Safety Science 80 (2015) 264–273

Contents lists available at ScienceDirect

Safety Science

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

A reliability model for safety instrumented system

Rachid Ouache [a,*], Muhammad Nomani Kabir [b,1], Ali A.J. Adham [c,2]

[a] Faculty of Engineering Technology, University Malaysia Pahang, 26300, Malaysia
[b] Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, 26300, Malaysia
[c] Faculty of Industrial Management, University Malaysia Pahang, 26300, Malaysia

ARTICLE INFO

Article history:
Received 14 May 2015
Received in revised form 6 July 2015
Accepted 3 August 2015

Keywords:
Reliability
Safety Integrity Function (SIF)
Atmospheric element
Safety assessment
Probability of failure on demand

ABSTRACT

Safety analysis in the companies is an important issue besides the quality, productivity and profitability. Safety integrity function in many industries is based on safety instrumented systems. Uncertainty is the main problem of safety analysis. In this paper, a new mathematical model is developed to compute the probability of failure on demand (PFD) following the three steps. First, KHALFI (Characteristics of Hazard Analysis based on Logic Frequency Initiative) mathematical model is formulated to identify the real PFD at any geographical location considering five intermediate factors: temperature, humidity, pressure, wind speed and time which can affect the PFD. Second, probability binary state (PROBIST) is used to precise the values of PFD. Third, Bowtie method is employed to carry out the safety analysis for examining the safety of some scenarios by determining the PFD of safeguards, where new classification for the safety integrity level is proposed. Finally, Simulink model is developed implementing the proposed model to facilitate the automatic computation and analysis. Results indicate that all the atmospheric elements are significant and need to be taken into consideration to attain the best reliability in the calculation of PFD. The effectiveness of the proposed model gives the opportunity for the analysts to conduct safety analysis at any geographical location.

1. Introduction

Safety assessment is nowadays an integral part of the strategy of a company apart from quality, productivity and profitability. Understanding the process of safety is the first step for minimizing the level of risk. Different mechanical instruments such as basic process control system (BPCS) and safety instrumented system (SIS) are used to protect the company from undesirable events, where SIS is among the best instruments used to reduce the severity of consequences (Mkhida et al., 2014). Three essential parts: sensor, logic solver and final element are necessary to carry out SIS functions (IEC 61511-1, 2003; Liu and Rausand, 2013; Ouache and Adham, 2014). Furthermore, many companies especially oil and gas industries rely on the SISs to protect the workers, environment and properties in case of occurrence of undesirable events (Innal et al., 2014; Jin et al., 2015).

Reliability is the most important issue related to the SIS to prove its compliance and effectiveness. The uncertainty is the main problem in SIS analysis, where the uncertainty of input parameters gives the erroneous output. Two kinds of uncertainty appear in the analysis. First, randomness (aleatory) which is due to the natural variability of system. Second, imprecision (epistemic) which occurs due to the lack of knowledge on the system can be improved if the knowledge is available.

Safety integrity level (SIL) is the unit used to measure the level of safety instrumented functions (SIF) as described in IEC 61508 standard (IEC 61508-6, 1997; Lundteigen and Rausand, 2007). Many methods under three different approaches i.e., qualitative, quantitative and semi quantitative are proposed to determine the SIL (Baybutt, 2012). IEC 61508 standard mentioned that the quantitative method which is based on probabilistic evaluation is the best among the three methods. Risk graph is one of the methods proposed to determine the SIL (Baghaei, 2013). IEC 61508 (IEC 61508-1, 1997) and IEC 61511 (IEC 61511-1, 2003) are two standards used to measure the SIL of an SIS in the industries related to oil, gas, chemicals and electricity (Lundteigen and Rausand, 2007). The SIS is an essential instrument in modern industries to reduce the level of consequences from the undesirable events (Innal et al., 2015).

* Corresponding author at: Faculty of Engineering Technology, University Malaysia Pahang, Gambang 26300, Kuantan, Pahang, Malaysia. Tel.: +60 189062499.

E-mail addresses: drrachid_ouache@yahoo.fr (R. Ouache), nomanikabir@ump.edu.my (M.N. Kabir), aliadham12@yahoo.com (A.A.J. Adham).

[1] Tel.: +60 109154807.
[2] Tel.: +60 95492447.

http://dx.doi.org/10.1016/j.ssci.2015.08.004
0925-7535/

Fig. 1. Subsystems of safety instrumented system.

Probability of Failure on Demand (PFD) and failure data are the two significant factors used to study the safety barriers. Preventive (proactive) and protective (reactive) are the two kinds of safeguards to reduce the probability of undesirable events where preventive safeguards are used to reduce the risk and protective safeguards, to decrease the consequences of risk (American Institute of Chemical engineers, 1994; American Institute of Chemical engineers, 2001; Liu and Rausand, 2011; Ouache and Adham, 2014). However, the investigators raised the concern that some causes which may lead to the accidents in the industries are still not taken into consideration (Pekalski et al., 2005).

In this study, a new mathematical model following quantitative approach is developed to solve the problem of uncertainty in an SIS as follows. First, KHALFI is formulated to compute the PFD values at any geographical location. Second, the probability binary state (PROBIST) is used to determine the range of PFD. Third, Bowtie method is incorporated to carry out safety analysis for evaluating the PFD of safeguards where new classification for the SIL is proposed. Finally, Simulink model is developed implementing the proposed model.

2. Safety assessment and reliability

Safety assessment and reliability are the most important elements to design, construct and operate the safety instrumented systems (SISs) for a specific application and reliability requirements (Mary Ann Lundteigen Safety, 2009; Ouache and Adham, 2014). Reliability is the probability of proper operation of a system for a specified period of time (Kondakci, 2015). Unavailability is defined as the probability of failure of a system during a specified period of time (Verma et al., 2007). The rate of equipment failures is generally calculated by the ratio of the number of equipment failures to 1 million operating hours (or 1000 demands) (American Institute of Chemical engineers, 1989). The main aim of SIS is to react with hazardous events such as high pressure, gas leakage or any other unwanted event. The capability of SIS to get tolerable risk level is called the *safety integrity* (Innal et al., 2015). The value of average probability of failure on demand (PFD_{AVG}) of an SIS is calculated using the PFD values of one or more of input elements (sensors (SE) or transmitters), one or more logic solvers (LS) (e.g., programmable logic controllers, relay logic systems) and one or more final elements (FE) (e.g., safety valves, circuit breakers) (see Fig. 1) (Lundteigen and Rausand, 2007; Hokstad, 2014) as follows:

$$PFD_{AVG} = \sum PFD_{SE} + \sum PFD_{LS} + \sum PFD_{FE} \quad (1)$$

Probability of dangerous failure per hour (PFH) is measured for high demand mode in case of continuous operations such as with a basic process control system (BPCS). The aim of PFD and PFH is to keep the residual risk at an acceptable level (Chebila and Innal, 2015).

Markov model and reliability block diagrams are the most important techniques in quantitative method used to analyze the hardware safety integrity for the SIS whereas both approaches provide similar results (IEC 61508-6, 1997). K-out-of-N (KooN) is the configuration of SIS with N subsystems where K is the number of subsystems of the SIS which must be functional to allow the SIS work. Different configurations for SIS are available such as 1oo1, 1oo2, 1oo3 and 2oo3 (Liu and Rausand, 2011).

3. Determination of safety integrity level

The determination of the target safety integrity level (SIL) is an essential step to analyze the safety lifecycle (Chang et al., 2015). Safety instrumented systems (SISs) are classified as low-demand when the frequency of demands is not more than one per year and not more than two per year in case of proof and as high-demand when the number is more than two times per year (Liu and Rausand, 2011). New classification for the safety integrity level (SIL) based on the values of PFD, safety availability (SA) and probability of dangerous failure per hour (PFH) is proposed in Table 1 in order to increase the reliability of SIL.

Table 1
Reliability of safety integrity level.

Safety integrity level (SIL)	Probability of a failure on demand (PFD)	Safety availability (SA) (%)	Probability of dangerous failure per hour (PFH)
SIL 1	$[5 \cdot 10^{-1} \quad 1]$	[50 0]	$[5 \cdot 10^{-6} \quad 1 \cdot 10^{-5}]$
SIL 2	$[1 \cdot 10^{-1} \quad 5 \cdot 10^{-1}]$	[90 50]	$[1 \cdot 10^{-6} \quad 5 \cdot 10^{-6}]$
SIL 3	$[5 \cdot 10^{-2} \quad 1 \cdot 10^{-1}]$	[95 90]	$[5 \cdot 10^{-7} \quad 1 \cdot 10^{-6}]$
SIL 4	$[1 \cdot 10^{-2} \quad 5 \cdot 10^{-2}]$	[99 95]	$[1 \cdot 10^{-7} \quad 5 \cdot 10^{-7}]$
SIL 5	$[5 \cdot 10^{-3} \quad 1 \cdot 10^{-2}]$	[99.5 99]	$[5 \cdot 10^{-8} \quad 1 \cdot 10^{-7}]$
SIL 6	$[1 \cdot 10^{-3} \quad 5 \cdot 10^{-3}]$	[99.9 99.5]	$[1 \cdot 10^{-8} \quad 5 \cdot 10^{-8}]$
SIL 7	$[5 \cdot 10^{-4} \quad 1 \cdot 10^{-3}]$	[99.95 99.9]	$[5 \cdot 10^{-9} \quad 1 \cdot 10^{-8}]$
SIL 8	$[1 \cdot 10^{-4} \quad 5 \cdot 10^{-4}]$	[99.99 99.95]	$[1 \cdot 10^{-9} \quad 5 \cdot 10^{-9}]$
SIL 9	$[5 \cdot 10^{-5} \quad 1 \cdot 10^{-4}]$	[99.995 99.99]	$[5 \cdot 10^{-10} \quad 1 \cdot 10^{-9}]$
SIL 10	$[1 \cdot 10^{-5} \quad 5 \cdot 10^{-5}]$	[99.999 99.995]	$[1 \cdot 10^{-10} \quad 5 \cdot 10^{-10}]$