Reliability Engineering and System Safety 171 (2018) 18–33

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Unavailability assessment of redundant safety instrumented systems subject to process demand

Siamak Alizadeh [a], Srinivas Sriramula [b,*]

[a] School of Engineering, University of Aberdeen, Aberdeen AB24 3UE, UK
[b] Lloyd's Register Foundation Centre for Safety & Reliability Engineering, University of Aberdeen, Aberdeen AB24 3UE, UK

ARTICLE INFO

Keywords:
Markov chain
Unavailability assessment, Safety instrumented systems
Hazardous event frequency
Process demand

ABSTRACT

The process industry has always been faced with the challenging task of determining the overall unavailability of safeguarding systems such as the safety instrumented systems (SISs). This paper proposes an unavailability model for a redundant SIS using Markov chains. The proposed model incorporates process demands in conjunction with dangerous detected and undetected failures for the first time and evaluates their impacts on the unavailability quantification of SIS. The unavailability of the safety instrumented system is quantified by considering the probability of failure on demand (PFD) for low demand systems. The safety performance of the system is also assessed using hazardous event frequency (HEF) to measure the frequency of system entering a hazardous state that will lead to an accident. The accuracy of the proposed Markov model is verified for a case study of a chemical reactor protection system. It is demonstrated that the proposed approach provides a sufficiently robust result for all demand rates, demand durations, dangerous detected and undetected failure rates and associated repair rates for safety instrumented systems utilised in low demand mode of operation. The effectiveness of the proposed model offers a robust opportunity to conduct unavailability assessment of redundant SISs subject to process demands.

1. Introduction

Independent Protection Layers (IPLs) are predominantly used to prevent hazardous events, and to mitigate their consequences to humans, the environment, and financial assets. IPLs can be implemented by physical barriers such as mechanical systems, instrumented protective functions or in the form of administrative procedures. An Electric, Electronic and Programmable Electronic System (E/E/PES) such as a Safety Instrumented System (SIS) is an independent layer of protection that provides a protective function by detecting hazardous events, performing the required safety action and maintaining the safe status of the system. The unavailability of a SIS is usually realised from overall hazard and risk analyses. Without suitable design, implementation and maintenance, the SIS may fail to provide the necessary risk reduction. In this context, IEC 61508 [1] standard is a guide for designing, validating and verifying the safety function realised by an E/E/PES throughout all phases of its lifecycle. The principles introduced in this generic standard, are also customised in application specific standards, such as IEC 61511 [2] for the process industry, IEC 62425 [3] for the railway industry, and ISO/DIS 26262 [4] for the automobile industry.

In accordance with IEC 61508 [1] the performance of a SIS shall be proven using a suitable technique. Although no particular model is recommended by the international standards, some of the options are cited in their appendices. The most commonly used techniques include Simplified Equation (SE) [1,5], Bayesian methods [6] Reliability Block Diagram (RBD) [7,8], Fault Tree Analysis (FTA) [9,10], Markov Analysis (MA) [11–13] and Petri Nets (PN) [14]; all of which can be used to analyse the reliability of SIS utilised in various modes of operations. These diverse techniques have their own advantages and limitations. Zhang et al. [15] demonstrated that the simplified equations given in the standard are over simplistic and are more suitable for practicing engineers. The reliability block diagrams represent a success oriented logic system structure and hence the analyst will focus on functions rather than failures, and may thereby fail to identify all the possible failure modes [16]. The fault tree analysis is straightforward to handle for the practitioners and generates approximations which sometimes provide non-conservative results as argued by Dutuit et al. [14].

Whilst the main benefit of Markov models is accuracy and flexibility according to the specific feature of each mode, establishing a Markov model of k out of n ($koon$) with a high value of n, can be time consuming and error prone [17–19]. Signoret et al. [20] employed Petri Nets to categorise safety instrumented systems. Although Petri Nets allow assessment of the SIS performance very finely taking into account several parameters, the models of safety instrumented system produced by Petri Nets can be challenging to use and the analyst should make substan-

* Corresponding author
E-mail address: s.sriramula@abdn.ac.uk (S. Sriramula).

https://doi.org/10.1016/j.ress.2017.11.011
Received 11 December 2016; Received in revised form 17 November 2017; Accepted 18 November 2017
Available online 22 November 2017
0951-8320/

Notations

τ	proof test interval
$p_{ij}(t)$	system transition probability from state i to state j
a_{ij}	transition rate from state i to state j
A	transition rate matrix
λ	component failure rate
λ_{DE}	process demand rate
λ_D	dangerous failure rate
λ_{DD}	dangerous detected failure rate
λ_{DU}	dangerous undetected failure rate
μ	component repair rate
μ_{DD}	dangerous detected repair rate
μ_{DE}	demand reset rate
μ_{DU}	dangerous undetected repair rate
μ_T	renewal rate
π_i	steady state probability of system in state i
Π	steady state probabilities matrix
DC	diagnostic coverage rate
$P(t)$	transition matrix at time t
$P_i(t)$	probability of system in state i at time t
$\dot{P}_i(t)$	time derivative probability of system in state i at time t
r	states of stochastic process
β_D	detected common cause failure factor
β_U	undetected common cause failure factor

tial effort to obtain an understandable model to compute unavailability [20].

A comparison of reliability analysis techniques carried out by Rouvroye and Brombacher [21] concludes that Markov analysis covers most aspects for quantitative safety evaluation. Additionally, Innal [22] investigated the performance of different modelling approaches and observed that Markov methods are the most suitable approach due to their flexibility. Guo and Yang [7] also highlighted that Markov analysis shows more flexibility and is the only technique that can describe dynamic transitions amongst different states of a system. A number of Markov models were evolved in recent years that combine the dynamic behaviour of safety instrumented systems and the impact of process demand inflicted on the SIS. A simple Markov model of SIS was first created by Bukowski [12] which included both dangerous detected and undetected failures in conjunction with the process demand. Jin et al. [23] further developed the preliminary model of Bukowski [12] and incorporated the repair rate of dangerous undetected failures for safety instrumented system in addition to inclusion of safe failure and repairs. In a separate attempt to extend the boundaries of Markov analysis for redundant systems, a Markov chain was generated by Liu et al. [24] for a redundant configuration, however, the dangerous detected failures were omitted to adopt the core characteristics of a specific safety system known as a pressure relief valve.

This paper aims to address this limitation by proposing a unique Markov chain to model the unavailability of redundant SIS subject to process demand which includes both dangerous detected and undetected failures. Therefore, this model is deemed as one step closer to analysing actual behaviour of the redundant configurations since dangerous detected failures influence unavailability and safety performance of the safety instrumented systems and cannot be omitted in generic SIS architectures. The model available in Jin et al. [23] is extended further by using Markov chains for their ability to model accurately and correctly a redundant safety instrumented system in low demand. The proposed model integrates the following parameters: diagnostic coverage, dangerous undetected failures, dangerous detected failures, repair rates, process demand and demand reset rate. The concurrent consideration of process demand and system failures (dangerous detected and dangerous undetected) offers a unique opportunity to analyse the SIS behaviour using an integrated model as opposed to verifying SIS architecture in isolation by exclusion of the process demand. In Section 2 we recall the principle of safety instrumented systems. Section 3 entails the mathematical preliminaries and consists of basic elements required for reliability modelling. Section 4 is devoted to the Markov models of simple and redundant safety instrumented systems followed by a numerical analysis presented in Section 5. Applications of the proposed models are discussed in Section 6 based on the results obtained, and concluding remarks are drawn at the end of this section.

2. Safety instrumented systems

2.1. Definition & key parameters

The primary objective of a SIS is to bring the system it supervises to a safe position i.e. in a situation where it protects people, environment and/or asset when the equipment under control (EUC) deviates from its design intent into a hazardous situation and results in an unwanted consequence (e.g. loss of containment leading to explosion, fire, etc.). SISs are frequently utilised across process industry to prevent the occurrence of hazardous events or to mitigate the consequences of undesirable events. A SIS may execute one or multiple safety instrumented functions (SIFs) to attain or maintain a safe state for the EUC (e.g. equipment, system etc.) the SIS is protecting against a specific process demand [8].

A SIS is a system consisting of any combination of sensors, logic solvers and final elements for the purpose of taking the supervised process to a safe state when predetermined design conditions are violated [13,25]. A SIS (or SIS subsystem) is recognised to have a *koon* configuration when k units of its n total units have to function to provide the required system function. Typical SIS configurations comprised of 1oo1, 1oo2, 1oo3, and 2oo3 [22]. In this article, only the two first configurations are considered, a 1oo1 system (i.e. a single unit) and a 1oo2 system. This demarcation is established because we believe that the main features of our new model will be illustrated by these simple systems. The Markov models of systems with more components will be complex and the main features of the approach will easily disappear in the technical calculations. Another reason for this delimitation is that the aforementioned systems have been thoroughly assessed with other approaches [1,26], therefore facilitating comparison.

2.2. Low demand vs high demand

Two separate modes of SIS operation comprised of low demand and high demand are outlined by IEC 61508 [1] based on two main criteria: (1) the frequency at which the SIS is expected to operate in response to demands, and (2) the anticipated time interval that a failure may remain hidden, taking cognisance of the proof test frequency. A SIS is in low demand mode of operation if the demand is less than or equal to 1 per year and in high demand mode in other situations [1,27]. The demand rate for a SIS may vary from continuous to very low (i.e. infrequent demands) and the duration of each demand may fluctuate from instantaneous up to a rather long period (e.g. hours). High demand systems are different from low demand systems, and the same analytical techniques can normally not be applied to all systems in various modes of operations. FTA and analysis based on RBD are generally not suitable for high demand systems when the duration of demands is significant. Several authors have indicated that Markov methods are best suited for analysing both high demand and low demand systems [24].

Despite the clear distinction between the high demand and the low demand mode of operation, there are still some underlying issues that cause confusion and problems in the quantification of SIS unavailability and safety performance [28]. As such, instead of drawing a clear boundary between low demand mode and high demand mode of operation, some authors suggest to incorporate the rate of demands into the analysis of safety instrumented systems [10,12,28].