OPPORTUNITIES IN THE DESIGN OF INHERENTLY SAFER CHEMICAL PLANTS

Stanley M. Englund

The Dow Chemical Company
Midland, Michigan 48667

I. Introduction

The design of chemical plants to be more inherently safe has received a great deal of attention. This is due in part to the worldwide attention to issues in the chemical industry brought on by the gas release at the Union Carbide plant in Bhopal, India, in December, 1984. A number of articles have been written on designing inherently safe plants. The purpose of this chapter is to examine and categorize some techniques that can be used by design engineers to make the plants they design inherently safer.

A major contributor to the field of literature regarding inherently safe chemical plants is Trevor Kletz, formerly with Imperial Chemical Industries, Ltd. (England), who is quoted frequently in this chapter. Kletz is now an industrial professor at the Loughborough University of Technology, Loughborough, England. Another important source of information is Frank Lees, professor of plant engineering, Department of Chemical Engineering, Loughborough University of Technology, Loughborough, England. Lees' monumental two-volume encyclopedia, *Loss Prevention in the Process Industries* (1980), has a wealth of information on quantitative methods of providing loss prevention technology in the chemical, petrochemical, and petroleum industries.

The term inherent means "belonging by nature, or the essential character of something." An inherently safe plant is safe by its nature and the way it is constructed. The term intrinsic has a meaning similar to inherent, but common usage of intrinsic in the chemical industry usually means a protection technique related to electricity. According to Lees (1980), intrinsic safety is based on the restriction of electrical energy to a level below which sparking or heating effects cannot ignite an explosive atmosphere.

ADVANCES IN CHEMICAL ENGINEERING, VOL. 15

There is no method of making a plant truly inherently safe, since there is always risk when human activity is involved. But, if we carefully examine the technology available to us, we can make chemical plants inherently safer than they might be without such an examination. We can determine that a plant *can* be safe, but there are many factors that will determine whether a plant *will* be safe. CEFIC, the European Council of Chemical Manufacturers' Federations (*CEFIC*, 1986), reports "these include human factors that are so difficult to quantify that they are rarely taken into consideration." They include the human side of plant management, operation, and maintenance. Designers cannot do much about these human factors, but they can often do a lot to make the plant easy to operate, and reduce the chances of accidents that may result from human error and mechanical failure.

II. Identification of Hazards

Very often, indepth safety studies come late in the design of a plant. We then try to control hazards that are identified later in the design by adding protective equipment. If hazards can be identified early in the design, changes are usually much easier and cheaper, and often better, than changes made late in the design (Kletz, 1985a). Quantitative risk assessment of the plant design can be of great value in building a safer plant as well as in improving an existing plant. There are several groups of people who can contribute expertise to the safe design of chemical plants early in the design process. These people can be divided loosely into the following categories: (1) Process designers, (2) project managers, (3) manufacturing personnel, (4) research personnel, and (5) safety and loss prevention specialists. Management is responsible for any project, but many very important decisions are routinely made by the technical experts on whom management relies. There are many decisions that can and should be made primarily by management early in the design to provide the best possible plant design. Safety and loss prevention specialists can be very helpful to the process designer at all stages in design, especially in safety reviews and quantitative risk assesssment. Research people usually contribute most of their expertise early in the design. Manufacturing personnel should be well represented at all stages of a design project.

This chapter is divided into three sections. The first section discusses general design opportunities. These primarily involve policy, layout, inventory, and process decisions having a broad impact. To make the right decision, a strong input from management is required, although other expertise, especially from safety and loss prevention experts, is required to provide information that will lead to the best possible process decision. In the second section, process design opportunities will be discussed. These require primarily the knowledge and experience of technical experts in the areas of process design, research, and manufacturing, although in some cases strong management input is required, and in all cases, strong management support is needed. For example, the design of pressure relief systems is a highly technical and advanced field, but if the latest design methods are to be of any value, management has to make a decision to devote the necessary resources to use these design methods. In the third section of this chapter, equipment design opportunities will be discussed. These opportunities require input from a variety of technical support groups as well as manufacturing experts. The experience of a successful plant operation is especially valuable here so that proven techniques can be used as much as possible.

III. General Design Opportunities

A. Clear Responsibility for Safety in Design and Operation

It is very important that the responsibility for the safe design and operation of a plant be clearly defined early in the design process. This means that competent and experienced people should be made responsible and held accountable for decisions made from the start of plant design. It is desirable to have a person or persons experienced in manufacturing operations and available in a leadership role to assist in early decisions that will affect safety. Management people should make it clear that they support and insist on process design safety. It is the responsibility of management to make certain that responsibility for safe design is clearly understood, but process design personnel should make themselves heard if they don't think this is happening.

B. Critically Review Alternatives Early in Design

Much of the rest of this chapter will discuss alternatives available to process designers. They should attempt to identify hazards early in the design, and identify alternatives available to remove or reduce them. They may then be able to remove many of the hazards or reduce their severity by making changes early in the design. The poor alternative is to add protective equipment at the end of the design or after the plant is operating, which can be expensive and not entirely satisfactory.

One constraint on the development of inherently safer plants is logistic rather than technical. Hazards and operability studies as well as other safety studies and reviews normally take place late in the design. At this stage, it is usually too late to increase design pressure of vessels, relocate electrical equipment, revise the layout, or extensively revise the process. Time must be allowed in the early stages of design for critical reviews and evaluation of alternatives. This involves an early hazards and operability (HAZOP) study using the flowsheets before final design begins (Kletz, 1985a). The use of HAZOP, fault tree analysis, checklists, audits, and other review and checking techniques can be very helpful. The techniques are extensively discussed in technical literature and will not be discussed in detail in this chapter.

C. Incorporating Emergency Planning into Original Plant Designs

Emergency planning is often done *after* the plant is nearly completed and ready for start-up. At this point, it is difficult or perhaps even possible to make some of the desired changes for emergency planning. Emergency planning should cover such items as tornado and storm shelters, flood protection, earthquakes, possible vapor releases from the proposed plant and nearby plants, proximity to public areas, accessibility of fire protection equipment to the plant, and safe exit routes. This is primarily for the protection of plant personnel and people in nearby areas who could be affected by plant problems. Emergency planning should be considered early in the design so as to make it possible to have a good plan.

D. Providing Adequate Space between Process Plants, Tanks, and Roads

When designing a safe chemical processing plant, there are few things more important to consider than the amount of space provided for the processing, storage, loading, and unloading of raw materials. There are many methods that can be used as guidelines for spacing in the design of chemical plants. Normally, it is not a good idea to have tank car and tank truck loading and unloading facilities near each other or near the process area when hazardous materials are involved. Loading and unloading facilities for hazardous materials should also not be near storage facilities. Because of the volume of chemical usually stored, the potential severity of a gas release accident from the storage of a highly toxic or flammable chemical is far greater than might occur in the process area or in the loading or unloading area. On the other hand, the frequency of storage accidents is quite low compared to loading and unloading accidents and process accidents. This poses logistics problems, which should be faced early in process layout, of how to keep storage tanks for highly toxic or flammable chemicals as far from property lines as possible, and how to maintain adequate distances between loading, unloading, storage, and process areas. In addition, it is desirable to have adequate space between the storage, loading, unloading, and process areas, and the following other areas:

(1) Other tank farms
(2) Other plants
(3) Maintenance and other facilities
(4) Power generation and other utilities
(5) Warehouses
(6) Administration and other office buildings
(7) Roads and railroads

Buffer zones should be considered to separate relatively hazardous operations from surroundings such as residential areas or other public areas. One method to obtain adequate space between loading and unloading facilities, the process area, and the storage area is shown in Fig. 1, where triangular spacing is shown. This may be suited to small sites where there are a limited number of individual plants. No facilities involving people, significant equipment, or buildings would normally be allowed inside the triangle. Such things as storage ponds and effluent treatment facilities could be in the triangle. Other facilities such as a control room, boiler, maintenance facilities, and offices would be well removed from this triangle.

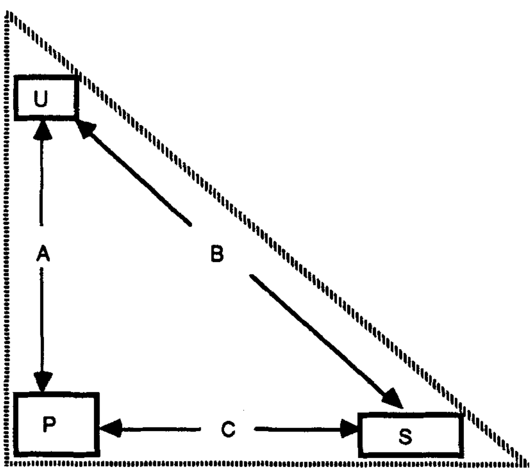

FIG. 1. Triangular spacing between the major process components. Offices, control rooms, maintenance, and similar departments should be located outside the triangle. Distances A, B, and C should be carefully selected based on the nature of the process and local conditions. U, Loading and unloading zone for hazardous materials; P, process plant; S, storage space for hazardous materials.

E. Using Minimum Storage Inventory of Hazardous Materials

The best way to minimize leaks of a hazardous or flammable material is to have less of it around. In the Flixborough disaster (Lees, 1980), on June 1, 1974, the process involved the oxidation of cyclohexane to cyclohexanone by air (with added nitrogen) in the presence of a catalyst. The cyclohexanone was converted to caprolactam which is the basic raw material for Nylon 6. The reaction product from the final reactor contained approximately 94% unreacted cyclohexane at 155°C and at over 200 psi. The holdup in the reactors was about 240,000 lbs, of which about 80,000 lbs escaped. It is estimated that ~20,000–60,000 lbs was actually involved in the explosion. The resulting large, unconfined vapor cloud explosion (or explosions, there may have been two) and fire killed 28 people and injured 36 at the plant and many more in the surrounding area. It also demolished a large chemical plant and damaged 1821 houses and 167 shops. The very large amount of flammable liquid, well above its boiling and flash point, contributed greatly to the extremely severe nature of the disaster.

In addition to the large in-process inventory of cyclohexane, there were over 430,000 gal of flammable materials, including cyclohexane and naphtha, stored at the Flixborough site. Licenses had only been issued for storage of 7000 gal of naphtha and 1500 gal of gasoline. However, the unlicensed storage of fluids had no effect on the disaster since the disaster was in the process area and not the storage area.

The results of the Flixborough investigation make it clear that the large inventory of flammable material in the process plant contributed to the scale of the disaster. It was concluded that "limitation of inventory (of flammable materials) should be taken as specific design objective in major hazard installations". Note that reduction of inventory may require more frequent and smaller shipments. There may be more chances for errors in connecting and reconnecting. These possibly negative benefits should also be analyzed. Some methods of reducing inventory of hazardous materials are discussed later in this chapter.

F. Designing Liquid Storage So Leaks and Spills Do Not Accumulate Under Tanks or Process Equipment

It is a good idea to design dikes that will not allow flammable or combustible materials to accumulate around the bottom of storage tanks or process equipment in case of a spill. If liquid spills and ignites inside a dike where there are storage tanks or process equipment, the fire may be continuously supplied with fuel and the consequences can be severe. It is usually much better

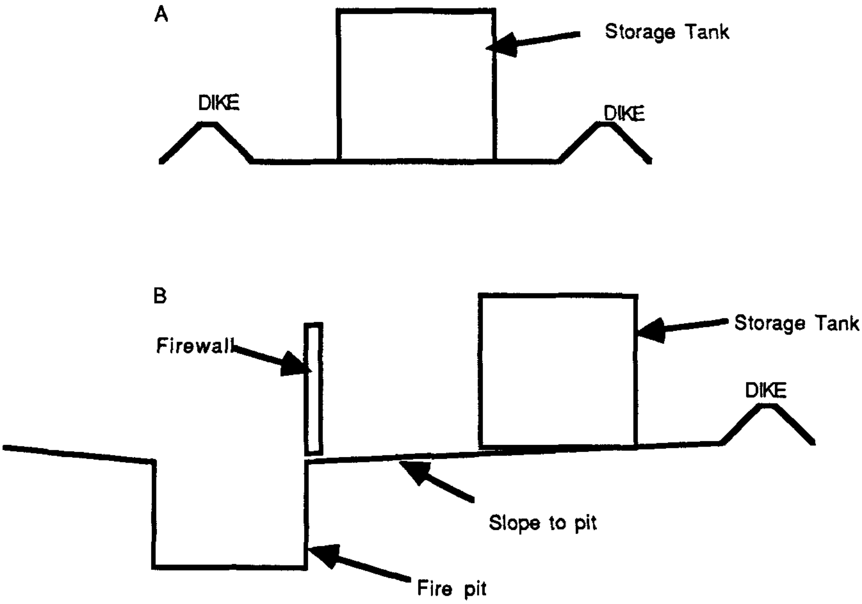

FIG. 2. Methods of diking for flammable liquids. A, Traditional diking method allows leaks to accumulate around the tank. In case of a fire, the tank will be directly exposed to flames that can be supplied by lots of fuel and will be hard to control. B, In the more desirable method, leaks are directed away from the tank. In case of fire, the tank will be shielded from most flames and fire will be easier to fight.

to direct possible spills and leaks to an area away from the tanks or equipment and provide a fire wall to shield the equipment from most of the flames if a fire occurs. Figure 2 shows schematically a traditional way to design diking as well as a better design that has met with success. Even if stored material is not flammable, allowing material to accumulate under tanks and equipment may not be desirable. For example, if bromine is spilled in a nondrained dike area containing bromine storage tanks, the automatic dump valve on the tanks may rapidly become corroded on the outside making it impossible to transfer contents to another storage vessel.

The design in Fig. 2A is usually undesirable for flammable liquids because it will allow flames from an ignited spill within the diked area to "cook" the tank. Such a fire may be very dangerous and hard to control because of the possibility of rupturing the tank. The better design in Fig. 2B will divert spills from the immediate area of the tank. In the event of a fire, the tank will be shielded by the fire wall. This safeguards the tank from direct exposure to the flames. Such a fire is easier to control, and the tank is less likely to rupture.

G. Use Open Structures for Plants Using Flammable or Combustible Materials

There are many examples of serious fires and explosions that probably resulted in part from handling moderate to large quantities of flammable or combustible liquids and liquefied flammable gases inside enclosed structures. If a sufficient quantity of flammable mixture should ignite inside an ordinary chemical processing building, it is highly probable an explosion will occur that will seriously damage the building. For this reason, processing equipment is often installed in a structure without walls, usually called an "open structure." This permits effective ventilation by normal wind currents and aids the dispersion of any vapors that escape. If gas ignites in the structure, the absence of walls minimizes the pressure developed from the combustion and the probability of flying shrapnel from a shattered structure (Howard and Karabinis, 1981). Substantial damage can be done to a building by the combustion of a surprisingly small quantity of a flammable gas–air mixture. If there is an explosion in a building where the flammable gas mixture occupies a space equal to only 1 or 2% of the building volume, the building may be seriously damaged if it does not have adequate explosion venting. This results because most buildings can suffer substantial structural damage from an internal pressure appreciably less than 1 psi (0.07 bar). Thus, a building does not need to be full or even close to full of a flammable mixture for a building explosion to occur that can cause considerable damage. This is not just theoretical, it has been proven in real life experience (Howard and Karabinis, 1981)!

Brasie (1976) reported on several hazard levels of interest for fires in enclosed or semiconfined spaces. For a fuel in vapor form that has a heat of combustion of 19,000 BTU/lb, the following weights of fuel enclosed in a 1000 ft^3 building are required to achieve the effects shown, assuming no venting.

Weight of Fuel (lbs).	Effect
0.15–0.2	Pressure reaches 1 psig: Significant building damage
0.18	Temperature reaches 125°C: Maximum personnel tolerance
0.25	Significant hazard
0.6	Temperature reaches 425°C: Cellulose ignites
3-	Room engulfed in flames

In 1950, a serious explosion occurred in Midland, MI at The Dow Chemical Company in a chemical processing unit. Butadiene and styrene, in vapor and liquid forms, were accidentally discharged into a large processing area. The building was 130 × 288 ft and one story high with some steel decks. All electrical equipment in the area was explosion proof, and there was adequate automatic fire sprinkle protection. The walls were brick, and the roof was precast concrete supported on exposed steel trusses. The leak occurred in a 50 × 130 ft section of the building which was separated from the rest of the building by a 12-in bonded brick firewall with one protected opening. The explosion caused the following events to occur:

(1) Of the 40 men in the building, eight were killed.
(2) Eighty percent of the concrete slabs were blown off the roof.
(3) Walls around the 50 × 130 ft section, including the firewall, were completely demolished.
(4) All piping and duct work was completely demolished.
(5) Process vessels were reduced to salvage value.
(6) Relatively minor damage was done to buildings within a radius of 1000 ft by flying debris and concussion waves.
(7) The entire department was out of operation for approximately six months.

This tragedy was instrumental in causing Dow to establish a policy of using open structures for chemical processes that use substantial quantities of flammable liquids and liquefied flammable gases.

H. Avoid Buried Tanks

At one time, burying tanks was recommended because this minimized the need for fire protection systems, dikes, and distance separation. At Dow, this is no longer considered good practice except in special cases. Mounding or burying tanks above grade has most of the same problem as burying tanks below ground and is usually not recommended. There are several problems with buried tanks.

(1) Difficulty in monitoring exterior corrosion and shell thickness
(2) Difficulty in detecting leaks
(3) Difficulty repairing tanks if the surrounding earth is saturated with chemicals from a leak
(4) Potential groundwater contamination from leaks

Governmental regulations concerning buried tanks are becoming more and more strict. This is because of the large number of leaking tanks that have been identified as causing adverse environmental and human health problems.

The Environmental Protection Agency's (EPA) office of underground storage tanks defines underground tanks as those with 10% or more of their volume underground, including piping. According to an article by Brooks and others (1986), the EPA found that about 65% of documented leak incidents involved retail gasoline stations and only 3% involved chemicals (as defined by the EPA). About 4% of underground tanks are believed to contain commercial chemical products. Leaks were caused by the following failures, which are based on a survey of 12,444 tanks: (1) Structural failure, 46%; (2) corrosion, 26%; (3) loose fittings, 14%; (4) improper installation, 7%; and (5) natural phenomena, 6%.

Eleven states have enacted laws setting standards for underground storage tanks. The EPA (1987) has issued regulations requiring notification to the appropriate regulatory agencies about age, condition, and size of tanks that store hazardous wastes and underground storage tanks containing commercial chemical products. Final technical requirements have been promulgated for hazardous waste storage tanks. At the time of this writing, technical requirements for underground storage tanks containing regulated substances have been proposed by the EPA. Florida reportedly requires owners, as an early detection measure, to install at least four monitoring wells around a buried tank area. It is estimated that it will cost $150,000–$250,000 per site to clean up leaking buried tanks in Florida.

Small leaks are difficult to detect. The National Fire Protection Association of Quincy, MA, has established 0.05 gal/hr as the rate above which a tank is considered to be leaking. Leak detection measurements can be influenced by many factors, making it difficult to detect small leaks. Some of these factors are changes in product temperature and pressure, vapor pockets, tank geometry and inclination, surface waves, water table, and operator error. The EPA (1987) has proposed new rules to prevent leaks from underground tanks. The rules require testing for leaks within three years and gradually end the use of leak-prone tanks within 10 years. Leaks detected in testing would have to be repaired immediately. The owners or operators would be responsible for any damage to people or the environment and for replacing tanks. All new petroleum tanks would have to be protected from corrosion and have a leak-detection apparatus and devices to contain overflow and spills. Tanks storing chemicals would be required to have double walls or be placed in a concrete vault or lined excavation.

Because of more stringent regulatory requirements and potential future liabilities associated with buried tanks, it is probably inherently safer to use above-ground open storage with suitable spacing, diking, and fire protection facilities. This will avoid most of the potential groundwater contamination problems that could result from a leak. The potential problems from leaks can be exceedingly expensive and harmful to the environment if buried tanks are improperly designed, constructed, and maintained. Some states, and parts of some countries, require flammable liquid storage tanks to be buried unless a modification is granted. Local authorities should be contacted to check legal requirements.

I. Constructing Process and Storage Areas Away from Residential or Potentially Residential Areas

The Bhopal, India plant of the Union Carbide Corp. was originally built 1.5 miles from the nearest housing; but with time, a shanty town grew up next to the plant. This demonstrates the need to prevent hazardous plants from being located near residential areas (Kletz, 1985a). If possible, the cost of a plant should include funds for an adequate buffer zone unless other means can be provided to ensure that the public will not build adjacent to the plant. The nature and size of this buffer zone depends on many factors, including the amount and type of chemicals stored and used. If the land required to separate the plant from public areas can be put to some other use, such as plants with low hazards, laboratories, or light industry, and maintain a low population density, a satisfactory buffer may be provided. This assumes that personnel in the buffer area can be protected or evacuated if necessary. If possible, the land should be under the control of the plant, or there should be assurance from credible sources that people in the buffer zone will not be allowed near the plant. Where feasible, zoning restrictions may provide an alternative to land purchase. A possible negative effect of increased distances from populated areas could be an increase in emergency-help response time. This should be considered when the overall effect of plant location is being reviewed.

J. Designing for Total Containment

In general, it is safer to totally contain, or nearly totally contain, hazardous and flammable materials in chemical processes, if it is reasonably practical to do so, than to allow these materials to escape into the environment. In many cases, this can be accomplished by designing the processing equipment to withstand the maximum pressure that can be expected from runaway polymerizations or other reactions or explosions. This requires detailed knowledge of the process and the possible overpressure that could result. This knowledge can best be obtained from experimental data combined with a theoretical analysis.

It is helpful if management establishes the goal of total containment early in the process design so that all those involved can contribute their part to achieving that goal. For example,

(1) Explosions involving organic dusts can usually be contained in equipment that can withstand about 7–10 times the initial pressure (Lees, 1980). Thus, if the system is originally at atmospheric pressure, the maximum pressure to be expected is about 100–150 psig. Data on explosion characteristics of the actual material to be processed are usually necessary to confirm the required design pressure.

(2) Dikes around the process and storage areas with only controlled pump discharge from the diked areas will make controlled liquid release from spills possible. The diked areas must not be allowed to fill with water, snow, or ice.

(3) Massive vapor releases can be minimized by choosing the proper design pressure for processing equipment and storage vessels.

(4) The design of emergency relief systems is important. The goal should be well-designed systems that will relieve pressure safely but not discharge material uncontrollably (as single frangible disks often do). The use of flares, incinerators, scrubbers, and emergency recovery tanks should be considered.

(5) Construction materials should be selected that will withstand long-term exposure to the chemicals used in the process. This includes gaskets, which tend to be weak points in piping and vessels. Gaskets are discussed in Section V,E of this chapter. Occasionally fire-safe emergency valves are installed with gaskets that will quickly burn away if there is a fire. This tends to defeat the purpose of fire-safe valves.

K. Redesigning Obsolete Plants Before Accidents Occur

Occasionally because of job rotation, promotion, retirement of key individuals, poor business, or just plain poor management, a "negative learning curve" occurs in a process plant. Process designers should do all they can to ensure that all existing process plants are operated safely. They may see things that are not apparent to those actually running the plant. Process designers should not be reluctant to point out the shortcomings of plants and suggest realistic corrective measures commensurate with the economic realities of the situation. At Dow there is a saying that you can "expect what you inspect." Management should support the idea of regular audits of plants so that existing hazards can be identified and either controlled or eliminated.

The Flixborough disaster in June, 1974 (Lees, 1980), is an example of a case where a modification was introduced into a mostly well designed and constructed plant. This modification destroyed the plant's integrity and contributed to a major accident. The modification was made when a reactor failed (a large crack had formed). The modification was inadequate and the remaining reactors were not examined.

L. Storing Liquefied Gases at Low Temperature and Pressures

Usually, leaks of liquefied gases are less serious if the liquefied gases are refrigerated at low temperatures and pressures than if they are stored at ambient temperatures under pressure. A leak of a volatile liquid held at atmospheric temperature and pressure results in only a relatively slow evaporation of the liquid. Escape of a refrigerated liquefied gas at atmospheric pressure gives some initial flashoff followed by an evaporation rate that is relatively slow but faster than the first case, depending on weather. Loss of containment of a liquefied gas under pressure and at atmospheric temperature, however, causes immediate flashing of a large proportion of the gas. This is followed by slower evaporation of the liquid residue and is usually the most serious case. The hazard from a gas under pressure is normally much less in terms of the amount of material stored if it is not liquefied, but the physical energy released is large if a confined explosion occurs at high pressure.

The economics of storing liquefied gases are such that it is usually attractive to use pressure storage for small quantities, pressure or semirefrigerated storage for medium to large quantities, and fully refrigerated quantities for very generally considered that there is a greater hazard in storing large quantities of liquefied gas under pressure than at low temperatures and low pressures. The trend is toward replacing pressure storage with refrigerated low pressure storage for large inventories. However, this is not always the case. It is necessary to consider the risk of the entire system, including the refrigeration system, and not just the storage vessel. The consequences of a failed refrigeration system must be considered. Lees (1980) states that the Imperial Chemical Industries Liquefied Flammable Gas (ICI LFG) code recommends the separation distance between storage and an ignition source to be, for ethylene, 60m for pressure storage and 90m for refrigerated low pressure storage, and for C_3s, 45m for both types of storage. The general approach taken by ICI is that there is a significant risk of failure for refrigerated storage tanks but a negligible risk for pressure storage vessels. Each case should be carefully evaluated on its own merits. In most cases, refrigerated storage of hazardous liquefied gases is undoubtedly safer, such as in the storage of large quantities of liquefied chlorine (Lees, 1980).

IV. Process Design Opportunities

The knowledge and experience of technical experts are important in identifying process design opportunities of inherently safer chemical plants. Management may or may not be familiar with the specific design opportunities that exist to make plants inherently safer. The process designer should make sure these design opportunities are adequately considered and put into practice whenever possible. Occasionally it is necessary for the process designer to point out problems and the possible benefits that could result from their solution. Occasionally it will be necessary to ask for additional resources, such as additional technical help to design pressure relief systems properly, in order to take advantage of the opportunities that will appear. A discussion of specific process design opportunities follows.

A. Understanding the Reactive Chemicals and Reactive Chemical Systems Involved

The main business of most chemical companies is to manufacture products through the control of reactive chemicals. The reactivity of chemicals that makes them useful can also make them hazardous. Therefore, it is essential that process designers understand the nature of the reactive chemicals involved in the process (*Corporate Safety*, 1981). Usually reactions are carried out without mishaps, but occasionally chemical reactions get out of control because the wrong raw materials were used, operating conditions were changed, unanticipated time delays occurred, or equipment failed. A chemical plant can be inherently safer if we use knowledge of the reactive chemicals systems in the plant's design. We must understand the chemistry of the process if we are to design a safe chemical processing plant.

1. *Reactive Hazard Evaluations*

Reactive hazard evaluations should be made on all new processes as well as existing processes on a periodic basis. There is no substitute for experience, good judgement, and good data when evaluating potential hazards. Reviews in process chemistry should include (a) reactions, (b) side reactions, (c) heat of reaction, (d) potential pressure buildup, and (e) intermediate streams. Reactive chemicals test data should be reviewed for evidence of flammability characteristics, exotherms, shock sensitivity, or other evidence of instability. Examine Planned operation of the process should be examined, especially for

(a) upsets,
(b) modes of failure,
(c) delays,
(d) redundancy,
(e) critical instruments and controls, and
(f) worst credible case scenarios.

2. *Worst Case Thinking*

At every point in the operation, the process designer should conceive of the worst possible combination of circumstances that could *realistically* exist such as

- Loss of cooling water
- Power failure
- Wrong combination or amount of reactants
- Wrong valve position
- Plugged lines
- Instrument failure
- Loss of compressed air
- Air leakage
- Loss of agitation
- Deadheaded pumps
- Raw material impurities

An engineering evaluation should then be made of the worst case consequences with the goal that the plant will be safe even if the worst case occurs. When the process designers know what the worst case conditions are, they should try to avoid worst case conditions, be sure adequate redundancy of safety systems exists, and identify and implement lines of defense. These lines of defense could be preventive measures, corrective measures or sometimes as a last resort, containment or possibly abandonment of the process if the hazard is unacceptable. It is important to note that the worst case should be something that is realistic, not something that is conceivable but extremely unlikely.

Dow has adopted the following philosophy for design scenarios in terms of independent causative effects:

(1) All single events that can actually and reasonably occur are credible scenarios.

(2) Scenarios that require the coincident occurrence of two or more totally independent events are not credible design scenarios.

(3) Scenarios that require the occurrence of more than two events in sequence are not credible.

(4) A failure that occurs while an independent device is awaiting repair represents but one failure during the time frame of the initiation of the emergency and is therefore credible. The lack of availability of the unrepaired device is a pre-existing condition.

3. *Reactive Chemicals Testing*

Much reactive chemical information involves thermal stability and the determination of the temperature at which an exothermic reaction starts, the rate of reaction as a function of temperature, and the heat generated per unit of material. Following is a review of some of the main sources of reactive chemicals data.

a. *Calculations.* Potential energy that can be released by a chemical system can often be predicted by computerized thermodynamic calculations. If there is little energy, the reaction still may be hazardous if gaseous products are produced. Kinetic data is usually not available in this way. Thermodynamic calculations should be backed up by actual tests.

b. *Differential Scanning Calorimetry (DSC).* Sample and inert reference materials are heated in such a way that the temperatures are always equal. If an exothermic reaction occurs in the sample, the sample heater requires less energy than the reference heater to maintain equal temperatures. If an endothermic reaction occurs, the sample heater requires more energy input than the reference heater. Onset-of-reaction temperatures reported by the DSC are higher than the true onset temperatures, so the test is mainly a screening test.

c. *Differential Thermal Analysis (DTA).* Sample and inert reference materials are heated at a controlled rate in a single heating block. If an exothermic reaction occurs, the sample temperature will rise faster than the reference temperature. If the sample undergoes an endothermic reaction or a phase change, its temperature will lag behind the reference temperature. This test is basically qualitative and can be used for identifying exothermic reactions. Like the DSC, it is also a screening test. Reported temperatures are not reliable enough to be able to make quantitative conclusions. If an exothermic reaction is observed, it is advisable to conduct tests in the Accelerating Rate Calorimeter (ARC[1]).

d. *Accelerating Rate Calorimeter.* This method determines the self-heating rate of a chemical under near-adiabatic conditions. It usually gives a conservative estimate of the conditions for, and consequences of, a runaway reaction. Pressure and rate data from the ARC may sometimes be used for pressure-vessel emergency-relief design. Activation energy, heat of reaction, and approximate reaction order can usually be determined. For multiphase reactions, agitation can be provided. The ARC can provide extremely useful and valuable data. An example of data from an ARC run is shown in Fig. 3. The Vent Sizing Package (VSP), which was recently developed, is an extension of ARC technology. The VSP is a bench scale apparatus for characterizing

[1] ARC is a trademark of Columbia Scientific Industries Corp.

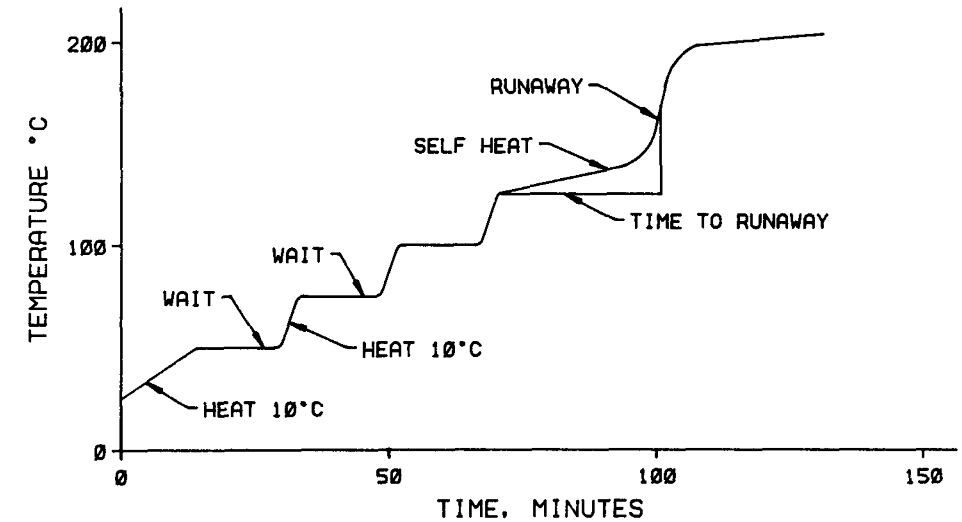

FIG. 3. Operation of the ARC.

runaway chemical reactions. It makes possible the sizing of pressure relief systems with less engineering expertise than is required with the ARC or other methods. The VSP is discussed in Section V,C of this chapter.

e. *Shock Sensitivity.* Shock sensitive materials react exothermally when subjected to a pressure pulse. Materials that do not show an exotherm on a DSC or DTA are presumed not to be shock sensitive. Three testing methods are listed here.

(1) Drop Weight Test—A weight is dropped on a sample in a metal cup. The test measures the susceptibility of a chemical to decompose explosively when subjected to impact. Weight and height can be varied to give semiquantitative results for impact energy. This test should be applied to any materials known or suspected to contain unstable atomic groupings.

(2) Confinement Cap Test—Detonability of a material is determined using a blasting cap.

(3) Adiabatic Compression Test—High pressure is applied rapidly to a liquid in a U-shaped metal tube. Bubbles of hot compressed gas are driven into the liquid and may cause explosive decomposition of the liquid. This test is intended to simulate "water hammer" and "sloshing" effects in transportation such as humping of railway tank cars. It is very severe and gives worst case results.

f. *Flammability: Flash Point.* The "closed cup" flash point determination produces the most important data for determining the potential for fire. The flash point is the lowest temperature at which the vapors can be ignited under conditions defined by the test apparatus and method.

g. *Flammability: Flammable Limits.* Flammable limits, or the flammable range, are the upper and lower concentrations (in volume percent) which can just be ignited by an ignition source. Above the upper limit and below the lower limit, no ignition will occur. Data are normally reported at atmospheric pressure and at a specified temperature. Flammable limits may be reported for atmospheres other than air, and at pressures other than atmospheric.

h. *Flammability: Autoignition Temperatures.* The autoignition temperature of a substance, whether liquid, solid, or gaseous, is the minimum temperature required to initiate self-sustained combustion in air with no other source of ignition. Ignition temperatures should be considered only as approximate. Test results tend to give temperatures higher than the actual autoignition temperature.

i. *Dust Explosions.* Combustible, dusty materials, with particle sizes less than ~200 mesh, can explore if a sufficient concentration in air is present along with an ignition source. The standard test has been designed to determine rates of pressure increase during an explosion, the maximum pressure reached, and the minimum energy needed to ignite the material. These data are useful in the design of safe equipment for handling dusty combustible materials in a process. One test apparatus widely applied is the Hartmann Tube which has a volume of 1.3 1. However, Bartknecht (1981) emphatically states "test results measured in the Hartmann Apparatus underrate the effects of dust explosions and are not a suitable basis for design of protective measures." Combustible dusts need a minimum volume to develop their full reaction velocity. Bartknecht states that to determine explosion data for combustible dusts, a minimum volume of 16 1 is required to ensure correlation with data from large test vessels. This has been confirmed by comprehensive testing with a 20 1 sphere (Kletz, 1985b).

B. Reducing Inventory by Changing Process Chemistry

If given enough time to develop new processes, research chemists and chemical engineers can often devise new processing techniques that will reduce the hazard of a process by reducing the maximum instantaneous inventory of hazardous materials. Occasionally these new techniques also provide increased productivity, quality, and improved properties. For example, in the past, synthetic rubber latex made from styrene and butadiene was usually made by adding all the ingredients to a batch reactor or a series of continuous reactors and carrying out the reaction. For small and specialty uses, it is not always practical or desirable to make these latexes by a continuous process. Indeed, some of the continuous processes for latex manufacturing have so much unreacted monomer present, they may be less safe than a conventional batch process. In conventional batch processes for making latex, all the reactants are added at the beginning of the reaction. There is a considerable amount of hazardous, flammable material present in the reactor at the beginning of the reaction, and many scenarios such as leaks, agitation failure, loss of cooling, and runaway polymerization could cause safety problems.

Methods have been developed for improving batch process productivity in the manufacturing of latex. One is the continuous addition of reactants so that the reaction takes place as the reactor is being filled (Englund, 1982). These are not continuous processes even though the reactants are added continuously during most of a batch cycle. The net result is that reactants can be added about as fast as heat can be removed. There is relatively little hazardous material in the reactor at any time because the reactants, which are flammable or combustible, are converted to nonhazardous and nonvolatile polymer almost as fast as they are added.

An example is given by U.S. Patent 3,563,946 (1971). In this example, styrene–butadiene latex is prepared by simultaneously feeding two separate streams (one a mixture of styrene and butadiene monomers, the other an aqueous solution of sodium lauroyl sulfate as emulsifier, and sodium persulfate as initiator) to a reactor that has an initial charge of water and emulsifier. The reactants are added at about 25°C and the reaction occurs at 90°C. A heat balance on the reactor jacket is usually used to make certain the monomers are reacting about as fast as they are added. Also, the charging rate of reactants is limited by suitable choices of pumps, orifices, and piping, which further reduce the possibility of monomers being added too rapidly. This is done to make sure the concentration of unreacted monomers in the reactor is not building up. This could possibly cause an unexpected "bomb" in the reactor, which would then resemble a conventional batch process, but with poor control.

Compared to a conventional batch reactor, there is less hazardous material in the reactor at any time, and the consequences of power loss, loss of temperature control, leaks, and runaway reactions are much less severe. In addition, it is easier to have good temperature control, which can provide a more reproducible, high quality product. Productivity is significantly better than in conventional batch processes since the reactor is polymerizing at its maximum rate most of the time and is normally limited only by heat transfer

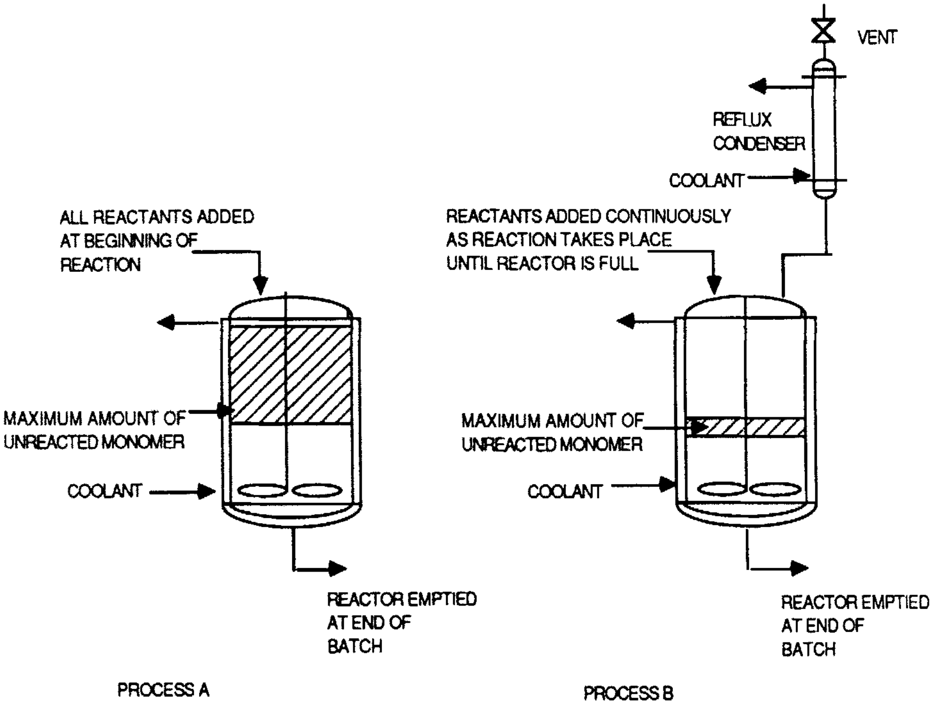

FIG. 4. Process A, Batch reaction with all reactants added at beginning of reaction. A considerable amount of flammable and hazardous material is in the reactor at the beginning of the process. Process B, a batch reaction with the reactants added during the reaction. Little flammable and hazardous material is present at any one time. Reflux (or Knockback) condensor is used to provide additional heat transfer.

capability. Heat transfer capability can be increased by adding a reflux or knockback condenser (U.S. Patent, 1977), which, in effect, provides additional heat transfer for the reaction, and consequently makes it possible to handle fast reactions or fast feed rates safely as long as there is sufficient volatile material to vaporize and be condensed. This process is shown in Fig. 4B, where it is compared to a more conventional batch process in Fig. 4A in which all the reactants are added at the beginning. Care must be taken so that when processes with less inventory are introduced, inadequately tested processes with unrecognized health, safety, and environmental risks do not result.

C. REDUCING INVENTORY BY CHANGING MIXING INTENSITY

Lees (1980) describes reduction in process inventory in the evolution of the processes for manufacturing nitroglycerine. The first is a batch process with a holdup of about 1000 kg. The second is a continuous process with a holdup of 200–300 kg. The third is a continuous process with reaction taking place in the nozzle and with a holdup of only about 5 kg. Occasionally an opportunity will arise in which a fast reaction can be made to take place in an inline pipe mixer, which has small inventory, instead of a tank with much larger inventory. The reactor volume required for continuous polymerization can sometimes be reduced by replacing a cascade of stirred tanks in series with a plug-flow tubular reactor (Levenspiel, 1979). Static mixers can sometimes be used as polymerization reactors, instead of stirred reactors or plug-flow tubular reactors, because they induce plug flow and create good radial mixing at low shear rates with low energy consumption.

Commercially available static mixer reactors (SMR) as large as 1.8 m in diameter are operating in the production of nylon, silicones, polystyrene, polypropylene, and other polymers. Removing heat from a highly exothermic reaction in a static mixer equipped with a simple cooling jacket is limited by heat transfer to small diameters, typically less than 6 in. A new type of static mixer has been developed to overcome laminar heat-flow transfer problems. It is called the SMR mixer–heater exchanger–reactor (Mutsakis *et al.*, 1986).

The SMR has mixing properties and plug flow similar to other static mixers. However, it has hollow crossing tubes that form the shape of the mixing elements. These hollow tubes carry heat-transfer fluid, greatly increasing heat-transfer surface area and making a virtually isothermal reaction possible. Such a system has the potential to be smaller than stirred tanks in series and has no internal moving parts, such as seals, that could fail.

D. Using Low Inventory in Distillation Processes

Distillation columns have a large inventory in the reboiler, and typically, an inventory several times greater in the column itself. Column holdup may be reduced by using low holdup internals. Conventional trays and packings differ by a factor of about 10 in inventory per theoretical plate (Kletz, 1985a). An estimate of holdup per theoretical plate is shown (Lees, 1980).

Intervals	Holdup/theoretical plate
Conventional trays such as sieve, valve, etc.	40–100 mm liquid
Packing	30–70 mm liquid
Film trays	10–20 mm liquid

High efficiency packing, such as oriented wire packing (Koch/Sulzer, Flexipack, Goodlow), has a thin film of liquid on the wires so that the total liquid holdup is relatively low. Other suggestions from Lees (1980) include using tall thin columns such as those used for heat sensitive materials, and

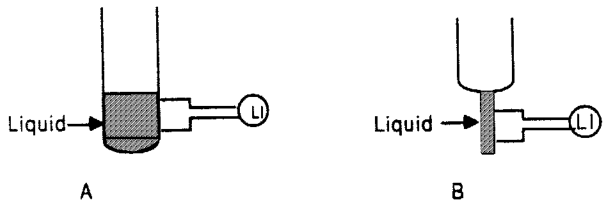

FIG. 5. A, Level indicator on the bottom of a distillation column; considerable liquid inventory. B, Level indicator on pipe leading from bottom of distillation column; low liquid inventory.

locating peripheral equipment, such as reboilers and bottoms pumps, inside the column.

A new distillation process using centrifugal force, called the Higee distillation process, is said to be able to provide a 1000-fold reduction in inventory (Kletz, 1985a). One simple method of reducing volume of liquid in the bottom of a distillation column is shown in Fig. 5B (Geyer, 1986). The inventory is reduced because the level control is used on a pipe leg on the bottom of the column, instead of using the entire column diameter as shown in Fig. 5A. This poses some control problems, but it has been shown, in practice, that they can be solved. It is often possible to reduce the inventory in distillation processes, although occasionally at somewhat increased costs. In the design of inherently safer plants, the options available to reduce inventory in distillation equipment should be carefully considered when flammable and toxic materials are involved, even though the apparent first costs may be greater.

E. Minimizing Inventory in Heat Exchangers

Heat exchangers fail in pressure service more often than pressure vessels, largely because of mechanical and corrosion problems (Lees, 1980). Failures that occur often are the result of exposure to operating conditions more severe than those for which the system was designed. The process designer should try to anticipate unusual conditions to which heat exchangers may be subjected and install safeguards or other features to prevent failure. Failures that can occur include

(1) excessive stress by external loads or uneven tightening of flanges,
(2) stress cycling caused by pressure changes,
(3) thermal shock and thermal cycling,
(4) hydrogen attack, and
(5) corrosion failure.

TABLE I
SURFACE COMPACTNESS OF HEAT EXCHANGERS

Type of exchanger	Surface compactness, M^2/M^3
Shell and tube	70–150
Plate	120–225
Spiral plate	up to 185
Shell and finned tube	up to 3300
Plate–fin	up to 5900
Regenerate—rotary	up to 6600
Regenerative—fixed	up to 15,000 (may be much less)

Since failure of heat exchangers can be a significant problem, it is desirable to minimize the inventory of hazardous materials in heat exchangers. Kletz (1985a) has reported on the classification of heat exchangers according to the ratio of heat-transfer surface to volume. Some typical figures are reported in Table I. Plate exchangers require a large amount of gasketing, which makes them unsuitable in some applications. Some of the difficulties seem to have been overcome since plate exchangers are now used extensively on off-shore oil platforms and increasingly in the oil industry. Plate heat-exchangers may fit into any flowsheet where heat may be exchanged between fluids at pressures and temperatures of up to 300 psi and 150°C, respectively. (Sjoren and Grueiro, 1983). Heat transfer in shell and tube exchangers can be improved, and thus the inventory reduced, by inserting a matrix of wire into the tubes, which promotes turbulence near the walls (Kletz, 1985b).

It may be possible to reduce the inventory of hazardous materials in shell and tube heat-exchangers by using careful design that results in a heat exchanger no larger than is necessary for the job. This also makes good sense from an economic point of view. Several heat-exchanger computer design programs are available that make close design possible easily and quickly. One of these programs that has received good acceptance is B-JAC[2] (Pase, 1986). This is an integrated, interactive program that can analyze in minutes dozens of alternatives that would require weeks to do by skilled individuals with hand calculators.

It also may be possible to reduce heat-exchanger inventory by using smaller tubes than usual. Manufacturing people generally don't like small tubes in heat exchangers because they are harder to clean than large tubes. Also, higher

[2] B-JAC is a registered trademark of B-JAC Computer Services, Inc., Midlothian, VA.

pressure drop may be required, which would cause higher power costs. Tubes with a diameter of $\frac{3}{4}$ in., instead of the more common 1-in. tubes, may be a reasonable compromise in many cases.

F. Reducing the Possibility of Losses from Dust Explosions (Brasie, 1986)

Most organic solids, metals, and some combustible inorganic salts can form explosive dust clouds. In order to have a dust explosion, certain elements are necessary: (1) Particles of dust of suitable size, (2) A sufficient source of ignition energy, (3) A concentration of dust within explosive limits. If an explosive dust in air that meets the above criteria occurs in a process, an explosion should be considered inevitable. The process designer of inherently safer plants must take into account the possibility of dust explosions and design accordingly.

In dust explosions the combustion process is very rapid. The flame speed is high compared to that in gas deflagrations. However, detonations normally do not occur in dust explosions in industrial plants. In a serious industrial dust explosion, two steps often occur. First, a primary explosion occurs in part of a plant, causing an air disturbance. Second, the air disturbance disperses dust and causes a secondary explosion. The secondary explosion is often more destructive than the primary explosion. There is a great deal of literature on dust explosions, which is available to the process designer. See, for example, Lees (1980) for a bibliography on dust explosions.

If, in a process, flammable (explosive) dust is inevitable, several alternatives or combinations of alternatives are available:

(1) Containment (maximum pressure is usually below 120 psig)
(2) Explosion venting to a safe place
(3) Inerting (most organic dusts are nonflammable in atmospheres containing less than about 10% oxygen)
(4) Suppression (usually a last resort)

A fundamental solution to the dust explosion problem is to use a wet process so that dust suspensions do not occur at all. If a wet process can be used, it is one of the most satisfactory methods. However, the process must be wet enough to be effective. Some dusts with a high moisture content can still ignite. Dust concentrations in major equipment can be designed below the lower flammable limit, but this often cannot be counted on in operation. Dust concentrations cannot be safely designed to be above an upper flammable limit, because such a limit is ill-defined (Lees, 1980). For a large number of flammable dusts, the lower explosion limit lies between 20 and 60 g/m^3. The upper explosion limit is in the range of 2000 and 6000 g/m^3, but this number is of limited importance. A small amount of flammable gas or vapor mixed in with a flammable dust can cause an explosive mixture to be formed even if both are at concentrations below the explosive range by themselves.

Containment is possible by using pressure vessels that have a design pressure at least seven times the normal operating pressure. Since the test pressure is usually 1.5 times the design pressure, testing ensures a vessel that will not fail under the normal maximum explosion pressure of $\sim$7–10 times the starting pressure (Bartknecht, 1981). For example, for a system operating at or near atmospheric pressure, a design pressure of $\sim$100 psig will contain most dust explosions without rupturing. Care must be taken that an explosion in the contained area does not pass into other parts of the equipment that are not as well protected. Properly designed quick-closing valves can stop dust explosions from passing into downstream or upstream equipment.

Venting is only suitable if there is a safe discharge for the material vented. Whenever an explosion-relief venting device is activated, it may be expected that a tongue of flame containing some unburned dust will first be ejected. The unburned dust will be ignited as it flows out the vent and can produce a large fireball that will extend outward, upward, and downward from the vent. It is essential for protection of personnel that venting is to an open place not used by people. If a duct must be used, the explosion pressure in the enclosure will be increased considerably. Therefore, particular attention must be paid to the design of the enclosure in which the explosion could take place. Dust explosion venting was formerly expressed traditionally as a vent area per unit volume of space protected. The National Fire Protection Association 68 (NFPA) (1988) guide has nomographs that can be used to select relief areas required for combustible dusts when test data on the dusts are available. The Nomographs in NFPA 68 are by far the preferred way to design dust explosion-relief devices. A quick but less accurate method, which can be used as a rough guide, is to use the following approximation for vent area (Lees, 1980) for volumes measuring up to 1000 ft^3:

Maximum rate of pressure rise (lb_f/in.^{2} sec)	Vent ratio ft^2/ft^3
$\langle < 5000 \rangle$	1/20
$\langle 5000–10{,}000 \rangle$	1/15
$\langle > 10{,}000 \rangle$	1/10

Relief venting to reduce dust explosion pressure requires that the equipment to be protected has a certain minimum strength. If the enclosure strength is too low, the enclosure will be damaged or destroyed before the explosion relief device can function. NFPA 68 (1988) states that the strength of the enclosure should exceed the vent relief pressure by at least 0.35 psi. For industrial equipment such as dryers and baghouses, it is often desirable to have considerably more strength built into the structure to reduce the size of the vent area required. Also, the supporting structure for the enclosure must be strong enough to withstand any reaction forces developed as a result of operating the vent. An example of industrial equipment designed for explosion venting is a baghouse sold by the Dust Control Equipment Co., Jeffersontown, KY. This baghouse, designed for explosive dust being handled in a 13,500 cfm air stream, normally operates at 6 in. negative water pressure. The unit is designed for 13,500 scfm, 1 psig negative water pressure, 2 psig positive design pressure, and an instantaneous pulse pressure of 10 psig. It is constructed of four modules, each having an explosion vent membrane that ruptures at 1.5 psig. The explosion vent membranes are on the "dirty" sides of the bags, and are located on the lower, vertical exterior walls to reduce internal pressure drop in the event of an explosion. The purpose of relief venting is to ensure that, in the event of an explosion within the installation, discharge of unburned mixture and combustion products to the atmosphere will occur in time to prevent unacceptably high pressures. The relief vent must be located in such a way that an explosion will not cause harm to personnel when the relief system vents.

There are several ways to achieve efficient relief venting. Bursting discs are widely used. Explosion doors are also widely used, but their effectiveness can be hindered by the inertia of the explosion door. If explosion doors are used, the flow of combustion products and unburned mixture during the relief process may be hindered, and it may be necessary to increase the relief area or increase the mechanical strength of the enclosure to be protected. Vent panels are being used more frequently. These may be blow out panels held in place by special clamps. These panels must be designed so they will release at as low an internal pressure as possible, yet stay in place when subjected to external wind forces. Rupture diaphragm devices may be designed as square, round, or to fit curved surfaces such as silos and cyclones. The use of vent relief devices is discussed in NFPA 68 (1988). Recent developments in venting of deflagrations are also available in NFPA 68 (1988).

Inerting is a very good preventive measure against dust explosions. The maximum oxygen concentration at which dust explosions are "just not possible" cannot be predicted accurately since it depends on the nature of the combustible material; testing is usually required. It has been found that in an atmosphere of 10% oxygen and 90% nitrogen, combustible organic dusts are no longer explosive. To allow a safety margin, it is good industrial practice to maintain oxygen concentrations below 8%. For metal dusts, the allowable oxygen content is ~4% (NFPA 68, 1988). Inert gases containing nitrogen may be supplied by combustion gases from a natural gas burner, nitrogen from a cryogenic unit, nitrogen from a membrane unit, or nitrogen from a pressure-swing adsorption unit. The economics from each of these and other possible sources should be investigated before making a choice. If inerting is used, a reliable, steady source of inert gas must be available. A number of sensors should be installed to be sure the installation can be started only when the oxygen content is below the critical limit and that automatic shutdown happens when this limit is exceeded. Continuous oxygen analyzers, frequently checked for accuracy and operability, should be used. Inerting leads to the possibility of asphyxiation of operating personnel if they are exposed to the inert gas. Strict precautions must be taken to prevent exposure of personnel to inerting atmospheres.

Other inert materials that can be used include water vapor and carbon dioxide, which are somewhat more effective than nitrogen because they have higher heat capacities. To use water vapor effectively as an inerting agent at atmospheric pressure, the temperature should be ~90–95°C. Carbon dioxide is an effective inerting agent, but it has significant solubility in water and other materials and is reactive with alkaline substances.

Explosion suppression systems are designed to prevent the creation of unacceptably high pressure by explosions within enclosures that are not designed to withstand the maximum explosion pressure (NFPA 69, 1986). They can protect process plants against damage and also protect operating personnel in the area. Explosion suppression systems restrict and confine the flames in a very early stage of the explosion, but suppression systems are expensive and require more maintenance than relief venting devices. These may be the reasons this type of safeguard has not been as widely used in industry as one might expect, although its effectiveness has been proven by much practical experience. Explosion suppression systems consist of a sensor system that will detect an incipient explosion and pressurized extinguishers in which rapid action valves will be activated by the sensor. The extinguishing medium is injected into the protected enclosure and evenly dispersed in the shortest possible time. The flames of the explosion are quenched, and the explosion is restricted. There are three types of sensors.

(1) Thermoelectrical—seldom used because they are effective only if installed close to the ignition source, which is usually not known

(2) Optical—which have the drawback of having their action considerably delayed by the dust cloud if a dust explosion occurs; infrared sensors are available that are said to function, even in dust clouds

(3) Pressure sensors—best used for suppression systems since the pressure at an early stage of an explosion in an enclosure will spread evenly and at the

speed of sound in all directions; these detect an incipient explosion with sufficient reliability to activate the extinguisher valves at a predetermined explosion pressure

The extinguishing agent used in dust explosions may be a powder ejected into the enclosure with a gas propellant (usually nitrogen) at 60–120 bar. Effective extinguishing agents include ammonium phosphate and sodium bicarbonate powders, which are popular in Europe. Tests should be made to be sure the extinguishing agent is effective for the dust being used. Occasionally water is used.

In the United States, suppression systems using Halon 1301 (bromotrifluoromethane) (NFPA 69, 1986) to quench the flames in industrial equipment are popular because damage to the product and to electrical components and other equipment is minimized. Halon 1301 is also used for flame suppression in areas occupied by people such as in computer rooms. Extinguishing flames successfully can usually be achieved at Halon 1301 concentrations of $\sim 5\%$ for about 10 min., which usually allows people time to escape the area without harm. Halon 1301 is colorless and odorless and has minimal, if any, central nervous effects to people below a 7% concentration for exposures of ~ 5 min. However, the decomposition products of Halon 1301 that may result from a fire are quite toxic. They have a characteristic sharp, acrid odor that provides a built-in warning system to people. Halon compounds are fluorocarbons which are being phased out of use because of environmental concerns. Substitutes are being developed and should be considered as they become available.

Explosion suppression is a proven technology and should be considered as a candidate for explosion protection. The NFPA has published a standard reference (NFPA 69, 1986) on explosion-suppression protection. Manufacturers should be consulted on design, installation, and maintenance. But, even with explosion suppression, it is common for the explosion pressure to reach 1 atm before it is suppressed. The added pressure surge from the injection of the suppressing agent must also be considered. Therefore, sufficient mechanical strength is always required for enclosures protected by explosion suppression.

G. Substituting Less Hazardous Materials in Processes, Transportation, and Storage

It may be possible to substitute a less hazardous material for a hazardous product. For example, bleaching powder can be used in swimming pools instead of chlorine (Kletz, 1985b). Benzoyl peroxide, an initiator used in polymerization reactions, is available as a paste in water, which makes it much less shock sensitive than the dry form. Phosgene is a highly toxic material used to make *N*-phenyl carbamate insecticides and other widely used chemicals. It is a key reactant in producing methyl isocyanate (MIC), the highly toxic gas released at Bhopal, India, in December, 1984. Enichem Co., of Italy, has developed a carbamation route to *N*- methyl carbamate insecticides that uses diphenylcarbonate instead of phosgene. For some uses, PPG Industries is providing diphenyl carbonate powder that is considerably less toxic to ship and handle than phosgene. Other work continues on phosgene substitutes and safer value-added phosgene products. Most of these substitutes involve higher initial costs (Brooks *et al.*, 1986a). Other substitutes have been used to make transportation, storage and processing safer.

(1) Shipping ethylene dibromide instead of bromine
(2) Shipping ethyl benzene instead of ethylene
(3) Storing and shipping chlorinated hydrocarbons instead of chlorine
(4) Storing and shipping methanol instead of liquefied methane
(5) Storing and shipping carbon tetrachloride instead of anhydrous hydrochloric acid; the CCl_4 is burned with supplemental fuel to make HCl on demand at the user's site
(6) Using magnesium hydroxide slurry to control pH instead of concentrated sodium hydroxide solutions, which are corrosive to humans and relatively hazardous to handle; magnesium hydroxide slurry is relatively safe to use in comparison
(7) Using pellets of flammable solids instead of finely divided solids to reduce dust explosion problems

The use of substitutes may appear to be more costly. However, the added safety provided by substitutes may make their use worthwhile and can, in some cases, actually lower the true cost of the project when the overall impact on the process, surrounding areas, and shipping is considered. Substitutes should be employed only if it is known that overall risk will be reduced. Inadequately tested processes and products may introduce unrecognized health, safety, and environmental problems.

H. In Situ Production and Consumption of Hazardous Raw Materials

Some process raw materials are so hazardous to ship and store that it is very desirable to minimize the amount of these materials on hand. Occasionally, it is possible to achieve this by making the hazardous materials on site out of less hazardous materials just before processing so there is only a small amount of the hazardous materials present at any time. An example of *in situ* manufacturing can be found in the batch suspension polymerization of vinyl compounds such as vinyl chloride. One initiator that is useful because of its short half-life and good polymerization properties is diisopropyl peroxydicarbonate (IPP). It has a half-life of 10 hrs as a 50% solution in toluene. This short half-life makes it a desirable initiator. However, storage of IPP is difficult and may be hazardous. A 50% solution of IPP in toluene should be kept between −20°C and −10°C. Above −10°C, it begins to decompose fairly rapidly, giving off flammable vapors and possibly bursting into flame. Below −20°C it freezes and becomes difficult to handle. A process has been developed (Cox and Shiah, 1970) in which IPP can be made as needed, *in situ*, before use by reacting dilute hydrogen peroxide and isopropyl chloroformate in part of the water phase of the suspension polymerization batch reaction just before polymerization. As a result, there is no need to ship and store IPP. The process is much safer, even though the starting materials (hydrogen peroxide and isopropyl chloroformate) are hazardous chemicals, because IPP is so much more hazardous.

The possibility for *in situ* manufacturing of hazardous chemicals for process use to minimize storage and handling may not be obvious in most processes. It may be appropriate to challenge the chemists, who are best able to develop *in situ* manufacturing, early enough in the process so they can develop the technology necessary to incorporate it into the plant design. These processes should be adequately tested to make certain additional unforeseen risks are not introduced.

I. Using Incineration to Dispose of Hazardous Materials

First consideration should be given to minimizing the production of hazardous waste materials at the source. The next consideration should be to recover, reclaim, and recycle hazardous materials. These activities minimize the need to manage hazardous wastes, resulting in minimal adverse impact on the environment. When all reasonable efforts have been made to minimize the production of hazardous waste materials, and it is impractical or uneconomical to further recover, reclaim, or recycle the remaining hazardous wastes, other means of handling these materials must be considered. Quite often the best solution for the disposal of nonrecyclable hazardous vapors and liquids is to burn them under carefully controlled conditions. The technology of incineration has advanced a great deal, and it is possible to burn hazardous materials routinely and obtain very high levels of destruction removal efficiency of the principal organic hazardous constituents (POHCs). It is common to generate steam with a system designed to burn hazardous vapors and liquids, so it may actually be more profitable and more environmentally sound to burn these materials than to dispose of or treat them in other ways. Chlorinated hydrocarbons may be burned to produce aqueous hydrochloric acid which has a value. The advantage of burning is that it is usually a final solution with no significant emission of hazardous materials. Other methods of recovery usually require some further treatment of the recovered waste (Frey, 1987).

Flares are often used to dispose of flammable gases that are produced at widely varying rates in normal startup and in upset conditions. The discharge of gas to a flare system is inevitably somewhat erratic. In large installations, the flame on a flare stack is often several hundred feet long and can have a heat release rate of 10^7 BTU/hr(Lees, 1980). There is intense radiation from a flare. It is generally necessary, therefore, to have an area around the flare where people may not be located. A large flare can thus sterilize a sizable area of land. The level of heat radiation from a flare that is acceptable at ground level is 1000 BTU/(ft^2)(hr), of which 250 BTU/(ft^2)(hr) is solar radiation. If people are required to work in this area, radiation should be limited to 500 BTU/(ft^2)(hr)(Lees, 1980). If a flare is used, the layout should be designed keeping in mind the large area that may be necessary to suitably isolate the flare. An alternative may be to use enclosed flares. Flare systems can explode because of flashback. Many devices and techniques are available to reduce the possibility of flashback and to prevent air from getting into the system. Open flares should not be used to burn material containing significant quantities of sulfur, chlorine, or other materials that produce toxic compounds when burned. When it is necessary to burn these materials, burners with scrubbing equipment that will remove toxic products of combustion should be used.

Enclosed Flares

Smoke, glare, and noise from a flare are environmentally objectionable. This may inhibit their use, even though from a strict safety point of view, these flares are desirable. Smoke can generally be eliminated or reduced to a low level by methods, often involving the use of steam, which promote combustion. Light and noise from the flame can be eliminated by using enclosed burning systems offered by several companies. John Zink Co. (4401 S. Peoria, Tulsa, OK), for example, offers enclosed flares that can handle up to 200,000 lb/hr of waste gas. The largest of these enclosed flares consists of a field-erected refractory-lined enclosure 44 ft in diameter and 125 ft high. Occasionally they are used along with an elevated flare to handle any waste gas in excess of the enclosed flare's capacity.

Relatively small enclosed flares are often more applicable in the chemical industry. For example, a unit to handle 25 ft^3/min of a waste hydrocarbon gas requires an enclosed, refractory-lined flare about 3 ft in outside diameter and 25 ft in height. Enclosed flare systems have been especially popular in Europe. These enclosed flare systems make it possible to flare waste gas in populated areas or other areas where normal flaring would be objectionable. They should remove some of the reluctance of process designers to use flares, when the flares are a safe way to solve some potential problems.

V. Equipment Design Opportunities

This part will discuss opportunities, primarily in the design of equipment, to make a plant inherently safer. This equipment includes mechanical equipment, piping systems, control systems, and electrical systems. There have been many developments in recent years that process designers can use to improve plant safety and make the plant inherently safer.

A. Avoiding Catastrophic Failure of Engineering Materials

The choices of the construction materials used in a chemical plant are some of the most important decisions a process designer will make. Inherently safer plants will be designed by people who take advantage of the latest and best available technology to avoid catastrophic failure (Liening, 1986a,b). It is not possible for most process designers to be experts in the field of corrosion. Therefore, it is necessary to make use of the resources available.

(1) *Previous plant experience*—this can be an ideal source of information. However, personnel turnover in manufacturing plants may diminish that source of expertise.

(2) *Judgements of professional technical experts*—these people, if they are available and understand corrosion, are often the best source of information, particularly if the problem is new.

(3) *Literature searches*—the problem here is that much of the information available on construction materials is not available in the usual chemical engineering journals and books. Also, there is so much information available, it is hard for the nonspecialist to choose the best information. A technical expert may be helpful here.

(4) *Vendors*—these sources can provide a great deal of information on existing well-known processes but may be of limited help on proprietary or new processes. Also, one must be careful of vendor data, since there is often no way of knowing how valid the information is and obviously, the vendor is usually trying to make a sale.

(5) *Laboratory testing*—sometimes there is no substitute for laboratory tests or tests in existing plant equipment. This can be expensive and time-consuming, but in critical applications, where there is inadequate knowledge, testing is necessary.

1. *Metals*

Uniform corrosion in metals can usually be predicted from lab tests or experience. Corrosion allowances that require thicker metal can be called for in the design of equipment when uniform corrosion rates are expected. However, uniform corrosion is often not the worst thing that can happen to materials. The most important materials failure to avoid in the design of metal equipment is *sudden catastrophic failure*. This occurs when the material fractures under impulse instead of bending. Catastrophic failure can cause complete destruction of piping or equipment and can result in explosions, huge spills, and consequent fires. Some of the more common types of catastrophic failure are described in the following sections.

a. *Low Temperature Brittleness.* Carbon steel becomes more brittle (less ductile) as temperature decreases. Almost any carbon steel will become brittle at −30°C (−20°F). Some grades of steel become brittle at surprisingly high temperatures.

(1) A515 steel can become brittle as high as 10°C (50°F)
(2) A53 steel can become brittle as high as 0°C (32°F)
(3) Grey cast iron is brittle at all usable temperatures
(4) Silicon cast iron, which is very corrosion resistant, is brittle at all usable temperatures and can fail due to thermal shock

Stainless steels can usually be used safely down to about cryogenic temperatures. Tanker ships carrying liquefied natural gas (LNG) are typically made of steel with 9% nickel added to impart cold temperature ductility properties.

Process designers should check on the possibility of cold temperatures in their process and be sure they have specified the right material for these conditions. Materials used in equipment handling low-temperature fluids should have a ductile–brittle transition temperature below not only the normal operating temperature, but also the minimum temperature that may be expected to occur under abnormal conditions (Lees, 1980).

b. *Stress Corrosion Cracking.* Stress corrosion cracking is a very serious corrosion problem because it has the potential to cause even inherently ductile alloys to fail catastrophically. Many alloys stress corrode crack in a variety of environments, but chloride induced stress corrosion cracking of stainless steel is the most well-known type. This can occur with many grades of stainless steels at 50°C or above. The corrosion depends on temperature, chloride ion concentration, stress, and to some extent, pH. Chloride ion stress corrosion cracking can become worse as a result of residual fabrication stresses, including those from shaping and welding. Stainless steel vessels can corrode and crack from the outside in salty atmospheres, especially near oceans. The corrosion can become worse from insulation that traps salty material on the equipment surface. Corrosion under insulation is a particularly insidious problem because the damage may not be apparent. Typically, corrosion occurs because the weather seal is damaged and moisture enters the insulation. The insulation holds moisture against the metal, possibly concentrating chlorides on the surface, causing continuous attack and extensive damage.

Stress corrosion cracking from chloride ions can usually be avoided by using alloys with a nickel content above ~32%. Alloys such as Carpenter 20CB3, Hastelloy G, and Incolloy 825 are high in nickel and are very resistant. Modern testing methods make it possible to predict chloride stress corrosion cracking in the laboratory in a relatively short time with a high degree of confidence.

c. *Hydrogen Embrittlement.* Hydrogen can come from corrosion reactions with water, producing hydrogen that diffuses into the metal. Hydrogen embrittlement occurs most often in high-strength steels such as in relief-valve springs. It can also occur in high-strength stainless steels such as those used in valve stems and springs. Hydrogen sulfide is especially troublesome with high-strength stainless steel.

d. *Other Types of Catastrophic Corrosion.* There are many other types of catastrophic corrosion that can occur, such as

(1) corrosion with very high penetration rates involving pitting and crevice corrosion and galvanic corrosion,

(2) fatigue failure,

(3) creep (usually unlikely under normal conditions but can be caused by misoperation or fire),

(4) mechanical shock which can be caused by water hammer,

(5) thermal fatigue, in which temperature cycles can cause failure of ductile materials

(6) thermal shock, in which high rates of temperature change can cause failure in brittle materials,

(7) zinc embrittlement, in which the amount of molten zinc required to cause embrittlement of stainless steel is small, and at high temperatures, can fail in seconds (Lees, 1980); this type of failure normally occurs only in a fire,

but can also result from welding stainless steel to galvanized steel,

(8) caustic embrittlement, which has been a frequent cause of failure in boilers, and

(9) nitrate stress corrosion, which can result from a high concentration of nitrates, low pH, temperature above 80°C. and high stress.

It was concluded that nitrate stress corrosion caused the crack in the reactor at Flixborough. The reactor was removed and replaced with a 20 in. pipe that failed. The cracking occurred because cooling water containing nitrite had been sprayed on the reactor (Lees, 1980). Many other types of corrosion can occur with catastrophic consequences. The process designer should be aware of special problems that can result in the process and should obtain specialized help if necessary since corrosion is a specialized and very complicated field. It is impossible for most process designers to keep up with corrosion technology without help.

Stainless steel clad over carbon steel can be treated, in terms of corrosion, as a monolithic stainless vessel. This type of construction, which requires special fabrication techniques, is typically used only for heavy wall vessels. A relatively new area of technology that has met with considerable success at Dow is called Resista-Clad.[3] In this process, a thin layer of highly corrosion-resistant (and usually relatively expensive) metal is welded by special techniques. The metal cladding may be several feet wide and is usually welded to a steel (or other metal) substrate, in rows with about 1 in. spacing. The weld bond is about 30% of the total surface. The resulting equipment has the corrosion resistance of the thin layer of cladding and the physical strength of the substrate. It can also withstand a vacuum, which is a big advantage. It can be more tolerant of abuses and upsets, both mechanical and chemical, than other types of less corrosion-resistant materials used in a solid, nonclad form, and still be of reasonable cost compared to less corrosion-resistant materials. It will probably be less likely to fail catastrophically. The metals that can be used for the cladding include tantalum, columbium (niobium), titanium, nickel and some nickel alloys (under development), and zirconium. Thickness can range from 0.02 to 0.1 in. The substrate can include mild steel, stainless steel, aluminum, and copper.

Cost of this process is about 50% more than glass-lined steel and about 67% of equivalent vacuum-proof, all-metal construction of the same metal as the cladding. It can be used in very large vessels and over complex curves. It might be better to use Resista-Clad with a very corrosion-resistant metal than to use a less corrosion-resistant solid metal construction in which there is a significant risk of failure. This may be especially true if there is doubt about the

[3] Resista-Clad is a registered trademark of the Pfaudler-USA Co.

resistance to catastrophic failure of the less corrosion-resistant material, or if there is no time to get data.

Explosively clad metals, of which Deta-Clad[4] is an example, are used mostly for small items such as tube sheets and heads for small heat exchangers or vessels. It is usually not economical for large surfaces or complex shapes. Nickel–chromium–molybdenum alloys and some other expensive metals can be applied to carbon steel by explosive bonding.

2. *Nonmetals*

Glass-lined steel is the material of choice in many applications, particularly in highly acidic conditions and where a smooth, nonsticking, easily cleanable finish is required. The technology has advanced to the point that glass-lined vessels can be made completely free of flaws where corrosion can occur. Agitators and seals can be made that have essentially no exposed metal. Glass linings with improved alkali resistance (up to pH 12) are available, however, glass is not suitable for hydrofluoric acid and hot concentrated phosphoric acid, nor for hot alkaline solutions (*Perry's*, 1984). The chief drawback of glass-lined steel is its brittleness and susceptibility to thermal shock. A nucleated crystalline composite form of glass has superior mechanical properties compared to conventional glass-lined steel. It has three to four times the thermal-shock resistance of glassed steel. However, this form of glass is somewhat less corrosion-resistant, in some conditions, than the best conventional glass-lined steel. Another drawback of glass-lined steel, compared to metals, is its reduced heat transfer capability.

Glass-lined vessels with alloy faced flanges are available at a reasonable cost. Alloy metal flanges on glass-lined vessels should be considered whenever hazardous, flammable, or toxic materials are handled under pressure. The alloy used must be compatible with the glass coating, which must cover the welded joint between the steel shell and the alloy flange. Metal flanges make possible the use of high-integrity gaskets such as spiral wound gaskets, which usually cannot be used on glass surfaces. The metal alloys available for flanges are resistant to a wide variety of extremely corrosive materials.

In general, if the special properties of glass-lined steel are not essential, many manufacturing and process design people prefer to use a highly corrosion-resistant metal instead of glass-lined steel. The brittle nature of glass and its possible failure are of continual concern in any plant that uses glass-lined steel. On the other hand, there are thousands of examples of glass-lined equipment that have served well for many years. Glass failure in a glass-lined vessel does not usually cause catastrophic failure in a short amount of

[4] Deta-Clad is a registered trademark of E. I. du Pont de Nemours & Co., Inc., Wilmington, DE.

time because the steel tank itself will usually survive for a significant amount of time. Glass failure may cause holes in the shell to occur, but the vessel does not usually quickly lose its ability to withstand pressure.

3. *Plastic Materials*

The number and combinations of plastics available to the chemical industry is very large and growing. The choices available to the process designer provide many opportunities but also some possible problems. There are numerous advantages in using plastics. They are

(1) lightweight,
(2) good thermal insulators,
(3) good electrical insulators,
(4) relatively easy to fabricate and install,
(5) often cheaper and faster to build,
(6) low in friction factors,
(7) excellent resistors to weak mineral acids,
(8) unaffected by most inorganic salt solutions, and
(9) do not corrode in the electrochemical sense, therefore they are resistant to changes in pH, minor impurities, and oxygen content.

There are also a number of disadvantages in using plastics. They are

(1) limited to relatively moderate temperatures (200°C is high for plastics),
(2) less resistant to mechanical abuse,
(3) high thermal expansion rates,
(4) relatively low strengths (unless reinforced),
(5) often only fair resistors to solvents,
(6) difficult to ground electrically,
(7) poor resistors to organics,
(8) can swell or dissolve in the presence of some solvents,
(9) permeable to some solvents,
(10) flammable and can produce toxic fumes,
(11) much lower heat-transfer coefficients than metals.

Several plastics, with high resistance to chemical attack and high temperatures, deserve special mention for process designers of inherently safer plants. For example, tetrafluoroethylene (TFE), commonly called Teflon brand TFE, is practically unaffected by all alkalies and acids except fluorine and chlorine gas at elevated temperatures, and molten metals. It retains its properties at temperatures up to 260°C. Other plastics that have similarly excellent properties (but are different enough that they each have their niche) include chlorotrifluoroethylene (CTFE); Teflon FEP, a copolymer of tetrafluoroethylene and hexafluoropropylene; polyvinylidene fluoride (PVF_2) (also known as PVDF or Kynar[5]), and perfluoroalkoxy (PFA) (an improved moldable grade of Teflon). These plastics have excellent properties for use in many areas of chemical plants and, when properly used, can provide excellent safety features in preventing leakage, corrosion, and solvent attack. They are not panaceas; each has its limitations, but in the right application, they provide excellent service.

Permeation can be a problem with these materials and can cause corrosion of the substrate. Some of these plastics are significantly less permeable than others. Permeation is especially a problem with Teflon when used with many liquids, including liquids as different as styrene and bromine. Kynar is generally more resistant to permeation than Teflon, but may be more brittle. Cold flow may also be a problem with some of these polymers. The use of glass filled polymers can help overcome cold flow.

Fiberglass reinforced plastics (FRPs) are very popular because they combine the chemical resistant properties of plastics with the considerable strength of glass. Other fibers may be used to reinforce plastics. The lack of homogeneity and the friable nature of FRP composite structures dictate that caution be used in mechanical design, vendor selection, inspection, shipment, installation, and use (*Perry's*, 1984). Many different resins can be used to manufacture FRP items. The choice depends on different mechanical and corrosion-resistance requirements. In general, when hazardous and especially flammable chemicals are involved, FRP vessels are not usually considered to be inherently safe to use for service involving significant pressures, unless great care and extensive testing of similar vessels to destruction is carried out. Large FRP vessels intended for vacuum service, or service where there could accidentally be a vacuum, should be used with great care, if at all. Many FRP tanks have inadvertently been destroyed by being "sucked in" when a vacuum was accidentally applied to them. FRP vessels are also not firesafe, as metal vessels are, and are not usually considered to be satisfactory for use with flammable materials in the chemical industry. It is difficult to construct FRP pressure vessels to meet the conditions of ASME code, Section 10, "Fiber Glass Reinforced Pressure Vessels." Up to this time, it has been required to build two vessels and test one to destruction to get ASME approval.

B. Using Adequate Redundancy of Instrument and Control Systems

Computer controlled chemical plants are becoming the rule rather than the exception. As a result, it is possible to measure more variables and get more

[5] Kynar is registered trademark of the Pennwalt Corporation, Pennwalt Building, Three Parkway, Philadelphia PA 19102.

process information than ever before. There is now an opportunity to make chemical plants inherently safer than ever before. However, it must be kept in mind that instruments and control components *will* fail. It is not a question of *if* they will fail, but *when* they will fail, and what the consequences will be. Therefore, the question of redundancy must be thoroughly considered. The system must be designed so that when failure occurs, the plant is still safe. Redundant measurement means obtaining the same process information with two like measurements or two measurements, using different principles.

Redundant measurements can be *calculated* or *inferred* measurements (Grinwis *et al.*, 1986). Two like measurements could be from two pressure transmitters, two temperature measurement, or two level measurements. An example of inferred measurement could be measuring temperature in a boiler and, using a pressure gauge and vapor pressure tables, measuring the pressure to check an actual temperature measurement.

A continuous analog signal that is continuously monitored by a digital computer is generally preferable to a single point or single switch such as a high-level switch or high-pressure switch. A continuous analog measurement can give valuable information about what the value is now and can be used to compute values or compare with other measurements. Analog inputs may be visual and one can see what the set point is and what the actual value is. The software security system determines who changes set points, and it is not easy to defeat.

A single point (digital) signal only determines whether switch contacts are open or not. It can indicate that something has happened, but not that it is going to happen. It cannot provide information to anticipate a problem that may be building up or a history about why the problem happened. Single point signals are easy to defeat. Some single point measurements are necessary, such as fire eyes and backup high-level switches. As a rule, it is best to avoid both pressure transmitters on the same tap, both temperature measuring devices in the same well, both level transmitters on the same tap or equalizing line, and any two measurements installed so that the same problem can cause a loss of both measurements. It is a good idea if possible, to use devices that use different principles to measure the same variable.

An alarm should sound any time redundant inputs disagree. In most cases, the operating personnel will have to decide what to do. In some cases the computer control system will have to decide by itself what to do if redundant inputs disagree. The more hazardous the process, the more it is necessary to use multiple sensors for flow, temperature, pressure, and other variables. Since it must be assumed that all measuring devices will fail, they should fail to an alarm state. If a device fails to a nonalarm condition, there can be serious problems. It is also serious if a device fails to an alarm condition, and there is really not an alarm condition. This is generally not as serious as the first case, but it can provide a false sense of security. Usually it is assumed that two devices measuring the same condition will not fail independently at the same time. If this is assumed, one can consider the effects of different levels of redundancy:

Number of Inputs	Consequence
One	Failure provides no information on whether there is an alarm condition or not.
Two	Failure of one device shows there is a disagreement, but without more information, it cannot be determined whether there is an alarm condition or not. More information is needed; the operator could "vote" if there is time.
Three	Failure of one device leaves two that work; three should be no ambiguity on whether there is an alarm condition or not.

As a matter of interest, if it is assumed that two devices can fail independently at the same time, five separate measuring devices would be required to determine, without ambiguity, that there is an alarm condition, unless more information is available. The vote would be "three out of five" as the consensus to determine if an alarm condition existed. This is rarely done except in the nuclear and aerospace industries.

Large continuous processes exist that are difficult to shut down, and a shutdown may be almost as dangerous or more dangerous than continuing to run in an alarm condition. When these processes do shut down, they must shut down in an orderly manner to avoid damage and hazards. If there is no time to wait for an operator to "vote," or if it is necessary for the operator to have more information, the computer must make the decision, and three or more measuring methods should be considered. The control mechanism should be "intelligent" enough to detect a problem and correct it before the problem gets to a serious stage. This may require corrective action at an early stage. There are numerous examples of this.

(1) If a pump starts up, downstream pressure should go up within a certain time interval. If it doesn't, there should be an alarm.

(2) Materials that react exothermically should require cooling when they are continuously added to a reactor. If cooling is not being called for, the materials are probably not reacting as they should, or there may be an error in flow measurements and there should be an alarm. If the reactants build up in the reactor without reacting as they should, there could be a "bomb" of reactants building up in the process, and waiting to react.

(3) If a signal, such as a level indicator signal, is usually noisy, and it becomes "frozen" on one value, the line to the sensor may be plugged. The computer system should detect this and give an alarm.

(4) The computer system should detect a value that is not following an expected trend. An example is a level indicator or weight indicator on a tank

that is being filled using a pump. If the weight does not increase as the pump operates, something is wrong and there should be an alarm.

(5) If a tank is being filled from another tank, the level or weight on the tank being filled should go up by the same amount as the tank being used to fill it goes down. The computer should check this and give an alarm if it doesn't happen.

(6) A device, such as a temperature or pressure measuring device, that suddenly shows a full-scale or down-scale reading has probably failed. The computer system should detect this and give an alarm.

In a computerized plant, it is best to avoid putting redundant inputs on or in the same slot, cluster, or board in the computer. The safety system should be continuously exercised. An independent safety system suffers from a major drawback, particularly if it is implemented using relays. This drawback is that the safety system usually remains inert for long periods of time. Electronic circuits or relays are subject to failures such that when the safety system is called on to operate, it may be incapable of doing so. The best way to ensure that the safety system has not suffered a fault is to continuously exercise it. This is best done if the safety system is also responsible for control calculations and is constantly in use (Wensley, 1986).

1. Critical Instrument System

Critical instrument systems are any instrument systems that must function properly for the safe operation of the process or to protect equipment. A major concern is instrumentation that has the potential for shutting down a process or unit operation. In computer-controlled plants, not only are the field devices critical. The system that reads the signal, interprets it, and displays it is also critical. Critical instrument systems must be tested and maintained regularly, and recalibrated if necessary. The instrument systems that are associated with the critical instrument should be tested, not just the instrument itself. An "insult" test is preferred—one that simulates a condition the instrument should detect, such as a high level alarm or high oxygen alarm. The insult test should activate the entire system from the sensor to the activating device it is supposed to activate. The design of the plant should take the need for testing into account and make it as easy as possible to test critical instruments systems regularly.

2. Fail-Safe Valves

Valves can have four modes of operation during failure: Fail open, fall closed, fail in the current position, and fail in any position without having an impact in the process (this is rarely a valid option). In order to fail safe, most valves should usually fail closed. There are exceptions. Often cooling water valves and valves in coolant circulating systems should fail open. Diverter valves in solids-handling systems should usually fail in the current position. There are very few cases where it does not matter how a valve should fail.

Many of the fail-safe valves used in chemical processes are quarter-turn valves. Generally, ball valves with spring loaded actuators are recommended so that there is positive fail-safe movement in case of power or air failure. It may not be practical for very large valves to be spring loaded. These large valves should generally have a local air supply tank to cause them to fail to the fail-safe condition.

C. Properly Designing Pressure Relief Systems

Emergency pressure relief systems should be installed to protect vessels and other equipment and their surroundings from the dramatic, often catastrophic, effects of an overpressure and subsequent failure. The process designer of inherently safer plants should use the best tools available to design appropriate pressure relief systems. Fortunately, since 1984 there have been significant developments in the complex field of pressure relief design that now make possible realistic system design. This pressure relief discussion differs from what is commonly referred to as "explosion venting." Events such as dust explosions and flammable vapor deflagrations propagate nonuniformly from a point of initiation, generating pressure and shock waves. Such venting problems are outside the scope of this discussion of pressure relief systems.

The design of relief systems involves, in general, the following steps:

(1) Generate a scenario—what could reasonably happen that could cause high pressures? This could be fire, runaway reactions, phase changes, or leaks from high pressure sources.

(2) Calculate the duty requirements, the lb/hr of material that has to be vented and its physical conditions including temperature, pressure, ratio of vapor to liquid, and physical properties. This is a rather involved calculation.

(3) Calculate the area required to relieve the pressure, based on the duty, inlet and outlet piping, and downstream equipment. This is also a rather involved calculation.

(4) Choose the pressures relief device to be used, which should be specified from vendor information.

A group of chemical companies joined together in 1976 to investigate emergency relief systems. This later resulted in the formation of The Design Institute for Emergency Relief Systems (DIERS), a consortium of 29 companies under the auspices of the American Institute of Chemical Engineers. DIERS was funded with $1.6 million to test existing methods for emergency relief system designs and to "fill in the gaps" in technology in this area, especially in the design of emergency relief systems to handle runaway reactions (Fisher, 1985). DIERS completed contract work and disbanded in 1984.

Huff was the first to publish details of a comprehensive two-phase flow computational method for sizing emergency relief devices, which with refinements, has been in use since 1977 (Huff, 1973, 1977, 1984b). The most significant theoretical and experimental finding of the DIERS program is the ease with which two-phase vapor-liquid flow can occur during an emergency relief situation. The occurrence of two-phase flow during runaway reaction relief almost *always* requires a larger relief system compared to single-phase vapor venting. The required area for two-phase flow venting can be from about twice the area to much more than than this in order to provide adequate relief than if vapor-only venting occurs (Huff, 1977). Failure to recognize this can result in drastically undersized relief systems that will not provide the intended protection.

Two-phase vapor-liquid flow of the type that can affect relief system design occurs as a result of vaporization and gas generation during a runaway reaction. Boiling can take place throughout the entire volume of liquid, not just at the surface. Trapped bubbles, retareded by viscosity and the nature of the fluid, reduce the effective density of the fluid and cause the liquid surface to be raised. When it reaches the height of the relief device, two-phase flow results.

An area that has received considerable attention is the downstream and upstream piping and equipment around a relief device. It is realized that these piping systems can be the flow-limiting elements for the entire relief system. The entire piping system, in which the relief system is located, as well as the relief device itself, must be considered. The expertise for designing relief systems for complex systems has been developed to a high degree. However, many systems are complicated, and the knowledge of exactly how to use the calculational systems described in the literature is not widely available.

The *DIERS Project Manual* (published by the American Institute of Chemical Engineers) is a helpful compendium for experienced safety-relief system engineers. Extensive background and experience are required to properly understand and apply the methodology. Help is available from the DIERS contractors and the DIERS Users Group.

DIERS sponsored development of a comprehensive computer program that can be used to size emergency relief systems for runaway reactions in industrial vessels, if appropriate information is available. This program has considerable potential for widespread use throughout the chemical industry (Grolmes and Lung, 1985). The JAYCOR Corp. has modified an existing proprietary program which is also capable of emergency relief design calculations (Klein, 1986).

An accelerating rate calorimeter (ARC) can be used to provide design values for emergency pressure-relief flow requirements of runaway systems. The ARC is a device used to obtain runaway history of chemical reactions in a closed system (DeHaven, 1983; Huff, 1982, 1984a; Townsend and Tou, 1980). The experimental technique is fairly straightforward, but considerable engineering expertise is required to do the calculations needed to design a relief system from the ARC data.

Another very useful tool called a "bench scale apparatus for characterizing runaway chemical reactions" or Vent Sizing Package (VSP) has been developed and can handle largely unknown systems with a small test cell (~ 100 ml) compared to 9 ml for the ARC. This is an extension of ARC technology, but less engineering expertise is required to do the actual vent sizing. This device allows direct and safe extrapolations on a large scale at relatively low cost. Vents may be sized with less information than is required with other methods. Key physical properties should be known for the processing materials involved. They can be either measured or estimated, although it is not necessary to know the identities of the chemicals involved. Before using the apparatus, differential thermal analysis (DTA) data, or equivalent data, on the materials to be used should be available. This can help determine if the system has such rapid energy release possibilities that detonations or rapid releases of energy could occur, which would be unsafe in the 100 ml test cell. Given the upset condition, the new method allows for the safe extrapolation to full-size process vessels (Fauske and Leung, 1985).

The VSP makes sizing emergency relief systems possible without a comprehensive computer program. The device is a bench scale experimental apparatus that will measure runaway reaction data under adiabatic conditions in a vessel with very low thermal inertia, or phi (ϕ) factor (phi denotes thermal inertia, which is the ratio of the heat capacity of the sample plus the bomb to the heat capacity of the sample). With this equipment, it is possible to predict the vapor–liquid disengagement regime and viscous vs. turbulent flow-pipe behavior. Useful data can be obtained as high as 400 psig. It has a typical thermal inertia, or ϕ factor, of 1.05. The equipment can withstand up to 2500 psig and is hydrostatically tested to 7500 psig.

The ability of the VSP to characterize the vapor–liquid disengagement regime and viscosity effects is important because of the dramatic effect these variables have on relief system size (Fauske and Leung, 1985). No other apparatus is known that can predict these variables under runaway conditions. Figure 6 shows schematically how the unit is designed.

The selection of an actual pressure relief valve to use when the area is known is not a trivial problem, since there are many vendor catalogs and each can be

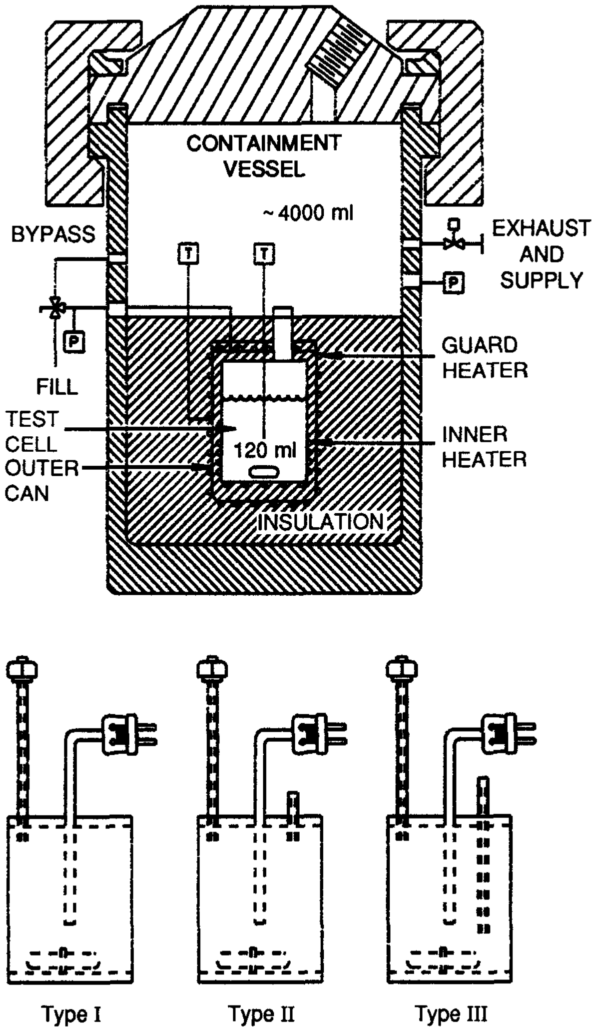

FIG. 6. Small-scale test equipment with closed and open test cell designs. Type I test cell, closed system thermal data; type II test cell, open system vent sizing and flow regime data; type III test cell, open system viscous effects data.

fairly difficult to use unless one is experienced with it. A selection program using a personal computer is available which makes it easy to select the model number for several manufacturers of relief devices (flanged full-nozzle valves only). It will also calculate the API and ASME code areas for certain design cases, but does not consider all cases. It provides good documentation. This program is called SARVAL[6].

When using safety valves to relieve pressure vessels, consider isolating them from the process by using rupture disks (frangible safeties). There are several reasons for this.

(1) They will prevent the process components from leaking into the atmosphere, which can happen with relief valves. Conventional relief valves have an allowable leakage rate; rupture disks do not.

(2) Relief valve life is extended since process components will not contact the valve.

(3) They can possibly extend the time between valve overhauls.

(4) Less-expensive valve material can be used.

Space between a rupture disk and a safety relief valve must be provided along with a monitoring system, or other indicator, to detect disk rupture or leakage. This space should also be provided with a small relief valve to prevent pressure from building up between the relief valve and rupture disk, possibly causing the system to effectively have a higher bursting pressure than intended.

Chemical process fluids can be too hazardous to permit direct venting to the atmosphere. In this case, the vent system can take on the character of a separate chemical processing unit. The configuration of such a vent system is shown in Fig. 7 (Huff, 1987). In this system, provision is made to handle an appreciable amount of liquid that may vent, along with the gases and vapors, from the uncontrolled reaction. This liquid is separated from the gas-phase materials in either a large catch tank or a cyclonic-type separator. The vapors and gases are then treated in a unit such as a scrubber. The discharge from the scrubber can be situated in order to assure adequate plume dispersion in the event of misoperation of the scrubber. If desired, the discharge could go to a flare or to an incinerator equipped with a scrubber to remove toxic compounds formed by burning, such as hydrochloric acid.

D. Providing Safe and Rapid Isolation of Piping Systems or Equipment

It should be possible to easily isolate fluids in equipment and piping when potentially dangerous situations occur. This can be done using emergency block valves (EBVs). An EBV is a manual or remotely-actuated protective device that should be used to provide manual or remote shut-off of

[6] SARVAL is available from Kenonics Controls, 3667 60th Avenue SE, Calgary, Alberta T2C 2E5, Canada.

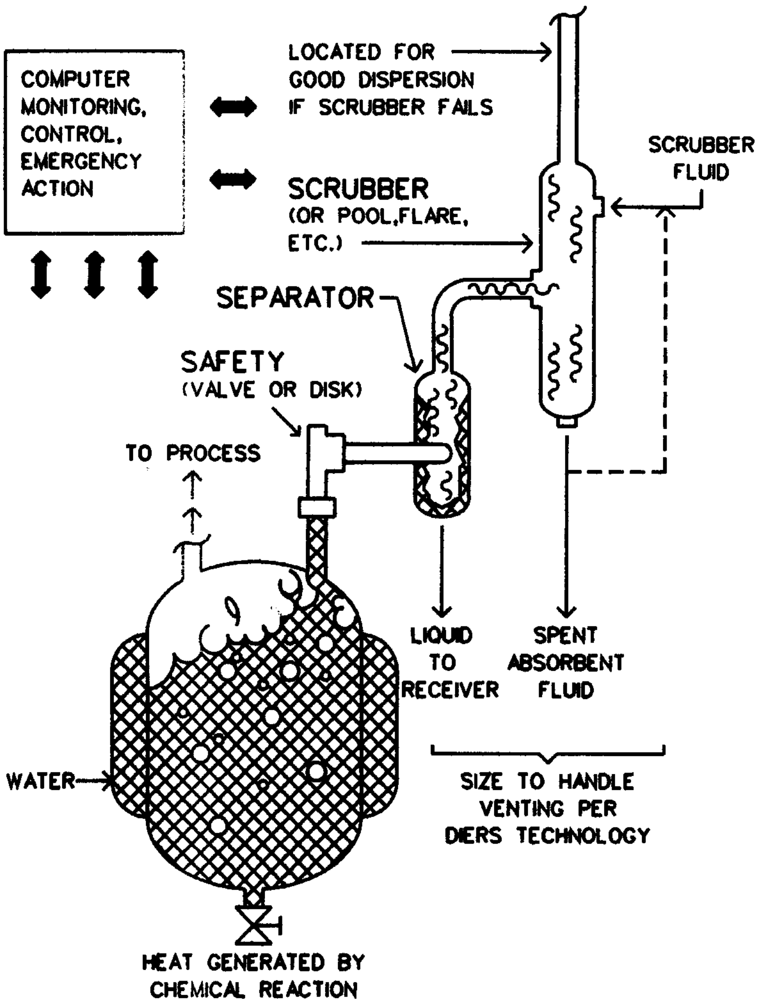

FIG. 7. Typical system for two-phase venting and containment.

uncontrolled gas or liquid flow releases. EBVs can be used to isolate a vessel or other equipment, or an entire unit operation. Manual valves are often used on piping at block limits where it is unlikely there would be a hazard to personnel if an accident occurs. Remotely controlled EBVs are recommended on tanks and on piping in areas where it may be hazardous for personnel in case of an accident or where quick response may be necessary. EBVs used on tanks should be as close as possible to the tank flange and not in the piping away

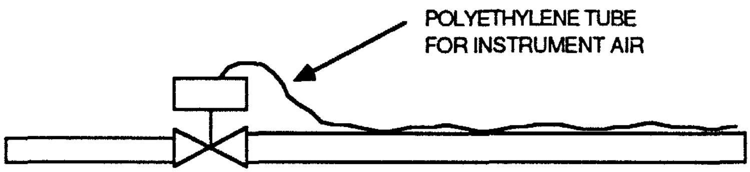

FIG. 8. Polyethylene tubing on fail-safe, spring-loaded, fire-safe valve used as an emergency block valve.

from the tank. In cases where EBVs may be exposed to fire, the valve and valve operator must be fire safe. The valve actuators for remotely controlled EBVs should be air, nitrogen, or hydraulic-pressure operated, with a spring to close to the fail-safe position. The air or nitrogen connection can be polyethylene tubing which will act as a fusible link, causing the valve to close if the tubing is melted or damaged resulting in a loss of air pressure (see Fig. 8). An alternative is to use heat actuated (such as a fusible link) valves. This could be in conjunction with separately operated remote valves, if desired.

In some cases, after careful evaluation, other valves may be considered for EBVs such as spring-loaded control valves that fail closed, back flow check valves (these are not normally considered reliable enough for EBVs by many engineers), and excess flow valves. Excess flow is the loss of material from the confined environment of a vessel or pipeline. Two approaches are available for the detection and valve action of excess flow valve systems: (1) External, where excess flow is detected outside the valve itself, and (2) internal, which is within the valve unit and has limited applications. Excess flow conditions are detected more readily because of loss of resistance to flow than because of loss of pressure. All excess flow detection systems are based on product physical properties as well as flow rate. A change of products or process conditions may require a change in the excess flow detection system. For example, a number of excess flow valves are rated for low pressure and are made of materials not suitable for hydrocarbons.

E. Using Piping, Gaskets, and Valves that Take Advantage of Modern Technology (Jackson, 1986)

1. *Piping*

All-welded pipes and flanges should be used in the inherently safer chemical plant. Since flanges are a potential source of leaks, as few flanges as possible should be used. This, of course, has to be realistic. If it is necessary to clean out pipes, flanges must be provided at appropriate places to make cleaning possible. Also, enough flanges must be provided to make maintenance and installation of new equipment reasonably easy. Screwed piping should be avoided for toxic and flammable materials. It is very difficult to make screwed fittings leakproof, especially with alloys such as stainless steel. Where screwed piping is necessary, use Schedule 80 pipe as a minimum. Pipe nipples should never be less than Schedule 80.

Pipe support design should be given special attention. It may be desirable to increase pipe diameter to provide more pipe strength and rigidity and make it possible to have greater distance between supports. Normally in chemical plants, it is not desirable to use piping less than $\frac{1}{2}$ in. in diameter and preferably not less than 1 in. in diameter, even if the flow requirements permit a smaller pipe, except for special cases. Pipe smaller than $\frac{1}{2}$ in. has insufficient strength and rigidity to be supported at reasonable intervals. Tubing should normally be used for anything smaller than $\frac{1}{2}$ in. Tubing is not as fragile as pipe in small sizes. It can be bent, which reduces the number of fittings required. If it is necessary to use smaller pipe or small tubing, special provisions should be made for its support and mechanical protection. Also, consideration should be given to using schedule 80 or schedule 160 pipe if small pipe is required to provide extra mechanical strength, even if the fluid pressure does not require it.

2. *Gaskets*

Gaskets are among the weakest elements of most chemical plants. Blown out or leaky gaskets have been implicated in many serious incidents. A leak at a flange can have a torch effect if ignited. A fire of this type was considered as a possible cause of the Flixborough disaster (Lees, 1980). Modern technology makes it possible to greatly reduce the incidence of gasket failure by using spiral wound gaskets. These are sold by several manufacturers, including Flexitallic, Parker Spirotallic, Garlock, and Lamons. When used properly, spiral wound gaskets are usually safer to use than most other types of gaskets. The preferred spiral wound gasket has an inner and outer metal ring which makes it virtually impossible for chunks of the gasket to blow out. The outer ring, called a gauge ring, makes it possible to accurately line up the gasket between the flange bolt holes. When the gasket is tightened, it is tightened down to the gauge ring which automatically provides the proper compression. The inner ring protects the spirals from spreading into the interior of the pipe and makes proper compression possible. Typical spiral wound gaskets are shown in Fig. 9.

Spiral wound gaskets cost about four to eight times more than compressed asbestos gaskets, but are easily worth it if they can prevent blowouts and leaks. Also, they generally last considerably longer than compressed asbestos-type gaskets. Spiral wound gaskets can be made in virtually any metal and filler

FIG. 9. Spiral wound gaskets.

combination. In many cases, the inner ring, which contacts the process fluid, can be stainless steel, and the outer ring can be steel. Typically the filler material is Teflon, Kevlar (an aramide fiber made by du Pont), or graphite, and the metal spirals are stainless steel. Graphite spiral wound gaskets are fairly expensive and fragile, but they are very resistant to chemicals and high temperatures.

When using 150 lb flanges with spiral wound gaskets, use only weld neck or lap-joint type flanges. Avoid the use of slip-on or threaded flanges because they are not strong enough and their use is discouraged by the American National Standards Institute (B16.5.). It is important that fire resistive gaskets be used with fire-safe emergency block valves.

Bolting with spiral wound gaskets is very important. Plain carbon steel bolts, such as A307 Grade B, should never be used with spiral wound gaskets. They are not strong enough. High-strength alloy bolts such as A193-B7, which contains Cr and Mo, should be used with A194 heavy hex nuts. To properly seal spiral wound gaskets, it is necessary to tighten the bolts to specified torque limits, which are generally higher than with conventional gaskets.

Spiral wound gaskets are not a solution to all gasket problems. They are usually not satisfactory for use with strong acids unless the metal exposed to the acid can tolerate it. Often Teflon envelope gaskets are better for such applications. Use the milled type or U-type Teflon envelope gaskets. Avoid the use of slit-type Teflon envelope gaskets. Spiral wound gaskets cannot be used on vessels with glass-lined flanges. Teflon envelope gaskets and some other types of gaskets are usually better on glass-lined surfaces. Teflon envelope gaskets can burn out in a fire and in some cases can be blown out. However, it is possible to specify metal flanges made of highly corrosion-resistant metal on glass-lined vessels. If this is done, spiral wound gaskets can be used on glass-lined equipment. A glass-lined reactor with metal flanges would usually be considered inherently safer than a glass-lined reactor with glass-lined flanges, assuming the metal used on the flanges can withstand the corrosion of the system.

3. *Valves*

It is desirable and inherently safer to use fire-safe valves whenever it is necessary to isolate flammable or combustible fluids in a pipeline, tank, or other type of equipment. Fire-safe valves should be considered for handling most fluids that are highly flammable, highly toxic, or highly corrosive and that cannot be allowed to escape into the environment. Fire-safe valves should also be used to isolate reactors, storage vessels, and pipelines. They can be used wherever EBVs are required.

A fire-safe ball valve is a valve that is free to move slightly, with pressure in the line, in order to contact a secondary metal seat if the line has been heated enough to melt the plastic seats (usually made of Teflon, but can be made of other plastics) used in the valve. The ball valve has fire-safe stem and body seals. Both ball valves and high-performance butterfly valves can be made fire-safe. Sleeve-type plugcocks are not normally considered completely fire-safe because their construction does not allow the plug to move if the plastic sleeve is melted. Lubricated plug cocks, globe valves, and gate valves are fire-safe if they are built with metal-to-metal seats and asbestos or graphite packing. However, these valves have very limited use in the chemical industry. It has been found that lubricated plug-cocks usually become inoperable if not cared for properly. The stem and body corrode and stick together if they are not lubricated and operated regularly. Lubricated plug-cocks should generally be avoided in the chemical industry.

With the increase in popularity of automated plants, quarter-turn valves are very popular and are used in most installations. The only common quarter-turn valves that are available as completely fire-safe valves are ball valves and high-performance butterfly valves. There are other special fire-safe valves, that are not common, which are used for special purposes. When fire-safe butterfly valves are required, they should pass the Exxon BP-3-14-4 (Modified) Fire Test. The basis for fire-safe valves in general is the API 607 standard Test for Firesafe Soft-Seated Valves.

4. *Dry Quick-Disconnect Couplings*

Spillage from regular and accidental disconnections of fluid couplings used at liquid-transfer points can be reduced by the use of dry quick-disconnect couplings. These devices combine a coupling connection that is easy to connect with a built-in valve that automatically closes unless the coupling is connected. This can minimize the hazards of handling toxic, flammable and corrosive liquids. They are especially useful for tank trucks and portable tanks where frequent connecting and disconnecting of the coupling is required. One type of high-quality dry quick-disconnect coupling is the Kamvalok coupling*.

5. *Spring-Loaded Check Valves*

When check valves are required, spring-loaded check valves provide more positive shut off than swing check valves. Swing check valves depend on gravity, and won't work if improperly installed. Occasionally, they won't work well even if they are properly installed. Swing check valves must be installed either horizontally or "vertically up." It is very easy to install them in the wrong position. Chances that a check valve will work are better if it is spring loaded than if it is a swing type. Positive shut off is available if Teflon seats can be used. If a small leak can be tolerated, metal-to-metal contact can be specified. It has been found that the potential for serious water hammer is much reduced if spring loaded check valves are used instead of swing checks. Swing checks slam shut at the last instant, possibly causing serious water hammer. Spring loaded check valves close smoothly and slowly, reducing the possibility of serious water hammer.

6. *Plastic Pipe and Plastic Lined Pipe*

Plastic lined pipe is excellent for many uses such as highly corrosive applications, where sticking is a problem, and where ease of cleaning is a factor. It is often the cheapest alternative. However, if a fire occurs there may be "instant holes" at each flange because the plastic will melt away, leaving a

* Manufactured by the Fluid Handling Group of the Dover Corp., Cincinnati, OH.

gap. Therefore, plastic lined pipe should not ordinarily be used for flammable materials that must be contained in case of a fire. An exception to this is a firesafe plastic lined pipe system made by the Resistoflex Corp., which provides a metal ring between each flange that will make plastic lined pipe firesafe. The pipe will probably have to be replaced after a fire, but the contents of the pipe will be contained during a fire.

In general, all types of solid plastic or glass-reinforced plastic pipe should not be used, if possible, with flammable liquids. Compared to metal, plastic piping melts and burns easier, is more fragile, is easily mechanically damaged, is harder to adequately support, and should be used with appropriate judgement.

F. Using Strong Vessels to Withstand Maximum Pressure of Process Upsets

It is sometimes possible to anticipate the worst reasonable process upset and design the process to withstand these conditions without relieving the contents through a pressure relief system. For example, it is possible to carry out a simulated styrene runaway polymerization reaction in an ARC apparatus (Section IV,A) to determine the highest pressure and temperature the system can achieve. Under certain conditions the actual composition used in the plant will contain some solvent and polymer. It may turn out, for example, that the maximum pressure reached by adiabatic polymerization is ~300 psig when the reaction starts at the normal operating temperature of 120°C. With this knowledge, it is possible to design polymerization equipment that will withstand this pressure, plus a reasonable safety factor, with the assurance that a runaway reaction will not cause a release of material or equipment rupture. The extra cost of the high pressure system may be justified not only by the extra safety. With high pressure systems, it may also be unnecessary to have elaborate collection equipment for the polymer and volatile material that may be released during runaways that cause venting from the pressure relief system from lower pressure reaction equipment.

It is still necessary to have a small relief system to allow for thermal expansion of a liquid-full system. This relief system is also necessary for handling hydraulic overfill and fire conditions, but the system is usually relatively simple.

Deflagration pressure containment is a technique for specifying the design pressure of a vessel and its appurtenances so that they are capable of withstanding the pressure that results from an internal deflagration. This may be inherently safer than relying on techniques to prevent deflagrations. These techniques are not to be used to contain a detonation. The ASME Boiler and

Presssure Code, Section VIII, provides guidelines for designing deflagration pressure containment. The design pressure is based either on preventing rupture of the vessel (i.e., on the ultimate strength of the vessel) or on preventing permanent deformation of the vessel (i.e., on the yield strength of the vessel) from internal positive overpressure. Because of the vacuum that can follow a deflagration, all vessels, in which deflagration pressure containment design is based on preventing deformation, shall also be designed to withstand a full vacuum (NFPA 69, 1986).

The possibility of equipment, which normally runs at or near atmospheric pressure, going into a vacuum condition should also be considered. Vacuum relief systems and vacuum breakers don't always work. On a hot summer day, a sudden rainstorm can cool a large tank or hopper very rapidly. This can cause rapid cooling and contraction of air inside the tank and condensation of vapors, if they are present. This can cause very rapid lowering of pressure inside the tank, which can implode the tank if insufficient provisions have been made for air to enter the tank. These conditions are common in northern climates where the rate at which a vacuum can be produced may be increased in cold weather. In many instances, vacuum devices that are supposed to work are frozen and inoperative and the tank implodes. It may be inherently safer to design tanks to handle a vacuum than to depend on vacuum relief devices alone.

G. Avoid Inherently Unsafe Equipment

Some equipment items are regarded as inherently unsafe for use in flammable or toxic service and should be avoided if possible. The items included are described in the following sections.

1. *Glass and Transparent Devices*

Glass devices such as sight glasses, bulls eyes, sightports, rotameters, and glass and transparent plastic piping and fittings are sensitive to heat and shock. Transparent plastic devices may be resistant to shock, but are not resistant to high temperatures (*Loss Prevention Principles*, 1986). If they fail in hazardous service, severe property damage and personnel injury can result. Two guidelines to consider are (1) if broken, would they release flammable material, and (2) if broken, would they expose personnel to toxic or corrosive materials? Some suggested ways to avoid glass and transparent devices are listed below.

Glass item	Nonglass equivalent
Glass rotameter	Magnetic flowmeter or dP cell
Bubbler	Pressure switch
Level gauge	Capacitance probe, conductivity cell, float gauge, magnetic liquid level detector, nuclear level detector
Glass or plastic pipe or tubing	Glass-lined steel pipe or plastic lined steel pipe
Sight port	Appropriate instrumentation or fiber optics with a video camera

If, after careful review, it is necessary to use a transparent device that could result in a hazard if broken, design safeguards should be used such as (1) shields or covers, (2) extra-strong devices (such as 300 psig equipment in 100 psig service), or (3) suitable excess-flow valves or remotely operated isolating valves.

2. *Flexible or Expansion Joints*

Eliminate flexible or expansion joints in piping wherever possible. Flexible joints and expansion joints are any corrugated or flexible transition devices designed to minimize or isolate the effects of thermal expansion, vibration, differential setting, misalignment, pumping surges, wear, load stresses, or other unusual conditions. *Almost without exception*, when a flexible joint is installed in a piping system, the flexible joint becomes the weak link in the system (*Safety Standards*, 1982). If, after considering all reasonable alternatives, it is necessary to use a flexible joint, make certain the temperature and pressure rating of the flexible joint are adequate for these conditions. The flexible joint system must be protected from overpressure, and provisions for isolating the flexible joint system should be provided. The need for flexible joints can sometimes be eliminated by properly designing piping so that solid piping will be able to handle misalignment and thermal changes by bending slightly. This is generally much preferred to using an expansion joint, which may be a weak point in the system.

It has been found at Dow, for example, that in many cases, electronic load cells can be used, with no flexible or expansion joints required, to accurately weigh large reactors or process tanks that have many pipes attached to them. This is done by "cantilevering" the pipes attached to the reactor or tank, and using sufficient runs of straight horizontal unsupported piping to take up movements and vibration without interfering significantly with the operation of the load cells. Flexible joints should not be used as a correction for piping errors.

H. Using Pumps Suitable for Hazardous Service

A wide variety of excellent pumps is available in the chemical industry. It is sometimes a problem to choose the best from the large number available. This discussion will be limited to centrifugal pumps. Assuming that one has sized the pump, decided on a centrifugal pump, and has chosen a suitable list of vendors, the remaining main choices to make are (1) the metallurgy to be used, (2) whether to use seal-less pumps or conventional centrifugal pumps, and (3) what type of seal, if using conventional pumps (Cromie, 1986).

1. *Metallurgy*

Don't use cast iron for flammable or hazardous service unless there is no other choice. In very few cases, only cast iron is available. This is true for large double-suction water pumps used by municipalities where types other than cast iron are not readily available. The minimum metallurgy for centrifugal pumps for hazardous or flammable materials is cast ductile iron, type ASTM A 395, having an ultimate tensile strength of $\sim$60,000 psi. This metal is not brittle at ordinary temperatures. Often, special alloys are required because of corrosion. In no case should brittle materials be used for a pump if other choices are available.

2. *Seal-less Pumps (Reynolds, 1989; Cromie, 1986)*

Seal-less pumps are becoming very popular and are widely used in the chemical industry. Mechanical seal problems account for most of the pump repairs in a chemical plant, with bearing failures a distant second. The absence of an external motor and a seal is appealing to those experienced with mechanical seal pumps. However, do not assume that just because there is no seal, seal-less pumps are always safer than pumps with seals, even with the advanced technology now available in seal-less pumps. Use seal-less pumps with considerable caution when handling hazardous or flammable liquids.

Seal-less pumps are manufactured in two basic types: canned motor and magnetic drive. Magnetic drive pumps have thicker "cans" which hold in the process fluid, and the clearances between the internal rotor and "can" are greater compared to canned motor pumps. This permits more bearing wear before the rotor starts wearing through the "can." Because most magnetic drive pumps use permanent magnets for both the internal and external rotors, there is less heat to the pumped fluid than with canned motor pumps. With magnetic drive pumps, containment of leakage through the "can" to the outer shell can be a problem. Even though the shell may be thick and capable of holding high pressures, there is often an elastomeric seal on the outer magnetic rotor with little pressure capability.

Canned motor pumps typically have a clearance between the rotor and the containment shell or "can," which separates the fluid from the stator, of only 0.008 to 0.010 in. The "can," which is typically 0.010–0.015 in. thick and made of Hastelloy, has to be thin to allow magnetic flux to flow to the rotor. The rotor can wear through the "can" very rapidly if the rotor bearing wears enough to cause the rotor to move slightly and begin to rub against the "can." The "can" may rupture causing uncontrollable loss of fluid being pumped. Some canned motor pumps have fully pressure-rated outer shells which enclose the canned motor; others don't.

Both canned motor and magnetic drive pumps rely on the process fluid fo lubricate the bearings. If the wear rate of the bearings in the fluid being handled is not known, the bearings can wear unexpectedly, causing rupture of the "can." Running a seal-less pump dry can cause complete failure. If there is cavitation in the pump, hydraulic balancing in the pump no longer functions and excessive wear can occur leading to failure of the "can."

A number of liquids require special attention when applying canned motor and magnetic drive pumps. For example, a low-boiling liquid may flash and vapor-bind the pump. Some liquids with high specific gravities (above about 1.3–1.7 cP) can cause the rotor to become magnetically uncoupled from the stator, which can cause considerable heat to be generated. Solids in the liquid can also be bad because of close clearances in the pump. Low viscosity (in the range of 1 to 5 cP) fluids are normally poor lubricators and one should be concerned about selecting the right bearings. For viscosities below 1 cP, it is even more important to choose the right bearing material.

A monitor to detect bearing wear is available on some seal-less pumps but they generally don't offer complete monitoring of all internal bearings for axial and radial wear. Seal-less pumps typically run so smoothly and quietly that it is usually not possible to determine by vibration or noise if a bearing is badly worn.

A mistreated seal-less pump can rupture with potentially serious results. The "can" can fail if valves on both sides of the pump are closed and the fluid in the pump expands either due to heating up from a cold condition, or if the pump is started up. If the pump is run dry for even a short time, the bearings can be ruined. The pump can heat up and be damaged if there is insufficient flow to take away heat from the windings. Seal-less pumps, especially canned motor pumps, produce a significant amount of heat since nearly all the electrical energy lost in the system is absorbed by the fluid being pumped. *If this heat cannot be properly dissipated, the fluid will heat up with possibly severe consequences.* Considerable care must be used when installing and maintaining a seal-less pump to be sure that misoperations cannot occur.

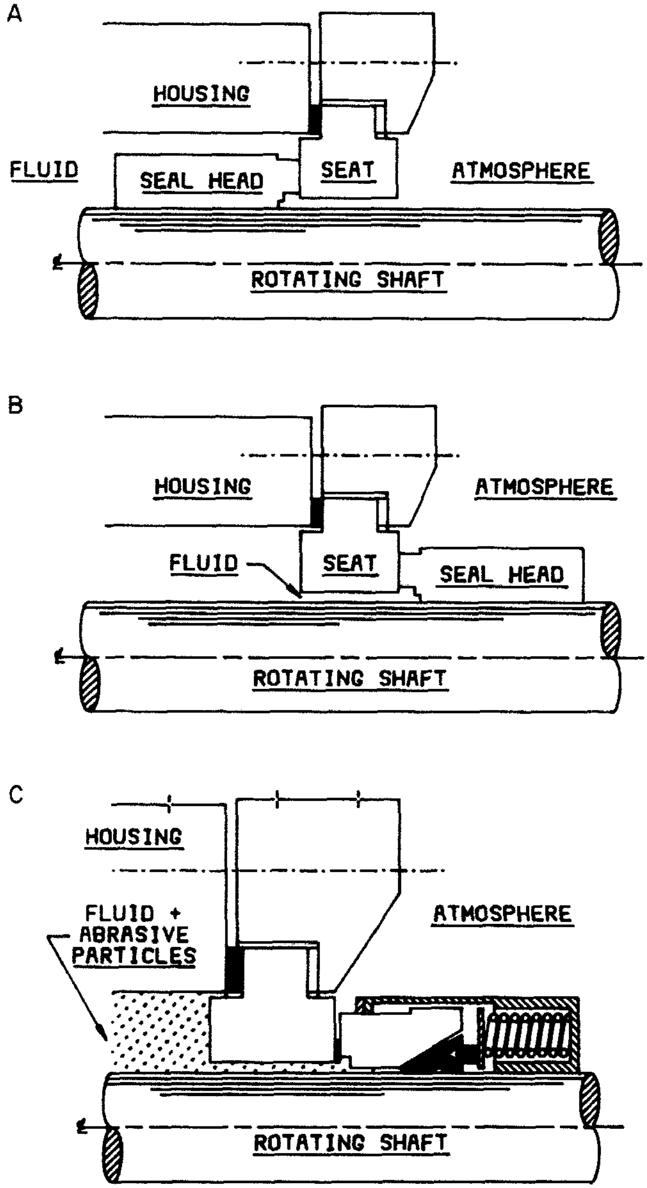

FIG. 10. Arrangements of mechanical seals. A, Single seal. It is the most common and handles most applications. B, Inside mounted seal. It operates better because it has positive lubrication; the entire seal is surrounded by fluid. C, Outside mounted seal. It is more easily accessible for maintenance and less of the seal is exposed to corrosive fluid.

Properly installed and maintained seal-less pumps, especially magnetic drive pumps, offer an economical and safe way to minimize leaks of hazardous liquids.

3. *Types of Seals*

a. *Single Mechanical Seals.* Single mechanical seals (Fig. 10) are the most common type of mechanical seals. They provide no opportunity for a second line of defense in case the seal fails and are not recommended for hazardous or flammable service. Double mechanical seals or tandem mechanical seals should be considered for hazardous and flammable service. The failure mode of these seals is such that catastrophic releases are probably unlikely. Double and tandem mechanical seals provide a means for failure to be positively detected before it becomes serious, and the fluid being handled can be nearly totally contained. Using stuffing boxes eliminate is normally not recommended for hazardous or flammable fluids, but is often used on water or high-viscosity fluids. Packing may be necessary where the fluid is very hot or corrosive, and mechanical seals will not perform well.

b. *Double-Seal Pumps.* With double seal pumps, as shown in Figs. 11 and 12, oil used to pressurize the space between the seals is kept at a slightly higher pressure than the process fluid being pumped (usually about 15 psi higher). There is a tiny amount of oil leakage into the process fluid under normal conditions. Oil lubricates both seals. The springs on the seals also run in oil. Running the pump without process fluid will not damage the pump as long as there is oil in the reservoir and the reservoir is under pressure. If there is seal failure, pressure on the reservoir holding the oil will force oil into the process fluid or out of the seal on the low pressure side, and the oil reservoir will show an abnormally low level. The system can be programmed to give an alarm and shut down the process and valves leading to the pump, if desired. The opportunity for major loss of the fluid being pumped is small. Whatever leakage occurs would be oil into the process fluid.

c. *Tandem-Seal Pumps.* If no contamination of the fluid being pumped can be tolerated, a tandem seal can be used. A tandem seal is the same as two single mechanical seals in series (see Fig. 12). The seal on the process fluid side is lubricated by the fluid being pumped. There is a very small amount of process fluid leakage into the reservoir. The reservoir tank is maintained at atmospheric pressure or a little higher. A failure of the mechanical seal on the process fluid side will cause the reservoir to fill up abnormally fast. The system can be programmed to give an alarm and automatically shut down the pump and valves leading to the pump, if desired, in case of an abnormal change in the

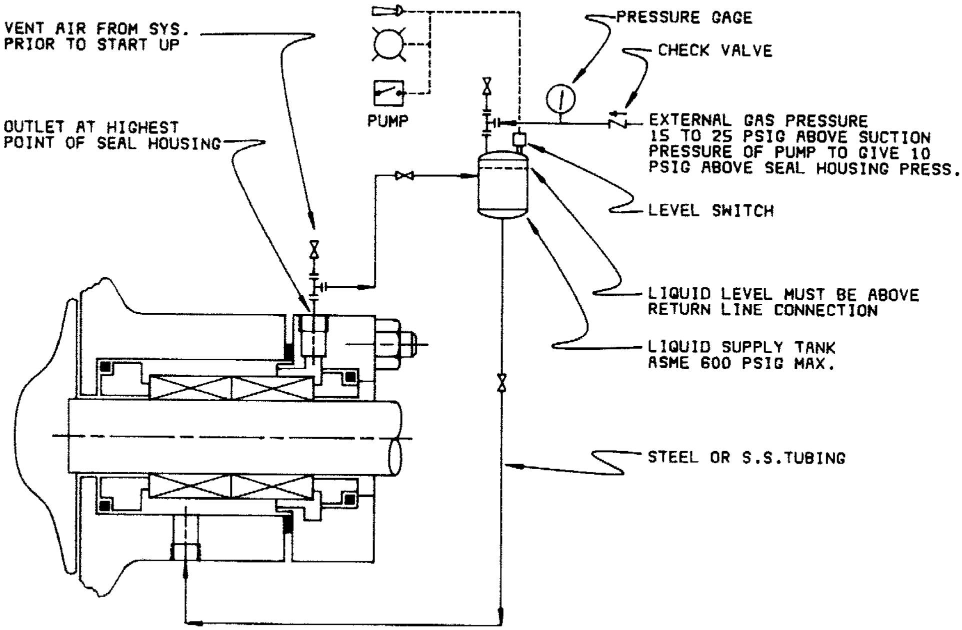

FIG. 11. Double mechanical seal accessories: Pressurized thermal convection system with liquid level switch and 1-gal ASME vessel.

reservoir level. The pump can run on the secondary seal (the normally low-pressure seal) until the system can be shut down.

A disadvantage of tandem seals is that they cannot safely be operated without process fluid because the seal on the process fluid side may run dry. Also, the springs and other internal seal mechanisms on the fluid side run in the process fluid, which may not be good in highly corrosive fluid. The big advantage of tandem seals is that they allow process fluid to be pumped without contamination from lubricating oil, and the chances for major loss of process fluid are small.

4. *Pumps in General*

There are many parts in pumps and pump seals. It is important to check all the details of internal gaskets and the internal construction of a pump to be certain these parts are compatible with the process fluids being pumped.

5. *DeadHeaded Pumps*

A deadheaded pump is a pump that is running, while full of liquid, with the inlet and outlet valves closed. Pumps should be protected against the

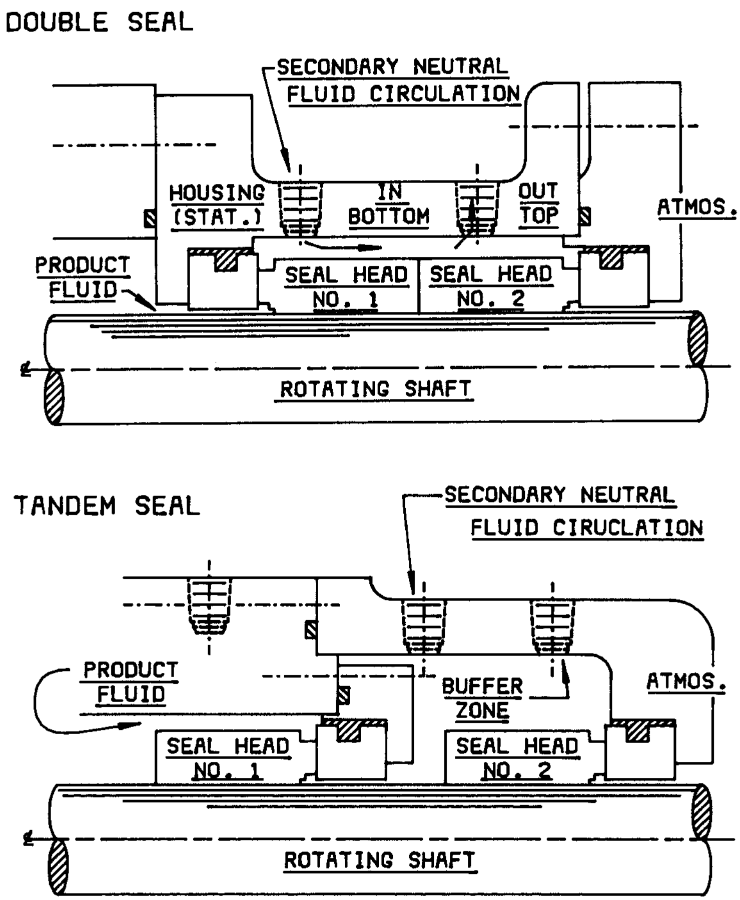

FIG. 12. Arrangements of mechanical seals. Double seal; higher pressure fluid between seals creates an "artificial environment" for seal operation. Tandem seal; two single seals with a buffer zone in between them. One backs up the other.

possibility of running deadheaded by installing a temperature device on the pump casing that can detect overheating, give an alarm, and shut the pump off. Deadheading of a centrifugal pump can result in extremely high pressures and explosions because the energy put into the liquid in the pump by the action of the impeller can cause rapid heating of the pump contents. This can result in hydraulic overpressure, high pressures caused by boiling liquid in the pump, or high pressures caused by possible chemical reactions in the pump. Water in deadheaded pumps has been the cause of several pump explosions at Dow. Other chemicals have also caused the same experience, sometimes made worse by reactions occurring within the deadheaded pump.

It has been found that in many cases, measuring amperage on the pump motor is not a very satisfactory way to detect deadheading because of the nature of pump curves. Also, the power factor of a motor operating at low capacity is generally low, which tends to obscure the actual power required if power use is deduced from amperage. For this reason, temperature devices on the pump are usually preferred as a reliable method for detecting deadheaded pumps. A positive way to measure flow from the pump may be a satisfactory method to detect and prevent dead-heading.

VI. Conclusion

This chapter addresses many of the factors to be dealt with by practicing process engineers who design chemical plants. There are many techniques that can be used to assure that a plant will be inherently safer than was ever possible before. Some of the latest knowledge available in the area of safe plant design is described. The people involved include those in management, process design, research, and manufacturing. Safety and loss prevention specialists and many other types of specialists are also of vital importance. A number of references are included for those who wish to pursue more fully any of the topics discussed.

References

Bartknecht, W., "Explosion Course Prevention, Protection," pp. 39, 55. Springer-Verlag, Berlin and New York, 1981.

Brasie, W. C., "Loss Prevention," Vol. 10, p. 135. Inst. Chem. Eng., New York, 1976.

Brasie, W. C., personal communication (1986).

Brooks, K., Rhein, R., and Bluestone, M., *Chem. Week* Sept. 24, p. 38 (1986).

"CEFIC Views on the Quantitative Assessment of Risks From Installations in the Chemical Industry." Eur. Counc. Chem. Manuf. Fed., Brussels, 1986.

"Corporate Safety and Loss Prevention." Dow Chem. Co., Midland, Michigan, 1981.

Cox, F. A., and Shiah, J. T., Gen. Pat. 1,964,213 to Goodyear Tire and Rubber Co., 1970 [C.A. Vol. 73, No. 13, 77855 (1970)].

Cromie, J., personal communication (1986).

DeHaven, E. S., *Plant Oper. Prog.* **3**, No. 1, p. 21 (1983).

Englund, S. M., *J. Chem. Educ.* No. 9, p. 59 (1982).

"EPA Asks Rules to Prevent Leaks in Underground Tanks," *New York Times* Apr. 3 (1987).

Fauske, H. K., and Leung, J., *Chem. Eng. Prog.* Aug., p. 39 (1985).

Fisher, H., *Chem. Eng. Prog.* Aug., p. 33 (1985).

Frey, K. R., personal communication (1987).

Geyer, G., personal communication (1986).

Grinwis, D., Larsen, P., and Shrock, L., personal communication (1986).

Grolmes, M. A., and Lung, J. C. (Fauske and Assoc.), *Chem. Eng. Prog.* Aug., p. 47 (1985).

Howard, W. B., and Karabinis, A. H., "Tests of Explosion Venting Buildings." Monsanto Co., St. Louis, MO, 1981.

Huff, J. E., *Loss Prev.* **7**, 43 (1973).

Huff, J. E., *Repr. Symp. Loss Prev. Saf. Promotion Process Ind., Heidelberg,* Vol. IV, p. 223. *DECHEMA,* Frankfurt am Main.

Huff, J. E., *Plant Oper. Prog.* **1**, No. 4, p. 211 (1982).

Huff, J. E., *Plant Oper. Prog.* **3**, No. 1, p. 50 (1984).

Huff, J. E., *Inst. Chem. Eng. Symp. Ser.* No. 85, p. 109 (1984b).

Huff, J. E., *Int. Symp. Preventing Major Chem. Accid., Washington, D.C.,* pp. 4.43–4.68, sponsored by Cent. Chem. Process Saf. Am. Inst. Chem. Eng., U.S. Environ. Agency and World Bank (1987).

Jackson, B. L., personal communication (1986).

Klein, H. H., *Plant Oper. Prog.* **1**, No. 4, pp. 1–10 (1986).

Kletz, T., "Cheaper, Safer Plants or Wealth and Safety at Work," p. 49. Inst. Chem. Eng., Rugby, England, 1985a.

Kletz, T. *Design Oppor.* Sept., p. 172 (1985b).

Lees, F., "Loss Prevention in the Process Industries," 2 Vols. Butterworth, London, 1980.

Levenspiel, O., "Chemical Reactor Omnibook," pp. 3.2, 5.2. Oregon State Univ. Bookstores, Corvallis, 1979.

Liening, G., personal communication (1986a).

Liening, G., *Chem. Process.* Sept. (1986b).

"Loss Prevention Principles." Dow Chem. Co., Midland, Michigan, 1986.

Mutsakis, M. (Koch Eng. Co.), Streiff, F. A., and Schneider, G. (Sulzer Bros., Ltd., Winterhur, Switz.) *Chem. Eng. Prog.* July, pp. 42–48 (1986).

NFPA (National Fire Protection Association) 69, "Explosion Prevention Systems." NFPA, Batterymarch Park, Quincy, Massachusetts, 1986.

NFPA (National Fire Protection Association) 68, "Explosion Protection Systems." NFPA, Batterymarch Park, Quincy, Massachusetts, 1988.

Pase, G. K., *Chem. Eng. Prog.* Sept., p. 53 (1986).

Perry's Chemical Engineer's Handbook," 6th Ed., pp. 23–48. McGraw Hill, New York, 1984.

Reynolds, J. A., *Chem. Process.* 71–75 (Nov. 1989).

"Safety Standards." Dow Chem. Co., Midland, Michigan, 1982.

Sjoren, S., and Grueiro, W. (Alfa-Laval, Inc.), *Hydrocarbon Process.* Sept., p. 133 (1983).

Townsend, D. I., and Tou, J. C., *Thermochim. Acta* **37**, 30 (1980).

U.S. Pat. 3,563,964 to Dow Chem. Co., 1971 [C.A. **74**, No. 127,159 (1971)].

U.S. Pat. 4,024,329, Lauer, R., Rankle, R., and Dehnke, T., to Dow Chem. Co., 1977 [C.A. **87**, No. 23985 (1977)].

Wensley, J. H., (Oct. 13, 1986). "Improved Alarm Management Through Use of Fault Tolerant Digital Systems," *Instrum. Soc. Am., Int. Conf. Exhibit, Houston, Tex.*