ioMosaic

Minimizing risk. Maximizing potential.®

Enhancing Safety Through Risk Management

Use this Nine-Step Plan for Every Process

An ioMosaic White Paper

ioMosaic

Contents

Introduction

The handling, use, processing, and storage of hazardous materials will always present risk. The goal of process safety management is to consistently reduce risk to a level that can be tolerated by all concerned — by facility staff, company management, surrounding communities, the public at large, and industry and government agencies.

A systematic, risk-based approach to safety design is discussed below. Such an approach can help eliminate those hazards that pose intolerable risk and mitigate the potential consequences of such hazards. Guidance for identifying tolerable risk levels is also provided.

In recent years, industrial standards for tolerable risk have become increasingly stringent. This trend reflects a convergence of public opinion, government regulations, and industry initiatives. In fact, to contain long-term costs and minimize liability, many leaders throughout the process industries are setting standards for their own companies that are well more than what is required.

At the same time, managers at many chemical process companies face unremitting pressure to run their activities "lean" and control and justify costs. The ability to reach rational decisions about process safety design based on a clear understanding of both the risk-reduction options and costs can greatly strengthen a manager's ability to meet the needs of internal and external stakeholders.

The Concept of Risk

To achieve a consistent approach to risk reduction, process designers must define "tolerable" and "intolerable" risks and document how risk is addressed in the design process. To meet a company's business needs, the process safety solutions that designers propose must be as cost-effective as possible. The goal is to enable designers to answer the needs of all process-safety stakeholders, without compromising on safety or spending too much on excessive prevention or mitigation measures.

In chemical process safety design, risk is understood in terms of the likelihood and consequences of incidents that could expose people, property, or the environment to the harmful effects of a hazard. Risks that are likely to occur should be addressed; those that are unlikely to occur need not be.

For example, it is always possible to identify scenarios that would be catastrophic for the system being designed. However, process and emergency relief system (ERS) design does not necessarily need to address the worst scenario someone can imagine. Rather, a line must be drawn (or at least a gray area defined) between likely scenarios and unlikely ones.

A process might use an alkyl chloride, which is known to react vigorously with water. If water is not present at the site, there is no need to address that potential reaction scenario in ERS design. Similarly, if water is on site, but is not used in the same process as the chloride, there is still no need to ad- dress it in the ERS design. However, if water is not used in the same process as chloride, but is stored in the same, or an adjacent, storage facility, then, de-pending on the circumstances, it might make sense to include a chloride-water reaction scenario in the ERS design.

A Systematic Approach

Risk-based approaches can assist managers by encouraging a clear, consistent approach to decision-making about risks, and by providing information about safety design choices. By systematically identifying the risks and choices, companies will gain a greater degree of confidence about the ultimate management of process risk.

Among other things, when designing a process, engineers first address the technology. The core design is defined by chemistry, heat and material balances, and basic process controls. Once the core design has been determined, engineers examine ways in which the system could break down. They look at issues concerning the reliability, safety, quality control, and environmental impact of the system. They try to determine what types of failures might occur at what likelihood, and what effect such failures (often called "impact scenarios") might have.

As they answer these questions and proceed with system design, engineers are continually making risk-based decisions. But too often, their decisions are not based on measurements of risk only perceptions. Without company wide harmonization of risk-management strategies, inconsistencies in the way risks are assessed and mitigated can develop between different processes and facilities.

Case Study: Evaluating Risk-Reduction Alternatives

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

Working closely with on site operations and design engineers, we used a risk-based approach to determine the relative benefit of various risk-mitigation alternatives. The approach involved a qualitative estimate of the consequences of exchanger leaks since almost any size leak 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 allow them to decide which option would meet the facility's risk tolerability criteria. The company opted for an inherently safer solution of substituting a non-reactive coolant for water. While the selected approach was not the one with the lowest capital cost reductions in maintenance costs, downtime, and administrative complexity, it helped to offset the anticipated operating costs, making it the most attractive alternative overall.

Get Started Early

Ideally, safety should be a theme at each stage in a systematic design cycle laboratory, pilot, production design, and operations. But the most cost-effective solutions tend to emerge in the earliest design stage.

A systematic approach does not necessarily mean a quantitative one. In fact, quantitative analysis (i.e., using frequency and fault-tree analysis, consequence analysis, and so on) is most time and cost-effective when it is used selectively. In many simple design situations, such as the design of heat exchangers, a qualitative approach (i.e., a risk matrix) is sufficient for selecting the basis of a safety system. More complex processes, such as those involving chemical reactors, often require quantitative risk analysis. Even then, quantitative methods should only be used where their results can support some action or decision.

For example, consider a company for which mandated toxic impact criteria limit off-site vapor cloud concentrations to a specific, quantified level. By performing vapor-cloud dispersion calculations, the company can determine whether loss-of-containment scenarios associated with specific types of failures exceed the toxic impact thresholds. If individual scenario consequences do not exceed the off-site toxic impact thresholds, then there is no need to continue analyzing event likelihood or quantifying further risk.

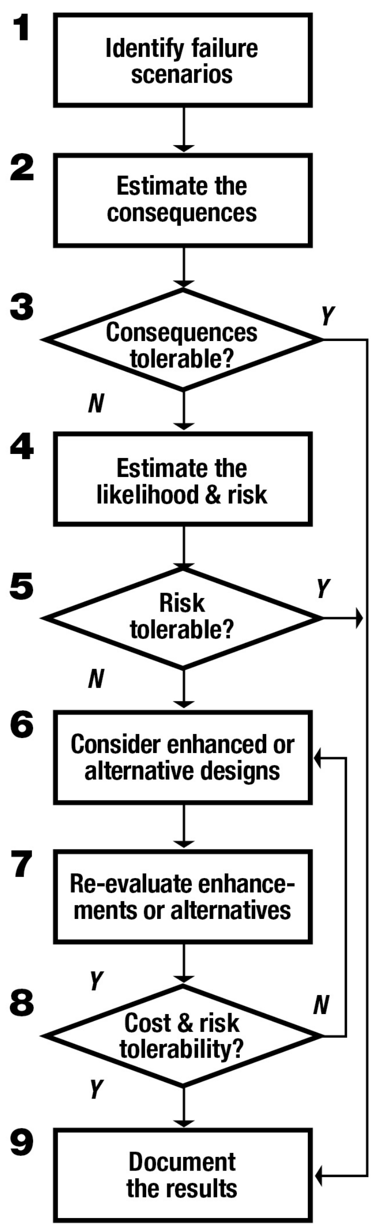

Figure 1: Using this decision tree, process engineers can systematically identify potential risks, and evaluate risk-mitigation opportunities and costs.

Nine Steps to Risk-Based Design

The technique outlined here derives from engineers' characteristic problem-solving methods and can be applied to all types of process design cases. The technique comprising a sequence of analysis and testing steps in the form of a decision tree provides for a disciplined approach and flexibility in its application (Figure 1).

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

2. Estimate the consequences. In this step, designers establish the potential consequences e.g., fires, explosions, toxic material releases, and major equipment damage that may result from the failure scenarios identified in Step 1. Quality, safety, health, and environmental impacts should be assessed.

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. Making such an assessment requires guidance from established tolerability criteria. These include company-specific criteria; engineering codes and standards; industry initiatives such as Responsible Care; and regulatory requirements. For ERS design, the potential

rise in pressure should be compared to the mechanical limits of the equipment under consideration.

4. Estimate likelihood and risks. This rests upon an understanding of the mechanism and frequency with which failure scenarios, such as those identified in Step 1, might occur. When available, historical data about the various equipment components and processes can be used to arrive at failure scenario frequency estimates.

When data are lacking, methods such as fault tree analysis can help in developing quantified estimates. Measures of risk are arrived at by combining risk and consequence estimates (i.e., risk = probability x consequence). A detailed review of methods for combining likelihood and consequence estimates to obtain risk measures can be found in "Guidelines for Chemical Process Quantitative Risk Analysis" (Center for Chemical Process Safety, AIChE, 1989). Some cases can be resolved through comparisons with similar systems, or with the use of qualitative tools, such as risk matrices. Others will require quantified approaches such as risk profiles and contours.

5. Determine risk tolerability. This means asking "Can we and our stakeholders tolerate this level of risk?" Guidance on tolerable levels of 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 that risk through further process design.

6. Consider enhanced or alternative designs. In an overall, risk-based design sequence, this step provides an opportunity to define changes that could reduce risk to a tolerable level. Four types of risk-reduction concepts have been classified by AIChE's CCPS: Inherently safer; passive; active; and procedural, in order of declining reliability. In ERS design, this step focuses on mitigation i.e., the lessening or controlling the consequences of an accidental release.

7. Re-evaluate enhancements and alternatives. Any 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 new process. Steps 1-4 should be followed again, to re-estimate process risk. The review should also estimate the cost of the proposed changes.

8**. Determine the tolerability of risk and associated costs.** 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 trade offs of each alternative design or mitigation solution.

Cost-benefit analysis can be qualitative or quantitative. A quantitative approach is especially useful when many competing process safety systems are being considered. If the analysis yields tolerable risk and costs for a particular design option, the results should be documented (Step 9). If not, it may be necessary to consider further enhancements and alternatives (Steps 6-8).

9. Document results. Documenting the process safety system and the design basis for the ERS and incorporating the failure scenarios and associated consequences, likelihood, and risk estimates developed above provides essential information for 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 baseline risks.

Case Study: Reducing Mitigation Costs Using A Risk-Based Approach

A worldwide 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. The company asked us to help its staff explore cost-effective alternatives for reaching an equal or superior level of risk reduction.

Working closely with the firms' scientists and process engineers, our team 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 (ERS) and emergency relief mitigation design.

After collaborating with the stakeholders on the development of risk matrices for risk reduction alternatives, we helped present the alternatives to 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 in risk could be achieved by spending additional money.

The manufacturer was able to achieve optimal risk reduction in two processes for one-tenth of the original cost estimate. This rigorous study also provided documentation for meeting new U.S.

Process Safety Management regulations [Appendix A]. Most importantly, the savings increased the capital available for technology upgrades and risk reduction in several of 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 stakeholders find acceptable when weighing the advantages and benefits of the activity or process. 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 upon several factors:

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? For example, risks associated with driving an automobile result from a voluntary act; risks associated with exposure to a toxic release from a nearby chemical plant are not.

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 important water or other resources at risk? Residential neighborhoods? Schools?

The degree to which the risk can be controlled or reduced. The design of process safety systems and especially emergency relief systems focus 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 takers' tolerability. For example, the average person understands the risk of driving an automobile but is uncertain regarding the risk of nuclear power generation.

Attitudes toward risk change over time. Given all these variables, how does a company establish risk tolerability criteria that can effectively contribute to decisions about the tolerability of certain consequences, likelihoods, and risks?

Risk criteria should 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.

Companies that have successfully established internal risk criteria focus on providing consistency in their decisions about risk. These criteria typically represent levels of risk that the firm believes will minimize impacts to continued operations. While this approach may not explicitly address specific stakeholder concerns, risk decisions that protect operations are likely to help reduce overall risk for facilities, employees, the surrounding community, and the environment.

Table 1: Characterizing Events

Characterizing Events				
		Consequence		
	Level 4	*Level 3*	*Level 2*	*Level 1*
Personnel	Potential for multiple life-threatening injuries or fatalities	Potential for life-threatening injury or single fatality	Potential for severe injury requiring physician's care	Injury requiring first aid
Public	Potential for multiple life-threatening injuries or fatalities	Potential for life-threatening injury or single fatality	Potential for severe injury requiring physician's care	Odor or noise nuisance, no direct impact
Environmental	Uncontained release with potential for major environmental damage	Uncontained release with potential for medium environmental damage	Uncontained release with potential for minor environmental damage	Contained release with localized impact
Equipment	Plant damage or losses in excess of $100M	Plant damage or losses valued at $10M - $100M	Plant damage or losses valued at $1M - $5M	Plant damage or losses valued at $100,000 - $1M
		Frequency		
	< Once every 100 years (e.g. single instrument or valve failures, hose leaks, or human error in every day activity)	Between 1/100 and 1/1,00 years (e.g. dual instrument or valve failures, hose ruptures, or piping leaks)	Between 1/1,000 and 1/10,000 years (e.g. combination of instrument failures and human errors, or full bore failures of process lines or fittings)	> 1/10,000 years (e.g. multiple instrument or valve failures, or human errors, or spontaneous tank or vessel failures)

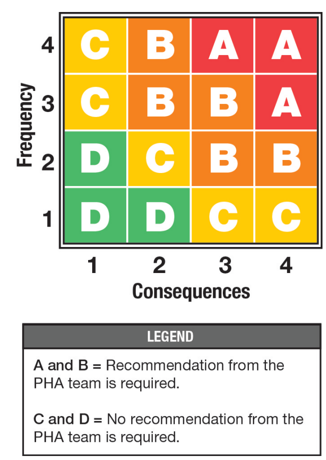

Figure 2: *The qualitative criteria shown in this table can be used to assess the potential consequence and frequency of a given event by severity level. Plotting these levels on a risk matrix then helps determine the course of action required.*

Review Your Options

The purpose of the procedure described above is to enhance the engineer's ability to make consistent choices about safe design and to introduce modifications where they can do the best for the least cost. Four basic types of safety design are available: Inherently safer, active controls, passive controls, and procedural controls.

All help to minimize risk, but each varies in terms of factors such as cost, reliability, and maintenance. When deciding among the hierarchy of mitigation options, designers should avoid the pitfall of "project mentality," i.e., focusing only on minimizing capital costs.

Inherently safe design solutions

Eliminate or mitigate the identified hazards by using materials and process conditions that are less hazardous. For example, faced with the hazard posed by a flammable solvent, designers may seek to substitute water-based solvents. When large inventories of hazardous intermediates increase risk levels, there may be a way to reduce or eliminate these on site inventories.

Passive design solutions

Offer a high level of reliability by operating without any devices that sense or actively respond to a process variable. Examples include incompatible hose couplings for incompatible substances and components; equipment designed to with- stand internal deflagration and other high-pressure hazards; and dikes that contain hazardous inventories with a bottom that slope to a remote area.

Active design solutions

Use devices that monitor process variables and activate to mitigate a hazardous situation. Active solutions often called engineering controls may be less reliable than passive or inherently safer design solutions because they require more maintenance and more operating procedures. The following are active design solutions:

- A pressure safety valve or rupture disk that prevents vessel overpressure
- A high-level sensing device inter- locked with a vessel inlet valve and pump motor to prevent overfilling
- Check valves and regulators

Procedural design solutions

Also known as administrative controls, avoid hazards by requiring a person to act. Such actions might include responding to an alarm, an instrument reading, a leak, a strange noise, or a sampling result, and might require the person to manually close a valve after an alarm sounds to prevent a vessel from overfilling or carry out preventive maintenance to reduce the likelihood that equipment will fail.

Involving a person in the safety solution means incorporating human factors and the risk of errors in the analysis. As a result, procedural solutions are generally less reliable than other design solutions.

As Figure 2 suggests, inherently safer approaches may require higher initial investment. But the cost of maintaining an active mitigation system to obtain an equivalent level of risk reduction can be significant. Therefore, the life-cycle cost of each design option should be considered before making the final selection.

In general, inherently safer, and passive solutions offer higher reliability and lower operating costs but may involve an initial cost that does not fit with the budget or business plan for the process. Active and procedural solutions cost less to begin with, but typically involve higher operating costs and are less reliable.

Authors

Georges Melhem, Ph.D., FAIChE
melhem@iomosaic.com

R. Peter Stickles
stickles@iomosaic.com

Regulatory Requirements and Industry Guidelines

European Regulations

The Seveso Directives. Under the first Seveso Directive passed by the European Community in 1982 specific industries are to meet safety requirements such as carrying out safety studies providing hazard notification develop and maintaining emergency response plan. Seveso II passed in 1984, covers the transport of hazardous wastes that cross national borders within the European Community.

U.S. Regulations

Risk Management Program (RMP) Rule — The EPA's RMP Rule, published in final form on June 20, 1996, as part of the 1990 Clean Air Act Amendments, requires facilities with regulated substances to prepare a risk management plan. These substances include 77 toxic substances, 63 flammables, and certain high explosives. The risk management plan required by the RMP Rule calls for an emergency response program, a hazard assessment program, a prevention program, and an overall system for developing and implementing a risk management program on site.

Process Safety Management (PSM) Rule — The OSHA PSM Rule, issued in 1992, addresses the process safety management of highly hazardous chemicals. The Rule's elements process safety information, process hazard analysis (PHA), and pre-startup safety review address activities related to process design and documentation. Under the PHA element, for example, regulated facilities must conduct a PHA and establish priorities for implementing risk reduction measures. While the OSHA PSM Rule requires hazard evaluation and prioritization, it does not emphasize risk-based approaches to managing process hazards.

State Regulations — OSHA's PSM Rule follows the regulatory lead taken by California, New Jersey, and Delaware for the management of process hazards. In California, facilities that store acutely hazardous materials (AHMs) must prepare a Risk Management and Prevention Program (RMPP) to document how AHMs are handled to minimize the possibility of a release. The RMPP law states that the RMPP "shall be based upon an assessment of the processes, operation and procedures of the business, and shall consider the results of the HAZOP study… and an off site consequence analysis." From these studies, facilities develop risk assessments that guide risk mitigation and emergency response planning.

Recommended Industry Practices

AIChE CCPS Guidelines

Since 1985, the Center for Chemical Process Safety (CCPS) has worked to promote process safety among those who handle, use, process, and store hazardous materials. They have published a series of publications covering the full range of technical and management issues in process safety and design, including Guidelines for Selecting the Design Basis for Process Safety Systems (October 1992).

Responsible Care

Introduced in 1988, the Responsible Care program of the Chemical Manufacturers Association, which changed their name to the American Chemistry Council (ACC) in 2000, requires each member organization to establish six key program elements, including guiding principles, codes of management practice and public advisory panels. Management practice codes include the Process Safety Code. Its four elements cover management leadership, technology, facilities, and personnel emphasizing company objectives rather than specific prescribed standards.

American Petroleum Institute (API) RP 752

Issued in 1995, this recommended practice uses a risk-based approach to manage hazards associated with the location of process plant buildings. Both flammable and toxic hazards are addressed, as well as the frequency and consequences of hazardous material releases. The intent is that the relative risk of individual buildings should be identified and used in planning projects that involve building changes.

Measures for Addressing Tolerable Risk Levels

Several measures discussed below are commonly used for assessing ‘tolerable risk’.

Release Limits

Address the tolerability of potential releases, by considering the amount of material that could be released. “Tolerable” quantities depend upon the physical states and hazardous properties of the materials. A hypothetical limit for gasoline might be as much as 5,000 lbs. while hypothetical limit for chlorine might be as little as 200 lbs.

Threshold Impact Criteria for Fence or Property Line

Uses standard damage criteria such as toxicity, thermal radiation, or blast overpressure, together with consequence modeling to determine whether the potential impact at a facility’s fence or property line exceeds a tolerable threshold.

Single versus Multiple Component Failures

Provide a qualitative approach to how many component failures will be tolerated. For example, a company might choose to tolerate event scenarios that would require three independent component failures, conduct further analysis of event scenarios that are triggered by two failures, and not tolerate events arising from single failures.

Critical Event Frequency

Addresses scenarios that have a defined high-consequence impact, such as a severe injury, fatality, critical damage to the facility, or impacts to the community. Firms often use a range of threshold frequencies for these scenarios, depending on the extent and nature of potential, worst-case consequences.

Risk Matrix Criteria

Use qualitative and semi-quantitative frequency and severity categories, to estimate the potential 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. While no consensus exists on appropriate thresholds, a maximum risk to the public of 1x10-5 fatalities per year is not unusual among companies that use these criteria.

Societal Risk Criteria

Can be used in lieu of or in addition to Individual Risk Criteria and provide a more detailed evaluation of the distribution of risk. Societal Risk Criteria explicitly addresses those events with a high frequency and low consequence, and those with a low frequency and high consequences. These criteria can be useful to firms that have recently experienced an adverse event and cannot tolerate another no matter how remote its likelihood.

Risk Matrix and Cost Threshold

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. But most design situations are not that simple. For example, a process enhancement or alternative that reduces a high risk to a medium risk and costs $15,000 may be considered feasible and effective, as might an alternative that costs $450,000 and reduces a high risk to a low risk. In these situations, a risk matrix and cost threshold with definite “rules” can help clarify the decision-making.

Cost Benefit Criteria

Define the amount of risk reduction expected for each dollar expended. They can be developed in conjunction with quantitative risk estimates. In some cases, firms might use two thresholds – one for the dollars needed to achieve a tolerable risk level, and another for further reduction beyond that level.

ioMosaic®

Minimizing risk. Maximizing potential.®

US Offices

New Hampshire (Salem) – *Headquarters*

Texas (Houston)

Minnesota (Minneapolis)

California (Berkeley)

International Offices

Kingdom of Bahrain (Al Seef)

United Kingdom (Bath)

Software Solutions

Process Safety Enterprise®

Centralize the process safety management lifecycle to accelerate business goals

Process Safety Office®

Identify, evaluate, and control process hazards with tools used by process safety consultants

Process Safety Learning®

Build your process safety competencies incrementally with online training

Process Safety tv®

View, share, and discuss PSM worldwide on a secure platform

Contact Us

www.ioMosaic.com

sales@ioMosaic.com

1.844.ioMosaic

About ioMosaic Corporation

Through innovation and dedication to continual improvement, ioMosaic has become a leading provider of integrated process safety and risk management solutions. ioMosaic has expertise in a wide variety of areas, including pressure relief systems design, process safety management, expert litigation support, laboratory services, training and software development.

As a certified ISO 9001:2015 Quality Management System (QMS) company, ioMosaic offers integrated process safety and risk management services to help you manage and reduce episodic risk. Because when safety, efficiency, and compliance are improved, you can sleep better at night. Our extensive expertise allows us the flexibility, resources, and capabilities to determine what you need to reduce and manage episodic risk, maintain compliance, and prevent injuries and catastrophic incidents.

Our mission is to help you protect your people, plant, stakeholder value, and our planet.

Consulting Services

- Asset Integrity
- Auditing and Due Diligence
- Combustible Dust Hazard Analysis and Testing
- Facility Siting
- Fault Tree/SIL/SIS Analysis
- Fire and Explosion Dynamics
- Incident Investigation, Litigation Support and Expert Testimony
- Liquefied Natural Gas Safety
- Pipeline Safety
- Process Engineering Design and Support
- Process Hazards Analysis (PHA)
- Process Safety Management (PSM)
- Reactive Chemicals Evaluation and Testing
- Relief and Flare Systems Design and Evaluations
- Risk Management Program Development
- Quantitative Risk Assessments (QRA)
- Software Solutions
- Structural Dynamics
- Training

Laboratory Testing Services (ISO accredited)

- Chemical Reactivity
- Combustible Dust
- Battery Safety
- Specialized Testing