Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

SIL determination as a utility-based decision process

Hamid Jahanian[a,*], *Qamar Mahboob*[b]

[a] *Siemens, Power and Gas, 160 Herring Road, Macquarie Park, NSW 2113, Australia*
[b] *Siemens, Rail Electrification, Mozart str. 33b, 91052 Erlangen, Germany*

ARTICLE INFO

Article history:
Received 22 February 2016
Received in revised form 31 May 2016
Accepted 7 June 2016
Available online 16 June 2016

Keywords:
Expected Utility Theory
SIL determination
Risk based optimisation
ALARP

ABSTRACT

Using the concept of ALARP (As Low As Reasonably Practicable) and the Expected Utility Theory (EUT), this paper introduces a risk-based optimisation approach to the SIL (Safety Integrity Level) determination process. In the commonly used SIL determination methods the target SIL is determined by comparing the existing level of risk to a pre-set corporate risk target; the gap defines the level of risk that should be reduced by additional layers of protection, such as safety systems. Such methods do not directly factor in the cost impact of the allocated target SILs, nor do they examine the practicability of all SIL alternatives in reducing the risk to as low as possible. The method presented in this paper is based on assigning utility values to different SIL alternatives, in accordance with the cost and benefits of each alternative, and comparing the expected utility values in order to determine the optimum SIL rating as target. A numerical analysis has been developed and applied to the SIL evaluation for a gas turbine over-speed protection to demonstrate the advantages and challenges of the new method.

1. Introduction

In the process industry, SIL (Safety Integrity Level) determination is a risk assessment process through which target SILs are allocated to Safety Instrumented Functions (SIFs) (IEC, 2003b, 2011a). A SIF is a preventive protection function implemented in a Safety Instrumented System (SIS), and it protects the plant against a specific hazard. A typical SIF in a gas turbine application is the over-speed protection. The SIF requires multiple sensors to measure the turbine speed; a logic solver to monitor the input signals and initiate an emergency shutdown command when the turbine speed is dangerously increasing; and a gas isolation valve to isolate the fuel and prevent the turbine from over-speeding. The main goal in a SIL determination study is to define how much risk should be reduced by a given SIF so that the final risk level is lower than the tolerable risk level. Allocated SILs reflect how harmful the associated hazards are and how reliable the SIFs should be. The target SILs are normally set by the plant owner and based on corporate risk criteria.

In some countries, e.g. the United Kingdom (UK), organisations are also required by law to eliminate or reduce the risk arising from work to as low as reasonably practicable (ALARP). Based on the ALARP principle, where more than one acceptable alternative are available to reduce risk, Cost-Benefit Analysis (CBA) can be carried out to determine which alternative reduces the risk more efficiently. Amongst other methods, utility maximisation can be used for CBA analysis in the context of ALARP (UKHSE, 2001; Schofield, 1998). Utility maximisation is a three-step decision process: assign measurable utility values to different outcomes, calculate the Expected Utility Values (EUV), and choose the alternative with the highest EUV.

SIL determination can be looked at as a risk-related investment decision: depending on the target SIL the value of investment changes and depending on the investment the

[*] *Corresponding author*. Tel.: +61 408473423.
E-mail addresses: hamid.jahanian@siemens.com (H. Jahanian), qamar.mahboob@siemens.com (Q. Mahboob).

http://dx.doi.org/10.1016/j.psep.2016.06.012

reliability of the safety system and consequently the probability of accident is affected. The current SIL determination methods, such as Layers of Protection Analysis (LOPA), are based on estimating the gap between the existing and tolerable risk levels (AIChE CCPS, 2001). Even where the SIL determination is studied in relation to the ALARP principle (Timms, 2005, 2006; UKHSE, 2004; IEC, 2011a), it is indeed the target SIL that is set based on the ALARP considerations; however the decision process remains the same: identify the gap between that target risk and the existing risk. This paper is an attempt to combine the expected utility as a decision criterion and the concept of ALARP as a risk minimisation guideline, and to present a new SIL determination method based on cost-benefit optimisation. Taking a utility-based approach we will try to look at SIL determination as a decision process aimed at finding the 'optimum' target SIL. The main objective is to examine the practicality of this new approach and demonstrate how this approach would work if applied to real-life applications. This paper uses an illustrative example, a turbine over-speed protection, to demonstrate the new method.

The rest of this article is organised as follows: Section 2 provides a short introduction to SIL determination, ALARP, Expected Utility Theory (EUT) and Influence Diagrams (ID) with a focus on the aspects which are important to this article. Following this introduction, Section 3 outlines the roadmap by explaining the problem and defining the methods and objectives. The concepts developed in Section 3 are then applied to turbine over-speed protection as a case study in Section 4. Finally, Section 5 concludes the discussion by reviewing the advantages and challenges of utility-based SIL determination.

2. Background

In this section sufficient background is provided on SIL determination, ALARP, EUT and ID so that the methods and models presented in the coming sections can be better understood.

2.1. *SIL determination*

Allocation of SIL to SIFs is a critical task in SIS architecture engineering in the process industry. Once the process hazards are identified and SIFs are defined, each SIF is allocated a target SIL. Based on the allocated SIL the basic configuration factors, such as Hardware Fault Tolerance (HFT), are determined in accordance with the IEC61508 (IEC, 2011a, 2011b, 2011c) and IEC61511 (IEC, 2003a, 2003b) standards. Parallel to the discrete scale of SIL, two other continuous measures are alternatively used to gauge the reliability of SIFs: the average Probability of Failure on Demand (PFD_{avg}) and the Risk Reduction Factor (RRF). Table 1 shows the relation between SIL, PFD_{avg} and RRF as defined by the safety standards (IEC, 2003a, 2011b). As shown in Table 1, the higher SIL/RRF a SIF can meet the higher risk reduction the SIF is capable of delivering, having in mind that meeting the requirements of higher SIL obviously implies a larger investment in implementation and maintenance.

Table 1 – SIL, PFD_{avg} and RRF for low demand mode.

Target SIL	Target PFD_{avg}	Target RRF
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to ≤100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤100

Amongst various methods that are available for determining target SILs (IEC, 2003b, 2011a), the semi-quantitative method of LOPA has been widely used in the process industry in recent years (AIChE CCPS, 2001; King, 2009). Simply put, LOPA calculates the gap between the present frequency of a hazardous event and the tolerable frequency of that event; the identified gap determines the extent of risk reduction that should be covered by other risk reduction measures, e.g. SIF. Fig. 1 illustrates this concept.

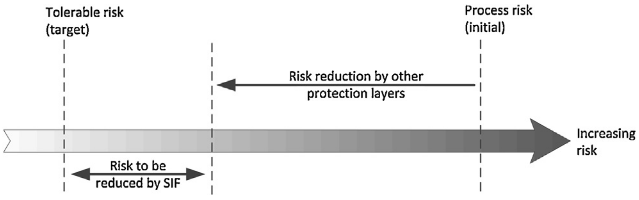

Fig. 1 – Risk reduction and SIL determination in LOPA.

The commonly used SIL determination methods, such as LOPA, rely on a predefined 'target' risk level, rather than on finding the best possible SIL. These methods are simple and practical, and they have been widely practiced and well established in the industry. However, when using these methods one should be aware that, firstly, these methods are aimed at finding minimum-effort solutions; for example, if the SIL study resulted in setting a risk reduction factor of RRF = 95 as target, it is technically adequate to implement a SIL1 solution even though the target RRF is so close to the lower limit of the SIL2 range (see Table 1). Secondly, these SIL determination methods are based on owner-set targets, which do not necessarily, or directly, reflect what may be important to society or authorities. Therefore, meeting such SIL targets does not necessarily mean that the regulatory obligations are met. Thirdly, these SIL determination methods do not take into account the costs associated with different solutions. In other words, the SIL determination team is not concerned about the cost of SIS architecture; nor can they always accurately estimate such costs at the early stage of a project. So, even if the costs of SIL1 and SIL2 solutions are hypothetically the same, these methods will suggest implementing the SIL1 solution if SIL1 is the lowest SIL with which the target can be met.

SIF may be deployed in Low Demand, High Demand, or Continuous mode. Unlike Continuous mode SIFs which are constantly in action to maintain the plant in its safe state, demand mode SIFs only act if a hazardous initiating event is formed and a demand for the SIF action is initiated. If the estimated frequency of demand is less than one per year, the SIF is known as Low Demand SIF, and otherwise as High Demand (IEC, 2003a, 2011b). This paper is focused on Low Demand mode SIFs.

2.2. *The concept of ALARP*

Originated in the UK in 1949, the term ALARP, and similarly SFAIRP (So Far As Is Reasonably Practicable), refers to reducing the risk to as low as reasonably practicable when the elimination of risk is not possible (UKHSE, 2001). While the ALARP principle is specified as a regulatory requirement for work-related health and safety in the UK and some other countries in different forms, ALARP is also referred to in the functional safety standards as a concept for determination of tolerable risk and safety integrity levels (IEC, 2003b, 2011a).