ioMosaic®
Minimizing risk. Maximizing potential.®

Risk Considerations for Safe Process Design

An ioMosaic® Publication

G. A. Melhem, Ph.D., FAIChE

This page is intentionally left empty

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

IOMOSAIC® CORPORATION

Risk Considerations for Safe Process Design

Process Safety and Risk Management Practices

authored by

G. A. Melhem, Ph.D., FAIChE

Printed November 15, 2024

This page is intentionally left empty

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

Notice:

This document was prepared by ioMosaic® Corporation (**ioMosaic**) for Public Release. This document represents ioMosaic's best judgment in light of information available and researched prior to the time of publication.

Opinions in this document are based in part upon data and information available in the open literature, data developed or measured by ioMosaic, and/or information obtained from ioMosaic's advisors and affiliates. The reader is advised that ioMosaic has not independently verified all the data or the information contained therein. This document must be read in its entirety. The reader understands that no assurances can be made that all liabilities have been identified. This document does not constitute a legal opinion.

No person has been authorized by ioMosaic to provide any information or make any representation not contained in this document. Any use the reader makes of this document, or any reliance upon or decisions to be made based upon this document are the responsibility of the reader. ioMosaic does not accept any responsibility for damages, if any, suffered by the reader based upon this document.

Revision Log:

Revision 1: November 16, 2024

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

...

Table of Contents

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

List of Figures

©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

List of Tables

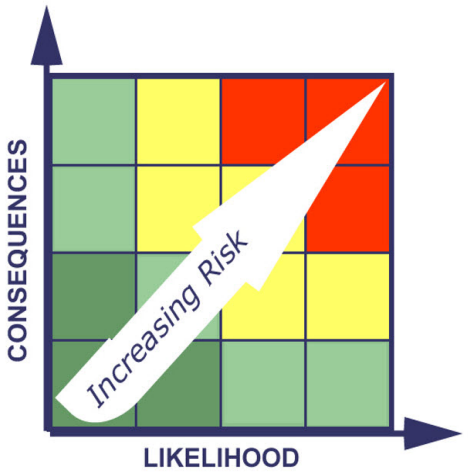
©ioMosaic Corporation ⇑ ⇓ All Rights Reserved Printed November 15, 2024

1 Introduction

Safe design has long been a priority in the process industries. It is a design that effectively minimizes the likelihood of process hazards and mitigates their potential consequences to achieve tolerable risk.

Today, the process industries need to be certain that their stakeholders have confidence in how they manage the environmental, health, security, 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, are critical for providing that level of confidence required for risk management.

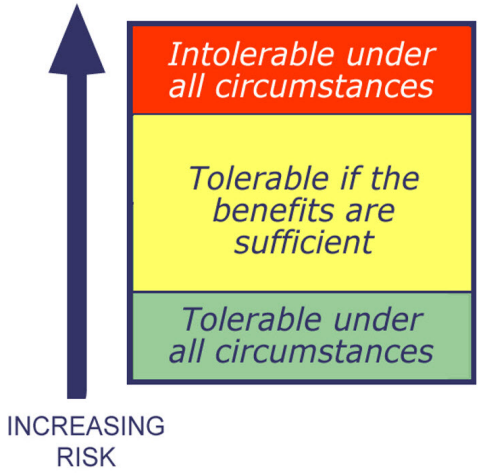
Figure 1: Risk concept



Source: ioMosaic®

Risks (see Figure 1) cannot be completely eliminated from the handling, use, processing, transportation, and storage of hazardous materials. Instead, the goal of process safety management is to consistently reduce risk to a level that can be tolerated (see Figure 2) by all concerned including facility staff, company management, surrounding communities, the public at large, industry, and government agencies. A systematic, risk-based approach to safe design can help eliminate hazards that pose high risk from the process and mitigate the potential consequences of hazards.

Figure 2: Risk tolerability concept



Source: ioMosaic®

To achieve a consistent, effective approach to risk reduction, design engineers must be able to define "tolerable" and "intolerable" risks. To meet the expectations of shareholders, employees, regulators, and the communities that surround process facilities, design engineers need to be able to document how risk and safety are addressed in the design process.

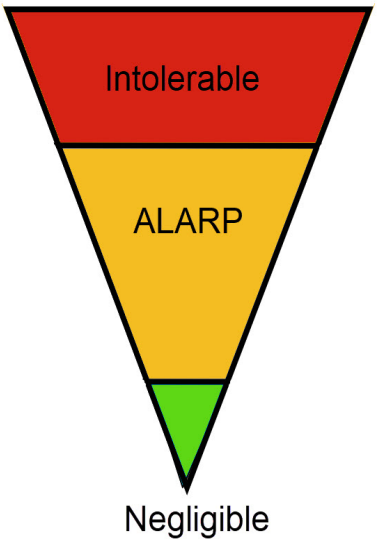
At the same time, to meet business needs of the company, process safety design solutions must be cost-effective. A risk-based approach to safe design enables design engineers to answer the needs of all process safety stakeholders without compromising on safety and without excessive prevention and mitigation measures. Risks are typically reduced to a level that is as low as reasonably practicable (ALARP) as shown in Figure 3.

2 The Concept of Risk

For chemical processing safe design, risk is understood in terms of the likelihood and consequences of hazard scenarios that could expose people, property, or the environment to the harmful effects of a hazard. Hazards, as defined by the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE), include chemical or physical conditions or characteristics that can harm people, property, or the environment. Incident likelihood encompasses frequency and probability; consequences refer to outcomes and impacts.

It is always possible to identify scenarios that would be catastrophic for the system being designed. Safe design does not necessarily need to address the worst scenario someone can identify. A line must be drawn (or a gray area defined) between likely scenarios and unlikely ones. For example, a process might use a chlorinated substance, which is known to react vigorously with water. If water is not present at the site, there is no need to address that reaction scenario in relief systems design. If water is on-site, but is not used in the same process as the chlorinated substance, there is still no need to address a reaction scenario in relief systems design. If water is not used in the same process as the chlorinated substance, but they share a storage facility, then, depending on the circumstances, it might make sense to include a chlorinated substance/water reaction scenario in relief systems design.

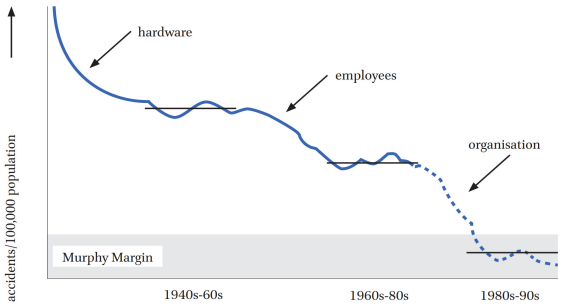
Figure 3: As low as reasonably practicable (ALARP) risk concept



Source: ioMosaic®

Risk-based approaches to decision-making have gradually gained ground in process safety. In other business areas, risk analysis has been an important part of decision-making for some time. Risk-based approaches can benefit process safety and environmental mangers by supporting a clear, consistent approach to decision-making about risks and by providing safe design choices that key stakeholders can understand.

Figure 4: The “Murphy Margin”

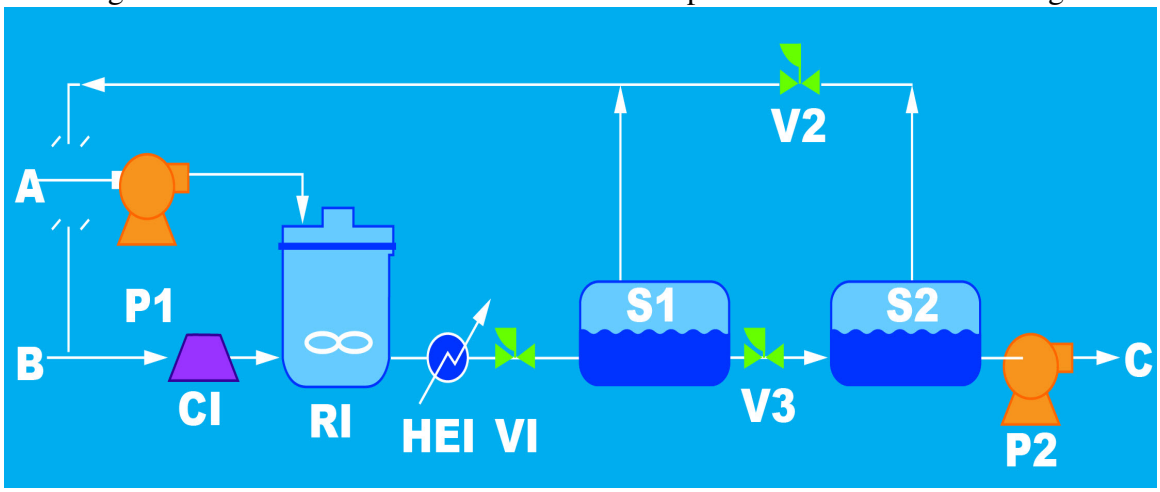


Source: [1]

When companies have managed to control all technical, personal, and systemic parts of the incident causation process [1, 2] they will have achieved maximum risk reduction (minimal risk), a level beyond which it is not possible to further reduce risk (see Figure 4). This minimal risk region is called the “Murphy Margin” and represents an area where effective risk management has achieved a level where few accidents occur. This is an area where factors beyond the control of both management and operating personnel will continue to influence the number of accidents and residual risks.

The technical nature of many aspects of process safety risk analysis has made this area something

Figure 5: Heat and material balances and basic process controls in core design



Source: ioMosaic®

of a specialists preserve. With an approach to risk analysis that combines technical sophistication with clear communication of risks and choices, companies and stakeholders can achieve a greater degree of confidence about the management of process risks.

3 A Systematic Approach

When designing a process (see Figure 5), design engineers first address the mechanics of making the product. A core design is defined by heat and material balances and basic process controls. Once the core design is defined, 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 design. They try to determine what failures might occur, what effect these failures ("scenarios") might have in terms of quality, safety, and the environment would be, and how likely these scenarios are.

As they answer these questions and proceed with system design, engineers are continually making risk-based decisions [3]. But all too often, their decisions may not be based on quantification of risk but only on perceptions. The process used may be neither systematic nor comprehensive and often times it may be biased by personal preferences.

The approach presented here offers a disciplined, consistent thought process and flexible implementation options. When the process for selecting the design basis lacks consistency, it is difficult to know whether the same risk-management philosophy supports all of a company's process safety and risk decisions. As a result, inconsistencies in approach can develop between different processes and facilities, and, in the case of large, complex design projects, different design engineers on the same project may be using different philosophies. Risk owners should manage their portfolio risks as consistency is key [4].

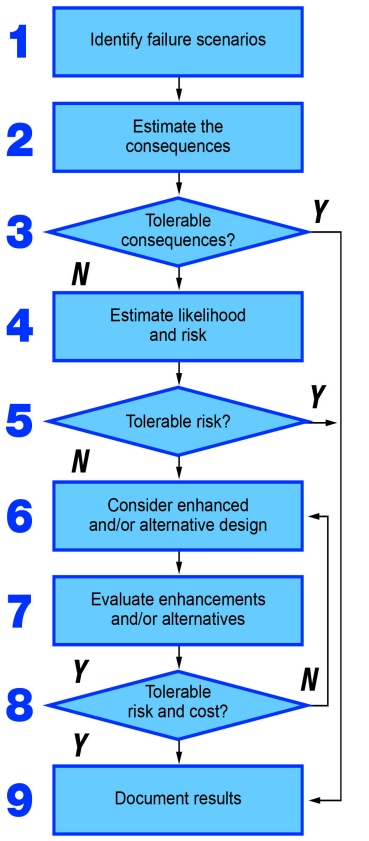
Ideally, safety should be a theme at each stage in a systematic design lifecycle. But the most cost-

effective solutions tend to emerge in the earliest front end engineering design stage (FEED). 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 a toxicity criteria limiting off-site vapor cloud concentrations to a specific, quantified level of concern. By performing vapor cloud dispersion calculations (through a quantitative characterization of the consequences of potential releases) the company can determine whether specific loss-of-containment scenarios associated with specific failures exceed the toxicity criteria. If the scenario consequences do not exceed off-site toxic impact tolerability criteria, then there is no need to continue with an analysis of event likelihood or further risk quantification.

4 Nine Steps to Cost-Effective Safe Design

Figure 6: Safe system design basis selection methodology



Source: ioMosaic®

The technique outlined here derives from process design engineers characteristic problem solving methods and can be applied to all safe design cases, from the simplest to the most complex. The technique provides for a disciplined thought process and flexibility in its application. It comprises a sequence of analysis and testing steps in the form of a decision tree (Figure 6).

1. Identify failure scenarios When design engineers have established a core process design, they can address things that can go wrong and identify failure scenarios that may require mitigation. Process hazard analysis (PHA) techniques and past experience can provide insight and information on possible failure scenarios.

2. Estimate the consequences In this step, design engineers 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. Are the consequences tolerable ? Answering this question requires guidance from established risk tolerability criteria. These include: company-specific criteria, engineering codes and standards, industry initiatives, and regulatory requirements. For relief systems design, the focus of this Step is on comparing the potential rise in pressure to the mechanical failure or deformation limits of the equipment under consideration.

4. **Estimate likelihood and risks** Estimates of likelihood rest upon an understanding of the mechanism and frequency with which failure scenarios such as those identified in Step 1 might occur. When historical data is available about equipment and processes, these data can be used to arrive at failure scenario frequency estimates. Failure rate data are also published in public taxonomy tables and in CCPS publications. When data is lacking, methods such as fault tree analysis help in developing quantified estimates. Measures of risk are arrived at by combining likelihood and consequence estimates. A detailed review of methods for combining likelihood and consequence estimates to obtain risk measures can be found in "CCPS Guidelines for Chemical Process Quantitative Risk Analysis". Some cases can be 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 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 considerations or modifications.

6. **Consider enhanced and/or alternative designs** In the overall risk-based design sequence, this step is an opportunity to consider the entire process design and define changes that can reduce risk to a tolerable level. Risk reduction concepts include inherently safer, passive, active, and procedural in declining order of reliability (see Figure 11). In emergency relief system design, this step can focus on mitigation to reduce or control the consequences of an accidental release.

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 1-4, the review should re-estimate process risk. The review should also estimate the cost of the proposed changes.

8. **Determine tolerability of risk** 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 (see Figures 11 and 13). 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 further design enhancements and alternatives (Steps 6-8).

9. Document results The failure scenarios and associated consequences, likelihood, and risk estimates developed during this process form the design basis for process safety information. Documenting process safety systems and relief systems design basis retains essential information that is extremely valuable for compliance, hazard evaluation, management of change, and subsequent design projects. When the findings from Step 3 or Step 5 show that consequences and risk meet the 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.

5 Guidelines for Risk Tolerability

Underlying this entire approach is the understanding that there is a continuum of risk levels. In most cases, risks cannot be eliminated, only reduced to a level that everyone who has a stake in the activity or process finds tolerable when weighed against the advantages and benefits of the activity or process (see Figure 3). Usually, risks will be tolerated in exchange for an economic or societal benefit.

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

The degree to which the risk can be controlled or reduced
Process safety design and especially emergency relief system design 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.

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

Companies that have successfully established risk criteria focus on providing consistency in their

decisions about risk. These criteria typically represent levels of risk that the company believes will minimize impacts to continued operations. This approach does not explicitly mention specific stakeholder concerns such as protection of the surrounding environment and communities. However, risk decisions that protect operations are very likely to help reduce risk across the board for facilities, employees, surrounding property, and the environment. Moreover, since demonstrably safe operations have become a cornerstone of a companys franchise to operate in many places, well-thought-out risk criteria that make continued operation their objective will also address most other stakeholder concerns.

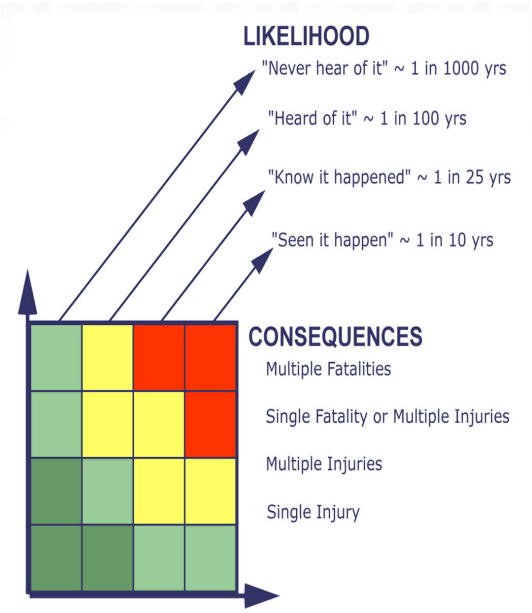
Risk criteria should also fit with a companys philosophy and culture and match the type of analysis its engineers normally conduct in the design stage. The selection of appropriate risk criteria is a corporate responsibility and requires the involvement and support of senior management, as it establishes the levels and types of risks the company will tolerate.

Once a company has established specific risk criteria, they 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. Figure 8 and Table 1 provide examples of some accepted risk criteria.

6 Representative Risk Tolerability Criteria

Release Limits address the tolerability of potential release consequences by considering the amount of material that could be released safely. “Tolerable” quantities depend upon 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.

Figure 7: A simple risk matrix



Source: ioMosaic®

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 impacts at the facilitys fence or property line exceed tolerable thresholds.

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 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. This type of risk assessment is often referred to as Layer of Protection Analysis (LOPA). The nuclear industry [5]

uses a similar approach called "defence-in-depth" which focuses on multiple safety layers including prevention, monitoring, and action to mitigate consequences of failures.

Critical Event Frequency (see Table 1) addresses event scenarios with a defined high-consequence impact. Examples would be a severe injury, a fatality, critical damage to the facility, or impacts on the surrounding community. Companies often use a range of threshold frequencies for these scenarios, depending upon the extent and nature of potential worst-case or worst-credible consequences.

Risk Matrix (see Figure 7) 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.

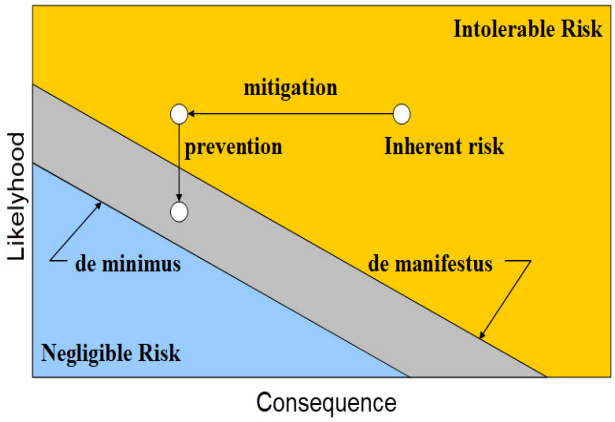
Individual Risk Criteria consider the frequency of the event or events to which an individual might be exposed, the severity of the exposure, and the amount of time for which the individual is at risk. While no consensus exists on appropriate thresholds, a maximum risk to the public of 1×10^{-5} fatalities per year (or 1/100,000 years) is not unusual among companies that use these criteria.

Table 1: Typical critical event frequencies

Industry	**Event**	**Source**	**Frequency**
Chemical	Unmitigated Overpressure	CCPS	1×10^{-4}/year
Airlines [6, 7]	Critical System Failure	FAA	4×10^{-6}/flight
Nuclear [5]	Core Damage Frequency Core Damage Frequency for New Designs	United States NRC European Safety Authorities	1×10^{-4}/reactor year 1×10^{-6}/reactor year
Oil Exploration & Production	> 10 Public Fatalities	Santa Barbara County, California	1×10^{-6}/year

Societal Risk Criteria can be used instead of or in addition to individual risk criteria and provide a more detailed evaluation of the distribution of risk [3]. In other words, societal risk criteria explicitly address both events with a high frequency and low consequence and events with a low frequency and high consequences. This class of criteria can be useful to companies that have recently experienced an adverse event and cannot tolerate another, no matter how small its likelihood (see Figure 8).

Figure 8: Typical societal risk criteria



Source: ioMosaic®

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, an 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 reduced a high risk to a low risk. In these situations, a risk matrix and cost threshold with definite "rules" can help

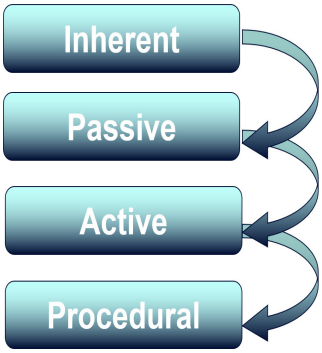
clarify decision-making.

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 (see Section 8.5), and another for any further reduction beyond that level.

7 Understanding the Design Options

The purpose of the procedure described in Section 4 is to enhance the ability of design engineers to make consistent choices about safe design and to introduce modifications where they can provide optimal risk reduction. Choices for safe design can be divided into four categories: inherently safer [1], passive, active, and procedural. For example, safe design options for a potential runaway chemical reaction can include:

Figure 9: Safe design options



Source: ioMosaic®

Inherent A reaction at atmospheric pressure using a non-volatile solvent that is not capable of generating pressure during a runaway reaction. There is no potential for overpressure.

Passive A reaction that is conducted in a pressure vessel and is capable of generating 150 psig of pressure in case of a runaway. The reactor is designed to contain its maximum pressure as long as its pressure rating is maintained.

Active A reaction that is capable of generating 150 psig of pressure in case of a runaway but is conducted in a 15 psig rated vessel with a 5 psig high pressure interlock or a pressure relief valve set at 15 psig. We note that the interlock can fail or the pressure relief valve may not open at its set pressure.

Procedural A reaction as described above in a 15 psig vessel with an instruction for the operator to manually stop the reactant feed when the pressure reaches 10 psig. The operator could fail to execute the task.

All of these design categories help to minimize risk. But they vary in terms of factors such as lifecycle cost, reliability, and maintenance (see Figure 11). Companies are in the best position to manage these design choices (see Figure 12) when they are prepared to follow consistent risk tolerability levels, understand how a specific facility or process fits into their overall business plan, and know what the business limitations are for the safety component of a process.

When deciding among the hierarchy of design options, design engineers should avoid the pitfall of "project mentality", i.e., focusing only on minimizing capital cost. As Figure 11 suggests,

[1] Also referred to as intrinsically safe

inherently safer approaches may have higher initial investment, however, the cost of maintaining an active system to obtain an equivalent level of risk reduction can be significant. Therefore, the correct approach should be to consider the lifecycle cost of the design options, before making the final selection.

7.1 Inherently Safer Design Solutions (IST)

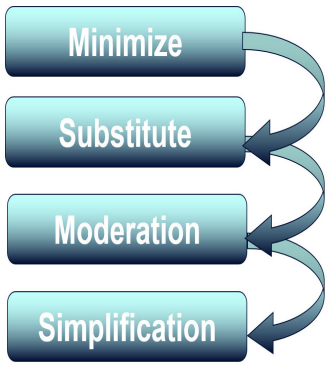
Inherently Safer design solutions eliminate or mitigate the identified hazard by using materials and process conditions that are less hazardous. For example, faced with the hazard posed by a flammable solvent, design engineers might seek to substitute water. When large inventories of hazardous "intermediates" increase risk levels, there may be a way to reduce or eliminate these inventories.

In general, inherently safer design can provide a better safeguard. For every pair of cause-consequence developed in a PHA or a hazard and operability study (HAZOP), safeguards must be developed that could prevent, detect, control, or mitigate the potential hazards. Four categories of inherently safer design solutions are typically considered (see Figure 10): minimize - use smaller quantities, substitute - replace with less hazardous materials, moderate - use less hazardous/severe conditions or materials least hazardous forms, and simplify - eliminate complexities to prevent errors. Typical inherently safer guide words are shown in Table 2.

7.2 Passive Design Solutions

Passive design solutions offer a high level of reliability by operating without any devices that sense and/or actively respond to a process variable. Examples of passive design solutions include incompatible hose couplings for incompatible substances and process components, equipment designed to withstand internal deflagration and other very high-pressure hazards, and dikes that contain hazardous inventories with a bottom sloping to a remote impounding area.

Figure 10: Inherently safer design options



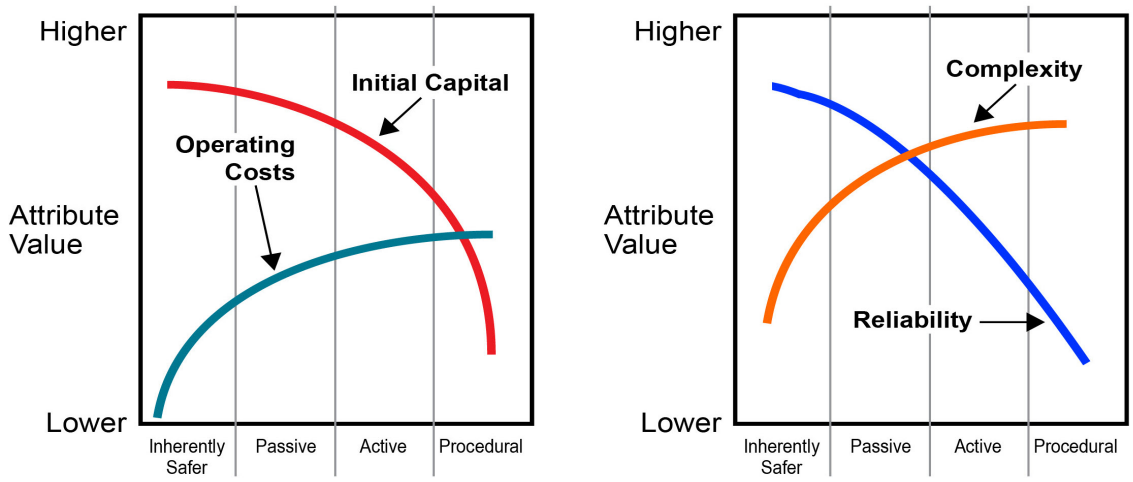
Source: ioMosaic®

7.3 Active Design Solutions

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

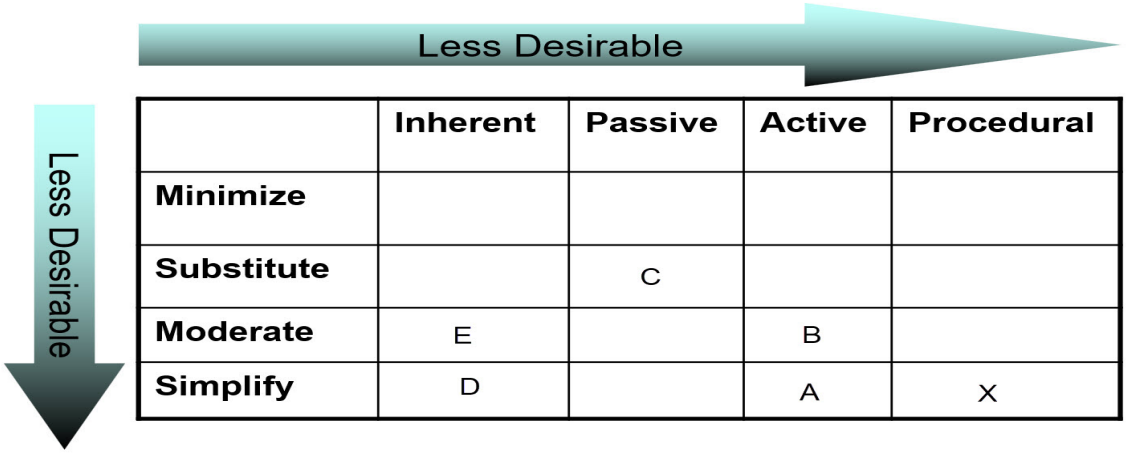
- a pressure relief valve or rupture disk that prevents vessel overpressure,
- a high-level sensing device interlocked with a vessel inlet valve and pump motor to prevent overfilling, and

Figure 11: Comparison of cost and functional attributes for design categories (typical trends)



Source: ioMosaic®

Figure 12: Safeguards selection based on effectiveness



	Inherent	Passive	Active	Procedural
Minimize				
Substitute		C		
Moderate	E		B	
Simplify	D		A	X

Source: ioMosaic®

- check valves and regulators.

7.4 Procedural Design Solutions

Procedural design solutions, also known as administrative controls, avoid hazards by requiring a person to take action. These actions might include reacting to an alarm, an instrument reading, a leak, a strange noise, or a sampling result and might involve steps such as manually closing a valve after an alarm sounds to prevent a vessel from overfilling or carrying out preventive maintenance to reduce the likelihood that equipment will fail. Involving a person in the safety solution means incorporating human factors in the analysis. These human factors, including an inappropriate division of tasks between machine and person and an unsupportive safety culture, contribute to making procedural solutions generally less reliable than other design solutions.

Choosing among these types of solutions is not simply a matter of selecting the most reliable approach. Inherently safer and passive design solutions tend to offer high reliability and low operating costs, but may involve an initial cost that may be prohibitive. Active and procedural solutions cost less to begin with, but typically involve higher operating costs and are less reliable (See Figure 11).

8 Case Studies

8.1 Total Containment vs. Vent Containment

Consider the case of a company that was handling a very energetic substance with a highly hazardous chemical reaction. The company had faced incidents with the substance and 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. While this approach was less expensive, it required the facility to deal with the potential of a hazardous effluent and to address the reliability of the relief system. This option was found to provide an equivalent tolerable risk level and a more reasonable cost of implementation.

8.2 Inherently Safer Fluid

In another case, a company was using water-cooled heat exchangers in a process that included a material that reacts violently with water, producing corrosive and toxic by-products. The company's design engineers considered various combinations of passive solutions such as heat exchangers that use non-pressurized water, active solutions such as advanced leak-detecting sensors,

and procedural solutions such as enhanced testing, inspection, and maintenance. All of the alternatives reduced risk levels, but none met the companys risk tolerability criteria. Faced with the prospect of sustaining high operating costs and staff efforts for a less-than-satisfactory risk effort, management chose a design that substituted a compatible heat transfer fluid for water. This choice required a higher initial investment in equipment replacement but eliminated a host of maintenance and administrative complexities down the line

8.3 Optimal Risk Reduction

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. Seeking a fresh angle on the technology and science of risk reduction, we helped the company to explore additional cost-effective alternatives for reaching an equal or superior level of risk reduction.

Working closely with the companys 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 expanding additional resources.

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 that is necessary to meet the compliance requirements of the OSHA PSM rule. Most important, the savings increased the capital available for technology upgrades and risk reduction in the companys other processes.

8.4 Risk Reduction Alternatives

A facility belonging to a large chemical manufacture was producing a family of chemicals that react vigorously with water, generating corrosive and toxic by-products. The production process utilized 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 and event. However, they needed a way to determine which risk reduction option or combination of measures was the most effective.

Working closely with the companies operations and design engineers, we utilized elements of 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

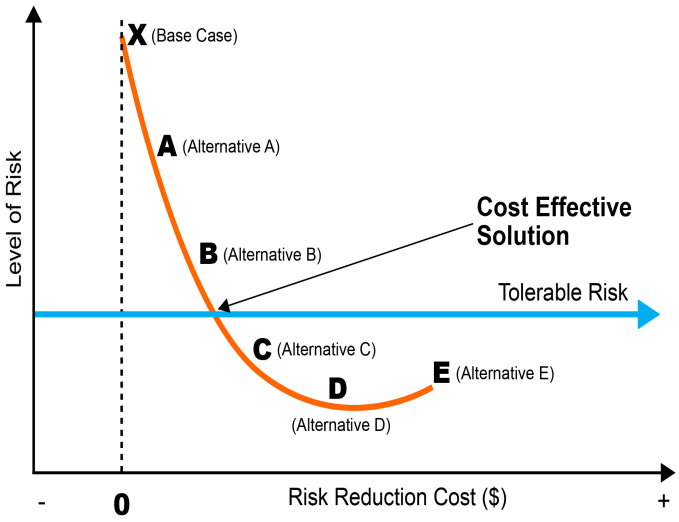
allow them to decide which option would meet their risk tolerability criteria. The company opted for the inherently safer solution of substituting a non-reactive coolant for water.

While the selected design approach was not the lowest capital cost alternative, there were offsetting operating cost benefits in terms of less maintenance cost, down-time, and administrative complexity.

8.5 Risk Reduction Cost vs. Frequency

A HAZOP identified a major loss scenario which can result in a total cost of $ 100,000,000 including plant replacement, product loss, business interruption, litigation costs, and subsequent environmental cleanup. The major loss scenario occurs with a frequency of λ per year.

Figure 13: Optimal risk reduction



Source: ioMosaic®

The proposed risk reduction cost is $ 1,000,000. After the mitigation measure is implemented, the scenario frequency becomes $\beta\lambda$, where β (< 1) is the frequency reduction multiplier [8]. We assume that the remaining plant life, N, is 30 years and the cost of money, i, is 8 %. If the benefit (annual expected loss reduction) outweighs the risk reduction cost, then the risk reduction measure is justified. To determine if the risk reduction measure is justified, we need to compare the annualized expected benefit, $L_0 - L_n$ to the annualized cost of risk reduction, A:

$$L_0 = 100,000,000 \times \lambda \quad \$/\text{yr before risk reduction} \tag{1}$$

$$L_n = 100,000,000 \times \beta \times \lambda \quad \$/\text{yr after risk reduction} \tag{2}$$

$$A = 1,000,000 \left[\frac{i\,(1+i)^N}{(1+i)^N - 1} \right] = 1,000,000 \frac{0.8050}{9.0626} = 88,826 \quad \$/\text{yr} \tag{3}$$

$$L_0 - L_n = 100,000,000 \times \lambda \times (1-\beta) \tag{4}$$

The risk reduction cost is justified if $L_0 - L_n > A$ or:

$$\lambda > \left(\frac{A}{100,000,000} \right) \frac{1}{(1-\beta)} > \left(\frac{88,826}{100,000,000} \right) \frac{1}{(1-\beta)} \tag{5}$$

If we expect a risk reduction factor of 10, $\beta = 0.1$, then the scenario frequency λ must be greater then 9.869×10^{-4}/yr in order for the risk reduction measure to be cost effective.

A more detailed cost-benefit analysis can be performed by considering the Net Present Value (NPV) of all costs associated with the major loss scenario. If the risk reduction measure is not implemented, the annual risk accrual and NPV will be for the jth year:

$$R^j = Q_0\lambda_0\,(1+x)^{j-1}\,(1+y)^{j-1} \tag{6}$$

$$NPV(R^j) = Q_0\lambda_0\left[\frac{(1+x)\,(1+y)}{1+i}\right]^{j-1} \tag{7}$$

$$NPV^{Total} = \sum_{j=1}^{j=N} NPV(R^j) \simeq Q_0\lambda_0\left[\frac{(1+x+y-i)^N-1}{x+y-i}\right] \tag{8}$$

where Q is the plant replacement cost (property damage) following the major loss scenario or product loss cost, or business interruption cost, or environmental cleanup cost, or litigation cost, or all of the above, x is annual increase in replacement cost, say 5 %, y is the annual increase in λ as the plant is aging, say 5 %.

If we consider the NPV concept, the major loss scenario threshold frequency would get smaller:

$$NPV_0^{Total} - NPV_n^{Total} \simeq 100,000,000 \times \lambda \times (1-\beta) \times \left[\frac{(1+x+y-i)^N-1}{x+y-i}\right] \tag{9}$$

$$NPV_0^{Total} - NPV_n^{Total} \simeq 100,000,000 \times \lambda \times (1-\beta) \times 40.568 > A > 1,000,000 \tag{10}$$

$$\lambda > \left(\frac{A}{100,000,000}\right)\frac{1}{40.568\,(1-\beta)} > \frac{0.01}{40.568\,(1-\beta)} \tag{11}$$

If we expect a risk reduction factor of 10, $\beta = 0.1$, then the scenario frequency λ must be greater than 2.7388×10^{-4} /yr in order for the risk reduction measure to be cost effective.

If we wanted to obtain a confidence level over the previous estimates, we can use Monte Carlo simulation.

1. Assume the interest rate follows a normal distribution with a mean of 8 % and a standard deviation of 4 %
2. Generate a random number from 0 to 1 (probability), and obtain the corresponding interest rate from the probability distribution
3. Plug the interest rate in the previous NPV and calculate the value of scenario frequency
4. Repeat the process 1000 times and store the results for λ
5. Count the number of times out of 1000 where λ exceeds 0.0001
6. Divide by 1000 to get the probability that the risk reduction investment will make sense if the scenario frequency is greater than 0.0001

In this approach, we have avoided attempting to evaluate human life [2] in financial terms because (a) it implies an acceptance of human fatality, (b) it leads to placing a value on human life with potential ethical issues arising if different values are assigned at different locations, (c) it suggests that fatalities are regarded as part of the natural cost of doing business. Projects/expenditures aimed toward process modifications that reduce the chance of injury or fatality will also significantly lessen the potential for financial loss. This cost/benefit methodology has been developed to identify such projects to emphasize the proposition that safe operation is good business.

9 Next Steps in Cost-Effective Reduction

In recent years, industrial standards for tolerable risk have tended to become increasingly more 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 leaders in the process industry setting standards for their companies that are well in excess of 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. The ability to reach decisions about process safety design based on a clear understanding of both the risk reduction options and costs can greatly strengthen managers ability to meet the needs of internal and external stakeholders for process safety.

10 Selected Regulatory Frameworks and Industry Guidelines

In many cases, companies have been revisiting process design basis issues to meet recent regulatory requirements and industry guidelines. These include:

10.1 United States Regulations

Risk Management Program (RMP) Rule

The U.S. Environmental Protection Agency (EPA) risk management program rule, was first published in final form on June 20, 1996 as part of the Clean Air Act Amendments (CAA) of 1990. The RMP rule implements Section 112(r) of the 1990 Clean Air Act amendments to improve chemical accident prevention at facilities. The RMP rule requires facilities that use extremely hazardous substances to develop a Risk Management Plan. The substances include 77 toxic chemicals, 63 flammable chemicals, and certain high explosives. The program required by the RMP rule includes an emergency response program, a hazard assessment program, a prevention program, and an overall system for developing and implementing a risk management program.

[2] Statistical value of a human life [9] has been set by the US EPA at $6.3 million, US FDA at $6.5 million, and the US DOT at $\simeq$ $9.1 million

More recently an updated RMP rule became effective May 10, 2024, "Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act; Safer Communities by Chemical Accident Prevention, 89 Fed. Reg. 17622 (Mar. 11, 2024)". Revisions include but are not limited to:

- Clarification to Process Safety Information (PSI) Recognized and Generally Accepted Good Engineering Practices (RAGAGEP) requirements
- PHA requirements and PHA "safety gap" analysis
- "Emphasis" on PHA consideration of natural hazards, power loss, and facility siting
- Public disclosure of declined PHA and facility siting recommendations
- Requirement to conduct Safer Technology and Alternatives Analysis (STAA) and new requirements for passive, active, and procedural safeguards
- Third-party audit requirements
- Incident investigation requirements
- Emergency planning
- Information availability

EPA intends to publish guidance one year after Final Rule for provisions such as: STAA, root cause analysis, third-party audits, and employee participation.

Process Safety Management (PSM) Rule

The Occupational Safety and Health Administration (OSHA) PSM rule, 29 CFR 1910.119, Process Safety Management of Highly Hazardous Chemicals, was first issued in 1992. The rule's process safety information, mechanical integrity, process hazard analysis, and pre-startup safety review elements address activities related to process design and documentation. Under the process hazard analysis element, for example, regulated facilities must conduct a process hazard analysis and establish priorities for implementing risk-reduction measures. But while the OSHA rule requires hazard evaluation and prioritization, it does not emphasize risk-based approaches to managing process hazards.

Since 1992 OSHA has issued compliance guidelines, enforcement procedures, numerous interpretation letters, and National Emphasis Programs (NEP). The interpretation letters (06-05-2015 and 05-11-2016) related to RAGAGEP should be reviewed.

State Regulations

The OSHA PSM rule followed 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, operations, and procedures of the business, and shall consider the results of a HAZOP study . . . and an offsite consequence analysis". From these studies, facilities develop risk assessments that guide risk mitigation and emergency response planning.

The California Accidental Release Prevention (CalARP) program was implemented on January 1, 1997 and replaced the California RMPP. The purpose of the CalARP program is to prevent accidental releases of substances that can cause serious harm to the public and the environment, to minimize the damage if releases do occur, and to satisfy community right-to-know laws.

This is accomplished by requiring businesses that produce, handle, process, distribute, or store certain chemicals over a threshold quantity to develop a Risk Management Program, prepare an RMP, and submit the RMP to the local Certified Unified Program Agency (CUPA). The California Emergency Management Agency (Cal EMA), formerly the Governors Office of Emergency Services, has developed regulations (Title 19 of the California Code of Regulations, 2735.1 and following) that incorporate elements of the Federal Accidental Release Prevention Program (also known as the Risk Management Program) into state regulations.

10.2 Regulations in European Countries

The Seveso Directives

The Seveso [3] directives are a series of European Union (EU) laws that aim to prevent major industrial accidents that involve dangerous substances. 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.

The Seveso III directive was adopted in 2012. It is one of the most important regulations in the EU, requiring operators of certain facilities storing dangerous chemicals to develop and implement emergency planning and response procedures. The Seveso III directive updated the original directive to include stricter legal requirements for installations that handle large amounts of dangerous substances. It also gave citizens more rights to access information and justice. The Seveso directives apply to over 12,000 industrial installations across the EU, including chemical plants, refineries, and oil depots. The directives require companies to: (a) Establish a safety management system, (b) Put in place an internal emergency plan, (c) Regularly inform the public who could be affected by an accident, and (d) Provide safety reports. The directives also give the public more information about the risks of nearby industrial installations and how to react in the event of an accident. This information must be available online.

BAT/BATNEEC [4]

[3] The name Seveso comes from a town in northern Italy.

[4] Source: IOGP Report No. 510, Operating Management System Framework for controlling risk and delivering high performance in the oil and gas industry, International Association of Oil & Gas Producers, June 2014. Global Standards

"Best Available Techniques" (BAT) and "Best Available Techniques Not Entailing Excessive Costs" (BATNEEC) are based on commonly applied, judgment-based principles to assess whether risk controls/barriers are sufficient to manage an environmental impact.

BATNEEC was introduced with the European 1984 Air Framework Directive and is only one example of commonly applied, criteria-based approaches to manage environmental risk towards acceptable levels.

Principles are generally regulatory-based and include Best Available Control Technology (BACT), introduced by the US EPA, or Best Available Technology (BAT), introduced in Europe by OSPAR [5].

REACH

The Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) Regulation is a European Union law that aims to protect human health and the environment from the risks of chemicals. REACH aims to protect human health and the environment, while also allowing the free movement of substances in the EU. REACH applies to all chemical substances used in the European Economic Area (EEA), including those in everyday products like paints, cleaning products, and clothes.

Manufacturers and importers of chemicals must register information about their products in the European Chemicals Agency (ECHA) database. They must also provide safety information to downstream users, such as customers. The ECHA evaluates the information provided by manufacturers and importers. REACH can restrict or phase out substances that are considered a very high concern. REACH promotes the use of alternative methods to assess chemical hazards, rather than animal testing. REACH came into effect on June 1, 2007, replacing many other European regulations and directives.

ATEX

A potentially explosive atmosphere can exist when a mixture of air, gases, vapors, mists, and/or dusts combine in a way that can ignite under certain operating conditions. Equipment and protective systems intended for use in potentially explosive atmospheres (ATEX) cover a range of products, including those used on fixed offshore platforms, petrochemical plants, mines, and flour mills, amongst others.

The ATEX Directive 94/9/EC is a directive adopted by the European Union (EU) to facilitate free trade in the EU by aligning the technical and legal requirements in the member states for products intended for use in potentially explosive atmospheres. The European Committee for Electrotechnical Standardization (CENELEC) design standards are still used. All products placed on the market or put into service in the EU for use in potentially explosive atmospheres must comply with the ATEX directive.

This directive covers "Equipment" and "Protective Systems" which may be used in potentially explosive atmospheres created by the presence of flammable gases vapors, mists or dust. "Equipment" is any item which contains or constitutes a potential ignition source and which requires special measures to be incorporated in its design and/or its installation in order to prevent the ignition source from initiating an explosion in the surrounding atmospheres. Also included in the term

[5] Oslo Paris

"equipment" are safety or control devices installed outside of the hazardous area but having an explosion protection function. A wide range of products comes within the definition of equipment, including electric motors, compressors, diesel engines, lighting fittings, control and communication devices and monitoring and detection equipment. "Protective Systems" are items which prevent an explosion that has been initiated from spreading or causing damage. They included flame arrestors, quenching systems, pressure relief panels and fast-acting shut-off valves.

The directive excludes the following types of products: medical devices, products for use in the presence of explosives, products for domestic use, personal protective equipment, sea-going vessels and mobile offshore units, means of transport - except vehicles for use in potentially explosive atmospheres, and military equipment.

10.3 Industry Guidelines

10.3.1 AIChE CCPS Guidelines

Since 1985, the Center for Chemical Process Safety, a part of the American Institute of Chemical Engineers, has worked to promote process safety among those who handle, use, process and store hazardous materials. CCPS publishes a series of publications covering the full range of technical and management issues in process safety and design, including the 1998 "CCPS Guidelines for Selecting the Design Basis for Process Safety Systems".

10.3.2 Responsible Care®

First introduced in 1988, the Responsible Care® program of the Chemical Manufacturers Association (CMA [6]) 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.

10.3.3 API Recommended Practice (RP) 752/753

First issued in 1995, this recommended practice employs a risk-based approach for management of hazards associated with 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 and projects that involve building changes. The 3rd Edition of API RP 752 was issued in December of 2009.

This Recommended Practice was developed for use at refineries, petrochemical and chemical operations, natural gas liquids extraction plants, natural gas liquefaction plants, and other onshore facilities covered by the OSHA PSM rule. Buildings covered by this RP are rigid structures intended for permanent use in fixed locations. Tents, fabric enclosures and other soft-sided structures

[6] The American Chemistry Council (ACC)

are outside the scope of this document. Portable buildings are now covered by RP 753, "Management of Hazards Associated with Location of Process Plant Portable Buildings, First Edition, June 2007". It is recognized, however, that portable buildings specifically designed for significant blast load represent a potential area of overlap between RPs 753 and 752.

11 Conclusions

Risks cannot be completely eliminated from the handling, use, processing, transportation, and storage of hazardous materials. Instead, the goal of process safety management is to consistently reduce risk to a level that can be tolerated by all concerned including facility staff, company management, surrounding communities, the public at large, industry associations, and government agencies. A systematic, risk-based approach to safe design can help to eliminate hazards that pose high risks from the process and to mitigate the potential consequences of hazards.

Table 2: Inherently safer guide words

Guide Word	Checklist Questions
Minimize	• Is the storage of all hazardous gases, liquids, and solids minimized ? • Are just in time deliveries used when dealing with hazardous materials ? • Is shift rotation optimized to avoid fatigue?
Substitute	• Can a less toxic, flammable, or reactive material be used ? • Can a water based product be used in place of a solvent or oil based product ? • Is there an alternate way of moving product or equipment as to eliminate human strain ?
Moderate	• can potential releases be reduced via lower temperatures or pressures, or elimination of equipment ? • Are all power tools de-energized when not in use for extended periods of time ?
Simplify	• Are all manuals, guides and instructional materials clear and easy to understand, especially those that are used in an emergency situation ? • Are equipment and procedures designed such that they cannot be operated incorrectly or carried out incorrectly ?

References

[1] J. Groeneweg. *Controlling the Controllable: The Management of Safety*. DSWO Press, 1994.

[2] V. Roggeveen. *The influence of leadership on the prevention of safety incidents: on risk reduction, leadership, safety principles and practices*. PhD thesis, Leiden University, 2022.

[3] R. P. Stickles and G. A. Melhem. How much safety is enough? *Hydrocarbon Processing*, pages 50–52, October 1998.

[4] G. A. Melhem and R. P. Stickles. Portfolio risk management for process safety. In *7th Global Congress on Process Safety*. CCPS Center for Chemical Process Safety, AIChE, 2011.

[5] World Nuclear Association. Safety of nuclear power reactors. https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors, August 2024.

[6] FAA. Certification maintenance requirements. Advisory Circular AC 25-19, November 1994.

[7] FAA. System design analysis. Advisory Circular AC 25.1309-1, September 1982.

[8] R. Goyal. Understand quantitative risk assessment - Part i. *Hydrocarbon Processing*, pages 105–108, December 1994.

[9] L. Nara. Spotlight on safety - What is safety worth ? *Chemical Engineering Progress*, page 57, August 2017.

....

Index

About the Authors

Dr. Melhem is an internationally known pressure relief and flare systems, chemical reaction systems, process safety, and risk analysis expert. In this regard he has provided consulting, design services, expert testimony, incident investigation, and incident reconstruction for a large number of clients. Since 1988, he has conducted and participated in numerous studies focused on the risks associated with process industries fixed facilities, facility siting, business interruption, and transportation.

Prior to founding ioMosaic® Corporation, Dr. Melhem was president of Pyxsys Corporation; a technology subsidiary of Arthur D. Little Inc. Prior to Pyxsys and during his twelve years tenure at Arthur D. Little, Dr. Melhem was a vice president of Arthur D. Little and managing director of its Global Safety and Risk Management Practice and Process Safety and Reaction Engineering Laboratories.

Dr. Melhem holds a Ph.D. and an M.S. in Chemical Engineering, as well as a B.S. in Chemical Engineering with a minor in Industrial Engineering, all from Northeastern University. In addition, he has completed executive training in the areas of Finance and Strategic Sales Management at the Harvard Business School. Dr. Melhem is a Fellow of the American Institute of Chemical Engineers (AIChE) and Vice Chair of the AIChE Design Institute for Emergency Relief Systems (DiERS).

Contact Information

Georges. A. Melhem, Ph.D., FAIChE
E-mail. melhem@iomosaic.com

ioMosaic Corporation
93 Stiles Road
Salem, New Hampshire 03079
Tel. 603.893.7009, x 1001
Fax. 603.251.8384
web. www.iomosaic.com

How can we help?

Please visit www.iomosaic.com and www.iokinetic.com to preview numerous publications on process safety management, chemical reactivity and dust hazards characterization, safety moments, video papers, software solutions, and online training.

In addition to our deep experience in process safety management (PSM), chemical reaction systems, and the conduct of large-scale site wide relief systems evaluations by both static and dynamic methods, we understand the many non-technical and subtle aspects of regulatory compliance and legal requirements. When you work with ioMosaic® you have a trusted ISO certified partner that you can rely on for assistance and support with the lifecycle costs of relief systems to achieve optimal risk reduction and PSM compliance that you can evergreen. We invite you to connect the dots with ioMosaic®.

We also offer laboratory testing services through ioKinetic® for the characterization of chemical reactivity and dust/flammability hazards. ioKinetic® is an ISO accredited, ultramodern testing facility that can assist in minimizing operational risks. Our experienced professionals will help you define what you need, conduct the testing, interpret the data, and conduct detailed analysis. All with the goal of helping you identify your hazards, define and control your risk.

Appendices

The following appendices provide a listing of potential failure scenarios for a variety of processing equipment along with potential mitigation and risk reduction measures. The potential mitigation and risk reduction measures are based on the "CCPS Guidelines for Design Solutions for Process Equipment Failures, August, 1998". Also see "Guidelines for Engineering Design for Process Safety, 2nd Edition, April, 2012" and "CCPS Guidelines for Inherently Safer Chemical Processes: A Life Cycle Approach, 3rd Edition, 2019".

A Vessels

A.1 Overpressure

A.1.1 Liquid overfill resulting in back pressure or excessive static head

- Vessel design accommodating maximum supply pressure
- Use open vent or overflow line
- Emergency relief devices
- Level device interlocked to prevent overfill
- Instructions to monitor level during transfer and intervene to prevent overfill
- Verify tank has sufficient free board prior to transfer

A.1.2 Inadvertent or uncontrolled opening of high pressure utility system

- No utility connections above pressure rating of vessel
- Incompatible utility couplings to prevent connections of high pressure utilities
- Mechanical flow restriction (e.g., restriction orifice) of utility with open vent on vessel
- Vessel design accommodating maximum utility pressure
- Emergency relief device on tank or utility line
- Pressure sensor interlocked to isolate utility pressure
- Labeling of utility connections

A.1.3 Ignition of flammable atmosphere in vessel vapor space

- Floating roof tank instead of fixed roof (see procedural)
- Ignition source controls (e.g., lightning protection, permanent grounding/bonding, non-splash filling including dip pipe, fill line flow restriction, or bottom inlet)
- Vessel design accommodating deflagration pressure
- Store below flash point (if not heating)
- Use non-intrusive instrumentation (e.g., radar level detection)
- Explosion venting (e.g. frangible roof for fixed roof tank)
- Store material at temperature below its flash point (cooling)
- Oxygen analyzer activated purge system with interlock to block tank flows
- Vapor space combustible concentration control
- Vapor space inerting
- Flame arrester
- Oxygen analyzer with alarm
- Instructions to feed empty tanks at low rate until fill line submerged, avoiding splash filling
- No transfers during electrical storms
- Low feed rate until floating roof is afloat

A.1.4 Excessive fill rate resulting in back pressure from venting vapor

- Use open vent (e.g., vent diameter larger than fill line for short vent lines)
- Flow restriction orifice in fill line
- Vessel design accommodating maximum supply pressure
- Flow shutdown interlock activated by high pressure or high flow
- Automated flow control loop on fill line with high flow alarm
- Emergency relief device
- Operating instructions to limit flow to a maximum safe value
- Operating instructions to monitor filling rate and intervene to prevent excessive fill rate

A.1.5 External fire

- Buried tank (consider environmental issues)
- Fireproof insulation (limits heat input)
- Slope-away diking with remote impounding of spills
- Locate outside fire affected zone
- Provide recommended tank-to-tank separation
- Secondary enclosure (submerged, tank-in-a-tank)
- Fixed fire protection water spray(deluge) and/or foam systems activated by flammable gas, flame, and/or smoke detection devices
- Emergency relief device
- Emergency response plan
- Manual activation of fixed fire protection water spray (deluge) and/or foam systems

A.1.6 Inadequate or obstructed vent path, resulting in high vapor space pressure during filling

- Use open vent
- Vessel design accommodating maximum supply pressure
- Vent screen to avoid entrance of foreign objects
- Emergency relief device
- Heat tracing of vent to avoid condensation and solidification
- Operating instructions to verify open vent path before initiating fill operation
- Operating instructions to periodically examine vent opening for obstructions

A.1.7 Internal heating/cooling coil leak or rupture

- Use of external heater/cooler (panel coil)
- Use of heating/cooling medium which is not reactive with vessel contents
- Vessel design accommodating maximum heating/cooling medium pressure
- Use electrical heating

- Emergency relief device
- High pressure interlock that activates utility closure
- Back pressure control with external heating/cooling circulation
- Periodic sampling/ analysis of contents for leakage
- Emergency action plan to transfer contents to safe location if adverse reaction can occur

A.1.8 Vessel contamination with high vapor pressure material (introduction of volatiles)

- Vessel design accommodating maximum expected pressure
- Use of incompatible couplings
- Emergency relief device
- Weak seam roof for tanks
- Isolation of volatile materials by blinding, removable spool, disconnection, etc.

A.1.9 Excessive heat input resulting in high vapor pressure

- Vessel design accommodating maximum expected pressure
- Limit the temperature or flow of the heating medium (e.g., use hot water instead of steam)
- Emergency relief device
- High temperature or pressure alarm and interlock which isolates the heating medium
- High temperature or pressure alarm with operator activation of heating medium isolation

A.1.10 Chemical reaction resulting in increased pressure

- Vessel design accommodating maximum expected pressure
- Limit or avoid the storage or unintended accumulation of reactive materials
- Consume reactive intermediate process materials as soon as they are produced
- Emergency relief device
- High temperature and/or pressure alarm and automatic addition of quench/diluent fluid or inhibitor
- Automatic activation of emergency cooling system

- Operating instructions to periodically test for inhibitor concentration
- High temperature and/or pressure alarm and manual addition of quench, diluent or inhibitor
- Manual activation of quench or cooling system
- Periodic draining of accumulation points (i.e., knock-out pots)

A.1.11 Control or equipment failure in vapor recovery system on refrigerated/chilled storage

- Vessel design accommodating maximum expected pressure
- Additional insulation to prolong acceptable refrigeration outage
- Emergency relief device
- High pressure interlock to automatically start spare compressor
- Operator startup of spare compressor on high pressure indication

A.1.12 Roll-over of stratified layers, resulting in high vapor pressure

- Vessel design accommodating maximum expected pressure
- Use of in-line mixer external to vessel to premix feeds
- Provide tank filling system design that avoids tank stratification (e.g., top splash filling)
- Mechanically agitate or recirculate tank contents
- Emergency relief device
- Operating instructions on filling procedure to avoid stratification

A.1.13 Failure of upstream process controls, resulting in vapor or flashing liquid feed

- Vessel design accommodating maximum expected or upstream pressure
- Ensure control valves are not oversized
- Emergency relief device
- High pressure alarm and interlock which isolates the inlet flow(s)
- Operator activation of flow isolation on high pressure indication

A.1.14 Ambient temperature change, resulting in higher vapor space pressure

- Vessel design accommodating maximum expected pressure
- Use of buried (underground or aboveground) tank
- Insulate tank
- Open vent on fixed roof tanks
- Place tank under a roof or indoors
- Emergency relief deviceor breather vent valve
- Automatic external cooling water spray
- Operator activation of water spray on indication of high temperature in vessel

A.1.15 Blocked outlet flow path

- Vessel design accommodating maximum upstream pressure
- Eliminate unnecessary outlet block valves
- Emergency relief device
- Interlock to isolate vessel inlet or trip feed pump on high pressure
- Procedures for securing valves open via seals or locks

A.1.16 Ignition/reaction due to high temperature at unwetted internal heating element surface

- Vessel design to accommodate maximum expected temperature and pressure
- Use of external heat recirculation system
- Maintain submergence of heating surface by locating liquid withdrawal connection above the heating element
- Limit temperature of heating medium
- Selection of materials to avoid rust (i.e., eliminate potential catalytic effects)
- Automatic level control with low level alarm and shutdown of liquid withdrawal system to ensure liquid is above heating surface at all times
- Vapor space inerting
- Operating instructions to maintain liquid level above heating surface at all times
- Manual response to low level indication

A.1.17 Heating and thermal expansion of liquid

- Install open overflow nozzle to containment system
- Elimination of all unnecessary heating connections
- Eliminate capability to "block in" system
- Temperature controls on heating medium to prevent overheating
- High level shutoff preventing liquid from rising above level where expansion would cause overfill
- Thermal expansion relief valve
- Operating instructions on control of temperature below a certain limit, or restrictions on the length of time that heat can be applied
- Instructions on limiting the maximum liquid level
- Manual shutoff on detection of high level
- Instructions on draining vessel or isolating source of heat input before blocking in

A.1.18 Electrostatic spark discharge and ignition of vapors during charging of solids through an open manhole or charging chute resulting in deflagration or flash fire (batch or semi-batch)

- Eliminate addition of materials as solids (e.g., use slurry)
- Charging of solids through a nozzle by means of a closed system (e.g., hopper and rotary airlock, screw feeder, double-dump valve system, etc.)
- Automatic inerting of vessel prior to solids addition
- Ground indicator with interlock to prevent manhole opening if ground connection is faulty
- Manual inerting of vessel prior to solids addition
- Procedures for manual grounding and bonding of solids container and funnel to vessel
- Ground operator
- Avoid use on non-conductive plastic containers

A.1.19 Ignition of flammable atmosphere in tank vapor space following seal failure on internal floating roof (Floating Roof Tank)

- Provide double roof seal
- Provide adequate natural ventilation between fixed roof and floating deck
- Eliminate fixed roof provided over the floating deck
- Ignition source controls (e.g., lightning protection, permanent grounding/bonding)
- Use of fixed roof tank with inerting
- Provide inerting between fixed roof and floating deck
- End-of-line flame arrester
- Periodic inspection of roof seals

A.2 Underpressure or Vacuum

A.2.1 Failure of vacuum system control

- Vessel design to accommodate maximum vacuum (full vacuum rating)
- Vacuum relief device
- Automatic isolation of vacuum system on high vacuum
- Manual vacuum breaking on indication of high vacuum

A.2.2 Obstructed vent path

- Vessel design to accommodate maximum vacuum (full vacuum rating)
- Use of blanketing gas pressure control system to minimize vacuum
- Vacuum relief device
- Heat tracing of vent to avoid condensation and solidification
- Low pressure interlock to isolate pump out
- Operating instructions to verify open vent path before initiating withdrawal operation
- Operating instructions to periodically examine vent opening for obstructions

A.2.3 Uncontrolled condensation/absorption of vapor phase component

- Vessel design to accommodate maximum vacuum (full vacuum rating)
- Insulation
- Open vent
- Locate tank inside building
- Use of blanketing gas pressure control system to minimize vacuum
- Vacuum relief system
- Feed heater
- Operating procedure for monitoring addition of materials

A.2.4 Excessive liquid withdrawal rate

- Vessel design to accommodate maximum vacuum (full vacuum rating)
- Open vent
- Restrict withdrawal rate
- Use of blanket gas pressure control system to minimize vacuum
- Vacuum relief system
- Procedural limitations on the maximum rate of liquid withdrawal

A.2.5 Ambient temperature change, resulting in vapor space vacuum

- Vessel design to accommodate maximum vacuum (full vacuum rating)
- Open vent on fixed roof tanks
- Insulation
- Locate tank inside building
- Use of blanket gas pressure control system to minimize vacuum
- Vacuum relief device
- Manual vacuum breaking on low pressure alarm

A.2.6 Control or equipment failure in vapor recovery system on refrigerated/chilled storage

- Vessel design to accommodate maximum vacuum (full vacuum rating)
- Use of blanket gas pressure control system to minimize vacuum
- Air vacuum breaker device
- Interlock to shutdown compressor/blower on low pressure
- Manual shutdown of compressor/blower on low pressure alarm

A.3 High external level liquid

A.3.1 High external pressure on vessel walls from water level in dike or vault resulting in dislodging tank or external collapse of tank wall

- Vessel design to accommodate maximum external pressure
- Use of remote impounding instead of dike
- Anchor tanks
- Elevate tank
- Dike level measurement with automatic drain or pump-out
- Storm water drain system
- Operating instructions to inspect dike periodically and drain as necessary
- Operating instructions to drain storm water collected in the dike after heavy rainfall
- Keep tanks filled to a minimum liquid level

A.4 High Temperature

A.4.1 High temperature material fed to vessel

- Vessel design to accommodate maximum expected temperature and pressure of feed material(s)
- High temperature interlock to activate cooling or shut off feeds at desired temperature
- Instructions to cool or shut off feed when temperature rises above a certain level

A.4.2 Control failure of heating/cooling system

- Vessel design to accommodate maximum expected temperature and pressure experienced due to loss of heat transfer
- Use of heating medium whose maximum temperature is limited to vessel design temperature
- High temperature alarm and shutdown interlock
- Auxiliary cooling/quench or heat transfer system
- Emergency relief device
- Manual shutdown on high temperature indication

A.4.3 Chemical reaction

- Vessel design to accommodate maximum expected temperature and pressure of a possible exothermic reaction
- Substitute less-reactive material
- Emergency relief device
- High temperature alarm and interlock shutdown
- Automatic addition of reaction inhibitor and/or quench fluid
- Automatic activation of emergency cooling system
- Manual initiation of high temperature shutdown and/or quench/cooling addition

A.4.4 External fire

- Use of buried (underground or aboveground) tank
- Insulate with fireproof insulation
- Provide remote impounding of flammable liquid spills
- Locate vessel to minimize exposure
- Fixed fire protection - water spray (deluge) and/or foam systems
- Emergency relief device
- Fire detectors
- Emergency response procedures

A.4.5 Excessive mechanical agitation

- Vessel design to accommodate maximum expected temperature and pressure
- Limit agitator motor power
- Leave vessel uninsulated to allow heat loss
- Agitator shutdown on high temperature detection
- Instructions to turn off agitator on high temperature indication

A.5 Low Temperature

A.5.1 Low ambient temperature

- Vessel design to accommodate minimum expected (ambient) temperature
- Use of buried (underground or aboveground) tank
- Insulate tank
- Locate equipment indoors
- Automatic activation of heating system
- Manually activate heating system or drain materials which could freeze

A.5.2 Control failure of heating/cooling system

- Vessel design to accommodate minimum expected temperature
- Low temperature alarm and shutdown interlock
- Auxiliary heating system
- Operate system manually or activate back-up heating/cooling system

A.5.3 Low temperature material fed to vessel

- Vessel design to accommodate minimum expected feed temperature
- Low temperature alarm and feed isolation interlock
- Low temperature alarm activates external heating
- Instructions to isolate feed on low temperature indication

A.5.4 Refrigerant leak into vessel

- Vessel design to accommodate minimum expected refrigerant temperature
- Use refrigerant with vapor pressure below process pressure
- Low temperature alarm and refrigerant system shutdown and/or isolation interlock
- Manual system shutdown on low temperature indication

A.5.5 Depressuring of vessel containing liquified gases

- Provide metallurgy suitable for low temperature
- Interlock to close depressuring valve at specific pressure
- Instructions to deinventory liquid before depressuring

A.6 Overfill

A.6.1 Level control failure causing spill

- Install open overflow nozzle to containment system
- Closed loop filling
- High level alarm and automatic feed cutoff/isolation
- Instructions to stop feed when level reaches a certain point

A.6.2 Incorrect or unanticipated cross-connection

- Install open overflow nozzle to containment system
- Use of dedicated connections
- Use of incompatible connections
- High level alarm and automatic feed cutoff/isolation
- Operating instructions on correct or permitted cross-connections between tanks and vessels
- Operating/maintenance instructions to isolate tanks via blinding and disconnection
- Manual isolation on high level

A.6.3 Leak from heating/cooling system

- Install open overflow nozzle to containment system
- External heating/cooling system
- Operation of heating/cooling system at pressures below process pressure
- Double tubesheet heat exchanger
- Intermediate heat transfer fluid at a pressure below process pressure
- High level alarm and automatic heating/cooling medium cutoff/isolation
- Leak detection devices (e.g., pH, conductivity, capacitance) and manual isolation

A.6.4 Leak or excessive fill from liquid utility system (e.g., utility water)

- Install open overflow nozzle to containment system
- Orifice restriction in utility connection
- High level alarm with utility isolation interlock
- Operator isolation (e.g., disconnection, blinding, double block and vent) of utilities
- Leak detection devices (e.g., pH, conductivity, capacitance) and manual isolation

A.7 Low Level

A.7.1 Level control failure

- Locate underflow nozzle to maintain a minimum liquid level in the vessel
- Low level alarm with shutoff preventing further liquid withdrawal from vessel via either pump shutdown or closure of block valve
- Manual shutoff on low level indication

A.7.2 Incorrect or unanticipated cross-connection causing uncontrolled outflow

- Locate underflow nozzle to maintain a minimum liquid level in the vessel
- Eliminate all unnecessary cross-connections
- Use incompatible couplings to avoid improper cross-connections where hoses are used

- Low level alarm with shutoff preventing further liquid withdrawal from vessel via either pump shutdown or closure of block valve
- Operating instructions on the correct or permitted cross-connections between tanks and vessels
- Operating/maintenance instructions to isolate tanks via blinding and disconnection
- Manual outflow isolation on low level indication

A.7.3 Ignition of flammable atmosphere in tank vapor space following low level that results in floating roof sitting on its internal legs (Floating Roof Tank)

- Locate underflow nozzle to maintain a minimum liquid level in the tank
- Low level alarm with interlock to automatically shutdown the transfer pump
- Operating instructions to monitor tank level periodically

A.8 Loss of Containment

A.8.1 Incompletely submerged agitator impeller causes excessive forces on vessel wall and heads

- Locate underflow nozzle to maintain a minimum liquid level in the vessel
- Agitator designed to run stably during filling and emptying (e.g., stiffer shaft, foot bearing)
- Low level shutoff preventing further liquid withdrawal from vessel
- Low level alarm with interlock to automatically shutdown the agitator
- Instructions to stop agitation at predetermined level

A.8.2 Corrosion from process fluid

- Use corrosion resistant materials of construction
- Protective coatings and paints
- Double walled tank design
- Automatic addition of corrosion inhibitor
- Cathodic protection
- Corrosion coupons with periodic withdrawal and analysis

- Regular thickness measurements (i.e., nondestructive testing) at key points
- On-line corrosion analysis with alarm

A.8.3 Subsidence of soil below vessel

- Design and construction of tank foundation (piling and soil compaction)
- Respond to indication of tank subsidence

A.8.4 Frost heave (on cryogenic tanks)

- Design and construction of tank foundation (elevated pedestal)
- Insulation between tank and foundation
- Foundation heating system

A.8.5 Open drain connections

- Eliminate bottom connections
- Limit size of drain connections
- Self-closing drain valves
- Excess flow check valves
- Operating/maintenance instructions to blind drains when not in use

A.8.6 Loss of sealing fluid to vessel agitator resulting in emission of flammable or toxic vapors

- Circulate vessel contents via external, seal-less pump
- Use of double or tandem mechanical seal
- Alternative design which does not use a sealed agitator (i.e., continuous reactor with static mixer)
- Flammable and/or toxic vapor sensors interlocked with agitators
- Operators to visually check reservoir levels on regular basis
- Seal liquid reservoir to have low level sensor and alarm
- Flammable and/or toxic vapor sensors
- Operator emergency response to indications of a seal leak

A.8.7 Floating roof sinks from snow or water on top of roof or corrosion of roof/pontoons (Floating Roof Tank)

- Provide fixed roof to protect the floating roof
- Double deck or pontoon floating roof
- Corrosion-resistant material selection for floating roof
- Operating procedures for periodic draining of roof
- Periodic inspection and repair of pontoons
- Emergency response procedures

A.8.8 Fire following seal failure on external floating roof (Floating Roof Tank)

- Use fixed roof tank
- Double roof seal
- Electrical bonding/grounding of roof and shell
- Fire fighting foam system

A.8.9 Underground Storage Tanks and Insulated Vessels Corrosin

Corrosion from:

- contaminated earth
- moisture trapped between insulation and vessel walls
- chemical contamination
- aggressive environment

Design options

- Protective coatings and paints
- Use above-ground construction
- Do not insulate tank
- Locate below-ground vessel in secondary containment
- Install weatherproof jackets to protect insulation from moisture especially where chlorides may also be present

- Corrosion coupons with periodic withdrawal and analysis
- Regular thickness measurements at key points
- Periodic leak detection

A.9 Wrong Composition

A.9.1 Incorrect or unanticipated cross-connection

- Use of dedicated connections
- Use of incompatible couplings
- Physically separate points of connection of incompatible materials
- Use of interlocks which prevent certain addition combinations
- Operating instructions on the correct or permitted cross-connections between tanks and vessels
- Isolate tanks and vessels via blinding and disconnection
- Sample/analyze prior to transfer
- Color coding and labeling of lines

A.9.2 Leaking tank roofs or coils

- Indoor location (shielded from rain)
- External heating/cooling with leak protection
- Electrical heating instead of steam
- Periodic analysis to detect the presence of water or other coil fluid in the stored material
- Periodic draining of floating roof

A.9.3 Change in feed composition

- Design for all possible feed variations
- On-line analyzer with alarms and interlock
- Intermittent sampling and analysis with instructions to cut-off feed

A.9.4 Incorrect inhibitor composition or concentration

- Operating instructions to analytically verify inhibition effectiveness periodically

A.10 Less Agitation

A.10.1 Failure of agitator causing stratification of immiscible layers

- External, inline mixing of feeds before entering tank
- Use of compatible/mutually soluble materials
- Agitator monitor interlocked to stop feed stream
- Automatic backup pump around system
- Manual activation of back-up pump around system
- Manual shut off of feed on detection of loss of agitation

B Reactors

The types of reactors covered in this section include:

- Batch reactors
- Semi-batch reactors
- Continuous-flow stirred-tank reactors (CSTR)
- Plug flow tubular reactors (continuous)
- Packed-bed reactors (continuous)
- Packed-tube reactors (continuous)
- Fluid-bed reactors

This following presents potential failure scenarios for reactors and suggests design alternatives for reducing the risks associated with such failures.

B.1 Overpressure (Batch, Semi-batch, and Plug Flow Reactors)

B.1.1 Overcharge of catalyst resulting in runaway reaction

- Use dedicated catalyst charge tank sized to hold only the amount of catalyst needed
- Vessel design accommodating maximum expected pressure
- Use different type of reactor
- Emergency relief device
- Pressure or temperature sensors actuating bottom discharge valve to drop batch into a dump tank with diluent, poison or short-stopping agent, or to an emergency containment area
- Automatic addition of diluent, poison, or short-stopping agent directly to reactor
- Limit quantity of catalyst added by flow totalizer
- Procedural controls on the amount or concentration of catalyst to be added
- Manual activation of bottom discharge valve to drop batch into dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area
- Manual addition of diluent, poison, or short-stopping agent directly to reactor
- Intermediate location for pre-weighed catalyst charges

B.1.2 Addition of a reactant too rapidly resulting in runaway reaction (Batch and Semi-batch Reactors)

- Limit delivery capacity of feed system to within safe feed rate limitations (e.g., screw feeder for solids or flow orifice for liquids)
- Vessel design accommodating maximum expected pressure
- Select feed system pressure characteristic so that feed cannot continue at reactor overpressure
- Use different type of reactor
- Temperature or pressure sensor interlocked to a shutoff valve in the feed line
- Emergency relief device
- Pressure or temperature sensors actuating bottom discharge valve to drop batch into a dump tank with diluent, poison or short-stopping agent, or to an emergency containment area
- Automatic addition of diluent, poison, or short-stopping agent directly to reactor
- High flow shutdown alarm and interlock
- Manual addition of diluent, poison, or short-stopping agent directly to reactor
- Manual shutdown on high flow alarm
- Manual activation of bottom discharge valve to drop batch into dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area
- Procedural controls on concentration of reactants

B.1.3 Loss of agitation resulting in runaway reaction or hot bearing/seals causing ignition of flammables in vapor space (Batch, Semi-batch and CSTR Reactors)

- Vessel design accommodating maximum expected pressure
- Use different type of reactor (plug flow)
- Alternative agitation methods (e.g., external circulation eliminates shaft seal as a source of ignition in vapor space)
- Agitator power consumption or rotation indication interlocked to cutoff feed of reactants or catalyst or activate emergency cooling
- Uninterrupted power supply backup to motor
- Emergency relief device

- Pressure or temperature sensors actuating bottom discharge valve to drop batch into a dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area
- Inerting of vapor space
- Provide nitrogen buffer zone around seal using enclosure around seal
- Automatic agitator trip on low agitation (velocity) sensor, low seal fluid, or low shaft speed
- Operators to visually check mechanical seal fluid on regular basis
- In-vessel agitation (velocity) sensor with alarm
- Mechanical seal fluid reservoir low level sensor with alarm
- Speed or vibration sensor with alarm
- Manual activation of bottom discharge valve to drop batch into dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area

B.1.4 Overcharge or overfeed of reactant resulting in runaway reaction (Batch and Semi-batch Reactors)

- Use of dedicated reactant charge tank sized only to hold amount of reactant needed
- Vessel design accommodating maximum expected pressure
- Use of continuous reactor
- Emergency relief device
- Reactant feed charge interlocked via feed totalizer or weight comparison in charge tank
- Pressure or temperature sensors actuating bottom discharge valve to drop batch into a dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area
- Automatic addition of diluent, poison, or short-stopping agent directly to reactor
- Manual feed charge shutdown via indication from feed totalizer or weight comparison in charge tank
- Manual activation of bottom discharge valve to drop batch into dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area

B.1.5 Addition of incorrect reactant resulting in runaway reaction

- Use of dedicated feed tank and reactor for production of one product
- Vessel design accommodating maximum expected pressure
- Elimination of cross-connections
- Use of dedicated hoses and incompatible couplings for reactants where hose connections are used
- Emergency relief device
- Automatic feed shutdown based on detection of unexpected reaction progress (i.e., abnormal heat balance)
- Procedures to shutdown feed based on indication of unexpected reaction progress
- Procedure for double checking reactant identification and quality
- Dedicated storage areas/unloading facilities for reactants

B.1.6 Loss of cooling resulting in runaway reaction

- Vessel design accommodating maximum expected pressure
- Use of large inventory of naturally circulating, boiling coolant to accommodate exotherm
- Low coolant flow or pressure or high reactor temperature to actuate secondary cooling medium via separate supply line (e.g., city water or fire water)
- Automatic isolation of feed on detection of loss of cooling
- Emergency relief device
- Pressure or temperature sensors actuating bottom discharge valve to drop batch into a dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area (this approach may not be effective for systems where there is a significant increase in viscosity such as polymerization of monomers.)
- Automatic addition of diluent, poison, or short-stopping agent directly to reactor
- Manual activation of secondary cooling system
- Manual activation of bottom discharge valve to drop batch into dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area
- Manual addition of diluent, poison, or short-stopping agent directly to reactor

B.1.7 Overactive and/or wrong catalyst results in runaway reaction

- Vessel design accommodating maximum expected pressure
- Use prediluted catalyst
- Emergency relief device
- Automatic isolation of catalyst and/or feed based on detection of unexpected reaction rate (i.e., abnormal heat balance)
- Pressure or temperature sensors actuating bottom discharge valve to drop batch into dump tank with diluent, poison, or short-stopping agent, or to an emergency containment area
- Passivate fresh catalyst prior to use
- Procedures for testing and verification of catalyst activity and identification
- Manual isolation of catalyst and/or feed based on detection of unexpected reaction rate
- Manual addition of diluent, poison, or short-stopping agent directly to reactor

B.1.8 Inactive and/or wrong catalyst leading to delayed runaway reaction in reactor or downstream vessel

- Reactor or downstream vessel design accommodating maximum expected pressure
- Emergency relief device
- Automatic isolation of catalyst and/or feed based on detection of unexpected reaction rate (i.e., abnormal heat balance)
- Procedures for testing and verification of catalyst activity and identification
- Manual isolation of catalyst and/or feed based on detection of unexpected reaction rate

B.1.9 Underfeed of diluent resulting in insufficient heat sink

- Vessel design accommodating maximum expected pressure
- Automatic feed isolation on detection of low diluent addition
- Automatic isolation of feed based on detection of unexpected reaction rate (i.e., abnormal heat balance)
- Manual feed isolation on detection of low diluent addition
- Manual isolation of feed based on detection of unexpected heat balance

B.1.10 Reactants added in incorrect order (Batch and Semi-batch)

- Vessel design accommodating maximum expected pressure
- Sequence control via programmable logic controller
- Interlock shutdown of reactant addition based on detection of mis-sequencing
- Automatic isolation of feed based on detection of unexpected reaction progress (i.e, abnormal heat balance)
- Manual isolation of feed based on detection of unexpected reaction progress
- Manual isolation of feed based on indication of mis-sequencing

B.1.11 External fire initiates runaway reaction

- Fireproof insulation (reduced heat input)
- Slope-away grading under reactor to remote spill collection
- Locate reactor outside of fire affected zone
- Automatically activated fixed fire protection - water spray (deluge) and/or foam systems
- Emergency relief device
- Automatic reactor dump to dump tank with diluent, poison, or short stopping agent
- Automatic injection of diluent poison or short-stopping agent into reactor
- Manual activation of fixed fire protection
- Manual reactor dump to dump tank with diluent, poison or short-stopping agent
- Manual injection of diluent, poison or short-stopping agent into reactor

B.1.12 Feed of monomer emulsion breaks into a separate oil phase on top of a water phase while being fed to the reactor leading to runaway reaction

- Vessel design accommodating the maximum pressure arising from runaway reaction of bulk (non-emulsified) monomer phase
- Static mixer ahead of reactor
- Emergency relief device accommodating the maximum pressure arising from runaway reaction of bulk (non-emulsified) monomer phase
- Automatic feed shut-off or dumping on change of heat balance

- Operator samples the monomer emulsion feed and observes that sample is stable without agitation for a predetermined length of time before feed is begun
- Manual feed shut-off or dumping on change of heat balance

B.1.13 High reactor temperature due to failure of heating system initiates runaway reaction

- Limit temperature of heating media
- Vessel designed for maximum pressure
- Emergency relief device
- Automatic depressuring
- Automatic injection of inhibitor
- Automatic isolation of heating media or feed
- Emergency cooling response
- Manual dumping of reactor contents
- Manual injection of inhibitor
- Manual isolation of heating media or feed

B.2 High Temperature (Continuous Packed Bed or Packed Tube Reactors)

B.2.1 Hot spot develops in catalyst exposing vessel wall to high temperature and potential mechanical failure or initiation of runaway reaction

- Use alternative reactor design (e.g., fluid bed)
- Use multiple small diameter beds to reduce maldistribution
- Minimize reactor head space volume to reduce residence time (partial oxidation reactors) and mitigate autoignition
- High temperature sensors interlocked to shut down reactor
- Automatic depressuring based on detection of high bed temperatures or low flow
- Automatic introduction of quench fluid into packed bed or tubes based on detection of high local temperature
- Manual shutdown of reactor upon detection of high temperature in bed
- Monitoring of exterior wall temperature with infrared optical detection system

- Manual depressuring based on detection of high bed temperature
- Manual introduction of quench fluid into packed bed or tubes on detection of high local temperature
- Procedures for packing tubes to ensure uniformity of catalyst filling

B.3 Reverse Flow

B.3.1 Reactor contents inadvertently admitted to upstream feed vessel resulting in runaway reaction

- Vessel design accommodating maximum expected pressure
- Provide positive displacement feed pump instead of centrifugal pump
- Elevate feed vessel above reactor with emergency relief device on reactor set below feed vessel minimum operating pressure
- Provide check valve(s) in feed line
- Automatic closure of isolation valve(s) in feed line on detection of low or no flow, or reverse pressure differential in feed line
- Emergency relief device on feed vessel or feed line
- Manual closure of isolation valve(s) in feed line on detection of low or no flow in feed line

B.4 Wrong Composition

B.4.1 Contamination from leakage of heating/cooling media or introduction of other foreign substances (e.g., corrosion)

- Use heat transfer fluid that does not react with process fluid
- Vessel design accommodating maximum expected pressure
- Use jacket rather than internal coil for heat transfer
- Upgrade metallurgy or use resistant liner
- Heat transfer loop pressure lower than process pressure
- Emergency relief device
- Periodic testing of process fluid for contamination
- Procedures for leak/pressure testing of jacket, coil or heat exchanger prior to operation
- Procedure for testing liner with continuity meter

B.4.2 Incomplete reaction due to insufficient residence time, low temperature, etc. leading to unexpected reaction in subsequent processing steps (in reactor or downstream vessel)

- Reactor or downstream vessel design accommodating maximum expected pressure
- Automatic feed isolation based on detection of low reactor temperature
- Automatic feed isolation based on continuous on-line reactor composition monitoring
- Manual feed isolation based on detection of low reactor temperature
- Manual feed isolation based on continuous on-line reactor composition monitoring or “grab” sampling

C Piping and Piping Components

This section presents potential failure scenarios for piping and piping components and suggests design alternatives for reducing the risks associated with such failures. The types of piping and piping components covered include:

- Piping (metallic, nonmetallic, lined, jacketed, double walled)
- Components (flanges, expansion joints, gaskets, bolts, etc.)

This section presents only those failure modes that are unique to piping and piping components. Some of the generic failure scenarios pertaining to vessels may also be applicable to piping and piping components. Consequently, this section should be used in conjunction with section A. Unless specifically noted, the failure scenarios apply to more than one class of piping and piping components.

C.1 Overpressure

C.1.1 Blockage of piping and valves and flame arresters due to solid deposition

- Size piping system to maintain minimum required velocity to avoid deposition
- Piping designed for maximum expected pressure
- Eliminate flame arrester
- Emergency relief device
- Removal of solids from process stream (KO pot, filter, etc.) with automatic blowdown of solids
- Tracing of piping to minimize solid deposition
- Removal of solids from process stream (KO pot, filter, etc) with manual blowdown of solids
- Periodic manual system cleaning
- Operator response to high pressure alarm
- Periodic cleaning via flushing, blowdown, internal line cleaning devices (e.g., “pigs”)
- Use parallel switchable flame arresters

C.1.2 Valve in line rapidly closed resulting in liquid hammer and pipe rupture

- Limit closing rate for motor operated valves via appropriate gear ratio
- Limit closing rate for pneumatic actuator via restriction orifice in air line
- Use slow closing manual valves (i.e., gate instead of quarter turn)
- Provide surge arrester
- Operating procedures to close valves slowly

C.1.3 Thermal expansion of liquid in blocked-in line leading to line rupture

- Elimination of potential for blocking in by removing valves and other closures (e.g. blinds)
- Pressure relief device
- Expansion tank
- Procedures for draining of all blocked-in lines during shutdown

C.1.4 Automatic control valve opens inadvertantly leading to high pressure downstream of the valve

- Design all downstream piping and equipment to handle full upstream pressure
- Provide limit stop to prevent control valve from opening fully
- Pressure relief device to protect downstream piping

C.1.5 Block valve upstream or downstream of relief device accidentally closed resulting in loss of relief capability

- Eliminate all block valves in relief path
- Provide trans-flow three-way block valve at inlet of dual relief device installation
- Car-seal open or lock open all block valves upstream and downstream of relief valves per applicable codes and provide administrative procedures to regulate opening and closing of such valves

C.1.6 Blockage of relief device by solids deposition (polymerization, condensation)

- Provide flow sweep fitting at inlet of relief device
- Use rupture disks alone or in combination with safety valves with appropriate rupture disk leak detection
- Automatic flush of relief device inlet with purge fluid
- Manual periodic or continuous flush of relief device inlet with purge fluid

C.1.7 Deflagration and detonation in pipelines causing loss of containment

- Limit temperature, pressure or pipe diameter to prevent DDT from occurring (e.g., acetylene)
- Multiple rupture disks/explosion vents located at appropriate points on piping
- Detonation or suitable deflagration arresters between protected equipment and potential ignition sources
- Seal pot isolating ignition source (e.g., flare)
- Operate outside flammable range, e.g., O2 analyzer or hydrocarbon analyzer and fast operated purge (N2 or enrichment)
- Detect gas flame and actuate fast closing valve or supression system

C.2 High Temperature

C.2.1 Faulty tracing or jacketing of line leading to hot spots resulting in exothermic reaction

- Use of insulating material between tracer and pipe (sandwich tracer)
- Use of heat transfer media with maximum temperature limited to a safe level (jacketed pipe)
- Electrical tracing with temperature limitation controls
- Operator action in response to high temperature indication and alarm

C.2.2 External fire leading to undesired process reaction (e.g., acetylene decomposition)

- SS weather barriers and banding
- Fireproof insulation
- Continuous welded pipe
- Graphitic gaskets

- Elimination of stagnant areas
- Automatic emergency response
- Manual emergency response

C.3 Low Temperature

C.3.1 Cold weather conditions causing freezing of accumulated water or solidification of product in line or deadends

- Insulation of process lines
- Elimination of collection points or deadends
- Deadends should be sloped to avoid accumulation
- Blowdown lines should be sloped to avoid accumulation
- Heat tracing of lines
- Automatic drainage of potential collection points
- Procedures to maintain a minimum flow through line
- Manual draining of potential collection points

C.3.2 Condensation in steam lines due to cold ambient conditions resulting in steam hammer

- Heat tracing of lines
- Procedures to slowly warm-up downstream piping

C.4 High Flow

C.4.1 High fluid velocity in pipe which causes erosion especially if two phase flow or abrasive solids are present leading to loss of containment

- Sizing of pipe to limit velocities
- Material selection to resist erosion
- Heavier walls at tees, elbows, and other high abrasion points
- Minimize use of fittings where erosion can occur
- Instructions to limit flow velocity
- Periodic inspection of high wear points

C.4.2 High pressure drop across control valve causing flashing/vibration leading to loss of containment

- Locate valve as close to the vessel inlet as possible
- Provide multiple intermediate pressure letdown devices

C.5 Reverse Flow

C.5.1 Differential pressure on joining lines, drains or temporary connections causing back flow of product resulting in undesirable reaction, overfilling, etc.

- Use incompatible fittings to prevent unwanted connections
- Use separate lines to final destination
- Check valve on lower pressure line to prevent reverse flow
- Automatic isolation on detection of low differential pressure
- Procedures for proper isolation of interconnected lines
- Manual isolation on detection of low differential pressure

C.6 Loss of Containment

C.6.1 Failure to isolate flow from sample connection, drain and other fittings resulting in discharge to environment

- Provide “deadman” (self-closing) valve
- Automatic closed loop sampling system
- Provide double block and bleed valves, valve plugs, caps, blinds, etc.

C.6.2 Breakage of sight glasses and glass rotameters due to overpressure, thermal stress, or physical impact

- Eliminate the use of sight glasses and rotameters
- Provide flow restriction orifice in glass connection
- Provide physical protection against damage (i.e., armored sight glass)
- Provide glasses with pressure design rating exceeding maximum expected pressure
- Provide excess flow check valves to limit discharge due to sight glass or rotameter failure

- Provide self-closing isolation valves or excess flow valves on inlet and outlet
- Procedure to normally isolate sight glass when not in use

C.6.3 Loss of containment from piping due to leak, flange leak, valve leak, pipe rupture, collision, or improper support

- Maximize use of all-welded pipe
- Avoid use of underground piping
- Use double walled pipe
- Minimize use of unnecessary fittings
- Use of higher integrity closures (e.g., clamped connectors)
- Shielding at flanges to prevent operator exposure
- Use of minimum diameter pipe for physical strength
- Proper design and location of piping supports
- Physical collision barriers
- Provide automatic isolation on detection of high flow, low pressure, or external leak
- Use fusible link valves for automatic closure under fire conditions
- Provide manual isolation via remotely located valve
- Procedural restrictions to avoid damage (crane restrictions, climbing restrictions)
- Periodic inspection for leaks

C.6.4 Pipe failure due to excessive thermal stress

- Expansion loops and joints
- Insulation of pipe joints
- Additional support to prevent sagging

C.6.5 Degradation of transfer hose between use results in hose leak

- Eliminate hose connections (hard piped)
- Use higher integrity hose (e.g., metallic braided)
- Use higher pressure hose
- Provide excess flow check valve upstream and check valve downstream of hose
- Automatic isolation based on detection of high flow, low pressure or external leak
- Use fusible link valves for automatic closure under fire conditions
- Pressure test transfer hose before use
- Manual isolation based on detection of high flow, low pressure or external leak
- Periodic replacement of hoses
- Provide hose protection (e.g., ramp) when laying hoses across roadway
- Avoid sharp angle changes in direction

C.6.6 Breakdown of pipe/hose lining

- Use pipe metallurgy which does not require lining
- Use semi-conductive liner to reduce degradation due to static build-up
- Use thicker liner material
- Limit liquid velocity to minimize static buildup
- Periodic thickness testing of metal pipe wall
- Periodic process stream analysis for metals content

C.7 Wrong Composition

C.7.1 Operator connects quick connect coupling to wrong connection

- Specify incompatible ends to prevent misconnections
- Avoid use of quick connects for hazardous service
- Procedures to prevent inadvertent cross-connections
- Labelling and color coding of lines

D Heat Transfer Equipment

This section presents potential failure scenarios for heat transfer equipment and suggests design alternatives for reducing the risks associated with such failures. The types of heat exchangers covered in this chapter include:

- Shell and tube exchangers
- Air cooled exchangers
- Direct contact exchangers
- Others types including helical, spiral, plate and frame, and carbon block exchangers

A summary of potential failure scenarios and available design options is provided below:

D.1 Overpressure

D.1.1 Corrosion/erosion of exchanger internals resulting in a heat transfer surface leak or rupture and possible overpressure of the low pressure side

- Double tube sheets
- Seal welding of tubes to tubesheets
- Open low pressure side return
- Design changes to reduce erosion (e.g., lower velocities, inlet baffle)
- Secondary heat transfer fluid
- Design pressure of low pressure side equal to design pressure of high pressure side
- Use of more corrosion resistant alloys
- Use of less corrosive heat transfer media
- Emergency relief device on low pressure side
- Corrosion detection device (e.g., coupons)
- Periodic inspection/ analysis of low pressure fluid for high pressure fluid leakage

D.1.2 Differential thermal expansion/contraction between tubes and shell resulting in tube leak/rupture (Fixed Tubesheet, Shell and Tube Exchanger)

- U-tube exchanger design
- Shell expansion joint or internal floating head
- Design pressure of low pressure side equal to design pressure of high pressure side
- Use of designs other than shell and tube (e.g., spiral, plate and frame)
- Emergency relief device on low pressure side
- Automatic control of introduction of process fluids on start-up and shutdown
- Procedural control of introduction of process fluids on start-up and shutdown
- Periodic inspection/ analysis of low pressure fluid for high pressure fluid leakage

D.1.3 Excessive tube vibration resulting in tube leak/rupture and possible overpressure of the low pressure side (Shell and Tube Exchanger)

- Mechanical design (e.g., proper baffle spacing) accommodating maximum anticipated inlet feed pressure/velocity
- Design pressure of low pressure side equal to design pressure of high pressure side
- Use of designs other than shell and tube (e.g., spiral, plate and frame)
- Emergency relief device on low pressure side
- Periodic inspection/ analysis of low pressure fluid for high pressure fluid leakage

D.1.4 Excessive heat input resulting in vaporization of the cold-side fluid (e.g., control system failure, cold-side bypass valve open)

- Limit the temperature of the heating medium
- Design pressure of cold-side fluid equal to maximum expected pressure
- Emergency relief device
- High temperature indication with alarm and interlock which isolates the heating medium
- Manual control of heating medium based on temperature indication

D.1.5 Loss of heat transfer due to fouling, accumulation of non-condensibles, or loss of cooling medium (Condensing Side)

- Design exchanger for suitable velocity to minimize fouling
- Heat exchanger design less prone to fouling (e.g., direct contact)
- Provide additional surface area in air cooler to heat transfer via natural convection
- Continuous open venting of non-condensibles
- Design for maximum expected pressure
- Emergency relief device
- Back-up cooling medium supply with automatic switch-over
- Automatic tempering of cooling medium temperature to avoid low tube wall temperature resulting in solids deposition
- Automatic venting of non-condensibles
- Automatic isolation of input flow on detection of high vent temperature
- Manual adjustment of cooling medium tempering
- Periodic exchanger cleaning
- Manual venting on high pressure indication
- Manual activation of backup cooling
- Manual isolation of input flow on detection of high vent temperature

D.1.6 Ambient temperature increase resulting in higher vaporization rate in air heated exchanger (air exchanger)

- Mechanical design accommodating maximum pressure/temperature
- Use heating medium other than air
- Emergency relief device
- Automatic adjustment of vaporization pressure to control vaporization rate
- Manual adjustment of vaporization pressure

D.1.7 Cold-side fluid blocked in while heating medium continues to flow

- Open cold side return
- Thermal relief device
- Interlock to isolate heating medium upon detection of no flow on cold-side
- Procedural controls on block valve closing
- Manual isolation of heating medium on indication of no flow on cold side

D.1.8 Excessive heat transfer rate due to ambient temperature drop or rain (Air Cooler)

- Mechanical design to accommodate minimum expected temperature and pressure
- Use of alternative heat exchanger designs
- Automatic vacuum breaking system
- Automatic air inlet temperature control via air preheating with steam or air recirculation
- Manual vacuum breaking
- Manual adjustment of air inlet temperature

D.2 High Temperature

D.2.1 External fire

- Use alternate heat exchanger design to minimize impact of external fire
- Fireproof insulation (limits heat input)
- Slope-away drainage with remote impounding of spills
- Locate outside fire affected zone
- Use cellular glass insulation to avoid insulation fires
- Fixed fire protection water spray (deluge) and/or foam systems activated by flammable gas, flame, and/or smoke detection devices
- Emergency relief device
- Emergency response plan
- Manual activation of fixed fire protection water spray (deluge) and/or foam systems

D.2.2 Loss of mechanical integrity of tube (High T on tube surface)

- Mechanical design to accommodate maximum expected temperature and pressure
- Design exchanger for suitable velocity to minimize fouling
- Use of heating medium whose design temperature is limited to exchanger design temperature
- Use of exchanger design less sensitive to fouling (e.g., scraped surface exchanger)
- Automatic control of heating medium temperature
- High temperature indication with alarm
- Manual control of heating medium temperature
- Periodic inspection

D.3 Low Temperature

D.3.1 Low ambient temperature causes fluid freezing and tube rupture air cooled exchanger

- Select different type of exchanger to minimize or eliminate consequences of freezing
- Provide air inlet temperature control via air preheating with steam or air recirculation
- Provide air flow control (e.g., variable pitch fans)
- Manual adjustment of air temperature or flow

D.4 Wrong Composition

D.4.1 Mixing of fluids resulting in exothermic reactions, phase changes, and/or fluid system contamination due to corrosion/erosion, vibration or differential thermal expansion

- Select heat transfer media which are chemically compatible with process materials
- Mechanical design to accommodate maximum expected temperature and pressure of a possible exothermic reaction
- Intermediate heat transfer fluid system
- Double tubesheet design
- Seal weld tubes to tubesheets
- Emergency relief device
- Downstream fluid analyzers with concentration alarms interlocked with automatic shutdown

- Downstream fluid analyzers with concentration alarms
- Periodic sampling and analysis of fluids

D.5 Loss of Containment

D.5.1 Vibration/fan failure and tube rupture due to impact with fan blade (Air Cooler)

- Use of alternative heat exchanger designs
- Vibration monitoring with automatic fan shutdown
- Manual fan shutdown on indication of excessive vibration

D.5.2 Scraper punctures heat transfer surface due to misalignment or entrance of foreign objects (Scraped Surface)

- Screens at entrance of heat exchanger to remove foreign objects
- Use of alternative exchanger designs
- Automatic shutdown of motor on high amperage or power
- Manual shutdown of motor on high amperage or power

D.5.3 Fire exposure causes gasket failure (Plate and Frame)

- Use of alternative exchanger design
- Locate exchanger outside fire affected zone
- Use fire resistant (metal jacketed) gaskets
- Use of welded plate design
- Provide splash shields around exchanger
- Emergency response procedures

D.5.4 Fire exposure causes combustion and failure of exchanger (Carbon Block)

- Use of alternative exchanger design
- Locate exchanger outside fire affected zone
- Emergency response procedures

E Mass Transfer Equipment

This section presents potential failure scenarios for mass transfer equipment and suggests design alternatives for reducing the risks associated with such failures. The types of mass transfer operations covered in this appendix include:

- Absorption
- Adsorption
- Extraction
- Distillation
- Scrubbing
- Stripping
- Washing

A summary of failure scenarios and design options follows below:

E.1 Overpressure

E.1.1 Migration of internals into lines resulting in blockages

- Design support grids, and hold down grids to minimize internal migration
- Vessel design accommodating maximum supply pressure
- Large surface area screens to avoid entrance of internals into lines
- Emergency relief device (e.g., upstream of potential blockage point)
- Differential pressure indication and automatic shutdown
- Differential pressure indication and manual shutdown and instructions to shutdown and inspect vessel

E.1.2 Blockage of packing / trays leading to excessive pressure in column

- Select and design internals to minimize blockage and fouling
- Use of vessel without internals (e.g., spray tower)
- Use of vessel designed for maximum expected pressure

- Emergency relief device upstream of potential blockage device
- Automatic shutdown on high pressure
- Differential pressure indication and instructions to shutdown and inspect vessel
- On-line wash to eliminate fouling material

E.1.3 Liquid/vapor decomposition initiated by high temperature resulting from loss of vacuum

- Vessel design accommodating maximum expected pressure
- Limit inventory of reactive materials
- Limit heating medium temperature
- Emergency relief device near expected point of reaction
- Automatic high temperature and/or pressure shutdown of heat input
- Continuous injection of reaction inhibitor
- Automatic isolation and purge of equipment with inert gas or loss of vacuum
- Operating instructions to periodically test for inhibitor concentration
- Operating instructions to shutdown on high temperature or high pressure

E.1.4 Autoignition/deflagration of vapor caused by air injection on loss of vacuum

- Vessel designed to accomodate maximum pressure
- Emergency relief device
- Automatic vacuum breaking on detection of low pressure with inert gas
- Pressure check for leaks before start-up

E.2 Underpressure or Vacuum

E.2.1 Uncontrolled condensation/absorption of vapor phase component

- Vessel design to accommodate maximum vacuum
- Use of blanketing gas pressure control system to minimize vacuum
- Vacuum relief system
- Operating procedure for manual addition of vacuum breaking gas

E.2.2 Process liquid reintroduced into improperly cooled adsorber and subsequent vaporization (adsorbers)

- Vessel design accommodating maximum expected pressure
- Emergency relief device
- Interlock to isolate feed on detection of high bed temperature or pressure
- Proper procedures for reinstating process flow after regeneration and cooling
- Manual isolation procedure on high temperature/pressure alarm

E.3 High Temperature

E.3.1 Premature introduction of process stream containing air to hot adsorbent bed (adsorber)

- Select adsorbent to minimize combustion potential
- Interlock to isolate feed on detection of high bed temperature
- Automatic emergency depressuring and/or flooding/inerting on detection of high temperature
- Procedures for reinstituting process flow after regeneration
- Manually isolate feed on detection of high bed temperature
- Manual emergency depressuring and/or flooding/inerting on detection of high temperature

E.3.2 Fire when exposing packing internals with flammable material to air during maintenance or by air introduction on loss of vacuum

- Use of non-stick internals (e.g., plastic packing)
- Use vessel without internals (e.g., spray tower)
- Instructions for proper vessel wash-out/cooldown prior to opening
- Procedures for maintenance under inert atmosphere if necessary

E.3.3 Poor vapor flow distribution through adsorbers leads to hot spots and fire (adsorbers)

- Proper design of vessel distributors to avoid regions of flow maldistribution in the bed
- Minimize adsorber cross sectional area
- Continuous monitoring of bed temperatures or CO at certain locations and interlock shutdown and/or inerting/flooding on high temperature
- Instructions to monitor bed temperature/CO and take appropriate action (e.g., inerting/flooding)

E.4 High or Low Level

E.4.1 Interfacial level control failure in liquid-liquid extractor resulting in carryover of unwanted material to downstream equipment (extractor)

- Control interface level via overflow leg or weir
- High/low interfacial level alarm with shutoff preventing further liquid withdrawal from vessel
- Manual vessel interfacial level control

E.5 Wrong Composition

E.5.1 High concentration of flammables in the inlet stream to a carbon bed adsorber leading to deflagration (carbon bed adsorber)

- Vessel design to accommodate maximum expected pressure
- Automatic control of inlet stream outside flammable limits
- Deflagration venting
- Inerting of process stream
- Automatic isolation of feed on detection of high flammable concentration
- Manual isolation on detection of high flammable concentration

E.5.2 Impurities in adsorbents catalyze decomposition / reaction of adsorbate (adsorber)

- Verification of adsorbent compatibility with process materials
- Testing of adsorbents prior to loading into vessel

E.5.3 Low moisture content in activated carbon bed adsorber leads to fire (carbon bed adsorber)

- Automatic steam injection to rehydrate bed prior to feed start
- Automatic water deluge on detection of fire
- Verification of adsorbent moisture content prior to placing in service
- Manual steam injection to rehydrate bed prior to feed start-up
- Manual water deluge on detection of fire

E.5.4 Excessive vapor flow resulting in carryover of liquid to undesired location

- Vessel design with proper vapor-liquid disengagement (e.g., low superficial vapor velocity)
- Liquid removal via demister, cyclone or other device with open liquid discharge
- Removal of liquid from the vapor stream using, for example, knock out pots with automatic level control
- Differential pressure indication and automatic reduction of vapor flow
- Differential pressure indication and instructions to reduce vapor flow

E.5.5 Failure to precondition adsorber bed before readmission of process stream resulting in high temperature (adsorber)

- Select adsorbents to adsorb only trace contaminants and not carrier gas (e.g., olefin purification)
- Automatic preconditioning sequence prior to feed startup
- Multi-point temperature monitoring with automatic shutdown of feed (for high pressure adsorbers)
- CO monitoring with automatic shutdown (for carbon bed adsorbers)
- Procedures for preconditioning adsorber bed

E.5.6 Accumulation of reactive material in section of fractionator leads to rapid decomposition (distillation columns)

- Vessel design accommodating maximum expected pressure
- Change in feedstock to avoid reactive material

- On-line measurement (e.g., level, temperature, analysis) and automatic side draw-off of reactive material
- On-line measurement (e.g., level, temperature, analysis) and manual removal of reactive material

E.5.7 Insufficient or excessive fractionation leading to compositions outside of metallurgical limits (e.g., corrosion)

- Select metallurgy suitable for worst case composition.
- On-line measurement (e.g., corrosion probes, stream analysis, temperature) and automatic operating adjustment
- On-line measurement (e.g., corrosion probes, stream analysis, temperature) and manual operating adjustment

F Fluid Transfer Systems

This section presents potential failure scenarios for fluid transfer systems and suggests design alternatives for reducing the risks associated with such failures. The types of fluid transfer equipment covered in this appendix include:

- Blowers
- Pumps
- Compressors

F.1 Overpressure

F.1.1 Failure of control or closure of downstream block valve, or failure to remove blind, or plugged outlet which deadheads pump/compressor resulting in possible overpressure and/or excessive temperature

- Minimum flow recirculation line to ensure a minimum flow through the machine (flow controlled by orifice)
- Downstream piping and seal specified to withstand deadhead pressure
- High temperature shutdown interlock
- High pressure shutdown interlock
- Low flow shutdown interlock
- Pressure relief device
- Minimum flow recirculation line (flow automatically controlled)
- Operator action in response to high temperature, pressure and/or low flow indication
- Procedural controls to avoid deadheading pump/compressor

F.1.2 Pump/compressor used for higher than design density fluid service especially during startup and upset conditions

- Design for maximum expected pressure
- Pressure relief device
- Automatic pump/compressor shutdown on high discharge pressure detection
- Operator action in response to high pressure indication

F.1.3 Leakage on suction side of blower/compressor pulls air into system creating a flammable atmosphere (blower or compressor)

- Positive pressure throughout system
- Automatic oxygen monitoring interlocked to blower and/or isolation valves on high oxygen measurement
- Inerting or gas enrichment system
- Automatic pressure control which limits rate of oxygen infiltration or negative pressure
- Flame arresters
- Explosion suppression systems

F.1.4 Exothermic decomposition of pumped/compressed fluid (e.g., acetylene) leading to overpressure

- Design casing to contain decomposition overpressure
- Limit individual stage compression ratio to avoid high temperature
- Eliminate dead legs and other stagnant regions
- High temperature/pressure shutdown interlock
- Emergency relief devices
- Operator action in response to high temperature indication

F.2 High Temperature

F.2.1 Failure of lubrication system resulting in bearing failure due to overheating(bearing)

- High bearing temperature shutdown interlock
- Low lubrication pressure/level shutdown interlock
- Operator action in response to high temperature indication/alarm on lube oil reservoir
- Operator action in response to low pressure alarm on the discharge of lube-oil pump

F.2.2 Loss of upstream/interstage cooling resulting in high enough inlet temperature in subsequent stages of the compressor to cause compressor damage (compressor)

- Choice of materials and design to maximum temperature conditions
- High temperature shutdown interlock
- Low coolant flow shutdown interlock
- Operator action in response to high inlet temperature and/or or low coolant flow indication / alarm.

F.2.3 Operation on total recycle without adequate cooling

- Choice of materials and design to maximum temperature conditions
- High temperature shutdown interlock
- Cooler in recycle loop
- Operator action in response to high temperature indication

F.3 Low Flow

F.3.1 Reduced flow to the inlet of a centrifugal pump causing cavitation, excessive vibration and damage to pump seal (centrifugal pump)

- Eliminate suction system restrictions
- Low flow shutdown interlock
- High vibration shutdown interlock
- Automatic recirculation from discharge to suction side on low flow alarm
- Operator action in response to low flow indication and/or high vibration

F.3.2 Reduced flow through a centrifugal compressor causing surge leading to high vibrations and compressor damage (centrifugal compressor)

- Use compressor design other than centrifugal
- Automatic anti-surge system
- Low flow shutdown interlock
- High vibration shutdown interlock

F.4 Reverse Flow

F.4.1 High pressure on discharge side of pump/compressor causes backflow leading to seal failure and loss of containment

- Use seal-less pumps
- Eliminate parallel machine
- Check valve placed at the discharge side
- Automatic isolation valve on discharge activated on machine trip or high pressure
- Pressure relief device
- Procedure for isolation of non-operating parallel machine

F.4.2 Backflow via recycle loop due to control system failure resulting in overpressure of low pressure stages and loss of containment (centrifugal compressor)

- Design low pressure stages for higher pressure
- Check valve or automatic isolation valve to protect against backflow from downstream side
- Restriction to limit recycle flow
- Pressure relief valve for protection of low pressure stages sized for maximum backflow

F.5 Overspeed

F.5.1 Compressor overspeed leading to equipment damage due to speed control system failure and loss of containment (Compressor)

- Use solid versus built-up rotor
- High speed alarm and compressor overspeed shutdown system

F.6 Loss of Containment

F.6.1 Particulate matter in pump feed leading to seal damage and loss of containment

- Double or tandem seals
- Use pump design that can accommodate solids (e.g., diaphragm)
- Automatic pump trip on detection of loss of seal fluid

- Automatic back-flushing strainer
- Provide a strainer or filter in pump or compressor inlet with manual cleaning
- Provide seal leak detection system with alarm
- Provide remotely operated isolation valves at inlet and outlet with manual activation
- Periodic inspection of shaft seals

F.6.2 Pump operated at a fraction of capacity resulting in excessive internal recirculation, frequent seal and bearing failure

- Use a pump size matched to the service
- Minimum flow recirculation line to ensure a minimum flow through the pump (flow controlled by orifice)
- Minimum flow recirculation line (flow automatically controlled)
- Procedural controls to avoid operating at too low a flow

F.6.3 Improper shaft alignment causing bearing and/or mechanical seal problems leading to seal leakage or hot-spot, resulting in ignition

- Alternative pump or compressor design without shaft alignment needs (e.g., diaphragm/piston)
- On-line vibration monitoring with automatic shutdown
- Operator action on alarm from axial displacement sensors
- Periodic audible/visual inspection of machine

F.7 Wrong Composition/Phase

F.7.1 Liquid in compressor suction leading to damage of compressor rotor (compressor)

- Use liquid-tolerant design (e.g., liquid ring compressor)
- Provide a Knock Out (KO) pot with automatic liquid removal and high level switch to trip the compressor.
- Heat trace the line between the KO pot and the compressor
- On-line vibration monitoring with automatic shutdown
- Operator action in response to high level alarm in the KO pot

G Solid/Liquid Separators

This section presents potential failure scenarios for solid-fluid separators, and suggests design alternatives for reducing the risks associated with such failures. The types of equipment covered in this appendix include:

- Centrifuges
- Filters
- Dust collectors
- Cyclones
- Electrostatic precipitators

G.1 Overpressure

G.1.1 Ignition of flammable vapors in centrifuge by static electricity(Centrifuges)

- Permanent grounding and bonding
- Use more electrically conductive wash liquid
- Use less volatile/flammable wash liquid
- Avoid use of non-conductive lined centrifuge
- Centrifuge design accommodating maximum expected pressure
- Use nonflammable or high flash point solvent
- Provide automatic inerting
- Provide low pressure or low flow sensor on nitrogen supply line with interlocks to shut down filter or centrifuge
- Deflagration venting
- Deflagration suppression
- Procedures for re-inerting prior to restart of a batch centrifuge
- Manual shutdown of batch centrifuge on detection of low inert gas pressure or flow
- Manual bonding and grounding for portable units

G.1.2 Relief device plugged by filter cake particles negating adequate overpressure protection (Pressure filters)

- Provide flow sweep fitting at inlet to relief device
- Filter design accommodating maximum expected pressure in place of relief device
- Provide rupture disk upstream of relief valve with appropriate rupture disk leak detection
- Automatic sweep of inlet to relief device with purge fluid
- Manual periodic flush of inlet to relief device with purge fluid

G.1.3 Ignition of flammable vapors in centrifuge or major mechanical damage caused by mechanical friction, e.g., out-of-balance basket rubbing against housing or bottom chute (Centrifuges)

- Elimination of flammable solvent
- Provide proximity/ vibration sensor interlocked to shut down centrifuge
- Provide automatic inerting
- Provide low pressure or low flow sensor on inert gas supply with interlock to shut down centrifuge
- Deflagration venting
- Deflagration suppression
- Operator shut down of centrifuge on detection of excessive vibration

G.1.4 Dust deflagration due to electrostatic spark discharge or glowing particles from upstream equipment(Cyclones, dust collectors, and electrostatic precipitators)

- Permanent bonding and grounding
- Equipment design accommodating maximum expected pressure
- Use other type of separator (e.g., wet-type precipitator or scrubber)
- Use nitrogen as conveying gas
- Deflagration venting
- Deflagration suppression
- Automatic isolation of associated equipment via quick closing valves or chemical barrier (flame suppression)

- Automatic introduction of inert gas via on-line oxygen analyzer
- Manual introduction of inert gas on detection of high oxygen via on-line oxygen analyzer

G.2 High Temperature

G.2.1 Fire caused by ignition of dust deposits on walls (tarry or sticky dust) or bags (fire may initiate deflagration)(Cyclones, dust collectors, and electrostatic precipitators)

- Use fire-retardant filter bags or ceramic cartridges
- Use of other type of separator (e.g., wet-type precipitator or scrubber)
- Automatic fire suppression system activated by high temperature sensor
- Automatic inerting system
- Operator activation of fire suppression system in response to high temperature indication
- Periodic cleaning of accumulated flammable dust deposits

G.2.2 Fire from pyrophoric filter cake exposed to air when filter is opened to remove cake (Batch Filters)

- Use filter with cake removal by spinning plates and/or sluicing with liquid (filter does not have to be opened up)
- Automatic fixed water spray
- Procedures to ensure that filter cake is sufficiently flushed with water before filter is opened up
- Manual activation of fixed water spray

G.3 Loss of Containment

G.3.1 (Vacuum belt filter, vacuum pan filter, rotary vacuum filter) Loss of vacuum on discharge resulting in excessive emission of toxic or flammable vapors

- Use totally enclosed, vapor-tight filter
- Local exhaust ventilation connected to a control system (vent condenser, adsorber, scrubber or incinerator)
- Operator shuts down operation in response to vapor detection alarm

G.3.2 Catastrophic bearing failure results in major equipment damage and possible process fluid leak/fire (Centrifuges)

- Interlock bearing temperature sensor to shut down the centrifuge at high temperature
- Automatic centrifuge shutdown on detection of lubricating oil low flow or pressure
- Automatic centrifuge shut down on detection of excessive vibration
- External automatic fire suppression system
- Operator shut down of centrifuge on detection of high bearing temperature, or lubricating oil low flow or pressure
- Manual activation of external fire suppression system

G.3.3 Mechanical failure caused by basket imbalance and vibration due to improper loading (Batch Centrifuges)

- Use continuous centrifuge design
- Consider alternate solid/fluid separator designs
- Provide vibration sensor interlocked to shut down centrifuge
- Provide control system to admit feed at proper flow rate and appropriate time in acceleration period
- Operator control of feed rate to avoid imbalance of basket and vibration
- Operator shut down of centrifuge on detection of excessive vibration

G.3.4 Mechanical failure due to centrifuge operating above the maximum design speed (Centrifuges)

- Consider alternate solid/fluid separator designs
- Provide speed detector interlocked to shut down the centrifuge at overspeed point
- Operator shut down of centrifuge on detection of high speed

G.3.5 Spills or leaks of flammable or toxic liquids due to gasket failure(Filter presses)

- Use different type of filter or centrifuge with fewer gaskets
- Enclose filter in splash shield housing
- Locate filter in leak containment trough

- House filter in containment vessel
- Use higher integrity gaskets
- External automatic fire suppression system
- Pretest filter for leaks with water before feeding process slurry
- Procedures for testing compatibility of gasket material with process fluid
- Manual activation of external fire suppression system

G.3.6 Mechanical failure due to loss of feed (running dry)

(Clarifier and separator centrifuges, i.e., disc bowl, nozzle bowl, chamber bowl, desludger, opening bowl)

- Use a design that is more tolerant to loss of feed (e.g., pusher type centrifuge)
- Provide adequate supply of wash liquid or water automatically as feed is reduced under emergency shutdown conditions
- External automatic fire suppression system
- Provide adequate supply of wash liquid or water manually as feed is reduced under emergency shutdown conditions
- Manual activation of external fire suppression system

H Dryers

This section presents potential failure scenarios for dryers and drying systems, and suggests design alternatives for reducing the risks associated with such failures. The types of equipment covered in this appendix include:

- Spray dryers
- Tray dryers
- Fluid bed dryers
- Conveying (flash, mechanical, and pneumatic) dryers
- Rotary dryers

H.1 Overpressure

H.1.1 Buildup and autoignition of deposits in dryers and ductwork resulting in fire/explosion

- Dryer design which minimizes buildup of deposits (smooth surfaces, elimination of potential points of solids accumulation)
- Use dryer with short residence time (e.g., flash dryer)
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Automatic sprinkler system/CO2 total flooding system
- Use of inerting atmosphere
- Deflagration venting
- Deflagration suppression system
- Automatic isolation of associated equipment via quick closing valves
- Periodic inspection and cleaning
- Emergency response procedures
- Procedure to process most stable materials first when campaigning multiple products to avoid ignition of unstable materials
- Procedure for determining maximum tolerable material accumulation
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.2 Ignition of condensing flammable vapor in ductwork resulting in fire/explosion

- Dryer design to prevent condensation in ductwork
- Provision for drainage of ducts (e.g., sloped, low point drains)
- Eliminate ignition sources within the ductwork
- Eliminate flammables
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Automatic sprinkler system/CO2 total flooding system (based on on-line gas detection)
- Ventilation system to keep flammable concentration below lower flammable limit
- Deflagration vents
- Use of inerting atmosphere
- Automatic isolation of associated equipment via quick closing valves
- On-line flammable gas detection and manual activation of CO2 total flooding system
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.3 Ignition of deposits in ductwork due to static discharge resulting in fire/explosion

- Dryer design which minimizes buildup of deposits (smooth surfaces, elimination of potential points of solids accumulation.)
- Grounding/bonding
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Automatic sprinkler system/CO2 total flooding system
- Use of inerting atmosphere
- Deflagration vents
- Deflagration suppression system
- Automatic isolation of associated equipment via quick closing valves

- Automatic activation of fire fighting/inerting system
- Good housekeeping
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.4 Ignition of deposits in ductwork due to sparks from electrical equipment or mechanical sources such as motors, switches, wiring, fans, bearings, conveyor chains resulting in fire/explosion

- Dryer design which minimizes buildup of deposits (smooth surfaces, elimination of potential points of solids accumulation)
- Use of electrical equipment with the correct classification to reduce the probability of ignition
- Selection of appropriate electrical area classification
- Use of non-sparking materials
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Automatic sprinkler system/CO2 total flooding system
- Use of inerting atmosphere
- Deflagration vents
- Deflagration suppression system
- Automatic isolation of associated equipment via quick closing valves
- Automatic shutdown on vibration alarm
- Good housekeeping
- Vibration monitoring of rotating equipment
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.5 Inadequate ventilation due to obstructions or closed dampers leading to creation of flammable atmosphere and subsequent ignition resulting in fire/explosion

- Eliminate flammables
- Design dampers so that system will handle the minimum safe ventilation rate at maximum damper throttling
- Provide damper mechanical position stop to prevent complete closure of damper
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Automatic sprinkler system/CO2 total flooding system
- Ventilation system to keep flammable concentration below lower flammable limit
- Deflagration vents
- Deflagration suppression system
- Use of inerting atmosphere
- Automatic isolation of associated equipment via quick closing valves
- Automatic feed trip on loss of ventilation or high LFL reading
- Manual feed trip on loss of ventilation
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.6 Increase in conveyor speed causing excessive generation of solvent vapors from the feed and subsequent ignition resulting in fire/explosion (conveyor dryer)

- Ventilation system designed to handle the maximum solvent evaporation rate
- Eliminate flammable solvent (e.g., water based)
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Ventilation system flow rate interlocked with the conveyor speed
- Automatic sprinkler system/CO2 total flooding system
- Deflagration vents

- Use of inerting atmosphere
- Deflagration suppression system
- Automatic isolation of associated equipment via quick closing valves
- Conveyor speed control with high alarm and shutdown
- Operator response to indication of higher conveyor speed
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.7 Excessive solvent load on ventilation system due to feed supply variations causing buildup of flammables with subsequent ignition resulting in fire/explosion

- Ventilation system designed to handle the maximum solvent load
- Eliminate flammable solvent (e.g. use water based solvents)
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Ventilation system flow rate interlocked with the feed flow rate
- Automatic sprinkler system/CO2 total flooding system
- Deflagration vents
- Deflagration suppression system
- Use of inerting atmosphere
- Provide upstream surge capacity to equalize composition
- Automatic isolation of associated equipment via quick closing valves
- Automatic control of feed rate
- Operator response to indication of higher feed rate
- Manual activation of fire fighting/interting system
- Manual bonding and grounding

H.1.8 Batch operation resulting in a high peak evaporation rate of flammable solvent causing buildup of flammables with subsequent ignition leading to fire or explosion

- Ventilation system designed to handle the peak solvent evaporation rate
- Dryer designs where natural circulation is sufficient to keep solvent concentration at a safe level
- Use continuous or semi-continuous dryer design
- Eliminate flammable solvent (e.g., water based)
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Automatic sprinkler system/CO2 total flooding system
- Deflagration vents
- Deflagration suppression system
- Use of inerting atmosphere
- Automatic isolation of associated equipment via quick closing valves
- Startup and normal operating procedures which allow for the unsteady evaporation rates during batch operations
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.9 Inadequate circulation in dryers causing accumulation of flammable pockets with subsequent ignition leading to fire or explosion

- Dryer designs where natural circulation is sufficient to prevent accumulation of flammables
- Eliminate flammable solvent (e.g., water based)
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Automatic sprinkler system/CO2 total flooding system
- Deflagration vents
- Deflagration suppression system
- Use of inerting atmosphere

- Automatic isolation of associated equipment via quick closing valves
- Automatic shutdown on detection of low circulating flow
- Manual dryer shutdown on low circulation
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.10 Shutdown of fans/ventilation system immediately following shutdown of heat input resulting in hot spots and flammable pockets with subsequent ignition resulting in fire or explosion

- Dryer designs where natural circulation is sufficient to prevent accumulation of flammables and/or creation of hot spots
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Post ventilation interlocks keep fans running for a sufficient time after shutdown of heating
- Automatic sprinkler system/CO2 total flooding system
- Deflagration vents
- Deflagration suppression system
- Use of inerting atmosphere
- Automatic isolation of associated equipment via quick closing valves
- Shutdown procedures to maintain fans running for a sufficient time, after shutdown of heating
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.11 Excessive atomization in nozzle leading to production of fine powder, and possibility of a dust/hybrid explosion (Spray Dryer)

- Use alternate type of dryer
- Design dryer to contain overpressure where practical
- Inlet temperature of heating medium should be sufficiently below the minimum ignition temperature

- Eliminate flammable solvent
- Permanant bonding and grounding
- Pressure control to regulate the nozzle pressure
- Deflagration vents
- Deflagration suppression system
- Use of inerting atmosphere
- Automatic isolation of associated equipment via quick closing valves
- Automatic sprinkler system/CO2 total flooding system
- Manual activation of firefighting/inerting system
- Manual bonding and grounding

H.1.12 Manifolding of ventilation exhaust ducts of several dryers leading to spread of fire or deflagration from one location to the next

- Use dedicated exhaust ducts
- Design dryer and ductwork to contain overpressure where practical
- Permanent bonding and grounding
- Automatic isolation via quick closing valves of manifold duct system on detection of fire/ flammable atmosphere in duct system
- Automatic sprinkler system/CO2 total flooding system
- Deflagration vents
- Deflagration suppression system
- Operator action to isolate various ducts on detection of fire / flammable atmosphere
- Manual activation of fire fighting/inerting system
- Manual bonding and grounding

H.1.13 Attrition of solids resulting in particle size reduction and subsequent dust explosion

- Select alternate dryer design which reduces attrition rate
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Use inert atmosphere
- Automatic sprinkler system/CO2 total flooding system
- Deflagration venting
- Deflagration suppression system
- Operating conditions to keep particle size out of explosive range
- Manual bonding and grounding

H.1.14 Deflagration due to ignition of flammable dust/vapor caused by an electrostatic spark (Double-Cone Tumbling Dryer-Glass-Lined, vessel is non-conductive due to glass lining)

- Use alternative dryer design
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Use of inerting atmosphere
- Automatic shutdown on high outlet temperature
- Automatic isolation of associated equipment via quick closing valves
- Manual bonding and grounding

H.1.15 Deflagration due to ignition of flammable vapors above the bed caused by an electrostatic spark (Fluid Bed Dryer)

- Permanent grounding and bonding
- Design dryer to contain overpressure where practical
- Permanent bonding and grounding
- Deflagration vents
- Deflagration suppression

- Use nitrogen as fluidizing gas in a closed loop system
- Automatic isolation of associated equipment via quick closing valves
- Manual grounding and bonding for portable units

H.2 Underpressure

H.2.1 Sudden loss of heating medium with vapor condensation resulting in partial vacuum

- Dryer design for minimum expected pressure
- Automatic vacuum relief system on detection of low pressure
- Procedure to limit rate of temperature decrease in dryer

H.3 High Temperature

H.3.1 Ignition of surrounding combustibles (including fugitive emissions from the dryer) caused by high surface temperature in dryers and ductwork resulting in fire

- Limit temperature of the dryer to below the safe temperature limit of surrounding materials
- Insulation of external dryer surfaces to reduce surface temperature to a safe limit
- Maintain proper clearances between hot surfaces and combustible materials
- Automatic fixed fire protection systems
- Fines removal from exit gas (bag filters)
- Operator action in response to observing high surface temperatures
- Good housekeeping
- Emergency response procedures
- Manual activation of fire fighting/inerting system

H.3.2 Ignition of combustible material used in the construction of dryer in the event of a high temperature excursion resulting in a fire

- Dryer design which does not use combustible materials of construction
- Use of heating medium which automatically limits the temperature exposure of dryer internals

- Automatic control of dryer temperature
- High temperature alarms and shutdown systems
- Automatic sprinkler system/CO2 total flooding system
- Use of inerting atmosphere
- Operator action in response to observing high dryer temperature and/or high temperature alarm
- Emergency response procedures
- Manual activation of fire fighting/inerting system

H.3.3 Decomposition of process material caused by exposure to high temperature resulting in a fire/explosion

- Use of heating medium which automatically limits the temperature to which the feed is exposed
- Alternative dryer design limiting feed inventory
- Design dryer to minimize internal accumulation of product
- Automatic control of dryer temperature
- High temperature alarms and shutdown systems
- Use of inerting atmosphere
- Automatic heating medium temperature control (e.g., steam desuperheating)
- Automatic sprinkler system/CO2 total flooding system
- Operator action in response to observing high dryer temperature and/or high temperature alarm
- Emergency response procedures
- Manual activation of fire fighting/inerting system

H.3.4 Decomposition of process material caused by low feed rate to dryer resulting in a fire/explosion

- Use of heating medium which automatically limits the temperature to which the feed is exposed
- Alternative dryer design
- Automatic control of heat input to dryer based on feed flow rate
- High temperature alarms and shutdown systems
- Use of inerting atmosphere
- Automatic sprinkler system/CO2 total flooding system
- Automatic control of feed rate
- Operator action in response to observing high temperature, and low feed rate
- Emergency response procedures
- Manual activation of fire fighting/inerting system

H.3.5 Introduction of flammable liquid into dryer via lube oil leakage from damaged bearing/seal and subsequent ignition resulting in a fire/explosion

- Double mechanical seals
- Use dryer with no mechanical seals
- Automatic sprinkler system/CO2 total flooding system
- Use of inert atmosphere
- Periodic bearing and seal inspection
- Manual activation of fire fighting/inerting system

H.3.6 Decomposition of heat sensitive process material due to heat generated from mechanical input (i.e., plugging of rotary feeders, paddle dryers, screw conveyors)

- Use dryer component types which minimize mechanical heat input
- Alternative dryer design
- Use non-flammable/high flash point lubricants
- Provide torque limiting devices (i.e., shear pins) for mechanical components

- Deflagration venting
- Deflagration suppression system
- Provide high and low torque alarms or mechanical devices
- Manual response to lube oil reservoir low level alarm

I Fired Equipment

This section presents potential failure scenarios for fired equipment and suggests design alternatives for reducing the risks associated with such failures. The types of fired equipment covered in this appendix include:

- Process furnaces
- Boilers
- Thermal incinerators
- Catalytic incinerators

This appendix presents only those failure modes that are unique to fired equipment. Some of the generic failure scenarios pertaining to vessels and heat transfer equipment may also be applicable to fired equipment.

I.1 Overpressure (Firebox)

I.1.1 Deflagration in firebox due to delayed ignition on light-off, fuel leakage into the firebox, or insufficient firebox purging

- Provide continuous pilots for all burners
- Timed purge prior to light off with interlocks to ensure that all fuel supply valves are closed
- Reliable fuel gas isolation (e.g., double block and vent)
- Provide flame surveillance system to prevent fuel admission until an ignition source is present
- Provide interlocks to ensure that fuel and combustion air controls are in proper lighting off positions, before the ignition sequence can proceed
- Lighting procedures which ensure that each ignition trial is of limited duration, and is followed by purge, if unsuccessful
- Ensure that all individual gas cocks to burners are closed until light-off
- Procedures/valving to ensure that only one burner is ignited at a time
- Provide individual burner cocks, where practical, so that only one burner may be lighted at a time to minimize potential accumulation of fuel prior to light-off

I.1.2 Failure to establish reliable pilot flames before opening main fuel supply leading to explosion

- Provide pilot burners with a separate fuel line
- Take pilot gas supply from the upstream side of the main shutoff valve for all burners
- Provide flame surveillance system to prevent fuel admission until an ignition source is present
- Lighting procedures to ensure pilots are lit and stable before admission of burner fuel

I.1.3 Rapid readmission of air to correct insufficient air situation leading to positive firebox pressure

- Interlock fuel supply and air supply so that loss of, or significant reduction in, either fuel or air will shut off and lock out the fuel supply
- Provide "lead-lag" firing control system to avoid firing without sufficient air
- Procedures to limit fuel firing to air availability
- Procedures to control rate of air readmission in response to insufficient air flow

I.1.4 Tube rupture due to thermal shock, overfiring, corrosion/erosion, or high temperature due to flame impingement

- Enhanced tube metallurgy
- Heavier wall thickness
- Indirect firing
- Elimination of liquid to burner by using non-condensing gas
- Automatic heater shutdown on high tube outlet temperature
- Automatic heater shutdown on low process flow
- Burner adjustment to eliminate flame impingement
- Procedures to prevent excessive firing rates
- Addition of inhibitors to reduce process coking rate
- Operator remote isolation of coil inlet/outlet in response to detecting tube rupture on indication of stack temperature increase, loss of tube pressure or high firebox pressure/temperature.
- Procedures to prevent acid dew point corrosion

- Visual observation of coils for hot spots
- Tube wall temperature indication and high alarm

I.1.5 Closure of flue gas damper or trip of induced draft fan

- Provide mechanical position stop to prevent complete closure of damper
- Design firebox for shutoff pressure of forced draft fan
- Use natural draft design to eliminate induced draft fan
- Automatic heater shutdown on closure of damper
- Automatic heater shutdown on trip of induced draft fan
- Automatic heater shutdown on high firebox pressure
- Manual heater shutdown on indication of high firebox pressure

I.2 Overpressure

I.2.1 Flashback into waste gas supply manifold to incinerator

- Use alternative waste gas disposal method (e.g., adsorption)
- Provide automatic fire suppression system
- Provide deflagration or detonation arresters as appropriate
- Deflagration venting
- Automatic control of waste gas concentration
- Automatic temporary diversion of waste gas to alternative disposal
- Manual control of waste gas concentration
- Manual temporary diversion of waste gas to alternative disposal

I.3 Underpressure (Firebox)

I.3.1 Trip of forced draft fan in balanced draft system

- Design firebox for minimum pressure produced by induced draft fan
- Select alternative design without induced draft fan

- Automatic heater shutdown on loss of forced draft fan
- Automatic transfer to natural draft operation

I.4 High Temperature (Process side

I.4.1 Process side fouling (e.g., coking of tubes) resulting in localized hot spots and tube rupture

- Enhanced tube metallurgy
- Heavier wall thickness
- Design heater for reduced heat fluxes
- Indirect firing
- Continuous injection of additive to retard fouling
- Visual observation of tube surface for hot spots
- Periodic decoking

I.5 High Temperature (Firebox)

I.5.1 Firing with insufficient air resulting in afterburning in convection section and flue gas system

- Provide “lead-lag” firing control system to avoid firing without sufficient air
- Automatic heater shutdown on low air flow and/or low air/fuel ratio
- Procedures to limit fuel firing to air availability
- Procedures to take corrective action or shutdown heater on indication of high flue gas temperature or low stack oxygen concentration

I.5.2 High or low burner fuel gas pressure resulting in incomplete combustion and possible afterburning and flame impingement on tubes

- Use burners with wider turndown ratio
- Automatic heater shutdown on low or high burner fuel pressure
- Manual shutdown on low or high burner fuel pressure
- Manual shutdown on high flue gas temperature

I.5.3 High or low burner liquid fuel pressure or loss of atomizing fluid differential pressure resulting in fuel burning on the heater hearth

- Use gaseous fuel
- Automatic heater shutdown on low or high burner fuel pressure
- Automatic heater shutdown on low atomizing fluid differential pressure
- Manual heater shutdown on low or high burner fuel pressure
- Manual heater shutdown on low atomizing fluid differential pressure
- Extinguishment with snuffing steam
- Visual inspection of firebox and manual adjustment

I.6 Low Temperature (Incinerator)

I.6.1 Low flow of fuel gas, high excess air, or insufficient oxygen results in incomplete destruction of hazardous materials

- Alternate means of disposal of hazardous material
- Increased stack height to reduce ground level concentration of hazardous materials
- Selection of catalyst with a wider temperature range of activity
- Automatic shutdown of incinerator on low fuel gas flow
- Automatic shutdown of incinerator on low combustion temperature
- Manual shutdown of incinerator on low fuel gas flow
- Manual shutdown of incinerator on low combustion temperature
- Manual sampling of incinerator offgas for concentration of hazardous materials

I.7 Low Flow (Process side)

I.7.1 Cessation of flow or flow maldistribution through individual heater passes results in high tube temperature and tube rupture

- Enhanced tube metallurgy
- Heavier wall thickness
- Automatic shutdown of heater on low process flow

- Automatic control of flow to individual heater passes
- Automatic shutdown of heater on high coil outlet temperature
- Automatic addition of cooling fluid to heater tubes
- Automatic shutdown on high flue temperature
- Manual shutdown of heater on low process flow or high tube outlet temperature
- Manual addition of cooling fluid to heater tubes
- Manual shutdown on high flue temperature

I.8 Low Level (Boiler Drum)

I.8.1 Loss of boiler water level leading to hot spot formation and tube rupture

- Design tubes in the convection section to operate "dry"
- Automatic boiler water level control
- Interlock to shutdown firing on low drum level

I.9 Wrong Composition (Fuel Gas)

I.9.1 Rapid increase in fuel gas heating value leading to overfiring

- Use of dedicated constant heating value fuel gas
- Automatic adjustment of firing on process outlet temperature and fuel heating value (on-line Btu analyzer)
- Automatic heater shutdown on high process outlet temperature or high firebox temperature
- Manual shutdown of heater on high firebox temperature or high process outlet temperature

I.10 Wrong Composition (Fuel)

I.10.1 High sulfur/ vanadium/sodium in fuel

- Enhanced metallurgy at points of possible acid dew point corrosion
- Use of sulfur, vanadium or sodium-free fuel source
- Periodic analysis of fuel for sulfur, vanadium and/or sodium

I.11 Wrong Composition (Catalytic Incinerator)

I.11.1 Introduction of liquid onto hot catalyst bed resulting in high temperature or fire

- Alternative incinerator design
- Liquid knock-out drum with automatic liquid removal
- Heat tracing of feed system
- Feed preheating to vaporize any entrained liquid
- Automatic shutdown of incinerator on high offgas temperature
- Liquid knock-out (KO) drum with manual liquid removal
- Manual shutdown of incinerator on high offgas temperature

I.12 Wrong Composition

I.12.1 Introduction of liquid (flammable or non-flammable) into firebox via fuel system

- Alternate design more tolerant of liquid introduction
- Liquid knock-out drum with automatic liquid removal
- Heat tracing of fuel gas system
- Liquid knock-out (KO) drum with manual liquid removal

I.13 Wrong Composition (Process side)

I.13.1 Introduction of liquid to gas heater resulting in thermal shock and tube failure

- Eliminate piping cross-connections upstream of heater which could inadvertently admit liquid
- Liquid knock-out drum with automatic liquid removal
- Liquid knock-out (KO) drum with manual liquid removal

J Solids Handling and Processing Equipment

This section presents potential failure scenarios for solids handling and processing equipment, and suggests design alternatives for reducing the risks associated with such failures. The types of equipment covered in this appendix include:

- Mechanical conveyors
- Pneumatic conveying systems
- Comminution equipment (mills, grinders, crushers)
- Sieving (screening) equipment
- Powder blenders (mixers)
- Solids feeders (rotary valves, screw feeders, etc.)
- Solids enlargement equipment (extruders, briquetters, etc.)
- Spray granulators and coaters

This appendix presents only those failure modes that are unique to solids handling and processing equipment. Some of the generic failure scenarios pertaining to vessels and solid-fluid separators may also be applicable to solids handling and processing equipment.

J.1 Overpressure (Pneumatic conveying system)

J.1.1 Dust deflagration in end-of-line equipment (silo, cyclone, dust collector) due to electrostatic spark discharge generated by pneumatic conveying

- Permanent grounding and bonding via continuous metal piping
- Use of heavy wall piping and flanges in lieu of tubing and couplings so that system can withstand maximum expected deflagration pressure
- Use of nitrogen in lieu of air for conveying gas (closed loop system)
- Use dense phase conveying instead of dilute phase
- Convey solids as pellets instead of granules or powder. However, avoid transport of pellets containing easily ignitable fines fraction.
- Increase particle size
- Use non-friable solids formulation (avoid fines)
- Use additives with high ignition energy

- Use of conductive rubber sleeves (boots and socks) when flexible connections are required
- Deflagration venting of end-of-line equipment
- Deflagration suppression in end-of-line equipment
- Quick-closing isolation valve at inlet to end-of-line equipment
- Deflagration suppression barrier in piping at inlet to end-of-line equipment
- Manual bonding across potential breaks in continuity such as non-conductive rubber socks

J.2 Overpressure (Mills, Grinders and other size reduction equipment)

J.2.1 Dust deflagration due to mechanical energy or electrostatic spark

- Permanent grounding of housing
- Equipment design accommodating maximum expected pressure
- Use of fluid energy mill with inert gas instead of air
- Use screens to remove tramp metals and other foreign materials
- Provide inerting
- Deflagration venting
- Water deluge system in mill
- Deflagration suppression in the mill
- Deflagration suppression/barrier in inlet/outlet piping
- Use magnets to remove tramp metals and other foreign materials
- Manual removal of tramp metals and other foreign materials
- Manual bonding and grounding

J.3 Overpressure and Loss of Containment (gyratory screener)

J.3.1 Dust deflagration causing rupture of flexible sleeves and subsequent secondary deflagration in building

- Use of non-gyratory (rotary) type of screener
- Permanent bonding and grounding

- Use of outboard bearings to avoid potential source of ignition
- Install gyratory screener in a separate room with blow-out walls (deflagration vents)
- Operate under vacuum to avoid escape of dusts into building
- Good housekeeping to reduce dust
- Frequent routine inspection and scheduled replacement of sleeves
- Manual bonding and grounding

J.4 Overpressure (bucket elevators and en-mass conveyors)

J.4.1 Dust deflagration due to impact or frictional heating from slipping belts or chains with possible secondary deflagration in building

- Equipment design accommodating maximum expected pressure for tubular en-mass conveyors
- Permanent grounding and bonding
- Convey solids as pellets instead of granules or powder
- Increase particle size
- Deflagration venting
- Deflagration suppression
- Provide chokes
- Provide negative pressure for bucket elevators installed inside buildings to minimize dust leakage
- Provide deflagration suppression/barrier at feed and discharge points
- Provide hot material detection and automatic quench system
- Provide inerting for small en-mass conveyors
- Good housekeeping to reduce dust in building
- Manual grounding and bonding

J.5 Overpressure (orbiting screw powder blender, fluid bed blender, or ribbon blender)

J.5.1 Dust deflagration due to electrostatic spark discharge or frictional heating (orbiting screw or ribbon rubbing against vessel wall)

- Equipment design accommodating maximum expected pressure
- Permanent grounding and bonding
- Increase particle size
- Provide inerting
- Deflagration venting
- Deflagration suppression
- Provide an overload trip on the motor driving the orbiting screw
- Procedures to verify adequate purging of bottom bearing
- Manual grounding and bonding

J.6 Overpressure (spray granulators and coaters)

J.6.1 Deflagration and/or fires caused by use of flammable or combustible solvents

- Permanent grounding and bonding
- Equipment design accommodating maximum expected pressure
- Eliminate use of flammable solvents (e.g., aqueous solvents)
- Use high flash point solvents
- Provide inerting
- Deflagration venting
- Deflagration suppression
- Deflagration barriers (quick-closing isolation valve or suppressant) in the path from granulator or coater to downstream equipment (dust collector, scrubber)
- Procedures for periodic inspection and cleaning of combustible materials on walls
- Procedures to process most stable materials first when campaigning multiple products to avoid ignition of unstable materials
- Manual grounding and bonding

J.7 Overpressure (extruder)

J.7.1 Blockage of die

- Provide emergency relief device
- Provide overload trip on motor
- Provide pressure measurement at die with interlock shutdown on high pressure
- Manual shutdown on motor overload
- Manual shutdown on detection of high pressure

J.8 High Temperature (screw conveyors or extruders)

J.8.1 Fire caused by jamming of conveyed material and frictional heating

- Use other type of conveyor (e.g., vibratory conveyor)
- Use screens to remove tramp materials
- Provide an overload trip on the motor driving the screw
- Provide a temperature sensor in the conveyor trough/barrel automatically tripping the motor and/or activating a water deluge system or snuffing steam
- Use magnets to remove tramp ferrous metals
- Provide a temperature sensor in the conveyor trough/barrel with an alarm alerting the operator to activate deluge system or deluge steam
- Manual removal of tramp ferrous metals

J.9 High Temperature (belt conveyors)

J.9.1 Fire caused by overheating due to a jammed idler roller, or if the belt jams, as a result of drive rollers continuing to run

- Provide “fire retardant” belts
- Use other type of conveyor (e.g., vibratory type)
- Use sealed roller bearings to minimize ingress of solids
- Provide automatic sprinklers or water spray protection interlocked to shutdown the belt drive on sprinkler water flow initiation

- Provide belt velocity detection interlocked to shutdown on low speed
- Operator activation of sprinklers or water spray
- Manual shutdown on detection of low speed

J.10 High Temperature (belt conveyors)

J.10.1 Fire caused by electrostatic sparks igniting powder on the belt

- Provide belts of anti-static material
- Increase minimum ignition energy
- Provide passive static elimination device (e.g., tinsel bar)
- Provide automatic sprinklers or water spray protection interlocked to shutdown the belt drive on sprinkler water flow initiation
- Provide ionizing blower to eliminate static charge
- Operator activation of sprinklers or water spray

J.11 High Temperature (rotary valves)

J.11.1 Fire caused by jamming and frictional heating

- Design dust collector bag cages and filters to be properly secured to avoid falling into rotary valve
- Provide robust bar screen at rotary valve inlet
- Provide outboard bearings to prevent failure due to solids contamination
- Provide an overload trip on the motor driving the rotary valve
- Provide a temperature sensor in the valve body automatically tripping the motor and/or admitting quench water into the valve
- Provide a temperature sensor in the valve body with an alarm alerting the operator to trip motor and activate quench
- Ensure dust collector bags and cages are properly secured

J.12 High Temperature (screw conveyors)

J.12.1 Fire caused by shaft misalignment resulting in frictional heating due to the shaft rubbing against the trough

- Use different type of conveyor (e.g., vibratory conveyor)
- Provide an overload trip on the motor driving the screw
- Provide temperature sensors (multipoint or line type) in the trough automatically tripping the motor and/or admitting quench water to the conveyor trough
- Provide temperature sensors in the trough with an alarm alerting the operator to trip motor and activate quench

J.13 High Temperature (extruders)

J.13.1 Fire caused by jamming and frictional heating

- Provide an overload trip on the motor driving the extruder screw
- Provide a temperature sensor in the extruder barrel (body) automatically tripping the motor
- Provide a temperature sensor in the extruder barrel (body) with an alarm to alert the operator to take action

J.14 Loss of Containment (bucket elevators, screw conveyors)

J.14.1 Emission of combustible and/or toxic dusts to the atmosphere or building

- Provide “dust-tight” design
- Use other type of conveyor (e.g., en-mass conveyor)
- Provide negative pressure ventilation to contain and capture any emissions
- Periodic contamination testing of area

ioMosaic®
Minimizing risk. Maximizing potential.®

About ioMosaic Corporation

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

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 disciplines, 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.

Consulting Services

- Asset Integrity
- Auditing
- Due Diligence
- Facility Siting
- Fault Tree/SIL Analysis
- Fire & Explosion Dynamics
- Incident Investigation, Litigation Support, and Expert Testimony
- Hydrogen Safety
- LNG Safety
- LPG Safety
- Pipeline Safety
- Process Hazard Analysis
- Process Engineering Design and Support
- Process Safety Management
- Relief and Flare Systems Design and Evaluation
- Risk Management Program Development
- Quantitative Risk Assessment
- Software Solutions
- Structural Dynamics
- Sustainability Reporting Support
- Technology Transfer Package Development
- Process Safety Training

Laboratory Testing Services (ISO Accredited)

- Battery Safety Testing
- Chemical Reactivity Testing
- Combustible Dust Hazard Analysis and Testing
- Flammability Testing
- Physical Properties Testing
- Process Safety Services
- Specialized Testing

US Offices

Salem, New Hampshire
Houston, Texas
Minneapolis, Minnesota
Berkeley, California

International Offices

Al Seef, Kingdom of Bahrain
Bath, United Kingdom

Software Solutions

Process Safety Office® : A suite of integrated tools for process safety professionals and risk analysts.

Process Safety Enterprise® : Process Safety Management compliance made easy with enterprise workflows, dynamic forms, document management, key performance indicators and metrics, and more.

Process Safety Learning® : Build your process safety competencies incrementally using learning modules.

Process Safety tv® : The worldś first video streaming platform dedicated to process safety.

Contact us

www.ioMosaic.com
sales@ioMosaic.com
1.844.ioMosaic