ISA Transactions ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

ISA Transactions

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

Reliability modelling of redundant safety systems without automatic diagnostics incorporating common cause failures and process demand

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

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

ARTICLE INFO

Article history:
Received 2 October 2016
Received in revised form
9 May 2017
Accepted 11 September 2017

Keywords:
Markov analysis
Safety instrumented systems
Common cause failure
Process demand
Hazardous event frequency

ABSTRACT

Redundant safety systems are commonly used in the process industry to respond to hazardous events. In redundant systems composed of identical units, Common Cause Failures (CCFs) can significantly influence system performance with regards to reliability and safety. However, their impact has been overlooked due to the inherent complexity of modelling common cause induced failures. This article develops a reliability model for a redundant safety system using Markov analysis approach. The proposed model incorporates process demands in conjunction with CCF for the first time and evaluates their impacts on the reliability quantification of safety systems without automatic diagnostics. The reliability of the Markov model is quantified by considering the Probability of Failure on Demand (PFD) as a measure for low demand systems. The safety performance of the model is analysed using Hazardous Event Frequency (HEF) to evaluate the frequency of entering a hazardous state that will lead to an accident if the situation is not controlled. The utilisation of Markov model for a simple case study of a pressure protection system is demonstrated and it is shown that the proposed approach gives a sufficiently accurate result for all demand rates, durations, component failure rates and corresponding repair rates for low demand mode of operation. The Markov model proposed in this paper assumes the absence of automatic diagnostics, along with multiple stage repair strategy for CCFs and restoration of the system from hazardous state to the "as good as new" state.

1. Introduction

Safety systems are widely used to respond to hazardous events e.g. high pressure, high temperature, gas release etc and to mitigate their consequences to humans, the environment, and plant/financial assets. A safety system should provide an independent layer of protection by implementing the safety function through various techniques. In this regard Safety Instrumented Systems (SISs) have acquired specific attention in hazardous industries due to their prominent role in preventing undesirable events. The required functionality and reliability of a safety system are usually deduced from overall hazard and risk analyses. Without adequate design, fabrication, installation, construction, commissioning and maintenance the safety system may fail to provide the necessary risk reduction. Hence, a number of standards and guidelines have been developed to assist in designing and implementing safety systems. One such standard is IEC 61508 [1], that outlines key requirements to all phases of the SIS life cycle of Electric, Electronic and Programmable Electronic Systems (E/E/PES). The principles introduced in this generic standard are also reflected in its sectorial standards, such as IEC 61511 [2] for the process industry.

The SIS performance must be verified using a suitable methodology. No specific technique is recommended in IEC 61508 or IEC 61511, although some of these are cited in their appendices. Amongst these methods proposed for analysing the SIS reliability are Simplified Equation (SE) [1,3], Reliability Block Diagram (RBD) [4,5], Fault Tree Analysis (FTA) [6,7] and Markov Analysis [8–10]. More recently, Petri Nets (PN) approach has also been introduced to model the SIS reliability [11]. A comparison of these techniques conducted by Rouvroye and Brombacher concludes that Markov analysis covers most aspects for quantitative safety evaluation [12]. Furthermore, Guo and Yang [4] highlighted that Markov analysis shows more flexibility and is the only technique that can describe dynamic transitions among different system states. Jin et al. [13] utilised Markov analysis to calculate hazardous event frequency (HEF), which also relates to the safety performance of SIS. Innal [14] investigated the performance of different modelling approaches and concluded that Markov methods are the most suitable, predominantly due to their flexibility (see also [9,15]). Although Markov analysis is one of the most comprehensive

* Corresponding author.
E-mail addresses: Siamak.Alizadeh@hotmail.co.uk (S. Alizadeh), s.sriramula@abdn.ac.uk (S. Sriramula).

http://dx.doi.org/10.1016/j.isatra.2017.09.007
0019-0578/

Nomenclature

P_i	steady state probability for state i
τ	proof test interval
$p_{ij}(t)$	system transition probability from state i to state j
q_{ij}	transition rate from state i to state j
β	total common cause failure factor
β_D	detected common cause failure factor
β_U	undetected common cause failure factor
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
λ_S	safe failure rate
λ_{SD}	safe detected failure rate
λ_{SU}	safe undetected failure rate
λ^C	common cause failure rate
λ^I	independent failure rate
λ^I_{DD}	dangerous detected independent failure rate
λ^C_{DD}	dangerous detected common cause failure rate
λ^I_{DU}	dangerous undetected independent failure rate
λ^C_{DU}	dangerous undetected common cause failure rate
λ^I_{SD}	safe detected independent failure rate
λ^C_{SD}	safe detected common cause failure rate
λ^I_{SU}	safe undetected independent failure rate
λ^C_{SU}	safe undetected common cause failure rate
λ^T	total failure rate
μ	component repair rate
μ_{DD}	dangerous detected repair rate
μ_{DE}	demand reset rate
μ_{DU}	dangerous undetected repair rate
μ_S	safe repair rate
μ_T	renewal rate
π_i	steady state probability of system in state i
DC	diagnostic coverage rate
$P(t)$	transition matrix at time t
$P_i(t)$	probability of system in state i at time t
Q	transition rate matrix
r	states of stochastic process

techniques used today, it is very time consuming to construct the model for a large and complex system manually as the number of states increases with the number of system components. Moreover, it is very difficult to handle large Markov models as they require a substantial amount of calculation. Therefore, it has been widely recognised that the design of Markov models for a complex SIS architecture is challenging and error prone [13].

Bukowski [9] presented a simple Markov model of SIS that explicitly incorporates process demand. This model includes both dangerous detected and undetected modes of failure in conjunction with process demand, imposed by process system. Jin et al. [13] further developed the model created by Bukowski [9] and incorporated the safe failure rate for safety instrumented system and repair rate for dangerous undetected failures. A Markov chain was generated by Liu et al. [16] for a 1oo2 system which extends the application of Markov analysis to redundant configurations subject to process demand. The Markov transition diagram introduced by Liu et al. [16] overlooks the impact of CCF by exclusion, imposing a deficiency on the reliability model for 1oo2 systems. In this paper we intend to address this limitation by embedding CCF for a 1oo2 redundant structure as well as other established component failure modes, in addition to incorporating process demand. Furthermore, this model is deemed as one step closer to analysing actual behaviour of the redundant configuration since CCF influences reliability and safety performances of the safety systems and cannot be discarded.

The main objective of the present article is to explore the relationships between the CCF and SIS reliability and safety performance when incorporating both the demand rate and the demand duration by using Markov methods. Typical SIS configurations consist of 1oo1, 1oo2, 1oo3 and 2oo3 [14]. In this study, only the first two configurations are considered, a 1oo1 safety system (i.e. a single unit) and a 1oo2 redundant safety structure. The Markov models of systems with more components will be complex and the salient features of the approach will easily disappear in the technical calculations. The reliability model developed as part of this research is based on Markov chains for their ability to model safety systems precisely and correctly in low demand. The paper proposes the integration of the following parameters: dangerous undetected failures, common cause failure, safe failures, repair rates, process demand and demand duration.

The proposed reliability model is flexible to accommodate different repair strategies. In this paper only the multiple stage repair strategy of CCF has been considered however, where single stage repair for CCF is possible (e.g. removal of the vibration source, unblocking the common header etc.) the proposed Markov chain can be re-arranged to accommodate an alternative repair strategy of redundant configuration. The remainder of this article is organized as follows: Section 2 discusses the modelling considerations and Section 3 consists of SIS fundamentals. Section 4 is devoted to Markov Analysis and Section 5 entail the analysis of 1oo1 and 1oo2 safety systems followed by a numerical analysis studied in Section 6. Applications of the developed model are discussed in Section 7 based on the results obtained, and conclusions are outlined at the end of this section.

2. Modelling considerations

2.1. Safe state

The primary objective of SIS design is to lead the Equipment Under Control (EUC) to a safe state in response to a demand. As the EUC have various modes of operations e.g. start-up, shutdown, normal operation etc., it is not always straightforward to define the safe state. In some cases, the safe state is to retain the original state of the EUC prior to occurrence of the demand such as a Dynamic Positioning (DP) system. In other cases, the safe state corresponds to cease the operation of EUC e.g. when equipment is overheated etc. It is common that the EUC remains in the safe state after the SIS has responded to a demand in the process hydrocarbon industry. The SIS is only reset back to the original state upon deciding to restart the EUC. For instance in the event of a loss of containment e.g. gas leakage, the Emergency Shutdown (ESD) system ceases the process by closing dedicated Emergency Shutdown Valves (ESDVs). The ESD system maintains this state, until the remedial action for repair of the leak point has been undertaken and the operators have decided to restart the EUC. When the safe state is defined, the next step is to design SIS, taking cognisance of “fail-safe” position. This means that upon foreseeable SIS failures such as loss of power supply etc, the SIS automatically leads the EUC to a safe state.

2.2. Hazardous event

A hazardous event is defined as a significant deviation from the normal operating conditions that may, if not controlled develop into an accident [5]. As discussed previously, a preventative SIS

Please cite this article as: Alizadeh S, Sriramula S. Reliability modelling of redundant safety systems without automatic diagnostics incorporating common cause failures and process demand. ISA Transactions (2017), http://dx.doi.org/10.1016/j.isatra.2017.09.007