High/Continuous Demand Hazardous Scenarios in LOPA

Hui Jin, PhD
Risk Analyst, SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120
Houston, TX 77034
hjin@sis-tech.com

William (Bill) L. Mostia, Jr., PE, ISA Fellow
SIS-TECH Fellow, SIS-TECH Solutions, LP
bmostia@sis-tech.com

Angela Summers, PhD, PE
President, SIS-TECH Solutions, LP
asummers@sis-tech.com

Prepared for Presentation at
American Institute of Chemical Engineers
2016Spring Meeting
12thGlobal Congress on Process Safety
Houston, Texas
April 11-23, 2016

High/Continuous Demand Hazardous Scenarios in LOPA

Hui Jin, PhD
Risk Analyst, SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120
Houston, TX 77034
hjin@sis-tech.com

William (Bill) L. Mostia, Jr., PE, ISA Fellow
SIS-TECH Fellow, SIS-TECH Solutions, LP
bmostia@sis-tech.com

Angela Summers, PhD, PE
President, SIS-TECH Solutions, LP
asummers@sis-tech.com

Keywords: High demand; Continuous mode; LOPA; PFH; PFD; Safety instrumented system

Abstract

Layer of protection analysis (LOPA) has become one of the most important risk analysis techniques in the process industry. It is commonly used to determine the safety integrity requirements for protection layers, especially the safety integrity level (SIL) for safety instrumented functions (SIF). Once a SIL has been assigned to a SIF, the SIF is designed, installed, operated, maintained, tested, and managed according to IEC 61511. The standard requires that the SIL of the SIF be verified quantitatively against defined ranges based on its mode of operation. A key question is how the mode of operation impacts LOPA calculation.

One basic assumption in LOPA is that the safety integrity of the protection layers (including SIF) is given by the well-known average probability of failure on demand (PFD), which is the safety integrity measure for low demand mode per IEC 61511. However, what if the hazard scenario involved has a high (nominally defined as more than once a year) or continuous demand function? IEC 61511 explicitly defines the safety integrity measure for high/continuous demand SIF as the frequency of dangerous failures per hour (PFH), instead of PFD. In some scenarios, there is a mixture of safeguards operating in different modes, e.g. both low demand and high/continuous modes. Does LOPA still work? Is your SIL determination correct? Are your verification calculations correct?

A method is presented to allow both high demand and continuous mode scenarios to be assessed in LOPA without changing the general LOPA framework. The LOPA calculation of high

demand and continuous mode functions is illustrated, showing how improper treatment of the operating mode results in excessive target SIL. A case study encountered in an actual project is used as an example to showcase the proposed calculation method.

1 Introduction

The defense-in-depth philosophy using multiple independent protection layers (IPL) is by far the most common risk analysis methodology utilized in the process industries. Layer of protection analysis (LOPA) is commonly used to analyze hazard scenarios and to assess the risk associated with the process. In addition to being a risk analysis method, LOPA is used as an allocation tool to determine what IPL are available, what estimated risk reduction is provided by the IPL, what the residual risk gap is, and what risk reduction is needed to close the risk gap.

The risk gap is often closed using a safety instrumented function (SIF) implemented by a safety instrumented system (SIS). The risk reduction allocated to the SIF determines the required safety integrity level (SIL) of the SIF. The SIS is then designed, installed, operated, maintained, tested and managed according to IEC 61511[1]. This standard requires in clause 11.9.1 that the design and management strategy be verified by calculation to demonstrate a performance better than the target criteria determined in the LOPA.

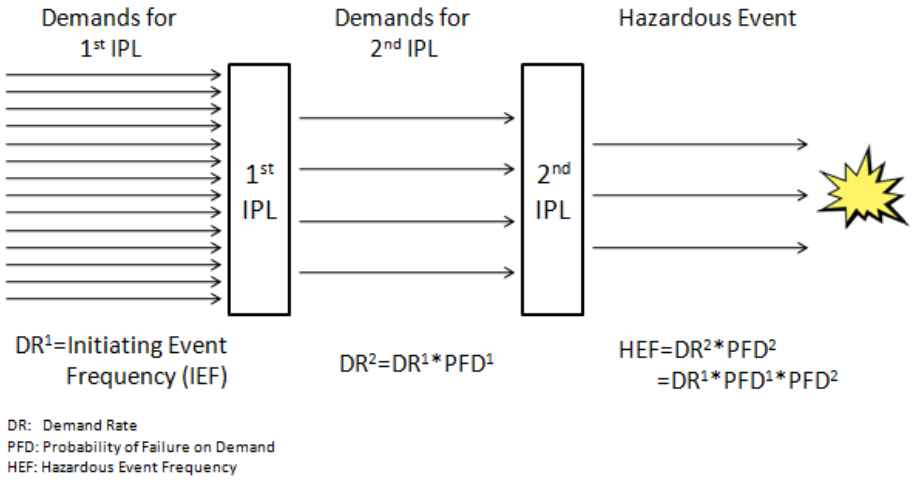

Figure 1. Defense-in- depth philosophy

The defense-in-depth philosophy may be illustrated by the incident sequence shown in Figure 1. A hazardous event starts with an initiating event that places a demand on the IPL, such as a process disturbance, human error, equipment failure, etc. IPLs are specifically designed and implemented to stop the initiating event from propagating into a hazardous event. When an initiating event occurs, a demand is placed on the first IPL. If this IPL functions properly, the hazard scenario stops. But if the first IPL fails to stop the initiating event, a demand is placed on the second IPL. If the second IPL fails, a demand is placed on the next IPL. If all of the IPLs fail to act properly, a hazardous event occurs. Therefore the hazardous event frequency (HEF) is a function of the initiating event frequency and the likelihood that the IPLs fail to work correctly.

The LOPA method [2, 3] is built upon the defense-in-depth philosophy and a fundamental assumption is that the safety integrity of an IPL is measured by the average probability of failure on demand (PFD). The LOPA method can be mathematically represented by Equation 1.

$$HEF = DR^1 \times PFD^1 \times PFD^2 \times \ldots \quad [1]$$

where:

HEF= Hazardous Event Frequency (per time)
DR^1= Demand Rate (Frequency, per time)
PFD^1= PFD of the first IPL (Probability, unitless)
PFD^2= PFD of the second IPL (Probability, unitless)

One condition that is often underappreciated is that for this calculation to be valid, the demand rate on the next IPL or HEF cannot be greater than the frequency of failure of the IPL under consideration. For example a demand rate of 10 times per year would greatly exceed the failure frequency achievable by most continuous interlocks of 1/10 years. If Equation 1 is used and the interlock PFD is 10^{-1}, the HEF = 10 times per year $\times 10^{-1}$ = 1 incident/year, which is greater than the failure frequency of the interlock. The hazardous event cannot happen at a frequency greater than the interlock failure frequency, which is 1/10 years. Mathematically, the limiting condition for this transition can be represented by Equation 2.

$$HEF \; or \; DR^{n+1} = DR^n \times PFD^n \leq PFH^n \quad [2]$$

where:

DR^n = The demand rate of n^{th} IPL
PFD^n = Average probability of failure on demand of the n^{th} IPL
PFH^n = Frequency of dangerous failures per hour of the n^{th} IPL.

As the demand rate increases, it is not uncommon that the limiting condition in Equation 2 is violated. When the conditions in Equation 2 are not met, the PFD is no longer an appropriate safety integrity measure for the IPL, and the typical LOPA calculation represented by Equation 1 leads to an incorrect risk analysis and SIL requirement.

IEC 61511 differentiates its requirements according to the mode of operation: low demand, high demand and continuous. The standard further prescribes that PFD is only valid in low demand applications, and PFH is used for high demand and continuous applications. Then, is the typical LOPA calculation still valid when PFH is the appropriate safety integrity measure? And how should the LOPA calculation be modified if the current one is not adequate?

An example is used to show how the typical LOPA calculation in high demand and continuous applications leads to incorrect SIL requirement. To address this problem, a revised calculation is presented. The remaining paper is structured as follows. Section 2 discusses the classification of SIF modes of operation, and section 3 reviews the typical LOPA calculation. In section 4, an example of a SIF in high demand mode from a flare gas recovery and compression (FGRC) unit is used to show how excessive target SIL can be result from the typical LOPA calculation. A method to address high and continuous applications is proposed and illustrated using the same example. A brief discussion of PFH calculation of high and continuous mode SIFs is provided in section 5. Concluding remarks are given in section 6. Two important LOPA topics uncertainty

and dependent failures are not covered in this paper. The readers are referred to Freeman and Summers [4] and Jin and Summers [5] for detailed discussions.

2 SIS Operation modes

IEC 61511[1] defines three modes of operation for a SIF:

- Low demand mode: *mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year.*
- High demand mode: *mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year*.
- Continuous mode: *mode of operation where the SIF retains the process in a safe state as part of normal operation.*

The mode of operation affects two key requirements in IEC 61511. The first is clause 11.4 on the minimum hardware fault tolerance (HFT) requirement for SIL 2. For a low demand SIF, the minimum HFT requirement is 0 to claim SIL 2, whereas for a high demand/continuous SIF, the minimum HFT requirement is 1 to claim SIL 2. The second is the safety integrity measure in clause 9.2. For a low demand SIF, the safety integrity requirement is measured by PFD, whereas for a high demand/continuous SIF, the safety integrity requirement is measured by PFH. See Table 1 for details of each SIL.

Table 1. Safety integrity requirements

Safety integrity level (SIL)	Low demand mode	High demand/continuous mode
	Average probability of failure on demand (PFD)	Frequency of dangerous failures per hour (PFH)
4	>=10E-05 to <10E-04	>=10E-09 to <10E-08
3	>=10E-04 to <10E-03	>=10E-08 to <10E-07
2	>=10E-03 to <10E-02	>=10E-07 to <10E-06
1	>=10E-02 to <10E-01	>=10E-06 to <10E-05

The HFT requirement has no impact on the LOPA process and hence is out of the scope of this paper. This paper focuses on the rationale for the differences in the safety integrity measure for low demand and high demand/continuous mode SIFs. Why are there different safety integrity measures for different operating modes?

Consider a SIF operating continuously as the last line of defense. A hazardous event occurs whenever the SIF fails dangerously. The HEF is equal to the dangerous failure frequency of the SIF. In IEC 61511, the SIL of a continuous mode SIF is determined by frequency of dangerous failures per hour (PFH) as shown in Table 1.

For a SIF operating in demand mode as the last line of defense, a hazardous event occurs when there is an initiating event (IE) demanding the SIF to respond and the SIF fails to do so. The HEF is equal to the IE frequency multiplied by the likelihood that the SIF is unavailable when the IE occurs. In IEC 61511, the SIL of a demand mode SIF is determined by PFD. This logic would seem to apply to any demand based operation. However at some rate of occurrence, the demands are so frequent that the SIF can no longer be judged by it probability of failure. The HEF is instead being limited by the SIF failure frequency. Where does this transition occur?

According to IEC 61511, the transition occurs at a demand rate of 1 per year. The rationale for this guidance is given in ISA TR 84.00.04 [6]. ISA TR 84.00.04 uses a single channel (1-out-of-1) system as an example. For such an IPL with a test interval of TI, the PFD and PFH can be calculated as follows:

$$\mathbf{PFD} = \frac{\boldsymbol{\lambda_{DU}} \times \mathbf{TI}}{\mathbf{2}} \qquad [\mathbf{3}]$$

$$\mathbf{PFH} = \boldsymbol{\lambda_{DU}} \qquad [\mathbf{4}]$$

If instead of average PFD, the maximum PFD at the time right before the testing is used for the purpose of being conservative, the PFD becomes

$$\mathbf{PFD} = \boldsymbol{\lambda_{DU}} \times \mathbf{TI} \qquad [\mathbf{5}]$$

Inserting the above PFD and PFH into Equation 2, the limiting condition on the LOPA calculation becomes:

$$\mathbf{DR} \times \boldsymbol{\lambda_{DU}} \times \mathbf{TI} \leq \boldsymbol{\lambda_{DU}} \text{ ==> } \mathbf{DR} \times \mathbf{TI} \leq \mathbf{1} \text{ ==> } \mathbf{DR} \leq \frac{\mathbf{1}}{\mathbf{TI}} \qquad [\mathbf{6}]$$

Assuming 1 year test interval, the limiting condition becomes a demand rate of less than or equal to 1 per year. When the demand rate is higher than 1 per year, PFH should be used as the safety integrity measure. This relationship is incorporated into the PFH and PFD ranges given in Table 1. The relationship of PFD and SIL was originally accepted in the 1980s and the PFD ranges were converted into PFH in the 1990s by assuming 1 demand per year with 1 year being comprised of 10,000 hours to keep the ranges as orders of magnitude. It should be pointed out that classification of a SIF as low demand or high demand is dependent on both the demand rate and the test interval. For example, if the test interval is 5 years, the limiting condition would be 1 demand every 5 years instead of 1demand per year.

3 Low Demand SIS System in a LOPA

When using LOPA, Equation 1 can be used to calculate the HEF for comparison with the tolerable event frequency (TEF) to determine whether the risk level is acceptable. When using LOPA to determine the safety integrity necessary to achieve the TEF, Equation 1 can be rearranged to as follow.

$$Residual\ Risk\ Gap\ SIS = \frac{TEF}{DR \times PFD^1 \times PFD^2 \ldots} \qquad [7]$$

As an example, consider a tower overfill scenario where the overfill may be initiated by a BPCS failure. The overfill can be prevented by 3 IPLs: 1) operator response to an alarm, 2) a SIF and 3) a relief valve (RV). Apply typical LOPA calculation as shown in Equation 1, the scenario may be illustrated by Equation 8:

$$TEF = BPCS\ Failure\ Frequency \times Alarm\ PFD \times SIF\ PFD\ \times\ RV\ PFD \qquad [8]$$

Assuming a TEF of 10^{-4} per year, a PFD of 10^{-1} for the alarm IPL, and 10^{-1} per year failure frequency for the BPCS, it is straightforward to yield a 10^{-1} risk gap and a SIL 1 requirement for the SIF.

$$Residual\ Risk\ Gap\ SIS = \frac{10^{-4}/\text{year}}{10^{-1}/\text{year} \times 10^{-1} \times 10^{-1}} = \frac{10^{-4}}{10^{-3}} \qquad [9]$$

$$= 10^{-1} ==> SIL\ 1\ SIF$$

It should be noted that the TEF and IE frequency are the only frequencies, which conforms to a basic reliability math rule that you can multiple probabilities and frequency but you cannot multiple frequencies together. It should also be noted that the expected operation sequence is:

Operation Sequence ==> Alarm ==> SIS==> RV [10]

This sequence determines the demand rate for each of the IPLs. In this particular example, with a BPCS failure frequency assumed to be 10^{-1} per year, the SIF implemented in the SIS are in the low-demand range. Hence, the LOPA for this scenario determines that the SIF has a SIL 1 requirement.

4 High Demand/Continuous Mode SIS in a LOPA

As discussed in Section 2,the transition between low demand and high demand/continuous mode is dictated by the limiting condition calculation. If the demand rate on the SIF exceeds the limit, the HEF is calculated using the frequency of IPL failure rather than the typical LOPA calculation, see Equation 11. *If the correct math is not used, the allocated SIL is likely to be higher than required.*

$$HEF = PFH^1 \times PFD^2 \times PFD^3 \times \ldots \qquad [11]$$

where:

HEF = Hazardous Event Frequency (per time)
PFH^1= Failure frequency of the first IPL (per time)
PFD^2= PFD of the second IPL (Probability, unitless)
PFD^3= PFD of the third IPL (Probability, unitless)

There is folklore in the industry that continuous mode SIFs do not exist within the process industry. This is simply not correct. While unusual, they exist in a wide range of processes. For example, consider the dynamic positioning of a drillship or the control of the ethylene/oxygen ratio in an ethylene oxide reactor. Both of these functions must work continuously or else the hazardous event propagates.

High demand SIFs are commonly encountered. High demand mode may be caused by how the SIF prevents the hazardous event. Consider a valve interlock where the operator is prevented from moving a particular valve until a set of valves is properly aligned. Each time the operator does the lineup, there is the potential that the interlock may need to prevent the valve movement. If the operator does this activity as part of a normal batch routine, the valve interlock is likely in high demand mode. High demand mode may also be due to the number of potential sources of the hazardous event. For example, in a subsea production system where several subsea production trees feed the same platform, an abnormal situation in any of the subsea production trees may require a process shutdown on the platform. Whereas demand from each subsea production tree may be in low demand range, taken together, the demand rate from all sources can be high. Finally, high demand mode can come from unstable process control where process deviations occur more frequently than desired. These latter sources of demand should be addressed through improvements in the control system to reduce the demand rate rather than relying on IPLs to achieve the TEF.

4.1 Example system description

Multiple initiating events can occur in an FGRC unit that demands the IPLs to react. One of those initiating events is unintended gas compressor shutdown in a string of flare gas recovery compressors that fed a flare. The potential consequence of gas compressor shutdown is rupture of a vessel and lines leading to fire and explosion. To avoid this consequence, two IPLs are used as part of the protection strategy.

- A SIF comprising 2-out-of-3 (2oo3) voted pressure transmitters, a safety PLC, and a quick open valve controlled by a de-energize to trip solenoid.
- A pressure relief system comprising two redundant buckling pin valves.

4.2 Misapplication of LOPA to high demand SIF

LOPA was performed by the operating company to determine the SIL requirement for the SIF. This high pressure scenario is illustrated by Figure 2. If the SIF operates as required when demanded, the hazard scenario stops, otherwise a demand on the buckling pin valves occurs. If the buckling pin valves operate as required, the hazard scenario stops, otherwise a hazardous event will occur. Hence:

- The demand rate for the SIF (DR1) is the initiating event frequency
- The demand rate for the buckling pin valves (DR2) is the initiating event frequency time the PFD of the SIF
- The HEF is the product of the initiating event frequency, PFD of the SIF and PFD of the buckling pin valves

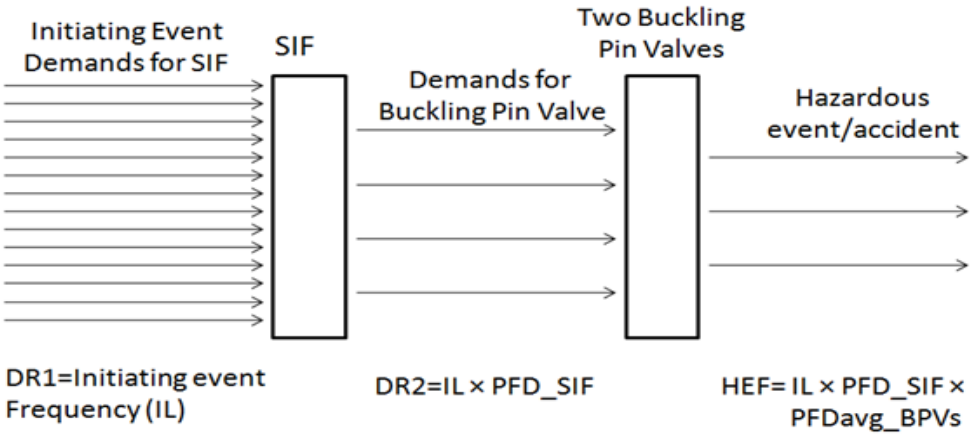

Figure 2. FRGU high pressure protection strategy low demand

In the LOPA, it is determined that the initiating event leading to high pressure occurs 50 times per year. With the two LOPA credits (PFD=10^{-2}) from the two buckling pin valves, it is determined that a SIL 3 (RRF =5000) SIF is required to achieve the desired TEF target of 10^{-4} per year. The SIL 3 requirement was determined based on the assumption that PFD was the appropriate measure for the proposed SIF. The typical LOPA calculation is given by Equation 12.

$$Residual\ Risk\ Gap\ SIS = \frac{TEF}{IL \times PFD^{BPV}} \qquad [12]$$

$$= \frac{10^{-4}/\text{year}}{50\ /\text{year} \times 1 \times 10^{-2}}$$

$$= 2 \times 10^{-4} ==> SIL\ 3\ SIS$$

$$==> Residual\ RRF = 5000$$

5 High Demand/Low Demand LOPA Methodology

For the FRGU example, the demand rate is 50 times per year, therefore the SIS is operating in high demand rather than low demand. For a SIF operating in high demand, we need to use PFH instead of PFD for the SIF, see Figure 3. Hence:

- The demand rate for the SIF (DR1) is the initiating event frequency
- The demand rate for the buckling pin valves (DR2) is approximately the PFH of the SIF
- The hazardous event frequency (HEF) is the product of PFH of the SIF and PFD of the buckling pin valves

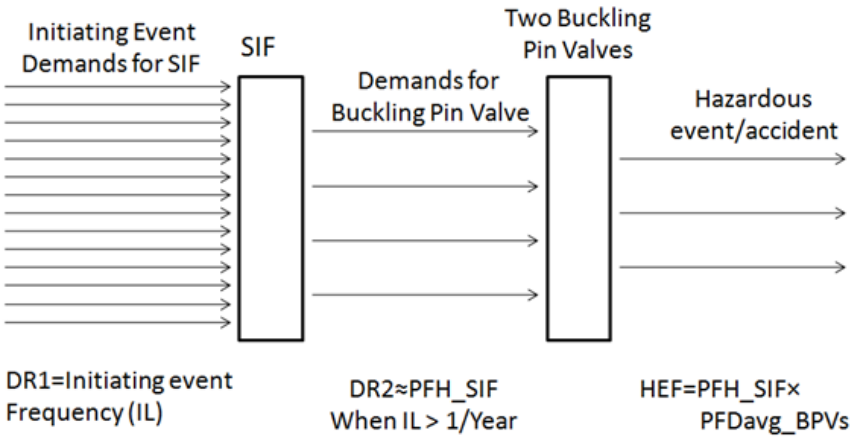

Figure 2. FRGU high pressure protection strategy high demand

We can modify the LOPA calculation to reflect this in Equation 13, and using the

$$Residual\ Risk\ Gap\ SIS = \frac{TEF}{PFD^{BPV}} \quad [13]$$

$$= \frac{10^{-4}\ per\ year}{1 \times 10^{-2}} = 10^{-2}\ per\ year$$

$$= 1.14 \times 10^{-6}\ per\ hour \Longrightarrow \text{SIL 1 SIF}$$

From the result, we can see that instead of a SIL 3 requirement as determined by the typical LOPA calculation, the actual requirement should be a SIL 1.

6 PFH Calculation

Lots of publications are available for PFD calculation, but not so many for PFH calculation [14]. To verify that a SIF operating in high demand/continuous mode meets the SIL requirement. The PFH of the SIF is calculated and compared with the values in the Table 1. Similar to PFD calculation, the PFH_{SIF} for a simple SIF is calculated as the sum of the PFH of the input subsystem (IS), logic solver (LS) and final element (FE):

$$PFH_{SIF} = PFH_{IS} + PFH_{LS} + PFH_{FE} \quad [14]$$

For the FRGU example, the input subsystem is 2-out-of-3(2oo3) voted pressure transmitters, the logic solver is a safety PLC, and the final element is a quick open valve controlled by a de-energize to trip solenoid.

The PFH of the logic solver is simply equal to the dangerous failure rate of the logic solver.

The PFH of the final element is equal to the sum of the dangerous failure rate of the solenoid and the quick open valve because the final element fails if either the solenoid or the quick open valve fails.

For the PFH calculation of the 2oo3 voted pressure transmitters, the calculation is a bit more complicated. The input subsystem fails when two or more transmitters fail. The input subsystem failure can be the result of independent failures or a common cause failure. The failures do not need to be simultaneous. The system failure could occur when the second transmitter fails before the first one is repaired. So, the PFH contribution from independent failures can be calculated as the product of the failure rate of one transmitter and the probability that one of the remaining two transmitters fails before the first transmitter is repaired. Mathematically, this is expressed as in Equation 15, where 3 represents that the first failure can happen to any of the 3 transmitters, the first λ_{PT} is the dangerous failure rate of first failed transmitter, 2 represents that the second failure can happen to any of the 2 remaining transmitters, and $\lambda_{PT} * (MTTR_{PT} + \frac{TI_{PT}}{2})$ is the probability that one transmitter fails before the first failure is repaired.

$$PFH_{IS} = 3 * \lambda_{PT} * 2 * [\lambda_{PT} * (MTTR_{PT} + \frac{TI_{PT}}{2})] \quad [15]$$

The contribution of common cause to the input subsystem failure can be calculated with the widely accepted beta factor method. The common cause PFH is the product of the beta factor and the transmitter dangerous failure rate.

Hence the PFH_{SIF} can be calculated by Equation 16.

$$PFH_{SIF} = 3 * \lambda_{PT} * 2 * \lambda_{PT} * \left(MTTR_{PT} + \frac{TI_{PT}}{2}\right) + \beta\lambda_{PT} + \lambda_{LS} + \lambda_{SOV} + \lambda_{QOV} \quad [16]$$

Using reliability parameters from SIL Solver® [8] in Table 2, the PFH of the SIF is calculated as 2.9×10^{-6} per hour. Compare with the PFH range for SIL in Table 1, the PFH_{SIF} meets the SIL 1 requirement for high demand mode.

Table 2. Example calculation parameters

Parameter	λ_{PT}(/yr)	λ_{LS} (/yr)	λ_{SOV} (/yr)	λ_{QOV} (/yr)	$MTTR_{PT}$ (hr)	TI_P (/yr)	β
Value	6.67×10^{-3}	2.10×10^{-4}	1.67×10^{-2}	8.33×10^{-3}	72	1	2%

It should be noted that from Equation 16, it seems that the test intervals of the solenoid and the quick open valve do not affect the SIF PFH. This conclusion is premature, because in Equation 16, the failure rates are based on the assumption that an appropriate mechanical integrity program is in place. Without a mechanical integrity program requiring inspection, testing and maintenance with appropriate interval, the failure rates used in Equation 16 cannot be sustained. Therefore it is important that the valves and solenoids are tested regularly.

7 Concluding remarks

Typical LOPA calculations have the inherent assumption that the IPLs are in low demand operation. Assessing high demand or continuous IPLs using low demand assumptions results in

excessive risk reduction requirements. An approach is proposed to correctly determine the SIL requirement when the SIF is operating in high demand or continuous mode. High demand and continuous mode SIFs are not uncommon in the process industry, so it is important to use appropriate calculation techniques to avoid incorrect application of LOPA and potentially excessive SIL requirements.

8 References (examples given to show format).

[1] IEC. IEC 61511 Functional safety: Safety Instrumented Systems for the Process Industry Sector - Part 1-3, Final Draft International Standard. Geneva: IEC. 2015.

[2] A. E. Summers. *Introduction to layers of protection analysis.* Journal of Hazardous Materials. Volume 104, Issue 1-3 (2003), Pages 163–168.

[3] CCPS. Layer of Protection Analysis: Simplified Process Risk Assessment. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2001.

[4] R. Freeman and A. E. Summers. *Evaluation of uncertainty in safety integrity level calculations.* Process Safety Progress. Available online since November 2015.

[5] H. Jin and A. E. Summers. *Dependent, Independent, and Pseudo-independent Protection Layers in Risk Analysis*. Process Safety Progress. Available online since November 2015.

[6] ISA. ISA TR 84.00.04. Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod). The International Society of Automation, North Carolina, 2015.

[7] H. Jin, M.A. Lundteigen and M. Rausand. *New PFH-formulas for k-out-of-n:F-systems*. Reliability Engineering and System Safety. Volume 111 (2013), Pages 112–118.

[8] SIS-TECH. SIL Solver 7.0, SIS-TECH Solution, Houston, TX.