CHEMICAL ENGINEERING TRANSACTIONS

VOL. 31, 2013

A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet

Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; ISSN 1974-9791

DOI: 10.3303/CET1331013

SIL Determination: Dealing with the Unexpected

Alan G King

ABB Consulting, Pavilion 9, Byland Way, Billingham,Cleveland, TS23 4EB, UK
Alan.g.king@gb.abb.com

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 the determination of the required risk reduction and the appropriate safety integrity level (SIL) for the safety instrumented functions. One significant area for consideration is the application of this technique to certain hazardous events. Experience has identified that there is a type of hazardous scenario that occurs within the process sector that is not well recognised by practitioners, and is therefore not duly 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.

1. Introduction

SIL Determination is the process of reviewing the level of risk associated with a specific hazardous event and assessing the contribution to risk reduction that is required from instrumented measures, such as a safety instrumented function, in order that, overall, sufficient risk reduction is achieved. 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 in fact occurs quite frequently. The problem is in knowing how to recognise the situations where this occurs and also understanding how it affects SIL Determination.

2. International Standards IEC 61508 and IEC 61511

IEC 61508 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:

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

Please cite this article as: King A., 2013, Sil determination: dealing with the unexpected, Chemical Engineering Transactions, 31, 73-78
DOI: 10.3303/CET1331013

IEC 61511 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.

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

Low Demand Mode

Safety Integrity Level (SIL)	Average PROBABILITY of Dangerous Failure on Demand (PFDavg)
1	$\geq 10^{-2}$ to $< 10^{-1}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
4	$\geq 10^{-5}$ to $< 10^{-4}$

High Demand Mode

Safety Integrity Level (SIL)	Average FREQUENCY of a Dangerous Failure per hour
1	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
4	$\geq 10^{-9}$ to $< 10^{-8}$

Figure 1: Target failure measures: low demand mode and high demand mode [1]

For low demand mode, the failure measure is based on average Probability of dangerous Failure on Demand (PFDavg) and for high demand mode it is based on average Frequency of Dangerous failure per Hour. The target failure measures are tabulated in Figure 1.

3. Recognising High Demand Mode

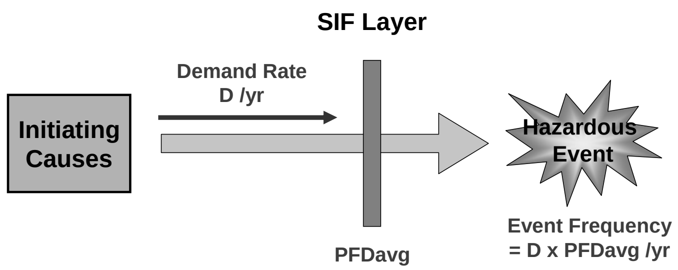


Figure 2: Typical Process Sector Low Demand Scenario

A typical process sector scenario is illustrated in Figure 2. 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/y) on the Safety Instrumented Function (SIF) times the probability of failure (PFDavg) for the SIF. If we put some numbers to the scenario (Demand rate = 0.1/y and SIF dangerous failure rate (λ) = 0.04/y with proof test interval of 1 y and assuming a single channel function), we obtain a hazardous event frequency of 0.002/y; see Figure 3.

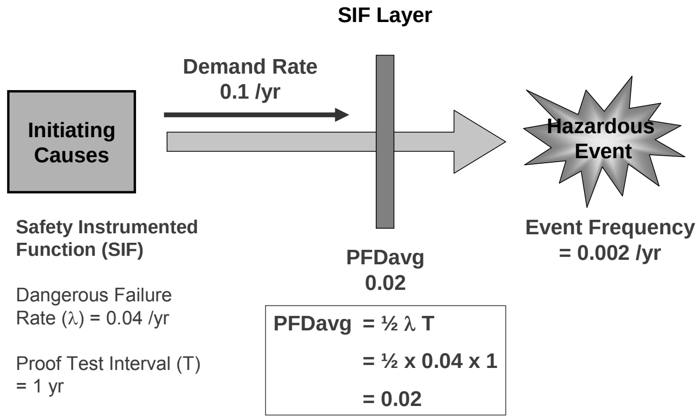


Figure 3: Low Demand Scenario Calculation

Consider instead the situation illustrated in Figure 4. This shows the same arrangement; the only change is that the demand rate is now 100/y instead of 0.1/y. The hazardous event frequency has now apparently increased to 2/y. However, the dangerous failure rate for the safety instrumented function is only 0.04/y and it is therefore not credible to have a hazardous event frequency greater than 0.04/y.

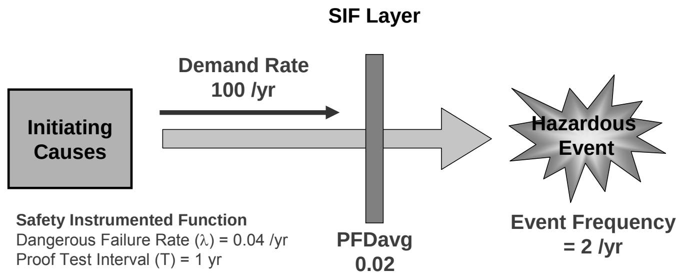


Figure 4: High Demand Scenario but with wrong (Low demand rate) Calculation

So what is wrong with the calculation? Well, essentially it is using a low demand calculation for a high demand scenario. The low demand calculation follows a straight line as shown in Figure 5, arriving at 2/y when the frequency should be no greater than 0.04/y.

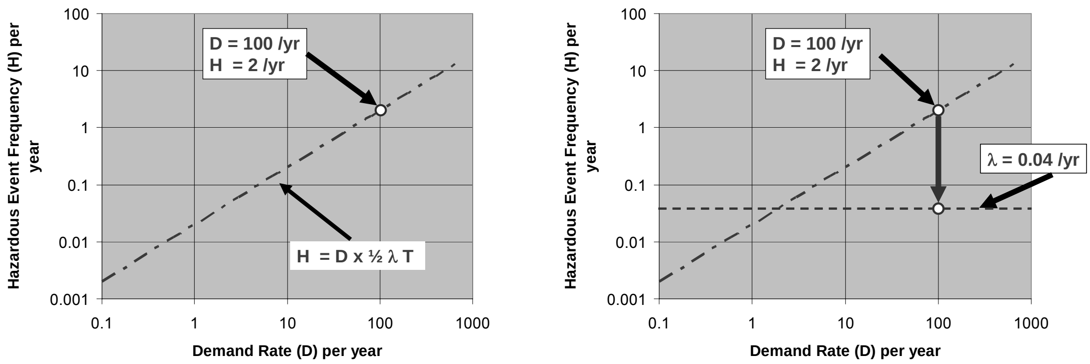
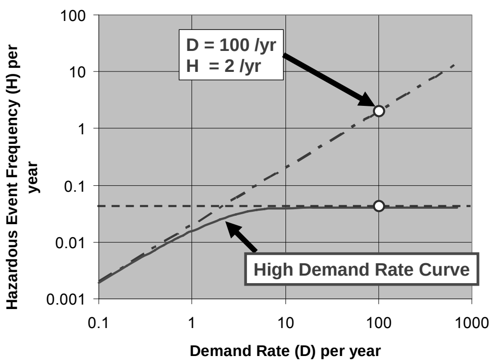


Figure 5: Graphs illustrating the problem with the calculation in Figure 4

The analysis should follow the high demand rate curve as shown in Figure 6. The high demand rate curve follows the low demand line when the demand rate is low and then curves to meet the failure rate of the SIF as the demand rate increases.

---

[1] See IEC 61508-1 Edition 2 Tables 2 and 3



- Hazardous Event Frequency (H) = λ **(1 – exp (-DT/2))** **
- If Demand Rate (D) is low:

  H = λ **(1 – (1 -DT/2 + …))**

  $\approx$ λ **DT/2 or D x ½λT**
- If the Demand Rate (D) is high:

  H = λ **(1 – exp (-DT/2))**

  $\approx \lambda$

*** High Demand Rate Single Channel SIF Equation*

Figure 6: High Demand Rate Curve

To the right of the graph is the high demand rate equation for a single channel SIF (top bullet) and the two lower bullets show what happens to that equation when (a) the demand rate is low and (b) when the demand rate is high.

The important requirement is to recognise when the demand rate on the SIF is “high”. This is illustrated in left diagram in Figure 7. The demand rate to consider is that after any alarm layers and any other factors that would apply prior to a real demand on the SIF Layer. If this demand rate is greater than 1/yr then IEC 61508 regards this as high demand mode. It would also be high demand mode if the demand rate (D) x proof test interval (T) is significantly greater than 1.

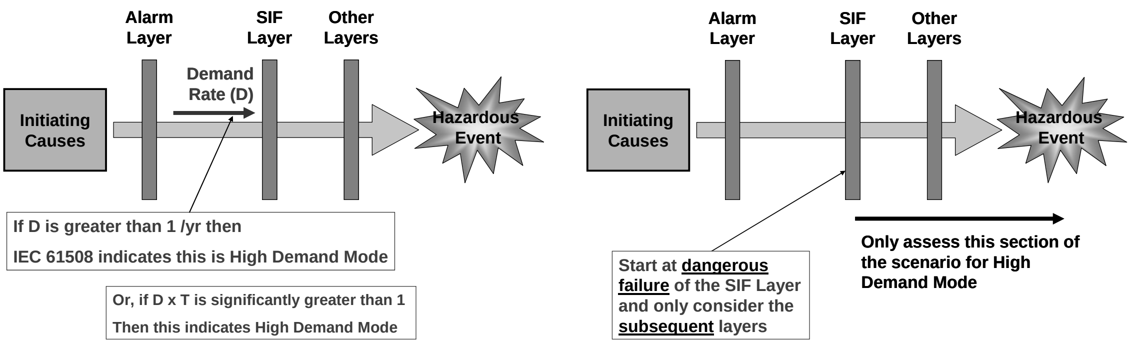


Figure 7: Recognising and Assessing High Demand Mode

If high demand mode is established, then SIL Determination assessment starts at the SIF layer and only considers those aspects of the scenario that would be relevant should the SIF layer be in a failed state. This is illustrated in the right diagram in Figure 7.

4. Process Sector SIL Determination Case Study

Let us now have a look at a case study from the process sector. The case study here is from a project in the oil and gas industry. Figure 8 shows a schematic diagram of the relevant section of the process. It shows the flare knock-out drum. Normally, the hydrocarbon gas stream from various sections of the plant going to the knock-out drum is recycled to the gas compressor. However, if the feed to the knock-out drum exceeds the compressor capacity, then the High Pressure Safety Instrumented Function (SIF) shown prevents overpressure of Flare Knock-out Drum. There are three pressure sensors with a 2oo3 voting configuration to trigger the SIF. The action on detection of high pressure is to open Valve B and to close Valve A. However, the action of closing Valve A is not an essential action and therefore the SIF is considered only to comprise the three pressure sensors and Valve B. There are two other risk reduction measures preventing overpressure of the knock-out drum; these are designed to act should the SIF be in a failed state. These measures are (a) a bursting disc and (b) a rupture pin valve.

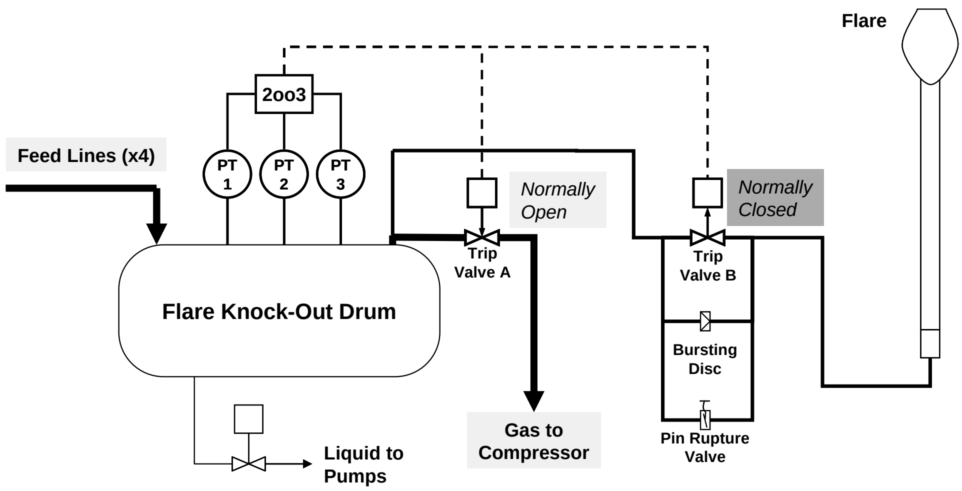
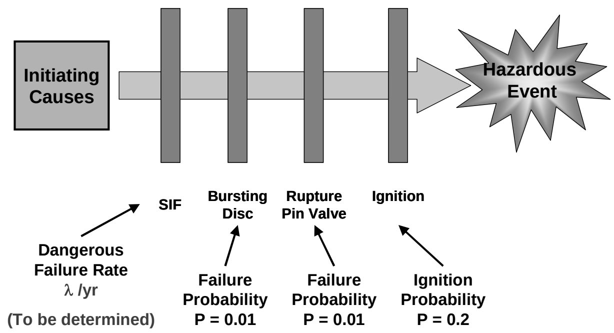


Figure 8: Schematic diagram of process section

It had originally been expected that this would be another low demand rate scenario, in common with the previous scenarios in the project. However, during discussions with the operations representatives, it quickly became apparent that the frequency of demands would be well in excess of once a year. The operations team had several years of experience of working on similar facilities and estimated that the demand frequency would be around 22/y. Identified sources of demand on the SIF were: (a) Gas Feed exceeds Compressor capacity or (b) Compressor trips or (c) Spurious closure of Trip Valve A. To the left, Figure 9 shows the scenario diagram and the probabilities associated with the post-SIF features.



- Target Event Frequency = 10^{-6} per year
- Therefore, we need:

$\lambda \times 0.01 \times 0.01 \times 0.2 = 10^{-6}$ per year

$\lambda = 5 \times 10^{-2}$ per year

$= 5.7 \times 10^{-6}$ per hour (SIL 1)

Figure 9: High Demand Scenario and High Demand Rate SIF Calculation

To the right, Figure 9 shows the calculation of the required dangerous failure rate for the SIF that is required to enable the target event frequency to be achieved. The calculated value of 5.7×10^{-6} per hour for the dangerous failure rate for the SIF is in the range for SIL 1.
However, if the calculation for the SIF is mistakenly made on a low demand basis against the same target event frequency, we get a significantly different result:

For a target event frequency of 10^{-6}/y, a failure probability for the SIF designated by PFDavg, and a Demand Rate (D) of 22 /y, we get the following equation:

D x PFDavg x 0.01 x 0.01 x 0.2 = 10^{-6}/ y

22 x PFDavg x 0.01 x 0.01 x 0.2 = 10^{-6} /y

PFDavg = 10^{-6} / (22 x 0.01 x 0.01 x 0.2)

= 0.0023 (SIL 2)

This calculation indicates a target PFDavg of 0.0023 which is in the range for SIL 2.

We can conclude that that using the correct high demand rate approach, it is clear that a SIL 1 function will be sufficient to achieve the target event frequency. However, if the wrong approach is used with a low demand calculation, then the calculation suggests a need for SIL 2. A function achieving SIL 2 would cost more to design, more to install, more to maintain and is not actually needed; only SIL 1 is needed to achieve the target frequency.

5. High Demand Mode in the Process Sector

In order to gauge how frequently high demand mode might be encountered in the process sector, some data was gathered from a number of specialists working in the sector. This suggests that across the process sector high demand mode scenarios may account for anything up to 10% of the total. This is illustrated in Table 3.

Table 3: High Demand Mode in the Process Sector

Sector	Description	Total SIFs	High Demand SIFs	Percent High Demand
Oil and Gas	Project Front End Studies	60	2	3%
Oil and Gas	Project Front End Studies	60	2	1%
Oil and Gas	Revalidation - Selected Functions	39	2	5%
Chems - Batch	Existing Legacy - Selected Functions	60	2	7%
Pharma - Batch	Existing Legacy - Selected Functions	60	2	10%

This clearly demonstrates that high demand mode certainly does occur in the process sector and, though it may be unexpected, it is definitely not that rare.

6. Conclusions

The conclusions can be summarised as follows. Firstly, it is important to identify high demand scenarios and then use the correct form of calculation. High demand mode calculations disregard the part of the scenario leading up to the demand on the SIF; the assessment calculation starts with the SIF failure and then incorporates just the post SIF risk reduction features. Secondly, the use of a Low Demand approach is conservative, but leads to over specifying the SIL and hence more expenditure. Using a High Demand calculation gives a more appropriate assessment with a lower, less onerous, SIL requirement (e.g. SIL 1 instead of SIL 2) but still achieving the hazardous event target frequency. Finally, we must conclude that High Demand Mode really does occur in the Process Sector and analysts must be ready to meet the challenge.

References

International Electrotechnical Commission, 2010, IEC 61508 Ed 2 Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 – 7, Geneva, Switzerland

International Electrotechnical Commission, 2003, IEC 61511 Functional safety – Safety instrumented systems for the process industry sector, Parts 1 – 3, Geneva, Switzerland

Center for Chemical Process Safety, 2000, Guidelines for chemical process quantitative risk analysis, Edition 2, New York, USA.

Kletz T., 2006, HAZOP and HAZAN, Identifying and Assessing Process Industry Hazards, 4th Edition, The Institution of Chemical Engineers, Rugby UK.