5th Annual Symposium, Mary Kay O'Connor Process Safety Center
"Beyond Regulatory Compliance: Making Safety Second Nature"
Reed Arena, Texas A&M University, College Station, Texas
October 29-30, 2002

INTRODUCTION TO LAYER OF PROTECTION ANALYSIS

Angela E. Summers, Ph.D., P.E, President
SIS-TECH Solutions, LLC
PMB 295
2323 Clear Lake City Blvd.
Houston, TX 77062-8032
Phone: 281-922-8324
Email: asummers@sis-tech.com
www.sis-tech.com

The process industry is obligated to provide and maintain a safe, working environment for their employees. Safety is provided through inherently safe design and various safeguards, such as instrumented systems, procedures, and training. During a HAZOP, the team is responsible for assessing the process risk from various process deviations and determining the consequence of potential incidents. The team identifies the safeguards used to mitigate the hazardous event. If the team determines that the safeguards are inadequate, the team will make recommendations for further risk reduction.

The team is instructed to list all safeguards, whether these safeguards partially or completely mitigate the process risk or whether the safeguards are independent from one another. This often results in the team assuming more risk reduction from the safeguards than is possible based on the integrity of the individual components. Furthermore, a team's perception of the integrity of a specific safeguard impacts the assumed risk reduction for that safeguard, resulting in inconsistency in the number of required safeguards for successful mitigation of the process risk. Unfortunately, the inconsistency can result in over- and under-protected process risk, depending on the team composition. Consequently, there must be an independent engineering assessment of the safeguards to ensure that adequate risk reduction is being provided.

What is LOPA?

Layers of protection analysis (LOPA) is a semi-quantitative methodology that can be used to identify safeguards that meet the independent protection layer (IPL) criteria established by CCPS[1] in 1993. While IPLs are extrinsic safety systems, they can be active or passive systems, as long as the following criteria is met:

[1] CCPS/AIChE, Guidelines for Safe Automation of Chemical Processes, 1993, pp. 7-16.

Specificity: The IPL is capable of detecting and preventing or mitigating the consequences of specified, potentially hazardous event(s), such as a runaway reaction, loss of containment, or an explosion.

Independence: An IPL shall be independent of all the other protection layers associated with the identified potentially hazardous event. Independence requires the performance shall not be affected by the failure of another protection layer or by the conditions that caused another protection layer to fail. Most importantly, the protection layer shall be independent of the initiating cause.

Dependability: The protection provided by the IPL shall reduce the identified risk by a known and specified amount.

Auditability: The IPL shall be designed to regular periodic validation of the protective function.

Examples of IPLs are as follows:

- Standard operating procedures,
- Basic process control systems,
- Alarms with defined operator response,
- Safety instrumented systems (SIS),
- Pressure relief devices,
- Blast walls and dikes,
- Fire and gas systems, and
- Deluge systems.

LOPA is not just another hazard assessment or risk assessment tool. It is an engineering tool used to ensure that process risk is successfully mitigated to an acceptable level. LOPA is a rational, defensible methodology that allows a rapid, cost effective means for identifying the IPLs that lower the frequency and/or the consequence of specific hazardous incidents. LOPA provides specific criteria and restrictions for the evaluation of IPLs, eliminating the subjectivity of qualitative methods at substantially less cost than fully quantitative techniques.

When is LOPA Used?

LOPA can be used at any point in the lifecycle of a project or process, but it is most cost effective when implemented at the detailed design stage when process flow diagrams are complete and the P&IDs are under development. For existing processes, LOPA should be used during or after the HAZOP review or revalidation. LOPA is typically applied after a qualitative hazards analysis has been completed, which provides the LOPA team with a listing of hazard scenarios with associated consequence description and potential safeguards for consideration.

A LOPA program is most successful when a procedure is developed that sets the criteria for when LOPA is used and who is qualified to use it. A well-written procedure will also incorporate criteria for evaluation of initiating cause frequency and IPL probability to fail on demand (PFD). The development of these criteria takes time, but this cost is rapidly offset by the increased speed at which LOPA can be implemented on specific projects.

What is the LOPA process?

The overall LOPA process is illustrated in Figure 1. Depending on the project stage, the process may be initiated differently from what is represented. This should be considered a general overview of LOPA and not a limitation on its applicability.

The six major steps to the LOPA process are as follows:

1) Record all reference documentation, including hazards analysis documentation, pressure relief valve design and inspection reports, protection layer design documents, etc.
2) Document the process deviation and hazard scenario under consideration by the team. It is important to focus the team on a specific hazard scenario, such as high pressure resulting in pipeline rupture.
3) Identify all of the initiating causes for the process deviation and determine the frequency of each initiating cause. The team should list all initiating causes of the hazard scenario, such as loss of flow control, loss of pressure control, excess reaction, etc. The initiating cause frequencies should be based on industry-accepted and standards-compliant failure rate data for each device, system, or human. For rapid execution of the LOPA methodology, the initiating cause frequency for common systems should be provided in the procedure.
4) Determine the consequence of the hazard scenario. This evaluation should include an examination of safety, environmental, and economic losses. Safety and environmental impacts must be mitigated for OSHA compliance. However, economic loss prevention is strictly a company decision and is not covered under any regulatory mandate. The economic risk should be assessed to ensure that loss prevention goals are met, but the risk should be clearly delineated to allow flexibility in the IPL selection and design.

For instance, a hazard scenario may describe damage to furnace tubes, causing substantial downtime, but no safety impact. An instrumented system may be used to prevent this economic impact, but the IPL selection, design, operation, testing, and maintenance is not driven by the SIS standards. Cost/benefit analysis can be used to determine what the actual design should be.

Once the team has an understanding of the frequency and consequence of the potential hazardous event, a risk matrix is used to determine whether the risk is acceptable or whether IPLs are required for further risk reduction. The risk matrix is developed, as part of the LOPA procedure, using Corporate risk criteria and provides consistency to the assessment of acceptable risk. Quantitative targets can also be used to assess whether additional risk reduction is required. However, this does require more specific assessment of the consequence and the declaration of a specific numerical risk tolerance, e.g. tolerable fatality rate. Whether a risk matrix or specific numerical risk tolerance is used, if it is determined that additional risk reduction is necessary, the team is required to identify IPLs (Step 5) or list recommendations (Step 6).

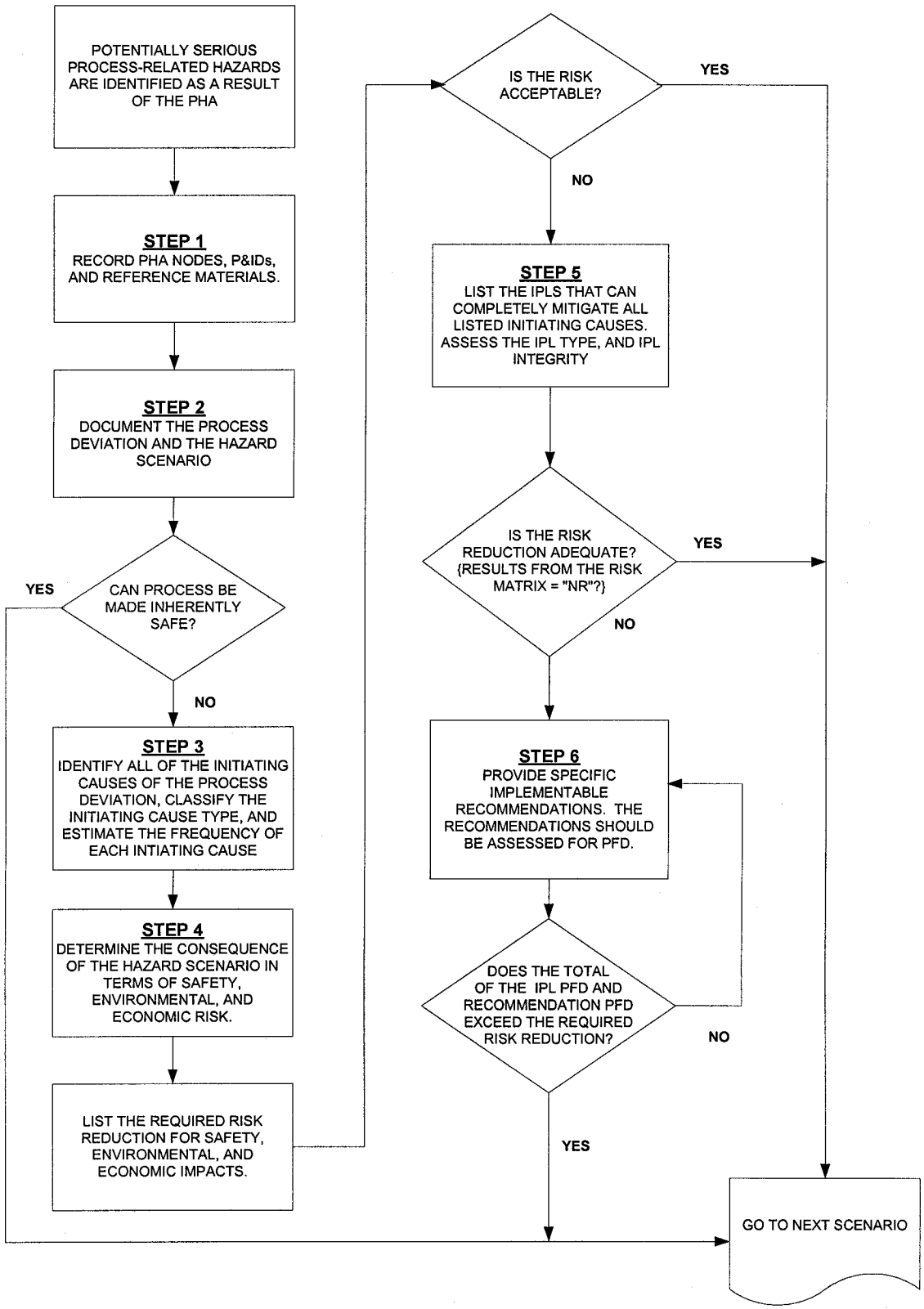
POTENTIALLY SERIOUS PROCESS-RELATED HAZARDS ARE IDENTIFIED AS A RESULT OF THE PHA
STEP 1
RECORD PHA NODES, P&IDs, AND REFERENCE MATERIALS.
STEP 2
DOCUMENT THE PROCESS DEVIATION AND THE HAZARD SCENARIO
CAN PROCESS BE MADE INHERENTLY SAFE?
YES
NO
STEP 3
IDENTIFY ALL OF THE INITIATING CAUSES OF THE PROCESS DEVIATION, CLASSIFY THE INITIATING CAUSE TYPE, AND ESTIMATE THE FREQUENCY OF EACH INTIATING CAUSE
STEP 4
DETERMINE THE CONSEQUENCE OF THE HAZARD SCENARIO IN TERMS OF SAFETY, ENVIRONMENTAL, AND ECONOMIC RISK.
LIST THE REQUIRED RISK REDUCTION FOR SAFETY, ENVIRONMENTAL, AND ECONOMIC IMPACTS.
IS THE RISK ACCEPTABLE?
YES
NO
STEP 5
LIST THE IPLS THAT CAN COMPLETELY MITIGATE ALL LISTED INITIATING CAUSES. ASSESS THE IPL TYPE, AND IPL INTEGRITY
IS THE RISK REDUCTION ADEQUATE? {RESULTS FROM THE RISK MATRIX = "NR"?}
YES
NO
STEP 6
PROVIDE SPECIFIC IMPLEMENTABLE RECOMMENDATIONS. THE RECOMMENDATIONS SHOULD BE ASSESSED FOR PFD.
DOES THE TOTAL OF THE IPL PFD AND RECOMMENDATION PFD EXCEED THE REQUIRED RISK REDUCTION?
NO
YES
GO TO NEXT SCENARIO

Figure 1

5) List the IPLs that can completely mitigate all listed initiating causes. The IPLs must meet the independence, specificity, dependability, and auditability requirements. This means that the IPL must be completely independent from the initiating cause, e.g., if a process control loop is the initiating cause, an alarm generated by the process control transmitter can not be used for risk reduction.

   For each IPL, determine the probability to fail on demand (PFD). The PFD is a measure of the risk reduction that can be obtained using the IPL. For safety instrumented systems, the PFD is equivalent to the Safety Integrity Level (SIL), which serves as the benchmark for Safety Instrumented System design, operation, and maintenance according to ANSI/ISA 84.01-1996[2] and IEC 61511[3].

   As in Step 3, it is important to provide the team with a list of acceptable IPLs, including design criteria and limitations. Also, for each IPL provide a PFD or range of PFDs based on the design criteria. Having a pre-approved list will substantially improve the consistency of the assessment and reduce the amount of time required for the analysis.

6) Provide specific implementable recommendations. The recommendations from the LOPA team must be considered options for implementation. The LOPA team should be encouraged to develop as many recommendations as possible to allow the project team to select the best option from an implementation ease and cost standpoint.

What is the Benefit of Using LOPA?

There are four primary benefits to implementing LOPA over other SIL assignment methodologies procedures.

1) Due to its scenario-related focus on the process risk, LOPA often reveals process safety issues that were not identified in previous qualitative hazards analysis.
2) Process hazards are directly connected to the safety actions that must take place, providing clear identification of the safety instrumented systems and associated SIL.
3) It has been proven effective in resolving disagreements related to qualitative hazards analysis findings.
4) LOPA often identifies acceptable alternatives to the SIS, such as adding other layers of protection, modifying the process, or changing procedures. This provides options for the project team to evaluate using cost/benefit analysis, allowing the most cost effective means of risk reduction to be selected.

---

[2] "Application of Safety Instrumented Systems for the Process Industries," ANSI/ISA-ISA 84.01-1996, ISA, Research Triangle Park, NC (1996).

[3] "Functional safety of electrical/electronic/programmable electronic safety related systems," IEC 61511, International Electrotechnical Commission, Geneva, Switzerland (expected mid- 2oo3).