4

An Introduction to Reliability Theory

4.1 Introduction

The study of reliability specification and performance requires a thorough understanding of many different concepts from reliability theory. Reliability theory deals with the interdisciplinary use of probability, statistics, and stochastic modelling, combined with engineering insights into the design and the scientific understanding of the failure mechanisms, to study the various aspects of reliability. It encompasses issues such as:

- Reliability modelling
- Reliability analysis and optimization
- Reliability engineering
- Reliability science
- Reliability technology
- Reliability management

In this chapter we briefly discuss these concepts that will be used in later chapters of the book. For readers who are familiar with reliability theory this chapter serves as a review chapter. For readers who are not familiar with reliability theory, we indicate references where they can get more details of the topic under consideration. The two references that are cited often are Blischke and Murthy (2000) and Rausand and Høyland (2004). Other references are indicated as and when appropriate.

The outline of the chapter is as follows: Section 4.1 defines basic concepts of reliability, like functions, failures, and failure modes and effects. Section 4.2 introduces reliability measures and lifetime models with focus on the exponential and Weibull models. System modelling by means of reliability block diagrams and fault tree analysis is outlined. How to incorporate environmental effects into life models, for example, by using proportional hazards models is also briefly discussed. Section 4.5 deals with modelling of repairable systems with both corrective and preventive maintenance strategies. Qualitative and quantitative reliability analyses are presented in Section 4.6 and reliability engineering issues are discussed in Section 4.7 with a special focus on reliability allocation and reliability growth. Sections 4.8 and 4.9

present a brief introduction to reliability prediction and to reliability management issues. The chapter concludes in Section 4.10 with a case study on cellular phones.

In the rest of this chapter we will use the term *item* to denote any physical entity, be it a large system or a small component.

4.2 Basic Concepts

In Section 1.3.1 we presented the definition of reliability from IEC 60050-191. The concept of reliability is related to one or more product functions that are required or wanted. Some functions are very important, while others may be of the category "nice to have". When we use the term reliability, we should always specify the required functions. The reliability of a product is dependent on the environmental and operational conditions during the product's post-production phase. These conditions have to be properly understood and assessed in order to develop a reliable product.

4.2.1 Product Functions

The key term in the definition of reliability is the ability of the item to perform a required *function*. The different functions of a complex item may be classified as follows (Rausand and Høyland, 2004).

Essential functions: These functions are the intended or primary functions, and may be considered as the reason why the item has been developed. The essential function of a pump is, for example, to pump fluid.

Auxiliary functions: These functions are required to support the essential function. An auxiliary function of a pump is, for example, to contain the fluid and prevent leakage to the environment.

Protective functions: These functions are intended to protect people, material assets, and the environment from damage, negative health effects, and injury.

Information functions: These functions give information from condition monitoring gauges, alarms, and so on.

Interface functions: These functions are related to the interfaces between the item considered and other items.

Superfluous functions: In some cases an item may have functions that are never used. This is sometimes the case with electronic equipment that has a wide range of "nice-to-have" functions that are often not necessary. In some cases, failure of a superfluous function may cause failure of a required function.

4.2.2 Failure and Related Concepts

Failure

A failure occurs when the item is not able to perform one or more of its required functions. Two definitions of failure are:

1. The termination of the ability of an item to perform a required function (IEC 60050-191).
2. Equipment fails if it is no longer able to carry out its intended function under the specified operational conditions for which it was designed (Nieuwhof, 1984).

Failures are events that occur in a random manner and are influenced by factors such as design, manufacture or construction, maintenance, and operation.

Fault

A fault is the state of the item characterized by its inability to perform its required functions.[1] A fault is hence a state resulting from a failure.

Failure Mode

A failure mode is a description of a fault, that is, how we can observe the fault. A failure mode is observed as a deviation from the accepted performance of a function.

Example 4.1. Consider a pump that is required to pump between 100 and 110 litres of water per minute. As long as the pumping rate is kept within these limits, its performance is acceptable. A failure occurs as soon as the output deviates from the acceptable performance. Relevant failure modes of the pump are therefore: (i) No output, (ii) too low pumping rate, i.e., $<$ 100 litres per minute, and (iii) too high pumping rate, i.e., $>$ 110 litres per minute. ⊕

Failure Cause

Failure cause is the circumstances during design, manufacture or use which have led to a failure (IEC 60050-191).

Knowledge about failure causes is useful information in order to prevent failures or their recurrence. A classification scheme for failure causes is as follows:

- Design Failure: Due to inadequate design.
- 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.
- Manufacturing failure: Due to non-conformity during manufacturing.
- Aging failure: Due to the effects of age and/or usage.
- Misuse failure: Due to incorrect handling and/or lack of care and maintenance, or due to operating in environments and for purposes for which it was not designed.

Failure Mechanisms

The physical, chemical or other processes that may lead to a failure (IEC 60050-191). Failure mechanisms are important failure causes.

[1] Note that this excludes situations arising from preventive maintenance or any other intended shutdown during which the system is unable to perform its required function(s).

Failure Classification

Blache and Shrivastava (1994) suggested the following classification scheme for failure modes:

- Intermittent failures: Failures that last only for a short time.
- Extended failures: Failures that continue until some corrective action rectifies the failure. They can be divided into the following two categories:
  - Complete failures that result in total loss of function.
  - Partial failures that result in partial loss of function.

  Each of these can be further sub-divided into the following:
  - Sudden failures: Failures that occur in a very short time and often with limited or no warning.
  - Gradual failures: Failures that occur with signals to warn of the occurrence of a failure if properly monitored.

A complete and sudden failure is called a catastrophic failure and a gradual and partial failure is designated a degraded failure.

The failure modes may also be classified according to their failure causes:

Primary failure: A primary failure is a failure caused by natural aging. The failure occurs under stresses and conditions foreseen during the design process. Primary failures can only be prevented by redesigning the physical item.

Secondary failure: A secondary failure is a failure caused by overstress, i.e., stress levels outside the design envelope of the item. These overstresses were not foreseen during design or may be due to deliberate misuse of the item. A secondary failure is also called an overstress failure. To prevent an overstress failure we need to reduce the possibility of excessive stresses (e.g., through better information to users) and/or to make the item more robust to overstress.

Command fault: A command fault is a failure caused by an improper control signal or noise. A command fault does not represent a physical failure of the item. The item is not able to perform a required function because of an erroneous or lacking input signal. When the signal is corrected, the item will be functioning again. A command fault is therefore usually an intermittent failure.

In some applications, it may be useful to classify failures into the two following types (e.g., see IEC 61508):

Random (hardware) failures: A random hardware failure is a failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.

Systematic failures: Systematic failures are due to errors in hardware or software, which under some particular combination of inputs or environmental conditions, will permit a failure. Corrective maintenance without modification will usually not eliminate the cause of a systematic failure.

Example 4.2 (Safety Instrumented System). A gas detector in a safety instrumented system that is not able to detect gas because an efficient ventilation system prevents

the gas from reaching the gas detector, has a systematic failure. The same applies to a flame detector that is not able to "see" a flame because the flame is hidden behind some temporary scaffolding. ⊕

Common Cause Failures

A common cause failure is a multiple component failure that occurs due to a common cause. Common cause failures may be classified in two main types:

1. Multiple failures that occur at the same time due to a common cause (e.g., an external shock)
2. Multiple failures that occur due to a common cause, but not necessarily at the same time

The common cause for type 2 may, for example, be higher than normal temperatures, humidity or vibrations. The time between the failures may in some cases be rather long.

Common cause failures are especially important for redundant components, for example, for multiple input elements in a safety instrumented system.

Consequences of Failures

When a failure occurs, no matter how benign, its impact is felt. Many different classifications have been proposed to indicate the severity of item failure. The following classification is adapted from Dhudshia (1992):

Level 5: Failure will result in major customer dissatisfaction and cause non-operation of the item or non-compliance with governmental regulations.
Level 4: Failure will result in high degree of customer dissatisfaction and cause non-functionality of the item.
Level 3: Failure will result in customer dissatisfaction and annoyance and/or deterioration of part or item performance.
Level 2: Failure will result in slight customer annoyance and/or slight deterioration of part or item performance.
Level 1: Failure is of such minor nature that the customer (internal or external) is probably unable to detect the failure.

A classification scheme that is often used in applications involving health, safety, and environment (HSE) aspects is the following:

Catastrophic: Failure that results in major injury or death of personnel.
Critical: Failure that results in minor injury to personnel, personnel exposure to harmful chemicals or radiation, or release of chemicals into the environment.
Major: Failure that results in a low level exposure to personnel, or activates a plant alarm system (for items used in such plants).
Minor: Failure that results in minor damage but does not cause injury to personnel, allow any kind of exposure to operational or service personnel or allow any release of chemicals into the environment.

4.2.3 Different Notions of Product Reliability

There are several different notions of reliability as indicated in Figure 4.1.

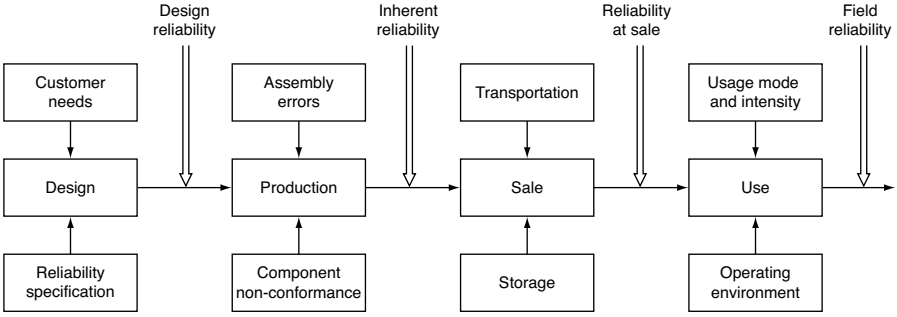

Figure 4.1. Different notions of product reliability

Design Reliability

The design reliability of a product is the predicted reliability performance of the product at the end of the design and development phase. The prediction may be based on field experience from similar products or parts thereof, testing of the product, expert judgement, and various types of analysis and testing. The prediction is based on nominal environmental and operational conditions used during the design process.

Inherent Reliability

The reliability of the products produced will tend to differ from the design reliability due to quality variations. The variations result from some of the components not conforming to the design specification and/or assembly errors. The reliability of produced items is often referred to as the inherent reliability.

Field Reliability

The reliability at sale depends on the inherent reliability and the effects of transportation and storage, as they can degrade the reliability. The field reliability is the reliability of the product subsequent to the sale of the product. The field reliability is calculated based on recorded failures and malfunctions. For some products, like cars, failure data are collected and analysed by various organizations and the field reliability is made public in special journals and on the Internet. The field reliability is also called the actual reliability and is the same as our concept actual (reliability) performance.

Very often, the field reliability of a product differs from the design reliability due to environmental and operational conditions varying from customer to customer and differing from the nominal values used in the design process. It also depends on the maintenance actions carried out by the customers during the use of the product.

4.3 Reliability Science

Failure of an item is often a result of deterioration of some characteristics (such as strength). The rate at which the deterioration occurs is a function of time and/or usage intensity. The deterioration process is often a complicated process and varies with the type of item and the materials used. Reliability science is concerned with the properties of materials and the causes of deterioration leading to item failures. It also deals with the effect of manufacturing processes (e.g., casting, annealing) on the reliability of the part or component produced.

4.4 Reliability Modelling – I

Reliability modelling deals with model building to obtain solutions to 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. As such, reliability modelling plays a very important role in reliability performance and specification in new product development.

The modelling of the first failure is different from the modelling of the subsequent failures. This is because the modelling of subsequent failures depends on the corrective maintenance actions taken to restore a failed item into operational state.

In this section we focus on the modelling of the first failure at component and system levels.

4.4.1 Reliability Modelling of Single Items

The time to the first failure of a single item (a component or a system) is often modelled by considering only two possible states of the item; a working state and a failed state. When the item is put into operation, it is in working state and when failure occurs, the state changes from working to failed state. The time for which the item is in working state is the time to the first failure, T. Since failures occur in a random manner, T is a random variable. The distribution of T may be selected in different ways:

- Based on recorded field data from the same type of items without considering the failure mechanisms involved. This is sometimes referred to as "empirical or data-driven modelling" and is also called a black-box approach.
- Based on a careful consideration of the underlying causes and mechanisms that may lead to item failure, and modelling of the degradation of the item as a function of time. The time to the first failure, T, is the time until the degradation passes a specified threshold value. This is referred to as physical modelling and is also called a white-box approach.

In many applications, a combination of these two approaches is used, and may also be combined with expert judgement.

Failure Distribution and Failure Rate Function

Let T denote the time from when the item is put into operation until the first failure. T is a non-negative random variable that can assume any value in the interval $[0, \infty)$. As such, T can be modelled by an absolutely continuous failure distribution function. The failure distribution function $F(t;\theta)$ is given by

$$F(t;\theta) = \Pr(T \leq t) \quad \text{for } t > 0 \tag{4.1}$$

where θ is the parameter set of the distribution function.[2] We note that $F(t)$ [$= F(t;\theta)$] is the probability that the first failure will occur in the time interval $(0, t]$.

The probability density function associated with the distribution function $F(t)$ (if $F(t)$ is differentiable) is given by

$$f(t) = \frac{dF(t)}{dt} \quad \text{for } t > 0 \tag{4.2}$$

The probability density function $f(t)$ can also be expressed by the approximation

$$\Pr(t < T \leq t + \Delta t) \approx f(t) \cdot \Delta t \tag{4.3}$$

when Δt is "small". This equation indicates why $f(t)$ is called a density function.

The survivor function, $R(t)$ is given by

$$R(t) = \Pr(T > t) = 1 - F(t) \quad \text{for } t > 0 \tag{4.4}$$

and denotes the probability that the item will survive the time interval $(0, t]$, that is, the probability that the item will not fail before it reaches the age t. $R(t)$ is also called the reliability of the item and is sometimes denoted $\bar{F}(t)$.

The conditional probability that the item will fail in the interval $(t, t + \Delta t]$ given that it has not failed prior to time t, is given by

$$\Pr(t < T \leq t + \Delta t \mid T > t) = \frac{F(t + \Delta t) - F(t)}{1 - F(t)} \quad \text{for } t > 0 \tag{4.5}$$

The failure rate function, $z(t)$, associated with $F(t)$ is defined as[3]

$$z(t) = \lim_{\Delta t \to \infty} \frac{\Pr(t < T \leq t + \Delta t \mid T > t)}{\Delta t} = \frac{f(t)}{1 - F(t)} = \frac{f(t)}{R(t)} \tag{4.6}$$

Similar to (4.3) the failure rate function can be expressed by the approximation

$$\Pr(t < T \leq t + \Delta t \mid T > t) \approx z(t) \cdot \Delta t \tag{4.7}$$

[2] Often we will suppress the parameter θ for notational ease and write $F(t)$ instead of $F(t;\theta)$.

[3] A variety of symbols are used in the literature to denote the failure rate function. Among these are $h(t)$, $r(t)$, and $\lambda(t)$.

when Δt is "small." The expression $z(t) \cdot \Delta t$ denotes the probability that the item will fail in $(t, t + \Delta t]$ when we know that it has not failed prior to t. In other words, it characterizes the effect of age on item failure more explicitly than $F(t)$ or $f(t)$. The failure rate function $z(t)$ is also called the hazard rate function or the force of mortality (FOM) to explain that the failure rate indicates the "proneness to failure" of the item after it has reached an age t.

The cumulative failure rate function is

$$Z(t) = \int_0^t z(u)\, du \tag{4.8}$$

and it is seen from Equation (4.6) that

$$R(t) = e^{-\int_0^t z(u)\, du} = e^{-Z(t)} \tag{4.9}$$

The mean time to the first failure is given by

$$\text{MTTF} = \int_0^\infty t\ f(t)\, dt = \int_0^\infty R(t)\, dt \tag{4.10}$$

Many different types of distributions have been proposed for modelling component failures. Among these are the exponential distribution and the Weibull distribution.

Exponential Distribution

Consider an item that is put into operation at time $t = 0$. If the time to failure, T, has the probability density function

$$f(t) = \lambda e^{-\lambda t} \quad \text{for } t > 0 \tag{4.11}$$

then T is said to have an exponential life distribution, and we sometimes write $T \sim \exp(\lambda)$. The exponential distribution is the most used – and misused – distribution in the field of reliability. This is mainly due to its mathematical simplicity.

The survivor function is

$$R(t) = \Pr(T > t) = \int_t^\infty f(u)\, du = e^{-\lambda t} \quad \text{for } t > 0 \tag{4.12}$$

The conditional survivor function at age x is

$$\begin{aligned} R(t \mid x) &= \Pr(T > t + x \mid T > x) \\ &= \frac{\Pr(T > t + x)}{\Pr(T > x)} = \frac{e^{-\lambda(t+x)}}{e^{-\lambda x}} = e^{-\lambda t} \quad \text{for } t > 0 \end{aligned} \tag{4.13}$$

This means that that the probability of surviving a time interval of length t is the same for a used item of age x, as it is for a new item. An item with this property is "as good as new" as long as it is functioning. Failures will be pure chance failures and will not depend on the age of the item.

The corresponding failure rate function is

$$z(t) = \frac{f(t)}{R(t)} = \lambda \quad \text{for } t > 0 \tag{4.14}$$

The mean time to failure is

$$\text{MTTF} = \int_0^\infty R(t)\,dt = \int_0^\infty e^{-\lambda t}\,dt = \frac{1}{\lambda} \tag{4.15}$$

The exponential distribution is often used as a life distribution for electronic components and for high reliability components that are regularly tested and maintained.

Weibull Distribution

Another well-known distribution is the two-parameter Weibull distribution given by

$$F(t) = 1 - \exp\left(-\left(\frac{t}{\alpha}\right)^\beta\right) \quad \text{for } t > 0 \tag{4.16}$$

where $\alpha > 0$ and $\beta > 0$. The parameter α is called the *scale* parameter and β is called the *shape* parameter. The parameter α is also called the *characteristic life* of the item. The probability that an item survives its characteristic life, is from (4.16) seen to be $R(\alpha) = \exp(-1) \approx 0.3679$ for all values of the shape parameter β.

The probability density function is

$$f(t) = \frac{\beta}{\alpha^\beta}\,t^{\beta-1}\,\exp\left(-\left(\frac{t}{\alpha}\right)^\beta\right) \quad \text{for } t > 0 \tag{4.17}$$

and the failure rate function is given by

$$z(t) = \frac{\beta}{\alpha^\beta}\,t^{\beta-1} \quad \text{for } t > 0 \tag{4.18}$$

The failure rate function is seen to be increasing when $\beta > 1$, constant when $\beta = 1$, and decreasing when $\beta < 1$. The mean time to failure is

$$\text{MTTF} = \alpha \cdot \Gamma\left(\frac{1}{\beta} + 1\right) \tag{4.19}$$

where $\Gamma(\cdot)$ denotes the Gamma function (Rausand and Høyland, 2004).

The shape of the failure rate function changes significantly as the shape parameter β varies. As a result, the Weibull distribution may be used to model many failure patterns and it is widely used in practice. The exponential distribution is a special case of the Weibull distribution with shape parameter $\beta = 1$ and scale parameter (characteristic life) $\alpha = 1/\lambda$.

Several other failure distributions may be derived from the Weibull distribution; see, for example Blischke and Murthy (2000). There are many other non-Weibull distributions that have been used in reliability modelling. For more on these, see, for example Murthy et al. (2003) and Rausand and Høyland (2004).

Model Selection

In the black box approach the model selection is based on an analysis of the data available. The data can be failure times of items that have failed (complete data) and the age of items still working (censored data). Often, item failures are grouped into different intervals and the data available are the number of failures in different groups (grouped data). Various data plotting techniques have been developed to assist the model builder. These include both non-parametric (e.g., histograms, Kaplan Meier plots, hazard plots, and total time on test (TTT) plots) and parametric (e.g., empirical Weibull probability plots). For more on these, see Ansell and Phillips (1994); Crowder et al. (1991); Blischke and Murthy (2000); Rausand and Høyland (2004).

Bathtub and Roller Coaster Failure Rate Function

Sometimes, the empirical plots of the failure rate function indicate that we need to select a failure distribution that has a bathtub shape (see Figure 4.2) or roller coaster shape (see Figure 4.3) for the failure rate function. The roller coaster failure rate function requires more complicated formulations involving two or more distributions.

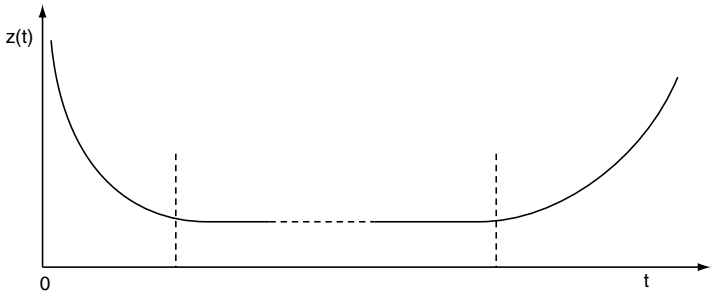

Figure 4.2. Bathtub failure rate function

Parameter Estimation

Once a distribution has been selected, we need to assign numerical values to the parameters of the distribution. Many different methods have been proposed and they can be broadly grouped into two categories – graphical and statistical. The graphical approach uses the plots (e.g., Weibull probability plot) to estimate the parameters. In the case of the two-parameter Weibull distribution, the slope and the intercept are used to obtain the parameter estimates. Methods based on the statistical approach include the method of moments, maximum likelihood, Bayesian, and so forth. These can be found in most books on reliability data analysis, for example, Lawless (1982); Ansell and Phillips (1994); Meeker and Escobar (1998).

Model Validation

If the data available are extensive, we can divide the data into two sets. The first set is used for model selection and parameter estimation. The second set is used for model validation. Many different statistical tests have been developed to see if the data from the second fits the model derived from the first set. For more on this, see Blischke and Murthy (2000); Murthy et al. (2003).

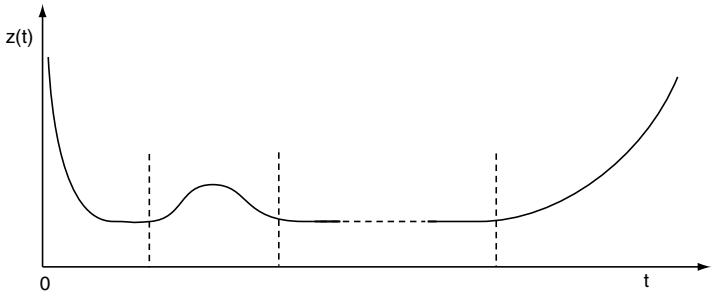

Figure 4.3. Roller coaster failure rate function

4.4.2 Physical Modelling

Physical modelling (white-box approach) requires a thorough understanding of the failure causes and mechanisms that may lead to item failure. This knowledge has to be translated into knowledge about the shape of the failure rate function. A lot of research efforts have been devoted into understanding how specific deterioration mechanisms, like corrosion, wear, and fatigue, progress as a function of time, and hence how they influence the failure rate function (Rausand and Høyland, 2004). If we know that an item will be exposed to a dominating failure mechanism, we have a good basis for selecting an appropriate failure distribution.

In some cases, it may be relevant to use stochastic processes to model the gradual degradation of the item and to derive the distribution of the time to first failure by solving a level-crossing problem. For example, in the case of fatigue failures, we may start by modelling the spread of the crack by a suitable stochastic process. If the spread is due to external shocks, then the occurrence of shocks needs to be modelled by a marked point process where the points corresponds to random time instants when shocks occur and the mark (a random variable) denotes the increase in the crack length due to the shock. The time to failure is the first time instant when the crack length exceeds some critical length.

These types of models involve very complex model formulations and are hence not very relevant in the context of reliability specification. As such, these models will not be discussed any further.

Combined Component Level Modelling

When we develop models for the time to first failure, T, of rather new items, the data available are only related to a short life span of the items. The data will typically be strongly censored and only contain some few failures. By using the black-box approach, it is impossible to conclude anything about the reliability of the item after the observed life span. In most cases it is, for example, impossible to distinguish whether the data fit best to a Weibull distribution or to a lognormal distribution. These two distributions have similar failure rate functions in the first part of the life span, but are very different in the last part of the life span (Rausand and Høyland, 2004). To be able to come up with a realistic model, we have to combine the black-box and the physical approach.

4.4.3 System Modelling

System failure is modelled in terms of the failures of the components of the system. Let n denote the number of components in the system. The linking of component failures to system failures can be done in several ways. Two of these are the reliability block diagram and the fault tree analysis.

Reliability Block Diagram

A reliability block diagram (RBD) is a success-oriented network describing a function of a system. The diagram has one source (a) and one terminal (b) as illustrated in Figure 4.4. Each block in the diagram represents a function of a component. If the function is available, we have connection through the block, and if the function is failed, there is no connection through the block. If we have connection between (a) and (b), this means that the system is functioning. Note that a reliability block diagram only represents a specified function of a system. Two different systems functions will therefore have two different reliability block diagrams.

Example 4.3 (Safety Instrumented System). Consider a simple safety instrumented system comprising three sensors (components 1, 2, and 3) that are connected to a single logic solver (component 4) in a 2-out-of-3 configuration. The logic solver is connected to two actuating items (components 5 and 6) in a 1-out-of-2 configuration. If a process demand occurs, at least two of the three sensors, the logic solver, and at least one of the two actuating items have to function to have a successful function of the safety instrumented system. A reliability block diagram of the safety function of the safety instrumented function is illustrated in Figure 4.4. ⊕

As illustrated in Figure 4.4, the same component may appear at several places in a reliability block diagram. It is important to realize that a reliability block diagram is not a physical layout diagram, but a diagram illustrating a specified system function.

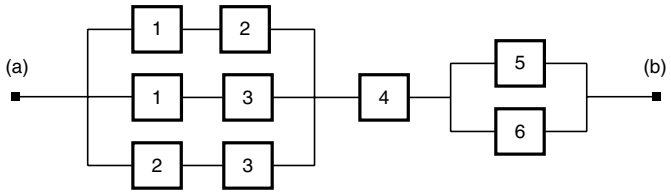

Figure 4.4. Reliability block diagram of the safety instrumented system in Example 4.3

Structure Function

Let $X_i(t)$ denote the state of component i at time t, for $i = 1, 2, \ldots, n$, where

$$X_i(t) = \begin{cases} 1 \text{ if component } i \text{ is in a working state at time } t \\ 0 \text{ if component } i \text{ is in a failed state at time } t \end{cases} \tag{4.20}$$

where "working state" refers to a specified function.

Let $\mathbf{X}(t) = (X_1(t), X_2(t), \ldots, X_n(t))$ denote the state of the n components at time t. Let $X_S(t)$ (binary random variable) denote the state (working or failed) of the system at time t. Then, from the reliability block diagram we can derive an expression of the form

$$X_S(t) = \phi(\mathbf{X}(t)) \tag{4.21}$$

which links the component states to the system state. $\phi(\cdot)$ is called the structure function.

The reliability block diagrams of (i) a series system, (ii) a parallel system, and (iii) a 2-out-of-3 system are illustrated in Figure 4.5. The series system is functioning

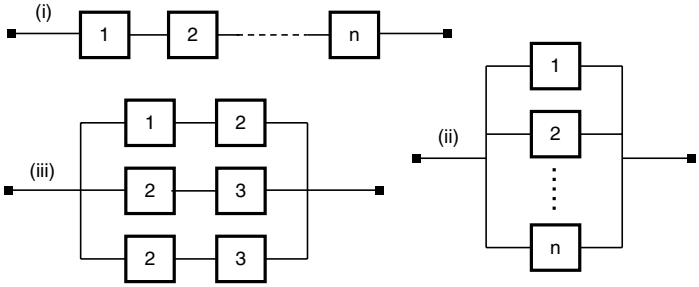

Figure 4.5. Reliability block diagrams (i) a series system, (ii) a parallel system, and (iii) a 2-out-of-3 system

if and only if all the components are functioning, i.e., the state of the system $X_S(t)$ is 1, if and only if $X_i(t) = 1$ for $i = 1, 2, \ldots, n$. The structure function of a series system is therefore the product of the state variables of the components.

$$\phi(\mathbf{X}(t)) = \prod_{i=1}^{n} X_i(t) \quad \text{for the series system} \tag{4.22}$$

The parallel system is functioning if at least one of its components is functioning, i.e., the system state $X_S(t)$ is 0 if and only if $X_i(t) = 0$ for all $i = 1, 2, \ldots, n$. The structure function of the parallel system is therefore

$$\phi(\mathbf{X}(t)) = 1 - \prod_{i=1}^{n} [1 - X_i(t)] \quad \text{for the parallel system} \tag{4.23}$$

The 2-out-of-3 system is functioning if at least two of the three components are functioning, and can be considered as a parallel system of three series systems as illustrated in Figure 4.5(iii). The structure function is therefore

$$\phi(\mathbf{X}(t)) = 1 - [1 - X_1(t)X_2(t)]\,[1 - X_1(t)X_3(t)]\,[1 - X_2(t)X_3(t)] \tag{4.24}$$

Since $X_i(t)$ is a binary variable, then $X_i(t)^2 = X_i(t)$. By using this property, the structure function of the 2-out-of-3 system can be reduced to:

$$\phi(\mathbf{X}(t)) = X_1(t)X_2(t) + X_1(t)X_3(t) + X_2(t)X_3(t) - 2X_1(t)X_2(t)X_3(t) \tag{4.25}$$

System Reliability

Let $R_S(t)$ denote the reliability of the system and $\mathbf{R}(t) = (R_1(t), R_2(t), \ldots, R_n(t))$ denote the reliabilities of the n components. If the component failures are independent, and the structure function has been reduced to an algebraic expression without any powers of $X_i(t)$, we get

$$R_S(t) = \phi(\mathbf{R}(t)) \tag{4.26}$$

so that we have the system reliability in terms of the component reliabilities (Rausand and Høyland, 2004).

The failure distribution for the time to first time to system failure is given by

$$F_S(t) = 1 - R_S(t) \tag{4.27}$$

Example 4.4 (Safety Instrumented System). Reconsider the system in Example 4.3. The structure function of the system is

$$\begin{aligned}\phi(\mathbf{X}(t)) = {} & [X_1(t)X_2(t) + X_1(t)X_3(t) + X_2(t)X_3(t) - 2X_{(}t)X_2(t)X_3(t)] \\ & \cdot X_4(t) \cdot [X_5(t) + X_6(t) - X_5(t)X_6(t)]\end{aligned}$$

Let $R_i(t)$ denote the reliability of component i, for $i = 1, 2, \ldots, 6$. The system reliability is then

$$\begin{aligned}R_S(t) = {} & [R_1(t)R_2(t) + R_1(t)R_3(t) + R_2(t)R_3(t) - 2R_1(t)R_2(t)R_3(t)] \\ & \cdot R_4(t) \cdot [R_5(t) + R_6(t) - R_5(t)R_6(t)]\end{aligned}$$

$\oplus$

Fault Tree Analysis

A fault tree illustrates the interrelationships between a potential system fault (denoted the TOP event) and the possible causes of this fault. The causes may comprise component faults, human errors, and environmental events/states. The fault tree is a "static picture" of a potential system fault. The fault tree does not illustrate any dynamic properties of the event chain that may lead to a system fault.

The starting point of a fault tree analysis (FTA) is a system fault, that is, the system state after a failure has occurred. The fault tree is developed by repeatedly asking the question "what can the causes of this event be". This is done successively when moving down a tree structure as illustrated in Figure 4.6. The lowest level causes in the fault tree are called basic events. The connections between these causes are done using logic gates, where the output from a gate is determined by the inputs to it. A special set of symbols is used for this purpose. We illustrate this by Example 4.5. More details may be found in Rausand and Høyland (2004); IEC 61025 (1990); NASA (2002).

Example 4.5 (Safety Instrumented System). Reconsider the safety instrumented system (SIS) in Example 4.3. When a process demand occurs (e.g., fire, gas leakage), at least two of the three sensors (components 1, 2, and 3) in Figure 4.4 must respond and send a signal to the logic solver (component 4). The logic solver will then send a signal to the two valves (components 5 and 6). At least one of the valves must close to shut down the process. A fault tree with respect to the TOP event "SIS fails to function on demand" is shown in Figure 4.6. ⊕

4.4.4 Modelling Environmental Effects

The stress (e.g., voltage, pressure, temperature) on an item affects the time to failure and hence the failure distribution of the item. The effect of increasing the stress is to accelerate the time to failure. Many different models have been developed to model this. Two of the well-known ones are the following:

Accelerated Failure Time Model

Let T_s denote the time to failure at a specified stress level s. In the accelerated failure time model the survivor function of T_s is given by

$$R(t;s) = R_0(t/\psi(s)) \tag{4.28}$$

where $R_0(t)$ is a baseline survivor function associated with a reference value of the stress level, s_0, and $\psi(s)$ is a function of the stress s.

In this model the scaled lifetime $T/\psi(s)$ has the survivor function

$$R_s(t) = \Pr(T_s/\psi(s) > t) = \Pr(T_s > \psi(s) \cdot t) = R(\psi(s) \cdot t) = R_0(t) \tag{4.29}$$

This means that the scaled lifetime $T_s/\psi(s)$ will have the same distribution for all stress levels s.

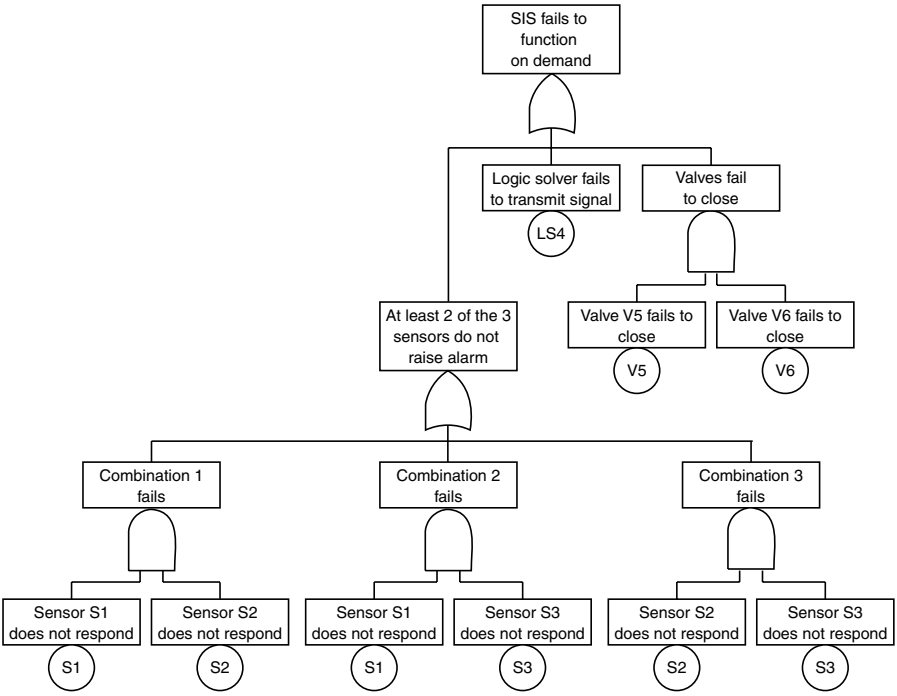

Figure 4.6. Fault tree for the TOP event "SIS fails to function on demand" of a safety instrumented system; Example 4.5

A typical choice of $\psi(s)$ is

$$\psi(s) = e^{\gamma s} \tag{4.30}$$

The scaled lifetime $e^{-\gamma s} T_s$ then has a distribution that does not depend on the stress level s. The mean value of T_s is $E(T_s) = e^{\gamma s}\mu_0$ where $\mu_0 = E(T_0)$ is the mean time to failure at the reference stress level s_0. By taking the logarithm, we get

$$\ln T_s = \mu_0 + \gamma s + \epsilon \tag{4.31}$$

where ϵ is a random error with a distribution that does not depend on s. This is seen to be a linear regression model and we may hence use linear regression methods to estimate the unknown parameters μ_0 and γ (e.g., see Ansell and Phillips, 1994).

Proportional Hazards Model

In the proportional hazards model, the failure rate function of an item with life length T_s when operated under stress level s is given by

$$z(t; s) = z_0(t) \cdot h(s) \tag{4.32}$$

where $z_0(t)$ is a baseline failure rate function associated with a reference stress level s_0, and $h(s)$ is a function of s. By using this model, we split the failure rate function into two parts, one part that is a function of the time t (and not the stress s), and one part that is a function of the stress level s.

The survivor function at stress s is

$$R(t;s) = \exp\left(-\int_0^t z(u,s)\,du\right) = \left(\exp\left(-\int_0^t z_0(u)\,du\right)\right)^{h(s)} = (R_0(t))^{h(s)} \tag{4.33}$$

Let s_1 and s_2 be two different stress levels. The relationship between the failure rate function at these stress levels may be expressed as

$$\frac{z(t;s_1)}{z(t;s_2)} = \frac{z_0(t)\cdot h(s_1)}{z_0(t)\cdot h(s_2)} = \frac{h(s_1)}{h(s_2)} \tag{4.34}$$

The relation between the two failure rate functions at time t is hence independent of t, and only dependent on the stress levels s_1 and s_2. This explains why the model is called a proportional hazards (i.e., failure rate) model.

To get a convenient functional form of the failure rate function, we often have to transform the stress levels, for example, by taking logarithms or using power functions. Sometimes, we also combine two or more stresses. If we, for example, have a pipeline that is exposed to erosion caused by sand particles in the fluid in the pipeline, the rate of erosion (and thereby the failure rate function) will depend on the sand content *and* the flowrate. It is the combined effect that is important, and not the single stresses.

After having transformed and combined the relevant stresses, we get a vector of stressors $\boldsymbol{x} = (x_1, x_2, \ldots, x_m)$. It is also common to use physical parameters, like the diameter of a tube, as stressors, which are also called covariates or concomitant variables. The proportional hazards model may, alternatively, be expressed by

$$z(t;\boldsymbol{x}) = z_0(t)\cdot\psi(\boldsymbol{x},\boldsymbol{\beta}) \tag{4.35}$$

where $\psi(\boldsymbol{x},\boldsymbol{\beta})$ is a function and $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots)$ is a row vector of unknown parameters.

Example 4.6 (Constant failure rate). Assume that the failure rate is constant, such that, $z(t;\boldsymbol{x}) = \lambda_0\cdot\psi(\boldsymbol{x},\boldsymbol{\beta})$. The survivor function is now

$$R(t;\boldsymbol{x}) = \exp\left(-\lambda_0\cdot\psi(\boldsymbol{x},\boldsymbol{\beta})\right) \tag{4.36}$$

and the mean time to failure is

$$\mathrm{MTTF}_s = \frac{1}{\lambda_0\cdot\psi(\boldsymbol{x},\boldsymbol{\beta})} = \mathrm{MTTF}_0\cdot\frac{1}{\psi(\boldsymbol{x},\boldsymbol{\beta})} \tag{4.37}$$

where MTTF_0 and $\mathrm{MTTF}_{\boldsymbol{x}}$ are the mean time to failure at the baseline stress and stress level $\boldsymbol{x}$, respectively.

Note that the simple model used in MIL-HDBK-217F to determine the failure rate of electronic components is a special case of this model. ⊕

The most commonly used form of $\psi(\cdot)$ was introduced by Cox (1972) and has since then been referred to as the *Cox model*. This model uses

$$\psi(\boldsymbol{x};\boldsymbol{\beta}) = \exp(\boldsymbol{\beta}\boldsymbol{x}) = \exp\left(\sum_{j=1}^{m} \beta_j x_j\right) \tag{4.38}$$

where m is the dimension of the (column) vector $\boldsymbol{x}$ of stressors. By taking logarithms, we get the linear relationship

$$\ln z(t;\boldsymbol{x}) = \ln z_0(t) + \sum_{j=1}^{m} \beta_j x_j \tag{4.39}$$

Estimators for the unknown parameters may, for example, be found in Ansell and Phillips (1994); Crowder et al. (1991); Kumar and Klefsjø (1994).

4.5 Reliability Modelling – II

The modelling of subsequent failures (at component, system or some intermediate level) depends on the maintenance actions. IEC 60050-191 defines maintenance as "The combinations of all technical and corresponding administrative actions, including supervision actions, intended to retain an entity in, or restore it to, a state in which it can perform its required functions." Maintenance involves one or more of the following actions: servicing (e.g., cleaning and lubrication), testing/inspection, removal/replacement, repair/overhaul, and modification through redesign.

Maintenance actions to control the deterioration process leading to failure of an item are called preventive maintenance (PM) actions and actions to restore a failed item to its functioning state are called corrective maintenance (CM) actions. The time needed to carry out CM and PM actions can vary and needs to be modelled properly. For minor PM and CM actions, the time needed is small relative to the time between failures and can be ignored. For a major overhaul, the time can be significant and cannot be ignored.

4.5.1 Modelling CM Actions

The options available depend on whether the failed item is repairable or not.

Replace by New or Used Item

If the item is non-repairable, then the only CM action is to replace a failed item by a working (new or used) item. If a new item (similar to the failed item) is used in the replacement, then the time to failure is a random variable with the same distribution $F(t)$ as for the initial item, and the repair action has brought the item to an "as good as new" condition, as illustrated in Figure 4.7.

If a used item of age x is used in the replacement, the time to failure is a random variable with conditional failure distribution

$$F(t \mid x) = \Pr(T \le t + x \mid T > x) \quad \text{for } t \ge 0 \tag{4.40}$$

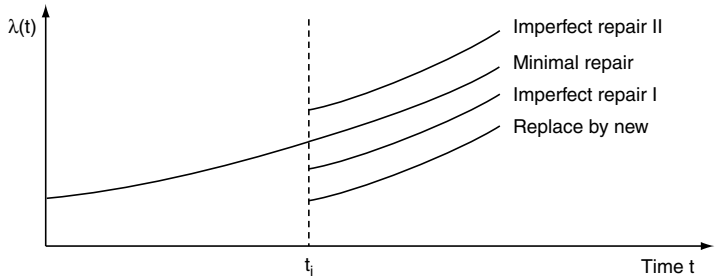

Figure 4.7. Failure rate under imperfect repair

Minimal Repair

This model is mainly used for complex items comprising a number of components. If one component fails and causes item failure, only the failed component is repaired. After the repair action is completed, the status of the system is approximately the same as just before the failure. The repair action has a *minimal* effect on the system, since the likelihood of failure just after the repair action is approximately the same as it was just before the component failed. The repair action is therefore called a *minimal repair* and the item condition after the minimal repair is often called "as bad as old."

Let $z(t)$ denote the failure rate of a new item. If the item fails at time t_i and the time to repair is negligible (so that it can be ignored), then the failure rate of the repaired item is given by $\tilde{z}(t) = z(t)$ for $t > t_i$, as illustrated in Figure 4.7.

Imperfect Repair

An imperfect repair is somewhere between a replacement and a minimal repair, and may also be called a *normal repair*. Just after an imperfect repair action, the failure rate of the item is greater than for a new item and, in general, less than that under minimal repair (imperfect repair I in Figure 4.7). It is also possible that additional failures are introduced during the maintenance action such that the failure rate after the (imperfect) maintenance action is higher than it was just before the action. This is illustrated as imperfect repair II in Figure 4.7.

Many different models have been proposed for imperfect repair and details can be found in Pham and Wang (1996).

4.5.2 Modelling PM Actions

Preventive maintenance (PM) is the set of actions to control the rate of degradation and reduce the likelihood of failure occurrence. As such, these actions are taken when the item is still in operational state as opposed to CM, which is the set of actions that are taken after the item fails. Many different kinds of PM policies are used and these include the following:

Age-based policy: PM actions are based on the age of the item.
Clock-based policy: PM actions are carried out at set times.
Usage-based policy: PM actions are based on the usage of the item.
Condition-based policy: PM actions are based on the condition of the item. This involves monitoring one or more variables characterizing the wear process causing the degradation.
Opportunity-based policy: This is applicable for multi-component items, where a CM action for a failed component provides an opportunity to carry out PM actions on one or more of the remaining components.
Design-out policy: This involves re-designing the very unreliable components of an item. As a result, the new item will (hopefully) have better reliability characteristics than the earlier item.

ROCOF

The rate of occurrence of failures (ROCOF) is a very useful concept in the modelling of failures over time and the effect of PM (and CM) actions. It characterizes the probability that the system fails in the interval $(t, t + \Delta t)$ given the history, $\mathcal{H}(t)$, of failures and maintenance actions over the interval $(0, t)$ and is given by an intensity function

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{\Pr(N(t + \Delta t) - N(t) > 1 \mid \mathcal{H}(t))}{\Delta t} \tag{4.41}$$

where $N(t)$ is the number of failures in the interval $(0, t)$. Since the probability of two or more failures in the interval $(t, t + \Delta t)$ is zero as $\Delta t \to 0$, the intensity function is equal to the derivative of the conditional expected number of failures, so that

$$\lambda(t) = \frac{d}{dt} \mathrm{E}\left(N(t) \mid \mathcal{H}(t)\right) \tag{4.42}$$

The cumulative ROCOF is

$$\Lambda(t) = \int_0^t \lambda(u)\, du = E(N(t)) \tag{4.43}$$

Two models of PM actions that have been used extensively in the reliability literature are the following (e.g., see Doyen and Gaudoin, 2004):

Reduction in Age

This involves the concept of virtual age, which increases linearly with time and every PM action results in a reduction in the virtual age. The ROCOF is a function of the virtual age.

Let $B(t)$ denote the virtual age of the item at time t, and let t_i, for $i = 0, 1, 2, \ldots$, denote the time instants at which PM actions are carried out. After the ith PM action, the reduction in the virtual age is τ_i so that virtual age is given by $B(t) = t -$

$\sum_{j=0}^{i} \tau_j$, for $t_i < t \leq t_{i+1}$ with $\tau_0 = 0$ and $t_0 = 0$. As a result, the ROCOF is given by the intensity function

$$\lambda(t) = z(B(t)) = z\left(t - \sum_{j=0}^{i} \tau_j\right) \quad \text{for } t_i < t \leq t_{i+1} \text{ and } i = 0, 1, 2, \ldots \tag{4.44}$$

The reduction in the virtual age at the ith PM action and i are constrained by the relationship

$$0 \leq \tau_i < t_i - t_{i-1} \quad \text{for } i = 1, 2, \ldots \tag{4.45}$$

This implies that the item can never be restored to as good as new. Figure 4.8 shows a plot of the virtual age $B(t)$ and the intensity function $\lambda(t)$.

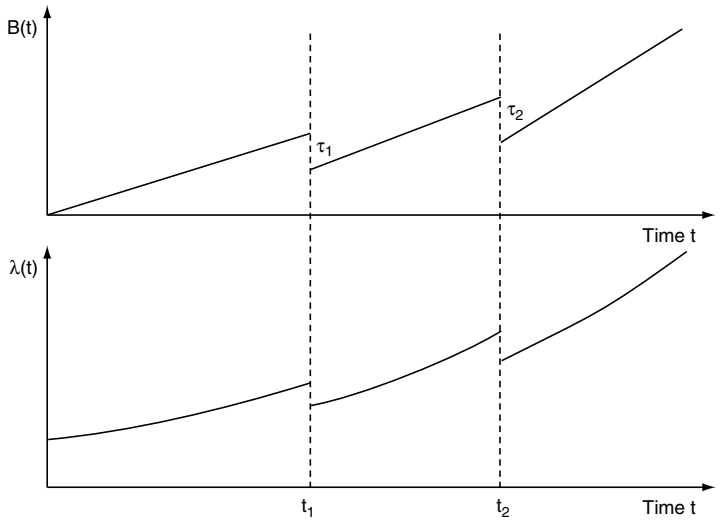

Figure 4.8. ROCOF with age reduction during PM actions

Reduction in ROCOF

In this model, there is reduction in the ROCOF associated with each PM action, so that after the ith repair, the ROCOF is given by

$$\lambda(t) = z(t) - \sum_{j=1}^{i} \delta_i \quad \text{for } t_i < t \leq t_{i+1} \tag{4.46}$$

where δ_i is the reduction in the ROCOF at the ith PM and is constrained by the relationship

$$\lambda(0) \leq \sum_{j=1}^{i} \delta_i < \lambda(t_i) \tag{4.47}$$

for $t_i < t < t_{i+1}$. This ensures that the ROCOF never goes below the failure rate for a new item. Figure 4.9 shows a plot of the intensity function $\lambda(t)$.

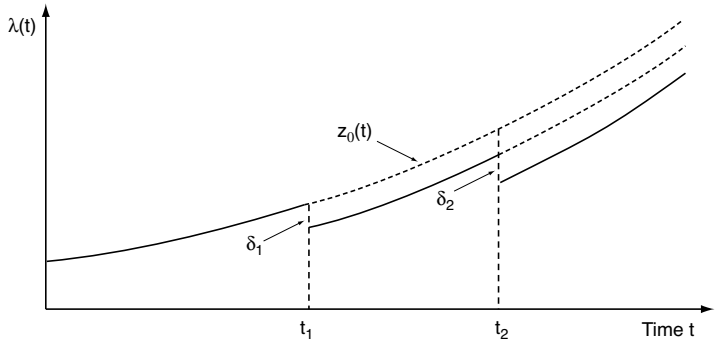

Figure 4.9. Reduction in ROCOF with PM actions

Note. When the time needed to carry out a PM action cannot be ignored, then the ROCOF is not defined over the period when PM actions are carried out.

4.5.3 Other Approaches

Many other approaches have been used for modelling failures over time at system level. These include Markov and semi-Markov formulations (Bhat, 1972; Ross, 1996; Limnios and Oprisan, 2001) to name a few.

4.6 Reliability Analysis

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

4.6.1 Qualitative Analysis

The two main topics in the qualitative analysis are (i) FMEA/FMECA and (ii) Fault tree analysis. We discussed briefly fault tree analysis in Section 4.4.3. In this section we discuss FMEA.

Failure Modes and Effects Analysis (FMEA)

A failure modes and effects analysis (FMEA) is used to identify, analyse, and document the possible failure modes that can exist for a system, and the effects of such failures on the system's performance. If the criticality of each failure mode is analysed, the analysis is called a failure modes, effects, and criticality analysis (FMECA). According to IEEE Std. 352, the basic questions to be answered by FMEA are the following:

- How can each part conceivably fail?
- What mechanisms might produce these modes of failure?
- What could the effects be if the failures did occur?
- How is the failure detected?
- 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:

1. Description of the different parts. This is done through a proper reference number, the intended function of the part and the normal operational mode
2. Characterization of failure. This involves listing the different possible failure modes, failure mechanisms responsible for the different failure modes and the various means of detecting the different failure modes
3. Effect of failure on other components of the system and the system performance.
4. Severity ranking that characterizes the degree of the consequences of each failure mode.

There are two main approaches to FMEA. One is the hardware approach that starts with the hardware components at the lowest level in the system hierarchy and analyses their possible failure modes. The other is the functional approach that focuses on the functions rather than the hardware components. The FMEA may start at the highest system level and proceed down to lower levels (top-down), or start at the lowest part level and proceed to the highest system level (bottom-up). The hardware bottom-up approach is normally used when we are analysing a system where hardware components can be uniquely identified from drawings or other system descriptions. The functional top-down approach is normally used when we analyse a system in an early design phase before all details about hardware components have been decided.

The most critical failure modes are sometimes extracted from the FMEA/FMECA and entered into a critical items list. The critical item list is a living document that provides valuable input to design changes, test planning, safe operational procedures, and so on.

Example 4.7 (Safety Instrumented System). A process shutdown system is a common example of a safety instrumented system. The shutdown action is usually carried out by fail-safe valves, that is, valves that are kept in an open position by hydraulic or pneumatic pressure during normal operation. When the valve receives a signal to

close, the pressure is bled off and the valve will close by some built-in mechanism (e.g., spring force).

The failure modes for the shutdown valve and the effect of the failures are as follows:

Failure mode	Failure effect
Fail to close	Flow cannot be stopped
Leakage in closed position	Flow is partly stopped
External leakage	Fluid leaks to the environment
Spurious closure	Flow stopped without signal
Fail to open	Flow cannot be opened after a closure

The severity of the various failure modes will depend on the process, the environment, and the type of fluid. ⊕

4.6.2 Quantitative Analysis

Quantitative analyses are used to evaluate various performance measures. We briefly discuss some main measures.

Availability

Let $X(t)$ denote the state of an item at time t. It is a binary variable with $X(t) = 1$ if the item is in working state and $X(t) = 0$ if not. There are several different notions of availability, as indicated below.

- The availability $A(t)$ at time t (also called point availability) is given by

$$A(t) = \Pr(X(t) = 1) = \mathrm{E}(X(t)) \tag{4.48}$$

- The limiting availability is given by

$$A = \lim_{t \to \infty} A(t) \tag{4.49}$$

  when the limit exists.
- The average (mean) availability in $(0, \tau)$ (also called mission availability) is given by

$$A(0, \tau) = \frac{1}{\tau} \int_0^\tau A(t)\, dt \tag{4.50}$$

  where $A(0, \tau)$ can be interpreted as the mean proportion of the time in $(0, \tau)$ where the item is in a functioning state.
- The limiting average availability (also called steady state availability) is given by

$$A_\infty = \lim_{\tau \to \infty} \frac{1}{\tau} \int_0^\tau A(t)\, dt \tag{4.51}$$

In the special case where the item is repaired to an "as good as new" condition after each failure, such that all up-times are independent and identically distributed, and that also all down-times are independent and identically distributed, the (steady state) average availability is given by

$$A_\infty = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \tag{4.52}$$

where MTTR denotes the average down-time for a repair action.

The *unavailability* of an item at time t, $\bar{A}(t)$, is defined as $\bar{A}(t) = 1 - A(t)$, and similarly for the other availability notions.

Probability of Failure on Demand

Consider an item that is put into operation at time $t = 0$. Some critical failure modes of the item are hidden. The item is therefore function-tested after regular intervals of length τ. We assume that all failures are detected during the function test. If failures are revealed, they are repaired and the item is considered to be "as good as new" after each test. The test and repair times are considered to be negligible compared to τ. The average unavailability is, in this case, usually called *probability of failure on demand* (PFD). The PFD can here be determined from (see Rausand and Høyland, 2004)

$$\text{PFD} = 1 - \frac{1}{\tau}\int_0^\tau R(t)\,dt \tag{4.53}$$

Example 4.8 (Safety Instrumented System).

(a) Consider a safety instrumented system with a single input element (e.g., a sensor) with constant failure rate λ with respect to hidden fail-to-function (FTF) failures. The survivor function of the element is $R_a(t) = e^{-\lambda t}$. With test interval τ, the PFD becomes

$$\text{PFD}_a = 1 - \frac{1}{\tau}\int_0^\tau e^{-\lambda t}\,dt = 1 - \frac{1}{\lambda\tau}\left(1 - e^{-\lambda\tau}\right) \approx \frac{\lambda\tau}{2}$$

The approximation is acceptable when $\lambda\tau$ is small (e.g., $\leq 10^{-2}$).
If a demand for the safety instrumented system occurs, the PFD denotes the (average) probability that the sensor will not be able to raise alarm.

(b) Consider a safety instrumented system with three identical and independent input elements that are configured as a 2-out-of-3 system. The elements have constant failure rate λ and are tested at the same time with test interval τ. The survivor function of the 2-out-of-3 system is $R_b(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$ and the PFD is

$$\text{PFD}_b = 1 - \frac{1}{\tau}\int_0^\tau \left(3e^{-2\lambda t} - 2e^{-3\lambda t}\right)\,dt \approx (\lambda\tau)^2$$

(c) Consider a safety instrumented system with two independent elements that are configured as a series (2-out-of-2) system. The elements have constant failure rates λ_1 and λ_2, respectively. The survivor function of the system is $R_c(t) = e^{\lambda_1 t} \cdot e^{-\lambda_2 t} = e^{-(\lambda_1+\lambda_2)t}$ and the PFD is

$$\text{PFD}_c = 1 - \frac{1}{\tau}\int_0^{\infty} e^{-(\lambda_1+\lambda_2)t}\, dt \approx \frac{(\lambda_1+\lambda_2)\tau}{2} = \text{PFD}_1 + \text{PFD}_2$$

where PFD_i is the PFD of element i for $1 = 1, 2$.

Safety instrumented systems (SISs) are classified into *safety integrity levels* (SIL). For a SIS that is operated in a so-called low demand mode, the safety integrity level is (partly) defined from the PFD as given below:

Safety integrity level (SIL)	PFD
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

To supply a SIL 3 system, the manufacturer has to verify that the SIS has a PFD $< 10^{-3}$. In addition comes a set of qualitative requirements. ⊕

Number of Failures in $(0, t)$

Let $N_f(t)$ denote the number of failures in the time interval $(0, t)$. We consider two cases and present the final results and omit the details of the derivation. Interested readers can find details in the references cited.

Non-repairable Item: Consider an item that, upon failure, is replaced by a new item of the same type (i.e., that is statistically identical to the failed item), and assume that the replacement times are negligible. In this case the failures occur according to a *renewal process* since each failure results in the item getting renewed back to new. Let $p_n(t)$ denote the probability of $N_f(t) = n$. Then it can be shown that

$$p_n(t) = F^{(n)}(t) - F^{(n+1)}(t) \tag{4.54}$$

where $F^{(n)}(t)$ is the n-fold convolution of $F(t)$ with itself.[4] Let $M(t)$ denote the expected value of $N_f(t)$, then $M(t)$ is given by the solution of the following integral equation (also called the renewal integral equation)

$$M(t) = F(t) + \int_0^t M(t-x)\, f(x)\, dx \tag{4.55}$$

[4] See Ross (1996) for details about convolution formulas.

Case (2) Repairable Item: Consider an item that, upon failure, is subject to a *minimal repair* (see page 74), and assume that the repair times are negligible. In this case, $N_f(t)$ is distributed according to a non-homogeneous Poisson process with intensity function given by $\lambda(t) = z(t)$ so that

$$p_n(t) = \frac{(Z(t))^n}{n!} e^{-Z(t)} \quad \text{for } n = 0, 1, 2, \ldots \tag{4.56}$$

where $Z(t)$ is the cumulative failure rate function given by Equation (4.8). The expected number of failures over the interval $(0, t)$ is given by

$$\mathrm{E}(N_f(t)) = Z(t) \tag{4.57}$$

4.6.3 Simulation

Sometimes, the situation is so complex that we are not able to find the desired solutions by analytical methods. In these situations, we may use so-called next-event Monte Carlo simulation (Mitrani, 1982; Ross, 2002). The Monte Carlo simulation is carried out by simulating "typical" lifetime scenarios on a computer. We start with a model of the system, usually a flow diagram or a reliability block diagram. Component failures, CM and PM actions and other scheduled events and conditional events are included to create a simulated lifetime scenario that is as close to the real lifetime scenario as possible. A set of performance measures (e.g., number of failures, downtime) are calculated from the lifetime scenario.

The simulation is carried out a high number of times and estimates of the performance measures are deducted from the resulting data. The simulator has an internal clock and it is therefore possible to take into account both seasonal variations and long term trends in the simulation.

4.7 Reliability Engineering

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

4.7.1 Reliability Allocation

Reliability allocation (or reliability apportionment) is the process of allocating product (system level) reliability requirements to sub-systems, and component levels – in the design phase. Preliminary reliability allocation is often based on historical performance data, that is, what reliability has been achieved by similar products.

At the component level, the assigned target value can exceed the reliability of commercially available items. In this case we need to improve the reliability of the component or use preventive maintenance where the component is replaced periodically.

Example 4.9. Consider a series system of n independent components with survivor functions $R_1, R_2(t), \ldots, R_n(t)$. The system survivor function is then $R_S(t) = \prod_{i=1}^{n} R_i(t)$. Assume that the system reliability requirement specifies that $R_S(t) \geq R^*(t)$, for some specified time t. If

$$R_S(t) = \prod_{i=1}^{n} R_i(t) \geq R^*(t) \tag{4.58}$$

then the requirement is fulfilled. If not, we have to improve one or more of the n components. In this process we have to take into account the cost, and the relative difficulty, of improving the different components. ⊕

Several methods have been developed for this purpose. Among these are:

- Equal apportionment method
- ARINC apportionment method
- AGREE apportionment method
- Feasibility of object method
- Minimum effort algorithm

For more information, see, for example, MIL-HDBK-338B and Ebeling (1997).

4.7.2 Reliability Improvement

There are two basic approaches to improving component (or system) reliability. They are as follows:

Use of Redundancy

This involves the use of replicates rather than a single item (sub-system to component level). Redundancy can only be used when the functional design of the system allows for the incorporation of replicated components.

Building in redundancy corresponds to using a module of replicated items as opposed to a single item. The manner in which these replicates are put into use depends on the type of redundancy. A module failure occurs only when some or all of the replicates fail. There are two types of redundancy:

Active redundancy: Active redundancy means that all the items in the module are in operational state, or "fully energized," when put into use. In the latter case, the active redundancy is often called hot standby.

Passive redundancy: In passive redundancy, only a part of the items in the module are fully energized. The remaining items are either partially energized (also called partly loaded standby) or kept in reserve and energized when put into use (cold standby). When a fully energized item fails, it is replaced by one of the standby items using a switching mechanism, provided that not all of the items in the module have failed.

Reliability Growth

The objective of reliability growth testing is to improve the reliability of an item through minor design changes and changes in manufacturing processes and procedures. The reliability growth is achieved through a test, analyse, and fix (TAAF)[5] programme in an iterative manner. It involves a sequential execution of the four stages shown in Figure 4.10 during each iteration.

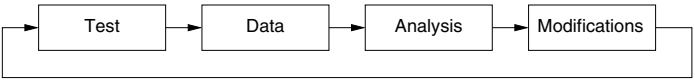

Figure 4.10. Test, analyse, and fix (TAAF) cycle

The TAAF process begins in the design phase and consists of tests that are specifically designed to expose the item to all types of stresses the item is expected to encounter during its life cycle. Deficiencies and failures are recorded and carefully analysed by engineers to reveal the root causes of the deficiencies. Design changes are made to remove the failure causes and to prevent the failure modes. The process is repeated until the test results are satisfactory. For further discussion of TAAF, TAAF test design principles, and relationship of TAAF to other testing programmes, see IEC 61014 and Priest (1988, Chapter 9).

A number of reliability growth models have been developed to monitor the progress of the development programme and the improvements in reliability of the item under consideration. The models can be broadly categorized into two types – continuous and discrete models. Each of these can be further sub-divided into parametric models (which involve a specified distribution of time to failure) and non-parametric models (which involve specification of a functional form for the reliability improvement relationship apart from the failure distribution). Some well-known reliability growth models are:

- Duane model
- IBM model
- Crow/AMSAA model
- Lloyd and Lipow model
- Jelinski and Moranda model
- Littlewood and Verrall model
- Littlewood model
- Musa model
- Musa–Okumoto model

For further discussion and many additional references, see Lloyd and Lipow (1962); Amstadter (1971); Dhillon (1983); Walls and Quigley (1999); MIL-HDBK-338B (1998).

[5] Some authors use the acronym TAFT (test, analyse, fix, test)

A failure reporting and corrective action system (FRACAS) is sometimes initiated to record failure data gathered through the testing and improvement programme. The FRACAS is a closed-loop reporting system that is a parallel to the TAAF cycle. Most benefit from the FRACAS is realized when it is implemented early in the test programme and is directly linked to the modelling effort. For more details about FRACAS, see O'Connor (2002); Dhudshia (1992); MIL-STD-2155 (1985). Approaches to statistical analysis of data from reliability growth testing are outlined in IEC 61164.

4.7.3 Root Cause Analysis

A root cause analysis is carried out after a failure has occurred with the intention to learn how and why the failure occurred. The analysis is mainly focused on the fundamental (root) causes of failure. The question "why?" is asked several times until a satisfactory explanation is found. Once the root cause is identified, the problem may be fixed by taking appropriate corrective actions by way of changes to the design or the material selection. For more on root cause analysis of mechanical components, see Nishida (1992) and DOE-NE-STD-1004-92 and for electronic components, see MIL-HDBK-338B.

4.8 Reliability Prediction and Assessment

Reliability prediction is a process used for estimating item reliability during the design phase. Reliability predictions provide a basis for deciding on reliability improvement, which can involve reliability growth during the development phase (Meeker and Escobar, 1998; Blischke and Murthy, 2000). Reliability prediction is the reliability potential of an item based on available design information. During the development phase, we can obtain an estimate of the actual reliability by testing. This process is called reliability assessment.

4.8.1 Reliability Prediction

Prediction involves models rather than actual systems and provides a basis for test planning, manufacturing, evaluation of reliability growth, maintenance, and other management activities. Reliability predictions should be continually updated when design changes are performed, and when test results become available. Healy et al. (1997) discuss the different purposes for reliability predictions and they include the following:

- Performing trade-off studies
- Setting plans for developmental testing
- Planning for design improvements
- Cost analyses, including life cycle cost studies
- Providing a basis for evaluation of reliability growth
- Studies of maintenance requirements and logistics

4.8.2 Reliability Assessment

The most important reason for careful reliability assessment is to verify that the predicted reliability is attained or is attainable. Other reasons for assessment include verification of updated predictions, monitoring of product quality, determination of reliability growth, and so forth. Data generated from testing forms the basis for reliability assessment. The assessment of reliability involves the use of statistical estimation methods which can be found in many books.

During the development phase, data is generated through several types of testing. Meeker and Hamada (1995) discuss the various tests and these include the following:

- Laboratory tests for materials evaluations
- Laboratory life tests of parts, components, and so on
- Environmental stress screening
- Tests of prototypes
- Degradation tests of materials, parts, and so on
- Test results from suppliers
- Qualification testing
- Stress life tests
- Reliability demonstration tests

To ensure data validity and reliability, carefully designed experiments are necessary.

An important additional experimental technique is accelerated testing, that is, testing under conditions involving stresses somewhat or far in excess of those encountered in normal operation. This allows the analyst to obtain data in a shorter time frame, but this can induce new modes of failures that do not exist under normal stress.

Testing during manufacturing is to eliminate manufacturing defects and early part failures. Two types of testing are commonly used:

Environmental Stress Screening

Environmental stress screening (ESS) is a screening process in which an item is subjected to environmentally generated stresses to precipitate latent item defects. The environmental stresses may be any combination of temperature, vibration or humidity.

Burn-in Testing

Burn-in is a process used to eliminate the high initial failure rate due to manufacturing defects. It involves putting items on a test bed to detect early failures, so that they can be weeded out before the item is released for sale.

4.9 Reliability Management

Reliability management deals with the many different management issues in the context of managing the design, manufacture, and/or operation of reliable products and systems. The manufacturer needs to look at these issues from an overall business perspective, taking into account the issues of concern to customers, such as product reliability, safety, operating costs, warranty, maintenance service contract, and so on. Two topics of great importance in the context of reliability performance and specifications are (1) costs and (ii) data for effective management.

4.9.1 Costs

Building reliability into a product is a costly exercise. From the manufacturer's point of view, some of the costs are as follows:

- Design cost
- Development cost
- Production cost
- Post-sale support costs

From the customer point of view, the main cost is the maintenance costs over the useful life of the product.

For an expensive custom-built product, the life cycle cost (LCC) is critical in the customer's decision to proceed with the project. The LCC process involves several steps as illustrated in Figure 4.11. For more on LCC, see IEC 60300-3-3 (2005); Fabrycky and Blanchard (1991); Kawauchi and Rausand (1999).

There are many indirect costs that result from product unreliability. From the manufacturer point of view these include the following:

- Warranty costs
- Loss of sales
- Dissatisfied customers
- Impact on product and business reputations

From the customer point of view, the indirect costs are the costs resulting from unavailability of the product.

4.9.2 Data for Effective Management

Many different kinds of data are needed for reliability related decision making in the different stages on the product life cycle. The relevant data will be discussed in Chapters 5 to 9 separately, and then in an integrated manner in Chapter 11.

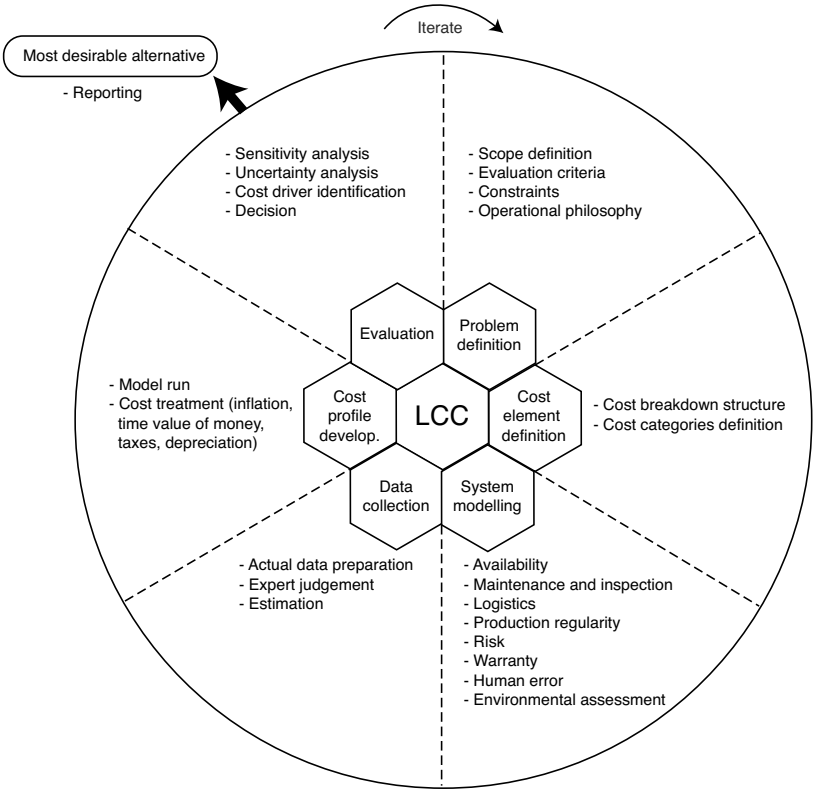

Figure 4.11. The steps of the LCC process (from Kawauchi and Rausand, 1999)

4.10 Case Study: Cellular Phone

The cellular phone is composed of several elements and the integrated circuit (also known as IC or chip) is an important element. ICs can be classified into three groups: digital, analogue, and mixed signal (both analogue and digital on the same chip). Digital ICs contain a large number of logic gates, flip-flops, multiplexers and other circuits. Analogue ICs (such as sensors, operational amplifiers etc) process continuous signals and are used to perform various functions (e.g., amplification, filtering, demodulation). The mixed signal ICs carry out functions such as A/D and D/A conversions.

ICs are fabricated in a layer process involving the following three steps: (i) imaging, (ii) deposition, and (iii) etching. These processes are supplemented by doping, cleaning, and planarization steps.

The process starts with a mono-crystal silicon wafer as a substrate. Photolithography is used to mark different areas of the substrate to be doped or to deposit polysilicon, insulators or metal tracks. This is done over several layers. The wafer is cut into rectangular blocks, each called a die. The die is then connected to a package.

There are many different technologies for packaging. In the flip-chip ball grid array (FCBGA) package, the die is mounted upside down (flipped) and connects to the package balls via a package substrate that is similar to a circuit board rather than by wires. This allows an array of input–output signals to be distributed over the entire die.[6]

The reliability of chips has received a lot of attention since its appearance. Roesch (2006) presents a historical review of IC reliability for silicon and compound semiconductors. The different reliability eras, and the focus of attention in each era, for the silicon case are indicated below.

First era (1975–1980): Learning about material properties of silicon (Si), aluminium (Al), and silicon oxide (SiO_2) and their various interactions for reliability improvement.

Second era (1980–1985): Identification and study of the mechanisms for the major reliability problems such as electro-migration, stress migration, time-dependent dielectric breakdown (TDDB), cracked die, broken bond wires, and so on.

Third era (1985–1990): Developing degradation models for the different mechanisms (reliability physics) and deriving the acceleration factors for the environmental stresses of temperature cycling and corrosion.[7]

Fourth era (1990–1995): Building-in-reliability (BIR) with a lot of emphasis on wafer-level reliability.

Fifth era (1995–2000): Merging the metrics of reliability and quality with a focus on a major defect-reduction effort.

[6] For more details of IC, see Mead and Conway (1980); Hodges et al. (2003).

[7] For more details of the failure mechanisms in semiconductor devices, see Amerasekera and Campbell (1987).