Reliability Engineering and System Safety 133 (2015) 212–222

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Switching Markov chains for a holistic modeling of SIS unavailability

Walid Mechri [a,*], Christophe Simon [b,c], Kamel BenOthman [a]

[a] École Nationale d'Ingénieurs de Tunis, Laboratoire de Recherche LR-Automatique, LR-11-ES18, Le Belvédère, 1002 Tunis, Tunisia
[b] Université de Lorraine, Centre de Recherche en Automatique de Nancy, UMR 7039, Vandoeuvre-lès-Nancy F-54506, France
[c] CNRS, Centre de Recherche en Automatique de Nancy, UMR 7039, Vandoeuvre-lès-Nancy F-54506, France

ARTICLE INFO

Article history:
Received 30 May 2013
Received in revised form
19 August 2014
Accepted 1 September 2014
Available online 21 September 2014

Keywords:
Safety systems
Probability of failure on demand
Proof test
Common cause failure
Diagnostic coverage
Markov chains

ABSTRACT

This paper proposes a holistic approach to model the Safety Instrumented Systems (SIS). The model is based on Switching Markov Chain and integrates several parameters like Common Cause Failure, Imperfect Proof testing, partial proof testing, etc. The basic concepts of Switching Markov Chain applied to reliability analysis are introduced and a model to compute the unavailability for a case study is presented. The proposed Switching Markov Chain allows us to assess the effect of each parameter on the SIS performance. The proposed method ensures the relevance of the results.

1. Introduction

In many fields of application, it is necessary to reduce the consequences of hazardous events that could generate potential sources of harms for the environment or the health of persons. The goal of safety systems is to cover such potential hazards. A safety system should provide an independent layer of protection by implementing the safety function through many techniques. In this context, IEC61508 [1] standard is a guide for designing, validating and verifying the safety function realized by Electric, Electronic and Programmable Electronic Systems (E/E/PES). A E/E/PES like Safety Instrumented Systems (SIS) is used to implement the Safety Instrumented Function (SIF). Its goal is to detect hazardous events, to perform the required safety action and to maintain or bring the Entity Under Control (EUC) in a safe situation. The study of SIS is framed by the IEC 61508 standard [1] or its application specific standards which are now recognized as the most important standard concerning E/E/PES in several industry sectors.

Its introduction in 1998 [2] has induced many works to understand the new concepts introduced and the influence of all parameters in the SIS performance assessment. This performance is the unavailability to fulfill the safety function and the confidence of the SIS is defined by the well known 4 Safety Integrity Level (SIL) [3], thanks to the computation of a probabilistic parameter (PFD_{avg} or PFH). SIS in low demand mode, which are the subject of this paper, are a particular case. As they are in low demand mode, latent failures can occur but are discovered only when a demand occurs. To thwart this problem, integrated diagnostics are implemented and repeated proof tests are realized. Finally, whereas SIS have usually a low structure complexity, their study can be more complex than expected.

Dutuit et al. [3] argue that Fault Trees (FT) are easy to handle for the practitioners but provide approximations which sometimes give non-conservative results. They propose the use of Switching Markov Chains to take into account dependencies due to proof testing, common cause failures, etc. The several phases correspond to the different period of functioning (operating, test, etc.). Catelani et al. [4] use a Failure Mode Effect and Diagnostic Analysis (FMEDA) approach to identify several influence parameters and finally use the equation proposed in the appendices of IEC61508 [2] for well known architectures. Nevertheless, they pointed out the problem of quantifying the diagnostic coverage rate and other parameters. For instance, Hokstad and Rausand [5] and Lundteigen and Rausand [6] discuss the significant contribution of Common Cause Failure (CCF) in SIS performance. Rahimi and Rausand [7] discuss the impact of Human and Organizational factors on the quantification of CCF through the β factor model. Xu et al. [8] questioned the impact of parameter uncertainties on the achieved safety integrity.

Oliveira and Abramovitch [9] extend equations to *k*-out-of-*n*: F (*koon*) architectures [10]. But, as analyzed in [11], equations should be used cautiously and a particular attention must be paid to the parameters which should correspond to the real situations. In [12],

* Corresponding author.
E-mail address: walid.mechri@isim.rnu.tn (W. Mechri).

http://dx.doi.org/10.1016/j.ress.2014.09.005
0951-8320/

Nomenclature

DC	diagnostic coverage rate
PFD_{avg}	average probability of failure on demand
T_i	test interval
T_M	mission time
λ	failure rate
μ	restoration rate
$P_i(t)$	probability of finding the system in state i at time t
Δt	a small time interval (for Markov chain simulation)
q_{ij}	transition rate from state i to state j, $i \neq j$
Q	transition matrix
M	passage matrix
β	beta factor for quantification of CCF
β_D	proportion of dangerous detected CCF
β_U	proportion of dangerous undetected CCF
ξ	probability of not detecting a failure during a test
γ	probability of failure due to the test
λ^T	total failure rate
λ^C	CCF rate
λ^I	independent failure rate
λ_D	dangerous failure rate
λ_{DD}	dangerous detected
λ_{DU}	dangerous undetected
λ^I_{DD}	dangerous detected independent
λ^C_{DD}	dangerous detected CCF rate
λ^I_{DU}	dangerous undetected independent
λ^C_{DU}	dangerous undetected CCF rate
λ_{SD}	safe detected
λ_{SU}	safe undetected
λ^I_{SD}	safe detected independent
λ^C_{SD}	safe detected CCF rate
λ^I_{SU}	safe undetected independent
λ^C_{SU}	safe undetected CCF rate

ABBREVIATIONS

CCF	common cause failure
CRPS	chemical reactor protection system
DC	diagnostic coverage
EUC	entity under control
E/E/PES	Electric, Electronic and Programmable Electronic Systems
FMEDA	failure mode effect and diagnostic analysis
IEC	International Electrotechnical Commission
HIPS	high integrity protection system
MooN	M out of N voting system
MTTR	mean time to repair
MGL	Multiple Greek Letters
PDS	reliability of safety instrumented systems
PFD	probability of failure on demand
PFH	probability of failure per hour
SIF	safety instrumented function
SIL	safety integrity level
SIS	safety instrumented system

the authors compute the PFD_{avg} of a SIS by a Reliability Block Diagram (RBD) approach with strong assumptions given the method. For instance, the unavailability is considered as the unreliability and no dependencies due to test are considered. Lundteigen et al. [13] questioned the effect of the SIS structure (Hardware Fault Tolerance) and the Safe Failure Fraction proposed in the standard. In [6], the authors studied the effect of tests according to the common cause failures and their relation with the SIS performance, given that quantifying the CCF parameters remains a problem. Jin et al. [14] propose a Markov model to compute the SIS performance whatever is the demand mode. The main advantage of Markov model is to be more accurate and flexible according to the specific feature of each mode. Nevertheless, as mentioned in [15,16], establishing the Markov model of *koon* with a high value of n can be time consuming and error prone [10]. Signoret et al. [17] use Petri Nets to classify SIS. Petri Nets allow us to assess the performance very finely and to take into account several parameters. Nevertheless, Petri Net model of SIS can be difficult to use and the analyst should make efforts to obtain an understandable model. It which is the object of paper [17]. Torres-Echeverria et al. [18,19] pay more attention to modeling the test strategies and how to compute the SIS performance through Fault Tree for redundant SIS layers or *koon* SIS layers. They propose a model that integrates several parameters like CCF, Diagnostic Coverage (DC), test instants, etc.

In this paper, we follow the idea of Dutuit et al. in [3] by using Switching Markov Chains for their ability to model precisely and correctly SIS in low demand. The paper proposes the integration of the following parameters : dangerous failure, diagnostic coverage, common cause failure, test interval, repair rate, probability of failure due to the test γ and the probability of not detecting a failure in a test ξ, in a unique equation modeling the unavailability of periodically tested SIS. The test duration is not considered here because it requires a significant change of complexity in the proposed model. In Section 2, we recall basics elements of SIS and useful parameters. Section 3 is devoted to the Markov models and their extension to Switching Markov Chains to compute the PFD_{avg}. Section 4 is devoted to an illustration on a HIPS supervising a chemical reactor [18].

2. Safety instrumented system

The goal of a SIS is to bring the system it supervises in a safe position *i.e.* in a situation where it does not create a risk for the environment or people when the Entity Under Control (EUC) goes to a hazardous situation involving a real risk to people or the environment (blast, fire, etc.). A SIS is a system composed of any combination of sensors, logic solvers and final elements for the purpose of taking the supervised process to a safe state when predetermined conditions are violated. A SIS is in low demand mode if the demand is less or equal to 1 per year and in high demand mode in other situations [20,1].

IEC 61508 [1] can now be considered as the main standard for the specification and the design of SIS. Its sectorial variation for the process industry [21] is intended to the integrators and users of this field. The requirements of safety function exhibited in [1,21] also introduce a probabilistic approach for the quantitative evaluation of the safety performance. The introduction of probability into the assessment of the integrity level involved the particular concept of average probability of failure on demand (PFD_{avg}). The qualification of this performance is determined by referred levels of safety (SIL). Thus, the PFD_{avg} is in fact the unavailability of the system that affects its ability to react to hazards, *i.e.* the safety unavailability [22,23,20]. The IEC 61508 standard [1] establishes 4 classification levels based on the PFD_{avg} (for low demand