Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

SIL determination: Recognising and handling high demand mode scenarios

*Alan G. King**

ABB Consulting, Pavilion 9, Belasis Hall Business Park, Billingham, Cleveland TS23 4EB, UK

ABSTRACT

The International Standards for Functional Safety (IEC 61508 and IEC 61511) are well recognised and have been adopted globally in many of the industrialised countries during the past 10 years or so. Conformance with these standards involves determination of the requirements for instrumented risk reduction measures, described in terms of a safety integrity level (SIL). During this period within the process sector, layer of protection analysis (LOPA) has become the most widely used approach for SIL determination. Experience has identified that there is a type of hazardous event scenario that occurs within the process sector that is not well recognised by practitioners, and is therefore not adequately handled by the standard LOPA approach. This is when the particular scenario places a high demand rate on the required safety instrumented function. This paper will describe how to recognise a high demand rate scenario. It will discuss what the standards have to say about high demand rates. It will then demonstrate how to assess this type of situation and provide a case study example to illustrate how to determine the necessary integrity level. It will conclude by explaining why it is important to treat high demand rate situations in this way and the resulting benefit of a lower but sufficient required integrity level.

Keywords: SIL determination; IEC 61508; IEC 61511; Layer of protection analysis; LOPA; High demand rate

1. Introduction

SIL determination is the process of reviewing each specific hazardous event and assessing the contribution to risk reduction that is required from instrumented measures. Each safety instrumented function (SIF) is then assigned a safety integrity level to describe the performance level required from that function. The objective of this paper is to highlight and discuss some of the issues relating to high demand mode SIL determination assessments and then to illustrate this with a typical case study from the process sector.

For many years, the prevailing wisdom has been that high demand mode occurs in transport, manufacturing and some other sectors, but is not found very much, if at all, in the process sector. However, recent experience suggests that high demand mode is found within the process sector and occurs not infrequently. The problem is one of knowing how to recognise the situations where high demand situations occur and understanding how this affects SIL determination. This paper explores the challenge and is based on an earlier publication by the author (see King, 2013).

2. International Standards IEC 61508 and IEC 61511

IEC 61508 (IEC, 2010) is the generic standard covering the field of Functional Safety achieved by electrical, electronic and programmable electronic systems. This standard recognises three modes of safety function operation: (a) low demand mode, (b) high demand mode and (c) continuous mode. These modes of operation are defined as follows in Table 1 .

Table 1 – IEC 61508 Ed 2 – modes of operation.

Mode	Description
Low demand mode	Safety function demand rate is less than or equal to once a year
High demand mode	Safety function demand rate is greater than once a year
Continuous mode	Safety function is operating as a continuous control function

* Corresponding author.
E-mail addresses: alan.g.king@gb.abb.com, agking@iee.org

0957-5820/$ – see front matter
http://dx.doi.org/10.1016/j.psep.2014.01.002

IEC 61511 (IEC, 2003) is the process sector standard based on IEC 61508 and describes how the principles of IEC 61508 should be applied in the process sector. IEC 61511 essentially adopts the same approach as IEC 61508 though it uses slightly different terminology. This is shown in Table 2.

Table 2 – IEC 61511 – modes of operation.

Mode	Description	Comment
Demand mode	Where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands	This is equivalent to the IEC 61508. Low demand mode
Continuous mode	Where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it	This is equivalent to the IEC 61508. High demand mode and continuous mode

For safety instrumented functions, the safety standards have different failure measure parameters for defining the safety integrity levels depending on the mode of operation.

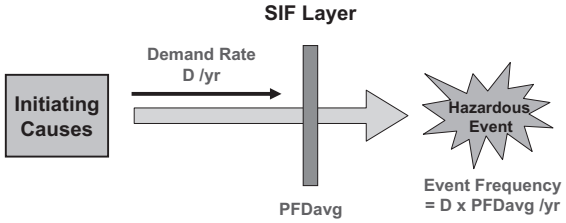

Fig. 1 – Typical process sector low demand scenario.

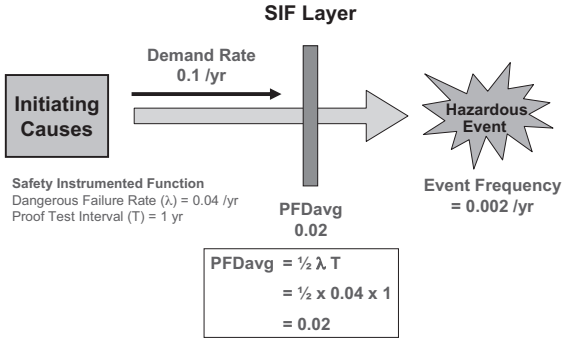

Fig. 2 – Low demand scenario calculation.

Table 3 – Target failure measures: low demand mode and high demand mode.[a]

Low demand mode		High demand mode	
Safety integrity level (SIL)	Average PROBABILITY of dangerous failure on demand (PFDavg)	Safety integrity level (SIL)	Average FREQUENCY of a dangerous failure per hour
1	$\geq 10^{-2}$ to $<10^{-1}$	1	$\geq 10^{-6}$ to $<10^{-5}$
2	$\geq 10^{-3}$ to $<10^{-2}$	2	$\geq 10^{-7}$ to $<10^{-6}$
3	$\geq 10^{-4}$ to $<10^{-3}$	3	$\geq 10^{-8}$ to $<10^{-7}$
4	$\geq 10^{-5}$ to $<10^{-4}$	4	$\geq 10^{-9}$ to $<10^{-8}$

[a] See IEC 61508-1 Edition 2 Tables 2 and 3, or IEC 61511-1 Tables 3 and 4.

For low demand mode, the failure measure is based on average *Probability* of dangerous failure on demand (PFDavg), whereas for high demand mode it is based on average *Frequency* of dangerous failure per hour. These target failure measures are tabulated in Table 3.

3. Recognising high demand mode

A typical process sector scenario is illustrated in Fig. 1. The specific hazardous event is shown on the right and to the left is a box indicating the identified initiating causes. The safety instrumented function (SIF) layer is a means of preventing the hazardous event from happening when one of the causal failures occurs. The hazardous event frequency can then be calculated from the frequency of demands (*D*/year) on the safety instrumented function (SIF) times the average probability of failure on demand (PFDavg) for the SIF. If we put some numbers to the scenario (demand rate = 0.1/year and SIF dangerous failure rate (λ) = 0.04/year with proof test interval of 1 year and assuming a single channel function), we obtain a hazardous event frequency of 0.002/year; see Fig. 2.

For low demand mode of operation the calculation above works fine.

Now consider instead, the situation illustrated below in Fig. 3. This shows the same arrangement; the only change is that the demand rate is now 100/year instead of 0.1/year. The hazardous event frequency has now apparently increased to 2/year. However, the dangerous failure rate for the safety instrumented function is only 0.04/year and it is therefore not

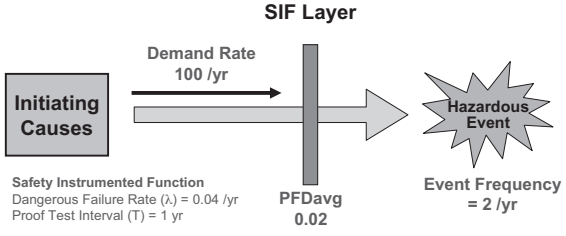

Fig. 3 – High demand scenario but with wrong (low demand rate) calculation.