

Incorporating Inherently Safer Design Practices into Process Hazard Analysis

By

David A. Moore, PE, CSP
President

AcuTech Consulting, Inc.
100 Bush Street, Suite 200
San Francisco, CA 94104

Tel.: (415)772-5972

Fax: (415)772-5975

e-mail: inquire@acutech-consulting.com
www.acutech-consulting.com

Inherently safer design concepts are particularly useful for risk reduction and are highly recognized and recommended by safety professionals as a first choice in process design practices. 'Inherently safer designs' are designs where engineers employ a variety of techniques to achieve classical risk reduction through design. These methods include:

1. **Hazard Elimination** - eliminate hazards as a first priority (rather than accepting them and mitigating them as a risk reduction strategy once they exist);
2. **Consequence Reduction** - where hazards cannot be completely eliminated, find less hazardous solutions to accomplish the same design objective by techniques such as reducing exposure to a hazard, reducing inventory of hazardous materials, and substitution of less hazardous materials;
3. **Likelihood Reduction** - reduce the likelihood of events occurring by techniques such as simplification and clarity (lowering the likelihood of an initiating event), and layers of protection and redundancy of safeguards (to reduce the progression of an incident).

I. The Need for Inherent Safety

Engineers often approach safety as an afterthought in the design. They may use a safety review or Process Hazards Analysis (PHA), such as a Hazard and Operability Study (HAZOP) or a What if?/Checklist Study, merely as a project 'check' instead of a preemptive hazards reduction tool. If these studies are done at the latter stages of engineering or during construction, there is a natural tendency to avoid expensive redesign or rework. Inherent safety benefits are often missed.

There may be several explanations for the claim that inherently safer design practices are not being used to their maximum advantage: These may include factors such as:

- the lack of standardized approaches to commonly applied process hazard analysis studies and a failure to include inherent safety in PHAs;

- the lack of a recognized method for incorporating inherently safer design issues into the process safety management process or a discipline to review the merits of options for inherent safety, and;
- the lack of safety experience and knowledge of many of the teams who are applying these approaches, and;
- the lack of clear measures of acceptability of risks so teams do not have good rules to follow in risk decision-making.

Due to regulatory requirements to conduct process hazard analyses, such as OSHA's Process Safety Management standard (29 CFR 1910.119) and EPA's Risk Management Planning regulation (40 CFR Part 68), Process Hazard Analysis reviews are being conducted more than ever. There is a requirement in these regulations to establish and maintain a baseline risk understanding by retroactively evaluating existing processes and by evaluating new or modified processes. With all of this effort being expended, a major opportunity to improve process safety of U.S. businesses may be lost if teams are not well informed and prepared for the job.

AcuTech has made the following observations of several trends that have emerged over the past 5-7 years due to the new regulatory developments for process safety and risk management:

- hundreds of engineers inexperienced in many of the principles of process safety and inherently safer design are conducting or participating in studies;
- many companies, particularly medium to smaller ones, do not conduct any other type of formal safety design review. In fact, in many cases, they either eliminated other reviews due to the need for regulatory compliance and the amount of resources required to conduct the PHAs, or they never had an approach and they do not realize the proper approach to consider inherent safety.

II. Methods for Implementing Inherent Safety in Design Reviews and PHAs

These concepts can be easily applied, particularly in the design phase of a new or modified process, and may have very powerful benefits at relatively low cost. During the engineering process, however, these concepts are often not incorporated in a structured manner. Without knowledge or insight of these concepts, engineers may be retaining unnecessary risk or employing less reliable and more expensive alternatives to reducing risk in their projects.

Process incidents tend to have common causes based on fundamental principles of safety being violated. The design challenge is to recognize these hazards, and, considering the likelihood and consequences of them occurring, to assess whether improvements are justified. The basis for justification is a combination of regulations, codes of practice, engineering principles, and other forms of acceptable risk reference versus the costs, benefits, and risk tolerances of the company. Given this assumption, a common set of inherent safety questions, commonly applied, could be a powerful way to reduce risk.

Inherent safety is best accomplished by first educating the engineers who will be involved in the design on the principles available. Through an improved understanding of the basic principles as a design philosophy, engineers will be far more informed of the priorities and options available to them and are more apt to apply them. The PHA session is an efficient time to conduct an assessment of whether the design and intended operation has been reduced to the lowest common denominator considering inherent safety concepts.

The intent is to find a smarter solution to the classical conflict between the 'added costs' of providing safety into a process design. It is often possible to not only find solutions that balance costs, risks, and benefits, but to find solutions that greatly lower risk at reduced cost and increased benefits. The difference is often in the understanding of the principles of what constitutes a hazard and the classical options (inherent safety principles) available for risk reduction. The benefits of risk reduction and improved operability may be greatly outweighed by the costs of design or operating changes if considered in the stages of concept or early design engineering.

III. Inherent Process Safety Considerations

The general philosophy is illustrated in the Inherent Process Safety Process Flow Diagram in Appendix A. PHA teams can employ this simple flow chart, along with checklists of ideas for each of the three key concepts, during the session. Considerations can be documented in the PHA worksheets as comments or possible ideas for further consideration so as to not lose the ideas while not spending an extraordinary amount of additional time in the meetings. Simple is best since the creative aspects of the PHA process will prevail, but some guidance is necessary.

For inherent safety, while prevention, detection, and mitigation are all considered, the emphasis should be on prevention. For example, moving the proposed location of a flammable liquid storage tank away from a public fence line may greatly reduce the consequences of a release and may reduce or eliminate the costs of providing the added protection systems required if it is not.

Inherent safety includes the consideration of more than just design features of a process. Inherent safety principles include human factors, in particular the opportunities for human error given the design and operating conditions and parameters. Finding an error-likely situation, such as controls being too difficult to access or too complicate, and working to reduce the clutter and confusion or to improve the accessibility to reduce the chance of a human error is an example of inherent safety in action.

Inherently safer design concepts include the following key ideas:

1. **Hazard Elimination:**

- **Concept** - eliminate hazards as a first priority (rather than accepting them and mitigating them as a risk reduction strategy once they exist);
- **Potential Methods** -

- Eliminate the hazardous material
- Substitute a non-hazardous material
- Discontinue the operation

2. **Consequence Reduction:**

- **Concept** - where hazards cannot be completely eliminated, find less hazardous solutions to accomplish the same design objective by focusing on the consequences;
- **Potential Methods** -
 - Reduce the quantity of the hazardous material
 - Provide a curbed area with a drain to contain and evacuate a spill and produce a smaller pool area of a spill
 - Separate the operation by adequate spacing to reduce exposure to adjacent operations and personnel

3. **Likelihood Reduction:**

- **Concept** - where hazards cannot be completely eliminated and after consideration of consequence reduction, consider ways such to reduce the likelihood of events occurring;
- **Potential Methods** -
 - Reduce the potential for human error through simplicity of design
 - Control ignition sources
 - Provide redundant alarms

IV. Conclusions

Clearly there is room for improvement in reducing risks through more frequent and clever use of inherent safety methods. A simple, yet effective approach is needed that can be well recognized, accepted and practiced by a wide spectrum of industrial companies. Incorporating these concepts into process hazard analysis studies ensures that they are considered and is more efficient than conducting a separate review. As such, they are more likely to actually be used. One simple suggestion is a three step checklist of hazard elimination, consequence reduction, and likelihood reduction, combined with additional guidance and training for PHA team members to be better informed of process safety principles.

Inherent Process Safety PHA Process Flow Diagram

