ISA Transactions®

Volume 45, Number 4, October 2006, pages 611–621

Minimizing costs while meeting safety requirements: Modeling deterministic (imperfect) staggered tests using standard Markov models for SIL calculations

Jan L. Rouvroye*

Subdepartment Quality and Reliability Engineering, TU/e Technische Universiteit Eindhoven, Department of Technology Management, Building PAV. C 12, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

Jan A. M. Wiegerinck

Shell Global Solutions International B.V., Carel van Bylandtlaan 30, P.O. Box 541, 2501 CM The Hague, The Netherlands

(Received 24 June 2005; accepted 20 December 2005)

Abstract

In industry, potentially hazardous (technical) structures are equipped with safety systems in order to protect people, the environment, and assets from the consequences of accidents by reducing the probability of incidents occurring. Not only companies but also society will want to know what the effect of these safety measures is: society in terms of "likelihood of undesired events" and companies in addition in terms of "value for money," the expected benefits per dollar or euro invested that these systems provide. As a compromise between demands from society (the safer the better) and industry (but against what cost), in many countries government has decided to impose standards to industry with respect to safety requirements. These standards use the average probability of failure on demand as the main performance indicator for these systems, and require, for the societal reason given before, that this probability remain below a certain value depending on a given risk. The main factor commonly used in industry to "fine-tune" the average probability of failure on demand for a given system configuration in order to comply with these standards against financial risk for the company is "optimizing" the test strategy (interval, coverage, and procedure). In industry, meeting the criterion on the average probability of failure on demand is often demonstrated by using well accepted mathematical models such as Markov models from literature and adapting them for the actual situation. This paper shows the implications and potential pitfalls when using this commonly used practical approach for a situation where the test strategy is changed. Adapting an existing Markov model can lead to unexpected results, and this paper will demonstrate that a different model has to be developed. In addition, the authors propose an approach that can be applied in industry without suffering from the problems mentioned above. © 2006 ISA—The Instrumentation, Systems, and Automation Society.

Keywords: Markov model; Safety system; Probability of failure; Periodic testing

1. Introduction

Safety systems are used in a wide range of industries where (failures in) technical structures have the potential to negatively affect people, companies, or society. Examples are the process, medical, food, nuclear, and machinery industries. The function of the safety system is to monitor a process or a piece of equipment to determine if it is working within predetermined safe operating limits. When the process or equipment is outside

*Author to whom all correspondence should be addressed. Tel.: +31 40 2472956/3601; Fax: +31 40 2467497; E-mail address: J.L.Rouvroye@tue.nl the safe operating limits, the safety systems intervene and prevent or mitigate the consequences, often by shutting down the process or equipment.

Despite being built to achieve a very high availability, safety systems, like all other technical systems, may fail. In principle, these systems have two main operating modes and two main failure modes. The first main operating mode is when all subsystems are working perfectly. The second main operating mode is when one or more subsystems have failed but, due to built-in redundancy, the system is still able to fulfill its function. The first main failure mode is when, due to subsystem failure(s), the safety system activates erroneously, i.e.,without a requirement from the safeguarded process or equipment. This system failure mode is often called failed safe, false trip, or false alarm. The second main failure mode is when, due to subsystem failure(s), the safety system is no longer able to be activated. This system failure mode is called failed dangerous. Depending on the system, a part of the dangerous failures might be detected by diagnostics and indicated to the operator, who can initiate repairs. The remaining part of undetected dangerous failures can be found only by periodically testing the system. The remainder of this paper only considers these undetected dangerous failures and the related, underlying subsystem failures. The common assumption is that these systems are designed in such a way that the subsystems are to a large extent independent and that system failure is only possible as a result of failure of individual subsystem(s) (with the exception of so-called common cause failures).

Society as well as companies like to know the effect or contribution of safety systems. Society wants to reduce risks from companies as far as possible. In practice this is often performed by reducing the likelihood of undesired events, which is a main task of safety systems. Companies try to comply with society's wishes against minimal costs or with maximum benefits. In recent standards such as IEC61508 [1], IEC61511 [2], and ANSI S84.01 [3], the main performance indicator for a safety system is given in terms of the average probability of failure on demand, i.e., the average probability that the safety system is not able to fulfill its function when required. Once the design of a safety system is finalized, the only way to control (often reduce) the average probability of failure on demand is by means of testing the subsystems. This is especially important for safety systems, which normally are dormant and only have to fulfill their function at the moment this is needed because of an (often rare) demand from the safeguarded process or equipment. In [2] this situation is referred to as the system being in the "demand mode." This implies that if these systems are not tested regularly, failures might not be noticed before the next demand for action from the safeguarded process or equipment. These tests are generally performed at regular prescheduled intervals according to the test procedures described in a test strategy (see [4]).

As mentioned before, the average probability of failure on demand is defined by most standards as one of the key-performance indicators for a safety system. To comply with the requirements for this characteristic, a quantitative analysis is required. Generally, the industry uses standard analysis methods with corresponding sets of quantitative models for this type of analysis for example [5,6]. The industry attempts to optimize the performance of safety systems (i.e., to maintain safety at an acceptable level while disturbing the safeguarded process as little as possible by performing tests in this way minimizing costs in terms of production losses and undesired stops/starts of the process). This can be done by changes in the test strategy, for example by changing of the test interval or the test procedures [7].

One of the well known strategies, often used in industry, is the use of so-called staggered testing. In order to reduce down-time of the equipment, the system is not tested as a whole (often resulting in a total system shutdown) but as independent redundant branches. Since during the test part, the redundant structure is still on-line, a system shutdown (often costly and time-consuming) is not considered necessary.

This paper will evaluate the impact of a simple change of test strategy (changing from simultaneous testing to staggered testing of a redundant configuration) using existing, commonly used, standard Markov models [5,8,9] and will show that this simple change leads to unexpected results when compared to existing models for staggered testing in terms of (long-term) average probability of system failure [9–11]. First this paper will give a short summary of Markov models and how to incorporate deterministic testing. Then a case study shows that a simple standard Markov model