Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Optimization, a rational approach to SIL determination

Hamid Jahanian

Siemens, 160 Herring Road, Macquarie Park, NSW 2113 Australia

ARTICLE INFO

Article history:
Received 27 November 2016
Received in revised form 1 April 2017
Accepted 11 April 2017
Available online 27 April 2017

Keywords:
SIL determination
PFDavg
PFH
Cost benefit analysis
ALARP
Expected utility

ABSTRACT

In process industry, SIL determination is a risk assessment process through which target Safety Integrity Levels (SIL) are allocated to Safety Instrumented Functions (SIF). A target SIL represents the significance of the hazard against which the SIF protects the plant. This paper introduces new SIL determination methods by taking an optimization approach. Unlike the conventional methods, which are generally focused on calculating the gap between the existing and tolerable levels of risk, the methods introduced in this paper are aimed at optimizing the marginal cost or the benefit-cost ratio. By incorporating the cost factor into the SIL determination process, these methods deliver the most reasonably practicable solutions that can minimize the risk while taking into account the cost of solution. The new methods are formulated for corporate risk and the risk to community (i.e. ALARP). Both methods are derived for demand and continuous modes of SIF operation. Furthermore, a new Safety Index is introduced to combine the SIL and the average Probability of Failure on Demand (PFD) or Frequency of Failure per Hour (PFH). The application of the mathematical models is demonstrated through a practical example from power industry.

1. Introduction

In the process industry, Safety Integrity Level (SIL) is a discrete number between 1 and 4 which indicates the significance of a process-related hazard. The higher the SIL number, the riskier the hazard; and the riskier the hazard, the more effort needs to be made to protect against it. SIL is an attribute of Safety Instrumented Function (SIF)—the protection mechanism that needs to be established to protect against the hazard. In addition to the discrete scale of SIL, the reliability of a SIF may be represented by other measures in continuous scale, such as Probability of Failure on Demand (PFD), Risk Reduction Factor (RRF), and Frequency of Failure per Hour (PFH). The relation between PFD, RRF, PFH and SIL is defined in the functional safety standards, i.e. IEC61508 and IEC61511.

Determining the appropriate SIL (or PFD/RRF/PFH) is crucial from both SIF architectural and operational perspectives. A SIF with higher SIL typically requires a more complex hardware with lower failure rate. Higher SIL also entails more stringent engineering, operation and maintenance practices. In essence, SIL directly regulates the cost of the protection mechanism, i.e. the SIF. Unless an analysis is conducted to determine the right SIL, the design of the SIF may result in unnecessary costs, when the risk is overrated, or compromising safety if it is underrated. Such analyses are often referred to as SIL determination, SIL allocation or SIL study.

Cost is a fundamental reason for the necessity of SIL determination; however, what commonly is left out of such studies is the cost factor itself. The conventional SIL determination methods (IEC61508, 2011a; IEC61511, 2016a) are generally based on calculating the gap between the existing and tolerable risk levels, without taking into account the cost of solution. Questions such as "How costly a SIL2 solution is going to be?" or "Would it be still affordable, or reasonable, to aim at SIL2 even though SIL1 already fills the gap? " are not meant to be addressed by the typical SIL determination methods. The common perception is that a higher SIL always results in a larger cost and therefore there is no need to opt for higher SIL if the gap is already filled. While this assumption may generally be true, the conventional methods do not provide quantitative indications as to 'how costly' a solution can be, given its contribution to risk reduction. Therefore, using the conventional methods, one will not be able to estimate the effectiveness of each individual SIL option; nor one can compare the relative suitability of two SIL alternatives. Such methods may result in inadequate safety where a reasonable amount of further investment can lead to considerable reduction of risk.

Unlike the conventional methods, SIL determination can be looked at as a risk-related investment decision: depending on the target SIL

E-mail address: hamid.jahanian@siemens.com
http://dx.doi.org/10.1016/j.psep.2017.04.015

the value of investment varies, and depending on the investment the reliability of safety system and consequently the probability of accident will be affected. With this approach, the SIL determination problem can be redefined as a cost-benefit optimization problem in which each SIL alternative is assigned a 'value' and the SIL with the highest value is selected as the optimum choice. Note that the terms cost and benefit here do not reflect the business cost and business profit, but they rather refer to risk and safety in general. By using this concept one can assure that all possible alternatives are examined and the final outcome is the most efficient option. This approach can be particularly helpful in the context of ALARP (As Low As Reasonably Practicable) where, amongst other requirements, a cost-benefit analysis should be conducted to demonstrate that further risk reduction is not reasonably practicable due to the disproportionate ratio between cost and the risk reduction measure.

This paper introduces new methods of SIL determination that can factor in the cost of solution and quantify the absolute and relative effectiveness of SIL alternatives. Unlike the conventional methods that are focused on minimum-effort solutions, the optimization methods given here aim at finding the maximum risk reduction effort that can be reasonably achieved.

Neither SIL determination nor risk optimization is a new subject. Numerus research works have been published on the two topics in the past (see the list of references for some examples); however, applying optimization methods to SIL determination problems is quite recent. The idea was previously examined in a case study to determine optimum SIL for a low demand mode SIF by using numerical methods (Jahanian and Mahboob, 2016). This paper develops an analytical formulation of the problem; it covers all the SIF operation modes, including low demand, high demand and continuous modes (IEC61508, 2011d); and it introduces two different methods for optimizing corporate risk and ALARP. Taking an analytical approach, this paper uses the continuous measures of PFD/PFH as the primary target variables, based on which the discrete value of SIL can be calculated. Furthermore, we will introduce a continuous form of SIL by combining the SIL and PFD (or PFH) measures into one index, namely Safety Index, and we will show how this single measure can represent a SIF. While focusing on analytical concepts, we will also use a numerical case study to demonstrate the application of the methods in real-life situations. The main objective of this paper is to open a new perspective to the SIL determination problem and to demonstrate how optimization methods can minimize both risk and cost.

The rest of this article is organized as follows: Section 2 provides an introduction to probabilistic modelling of major plant accidents and the basis of conventional SIL determination methods. With a reference to rational decision making and the Expected Utility Theory (EUT), Section 3 establishes a risk optimization model for SIL determination based on corporate risk, where the risk consists of all types of consequences, including damage to asset and business. The model is formulated in detail for both demand mode and continuous mode SIFs. Section 3 also introduces the Safety Index, which can be used as a continuous form of SIL for reliability analysis. Section 4 changes the perspective and analyzes the optimization problem from the point of view of ALARP. This section focuses on health and safety of people and the proportionality of risk against cost. The ALARP-based model, too, is detailed for both demand and continuous SIF operation modes. Section 5 demonstrates the application of the utility-based and ALARP-based models in a case study from power industry. Further analysis is included in Section 5 to verify the behaviour of the models when key factors, such as demand rate and loss, vary. Finally, Section 6 concludes the discussion by reviewing the advantages and challenges of the proposed methods in comparison with the conventional approach.

2. Background

A major plant accident takes place when a hazardous initiating event occurs and all protection layers fail to confine it. Initiating events and accidents are typically quantified by their frequency of occurrence, whereas protection layers are represented by their average probability of failure in responding to demands.

Consider a simplified combination of the process, Basic Process Control System (BPCS) and SIF as shown in Fig. 1. In scenario (a), the hazardous initiating event occurs in the process and it raises a demand on the BPCS to take a preventive action and contain the situation. If the BPCS fails to respond effectively, a demand will be initiated for the SIF's action, and failure of the SIF to respond to the demand will result in an accident. To formulate the frequency of accident in this scenario, let λ_e be the frequency of hazardous event initiated in the process and P_c and P_f the average probability of unavailability of the BPCS and SIF respectively. Using these variables, the overall frequency of accident (λ_h) can be formulated as follows:

$$\lambda_h = \lambda_{e \cdot P_c \cdot P_{f \text{ for scenario (a)}}} \quad (1)$$

Scenario (b) shows the situation where BPCS controls a part of the process. Imagine a turbine governor system which constantly modulates the fuel control valve in order to maintain the turbine in its desired operating point. A dangerous fault in the governor initiates a demand on the SIF to isolate the fuel in order to protect the plant; and an accident takes place if the SIF fails to respond to the demand. With λ_c being the frequency of hazardous event initiated in the BPCS, the overall frequency of accident will be as follows:

$$\lambda_h = \lambda_{c \cdot P_{f \text{ for scenario (b)}}}$$

Finally, in scenario (c) the SIF operates in continuous mode and it controls the plant. An accident can occur as a result of an internal dangerous failure in the SIF itself. Examples of such SIFs can include continuous control of dosing in a critical chemical process or speed control in heavy rotating machinery. In such cases, the SIF is consistently controlling the process, and the failure of the SIF immediately results in a catastrophic situation. This is different to the demand mode (scenarios (a) and (b)) in which the SIF is in standby state for most of its lifetime and it only comes into action when a demand is initiated. In scenario (c) the frequency of accident will be equal to the frequency of dangerous failure in the SIF, i.e. λ_f:

$$\lambda_h = \lambda_{f \text{ for scenario (c)}}$$

IEC61508 and IEC61511 use the terms PFD_{avg} and PFH to represent the SIF's average Probability of Failure on Demand (PFD) and the average Frequency of Failure per Hour (PFH) —for simplicity in mathematical formulation in this paper we use the short form PFD, instead of PFD_{avg}. With respect to P_f and λ_f, PFD is identical to P_f and PFH equates λ_f for $\lambda_f \ll 1$. The only difference here is that PFD and PFH are average values, i.e. they are calculated over a given period of time, whereas P_f and λ_f are absolute figures and independent of time. For a 1-out-of-1 system with exponential random distribution, the PFD and PFH are as follows (Rausand, 2014):

$$\text{PFD} = 1 - \left(1 - e^{-\lambda_f \tau}\right) / \left(\lambda_f \tau\right) \quad (2)$$

$$\text{PFH} = \left(1 - e^{-\lambda_f \tau}\right) / \tau \quad (3)$$

In Eqs. (2) and (3), τ is the time period over which the average values of PFD and PFH are calculated. For PFD, τ is commonly defined as the proof test interval, a time period at the end of which the SIF is proof tested and returned to service as