Journal of Loss Prevention in the Process Industries 41 (2016) 31–39

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams

Grzegorz Kaczor, Stanisław Młynarski, Maciej Szkoda*

Cracow University of Technology, Faculty of Mechanical Engineering, Jana Pawla II Str. 37, 31-864 Krakow, Poland

ARTICLE INFO

Article history:
Received 18 December 2014
Received in revised form
28 January 2016
Accepted 5 March 2016
Available online 9 March 2016

Keywords:
Functional safety
Safety integrity level
Monte Carlo simulation
Reliability block diagrams

ABSTRACT

The paper presents functional safety problems of technical systems. It aims to verify the safety integrity level for a selected integrated safety system. The paper provides a comparative analysis of the safety integrity level with the application of the Monte Carlo simulation and Reliability Block Diagram (RBD) methods. Additionally, a solution is proposed to section off, from the logical structure, so called voting zones to significantly reduce the risk of causing false alarms. The calculations were preceded with a review of existing studies of functional safety in extensive technical systems. The verification was done following the requirements of IEC 61508, which is a commonly accepted standard in the field of functional safety of programmable electronic and control engineering systems.

1. Introduction

Machines and technical equipment functioning in modern industry are, in many cases, controlled by automatic and electronic systems (Calixto, 2012; Reliasoft Corporation, 2007; Smith, 2000). The growing responsibility of these systems for correct recognition of input signals and their processing requires methods to be developed in order to detect potential hazards. Despite a reduction in the number of accidents caused by technical factors of machines and equipment, negative consequences of such occurrences are increasingly serious. One of the measures aimed to improve the situation was the introduction of functional safety standards. The International Society of Automation resolved to adopt the IEC 61508 standard on *Functional safety of electrical/electronic/programmable electronic safety-related systems* (IEC, 2010a) intended to facilitate quantitative assessment of safety for programmable automation systems (Smith, 2000). Being a quantitative measure of technical systems' functional safety, the concept of Safety Integrity Level (SIL) makes it possible to determine the risk level limit relating to the occurrence of certain undesirable events. As a result of safety evaluation, the probability of dangerous failures on demand (PFD) or the probability of dangerous failures per hour (PFH) for the system is obtained.

There is a great variety of methods for SIL verification, as described in IEC 61508-7. This paper verifies the integrated system's SIL level with the application of two calculation methods:

1. Monte Carlo simulation:
   – with no voting zones,
   – with voting zones, and
2. Reliability Block Diagrams (RBDs).

The calculation results obtained using Monte Carlo simulation (IEC 61508-7, section B.6.6.8) were compared with the results obtained with the application of the RBD method, recommended and described in IEC 61508 (IEC, 2010d). The research demonstrated the effectiveness of the Monte Carlo method in SIL verification. Moreover, as the analysis of the current condition demonstrated, the operation of complex safety systems consisting of a high number of elements, is burdened with numerous technical, organisational and economic problems. One of them relates to false alarms which generate considerable financial losses involved in the stoppage of the supervised process. Through the application of the 2-out-of-N reliability structure and the sectioning off of so-called voting zones, the paper proposes an innovative system for reducing the number of unreasonable alarms.

2. Functional safety analysis in the light of existing studies

The complexity of reliability and functional safety of technical

* Corresponding author.
E-mail address: maciej.szkoda@mech.pk.edu.pl (M. Szkoda).

http://dx.doi.org/10.1016/j.jlp.2016.03.002
0950-4230/

systems and the increase in their importance have resulted in the elaboration of numerous research studies on this subject (Fuchs and Zajicek (2013); Han and Weng, 2010; Hietikko et al., 2011; Jo and Ahn, 2005; Kaczor, 2012; Khalii et al., 2012; Langeron et al., 2008; Lundteigen and Rausand, 2007; Marszal, 2003; Misumi and Sato, 1999; O'Conor et al., 2000; Smith et al., 2011).

Paper (Beugin et al., 2007) presents a quantitative probabilistic model which makes use of SILs to evaluate the safety of a selected transport system. The Monte Carlo simulation method, amongst others, was used to evaluate the system's safety. In Młynarski and Oprzędkiewicz (2012), the authors describe a comprehensive approach to the problem of technical objects' safety. They provide algorithms and systemic solutions to ensure operational safety of technical objects. The authors of Młynarski and Pałka (2011) present the use of programmes with the application of simulation methods to analyse the safety of vehicles. In turn, the authors of Guo and Yang (2007) describe a method of evaluating functional safety based on a structural reliability analysis. It was proven that the results obtained using this method compare with the calculation results obtained according to the IEC 61508 standard. The methods available for verifying the SILs according to IEC 61508 include Markov's analysis which, for complex technical systems, is time-consuming due to the number of possible states of the stochastic process (Rouvroye and Wiegerinck, 2006). The authors of Knegtering and Brombacher (1999) claim that the number of such states for high redundancy systems may be between 500 and 600. The said paper presents Markov's model where a maximum of 48 states are distinguished. Another method of determining the SILs using a failure tree and an AND gate with priority is presented in Misumi and Sato (2007). Also, new terms referring to the operation of programmable electronic systems (new modes of operation) are proposed. It is worthwhile to mention paper (Lundteigen and Rausand, 2009) where the authors take a holistic approach to the main requirements for RAMS analysis for an integrated safety system. They combine aspects of RAMS analysis included in IEC 61508 with Murthy's model, claiming that it supplements the structure of safety life cycle as provided for in the aforementioned standard. As an example of their approach to the problem, they use an inshore oil and gas extraction system.

Functional safety analysis is often supported by additional system methods. These include e.g. HARA and FMEDA, used in Kim and Kim (2013) which deals with a verification of functional safety of a flame scanner. The HARA analysis is applied to determine the safety requirements for the analysed system, whilst FMEDA is used to evaluate the SIL in an eight-step reliability verification process. Each element is assigned a variety of possible failures and their impact on system operation. Failure mechanisms and their intensity coefficients are paired off with system elements. The ability to detect these failures is also determined.

In turn, paper (Khali et al., 2012) proposes a method of improving functional safety for a natural gas distribution system. The concept consists in the use of LOPA and Fuzzy Logic methods to eliminate accidents in the gas industry and keep the SIL at an acceptable level. The proposed solution was checked in a system of medium and high risk levels of hazard occurrence, and the results obtained prove its considerable effectiveness. The author of Kosmowski (2006) presents a review of selected problems concerning functional safety analysis, in accordance with the current standard IEC 61508. The significance of the probabilistic approach to quantitative analyses in verifying SIL levels is described. The paper also describes certain aspects of functional safety in detecting flammable and toxic gases with reference to the assumptions of standard CENELEC prEN 50402.

International standard IEC 61508 which provides general information for the design and implementation of functional safety systems, does not take account of human and organizational factors (Smith et al., 2011). The authors of Schönbeck et al. (2010) present their own concept of verifying the SILs and prove that with those factors taken into consideration the functional safety of technical systems might be improved.

3. The basis for safety evaluation according to IEC 61508

IEC 61508 is a commonly accepted standard in the field of functional safety of programmable systems. Electrical, electronic and programmable electronic equipment (E/E/PE) perform more and more functions to ensure the required safety level. Safety systems, consisting of a great number of elements, usually have complex reliability structures, such as k-out-of-n redundancy or with a sliding reserve, which, from the practical point of view, complicates precise determination of potential failure types and the performance of an analysis in different operation conditions. The IEC 61508 standard provides detailed guidelines enabling realisation and evaluation of the safety system whose task is to reduce the failure risk to a minimum acceptable level, according to the ALARP (As Low As Reasonably Practicable) principle (IEC, 2010b). An important consideration for any safety related system or equipment is the level of certainty that the required safe response or action will take place when needed. This is normally determined as the probability that the safety loop will fail to act as and when it is required to and is expressed as a probability. In accordance with IEC 61508, the calculations for the safety system depend on the kind of operations the system performs (Rouvroye and Wiegerinck, 2006). The standard applies both to safety systems operating on demand, such as an emergency shut-down system, and to systems operating continuously or in high demand, such as the process control system:

- low demand operation – when the safety system is on demand no more frequently than once a year and no more frequently than twice the periodical tests,
- continuous or high demand operation – when the safety system is on demand more frequently than once a year and more frequently than twice the periodical tests.

For a safety loop operating in the demand mode, the relevant factor is the PFD_{avg}, which is the average probability of failure on demand. For a continuous or high demand mode of operation, the probability of a dangerous failure per hour (PFH) is considered rather than PFD_{avg}. IEC 61508 requires that reliability targets for the safety instrumented systems (SIS) be defined and demonstrated (Schönbeck et al., 2010). The reliability targets are assigned to each safety instrumented function (SIF) that is implemented into the SIS. A simplified safety instrumented system is illustrated in Fig. 1, where according to IEC 61508, three subsystems are distinguished to provide the selected safety function:

- detector subsystem (DS) providing information on specific parameters from the area covered by a safety system performing specific safety functions,
- logical subsystem (LS) which, according to the programmed logics, performs logical operations on detector signals and generates, as a result, the appropriate signal for a given safety function, transferring it to the systems which control the performing elements,
- performing subsystem (PS) which, if required, does operations required for the safety function concerned.

Determining the PFH of each of the subsystems and their summing up yields (according to IEC 61508-6) the PFH of the whole