Lessons Learned from Application of LOPA throughout the Process Lifecycle

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

Prepared for Presentation at
10th Global Congress on Process Safety
New Orleans, LA
March 31-April 2, 2014

Keywords: layer of protection analysis, LOPA, independent protection layer, IPL, initiating event, PFD, IEF

Abstract

LOPA has been implemented throughout major capital projects, on existing facility PHAs, and in PHA revalidations and management of change risk reviews. This paper discusses lessons learned for implementing LOPA in each phase of a process lifecycle and outlines some of the ways to optimize the use of LOPA. The paper describes how implementation of standards for IPLs and initiating event maintenance is necessary in each company. The paper also covers consolidation of SIL evaluation into the related PHA and LOPA at each life cycle phase. Special emphasis is given to optimizing the application of LOPA and SIL evaluation through the various phases of a major capital project.

1. Brief History of LOPA

The initial development of layer of protection analysis (LOPA) was done internally within individual companies. However, once a method had been developed and refined, several companies published papers describing the driving forces behind their efforts to develop the method, their experience with LOPA, and examples of its use (Bridges, 1997[1]; Dowell, 1997[2]; Ewbank and York, 1997[3]). In particular, the papers and discussion among the attendees at the October 1997 CCPS (Center for Chemical Process Safety, part of AIChE), International Conference and Workshop on Risk Analysis in Process Safety, brought agreement that a book describing the LOPA method should be developed.

In parallel with these efforts, discussions took place on the requirements for the design of safety instrumented systems (SIS) to provide the required levels of availability. United States and international standards (ISA S84.01 [1996], IEC [1998, 2000])[4,5,6] described the architecture and design features of SISs. Informative sections suggested methods to determine the required safety integrity level (SIL), but LOPA was not mentioned until the draft of International Electrotechnical Commission (IEC) 61511, Part 3, which appeared in late 1999. These issues were summarized in the CCPS workshop on the application of ISA S84, held in 2000.

The first LOPA book was developed by a CCPS committee from 1997 through 2000 and was published in 2001[7] (William Bridges and Art Dowell were the two co-originators and principal authors of the book). LOPA became widely used following the publication and most companies around the world have used LOPA, with some companies having used LOPA a lot. During roughly 15-years of widespread use of LOPA, and especially during the last 10-years, use of LOPA has greatly accelerated. It is likely that several million LOPAs have been performed. During this same period, many abuses of LOPA have been noted and several innovations have occurred.

In 2007, CCPS commissioned a new guideline book (1) to expand the list of independent protection layers (IPLs) and initiating events (IEs) and (2) to try to remedy some of the major issues noted in the use of LOPA. The new book is discussed in another paper at this conference; this book is due into publication this year (2014; William Bridges was the primary contractor/author of this book until April 2012). Another companion book on the related topics of conditional modifiers and enabling events and conditions was published in 2013 (Mr. Bridges was committee member and contributed to this book as well).

2. Intent of LOPA

LOPA is one of many methods for assessing a given scenario to determine if the risk is acceptable. It uses rigid rules to simplify and standardize the definitions of independent protection layers (IPLs) and initiating events (IEs). If these rules are followed, then the simplified risk assessment math of LOPA is valid and the risk assessment should give an order-of-magnitude approximation of the risk of a given cause-consequence pair

(scenario). The rules also cover the minimum criteria for maintaining features and task executions that relate to IEs and IPLs.

LOPA is only one option for judging risk. The most common and still the best method for judging the risk of most scenarios is the process hazard analysis (PHA) team; their judgment is qualitative, but the "fuzzy" math of the individual team members usually coalesces into excellent judgment of risk for nearly all accident scenarios.

3. Relationship to SIL determination

LOPA started with and continues to have a unique relationship with SIS, and particularly to SIF identification and SIL assignment (sometimes called SIL determination). Some of the originators of LOPA needed LOPA to defend against an arbitrary assignment of safety instrumented functions (SIFs) for systems that were already "adequately" safeguarded by other means. This became apparent in the mid-1990s with the early development of SIS standards within chemical companies and by (at that time) the Instrument Society of America (ISA). Some of these early standards would have imposed a minimum SIL for a given consequence, without much regard for the number and value of other IPLs that already existed or were viable alternatives to the SIFs. Much of these arbitrary requirements for SIS have disappeared, but some remain.

For the most part today, LOPA is seen as one tool (in many parts of the world, the preferred tool) for determining if a SIF is necessary and if it is the correct choice of risk reduction; and LOPA is the preferred method for determining what SIL is necessary, if an SIF is chosen as the risk reduction method. With that said, PHA teams are also allowed by IEC 61508, 61511, and related TR from ANSI/ISA to make these same determinations. Per ISA TR 84.00.02, 2002 (and 2004), Section 3.8[8]:

> *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.*

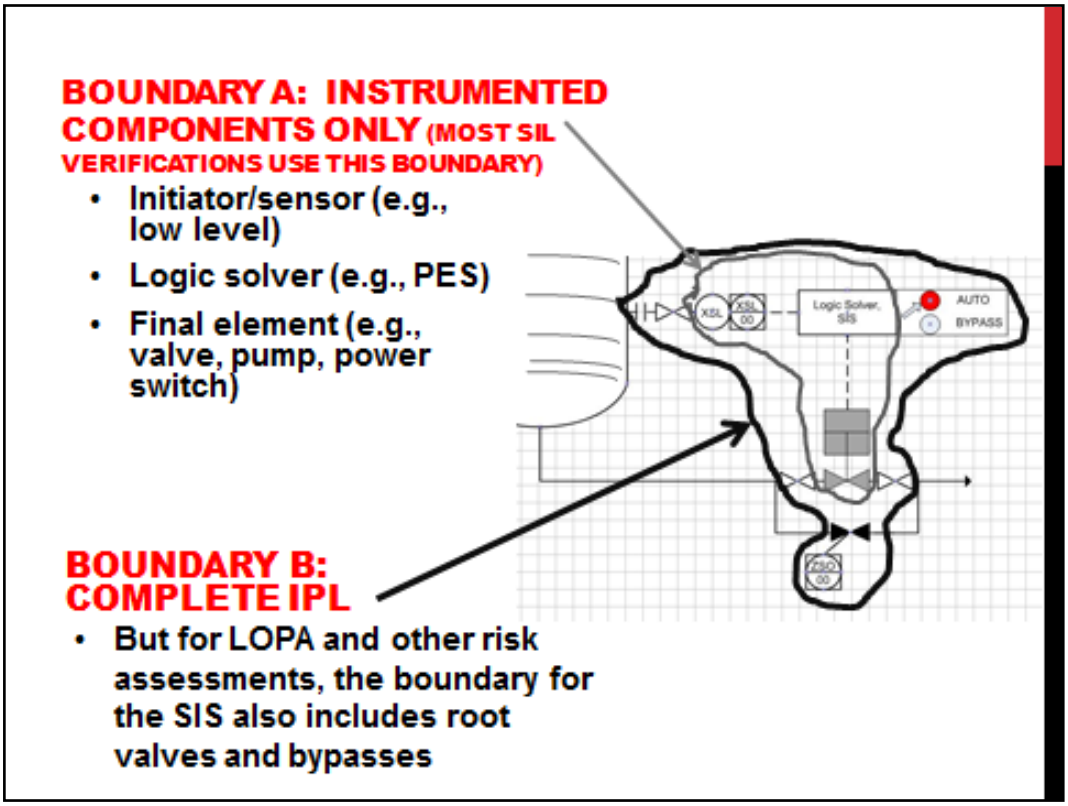
However, some organizations use LOPA to answer the question: "What SIL is needed to lower the risk to the risk target?" without first asking, "Are we at tolerable risk already?" or "Are there better alternatives for lowering the risk?" This leads to a huge over-specification of SIFs (and the wasting of resources to design, implement, and maintain these SIFs) and to many spurious shutdowns of units (which also waste money and

NOTE: As stated in all books and papers on the topic, LOPA does not find accident scenarios. Typically only the qualitative hazard evaluation methods (such as HAZOP, What-if, and FMEA) can find new accident scenarios.

increase the risk of accidents that can occur during re-start of the process).

Note that the system (loop) boundary for an instrumented safety system is defined differently by SIS standards versus LOPA (see Figure 1). As illustrated below, the system boundary for calculating the SIL for a given SIF includes only the instrumented components of the system. This omits the systemic failures possible from the process itself and more importantly omits the specific human errors of leaving the system in bypass or dependent errors of mis-calibrating multiple sensors in high SIL SIFs. LOPA however, requires that the system boundary for any IPL include all aspects of the IPL. This difference in system boundary definitions can make the difference between an SIF being a SIL 1 or a SIL 3 (installed predicted performance versus instrument only reliability).

Figure 1: Boundary for SIF ***(courtesy of Process Improvement Institute, Inc.)***



4. When to Use LOPA (in general)

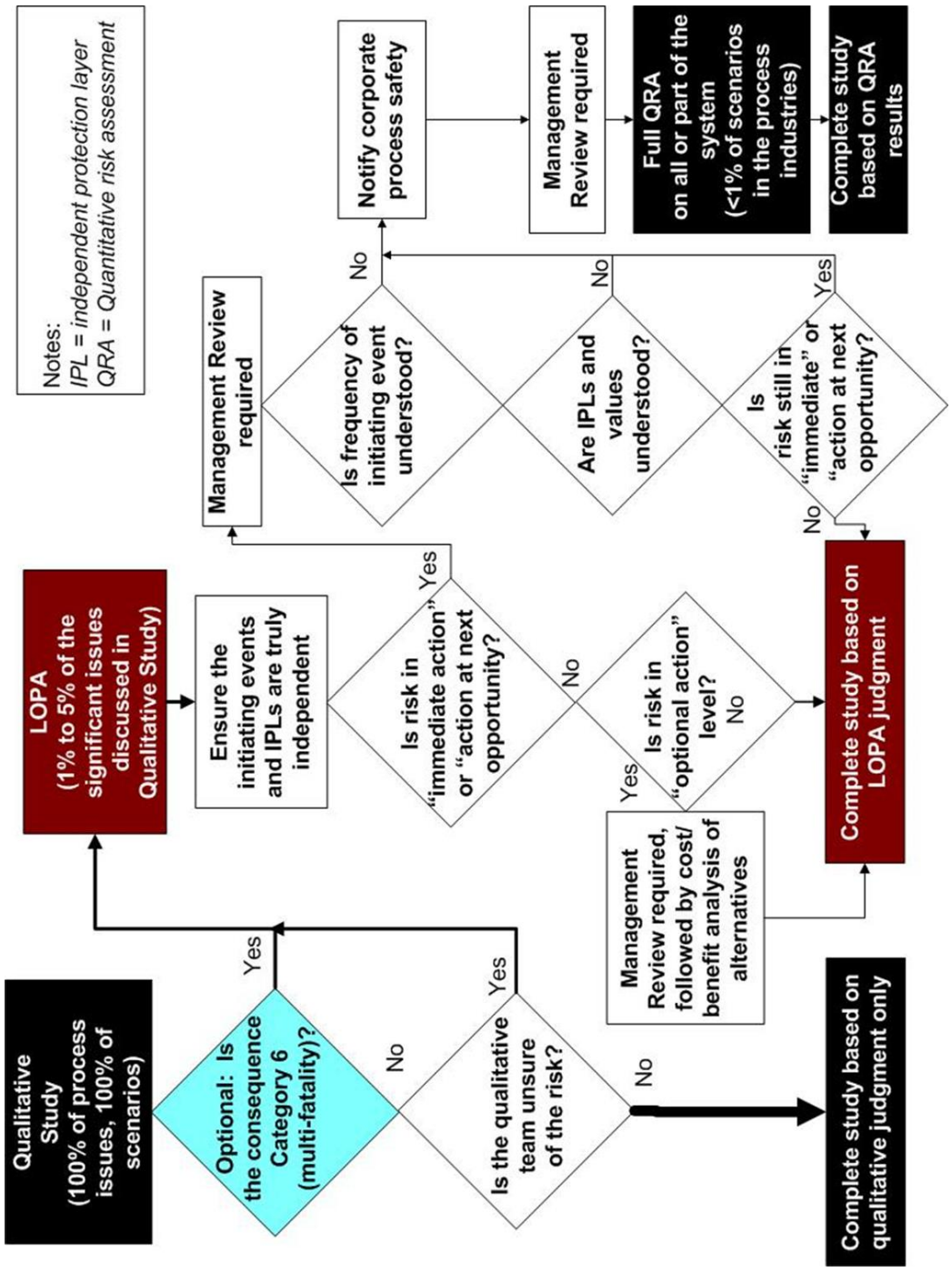
The originators thought LOPA would be used a lot less frequently than it is currently. As shown in Figure 2, it was anticipated that LOPA would be used on 1-5% of the scenarios uncovered in PHAs. It was also anticipated that LOPA would eventually be used "after" a PHA team meeting, since that is how the originators were using it. Various examples of overuse are discussed below *(Bridges 2007[10], discussed these issues in detail):*

- **Using LOPA within PHAs - a bad idea as it detracts from brainstorming.** Many of us on the original LOPA book authorship considered LOPA a single analyst job, after a PHA/HAZOP, for just a few scenarios (maybe after 100 HAZOP nodes, you

would do 1-10 LOPA). Instead, the trend appears to be that companies (or perhaps their consultants) make LOPA part of the PHA (in-situ). If the PHA/HAZOP team is properly disciplined on what qualifies as a safeguard (a qualitative definition of an IPL from LOPA), then performing LOPA in situ is usually overkill. In most situations, a qualitative team (HAZOP team) can make just as good or better judgment than provided by LOPA. LOPA is just another way to make a decision, has many pitfalls, and doesn't work for many types of scenarios. Other issues with use of LOPA within a PHA setting is that it distracts the team from brainstorming and it adds to team burnout because it takes time away from what is critical for the PHA team to do: *Identify scenarios for ALL modes of operation.*

- **Use for every Medium and High Risk Scenario --** Like in the point above, increasing the number of scenarios that must go through LOPA, reduces the resources available to find (in a PHA/HAZOP/What-if) the undiscovered scenarios and to manage existing layers of protection.
- **When to use LOPA** The following is the guide we use to decide when a LOPA is required (Category 6 is equivalent to consequences greater than $100,000,000 and/or with potential multiple fatalities):

FIGURE 2: When to use LOPA *(courtesy of Process Improvement Institute, Inc., 2004)*[11]



4.1 Hazard Evaluation at Different Plant Lifetime Stages

Process hazards can be identified from the onset of a project through its end (or assimilation into another project), and process hazards of changes are evaluated in mini-PHAs during the operating phase of the lifecycle. Hazard evaluations are also required for decommissioning. Industry has found that hazard evaluation must be used in all phases of a unit life cycle to ensure safe operations.

As usual, LOPA can be used in conjunction with any of these hazard evaluations to help estimate the risk of selected scenarios.

The following plant lifetime stages will be used in this section:

- Process development (perhaps several hazard evaluations during lab and pilot phases)
- Capital Projects
    - Conceptual and Preliminary design (1-2 hazard evaluation phases)
    - Detailed design (1-3 hazard evaluation phases)
    - Construction and start-up (completion of the initial and post-startup PHA)
- Operating lifetime (revalidations and MOC risk reviews)
- Extended shutdowns
- Decommissioning

4.2 Process Development Phase (Technology Phase) of Lifecycle

During the process development phases, various hazard reviews are necessary to help understand the risks and more and more is known of the chemistry and operations. HAZOP, What-if, and checklists are very useful during process development.

LOPA may be required for selected scenarios during normal, startup, switch-overs, modifications, etc., especially for large pilot plants.

4.3 Major Capital Project Phase of Lifecycle

There are various sizes and structures of projects, depending on the scope of the endeavor, the urgency, the nature of the business, the company culture, the company sophistication, and many other factors. The two most important project types (factors) for purposes of this paper are (1) project size (expressed usually in expenditure expected or size and number of pieces of equipment to be installed) and (2) type of financial control for the project.

4.3.1 Typical Project Sizes:

Table 1 below provides a basic definition of projects sizes and the typical number of risk reviews conducted during the project:

Table 1: Project Size/Scopes, Relative Project Length, and Risk Review Effort

Project Size	Example Project Scope	Example Project Length/Duration (concept→ commissioning)	Number of Risk Reviews
Major	Major projects handled **external** to an affiliate/plant, such as expansions and new facilities	12-36 months	4-7
Moderate	Works **engineered by an affiliate/ plant** (installing a new design of knockout pot for a feed to a unit)	6-9 months	2-3
Small	**Minor** affiliate/plant works (installing piping to bypass a control valve)	1-2 months	1

4.3.2 Scope of Risk Reviews and PSM Development For Each Project Phase

As mentioned earlier, major projects can have 4 to 7 or more phases and these can be spread over 12 months to 36 months or more depending on the project size. However, decisions for controlling risk made during the project phases echo through the next 20 to 50 years of operation, because design features, automated control features, and human interactions must be managed continuously to control the inherent hazards of chemical processes.

Figure 4 presents an example of a major capital project's phases for a large new chemical process unit or plant, with six "in-project" phases and one "post-project" phase. Though not universal, this approach appears to be a widely accepted view of major project phases. For smaller projects, condense this approach to 5, 4, or a minimum of two phases. **Table 2** on the following pages provides much more detail on the risk review for each project phase.

Note the six hazard evaluations (risk reviews) that are required. The six build on the prior risk review; at the end, the site has a complete PHA/HAZOP for use as the initial PHA for the new process. Further note that LOPA would only be used on the middle 3-4 hazard reviews, and only for scenarios that the PHA/HAZOP team has trouble in making tolerable risk decisions.

Figure 4: Example Project Phases and Related Scope of Risk Reviews (RR), which in this instance means the same as hazard evaluation[12]

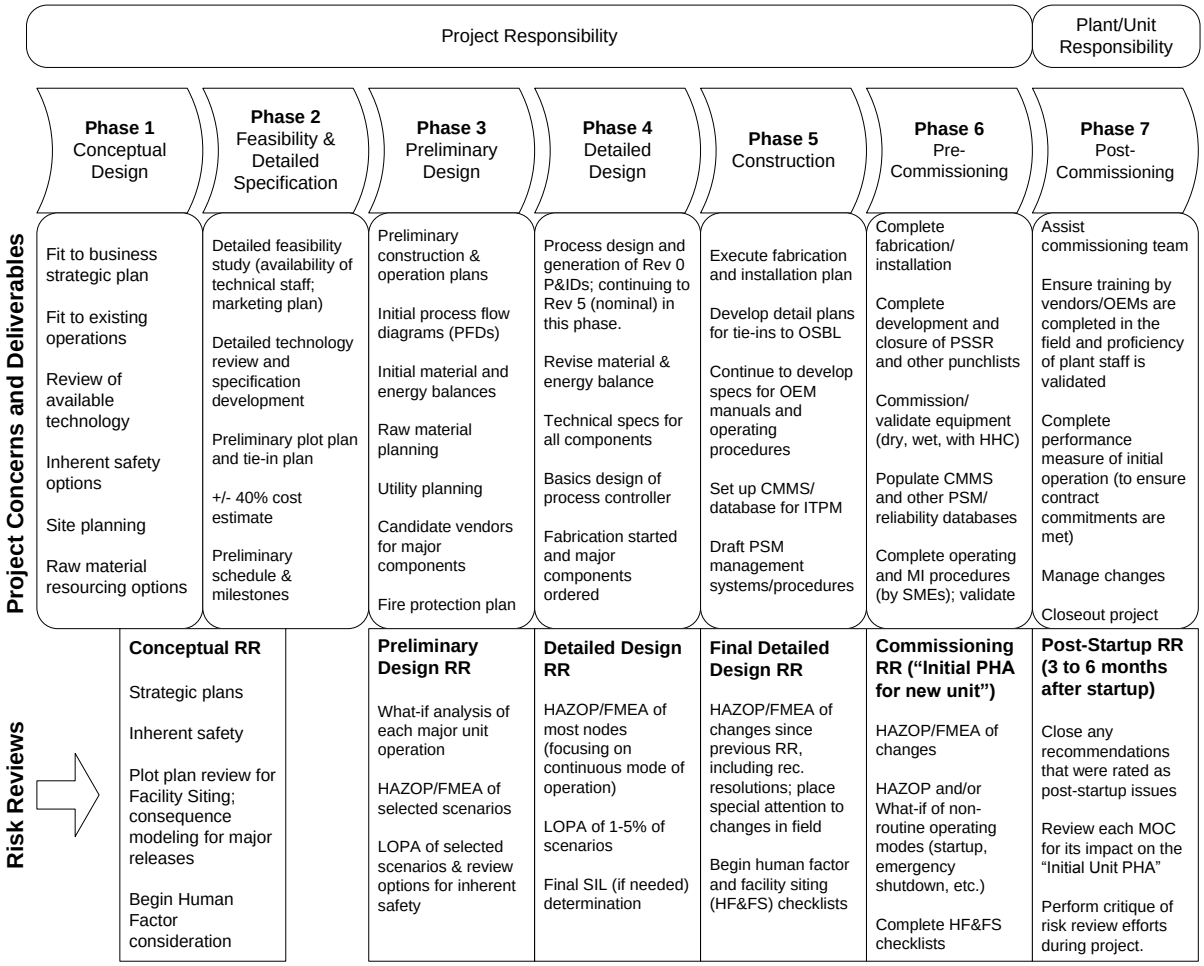


Table 2: Details of Process Safety Development Phases of a Major Capital Project (with LOPA highlighted)[12]

Project Phase #	Phase Name	Goals of RISK REVIEW	RISK REVIEW Methodology	RISK REVIEW Team Membership (in addition to leader & scribe)
1&2	Conceptual	Choose inherently safer option, ensure overall feasibility, estimate impact on neighbors	• Consequence modeling (to help on next project phase) • What-If (no guidewords) • Selected checklist for judging inherent safety	• Senior operator for unit or from similar unit • Senior process engineer for unit or from similar unit • Process/design engineer from project • Process Safety specialist (if not already listed above)
3	Preliminary Design	Identify and resolve most expensive design alternatives, including layout of plant, facility siting concerns, environmental protection issues, and major tie-ins	• What-If (no guidewords) • HAZOP/FMEA of selected scenarios • **LOPA of selected scenarios (note that sufficient information for LOPA will likely be missing for 20-30% of accident scenarios at this phase)**	• Senior operator for unit or from similar unit • Senior process engineer for unit or from similar unit • Process/design engineer from project • Process Safety specialist (if not already listed above) • Possibly I&E Engineer • **LOPA should be performed by a single analyst**
4	Detailed Design	Begin detailed identification of potential accident scenarios, primarily focused on normal (usually continuous) mode of operation. Begin risk assessment for scenarios with large residual risk	• HAZOP/FMEA of equipment nodes, focusing on normal (usually continuous) mode of operation • What-If of lower consequence & lower complexity systems • **LOPA of 1-5% of the scenarios; determine SIL, as necessary**	• Senior operator for unit or from similar unit • Senior process engineer for unit or from similar unit • Process/design engineer from project • Process Safety specialist (if not already listed above) • Possibly I&E Engineer • Possible vendor of unique equipment • **LOPA should be performed by a**

Project Phase #	Phase Name	Goals of RISK REVIEW	RISK REVIEW Methodology	RISK REVIEW Team Membership (in addition to leader & scribe)
				single analyst
5	Final Design	Update results of previous RR for new details, identify potential accident scenarios for nodes not previously reviewed, primarily focused on normal (usually continuous) mode of operation. Resolve most previous recommendations Complete risk assessment for scenarios with large residual risk	• Complete HAZOP, FMEA, or What-If for nodes started in previous RR • Perform HAZOP, FMEA, What-If for nodes not covered in previous RR (due to previously missing information) • Begin Human Factors and Facility Siting checklist • Perform general Utility Failure checklist • **LOPA of 1-5% of the scenarios; determine SIL, as necessary**	• Senior operator for unit or from similar unit • Senior process engineer for unit or from similar unit • Process/design engineer from project • Process Safety specialist (if not already listed above) • Possibly I&E Engineer • Possible vendor of unique equipment • **LOPA should be performed by a single analyst**
6	Commis-sioning	Conduct full hazard/risk review of operating procedures to control risk of errors during startup, shutdown, emergency shutdown, and other non-routine modes of operation Close out previous RISK REVIEW issues (from earlier phases of project) and complete the human factors & facility siting checklist This RISK REVIEW creates the "Initial PHA" of the process	• HAZOP (2 guideword or 8 guideword) or What-If (no guideword) of operating procedures (choose method based on hazard and complexity of each task) • Complete HAZOP, FMEA, or What-If for nodes started in previous risk reviews • Perform HAZOP, FMEA, What-If for nodes not covered in previous risk reviews (due to previously missing information) • **LOPA of 1-5% of the scenarios; determine SIL, as necessary** • Complete Human Factors and Facility Siting checklist	• Senior operator for unit or from similar unit • New/junior operator for unit • Senior process engineer for unit or from similar unit • Process/design engineer from project • Process Safety specialist (if not already listed above) • Possibly I&E Engineer • **LOPA should be performed by a single analyst**
7	Post-Startup	Conducted 3-6 months after startup similar to the future Revalidations, but with the goal of compensating for	• Audit of MOCs (and P&IDs and SOPs) since "Initial PHA" (since commissioning RR) to ensure nothing has been missed by MOC	• Senior operator for unit or from similar unit • New/junior operator for unit • Senior process engineer for unit or

Project Phase #	Phase Name	Goals of RISK REVIEW	RISK REVIEW Methodology	RISK REVIEW Team Membership (in addition to leader & scribe)
		weaknesses in MOC process at the initial startup of the new unit/process	• HAZOP or What-If of missed or poorly reviewed changes • Update PHA for the entire set of changes (looking at whole picture for effect of all changes) • Close any pending recommendations (if possible)	from similar unit • Possibly project/design engineer (for QA of project)

4.3.4 Risk Control – Initial Phases of a Major Capital Project

As described in **Figure 4** and **Table 2**, the first two project phases are critical for establishing the inherent safety of the process, and therefore an opportunity for company leadership to show their true colors.

There typically is no call for LOPA during the conceptual stage or very preliminary design phase of a major capital project.

4.3.5 Risk Control – Detailed Design Phases of a Major Capital Project

The risk reviews are a major risk control feature of the design phases of a project as well. These risk reviews can be one to three progressive efforts over one to three project phases, depending on the size of the "major capital project," with the Risk Review report building toward the "initial" official hazard review report for the process unit (discussed in the next section).

LOPA occur frequently during this Detailed Design project phase

The Risk Reviews during the detailed design phases can typically include:

- Using HAZOP, FMEA, and/or What-if (brainstorming methods) in progressively more detail
- Initiating and then progressively improving (from phase to phase) the risk review record (HAZOP tables, What-If tables, checklist tables)
- As mentioned in **Figure 1** and **Table 2**, the risk reviews during detailed engineering will evaluate the risk of any design modifications and/or newly identified hazardous scenarios, which have been added since the previous reviews.
- Maximize inherently safer design in the selected process
- Addressing damage mechanisms and ensuring materials and equipment location and engineered safeguards minimize the likelihood or effects of external impacts
- Performing a final review of equipment, ventilation, containment, and environmental safeguards, including instrumentation, interlocks, fail-safe decisions, detailed layouts, and fire protection provisions
- Begin the Human Factors risk review (checklist-based)
- Continue the Facility Siting risk review initiated earlier (checklist-based and modeling-based risk reviews)

- **Apply Layers of Protection Analysis (LOPA) to complex risk scenarios and use this to define Safety Instrumented Systems' needs. These phases of the project are where LOPA gets used the most. With that said, only 1-5% of potential accident scenarios will require LOPA in the risk decision making process. Exceptions will be for novel technology:**

Example: ***We performed a PHA/HAZOP over a six (6) week period for a new way to make an explosive. There had only been limited pilot testing of some of the technology before scale up. The PHA/HAZOP normally would have taken two (2) weeks, but the PHA/HAZOP was doubling as a design review. In addition, since the controls and safeguarding for this process were all novel, about 7% of the accident scenarios went to LOPA. This is more than the 1-5% of the scenarios that normally go to LOPA. About 30 LOPA in all were performed.***

As before, the Risk Reviews during the detailed engineering phase require intensive participation by operations' senior staff, including operators, supervisors, and process engineers.

And as before, the LOPA is usually performed by a single analyst, outside of the qualitative risk review (PHA/HAZOP).

4.3.6 Risk Control – Pre-Commissioning / Commissioning (Initial Startup) Phase of a Major Capital Project

The pre-commissioning Risk Review builds upon the previous Risk Reviews in the project. As the equipment design is completed the fabrication and construction begins. During this same period, initial training of the new or transferred staff occurs, using the procedures mentioned in the previous section. The pre-commissioning Risk Review can begin just prior (4-6 weeks prior) to start-up of a new facility, or a little earlier if possible. The key consideration for this project phase is to complete the risk review of non-routine modes of operations. The project Risk Reviews to this point will not have covered these modes of operation very well. (Note that in perfect world, the risk review of the non-routine modes of operations, which uses the operating procedures as a basis, would be completed before training begins. However, in most cases, the training begins as the procedures are being completed and as the risk review is done.) The risk review of non-routine operating modes can be performed using a full 8 guideword HAZOP, a streamline 2 Guideword approach (which is what was used before HAZOP was invented in the 1960s), or a No Guideword What-if.[13] All of these approaches are described elsewhere[13] and will be explained in some detail in the 3rd Edition of the Guidelines for Hazard Evaluation Procedures, CCPS[14]. This procedural analysis is to ensure that hazards due to human error in association with the process design have been identified and analyzed.

During this final risk review before start up, the project team must also ensure that all the PSM requirements for initial PHAs have been met. PHAs must address the hazards of the process; therefore hazards during all modes of operation must be analyzed. The resulting report will be the "initial PHA" of the process unit, which is required to meet PSM standards.

This pre-commissioning risk review should not be confused with the pre-startup safety review (PSSR; also referred to as Operational Readiness Review [ORR]), which is also necessary but the purpose of the PSSR is to validate that the process design and specifications have been met.

This final Risk Review session before startup consists of:

- Reviewing and evaluating changes made during construction, ensuring that no new hazards have been added since the last hazard review. High priority is given to detecting details which may have been overlooked, and to concentrating on the adequacies of plans to cope with operating emergencies that might arise
- Maximizing inherently safer design in the selected process, such as planning for rework of initial product
- Completing reviews for Facility Siting and access issues
- Completing the review for Human Factors issues
- Reviewing (HAZOP/What-If) of start-up, shutdown, emergency shutdown, and on-line maintenance procedures. Some believe this risk review to be another "validation" review of procedures, to ensure they are correct. But that is not the purpose of this risk review of procedures. Our aim in the HAZOP/What-If of the procedures is to ensure we have adequate safeguards (hardware, interlocks, SIL, and/or independent administrative safeguards) to offset the errors of skipping steps and performing steps wrong – such human errors WILL occur, it is just a matter of when.[13]
- **Performing any LOPA, if necessary for the new scenarios that are uncovered during the hazard review of non-routine modes of operation.**

Although LOPA is valuable during this project phase, the lack of risk review of non-routine mode of operations, such as by HAZOP or What-if of procedural steps, is the most frequently observed weakness in the project risk review cycle

After this risk review, the project team can proceed to close recommendations, decide which (if any) of the recommendations can be deferred until after initial startup, close the PSSR (not part of the risk review, but part of PSM in general), and finalize the initial PHA report for the new process unit. Typically, the plant MOC system begins to take over control of new risks after the pre-commissioning Risk Review meeting is closed.

There are of course many deliverables from the project team, including the finished equipment, ready to commission and then smoothly commissioned, operating and maintenance procedures, populated databases for mechanical integrity (MI), Process Safety Information - files of all necessary design bases for relief valves, completed drawings, complete equipment files of all types, etc.

4.4 Operating Phase of Lifecycle

4.4.1 Management of Change

Change is an inevitable and necessary feature for all organizations. When changes occur in an operation that contains hazards of any sort, it is necessary that the change process be managed to understand and control those hazards. Most organizations have some "Management of Change" (MOC) policies and procedures in place to address the wide range of issues related to changes. Regardless of the type of change, the risk of change must be analyzed. All of the hazard evaluation methods are applicable to MOC risk reviews and the criteria for selecting the appropriate technique is the same as for other risk reviews. However, one nuance is that the choice of technique may depend also on how the unit hazard evaluation will be revalidated (updated). For instance, if the unit hazard evaluation (called a Process Hazard Analysis in the US) was accomplished using primarily HAZOP, then long-term it might be best if the risk review of the "change" also be documented in HAZOP format; this will make rolling-up the data into the next revalidation that much easier for the company.

Some of the MOC risk reviews may affect an existing LOPA or the risk review team (best understood as a mini-PHA team) may recommend a LOPA for a new scenario resulting from the change. For the case of an MOC effecting and existing LOPA, the prior LOPA should be updated, with a notation on the LOPA documentation that makes it easy for the change to be incorporated in the next Revalidation cycle. Again, LOPA will likely only be required for 1-5% of the scenarios.

4.4.2 Cyclic Reviews (Revalidations)

Even as process changes never end during the life of a facility, there will always be the necessity to continue hazard evaluations. Periodic updating or revalidation of the hazard study is the method used to maintain adequate safeguards. The timing of these cyclic reviews depends on factors such as regulations, the rate of process changes, and the nature of those changes. A significant change outside the fence line can also trigger the need for a hazard review. Examples of such changes are:

- Population changes such as new residential housing nearby
- Land/water/air traffic pattern changes
- Necessary community emergency and security adjustments
- New buildings such as schools or commercial establishments
- Demolished buildings.

Although MOCs may require a few LOPA, Revalidations almost never require new LOPA. But, if one or more of the MOCs affect existing LOPAs or the MOC risk review team required a new LOPA, then related changes or notation are likely necessary for the Revalidation report.

4.4.3 Restarts

During the normal operating phase, units restarted following:

- a normal shutdown
- an emergency (abnormal) shutdown
- a "turnaround" or maintenance phase.

LOPA may be required for the new scenarios that are uncovered during the hazard review of these unique, non-routine modes of operation.

Each has safety issues associated which could be unique to the shutdown event. Start-up from a normal or scheduled shutdown (without maintenance action) should already have been addressed as a procedure-based hazard evaluation (HAZOP, What-if, or 2 Guide Word technique) of non-routine operations. Less likely to have had an established safety review is the start-up from an emergency or abnormal shutdown, since not all possible emergency scenarios would have been predicted. These are frequently considered to be operated like a normal start-up once the system has reached a safe state. A careful restart review (usually 2 Guide Word or What-if) is advised, since by the (hopefully) unique nature of the emergency, experience with the specific type of restart is limited.

4.5 Extended Shutdowns

Although LOPA is likely not needed for preparation for extended shutdown, a restart back to the "normal" mode of operation may need a new PHA/HAZOP and therefore some LOPA may be required.

Mothballing a plant or a unit within a plant site goes beyond the steps taken to shut down a process to an established safe state. Tanks, lines, and valves must all be drained and any residual reactive materials neutralized. Most of these operations will likely be performed only once during the lifetime of the operation, and hence will have no history to help guide the safe implementation of the mothballing effort. A potentially riskier activity is a restart from an extended shutdown. In that event, the condition and intended operation of all equipment and instruments must be checked. In particular, the safety systems must be re-verified and validated. The restart of a mothballed unit within and perhaps attached to an active production site should include a review of the hazard evaluation for the connected active units.

4.6 Decommissioning Phase of Lifecycle

An active plant or unit that is slated for decommissioning would go through the stages of a normal shutdown, then cleanout in preparation for mothballing, followed by disassembly. In the refining industry as well as in other process industries, a hazard review is conducted before decommissioning. Health, safety, and environmental issues would be related to uncontrolled pressure releases, workers potentially exposed to noxious or toxic vapors, and spills during line separation. A plant or unit that has been previously mothballed would have all the issues associated with the decommissioning of an active plant or unit, with the added potential hazard associated with corrosion products. Over a period of time, residues can change such that these new compounds may be unknown and have unknown health and environmental effects or thermal decomposition sensitivities.

LOPA would only rarely be required for decommissioning of an entire process; but if a part of a process is decommissioned; this may affect existing LOPA scenarios for the portion of the process that will remain in operation.

6. Conclusions

LOPA is one risk assessment tool that has proven useful in helping organizations judge if selected accident scenarios have sufficient safeguards. Throughout the process lifecycle, from the technology phase through the end of ongoing operations, LOPA has and continues to be used. If the general rules outlined in this paper are followed and if LOPA is not arbitrarily applied, then it will continue to benefit industry as a valuable tool for risk assessment.

7. ABBREVIATIONS and GLOSSARY

HAZOP – Hazard and Operability; as in HAZOP Analysis or HAZOP Study
IE – Initiating Event
IEC – International Electrotechnical Commission
IEF – Initiating Event Frequency
IPL – Independent Protection Layer
ISA – International Society of Automation
LOPA – Layer of Protection Analysis
MOC – Management of Change
PFD – Probability of Failure on Demand
PHA – Process Hazard Analysis
P&ID – Piping & Instrumentation Diagram

PSM – Process Safety Management
SIF – Safety Instrumented Function
SIL – Safety Integrity Level
SIS – Safety Instrumented System

8. References

1. Bridges, William G., and Tom R. Williams (1997), "Risk Acceptance Criteria and Risk Judgment Tools Applied Worldwide within a Chemical Company," *International Conference and Workshop on Risk Analysis in Process Safety*, October 21–24, 1997, Atlanta, GA, pp. 13–28. New York: American Institute of Chemical Engineers.
2. Dowell, A. M., III (1997), "Layer of Protection Analysis: A New PHA Tool, After HAZOP, Before Fault Tree," *International Conference and Workshop on Risk Analysis* in Process Safety, October 21–24, 1997, Atlanta, GA, pp. 13–28. New York: American Institute of Chemical Engineers.
3. Ewbank, Rodger M., and Gary S. York (1997), "Rhône-Poulenc Inc. Process Hazard Analysis and Risk Assessment Methodology," *International Conference and Workshop on Risk Analysis in Process Safety*, October 21–24, 1997, Atlanta, GA, pp. 61–74, New York: American Institute of Chemical Engineers.
4. IEC 61508, *Functional Safety of Electrical Electronic/Programmable Electronic Safety-Related Systems*, The International Electrotechnical Commission, 2010.
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, 2003.
6. ANSI/ISA 84.00.01-2004 (IEC61511-1 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements*, 2004.
7. *Layer of Protection Analysis: Simplified Process Risk Assessment*, CCPS/AIChE, 2001.
8. ISA TR84.00.02, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques*, International Society of Automation, 2002.
9. *Guidelines for Initiating Events and Independent Protection Layers*, 2014 (pending), CCPS/AIChE.
10. Bridges, W. and Clark, T., "Key Issues with Implementing LOPA (Layer of Protection Analysis) – Perspective from One of the Originators of LOPA,*"*, *5th Global Congress on Process Safety*, April 2009, AIChE.
11. *Layer of Protection Analysis*, Training Course Notebook, Process Improvement Institute, Inc., 2004-2014.

12. Bridges, W. and Tew, R., "Controlling Risk During Major Capital Projects," *24th CCPS International Conference and Workshop on Process Safety (CCPS/AICHE)*, New Orleans, LA, April 2008.
13. Bridges, W. and Clark, T., "How to Efficiently Perform the Hazard Evaluation (PHA) Required for Non-Routine Modes of Operation (Startup, Shutdown, Online Maintenance)," *7th Global Congress on Process Safety*, Chicago, AIChE, March 2011.
14. *Guidelines for Hazard Evaluation Procedures*, 3rd Edition, 2008, CCPS/AIChE.