

# Design an Inherently Safer Plant

STEVEN T. MAHER, P.E.  
KRISTIN D. NORTON, P.E.  
SENEM SURMELI  
RISK MANAGEMENT PROFESSIONALS, INC.

Continue to search for ways to build safety into your process — from conceptual through detailed design, to procurement and construction, and even into operation.

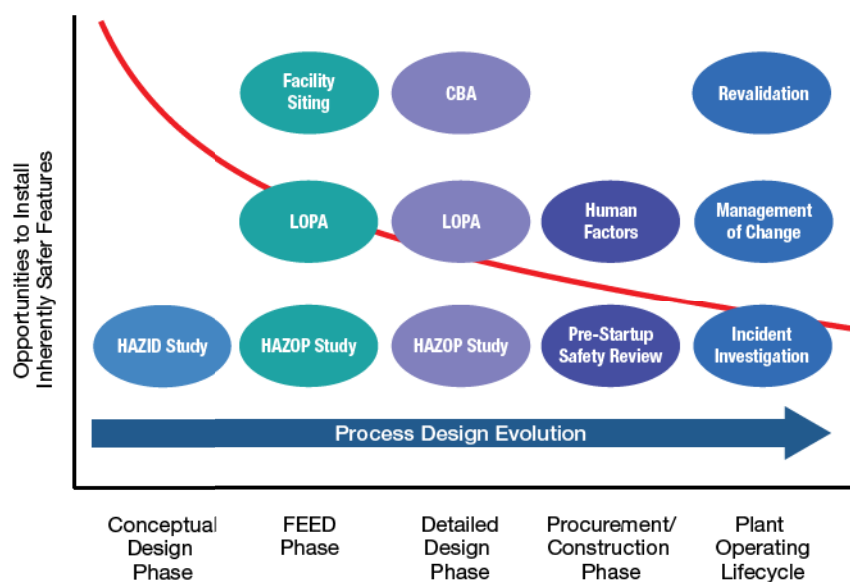
Inherently safer design (ISD) evaluations are important for identifying fundamental process improvements that can eliminate hazards or reduce the consequences of plant accidents. They are typically performed at the earliest stages of process design, where changes are most cost-effective. As the detailed design comes into focus, inherently safer options are rarely revisited because the designer's emphasis has shifted. Although fundamental changes during later design phases are more difficult, there may still be opportunities to entertain new ideas of inherently safer design. Thus, engineers should continue to look for new mechanisms to improve plant safety throughout the design process.

This article describes some of the tools that can be used to identify these opportunities, provides examples of inherently safer design strategies (*i.e.*, minimize, substitute, moderate, simplify) that can be applied at different points during the design work, and offers guidance on how to apply these concepts during the various risk-assessment studies that are routinely carried out during the design process. As shown in Figure 1, opportunities to incorporate inherently safer features decrease (due to associated costs and other impediments) as the process design evolves from a conceptual idea

to an operating plant. However, it is the process designer's responsibility to employ whatever tools may be available throughout the design progression, as each can provide different, yet valuable, insights.

## Conceptual design

The conceptual design phase contains the most opportunities for the identification and incorporation of inherently safer technologies into the process. Identifying these opportunities and making changes prior to detailed design avoids the added costs and schedule delays that would



▲ Figure 1. Opportunities to incorporate ISD into a process exist throughout the design activity.

\* This article is based on a paper presented at the American Institute of Chemical Engineers 2011 Spring Meeting and 7th Global Congress on Process Safety, Chicago, IL, Mar. 13–16, 2011.

# Safety

be incurred later for design rework.

Detailed piping and instrumentation diagrams (P&IDs) are not available during the conceptual design phase. Thus, potential process hazards and associated ISD opportunities can be identified through a hazard identification (HAZID) study using the process flow diagrams.

*Hazard identification study.* Application of HAZID at early stages of the design cycle allows for the identification of high-level ISD opportunities.

Although minimization — minimizing the hazardous material inventory — and substitution — replacing a hazardous material with one that is less hazardous — are usually the most effective ISD strategies during conceptual design due to the limited availability of detailed design process information, opportunities for moderation and simplification should not be overlooked. Table 1 presents examples of options that may be considered as part of the HAZID study.

## Front-end engineering and design

The front-end engineering and design (FEED) phase consists of activities to determine the project's feasibility and to develop initial project cost estimates. During this stage, the scope of work and the responsibilities of all involved parties are outlined and agreed upon. Although it is more detailed than the conceptual design phase, the

FEED phase also relies on estimates of process variables, as detailed design information is not yet available.

Identification of ISD options plays an important part in determining project feasibility and cost estimates. As design decisions are made, opportunities to include ISD alternatives into the design and minimize the potential for rework arise, thereby increasing project efficiency.

The tools available to help the process designer identify ISD alternatives during the FEED phase include the hazard and operability (HAZOP) study and the layer of protection analysis (LOPA). Facility siting studies and equipment layout decisions should also be brought up during the FEED phase so that ISD alternatives can be incorporated into these aspects of plant design.

*Hazard and operability study.* Once the first draft of the P&IDs is completed based on the project specifications, a HAZOP study is often conducted to determine the potential worst-case consequences of failures in the design. A team of individuals knowledgeable about the design and controls of the process discuss the potential hazards that could cause equipment/instrumentation failures or loss of containment and the resulting health, environmental, and economic impacts. The team uses a risk-ranking matrix to evaluate the severity and the likelihood of the consequences (based on the worst consequences of each

**Table 1. The conceptual design phase presents opportunities to minimize excess inventory and eliminate hazardous materials.**

Minimize
Minimize hazardous feedstock, intermediate, and product inventories
Reduce equipment size
Reduce piping lengths
Substitute
Use less-hazardous or nonhazardous reaction chemistry
Use lower-volatility solvent
Use less-hazardous or nonhazardous heat-transfer media
Use liquid form instead of vapor (if the risk is lower)
Use a less-concentrated form
Moderate
Identify an alternative catalyst that operates effectively at a lower temperature or pressure
Consider alternative chemistries that operate at less severe conditions
Simplify
Eliminate process steps
Identify a more selective catalyst that avoids the formation of byproducts and the need for product purification steps

**Table 2. During the FEED phase, efforts aimed at creating less-hazardous conditions may be effective.**

Moderate
Reduce pressure
Reduce temperature
Refrigerate storage facilities (not with ammonia)
Limit sources of ignition; identify possible sources and remove them if possible, or keep them separated from flammable materials
Design buildings to withstand blast pressure
Limit escalation of an incident through proper equipment spacing (reduce congestion), buffer zones between units, secondary containment, barriers, segregation of hazardous materials, and an overall plant layout that considers wind direction
Simplify
Eliminate pumps and instead use gravity or pressure/vacuum differentials to transfer hazardous materials
Eliminate storage of highly hazardous intermediates by using such chemicals as they are produced
Minimize
Reduce equipment sizes (e.g., of intermediate storage vessels)
Substitute
Use less-hazardous chemicals

scenario). Although the likelihood of a consequence can be reduced by adding layers of protection (*i.e.*, safeguards), the design team should first consider ISD alternatives.

*Layer of protection analysis.* Although LOPA is frequently conducted in conjunction with the HAZOP study, in some organizations they are performed separately by different individuals to improve objectivity. LOPA uses equipment reliability data to calculate the expected frequency of an initiating event (*i.e.*, an event that creates a disturbance in process operation) and the combined effectiveness of existing independent layers of protection. It then compares the LOPA results to the company's risk-tolerance criteria (*i.e.*, the acceptable (or target) frequency of an event that would cause that consequence). Large gaps between the probability of the scenario's consequences occurring and the associated target frequency of the event indicate that the designer either needs to install additional or more-effective safeguards to further reduce the probability or change the design such that the consequence identified is no longer credible.

Table 2 lists some of the ISD considerations that may be explored during the FEED phase.

*Facility siting and equipment layout.* Although it is impossible to eliminate all risk associated with hazardous materials, ISD can prevent an incident from spreading throughout the facility. This can be done, for example, by providing adequate spacing between process units or sections of a large unit, orienting cylindrical tanks so that the heads do not face other equipment or the local community beyond the fence line, installing adequate containment areas, and locating frequently occupied portable buildings away from the process units. Facility siting checklists can be used to guide this evaluation. Tables of typical equipment spacing can be found in Ref. 1.

## Detailed design

Although the design is more mature during the detailed design phase, opportunities to incorporate ISD features for high-severity hazards or to correct design flaws do exist. Many of the opportunities at this stage involve simplification — for example, designing equipment to be more robust instead of adding equipment or controls to mitigate hazards.

Such opportunities may be more limited due to the higher costs associated with engineering rework, but it is essential to systematically evaluate these opportunities. Simplification may also reduce the costs associated with additional equipment and controls. Tools well suited for use in the detailed design phase include the HAZOP study, LOPA, and cost/benefit analysis.

*HAZOP study.* A HAZOP study in the detailed design phase differs from a HAZOP study in the FEED phase in that more-detailed P&IDs and specific design param-

eters are available. Thus, the team is able to characterize the hazards and risks more accurately, as well as identify hazards that were not evident during the conceptual design or FEED phase. Hazards identified during detailed design are usually mitigated with engineered solutions, such as additional equipment redundancy and safety instrumented systems. However, the addition of equipment introduces new risks into the system. Instead, the team should consider mitigating these hazards through simplification or other ISD strategies (Table 3).

*Layer of protection analysis.* The application of LOPA in the detailed design phase typically focuses on determining the required safety integrity level (SIL) targets for safety instrumented systems (SIS). As discussed previously, LOPA evaluates the gap between the target initiating-event frequency and the probability of the event, taking into account the likelihood of the initiating cause and the probability of failure on demand of the independent safeguards. If the probability of the event is not an acceptable risk, then either additional independent safeguards need to be incorporated into the design or the SIL of the safety instrumented system (*i.e.*, SIL-1, SIL-2, SIL-3, or SIL-4)

**Table 3. Look for ways to simplify complex designs during the detailed design phase.**

<b>Simplify</b>
Use equipment with higher pressure rating
Use spiral-wound and flexible graphite gaskets
Use pumps with double mechanical seals, diaphragm pumps, eductors, seal-less pumps (keep in mind that seal-less pumps may overheat and leak internally)
Design vessels for full vacuum
Design equipment containing liquid to withstand the maximum hydrostatic load when full
Select materials that are impervious to corrosion and resistant to erosion
Select heat exchanger shells that withstand the maximum expected tubeside or shellside pressure
Transfer materials by gravity or pressure/vacuum differential
<b>Minimize</b>
Use smaller-diameter piping where process requirements allow
Route pipes along the shortest path to minimize length and thus inventory
Minimize the inventory in specific pieces of equipment ( <i>e.g.</i> , heat exchangers, surge tanks, vaporizers)
<b>Moderate</b>
Locate equipment to maximize the distance to receptors of concern
<b>Substitute</b>
Use less-concentrated forms of hazardous materials

## Safety

must be sufficient to reduce the probability of the event to a tolerable level. The design team should also consider whether an inherently safer design would reduce the consequence of the event. While LOPA does not directly address the potential for incorporating ISD features, the study may reveal situations where ISD may be a more cost-effective way to achieve a tolerable risk.

LOPA can also be useful for quantifying the relative improvements offered by several design options. For example, the LOPA may indicate that a high safety integrity level (e.g., SIL-3 or SIL-4) is required. However, the cost associated with purchasing such robust SIS equipment is extremely high, and it may be more cost-effective to rework the design to be inherently safer — for instance, by specifying equipment and piping with a higher pressure rating. SIL-4 is typically used only in the nuclear industry due to the complexity associated with a system that can achieve that level of reliability. Similarly, although the implementation of SIL-3 in the chemical industry is possible, it is difficult due to the SIS proof-test requirements that must be met to ensure the necessary level of reliability. Simplifying the process through ISD not only provides

safety and environmental benefits, but also has the potential to reduce costs.

*Cost/benefit analysis.* This quantitative technique (sometimes referred to as benefit/cost analysis) is used to compare the cost-effectiveness of design alternatives. During the detailed design phase, it can be used to evaluate the costs and benefits of inherently safer design modifications vs. robust control system modifications (as identified through the LOPA). Cost/benefit analysis allows decision-makers to systematically consider design alternatives, taking into account both benefits and costs. Potential costs, such as direct project costs for engineering rework and additional equipment and economic impacts of worst-case scenario consequences — as well as potential benefits, such as direct project savings and increased efficiency — are quantified. These values are then used to calculate the annualized hazard probability and determine the cost/benefit ratio for each project alternative. When comparing the project alternatives side-by-side, the project with the lowest cost/benefit ratio (or highest benefit/cost ratio) is the most cost-effective solution.

### Procurement/construction phase

Changes made during the procurement/construction phase are expensive and time-consuming. As a result, ISD is often left out of the thought process, since it is commonly viewed as changing the design. But even at this late stage, it is possible to incorporate ISD features into the plant. Two useful tools at this stage are human factors checklists and pre-startup safety reviews.

*Human factors.* Human actions are among the most significant contributors to accidents. The U.S. Occupational Safety and Health Administration (OSHA) requires all facilities subject to its Process Safety Management of Highly Hazardous Chemicals standard (29 CFR 1910.119), or PSM regulation, to address human factors as part of the process hazard analysis (PHA). Whenever possible, processes should be simplified to minimize the potential for human error (Table 4). A detailed human factors checklist can be found in Ref. 2.

*Pre-startup safety review.* An effective pre-startup safety review (PSSR) is essential to verify that any changes to the project scope made after the conceptual design phase meet or exceed the original design intent. As a final check prior to startup, PSSR should also be used as a tool to confirm that all ISD recommendations made during previous risk assessment studies are addressed. Although it is required only for the facilities covered by the OSHA PSM regulation, PSSR is a generally accepted practice throughout the industry that should be applied to all new process installations. A detailed discussion on PSSR, including example checklists, can be found in Ref. 3.

**Table 4. Human factors should be re-examined during the procurement/construction phase.**

<b>Simplify</b>
Reduce instrumentation complexity to avoid information overload
Provide adequate lighting in the field and easy access to equipment so operators can easily determine equipment condition
Install valves so their position (open or closed) can be easily identified; install manually controlled equipment in line-of-sight of measuring element
Use signage that is easy to read, clear, and unambiguous
Maintain housekeeping and general work environment conducive to efficient performance
Use board and screen displays that match the actual equipment configuration
Design console layouts that are logical, consistent, and effective
Design components with unique shapes to prevent improper connection or assembly
<b>Minimize</b>
Schedule just-in-time deliveries
<b>Substitute</b>
Retrofit chemical dosing systems (e.g., replace anhydrous ammonia with aqueous ammonia for NOx reduction)
<b>Moderate</b>
Limit sources of ignition; identify possible sources and remove them if possible, or keep them separated from flammable materials

## Plant operations

An operating plant is dynamic and provides numerous opportunities to incorporate ISD into expansion projects and facility upgrades. The article by Edwards and Chosnek on pp. 48–52 discusses the application of ISD in existing plants in more detail.


ISD should also be addressed during safety evaluations required by the U.S. Environmental Protection Agency (EPA) Risk Management Plan (RMP) and OSHA PSM regulations, such as PHA revalidation, management of change (MOC), and incident investigation.

**PHA revalidation.** The RMP and PSM standards require facilities to revalidate their PHA (*i.e.*, the HAZOP and/or LOPA) every five years or when major changes are made. As discussed earlier, a HAZOP study evaluates potential hazards and allows the team to discuss mitigation measures, including engineered systems, administrative controls, and, most importantly, inherently safer design. Revalidating these studies periodically allows the facility to evaluate the hazards and consider new mitigation measures based on technology advancements since the last study was completed.

**Management of change.** MOC is a specific procedure for managing changes in the chemicals, technology, equipment, and procedures used in the facility. Proposed changes are analyzed to determine whether new hazards are introduced and to ensure that the changes are designed and implemented according to good engineering practices. As part of the MOC evaluation, the team may be required to revisit the HAZOP study, which provides an additional opportunity to consider ISD. Even if a HAZOP study is not required, the MOC process should investigate whether ISD options exist.

**Incident investigation.** Any facility that experiences an incident or a near-miss is required to conduct a detailed incident investigation to determine the root cause and to develop recommendations for preventing its recurrence. As the team brainstorms recommendations to mitigate the hazard or the conditions and events that contributed to the incident, it should look for opportunities to make the design inherently safer. A good way to ensure that ISD discussions take place during the incident investigations is to include a checklist in the site's incident investigation procedures.

## Closing thoughts

Although more options and flexibility are available, and the cost-effectiveness of changes is generally higher, during the early design phases, there can be many tangible benefits to implementing ISD throughout the lifecycle of the facility. Some ISD strategies may present more opportunities than others during a specific design phase. However, it is important to realize that all of the strategies are applicable in all phases of plant design and operation, and none should be excluded from consideration at any particular stage. 

## LITERATURE CITED

1. **Center for Chemical Process Safety**, “Guidelines for Facility Siting and Layout,” American Institute of Chemical Engineers, New York, NY, and John Wiley & Sons, Hoboken, NJ (2003).
2. **Crowl, D., ed., et al.**, “Human Factors Methods for Improving Performance in the Process Industries,” Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, and John Wiley & Sons, Hoboken, NJ (2007).
3. **Center for Chemical Process Safety**, “Guidelines for Performing Effective Pre-Startup Safety Reviews,” American Institute of Chemical Engineers, New York, NY, and John Wiley & Sons, Hoboken, NJ (2007).

## FURTHER READING

- Center for Chemical Process Safety**, “Inherently Safer Chemical Processes – A Life Cycle Approach,” 2nd ed., American Institute of Chemical Engineers, New York, NY (2009).
- Kletz, T. A., and P. Amyotte**, “Process Plants: A Handbook for Inherently Safer Design,” 2nd ed., Taylor CRC Press, Boca Raton, FL (2010).
- Sutton, I.**, “Inherent Safety in Front End Engineering,” presented at the American Institute of Chemical Engineers 2011 Spring Meeting and 7th Global Congress on Process Safety, Chicago, IL (Mar. 13–16, 2011).
- Sutton, I.**, “Prestartup Safety Reviews,” 4th ed., Sutton Technical Books, Houston, TX, [www.stb07.com](http://www.stb07.com) (Jan. 2012).

**STEVEN T. MAHER, P.E., CSP**, is a principal engineer with Risk Management Professionals, Inc. (300 Goddard, Suite 200, Irvine, CA 92618; Phone: (949) 282-0123; Fax: (949) 743-2932; Email: [steve.maher@rmppcorp.com](mailto:steve.maher@rmppcorp.com); Website: [www.rmppcorp.com](http://www.rmppcorp.com)). He has been a safety consultant for more than 31 years, the past 28 of which he has focused on high-quality applications of process safety, risk management, and loss prevention technologies such as PSM, SEMP, SEMS, and RMP for a wide range of industries. HAZOP studies and LOPA are his specialties. He received a BSME degree from Duke Univ. and MSME degree from Carnegie Mellon Univ., is a Certified Safety Professional (Systems Safety) and a registered professional engineer in Pennsylvania and California, and is a member of AIChE.

**KRISTIN D. NORTON, P.E., CFSE**, is a senior engineer at Risk Management Professionals (Email: [kristin.norton@rmppcorp.com](mailto:kristin.norton@rmppcorp.com)), where she provides a variety of risk and safety consulting services, including the facilitation of hazard and operability (HAZOP) studies and layer of protection analyses (LOPA), and the development and auditing of EPA-mandated risk management plans (RMPs) and OSHA process safety management (PSM) programs. Much of this work has included evaluations of inherently safer technologies during the design phases of large capital projects in a wide range of processes in a multitude of industries, both domestic and international. She graduated from the Univ. of Southern California with a degree in mechanical engineering, and is a registered professional engineer in California and a Certified Functional Safety Expert (CFSE).

**SENEM SURMELI** is a senior engineer with Risk Management Professionals (Email: [senem.surmeli@rmppcorp.com](mailto:senem.surmeli@rmppcorp.com)), where she provides process safety and risk management consulting services to clients in various industries, with a focus on petroleum and chemical production facilities. She specializes in facilitating hazard and operability (HAZOP) studies and layer of protection analyses (LOPA), assisting her clients with risk-based decision-making in various phases of capital improvement projects, as well as supporting clients in meeting applicable regulatory requirements associated with the handling and processing of highly hazardous chemicals. She received her chemical engineering degree from the Univ. of California at Berkeley and is a member of AIChE.