Inherent Safety and Reliability in Plant Design

Dennis C. Hendershot
EMail: Dennis_C_Hendershot@rohmhaas.com

Robert L. Post
EMail: Robert_L_Post@rohmhaas.com

Rohm and Haas Company
Engineering Division
PO Box 584
Bristol, PA 19007

Prepared for Presentation at the
Mary Kay O'Connor Process Safety Center 2000 Annual Symposium:
Beyond Regulatory Compliance, Making Safety Second Nature

Track II: Inherently Safer Design Session

Reed Arena, Texas A&M University
College Station, TX
October 24-25, 2000

ROHM AND HAAS

Responsible Care®
A Public Commitment

Inherent Safety and Reliability in Plant Design

Dennis C. Hendershot and Robert L. Post
Rohm and Haas Company
Engineering Division
Bristol, PA 19007

Abstract

Inherent safety principles apply at all stages in a process life cycle. While the biggest gains are achieved early, through the selection of inherently safer process technology, there are many opportunities for enhancing the inherent safety and reliability of a plant at the detailed design stage. Specific examples will be discussed, including examples of pump and compressor selection, vessel design, human factors in equipment design, and design modifications to reduce the frequency of plant startup and shutdown. We will also discuss the connection between the inherent safety of a plant and plant reliability.

Introduction

Inherently safer process design – the elimination or substantial reduction of hazards from a manufacturing process, rather than the application of engineering and procedural controls to manage hazards – has the greatest benefits early in process development. However, there are opportunities for application of inherently safer design principles throughout the process life cycle. The term “inherently safer design” is relatively recent, but many of its principles have been a part of good engineering design for many years. In this paper we will describe an early example of the application of inherently safer design principles, and then focus on opportunities for enhancing the inherent safety of chemical plants during detailed design. In particular, we will emphasize the relationship between plant reliability and inherent safety. A reliable plant is inherently safer, and design features, which enhance reliability, will generally also enhance safety.

A Historical Example of Inherently Safer Material Handling

On Tuesday April 3, 1866, a massive explosion destroyed the steamship *European* while it was being unloaded at the port of Aspinwall, on the Caribbean coast of the Isthmus of Panama. The *European* was carrying seventy crates of nitroglycerine, which were being shipped to California for use in mines and construction. More than fifty people were killed, a nearby ship was severely damaged, and all of the buildings near the waterfront were badly damaged.

About two weeks later, on April 15, 1866, an explosion destroyed a freight office of the Wells Fargo Company in downtown San Francisco. Fifteen people were killed, and the freight office, the

Union Club, an assay office, the water works office, and other buildings were destroyed. Two damaged crates of nitroglycerine had been refused delivery because of their condition and had been sent to the freight office to determine what to do with them. The explosion resolved that question.

A couple of days later, on April 17, 1866, another nitroglycerine explosion killed six laborers in the Sierra Nevada, where the Central Pacific Railroad was working its way through the mountains on its way to becoming the western section of the first transcontinental railroad in the United States. The railroad was having an extremely difficult time in blasting its way through the hard granite of the Sierra Nevada, and was experimenting with nitroglycerine, which was estimated to be eight times more powerful than the black powder previously used.

Following this series of disasters, California authorities quickly passed laws forbidding the transportation of nitroglycerine through San Francisco and Sacramento, making it virtually impossible to use the material for construction of the Central Pacific Railroad. The railroad desperately needed the explosive to maintain its construction schedule in the mountains. Fortunately, a British chemist, James Howden, approached the Central Pacific and offered to manufacture nitroglycerine at the construction site. This is an early example of an inherently safer design principle – *minimize* the transport of a hazardous material by in situ manufacture at the point of use. While nitroglycerine still represented a significant hazard to the workers who manufactured, transported, and used it at the construction site, the hazard to the general public from nitroglycerine transport was eliminated. At one time, Howden was manufacturing 100 pounds of nitroglycerine per day at the railroad construction sites in the Sierra Nevada Mountains. The Central Pacific Railroad's experience with the use of nitroglycerine was quite good, with no further fatalities directly attributed to use of the explosive during the Sierra Nevada construction.[1]

Clearly, by today's standards, little about 19th Century railroad construction would qualify as safe, but the in situ manufacture of nitroglycerine by the Central Pacific Railroad did represent an advance in inherent safety for its time. A further, and probably more important, advance occurred in 1867, when Alfred Nobel invented dynamite by absorbing nitroglycerine on a carrier, greatly enhancing its stability. This is an application of another principle of inherently safer design – *moderate*, by using a hazardous material in a less hazardous form.

Review of Inherently Safer Design Principles

A chemical process is described as **inherently safer** if it reduces or eliminates one or more process hazards and this reduction or elimination is accomplished through changes that are permanent and inseparable. Approaches to the design of inherently safer processes and plants have been grouped into four major strategies[2]:

Minimize	Use small quantities of hazardous substances
Substitute	Replace a material with a less hazardous substance
Moderate	Use less hazardous conditions, a less hazardous form of a material, or facilities, which minimize the impact of a release of hazardous material or energy

Simplify Design facilities which eliminate unnecessary complexity and make operating errors less likely, and which are forgiving of errors which are made

The examples discussed in this paper would generally fall into the "simplify" strategy. Design improvements intended to improve plant reliability will simplify plant operations by reducing the frequency of startup and shutdown, whether planned for anticipated maintenance or repair, or unplanned due to the sudden failure of a piece of equipment which causes a plant shutdown.

Safety and Reliability

Improved reliability decreases plant and process risks. Equipment failure increases risk in several ways:

- Directly, by the immediate consequences of the equipment failure, such as leaks and spills
- Indirectly, by disabling protective systems which may not be available when needed (for example, alarms and interlocks, sprinkler systems, relief valves)
- Indirectly, by increasing the amount of time that a plant or process spends in "higher risk" phases of operation
    - ◊ Planned startup and shutdown
    - ◊ Unplanned and unanticipated shutdown
    - ◊ "Hardship" operation with equipment out of service

The relationship between reliability and safety is clear for the first two items above. Design and specification of equipment which is less likely to leak, which will exhibit a gradual failure which can be detected and repaired before catastrophic failure, which can be easily inspected and maintained to prevent failure, clearly results in a safer plant design. Similarly, design of inherently more reliable protective equipment, design of plant systems so that protective equipment can be regularly tested to detect hidden failures, and design of systems in which normal process operations provide verification of the correct operation of some components of protective systems clearly improves plant safety. The third item postulates that a plant, which spends a greater portion of the time in routine operation at steady state, producing good quality product and profits for the owner, is also a safer plant.

Most process engineers have an intuitive feeling that a continuous plant is more likely to have a safety or environmental incident during startup or shutdown than during routine, steady state continuous operation. We have confirmed that intuitive understanding of continuous plant risk in several chemical process quantitative risk analysis (CPQRA) studies for a variety of different kinds of continuous plants.

Plant A consists of a continuous stirred tank reactor and its associated feed and downstream processing vessels. The reaction is highly exothermic, and can generate a large amount of gas and pressure if not properly controlled. A CPQRA of the system identified two primary runaway reaction scenarios, which were the dominant contributors to total risk. Figure 1 shows the portion of time that the plant spends in startup and shutdown mode, about 2 % of the time each. Figure 1

also shows the contribution to risk for the two dominant contributors for startup, continuous operation, and shutdown. Clearly, the contribution to total risk of the startup and shutdown phases of operation is disproportionately high.

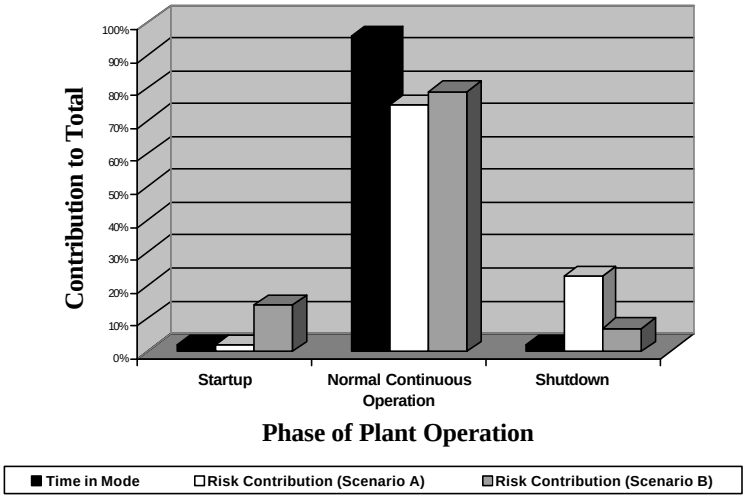

Figure 1: Risk Contribution for Startup, Normal Operations, and Shutdown for Plant A

Plant B consists of a continuous gas phase reactor and its associated feed and downstream treatment systems. Again the reaction is highly exothermic, and the gas being processed is highly flammable. Figure 2 shows the portion of time that Plant B spends in startup, continuous operation, and shutdown, along with the contribution to total risk of the two dominant risk scenarios for this plant. Again, the startup and shutdown phases of operation contribute disproportionately to risk.

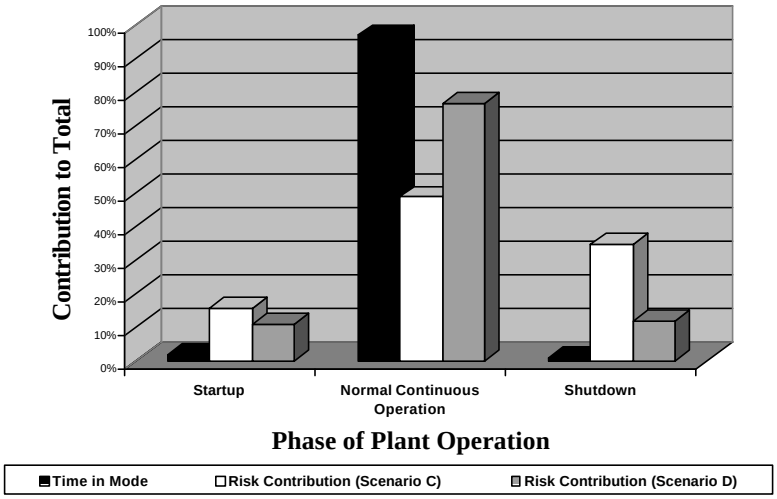

Figure 2: Risk Contribution for Startup, Normal Operations, and Shutdown for Plant B

Clearly, it is desirable that Plant A and Plant B be kept operating in the normal continuous operating mode as much as possible. Starting up and shutting down both of these plants is a higher risk operation than normal operation. Therefore, if the plant designers can improve the reliability

of the plant equipment, it will be shut down less frequently, will have to be started up less frequently, and will be safer. Nearly everybody should be happier with this situation. Obviously, the business managers will find this desirable; the plant will be running and producing product instead of being shut down for repairs. Operators realize that there is a lot more hard work involved in starting a plant and shutting it down, compared to routine continuous operations. And the mechanics other maintenance staff will be able to spend their time doing planned and scheduled maintenance tasks rather than rushing about trying to react to the latest failure so the plant can get back on line. Perhaps the only unhappy people will be the outside contractors that the plant will no longer have to hire to do emergency maintenance, or the mechanic with a boat payment due who is counting on a lot of overtime pay!

Specific Examples of More Reliable Design

Pumps

When specifying a pump, the design should be robust enough to allow the pump to deliver the required flow rate over a wide range of operating conditions. In particular, the pump should be insensitive to variation in the downstream pressure, perhaps caused by fouling or plugging of pipes, valves stuck in a partially open position, failure of control valves, or operator error in setting manual valves. Figure 3 shows a pump, which is very sensitive to an increase in downstream pressure. A better pump selection is shown in Figure 4 – this pump will deliver the required flow rate with a much larger increase in downstream pressure. Perhaps the material being pumped is a critical reactant to the CSTR in Plant A, Figure 1. If the flow drops below the critical value, perhaps the plant will have to be shut down because of product quality or safety problems. This is much less likely to happen with the pump of Figure 2, reducing the number of shutdowns and subsequent startups and therefore improving plant safety.

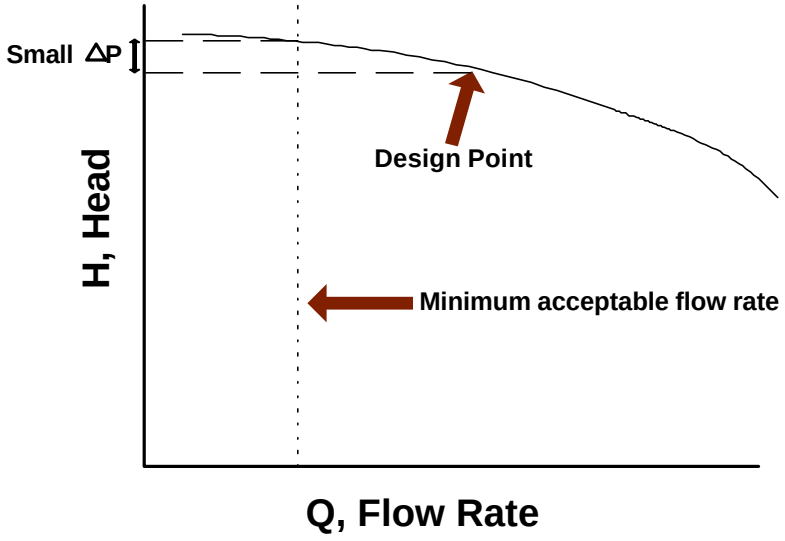

Figure 3: A Sensitive Pump Design

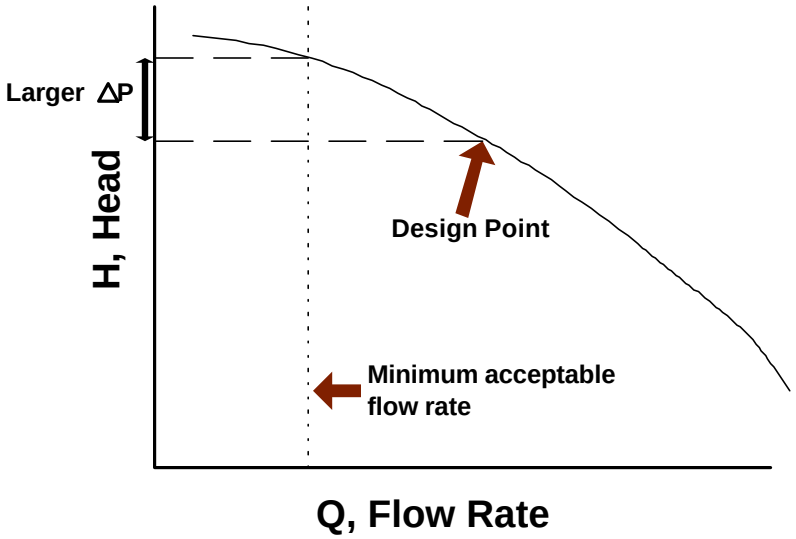

Figure 4: A More Robust Pump Design

Compressors

Similar attention to performance curves can improve the reliability of a compressor design also. The vendors do provide this information for a good reason, and it is up to the plant designer to use the available data to specify a robust design which will provide acceptable performance over a wide range of operating conditions which may be encountered in plant operation. Figure 5 shows a sensitive compressor design, which can easily go into a surge condition with a slight variation in operating conditions. Figure 6 shows a much more robust design, much more tolerant of variation in operating conditions. Again, perhaps this compressor is a critical piece of equipment for plant operability or safety – for example, it might be the refrigeration compressor for the brine supply to a reactor with a highly exothermic reaction.

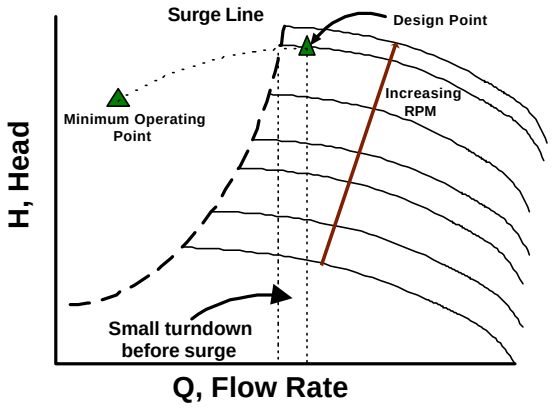

Figure 5: A Sensitive Compressor Design

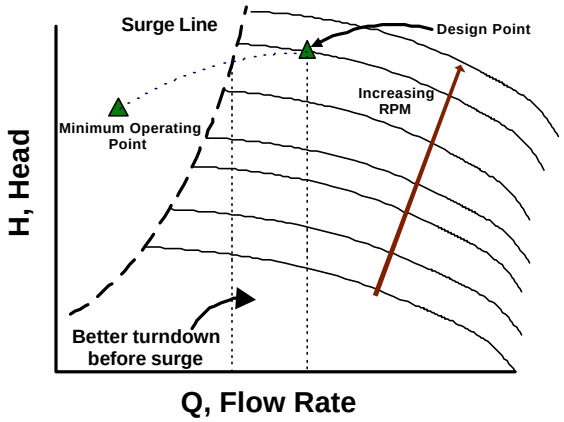

Figure 6: A More Robust Compressor Design

Fans

The selection of fan type can impact the robustness of a design, and the potential for the fan to trip out due to high power draw for the fan motor. The power draw for a radial blade fan increases as downstream dampers are opened, and it could reach a point where the motor would trip due to high power (Figure 7). A fan with backward curved blades has a maximum possible power draw, and it is possible to design the system so the fan cannot trip due to high power (Figure 8).

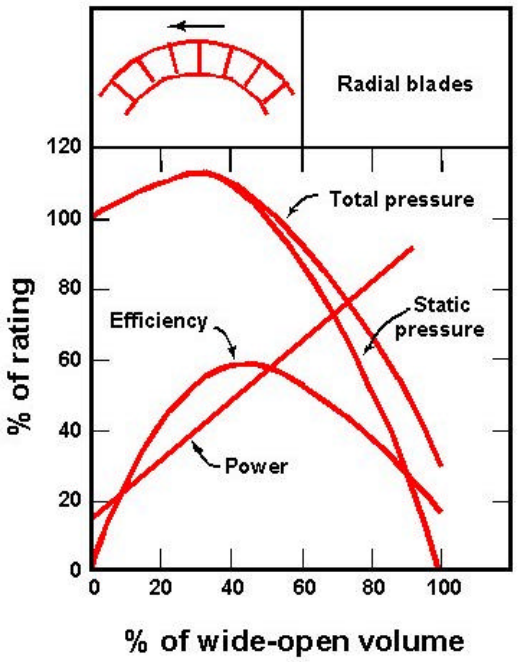

Figure 7: Power Characteristics for Radial Blade Fans

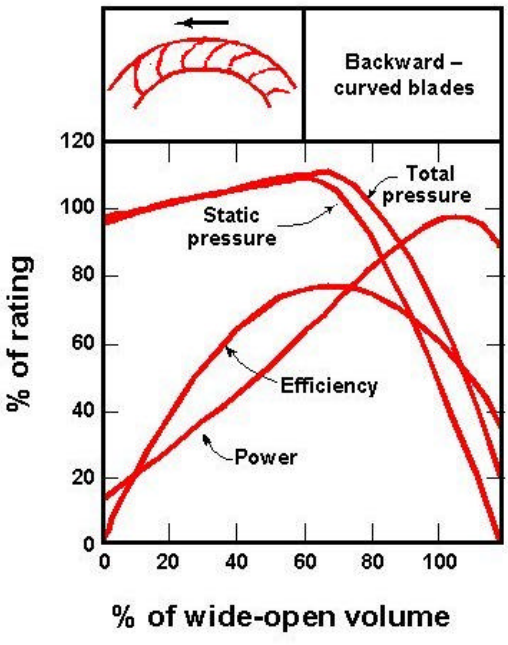

Figure 8: Power Characteristics for Backward Curved Blade Fans

Vessel Design

Many years ago, emergency relief systems from reactors and other vessels discharged directly to the atmosphere, usually through a stack or to a building roof where potential exposure to people could be minimized. This is no longer acceptable for many vessels today because of environmental concerns, and a better understanding of the potential health and safety issues arising from an emergency relief system release. Therefore, it is often necessary to provide a complex system to treat the effluent from an emergency relief device. This might include equipment such as catch tanks, quench tanks, scrubbers, absorbers, or flare systems. Figure 9 shows an example system. Such systems are expensive to build and operate, and they can never be 100% reliable. Because they are emergency systems, which do not normally operate when the plant is functioning properly, failures may be hidden, detectable only by testing and other preventive maintenance programs. In many cases it may be possible to eliminate the need for complex emergency relief and effluent treatment systems by building a stronger reaction vessel, as shown in Figure 10. If the vessel can be designed to be strong enough to contain the maximum pressure from the worst credible runaway reaction event, the emergency relief system might be eliminated or greatly simplified while still complying with code and regulatory requirements. Of course, if this strategy is adopted, it is absolutely essential that the design engineers fully understand all chemical reactions, which can occur at the extreme conditions of temperature and pressure, which will result from a runaway reaction. Experimental data for all credible runaway scenarios must be available to confirm the maximum runaway pressure and temperature.

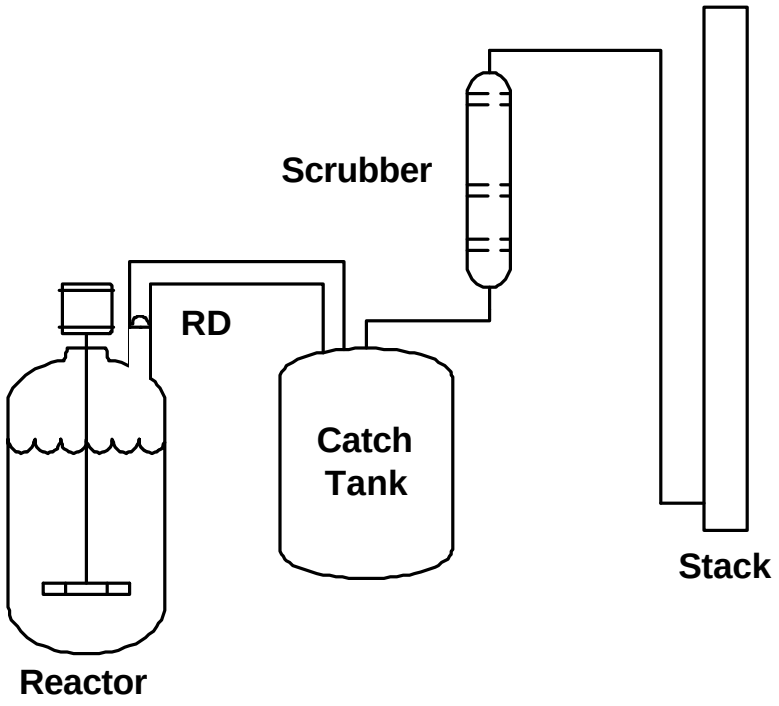

Figure 9: A Complex Emergency Relief System for a Batch Reactor with a Potential Exothermic Runaway Reaction

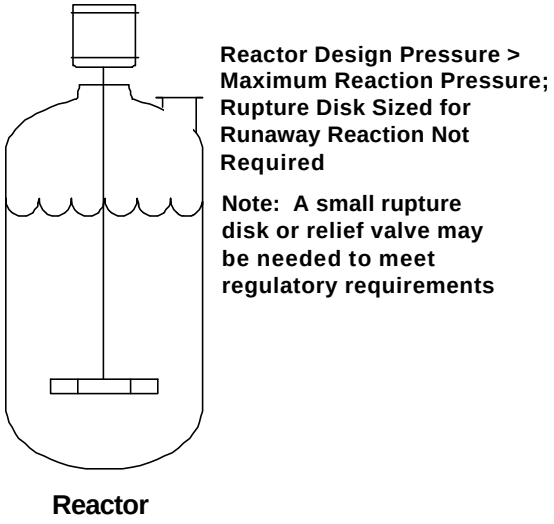

Figure 10: A Reactor with a Higher Design Pressure May Eliminate the Need for the Complex Emergency Relief System

(Note: It is essential that the chemistry, kinetics, thermodynamics, maximum temperature, and maximum pressure for the runaway reaction are thoroughly understood to properly design the reactor.)

A Piping Design Example

To avoid overpressurization due to gas and heat generation from solid packing material, the column in Figure 11 must always be lined up either to the process flow (which will carry the gas and heat away) or vented to a collection and treatment system if column is taken off line. Use of a three way valve which is designed to always be open to at least one of the flow paths (either to the process flow or to the vent system) will ensure that the column cannot be blocked in by closing the process feed valve without opening the vent valve.

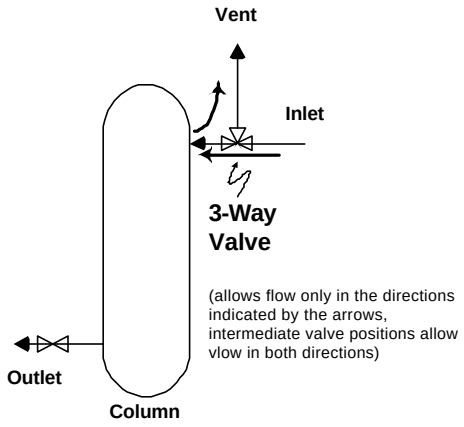

Figure 11: A Three Way Valve Ensures that the Column Is Always Either On Line or Vented

Human Factors

Attention to human factors can have a large impact on inherent safety and plant reliability. The impact of design on a person's ability to operate equipment correctly and safely has been recognized for a long time. In 1828, the pioneering railway engineer Robert Stevenson stated the basis of his design policy in improving the newly developed steam locomotive when he said that his father, George Stevenson

> "...has agreed to an alteration which I think will considerably reduce the quantity of machinery as well as the liability to mismanagement. Mr. Jos. Pease writes my father that in their present complicated state they cannot be managed by 'fools', therefore they must undergo some alteration or amendment."[3]

Today, most of us would not agree with Stevenson's characterization of early locomotive drivers as "fools", but rather recognize their behavior as typical for most people most of the time. We are unlikely to be successful in redesigning people, so a more effective approach is to design equipment and systems to be tolerant of human error.

Logical layout of controls and equipment is critical. Figure 12 shows the control and equipment layout for an actual plant, which was shut down a number of years ago. From this design, a high frequency of errors due to improper identification of equipment would not be surprising. Many more examples of human factor considerations in design are described in Reference 2.

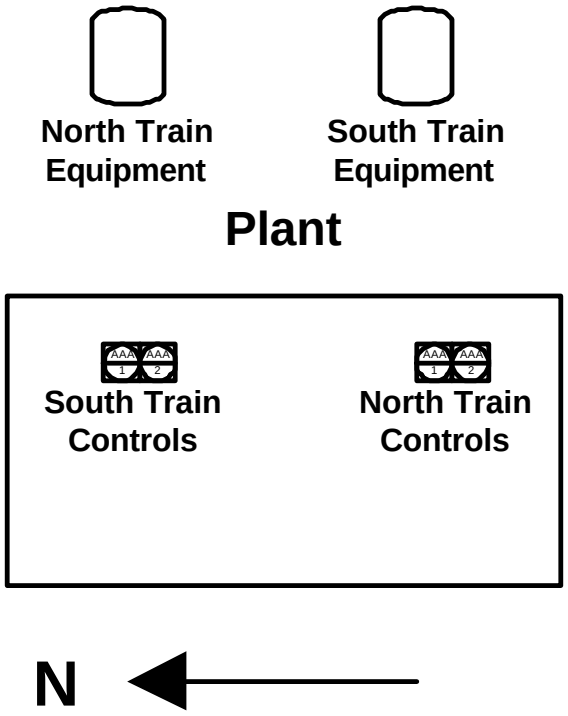

Figure 12: Poor Design of Plant Control Room

Robustness of the plant design impacts how quickly an operator must be able to diagnose and correct the cause of an abnormal situation before the plant shuts down or moves into an unsafe state. For example, the sensitive pump and compressor designs of Figures 3 and 5 above will allow the plant to get into a shutdown stage much more quickly in case of an upset condition, requiring more rapid operator diagnosis and response. The operator is much more likely to be able to correctly diagnose the problem if he has more time, as shown by the data in Table 1.

Table 1: Operator Diagnosis of a Problem as a Function of Available Response Time
(from Swain and Guttmann[4])

Available Response Time (Minutes)	Probability of Incorrect Diagnosis
1	~ 1
10	0.5
20	0.1
30	0.01
60	0.001

The design of operating and control displays also significantly impacts operator performance. Table 2 shows the probability of selecting the correct display for a variety of different ways of presenting plant information to the operator in the control room.

Table 2: Probability of Selection Error for Different Process Information Displays
(from Swain and Guttmann[3])

Display Appearance Description	Probability of Selection Error
Dissimilar to adjacent display	Negligible
Similar displays, but with clearly drawn “process mimic” lines	0.0005
Similar displays in functional groups in a panel	0.001
Similar displays in an array identified by label only	0.003

Design engineers need to pay attention to human factors with respect to operation of the plant, and also with respect to maintenance of the process equipment. Maintenance tasks which are extremely difficult are much less likely do actually be done.

General Attention to Good Design

Paying attention to design details when laying out a plant can have a major impact on plant reliability and safety. It is hard to establish a set of rules on what is a “good design”, but a thorough review of a design by engineers, operators, and mechanics using their own experience and common sense might identify design problems such as those in the following examples.

- In Figure 13, flammable and reactive additives in small containers are stored directly below an important instrument cable tray. The plant designer did not provide appropriate storage for these materials near the point of use.
- The instrument lines in Figure 14 are prone to filling up with condensate. Clearly somebody realized this and provided drains, but does anybody ever drain the condensate?
- In Figure 15, a conduit enters the top of a junction box, possibly allowing water to get in. The conduit should enter the bottom of the box.

On the other hand, attention to design details can enhance safety. In Figure 16, all nitrogen connections to a reactor have are taken from a supply through a flexible hose which passes across the reactor man way. It is not possible to open the man way without physically disconnecting the nitrogen from the reactor. Of course, this does not guarantee that the reactor atmosphere is safe for entry, but it does positively eliminate one hazard when the reactor is entered.

Many tools are available for detailed review of a plant design. These tools should be applied early in detailed design, so that any improvements and modifications can be easily and economically implemented. We have found that a combined Hazard and Operability and Reliability Centered Design review, or HAZROP (HAZard, Reliability, and OPerability) study is a particularly valuable tool. By bringing together the process and reliability experts, along with operations, safety, environmental, and other disciplines, the resulting study enhances the quality from both an EHS and reliability perspective[5, 6].

Conclusions

A process design engineer is often presented with the need to provide a detailed design for a plant for which the basic process technology has been determined. While the opportunities for a fundamentally inherently safer design through use of different manufacturing technology may be past, the design engineer has many opportunities to enhance the inherent safety of the technology which has been selected. In particular, he must pay attention to the inherent reliability and user friendliness of the plant. Plant startup and shut down tend to have a disproportionately large contribution to the total risk of operation. A more reliable plant design will minimize the number of startups and shut downs, minimizing the risk from these unsteady state operations, while improving the plant economics and operability. We have presented examples of the major contribution of startup and shut down to overall plant operating risk. We have also presented a number of specific examples of how detailed plant design can impact reliability and safety. Incorporating reliability and inherent safety principles into a plant design requires painstaking attention to details of the design, including thorough review by a multidisciplinary team of process and equipment experts.

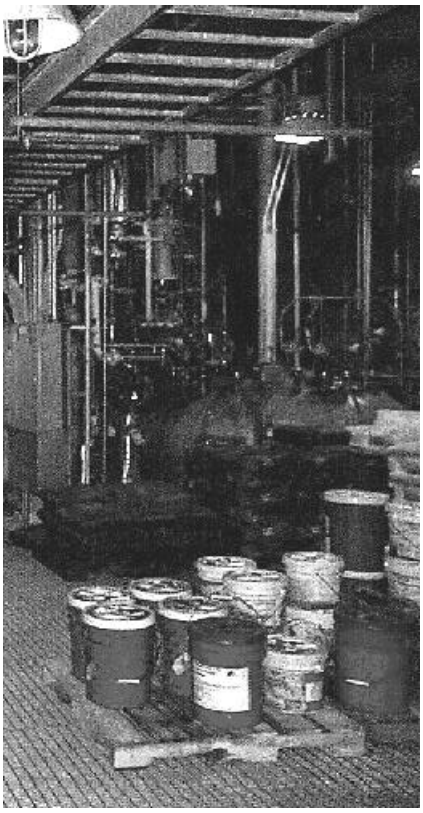

Figure 13: Flammable Materials Stored Below Cable Trays

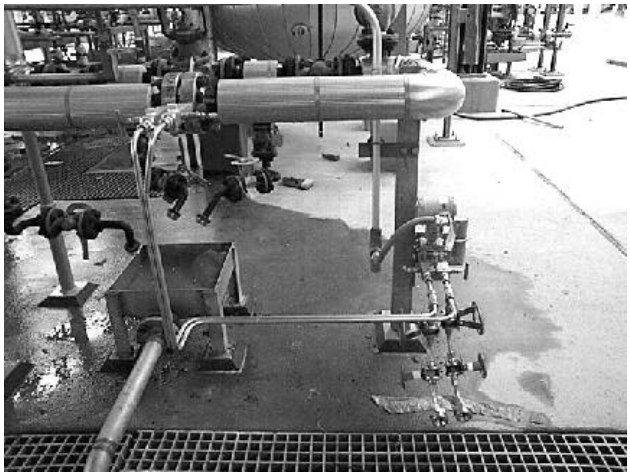

Figure 14: Instrument Connection Subject to Condensation

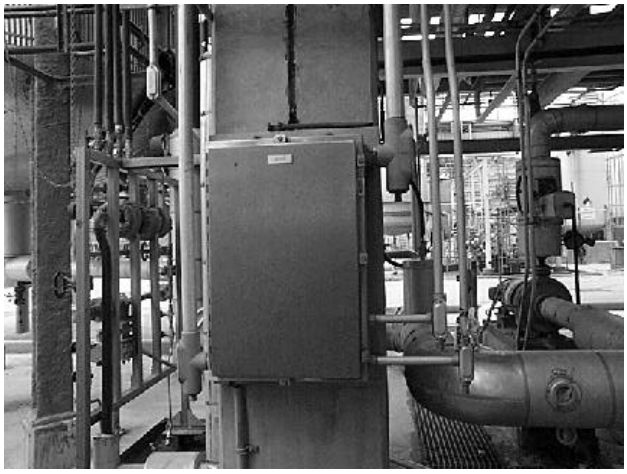

Figure 15: Conduit Box Prone to Water Entry

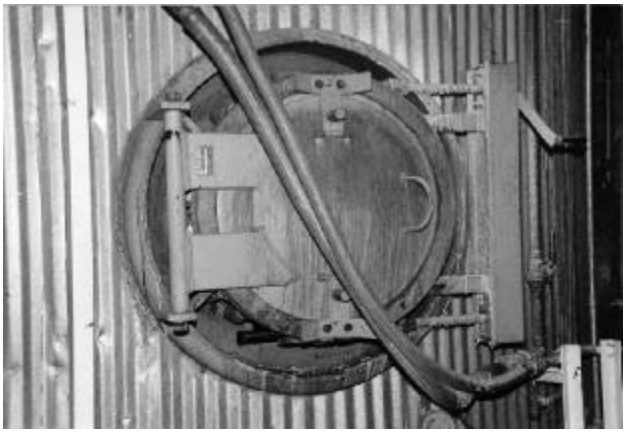

Figure 16: Nitrogen Connection Must Be Removed for Vessel Entry

References

[1] Bain, D. H. *Empire Express: Building the First Trans-continental Railroad*. Viking: New York, 1999.

[2] Center for Chemical Process Safety (CCPS). *Inherently Safer Chemical Processes: A Life Cycle Approach*, ed. D. A. Crowl. New York: American Institute of Chemical Engineers, 1996.

[3] Rolt, L. T. C. *The Railway Revolution: George and Robert Stevenson*. New York: St. Martin's Press, 1960, p. 147.

[4] Swain, A. D., and H. E. Guttmann. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Final Report).* Washington, D. C.: United States Nuclear Regulatory Commission, NUREG/CR-1278-F, August 1983.

[5] Hendershot, D. C., R. L. Post, P. F. Valerio, J. W. Vinson, and D. K. Lorenzo. "Let's Put the 'OP' Back in 'HAZOP'." *International Conference and Workshop on Reliability and Risk Management*, September 15-18, 1998, San Antonio, TX, 153-167. New York: American Institute of Chemical Engineers, 1998.

[6] Hendershot, D. C., R. L. Post, P. F. Valerio, J. W. Vinson, D. K. Lorenzo, and D. A. Walker. "Putting the 'OP' Back in 'HAZOP'." *MAINTECH South '98 Conference and Exhibition*, December 2-3, 1998, Houston, TX.