Observing Your LOPAs in the Wild

Field Validation of LOPA Assumptions in Operating Plants

A.M. (Tony) Downes
Downes Process Safety LLC
Morristown, NJ 07960 USA
Anthony.M.Downes@gmail.com

Prepared for Presentation at
American Institute of Chemical Engineers
2024 Spring Meeting and 20th Global Congress on Process Safety
New Orleans, LA
March 24-28, 2024

Keywords: LOPA Validation, SIL Validation, Layer of Protection Analysis (LOPA), Process Safety, Risk Assessment, Validation, Industrial Process.

Abstract

For many years, Process Hazards Analyses were the standard in the industry. Beginning in the 1990s some companies implemented Layer of Protection Analyses (LOPAs) for the high consequence scenarios from the PHAs. The assumptions from the CCPS LOPA book "Layer of Protection Analysis: Simplified Process Risk Assessment" have been widely used since then.

Organizations must now ask "what's the real experience like? Are the safeguards as identified during the LOPA going to be effective? Is the preventative maintenance schedule in place and is that schedule being followed properly? Is there a test procedure for credited safeguards, and does that procedure make sense? What do those tests reveal?"

In scenarios like loading/unloading, which have a significant human error/human factor component, are the frequency assumptions still valid? Are the procedures and practices credited during the LOPA study really being followed? Are the independent protection layers (IPLs)? If checklists are credited, are they being used properly? Do alarms make sense? Regarding the human element, do operators understand the scenarios described in the LOPA? Do they understand the safeguards, how they work and why they are important?

Companies should ask themselves these questions. At least two large chemical operating companies began doing exactly that some time ago. A small group of corporate process safety engineers began putting their companies' most significant scenarios "under a microscope". They performed a deep dive on each site's LOPA scenarios, looking carefully at every aspect - from the consequence analysis to the maintenance records.

The results were interesting, and sometimes a little frightening. It may be instructive to other companies wondering how well their risks are actually managed, or to those looking to conduct the validations required by recognized and generally accepted good engineering practices (RAGAGEP) like ISA/IEC-61511. This paper will discuss methods used and real (though anonymized) patterns found.

1 Introduction

This paper focuses on the results from the LOPA for several reasons. The primary reason is that it focuses efforts for the validation. In the industry, LOPAs are only done for potentially catastrophic scenarios, so there are (hopefully) a limited set versus the myriad possibilities identified by the PHA.

The second reason is that the LOPA process specifically breaks the risk into its component parts. An example scenario is one where a pressure-storage vessel might rupture due to a control system fault. In this example, in order for this scenario to occur, a specific control valve must stick or be running in manual mode. A specific alarm must fail or be missed. A specific relief valve must fail to open. Personnel are assumed (in the LOPA) to be in the tank farm area less than 10% of the time. The LOPA process has already peeled apart the layers so they can be examined one by one.

Third, is that the LOPA sets out the expectations for the scenario in (semi) quantitative form. Instead of looking for something that should only happen less than once per 10,000 – or 100,000, or 1,000,000 years, a company can look at things expected to happen once per 10 years. They can see how often faults are being found in safeguards – faults that are expected to occur less often than once per 100 demands. They can check whether those safeguards are actually on-line and working more than 90% or 99% or 99.9% of the time, as they are intended to be. In other words, a company can see how well these components of the scenario have performed over the past 5-10 years to see if that performance matches with the LOPA expectations.

The following are real-world examples:

Example 1: A filtration system for hydrogen peroxide was protected by an active interlock. It was designed to open purge valve XZV-G101 in case of loss of flow detected by FZLL-101. However, this interlock was not put into the computerized maintenance management system (CMMS) for inspection. Approximately five years later, the interlock was called on to operate, but one of the valves stuck closed. The filter housing was damaged by the decomposition reaction and overpressure. Relief valve PSV-101 partially relieved the pressure but was not sufficient by itself. Fortunately, no one was hurt. A validation of the inspection, testing and preventive maintenance (ITPM) process would have discovered the FZLL-101 interlock was not being executed, so its risk reduction factor (RRF) had fallen well below the target.

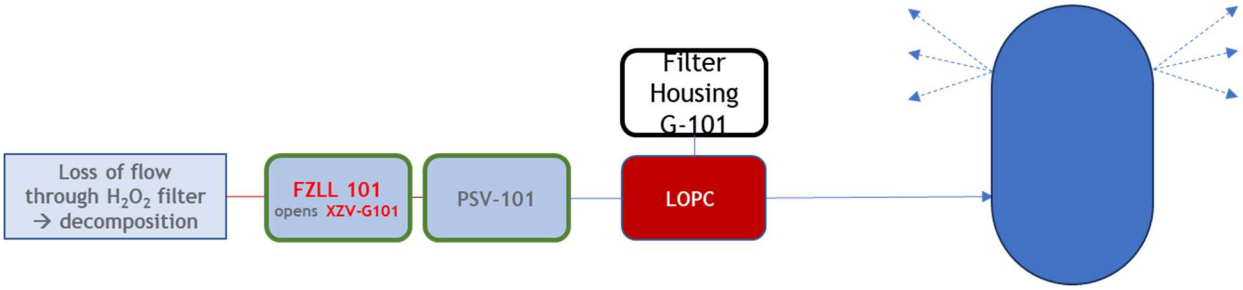


Figure 1. Simple "bowtie" diagram for a filter (one cause/one consequence)

Example 2: A reactor had the potential for an exothermic runaway that could burst the vessel leading to one or more fatalities if it were to occur. In the LOPA, it was assumed to have a temperature control loop fault about once per ten years (standard LOPA number per CCPS[i]). There was also an independent high-high-temperature interlock intended to prevent runaway reactions. It was found to have activated three times in one year. In other words, the initiating event frequency (IEF) appeared to be about 30 times higher than estimated by the LOPA. Clearly some further work was appropriate.

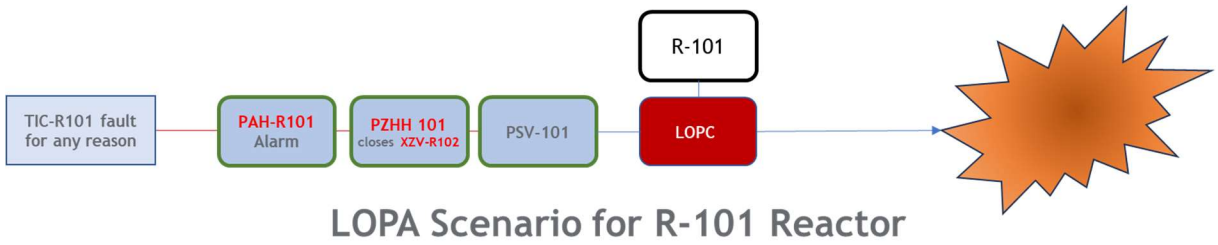


Figure 2. Reactor LOPA

Example 3: When looking across multiple scenarios, one company found that nearly half of their high hazard scenarios had been incorrectly evaluated for consequences by the PHA teams. Some had exaggerated the potential consequences, and some had underestimated them. Another found that the best starting place for validating LOPAs was to ensure that the estimated consequences made sense – perhaps the most logical approach to take.

The introduction outlined why the LOPA report is the right starting point. The rest of this paper will talk about the process that several companies have followed to validate their own LOPAs and sum up with conclusions and lessons learned. It will touch on each of the following topics:

- The input data sources (incidents, maintenance records and automation/controls data) used in the validation
- The rudiments of LOPA validation
- A method to validate procedural safeguards, including alarm responses
- A suggested sequence, including practical advice on how and where to start doing LOPA validations
- Skills, procedure and organization to conduct the validation.

2 Input data sources used in the validation

The LOPA results will be the key input used in the validation. The owner of the LOPA – usually the risk analyst - can outline and explain the scenario and its safeguards, ensuring the company understands the issues and will be invested in fixing them. Therefore, it is important that process safety information (PSI) match and document the cause and subsequent safeguards; the Piping & instrumentation diagrams (P&IDs), loop sheets, safe operating limits tables, cause and effect matrices and safety requirement specifications (SRS) should all align with the specifics of the scenario. The likelihood that the risk will be properly understood and kept sustainably low through the life of the unit will inherently increase.

The next sources of data are the site's incident and near-miss history, followed by the ITPM program and results which are usually found in the CMMS. Meetings with operators will confirm they understand the hazards as well as the administrative safeguards and/or any applicable emergency response protocols that they may have to execute. Their input into how and why the scenario could – or perhaps couldn't – occur is important.

The next source will come from the automation staff. It is a data dump from the alarm and event historian for the pertinent tags going back as far as they have data.

Table 1. LOPA/HAZOP assumptions and data sources to validate

Data source	Consequence	IEF	Safeguards	CM/EC
PSI/PHA/LOPA	**X**	**X**	**X**	**?**
Risk Analyst interviews	**X**	**X**	**X**	**X**
Incident/Near Miss reports		**X**		
ITPM / CMMS		**X**	**X**	
Operator Interviews		**X**	**X**	**X**
A&E History		**X**	**X**	**?**

3 The rudiments of LOPA validation

Lopa validation is about quantitatively confirming (or not) each of the assumptions that went into the LOPA for a specific scenario. LOPAs have four main components:

A. Consequence analysis (or a summary of the findings from the analysis)
B. Initiating event frequency (including the specific cause)
C. Identified independent protection layers (IPLs) and their availability/effectiveness
D. Enabling conditions and conditional modifiers (if any)

LOPA validation puts each of these under the microscope.

A. Consequence analysis (or a summary of the findings from the analysis)

It is worth the effort to validate the general scenario including its consequences. In one instance, a company found that teams had estimated overly conservative consequences for a substantial fraction of its scenarios. In some ways, this may seem like it is failing “safe”. If teams are going to get it wrong, it’s better that they overestimate the consequences of scenarios. In fact, several companies have PHA and LOPA “rules” that are deliberately conservative so PHA teams are unlikely to miss scenarios.

There are benefits to this approach, but it should not be overlooked that there is a natural tendency to be conservative. If an organization has any skeptics, they may point to these examples as “exaggerating the risk”. It can undermine the credibility of the entire risk management process which is necessary to get continued support from the organizations. To deal with this conservative-bias, it is helpful to have a corporate-oversight process for high-consequence scenarios. Another consideration is that resources are always limited. Spending valuable time and money on unnecessary safeguards is wasteful.

This may be as simple as an A-E categorization of the possible consequences before considering active safeguards. Key categories include:

1. Potential catastrophes, such as multiple fatalities [1]
2. Single fatality

3-5 Less severe consequences (Injury etc.)

The first question should be "is this scenario really going to have catastrophic[2] consequences?" It may be necessary to use expert judgement and/or more sophisticated consequence analysis. The consequences can be validated using two steps. The first is qualitative - does the site's analysis "feel" correct? Some process safety professionals have been doing quantitative analysis of gas releases using computer tools since 1988, so their experience may be slightly different than others', but it is possible to develop a feel for whether a release could be large and whether it could affect large or sensitive receptors. A safety analyst visited the proposed location for a chlorine railcar unloading facility many years ago. Looking through fence they could see a daycare across the highway. There have been times when the PHA team was being overly conservative. If the consequence analysis "feels" right to an experienced risk analyst, it may be best to accept it and move on. In the case of the chlorine railcar unloading facility, the analyst and company moved on to step 2 – quantitative analysis.

For any consequence analysis that fails the qualitative screening, it is worth developing a computer model of both release rate for the chemical of interest, as well as its state, followed by dispersion analysis of the cloud. In an analysis of one company, more than half the "catastrophic" scenarios found could not have been so bad in reality. Simple models like ALOHA, as well as sophisticated engineering tools like SAFER, PHAST and others can be used. Specialized companies who evaluate occupied structures to see how they would fare if an incident were to occur can also be hired. These tools can more than pay for themselves as a company decides how to either reinforce or relocate control rooms or protect workers in maintenance shops.

B. Initiating event frequency (and cause)

Once the potential consequences of a scenario are found to be significant enough – usually one or more fatalities – it is time to validate the cause and the likelihood/frequency of the initiating event that could lead to that consequence. For example, if a control system fault could cause the incident, CCPS' LOPA book[ii] suggests this would be expected to occur about once per 10 years.

There are several ways to validate that a fault rate is similar to this general industry estimate. The first is to check the incident history. Most operating companies have good computer records that include "near miss" reporting. Recall Example 2 cited earlier in this paper. Too

[1] or some roughly equivalent environmental or business consequence such as devastating and long term environmental damage, or possible great economic/business loss.

[2] Most sophisticated operating companies have a risk matrix to focus their efforts on the highest consequence scenarios.

much weight should not be given to an absence of "near miss" reports though. A better source of data is to select an instrument with an alarm or interlock to protect against the scenario in question. Then look for activations of those alarms/interlocks in the site's alarm and event history record. While there is sophisticated software to monitor these, a lot can be done by exporting these from the control system, migrating them into Excel and filtering. When a list of activations has been compiled, the site should review them. Sometimes there are "innocent" explanations like testing, or other operations that could not have led to catastrophe. It is also important to look in the alarm and event history for "events" like mode changes (MD) where a control loop is taken out of automatic and placed into manual mode. The probability of a parameter going outside of its safe operating envelope can be much higher when its control loop is in manual mode. At the least, it should be noted if the event happens often or for long periods of time.

Three notes of caution on over-interpreting alarm and event history data:

1. In the case of more than one "instrumented" layer of protection – for example, if there is a high-pressure alarm that should activate before a high-high pressure interlock, then the focus should be on whichever should activate first.
2. The analysis usually looks for factor-of-10 differences in frequency.
3. This analysis only helps identify frequencies that are on the high side. Finding that there has only been one activation in the past 20 years is not statistically significant.

If a control system fault could cause a serious or catastrophic event, then its sensor should be in the site's calibration program, and that program should be managed through the computerized maintenance management system (CMMS), with records showing that calibrations are done on schedule. It is important to validate that the site is not finding big calibration issues. CMMS can also provide information on the number of repair work-orders being written for these transmitters. Both repair and preventive maintenance work orders should show up.

In the same CCPS table, "operator error" is expected to occur about once per 100 opportunities. Close examination of a company's procedures can determine how often a filter has to be changed or the tank-farm line-up changes. These data points can identify the number of opportunities per year for an operator to line something up incorrectly. If an operator error could lead to catastrophic consequences, then they'll have safeguards and memory-joggers like checklists or indicators. These instances should not be used in your "unmitigated" initiating event frequency. In some cases, it may be necessary to engage human factors specialists to evaluate cases where errors could lead to catastrophic consequences and the only safeguards are administrative.

Regarding operator error frequency, evaluators should ensure that the hazardous scenarios are described in the standard operating procedures (SOPs); check that operators are being trained; and interview some operators to make sure they know about the hazard and how their actions protect against it. There have been cases where operators were expected to take a specific action that newer employees were unaware of. Even when there are no issues identified, it is good reinforcement.

C. Safeguards and their availability/effectiveness

The first step in validating safeguard effectiveness is to verify to the extent possible that a particular safeguard could reliably protect against the scenario or its consequences. For example, a process safety professional investigated a batch makeup tank that had overflowed into its dike. It made a mess but was not particularly hazardous. During the investigation, it became clear that similar incidents had occurred recently. The high-level alarm was installed so that it was just a few inches below the overflow from the tank. The operators had less than 5 minutes to receive the alarm in the control room, relay it to the field, and for the field operator to stop the filling. After speaking with the operators, it became clear that this was not sufficient time to reliably[3] stop the pump.

Operator-based safeguards should be described in the SOP, and operators must be trained on them – to the point where they can describe them to the validation team. When validating administrative or human-based safeguards like checklists or secondary-signoff, analysts should go to the place where they are used and confirm that operators use them as intended. In several cases, analysts have observed paper checklists intended to prevent operation in the wrong order where the operators are in complete chemical-resistant suits. In each case, the operators filled in the checklist after the field task was over – defeating the safety purpose of the checklist.

For engineered safeguards, "effectiveness" is the probability that the given IPL will be effective in preventing the consequence of concern. Example scores would be: 9 times out of 10 or one LOPA order of magnitude credit, or better than 999 times out of 1000 for a SIL-3 safety instrumented function.

Beyond "actual functionality", there are two factors in effectiveness:

a. Does the IPL have an effective preventive maintenance program?
    a. Is the specific IPL in the site's scheduled ITPM program?
    b. Is the schedule being followed for that IPL?
    c. Do the results from the "as found" tests show that the IPL was working[4]?

The following are some examples of findings at two large chemical companies when they began detailed validation of ITPM for engineered IPLs. In both companies, a corporate CMMS had been implemented in the late 1990's. About ten - twenty years later, the corporate process safety staff began working with the corporate reliability staff to ensure that PHA-credited safeguarding systems appeared in the CMMS and had a scheduled ITPM plan. Here's what they found:

- More than 97% of the pressure safety valves (PSVs) appeared in the CMMS and had scheduled ITPMs. Where there were difficulties, they were related to PSV

[3] In fact, they were able to stop the transfer about 3 times out of 4. This data is available because the situation occurred every Friday when they were making a double batch of additive to get through the weekend.
[4] While occasionally failing an "as found" test is ok, this should be rare. For example, any specific SIL-2 interlock should fail the "as-found" test considerably less often than once per 100 tests.

tag-numbering as well as management of change (MOC) issues where valves had been added or changed after the site implemented the CMMS.

- At first, only a small fraction of the credited interlock "loops" appeared in the CMMS. In about half the cases, analog transmitters with only a "safety" function appeared in the maintenance calibration program, though rarely tag-by-tag which complicated validation.
- In many cases, safeguard layers had been added by PHA's once these began in the 1990's, but the information about these new items had not been passed to maintenance or was not entered into the CMMS.
- As the corporations became more sophisticated in their use and documentation of safety instrumented systems (SIS) for IPLs, ITPM procedures became more sophisticated in their use of test procedures and adjusting test intervals to achieve the target safety integrity level (SIL) value required by the PHA/LOPA. One upside of adopting SIS was that it was easier for maintenance to identify the associated sensor and final element devices as safety-critical.

At a few sites, the testing of interlocks was done by operations rather than maintenance. Only faults were reported to maintenance for repairs. As the number and sophistication of such interlocks increased, and as the corporate oversight of safety-critical ITPM increasingly relied on reporting via the CMMS, this became untenable.

b. Ensure that the IPL is NOT bypassed.
There are a couple of ways to survey this. The first way to check is to look through the unit's "bypass logbook". In the days of relay-based interlocks, these were called "jumper logs". Some companies manage their bypasses through their temporary MOC system. All sites should maintain a bypass log system to record, approve and manage their bypasses and to ensure the bypass is removed when it is no longer needed.

If the IPL is implemented via a programmable electronic system, the status is probably being recorded in the alarm and event (A&E) historian. The easiest way to check this is to look for the input or output "tags" of the safety-critical interlock loops. If they have been put into bypass mode (e.g. "BYP" in Honeywell systems) over the available history, explanations should be found for why each bypass was done. Implementing a bypass for a scheduled ITPM test is reassuring. Finding that a bypass was implemented after an input was activated but before final action could occur would be an indication[4] of some problem.

One company discovered an issue with bypassing of an interlock in a new unit, shortly after commissioning. When the corporate engineering staff reviewed the A&E history, they discovered dozens of activations of alarms that indicated a possible heat exchanger tube leak. In each case, the control board operator had bypassed the alarm. As it turned out, the issue was a combination of the setpoint for the analyzer being too "low" as well as the inherent drift and unreliability of process analyzers. This "unreliability" as well as a high spurious trip rate is a well-known attribute of analyzers. The answer was to adjust the setpoint "up" out of the signal noise and to move to a two-out-of-three voting system for the analyzer setup.

Bypassing a given interlock multiple times per year or for long periods of time would be an indication of another problem. After a serious near miss, one company implemented a project to find and eliminate situations where interlocks had to be bypassed in order to start processes. In some cases, this required automatic timers on bypasses. In some cases, it required process design changes.

The following are some examples of findings at several large chemical companies when they began checking for interlocks being in bypass-mode. While these numbers are much smaller than the issues identified via the ITPM analysis, they are at least as significant to the risk at the locations.

- When a company first started looking at bypasses on interlocks, they found more than 10% across the company.
- This varied widely from site to site, with at least one site having all more than twenty interlocks in bypass at the time of checking.
- About half the sites in in one company were found not to have robust bypass management systems.
- One company made it a project engineering objective to design processes to avoid the need for startup bypasses.
- In another company, one unit was found bypassing SIL-3 interlocks more than 200 times per year.

D. Enabling conditions and conditional modifiers

Consider modifiers like “occupancy” or the probability that someone will be in a remote part of the plant when an accident occurs, versus how often people are actually in that area, based on interviews or observations. Similarly, it should be noted if a particular regeneration process is expected to occur only once per year and last a couple of days (i.e. 2 days/year) but the validator finds that it takes 5 days and is done every quarter (i.e. 20 days/year).

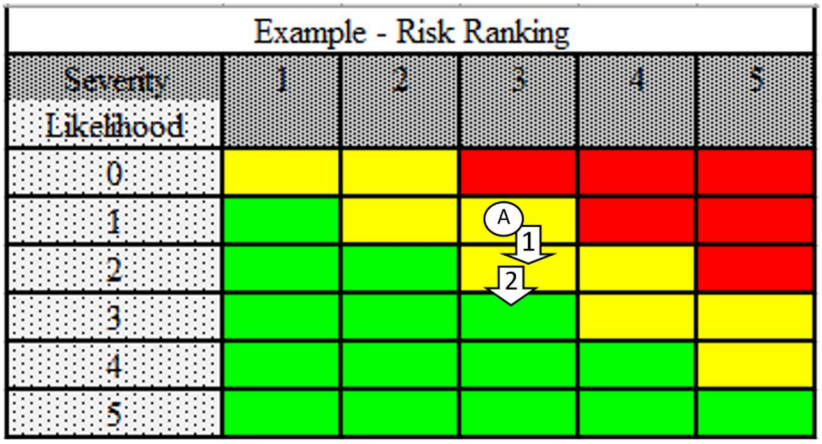


Figure 3. Risk ranking for a possible gasoline tank overfill

4 Suggested sequence, including practical advice on how and where to start doing LOPA validations

For those interested in trying LOPA validation in their company or at their site, here are some suggestions on how to get started:

- Start small. Pick three or four scenarios that already have LOPAs. Pick scenarios where management will care about the results – and be willing to fund further analysis if significant issues are found. It will take some effort to go through steps A-D above. Initially, it may take up to a week, spread across several weeks, to go through all aspects of a single LOPA scenario. With experience, this will come down to a day or two each, including time to document findings and recommendations.
- This should not be associated with an auditing process. Validating a risk assessment is still best done as a risk assessment process. It is too time-consuming to add onto the workload during an audit. Also, LOPA is a process of discovery. Operations and maintenance staff need to find value in it. Despite best efforts, audits can be viewed as nit-picky.
- Report the findings back to leadership. For example, "We looked at four high-consequence scenarios and found significant issues – significant enough that a risk gap may exist - in X percent of them". Don't be surprised if X is 50% or higher. That should build support for doing more such validations.

5 Skills, procedure and organization to conduct the validation

In previous companies, these validations have been a closely-held activity within the corporate or division level process safety team. To maintain the ability to compare results across sites, either a single experienced risk analyst is used, or a small team with tight technical oversight to ensure consistency. In several instances, delegating this to site staff or to larger groups of experienced risk analysts, led to such uneven results that it was undermining the credibility of the process. It also led to updating PHA/LOPA guidance based on these findings. This validation procedure and the feedback on its findings were shared with site-level PHA leaders and others.

Corporate reliability engineers can digitalize the ITPM validation efforts using the corporate CMMS with "PHA-credited safeguard" as a designator. This requires a good cross-functional team, excellent support/engagement from senior operations leadership and several years of steady effort to establish. Where this was done, results showed the value of the effort. Many critical IPLs were found to have preventive maintenance deficiencies: everything from higher-than-expected as-found faults to not being a part of the ITPM program at all. As a bonus, some devices/loops were found marked "PHA" in the CMMS, even though the PHA no longer credited them. With the support of the process safety team, these were redesignated, enabling maintenance to reduce their workload.

A number of major operational companies in the process industries are now using process historian data in their validation efforts. This requires close cross-functional efforts between process safety and automation staff. Again, enough problems are being found – and fixed – to justify further efforts.

6 Conclusions

This experience – demonstrated now over many sites at several different companies – makes it clear that the HAZOPs and LOPAs "as written" only reflect the true site risk level accurately a fraction of the time. Sometimes it is higher than the estimate. Sometimes it is lower.

Consequence analysis is a specialized activity. It is not unusual for consequence estimates done by site staff to be one to two orders of magnitude off – either overestimating or underestimating likely consequences – about half the time.

Many important safeguards have been found to either be bypassed or not tested as required by the ITPM program - or not be in the ITPM program at all. The fraction of active safeguards with problems varies from site to site as well as company to company. When process safety professionals validated these safeguards for the first time, they found 10-40% of SIL-rated safeguards had some problems. At a few sites, it was even higher than that.

Safeguards that rely on the actions of people have sometimes been found to be unlikely to work, either because operators were not following the requirements or had not been trained on them; or because there wasn't enough time for the operator to accomplish the required action.

PSM compliance audits very rarely have the time to get to the required level of detail to find the sort of problems described in this paper. Instead, one or more experienced process safety engineers had to do this validation as an additional activity. Once problems have been identified, leadership will be more willing to dedicate resources to finding where the real-world deviates from the LOPA and to fixing problems.

Remember, you don't reliably get what you *expect* – you get what you *inspect*.

7 References

Journal Article:
[1] Downes, A., Twarowski, A. *The benefits of comparing similar hazards across 'sister' plants*. Process Safety Progress, April 2009

[2] Downes, A., Goteti, P., Lindsay, S., Loseto, M. *Use Process Historian Data to Verify Safeguards.* Chemical Engineering Progress, February 2023

Book:
[3] "Layer of Protection Analysis" CCPS, 2001

Online Reference:
[4] Jamison C., Mentzer, R, *Study of Tank Overfill Incidents.* Purdue University, 2019

[i] CCPS "Layer of Protection Analysis" AIChE, 2001
[ii] CCPS "Layer of Protection Analysis" AIChE, 2001 pp 71

SPRING24
+20TH GCPS
A Joint AIChE and CCPS Meeting
March 24–28, 2024
New Orleans Ernest N. Morial
Convention Center
New Orleans, LA

1

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

Observing Your LOPAs in the Wild

Layer of Protection Analysis (LOPA) is a **Static** estimation of Risk.

We can and should do better in the data-rich 21st century.

2

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

Presenter
A.M. (**Tony**) **Downes**

1978-1988 **DuPont** Canada. Project Eng, Process Eng, Product Development, Maintenance Eng, Project Manager
1988-1992 **Bayer** Canada, Supervisor Process Safety/LP
1992-2001 **Westlake** Group, Principle PS Eng.
2001-2010 **FMC**. Global Safety & Sec. Mgr
2010-2022 **Honeywell PMT** Global PS Advisor
June 2022 Semi-retired **Consultant** for hire ☺

- Led over 100 PHAs
- Did first hazard review in 1979 (Fault Tree)
- Did first LOPA in 1999
- Led over 100 Incident Investigations
- Launched 4 Risk Reduction programs

- CCPS Certified Process Safety Engineer
- TUV Certified Functional Safety Expert
- CCPS Fellow

"Everything I know about Process Safety, I learned in an investigation"

3

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

Why start with the LOPA?

Focuses our efforts for the validation.

- Only done for potentially catastrophic scenarios therefore limited set
- Breaks the risk into its component parts
- Semi-quantitative format enables comparison to actual data

4

LOPA Components:

- Consequences
- Initiating Event Frequency
- Independent Protection Layers (IPLs)
- Enabling Conditions & Conditional Modifiers

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

Under- (and Over-) Estimating Consequences

Company A reviewed/evaluated their high hazard scenarios :

- Nearly half had been incorrectly evaluated for consequences by the PHA teams.
- Some had exaggerated the potential consequences, and some had underestimated them
- At "sister plants", ~20% had completely missed at least one major scenario.

Company B reviewed their LOPAs :

- About half of high consequence scenarios were overly conservative
- Also found "some" (5 -10%) of credible, high -consequence scenarios were either under -rated or missed * entirely.

* Requires deep expertise of processes and their hazards

IEF is Higher (or lower) than estimated

Company A reviewed/evaluated their high hazard scenarios:

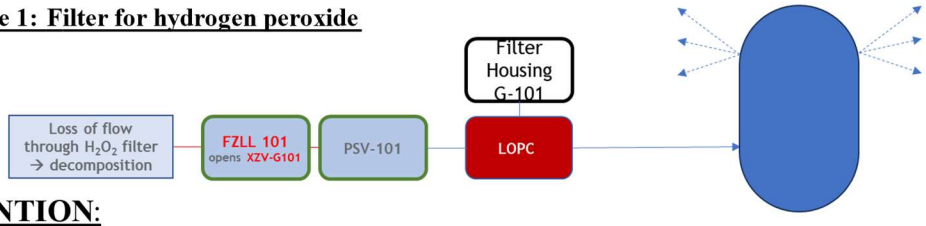
- Loading/unloading scenarios often evaluated at one-error-per-10-years instead of opportunity-for-error frequency.

Company B reviewed their LOPAs:

- Similar issue evaluating IEF for human-error scenarios
- Used incident data, "near-miss" data, alarm data and CCPS Tier 3 data (interlock activations, PSV lifts).
- Caused changes to IEF for ~20% of scenarios

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

Example 1: Filter for hydrogen peroxide



INTENTION:

- Low flow interlock switch FZLL -101 opens purge valve XZV-G101

REALITY:

- NOT entered into computerized maintenance management system (CMMS) for inspection.
- Approximately five years later, the interlock was called on to operate, but one of the valves stuck closed. The filter housing was damaged by the decomposition reaction and overpressure.
- Relief valve PSV-101 partially relieved the pressure but was not sufficient by itself.

➢Company initiated a review of the ITPM process to ensure **all credited PHA safeguards** were included:

- PHA → ITPM
- ITPM → Corporate oversight

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

Main failure modes for IPLs

Mode		Validation
1. Design of IPL has some technical issue.	→	Expert evaluation
2. Failure to Maintain	→	Maintenance/CMMS
a) Not in ITPM schedule, or b) Not tested per schedule, or c) Not evaluating/ "bad" results		
3. IPL in Bypass	→	Alarm/Event History
4. More demands than expected	→	*(see IEF discussion)*

9

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

Validating IPL Availability

Company A reviewed IPL/Safeguards against high hazard scenarios:

- In ~2001, less than 20% of instrumented IPLs had a scheduled PM
- Started to produce report of Credited Safeguards after PHA Revalidation → Maintenance
- In ~2004, still found many issues. Maintenance complained the Equipment Tag numbers not in PHAs
- Added to Corporate PSM Audit protocol
- Rose to >95% by 2009

Began looking for IPLs in "bypass"

- By chance Company A found that one site had many reactor interlocks in "bypass" mode all the time!
- Began a serious examination of "credited IPLs" to ensure they were active
  - Requirement in 2005 to use a bypass /jumper log
  - Added to PSM Audit protocol to check there was a jumper log; it was being used; there were very few (ideally 0) bypasses in p lace.
  - Big effort to "fix" situations where interlocks caused many (spurious) trips

10

Getting started

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

Crawl

1. Pilot - Select a few LOPAs to review

- Pick ones where everyone will agree the findings will matter
- Put them through the process – use an expert ideally from inside
- If you find issues or opportunities, look at other LOPAs

Walk

2. Form a team & go broad

- Select more LOPAs to review
- Continue to put them through the process
- If/as you find issues or opportunities, share them with "sister" sites or operations with similar scenarios

Run

3. Automate the process

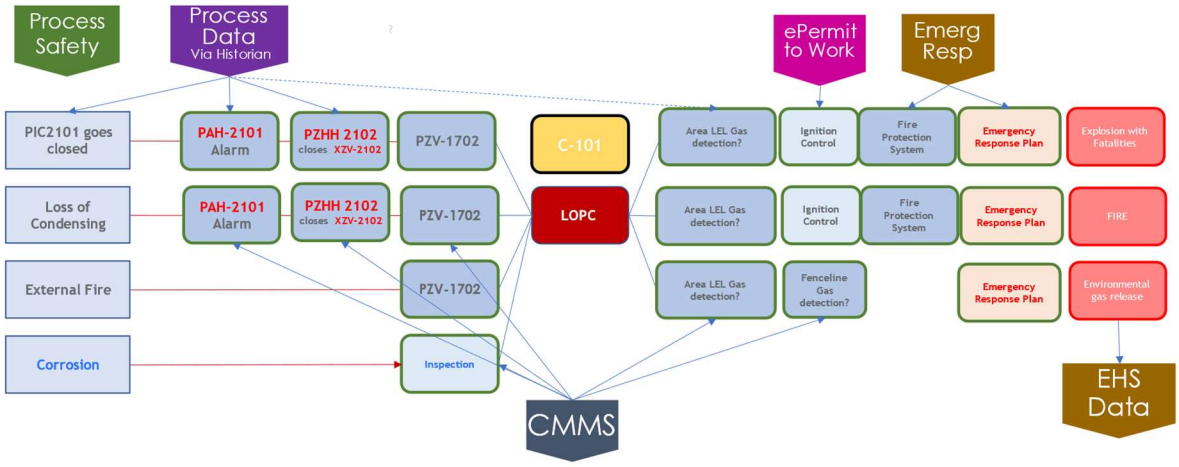
- Evaluate real-time-risk software providers
- Attend CCPS "Process Safety & Digitalization"

11

SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting

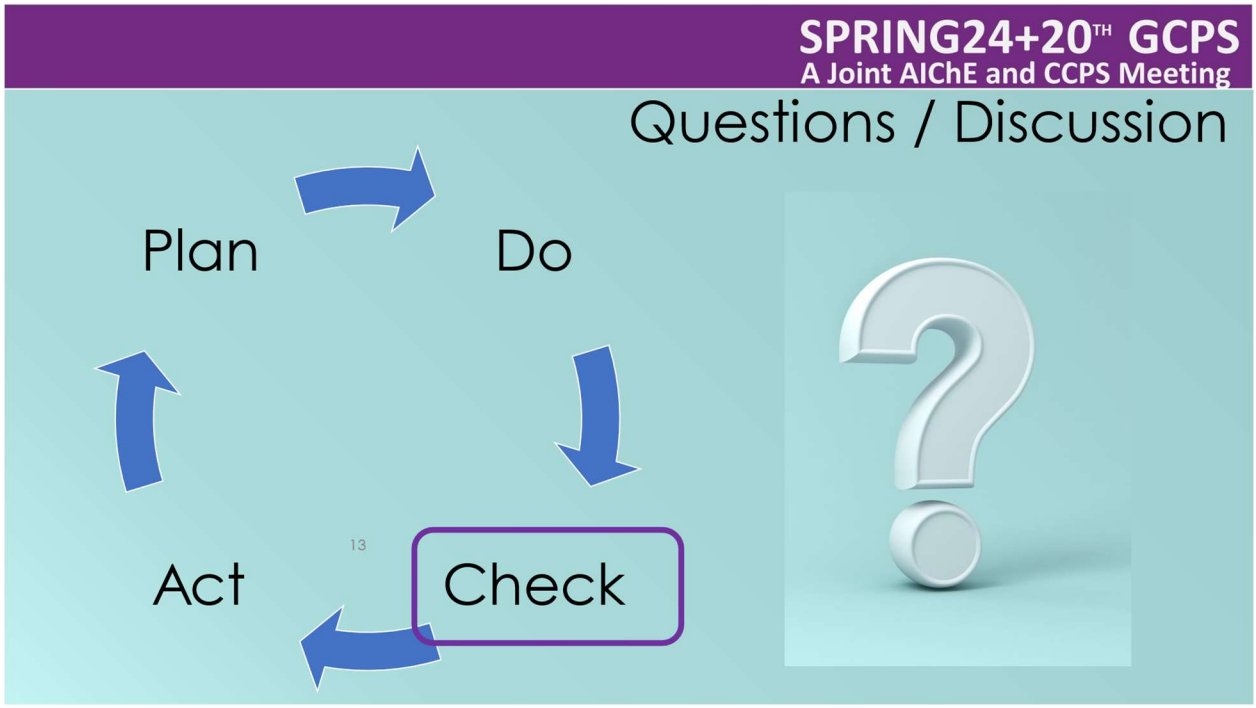
The Vision: Digitalization for Process Safety

One example: Realtime Risk



Bowtie for C-101 Distillation Column

12


SPRING24+20TH GCPS
A Joint AIChE and CCPS Meeting
Questions / Discussion
Plan
Do
Check
Act
13