RELIABILITY

1. Introduction

A chemical plant is a complex system comprising many interconnected engineered objects such as pumps, pipes, valves, pressure vessels, heat exchangers, control devices, and sensors. By and large, such objects perform satisfactorily, but occasionally they fail and this has an impact on the operation of the plant. In extreme cases when the failure is catastrophic (as, for example, an explosion in a chemical plant resulting in the release of toxic chemicals), the total economic damage and loss of life can be very dramatic, affecting society as a whole. A good example is the Bhopal disaster in India. For more on this and other similar cases, see Ref. 1.

Failures occur in an uncertain manner and are influenced by several factors such as design, manufacture or construction, maintenance, and operation. In addition, the human factor is important in this context.

All engineered objects are unreliable in the sense that they will fail sooner or later, even with the best design, construction, and operation. However, one can reduce the chance of a failure (within a specified time frame) through effective integration of good engineering with good management so that the failures and their consequences are minimized and the object can fulfill its intended purpose.

In this article, we discuss various topics from reliability theory to help engineers in the design, construction, and operation of chemical plants. In the chemical industry, one deals with material (which can be toxic) that needs to be stored and transported, in addition to operations to transform the material. We focus on the equipment needed for the transformation. The reliability of equipment depends on design, operation, and maintenance as well as on human operator and software needed for control. We do not look at human and software reliability issues in this article. The outline of the article is as follows. We start with a brief discussion of some basic concepts in Section 2. Section 3 deals with reliability science. The focus here is on the different mechanisms of degradation that can lead to failure. Section 4 looks at reliability analysis. This is important in both the design and the operation of chemical plants. A quantitative approach is critical for making reliability-related decisions during the design, construction, and operation phases. This involves building mathematical models at system and part levels and is the focus of Section 5. Section 6 deals with reliability engineering and looks at the tools and techniques needed for building reliable plants and operating them. Building in reliability is costly, but the implications of unreliability are costlier in the long run, which implies that reliability-related decisions must be made in the product lifecycle context and from an overall business viewpoint. This is discussed in Section 7. We conclude with an illustrative example in Section 8 to highlight some of the topics discussed earlier.

This article is based to a large extent on Blischke and Murthy (2). The relevant chapters of this book are indicated along with other books on reliability where additional details can be found.

2. Basic Concepts

In this section we introduce some basic concepts needed for a proper understanding of reliability.

2.1. Failure, Fault and Failure Mode.

There are many different definitions of *failure*. For example, according to Ref. 3, failure is the termination of the ability of an item to perform a required function. However, a more appropriate definition is as follows (4):

> It (failure) can be any incident or condition that causes an industrial plant, manufactured product, process, material, or service to degrade or become unsuitable or unable to perform its intended function or purpose safely, reliably, and cost effectively.

A *fault* is the state of an item characterized by its inability to perform its required function. Thus, a fault is a state resulting from a failure.

A *failure mode* is a description of a fault and is sometimes referred to as fault mode (3). The following is a classification scheme for failure modes (5):

1. *Intermittent failures*: Failures that last only for a short time.
2. *Extended failures*: Failures that continue until some corrective action rectifies the failure. They can be further divided into (a) *complete failures* (which result in total loss of function) and (b) *partial failures* (which result in partial loss of function).
3. *Sudden failures*: Failures that occur without any warning.
4. *Gradual failures*: Failures that occur with signals to warn of an impending failure.

2.2. Failure Cause and Severity. According to Ref. 5, *failure cause* is the set of circumstances during design, manufacture, or use that have led to a failure. Knowledge of the cause of failure is useful in the prevention of failures or their reoccurrence. A classification of failure causes is as follows:

1. *Design failure*: Due to inadequate design.
2. *Weakness failure*: Due to weakness (inherent or induced) in the system so that the system cannot withstand the stress it encounters in its normal environment.
3. *Manufacturing failure*: Due to nonconformity of item to design specifications during manufacturing.
4. *Aging failure*: Due to the effects of age and/or usage.
5. *Misuse failure*: Due to misuse of the system (operating in environments for which it was not designed).
6. *Mishandling failures*: Due to incorrect handling and/or lack of care and maintenance.

The *severity* of a failure mode indicates the impact of the failure mode on the system and on the outside environment. A severity ranking classification scheme (6) is as follows:

1. *Catastrophic*: Failures that result in death or total system loss.
2. *Critical*: Failures that result in severe injury or major system damage.
3. *Marginal*: Failures that result in minor injury or minor system damage.
4. *Negligible*: Failures that result in less than minor injury or system damage.

The following (7) is a classification of severity levels, in descending order of importance:

1. Failures with safety consequences.
2. Failures with environmental consequences.
3. Failures with operational consequences.
4. Failures with nonoperational consequences.

2.3. Deterioration. The deterioration process leading to a failure is a complicated process, and this varies with the type of object and the material used. The rate at which the deterioration occurs is a function of time and/or usage intensity.

2.4. Reliability. The reliability of a system conveys the concept of dependability, successful operation or performance, and the absence of failures. Unreliability (or lack of reliability) conveys the opposite. As the process of deterioration leading to failure occurs in an uncertain manner, the concept of reliability requires a dynamic and probabilistic framework. A more technical definition is as follows (Ref. 2, p. 18):

> The *reliability* of a system is the probability that the system will perform its intended function for a specified time period when operating under normal (or stated) environmental conditions.

2.5. Reliability Theory. Reliability theory deals with the interdisciplinary use of probability, statistics, and stochastic modeling, combined with engineering insights into the design and the scientific understanding of the failure mechanisms, to study the various aspects of reliability. As such, it encompasses topics such as (*1*) reliability science, (*2*) reliability modeling, (*3*) reliability analysis and optimization, (*4*) reliability engineering, (*5*) reliability technology, and (*6*) reliability management.

3. Reliability Science

Reliability science is concerned with the properties of materials and the causes for deterioration leading to part and component failures. It also deals with the effect of manufacturing processes (eg, casting, annealing) on the reliability of the part or component produced.

There are several different failure mechanisms, and most can be grouped into the following two categories: overstress failures and wear-out failures. We briefly describe a few from each category.

3.1. Overstress Failure Mechanisms. *Brittle Fracture.* In brittle materials (such as glass and ceramics), overstress can cause high stress concentrations to occur at local microscopic flaws. This excessive stress can cause a failure of the item as a result of sudden catastrophic propagation of the dominant micro-flaw. Failure is not only related to the applied stress on the component but also depends on the size of the flaw. A failure resulting from brittle fracture is also referred to as cracking. Brittle fractures typically occur as a result of nucleation and sudden propagation of cracks at preexisting microscopic flaws. The most common type of brittle fracture is a cleavage fracture, which occurs by direct separation along crystallographic planes and is due to tensile breaking of molecular bonds. For further details, see Ref. 8.

Ductile Fracture. In ductile fracture, the failure is due to sudden propagation of a preexisting crack in the material under external stress. It differs from brittle fracture in that in ductile fracture, there is large-scale yielding at the tip of the crack that precedes crack propagation. Ductile fracture is dominated by shear deformation and occurs by nucleation and coalescence of micro-voids due to pileups of dislocation at defects such as impurities and grain boundaries. For further details, see Ref. 9 and the references cited therein.

3.2. Wear-out Failure Mechanisms. *Corrosion and Stress Corrosion Cracking.* Corrosion is the process of chemical or electrochemical degradation of materials and is a very pervasive problem in the chemical industry. The three common forms of corrosion for ferrous material are as follows:

Uniform Corrosion. Here the reactions occurring at the metal–electrolyte interface are uniform over the surface of the item. Continuation of the process depends on the nature of the product and the environment. If the corrosion product is washed off or otherwise removed, fresh metal is exposed for further corrosion.

Galvanic Corrosion. This occurs when two different metals are in contact. In this case, one metal acts as a cathode (where a reduction reaction occurs) and the other acts as an anode (where corrosion occurs as a result of oxidation).

Pitting Corrosion. In this case, the reaction occurs at localized areas and results in the formation of pits. The corrosive conditions inside the pit accelerate the corrosion process.

Stress corrosion cracking is an interaction between the mechanisms of fracture (eg, resulting from fatigue) and corrosion. It occurs as a result of the simultaneous action of mechanical stress and corrosion. The corrosion process reduces the fracture strength of the material. The process is synergistic—each process assisting the other in leading to item failure.

Wear. Wear is the erosion of material resulting from the sliding motion of two surfaces that are in contact. Erosion is a result of physical and/or chemical interactions between the two surfaces. The various microscopic physical processes, by which the particles are removed as wear debris, are called wear mechanisms. The discipline dealing with the study of this phenomenon is called tribology.

Wear mechanisms can be broadly classified into five categories—adhesive, abrasive (when a hard material is sliding against a soft material), surface-fatigue, corrosive, and thermal. Wear erosion can be uniform or nonuniform. For further details, see Ref. 10 and the references cited therein.

Other Mechanisms. There are many other failure mechanisms, and these can be found in Ref. 2, pp. 170–175.

4. Reliability Analysis

Reliability analysis can be divided into two broad categories: (*1*) qualitative and (*2*) quantitative. The former is intended to verify the various failure modes and causes that contribute to the unreliability of a product or system. The latter uses real failure data in conjunction with suitable mathematical models to produce quantitative estimates of product or system reliability.

4.1. Qualitative Analysis. A key element of reliability analysis is the linking of component failures to system failures. There are two approaches to this: the *forward* (or bottom-up) approach and the *backward* (or top-down) approach.

In the forward approach, one starts with failure events at the part level and then proceeds forward to the system level to evaluate the consequences of such failures on system performance. *Failure mode and effects analysis* (FMEA) uses this approach. In the backward approach, one starts at the system level and then proceeds downward to the part level to link system performance to failures at the part level. *Fault tree analysis* (FTA) uses this approach.

4.2. Failure Mode, Effects, and Criticality Analysis. According to Ref. 11, the objectives of FMEA are as follows:

1. Assist in selecting design alternatives with high reliability and high safety potential during the early design phase.
2. Ensure that all conceivable failure modes and their effects on operational success of the system have been considered.
3. List potential failures, and identify the magnitude of their effects.

4. Develop early criteria for test planning and the design of the test and checkout systems.
5. Provide a basis for quantitative reliability and availability analysis.
6. Provide historical documentation for future reference to aid in the analysis of field failures and consideration of design changes.
7. Provide input data for tradeoff studies.
8. Provide a basis for establishing corrective action priorities.
9. Assist in the objective evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, and automatic and manual override.

FMEA involves reviewing a system in terms of its subsystems, assemblies, and so on, down to the part level, to identify failure modes and causes and the effects of such failures. According to Ref. 11, the basic questions to be answered by FMEA are as follows:

1. How can each part conceivably fail?
2. What mechanisms might produce these modes of failure?
3. What could the effects be if the failures did occur?
4. How is the failure detected?
5. What inherent provisions are provided in the design to compensate for the failure?

For each component at the part level, the failure modes and their effects are usually documented on worksheets. The documentation involves the following:

A) Description of the different parts. This is done through
 - A proper reference number
 - The intended function of the part
 - The normal operational mode

B) Characterization of failure. This involves
 - Listing the different possible failure modes
 - Failure mechanisms responsible for the different failure modes
 - The various means of detecting the different failure modes

C) Effect of failure on
 - Other components of the system
 - System performance

 If, in addition to FMEA, a criticality analysis is carried out, the process is called a *failure mode, effects, and criticality analysis* (FMECA). In this case, in addition to A)–C) of FMEA, the procedure involves documentation of the following:

D) Severity ranking, which characterizes the degree of the consequence of each failure.

FMECA is usually carried out during the design phase. The objective is to reveal weaknesses and potential failures, which enables the design engineer to make appropriate modifications that may reduce the likelihood of failures and/or the seriousness of their consequences.

4.3. Fault Tree Analysis.

A fault tree is a logic diagram that displays the relationship between a potential event affecting system performance and the reasons or underlying causes for this event. The reason may be failures (primary or secondary) of one or more components of the system, environmental conditions, human errors, and other factors. In this section, we focus on qualitative fault tree analysis.

The values of a fault tree (12) are as follows:

1. Directing the analysis to ferret out failures.
2. Pointing out the aspects of the system important to the failure of interest.
3. Providing a graphical aid to those in systems management who are removed from design changes.
4. Providing options for qualitative and quantitative systems reliability analysis.
5. Allowing the analyst to concentrate on one particular system failure at a time.
6. Providing an insight into system behavior.

A fault tree illustrates the state of the system (denoted the TOP event) in terms of the states (working/failed) of the system's components (denoted basic events). The connections are done using *gates*, where the output from a gate is determined by the inputs to it. A special set of symbols is used for this purpose; these will be discussed later.

A fault tree analysis involves the following steps:

1. Definition of the TOP event.
2. Construction of the fault tree.
3. Qualitative and, if desired, quantitative analysis of the fault tree.

4.4. Reliability Block Diagram (RBD).

System failure can be represented by a block diagram representation involving the components of the system and their interconnections. This type of representation is also referred to as a network representation.

5. Reliability Modeling

Reliability modeling deals with model building for use in analysis of problems in predicting, estimating, and optimizing the survival or performance of an unreliable system, the impact of the unreliability, and actions to mitigate this impact.

A system, in general, can be decomposed into many different levels. An eight-level decomposition is given in Ref. 2, p. 5, where the system is at the top and components are at the bottom. The model relates system failure to component failures. As such, the process begins with the modeling of component failures. When a new component is put into operation, it is in a working state and the state changes when the part fails after a certain length of time (called time to first failure). For a nonrepairable component, we need to consider only the first failure. For repairable components, it is necessary to differentiate first failure from subsequent failures, because the latter depend on the type of repair action taken. The failure of a component can be characterized in many ways, corresponding to the many different mathematical formulations that may be used in modeling failures.

There are two basic approaches to modeling failures, the “black-box” approach and the “white box” approach. In the “black-box” approach, one models the uncertainty in the time to failure without directly considering the mechanisms responsible for failure. In contrast, in the “white-box” approach, the failure is characterized in terms of the underlying failure mechanism.

We first consider modeling failures at the component level and then look at the system level.

5.1. Component-Level Modeling.

Black-box Approach. *First Failure.* The time to first failure X is a random variable that can assume values in the interval $[0,\infty)$. It can be described through a distribution function $F(x;\theta)$ that characterizes the probability $P\{X \leq x\}$ and is defined as

$$F(x;\theta) = P\{X \leq x\}, \quad 0 \leq x < \infty \tag{1}$$

$F(x;\theta)$ is a nondecreasing function with $F(0;\theta) = 0$ and $F(\infty;\theta) = 1$. θ denotes the parameter set of the distribution function.

The *density function* associated with the distribution function $F(x;\theta)$ (if F is differentiable) is given by

$$f(x;\theta) = \frac{F(x;\theta)}{dx} \tag{2}$$

The *survivor function* $S(x;\theta)$ [and often denoted $\bar{F}(x;\theta)$] characterizes the probability that the component will not fail before it reaches an age x. It is also often called the *reliability* of the item and is related to $F(x;\theta)$ by

$$S(x;\theta) = P\{X > x\} = 1 - P\{X \leq x\} = 1 - F(x;\theta) \tag{3}$$

The conditional probability that the item will fail in the interval $[x, x + t)$ given that it has not failed prior to x is given by

$$F(t|x;\theta) = \frac{F(t + x;\theta) - F(x;\theta)}{1 - F(x;\theta)} \tag{4}$$

The *failure rate function* (or *hazard function*) $r(x;\theta)$ associated with $F(x;\theta)$ is defined as

$$r(x;\theta) = \lim_{t \to 0} \frac{F(t|x;\theta)}{t} = \frac{f(x;\theta)}{1 - F(x;\theta)} \tag{5}$$

The failure function can be interpreted as the probability that the component will fail in $[x, x + \delta x)$ given that it has not failed prior to x. In other words, it characterizes the effect of age on item failure more explicitly than $F(x;\theta)$ or $f(x;\theta)$.

Many different types of distributions have been proposed for modeling component failures. One of the most commonly used is as follows:

Weibull Distribution. The two-parameter Weibull distribution function is given by

$$F(x;\theta) = 1 - e^{-(x/\beta)^{\alpha}} \tag{6}$$

The parameter set is $\theta \equiv \{\alpha, \beta\}$ with $\alpha > 0$ and $\beta > 0$. The failure density and failure rate functions are given by

$$f(x;\theta) = \frac{\alpha x^{(\alpha-1)} e^{-(x/\beta)^{\alpha}}}{\beta^{\alpha}} \tag{7}$$

and

$$r(x;\theta) = \frac{\alpha x^{(\alpha-1)}}{\beta^{\alpha}} \tag{8}$$

β is called the scale parameter, and α is called the shape parameter, as the shape of the distribution changes significantly as α varies. (See Ref. 2, p. 107.) As a result, the Weibull distribution may be used to model many failure patterns and it is widely used in practice.

Bathtub Failure Rate. The bathtub failure rate is of special significance in modeling item failures. The shape of the failure rate is characterized by three regions, defined by boundaries x_1 and x_2. In the first region $(0 \le x < x_1)$, the failure rate is decreasing; in the second region $(x_1 \le x < x_2)$, it is roughly constant; and in the third region $(x_2 \le x < \infty)$, it is increasing. The first region corresponds to infant mortality where failures occur due to poor manufacturing. The failures in the second region are purely chance and age has no effect (as the failure rate is essentially constant). Finally, failures in the third region are due to the effect of aging.

Modeling Process. The modeling process begins with a preliminary analysis of data. Typical data consist of failure times for items that have failed and censored times (ages) of items that have not failed. The data are used to (*1*) decide on the most appropriate failure distribution and (*2*) estimate the numerical values to be assigned to the model parameters. This has received a great deal of attention—see Ref. 2, Chapter 11; Ref. 13; and Ref. 14.

White-box Approach. The modeling of failures based on the white-box approach requires modeling the physical mechanisms leading to the failure. The models used for this purpose involve a probabilistic construct called a *stochastic process*.

Modeling Failures Over Time. When a repairable component fails, it can either be repaired or replaced by a new component. In the case of a nonrepairable component, the only option is to replace the failed component by a new item.

Repairable Components. Often when a new component fails, it can be made operational through repair if the component is repairable. There are different types of repairs (Ref. 2, pp. 187–188). With *minimal* repair, the failure rate after repair is the same as the failure rate of the item immediately before it failed. With *imperfect* repair, the failure rate after repair is better than that just before failure but not as good as that for a new component.

With minimal repair (and the repair time negligible in relation to the mean time between failures), failures over time occur according to a *nonstationary Poisson process* (13). The mean number of failures over $[0,t)$, is given by

$$E[N(t)] = \Lambda(t) = \int_0^t r(x)\,dx \tag{9}$$

Nonrepairable Components. In the case of a nonrepairable component, every failure results in the replacement of the failed component by a new item. If the time to replace a failed component by a new one is small relative to the mean time to failure, then it can be ignored. In this case, the number of failures (replacements) over time is given by a *renewal process* and the mean number of failures over $[0,t)$ is given by the *renewal integral equation*:

$$M(t) = F(t) + \int_0^t M(t-x)\,dF(x) \tag{10}$$

In most cases, it is difficult to obtain an analytical expression for $M(t)$ and computational approaches are used to evaluate it. (See Ref. 2, Appendix B.)

Modeling Environmental Effects. The stress (voltage, force, temperature, etc) on a component affects the time to failure and hence the failure distribution of the lifetime of the component. The effect of increasing stress is to accelerate the time to failure. Many different models have been developed to model this effect.

Arrhenius Life-Temperature Relationship. According to the Arrhenius rate law, the rate at which chemical reactions occur is a function of the absolute temperature T and is given by

$$\text{rate} = A\,e^{-(b/T)} \tag{11}$$

where A is a constant that is characteristic of the item failure mechanism and $b = E/k$, where E is the activation energy of the reaction and k is Boltzman's constant. As a result, as T increases, the rate of reaction increases and hence hastens the time to failure.

Inverse Power Law. The underlying basis of the relationship called the Inverse Power Law is similar to the Arrhenius model, except that here the stress variable, say V, can represent any kind of stress rather than only temperature. The time to failure is modeled by $X \propto (1/V)^{\gamma}$, where γ is a constant.

Proportional Hazard Models. The failure times of repairable items are affected by several factors. These can be grouped into the following three categories:

1. Operating environment (temperature, pressure, humidity, vibration, dust, etc).
2. Operating history (failure repairs, preventive maintenance).
3. Design (selection of material) and manufacturing.

To take these factors into account, the failure rate of an item can be modeled as

$$\lambda(t; z) = \lambda_0(t)\psi(z; \beta) \tag{12}$$

where $\lambda_0(t)$, called the baseline failure rate, is dependent only on time and $\psi(z; \beta)$ is a functional term that is independent of time but incorporates the effects of the different factors that affect item failure through a row vector z (called the covariates) and a column vector β of parameters that characterize the effect of z. Various forms of $\psi(z; \beta)$ have been proposed. One of these is $\psi(z; \beta) = e^{z\beta}$. For more details, see Refs. 15 and 16.

5.2. System-Level Modeling. *Black-box Approach.* Failures over time are modeled by a point process with intensity function $\Lambda(t; \theta)$, with t representing the age of the system. $\Lambda(t; \theta)$ is an increasing function of t, reflecting the effect of age. One form of $\Lambda(t; \theta)$ is the Weibull intensity function given by

$$\Lambda(t; \theta) = \alpha\beta(\beta t)^{(\alpha-1)} \tag{13}$$

with $\alpha > 1$ and $\beta > 0$.

White-box Approach. In the white-box approach, system failure is modeled in terms of the failures of the components of the system. For more details, see Ref. 17.

6. Reliability Engineering

Reliability engineering deals with the design and construction of a system taking into account the unreliability of its components. It also includes testing and programs to improve reliability. Good engineering results in a more reliable end product.

Engineering requires judgment in order to adapt scientific knowledge to produce new systems that meet stated requirements in terms of technical performance and commercial constraints. The engineering process to achieve this involves the following three phases:

- Design and development.
- Construction.
- Pre-sale (pre-delivery) assurance.

In the context of the engineering process, reliability engineering focuses on the prevention, detection, and correction of reliability design deficiencies, weak parts, workmanship defects, and so forth. It is an integral part of the design process, including design changes. The process through which reliability engineering contributes to design, construction, and assurance is called the *reliability process*.

6.1. Design.

The design phase involves first defining reliability performance targets, taking into account the fact that building in reliability is costly but the consequence of unreliability is, in general, costlier. The design process involves deriving specifications (physical dimensions, material selection, etc) at the component level to ensure that reliability performance targets are achieved at the system level. This involves tradeoff studies, mathematical and simulation models, and cost analysis.

A major part of the design process is to minimize the potential effects of failures, and this involves fault tree and FMECA analysis. If at this stage the reliability of a component is found to be below a given target value, there are several options. These options are as follows:

1. *Development*: The development process involves testing components to failure, carrying out a root cause analysis for the failure, and then implementing design changes to eliminate the failure mode and thereby improve component reliability.
2. *Redundancy*: This involves replication of a component, resulting in a module of identical components. The reliability of the module will be greater than that of the individual components.
3. *Preventive maintenance*: Here a component is replaced before it fails based on its age, usage, or condition, thus ensuring that the reliability does not fall below the target value.

6.2. Testing.

Testing can be done by application of some form of stimulation to a system (or subsystem, module, or part), measuring the performance of the item in this environment, and comparing the results to design requirements. Testing is carried out during the development, construction, and operational phases.

The following types of testing are often done during the development phase:

1. *Testing to failure*: The test involves subjecting the item to increasing levels of stress until a failure occurs. Each failure is analyzed and fixed.
2. *Environmental and design limit testing*: This involves testing under worst-case operating conditions of temperature, shock, vibration, and so forth.
3. *Accelerated life testing*: This involves putting items on test under environmental conditions that are more severe than those normally encountered so as to hasten the failure and shorten the time required for testing.
4. *Critical item evaluation and part qualification testing*: The purpose of these tests is to verify that a part is suitable under the most severe conditions encountered under normal use.

The purpose of testing during manufacturing is to eliminate manufacturing defects and early part failures. Two types of testing commonly used are as follows:

1. *Environmental Stress Screening (ESS)*: Involves temperature cycling, random vibrations, electrical stress, thermal stress, and so on.
2. *Burn-in*: A process used to weed out early failures that result because of the high initial failure rate from manufacturing defects.

6.3. Maintenance.

As mentioned in Section 1, equipment degrades with age and usage and ultimately fails, even with the best design, construction, and operation. Maintenance involves actions to control or reduce equipment degradation (called *Preventive Maintenance* or PM) or to restore failed equipment to an operational state (called *Corrective Maintenance* or CM).

Both preventive and corrective maintenance have associated costs. CM costs include the direct costs of restoring the failed equipment to an operational state as well as indirect costs such as loss of production, opportunity loss due to customer dissatisfaction, and penalties and compensation when public safety is compromised. As the level of PM effort increases, the PM costs increase and the CM costs decrease. In *Reliability Centered Maintenance* (RCM), the maintenance level for each component is determined by taking into account its inherent reliability and the resulting consequence should it fail. For more on this, see Ref. 7.

7. Reliability Management

Reliability management deals with the various issues that must be considered in managing the design, construction, and/or operation of reliable systems. Here the emphasis is on the business viewpoint, as unreliability has consequences in cost, time wasted, and in certain cases, the welfare of an individual or society. To perform effectively, management must be done using a product lifecycle approach.

7.1. Product Lifecycle.

For reliability management purposes, the lifecycle of a product as defined in Ref. 18 consists of the following five phases:

1. Concept.
2. Design and development.
3. Manufacture (and installation, if relevant).
4. Operation and maintenance.
5. Conversion (or upgrade) or decommission (scrap).

Reliability-related decisions need to be made at each phase from an overall business perspective. Lifecycle cost is an important issue in this context.

7.2. Lifecycle Cost.

The lifecycle cost (LCC) is the total cost of owning, operating, maintaining, and finally discarding the product. Figure 1 is a simplified lifecycle cost model and shows the key elements. For further discussion on LCC and more detailed models, see Ref. 2, p. 442, and Ref. 19.

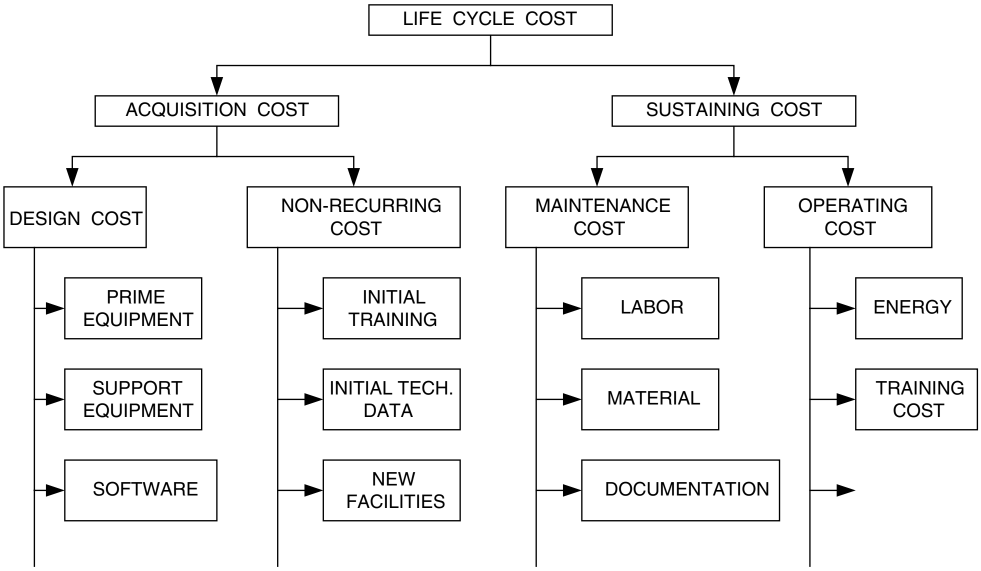

Fig. 1. Lifecycle cost [simplified version].

7.3. Reliability Programs. The reliability of a system is influenced by activities such as design, material selection, manufacturing, quality control, and testing. A reliability program provides a framework for a systematic approach to definition and management of the various reliability-related tasks. It includes a comprehensive list of activities that are considered to be essential to the success of the system. It further contains a description of each task and an assignment of responsibility and accountability. Reliability programs deal with reliability strategies at the functional as well as the operational levels.

There are many different standards for reliability programs. Reliability programs are influenced by the policies and practices of the company, the system being developed, and regulations and guidelines established by government and other organizations. Some well-known standards are as follows:

ISO Standards. The International Standards Organization [ISO] 9000 series (20) deals with standards for quality. Of relevance to reliability and maintainability is ISO 9000-4, Guide to Dependability Program. This defines dependability as the collective term used to describe availability performance and its influencing factors: reliability performance, maintainability performance, and maintenance support performance.

IEC Standards. The International Electrotechnical Commission [IEC] Technical Committee 56 (21) deals with dependability issues. The IEC 300 series deals with dependability issues and has links with the ISO 9000 series.

For other programs and standards, see Ref. 2, pp. 697–703. In the process industry, safety and risks are important issues that need to be managed effectively. For more on this, see Refs. 22 and 23.

7.4. Reliability Data Collection and Analysis. Various kinds of data need to be collected for effective management of reliability. These data are as follows:

- *Inventory data*: Relevant design information for each component.
- *Operational data*: Operating and maintenance history for each component.
- *Event data*: Failure events and relevant associated data.

For a general discussion of reliability data collection, see Ref. 24. See Refs. 25 and 26 for a discussion of data collection in the process industry.

Proper data collection allows for continuous improvement. In this context, root cause analysis is used extensively in reliability engineering to make design changes to improve component reliability and for better management of risks.

8. Illustrative Example [Ammonia Plant]

The following example highlights some of the concepts and issues discussed in this article.

8.1. Background. The Ammonia plant produces ammonia with coal as input. A simplified description of the process is as follows. The coal is pulverized and passed into a gasifier where it is mixed with oxygen and steam and burned. This produces raw synthesis gas (syngas—a mixture of carbon monoxide (CO), hydrogen (H_2), carbon dioxide (CO_2), and some impurities). The gas is cleaned to rid it of impurities and is compressed. It is heated to a high temperature in the synthesis unit to produce ammonia gas and chilled before being fed to storage units.

A reliability block diagram of the main subsystems of the ammonia plant is shown in Figure 2. Several other auxiliary subsystems (for example, to generate steam, oxygen) are not shown in the figure. It is apparent from the RBD of the ammonia plant that the plant is operational only if all subsystems are operational.

8.2. Some Failure Modes and Causes. Process shutdown valves are used in the ammonia plant to control the flow of fluids. Failure modes for a process shutdown valve with a spring-loaded hydraulic actuator are given in Ref. 27. The valve has four different operational modes—two of these are two stable states, and the other two are transition states between the two stable ones. There are several failure modes as indicated in Table 1.

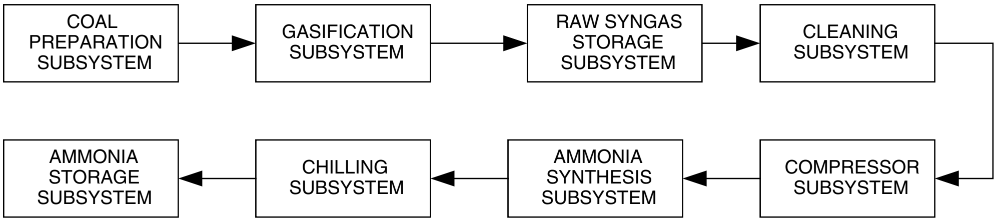
COAL PREPARATION SUBSYSTEM
GASIFICATION SUBSYSTEM
RAW SYNGAS STORAGE SUBSYSTEM
CLEANING SUBSYSTEM
COMPRESSOR SUBSYSTEM
AMMONIA SYNTHESIS SUBSYSTEM
CHILLING SUBSYSTEM
AMMONIA STORAGE SUBSYSTEM

Fig. 2. Ammonia plant (block diagram of main subsystems).

Table 1. **Operational and Failure Modes for Process Shutdown Valve**

Operational modes	Failure modes
Close flow (Transition state)	not closing at all
	not closing completely
	closing too slowly
	closing too fast
Keep flow closed (Stable state)	opening spuriously
	internal leakage
	external leakage
Open flow (Transition state)	not opening at all
	not opening completely
	opening too slowly
	opening too fast
Keep flow open (Stable state)	closing spuriously
	external leakage
	plugged

Some of the failure causes for the process shutdown valve are as follows:

- Excessive wear resulting from improper material selection (design failure).
- Usage outside specification limits (misuse failure).
- Inadequate lubrication due to poor maintenance (mishandling failure).
- Incorrect installation (mishandling failure).

8.3. Fault Tree Analysis. All eight subsystems (shown in Figure 2) and some auxiliary subsystems need to be in their operational state for the plant to be operational, and the plant shuts down should one of these subsystems fail. One way of reducing the likelihood of plant shutdown is through redundancy. Figure 3 shows the fault tree diagram with two compressors instead of one where the plant shutdown (due to compressor subsystem failure) occurs only when both compressors fail.

8.4. Design Considerations. The design of a plant is a highly complex process. We list only a few aspects to illustrate the role of reliability in this process.

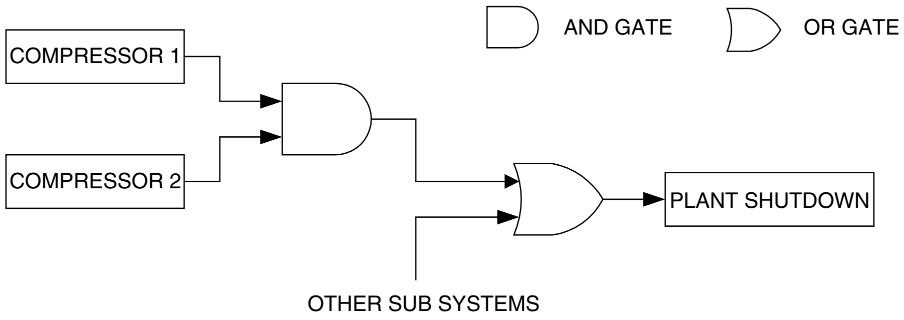

Fig. 3. Partial fault tree diagram.

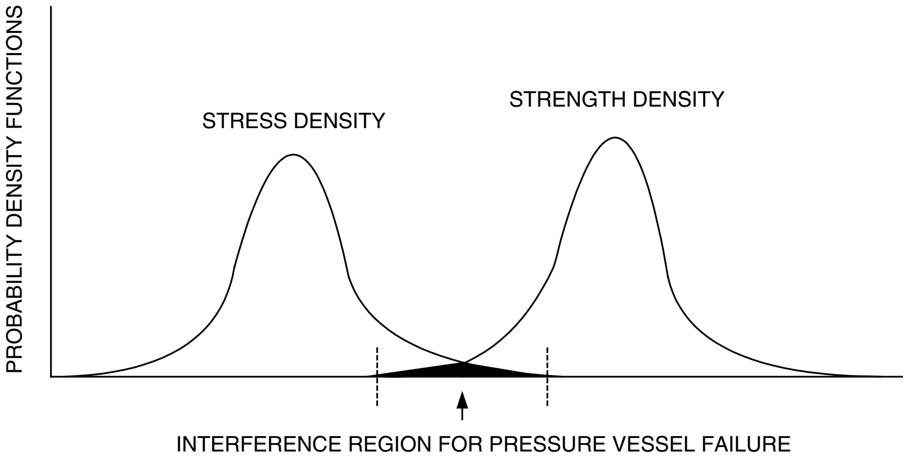
PROBABILITY DENSITY FUNCTIONS
STRESS DENSITY
STRENGTH DENSITY
INTERFERENCE REGION FOR PRESSURE VESSEL FAILURE

Fig. 4. Stress-strength interference diagram.

The shell of the pressure vessel in the ammonia synthesis unit must be of sufficient strength to withstand the maximum pressure (stress) to which it will be subjected. The strength of the shell depends on its thickness. Due to variations in stress and strength, there is a possibility that the strength will be less than the stress (see Figure 4); in which case, the vessel ruptures. The area of overlap of the stress and strength distributions shown in Figure 4 (called the *interference region*) plays an important role in determining the probability that the vessel ruptures. The modeling and analysis to calculate this probability can be found in Ref. 2. A decision problem during design is to assure that the strength is such that the probability of rupture is below some prespecified value (for example, 10^{-8}).

The strength of the vessel will decrease with time and operation due to wear (because of erosion and corrosion), and failure occurs when the strength of the vessel wall falls below an experienced stress.

For some components, redundancy can be used to increase reliability. Suppose, for example, that the plant is to be designed so that the probability of a shutdown occurring in a year is less than 0.0001, and that to achieve this the compressor subsystem must have a reliability of 0.99999 (or unreliability 0.00001). If the reliability of a compressor unit is only 0.999 (or unreliability 0.001), then having two connected in parallel (a configuration called *active hot standby*) will ensure the desired reliability.

8.5. Data Considerations.

Again, we look at only a few aspects of the enormous data requirements in the design, construction, and operation of the plant.

For the centrifugal pumps used in the ammonia plant, the data to be collected are as follows:

Inventory Data

- *Identification parameters*: Tag number, generic class, location, function, etc.
- *Manufacturing and design parameters*: Manufacturer, model/size, date of manufacture, design code, installation code, etc.

- *Maintenance and test parameters*: Recommended maintenance schedule and frequency and test schedule and frequency.
- *Engineering and process parameters*: Materials, components, speed, pressure, flow, temperature, process fluid, etc.

Operational Data

- Date of installation.
- Cumulative time of operation.
- Incidents of unavailability due to maintenance/test/failure/modification/replacement.
- Incidents and duration of standby mode.
- Cycle numbers, if used intermittently.

Event Data

- *Failure*: Mode/Cause/Consequences/How discovered.
- *Modification*: Reason.
- *Replacement*: Reason.

BIBLIOGRAPHY

1. K. A. Esaklul, ed., *Handbook of Case Histories in Failure Analysis*, Vols. 1 and 2, ASM International, Materials Park, Ohio, 1999.
2. W. R. Blischke and D. N. P. Murthy, *Reliability*, Wiley, New York, 2000.
3. IEC 50 (191), *International Electrotechnical Vocabulary* (IEV), Chapter 191—Dependability and Quality of Service, International Electrotechnical Commission, Geneva, 1990.
4. C. E. Witherell, *Mechanical Failure Avoidance*, McGraw Hill, New York, 1994.
5. K. M. Blache and A. B. Shrivastava, Defining failure of manufacturing machinery and equipment, *1994 Proceedings Annual Reliability and Maintainability Symposium*, 1994, pp. 69–75.
6. MIL-STD 882, *System Safety Program Requirement,* U.S. Dept. of Defense, Washington, D.C., 1984.
7. J. Moubray, *Reliability Centred Maintenance*, Butterworth-Hinemann, Oxford, U.K., 1991.
8. A. Dasgupta and J. M. Hu, Failure mechanism models for brittle fracture, *IEEE Trans. Reliability* **41**, 328–337 (1992).
9. A. Dasgupta and J. M. Hu, Failure models for ductile fracture, *IEEE Trans. Reliability* **41**, 489–495 (1992).
10. P. Engel, Mechanical failure mechanism models for mechanical wear, *IEEE Trans. Reliability* **42**, 262–267 (1993).
11. IEEE Std 352-1982, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems*.
12. J. B. Fussell, Nuclear power system reliability: A historical perspective, *IEEE Trans. Reliability* **33**, 41–47 (1994).
13. D. N. P. Murthy, M. Xie, and R. Jiang, *Weibull Models*, Wiley, New York, 2003.

14. W. Q. Meeker and L. A. Escobar, *Statistical Methods for Reliability Data*, Wiley, New York, 1998.
15. D. Kumar and B. Klefsjo, Proportional hazards model: A review, *Reliability Eng. Syst. Safety* **44**, 177–188 (1994).
16. D. Oakes, Survival analysis, *Eur. J. Oper. Res.* **12**, 3–14 (1983).
17. A. Hoyland and M. Rausand, *System Reliability Theory*, Wiley, New York, 1994.
18. SAE M-110, *Reliability and Maintainability Guideline for Manufacturing Machinery and Equipment*, Society of Automotive Engineers, 1993.
19. B. S. Blanchard, *Logistic Engineering and Management*, Prentice Hall, Englewood Cliffs, N.J., 1981.
20. ISO 9000 International Standard, *Quality Management and Quality Assurance Standards*, International Standards Organization.
21. IEC Standards, International Electrotechnical Commission, Geneva.
22. E. Pate-Cornell, Probabilistic risk analysis and safety regulation in the chemical industry, *J. Hazardous Mater.* **15**, 97–122 (1987).
23. M. Tweeddale, *Managing Risk and Reliability of Process Plants*, Gulf Professional Pub, Burlington, Mass., 2003.
24. A. G. Cannon and A. Bendell, eds., *Reliability Data Banks*, Elsevier Applied Science, London, 1991.
25. L. J. B. Koehorst and P. Bockholts, FACTS: Most comprehensive information system for industrial safety, in A. G. Cannon and A. Bendell, eds., *Reliability Data Banks*, Elsevier Applied Science, London, 1991.
26. H. J. Wingender, Reliability data collection in process plants, in A. G. Cannon and A. Bendell, eds., *Reliability Data Banks*, Elsevier Applied Science, London, 1991.
27. M. Rausand and K. Oien, The basic concepts of failure analysis, *Reliability Eng. Syst. Safety* **53**, 73–83 (1996).

D. N. Prabhakar Murthy
The University of Queensland

Wallace R. Blischke
University of Southern California (Emeritus)