More Issues with LOPA – from the Originators

William Bridges
President
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
wbridges@piii.com

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute, Inc.
2437 Bay Area Blvd, PMB 260
Houston, TX 77058-1519
Adowell@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2021 Spring Meeting and 17th Global Congress on Process Safety
Virtual
April 18 - 22, 2021

AIChE shall not be responsible for statements or opinions contained
in papers or printed in its publications

More Issues with LOPA – from the Originators

William Bridges
President
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
wbridges@piii.com

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute, Inc.
2437 Bay Area Blvd, PMB 260
Houston, TX 77058-1519
Adowell@piii.com

Keywords: LOPA, conditional modifiers, enabling conditions, time at risk

Abstract

Layer of protection analysis (LOPA) has now been around for more 25 years and in general use for now 20 years, starting with the initial textbook being officially published in 2001. Two companion books have been published on the topics of Enabling Events and Conditional Modifiers (2014) [9] and on Initiating Events and Independent Protection Layers (IPLs), (2015) [8]. Many papers have been published in the past 20 years on LOPA.

This paper shares observations and lessons learned from two originators of LOPA and provides further guidance on how to and how Not to use LOPA. The paper provides specific examples of best practices, some of which are not covered well enough in or are omitted from the textbooks on the topic. The originators of LOPA hope you will use this paper as an expansion on the concepts in the first LOPA textbook, and as an addendum to all three textbooks on the topic.

1 Introduction

1.1 Brief History of LOPA

The initial development of layer of protection analysis (LOPA) was done internally within several 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.

The first LOPA book was developed by a CCPS committee from 1997 through 2000 and was published in 2001 [7] (Art Dowell and William Bridges were the co-originators and were principal authors of the book). LOPA has become widely used following the publication of the LOPA textbook nearly 20 years ago. Especially during the last 16 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 (many of these are now even engrained across the chemical industry), 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. This book is *Guidelines for Initiating Events and Independent Protection Layers*, CCPS/AIChE, 2015 [8]. William Bridges was the primary contractor/author of this book from 2007 to April 2012. Another companion book on related topics, *Guidelines for Conditional Modifiers and Enabling Events* [9], CCPS/AIChE was published in 2013; Mr. Bridges was a committee member and contributed to this book as well. ***This paper comments on deficiencies and dangerous precedents in both of these newer textbooks, as well as commenting on issues with the implementation of LOPA as observed in industry while working around the world***.

1.2 Intent of LOPA

LOPA is one of many methods for assessing a given scenario to determine if the risk is tolerable. It uses rigid rules to simplify and standardize the definitions of and 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. A common 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 frequently coalesces into excellent judgment of risk for most accident scenarios. On the other hand, the judgment of the PHA team is slanted by the experience of the team members, and it frequently can be helpful to use LOPA to provide consistency in risk decisions. A key responsibility of the PHA team (or LOPA analyst) is to assess the consequence severity correctly. Given an accurate understanding of the consequence severity, LOPA can quickly evaluate the likely frequency of the initiating event and the effectiveness of the IPLs.

1.3 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 International Society of Automation (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 for risk reduction; and LOPA is the preferred method for determining what SIL is necessary, if a SIF is chosen as the risk reduction method.

2 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 15+ years of use. As the originators, we believe we are in a unique position to point these out and we believe we also have a unique obligation to highlight misuse of LOPA.

2.1 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 (1) not 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 [10]:

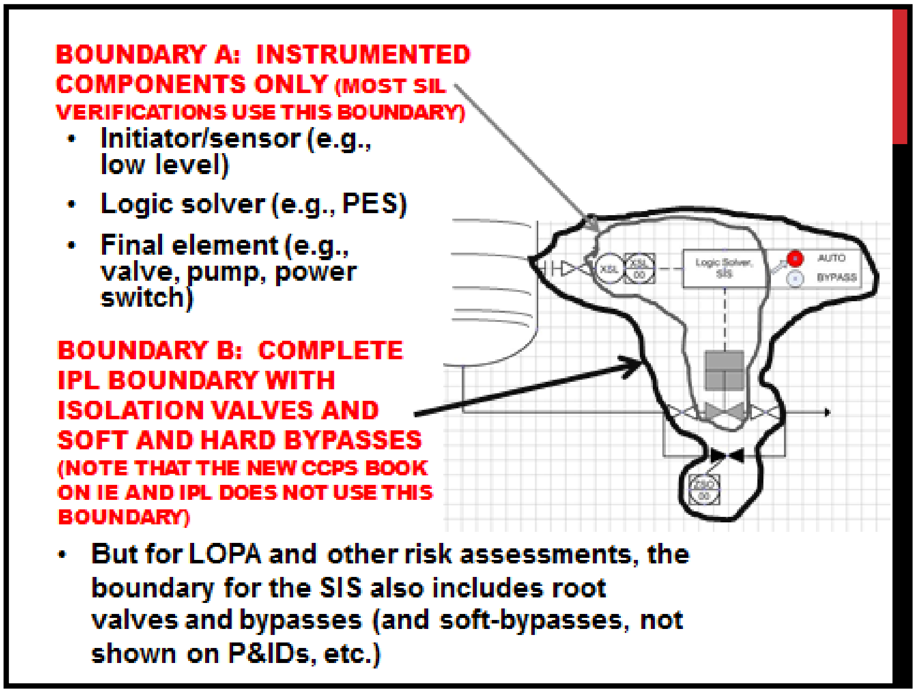
- **The frequency (likelihood) for an IE or the probability of failure on demand (PFD) for an IPL applies to the entire boundary of that IE or IPL**. The IE or IPL includes any items on or off of the P&IDs and other reference documents that could increase the unreliability or unavailability of the IE or IPL. So, root valves, isolation valves, and hardware or software bypasses are all part of the definition of an IPL or IE. This concern is especially important for high integrity protection systems such as PSVs – pressure safety valves (where PFDs can be 0.01 for a single PSV to 0.001 for dual, full-size PSVs) and for SIL 2 and SIL 3 instrumented functions. A paper by Dowell [2018, 2019], *Understanding IPL Boundaries*, focused on this one issue [11]. In practice, we have found this rule to be toughest to learn for PHA teams and new LOPA analysts. See the example of boundaries provided later in this paper.

- **If the IPL is a PSV, then the IPL system must include upstream and downstream features, such as isolation valves.** Therefore, the probability of leaving an isolation valve closed should be included as a contribution to the overall PFD of the PSV IPL system.

  In this case, actual data from industrial plants of all types have shown that the probability of leaving a block valve closed (upstream or downstream of the PSV) is a significant portion of and sometimes dominating factor in the PFD of the PSV. In several studies by different companies shared during the writing of *Guidelines for Initiating Events and Independent Protection Layers* [8], the sites found that the PFD of the PSV was in the range of 0.001 to 0.02, whereas the probability of the upstream or downstream block valve being in the inadvertently-left-closed position (but with a CSO [car sealed open] tag in place!!) was about 0.01 to 0.04. This finding led that book writing committee to state that the PFD of a PSV with upstream or downstream block valves (using a standard CSO system for administrative control of the block valves) must be set at 0.1, until the site:

  - proves by independent auditing that the error rate of leaving a block valve closed in less than 0.005
  - installs more reliable means to ensure the flow path is open, such as:
    - using dual relief valves with a three-way Y-valve to switch flow paths (The three-way valve shall be configured to provide the full-flow path at all times during the switching operation.)
    - installing a captive key system of the proper sequence to ensure the block valves in one flow path are open before starting up (i.e., before opening a potential pressure source to the protected equipment)
    - installing limit switches to verify the block valves are open and interlocking the position switches to a permissive that must be cleared before startup

- **High integrity SIFs (SIL 2 and SIL 3).** Note that the system (loop) boundary for an instrumented safety system is defined differently by SIS standards (and the new CCPS book on IEs and IPLs) versus LOPA by the co-originators. In the SIS standards, the system boundary for calculating the SIL for a given SIF includes only the instrumented components of the system. This boundary omits the systematic failures possible from the process itself and more importantly omits the specific human errors of leaving the system in bypass or the dependent errors of miscalibrating 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 actual performance versus instrument-only [academic] reliability) [11]. Below is an illustration of the difference between the boundary of a SIF as used in SIS versus as used in LOPA; note that the LOPA boundary is the correct definition for risk assessment and process safety management:



BOUNDARY A: INSTRUMENTED COMPONENTS ONLY (MOST SIL VERIFICATIONS USE THIS BOUNDARY)

- Initiator/sensor (e.g., low level)
- Logic solver (e.g., PES)
- Final element (e.g., valve, pump, power switch)

BOUNDARY B: COMPLETE IPL BOUNDARY WITH ISOLATION VALVES AND SOFT AND HARD BYPASSES (NOTE THAT THE NEW CCPS BOOK ON IE AND IPL DOES NOT USE THIS BOUNDARY)

- But for LOPA and other risk assessments, the boundary for the SIS also includes root valves and bypasses (and soft-bypasses, not shown on P&IDs, etc.)

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

Since the documents from the SIS standards-writing committees (ISA and IEC) and since the CCPS book *Guidelines for Initiating Events and Independent Protection Layers* (2015) all fail to explicitly address this error in the definition of the boundary of a SIF, it is likely that many companies implementing a SIL 2 or SIL 3 protection system will follow the advice of the committees above and fail to realize that the PFDs they are depending upon for a SIL 2 or SIL 3 are not being met. The shortfall in SIL occurs because the specific human errors were not accounted for during the design of these SIFs or were not adequately prevented by other means (since the implementers would not know to take such measures). See the papers by Bridges *et al* for more detailed explanation and examples [12, 13].

- **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 meets the requirements of the updated SIF standards [14, 15]. That is, for two BPCS loops to be considered as IPLs, everything must be independent except the backplane – independent sensors, independent input cards, independent CPU cards, independent output cards, and independent final elements. Similarly, if a BPCS is used to “shadow” or “mirror” 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 a human operator or use another operator within the same work team; this practice 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 CCPS book (*Guidelines for Initiating Events and Independent Protection Layers, 2015* [8]) provides 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 mindset 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 environment of the equipment and the local control of human error. For example, a PSV in clean gas service has a much different reliability than a PSV in olefin or acid service. The CCPS book, *Guidelines for Initiating Events and Independent Protection Layers,* 2015 [8], addresses this issue well.

  In addition, some plant staff believe their components have much better reliability (lower PFD or IEF) than is provided in the textbook mentioned above, and yet the site may only have 20 years of operating history. But the site does not fully understand how to estimate the failure rate of such components. For instance, for a basic process control system (BPCS) loop, the site staff:

  - may not count failures of any component with the loop boundary (for issues on boundaries mentioned earlies)
  - may not count failures found and corrected before a problem occurs as a failure
  - may not have enough operating years for the loop to have a statistically significant failure rate

  Using IEF or PFD values lower than stated in other people's data (such as in the textbook mentioned above) must be defensible statistically and in writing. See the next few subsections for more information on this issue.

- **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 20+ years of LOPA implementation and is one of the problems addressed in *Guidelines for Initiating Events and Independent Protection Layers,* 2015 [8]. 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 issue is partly because the consensus codes and standards (except for the SIS standards) were developed *without* a specific PFD value in mind. LOPA rules, though, require organizations to maintain their IPLs (and also 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 sites that follow all of the practices in the related code or guide should eventually witness (by validation) the anticipated PFDs (or failure rates). Plant data should be reviewed to make sure the IEF or the IE or PFD of the 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 are identified) and also have these same staff provide the maintenance practices, test practices, and operator drill routines for use within an organization. *Guidelines for Initiating Events and Independent Protection Layers,* 2015 [8], addresses this issue well.

- **IPLs and IEs must be validated, and records must be kept and audited.** This issue also has been a huge problem in the past 18 years of LOPA implementation and is one of the problems addressed in *Guidelines for Initiating Events and Independent Protection Layers,* 2015 [8]. 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 specified in the LOPA. 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 PFD 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 last two IPLs, 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 about 2 (Bridges, 2000, 2008 [16], and 2012 [17]). 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 also IEs failure rates).

  Most companies we deal with recognize they must have an inspection, test, or PM (preventive maintenance) 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.

  Guidelines for Initiating Events and Independent Protection Layers, 2015 [8], addresses this issue well, except for human IEs and human IPLs, for which critical text is missing on how to establish and measure the PFD for a human response IPL, and how often to measure this PFD. Review the paper "LOPA and Human Reliability – Human Errors and Human IPLs (Updated)", Bridges and Clark, 2011 [18] for the additional guidance needed for human IEs and human IPLs.

- **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 the vessel is hydro-tested at 130% or 150% of the set point (depending on the vessel mechanical design code). The vessel is not expected to leak at the hydro-test pressure, but instrumentation and mechanical seals might begin to leak. Additionally, we would expect to see large leaks above 200% of the set point. Catastrophic rupture would not be expected until 300% or 400% of MAWP – maximum allowable working pressure – (again depending on the vessel mechanical design code).

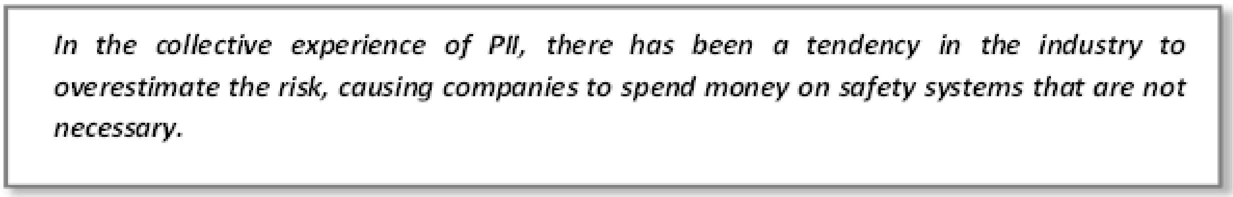
Therefore, some organizations are evaluating two scenarios for an increasing pressure scenario that exceeds MAWP:

1. A leak scenario that occurs above 130% or 150% of MAWP
2. A rupture scenario that occurs above 300% or 400% of MAWP

Such organizations provide guidance for two conditional modifiers, probability of leak and probability of rupture.

Of course, if the vessel has not been appropriately inspected and maintained, then the response of the vessel to an overpressure challenge is unknown.

On the other hand, the committee that wrote the CCPS book [8] on IPLs and IEs was convinced by industry data that the PFD for a PSV is likely 0.01 instead of the value of 0.001 stated in the example table of the first LOPA book (CCPS, 2001). [7]



In the collective experience of PII, there has been a tendency in the industry to overestimate the risk, causing companies to spend 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) [19], 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 up to around £1 billion (US$1.5 billion), which included 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 analysts 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.*

2.2 Overuse of LOPA.

Some of originators thought LOPA would be used a lot less frequently than it is currently. It was anticipated that LOPA would be used on 1-5% of the scenarios uncovered in PHAs. It was also anticipated that LOPA would be used "after" a PHA team meeting, since that is how the originators were using it. *Note that PII deals with hundreds of clients worldwide, and some of our clients listen to PII's advice on this issue, while others force us to do LOPA within the PHA and force us to do LOPA on every scenario (100% of the scenarios, not the 1 to 5% of scenarios that are confusing to the PHA team). This unfortunate stance by clients has had the benefit of clearly showing how wasteful these decisions are.*

Various examples of overuse are discussed below *(Bridges, 2009 [20], discussed these issues in detail):*

- **Using LOPA within PHAs - a bad idea as it detracts from brainstorming.** Many of the original LOPA book authors 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 scenarios). 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 (using a qualitative definition of an IPL), then performing LOPA in situ is usually overkill. In most situations, an experienced 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 -** Similar to 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. On the other hand, LOPA does provide a uniform, structured, consistent approach for making risk decisions for scenarios. For a **less** experienced PHA team, one of the authors has found LOPA to be more effective in making consistent decisions than the judgment of the PHA team. Again, both authors strongly recommend that the brainstorming and identification of hazards be done first in the PHA. Then the LOPA phase should be done after the PHA is complete. The LOPA can be done either by a LOPA analyst assisted by the appropriate expertise from the facility, or if required by the organization, by members from the PHA (as needed). With that said, ***if the PHA team is NOT experienced enough to understand and make good risk judgments, and you need to use a LOPA analyst or a team of risk judges to augment the PHA team, then why trust the PHA team to do the PHA in the first place?***

- **Use for situations covered by a specific standard** – Over time, organizations have observed that the same hazardous process situations are identified in different facilities and different locations. Many organizations have developed internal (or industry) standards that specify specific IPL configurations for specific hazardous process situations. An organization may choose to evaluate the application of its internal standard to a specific situation to confirm that the specified IPLs will reduce the risk to meet the organization's risk tolerance criteria. Once that determination has been made, the organization can choose to apply its standard whenever that hazardous situation is identified in the PHA. Since it is specifically covered by the standard it is no longer necessary to apply LOPA to every occurrence. In short, "if it is covered by standard, don't apply LOPA".

    - A typical application of NFPA requirements for fired equipment would cover nearly all of the scenarios for a package boiler. The highest risk scenario has been found to be lighting the burner with the operator at the furnace front. That risk can be mitigated by moving the operator station during lighting away from the furnace front (see the paper by Champion, 2006) [21].

PII has observed that most companies tend to go through phases of use of LOPA. First, a company that has not used LOPA before decides to use LOPA. Soon afterwards, they convince themselves (or consultants or regulators convince them) that if using LOPA for some scenarios is good, then using LOPA for many scenarios is better, and some companies eventually require use of LOPA for ALL scenarios. This use of LOPA is overkill, of course. On the other hand, the overuse of LOPA is good at training companies on the importance of (1) good PHA teams, (2) valid IPLs, and (3) solid programs for maintaining the PFD of stated IPLs.

Eventually, the companies realize that the extra effort, beyond the PHA team decision, of doing LOPA is not justified for about 95% of the scenarios identified by the PHA teams. This may be partially due to improvements in the competencies of PHA team leaders and team members as they learn and use LOPA more.

When to use LOPA - Figure 1 on the next page 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):

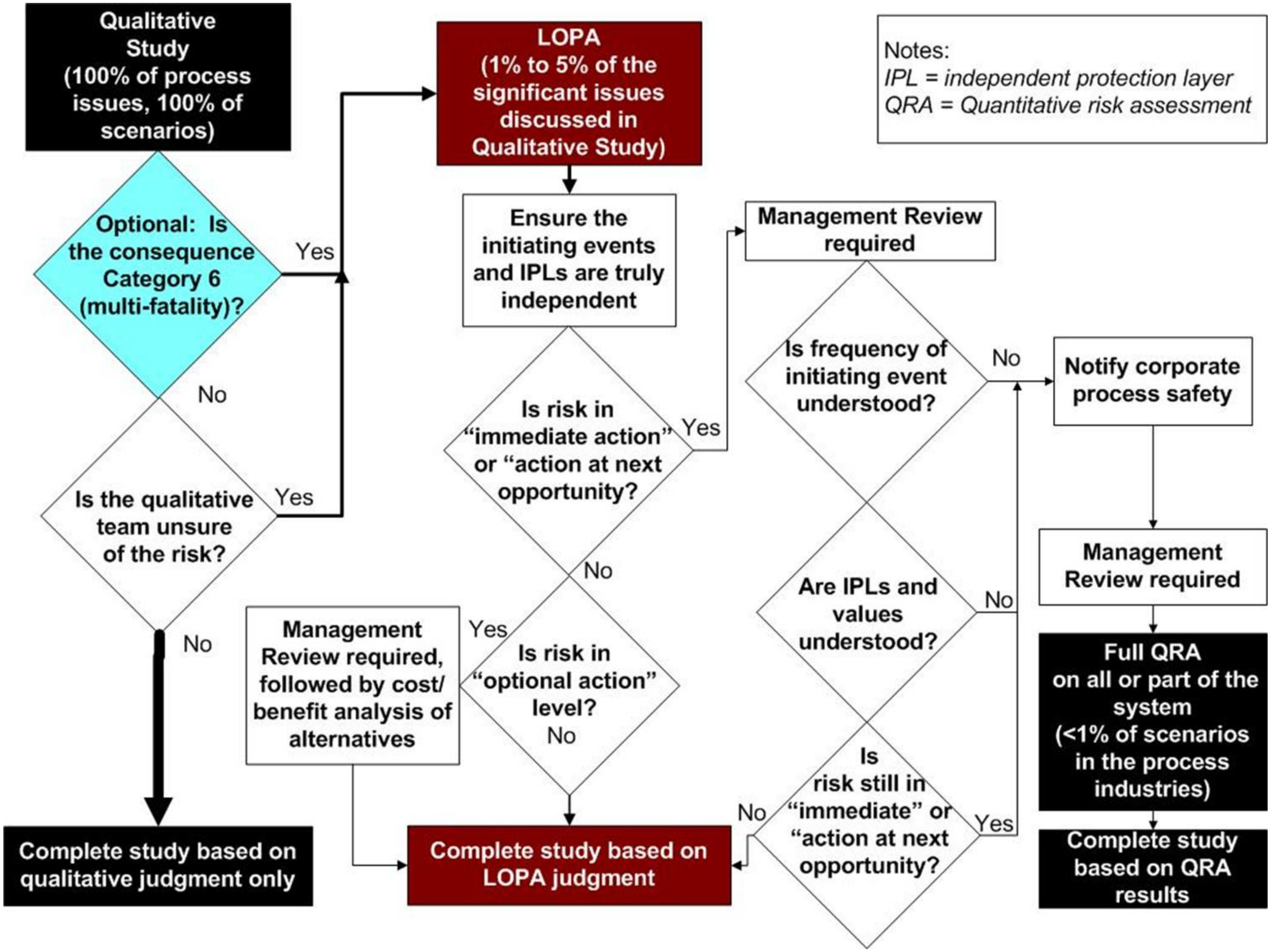

Qualitative Study (100% of process issues, 100% of scenarios)
Optional: Is the consequence Category 6 (multi-fatality)?
Yes
No
Is the qualitative team unsure of the risk?
Yes
No
Complete study based on qualitative judgment only
LOPA (1% to 5% of the significant issues discussed in Qualitative Study)
Ensure the initiating events and IPLs are truly independent
Is risk in "immediate action" or "action at next opportunity?
Yes
No
Is risk in "optional action" level?
Yes
No
Management Review required, followed by cost/ benefit analysis of alternatives
Complete study based on LOPA judgment
Notes:
IPL = independent protection layer
QRA = Quantitative risk assessment
Management Review required
Is frequency of initiating event understood?
No
Are IPLs and values understood?
No
Is risk still in "immediate" or "action at next opportunity?
No
Yes
Notify corporate process safety
Management Review required
Full QRA on all or part of the system (<1% of scenarios in the process industries)
Complete study based on QRA results

Figure 2: When to Use LOPA (Courtesy of Process Improvement Institute).

- **Use in studies that are redundant to PHAs, such as "separate SIL determination."** 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 or RiskGraph or QRA is valid for determining if a SIF is needed, and then they 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 originally 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). See IEC 61508, 61511 [1, 14], and related TR from ANSI/ISA to make these same determinations. See ISA TR 84.00.02, 2002 (and 2004), Section 3.8:[22], updated (2015) [23].

  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 for an SIF is needed to lower the risk to the risk tolerance criteria?" 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).

- **Use in studies that are redundant to PHAs, just to identify IEs and IPLs.** A PHA team can be just as capable as a LOPA analyst (or team, if a team is used) in determining which scenario features are IEs and which should be IPLs and which of those candidate IPLs meet the definition of an IPL, as explained in detail in Bridges, Dowell, "Identify SIF and Specify Necessary SIL, and other IPLs, as part of PHA/HAZOP" (2016) [25]. It is critical to identify all IEs and all IPLs for a process area, so that the company can maintain these features as safety-critical or process-critical features; but by following the advice in the referenced paper, the PHA teams can readily do this task, without the need to also perform LOPA for that task.

- **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 frequently perform the LOPA. Note that no brainstorming is necessary for LOPA, so the need for a team input (which may come from the LOPA analyst, if he or she was on the PHA team, is limited to confirmation of details of existing IPLs including configuration and independence, and to providing organizational preference for choosing IPLs and for detailed IPL configuration.

  - **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 limited need for a team. On the other hand, if the LOPA team (or PHA team) recommends an SIF, then a small team (2-3 experts) may be needed to specify the SIF design and functionality issues (such as sequence and delays) for the SIF. Also, later someone (usually one person) will be needed to validate that the SIF design will produce the SIL determined by the PHA or LOPA team (via SIL Verification calculations).

- **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 from PHA records into a LOPA form; in fact, one of the authors of this paper designed one of the first such applications for the *LEADER*^{TM} software [24]. 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. PII uses Excel templates for documenting LOPA.

3 Misuse of Conditional Modifiers and Enabling Events

We frequently observe misuse of conditional modifiers and enabling events. There is a temptation for some LOPA practitioners to use these when they see that a calculated mitigated consequence frequency is too high to meet the organizations risk tolerance criterion. They then try to adjust (or “cook”) the numbers to reduce the calculated frequency by inserting conditional modifiers and enabling events, many of which may not be applicable to the scenario.

3.1 Misuse of Conditional Modifiers

Some LOPA originators (or their organizations) used consequence severity categories based on human harm (e.g., fatality) or property damage (e.g., $MM). To properly evaluate scenarios, they found that conditional modifiers (CM) were needed. Given the calculated frequency of a release, conditional modifiers were needed to account for 1) the probability of ignition for a flammable release, *Pi*, 2) the probability of one or more persons present in the danger zone for toxic release or a fire, *Pp,* and 3) the probability of fatality, *Pf*. Omitting these conditional probabilities would overestimate the risk.

Where the conditional modifiers of *Pi*, *Pp*, and *Pf* are part of the LOPA system, their use should be constrained by the LOPA guidance for the organization to ensure consistency. Tables 1-3 provide recommended guidance used by PII that is reasonably consistent with CCPS guidelines [7, 9].

Several of the originators of LOPA completely avoided use of enabling events (EE) and conditional modifiers (CM), developing consequence severity categories based on the amount of the release from a loss of containment and the condition of the release (e.g., below the boiling point, above the boiling point). The consequence severity categories inherently included the conditional modifiers of *Pi*, *Pp*, and *Pf*. For this LOPA system, attempting to use *Pi*, *Pp*, and *Pf* would underestimate the risk. In such cases, some analysts have wrongly used EEs and CMs to "cook" the numbers to meet the risk tolerance criterion for the consequence severity category, even though the EEs and CMs do not apply in these cases.

Table 1: Probability of Ignition (given a release of flammable material) for LOPA Consequence Severity Categories Based on Human Harm or Property Damage

Situation	**Probability of Ignition, *Pi***	**Comments**
Consequence includes breaking of equipment due to high pressure, high temperature, crevice corrosion, or metal fatigue	1	Assumes electrical equipment associated with pressurized equipment will break, thereby providing an ignition source
Consequence includes breaking of equipment due to steady-state corrosion or erosion, or else overflow with no breakage, with release of flammable only within a C1D1 area	0.01	If release can flow outside of the C1D1, such as if a dike fails, then this value is changed to 1, and the dike is included with a PFD of 0.01, if the other criteria of dike IPL are met
Consequence includes breaking of equipment due to steady-state corrosion or erosion, or else overflow with no breakage, with release of flammable only within a C1D2 area	0.1	If release can flow outside of the C1D2, such as if a dike fails, then this value is changed to 1, and the dike is included with a PFD of 0.01, if the other criteria of dike IPL are met
Consequence includes overflow of **flammable** within 50 ft of road or access alley that is commonly used	1	
Consequence includes overflow of **combustible** liquid, below boiling point within 50 ft of road or access alley that is commonly used	0.01	

Situation	Probability of Ignition, *Pi*	Comments
If the site does not have excellent control of changes to maintaining or defeating an ignition classification	1	
For LOPA, dikes are not counted as an IPL if the release is above the boiling point of the flammable liquid.	1	

Probability of ignition estimates lower than 1.0 have proven wrong for some catastrophic scenarios. "Ignition sources are free, supplied by nature," paraphrased from Trevor Kletz. For example, no flammables were present when the hot work permit was issued for welding, but operating conditions changed, releasing flammable material to the location of welding sparks.

Table 2: Probability of Person Present (given a fire or a release of toxic material) for LOPA Consequence Severity Categories Based on Human Harm or Property Damage

Situation	Probability of Person Present, *Pp*	Comments
If human error is the cause of the initiating event	1	
If operator response to BPCS or SIF alarms is to go to the area of the scenario.	1	
Scenario occurs while workers are known to be nearby, such as during a step-by-step (such as batch, unloading, startup tasks)	1	
Initiating event is a random, unannounced event such as due to corrosion or erosion or metal fatigue; use one of cases below:		Calculated from average time in the area of ALL workers (operations and maintenance)
• Structure/area normally occupied	1	
• Structure/area occasionally occupied (less than 8 hr./day)	0.5	
• Remote facility or exclusion area (less than 1 hr./day)	0.1	
• If the site does not have excellent control of changes affecting normal *Pp*, or if the fraction of time in area is > 0.3 then use a factor of 1	1	

Pp estimates lower than 1 have normally proven wrong for actual catastrophic scenarios. In many cases, the initiating event is one or more people who are present in the danger zone. In at least one incident, personnel present at shift change troubleshooting a problem included two shifts for each of the following disciplines: operator, mechanic, operating foreman, maintenance foreman, engineer – yet a typical LOPA would not likely estimate that many people present.

Table 3: Probability of Fatality (given persons present in a fire or a release of toxic material) for LOPA Consequence Severity Categories Based on Human Harm or Property Damage

Situation	Probability of Person Fatality, *Pf*	Comments
For **fire or toxic release** and person is **in protected area**, given *Pp* and *Pi* and Consequence Severity (S) and IEF are independently estimated from *Pf*	0.1	Protected area must be specifically designed to protect against the scenario.
For **fire or toxic** release and person is **outside of protected area**, given *Pp* and *Pi* and Consequence Severity (S) and IEF are independently estimated from *Pf*	0.5	*Pf* for flash fire is usually 1.0; for jet fire or pool fire, escape may be possible, hence 0.5.
For **explosion** and person is **in protected area**, given *Pp* and *Pi* and Consequence Severity (S) and IEF are independently estimated from *Pf*	0.1	Protected area must be specifically designed to protect against the scenario.
For **explosion** and person is **outside of protected area**, given *Pp* and *Pi* and Consequence Severity (S) and IEF are independently estimated from *Pf*	1	

Pf estimates lower than 1 have proven wrong for some catastrophic scenarios. Some organizations do not use *Pf* as it is believed that this probability is sometimes a matter of chance and they do not want the calculated risk to be reduced.

Bottom line: Do not use CMs for LOPA scenarios where the consequence severities are based on the release quantity and the release conditions; the conditional modifiers have already been included in the consequence severities. Where conditional modifiers are included in the organization's LOPA follow the guidance; do not choose more optimistic conditional modifiers. In addition, do not CMs if there are no management of change controls in place for the CM or if the CM cannot be validated. These last two points apply to essentially all EEs and CMs, so it is best to simply not use EEs and CMs in LOPA risk estimates!

3.2 Misuse of Enabling Events

Enabling events are needed to account for two independent events that have to occur at the same time to initiate the scenario. Otherwise, the calculated mitigated consequence frequency would be too high, over-estimating the risk.

For example, an initiating cause is loss of power to the heat tracing on the water pipe. The consequence of interest is a frozen pipe with potential property damage. Assume the power loss occurs once per year. The pipe will not freeze unless the ambient temperature is below the freezing point of the contents [for water, less than 0°C (32°F)] for an extended time. The enabling event is the fraction of the year with freezing temperatures. For Houston, TX, the enabling event could be estimated conservatively at 7 days/yr, or 1 week/52 weeks = 0.02, a probability. The LOPA mitigated consequence frequency would be IEF 1/yr * EE 0.02 = 0.02/yr, two orders of magnitude less that the IEF.

An error frequently made is to overlook a lack of independency between the IE and the EE. If the IE and the EE are associated with the same cause or with each other, then the IEF should be used and an EE should not be used. Otherwise, the risk will be underestimated. (Note that some power failures are caused by the freezing weather, so they are not independent. Now, the mitigated consequence frequency is 1/yr with the power failure AND freezing weather at the same time.)

Another frequent error is to fail to convert the frequency for the EE to a probability. Note that probabilities are dimensionless and have a value between zero and one. There can be only one frequency in a LOPA scenario; using two frequencies would give a consequence frequency with units of reciprocal time squared, such as per year^2, which is an acceleration – not applicable to LOPA. The calculation should have the form of

$$IEF, per\ year * EE, probability = \ Consequence\ Frequency, per\ year$$

<u>**Bottom line:**</u> Do not use EEs as these are almost always used incorrectly!

3.3 Misuse of Time at Risk

A very dangerous misuse of enabling events can be "time-at-risk". For example, in an eight-hour batch reaction, loss of cooling can cause a runaway reaction only during a critical two-hour period. LOPA analysts can be tempted to calculate a time-at-risk enabling condition by the following equation:

$$Dangerous\ Enabling\ Condition\ Probability = \frac{\#\ of Batches}{year} * \frac{2\ hr\ time\ at\ risk}{8760\ hr/year}\quad \textbf{DO NOT USE}$$

An implicit assumption in this equation is that all the failures that can cause loss of cooling occur only during the critical two-hour time period when the runaway reaction can occur on loss of cooling. In reality, for a typical cooling water supply system, the causes of loss of cooling can be viewed as loss of water flow or high temperature of the cooling water, as shown in Table 4.

Table 4: Typical Causes of Loss of Cooling

Loss of Cooling Water Flow	High Temperature of Cooling Water
Cooling water pump tripped	Cooling tower fan tripped
Water flow control loop failed to low flow	High thermal load on cooling tower
Manual block valve closed or throttled	High ambient temperature (above design)
Line plugged	
Low level in cooling tower (level control loop failed to low level, loss of water makeup supply)	

Equipment failures that lead to loss of cooling can occur randomly during the time-at-risk interval, or during the time-**not**-at-risk phase. If the operators do not know the status of the cooling water before they enter the critical time-at-risk phase, they will find out when the runaway reaction occurs! Using time-at-risk without knowledge of the status of the enabling condition system can drastically underestimate the actual risk and give a false sense of confidence.

In order to use time-at-risk, it is essential to confirm that the cooling water system is operating correctly and has not failed before starting the critical time-at-risk phase. Some facilities have a cooling water supply pressure indicator with low alarm and a cooling water supply temperature indicator with high alarm to alert the operators to potential failures of the cooling water. Operator response to alarm procedures should be available and should include prohibitions against starting the critical time-at-risk phase of the reaction.

For high risk (high severity consequence) reactions, some facilities run a dummy batch that tests the critical control loops and utilities to ensure that everything is working correctly before running the actual production batch. It is appropriate to use time-at-risk in this situation.

Bottom line: Do not use “time-at risk” probabilities (a special case of EE) as these are almost always used incorrectly!

4 High Demand Not Recognized

If the demand on the first IPL is more than twice the frequency of the test frequency of that IPL, the IPL is in high demand mode. If the typical LOPA calculation is done, the calculated mitigated consequence frequency will be higher than actual, potentially leading to extra expenditure for additional risk reduction. For example, suppose the PFD for the first IPL is 0.01, the test interval for the first IPL is annual, and the demand on the first IPL is 10 times per year. The LOPA calculation would give IEF 10/year * 0.01 PFD = 0.1/yr mitigated consequence frequency.

The correct calculation for high demand mode is to ignore the IEF and to use the failure rate of the first IPL has the initiating cause frequency for the scenario. Estimate the failure rate of the IPL by solving PFD = λ*T/2, that is, λ = 2 *PFD/T. For the example, λ = 2*0.01/1year = 0.02/year, almost an order of magnitude lower than the typical calculation.

It is important to recognize when an IPL is in high demand and to calculate the frequency of the scenario correctly.

5 Not Treating Initiating Events as Critical Features

Some LOPA users do not count IEs as critical features while putting strong value on IPLs as critical features. This approach can lead to higher risk of an accident as the site may not be controlling the IE frequency (IEF) well enough. When we consider the factors in a LOPA calculation, the initiating event frequency is the starting point for the scenario. Each IPL reduces the mitigated consequence frequency by a factor of typically 10 or 100. A very effective way to reduce the risk of a scenario is to manage the equipment or human actions of the initiating cause to maintain the IEF (or perhaps to reduce the IEF). For example, inspections and periodic calibration of control loops can reduce the frequency of loop failure as an initiating event for a scenario, and these can maintain the IEF used by the LOPA team. Likewise, strong procedures, training, and checklists, refresher training, and drills can reduce the frequency of a human error as an initiating event.

It would make sense to balance the resource allocation between the initiating events and the IPLs for a scenario. IEs are just as important as IPLs for controlling the risk, other than there are more IPLs for a typical scenario while there is only one IE.

6 Over-confidence in the Calculation Results

Many companies believe that risk calculations using LOPA or QRA methods are accurate. But the factors (PFDs, IEFs, etc.) are not accurately known for a site. Any specific factor used in such risk calculations usually has a range of ***plus and minus an order of magnitude (a factor of 10)***. So, confidence in the resulting calculated values cannot be better than the factor with the largest range used in the calculation. Further, as the risk being calculated gets smaller and smaller, the result leaves the known world of reliability, because there are not enough "scenario-years" to validate that the results are reasonable.

Poor understanding of the SIGNIFICANT FIGURES:

How accurate is the risk calculation using LOPA? What is the uncertainty range for the answer? To help understand the problem, consider a range of data for PFD for a type of process component:

0.1 to 0.001 with a mean of 0.008

Without adjustment of the significant digit to account for the error range around the mean, what is the significant digit rule in this case so as not to overstate the precision? Some believe it is 1 significant digit (so 0.008, +/- 0.001). But, instead, for such a broad range, the best way to state the significance is the closest factor of 10 (order-of-magnitude). So, the mean should instead be expressed as 10^{-2} and not 8 x 10^{-3}. Further, so as not to be misleading, the error factor should be included with the mean. So, the PFD above should be shown as $10^{-2\pm1}$.

> ***Rationale for this expression:*** *Let's start with a tighter range of the data, indicated by a mean of 0.0081 ± 0.0002. In this case, the number of significant digits is 2. Now, suppose the data instead indicates a mean of 0.0081 ± 0.0022, then the number of significant digits is 1 and the expression is better written 0.008 ± 0.002. But as the range of data becomes broader, the nomenclature above becomes useless; for instance, if the range is 0.01 to 0.001, and the average (mean) is 0.008, then how do you express this? 0.008 +.002/-.007? This is clumsy. If you tried to express as a midpoint (median), then it makes sense for an expression such as: 0.0055 ± .0045, but then we lose the previous mean (0.008) in this expression. In this case, it seems we have No significant digit, but rather have a significant order of magnitude, which may be best expressed (if rounded up) as* $10^{-2\pm0.5}$. *Then what if the range is broader; say: 0.01 to 0.0001 with a mean and median of 0.001. How is that expressed? 0.001 ± a multiplication factor of*

> *10? So, again here only the single digit of the exponent is significant in the expression of the data: $10^{-3\pm1}$*

This is especially important since we multiply such numbers together and use the product of the multiplication in LOPA and QRA.

Take the following typical example from a LOPA scenario

$$P = (0.5\pm.5) \text{ x } (10^{-2\pm0.5}) \text{ x } (10^{-1\pm0.5}) \text{ x } (10^{-3\pm1}) = 0.5 \text{ x } 10^{-6\pm x}$$

The normal rounding convention would normally also be applicable, which is applied at the end; and, since the largest uncertainty is $x = 1$, then the best expression of the final product above is:

$$P = 10^{-6\pm1}$$

…since we cannot know the product any more accurately than the largest uncertainty in the probability calculation.

By the way, the result above is ONLY true if the high and low ends of the probability distribution of each factor in the LOPA equation (IEF* PFD* PFD* etc.) perfectly offset (cancel) each other. But this is not a good assumption, since for this offset to happen would require perfect independence of all factors. But the factors will likely drift in the same direction, since the failure rates of all IEs and IPLs are ultimately dependent on the same underlying management systems that control the component reliability and the human reliability.

Further, the following expression would be wrong (misleading): $1 \text{ x } 10^{-6}$ because that would imply there is a 1 significant digit, which is not correct (there is only 1 significant order of magnitude), since we cannot know the product any more accurate than the greatest uncertainty range of any of the factors in the equation (as stated earlier).

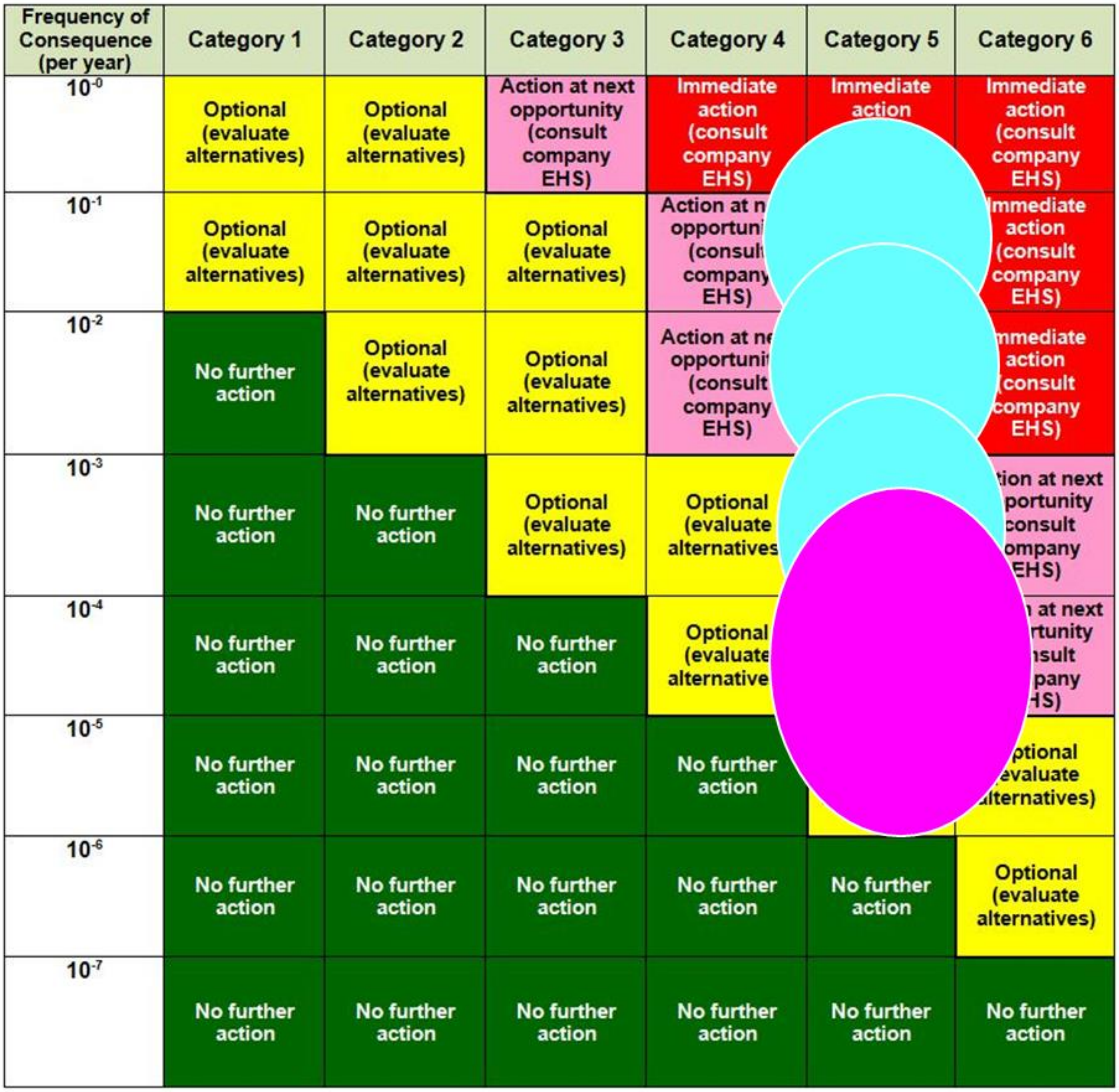
On the other hand, if the organization requires the use of conditional modifiers (such as, probability of ignition, probability of a person in the effect zone, probability of fatality), the calculations should be made in the format of $X.Y \text{ x } 10^{-Z}$, and the round off to the significant exponent should be made at the end of the calculation. This approach avoids the accumulation of inappropriate round off errors.

We need to remember that the lookup values for IEFs and PFDs are typically plus or minus an order of magnitude uncertainty. Likewise, the lookup values that were established for risk tolerance criteria are subject to the same order of magnitude uncertainty because most organizations established the risk tolerance criteria by doing LOPA or a similar quantitative or semi-quantitative analysis for scenarios that were protected by adequate IPLs based on expert judgment.

> ***EXAMPLE: Forgetting the Past (make a comparison to calculations performed for nuclear power plant licensing)***
>
> Another factor to consider in the uncertainly of the calculated risk, is “How many times has this scenario occurred and what does that the actual industry data show for that scenario?” Another way to state this is: “How many scenario-years do you have for comparison of the calculated value?” This is very difficult for a multifaceted industry such as the chemical-based industries to know.
>
> But we do have an interesting case study in the Probabilistic Risk Assessments (QRAs using FTA and ETA and HRA). To receive a license to build a commercial nuclear power station in the USA (and many other countries with nuclear power), it was required that the licensee prove that the residual risk for a core meltdown was 10^{-6} per year per reactor. So, just like we are doing thousands of LOPA today, the nuclear power industry did hundreds of QRA models and each result remarkably showed that that residual risk of a meltdown due to the summation of all scenarios was indeed 10^{-6} per year per reactor. (This includes the probability of natural phenomena such as earthquakes, floods, and tsunamis causing a scenario that leads to a meltdown.)
>
> There are about 437 commercial nuclear power units operating around the world (about 100 of these are in the USA). Though some power stations have been operating 40 years, the average operating years is about 21 years. This means that there are now about 9000 reactor-years of experience. From the original calculations, we would not expect a core meltdown in two thousand years of operation. How many meltdowns have occurred around the world (in the population of 440 reactors) in commercial power plants? In fact, there have been 8 (eight) meltdowns that reached the consequence of loss of the unit (about $1 billion USD to build each unit), but only 5 of these are published (the other three occurred in countries that do not allow open press reporting) and there have been many thousands of fatalities (though 99% of the fatalities are attributed to just Chernobyl). So, if we recalculate the probability of a meltdown, we find the actual average is: 8/9000 = about 10^{-3} or 5/9000 = about 6 x 10^{-4}, depending on the number of meltdowns you choose to use. Regardless, the result is 1000 times higher than predicted (actual is 10^{-3} per year instead of the predicted value of 10^{-6} per year).

Do we understand the reliability factors for chemical plants better than the nuclear power understand theirs? Do we understand the risk calculations better than they did? Are our management systems (that control the failure rates and error rates) better than theirs? We have not proven that the answer to any of these three questions is *Yes*.

From our experience, the uncertainty in probabilistic risk calculations tend to Increase as the residual risk decreases (as the probability gets smaller). Figure 3 (on the next page) illustrates how the uncertainty of the risk value likely increases as the calculated risk drops lower and lower to the 10^{-6} per year range. Note that each oval is an illustration of the plus/minus 2 sigma uncertainty of both the consequence value and the frequency value and any step in a quantitative risk assessment for a specific scenario, including risk assessments using LOPA. This is the more proper presentation of the results, especially since a risk matrix is a log-log (base 10) plot of risk assessment results. There is no need to illustrate any finer gradation than the approximate order of magnitude, since the data estimates with uncertainty included only supports an expression of : P = $10^{-X\pm1}$



Frequency of Consequence (per year)	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6
10^{-0}	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at next opportunity (consult company EHS)	Immediate action (consult company EHS)	Immediate action	Immediate action (consult company EHS)
10^{-1}	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at n opportuni (consul company EHS)		Immediate action (consult company EHS)
10^{-2}	No further action	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Action at ne opportuni (consult company EHS)		mmediate action (consult company EHS)
10^{-3}	No further action	No further action	Optional (evaluate alternatives)	Optional (evaluate alternatives		tion at next portunity consult ompany EHS)
10^{-4}	No further action	No further action	No further action	Optional (evaluate alternative		at next rtunity nsult pany HS)
10^{-5}	No further action	No further action	No further action	No further action		ptional evaluate lternatives)
10^{-6}	No further action	No further action	No further action	No further action	No further action	Optional (evaluate alternatives)
10^{-7}	No further action	No further action	No further action	No further action	No further action	No further action

Figure 3: Residual Calculated Risk, showing growing uncertainty in the results (risk) as the risk drops lower ***(courtesy of Process Improvement Institute, Inc.)***

We cannot prove how much the uncertainty grows, but if risk analysts were off by 3 orders of magnitude in the past in the 10^{-6} range of probability per year; it is likely that the chemical industry is off by 2 orders of magnitude in the range of 10^{-4} per year. Hence, we believe that P = $10^{-X\pm1}$ is appropriate representation of the results of each estimate and each calculation result for quantitative risk assessments, including LOPA. Further, since the data has so much uncertainty and since our overall industry has still limited experience with accident scenario risk prediction, we believe a risk calculation of less than 10^{-4} per year is meaningless and not supportable, as it is very likely that common-cause errors of the common humans in operations and maintenance departments will outweigh all other risk factors in the range of 10^{-4} per year and less, as shown in the study of the risk estimates in the nuclear power industry, mentioned above.

7 Conclusion

The introduction of the streamlined semi-quantitative risk assessment method, LOPA, has had a tremendous impact on the chemical and related industries. 99% of the quantitative risk assessments that may be necessary can now be performed in 1/10th the time of a QRA (quantitative risk assessment). Many benefits have been reaped, including a continual improvement on the identification and control of critical features and actions (IEs and IPLs). However, the initial rollout of LOPA has led to a few problems, including repetition of over-reliance on theoretical calculations, overly aggressive risk tolerance criteria which encourages misuse of EEs and CMs, and of course failure to maintain IEs and IPLs properly. The problems are easily remedied by:

- Increased (renewed) focus on the qualitative analyses (PHAs/HAZOPs)
- Judicious use of LOPA
- Carefully adhering to the rules of LOPA, especially validation of the maintenance of the IPLs and IEs at each site
- Avoiding use of EEs and CMs
- More focus on maintaining the failure rates of IEs and IPLs
- Not believing the numbers but believing the comparison of alternative risk reduction alternatives

The originators of LOPA hope you will use this paper as an expansion on the concepts in the first LOPA textbook, and as an addendum to all three textbooks [7, 8, 9] on the topic.

8 Acronyms Used

AIChE – American Institute of Chemical Engineers
BPCS – Basic process control system
CCPS – Center for Chemical Process Safety (of AIChE)
CM – Conditional Modifier
CSO – Car Sealed Open
EE – Enabling Event
EPA – Environmental Protection Agency (USA)
ETA – Event Tree Analysis
FTA – Fault Tree Analysis
HAZOP – Hazard and Operability Analysis – a hazard identification tool
HRA – Human Reliability Analysis
IE – Initiating Event
IEC – International Electrotechnical Commission

IEF - Initiating Event Frequency
IPL – Independent Protection Layer
ISA – International Society of Automation
ITPM – Inspection, Testing, and Preventive Maintenance
LOPA – Layer of Protection Analysis
MAWP – Maximum Allowable Working Pressure
MOC – Management of Change
P&ID – Piping & Instrumentation Diagram
PFD – Probability of failure on demand
PHA – Process Hazard Analysis
PM – Preventive Maintenance
PSI – Process Safety Information
PSM – Process Safety Management
PSV – Pressure Safety Valve
QRA – Quantitative Risk Assessment
SIF – Safety Instrumented Function
SIL – Safety Integrity Level
SIS – Safety Instrumented System
T – Test interval, years
λ – Failure rate, per yr

9 References

1. William G. Bridges 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, 1997

2. A. M. Dowell, III, "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, 1997

3. Rodger M. Ewbank and Gary S. York, "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, 1997

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. CCPS, *Layer of Protection Analysis, Simplified Process Risk Assessment,* American Institute of Chemical Engineers, New York, New York, 2001.

8. CCPS, *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis,* American Institute of Chemical Engineers, New York, New York, 2015.

9. CCPS, *Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis,* American Institute of Chemical Engineers, New York, New York, 2014.

10. W. G. Bridges and A. M Dowell, III, "Key Issues with Implementing LOPA – Perspective from the Originators of LOPA", *11th Global Congress on Process Safety*, Austin, TX, American Institute of Chemical Engineers, April 2015.

11. A. M. Dowell, III, "Understanding IPL Boundaries", *Process Safety Progress*, June 2019, **Vol. 38**, No. 2, pp 126–131, 2019

12. W. G. Bridges and H. Thomas, "Accounting for Human Error Probability in SIL Verification Calculations,", *8th Global Congress on Process Safety,* Houston, American Institute of Chemical Engineers, April 2012.

13. A.M. (Art) Dowell, III, W. Bridges, M. Massello, and H.W. (Hal) Thomas, "SIL-3, SIL-2, and Unicorns (There Is a High Probability Your SIL 2 and SIL 3 SIFs Have No Better Performance Than SIL 1)", *15th Global Congress on Process Safety*, New Orleans, LA, American Institute of Chemical Engineers, March 31-April 3, 2019

14. IEC 61511-1:2016+AMD1:2017 CSV, Consolidated version: Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements, International Electrotechnical Commission (IEC), 2010, Geneva, Switzerland, 2017.

15. ANSI/ISA-61511-1-2018 / IEC 61511-1:2016+AMD1:2017 CSV, Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, definitions, system, hardware and application programming requirements (IEC 61511-1:2016+AMD1:2017 CSV, IDT), International Society of Automation, Research Triangle Park, North Carolina.

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

17. W. Bridges, "Gains from Getting Near Misses Reported," *8th Global Congress on Process Safety,* Houston, American Institute of Chemical Engineers, April 2012.

18. W. G. Bridges and T. Clark, "LOPA and Human Reliability – Human Errors and Human IPLs (Updated)," *7th Global Congress on Process Safety,* Chicago, American Institute of Chemical Engineers, March 2011.

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

20. W. G. Bridges and T. Clark, "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, American Institute of Chemical Engineers.

21. J. Champion, "Using LOPA to Verify the Design of a Burner Management System", American Institute of Chemical Engineers, *40th Annual Loss Prevention Symposium*, Orlando, Florida, April, 2006

22. ISA TR84.00.02, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques*, International Society of Automation, Research Triangle Park, North Carolina, 2002.

23. ISA-TR84.00.02-2015, Safety Integrity Level Verification of Safety Instrumented Functions, International Society of Automation, Research Triangle Park, North Carolina, 2015.

24. A. M. Dowell, III, and Tom R. Williams, "Layer of Protection Analysis: Generating Scenarios Automatically from HAZOP Data", *Process Safety Progress*, **Vol. 24, No. 1**, pp 38-44, 2005

25. W. G. Bridges and A. M. Dowell, III, "Identify SIF and Specify Necessary SIL, and other IPLs, as part of PHA/HAZOP" *12th Global Congress on Process Safety*, Houston, AIChE, April 2016.