

Center for Chemical Process Safety

**An Introduction to
Inherently Safer Design**

Revision # 1, October 19, 2009



REVISION LOG

Revision No:	Reason for Change(s):	Date:
1	Original Issue	10/19/09

Copyright © 2009 by the American Institute of Chemical Engineers. All rights reserved.

Center for Chemical Process Safety of the American Institute of Chemical Engineers
3 Park Avenue
New York, New York 10016-5991

ISBN: 978-0-8169-1063-2

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior permission of the copyright owner. AIChE and CCPS are trademarks owned by the American Institute of Chemical Engineers. These trademarks may not be used without the prior express written consent of the American Institute of Chemical Engineers. The use of this product in whole or in part for commercial use is prohibited without prior express written consent of the American Institute of Chemical Engineers. To obtain appropriate license and permission for such use contact CCPS, 646-495-1371, ccps@aiiche.org.

It is sincerely hoped that the information presented in this document will lead to an even more impressive safety record for the entire industry; however, neither the American Institute of Chemical Engineers, its consultants, CCPS Technical Steering Committee and Subcommittee members, their employers, their employers' officers and directors, warrant or represent, expressly or by implication, the correctness or accuracy of the content of the information presented in this document. As between (1) American Institute of Chemical Engineers, its consultants, CCPS Technical Steering Committee and Subcommittee members, their employers, and their employers' officers and directors, and (2) the user of this document, the user accepts any legal liability or responsibility whatsoever for the consequence of its use or misuse.

What is Inherently Safer Design?

Inherently safer design (ISD) is a philosophy for addressing safety issues in the design and operation of chemical processes and manufacturing plants. When considering ISD, the designer tries to manage process risk by eliminating or significantly reducing hazards. Often, the traditional approach to managing chemical process safety has accepted the existence and magnitude of hazards in a process, and incorporated hardware, procedures, and management systems to reduce process risk. Where feasible, ISD provides more robust and reliable risk management, and has the potential to make the chemical processing technology simpler and more economical by eliminating the need for expensive safety systems and procedures. However, when one considers all of the multiple risks associated with any technology, including chemical processing, it is unlikely that any process or plant design can eliminate *all* hazards and risk. A combination of inherent, hardware, procedural, and management systems will always be required to adequately manage all process risks.

ISD addresses the immediate impact of single events (chemical accidents) on people, the environment, property, and business. In a chemical processing plant, this generally means the immediate impacts of fires, explosions, and the release of toxic materials. In many cases, an inherently safer design will also be beneficial for other types of process risk - for example, environmental risk, chronic health risk, or risk to consumers or users of a product. But this is not necessarily true - for example, a non-flammable solvent may be inherently safer from a fire and explosion risk viewpoint, but it may be a serious environmental contamination hazard, or it may be a chronic health hazard. While engineers recognize the potential benefits of ISD in managing other types of process risk, the main intent of ISD is to reduce the frequency and potential impact of chemical plant accidents - fires, explosions, and acute toxic exposures. Therefore, the application of ISD is one consideration in the selection of process and product technology, but the decision about what technology option is best overall must consider all risks.

History of ISD

The concept of ISD is not really new, and it is not really unique to the process industries. Technologists have always recognized the value of eliminating or reducing hazards. Applying ISD without calling it by that name, they simply considered it to be good design. For example, when a family of stone age cave dwellers decided to move to a cave higher above the river following a flood, they were practicing ISD by eliminating the risk of having their home flooded. They could have stayed in their old cave and managed the risk in other ways - for example, by building a dike around the cave mouth (hardware), or by assigning a family member to monitor the river level and warn everybody to move themselves and their possessions to higher ground when a flood was imminent (procedural).

The specific terminology "Inherently Safer Design" came into use in the process industries in the 1970s. Following a 1974 hydrocarbon vapor cloud explosion at

Flixborough, England (Figure 1), Trevor Kletz, a senior safety advisor for ICI, questioned the need for such large quantities of flammable or toxic materials in a manufacturing plant, and the need for processing at elevated temperature and pressure. Kletz suggested that industry should re-direct its risk management efforts toward elimination of hazards where feasible. Instead of devoting extensive resources to safety systems and procedures to manage the risks associated, industry could try to identify process modifications which reduce or eliminate hazards - reducing the quantity of hazardous material, using less hazardous materials, developing technology which operates at less severe conditions. Kletz and others in the chemical industry established a set of principles for ISD, and provided many examples of its implementation. In 1996, the Center for Chemical Process Safety (CCPS) published a landmark book, *Inherently Safer Chemical Processes: A Life Cycle Approach*, compiling up to date information on industry thinking on ISD. In 2009, CCPS published a second edition of this book, incorporating the latest developments on ISD based on more than a decade of additional industrial experience¹.



Figure 1: Dutch State Mines Nypro Plant in Flixborough, UK after the deadly 1974 explosion.

2.2 Inherently Safer Design Basics

in·her·ent: Adjective. Existing as an essential constituent or characteristic; intrinsic. From the Latin *inharens*, *inhaerent-*, present participle of *inhaerere*, to inhere.*

What do we mean by inherently safer design? One dictionary definition of “inherent” is “existing in something as a permanent and inseparable element.” This means that safety is built in to the process, not added on. Hazards are eliminated, not controlled, and the means by which the hazards are eliminated are so fundamental to the design of the process that they cannot be changed or defeated without changing the process. In many cases this will result in simpler and cheaper plants. If extensive safety systems are required to control major hazards, they will introduce complexity to a plant, along with cost - both in the initial investment for the safety equipment and also for the ongoing operating cost for maintenance and operation of the safety systems.

* Definition taken from *The American Heritage® Dictionary of the English Language, Fourth Edition* Copyright © 2000 by Houghton Mifflin Company.

Because the philosophy of ISD is to eliminate or reduce the hazard of a process, it is important to understand what we mean by the word “hazard”. The Center for Chemical Process Safety (CCPS) has defined hazard as “an inherent physical or chemical characteristic that has the potential for causing harm to people, the environment, or property.”² Hazards are intrinsic to a material or its conditions of use. Some examples of hazards are:

- Chlorine is toxic by inhalation
- Gasoline is flammable
- High pressure steam contains a large amount of potential energy, both from its elevated temperature and also from the high pressure

These hazards cannot be changed, except by changing the material or the conditions of use.

Chemical Process Safety Strategies

Chemical process safety strategies can be grouped in four categories: Inherent, Passive, Active, and Procedural (Figure 2). In general, inherent and passive strategies are the most robust and reliable, but elements of all strategies will be required for a comprehensive process safety management program when all hazards of a process and plant are considered.

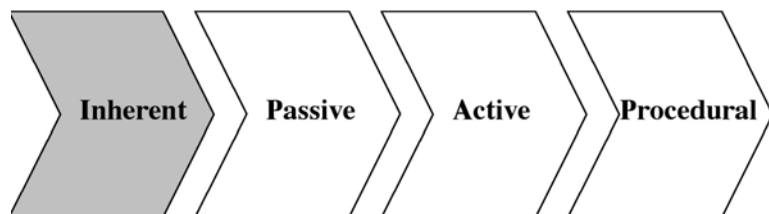


Figure 2: The four process safety strategies.

Inherent

The inherent approach to safety is, where feasible, to eliminate or greatly reduce the hazard by changing the process to use materials and conditions which are non-hazardous or much less hazardous. These changes must be integral to the process or product, and not easily defeated or changed without fundamentally changing the process or plant design. Substituting water for a flammable, and perhaps toxic, solvent as a carrier for a paint or coating - using water based latex paints instead of oil based paints - is an example. The elimination of the flammable or toxic solvent is an inherent characteristic of the product and its manufacturing process. The hazard of fire or exposure to toxic solvent vapors is eliminated, both in the manufacturing process and also throughout the manufacturing supply chain all the way to the product user.

Passive

Passive safety features minimize hazards using process or equipment design features which reduce either the frequency or consequence of an incident without the active functioning of any device. For example, if a chemical reaction which has a maximum possible pressure of 5 bar in case of a runaway reaction is done in a reactor designed to contain a pressure up to 10 bar, the maximum reaction pressure will be contained within the reactor vessel. The reactor contains the pressure because of its design and construction - the thickness and strength of the metal from which it is fabricated, the strength of the gaskets and bolts which hold it together, and its other physical components. This containment is very robust and reliable - the reactor does not need to sense high pressure and take any action to contain the pressure, and no moving parts are required to contain the pressure. But the hazard (5 bar pressure) still exists, so there is some risk that an incident will occur, and the passive strategy would be considered less robust than an inherent strategy which would eliminate or reduce the pressure. The reactor may be damaged, corroded, improperly constructed, or contain a faulty gasket, for example, and it is possible that it would fail to contain the pressure from the runaway reaction.

Active

Active safety systems include process control systems, safety instrumented systems (SIS), and automatic incident mitigation systems such as sprinkler systems to extinguish a fire. These active systems are designed to sense a hazardous condition and take an appropriate action. Active systems may be designed to prevent an incident, or to minimize the consequences of an incident. For example, a tank might have a high level interlock which shuts off a pump feeding the tank and closes all feed valves - this system is designed to prevent a tank overflow. A fire sprinkler system is an active system designed to minimize the consequences of a fire - it does not prevent the fire, and may not even be activated unless a fire is detected.

Procedural

Procedural safety features include standard operating procedures, safety rules and procedures, operator training, emergency response procedures, and management systems. For example, an operator may be trained to observe the temperature in the reactor and apply emergency cooling if it exceeds a specified critical value. In general, for a high hazard system, procedural risk management systems do not, by themselves, provide adequate risk management. Human reliability is not high enough, and people often cannot diagnose a problem, determine the appropriate action, and take that action quickly enough. However, procedural safety systems will always be a part of a comprehensive risk management program - at a minimum they will be required to ensure ongoing maintenance and management of active and passive safety systems.

Designing Inherently Safer Processes

CCPS has categorized strategies for designing inherently safer processes into four groups:

- **Substitute** - use less hazardous materials, chemistry, and processes
 - Examples: an alternate synthesis chemistry for a molecule uses less toxic raw materials; water based latex paints eliminate fire, toxicity, and environmental hazards associated with solvent based paints
- **Minimize** - use small quantities of hazardous materials, reduce the size of equipment operating under hazardous condition such as high temperature or pressure
 - Examples: nitroglycerine can be made in a continuous pipe reactor with a few kilograms of inventory instead of a large batch reactor with several thousand kilograms of inventory
- **Moderate** - reduce hazards by dilution, refrigeration, process alternatives which operate at less hazardous conditions
 - Example: a combustible solid was handled as a pellet instead of a fine powder, reducing the dust explosion hazard
- **Simplify** - eliminate unnecessary complexity, design “user friendly” plants
 - Example: Old piping which was no longer needed because of process modifications was removed from a plant, making it impossible to accidentally transfer material into a reactor through that piping by operating error or leaking valves

ISD and the Process Design Life Cycle

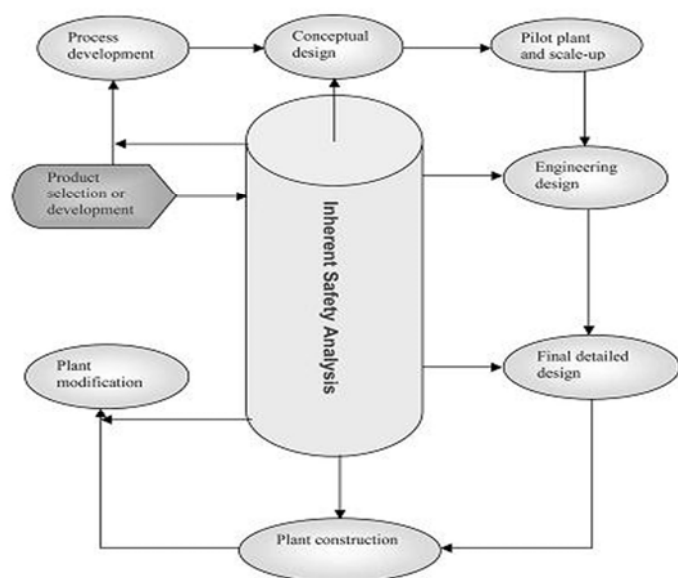


Figure 3: Inherently Safer Design in the process design life cycle.

Process design starts with the selection of a basic technology for a process operation. As the technology progresses through process development, conceptual plant design, scale up, engineering and detailed plant design, plant construction, startup, and ongoing operation and future modification, different kinds of choices and decisions are required by chemists, engineers, and other technologists (Figure 3). The philosophy of ISD applies at all stages, but the available options change. The best opportunities for implementation of inherently safer design are early in product or process research and development. At this point, there has not been any commitment to a

particular technology, resources have not been expended on research and development which would have to be done over again, potential customers have not committed to using products produced by a certain technology and developed their processes to fit this product, and capital has not been committed to build a plant to implement a particular technology. As the process moves through the life cycle, it becomes more difficult to change the basic technology. However, it is never too late to consider ISD - but options for implementation may be more limited in an existing plant. To illustrate how ISD can be applied at various levels of process development and design, disinfection of drinking water will be used as an example process.

Selection of basic technology

There are many ways to disinfect water - for example, chlorination, ozone, ultraviolet light, radiation, and others. These various technologies have differing ISD characteristics relative to different hazards of concern. For example, chlorine is toxic and may produce hazardous chlorinated organic materials in water containing certain organic precursors. Ozone and ultraviolet light provide disinfection at the point of treatment, but do not have residual activity should the water be contaminated downstream of the treatment plant. To consider ISD for basic technology selection, the decision maker must understand all hazards of concern and the inherent safety characteristics of the available process options relative to those hazards.

Implementation of the selected technology

Once the basic technology has been selected, there may be many options available for actual implementation of that technology. Using the water treatment example, assume that chlorination technology has been selected. Now the process designer has to decide how chlorination will be implemented. Some options he might consider include elemental chlorine gas, sodium hypochlorite, or solid chlorinating agents. Each option has specific ISD characteristics relative to various hazards of concern. The designer must also consider other factors such as economics, feasibility of the technology, state of development (proven technology, a new process which has never been used, or somewhere in between), and other risk concerns (environmental, chronic health, etc.).

Plant design

At this point in the process life cycle, the designer must consider ISD for a specific plant design. Factors might include:

- Location of the plant relative to surrounding population, in-plant occupied areas, sensitive environmental areas, etc.
- general layout of the equipment on the selected plant site
- number of parallel systems and size of those systems (one big plant, or two or more smaller plants, for example)

If we assume that the designers of this particular water treatment system have decided that disinfection using gaseous chlorine is the optimum process, ISD should be considered when determining where the facility is located in the community, where the chlorine is stored and handled on the site once the site has been selected, the number and size of the water chlorination systems, etc.

Detailed equipment design

The designer should consider ISD in the detailed design of each piece of equipment in the plant. There are many options in the design equipment such as heat exchangers, chlorine vaporizers, and other devices that might be included in the water treatment plant. Different equipment designs will have different ISD characteristics - for example, the inventory of hazardous material in the equipment. Also, the detailed layout of the equipment will impact things such as the length and diameter of piping containing hazardous materials. Consideration of human factors in the design of equipment, to minimize the potential for mis-operation and human error, will also result in an inherently safer plant.

Operation

Once a plant is built, ISD should be considered in the development of operating procedures and maintenance procedures. These must be clear, logical, and consistent with actual human behavior. Also, the plant should consider ISD options throughout the operational lifetime, particularly when modifications are made, or if new technology becomes available.

Some ISD Issues

ISD is not a magic bullet which will make all potential risk associated with chemical processing go away. For example, in many cases it is not possible to eliminate or reduce the hazard because the characteristic of a material or technology which makes it hazardous is the same as the characteristic which makes it useful.

- Jet airliners typically travel at about 600 miles per hour. This is what makes them useful - they can transport you half way around the world in less than a day. But that speed also makes them hazardous - an airplane traveling at 600 miles per hour has a large amount of kinetic energy which can cause major damage if it hits something, as well as likely killing all of the passengers.
- Gasoline is flammable, and has the potential for a major fire. But the flammability of gasoline is also why gasoline is useful - it stores a large amount of energy in a small mass of material making it a valuable transportation fuel.
- Chlorine is toxic. This makes it hazardous to most life, including people and animals. But this is also what makes it useful for killing pathogenic organisms in drinking water so that people can drink the water safely.

For these and other hazardous materials or technologies, the important factor in attaining the benefits of the technology and managing the hazard is control. In some cases there may be alternative technologies which are less hazardous or which are easier to control. But, for many technologies, there are no inherently safer technologies, those technologies are not economically feasible, or other risks (environmental, chronic health risks) are important enough that society chooses to use a technology which is less inherently safe. In these cases, we must rely on passive, active, and procedural safety strategies to manage the risk. These strategies can be highly effective - travel by airplane is extremely safe despite the significant inherent risks of flying. This is because of the highly effective safety management systems in place in the air transport system.

Every technology has multiple hazards. As an everyday example, consider automobile travel. Hazards include the speed of the car (kinetic energy), flammable fuel, toxicity of exhaust gases, hot surfaces in the engine, a pressurized cooling system for the engine, electricity, and others. For a chemical process, hazards might include acute toxicity, flammability, corrosiveness, chronic toxicity, reactivity, adverse environmental impacts, and others. The statement that a process is inherently safer can only be in the context of one hazard, or perhaps several specific, but not all, hazards. It is highly unlikely that any

technology will ever be inherently safer with respect to all possible hazards. Any change to a technology designed to reduce one or more hazards will also impact other hazards, perhaps such that these hazards will be increased or new hazards will be introduced.

Chlorofluorocarbon (CFC) refrigerants provide an example of ISD conflicts. When first developed in the 1930s, CFCs were considered to be safer alternatives to existing refrigerants such as ammonia and light hydrocarbons (the term “inherently safer” was not in use at that time). CFCs have low acute toxicity and are not flammable. Toward the end of the 20th century, the adverse environmental impacts of CFCs were recognized, and many of them have been phased out. But, CFCs are still inherently safer than many alternatives with respect to flammability and acute toxicity hazards. Society has decided that the previously unknown hazard of adverse environmental impact is unacceptable, and is willing to apply passive, active, and procedural risk management strategies to manage the hazards associated with CFC replacements for refrigeration systems.

Different populations of potentially impacted people may perceive the inherent safety of technology options differently. For example, for a process which requires relatively small quantities of chlorine gas, a plant may have a choice between supply in 1 ton cylinders or 90 ton railroad tank cars. A neighbor located several miles away from the plant would consider the 1 ton cylinder supply to be inherently safer because it is unlikely that a leak would impact him at that distance. On the other hand, the plant operators would have to connect and disconnect cylinders 90 times for every one time they would have had to connect and disconnect a railroad car. They would consider the railroad car to be inherently safer because they would be impacted by any release, even a small one. The operators would have a much higher frequency of relatively high risk operations - connecting and disconnecting hoses which could potentially contain chlorine. Of course, these hazards can be managed with procedures, personal protective equipment, and other safety management systems, but these are not inherent. Both the neighbor and the operator are correct in their perception of the ISD characteristics of the chlorine supply options, but they are concerned about different kinds of incidents. The challenge for the designer of the system is to understand these conflicting requirements and make an intelligent choice, including consideration of the entire risk management system (inherent, passive, active, and procedural).

It is also important to consider whether an ISD option actually reduces risk or transfers it somewhere else, perhaps increasing overall risk. A plant might reduce the size of a hazardous material storage tank at the site, reducing inventory and site risk. But use of the smaller tank may require a change from shipment of the material to the plant from railroad tank cars (typically about 300,000 pound shipments for many materials) to trucks (typically about 30,000 pound shipments) because the smaller tank cannot contain more than a truck load of material. Now there will be 10 times as many shipments, and they will go by road rather than by rail. Depending on the specific characteristics of a particular plant location, road shipment may be more hazardous. While the site risk is reduced, the overall risk to society may actually be increased.

Implementing Inherently Safer Design

How do we incorporate inherently safer design philosophies into the design and operation of chemical processing plants? The best answer is to start early in the life cycle, and never stop (Figure 4). The greatest opportunities for fundamental changes to processes occur early in the process life cycle, during initial process conception and early development. At this stage, the researcher may have opportunities to select less hazardous raw materials and intermediates or less hazardous chemical synthesis paths from among the many options which might be available. However, it is never too late to consider inherent safety. There are many published reports of significant inherent safety improvements in plants which have been operating for many years.

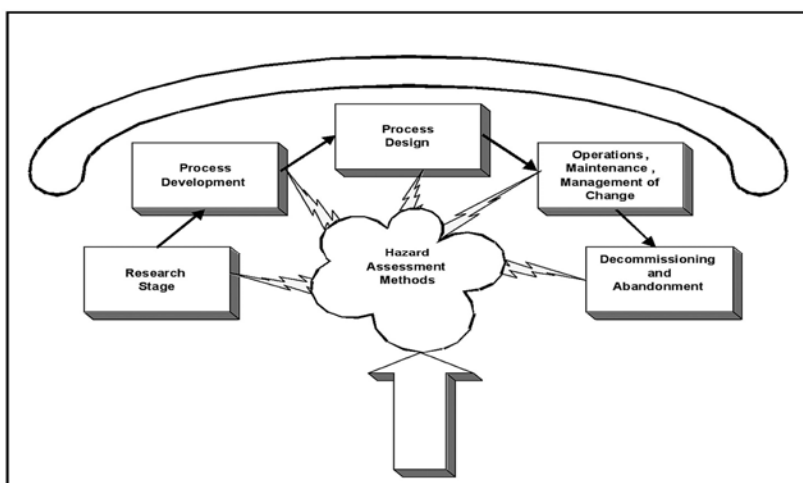


Figure 4: Hazard Assessment at various stages in the process life cycle.

The best opportunity to consider inherently safer design at all stages in the process life cycle is to incorporate inherent safety considerations into the process safety reviews that are normally done at these stages in the life cycle. CCPS and others have published checklists which are useful in doing this. In the new 2nd edition of the CCPS book on inherently safer design, these checklists are significantly improved. And, inherently safer design philosophy can be considered in the course of a process hazard analysis, in determining how to respond to an identified hazard. The PHA team is challenged to think about ways to eliminate or minimize hazards, rather than accepting that the hazard exists and focusing its efforts on controlling that hazard. The team should ask the following questions, in this order, once it has identified a hazard:

1. Can the hazard be eliminated?
2. If not, can the magnitude of the hazard be significantly reduced?
3. Do the alternatives identified in questions 1 and 2 increase the magnitude of any other existing hazards, or create new hazards? If so, consider all hazards in selecting the best alternative.

4. What technical and management systems are required to manage the hazards which inevitably will remain?

Designers and PHA teams often skip directly to the 4th question, identifying systems to manage hazards whose existence is accepted and believed to be unavoidable. This may be true in many cases, but no PHA team will ever eliminate or reduce a hazard if it does not ask if this is possible. PHA teams should challenge themselves to eliminate or reduce hazards, and then, only if this is not possible, shift to designing systems to manage risk from hazards which cannot be eliminated.

Summary

The designer and operator of a chemical manufacturing process should consider ISD options throughout the process life cycle, from initial conception through research and development, plant design, construction, operation, modification, and eventual shutdown. Usually the best opportunity for implementing ISD is early in research and development before significant resources have been expended in process or product development, and before a plant has been built. The complete process and product life cycle also needs to be considered to avoid local optimization and transfer of risk from one sector of the overall economy to another. This means consideration of raw materials, the manufacturing process, transportation, storage at all stages in the supply chain, end use, and the safety consequences of changing technology - demolition of old facilities and construction of new ones.

All hazards must be considered so that informed decisions can be made about conflicting goals and impacts. Other factors must also be considered - economics, resource allocation (including capital, research and development resources, operating costs), the feasibility, reliability, and effectiveness of other process risk management features (passive, active, procedural). This may result in different choices for different situations, even for the same technology. In a different environment, the relative importance of different hazards or other factors may be different, leading to a different choice about the optimal technology.

About CCPS

Just after midnight on December 3, 1984, water contamination of a tank of methyl isocyanate in Bhopal, India initiated a series of events that led to a catastrophic toxic release, killing more than 3000 residents and injuring over 100,000.

In February of 1985, leaders from 17 of the leading chemical and petroleum companies asked the American Institute of Chemical Engineers (AIChE) to lead a collaborative global effort to eliminate catastrophic process incidents by:

- ADVANCING state-of-the-art process safety technology and management practices
- SERVING as a premier resource for information on process safety
- FOSTERING process safety in engineering and science education
- PROMOTING process safety as a key industry value

On March 25, 1985, AIChE formed the Center for Chemical Process Safety (CCPS) with charter member companies. In the years that followed, CCPS has been the world leader in every area of process safety information, with over 60 guideline and resource books in print, and an ever-growing web knowledge base. CCPS membership now exceeds 100 companies, headquartered in more than 15 companies in four continents and operating in every part of the world.

View the CCPS book catalog www.wiley.com/go/ccps

Learn about CCPS membership www.aiche.org/CCPS/Corporate/index.aspx

Browse the CCPS Web Knowledge Base

www.aiche.org/CCPS/Resources/KnowledgeBase/overview.aspx

Attend CCPS events www.aiche.org/CCPS/Conferences/index.aspx

Contact CCPS ccps@aiiche.org or +1.646.495.1372

¹ Center for Chemical Process Safety. *Inherently Safer Chemical Processes: A Life Cycle Approach*. 2nd Edition. Hoboken, NJ, John Wiley & Sons, 2009.

² Center for Chemical Process Safety. *Guidelines for Hazard Evaluation Procedures*. 3rd Edition. Hoboken, NJ, John Wiley & Sons, 2008.



**Become a corporate member
of AIChE's**

**CENTER FOR CHEMICAL
PROCESS SAFETY**

CCPS members share a vision of a safer process industry

Working together, The Center for Chemical Process Safety (CCPS) and its member companies pool the resources, expertise, and knowledge needed to develop superior process safety management and technology. Members guide research initiatives and enjoy access to the latest research findings by participating in the development of CCPS guideline, concept, and safety alert publications. Members also contribute to and benefit from CCPS' extensive and coded databases of safety information.

Representatives may serve on over 15 subcommittees and attend four Technical Steering Committees each year, as well as world-class conferences. They join a community of peers with whom they can confidentially discuss safety concerns and benchmark programs.

CCPS membership makes good business sense

CCPS members share the costs and benefits of research, so every dollar goes farther. On average, CCPS members obtain safety R&D worth 70 times the value of their contribution. What's more, membership delivers over \$1.5 million in projects annually. Members of CCPS include major petroleum, chemical and pharmaceutical companies, as well as other manufacturers and users of chemicals, research centers, engineering contractors, safety consultants, insurance firms, and government agencies. CCPS members also benefit from:

- A large, effective network of colleagues who can help each other solve problems
- Learning from other industry experts
- Participating in development of process safety guidelines used by all of industry
- Exclusive programming at four Technical Steering Committee meetings per year, featuring workshops and special invited speakers.
- Free copies of new CCPS books and discounts on all other CCPS books.
- Preventing catastrophic process safety incidents

Membership contributions depend on the world value of the member's sales. CCPS and AIChE are both tax-exempt educational scientific organizations under IRS code 501 (c) (3), Federal I.D. No. 13-1623892. For more information on CCPS membership, contact CCPS at +1.646.495.1372 or ccps@aiiche.org.

CCPS MEMBERS: A POWERFUL ALLIANCE