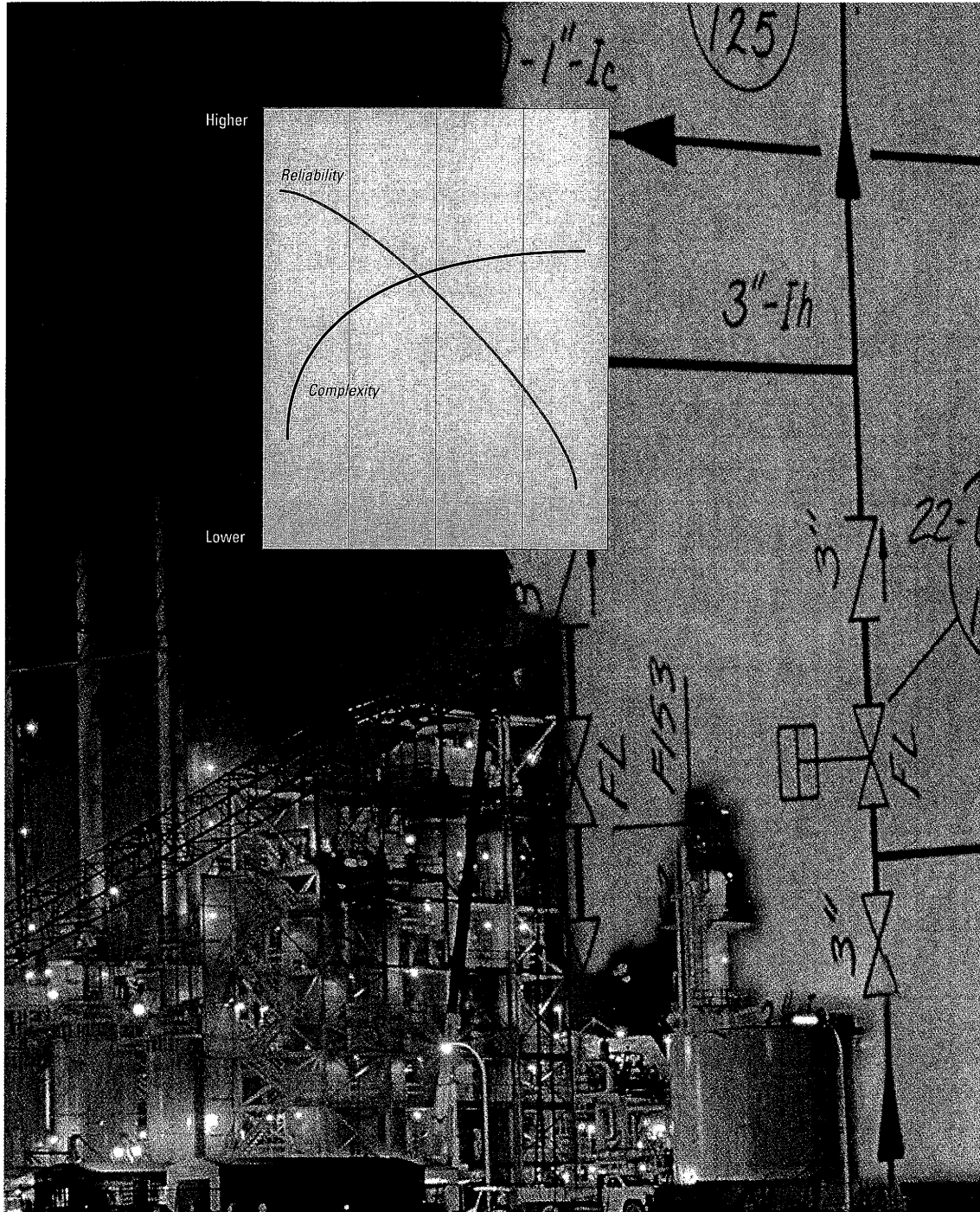


Interfaces



Arthur D Little

RISK-BASED DESIGN:
A Cost-Effective Route to Enhanced
Process Safety

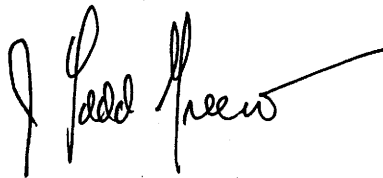
A Word To Our Readers

If you are responsible for the safe operation of industrial processes, you know that successful risk reduction means implementing measures that satisfy the concerns of all of your stakeholders while meeting the competitive needs of your business. Two factors, in particular, can help companies make sound—and cost-effective—decisions about managing risk: accurate data about hazards and risks, and the systematic use of those data, early and often, in the design process.

In this issue of *Interfaces*, Georges Melhem and R. Peter Stickle of Arthur D. Little's Environmental, Health, and Safety Consulting business present a rigorous, systematic approach to integrating risk and safety thinking into process safety design. The approach they outline enables businesses in process industries to make better, more cost-effective decisions about reducing risk. It opens the door to innovative solutions for process safety design challenges. And its outcomes help companies meet regulatory requirements for documenting how safety issues are addressed in process design.

At Arthur D. Little, we have been helping organizations around the world apply the best technology and management knowledge to environmental, health, and safety challenges for over 50 years. We hope you find this discussion valuable, and we welcome your comments on this topic and on your experiences with process safety design.

Sincerely,

A handwritten signature in black ink, appearing to read "J. Ladd Greeno". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

J. Ladd Greeno
Senior Vice President and Managing Director

Risk-Based Design

A Cost-Effective Route to Enhanced Process Safety

Nine Steps to Cost-Effective Risk-Based Design

Focus: The Concept of Risk

Case Study: Reducing Mitigation Costs

Guidelines for Risk Tolerability

Focus: Quantitative Analysis—

How Much is Enough?

Focus: Risk Tolerability Criteria

Design Solutions: Making the Right Decision

Focus: Cost-Effective Risk Reduction

Case Study: Evaluating Risk-Reduction Alternatives

Meeting Stakeholder Needs

Making decisions about risks is intrinsic to process safety design. Traditionally, to create a core design for a new process, engineers examine how the system could break down, determine the impact of system failures, and estimate their likelihood. Evaluating these issues produces a continuous stream of risk-related design decisions. All too often, however, these decisions have been based on perceptions, not measurements, of risk.

The result can be an unsystematic and incomplete design process, leading to inadequate, overly costly, or incompatible risk-reduction solutions. Moreover, when the process for determining the design basis lacks consistency, it is difficult to know whether the same risk-management philosophy supports all of a company's risk decisions.

Now, by basing process safety design and decision-making on a systematic, risk-based approach, companies can improve their

ability to understand and reduce risk, control process safety costs, and protect their investments and reputations. As risk-based thinking—already well established in other business areas—gains ground in process safety, it can also help managers translate the technical complexities of risk analysis into clear messages about risks and options.

Nine Steps to Cost-Effective Risk-Based Design

Working with leading companies and industry organizations in the process industries, Arthur D. Little has developed a risk-based design approach with a disciplined, highly consistent thought process and flexible implementation options (Figure 1). This approach integrates safety where it belongs: at each stage in the design cycle, including laboratory, pilot, production design, and operation. The technique can be grafted onto current design approaches because it derives from process design engineers' characteristic problem-solving methods. Moreover, it can be applied to all design cases, from the simplest to the most complex.

Equally important, systematic risk-based design helps engineers focus safety thinking at the earliest design stages, where the most cost-effective solutions to safety

Systematic risk-based design leads to creative risk-reduction solutions.

challenges tend to be found. And while it supports a disciplined thought process, it also opens the door to greater creativity and innovation in risk reduction by increasing the range

of possible solutions and bringing attention to risk-reducing options that may be overlooked in traditional approaches.

Our approach traces the most efficient possible path through the risk-assessment process. In the nine steps that follow, review and reassessment loops come into play only as needed.

1. Identify failure scenarios. When designers have established a core process design, they can address failure scenarios that might require a process safety system. Process hazard analysis techniques and past experience provide information on possible failure scenarios.

The Concept of Risk

In everyday conversation, people use words such as *risk*, *hazard*, and *danger* interchangeably. For example, crossing the street without looking both ways might be described as “risky,” “hazardous,” or “dangerous”—all meaning pretty much the same thing.

In chemical process safety design, risk is defined more precisely in terms of the *likelihood* and *consequences* of incidents that could expose people, property, or the environment to the harmful effects of *hazards*. As defined by the Center for Chemical Process Safety of the American Institute of Chemical Engineers:

- *Hazards* are potential sources of harm. Examples of hazards include a reactor vessel under high pressure, a very corrosive chemical, and an improperly sized emergency relief valve.
- *Likelihood* is determined in terms of two factors: frequency (How often does this happen?) and probability (What are the odds that it will happen?).
- *Consequences* cover specific outcomes or impacts of an incident, such as a toxic vapor cloud that spreads beyond the plant boundary into a neighborhood or an explosion that causes a fatality.

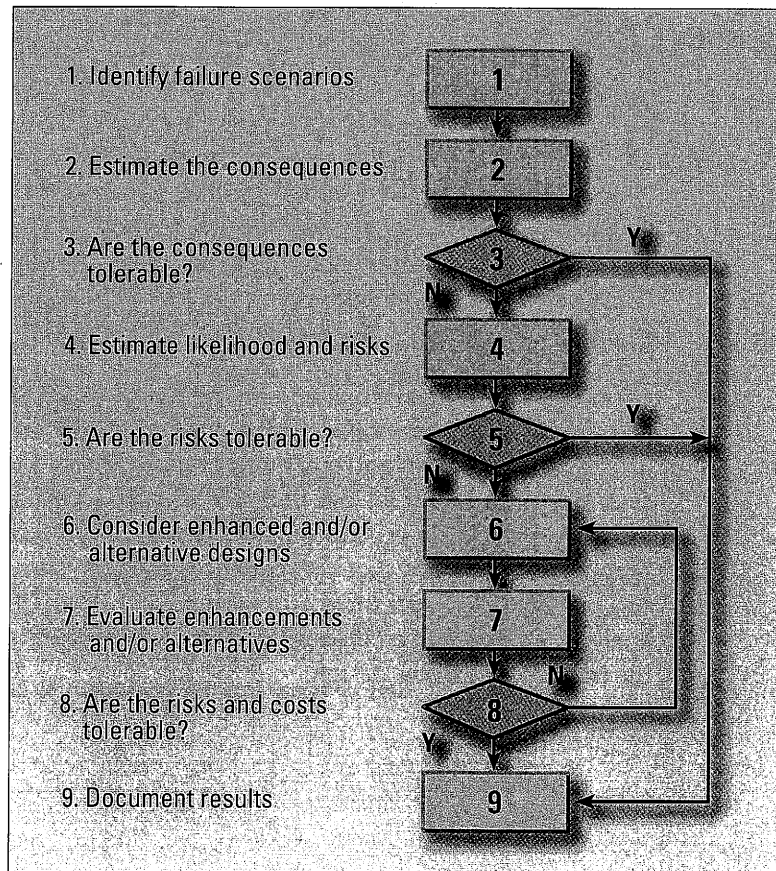
Risks cannot be completely eliminated from industrial processes any more than they can be eliminated from other activities. Instead, the goal of process safety is to consistently reduce risk to a level that can be tolerated by all concerned—facility staff, company management, shareholders, surrounding communities, the public, industry groups, and government agencies. For this reason, defining what constitutes “tolerable” and “intolerable” risk is a critical part of risk-based design.

2. *Estimate the consequences.* In this step, designers establish the consequences of the failure scenarios identified in Step 1. These scenarios typically involve quality, safety, health, and environmental impacts. Consequences of interest include fires, explosions, toxic materials releases, and major equipment damage. Some potential consequences can be determined through direct observation, engineering judgment, or the use of qualitative consequence criteria. Other cases require experimentation or analytical approaches such as the calculation of maximum hazard distances of vapor cloud dispersion.

3. *Determine the tolerability of the consequences.* Accomplishing this requires guidance from established tolerability criteria. These include company-specific criteria, engineering codes and standards, industry initiatives such as Responsible Care®, and regulatory requirements.

4. *Estimate likelihood and risks.* Estimates of likelihood rest upon an understanding of how, and how often, failure scenarios such as those identified in Step 1 might occur. When historical data are available about equipment and processes, these data can be used to estimate failure scenario frequency. When data are lacking, methods such as fault tree analysis help in developing quantified estimates. Measures of risk are arrived at by combining risk and consequence estimates. A detailed review of methods for combining likelihood and consequence estimates to obtain risk measures can be found in process safety literature. Some cases can be

Figure 1: The Technique for Safety Design Basis Selection



resolved through comparisons with similar systems or through the use of qualitative tools such as risk matrices. Others will require quantified approaches such as risk profiles and risk contours.

5. *Determine risk tolerability.* Determining risk tolerability means asking “Can we—and our stakeholders—tolerate this level of risk?” Guidance on tolerable levels of

Most risks cannot be eliminated, only reduced to levels that stakeholders accept.

risk can be gained from established risk criteria. If the criteria, when applied, indicate a tolerable level of risk, then the design of the process or the emergency relief system is satisfactory from a risk standpoint. If the criteria indicate

intolerable risk, the next step is to reduce risk through further design refinements.

6. *Consider enhanced and/or alternative designs.* This step is an opportunity to consider the entire process design and define changes that can reduce risk to a tolerable level. CCPS has classified risk-reduction concepts, in declining order of reliability, as follows: inherently safer, passive, active, and procedural.

7. *Evaluate enhancements and/or alternatives.* A design change intended to reduce risk can introduce new failure scenarios and new risks. Therefore, the evaluation of design changes should treat these changes as an integral part of the process. Following Steps 1 through 4, the review should re-estimate process risk. The review should also estimate the cost of the proposed changes.

8. *Determine tolerability of risk and cost.* As in Steps 3 and 5, established risk criteria can provide guidance on risk tolerability. Cost becomes an issue in this step because, like all designs, process safety designs must meet business criteria. Coupling estimates of cost and risk reduction provides a basis for assessing the cost/benefit tradeoff of each alternative design or mitigation solution. The cost/benefit analysis can be qualitative or quantitative. A quantitative approach is especially useful when a large number of competing process safety systems are being considered. If the analysis yields tolerable risk and cost for a design option, the results should be documented (Step 9). If not, it may be necessary to consider design enhancements and alternatives (Steps 6 through 8).

9. *Document results.* The failure scenarios and associated consequence, likelihood, and risk estimates developed during this process document the design basis for process safety systems and emergency relief systems. Documentation retains essential information for risk management situations such as hazard evaluations, management of change, and subsequent design projects. When the findings from Step 3 or Step 5 show that consequences and risk meet tolerability criteria, results still need to be documented. Doing so will cut down on needless repetitions of the analysis and ensure that design or operational changes reflect an understanding of the baseline risk of the design.

Case Study: Reducing Mitigation Costs

A global chemical manufacturer investigated “best available technology” options for risk reduction in two processes and found that optimal results would require a \$2.5 million capital expenditure. Seeking a fresh angle on the technology and science of risk reduction, the company asked Arthur D. Little to help its technical staff explore cost-effective alternatives for reaching an equal—or superior—level of risk reduction.

Working closely with the company’s scientists and process engineers, we used a risk-based approach to develop and rank risk-reduction measures and their costs. The approach, which included the evaluation of areas such as the design basis for pressure relief system sizing, drew on recent advances in emergency relief system and mitigation design. After collaborating with the company team on the development of risk matrices for risk-reduction alternatives, we helped present the alternatives to their senior management. The matrices showed that the most significant risk reduction could be achieved at a cost of \$200,000, and that almost no further reduction could be achieved by spending additional money.

The company immediately benefited from this work by achieving optimal risk reduction in two processes for one-tenth of the original cost estimate. The study also provided documentation for meeting new U.S. process safety management regulations. Most important, the savings increased the capital available for technology upgrades and risk reduction in the company’s other processes.

Guidelines for Risk Tolerability

Underlying this entire approach is the understanding that risk levels range along a continuum. In most cases, risks cannot be eliminated, only reduced to a level that everyone who has a stake in the activity or process finds acceptable. Because attitudes about the tolerability of risks are not consistent, there are no universal norms for risk tolerability. What your stakeholders view as a tolerable risk will depend on a number of factors, including the following:

- *The nature of the risk.* Is it a voluntary risk, one that those who are at risk accept as part of a choice? Or is it involuntary?
- *Who or what is at risk.* Does it affect a single person or many people? What about the surrounding environment? Is it an industrial landscape already altered by past uses, or a pristine or prized natural setting? Are areas such as schools or residential neighborhoods or resources such as water at risk?

Quantitative Analysis: How Much is Enough?

A systematic approach does not necessarily mean a quantitative one. Quantitative analysis is most time- and cost-effective when it is used selectively. In many simple design situations, qualitative approaches are sufficient for selecting process safety system design bases. More complex design cases may occasionally require quantitative risk analysis. But even then, quantitative methods should only be used up to the point where a decision can be made.

For example, consider a company that has toxic impact criteria limiting off-site vapor cloud concentrations to a specific, quantified level. By performing vapor-cloud dispersion calculations (through a quantitative characterization of the consequences of specific releases), the company can determine whether specific loss-of-containment scenarios associated with specific failures exceed the toxic impact tolerability criteria. If the scenario consequences do not exceed the criteria, then there is no need to continue with an analysis of event likelihood or further risk quantification.

- *The degree to which the risk can be controlled or reduced.* Process safety design, and especially emergency relief system design, focuses in large part on this issue. Making the case for a “tolerable” risk requires that the methods supporting the design basis be technically sound and defensible, clearly documented, and accurate.
- *Past experience.* Uncertainty regarding the risk impact influences the risk taker’s level of tolerance. For example, the average person understands and accepts the risk of driving an automobile but is uncertain about the risk of nuclear power generation.

Companies that have successfully established risk criteria focus on attaining consistency in their decisions about risk. These criteria typically represent levels of risk

Choosing risk criteria is a corporate responsibility and requires senior management involvement.

that the company believes will minimize impacts to continued operations. Risk criteria should also fit with a company’s philosophy and culture and match the type of analysis its engineers normally conduct in the design stage.

The selection of appropriate risk criteria is a corporate responsibility and requires the involvement and support of senior management, as it establishes the levels and types of risks the company will tolerate.

Once a company has established specific risk criteria, these can be used to check outcomes throughout the design process, at Steps 3, 5, and 8 of the approach outlined above. This iterative approach builds consistency into the process and increases the likelihood of making risk-based choices early in design—where they are often most cost-effective.

Risk Tolerability Criteria

Release Limits address the tolerability of potential release consequences by considering the amount of material that could be released. “Tolerable” quantities depend on the physical states and hazardous properties of released materials. A hypothetical release limit for gasoline, for example, might be as much as 5,000 pounds, while for chlorine, it would be only 200 pounds.

Threshold Impact Criteria for Fence or Property Line employ standard damage criteria, such as toxicity, thermal radiation, or blast overpressure, together with consequence modeling, to determine whether potential impact at the facility’s fence or property line exceeds a tolerable threshold.

Single Versus Multiple Component Failure Criteria provide a qualitative approach to how many component failures will be tolerated. For example, a company might choose to tolerate event scenarios that require three independent component failures, to conduct further analysis of event scenarios triggered by two failures, and not to tolerate events arising from single failures.

Critical Event Frequency addresses event scenarios with a defined high-consequence impact. Examples of such impacts would be a severe injury, a fatality, critical damage to the facility, or impacts on the surrounding community.

Risk Matrix Criteria use qualitative and semiquantitative frequency and severity categories to estimate the risk of an event. Events with a low risk ranking are considered tolerable.

Individual Risk Criteria consider the frequency of the event or events to which an individual might be exposed, the severity of the exposure, and the amount of time for which the individual is at risk.

Societal Risk Criteria explicitly address both events with a high frequency and minimal consequences and events with a low frequency and serious consequences. This class of criteria can be useful to companies that have recently experienced an adverse event.

Risk Matrix and Cost Thresholds can account for the risk-reduction level provided by a design enhancement and its cost. In cases where the benefit of a risk-reduction step is large and its cost is small, the way forward is obvious. In more complex situations, a risk matrix and cost threshold with definite “rules” can help clarify decision-making.

Cost-Benefit Criteria help define the amount of risk reduction expected for each dollar expended. They can be developed in conjunction with quantitative estimates of risk. In some cases, companies might use two thresholds—one for the dollars needed to achieve a tolerable risk level, and another for any further reduction beyond that level.

Design Solutions: Making the Right Decision

The best decisions about safety and risk reduction in process design bring together technical sophistication and clear business objectives. Decisions about risk should provide definite business value and fit into the business context: what is the business plan for this facility or process? They should reflect consistent thinking and standards for risk tolerability levels. And they need to be in line with an appropriate cost structure for the safety component of a process.

Decisions about risk should provide definite business value.

Understanding the core types of design choices for safety can help engineers

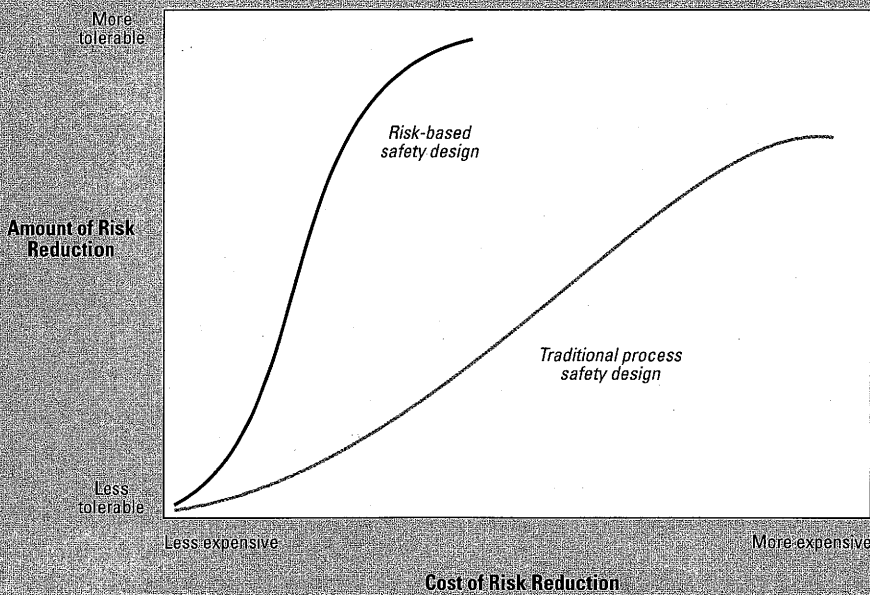
rank their options and introduce modifications where they can do the most good for the least cost. Most design solutions for reducing risk fall into one of these categories:

- *Inherently safer*—eliminates or mitigates identified hazards by substituting less-hazardous materials and process conditions. Inherently safer solutions tend to require relatively high capital costs, offset by relatively low operating costs. Examples include substituting water for a flammable solvent and reducing large inventories of hazardous “intermediates.”
- *Passive*—offers high reliability by operating without active devices that sense or respond to process variables. Like inherently safer design choices, passive systems often require a relatively high initial investment offset by relatively low operating costs. Examples include incompatible hose couplings for incompatible substances, equipment designed to withstand high-pressure hazards, and dikes that contain hazardous inventories.
- *Active*—uses devices that monitor process variables and trigger mitigation and control systems. Active systems can be less reliable than inherently safer or passive systems because they require more maintenance and more detailed operating procedures. They typically require moderate capital costs, followed by somewhat greater operating costs. Examples include check valves and regulators, pressure safety valves or rupture disks that prevent vessel overpressure, and high-level sensing devices that interlock with inlet valves and pump motors to prevent overfilling.
- *Procedural*—avoids hazards by requiring someone to take action. The capital cost of a procedural system is generally low, but operating costs, including staffing and training, can be high. Reliability, which rests on human variables such as company safety culture and the correct use and handling of mechanical devices, tends to be low. Examples of procedural approaches include manually closing a valve after an alarm sounds or carrying out preventive maintenance to reduce the likelihood of equipment failure.

Cost-Effective Risk Reduction

Incorporating systematic risk assessment in process safety design is sometimes viewed as an expensive way to achieve greater risk reduction. The reality, however, is that when risk assessment is left out of the design process, two problems are likely to occur. The system may be overdesigned, with safety protection costing more than it needs to, or the facility may be unprotected from significant, unidentified risks.

Systematic risk-based design helps companies more fully identify significant risks, rank them, and prioritize steps to address them. The result is that capital expenditures, operating expenses, staffing, and other resources are better allocated to risks, enabling companies to buy more risk reduction at a cost that is the same or less.



When deciding among the hierarchy of mitigation options, designers should avoid the “project mentality” pitfall: focusing only on minimizing capital cost. Nor can they simply select the most reliable approach. The key to successful risk reduction choices is to exploit the systematic design process’s detailed technical information about risks and hazards to judge the actual merits and disadvantages of each plausible solution. It is also important to examine the life-cycle costs of each option before making decisions (Figure 2).

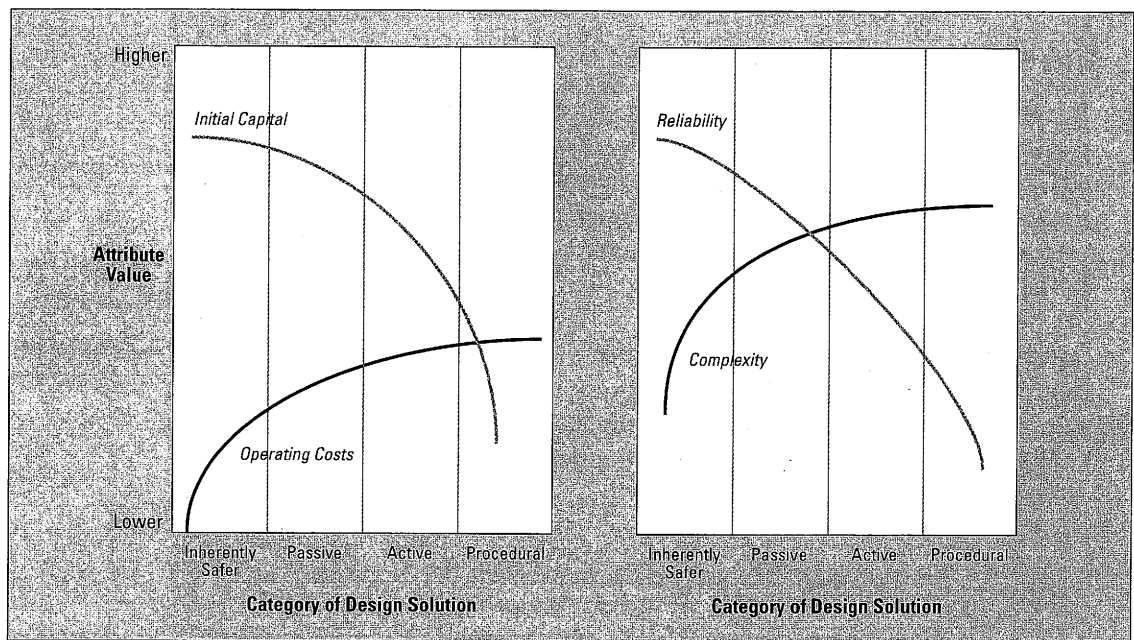


Figure 2: Comparison of Cost and Functional Attributes for Design Categories (typical trends)

Consider the case of a company that was handling a very energetic substance with a highly hazardous reaction. After several incidents, the company was now reviewing two options for reducing the risk posed by the substance. The first—total containment of the substance in a vessel rated to withstand a maximum pressure level of 1,200 psi—was an inherently safer approach. However, the cost of this vessel was very high. Furthermore, using such a vessel meant having it sit continually within the facility at a very high pressure—a hazard in and of itself.

The second option was to construct a catch system and allow the reactor to activate an emergency pressure relief system. This required a reactor vessel with a lower pressure rating and a large vessel to be used as a catch/quench tank. This approach was less expensive, but it required the facility to deal with the potential of a hazardous effluent and to address the reliability of the relief

Examine the life-cycle costs of each process safety design option before making decisions.

system. At the same time, the pressure relief/catch system was found to provide a tolerable risk level overall. The company chose to take advantage of this option's lower cost and to implement mitigation measures that helped attain a tolerable level of risk.

Case Study: Evaluating Risk-Reduction Alternatives

A facility belonging to a large chemical manufacturer was producing a family of chemicals that react vigorously with water, generating corrosive and toxic byproducts. The production process used water-cooled heat exchangers for condensing and cooling the process streams. Given the hazard potential due to exchanger leaks, the facility had embarked on a program to reduce the risk of such an event. However, the company needed a way to determine which risk-reduction option or combination of measures was the most effective.

Working closely with the company's operations and design engineers, we used elements of a risk-based approach to determine the relative benefit of various risk mitigation alternatives. These included passive solutions such as heat exchangers that use nonpressurized water, active solutions such as advanced leak-detecting sensors, and procedural solutions such as enhanced testing, inspection, and maintenance. The approach involved a qualitative estimate of the consequences of exchanger leaks, since a leak of almost any size would result in an undesirable outcome. A quantitative determination of the likelihood of such events for different risk-reduction measures was also conducted to establish the relative benefit of the various options. The results were presented to a group of engineers and managers to enable them to decide which option would meet their risk tolerability criteria. The company opted for an inherently safer solution, substituting a nonreactive coolant for water.

The selected design approach was not the least expensive alternative from the point of view of capital cost. However, because it required less maintenance, less downtime, and less administrative management, the facility could offset the capital cost with operational savings.

Meeting Stakeholder Needs

Safe design has long been a priority in the process industries. Today, process industry companies need to be certain that their stakeholders trust how they manage the environmental, health, and safety implications of industrial activities. A safe—and documented—design basis, together with a formal safety management system and safety practices, procedures, and training, is critical for providing the level of confidence required for risk management.

In recent years, regulations and industrial standards for tolerable risk have become increasingly stringent. This trend reflects a convergence of public opinion, government regulations, and industry initiatives. The momentum for controlling and reducing risk is likely to continue, with leading companies in process industries setting standards that go well beyond what is required.

At the same time, risk managers and environmental managers at many companies face unremitting pressure to run their activities “lean” and control and justify costs. Risk-based design can be a key piece in a successful company’s toolkit for reaching decisions about process safety design that integrate risk reduction and cost advantages without compromising on safety. By communicating options clearly to all concerned stakeholders and by addressing the full life-cycle cost of different options, risk-based design enhances the business value of process safety activities. Companies that are gaining the benefits of reduced risk—and reduced risk management costs—find their competitive position strengthened by lower capital costs and by a more secure franchise to operate.

Message for Managers

For companies that use a systematic, disciplined approach to incorporating risk thinking in process design, significant opportunities exist for gains in cost saving, profit protection, and risk reduction. These gains will be based on risk-reduction decisions that are smart about business issues, technically sound, and properly documented.

About the Authors

Georges A. Melhem is a Director of Arthur D. Little's Environmental, Health, and Safety business and leads the company's Safety and Risk Management Practice in North America. His areas of expertise include risk analysis, consequence analysis, thermal hazards assessment, mitigation design, hazard evaluation, computational fluid dynamics, and model development. He also manages Arthur D. Little's Thermal Analysis and Process Development Laboratory, which is primarily dedicated to experimental evaluation of chemical reactivity hazards and process optimization. Dr. Melhem received his B.S., M.S., and Ph.D. in Chemical Engineering from Northeastern University and is a member of AIChE.

R. Peter Stickles is a Principal in Arthur D. Little's Safety and Risk Management Practice. His areas of expertise include process hazard analysis, quantitative risk assessment, pre- and post-release mitigation design, and incident investigation. He received his B.S. and M.S. in Chemical Engineering from Northeastern University. He is a registered professional engineer in Massachusetts and a member of AIChE.

About Arthur D. Little

Arthur D. Little is one of the world's premier consulting firms, with offices and laboratories around the globe. Since 1886, we have worked side by side with outstanding organizations worldwide to help them expand their knowledge capital and discover new paths to sustained high performance. Across our three businesses—environmental, health, and safety consulting; management consulting; and technology and product development—we are distinguished from our competitors by the caliber of our people and the breadth and depth of our experience. We are also unique in our commitment to helping our clients reinvent their organizations, enhance their capacity for learning and change, and create lasting value.

For more information or additional copies, please contact the Director of Client Communications, Environmental, Health, and Safety Consulting, at one of the following locations:

Arthur D. Little, Inc.
Acorn Park
Cambridge, Massachusetts
02140-2390 U.S.A.
Telephone (1) 617.498.5777
Fax (1) 617.498.7019

Arthur D. Little International, Inc.
Boulevard de la Woluwe 2
B-1150 Brussels, Belgium
Telephone (32) 2.762.0731, ext. 377
Fax (32) 2.772.3666

Visit our web sites: www.arthurdlittle.com/ebs/
www.process-safety.com



0A03832-05JUM/MS/97/1987Z