Key Issues with Implementing LOPA (Layer of Protection Analysis) – Perspective from One of the Originators of LOPA

William (Bill) Bridges and Tony Clark
Process Improvement Institute, Inc. (PII)
Knoxville, TN, USA
wbridges@piii.com
www.piii.com

ABSTRACT

This paper focuses on problems observed with LOPA during the first 8-years of broad use.

- One the biggest issues is that organizations use LOPA without following the rules for LOPA, especially the rules related to maintaining, testing, and record-keeping for each independent protection layer (IPL) and for each "optimized" initiating event (IE). Some companies use the values for an IPL or IE listed in the LOPA guideline book (CCPS, 2001), or elsewhere, but without implementing the management systems to maintain the IPL or IE at the claimed PFD value.
- Another issue is that many companies and analysts overuse LOPA. For instance, IEC 61511 allows a qualitative PHA team to determine if a SIF is needed for a scenario and to specify a SIL 1 or 2, if one is needed. Yet, most folks believe that only LOPA, RiskGraph, or QRA is valid for determining if a SIF is needed and then use the same method to determine what SIL is needed. The LOPA book authors expected the number of scenarios going to LOPA (after a HAZOP/PHA) would be 1% to 10% (max) of those uncovered in a qualitative analysis (maybe after 100 HAZOP nodes, you would do 1-10 LOPA). Some of us believed that a PHA team would recommend (or use) LOPA only if the scenario was too complex for the PHA/HAZOP team. It appears that most companies are using LOPA for every scenario that has a severe consequence; this results in doing LOPA on much greater than 10% of the scenarios.
- Many times there is weak definition of the consequence that is being avoided, so an IPL does not always match up well with the consequence.
- LOPA is also overworked when it is used. Many of us on the original LOPA book authorship considered LOPA a single analyst job, after a PHA/HAZOP. Instead, the trend appears to be that companies (or perhaps their consultants) make LOPA part of the PHA (in-situ), therefore involving the whole PHA team.
- LOPA is used in PHA team settings, which distracts PHA teams from their primary task of brainstorming to identify the accident scenarios that can occur.

This paper also summarizes the many benefits LOPA has produced for the industry.

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; Dowell, 1997; Ewbank and York, 1997). 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 and 2000]) 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 (William Bridges was one of the principal authors of that guideline). 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 10-years of widespread use of LOPA, and especially during the last 5-years, use of LOPA has greatly accelerated. It is likely that 1 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 (future) book is discussed in another paper at this conference; this book is due into publication in early 2010.

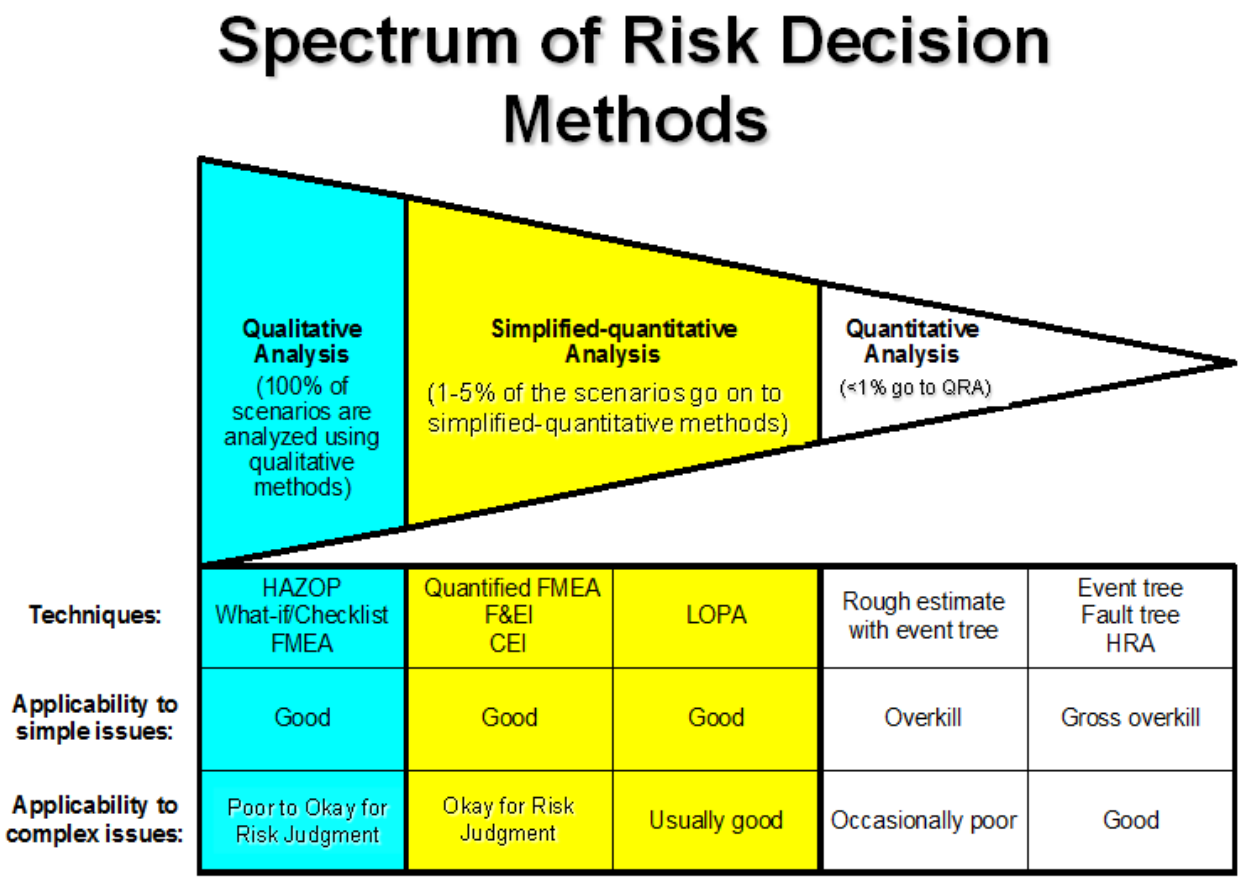
Intent of LOPA

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.

Figure 1, below, updated from the original figure contained in the LOPA book, illustrates where LOPA fits into the spectrum of methods for judging risk.

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.



Courtesy of Process Improvement Institute, Inc., 2004.

Relationship to SIL determination

LOPA started with and continues to have a unique relationship with SIS and 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 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 SISs. 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 an 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 to make these same determinations.

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

Summary of Gains from LOPA

Overall, LOPA has been highly successful in helping organizations to understand and control risk. Below is a listing of some of the benefits derived from LOPA:

- More consistent definition for protection layers. Information from LOPA helps an organization decide which safeguards to focus on during operation, maintenance, and related training. For instance, many companies decide to focus their inspection, test, and preventive maintenance activities on the IPLs identified during LOPA; these companies often decide to run the remaining safeguards (those not identified as IPLs) to failure or subject them to less rigorous test and maintenance schedules. Therefore, LOPA is a tool for implementing a comprehensive process safety management (PSM) mechanical integrity (MI) or risk-based maintenance system, and it aids in the identification of "safety critical" features and tasks.

- LOPA helps identify operations and practices that were previously thought to have sufficient safeguards, but on more detailed analysis (facilitated by LOPA), the analysis indicates there are far more safeguards than necessary. Therefore, the company/site can eliminate unnecessary safeguards (eliminate "extra" IPLs) or perhaps similarly eliminate the care and proof of these safeguards (i.e., run the extra IPLs to failure) – while still maintaining tolerable risk. This has been particularly helpful in cutting down a list of recommendations from a poorly run PHA/HAZOP; in one plant, the number of recommendations was reduced from 1500 to about 500 using LOPA (the initial PHA teams were not properly trained on how to make risk judgments).

- Improved evaluation in PHAs of which "listed" safeguards are "valid" safeguards. Even though LOPA was not meant for "live" use during a qualitative, team hazard review (like a PHA/HAZOP) because it normally distracts a team from their primary job of brainstorming what can go wrong, one of the main benefits realized from the first decade of implementing LOPA within an organization is that the qualitative hazard reviews (such as PHAs or HAZOPs) have improved. This is because now those in a qualitative hazard review are not likely to list a protective feature or action as a safeguard in a HAZOP or What-if analysis, unless that safeguard appears to meet (or is intended to meet) the requirements of an IPL (discussed later). This has improved the qualitative risk judgment of such teams because the safeguards they list and discuss are very likely independent, capable, validated, and audited.

- Justifying when SIS is not needed (proper SIL determination can usually show no SIL is needed). LOPA helps provide the basis for a clear, functional specification for an IPL (ANSI/ISA 84.00.01 [2004] and IEC 61508/61511 [1998; 2001; 2004]) and also facilitates assigning of the SIL needed (a quantitative approach is required by these standards for a SIL of 3).

- Faster quantification of severe risk scenarios. LOPA requires less time than quantitative risk analysis (QRA). This benefit applies particularly to scenarios that are too complex for qualitative assessment of risk. A full QRA of a scenario can take hours or days, whereas a LOPA for the same scenario will likely take about 1-hour.

- Common language among risk reviewers around the world. LOPA helps resolve conflicts in decision making by providing a consistent, simplified framework for estimating the risk of a scenario and provides a common language for discussing risk. LOPA provides a better risk decision basis compared to subjective risk judgment, especially for complex scenarios. Related to this point, LOPA gives clarity in the reasoning process and it documents everything that was considered. While this method uses numbers, judgment and experience are not excluded. In some cases, the LOPA analyst (or in some cases, LOPA team) was uncomfortable with the number calculated, so the analyst reviewed the assumptions for the frequency of the initiating event.

- LOPA offers a rational basis for managing layers of protection that may be taken out of service (such as bypass of a shutdown interlock). LOPA also provides clarity on what to pay attention to when an IPL is out of service for testing or repair.

Summary of Issues with the Current Implementation of LOPA

While LOPA has been a great benefit to industry, we have observed many issues with the implementation of LOPA over the past 10-years of use.

1. **One of the biggest problems with LOPA is that its users do not always follow the rules of LOPA.** A major problem is that IPL and IE values are picked from a list, while the specific IEs and IPLs are not (1) validated to have the stated value and (2) not maintained to sustain the stated value. Below is a listing of the rules for IPLs (with impact on IEs as well), and descriptions of the problems we have observed:

   - **IPLs must meet independence rule.** This most important rule is ***not*** often violated, at least not intentionally. But it is violated occasionally. For instance, a LOPA may use two basic process control system (BPCS) loops without first verifying that the BPCS qualifies for Approach B, as outlined in Chapter 11 of the LOPA guideline (CCPS, 2001). Similarly, if a BPCS is used to "shadow" a SIF, then the shadowing feature must be "negated" from consideration of the SIL value if the BPCS is the IE of the scenario.

     Sometimes the LOPA will re-use an operator or use another operator within the same work team; this usually will not pass the test of independence. Part of the reason for this latter problem is the lack of clarity in the first LOPA guideline. The next book being drafted by CCPS (scheduled for release in 2010) for IPLs and IEs will provide more clarification on the use of human IPLs. The basic rule is that you cannot use any work group (like an operations shift or maintenance/operator team doing online maintenance activities) more than once in the same LOPA scenario.

   - **IPL and IE values must be defensible.** This has been a problem. Many organizations choose values from handbooks (or from the original LOPA book) and papers/articles or obtain them from calculations based on discrete component failure rates from databases, and then assume those values apply to their situation. This is not a good assumption. The overriding factor in the reliability of a component, or the reliability of the human action, is often the local control of human error and the local environment of the equipment. For example, a PSV in clean, gas service has a much different reliability than a PSV in olefin or acid service.

   - **IPLs and IEs must be maintained such that they produce the IE or IPL values stated.** This has been a huge problem in the past 8-years of LOPA implementation and is one of the problems

we hope to fix with the new CCPS textbook on IPLs and IEs (pending 2010). An IPL cannot be assigned any risk reduction value if it is not maintained well enough to produce the risk reduction value. Part of the problem is that the industry is still struggling to know what tasks and how much effort (frequency) is needed to get these values. This is partly because the consensus codes and standards (except for the SIS standards) were developed *without* a specific IPL value in mind. LOPA rules, though, require organizations to maintain their IPLs and causes of IEs in a way that gives the probability of failure on demand (PFD) that they use in LOPA calculations. Where does an organization find this information on best practices for maintaining critical systems? Consensus codes provide a starting point for many IPLs and IEs; we expect these to gradually improve and they should eventually provide the anticipated PFDs (or failure rates) if the practices are followed. Plant data should be looked at to make sure the IE or IPL is not "outside" of the bounds expected. In the interim, we suggest to have very experienced operations and maintenance staff on the PHA teams (where scenarios are first identified and where the raw input data for LOPA is identified) and also have these same staff provide the maintenance practices, test practices, and operator drill routines for use within an organization.

- **IPLs and IEs must be validated and records must be kept and audited.** This has been a huge problem in the past 8-years of LOPA implementation and is one of the problems we hope to fix with the new CCPS textbook on IPLs and IEs (pending 2010). Currently, even if we follow industry advice, it means nothing if our own test data shows the IPL or IE value is worse than what we wanted. For instance, what if you follow industry advice for PSV maintenance and testing, but then your own records indicate that every time you pull a couple of specific PSVs, they are compromised in some way? Obviously, you have a problem with these specific PSVs and, therefore, using them as IPLs (or using the IPL value you hoped for) is not valid.

  Part of the problem is that the industry is still weak on reporting near misses. For many of us, any time we have challenged the last IPL or two, and anytime we find an IPL in a failed state, we have a near miss. Yet are these being reported and investigated? In most cases, they are not. There should be 20-100 near misses reported for each loss event, yet the ratio in the industry is currently 1-2 (Bridges, 2000 and 2008). The organization that gets many near misses reported (and a large percentage of these also get investigated), will have tremendous gains in loss prevention and will also have a much better idea of their reliability factors supporting the PFD values for IPLs and IEs failure rates.

  Most companies we deal with recognize they must have an inspection, test, or PM program for component and instrumented IPLs. But, most companies do not have a test program for response of humans to critical alarms or similar indications. Human action must be validated and documented to be an IPL. The specificity and frequency of such testing is still under debate, but it needs to occur. We hope to add more solid parameters to Human IPL qualification in the new CCPS textbook on IPLs and IEs (pending 2010).

  The follow is an example from the upcoming CCPS guideline on IPLs and IEs, which illustrates the requirements necessary for an organization to claim a given IPL and stated PFD value.

Example of Criteria Necessary to Qualify an IPL (extracted from rough draft of pending IPL/IE guideline, expected early 2010)

IPL Description	IPL PFD	Consequence Prevented	Special Considerations, including Special Independence Conditions	Proof Method	Proof Frequency
Deflagration Flame Arrester or Stable Detonation Arrester installed inline between an ignition source (e.g., TOX) and a source of flammable or combustible vapors	0.1	Deflagration, not detonation	- The piping between the ignition source and arrestor is well below the run-up distance required to allow a transition to detonation (DDT) for Deflagration type or formation of Unstable Detonation for a Stable Detonation type. - Location considered (avoid "hot side" on bottom of vertically mounted arrester since this decreases endurance burn; avoid accumulation of liquids in arrester, use drains to remove liquids). - Device does not impose excessive flow restriction on the process and any fouling issues have been addressed. - Temperature monitoring with a thermocouple directly in contact with the hot side of the device is highly recommended to allow operations to recognize when device is being challenged. Reference "Deflagration and Detonation Flame Arresters", Stanley S. Grossel, CCPS, 2002.	- Device is included on a routine maintenance schedule which specifies shutting down the line and opening the device for inspection. - Device is always inspected if it is suspected to have stopped a flame or if process upset could compromise its integrity. - Inspection includes determining whether the device is plugged and whether corrosion might compromise its capability to arrest a flame in accordance with most industry standards.	Initially, every 12 months or per vendor recommendation, then adjust the interval to 24, 36, or up to a maximum of 4 years, if no signs of corrosion.
Fire suppression system (water; water and foam; other suppressants); automatic	0.1	Explosion or further consequence beyond the external pool fire which can arise for whatever causes (such to prevent BLEVE of vessels, runaway reactions resulting in internal detonations, etc.). Not applicable to jet fires and not applicable to prevent a forming vapor cloud from exploding.	Using fire or smoke detectors to automatically activate a system designed to prevent or control a fire. For example, wet pipe or dry pipe systems with fusible links, deluge systems or water curtains applying water, foam. Can be within pipe or duct for flame-front suppression. Can be externals sprays for external fires (such as deluge system under pipe racks or under tansl/columns). See NFPA 13 Installation of Sprinkler Systems, NFPA 15 Standard for Water Spray Fixed Systems for Fire Protection, NFPA 16 Standard for the Installation of Foam-Water Sprinkler and Foam-Water Spray Systems or NFPA 750 Standard on Water Mist Fire Protection Systems for additional detail.	See NFPA 25 Inspection, Testing and Maintenance of Water-Based Fire Protection Systems for additional detail on what to test, how to test (methods), for water supply (tank, pond, etc.), water pressure source (head tank, pumps), activation systems, etc.	See NFPA 25 Inspection, Testing and Maintenance of Water-Based Fire Protection Systems for additional detail on testing frequency.
Fire suppression system (non-aqueous including dry agent) for room; automatic	0.01	Fire within an Enclosure	Refer to NFPA 17 Dry Chemical Extinguishing Systems, NFPA 2001 Clean Agent Fire Extinguishing Systems or NFPA 12A Standard on Halon 1301 Fire Extinguishing Systems for information on Dry Powder, Clean Agent and Halon Flooding Systems.	Refer to NFPA 17 Dry Chemical Extinguishing Systems, NFPA 2001 Clean Agent Fire Extinguishing Systems or NFPA 12A Standard on Halon 1301 Fire Extinguishing Systems for information on Dry Powder, Clean Agent and Halon Flooding Systems for Inspection, Testing and Maintenance Requirements	Refer to NFPA 17 Dry Chemical Extinguishing Systems, NFPA 2001 Clean Agent Fire Extinguishing Systems or NFPA 12A Standard on Halon 1301 Fire Extinguishing Systems for information on Dry Powder, Clean Agent and Halon Flooding Systems for Inspection, Testing and Maintenance Requirements.

- **Many times there is weak definition of the consequence that is being avoided, so an IPL does not always matchup well with the consequence.** This can cause both over- and under-estimates of the risk.

  One issue that we have come across is that the worst case consequences are being assumed for failure of a control system, which sounds wise, but for some cases, it is **overly pessimistic**. For instance a full bore pipework rupture is assumed due to brittle failure if the pipework is subjected to temperatures lower than its design temperature. While catastrophic brittle failure is remotely possible (this may only occur in 1 in 50 or 1 in 100 cases), we'd get a much better indication of the risk if operators recorded each occasion and the consequences of exceeding design parameters, even if nothing happened. Otherwise, we believe that we are being too pessimistic.

  Similarly, for overpressure scenarios, we see LOPA teams stating that the consequence will be catastrophic loss of containment if the pressure exceeds the set point of the PSV, whereas we normally have to reach 150% of the set point before we start to see leaks and normally have to reach >200% of the set point before the releases are large. And this 200% is still well below the deformation pressure for the system. On the other hand, the committee writing the new CCPS book on IPLs and IEs has been convinced by industry data that the PFD for a PSV is likely at 0.01 instead of the value of 0.001 stated in the example table of the first LOPA book (CCPS, 2001).

  > ***In the collective experience, there has been a tendency to overestimate the risk causing companies to spend far too much money on safety systems that are not necessary.***

  That said, there are cases where the **risks have been underestimated**, caused by predicting the consequences to be less severe than they would be. One illustrative example of this, is the Buncefield UK Incident (Buncefield, 2008), in which overfilling of one of the petrol tanks resulted in a series of explosions, which caused a huge fire, engulfing 20 large storage tanks (the largest fire in the UK since World-War II). The fire burned for 5 days. No one was killed, but there were 43 minor injuries. The incident happened early on a Sunday morning, but had it occurred during a normal working day there could have been a significant number of fatalities. The economic impact added to around £1 billion ($1.5 billion USD), which accounted for the emergency response, compensation for loss, costs to the aviation sector, and the investigation.

  > Consider conducting a LOPA on overfilling of a petrol tank before the incident. For the consequences, most LOPA analyst would have assumed that the petrol would run down the sides of tank and collect as a liquid in the bund (dike), which it did. But on igniting, what would you have assumed, bearing in mind that the area was not particularly confined? A pool fire in the bund (dike), most likely; serious, but not catastrophic. Few analysts would have perceived such massive explosions since the understanding was that petrol does not easily explode. The consequences, and hence the risk would therefore have been under-estimated and IPLs we consider necessary today would have been deemed over-kill.

2. **Overuse of LOPA.** Though we love LOPA, many of the originators thought LOPA would be used a lot less frequently than it is now. As shown in Figure 1, it was anticipated that LOPA would be used on 1-5% of the scenarios uncovered in PHAs. Further, though a couple of companies at the time were using LOPA within the PHA setting, it was anticipated that LOPA would eventually be used "after" a PHA team meeting. Various examples of overuse are discussed below:

- **Use within PHAs.** 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.

    - **Distracts PHA team from brainstorming** – The PHA teams have an awesome responsibility which is to find ALL scenarios that can lead to adverse risk, and do this for all modes of operation. This is the organization's one opportunity for finding most of these scenarios. Of course data has shown that a PHA team cannot find all scenarios; data on performing thousands of PHAs indicate that a PHA team usually misses 5% to10% of the large accident scenarios (even when they do thoroughly cover all modes of operation). Near misses and accidents are the other ways of finding these scenarios, but the industry (on average) still has trouble getting near misses reported, so our options for finding risky scenarios before catastrophe strikes is thin. Further, the mind is in a different pattern when brainstorming, compared to when analyzing. Analyzing is usually easier, so we tend to drift that way naturally. But, the job of the diverse members of a PHA team is to brainstorm. Since it is difficult to bring the team back into brainstorm mode after switching to analyzing mode, it is best for an organization to limit the amount brain-power expended by PHA teams on analysis.

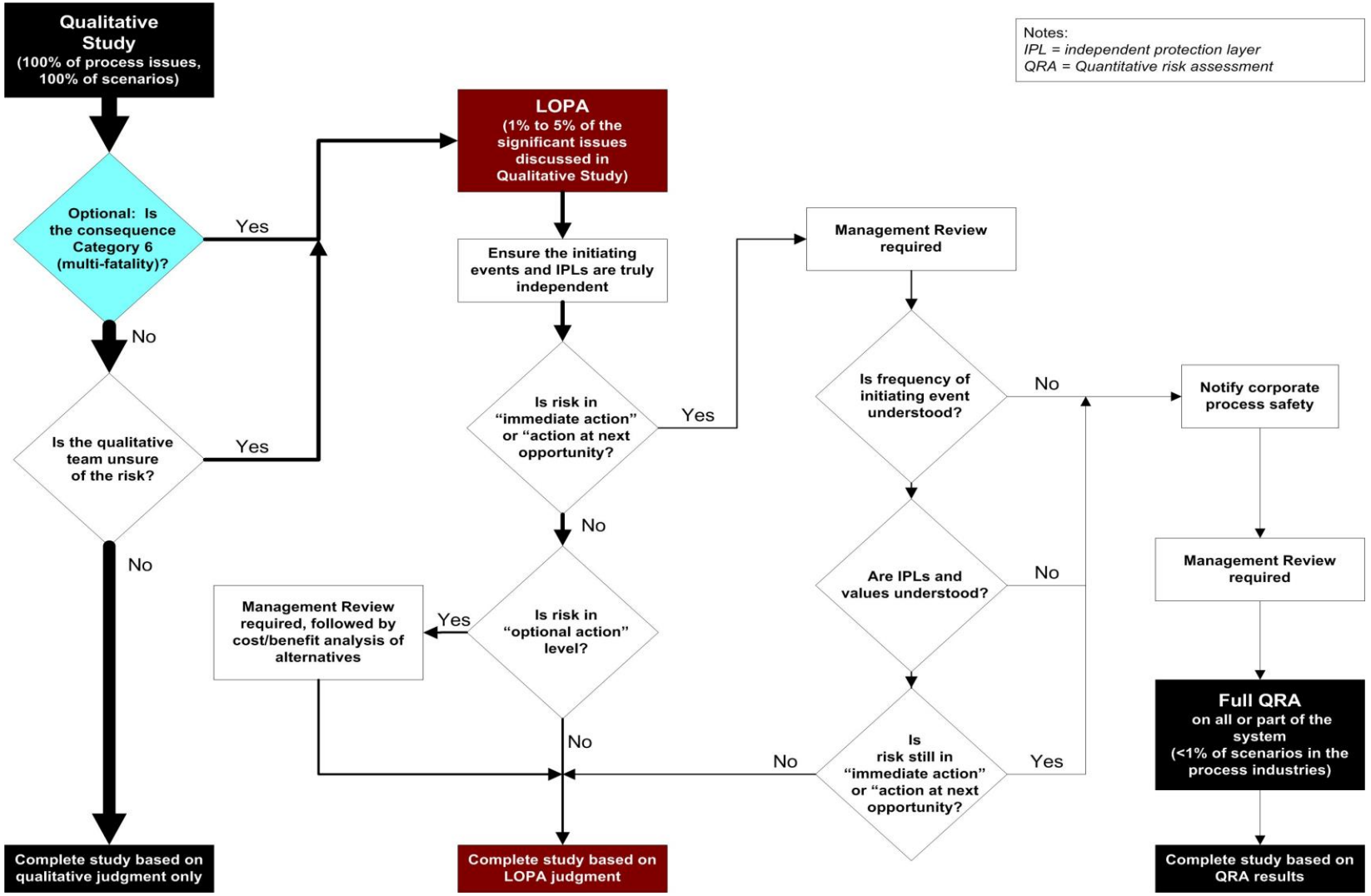
      One of the initial reasons for developing LOPA was to move semi-quantification of risk **out** of the PHA sessions, to enhance brainstorming. Notice the title that Art Dowell put on the first paper he wrote on the topic: "LOPA: **After** PHA/HAZOP, Before QRA" [emphasis added]. Now, many organizations are making the same mistake as in the early 1990s and moving LOPA (semi-quantification of risk) back into the PHAs. If an organization allows this, they will distract their multi-disciplinary teams from brainstorming and then they will miss accident scenarios. It makes no sense to analyze known scenarios in much more detail than before, while inadvertently causing the teams to miss other scenarios. It is the "undiscovered" scenarios that will cost the company more in the long run, since we will not have proper safeguards for many of these undiscovered scenarios.

    - **Takes time away from what is critical for the PHA team to do: Identify scenarios for ALL modes of operation.** LOPA is taking time away from proper identification of risky scenarios. For instance, folks feel now that they ***must*** do LOPA to validate the risk decision of PHA teams. However, those same PHA teams are NOT given time to do a proper identification of scenarios for all modes of operation. Many (perhaps most) PHA teams focus 90% on normal mode of operation, instead of focusing mostly on startup, shutdown, and other abnormal operations. Hence, they are not finding the majority of scenarios that account for 70% of the accidents that occur. (Historically, 70% of accidents occur during startup and shutdown modes of operation.) Yet, the same managers and staff who support LOPA for every scenario (which about doubles the time of an efficiently led qualitative risk review and risk judgment) are the same ones who say "What-if or 2-guideword analysis of startup and shutdown procedures takes too long" (yet this expansion of the qualitative studies to evaluate all modes of operation only takes about 50% more PHA team time). Perhaps in the future we will agree that more LOPA after a PHA will be beneficial; currently most PHA teams are only finding one half of the accident scenarios (focusing nearly entirely on normal [typically

continuous] modes of operation). We realize this is not a problem with LOPA itself, but it is an issue related to LOPA and is similar to the past trend in the UK where QRA was pushed hard (and still is) for each facility, even though they have not completed a proper PHA of all modes of operation. The only difference between the over-emphasis on QRA and what is happening now is that LOPA produces a faster QRA. The industry is still missing many of the largest and least protected scenarios in favor of over-analyzing the scenarios they know about. Chapter 9 of the HEP Guideline, 3rd edition (CCPS, 2008) explains how to analyze non-routine modes of operation.

On the other hand, for the scenarios found by the PHA/HAZOP team, once a LOPA is performed on the few critical or confusing scenarios, other related scenarios are thought of. So, LOPA does help discover "some" new or related scenarios, but overall, we believe LOPA will cause a PHA/HAZOP team to find less scenarios, if used in situ during a PHA/HAZOP team meeting.

- **Use for every Medium and High Risk Scenario**. This issue is likely covered adequately in the discussion above, but 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 (both issues are listed above). The following is the guide we use to decide when a LOPA is required (Category 5 is equivalent to consequences greater than $100,000,000 and/or with potential multiple fatalities):



When to use LOPA ***(courtesy of Process Improvement Institute, Inc., 2004)***

Example Situation where LOPA was not necessary – common sense only was needed

The PHA Issue:

- A tank truck containing a highly flammable and reactive chemical is being used as a feed material for a batch reaction system.
- The tank truck is not considered a pressure vessel but does have its own relief system. Relief set pressure is relatively low, suggesting the design pressure of the tank truck is somewhere between atmospheric and 15 psig.
- The reactor system operates at a higher pressure than the tank truck relief system set pressure.
- If the tank truck is exposed to a residual pressure from the reactor system, there is concern the tank truck could rupture or experience a significant leak leading to a large fire or resulting in a localized overpressure from a semi-confined vapor cloud explosion.

The PHA Team/LOPA issue:

- A comprehensive procedure is in place to make sure the reactor pressure is completely reduced to atmospheric before the block valves are opened to allow charging the reactor with material from the tank truck.
- The PHA Team felt that the procedures were not adequate and that this hookup and block valve opening procedure should be strengthened by the addition of a "permissive interlock" that would prevent the block valve from opening if the pressure in the reactor was above a value that was considered dangerous to the integrity of the tank truck.
- The PHA Team recommended that LOPA be used identify the required reliability (SIL) for the proposed permissive interlock.

LOPA/PHA Consultant response:

- The LOPA analyst took some time to understand the process and procedure involved in this reactor charging requirement. This included questions about the existing relief system on the tank truck, the number of people normally in the vicinity of the tank truck during the charging operation, who exactly was responsible for the reactor hookup and block valve opening procedure, and if there was any way the mistake could be discovered (such as high pressure in the reactor) before the block valve was opened exposing the tank truck to high pressure.
- A discussion around the consequence of developing a significant leak in the tank truck and potentially leading to a significant fire showed that the most likely result would be a significant injury but not necessarily a fatality. This allowed a more realistic discussion around the perceived need for additional safeguards.
- The PHA team felt strongly the permissive interlock needed to be evaluated and required reliability specified using LOPA. The following LOPA features were identified and discussed with the team:
  - ✓ The scenario involving the permissive interlock was dominated by operator procedures and therefore LOPA may not be the appropriate analysis tool.
  - ✓ If LOPA is used the required SIL would probably be at least a SIL 2. The consultant presented a strong position that the LOPA rules around independence between IPL's and the initiating event were going to be followed.
- The consultant offered the opinion that a SIL 2 permissive interlock made no sense and the actual design of this type system for a "make and break" connection would be very difficult to operate and maintain on a going basis.
- The final recommendation was to make the permissive interlock a SIL 1 system. This would go a long way to improving the safety of the operation because it added diversity and independence to the operation. (Usually, simply adding diversity to the IPLs is more valuable than the prospect of making the device a SIL 2 or higher.).
- The team was still concerned about documenting the conclusion and recommendation since it was not going to be in terms of an analysis system such as LOPA. The consultant asked what we would have done 15 years ago before the existence of these various analysis tools. The answer is we used "common sense" and our knowledge of the hazards associated with the systems we operate. The existence of tools like LOPA doesn't mean we are not allowed to think and be able to make reasonable risk reduction decisions.

- **Use in studies that are redundant to PHAs, such as "separate SIL determination."** IEC 61511 allows a qualitative PHA team to determine if a SIL is needed for a scenario and to specify a SIL 1 or 2, if one is needed. Yet, most folks believe that only LOPA or RiskGraph or QRA is valid for determining if a SIL is needed and then use the same methods to determine what SIL is needed. As a result, many people do LOPA on almost every scenario of moderate consequence or higher. The LOPA book authors expected the number of scenarios going to LOPA (after a HAZOP/PHA) be 1% to 10% (max) of those uncovered in a qualitative analysis, and some of us believed that usually a team would use LOPA only if the scenario was too complex for the PHA/HAZOP team. SIS standards allow a PHA team to determine (1) when a SIF is Not required and (2) what SIL is needed if an SIF is required (though for SIL 3 and higher, a LOPA or similar study is recommended by SIS standards).

3. Too many resources dedicated to LOPA studies.

- **Typically, one LOPA analyst is sufficient (if he/she has easy access to experts within the organization).** Once a LOPA is completed for a scenario, the results can be relayed to management or to a PHA team, or similar decision makers. The mention of a LOPA team in the first LOPA book was anecdotal, but many organizations now require a LOPA team (instead of single analyst). Some companies used a LOPA team early because (1) the analyst trained in LOPA was not in the PHA session, so translation from the PHA team to the analyst was necessary in many cases and (2) LOPA was new, so more heads were needed to decide "Is this the right way to apply LOPA." However, if the LOPA analyst was on the PHA team or if the teams get used to communicating to the LOPA analyst(s), then one person can perform the LOPA. Note that no brainstorming is necessary for LOPA, so there is no inherent need for a team.

- **Why use a LOPA team (with a LOPA leader and LOPA scribe)?** There is almost No brainstorming occurring during a true LOPA analysis so there is no need for a team. On the other hand, if the LOPA team (or PHA team) recommends a SIL, then a small team (2-3 experts) will be needed to "specify the SIL design and functionality issues (such as sequence and delays) for the SIL". Also, later someone (usually one person) will be needed to validate the SIL design will produce the SIL determined by the PHA or LOPA team.

4. Too much emphasis on software.

- **You do not need software for a 1+1+2=4 calculation (i.e.,** "Why use a sledgehammer to crack a nut?"). Most of the commercial packages for documenting PHAs (using HAZOP, What-If, or whatever methods) have options for sending scenarios to LOPA worksheets. These can ease the completion of LOPA and ease the exporting of some data for from PHA records into a LOPA form; in fact, one of the authors of this paper designed one of the first such applications for LEADER software. On the other hand, these PHA software options do not make it easier to document "why an IPL is valid." Many analysts and most operating companies have implemented their own spreadsheet applications, which:

  - Take very little effort to develop
  - Are easy for others in the company to learn
  - Can be linked to internal reliability data tables for company-approved IPLs and IEs
  - Are easy to use on multiple work-stations
  - Are easy to add and edit text that describes the scenario and factors
  - Are often easier to use than PHA software

The most important needs of LOPA documentation are to enter/record the scenario description in detail, explain clearly why an IPL is given credit, and most importantly, describe how each IPL is maintained to sustain the credit given. This can all be done freehand, and PHA (or LOPA) software does not help shortcut this necessary chore.

Closing

Introduction of the streamlined quantitative risk assessment method, LOPA, has had a tremendous impact on the chemical and related industries. 90% of the quantitative risk assessments that may be necessary can now be performed in $1/10^{th}$ the time of a QRA. Many benefits have been reaped, including a continual improvement on the identification and control of critical features and actions. However, the initial rollout of LOPA has led to a few problems, as discussed in this paper. The problems are easily remedied by judicious use of LOPA and by carefully adhering to the rules of LOPA.

References

1. *Guidelines for Hazard Evaluation Procedures, Third Edition with Worked Examples*, CCPS/AIChE, New York, NY, 2008.

2. *Initiating Events and Independent Protection Layers for LOPA, CCPS/*AIChE, New York, NY, 2010 [pending].

3. *Layer of Protection Analysis (LOPA); Simplified Process Risk Analysis*, CCPS/AIChE, New York, NY, 2001.

4. Bridges, W.G. (with T.R. Williams), "Risk Acceptance Criteria and Risk Judgment Tools Applied Worldwide Within a Chemical Company," *International Conference and Workshop on Risk Analysis in Process Safety, CCPS/AICHE,* Atlanta, GA, October 1997.

5. Bridges, W.G., "Getting Near Misses Reported - Revisited," *8th ASSE-Middle East Chapter Conference and Workshop*, Bahrain, February, 2008.

6. Bridges, W.G., "Get Near Misses Reported," *International Conference and Workshop on Process Industry Incidents, CCPS/AICHE*, Orlando, FL, October 2000.

7. Dowell, A. M., III, "Layer of Protection Analysis: A New PHA Tool, After Hazop, Before Fault Tree," *International Conference and Workshop on Risk Analysis in Process Safety*, CCPS/AIChE, Atlanta, GA, October 1997.

8. Ewbank, Rodger M., and Gary S. York, "Rhône-Poulenc Inc. Process Hazard Analysis and Risk Assessment Methodology," *International Conference and Workshop on Risk Analysis in Process Safety, CCPS/AIChE,* Atlanta, GA, October 1997.

9. IEC (1998), IEC 61508, *Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems, Parts 1–7,* Geneva: International Electrotechnical Commission.

10. IEC (2001), IEC 61511, *Functional Safety Instrumented Systems for the Process Industry Sector, Parts 1–3,* Geneva: International Electrotechnical Commission.

11. The Buncefield Incident, 11 December 2005, *The Final Report of the Major Incident Investigation Board*, Volume 1 (2008).

About the Authors

William G. Bridges (Bill)

Bill is President of Process Improvement Institute (PII). Formerly, he was a director of the Risk Consulting Division of ABS Consulting (formerly JBF Associates and EQE International). He is considered one of the leading authorities on process safety engineering, risk management, and human error prevention. He has a Bachelor and Masters degree in Chemical Engineering and he has over 30-years of chemical industry experience in process engineering, process/product development, management, safety evaluation, and operations. His last position in the chemical industry was as a chemical plant manager. Bill has helped many companies in the petroleum, petrochemical, plastic and chemical process industries develop, implement and assess PSM and risk management programs. Bill has taught PSM related courses, including process hazard analysis/HAZOP leadership, incident investigation/root cause analysis, and management of change (MOC) since 1987. Bill helped develop and teach the first LOPA course, when he co-developed it and co-taught it within ARCO Chemicals in 1995-1996. He was a principal author of the first LOPA book for CCPS/AIChE (2001) and he is the main author for the upcoming book related to LOPA, *Independent Protection Layers and Initiating Events*, CCPS/AIChE, pending 2010.

Dr. Tony Clark

After gaining a Bachelor and PhD in chemical engineering at Aston University in the UK, Tony began his career teaching chemical engineering to HND and B.Eng (Hons.) students at the Polytechnic of Wales, he then moved into consultancy and has more than 20-years experience in the fields of safety, loss prevention and environmental assessments. His work has included preparation of safety reports and QRA studies for a variety of onshore and offshore oil and gas installations, chemical and petrochemical plants both in the UK and overseas, and in particular, the Middle East. In the early 1990's, he was seconded to BP Exploration in Scotland where he was a safety coordinator for a large offshore gas development. Tony's training experience includes devising and presenting training programs covering the techniques of HAZOP, Hazard Analysis, and elements of PSM to the Chinese in Xinjiang. He has delivered hazard assessment and emergency planning training to Indian engineers and risk assessment & environmental analysis training in the Middle East. Tony continues to deliver consulting and training services to clients in UK, Europe, and the Middle East, including LOPA analysis, PHAs, HAZOPs, quantitative risk assessments, etc. Tony has been involved in several hundred LOPA and SIL determinations studies around the world since 2002, both as chairperson and as a design safety engineer. His most recent role has been as the Lead Design Safety Engineer for a gas processing and storage project in the UK, which has involved undertaking assessment work to determine the requirement and extent of safety systems. He is a co-author for the upcoming book related to LOPA, *Independent Protection Layers and Initiating Events*, CCPS/AIChE, pending 2010.

.