More Issues with LOPA - from the Originators

A. M. (Art) Dowell, III, PE
Process Improvement Institute, Inc. (PII)
2437 Bay Area Blvd PMB 260
Houston TX 77058-1519
phone: 713-865-6135
e-mail: adowell@piii.com

William G. Bridges, President
Process Improvement Institute, Inc. (PII)
1321 Waterside Lane
Knoxville, TN 37922
Phone: (865) 675-3458
Fax: (865) 622-6800
e-mail: wbridges@piii.com

Prepared for Presentation at
11th Global Congress on Process Safety
Austin, TX
April 27, 2015

UNPUBLISHED

More Issues with LOPA - from the Originators

A. M. (Art) Dowell, III, PE
Process Improvement Institute, Inc. (PII)

William G. Bridges, President
Process Improvement Institute, Inc. (PII)

Keywords: process safety culture, process safety management, near miss reporting, human factors, leadership, accountability, China

Abstract

Layer of protection analysis (LOPA) has now been around for more 20 years (and in general use for 15 years), with the initial textbook being officially published in 2001. Most recently, two companion books have been published on the topics of Enabling Events & Conditional Modifiers and on Initiating Events and Independent Protection Layers (IPLs). 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.

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. These issues were summarized in the CCPS workshop on the application of ISA S84, held in 2000.

The first LOPA book was developed by a CCPS committee from 1997 through 2000 and was published in 2001[7] (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 15 years ago. Especially during the last 10-years, use of LOPA has greatly accelerated. It is likely that several million LOPAs have been performed. During this same period, many abuses of LOPA have been noted (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. The new book has been discussed in other papers at past conferences; 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***.

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 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. 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.

Relationship to SIL determination

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

For the most part today, LOPA is seen as one tool (in many parts of the world, the preferred tool) for determining if a SIF is necessary and if it is the correct choice for risk reduction; and LOPA is the preferred method for determining what SIL is necessary, if an SIF is chosen as the risk reduction method.

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.

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 (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:

    - **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.

If the IPL is a PSV, then the IPL system must include upstream and downstream features, such as isolation valves (Figure 1). Therefore, the probability of leaving an isolation valve closed should be included as a contribution to the overall PFD of the PSV IPL system.

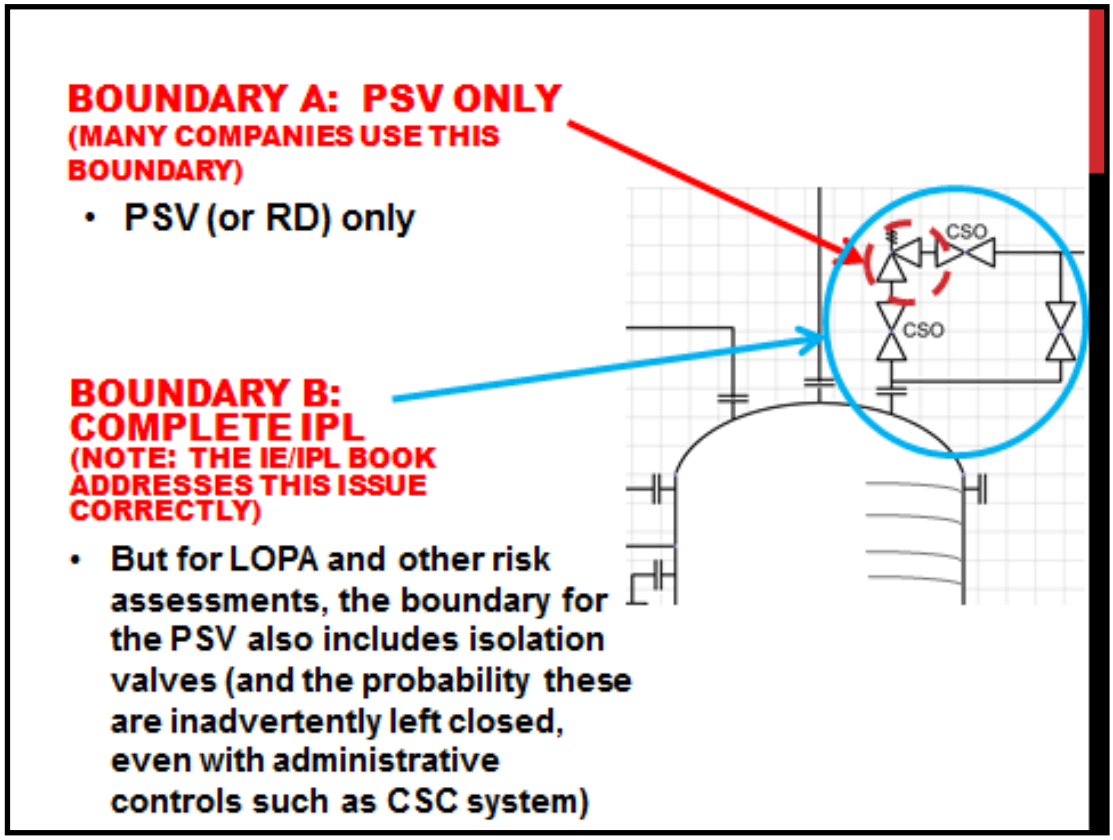

Figure 1: Boundary for PSV *(courtesy of Process Improvement Institute, Inc.)*

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 valves are open and interlocking the position switches to a permissive that must be cleared before startup

A similar situation relates to 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 (see Figure 2). As illustrated below, 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).

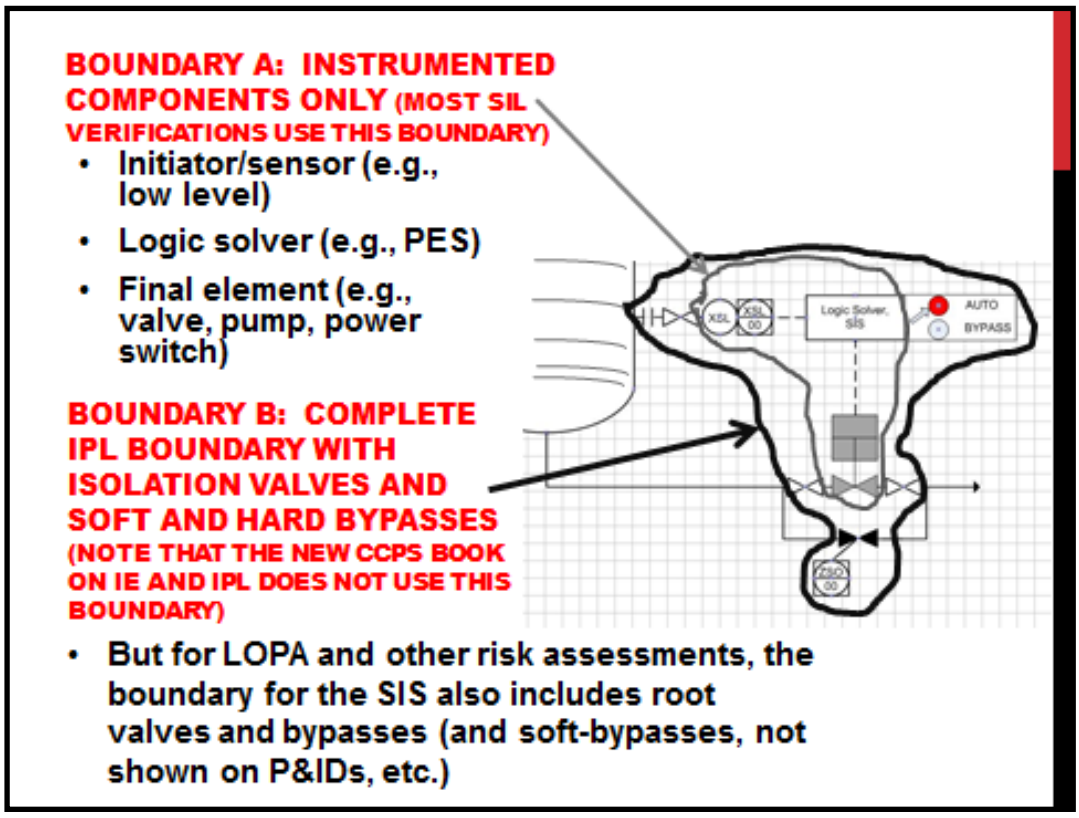

Figure 2: Boundary for SIF ***(courtesy of Process Improvement Institute, Inc.)***

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 paper[10] by Bridges (PII) and Thomas (exida) for more detailed explanation and examples.

- **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[7] (CCPS, 2001). 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 new 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 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. The new CCPS book, *Guidelines for Initiating Events and Independent Protection Layers,* 2015[8], addresses this issue well.

- **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 15+ years of LOPA implementation and is one of the problems we hope to fix with the new CCPS book *Guidelines for Initiating Events and Independent Protection Layers,* 2015. 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 is identified) and also have these same staff provide the maintenance practices, test practices, and operator drill routines for use within an organization. The new CCPS book, *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 also has been a huge problem in the past 13 years of LOPA implementation and is one of the problems we hope to fix with the new CCPS book *Guidelines for Initiating Events and Independent Protection Layers,* 2015. 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[11], and 2012[12]). 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.

  The new CCPS book, *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[13] 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 new CCPS book 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[14]), 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. **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 eventually be used "after" a PHA team meeting, since that is how the originators were using it.

   Various examples of overuse are discussed below *(Bridges, 2009[15], 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). 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 LOPA analyst or team of risk judgments 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 have 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).[16]

PII has observed that most companies tend to go through phases of use of LOPA. Figure 3 on the next page illustrates these phases. 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.

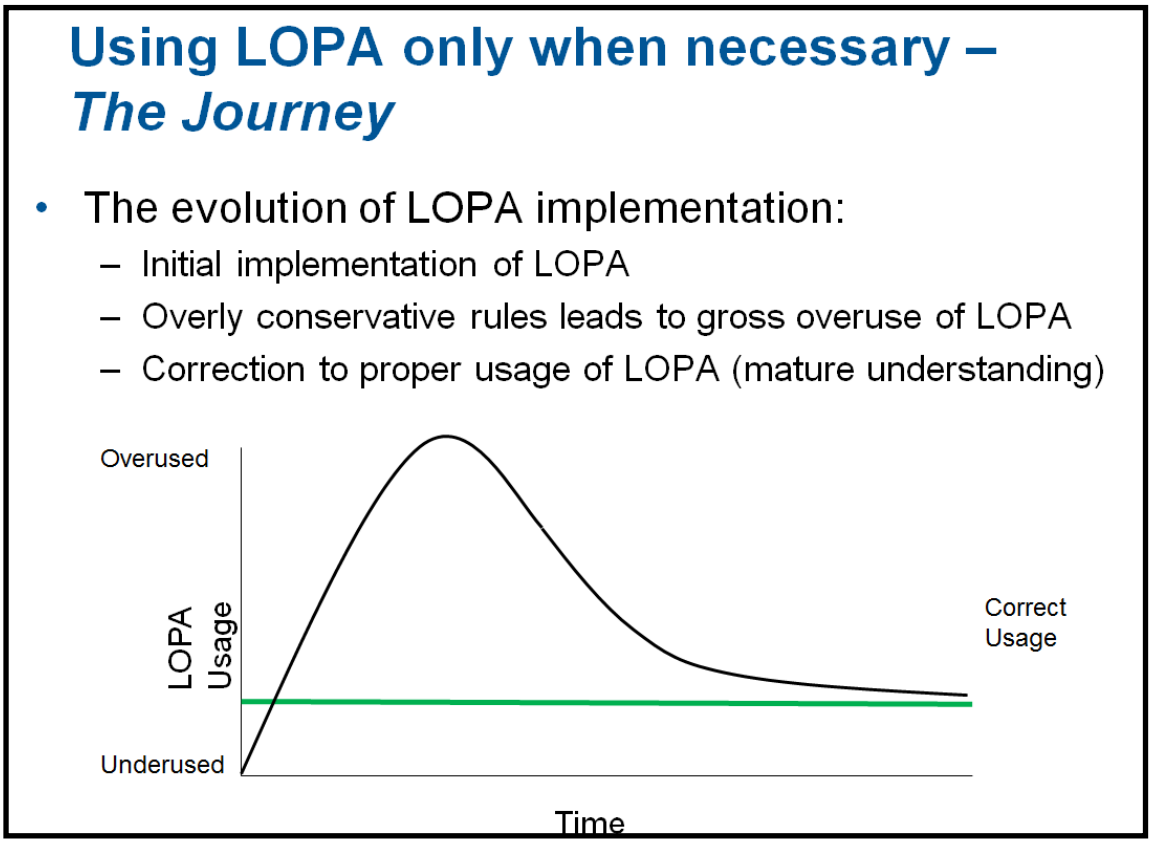

Figure 3: Typical Usage Rate for LOPA as application of LOPA matures within a company *(courtesy of Process Improvement Institute, Inc.)*

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 4 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):

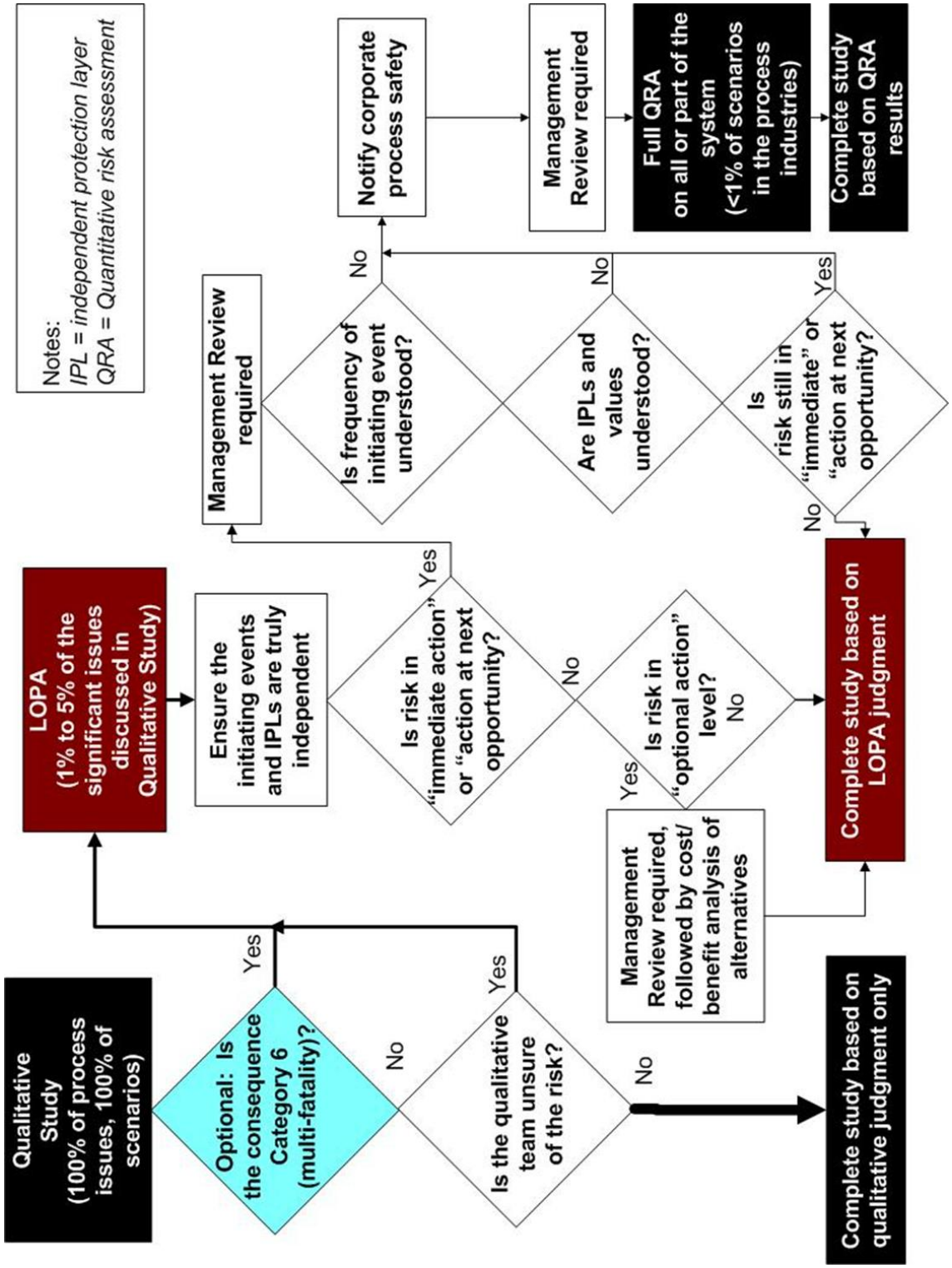

Figure 4: When to Use LOPA (*Courtesy of Process Improvement Institute, Inc.*)

3. **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, and related TR from ANSI/ISA to make these same determinations. Per ISA TR 84.00.02, 2002 (and 2004), Section 3.8:[17]

   > *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).

4. **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).

5. 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 *HazardReview LEADER*^{TM} 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. PII uses Excel templates for documenting LOPA.

6. Over-confidence in Conditional Modifiers (CMs) and Enabling Events (EEs)

CMs are applied to analyses when the risk criteria are based on ultimate consequences, often fatalities. Stated differently, the use of CMs would only be warranted when the severity part of the LOPA risk evaluation is based on the assessed possible impact (injuries/fatalities, property damage, environmental damage, etc.) of a loss event rather than just the occurrence of a loss event (hazardous material release, vessel rupture explosion, etc.), and this is consistent with the risk criteria established for performing the LOPA. The capabilities of the LOPA analyst(s), the established company or facility LOPA methodology, and the availability of relevant data would all need to support the use of CMs.

If a consequence categorization method is used for consequence estimation, the use of CMs is precluded, since such probabilities (the probability of people being present or the probability of ignition, and therefore the probability of harm due to these factors) are

inherently included in the estimation of the consequence already, so use of the CMs would be counting the same probability twice.

> ***MYTH:*** *Since Conditional Modifiers use numbers to express a more discrete breakout of factors, the results express the risk of the scenario more precisely.*
>
> ***REALITY:*** *This is NOT true. The precision of a LOPA estimate is typically within plus or minus an order or magnitude. Including the likelihood of presence or ignition inherently in the consequence severity is not less precise than using separate factors.*

Similarly, EEs do not apply if the IE of the scenario is a human error, yet many companies have not learned this simple rule.

Many organizations, including PII, prefer not to use CMs or EEs in LOPAs for various reasons. The approach of NOT using CMs and EEs was presented in LOPA (2001)[7] and that approach is widely used in the industry. Some drawbacks when using CMs and EEs include:

- The significant uncertainties in using CMs (an order of magnitude or more on either side of a point estimate) disqualify use of such factors. LOPA and other risk assessments can only produce an estimate of risk that is valid to an order-of-magnitude. Since the estimates for CMs are only predictions based on correlations, and since the assumptions in the correlations cannot be managed at a site in many cases, the actual factors may average close to 1.0.

- CMs and EEs cannot be validated (other than by the prediction method) for a specific site, since they cannot be tested or audited at the site (as compared with IEs and IPLs, for example). In fact, we are not aware of any facility that has the resources, capabilities, or management commitment to properly document the use of CMs and EEs and verify their ongoing validity by testing and auditing.

- Significant assumptions about "probability of presence" given a problem in the Unit that will draw staff into the vulnerability zone.

- How do you manage changes to EEs or CMs? What is the trigger for a Management of Change (request for change) for an EE or CM?

- The LOPA analyst(s) have insufficient knowledge of CMs or EEs to employ them correctly. There have been many instances where use of CMs or EEs have led to severe underestimate of the risk; this is one key reasons some companies do not allow use of these factors in LOPA.

- The company's or facility's established LOPA procedure is to not use any factor (including CMs or EEs) unless they provide a full order-of-magnitude effect on the risk calculation; many CMs or EEs are a probability of 0.5, and so do not reduce the risk by an order of magnitude.

- Unjustified complexity of a simplified risk assessment approach. It is much simpler to inherently estimate the order-of-magnitude consequence severity rather than complicate the estimation process with CMs or EEs.

- Legal/liability considerations. Can you defend the CMs or EEs in court?

The *Guidelines for CMs and EEs*[9], provide guidance on the appropriate use of such factors in LOPA and other risk evaluations. However, the general slant of the new book is encouragement of the use of CMs and EEs, which is a dangerous direction, in the opinion of the originators of LOPA.

7. 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 average, 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 8×10^{-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

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

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): 1×10^{-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 $X.Y \times 10^{-Z}$, 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.

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) 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 6×10^{-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 5 (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.

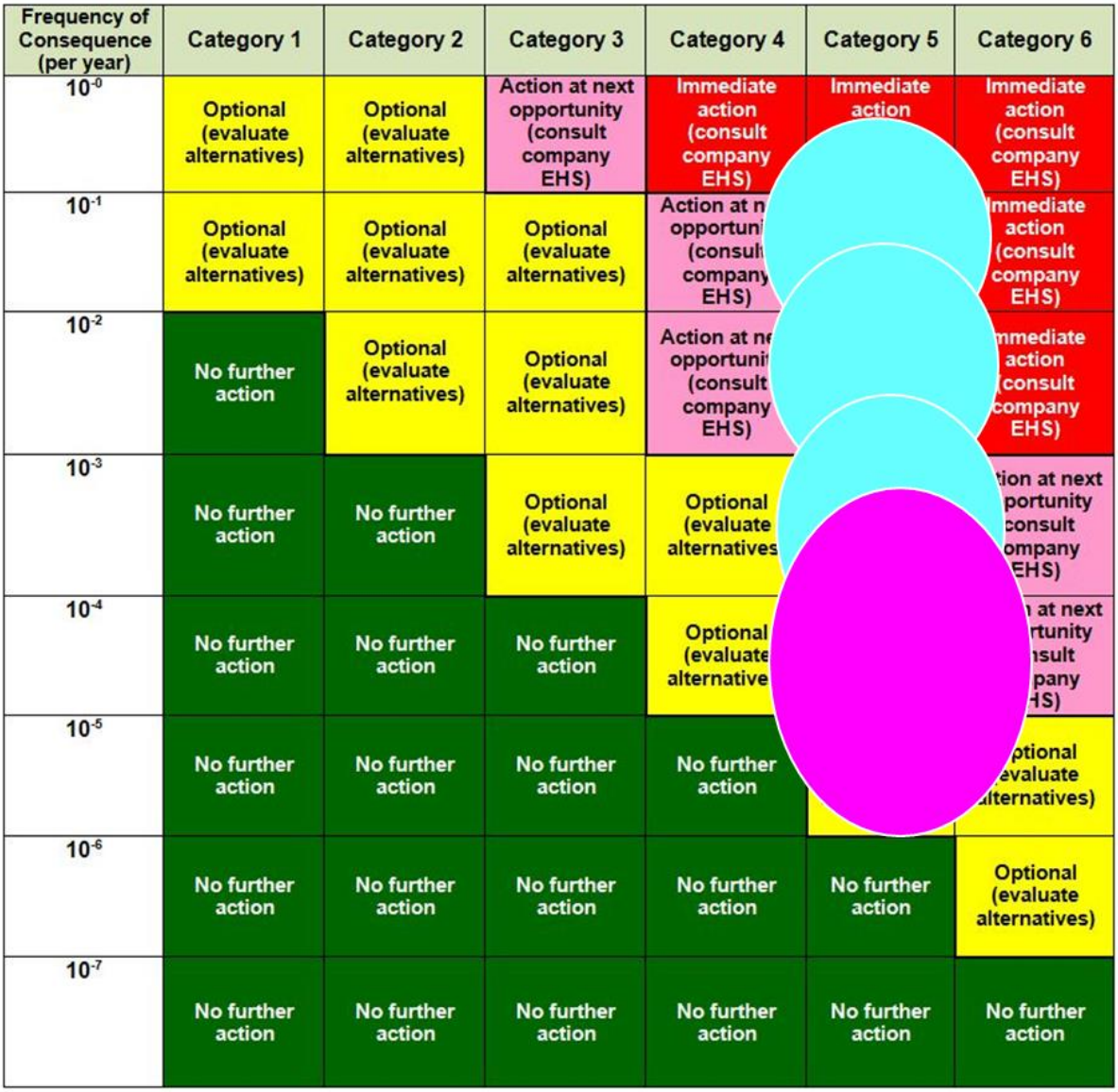

Figure 5: Residual Calculated Risk, showing growing uncertainty in the results (risk) as the risk drops lower *(courtesy of Process Improvement Institute, Inc.)*

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.

Conclusion

The introduction of the streamlined semi-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 (quantitative risk assessment). 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, including repetition of over-reliance on theoretical calculations, as discussed in this paper. The problems are easily remedied by

- Increase (renewed) focused 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
- Not believing the numbers but believing the comparison of alternative risk reduction alternatives

Acronyms Used

AIChE – American Institute of Chemical Engineers
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 - Inititating Event Frequency
IPL – Independent Protection Layer
ITPM – Inspection, Testing, and Preventive Maintenance
LOPA – Layer of Protection Analysis
MAWP – Maximum Allowable Working Pressure
MOC – Management of Change
PFD – Probability of failure on demand
PHA – Process Hazard Analysis
PM – Preventive Maintenance
P&ID – Piping & Instrumentation Diagram
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

References

1. Bridges, William G., and Tom R. Williams (1997), "Risk Acceptance Criteria and Risk Judgment Tools Applied Worldwide within a Chemical Company," *International Conference and Workshop on Risk Analysis in Process Safety*, October 21–24, 1997, Atlanta, GA, pp. 13–28. New York: American Institute of Chemical Engineers.

2. Dowell, A. M., III (1997), "Layer of Protection Analysis: A New PHA Tool, After HAZOP, Before Fault Tree," *International Conference and Workshop on Risk Analysis* in Process Safety, October 21–24, 1997, Atlanta, GA, pp. 13–28. New York: American Institute of Chemical Engineers.

3. Ewbank, Rodger M., and Gary S. York (1997), "Rhône-Poulenc Inc. Process Hazard Analysis and Risk Assessment Methodology," *International Conference and Workshop on Risk Analysis in Process Safety*, October 21–24, 1997, Atlanta, GA, pp. 61–74, New York: American Institute of Chemical Engineers.

4. IEC 61508, *Functional Safety of Electrical Electronic/Programmable Electronic Safety-Related Systems*, The International Electrotechnical Commission, 2010.

5. IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements*, International Electrotechnical Commission, 2003.

6. ANSI/ISA 84.00.01-2004 (IEC61511-1 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements,* 2004.

7. *Layer of Protection Analysis: Simplified Process Risk Assessment,* CCPS/AIChE, 2001.

8. *Guidelines for Initiating Events and Independent Protection Layers, CCPS*/AIChE, New York, NY, 2015.

9. *Guidelines for Conditional Modifiers and Enabling Events,* CCPS/AIChE, New York, NY, 2013.

10. "Accounting for Human Error Probability in SIL Verification Calculations," W. Bridges and H. Thomas (exida), *8th Global Congress on Process Safety*, Houston, AIChE, April 2012.

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

12. "Gains from Getting Near Misses Reported," W. Bridges, *8th Global Congress on Process Safety*, Houston, AIChE, April 2012.

13. "LOPA and Human Reliability – Human Errors and Human IPLs (Updated)," W. Bridges and T. Clark, *7th Global Congress on Process Safety*, Chicago, AIChE, March 2011.

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

15. Bridges, W. and Clark, T., "Key Issues with Implementing LOPA (Layer of Protection Analysis) – Perspective from One of the Originators of LOPA," *5th Global Congress on Process Safety*, April 2009, AIChE.

16. "Using LOPA to Verify the Design of a Burner Management System", John Champion, AIChE, 40th Annual Loss Prevention Symposium, Orlando, Florida, April, 2006

17. ISA TR84.00.02, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques*, International Society of Automation, 2002.