1.4.1 Safety in Mechanical Design

The code of Hammurabi, a Babylonian doctrine over 3000 years old, had this requirement:

> If a builder build a house for a man and do not make its construction firm, and the house which he has built collapse and cause the death of the owner of the house, that builder shall be put to death.

It could be argued that engineers are getting off a lot easier these days. Modern legal doctrines do not call for the death of manufacturers of unsafe products or of the engineers who designed them. Regardless of the penalty, however, engineers have a moral and legal obligation to produce reasonably safe products. A number of fundamental concepts and tools are available to assist them in meeting this challenge.

Safety Factor

If 500 tension tests are performed on a specimen of one material, 500 different yield strengths will be obtained if the precision and accuracy of measurement are high enough. With some materials, a wide range of strengths can be achieved; in others, a reasonable guaranteed minimum strength can be found. However, this strength does not usually represent the stress that engineers apply in design.

Using results from small-scale tension tests, a design engineer prescribes a stress somewhat less than the semi-empirical strength of a material. The **safety factor** can be expressed as

$$n_s = \frac{\sigma_{\text{all}}}{\sigma_d} \tag{1.1}$$

where σ_{all} is the allowable normal stress and σ_d is the design normal stress. If $n_s > 1$, the design is adequate. The larger n_s, the safer the design. If $n_s < 1$, the design may be inadequate and redesign may be necessary. In later chapters, especially Chapter 6, more will be said about σ_{all} and σ_d. The rest of this section focuses on the left side of Eq. (1.1).

It is difficult to accurately evaluate the various factors involved in engineering design problems. One factor is the shape of a part. For an irregularly shaped part, there may be no design equations available for accurate stress computation. Sometimes the load is uncertain. For example, the loading applied to a bicycle seat and frame depends on the size of the rider, speed, and size of bumps encountered. Another factor is the consequences of part failure; life-threatening consequences require more consideration than non-life-threatening consequences.

Engineers use a safety factor to ensure against such uncertain or unknown conditions. The engineering student is often asked, What safety factor was used in the design, and which value should be used? Safety factors are sometimes prescribed by code, but usually they are rooted in design experience. That is, design engineers have established through a product's performance that a safety factor is sufficient. Future designs are often based on safety factors found adequate in previous products for similar applications.

Particular design experience for specific applications does not form a basis for the rational discussion of illustrative examples or for the guidance of engineering students. The Pugsley [1966] method for determining the safety factor is a potential approach for obtaining safety factors in design, although the reader should again be warned that safety factor selection is somewhat nebulous in the real world and the Puglsey method can be unconservative; that is, it predicts safety factors that are too low for real applications. Pugsley systematically determined the safety factor from

Table 1.1: Safety factor characteristics A, B, and C.

Characteristic[a]		B			
A	C	vg	g	f	p
vg	vg	1.1	1.3	1.5	1.7
	g	1.2	1.45	1.7	1.95
	f	1.3	1.6	1.9	2.2
	p	1.4	1.75	2.1	2.45
g	vg	1.3	1.55	1.8	2.05
	g	1.45	1.75	2.05	2.35
	f	1.6	1.95	2.3	2.65
	p	1.75	2.15	2.55	2.95
f	vg	1.5	1.8	2.1	2.4
	g	1.7	2.05	2.4	2.75
	f	1.9	2.3	2.7	3.1
	p	2.1	2.55	3.0	3.45
p	vg	1.7	2.15	2.4	2.75
	g	1.95	2.35	2.75	3.15
	f	2.2	2.65	3.1	3.55
	p	2.45	2.95	3.45	3.95

[a] vg = very good, g = good, f = fair, and p = poor.
A = quality of materials, workmanship, maintenance, and inspection.
B = control over load applied to part.
C = accuracy of stress analysis, experimental data or experience with similar parts.

Table 1.2: Safety factor characteristics D and E.

Characteristic E[a]	D		
	ns	s	vs
ns	1.0	1.2	1.4
s	1.0	1.3	1.5
vs	1.2	1.4	1.6

[a] vs = very serious, s = serious, and ns = not serious
D = danger to personnel
E = economic impact

$$n_s = n_{sx} n_{sy} \tag{1.2}$$

where

n_{sx} = safety factor involving characteristics A, B, and C
A = quality of materials, workmanship, maintenance, and inspection
B = control over load applied to part
C = accuracy of stress analysis, experimental data, or experience with similar devices
n_{sy} = safety factor involving characteristics D and E
D = danger to personnel
E = economic impact

Table 1.1 gives n_{sx} values for various A, B, and C conditions. To use this table, estimate each characteristic for a particular application as being very good (vg), good (g), fair (f), or poor (p). Table 1.2 gives n_{sy} values for various D and E conditions. To use this table, estimate each characteristic for a particular application as being very serious (vs), serious (s), or not serious (ns). Substituting the values of n_{sx} and n_{sy} into Eq. (1.2) yields a proposed safety factor.

Although a simple procedure to obtain safety factors, the Pugsley method illustrates the concerns present in safety factor selection. Many parameters, such as material strength and applied loads, may not be well known, and confidence in the engineering analysis may be suspect. For these reasons the safety factor has sometimes been called an "ignorance factor," as it compensates for ignorance of the total environment, a situation all design engineers encounter to some extent. Also, the Pugsley method is merely a guideline and is not especially conservative; most engineering safety factors are much higher than those resulting from Eq. (1.2), as illustrated in Example 1.1.

Example 1.1: Safety Factor of Wire Rope in an Elevator

Given: A wire rope is used on an elevator transporting people to the 20th floor of a building. The design of the elevator can be 50% overloaded before the safety switch shuts off the motor.

Find: What safety factor should be used?

Solution: The following values are assigned:

A = vg, because life threatening
B = f to p, since large overloads are possible
C = vg, due to being highly regulated
D = vs, people could die if the elevator fell from the 20th floor
E = vs, possible lawsuits

From Tables 1.1 and 1.2 the safety factor is

$$n_s = n_{sx} n_{sy} = (1.6)(1.6) = 2.56$$

Note that the value of $n_{sx} = 1.6$ was obtained by interpolation from values in Table 1.1. By improving factors over which there is some control, n_{sx} can be reduced from 1.6 to 1.0 according to the Pugsley method, thus reducing the required safety factor to 1.6.

Just for illustrative purposes, the safety factor for this situation is prescribed by an industry standard [ANSI 2010] and cannot be lower than 7.6 and may need to be as high as 11.9. The importance of industry standards is discussed in Section 1.4.2, but it is clear that the Pugsley method should be used only with great caution.

Product Liability

When bringing a product to the market, it is probable that safety will be a primary consideration. A design engineer must consider the **hazards**, or injury producers, and the **risk**, or likelihood of obtaining an injury from a hazard, when evaluating the safety of a system. Unfortunately, this is mostly a qualitative evaluation, and combinations of hazard and risk can be judged acceptable or unacceptable.

The ethical responsibilities of engineers to provide safe products are clear, but the legal system also enforces societal expectations through a number of legal theories that apply to designers and manufacturers of products. Some of the more common legal theories are the following:

- **Caveat Emptor**. Translated as "Let the buyer beware," this is a doctrine founded on Roman laws. In the case of a defective product or dangerous design, the purchaser or user of the product has no legal recourse to recover losses. In a modern society, such a philosophy is incompatible with global trade and high-quality products, and is mentioned here only for historical significance.

- **Negligence.** In negligence, a party is liable for damages if they failed to act as a reasonable and prudent party would have done under like or similar circumstances. For negligence theory to apply, the injured party, or *plaintiff*, must demonstrate:

    1. That a standard of care was violated by the accused party, or *defendant*.
    2. That this violation was the *proximate cause* of the accident.
    3. That no contributory negligence of the plaintiff caused the misfortune.

- **Strict liability**. Under the strict liability doctrine, the actions of the plaintiff are not an issue; the emphasis is placed on the machine. To recover damages under the strict liability legal doctrine, the plaintiff must prove that:

    1. The product contained a defect that rendered it unreasonably dangerous. (For example, an inadequately sized or cracked bolt fastening a brake stud to a machine frame.)
    2. The defect existed at the time the machine left the control of the manufacturer. (The manufacturer used the cracked bolt.)
    3. The defect was a proximate cause of the accident. (The bolt broke, the brake stud fell off the machine, the machine's brake didn't stop the machine, resulting in an accident.) Note that the plaintiff does not need to demonstrate that the defect was the proximate cause; the actions of the plaintiff that contribute to his or her own accident are not considered under strict liability.

- **Comparative fault.** Used increasingly in courts throughout the United States, juries are asked to assess the relative contributions that different parties had in relation to an accident. For example, a jury may decide that a plaintiff was 75% responsible for an accident, and reduce the monetary award by that amount.

- **Assumption of risk.** Although rarely recognized, the *assumption of risk* doctrine states that a plaintiff has limited recourse for recovery of loss if they purposefully, knowingly, and intentionally conducted an unsafe act.

One important requirement for engineers is that their products must be reasonably safe for their intended uses as well as their *reasonably foreseeable misuses*. For example, a chair must be made structurally sound and stable enough for people to sit on (this is the intended use). In addition, a chair should be stable enough so that someone can stand on the chair to change a light bulb, for example. It could be argued that chairs are designed to be sat upon, and that standing on a chair is a misuse. This may be true, but represents a reasonably foreseeable misuse of the chair, and must therefore be considered by designers. In the vast majority of states, misuses of a product that are not reasonably foreseeable do not have to be considered by the manufacturers.

The legal doctrines and ethical requirements that designers produce safe products are usually consistent. Sometimes, the legal system does result in requirements that engineers cannot meet. For example, in the famous *Barker vs. Lull* case in New Jersey, the court ruled that product manufacturers have a nondelegable duty to warn of the unknowable.

Liability proofing is the practice of incorporating design features with the intent of limiting product liability exposure without other benefits. This can reduce the safety of machinery. For example, one approach to liability proofing is to place a very large number of warnings onto a machine, with the unfortunate result that all of the warnings are ignored by machine operators. The few hazards that are not obvious and can be effectively warned against are then "lost in the noise" and a compromise of machine safety can occur.

Case Study 1.1: *Mason v. Caterpillar Tractor Co.*

Wilma Mason brought action under negligence theory against Caterpillar Tractor Company and Patton Industries for damages after her husband received fatal injuries while trying to repair a track shoe on a Caterpillar tractor. Mr. Mason was repairing the track shoe with a large sledgehammer, when a small piece of metal from the track shoe shot out, striking him, and causing fatal injuries. The plaintiff alleged that the tractor track was defective because the defendants failed to use reasonable methods of heat treatment, failed to use a sufficient amount of carbon in the steel, and failed to warn the decedent of "impending danger."

The Trial and Appellate courts both granted summary judgements in favor of the defendants. They ruled that the plaintiff failed to show evidence of a product defect that existed when the machine left the control of the manufacturer. Mr. Mason used a large, 10-kg sledgehammer with a full swing, striking a raised portion of the track shoe. There was no evidence that the defendants were even aware that the track shoes were being repaired or reassembled by sledgehammers. It was also noted by the court that the decedent wore safety glasses, indicating his awareness of the risk of injury.

Safety Hierarchy

A design rule that is widely accepted in general is the **safety hierarchy**, which describes the steps that a manufacturer or designer should use when addressing hazards. The safety hierarchy is given in Design Procedure 1.1. Eliminating hazards through design can imply a number of different approaches. For example, a mechanical part that is designed so that its failure is not reasonably foreseeable is one method of eliminating a hazard or risk of injury. However, design of a system that eliminates injury producers or moves them away from people also represents a reasonable approach.

This book emphasizes mechanical analysis and design of parts to reduce or eliminate the likelihood of failure. As such, it should be recognized that this approach is one of the fundamental, necessary skills required by engineers to provide reasonably safe products.

Design Procedure 1.1: The Safety Hierarchy

A designer should attempt the following, in order, in attempting to achieve reasonable levels of safety:

1. Eliminate hazards through design.
2. Reduce the risk or eliminate the hazard through safeguarding technology.
3. Provide warnings.
4. Train and instruct.
5. Provide personal protective equipment.

There is a general understanding that primary steps are more efficient in improving safety than later steps. That is, it is more effective to eliminate hazards through design than to use guards, which are more effective than warnings, etc. Clearly, the importance of effective design cannot be overstated.

Failure Mode and Effects Analysis and Fault Trees

Some common tools available to design engineers are **failure mode and effects analysis** (FMEA) and **fault tree analysis**. FMEA addresses component failure effects on the entire system. It forces the design engineer to exhaustively consider reasonably foreseeable failure modes for every component and its alternatives.

FMEA is flexible, allowing spreadsheets to be tailored for particular applications. For example, an FMEA can also be performed on the steps taken in assembling components to identify critical needs for training and/or warning.

In fault tree analysis, statistical data are incorporated into the failure mode analysis to help identify the most likely (as opposed to possible) failure modes. Often, hard data are not available, and the engineer's judgment qualitatively identifies likely failure modes.

As discussed above, machine designers are legally required to provide reasonably safe products and to consider the product's intended uses as well as foreseeable misuses. FMEA and fault tree analysis help identify unforeseeable misuses as well. For example, an aircraft designer may identify aircraft-meteorite collision as a possible loading of the structure. However, because no aircraft accidents have resulted from meteorite collisions and the probability of such occurrences is extremely low, the design engineer ignores such hypotheses, recognizing they are not reasonably foreseeable.

Load Redistribution, Redundancy, Fail Safe, and the Doctrine of Manifest Danger

One potential benefit of failure mode and effects analysis and fault tree analysis is that they force the design engineer to think of minimizing the effects of individual component failures. A common goal is that the failure of a single component should not result in a catastrophic accident. The design engineer can ensure this by designing the system so that, upon a component failure, loads are redistributed to other components without exceeding their nominal strengths — a philosophy known as **redundancy** in design. For example, a goose or other large bird sucked into an aircraft engine may cause several components to fail and shut down the engine. This type of accident is not unheard of and is certainly reasonably foreseeable. Thus, modern aircraft are designed with sufficient redundancy to allow a plane to fly and land safely with one or more engines shut down.

Many designs incorporate redundancy. Redundant designs can be *active* (where two or more components are in use but only one is needed) or *passive* (where one component is inactive until the first component fails). An example of an active redundant design is the use of two deadbolt locks on a door: both bolts serve to keep the door locked. A passive redundant design example would entail adding a chain lock on a door having a deadbolt lock: if the deadbolt lock fails, the chain will keep the door closed.

An often-used philosophy is to design machinery with **fail-safe** features. For example, a brake system (see Chapter 18) can be designed so that a pneumatic cylinder pushes the brake pads or shoes against a disk or drum, respectively. Alternatively, a spring could maintain pressure against the disk or drum and a pneumatic system could work against the spring to release the brake. If the pressurized air supply were interrupted, such a design would force brake actuation and prevent machinery motion. This alternative design is fail safe as long as the spring is far more reliable than the pneumatic system.

The **doctrine of manifest danger** is a powerful tool used by machinery designers to prevent catastrophic losses. If danger becomes manifest, troubleshooting is straightforward and repairs can be quickly made. Thus, if a system can be designed so that imminent failure is detectable or so that single-component failure is detectable before other elements fail in turn, a safer design results. A classic application of the doctrine of manifest danger is in the design of automotive braking systems, where the brake shoe consists of a friction material held onto a metal backing plate by rivets. By making the rivets long enough, an audible and tactile indication is given to the car driver when the brake system needs service. That is, if the friction material has worn, the rivets will contact the disk or drum, indicating through noise and vibration that maintenance is required, and this occurs long before braking performance is compromised.

Reliability

Safety factors are a way of compensating for variations in loading and material properties. Another approach that can be extremely successful in certain circumstances is the application of **reliability** methods.

As an example, consider the process of characterizing a material's strength through tension tests (see Section 3.4). Manufacturing multiple tension test specimens from the same extruded billet of aluminum would result in little difference in measured strength from one test specimen to another. Thus, aluminum in general (as well as most metals) is a *deterministic* material, and deterministic methods can be used in designing aluminum structures if the load is known. For example, in a few hundred tensile tests, a guaranteed minimum strength can be defined that is below the strength of any test specimen and that would not vary much from one test population to another. This guaranteed minimum strength is then used as *the* strength for design analysis. Such deterministic methods are used in most solid mechanics and mechanics courses. That is, all specimens of a given material have a single strength and the loading is always well defined.

Most ceramics, however, would have a significant range of any given material property, including strength. Thus, ceramics are *probabilistic*, and an attempt to define a minimum strength for a population of ceramic test specimens would be an exercise in futility. There would not necessarily be a guaranteed minimum strength. One can only treat ceramics in terms of a likelihood or probability of strength exceeding a given value. There are many such probabilistic materials in engineering practice.

Some loadings, on the other hand, are well known and never vary much. Examples are the stresses inside intravenous (IV) bags during sterilization, the load supported by counterweight springs, and the load on bearings supporting centrifugal fans. Other loads can vary significantly, such as the force exerted on automotive shock absorbers (depends on the size of the pothole and the speed at impact) or on wooden pins holding a chair together (depends on the weight of the seated person or persons) or the impact force on the head of a golf club.

For situations where a reasonable worst-case scenario cannot be defined, reliability methods are sometimes a reasonable design approach. In reliability design methods, the goal is to achieve a reasonable likelihood of survival under the loading conditions during the intended design life. This approach has its difficulties as well, including the following:

1. To use statistical methods, a reasonable approximation of an infinite test population must be defined. That is, mean values and standard deviations about the mean, and even the nature of the distribution about the mean, must be known. However, they are not usually very well characterized after only a few tests. After all, if only a few tests were needed to quantify a distribution, deterministic methods would be a reasonable, proper, and less mathematically intensive approach. Thus, characterization can be expensive and time consuming, since many experiments are needed.

2. Even if strengths and loadings are known well enough to quantify their statistical distributions, defining a desired reliability is as nebulous a problem as defining a desired safety factor. A reliability of 99% might seem acceptable, unless that were the reliability of an elevator you happened to be occupying. A reliability of 100% is not achievable, or else deterministic methods would be used. A reliability of 99.9999...% should be recognized as an extremely expensive affair, and as indicative of overdesign as a safety factor of 2000.

3. The mathematical description of the data has an effect on reliability calculations. A quantity may be best described by a Gaussian or normal distribution, a lognormal distribution, a binary distribution, a Weibull distribution, etc. Often, one cannot know beforehand which distribution is best. Some statisticians recommend using a normal distribution until it is proved ineffective.

The implications are obvious: Reliability design is a complicated matter and even when applied does not necessarily result in the desired reliability if calculated from insufficient or improperly reduced data.

This textbook will emphasize deterministic methods for the most part. The exceptions are the treatments of rolling-element bearings and gears and reliability in fatigue design. For more information on reliability design, refer to the excellent text by Lewis [1995] among others.

1.4.2 Government Codes and Industry Standards

In many cases, engineers must rely on government codes and industry-promulgated standards for design criteria. Some of the most common sources for industry standards are:

1. ANSI, the American National Standards Institute
2. ASME, the American Society of Mechanical Engineers
3. ASTM, the American Society for Testing and Materials
4. AGMA, the American Gear Manufacturers Association
5. AISI, the American Iron and Steel Institute
6. AISC, the American Institute of Steel Construction
7. ISO, the International Standards Organization
8. NFPA, the National Fire Protection Association
9. UL, Underwriters Laboratories