SIL Determination and High Demand Mode

Alan G King, Hazard & Reliability Specialist, ABB Consulting, Billingham, Cleveland UK

SIL Determination, the setting of target safety integrity requirements for safety instrumented functions, has become one of the accepted features of Process Safety Management (PSM). The need for SIL Determination was highlighted when the international standards for functional safety (IEC 61508 and IEC 61511) were published 10 years or so ago. These standards are now well recognised and have been adopted globally in many of the industrialised countries. Conformance with these standards involves determination of the requirements for instrumented risk reduction measures, described in terms of a safety integrity level (SIL).

Layer of Protection Analysis (LOPA) has, within the process sector, become the most widely used approach for the determination of the required risk reduction for a hazardous event scenario and the appropriate safety integrity level (SIL) for safety instrumented functions. For many types of scenario LOPA is highly effective. However, experience has identified that there is a type of hazardous event scenario that occurs within the process sector that is (a) not well recognised by practitioners, and (b) is not properly handled by the standard LOPA approach. This occurs when the particular scenario places a high demand rate on the required safety instrumented function.

The analysis of high demand rate scenarios is not new: Trevor Kletz, in his book "HAZOP and HAZAN" (1986, 1992, 1999), makes mention of them, but with the advent of the widespread use LOPA and a dominating focus on assessments involving low demand rates, practitioners have lost sight of the high demand rate class of scenario. This has led to shortcomings and inappropriate assessment of the related integrity level requirements.

This paper will describe how to recognise a high demand rate scenario; this is essential understanding for SIL Determination practitioners. It will also discuss what the international standards have to say about high demand rates. It will then proceed to 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, though that case study, why it is important to treat high demand rate situations in this way and will highlight the resulting benefit of a lower, but sufficient, target safety integrity level.

Keywords: High Demand Mode, SIL Determination, LOPA, Layer of Protection Analysis, IEC 61511, IEC 61508

Introduction

SIL Determination within the process industry has been carried out by a number of techniques following the publication of the international standards IEC 61508 and IEC 61511. The techniques used have included Risk Graphs, Fault Tree Analysis and Layer of Protection Analysis, amongst others. In recent years, Layer of Protection Analysis has, one might say, become the method of choice for a number of organisations.

Within the process industry sector, there has been the tacit assumption that all the scenarios place the safety instrumented function being assessed into what the standards describe as low demand mode, and the analysis has been carried out based on this assumption. The other mode of operation for a safety instrumented function, high demand mode (or continuous mode) has been seen as something that occurs in other sectors of industry, such as the machinery, manufacturing, and the various transport sectors.

However, it is becoming apparent that within the process sector high demand mode operation of safety instrumented functions does occur; it is just not recognised by many SIL Determination practitioners and as a consequence, it is not being handled effectively using the proper approach. This paper will discuss how to recognise high demand mode situations and how to undertake SIL Determination in those situations. It is based on previous papers [King 2013a and 2013b] on this topic and has been presented again here to reach a wider audience; such is considered the significance of the issue raised.

International Standards

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 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

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. 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.

Table 3 Target failure measures: low demand mode and high demand mode [1]

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 $< 10^{-8}$

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.

Recognising High Demand Mode

In order to decide whether to use a low demand mode approach or a high demand mode approach, the SIL Determination practitioner needs to be able to identify which type of scenario they are facing. The diagram below in Figure 1 shows the typical low demand scenario. The hazardous event frequency can be calculated from the demand rate (D) multiplied by the average probability of failure on demand (PFDavg) of the Safety Instrumented Function (SIF).

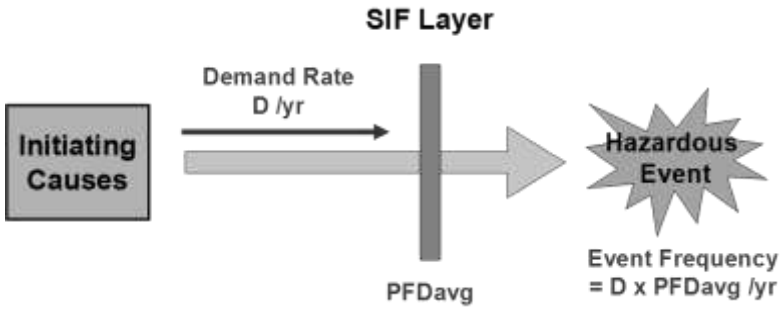

Figure 1 Typical Process Sector Low Demand Scenario

This is the sort of scenario with which most practitioners in the process sector will be familiar. Figure 2 shows the calculation for a typical situation. The demand rate is once in ten years (D = 0.1/yr) and the dangerous failure rate for the SIF Layer is once in 25 years (0.04 /yr), with a proof test interval (T) of one year.

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

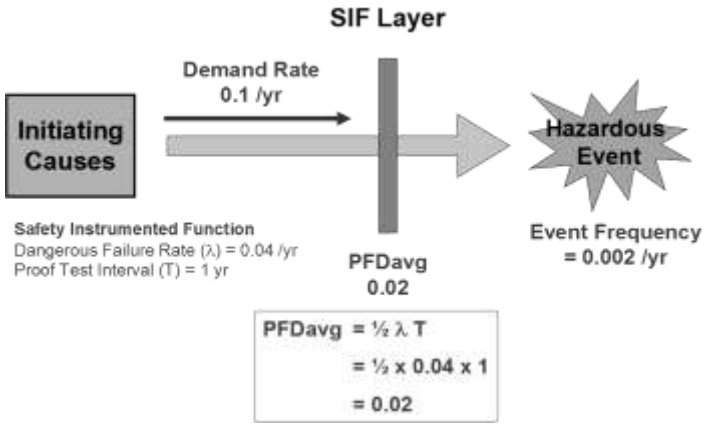

Figure 2 Low Demand Scenario Calculation

The overall hazardous event frequency is then once in 500 years (0.002/yr).

If we now consider the situation shown in Figure 3 where the demand rate on the SIF has increased to 100 per year, and the characteristics of the SIF are unchanged, then we can calculate a hazardous event frequency of 2 per year.

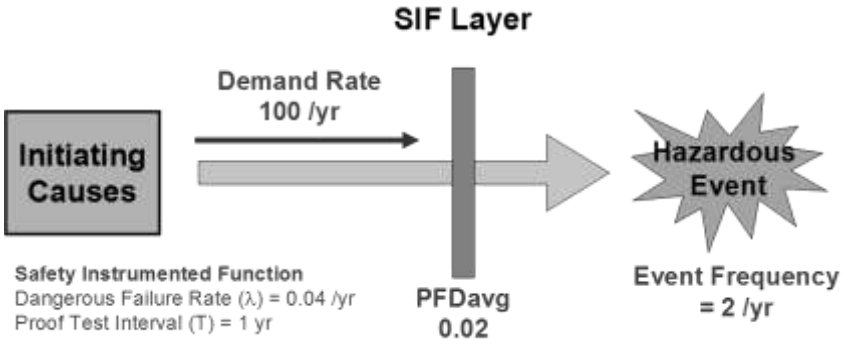

Figure 3 High Demand Scenario but with wrong (Low demand rate) Calculation

Clearly, this does not make sense when the dangerous failure rate for the SIF is 0.04 per year. The hazardous event cannot take place more frequently than the failure of the SIF layer. The explanation is that we have used the wrong approach for the calculation. This can be seen in Figure 4.

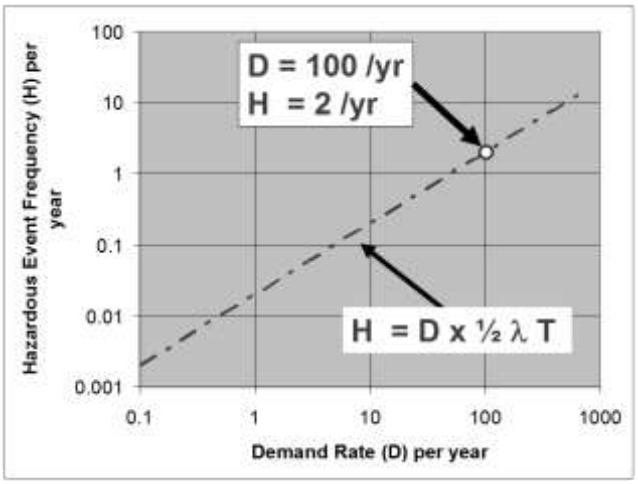

Figure 4 Graph illustrating the calculation in Figure 3

In Figure 4, we can see the line representing the standard low demand mode calculation and the point (D = 100/yr, H = 2/yr) corresponding to the situation in Figure 3. However, it is also clear that the hazardous event frequency cannot be more than the dangerous failure rate of the safety instrumented function. This is illustrated in Figure 5 showing the limiting value of

the safety instrumented function dangerous failure rate and the maximum hazardous event frequency for a demand rate of 100/yr. The hazardous event frequency is therefore bounded by the two lines shown in Figure 5.

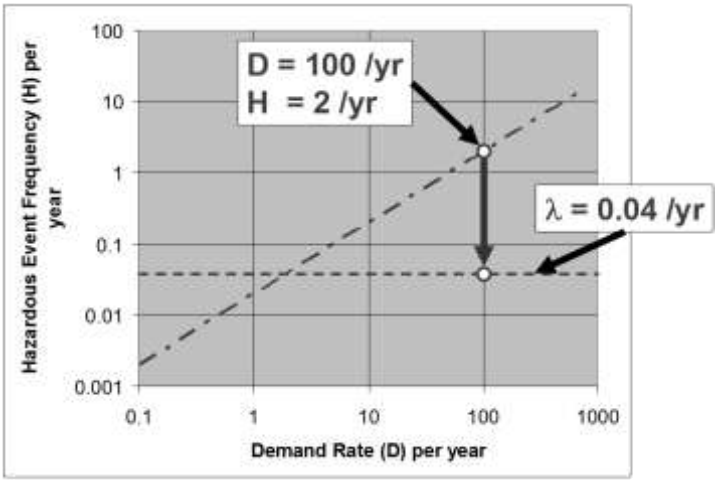

Figure 5 Graph illustrating the problem with the calculation in Figure 3

We can understand this situation better if we consider the way in which the hazardous event frequency changes as the demand rate increases.

Understanding High Demand Mode

Figure 6 shows the lines plotted in Figure 5 together with the high demand rate curve that shows the transition between low demand mode and high demand mode.

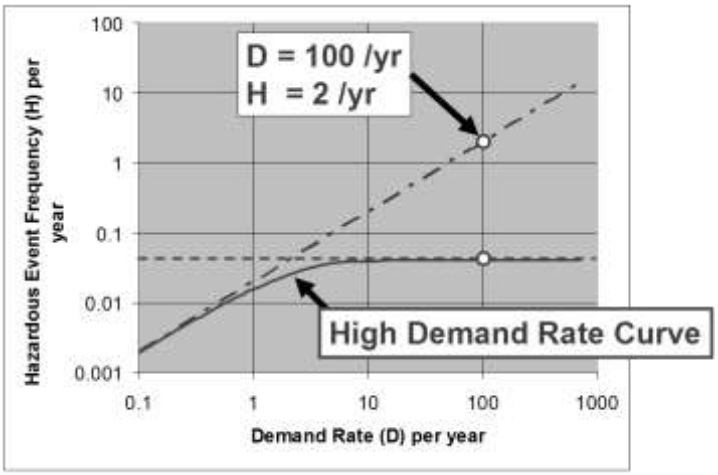

Figure 6 High Demand Rate Curve

Our 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. The high demand rate curve in Figure 6 is based on the equation:

$$\text{Hazardous Event Frequency (H)} = \lambda\left(1-\exp\left(-DT/2\right)\right) \qquad (1)$$

This equation applies to the situation with a single channel safety instrumented function, with λT small (see Kletz 1999, page 110)[2]. When the demand rate (D) is low this equation can be simplified by expanding the exponential and becomes:

[2] Calculations for multichannel SIFs are more complex. See references at the end of this paper.

$$\text{Hazardous Event Frequency (H)} = \lambda\left(1-\left(1-\frac{DT}{2}+\ldots\right)\right) \quad (2)$$

$$= \lambda\left(\frac{DT}{2}\right) \text{ or } D\times\tfrac{1}{2}\lambda T \quad (3)$$

This is now just the Demand rate (D) multiplied by the familiar single channel SIF PFDavg[3]. We can also consider what happens to equation (1) when the demand rate (D) is high. The product D x T becomes large and so the exponent Exp(-DT/2) becomes very small:

$$\text{Hazardous Event Frequency (H)} = \lambda\left(1-\exp\left(-DT/2\right)\right)$$

$$\text{Hazardous Event Frequency (H)} = \lambda\left(1-0\right)$$

$$\text{Hazardous Event Frequency (H)} = \lambda \quad (4)$$

In other words, when the Demand rate (D) is high the hazardous event frequency is limited to the dangerous failure rate of the SIF.

Handling High Demand Mode

The first requirement is to recognise when a situation represents high demand mode. The key to this is the demand rate on the SIF layer, see Figure 7. IEC 61508 regards high demand mode as any situation where the demand rate on the SIF layer is greater than once a year.

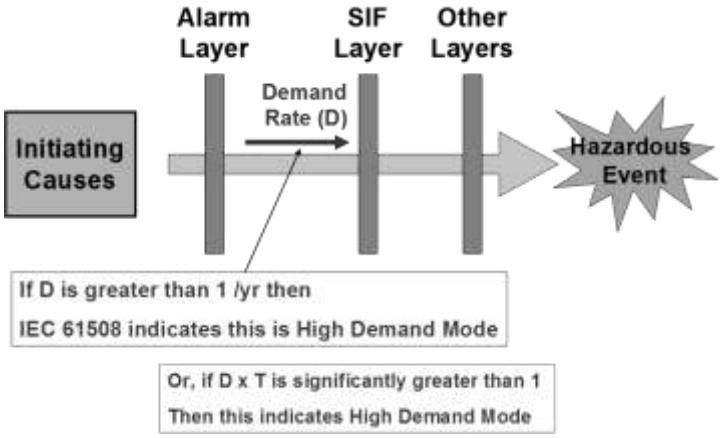

Figure 7 Recognising High Demand Mode

However, it should also be noted from consideration of Equation (1) that if D x T is significantly greater than 1, this will also indicate high demand mode. In other words, high demand mode will become more likely when larger proof test intervals are used.

Once it has been established that the scenario puts the SIF in high demand mode, the frequency of initiating causes can be disregarded, as too can the risk reduction layers that precede any demand on the SIF layer. The key features for SIL Determination are the dangerous failure rate of the SIF layer and any risk reduction features that apply post failure of the SIF layer. This is illustrated in Figure 8.

[3] PFDavg = ½λT

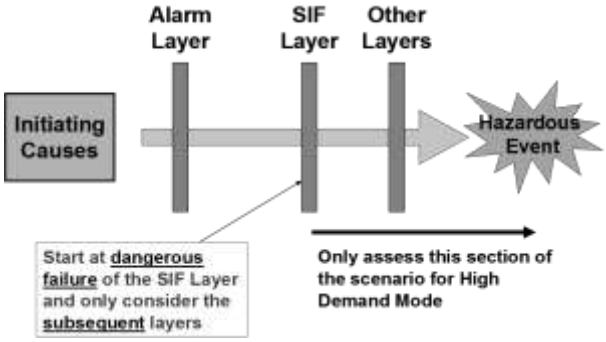

Figure 8 Assessing High Demand Mode

The question to be addressed then is, "with the performance of post SIF failure measures included, what dangerous failure rate target needs to be assigned to the SIF, in order that the hazardous event frequency achieves the event target frequency".

Process Sector Case Study

Let us now have a look at a case study from the process sector to illustrate this further. The case study here is from a project in the oil and gas industry. Figure 9 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 it could potentially lead to a hazardous event. The hazardous event of concern here is overpressure of the flare knock-out drum, release of hydrocarbons, and ignition of those hydrocarbons leading to an explosion. Such an explosion could harm people, harm the environment, and cause equipment damage.

The process design includes a High Pressure Safety Instrumented Function (SIF) to help prevent overpressure of the flare knock-out drum. It has three pressure sensors with a 2oo3 voting configuration to trigger the SIF[4]. 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.

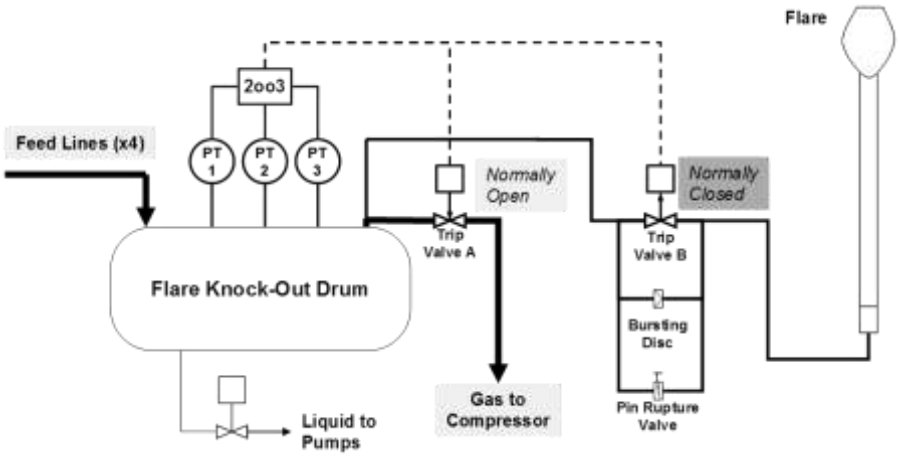

Figure 9 Schematic diagram of process section

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/yr. 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. Figure 10 shows the scenario diagram and the probabilities associated with the post-SIF features.

[4] For the illustrative analysis of the scenario, it is sufficient to treat the overall function as a simple single channel function. The 2oo3 voting of the sensors can be considered as dominated by the common cause contribution at this stage.

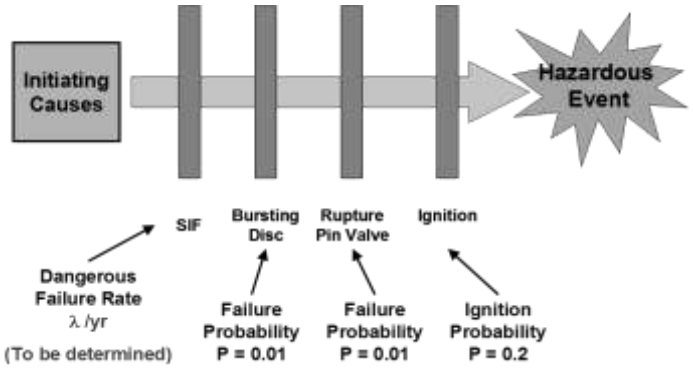

Figure 10 High Demand Scenario

Given a target hazardous event frequency for this scenario of 10^{-6} per year, we can calculate the required dangerous failure rate (λ) for the SIF that is needed to meet this target event frequency:

$$\lambda \times 0.01 \times 0.01 \times 0.2 = 10^{-6} \text{ per year} \quad (6)$$

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

$$= 5.7 \times 10^{-6} \text{ per hour} \quad (7)$$

This calculated value of 5.7×10^{-6} per hour for the dangerous failure rate for the SIF is in the range for SIL 1 (see the High Demand Mode section of Table 3).

However, if the calculation for the SIF is mistakenly made on a low demand basis against the same target event frequency, but with the demand rate (D) having a value of 22 /yr, we get a significantly different result:

$$D \times PFDavg \times 0.01 \times 0.01 \times 0.2 = 10^{-6} \text{ per year} \quad (8)$$

$$22 \times PFDavg \times 0.01 \times 0.01 \times 0.2 = 10^{-6} \text{ per year} \quad (9)$$

$$PFDavg = 10^{-6} / (22 \times 0.01 \times 0.01 \times 0.2)$$

$$= 0.0023 \quad (10)$$

This calculation indicates a target PFDavg of 0.0023 which is in the range for SIL 2 (see the Low Demand Mode section of Table 3).

We can conclude from this 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 for the hazardous event of concern.

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 4.

Table 4 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	150	2	1%
Oil and Gas	Revalidation - Selected Functions	39	2	5%
Chems - Batch	Existing Legacy - Selected Functions	14	1	7%
Pharma Batch	Existing Legacy - Selected Functions	10	1	10%

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

Conclusions

The conclusions can be summarised as follows. Firstly, it is all 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 required 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 and demonstrate the necessary competence.

References

1. International Electrotechnical Commission, 2010, IEC 61508 Ed 2 Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 – 7, Geneva, Switzerland
2. International Electrotechnical Commission, 2003, IEC 61511 Functional safety – Safety instrumented systems for the process industry sector, Parts 1 – 3, Geneva, Switzerland
3. Center for Chemical Process Safety, 2000, Guidelines for chemical process quantitative risk analysis, Edition 2, New York, ISBN 0-8169-0720-X
4. Kletz T., 1999, HAZOP and HAZAN, Identifying and Assessing Process Industry Hazards, 4th Edition, The Institution of Chemical Engineers, Rugby, UK, ISBN 978-0-85295-506-2
5. King, Alan G, 2013a, SIL Determination: Dealing with the Unexpected, Chemical Engineering Transactions, Vol 31, ISBN 978-88-95608-22-8; ISSN 1974-9791
6. King, Alan G, 2013b, SIL Determination: Recognising and handling high demand mode scenarios, Process Safety and Environmental Protection, Official journal of the European Federation of Chemical Engineering: Part B, Special issue: Loss Prevention 2013.