Journal of Loss Prevention in the Process Industries 32 (2014) 254–264

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Reliability analysis of safety-instrumented systems operated in high-demand mode

Yukun Wang [a, b, *], Marvin Rausand [b]

[a] College of Management and Economics, Tianjin University, NO 30072 Tianjin, China
[b] Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

ARTICLE INFO

Article history:
Received 27 January 2014
Received in revised form
17 September 2014
Accepted 17 September 2014
Available online 18 September 2014

Keywords:
Safety-instrumented systems
Reliability
High-demand
PFH

ABSTRACT

The international standards IEC 61508 and IEC 61511 give safety integrity requirements to safety-instrumented systems (SISs) that are used in the process industry. A SIS performs one or more safety-instrumented functions (SIFs). IEC 61508 distinguishes between SIFs operated in low-demand and high-demand/continuous mode, whereas IEC 61511 distinguishes between demanded and continuous mode of operation. In the past, almost all attention has been paid to low-demand SIFs, and this is reflected in IEC 61511, the available guidelines, and the scientific literature. Recently, however, suppliers of SISs to the process industry have been met with safety requirements to SIFs operated in high-demand and continuous mode. This paper intends to help suppliers and reliability analysts who are familiar with the mathematical formulas in IEC 61508-6 for safety integrity assessment of low-demand SIFs to verify the safety integrity of SIFs in high-demand and continuous mode. This is done by highlighting the similarities and differences between the required approaches and by presenting two new sets of approximation formulas for the PFH of general *koon*:G voted groups. One set of PFH formulas extends the IEC formulas for PFH based on the ideas applied in IEC 61508-6. The other set of PFH formulas is derived considering the risk contribution also from DD-failures when the demand rate is high. The results of the IEC formulas of PFH and the two new sets of PFH formulas are compared and discussed.

1. Introduction

Safety-instrumented systems (SISs) are widely used in the process industry to protect humans, the environment, and material assets against *hazardous events*, such as gas leaks and runaway reactions. The risk related to a specific hazardous event in a process may be illustrated by a bow-tie diagram (Rausand, 2011) as shown in Fig. 1, which illustrates the possible causes and consequences that are related to the hazardous event. A SIS may be used as a *proactive* safety barrier to prevent the hazardous event from occurring, or as a *reactive* safety barrier to prevent or mitigate the consequences of the hazardous event. A proactive barrier is sometimes called a frequency-reducing barrier, whereas a reactive barrier is called a consequence-reducing barrier.

A SIS generally consists of three parts: a sensor subsystem, a logic solver subsystem, and a final element subsystem. The sensor subsystem detects the onset of possible hazardous situations, the logic solver subsystem decides what to do by evaluating the information from the sensor subsystem, and the final element subsystem takes action through safety valves, circuit breakers, and so on.

To provide a specified risk reduction, the SIS must fulfill certain safety requirements. A number of standards and guidelines have been issued, which define the required safety-instrumented functions (SIFs), establish their *safety integrity levels* (SILs), and give guidance on how to implement them to achieve the desired functional safety. The most important of these standards is IEC 61508 (IEC 61508, 2010), which is a generic standard specifying the functional safety requirements for SISs. IEC 61508 (IEC 61508, 2010) serves also as an overall guideline for the development of sector-specific safety standards, such as IEC 61511 (IEC 61511, 2003) for the process industry and IEC 62061 (IEC 62061, 2012) for machinery systems.

IEC 61508 and the associated sector-specific standards adopt a risk-based approach to determine the safety requirements of a SIS in a safety life-cycle. Risk assessments are carried out to determine the process risk and the necessary risk reduction that should be

* Corresponding author. College of Management and Economics, Tianjin University, No. 92, Weijin Road, Nankai District, Tianjin, China.
E-mail address: yukunwang89@gmail.com (Y. Wang).

http://dx.doi.org/10.1016/j.jlp.2014.09.007
0950-4230/

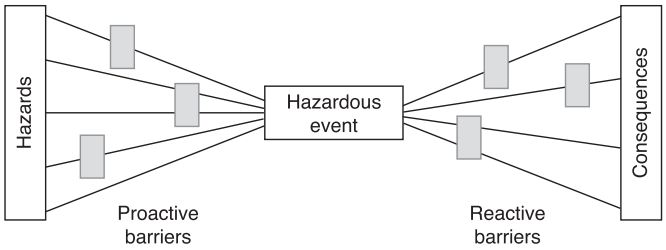

Fig. 1. Bow-tie diagram for a hazardous event with proactive and reactive safety barriers.

achieved by one or more SISs. Accordingly, the safety requirements of the SIS, including safety functional requirements and safety integrity requirements, are derived to achieve the necessary risk reduction. The safety functional requirements specify which SIFs are to be performed by the SIS, and the associated safety integrity requirements specify the required reliability performance of the SIF in terms of a SIL. A SIS may perform one or more SIFs to achieve the required functional safety. SIFs are classified according to how often they are demanded. IEC 61508 distinguishes between low-demand, high-demand, and continuous mode safety functions, where the boundary between low-demand and high-demand/continuous mode is the demand rate of once per year.

IEC 61511 distinguishes between two modes of operation: demanded mode and continuous mode. SIFs operating in demanded mode are mainly reactive barriers, while SIFs operating in continuous mode are mainly proactive barriers, see Fig. 1.

In the process industry, most attention has been paid to demanded SIFs, and especially low-demand SIFs. This is reflected in the available publications where the vast majority treat problems related to low-demand SIFs (Dutuit et al., 2008; Hokstad and Corneliussen, 2004; Innal et al., 2010; Jin et al., 2011, 2012; Langeron et al., 2008; Liu and Rausand, 2013; Lundteigen and Rausand, 2009; Rausand, 2011; Rausand and Høyland, 2004). The same focus is also reflected in the standards and IEC 61511 treats only demanded SIFs with the main focus on the low-demand mode of operation.

Recently, suppliers of SISs to the offshore oil and gas industry have been met with requirements to document the safety integrity of SIFs in high-demand and continuous mode, for example for machinery systems. Many suppliers have procedures and competence related to safety integrity assessment of low-demand SIFs, but limited experience with high-demand SIFs (IEC 61511, 2003). IEC 61511 does not provide much help on SIFs operated in high demand mode, but this topic is treated in slightly more detail in IEC 62061 for machinery systems. Recently, some attention has been paid to high-demand systems in scientific publications (Innal, 2008; Innal et al., 2010; Jin et al., 2013; Rausand, 2014), but this field is still immature.

Several reliability analysts find it difficult to follow the recommendations of IEC 61508 when the demand rate is close to the boundary-point (i.e., once per year) between low-demand and high-demand mode. By using the approximation formulas suggested in IEC 61508-6, they may be able to meet the reliability requirements for a specified SIL by using the PFD_{avg}, but may not be able to meet the same requirements if using PFH (or vice versa). PFD_{avg} is the average probability of a dangerous failure on demand of the SIF, and PFH is the average frequency of dangerous failures of the SIF per hour (IEC 61508, 2010; Rausand, 2014). Both reliability measures are further discussed in the current paper. It is therefore a reason to question whether the requirements are appropriate when the demand rate approaches once per year – or, maybe the approximation formulas in IEC 61508-6 are not sufficiently accurate in this case? The approach outlined in IEC 61508-6 does not solve this challenge, since we may get different SILs depending on which safety performance measure we choose.

The objectives of this paper are to (i) compare the requirements to risk assessment and safety requirements for low-demand and high-demand/continuous SIFs in IEC 61508, IEC 61511, and IEC 62061, (ii) explore the consistency of PFD_{avg} and PFH in determining the SIL of a SIF, and (iii) derive two sets of approximated PFH formulas based on different assumptions, and discuss their strengths and weaknesses.

The rest of the paper is organized as follows. The hazard and risk assessment of the protected system which aims at deriving safety requirements of SIS is discussed in Section 2. In Section 3, the specified functional requirements and safety integrity requirements in low-demand and high-demand (continuous) mode are compared. In Section 4, the available modeling approaches to evaluate safety performance are listed and discussed to find whether the two performance measures have consistency in leading to the same SIL by using the approximated formulas presented by IEC 61508-6. In Section 5 and Section 6, two sets of approximated PFH formulas are derived, respectively. The results of these two sets of formulas are compared with the IEC formulas and discussed in Section 7. Finally, concluding remarks are given.

2. Hazard and risk assessment

IEC 61508 and its sector-specific standards are risk-based, which means that reliability requirements to the SIFs have to be deduced from the results of a risk assessment of the process.

In the process industry, a hazard and risk assessment must be carried out to determine the safety requirements of each SIF. The hazards, non-hazardous operability problems, and potential demands are commonly identified through a hazard and operability (HAZOP) study, and the process risk is determined by a quantitative or semi-quantitative risk assessment (IEC 61511, 2003; Rausand, 2011) to derive the necessary risk reduction. Based on the evaluated process risk, the safety integrity requirements are determined and allocated to each SIF.

For machinery applications, the standard ISO 12100 (ISO 12100, 2010) gives guidance on risk assessment of machinery systems. The risk analysis is initiated by defining the physical and operational boundaries of the machinery system. The potential hazards, hazardous situations, and hazardous events are identified by using the checklists provided by the standard. For each hazardous situation, the risk is estimated through preliminary hazard analysis, failure modes, effects, or criticality analysis (FMECA), and/or fault tree analysis (FTA). Based on the results from the risk estimation, the risk is evaluated to decide which hazardous situation requires further risk reduction. The terminology used in the sector-specific standard IEC 62061 for machinery systems is different from the one used in IEC 61511; a SIS is called a safety-related control system (SRECS) and a SIF is called a safety-related control function (SRCF).

The approaches to hazard and risk assessment in IEC 61511 and IEC 62061 are comparable and we may use approximately the same methods to identify hazards and allocate SIL requirements to the various SIFs (SRCFs).

3. Safety requirements

Based on the hazard and risk assessment, safety requirements are determined and allocated to one or more SIFs and other risk reduction measures. The safety requirements to a SIF consist of two parts – the functional requirements and the associated safety integrity requirements to be achieved.