considerably close in Ref. [5]. Hauge et al. [15] introduced a method called PDS to quantify the safety unavailability and loss of production

*Corresponding author. Tel.: +86 10 6278 5845x231; fax: +86 10 6279 0497.
E-mail address: guoht03@mails.tsinghua.edu.cn (H. Guo).

0951-8320/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2006.08.002

for safety instrumented systems. PDS accounts for all types of failure categories: technical, software, human, etc.

RBD, which has equivalent mathematical characteristic to FTA, has been widely used in reliability engineering for many years. By the RBD technique, IEC 61508-6 shows the verification of SIL through calculating average probability of failure on demand (PFD_{avg}). While IEC 61508 has been adopted as national standard of many countries, its demonstration can also be regarded as a guide to do PFD_{avg} calculations. A RBD model reveals the logical reliability structure of the involved SRS and can easily be created even for a complex large SRS. However, IEC 61508-6 does not give detailed description of RBD it uses and its results are different from those of Markov model by Zhang et al. [8]. Consequently, the technique used in IEC 61508-6 gets questioned. Besides, no other papers dealing with SIL verification by RBD technique can be found yet, and so RBD needs more supports in the field of functional safety.

Because IEC 61508-6 does not give explanations of the definitions and PFD_{avg} calculations for its examples in detail, it is difficult to use the standard as guidance in practice. In order to provide a clear and feasible way of SIL verification, a method of RBD for PFD_{avg} calculation is presented in this paper with detailed explanation including the definitions, assumptions and parameters regulated in IEC 61508-6 [6] based on specific system architectures and associated conditions. The method finds mean down time (MDTs) of both channel and voted group first and then PFD_{avg}. The results achieved in this study are compared with those of IEC 61508-6 demonstration and Ref. [8]. Through the comparison, an interesting outcome can be realized. The method of RBD in this study can be applied to the quantitative SIL verification and helps those who take IEC 61508-6 as their guidance.

2. Reliability block diagram

Reliability block diagram (RBD) is a graphical analysis technique, which expresses the concerned system as connections of a number of components in accordance with their logical relation of reliability. Series connections represent logic "and" of components, and parallel connections represent logic "or", while combinations of series and parallel connections represent voting logic. From leftmost node to rightmost node, there are several paths that are the conditions for successful operation of system. If a component fails, the corresponding connection will be cut off. As failures of components occur, System keeps operating successfully until no valid path from leftmost node to rightmost node can be made up of available connections. Then, probability of the failure of system can be calculated according to probabilistic principles.

RBD model is intuitive and easy to establish. For instance, 1oo2 voted group consists of two voted channels, each of which has their own component(s). Common cause failure can take place upon the two channels. 1oo2 voted group with one sensor for each channel can be represented by the RBD shown in Fig. 1.

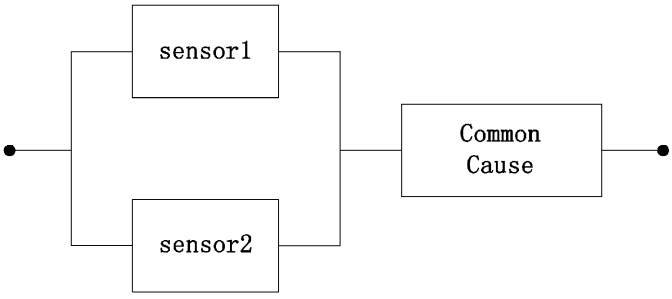

Fig. 1. A RBD example.

3. Definitions and assumptions

3.1. Equivalent MDT

In IEC 61508-6, one system architecture (group) consists of one or redundant channels and there is a voting logic for the architecture, such as 1oo1, 1oo2. In steady state, the normal operation and failure states of the channel(s) and the group appear by turns because of failure detection and reparation. The voting logic determines that how many failures of channels will cause the group to fail.

Equivalent MDT of a component is defined as the average of the period of time when the component is in dangerous failure state at the steady state. Dangerous failure state refers to the state that the component cannot take the proper response to dangerous process demands, which may lead to unexpected accidents, while the process is still operating.

The PFD_{avg} calculations in this study depend on equivalent MDTs, group equivalent MDT and channel equivalent MDT.

3.2. Average probability of failure on demand

Probability of failure on demand is defined as the probability of failing to take correct action when a process demand arises. Since the steady state is under consideration, PFD is averaged for infinite.

3.3. Assumptions

The technique and results developed in this paper are based on the assumptions following:

(i) The resulting average probability of failure on demand for the subsystem is less than 10^{-1}, or the resultant probability of failure per hour for the subsystem is less than 10^{-5}.
(ii) Component failure and repair rates are constant over the life of the system.
(iii) The hardware failure rates used as inputs to the calculations and tables are for a single channel of the subsystem.