LOPA: Performed When and by Whom

A.M. (Art) Dowell, III
Process Improvement Institute Inc. (PII)
adowell@piii.com

William G. Bridges
Process Improvement Institute Inc. (PII)
1321 Waterside Lane, Knoxville, TN 37922 USA
wbridges@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2019 Spring Meeting and 15th Global Congress on Process Safety
New Orleans, LA
March 31 – April 3, 2019

LOPA: Performed When and by Whom

A.M. (Art) Dowell, III
Process Improvement Institute Inc. (PII)
adowell@piii.com

William G. Bridges
Process Improvement Institute Inc. (PII)
wbridges@piii.com

Keywords: LOPA, IPLs, PHA, leader

Abstract

Layer of protection analysis (LOPA) was introduced in the mid-1990s by Art Dowell at Rohm and Haas Chemical Company (became Dow Chemical, now DowDuPont, Inc.) and by William Bridges at ARCO Chemical (now Lyondell-Basel) and JBF Associates. The first book was published in 2001 by CCPS. Since then, the method has swiftly grown in popularity for use in making risk judgments and in deciding on the SIL rating for an SIF. But, many users of LOPA do not know when to use LOPA and so they overuse this tool; and they do not know who should be doing LOPA, so they many times use a team, similar to or the same as a PHA/HAZOP team. This paper explains what the originators of LOPA intended and why, and also brings the industry up-to-date on the lessons learned from different approaches to using LOPA, related to when to do LOPA and who should do LOPA.

1. Introduction

The initial development of layer of protection analysis (LOPA) was done internally within several individual companies. However, once this method was 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) of a safety instrumented function (SIF), 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). 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.

Since the first book was published, the method has swiftly grown in popularity for use in making risk judgments and in deciding on the SIL rating for an SIF. But, many users of LOPA do not know when to use LOPA and so they overuse this tool; and they do not know who should be doing LOPA, so they many times use a team, similar to or the same as a PHA/HAZOP team. This paper explains what the originators of LOPA intended and why, and also brings the industry up-to-date on the lessons learned from different approaches to using LOPA, related to when to do LOPA and who should do LOPA.

2 When do to LOPA? – Timing

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, 1-10 LOPA scenarios would be done). 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 safeguards qualifies as independent protection layers (IPLs; using a qualitative definition of an IPL), then performing LOPA in situ is usually overkill. In some 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 some pitfalls, and doesn't work for many types of scenarios.

In summary, the three major approaches seen in the industry on WHEN to do LOPA are:

- Do it during the PHA, scenario by scenario.
- Do it during PHA, at the end of a major HAZOP section (or group of sections), when scenarios are complete.
- Do it outside of PHA.

Every approach has different human resource requirements and also has its advantages and disadvantages. Each approach is described below.

2.1 During the PHA, scenario by scenario (NOT RECOMMENDED)

Some organizations do LOPA during the PHA, scenario by scenario. The authors have participated in this timing of LOPA.

For this option (which we DO NOT recommend), the personnel required is the full PHA team.

Practitioners of this approach suggests that the advantages are

- The scenarios are fresh in mind of personnel.
- If the Process Safety Information is in the minds of personnel (that is, the Process Safety Information is not well-documented), they may be able to answer questions more efficiently.

The Process Safety Information should be well-documented to ensure that the PHA is based on the correct information. And the PHA itself should be well documented so that all of the actions and future activities based on the PHA use the correct information.

The disadvantages of this approach are

- <u>It is counterproductive to switch back and forth from the PHA brainstorming</u> (inductive) thought process to the LOPA (deductive) thought process. An entirely different mindset and way of thinking are required for these two thought processes. It is important to keep the brainstorming mindset to identify hazards. A company should ensure NOTHING detracts from brainstorming, because if a scenario is missed, how will the company know if they have enough IPLs for that missed scenario?
- <u>All the hazards and candidate IPLs have not been identified yet.</u> The PHA team may or may not have pursued the cause to the ultimate consequence; sometimes the ultimate consequence is in a different node from the initiating cause and may not be fully understood until the team undertakes the LOPA on the initiating cause. Further, the LOPA done during the PHA of a node or step may generate recommendations for IPLs whose function may be provided by other candidate

IPLs. The authors' experience is that it is better to have a complete picture of a process (or at least a group of sections of a process) before undertaking LOPA.

- Wastes time of PHA team. Some members of the PHA team are not necessary for the LOPA process. It is more efficient to do LOPA with a smaller group and bring in the needed expertise only for the scenarios where their knowledge is required.
- May lack needed expertise. Many PHA teams do not include full-time participation by instrumentation/control engineers, or maintenance engineering, supervision, or mechanics. That expertise may be brought in periodically during the PHA to answer questions that have accumulated. Consequently, the LOPA scenarios done during the PHA node may lack critical knowledge and skills, particularly, for understanding independence between the basic process control system and safety instrumented functions. Understanding independence frequently requires the control engineer to drill down into the specific hardware configuration (including wiring) and into the specific software configuration.

Consequently, this approach is **NOT Recommended**.

2.2 During PHA, at the end of a major HAZOP section or group of sections when scenarios are complete (NOT RECOMMENDED)

Some organizations have found it effective to evaluate the required LOPA scenarios with the PHA team at the end of the brainstorming for a major HAZOP section or group of sections. The authors have participated in LOPA done in this fashion.

The personnel required are typically the full PHA Team plus instrumentation and control engineer. The control engineer is needed to understand independence.

The advantages of this approach are

- The scenarios are fresh in mind of personnel.
- All the hazards and candidate IPLs should have been identified.
- If the Process Safety Information is in the minds of personnel (that is, the Process Safety Information is not well-documented), they may be able to answer questions.

As discussed in the previous section, the Process Safety Information should be well-documented to ensure that the PHA is based on the correct information. And the PHA itself should be well documented so that all of the actions and future activities based on the PHA use the correct information.

The disadvantage of this approach is

- It is counterproductive to switch back and forth from the PHA brainstorming (inductive) thought process to the LOPA (deductive) thought process. An entirely different mindset and way of thinking are required for these two thought processes. It is important to keep the brainstorming mindset to identify hazards. A company should ensure NOTHING detracts from brainstorming, because if a

scenario is missed, how will the company know if they have enough IPLs for that missed scenario?

- Wastes time of PHA team. Some members of the PHA team are not necessary for the LOPA process. It is more efficient to do LOPA with a smaller group (on average 1.5 staff) and bring in the needed expertise only for the scenarios where their knowledge is required.
- May lack needed expertise. Many PHA teams do not include full-time participation by instrumentation/control engineers, or maintenance engineering, supervision, or mechanics. That expertise may be brought in periodically during the PHA to answer questions that have accumulated. Consequently, the LOPA scenarios done during the PHA node may lack critical knowledge and skills, particularly, for understanding independence between the basic process control system and safety instrumented functions. Understanding independence frequently requires the control engineer to drill down into the specific hardware configuration (including wiring) and into the specific software configuration.

This approach is also **NOT RECOMMENDED**, though the issues with harm to brainstorming and lack of expertise are easier to manage with this approach.

2.3 Outside of PHA (RECOMMENDED)

The original LOPAs were done outside of the PHA, in many cases, a long time after the PHAs had been completed, and this is still the best approach (with the one improvement of shortening the time between PHA and LOPA).

The personnel required are typically a LOPA analyst, a process engineer (by phone or email, as needed), and other expertise – such as control engineering – by phone or email, as needed. In the authors' experience, the average is about 1.5 people per LOPA scenario.

The advantage of this approach is:

- Provides efficient use of personnel time. There are no large meetings with some personnel not needed and not participating.

The disadvantages of this approach are

- Requires well documented Process Safety Information. Remember that we need good process safety information to do a good PHA and to do all the continuing activities to maintain good process safety for the facility.
- Requires well documented PHA.

This is the **recommended approach** today and in the original LOPA textbook as well. This approach can be practiced immediately after the PHA completed while the PHA is still fresh in the memories of those who would support LOPA on a part-time basis.

3. When do to LOPA? – Triggering: What scenarios go to LOPA?

Similar to the decision on WHEN to do LOPA, there are three main approaches for how to decide WHAT SCENARIOS are selected for LOPA:

- Every scenario.
- All scenarios that have fatality as a consequence.
- All scenarios that have or require a SIF (to determine the target SIL)
- Scenarios recommended by the PHA team.
  - When the PHA team is not sure.
  - When the scenario is complex.

This section describes those approaches.

3.1 Every scenario

Some organizations require that every scenario be assigned a consequence severity and an initiating cause frequency. And they require that every scenario be evaluated by LOPA.

The apparent advantage of this approach is

- Appears to be thorough. In reality, it is overkill.

The disadvantages of this approach are

- Overkill, waste of PHA time.
- Review can easily become superficial because of the high workload for the PHA team.
- When coupled with doing the LOPA in situ with the PHA, with the full PHA Team, this approach has all of the disadvantages listed in section 2.1 as well.

This approach is **NOT Recommended**.

3.2 All scenarios that have fatality

Many organizations require that all scenarios that have multiple fatalities, or a single fatality be evaluated by LOPA. The authors have worked extensively in this system with mixed results:

The advantage of this approach is

- Conservative. It is a good starting point for risk reduction.
- Good practice for PHA teams that are not familiar with LOPA.
- Good practice for organizations are just starting to use LOPA.

The disadvantage of this approach is

- May be more work than required (waste valuable engineering/analyst resources)
- LOPA does not work for all fatality scenarios; it only works for scenarios with multiple types of IPLs available.

A PHA Team with the following characteristics:
- A PHA leader who is a well-trained and vetted LOPA analyst,
- An experienced, knowledgeable PHA team,
- Working on a well understood process technology,

Has proven capable of determining whether risk reduction is needed and how much is required without doing a formal LOPA. However, the authors have observed that many PHAs have not identified the obvious hazards, and consequently cannot correctly evaluate the required risk reduction.

All scenarios that lead to fatalities (for scenarios for which LOPA works) is the **Recommended** approach **when the PHA Leader is NOT a trained and vetted LOPA analyst,** because use of LOPA will continue to train the PHA Leader on independence rules and on process and human reliability.

3.3 All scenarios that have or require a SIF (to determine the target SIL)

Many organizations require that all scenarios that have a SIF or that the PHA think may require a SIF be evaluated by LOPA. The authors have worked extensively in this system with mixed results:

The advantage of this approach is
- Conservative. It is a good starting point for risk reduction.
- Good practice for PHA teams that are not familiar with LOPA.
- Good practice for organizations are just starting to use LOPA.

The disadvantage of this approach is
- Is definitely more work than required.
- LOPA does not work for all fatality scenarios; it only works for scenarios with multiple types of IPLs available.

A PHA Team with the following characteristics:
- A PHA leader who is a well-trained and vetted LOPA analyst, and with moderate competency in SIS fundamentals
- An experienced, knowledgeable PHA team,
- Working on a well understood process technology,

Has proven capable of determining whether risk reduction is needed and how much is required without doing a formal LOPA, including determining when a SIF is required and what the target SIL should be [10]. However, the authors have observed that many PHAs do not have the required expertise in their PHA team leader [11].

All scenarios that lead to SIFs is the **Recommended** approach **when the PHA Leader is NOT a trained and vetted LOPA analyst and does not have a fundamental understanding of SIS,** because use of LOPA will continue to train the PHA Leader on independence rules and will compensate for lack of understanding of SIS.

3.4 Scenarios recommended by the PHA team

As described in the discussion on the previous approach, a PHA with a leader who is a well-trained and vetted LOPA analyst (and who understands the fundamentals of SIS), and an experienced knowledgeable PHA team, working on a well understood process technology, may be able to determine the requirements for risk reduction and SIF/SIL for most scenarios without doing LOPA. Thus, the only scenarios that go to LOPA are those recommended by the PHA team. This recommendation is usually only made when the PHA team is confused on the scenario itself.

The advantage of this approach is:

- LOPA is done only on the scenarios that are uncertain or that are complex.
- Efficient.

The disadvantage of this approach is

- The PHA team may feel comfortable with serious consequence scenarios that do not have sufficient IPLs
- It requires a PHA leader who thoroughly understands LOPA principles, especially independence.
- The PHA leader should understand the basics of SIS.
- It requires knowledge and expertise on the PHA team (or in situ coaching by the team leader) to understand independence of initiating causes and IPLs. The PHA team must be aware when they do not know for certain that the LOPA requirements for independence are met, or are otherwise confused on the scenario. Then they must recommend that scenario for the formal LOPA evaluation.

This is the **Recommended Approach when the PHA Leader is a trained and vetted LOPA analyst**.

3.5 Observed Phases of LOPA Application

PII has observed that most companies tend to go through phases of the use of LOPA.

Figure 1Figure 1 illustrates these phases. First, a company that has not used LOPA in the past 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 of doing LOPA, beyond the PHA team decision may not be justified for about 95% of the scenarios identified by the PHA teams. This transition may be partially due to improvements in the competencies of PHA team leaders (especially) and/or team members as they learn and use LOPA more.

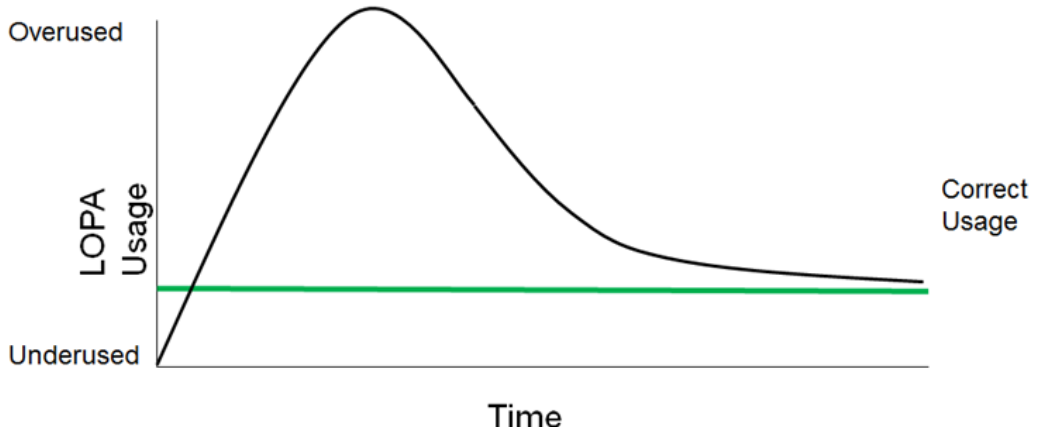

Figure 1: Typical Usage Rate for LOPA as application of LOPA matures within a company (*Courtesy of Process Improvement Institute, Inc. all rights reserved)*

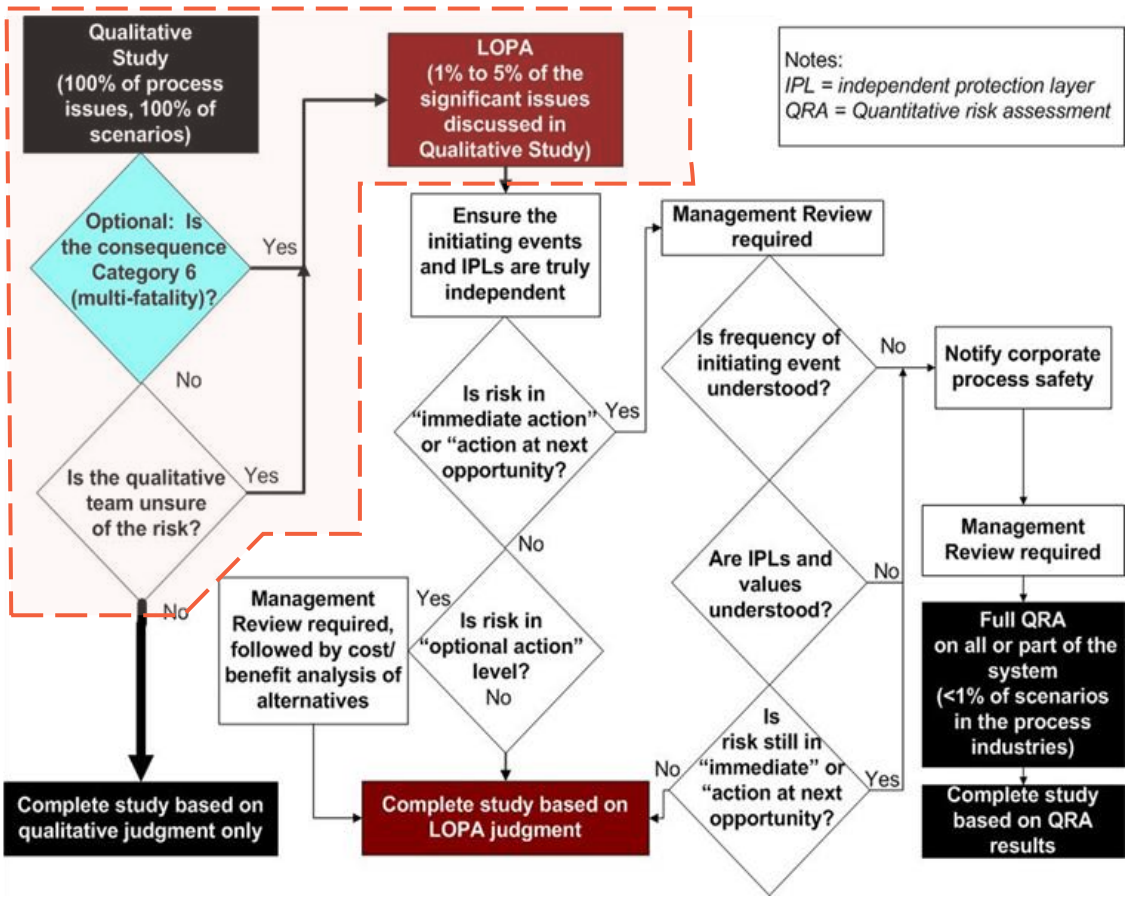

Figure 2: Criteria of when to use semi-quantitative/quantitative risk assessment

Figure 2 shows the decision-making process to go from Qualitative assessment to Quantitative. In particular, the criteria for going from Qualitative (PHA/HAZOP) to Semi-quantitative (LOPA) are highlighted. The approach recommended by PII (and the inventors of LOPA) is that shown in Figure 2.

4. Who performs LOPA?

The mention of a LOPA team in the first LOPA book was isolated and anecdotal; in fact the first LOPA book stressed the use of a LOPA analyst (singular). But many organizations now require a LOPA team (instead of a 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?" A more likely situation is Your company learned wrongly from other companies or from misleading consultants that a team is always required with 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.

The three "LOPA team" configurations still seen today are:

- Full PHA Team
- Full PHA Team plus instrumentation and control engineer
- LOPA analyst with occasional into from process engineer, instrumentation engineers, other expertise by phone or text or e-mail mail, as needed, for an average 1.3 people per LOPA scenario, with the LOPA analyst being the only full-time staff doing LOPA

As mentioned before, the third option is the recommended approach.

5. Conclusions

The best approach for when to use LOPA, who performs it and on what scenarios is summarized in Table 1.

Table 1: Best approach for LOPA

WHEN: Timing	WHEN: Trigger	WHO
Outside the PHA	• Scenarios recommended by the PHA team *(If PHA Leader is a LOPA analyst)* • All scenarios that have fatality *(If PHA Leader is **NOT** a LOPA analyst and or not trained in fundamentals of SIS)*	• LOPA analyst • Process engineer (by phone or e-mail, as needed) • Other expertise (by phone or email, as needed)

6. References

1. William G. Bridges and Tom R. Williams, "Risk Acceptance Criteria and Risk Judgment Tools Applied Worldwide within a Chemical Company," *International Conference and Workshop on Risk Analysis in Process Safety*, October 21–24, 1997, Atlanta, GA, pp. 13–28. American Institute of Chemical Engineers. New York, NY. 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. American Institute of Chemical Engineers. New York, NY. 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. American Institute of Chemical Engineers. New York, NY. 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, NY. 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. W. Bridges and A. Dowell III, "Identify SIF and Specify Necessary SIL, and other IPLs, as part of PHA/HAZOP – or - Why it is not necessary to 'Boldly Go Beyond HAZOP and LOPA'", *12th Global Congress on Process Safety*, Houston, TX, AIChE, April 2016.
11. A. Dowell III and W. Bridges, "More Issues with LOPA - from the Originators", *11th Global Congress on Process Safety*, Austin, TX, AIChE, April 2015.