Not only does safety have to be designed into the product life cycle, it must also have management commitment to thrive and persevere. A good system safety management program does significantly lower business-operating costs. According to the U.S. Occupational Safety and Health Administration (U.S. OSHA, 2013), there are 60%–80% fewer lost workday injuries than the national average by using system safety as part of the Volunteer Protection Program (VPP). According to OSHA (Gibbs and Lahale, 2014), it is a quite significant reduction:

- 54% below the Bureau of Labor Statistics (BLS) Total Case Incident Rate (TCIR) for their industries.
- 53% below the BLS days away, restricted and transfer (DART) rate for their industries.
- 354 VPP sites experienced zero recordables.

In the same report, Gibbs and Lahale give examples of how safety saves money:

- Within 1 year of achieving star status, Lockheed Martin's Moorestown site's worker compensation costs decreased by 75% from over $740,000 per year to $188,869 per year. VPP participation continued to positively impact the site's bottom line, and in 2006, their workers' compensation costs were about $94,000 annually.
- In 2002, MYR Group, one of the largest electrical transmission and distribution companies in the United States had a TCIR of 7.3 and a DART rate of 3.9; they were also facing significant enforcement actions. Through concerted efforts throughout the organization, safety and health has been transformed into a key corporate value. By 2007, MYR's TCIR was reduced to 2.7 (a 63% decrease) and their DART to 1.2 (a 69% decrease). Their 2007 TCIR and DART rates are also 53% and 63% below the 2006 BLS national average for the power and communication line construction industry, respectively.

The company's system safety program, as executed through a safety management system (SMS), is the umbrella organization that will apply the safety concepts discussed in Chapter 2 to real-life situations. How the safety program is implemented and managed is critical to its success. A closed-loop process is really the only way to track and resolve identified hazards adequately. Safety reviews and audits are also part of this process. A good system safety management program (SMS) fits neatly into the new voluntary protection programs (VPPs) that various governments are implementing.

4.1 SAFETY IN THE SYSTEM LIFE CYCLE

Even today in the United States there are about 13 deaths daily in the workplace and 4 million injuries per year (Barab, 2012), which means we have to better integrate system safety into all engineering aspects. "Studies conducted at Stanford University estimate the cost of accidents for users of commercial and industrial construction at $1.6 billion annually. Hidden costs were found to be two to 18 times higher. Researchers also found that construction safety research over a 10-year period showed irrefutable

evidence that accidents are controllable, to some extent, by all levels of construction management" (Gallagher, 1993). The UK Health and Safety Executive (Institution of Engineering and Technology, 2012) studies show that even minor accidents have ongoing costs, which can be quite high. A few examples they cite are as follows:

- In one organization, accident costs (when all factors were included) amounted to 37% of profit
- In another, it was 8.5% of tender prices.
- In the third, it was 5% of running costs.

Of course, the statistics vary from industry to industry; what is important to note is that accidents do happen, even minor ones, but they can be prevented.

The primary method of preventing accidents is through a comprehensive and systematic approach to safety management. The most cost-effective way to control risks is to implement and maintain a comprehensive SMS throughout the product or system life cycle—from cradle to grave. This will lower failures or mistakes (by both people and machines), prevent gaps in analysis (avoid overlooking valuable data and warning signs), and provide demonstrable safety coverage (meeting federal and local laws and creating a legally defensible audit trail). If you have a comprehensive SMS, you can protect yourself from liability claims in the most cost-effective manner possible.

4.1.1 System Life Cycle

Every industry has its own way to define the system or product life cycle. For example, the facility construction industry life-cycle phases are requirements, planning, design, construction, activation, operation, and disposal. For purposes of discussion, the system life cycle is defined as (cradle to grave) follows:

Concept: The idea of the project is *hatched*. During this phase, engineers develop an idea to accomplish the goal. More than one concept can be presented at this phase.

Definition: At this phase, the selected concept is amplified to exactly how the product or system is to be built. Preliminary design is performed.

Detailed design: The critical design is conducted. Detailed drawings and calculations are performed.

Development: The design is now mature and the system is constructed. As every engineer knows, there can be various iterations back and forth between the detailed design and development phases.

Test and evaluation: Once the system is built, it must be tested and evaluated. If serious problems still exist, the product can go back to the design and development phases.

Production: The system or product now enters the manufacturing phase.

Deployment: At this phase, the system is placed into its service location. Preoperation (or prerevenue) tests and adjustments are made at this time.

Operation: The system performs its intended function.

Modification (optional): Sometimes, the product or system must be changed due to design or operation deficiencies that were not identified earlier.
Disposal: The system is retired from operation and decommissioned.

For each life-cycle phase, the hazards should be assessed and controlled. The earlier in the life cycle this is done, the cheaper it is to accomplish. An SMS is a sustainable management system that is built around this process. Section 4.2 will discuss this in detail.

4.1.2 Safety and the System Life Cycle

Of course, system safety tools can be applied during any one of the aforementioned phases; however, you need to be judicious in deciding when, where, and how much intervention is required. Probably all of the activities shown in the following should be performed, but not necessarily to the same level of detail. You will need to tailor the safety engineering to the appropriate level of operation. Obviously, the earlier in the project design phase this is done, the better. If the design is still on the computer-aided design system (what used to be the drawing board), it is 10- to 100-fold less expensive to modify the design than after deployment in the field.

What is also important to realize is that different activities are done during the various life-cycle phase. Some of the activities are repeated and some are not. Also, some of the work is performed as a management function and some as an engineering function. The rest of this book details how each of these safety tools can be applied, their pitfalls, and suggestions for maximum utilization at the most reasonable cost.

Table 4.1 shows where each of the major safety milestones fits into the system life cycle. Safety activities are listed on the left-hand side. The remainder of the table describes the kinds of activities to be performed during each phase of the life cycle. As you can see, many of the activities are repeated throughout the life of the system, such as implementing and maintaining the system safety program plan (SSPP).

4.1.3 Case Studies of Poor Application of Safety in the System Life Cycle

We all remember numerous technological *disasters* where management or engineering intervention might have averted a catastrophic situation. To refresh your memory with just a few choice examples, the column on the left of the table in Table 4.2 was taken from the first edition of this book, and the column on the right represents more recent accidents. One quickly realizes that in spite of the many year intervals between the two editions, we are still having horrendous, preventable, disasters.

As society becomes more and more complex and our engineered systems are more difficult for one individual or group to master and control, it becomes important for us to understand how some of these accidents came about. Many of today's disasters not only affect the plant but also many times cross international borders. If you are following appropriate engineering and safety processes and standards, the likelihood of such a catastrophic disaster is lowered. It is hoped that you will find that your own plant or system is not following along the same path of the infamous accidents mentioned.

The Flixborough explosion and the *Challenger* accident are two case studies of poor safety management. What can be seen is that the accidents were *destined* to occur.