# 14

# Anticipating Failure

## Chapter Overview

An engineering system fails when it is unable to fulfill its expected functions and requirements. The potential economic, environmental, and human consequences of failure can be severe. As such, it is essential for engineers to do their best to safeguard against failures, and to design systems to minimize the consequences of failures when they do occur. In general, the effort to control failures in engineering is focused on three avenues: [1] identifying all possible modes of failure, [2] preventing failures by using a large safety factor, and [3] controlling the impact of failure. There are systemic approaches to each of these avenues.

In order to control failures, we must first identify all possible ways an engineering system can fail. Often, this task is accomplished through two complementary systematic methods: Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). In FMEA, the overall engineering system is decomposed into subsystems, and the failure modes of each subsystem are identified. Each subsystem is then treated as a separate engineering system and FMEA is performed on them again by decomposing them into sub-subsystems. Eventually, a hierarchy of FMEA is generated that covers every component of the engineering system. In this way, FMEA systematically considers all the components of a system and how they may fail. However, FMEA does not consider failures caused by chains of events involving multiple components, making it better suited for uncomplicated systems. FTA addresses this weakness of FMEA by explicitly considering chains of events, producing a tree-like graph where the base of the tree represents the final failure being considered and each branch of the tree being one chain of events that could lead to failure. For more complex systems, it is good to perform both FMEA and FTA.

An engineering system fails when the demand placed on it exceeds its capacity to handle the demand, or when it is exposed to unexpected demands. Safety factor is the ratio between the capacity of the system to handle demand and the maximum demand expected to be placed on it. Typically, safety factors are established from experience, and are captured in codes and regulations. Safety factors are influenced by three factors: [1] the uncertainty associated with the capacity and demand of the engineering system as well as the uncertainty associated with how the engineering system will behave in response to unexpected demand, [2] the severity of the consequences of the failure, and [3] the cost of increasing factor of safety.

Paradoxically, even though we do our best to prevent failures, we must also prepare for the possibility of failures by designing our systems to minimize the consequence of failures. There are five approaches to achieve this: redundancy, failsafe design, progressive failure, weak links, and operational safeguards. By designing our system with redundancy, we ensure that the system does not fail if one part of the system fails. However, redundancy does not protect the system from common-mode failure. A failsafe is a design decision that shuts down a system's operation if failure occurs, thereby preventing more severe consequences of failure from developing. In some situations, it may be possible to encourage a system to fail progressively through stages, giving users sufficient early warnings to develop counter-measures or to evacuate. An intentional "weak link" may be designed into the system in order to encourage this "weak link" to fail first if demand exceeds capacity, thereby avoiding failures of more serious consequence. The downside of introducing a "weak link" is that the overall capacity of the system is reduced through its introduction. Lastly, the consequence of failure can be minimized by teaching users of the system to respond to specific failure modes in predetermined ways. This approach, called operational safeguards, can be cost-effective compared to design modifications, particularly when there is uncertainty regarding how the system will behave. The weakness of this approach is that users may become lax after years of failure-free experience.

## Learning Objectives

In this chapter, you will:

- learn about the possibility and consequence of failures in engineering systems;
- learn to use a large safety factor to safeguard against failure; and
- learn to design systems so that the consequence is limited if failure does occur.