Reliability Engineering and System Safety 142 (2015) 525–538

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees

Antonio Eduardo Bier Longhi [a,*], Artur Alves Pessoa [b,1], Pauli Adriano de Almada Garcia [c,2]

[a] Petrobras, Av. Henrique Valadares, 28, Torre A, 9° Andar, Centro, CEP: 20231-030 Rio de Janeiro, RJ, Brazil
[b] Universidade Federal Fluminense, Rua Passos da Pátria, 156, Bloco D, Sala 309, São Domingos, CEP: 24210-240 Niterói, RJ, Brazil
[c] Universidade Federal Fluminense, Rua Desembargador Hermydio Ellis Figueira, 783, Bloco A, Sala 304, Aterrado, CEP: 27258-145 Volta Redonda, RJ, Brazil

ARTICLE INFO

Article history:
Received 20 February 2015
Received in revised form
3 June 2015
Accepted 11 June 2015
Available online 26 June 2015

Keywords:
Safety instrumented systems
Evolutionary optimization
Operation
Testing
Fault trees
Genetic algorithms

ABSTRACT

Since low-demand safety instrumented systems (SISs) do not operate continuously, their failures are often only detected when the system is demanded or tested. The conduction of tests, besides adding costs, can raise risks of failure on demand during their execution and also increase the frequency of spurious activation. Additionally, it is often necessary to interrupt production to carry out tests. In light of this scenario, this paper presents a model to optimize strategies for operation and testing of these systems, applying modeling by fault trees associated with optimization by a genetic algorithm. Its main differences are: (i) ability to represent four modes of operation and test them for each SIS subsystem; (ii) ability to represent a SIS that executes more than one safety instrumented function; (iii) ability to keep track of the down-time generated in the production system; and (iv) alteration of a genetic selection mechanism that permits identification of more efficient solutions with smaller influence on the optimization parameters. These aspects are presented by applying this model in three case studies. The results obtained show the applicability of the proposed approach and its potential to help make more informed decisions.

1. Introduction

Safety instrumented systems (SISs) provide a layer of independent protection. They are used to control or mitigate risks related to the operation of many industrial installations [1]. SISs can be subdivided into three subsystems: (i) sensor elements (SEs); (ii) logic solver (LS) units; and (iii) final elements (FEs). They have two main functions: (a) to activate the final elements when a specific demand occurs in the system being monitored, where failure to carry out this function is called a failure on demand or failure to function (FTF); and (b) to remain deactivated without the occurrence of a defined demand, where failure is called spurious activation, or a spurious trip (ST) [2].

Each SIS is responsible for executing one or more safety functions. For each of these there is a safety instrumented function (*SIF*) and an associated safety integrity level (SIL) [3]. There are three operating modes of a *SIF* [4]: (i) low demand, when the function is required to operate less often than once per year; (ii) high demand, when the function is required to operate more than once a year; and (iii) continuous, when the function has to assure safety of the system during all normal operations. The parameter to assess the reliability of a low-demand *SIF*, with respect to the FTF, is the probability of failure on demand (*PFD*), while for high-demand and continuous modes the parameter is the probability of failure per hour (PFH) [4]. Finally, the parameter to assess reliability regarding ST is the spurious trip rate (STR) [5].

In a SIS operating under low demand, some failures to their components can remain hidden, only being detected when the system is tested or a real demand occurs [2]. Although periodic tests can detect some hidden problems, they increase costs and can heighten risks during their execution, by increasing the *PFD* during testing [6], also increasing the spurious trip rate (STR) [7]. In factories where production is continuous, it is normally necessary to interrupt production of the protected system to test some SIS components, thus causing a conflict between ongoing production and execution of the test [8]. On the other hand, various tests can be conducted during scheduled shutdowns for maintenance, which normally happen at intervals ranging from two to six years. In these situations, it is possible to perform tests without increasing the likelihood of spurious activation or impairing production.

* Corresponding author. Tel.: +55 21 2166 5745.
E-mail addresses: alonghi@petrobras.com.br (A.E.B. Longhi), artur@producao.uff.br (A.A. Pessoa), pauliadriano@id.uff.br (P.A.d.A. Garcia).
[1] Tel.: +55 21 2629 5709.
[2] Tel.: +55 24 3076 8776.

http://dx.doi.org/10.1016/j.ress.2015.06.010
0951-8320/

Many studies have investigated questions related to estimating the reliability parameters of safety instrumented systems. However, these studies only considered part of the subsystems, did not estimate the rate of spurious activation and disregarded the possible strategies for operation and execution of the tests [9–11]. In turn, [12] estimated the spurious activation but disregarded the possible strategies for operation and test execution. Other studies [6,13] considered spurious activation and two testing modes in their SIS test optimization models. However, in some situations the selection between the testing modes provided solutions that cannot be applied in real systems in the same way they were modeled. These studies also disregarded, in estimating the total operating cost of these systems, the fraction caused by the production down-time during execution of the tests or repairs to the safety system. The PDS method [5] considers three operating and testing philosophies and evaluates the down-time of the productive system, using simplified equations for this purpose. Nevertheless, this method does not consider the costs of its formulation, nor does it handle optimization of its tests. Besides this, more than one safety function can be implemented in a single SIS, through sharing of some of its subsystems [14]. In these situations, the operating and testing strategy applied must meet the needs of the various safety functions in correlated form.

Therefore, the main goal of this paper is to present a model for multiobjective optimization of the strategies for operation and testing of low-demand SISs. The model considers the probability of failure of each of the instrumented functions, to try to satisfy the required SIL and minimize the impact on the cost over the installation's life cycle. Based on these objectives, it was possible to formulate more realistic models to represent the interrelationship of one or more safety functions with the production system. It was also possible to identify workable testing strategies, even in complex systems, able to assure the integrity of the safety system while minimizing its impact on the business.

The main advantages of the approach presented are: (i) the model's ability to represent four different modes of operation and to test each subsystem of the SIS, allowing selection of the most suitable mode for each context by means of optimization; (ii) the ability to represent a SIS that carries out more than one instrumented function, with or without sharing of components; (iii) the ability to keep track of the production down-time generated by SIS tests and repairs; and (iv) the possibility of altering a selection mechanism applied to the genetic algorithm, enabling identification of more efficient solutions with less influence of the optimization parameters.

2. Probabilistic model

To compare the safety integrity level (SIL) and composition of the associated costs over the entire life cycle of each *SIF*, we calculated the parameters PFD_{avg}, STR_{avg} and U_{avg}, where the last one represents the average unavailability of the protected system resulting from maintenance or testing of the *SIF*.

In developing the model we considered four possible modes of operation and testing, applicable to each subsystem of the SIS. These modes were defined based on the philosophies for operation and testing presented in [5] and the testing modes utilized in [15]. They are described below

i. *M*1—always stop: production will be interrupted any time a failure is detected or a test is conducted;
ii. *M*2—always open: the voting logic will be altered any time a failure occurs or components are tested. This change in voting logic means the tested or failed component votes for activation of the *SIF*.
iii. *M*3—always close: the voting logic will be altered any time a failure occurs or components are tested. However, in this case the change in the voting logic means the tested or failed component cannot vote to activate the *SIF*.
iv. *M*4—always bypass: the *SIF* will be removed from operation any time a failure is detected or a test is conducted, with the system operating without the referred protection during the period necessary to restore the normal condition.

Modes *M*1 and *M*4 are only applicable to subsystems where the tests are conducted of all the components simultaneously.

We parameterized the execution of the complete tests using three variables for each SIS subsystem: (i) execution time of the first test (T_{FT}); (ii) testing interval factor (f_{TI}), with values in the interval [0, 1] and; (iii) testing cycle period (T_C), which represents the time between conducting a test of any of the components and the next test of the same component. If $f_{TI}=0$, the tests of the various components are carried out simultaneously and if $f_{TI}=1$ the tests are evenly spaced in the interval T_C. These definitions are similar to those used in the SIS testing optimization study of [6]. For the subsystems of final elements, we added one more variable, with the aim of representing the partial movement or partial stroke tests (PSTs) [16]. This variable, N_{PST}, represents the number of partial tests that will be conducted in each complete testing cycle (T_C).

The complete tests have defined duration (T_D) and the partial tests (PST) are considered to be instantaneous. If the mode of operation chosen is *M*1, we assume the test duration is the mean time to stop and start the protected system (*MTTSS*). Besides this, the proposed model considers the existence of testing windows, resulting from scheduled shutdowns for maintenance of the production system, in a defined period (t_{max}).

We consider homogeneous components in each subsystem and that the time to failure of each of these obeys the homogeneous Poisson process. The failure rate of each component is subdivided into the four fractions: dangerous detected (λ_{DD}), dangerous undetected (λ_{DU}), safe detected (λ_{SD}) and safe undetected (λ_{SU}) [2,4]. The model presented here also considers a fraction of failures that is independent of conduction of the tests (P_{TIF}) [5]. Besides this, the PST can detect a fraction θ_{PST} of the undetected failures [17]. The mean time to repair (*MTTR*) and mean time to stop and start (*MTTSS*) of the protected system are considered to have constant duration. The model used to represent the failures with common cause is the modified beta factor model [5], which can easily be reduced to the beta factor model [18] and is described in the IEC standard [4].

The values of the basic events of the fault trees were obtained from the equations presented. The value of the top event was computed discretely each hour in the interval [1, t_{max}]. Its average values were obtained from the mean of these top values, similar to that presented in [6]. The equations of the probability of occurrence of the basic events considered three distinct moments: (i) normal operation—when the component is not subject to testing or repair; (ii) during testing—when the component is being tested; and (iii) during repair—period after a test, when a repair might being carried out to correct a failure identified.

2.1. Probability of failure on demand

To obtain the *PFD* of each *SIF*, we used the quantitative fault tree technique and its complete structure functions, since its minimum cutsets can be changed while conducting the tests [15].

Fig. 1 shows the fault tree to obtain the *PFD*, where the top event is "*SIF* Unavailable". In the model developed here, the top event occurs any time one of the *SIF* subsystems is unable to operate ("*SIF* Failure"), or any time one of the subsystems is