CHAPTER 1

Introduction

Things fail. During the past two years this author has experienced a lawn-mower casing crack, a washing machine fail, a car battery go dead, a toaster oven electrical plug burn, a water-heater leak, a floppy disk drive go bad, a TV remote control quit functioning, a stereo amplifier quit, an automobile engine starter fail, and a house roof leak. The cracked lawn-mower casing was a result of its aluminum construction having insufficient strength to withstand the stresses placed on it. The car battery, the engine starter, and the washing-machine motor experienced wearout after a "normal" life. The toaster oven plug was a poor design, considering the amount of current passing through it. Corrosion of the hot water tank caused it to leak. The corrosion was partly attributed to the lack of preventive maintenance, which required periodical draining of the bottom of the tank. The failure of the disk drive was a result of an unknown (premature) mechanical failure, and the TV remote control's failure was caused by a "random" electronic component failure. On the other hand, the stereo amplifier failure was caused by an open at a solder joint. Poor construction resulted in the house roof leaking adjacent to the dormers. Some of these failures caused much inconvenience in addition to their economic impact. Several of the failures raised concerns about personal safety, although no injuries resulted from them.

Many failures, however, are much more significant in both their economic and safety effects. For example, in 1946 the entire fleet of Lockheed Constellation aircraft was grounded following a crash killing four of the five crew members. The crash was attributed to a faulty design in an electrical conduit that caused the fuselage to burn. In 1979 the left engine of a DC-10 broke away from the aircraft during takeoff, killing 271 people. Poor maintenance procedures and a bad design led to the crash. Engine removal procedures introduced unacceptable stresses on the pylons. The Ford Pinto, introduced in 1971, was recalled by Ford in 1978 for modifications to the fuel tank to reduce fuel leakage and fires resulting from rear-end collisions. Numerous reported deaths, lawsuits, and the negative publicity eventually contributed to Ford discontinuing production of the Pinto. Firestone's steel-belted radials, introduced in 1972, failed at an abnormal rate as a result of the outer tread

coming apart from the main body of the tire. Because of the excessive number of failures, Firestone was forced to recall 7.5 million tires. On November 8, 1940, the Tacoma Narrows Bridge, five months old, collapsed into Puget Sound from vibrations caused by high winds. Metal fatigue induced by several months of oscillations led to the failure. The Manus River bridge (Greenwich, Connecticut) collapsed in 1983, killing three people and injuring three. While there is disagreement on the cause of the disaster, blame has been placed on the original design, on corrosion that had caused undetected displacement of the pin-and-hanger suspension assembly, on poor maintenance, and on inadequate inspections. The Hartford (Connecticut) Civic Center Coliseum roof collapsed in 1978 from structural failure due to the weight of the snow and ice accumulated on the roof. A major shortcoming in the roof frame system was the lack of redundancy of members to carry loads when other individual members failed. An inadequate safety margin may also have contributed. The Three Mile Island disaster in 1979, which resulted in a partial meltdown of a nuclear reactor, was a result of both mechanical and human error. When a backup cooling system was down for routine maintenance, air cut off the flow of cooling water to the reactor. Warning lights were hidden by maintenance tags. An emergency relief valve failed to close, causing additional water to be lost from the cooling system. Operators were either reading gauges that were not working properly or taking the wrong actions on the basis of those that were operating. The 1986 explosion of the space shuttle *Challenger* was a result of the failure of the rubber O-rings that were used to seal the four sections of the booster rockets. The below-freezing temperatures before the launch contributed to the failure by making the rubber brittle.[1]

From the above examples one can conclude that the impact of product and system failures varies from minor inconvenience and costs to personal injury, significant economic loss, and death. Causes of these failures include bad engineering design, faulty construction or manufacturing processes, human error, poor maintenance, inadequate testing and inspection, improper use, and lack of protection against excessive environmental stress. Under current laws and recent court decisions, the manufacturer can be held liable for failing to account properly for product safety and reliability. Engineers responsible for product design must therefore include both reliability and maintainability as design criteria. The objective of this text is to introduce the technical manager and the engineer to the concepts, models, and analysis techniques that form the basis of reliability and maintainability engineering.

This, then, is a book on the failure and repair characteristics of systems, products, and their component parts. Reliability and maintainability engineering attempts to study, characterize, measure, and analyze the failure and repair of systems in order to improve their operational use by increasing their design life, eliminating or reducing the likelihood of failures and safety risks, and reducing downtime, thereby increasing available operating time. Closely associated with reliability and maintainability for systems or components that can be repaired or restored to an operating state once they have failed is the concept of availability. Availability measures the combined

[1]Details of these and other disasters may be found in the highly interesting book *When Technology Fails* [Schlager, 1994].

effect of both the failure and the repair process and is an important characteristic of the system.

1.1 THE STUDY OF RELIABILITY AND MAINTAINABILITY

As engineering disciplines, reliability and maintainability are relatively new. Their growth has been motivated by several factors, which include the increased complexity and sophistication of systems, public awareness of and insistence on product quality, new laws and regulations concerning product liability, government contractual requirements to meet reliability and maintainability performance specifications, and profit considerations resulting from the high cost of failures, their repairs, and warranty programs.

A Gallup poll conducted in 1985 for the American Society for Quality Control interviewed over 1000 individuals to determine what attributes were most important to them in selecting a product. The 10 attributes listed in Table 1.1 were ranked by each individual on a scale from 1 (least important) to 10 (most important); the average scores are as shown in the table. Obviously, both reliability and maintainability are important considerations in consumer purchasing.

Reliability and maintainability are not only an important part of the engineering design process but also necessary functions in life-cycle costing, cost benefit analysis, operational capability studies, repair and facility resourcing, inventory and spare parts requirement determinations, replacement decisions, and the establishment of preventive maintenance programs.

1.1.1 Reliability Improvement

A product has value as a result of its utility or performance in satisfying a need or requirement. Factors that contribute to a high value for a product are its versatility,

TABLE 1.1
Ten most important product attributes

Attribute	Average score
Performance	9.5
Lasts a long time (reliability)	**9.0**
Service	8.9
Easily repaired (maintainability)	**8.8**
Warranty	8.4
Easy to use	8.3
Appearance	7.7
Brand name	6.3
Packaging/display	5.8
Latest model	5.4

Source: *Quality Progress,* vol. 18 (Nov.), pp. 12–17, 1985.

ease of use, safety, aesthetics, and reliability. The primary reason for reliability and maintainability engineering is to improve the reliability and availability of the product or system being developed and thereby add to its value. During the initial design activity, this improvement can be achieved in several ways. For critical and high–failure rate components, redundancy or duplication of functions may be feasible. Designing excess strength into components or careful selection of material or parts will decrease the probability of failure. *Derating,* meaning operating the system below its rated stress level, provides an alternative means of achieving a desired reliability goal. For example, an electronic component may be designed to operate at 200 volts at a specified temperature but normal usage may dictate only 120 volts. Choice of technology, such as mechanical versus electronic switches or transistors versus integrated circuits, can have a significant effect on reliability. Reducing the complexity of the system, particularly as measured by the number of components or subassemblies, will also reduce the failure rate. As will be shown later, as the number of components in a system increases, the reliability of the components must be significantly increased in order to maintain a target system reliability. Once the limits of reliability improvement have been reached, further gain in product availability may be obtained by decreasing downtime through good maintainability design. To a large degree, then, reliability and maintainability must be addressed during system design, and they therefore become an inherent design feature of the system.

Reliability improvement, however, is not limited to the product design itself. For example, during initial product development an aggressive reliability growth program can play a major role in determining final product reliability. During manufacture a good quality control program will maintain product design reliability by ensuring conformance to production specifications and tolerances and by reducing variability in the manufacturing process. Inspection and acceptance sampling procedures ensure that raw material and supplier parts meet agreed standards. Once a product becomes operational, failures may be reduced through preventive maintenance, sound parts replacement policies, engineering modifications, and careful attention to environmental conditions and operating loads. Once the system is operational, downtime can be decreased (maintainability improved) with the proper amount of repair resources, including maintenance technicians, test equipment, and available spare parts. Secondary considerations such as skill levels, resupply lead times, maintenance training, and the ease of use of technical manuals will also improve maintainability. Reliability and maintainability engineering, therefore, must be practiced throughout the product's life cycle.

1.1.2 Random versus Deterministic Failure Phenomena

The traditional approach to safety in engineering is to design a high safety margin or safety factor into the product. This is a deterministic method in which a safety factor of perhaps 4 to 10 times the expected load or stress would be allowed for in the design. Safety factors often result in overdesign, thus increasing costs, or, less frequently, in underdesign, resulting in failure caused by an unanticipated load or a material weakness. On the other hand, the classic point of view taken in developing

reliability is to treat system and component failures as random, or probabilistic, occurrences. In theory, if we were able to comprehend the exact physics and chemistry of a failure process, many internal failures of a component could be predicted with certainty. In practice, however, with limited data on the physical state of a component and an incomplete knowledge of the physical and chemical (and perhaps biological) processes that cause failures, failures will appear to occur at random over time. Even failures caused by events external to the component, for example, environmental conditions such as hurricanes, earthquakes, or excessive heat or vibration, will appear to be random. However, if we had sufficient understanding of the conditions resulting in the event as well as the effect such an event would have on the component, then we would also be able to predict these failures deterministically. This uncertainty, or incomplete information, about a failure process is therefore a result of its complexity, imprecise measurements of the relevant physical constants and variables, and the indeterminate nature of certain future events.

This random process may exhibit a pattern that can be modeled by some probability distribution. Such phenomena are often observed in practice, especially when large numbers of components are involved. We are able to predict the failure (or nonfailure) behavior of these systems statistically.

A currently fashionable alternative view of reliability attempts to analyze the physics of the failure process and, through a mathematical model, determine the time to failure. This approach requires knowledge of the failure mechanisms and the basic causes of failures. Mean times to failure are determined on the basis of known or predicted stresses, environmental factors, operating conditions, material properties, and part geometries. We will return to the physics-of-failure approach later. The definitions and much of the development that follow are based on the probabilistic and statistical view of reliability.

1.2 CONCEPTS, TERMS, AND DEFINITIONS

Reliability *is defined to be the* ***probability*** *that a component or system will perform a required function for a given period of time when used under stated operating conditions.* It is the probability of a nonfailure over time. To determine reliability in an operational sense, the definition must be made specific. First, an unambiguous and observable description of a failure must be established. Failures should be defined relative to the function being performed by the system. Second, the unit of time must be identified. For example, the specified time interval may be based on calendar or clock time, operating hours, or cycles. A cycle, for example, may be the landing of an aircraft, a load reversal, or the turning on of an electric motor. In some cases reliability is not defined over time but over another measurement, such as miles traveled. For production systems failures may be defined in terms of units or batches produced. Third, the system should be observed under normal performance. This would include such factors as design loads (e.g., weight, voltages, pressure), environment (e.g., temperature, humidity, vibration, altitude), and operating conditions (e.g., use, storage, maintenance, transportation).

Maintainability *is defined to be the probability that a failed component or system will be restored or repaired to a specified condition within a period of time when maintenance is performed in accordance with prescribed procedures.* Maintainability is the probability of repair in a given time. Usually, when maintainability is computed, time is defined to be clock time (although it could, for example, be duty or shift time). It may or may not include such measures as waiting time for maintenance personnel and parts, travel time, and administrative time. Often, however, maintainability refers to the inherent repair time, which includes only the hands-on repair of the failed unit and not any administrative or resource delay times.

Prescribed maintenance procedures include not only the manner in which repair is to be performed but also the availability of maintenance resources (people, spare parts, tools, and manuals), the preventive maintenance program, skill levels of personnel, and the number of people assigned to the maintenance crew.

Availability *is defined as the probability that a component or system is performing its required function at a given point in time when used under stated operating conditions.* Availability may also be interpreted as the percentage of time a component or system is operating over a specified time interval or the percentage of components operating at a given time. As we will see later, availability can be mathematically defined in several different ways depending on how system uptime and downtime are measured. It differs from reliability in that availability is the probability that the component is currently in a nonfailure state even though it may have previously failed and been restored to its normal operating condition. Therefore system availability can never be less than system reliability. Availability may be the preferred measure when the system or component can be restored since it accounts for both failures (reliability) and repairs (maintainability). These definitions will become more precise in subsequent chapters when these concepts are defined mathematically.

Reliability versus quality

Reliability is closely associated with the quality of a product and is often considered a subset of quality. Quality can be defined qualitatively as the amount by which the product satisfies the users' (customers') requirements. Product quality is in part a function of design and conformance to design specifications. It also depends on the production system and on adherence to manufacturing procedures and tolerances. Quality is achieved through a good quality assurance program. Quality assurance is a planned set of processes and procedures necessary to achieve high product quality.

On the other hand, reliability is concerned with how long the product continues to function once it becomes operational. A poor-quality product will likely have poor reliability, and a high-quality product will have a high reliability. As we have seen, however, reliability may depend on external factors and not just the quality of the product itself. Nevertheless, reliability may be viewed as the quality of the product's operational performance over time, and as such it extends quality into the time domain.