A Streamlined Approach for Full Compliance with SIF Implementation Standards

William G. Bridges, President
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)
1321 Waterside Lane, Knoxville, TN 37922
Phone: (865) 675-3458
Fax: (865) 622-6800
e-mail: wbridges@piii.com

Art Dowell III, Principal Engineer
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)
2437 Bay Area Blvd PMB 260
Houston, TX 77058
Phone: 713-865-6135
e-mail: adowell@piii.com

Prepared for Presentation at
13th Global Congress on Process Safety
San Antonio, TX
March 27-29, 2017

UNPUBLISHED

A Streamlined Approach for Full Compliance with SIL Implementation Standards

William G. Bridges, President
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)
e-mail: wbridges@piii.com

Art Dowell III, Principal Engineer
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)
e-mail: adowell@piii.com

Keywords: Safety Instrumented System, SIS, Safety Integrity Level, SIL, LOPA, Layer of Protection Analysis, Independent Protection Layers, IPLs, human factors

Abstract

Many companies put FAR too much redundant effort into determining what SIL (safety integrity level) is needed and then verifying the SIF (safety instrumented function) design will give the SIL targeted. This paper shows how to apply the qualitative definition of independent protection layers (IPLs) within the setting of a process hazard analysis (PHA) to get most of the gain from Layer of Protection Analysis (*LOPA)* without doing a LOPA (without using numerical values). We show how we use a PHA team to identify when a SIF is needed and to select the proper target SIL. This portion of the SIL evaluation and the identification and labeling of the IPLs during the PHA/HAZOP does not take any longer than a normal PHA/HAZOP, once the right habits are established. Note that this approach eliminates the need for a separate SIL Evaluation Study to identify the SIFs and select the target SIL. Then, this paper describes how to perform the SIL Verification and Safety Requirements Specification (SRS) remotely, again without the need for a redundant team meeting. This approach has been used at many sites and for thousands of SIFs.

Background

Typically, hazardous consequences, their causes, and safeguards are identified in a PHA/HAZOP (process hazard analysis / hazard and operability analysis)[1]. The PHA may determine if additional protection layers are required or if additional analysis is required.[2]

In many organizations, a separate LOPA (layer of protection analysis)[3] meeting is held to determine which HAZOP safeguards are independent protection layers (IPLs) and to determine if additional IPLs are needed to meet the risk tolerance criteria. If SIFs are needed, the required risk reduction (PFD, probability of failure on demand) is determined in LOPA, which then sets the SIL.

Some organizations may even have a separate SIL evaluation study, which is certainly redundant to a well-run PHA and is wasteful if the PHA is properly staffed and managed and/or if any subsequent LOPA are performed well.

Fundamentals of SIL Assessment

The lifecycle requirements for safety instrumented functions are specified in industry standards IEC 61511 (ANSI/ISA 84.00.01-2004, Part 1)[4,5]. The required steps to specify the SIS (safety instrumented system) are:

1. Safety Instrumented Function (SIF) identification.
2. Determining the Safety Integrity Level (SIL) for each SIF.
3. Designing the SIF to meet the required SIL.

   SIL Verification Calculation (actually, this calculation is iterative with step 3, but the end calculation is a deliverable that proves 3 is correct). The SIL standards allow the following methods to use to determine the required SIL (ANSI/ISA 84.00.01-2004, Part 3, Section 3.8)[4]:

   - Fault Tree Analysis (FTA), Full Quantitative Risk Analysis (QRA)
   - LOPA – simplified quantitative analysis
   - Qualitatively within PHA (HAZOP, etc.)

   > "A qualitative method may be used as a first pass to determine the required SIL of all SIFs. Those which are assigned a SIL 3 or 4 by this method should then be considered in greater detail using a quantitative method to gain a more rigorous understanding of their required safety integrity." – *ANSI/ISA 84.00.01-2004, Part 3, Section 3.8*[4]

Table 1 compares risk analysis approaches for Steps 1 and 2.

FTA and QRA are very detailed and labor-intensive and would be required for complicated systems, particularly where there is not complete independence between safeguards.

LOPA is a simplified analysis tool that requires fewer resources, but is heavily dependent on the requirement that all the safeguards be completely independent.

However, for many processes, there are a number of scenarios (cause leading to a consequence) where the PHA team can readily determine sufficient independent protection layers are already in place.

Table 1: Comparison of Risk Analysis Approaches

Approach	Assessment Methods	Risk Judgment Method	Risk Judgment Method	Estimated Range of the Results
Qualitative Only	HAZOP, FEMA	Expert Voting, focusing on site data	**Capable >95% of time**	Plus or minus 1/2 order of magnitude
Simplified Quantitative	LOPA, Risk Graph	Multiplication of statistical averages of general failure rate data; with broad assumptions on management systems	**Needed on about 5% of the scenarios**	Plus or minus 1 order of magnitude
Full Quantitative	FTA, ETA, QRA, HRA		**Needed for less than 0.01% of the scenarios**	Plus or minus 1 order of magnitude

Figure 1 contrasts the typical approach to SIL assessments with the optimized streamlined approach.

Typical SIL Determination versus Streamlined Approach

In the typical approach,

- **Step 1**: The PHA/HAZOP is performed using a multidisciplinary team of engineers, operators, instrumentation staff, maintenance staff, and perhaps vendors. Then in a separate SIL study, a multidisciplinary team of engineers, instrumentation staff, maintenance staff, and perhaps vendors brainstorm the hazard scenarios (again) and decide which are candidates for SIFs. A semi quantitative approach, such as RiskGraph, or layer of protection analysis, determines if an SIF is required.
- **Step 2:** The RiskGraph dictates the required SIL, or the LOPA compares the mitigated risk to the risk tolerance criteria and determines the SIL from the order-of-magnitude risk reduction needed.

In contrast, in the streamlined approach,

- **Step 1:** The PHA/HAZOP is performed using a multidisciplinary team of engineers, operators, instrumentation staff, maintenance staff, and perhaps vendors (to this point the same as the typical approach). Within the PHA/HAZOP, the team estimates the risk of each scenario using qualitative judgment (based on experience, knowledge, and memory of site-specific data). The PHA/HAZOP team then qualitatively determines if the best risk reduction method is an SIF.
- **Step 2:** The PHA/HAZOP team qualitatively determines the SIL needed (typically by judging the level of redundancy needed based on the value they place on each IPL and the new or modified SIF needed)

Figure 1: Comparison of the Typical and the Optimized Streamlined Approach from PII for SIL Assessments (Steps 1 and 2)

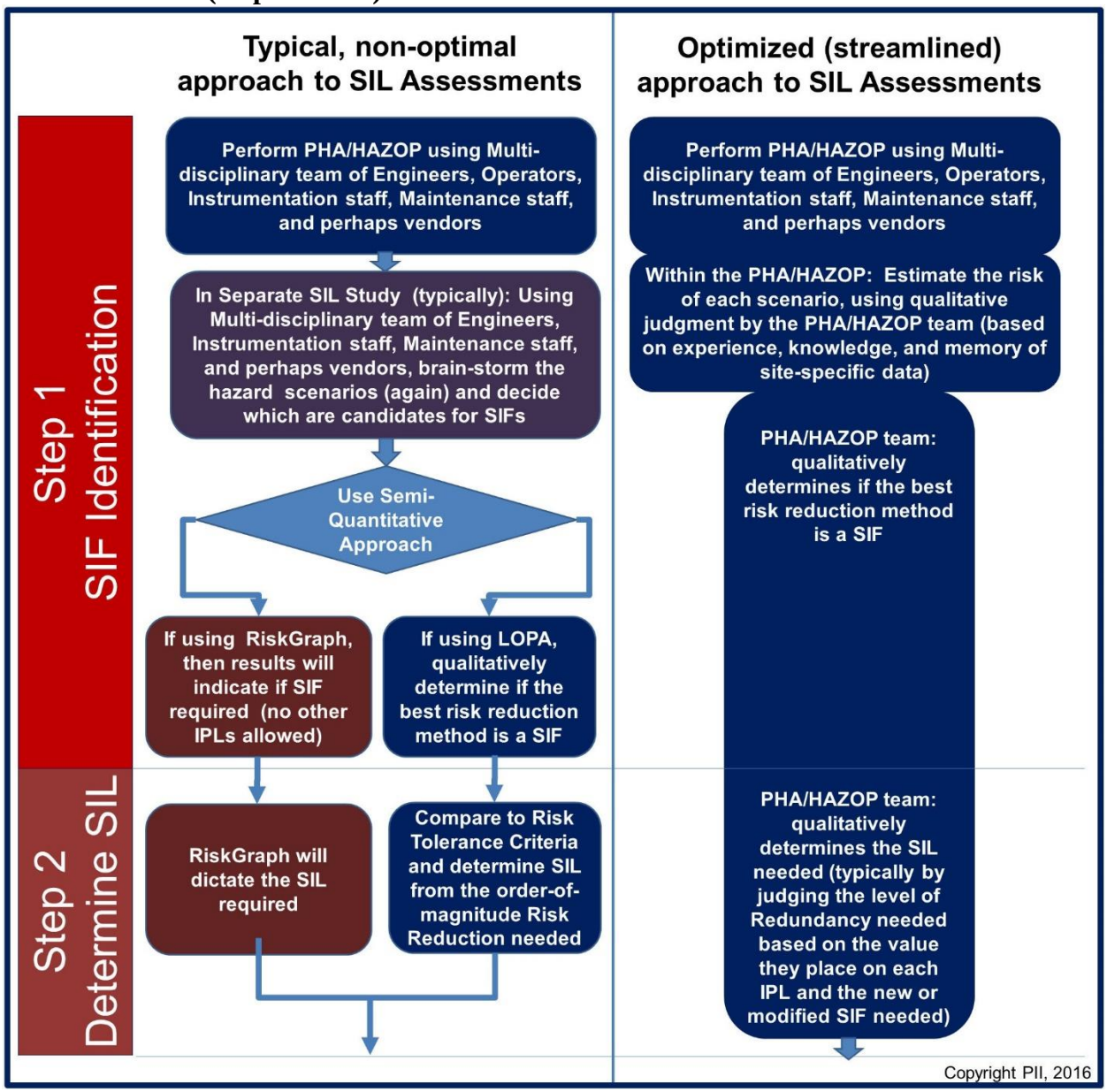


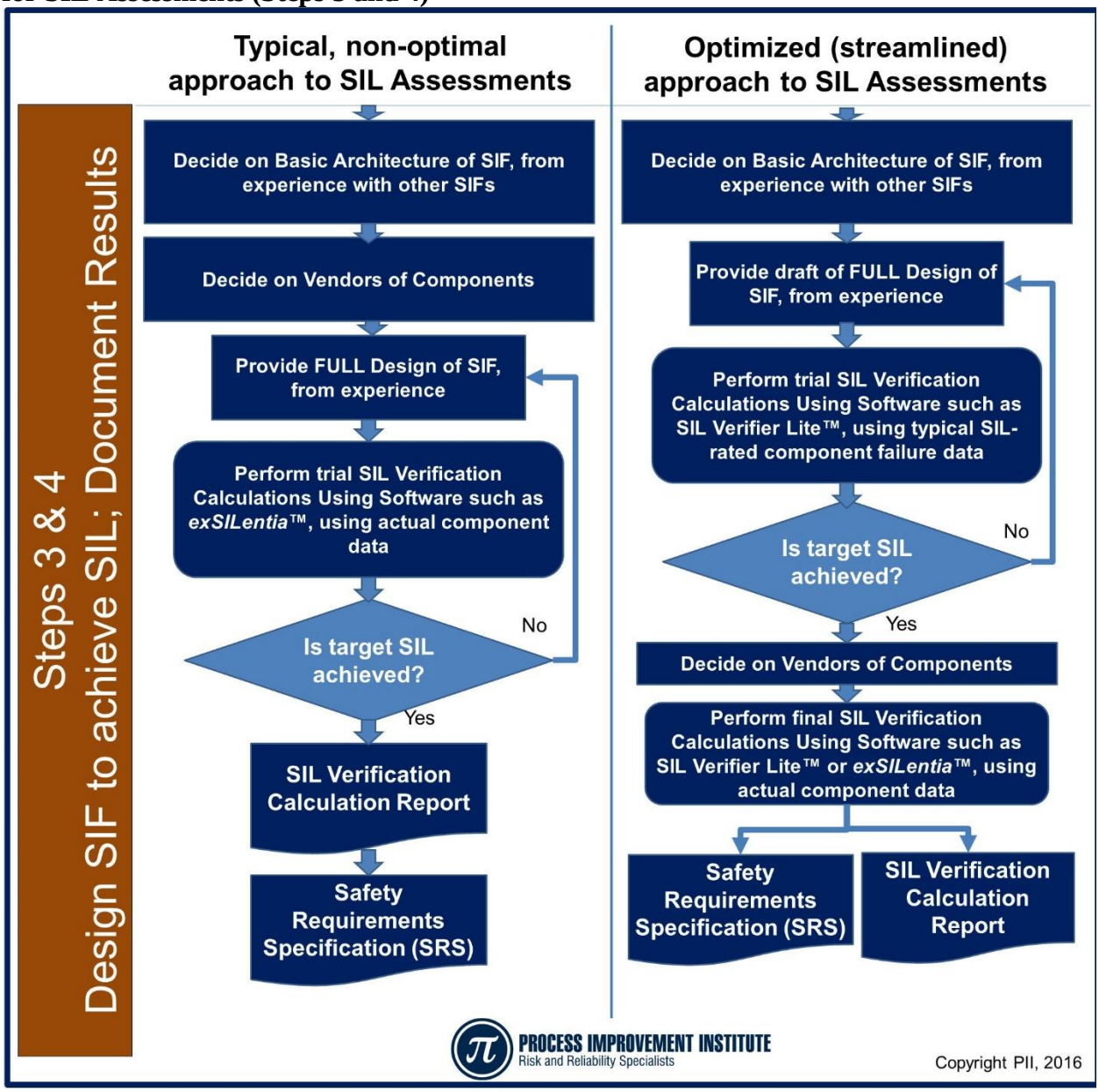
Figure 2 also contrasts the typical approach to SIF design and verification with the streamlined approach. Steps 3 and 4 are iterative.

In the typical approach,

- **Steps 3 and 4**:
  - Decide on basic architecture of SIF, from experience with other SIFs.
  - Decide on vendors of components
  - Provide full design of SIFs from experience

- Perform trial SIL verification calculations using software such as exSILentia™ using actual component data
- If the target SIL is achieved, issue the SIL verification calculation report and the safety requirement specification (SRS)
- If the target SIL is not achieved, revise the design and recalculate.

Figure 2: Comparison of the Typical and the Optimized Streamlined Approach from PII for SIL Assessments (Steps 3 and 4)



In the streamlined approach,

- **Steps 3 and 4**:
  - Decide on basic architecture of SIF, from experience with other SIFs.

- Provide draft of full design of SIF, from experience.
- Perform trial SIL verification calculations using software such as SIL Verifier Lite™ using typical SIL-rated component failure data.
- If the target SIL is not achieved, revise the design and recalculate.
- If the target SIL is achieved,
    - Issue the SIL verification calculation report and the safety requirement specification (SRS).
    - Decide on vendors of components.
    - Perform final SIL Verification Calculations Using Software such as *SIL Verifier Lite*™ (from PII) or *exSILentia*™ (from exida) using actual component data.
    - Issue the SIL verification calculation report and the safety requirement specification (SRS).

The advantage of the streamlined approach is determination of the need for an SIF and of its SIL quicker and with fewer resources than the typical approach.

Requirements for the Qualitative Streamlined Approach for SIL Determination

For the qualitative streamlined approach to be used effectively, there are important requirements for the PHA/HAZOP team.

- PHA/HAZOP team leader is knowledgeable and proficient in LOPA.
- PHA/HAZOP team members have the following information in memory:
    - Consequence severity.
    - Initiating cause frequency.
    - Independent protection layer (IPL capability).
    - Risk tolerance criteria.

An experienced PHA team, who is knowledgeable in the process technology, can effectively and efficiently analyze a scenario and mentally perform a layer of protection analysis. The team determines the consequence severity and the initiating cause frequency. A highly competent team understands which safeguards are truly independent protection layers and can judge the risk reduction provided by each. Then the team can determine if additional IPLs are required to meet the risk tolerance criteria. For some scenarios, an SIF may be required and the team can determine the required probability of failure on demand for the SIF and can thus determine the required SIL.

A best practice is that the PHA team recommends the functional description and the SIL for the proposed SIF. The functional description does not specify the details of the SIF design, rather it specifies what process variables should be considered and what action should be taken to detect the upset and to prevent the consequence. For example, the functional description may say “monitor the level of a vessel and stop the flow into the vessel to prevent overflow”.

If the PHA team is uncertain, or if the scenario is complex, then the PHA can recommend a detailed LOPA be done for the scenario.

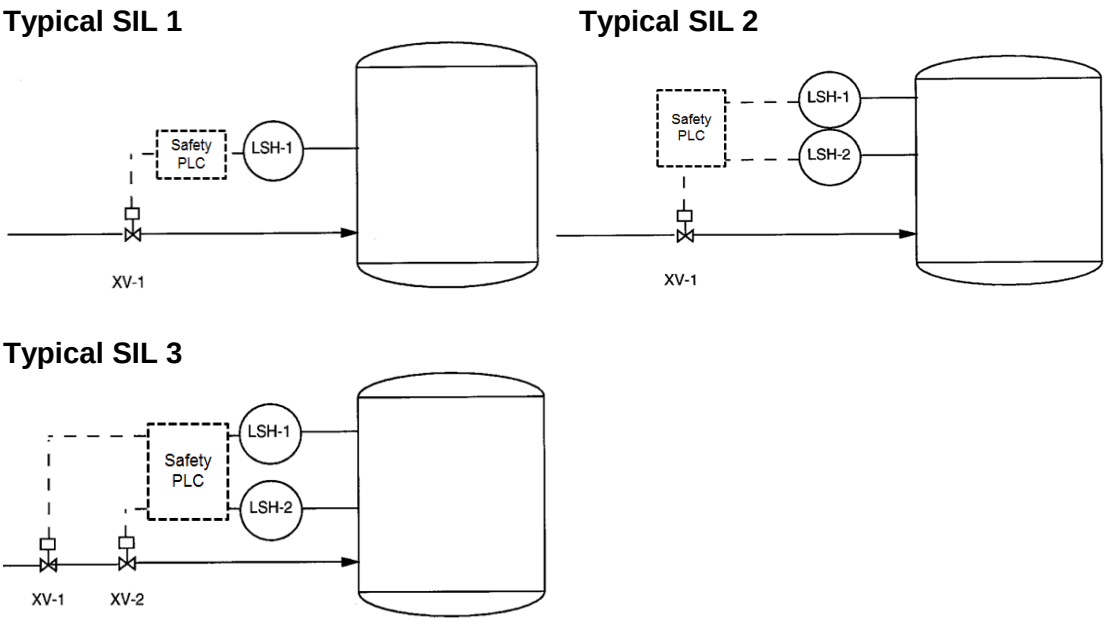
These conclusions are based on more than 8000 PHA/HAZOPs, 3000 LOPAs, and about 100 QRAs and HRAs. We have observed PHA participants becoming knowledgeable about LOPA and IPL requirements. The participants then began to apply the principles of LOPA spontaneously in the PHA. With good leadership, the PHA team could then easily move to the full streamlined approach.

The experience and competency of the PHA leader and the PHA team is extremely important. If the PHA team is not comfortable with the principles of LOPA, and especially the principles of IPLs, the streamlined approach is not appropriate. Likewise, the PHA team must have the required information and understanding in its memory. Otherwise, the qualitative approach can degenerate into the "arm wrestling" arguments that PHA teams used qualitatively to determine SIL requirements before the introduction of LOPA.

Suggestions for the Streamlined Approach for SIF Design

Likewise, there is a streamlined approach for the SIF design. Organizations have developed a recipe book of typical SIF designs for SIL 1, SIL 2, and SIL 3. Depending on the required SIL, the designer can choose a design from the recipe book (as described in Figure 2, "from experience"). The recipe book provides a starting point for the detailed SIF design. Figure 3 shows a small sample of SIF designs that could be included in a recipe book.

Figure 3: Typical SIF Architectures for Information



Case Study 1

An example of the streamlined approach is summarized in Table 2 for a facility with storage spheres (in China; the PHA and other analyses were performed in 2014). The table shows two deviations from the PHA. IPLs are identified and existing SIFs are assigned an SIL, based on the architecture. (Note that the achieved SIL for each of the SIFs (existing or recommended) must be confirmed by a SIL verification calculation that includes the failure rate of the components, the voting architecture, and the proof test interval.)

For the high-level deviation, the high-level SIF was assigned SIL 1. The overflow through the pressure equalization line to other spheres was determined to be an IPL.

For the low level deviation, the low level indication and low level alarm were determined not to be an IPL because they are part of the initiating cause. The PHA team concluded that feeding from two spheres at all times is an IPL for this facility because of the unlikelihood for both spheres to have low level at the same time. The PHA team also thought that an additional SIF level alarm with operator response to switch tanks within 60 minutes could be a possible IPL, if the action of the operator is quick enough. The team wrote a recommendation to ensure that the operator response could be an IPL.

In this case study, the PHA team was able to determine in the PHA meeting which safeguards were IPLs. They also determined the nominal SIL for existing SIFs (to be confirmed in a later SIL verification). And the team determined that operator response could be an IPL if there was a documented procedure and an annual drill. For these two deviations, the PHA team did the work that would be done in a later LOPA meeting in the typical approach.

Next, the SIL Verification was performed for the SIL 1 SIF (and all other SIFs in the unit). This SIL Verification was accomplished using exSILentia™ software and the analysis and documentation took less than 2 hours.

Thus, the entire requirements for a SIL identification, SIL target level determination, and SIL Verification were accomplished very quickly compared to typical approaches.

Table 2: Storage Sphere PHA

No.: 2 XXXX storage spheres xxx-T-XX A/B/C/D/E/F/G/H/I/J/K/L (1 of 12)					
#	**Dev.**	**Causes**	**Consequences**	**Safeguards**	**Recommendations**
2.1	High level	Too much flow to one sphere from XX Plant (through their pump; about 40 bar MDH)	High pressure (see 2.5)	High level SIF with level sensors voted 2oo2, to close inlet valve - **SIL 1** Overflow thru pressure equalization line to other spheres (through normally open [NO] valve) - **IPL**	
2.2	Low level	Failing to switch from the sphere with low level in time (based on level indication)	Low/no flow - Liquid from spheres through high pressure product pumps to the vaporizer (see 4.2)	Level indication and low level alarm, inspected each year, per government regulation **(not IPL; part of the cause)** 9 other spheres with possibly enough level to switch to Feeding from two spheres at all times, so unlikely for BOTH spheres to have low level at the same time - **IPL**	Rec 4. Make sure the Human IPL of response to low level in all spheres and tanks is described in a trouble-shooting guide (like an SOP) and practiced once per year per unit operator. This will make this response a valid IPL.
			Low/no flow - Unqualified liquid from spheres back to Plant (see 6.2)	Two level indication from SIS level transmitter, with low level alarm, with more than 60 min available to switch tanks (SIF driven alarm and response) - **possible IPL, if action of the operator is quick enough**	

Case Study 2

In 2014 and 2015, an identical approach to that of Case Study 1 (the streamlined approach of this paper) was performed for a large gas producer in South America. In that work, the PHAs for more than 500 nodes plus all procedures of all operating modes was completed in about 10 weeks of PHA meetings. The PHA team identified more than 800 SIFs, along with their target SILs, using the approach in Steps 1 and 2.

Next, staff within PII but separate from the PHA team performed about 60 LOPA to clarify certain issues, some related to SIFs. But less than 5% of the SIFs were established with LOPA; 95% were established with the PHA alone.

Finally, staff separate from the PHA performed SIL Verification of the 800+ SIFs, using exSILentia™. The verification was for a combination of SIL 1 and SIL 2 SIFs; a couple of SIL 3 SIFs were also analyzed and debated. The relatively few LOPAs took about 2-3 hours each (due to the complexity of the 5% of scenarios that went to LOPA) and each SIL Verification took about 2-3 hours to perform and document.

Caution – the issue of human factors for SIL 2 and SIL 3 SIFs[6]

There is an important aspect of important aspect of SIFs and the possible achieved SIL that is not addressed in this paper. Relying on a high integrity SIF, without accounting for human error during interventions, is also a waste of resources. You may believe that you have reduced the

risk by a factor of 100 for a SIL 2 SIF, or a factor of 1000 for a SIL 3 SIF, when in fact the human factors during commissioning and proof testing may degrade the overall risk reduction factor to about 10. If the human factor is accounted for in the SIF design phase and the SIL verification phase, then the human error can also be prevented to allow the higher reduction in risk that is targeted.

Conclusions

Based on experience in a multitude of PHAs, LOPAs, QRAs, and HRAs, we have seen that experienced, competent PHA teams with an experienced, competent leader can effectively apply the principles of LOPA to many scenarios during the PHA meeting. The team can determine the approximate SIL of existing SIFs, the team can determine which safeguards are truly IPLs, and the team can recommend additional IPLs, including SIFs with specific SILs. If the scenario is too complex, or the PHA team is uncertain, the team can recommend a detailed LOPA. The streamlined qualitative makes better use of resources and time than the typical approach with separate meetings for PHA and LOPA.

It is critical that the PHA leader is experienced and competent in LOPA. It is critical that the PHA team has in its memory the data for consequence severity, initiating cause frequency, IPL requirements, and the risk tolerance criteria.

Acronyms Used

AIChE– American Institute of Chemical Engineers
CCPS – Center for Chemical Process Safety (an AIChE technology alliance)
HAZOP – Hazard and Operability Analysis
HRA – Human Reliability Analysis
IEC – International Electrotechnical Commission
IEF – Initiating Event Frequency
ETA – Event Tree Analysis
FMEA – Failure Mode Effect Analysis
FTA – Fault Tree Analysis
HRA – Human Reliability Analysis
IPL - Independent Protection Layer
LOPA – Layer of Protection Analysis
PHA – Process Hazard Analysis
PII – Process Improvement Institute, Inc.
QRA – Quantitative Risk Analysis
SIF – Safety Instrumented Function
SIL – Safety Integrity Level
SIS – Safety Instrumented System
SRS – Safety Requirements Specification

References

1. *Guidelines for Hazard Evaluation Procedures,* 2008, CCPS/AIChE.
2. Bridges, W., & Dowell, A., "Identify SIF and Specify Necessary SIL, and other IPLs, as part of PHA/HAZOP," *12th Global Congress on Process Safety*, AIChE, 2015.
3. *Layer of Protection Analysis: Simplified Process Risk Assessment,* 2001, CCPS/AIChE.
4. *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels*; ANSI/ISA 84.00.01 Part 3, 2004.
5. IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements*, International Electrotechnical Commission
6. Bridges, W., and Thomas, H., "Accounting for Human Error Probability in SIL Verification Calculations," *8th Global Congress on Process Safety*, Houston, AIChE, April 2012.