SPRING25
+21ST GCPS
A Joint AIChE and CCPS Meeting

Making Inherently Safer Design (ISD) a Vibrant Part of Corporate Risk Management ©

Or

"How to Do Effective 'Safer Technology Alternatives Assessments (STAA)'"

A.M. (Tony) Downes
ABSG Consulting Inc.
Knoxville TN
ADownes@ABSconsulting.com

Don Lorenzo
ABSG Consulting Inc.
DLorenzo@ABSconsulting.com

Jim Klein
ABSG Consulting Inc.
JKlein@ABSconsulting.com

Gary Carrithers
ABSG Consulting Inc.
GCarrithers@ABSconsulting.com

Derek Bergeron
ABSG Consulting Inc.
DBergeron@ABSconsulting.com

Keywords: IST, ISD, Inherently Safer Design, STAA

Prepared for Presentation at
American Institute of Chemical Engineers
2025 Spring Meeting and 21st Global Congress on Process Safety
Dallas, TX
April 7-10, 2025

Making Inherently Safer Design (ISD) a Vibrant Part of Corporate Risk Management

Or

"How to Do Effective 'Safer Technology Alternatives Assessments (STAA)' "

A.M. (Tony) Downes
ABSG Consulting Inc.
ADownes@ABSconsulting.com

Don Lorenzo,
ABSG Consulting Inc.
DLorenzo@ABSconsulting.com

Jim Klein
ABSG Consulting Inc.
JKlein@ABSconsulting.com

Gary Carrithers
ABSG Consulting Inc.
GCarrithers@ABSconsulting.com

Derek Bergeron
ABSG Consulting Inc.
DBergeron@ABSconsulting.com

Keywords: IST, ISD, Inherently Safer Design, STAA

Abstract

Today, many companies incorporate inherently safer design (ISD) in their initial design processes and technology selection. Companies including Dow/Rohm&Haas, DuPont, Honeywell Performance Materials and many others have evolved in their approaches over the years. There have been many learnings about the best ways to incorporate ISD into new and existing plants in a sustainable way. For example, an ISD checklist and procedure are a good idea, but training, management support and expectations are also needed.

This is an important topic, especially now that EPA has mandated that many plants governed by its RMP regulation complete a safer technology alternatives analyses (STAA) no later than May of 2027. This paper will discuss how and when to do an STAA and who should be involved. The paper will also review "war stories" about successful adoption of inherently safer designs at many different companies - as well as a few "tick the box" exercises that don't add much value. Patterns have emerged. This paper will explain the patterns and what the authors consider to be the most effective of the possible processes to conduct ISD/STAA's.

Introduction - Inherently Safer Design is a good thing

Designing plants to be inherently safer is highly desirable. This paper will describe successful ISD efforts both within operating companies. These successfully reduced process safety risk without the added burden of maintaining add-on safeguards.

But there have also been unsuccessful or even wasteful efforts to apply ISD thinking to either new projects or to revalidation PHAs. There are differences and factors that make success more likely. This paper will describe these success factors.

For many years, leading operating companies in the process industries have addressed process safety hazards through a comprehensive program of hazard identification and risk analysis. As the industry began to evaluate risks more quantitatively and applied sound engineering practices such as layer of protection analysis (LOPA) and IEC-61511, more SIL-rated active safeguards were installed. These safeguards proved effective but came at a significant cost, both in terms of capital investment for installation and ongoing operating expenses, not to mention the occasional expense of spurious trips.

A combination of factors led engineering leaders at forward-thinking companies to reassess the approach of managing risks with added active safeguards alone. These factors included the recognition that the most cost-effective risk management occurs early in the design process, where safety can be integrated into the core process design rather than later adding extra layers of protection. Additionally, corporate stakeholders outside the process safety function asked for cost-efficient risk mitigation to preserve capital.

This paper will use a lifecycle approach to discuss how to identify ISD opportunities, with real-world examples from each phase of the lifecycle:

1. Chemistry (in R&D)
2. Process Design (in Project Engineering)
3. Process Engineering (in projects, and ongoing for the rest of the plant's life)

We will point out how ISD reviews can be conducted "upstream" in Phase 1 of the project lifecycle or even before Phase 1 in partnership with R&D. The paper will review specific practical issues and lessons learned along the way, such as selecting effective ISD chemistries early on, as well as how to document ISD "safeguard features" within process hazards analyses so they will not be forgotten – and possibly removed – over the years.

But what to do once the plant has been built? For many years, our industry has managed its process safety hazards through a robust process of hazard identification. We have advocated the use of risk matrix rating systems (qualitative and quantitative). As long-time practitioners in process safety, most of our collective efforts have followed a familiar path. Identify a hazard, estimate its potential consequences (How bad could it be?), estimate the initiating event frequency (How often might it happen?), then add safeguards as needed (Is the risk tolerable yet?). However, safeguards typically only reduce the likelihood or frequency dimension in a risk matrix. The other key aspect of risk is the consequence of a scenario. If we can reduce the consequence severity, then we may not need as many safeguard layers to achieve our tolerable risk target.

Perhaps most importantly, we'll discuss how companies should focus their efforts on the most important hazards (hint: highest potential consequences as well as higher-than-normal initiating event frequencies).

What is inherently safer design?

Here's a brief refresher on what is meant by "ISD":

Eliminate or Reduce the consequence of a hazard (The other dimension on a risk matrix)

Kletz famously said "What you don't have, can't leak" (Substitute or Eliminate). Similarly, if you have a lot less of a material (Minimize/Intensify) or operate at lower pressure or temperature (Moderate) then the size of the leak – and its consequences – will be much less.

Passive safeguards

Passive safeguards don't eliminate the hazard, but they do very reliably reduce the consequences of that hazard if it does occur. Spacing or distance has been used for many years. Since about the 1860's, the explosives business has used bunkers for both manufacturing and for storage. These passive blast-resistant structures don't make explosions any less likely, but they do limit the consequences of an explosion by venting the force upwards, away from other workers and the neighboring community.

Reduced frequency/likelihood "by design"

This factor might be controversial but is consistent with Kletz's "Simplify" principle in ISD. In many cases, it reduces the opportunity for human errors. It makes them less likely – ideally, almost impossible.

Human performance gaps contribute to almost all process safety incidents. These performance gaps fall into three main categories: failure to prevent the abnormal condition, failure to detect the abnormal condition quickly enough to take corrective action, and failure to execute corrective action before the incident occurs. ISD may improve human performance in any of these areas, but the emphasis is on preventing abnormal conditions. For example, inadvertently reversing the compressed gas tank connections to an oxy-acetylene torch is virtually impossible because of their inherently safe design (Figure 1). Even if the worker cannot read and/or is color-blind, the oxygen hose threads are right-handed, and the acetylene hose threads are left-handed. The hoses only connect one way - the correct way.

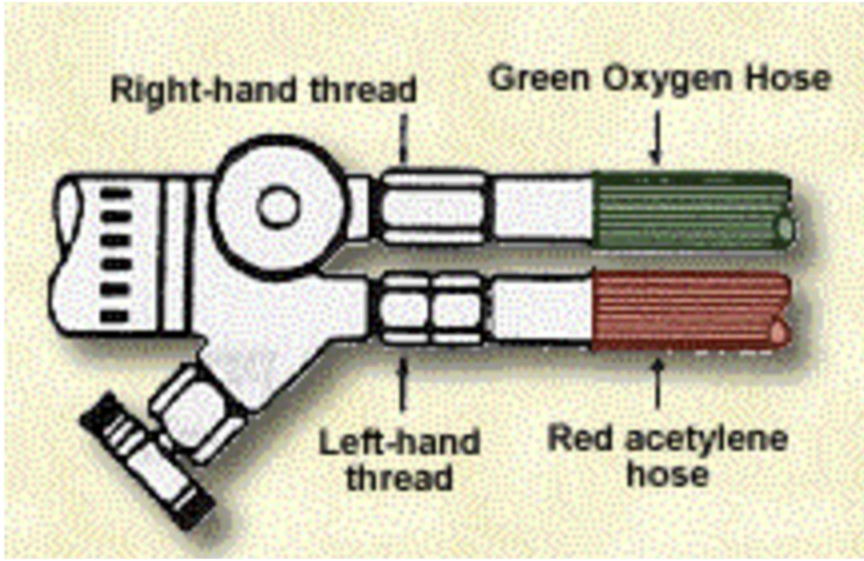

Figure 1 Oxy-acetylene torches can't be assembled incorrectly (image credit NOAA.gov)

How (and when) to look for ISD opportunities (including STAA)

Process hazards analysis (PHA) is the main process to discover, assess and manage process safety hazards. It makes sense to leverage this process to look for ways to reduce the inherent risk of a process. CCPS guidance and other authors have made this clear for years. And regulations such as New Jersey's TCPA, Contra Costa County's ISO and now EPA's 2024 revision to RMP all recognize this. The following sections illustrate how ISD and PHA can work together during initial project PHAs as well as during revalidation PHAs.

Chemistry (Best done in Research & Development or the first front-end loading (FEL) phase)

When Trevor Kletz first coined the phrase "inherently safer", he explained that the best time to put in inherently safer designs was when the plant was first being designed and built. Trevor used this very simple analogy: the most dangerous part of a house is the staircase. More people are injured falling down the stairs than in any other part of a house. "Many decisions about inherent safety have to be made early in design. It is too late to tell the builder when our house is complete that we do not want any stairs; it is too late to tell the architect when the drawings are complete." One can eliminate this hazard by building a single-story home, but that decision must be made at the earliest design stage. (See Ref 3)

Example of endothermic and gas-phase reaction

One operating company used quantified risk analysis to aid in designing their new processes and facilities. At least one of their raw materials was toxic. They realized that liquid-phase reactions, especially exothermic reactions, meant that achieving risk targets was becoming harder over the years. As design temperatures and pressures rose, the equipment, pipe-wall and the add-on safeguards were all making the plants more expensive. The research and development group began favoring chemistry that was either an endothermic reaction, or a gas-phase reaction – preferably at lower pressures. Both are inherently less likely to run away and lose containment.

Vapor-phase processes are particularly well-suited for continuous operation due to their operational characteristics. In contrast to batch liquid processes, continuous operations offer a distinct safety advantage, primarily stemming from smaller reactor sizes, the reduced inventory mass of materials at any given time, and the capability to promptly halt the reaction when process conditions begin to deviate from predefined limits. These advantages are especially pronounced when exothermic reactions cannot be avoided and where the effective control of heat generation is critical to maintaining process stability and safety.

This is not to say that nothing can be done after construction – we'll provide some real-world examples - but the opportunities *are* severely limited.

Expertise

We have watched teams struggle to identify ISD opportunities in the design phase. Having one PHA leader, even with the CCPS checklist, did not provide good results after two full days of discussion. That is unfortunate, because we later found that there had been ISD opportunities in that same project. We just needed one expert and a little training for the rest of the team to tease out those opportunities.

Table 10.1 from the CCPS Inherently Safer Chemical Processes Book: Inherent Safety Review Team Composition *(Updated for PHA/STAA)*

	Product Development		Design Development		Design Stage		Ongoing Operations	
	PHA	STAA	PHA	STAA	PHA	STAA	PHA	STAA
IH/ Toxicologist	☑	☑	☎	☎	☎	☎	☎	☎
Chemist	☑	☑	☑	☑	☎	☎	☎	☎
Process Engineer	☑	☑	☑	☑	☑	☑	☑	☑
Safety Engineer	☑	☑	☑	☎	☎	☎	☎	☎
Process Technology Leader / R&D	☑	☑	☑	☑	☎	☑	☎	☑
Environmental Scientist/Engineer	☑	☑	☎	☎	☎	☎	☎	☎
Control Engineer	☎	☎	☑	☎	☑	☎	☑	☑
Operator					☑	☑	☑	☑
Ops. Supervisor			☎	☑	☎	☑	☎	☑
Maintenance/ Maint. Engineer			☎	☎	☎	☎	☎	☎
Trained Leader *	☑	☑ *	☑	☑ *	☑	☑ *	☑	☑ *

☑ - Indicates team members normally required during meetings
☎ - Team members normally on call, or consulted as a subject matter expert
* - STAA leaders are normally highly experienced and well-versed in the technology of a process, as well as individual hazards

In addition to – or perhaps instead of - some of the team members CCPS refers to in their Table 10.1, ABS has found it more effective to include "Consequence SME's with broad exposure who have seen ISD done before". As with all PHA-like activities, there is a balance. With too few people, or too little expertise in ISD, the team may not find anything worthwhile. With too many people, the creativity required to generate ideas may be stifled.

As always, committees are good for identifying opportunities. Actual design is better done by individuals or a very small group. Again, think of a smaller LOPA team working to resolve issues identified by a full HAZOP team.

Techniques/checklists

In 2019 CCPS published the third edition of "Guidelines for Inherently Safer Chemical Processes: A Life Cycle Approach". This is one of the most widely read books on the topic. CCPS included a checklist for use by PHA teams. The checklist is good but was designed to be comprehensive and includes every ISD opportunity at every process design phase.

The text of the book explains that not all are applicable at all phases, especially not once the plant is built. Remember Kletz's analogy. For example, the first question in the raw list is:

1	SUBSTITUTE
1.1	Is this (hazardous) process/product necessary?

While this is a legitimate question to ask, you may wish to think carefully about who should be answering it. Teams who are approaching ISD for the first time are turned off by it. It becomes a distraction that undermines the credibility of the process without providing a benefit. And those answering the question for an existing process will likely feel it is moot "Of course, we need this process where I am currently employed."

Similarly, questions about chemistry that get settled in the R&D phase are not worth asking again in the process design phase. One company chose to break up the CCPS ISD checklist so it aligned better with the design and operating phases of the project & plant life-cycle.

Process Design (in Project Engineering)

The first version of the process flow diagram (PFD) can pinpoint where high hazard scenarios will be present. If the potential consequences of these scenarios can't be reduced or eliminated by design, then they may require add-on safeguards to manage the risk in the detailed-design PHA to reach the company's tolerable risk target.

It may be necessary to recycle back to the PFD from facility siting/QRA in FEL2 if issues arise. In one company, results from consequence analyses in FEL-2 triggered a recycle on the design aimed at eliminating one possible release scenario. The design was changed (see Fig 2) in such a way that it successfully eliminated some potential leak-sources, thus eliminating them as contributors to the overall risk.

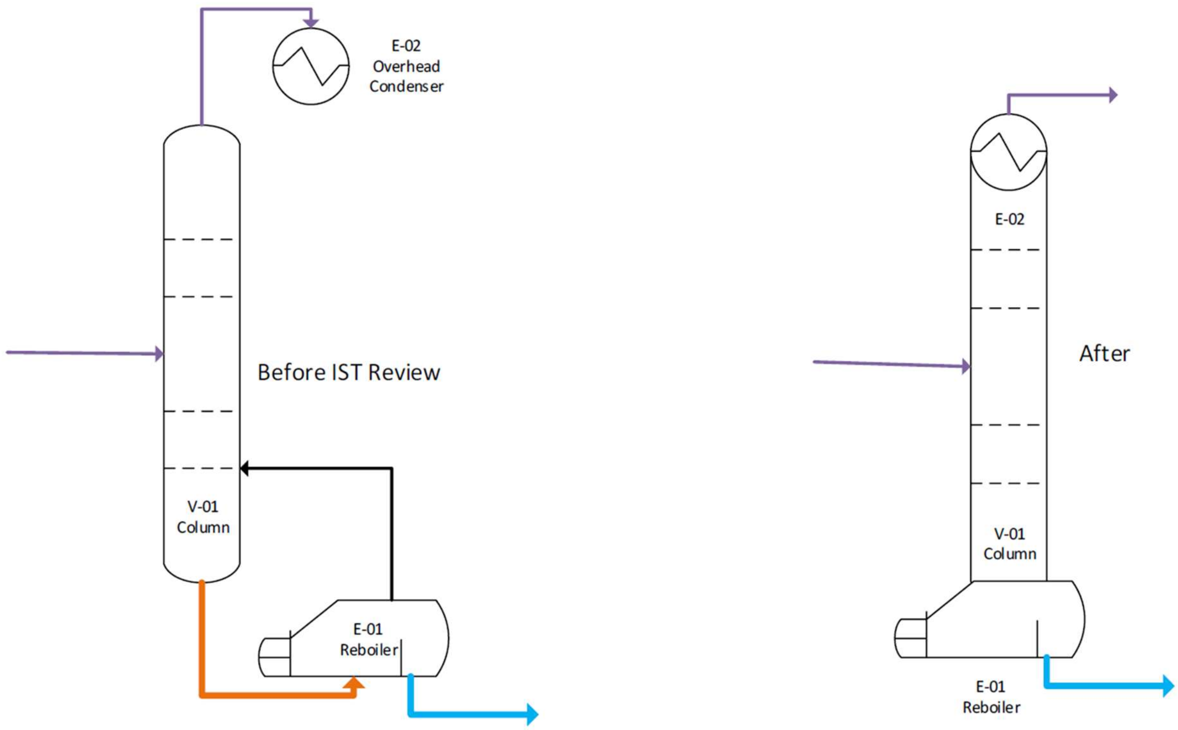

Figure 2 Eliminate specific piping to reduce offsite consequence (Ref. 2)

Which hazard scenarios should be the focus?

It does not make sense to try to look for an ISD solution to every possible hazard. As explained above, there are a number of options that could be used to focus the team's efforts to find an inherently safer process. Early ISD efforts used the checklists of possible solutions as the structure for the review (Fig 3). In other words, they were "solutions looking for a problem". ABS's observation of these efforts has been that they could be time-consuming check-the-box exercises that produced little real-world reduction in risk.

We prefer a different approach – hopefully one that is more productive and additive to our current risk management processes. It is useful to think of the IST/ISD review in cost/benefit terms. It is definitely going to take effort and likely financial resources to find safer alternatives. If you are going to rethink the design like that, it makes sense to work first on the areas that have the highest risk – particularly if that risk is elevated above the operating company's tolerable risk criterion. Essentially, ISD efforts should focus first on scenarios that are "problems" because they are not already ranked "tolerable" on your risk matrix. The IST/ISD checklist can now be used to suggest possible solutions to the site's list of actual problems.

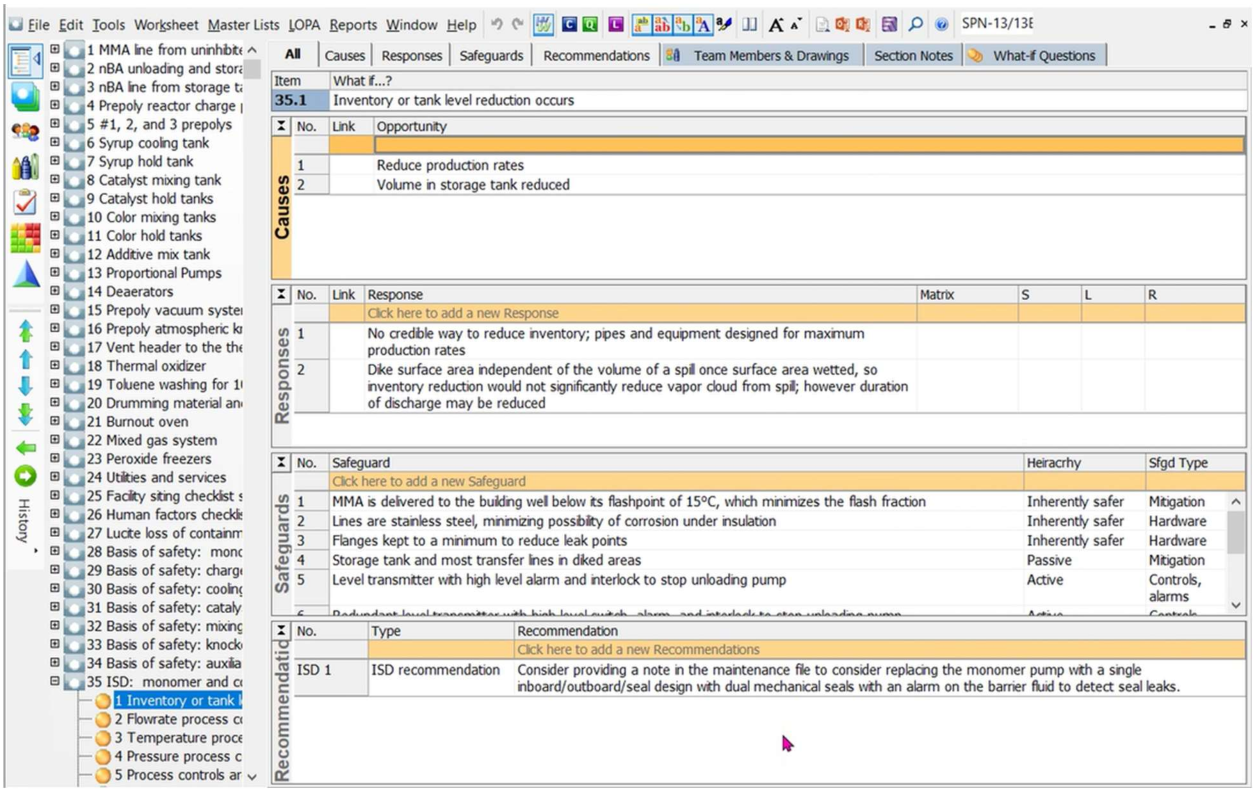

Figure 3 ISD Checklist in ABS Leader™ software (ABSG Consulting Inc., all rights reserved)

There are several examples below:

<u>Example 1:</u> The team did not specifically ask STAA/ISD questions when developing a recommendation to address a potential fire hazard concern. Therefore, the suggested action is a “Procedural” safeguard only and does not identify inherently safer opportunities.

> *Consider updating operating procedures to include specific instructions for operators to remain present at all times while draining water from vessel V-1. If the water from V-1 is fully drained, flammable liquid can flow from V-1 to the sewer and result in a fire hazard.*

<u>Example 2</u>: The team did specifically ask STAA/ISD questions when developing a recommendation to address a potential fire hazard concern. Therefore, the recommendation suggestions include options to (1) eliminate the hazard and/or (2) provide higher order “active” safeguards.

> *Consider providing additional safeguards or design changes to reduce the risk of draining the vessel V-1 water boot to the open sewer. The team suggests routing the V-1 drain to an alternate (safe) location such as the nearby feed drum V-2 and considering the installation of automatic controls to drain V-1 (eliminating the hazard/scenario). If this option is not feasible, the team suggests at least two of the following: (1) installing a spring loaded manual valve in the V-1 water drain line, (2) upgrading LSL-2345 to have an audible low level alarm (in the control room) and considering whether this low level*

switch should also close a valve in the drain line, and (3) installing a low explosive limit (LEL) detector in the immediate vicinity of the drain line open sewer location, with a locally audible alarm. If the water from V-1 is fully drained, flammable liquid can flow from V-1 to the sewer and result in a fire hazard.

What do you do if all your scenarios are already ranked "tolerable"? Some companies review PHA scenarios based on consequence severity (e.g., what scenarios have potential offsite consequences?) and look for IST/ISD opportunities or higher order safeguards there. If compliance with EPA STAA is a consideration, it makes sense to focus on scenarios that could have an offsite consequence. Example 3 shows how this might look, using the scenario from Example 2 where more safeguards were present, and risk was "tolerable". Using STAA/ISD principles resulted in the same recommendation as when risk was "unacceptable".

Example 3: HAZOP Table Recommendation **with** STAA/ISD Principles in the HAZOP table

Deviation	Cause	Consequence	S	L	R	Safeguards	Recs	Comment
Mis-directed flow	Manual valve to open drain left open	Potential to drain water from vessel V-1 followed by flammable liquid to the open sewer; fire hazard **ISD Opportunity:** A safer option would be to eliminate the need for operators to drain to the open sewer (see Rec)	1	5	5	Initial operator training is to be present during all water drains **Hierarchy:** Procedural Spring return manual valve, closes automatically when operator lets go of handle **Hierarchy:** Active	16. See text in Example 2 above **ISD Strategy/ Hierarchy:** (1) Eliminate/ Moderate, (2) Active Safeguards	Previous incident 123456 - this valve was left open, resulting in a fire and burns to a nearby employee (this resulted in the team selecting a high likelihood for this event)

Exhaust Stack Height (Passive)

A new plant was being designed. As the team went through the FEL 3[1] PHA process, they realized there was a secondary hazard to workers in the structure if the emergency scrubber was overwhelmed. This scenario showed up in the list of Scenarios that had not yet reached the risk target. These scenarios were sent to the LOPA process. In this operating company, the LOPA

[1] The Project Management Institute recommends capital projects in the process industries be split into 7 phases, with the first three being Front End Loading (FEL), prior to capital approval and detailed design.

process was used as a secondary PHA method to manage scenarios that either weren't brought to "green" in the HAZOP process, or where the recommended action was proving to be either technically difficult or very expensive.

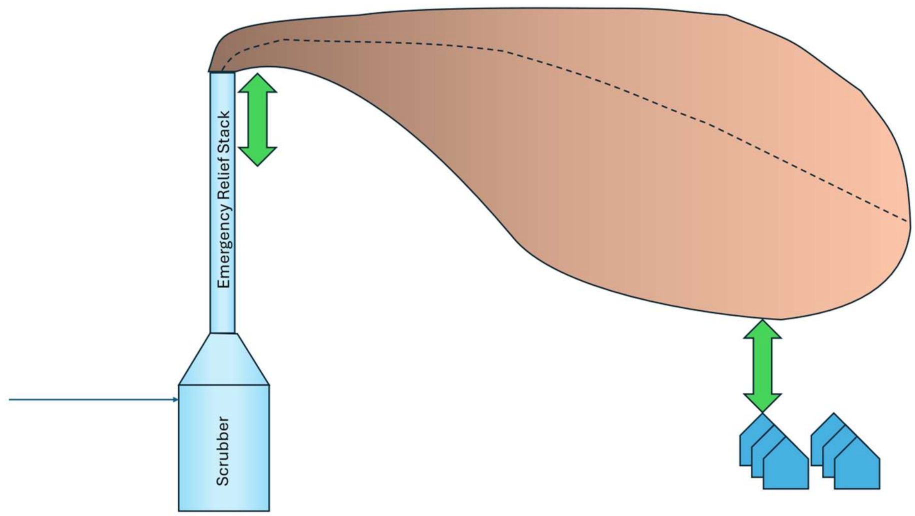

Figure 4 Raise stack height to reduce downwind concentration at grade

The LOPA team realized the simplest solution would be to extend the tip of the vent stack to the point where dispersion analysis showed a dangerous concentration would not reach grade (see Fig 4). This is an example of a passive safeguard. Similar tall vent stacks and chimneys have been used for more than a hundred years to protect workers and the community.

The stack height example illustrates another important point. The suggestion to raise the stack height came from a very experienced process safety engineer who understood vent stack gas dispersion and had access to consequence-modeling software to calculate how much the stack needed to be elevated to solve the problem.

This implies the ISD should focus (first) on Recommendations – i.e. where the PHA team found a problem – a risk gap. The LOPA team could do this if they had some ISD expertise on the team. Otherwise, do it *before* you try to reduce likelihood with add-on safeguards.

Specifics to comply with EPA RMP STAA

This section is meant to be a quick refresher on the STAA requirements. The regulation was issued about a year ago and the safer technologies and alternatives analysis (STAA) requirement came into immediate force, with a deadline for completion in May 2027, so the affected sites *should* all be about one-third of the way through these.

(a) **WHICH PROCESSES** MUST do STAA per March 2024 revisions? (Brief highlights on Applicability)

- If you have any NAICS 324 (refinery) or 325 (petrochemicals) process, AND it is RMP Program level 3

- And either:
  - (a) "within one mile of another stationary source having a covered process in NAICS code 324 or 325;" that is RMP Program 3

    OR
  - (b) a "hydrofluoric acid alkylation processes classified under NAICS 324"

    OR
  - (c) have had one RMP accident since the facility's most recent process hazard analysis;

(c) <u>WHEN</u>

Companies with processes subject to STAA have until <u>May 2027</u> to comply to the STAA requirements. EPA has stated that the initial STAAs can be completed with the next PHA/PHA revalidation or as a standalone analysis if needed because of PHA revalidation schedules. The EPA expects that many of these analyses will be combined at the next PHA revalidation. Since the STAA requirements are part of the PHA, it would then be revalidated on the same schedule as PHAs.

(d) <u>By WHOM</u>

(iii) The analysis shall be performed by a team that includes members with expertise in the process being evaluated, including at least one member who works in the process. The team members shall be documented.

Note that EPAs STAA requirements focus on existing operating processes. CCPS Table 10.1 has guidance about who might be included. Note ABS's comments about including ISD and consequence SME in the team makeup above. Experience, both good and not-so-good, tells us this is one of the most important success factors.

(e) <u>WHAT</u>

1) Conduct a "Practicability assessment of inherently safer technologies (IST) and designs (IST/ISD)"
   a) determine and document the practicability of the inherently safer technologies and designs considered.

2) FOLLOWED BY
   - (a) Implementation of at least one passive measure at the "stationary source", or
   - (b) IST/ISD, or
   - (c) a combination of active and procedural measures equivalent to or greater than[2] the <u>risk reduction of a passive measure</u>
3) Document "A justification in the Risk Management Plan when STAA recommendations are not adopted."

[2] EPA has not defined what it means by this.

Example risk matrix from CCPS

		REQUIRED RISK REDUCTION FACTOR				
Frequency in X years	1	100,000	10,000	1,000	100	10
	10	10,000	1,000	100	10	TR
	100	1,000	100	10	TR	TR
	1,000	100	10	TR	TR	TR
	10,000	10	TR	TR	TR	TR
	100,000	TR	TR	TR	TR	TR
		A	B	C	D	E
		Consequence Severity				

(f) **DOCUMENTATION**

In the Report, it makes sense to document the following as both a practical matter and/or because EPA requires it:

4) Date of the review
5) Scope (processes)
6) Team makeup and their qualifications
7) List of scenarios considered within each process and their basis for selection (e.g. Risk above target and/or Consequences could reach offsite)
8) For each scenario,
   a) the risk before any IST/ISD or passive safeguard recommendation,
   b) any IST/ISD or passive safeguard the team suggests for possible follow-up OR an indication that the team did not identify such an opportunity
9) For each opportunity identified by the team,
   a) a description of what was actually done to resolve and track each suggestion OR
   b) an indication of why it was rejected (following OSHA's guidance on the four acceptable reasons for rejecting a recommendation).
      (a) The analysis upon which the recommendation is based contains material factual errors;
      (b) The recommendation is not necessary to protect the health and safety of the employer's own employees, or the employees of contractors;
      (c) An alternative measure would provide a sufficient level of protection; or
      (d) The recommendation is infeasible.

NOTE: EPA requires at least one of the STAA team's suggestions be adopted OR an equivalent level of risk reduction be achieved using active measures.

In RMP*Submit system

EPA has required some information be included in the RMP*Submit system. Specifically:

"7) Inherently safer technology or design measures implemented since the last PHA, if any, and the technology category (substitution, minimization, simplification and/or moderation)"

A final thought on documenting ISD safeguards

It is important to document your ISD safeguards. Even if your team was clever enough to completely eliminate a hazard, it is worth mentioning this somewhere. These important design features do not look like other safeguards such as relief devices or interlocks. Ideally, they do not even need inspection or maintenance. Nevertheless, technical and operations staff need to understand that they have an important purpose. Otherwise, they can be rendered ineffective.

Consider this example: an exothermic batch reaction had a catalyst 'shot-pot" as shown in Fig 5. In an effort to reduce operator workload the site proposed to go directly from the catalyst storage to the reactor using a flow totalizer to control the flow. Fortunately, the team asked the question "Is there something special about the size of the shot-pot?"

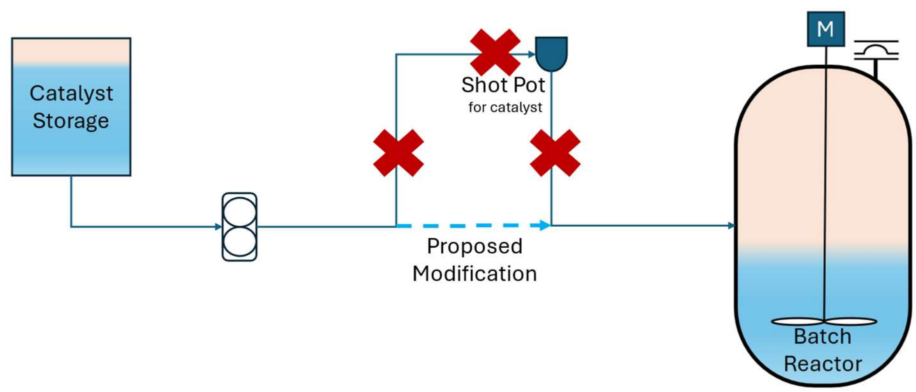

Figure 5 Shot-Pot limits catalyst quantity to relief device design case (ref 2)

It turned out that there was. The relief device could relieve a possible runaway reaction related to agitator failure, but only so long as there was not more than X liters of catalyst in the reactor. The shot pot was X liters in size, so catalyst could not be overcharged. This important "inherently safer design" safeguard feature was not mentioned on the P&ID, nor in the PHA. It *was* mentioned in the detailed calculations for the relief system. The site cancelled the project and added notes about the shot-pot on the P&ID and in the PHA.

Conclusion

Experience has shown that there are a number of factors that make the search for ISD/STAA opportunities more likely to be successful. Focus your efforts on "the problem" - on elevated risk and highest-consequence scenarios as identified by the PHA - rather than with a long list of potential solutions.

Have the right experience and expertise on the team. Engage the team-members. Use the questions from the ISD checklists that are relevant to the design phase of the project – or the revalidation of existing facilities. We have seen success when the team looked for ISD (which aims to reduce consequences) after the PHA but before the LOPA.

For scenarios with higher-than-normal initiating event frequencies triggered by a human error, consider whether the Simplify/Mistake-proofing principles of ISD could be helpful. It might require a design change – like the lefthand threads on oxyacetylene torches – but it could be far simpler and cheaper than an active interlock and more reliable than a double-signoff procedure.

Never confuse motion with progress. Simply chanting the ISD principles during a PHA is unlikely to make a real-world difference, even if there is a nice report afterwards.

1 References

[1] Hendershot, Dennis C. The Impact of Chemistry on Process Safety. *Paper presented at the 1st Annual Symposium of the Mary Kay O'Connor Process Safety Center,* 1998

[2] Downes, A.M. (Tony), Prior, David, Bolomey, Pascal, Misa, Noel, Incorporating Inherently Safer Technology into a Corporate Risk Management Program. *Paper presented at the Hazards 30 Conference, IChemE,* 2020

[3] Kletz, Trevor A., Amyotte, Paul, Process Plants - A Handbook for Inherently Safer Design (Second Edition), *Routledge* 2010