CHAPTER

ONE

INTRODUCTION—WHAT ARE INHERENTLY SAFER AND USER-FRIENDLY PLANTS?

We can pull and haul and push and drive,
We can print and plough and weave and heat and light,
We can run and race and swim and fly and drive,
We can see and hear and count and read and write . . .

But remember please, the law by which we live,
We are not built to comprehend a lie,
We can neither love nor pity not forgive —
If you make a slip in handling us, you die.

—Rudyard Kipling, *The Secret of the Machine*

1-1 INTRODUCTION

The aim of this book is to show that the last line in the poem above need not always be true and that we can often design plants that can tolerate human error and equipment failure without serious effects on safety, output, and efficiency.

The chemical industry expanded rapidly during the 1960s, and two unforeseen results were a series of major fires and explosions, culminating in those at Flixborough, United Kingdom, and Seveso, Italy, and a consequent demand for higher standards of safety. In response, the industry installed more and more safety equipment, and costs rose. People began to ask, Where will it end? How much safety equipment should we add to our plants? One answer was quantitative risk assessment: setting a target level of risk and not going beyond it (see Chapter 12). This approach has become widely

accepted; it is an approach I use and advocate.[1] Nevertheless, it should be our second best choice. Before we estimate the probability and consequences of a hazard and compare them with a target, we should ask if the hazard can be eliminated.

In all industries, equipment failures and errors by operators and maintenance workers are recognized as major causes of accidents, and much thought has been given to ways of reducing them or minimizing their consequences.[2] However, it is difficult for operators and maintenance workers to keep up an error-free performance all day, every day. We may keep up a tip-top performance for an hour or so while playing a game or a piece of music, but we cannot keep it up continuously. Designers have a second chance, opportunities to go over their designs again, but not operators and maintenance workers. Plants should therefore be designed, whenever possible, so that they are user-friendly, to borrow a computer term, and can tolerate departures from ideal performance by operators or maintenance workers without serious effects on safety, output, or efficiency.

Similarly, although much attention has been paid to the improvement of equipment reliability, 100% reliability is unattainable, and compromises have to be made between reliability and cost. Plants should therefore be designed, whenever possible, so that equipment failure does not seriously affect safety, output, and efficiency.

These arguments apply to all industry but particularly to the chemical and nuclear industries, where hazardous materials are handled and the consequences of failure—by people or equipment—are serious. The levels of reliability required are high and may be beyond the capabilities of people or materials. For example, a joint leaked after a shutdown in which 2000 joints were broken and remade. Only one was remade wrongly, but it was the only one that anyone heard about. Afterwards the fiber gaskets in most of the 5000 joints in the unit—all those exposed to liquid—were replaced by friendlier spiral-wound gaskets.

A *hazard* is a situation that can lead to harm. A *risk* is the probability that the harm will occur. Traditional plant designs try to reduce the risk by adding protective equipment and following safe methods of working. Inherently safer and friendlier plants remove or reduce the hazards. Following traditional methods, we become more and more efficient at things we should not be doing, except as a last resort.

The ways by which friendliness in plant design can be achieved are summarized below and discussed in detail in later chapters. The characteristics are not sharply defined and merge into each other.

1. *Intensification or minimization.* Friendly plants contain low inventories of hazardous materials—so little that it does not matter if the entire inventory leaks out. What you don't have, can't leak. This may seem obvious, but until the explosion at Flixborough in 1974 little thought was given to ways of reducing the amount of hazardous material in a plant. Engineers simply designed a plant and accepted whatever inventory the design required confident that they could keep it under control. At Bhopal, India, in 1984, the material that leaked, killing over 2000 people, was an intermediate that it was convenient, but not essential, to store. Inventories can often be reduced in almost all unit operations as well as storage (see Chapter 3).
2. *Substitution.* If intensification is not possible, then an alternative is substitution: using a safer material in place of a hazardous one. Thus, it may be possible to replace

flammable refrigerants and heat-transfer media by nonflammable ones, hazardous products by safer ones, and processes that use hazardous raw materials or intermediates by processes that do not (see Chapter 4).

Intensification, when it is practicable, is better than substitution because it brings about greater reductions in cost. If less material is present, we need smaller pipes and vessels as well as smaller structures and foundations. Much of the pressure for intensification has come from those who are primarily concerned with cost reduction. In fact, friendliness in plant design is not just an isolated but desirable concept but rather part of a total package of measures, including cost reduction, lower energy usage, and simplification that the chemical industry needs to adopt in the years ahead (see Section 2-4).

3. *Attenuation or moderation.* Another alternative to intensification is attenuation by using a hazardous material under the least hazardous conditions. Thus, liquefied chlorine and ammonia can be stored as refrigerated liquids at atmospheric pressure instead of storing them under pressure at ambient temperature. Dyestuffs that form explosive dusts can be handled as slurries (see Chapter 5).

Attenuation is sometimes the reverse of intensification, for if we make reaction conditions less extreme we may need a longer residence time and a larger inventory. In designing friendly plants we may have to compromise between different possibilities (see the quotation by David Pye at the front of the book).

4. *Limitation of effects by changing designs or reaction conditions rather than by adding protective equipment that may fail or be neglected.* If friendly equipment does leak, it does so at a low rate, which is easy to stop or control. Spiral-wound gaskets, as already mentioned, are friendlier than fiber gaskets because, if the bolts work loose or are not tightened correctly, the leak rate is lower. A tubular reactor is friendlier than a pot reactor because the leak rate is limited by the cross section of the pipe and can be stopped by closing a valve in the pipe. Vapor phase reactors are friendlier than liquid phase reactors, for the mass flow rate through a hole of a given size is less.

By changing reaction conditions (e.g., the temperature or the order of operations) it is often possible to prevent runaways or make them less likely. By carrying out different stages of a batch process in different vessels it may be possible to tailor the equipment more closely to the needs of each step. By using steam or oil as a heating medium, and limiting its temperature, it may be possible to prevent overheating (see Chapter 6).

Intensification, substitution, attenuation, and limitation of effects produce **inherently safer design** because they *avoid* hazards instead of controlling them by *adding* protective equipment. The term *inherently safer* implies that the process is safe because of its very nature and not because equipment has been added to make it safer. Note that we talk of inherently safer plants, not inherently safe ones, for we cannot remove all hazards. Note also that some writers use the term inherently safer design in a wider sense to include all the methods of making plants friendlier that I discuss in this book. Some go even further and include in inherently safer designs methods of locating or confining equipment so that the effects of fires and explosions are minimized. I regard such protective measures as add-ons. The inherently safer solutions are to use nonflammable materials or so little flammable material that a

leak would hardly matter or, if that is impossible, to use the hazardous material in the least hazardous form. If we make the definition of any concept too broad, designers will say they are using it when they are hardly doing so.

To use an analogy, How deep does the water have to be before we can say we are bathing? Walking in water up to our ankles may be better than nothing but hardly allows us to claim we are bathing.

5. *Simplicity.* Simpler plants are friendlier than complex plants because they provide fewer opportunities for error and less equipment that can fail. They are usually also cheaper.

   The main reason for complexity in plant design is the need to add equipment to control hazards. Inherently safer plants are therefore also simpler plants. Other reasons for complexity are as follows:

   a) Design procedures that result in a failure to identify hazards or operating problems until late in design. By this time it is impossible to avoid the hazards, and all we can do is add complex equipment to control them (see Chapter 7).
   b) A desire for flexibility. Multistream plants with numerous crossovers and valves, so that any item can be used on any stream, have numerous leakage points, and errors in valve settings are likely (see Section 8-2).
   c) Lavish provision of installed spares with the accompanying isolation and changeover valves (see Section 8-1-4).
   d) Persistence in rules or practices that are no longer necessary (see Section 8-1).
   e) Our intolerance of risk. Do we go too far? (See Chapter 12.)

   Equipment can, of course, combine more than one of the features of friendly plants, and they are interlinked. Thus, intensification and substitution often result in a simpler plant because there is less need for added safety equipment. At other times we may have to choose between, say, using a hazardous raw material in a reaction that cannot run away or using a less hazardous raw material in a reaction that may run away (see Section 4-2-3).

6. *Avoiding knock-on effects.* Friendly plants are designed so that those incidents that do occur do not produce knock-on or domino effects. For example, friendly plants are provided with firebreaks between sections, like those in a forest, to restrict the spread of fire, or, if flammable materials are handled, the plants are built out-of-doors so that leaks can be dispersed by natural ventilation (see Section 9-1).
7. *Making incorrect assembly impossible.* Friendly plants are designed so that incorrect assembly is difficult or impossible. For example, compressor valves should be designed so that inlet and exit valves cannot be interchanged (see Section 9-2).
8. *Making status clear.* With friendly equipment it is possible to see at a glance if it has been assembled or installed incorrectly or whether it is in the open or shut position. For example, check (nonreturn) valves should be marked so that installation the wrong way round is obvious (it should not be necessary to look for a faint arrow hardly visible beneath the dirt), and gate valves with rising spindles are friendlier than valves with nonrising spindles because it is easy to see whether they are open or shut. Ball valves are friendly if the handles cannot be replaced in the wrong position (see Section 9-3).
9. *Tolerance of misuse.* Friendly equipment will tolerate poor installation or operation