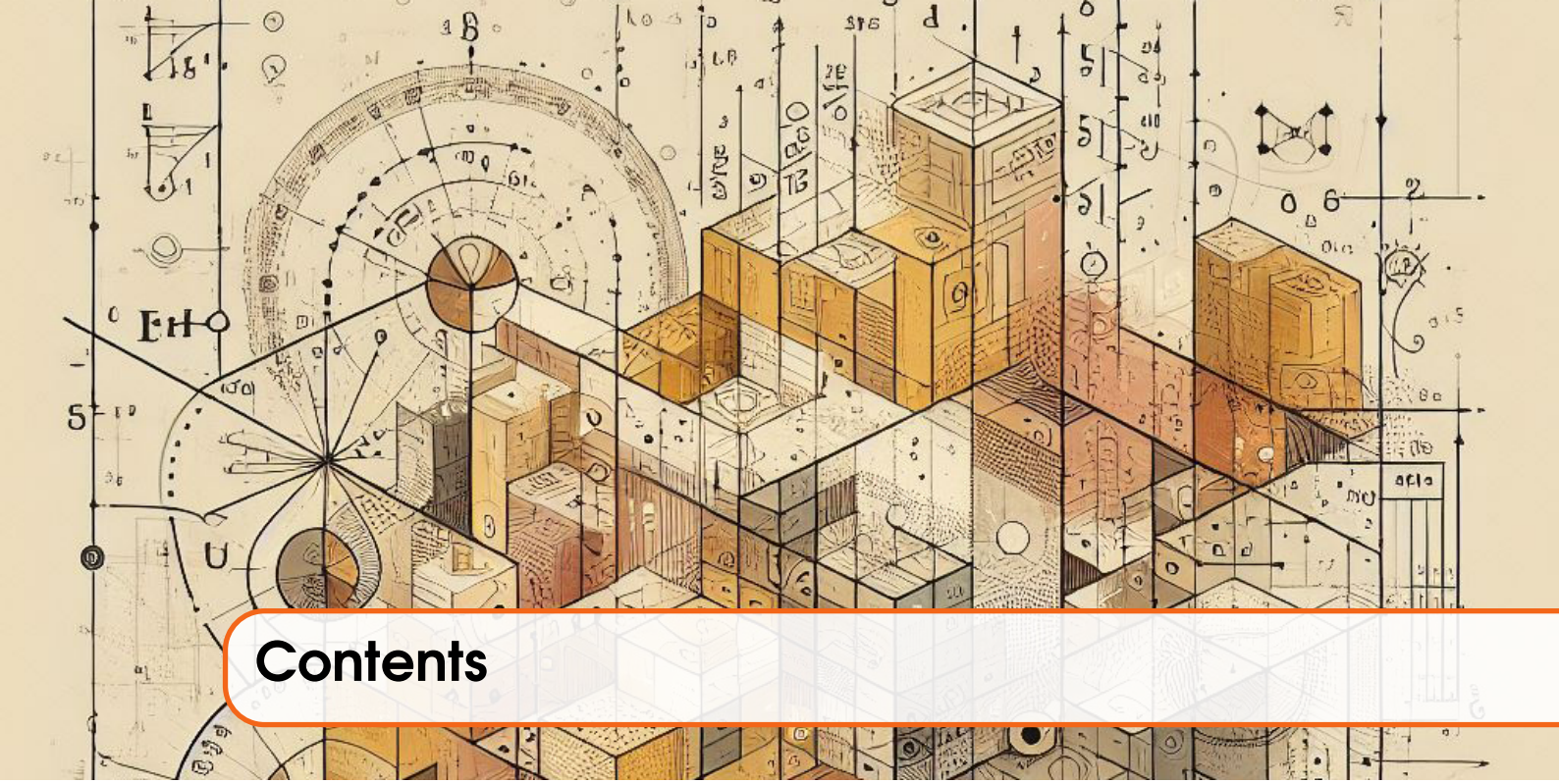
Student Textbook

Reliability Fault Tolerance

Dan Ștefan Tudose

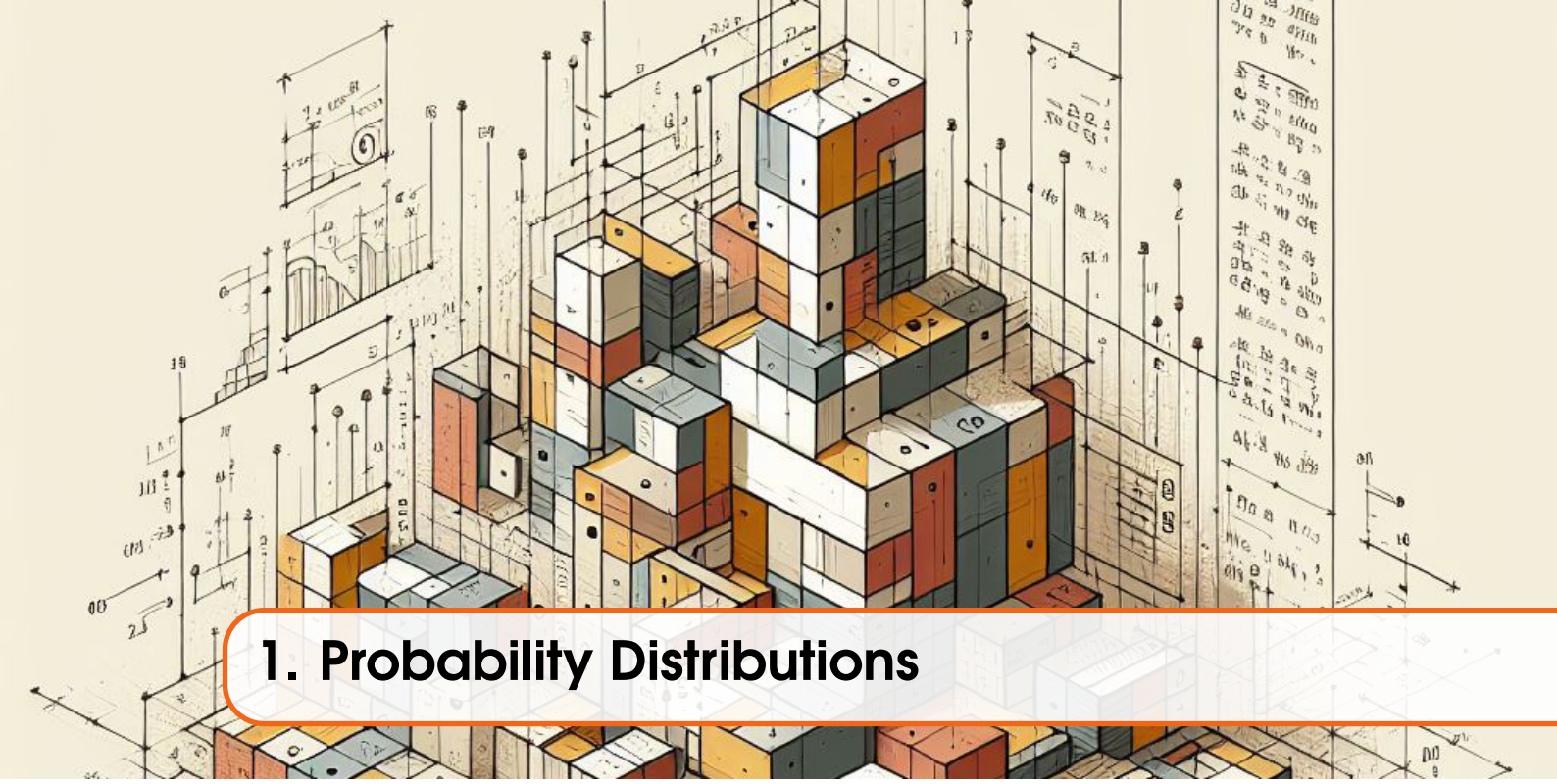
AS OF YET, UNPUBLISHED. PROBABLY NEVER WILL.

First printing, March 2024



Contents

Part One



1. Probability Distributions

1.1 Probability Theory Basics

Probability theory is the study of how likely it is that random events will occur. It is a branch of mathematics that is used in many different fields, including statistics, physics, economics, and engineering.

Random events are events that cannot be predicted with certainty, but that can still be described according to their likelihood. For example, the outcome of a coin toss is a random event, because it is impossible to predict whether the coin will land heads or tails before it is tossed. However, we can still describe the likelihood of each outcome based on the fact that there are two equally likely possibilities.

Probability theory provides a mathematical framework for describing the likelihood of random events. It does this by using probability measures, which assign a value between 0 and 1 to each event. A probability of 0 means that the event is impossible, a probability of 1 means that the event is certain, and a probability between 0 and 1 means that the event is possible, but not certain.

There are two main types of probability measures: discrete probability measures and continuous probability measures. Discrete probability measures are used to describe the likelihood of discrete events, such as the outcome of a coin toss or the number of heads that appear when a fair coin is tossed 10 times. Continuous probability measures are used to describe the likelihood of continuous events, such as the height of a randomly selected person or the temperature on a random day in June.

The first axiom of probability theory states that the value of probability of an event A lies between 0 (impossibility) and 1 (certainty):

$$0 \leq P(A) \leq 1 \tag{1.1}$$

$\overline{A}$ denotes the event "*not* A". For example, if A stands for "it rains", $\overline{A}$ stands for "it does not rain". The second axiom of probability theory says that the probability of an event A is equal to 1 minus the probability of the event A:

$$P(\overline{A}) = 1 - P(A) \tag{1.2}$$

Suppose that one event, A is dependent on another event, B. Then $P(A \mid B)$ denotes the conditional probability of event A, given event B. The fourth rule of probability theory states that the probability $P(A \cdot B)$ that both A and B will occur is equal to the probability that B occurs times the conditional probability $P(A \mid B)$:

$$P(A \cdot B) = P(A \mid B) \cdot P(B) \tag{1.3}$$

If P(B) is greater than zero, then equation 1.3 can be written as

$$P(A \mid B) = \frac{P(A \cdot B)}{P(B)} \tag{1.4}$$

An important condition that we will often assume is that two events are mutually independent. For events A and B to be independent, the probability *P(A)* does not depend on whether B has already occurred or not, and vice versa.

Thus, $P(A \mid B) = P(A)$. So, for independent events, the rule 1.4 reduces to

$$P(A \cdot B) = P(A) \cdot P(B) \tag{1.5}$$

This is the definition of independence, that the probability of two events both occurring is the product of the probabilities of each event occurring. Situations also arise when the events are mutually exclusive. That is, if A occurs, B cannot, and vice versa. As such, we can write the following

$$P(A \cdot B) = P(B \cdot A) = 0 \tag{1.6}$$

This is the definition of mutually exclusiveness, that the probability of two events both occurring is zero.

Let us now consider the situation when either A, or B, or both event may occur. The probability $P(A+B)$ is given by

$$P(A+B) = P(A) + P(B) - P(A \cdot B) \tag{1.7}$$

Combining 1.6 with 1.7, we get the following expression for mutually exclusive events

$$P(A+B) = P(A) + P(B) \tag{1.8}$$

1.2 Common Probability Distributions

Probability theory operates on a series of fundamental notions:

- Random experiment: any procedure that can be repeated indefinitely and has a well-defined set of possible outcomes.
- Sample space: the set of all possible outcomes of an experiment.
- Event: a subset of the sample space.
- Probability of an event: the number between 0 and 1 assigned to an event by a probability measure.

A simple example of a random experiment, and one that is frequently mentioned in probability theory textbooks is the toss of a coin. It has a defined set of possible outcomes: *heads*, *tails* which constitutes the sample space of the experiment. Each of the two events in the sample space, *heads* or *tails* has an associated probability of occurrence.

Another example of a random experiment is googling something or someone and measuring how fast the search was performed. The sample space is now made from all possible response times the search engine will report $\{t|t > 0\}$ and is no longer discrete, as in the coin toss experiment, but continuous.

A *random variable* is a variable that assigns a numerical value to each outcome in a sample space. In other words, it is a function that takes an outcome as an input and returns a number as an output. Random variables are used to quantify the uncertainty associated with random experiments.

There are two main types of random variables: discrete and continuous.

- *Discrete random variables* take on a finite or countably infinite number of values. A discrete random variable for the coin toss example could map *heads* to 1 and *tails* to 0, for example.
- *Continuous random variables* can take on any value within a certain interval. For the web search example above, the sample space is already composed of numbers, as the possible response times of the search query. This is a case in which the random variable could map the sample space to itself.

Contrary to their definition as functions, random variables are usually denoted with capital letters such as X, Y, T without including their parameter.

Given a random variable X that we use to map search engine response times, we can ask the question: "How likely is that the value of this random variable for a web search is equal to a tenth of a second?". We can write this as a probability $P(X = 0.1)$.

If we record all probabilities of all the outputs of a random variable X, we get the *probability distribution of X*.

Then we can ask another question: "What is the probability that a web search will yield a result in less than a tenth of a second?". To answer this, we will need to use the *cumulative distribution function* (CDF).

1.2.1 Cumulative Distribution Functions

The CDF of a random variable X is a function that gives the probability that X is less than or equal to a certain value x. We usually note CDF by $F_X(x)$, or, if the random variable is implicit or there's no ambiguity, just by $F(x)$:

$$F_X(x) = P(X \leq x) \tag{1.9}$$

CDF is a non-decreasing function, meaning that as x increases, the CDF(x) also increases.

The CDF is a useful tool for understanding the distribution of a random variable. It can be used to calculate probabilities, such as the probability that a random variable will be between two values.

■ **Example 1.1** For a coin toss experiment, we can define the CDF as:

$$F(x) = \begin{cases} 0 & ,x < 0 \\ q & ,0 \leq x < 1 \\ 1 & ,x \geq 1 \end{cases} \tag{1.10}$$

If the coin is fair, then $q = 0.5$. ■

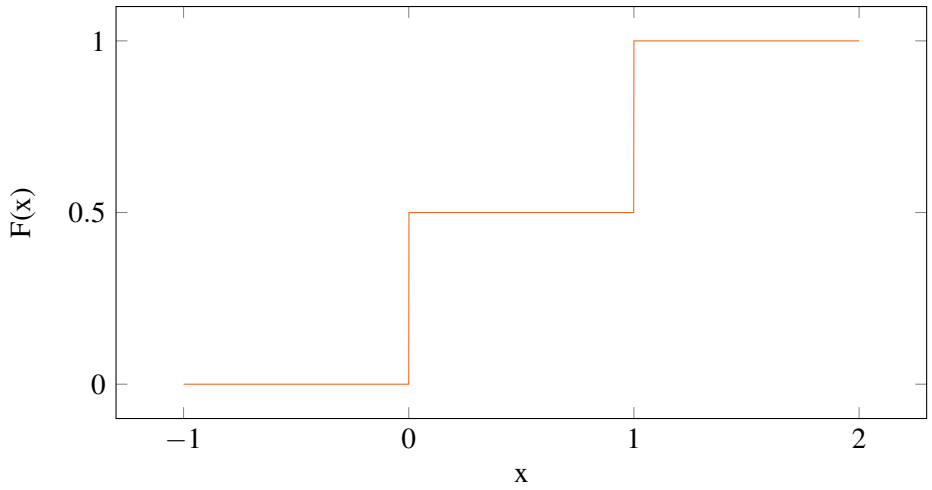


Figure 1.1: CDF of the random coin toss experiment

In computing, we are most often interested in time as a continuous random variable: time of completion of a certain query, system uptime, reliable operation time etc. Therefore, we will be frequently using CDF as $F(t)$ for positive values of time: $0 \leq t < \infty$.

Definition 1.2.1 — CDF Properties. The CDF for a continuous random variable that has only positive values has the following properties:

$$0 \leq F(t) \leq 1 \forall t \geq 0 \tag{1.11}$$
$$F(0) = 0 \tag{1.12}$$
$$\lim_{t \to \infty} F(t) = 1 \tag{1.13}$$
$$F(t) \textit{ is a monotone increasing function of time} \tag{1.14}$$

■ **Example 1.2** $F(t) = 1 + 2e^{-3t} - 3e^{-2t}$ is a valid CDF and is plotted in Figure 1.2. ■

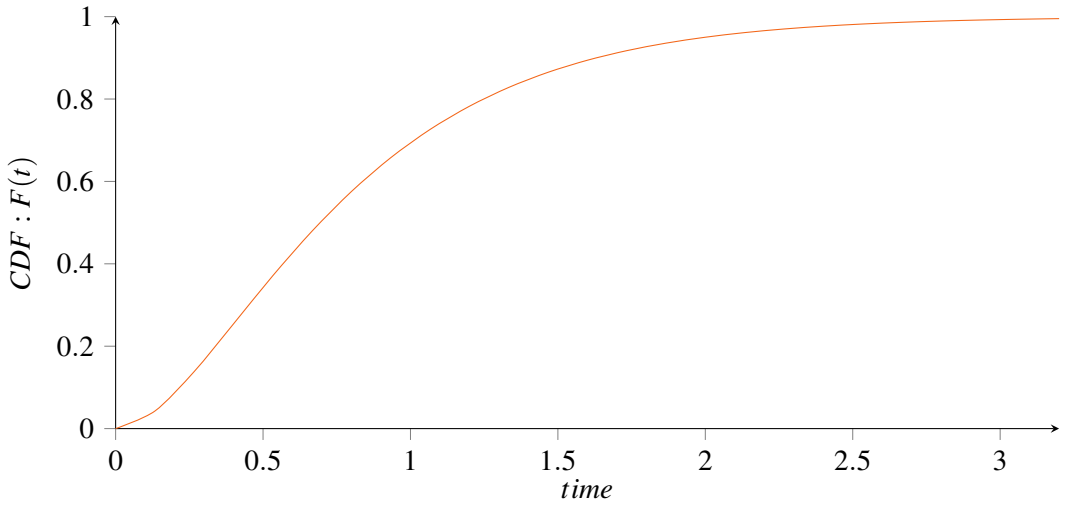


Figure 1.2: CDF of a continuous random variable

1.2.2 Probability Density Functions

Another important metric used in reliability is the *probability density function* (PDF) of a continuous random variable X. It is a function that describes the relative probability of each value of X and is denoted by $f(x)$.

In other words, the PDF gives the probability that X will take on a value in the infinitesimally small interval from x to $x + dx$.

For a continuous random variable X, there is an immediate link between the cumulative distribution function $F(x)$ and the probability density function $f(x)$:

$$f(x) = \frac{\mathrm{d}F(x)}{\mathrm{d}x} \tag{1.15}$$

Definition 1.2.2 — PDF Properties. Looking at the properties of the CDF $F(t)$, we can deduce the following properties for the PDF, $f(x)$:

$$\int_0^\infty f(x)dx = 1 \tag{1.16}$$

$$F(t) = \int_0^t f(x)dx \tag{1.17}$$

$$P(X \geq t) = \int_t^\infty f(x)dx \tag{1.18}$$

$$P(a \leq X \leq b) = \int_a^b f(x)dx = F(b) - F(a) \tag{1.19}$$

■ **Example 1.3** Taking our previous example of the CDF $F(t) = 1 + 2e^{-3t} - 3e^{-2t}$ we can derive $f(t) = -6e^{-3t} + 6e^{-2t}$, as plotted in Figure 1.3. ■

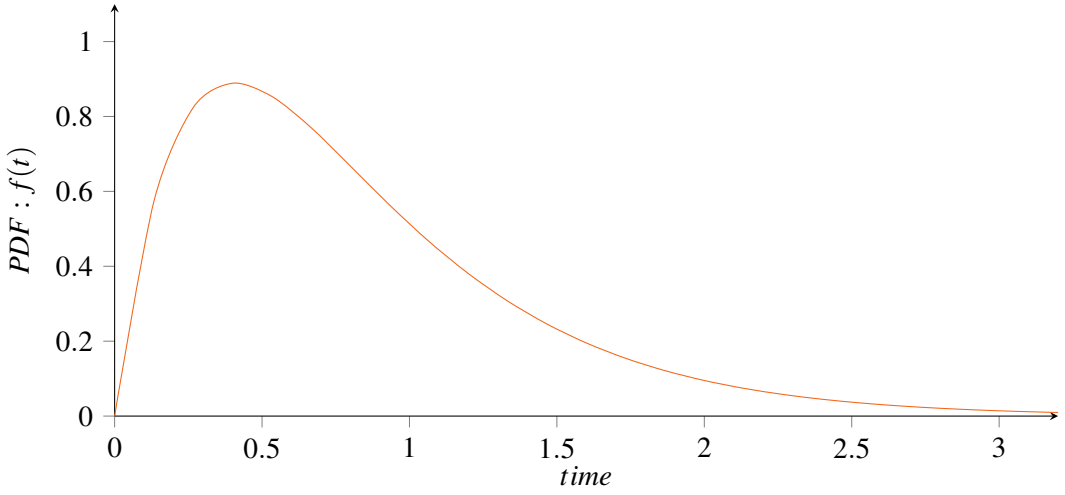


Figure 1.3: PDF of a continuous random variable

1.2.3 The Expected Value of a Random Variable

When dealing with random variables, a key objective is to identify the average value that represents the overall outcome of the underlying random experiment.

The *expected value* of a random variable, intuitively, is the long-run average value of repetitions of the experiment it represents.

For example, the expected value in rolling a six-sided die is 3.5 because, roughly speaking, the average of all the numbers that come up in an extremely large number of rolls is very nearly always quite close to three and a half.

Definition 1.2.3 — Expected value of a random variable. Suppose random variable X can take value x_1 with probability p_1, value x_2 with probability p_2, and so on, up to value x_k with probability p_k. Then the expected value of this random variable X is defined as:

$$E[X] = p_1x_1 + p_2x_2 + p_3x_3 + .. + p_kx_k \tag{1.20}$$

Since all probabilities p_i add up to one $(p_1 + p_2 + .. + p_k = 1)$, the expected value can be viewed

as the weighted average, with p_i being the weights:

$$E[X] = \frac{p_1x_1 + p_2x_2 + p_3x_3 + .. + p_kx_k}{1} = \frac{p_1x_1 + p_2x_2 + p_3x_3 + .. + p_kx_k}{p_1 + p_2 + .. + p_k} \tag{1.21}$$

■ **Example 1.4** Let X represent the outcome of a roll of a fair six-sided die. More specifically, X will be the number of pips showing on the top face of the die after the toss. The possible values for X are 1, 2, 3, 4, 5, and 6, all equally likely (each having the probability of $\frac{1}{6}$. The expectation of X is

$$E[X] = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = 3.5 \tag{1.22}$$

If one rolls the die n times and computes the average (arithmetic mean) of the results, then as n grows, the average will almost surely converge to the expected value, a fact known as the strong law of large numbers. One example sequence of ten rolls of the die is 2, 3, 1, 2, 5, 6, 2, 2, 2, 6, which has the average of 3.1, with the distance of 0.4 from the expected value of 3.5. The convergence is relatively slow: the probability that the average falls within the range 3.5±0.1 is 21.6% for ten rolls, 46.1% for a hundred rolls and 93.7% for a thousand rolls. ■

Definition 1.2.4 — Expected value for a continuous random variable. If the probability distribution of X admits a probability density function f(x), then the expected value can be computed as:

$$E[X] = \int_{-\infty}^{\infty} xf(x)dx \tag{1.23}$$

Since in most reliability calculations the random variable is time, which is quantified from 0 to infinity, we can simplify the previous expression to:

$$E[X] = \int_{0}^{\infty} tf(t)dt, \forall t \geq 0 \tag{1.24}$$

■ **Example 1.5** Taking our previous example of the probability density function $f(t) = -6e^{-3t} + 6e^{-2t}$, we can assess its expected value by plugging it into the previous equation:

$$E[X] = \int_{0}^{\infty} t\left(-6e^{-3t} + 6e^{-2t}\right) dt = \left(\frac{1}{6}e^{-3t}(12t - 9e^{t}(2t+1) + 4) + c\right)\Big|_{0}^{\infty} = \frac{5}{6} \tag{1.25}$$

■

1.2.4 Probability Distributions Commonly Used in Reliability

Probability distributions play a crucial role in reliability assessment. For discrete random variables, the binomial and Poisson distributions are particularly useful. When dealing with continuous random variables, the normal, Weibull, and exponential distributions are commonly employed. Additionally, the lognormal, the uniform distribution, Student's t-distribution, and chi-square (χ^2) distribution find applications in specific reliability evaluation scenarios.

The Binomial Distribution

The binomial distribution is a discrete probability distribution that calculates the likelihood of obtaining x positive outcomes in n trials, given that the probability of success in each trial is p. It's frequently used to model real-world scenarios involving discrete events, such as the number of heads in multiple coin flips or the number of defective items in a batch.

Definition 1.2.5 — Probability function of the binomial distribution. We can attach a probability function to the binomial distribution as follows:

$$p(x) = C_n^x p^x (1-p)^{n-x} \tag{1.26}$$

■ **Example 1.6** Imagine a scenario where you're inspecting a batch of 100 light bulbs to determine the proportion of faulty ones. If you know that the overall defect rate is 5%, the binomial distribution can help you predict the probability of finding a specific number of defective bulbs in your sample. For instance, the probability of finding exactly 2 defective bulbs in your sample can be calculated using the binomial distribution formula:

$$p(x=2) = C_{100}^2 0.05^2 (1-0.05)^{100-2} \approx 0.081(8.1\%) \tag{1.27}$$

■

The Poisson Distribution

The Poisson distribution is a discrete probability distribution that models the number of events that occur in a fixed interval of time or space, given a known average rate of occurrence. It is named after French mathematician Simeon Denis Poisson, who introduced the distribution in 1837.

The Poisson distribution is better suited than the binomial distribution for events that have a low probability of occurrence.

Definition 1.2.6 — Probability function of the Poisson distribution. The function is characterized by the average rate of occurrence λ (lambda) that has a value of $\lambda = p \times n$, where n is the number of trials, given that the probability of success in each trial is p:

$$p(x) = \frac{\lambda^x e^{-\lambda}}{x!} \tag{1.28}$$

■ **Example 1.7** Using the same light bulb example from the binomial distribution, we can calculate the probability of getting 2 defective light bulbs in a batch of 100, if the defect rate is 5% as:

$$\lambda = 0.05 \times 100 \tag{1.29}$$

$$p(x=2) = \frac{\lambda^2 e^{-\lambda}}{2!} \approx 0.09(9\%) \tag{1.30}$$

■

The Normal Distribution

The normal distribution, also known as the Gaussian distribution, is one of the most widely used probability distributions in statistics. It is a continuous probability distribution that is bell-shaped, symmetrical, and unimodal. This means that most of the data points in a normal distribution are clustered around the middle of the distribution, and the distribution tails off gradually towards either extreme.

Definition 1.2.7 — Probability function of the normal distribution. The normal distribution has the following probability density function:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2\right) \tag{1.31}$$

The normal distribution is also characterized by its mean μ and standard deviation σ. The mean is the average of all the data points in the distribution, and the standard deviation is a measure of how spread out the data is:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i-\mu)^2}{n-1}} \tag{1.32}$$

, where μ is the mean:

$$\mu = \frac{\sum_{i=1}^{n} x_i}{n} \tag{1.33}$$

The CDF of the normal distribution is expressed as:

$$F(x) = \int_{-\infty}^{x} f(t), dt = \frac{1}{2}\left[1 + \text{erf}\left(\frac{x-\mu}{\sigma\sqrt{2}}\right)\right] \tag{1.34}$$

, where $erf(x)$ is the error function and gives the probability of a random variable with normal distribution falling in the range $[-x, x]$

The normal distribution is often used to model data that is naturally occurring, such as heights of people or test scores. It is also used in many statistical analyses, such as hypothesis testing and confidence intervals.

One particular case is the *standard normal distribution* which is a normal distribution with $\mu = 0$ and $\sigma = 1$ (Figure 1.4)

The Weibull Distribution

The Weibull distribution is a continuous probability distribution with a wide range of applications in reliability analysis and modeling the lifetime of components. It is characterized by its shape parameter, which determines the shape of the distribution, and its scale parameter, which determines the scale of the distribution.

Definition 1.2.8 — Probability function of the Weibull distribution. The Weibull distribution has the following probability density function, where λ represents the *scale* parameter and β represents the *shape* parameter:

$$f(x) = \frac{\beta}{\lambda}\left(\frac{x}{\lambda}\right)^{\beta-1} e^{-(x/\lambda)^\beta} \tag{1.35}$$

The cumulative distribution function (CDF) of the Weibull distribution is given by:

$$F(x) = 1 - e^{-(x/\lambda)^\beta} \tag{1.36}$$

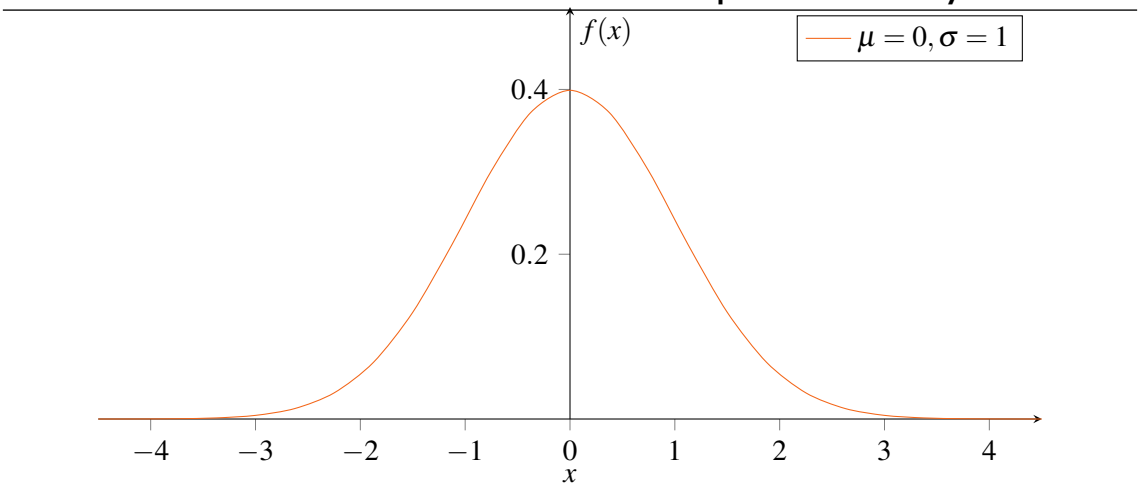


Figure 1.4: Standard normal distribution probability density function

The Weibull distribution is often used to model the failure times of components that experience wear and tear over time. It is also used to model the lifetimes of biological organisms and the times between events in a variety of other applications.

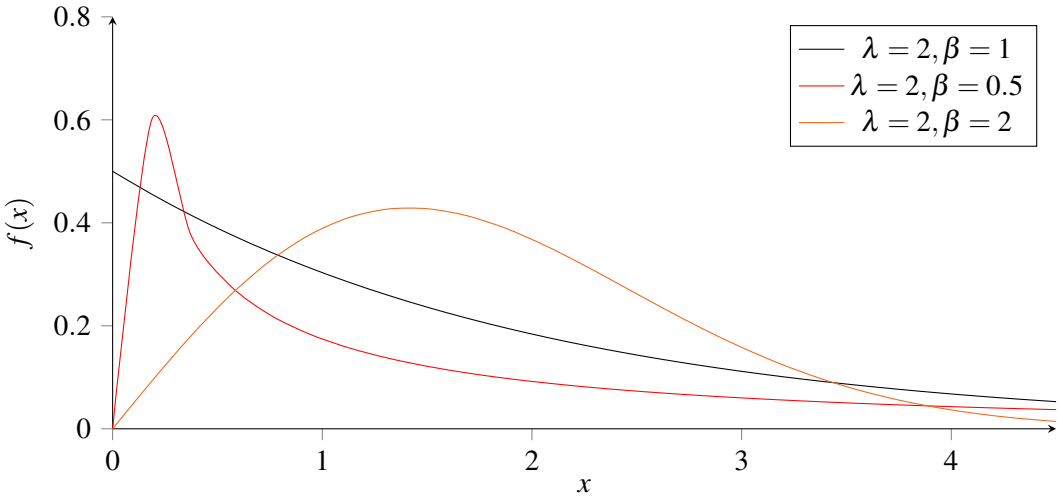


Figure 1.5: Weibull distribution probability density function for different values of λ and β

When the time duration until a failure occurs is represented by the random variable X, the Weibull distribution provides a probability distribution where the failure rate is directly proportional to a power of time. The shape parameter, β, corresponds to that power plus one, allowing for a straightforward interpretation of its value:

- $\beta < 1$: The failure rate decreases over time. This scenario arises when there is a significant amount of "infant mortality," meaning defective items fail early, and the failure rate diminishes as these defective items are gradually eliminated from the population.
- $\beta = 1$: The failure rate remains constant over time. This could indicate that random external events are causing failures or that the underlying failure mechanism is time-independent. In this case, the Weibull distribution simplifies to the exponential distribution.
- $\beta > 1$: The failure rate increases over time. This situation occurs when there is an "aging" process, where components become more prone to failure as time progresses. This could

be due to wear and tear, fatigue, or other cumulative factors that gradually degrade the component's integrity.

In summary, the Weibull distribution offers a flexible framework for modeling failure rates across various scenarios, ranging from decreasing failure rates due to infant mortality to increasing failure rates due to component aging.

The Exponential Distribution

The exponential distribution is a continuous probability distribution that describes the time between events in a Poisson process. It is a memoryless distribution, meaning that the probability of an event occurring in a given interval is independent of the time that has elapsed since the last event.

The exponential distribution is a special case of the Weibull distribution in which the shape parameter $\beta = 1$. Therefore, the exponential distribution is characterized only by its rate parameter, λ (lambda), which represents the average number of events that occur per unit of time.

Definition 1.2.9 — Probability function of the exponential distribution. The probability density function (PDF) of the exponential distribution depends on the *rate* parameter λ and can be written as:

$$f(x) = \lambda e^{-\lambda x} \tag{1.37}$$

The cumulative distribution function (CDF) of the exponential distribution is given by:

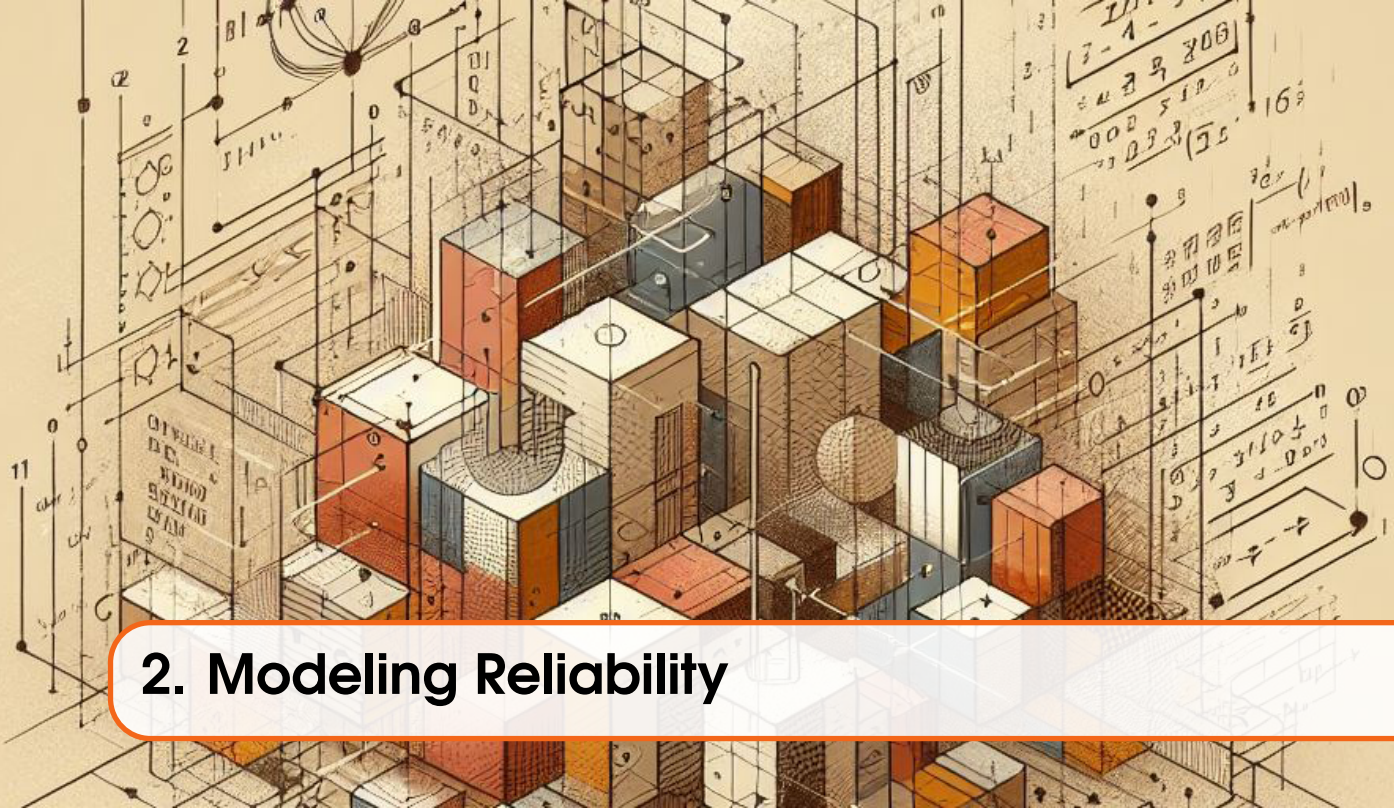
$$F(x) = 1 - e^{-\lambda x} \tag{1.38}$$

The exponential distribution is widely used in reliability analysis to model the time to failure of components. It is also used in other fields, such as queuing theory and survival analysis. Its memoryless property, meaning the likelihood of an event occurring in a specific interval is independent of the time elapsed since the previous event, makes it well-suited for modeling processes with independent inter-arrival times, such as:

- Networking traffic congestion: The exponential distribution is used to model the arrival and departure of data packets in congested networks. This helps in analyzing network performance under varying traffic conditions and identifying bottlenecks.
- Server performance: The exponential distribution is used to analyze the performance of servers in handling requests, such as web servers or file servers. This helps in predicting server response times and ensuring efficient resource utilization.
- Predictive analytics: The exponential distribution is used in predictive analytics models to forecast future events, such as system failures or traffic congestion patterns. This enables businesses to take proactive measures to prevent disruptions and optimize resource allocation.

■ **Example 1.8** We can use the exponential distribution to model the arrival of web requests: suppose that the average number of web requests per minute is 10. The rate parameter can then be calculated as $\lambda = 10$. Using this rate parameter, we can calculate the probability of receiving a web request in any given minute. The probability of receiving a request in the next minute is $1 - e^{-10} \approx 0.995$. ■

■ **Example 1.9** The exponential distribution can also be used to model the waiting time for a web request. The waiting time is the time that it takes for a request to be queued up and processed by the web server. The waiting time can be calculated by using the cumulative distribution function (CDF) of the exponential distribution. For example, the probability of waiting for more than 10 seconds for a web request is $1 - F(10) \approx 0.368$. ■



2. Modeling Reliability

2.1 Reliability and Availability

Fault tolerance is the ability of a system to continue functioning in spite of malfunctions or faults. As a notion, it is tightly coupled with the concept of reliability, the lack of defects and the availability of a system.

2.1.1 Reliability

The reliability of a system is its ability to function correctly over a given time period. Mathematically, the *reliability R(t)* of a system at time t is the probability that the system operates without failure in the interval [0,t), given that the system was performing correctly at time 0. As a probability function, its values lie in the [0, 1] interval.

Definition 2.1.1 — Reliability function. We can express the reliability of a system S at time t by:

$$R(t) = P(S \text{ is fully operational in } [0,t]) \tag{2.1}$$

Notice that we are assuming the system is functioning until it completely stops its normal operation and we are not factoring in the possibility of the system to be repaired. This measure is suitable for applications in which even a momentary disruption can prove costly, for example the autopilot system of a passenger airplane, for which failure would result in catastrophe.

We can consider a random variable X to be the lifetime, or the time until a failure occurs for system S. We can also consider $F(t)$ to be the corresponding cumulative distribution function (CDF) for the random variable X. We can then write the system reliability as:

$$R(t) = P(X > t) = 1 - F(t) \tag{2.2}$$

It is usually considered that the system in operation at $t = 0$ without any faults, therefore we can write that $R(0) = 1$. Also, as it is deeply ingrained in this Universe that any working system will cease to operate at some future point in time, we can assume $\lim_{t\to\infty} R(t) = 0$.

We can therefore infer that R(t) is a decreasing, continuous, monotone function with values ranging between 0 and 1 in the interval $[0, \infty)$ as in Figure 2.1.

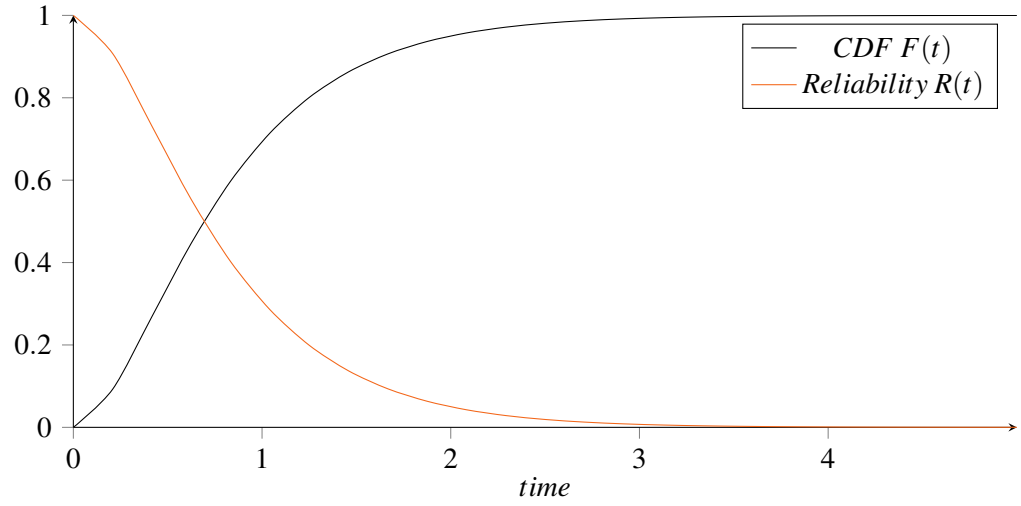


Figure 2.1: Relationship between Reliability and the CDF of a system

Let us consider $f(t)$ the probability density function (PDF) of the system. We have already established its relationship with the CDF of the system to be $F(t) = \int_0^t f(\tau)d\tau$, therefore we can infer that the reliability function, as the inverse of the CDF, can be written as:

$$R(t) = \int_t^{\infty} f(\tau)d\tau \tag{2.3}$$

Therefore, in a graphical representation, reliability $R(t)$ represents the area under the $f(t)$ curve from t to infinity, as in Figure 2.2.

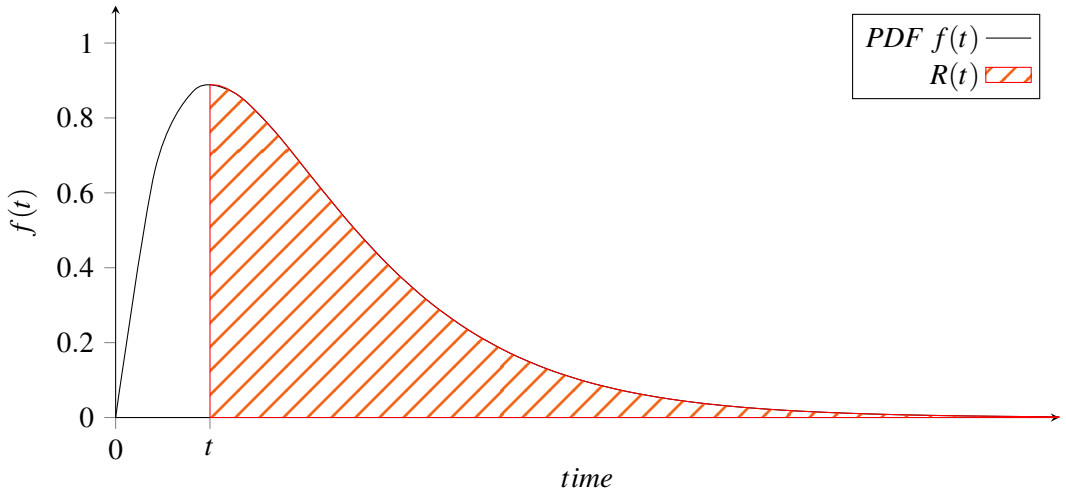


Figure 2.2: Graphical representation of the meaning of Reliability

2.1.2 Failure Rate

So far we have quantified the probability of a fault not happening in a given time interval. It is also of interest to determine the probability a fault will happen at a given time, or, in a quantifiable small interval $[t, t+\Delta t]$, given that the system has functioned properly until time t. We can write this probability as:

$$P(t < X < t+\Delta t \mid X > t) = \frac{P(t < X < t+\Delta t)}{P(X > t)} = \frac{F(t+\Delta t) - F(t)}{R(t)} \tag{2.4}$$

Definition 2.1.2 — Failure rate. The *instantaneous failure rate*, also named *the hazard function* or the age-dependent *failure rate* of the system is defined as:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{F(t+\Delta t) - F(t)}{R(t)\Delta t} = \lim_{\Delta t \to 0} \frac{R(t) - R(t+\Delta t)}{R(t)\Delta t} = \frac{f(t)}{R(t)} \tag{2.5}$$

Plotting the failure rate as a function of time to time yields a distinctive shape called the "bathtub curve", such as the one in Figure 2.3.

Manufacturing or design defects tend to lead to failure in the initial stage of a product's life. This stage is also known as "infant mortality" and is characterized by a large but decreasing failure rate, as more products are eliminated from the initial batch due to failures. Infant mortality can be eliminated at the manufacturing stage through system testing and accelerated aging of the product before it is sold or released into circulation.

Once this stage is over, the product enters a period in which failure rate is constant. This is usually the stage at which the product experiences its entire useful life. Fault rate is non-zero but low and is typically due to environmental conditions.

In the last stage, failure rate increases due to extensive wear. A failure becomes more likely as more time goes by, until all of the products from the initial population become defective.

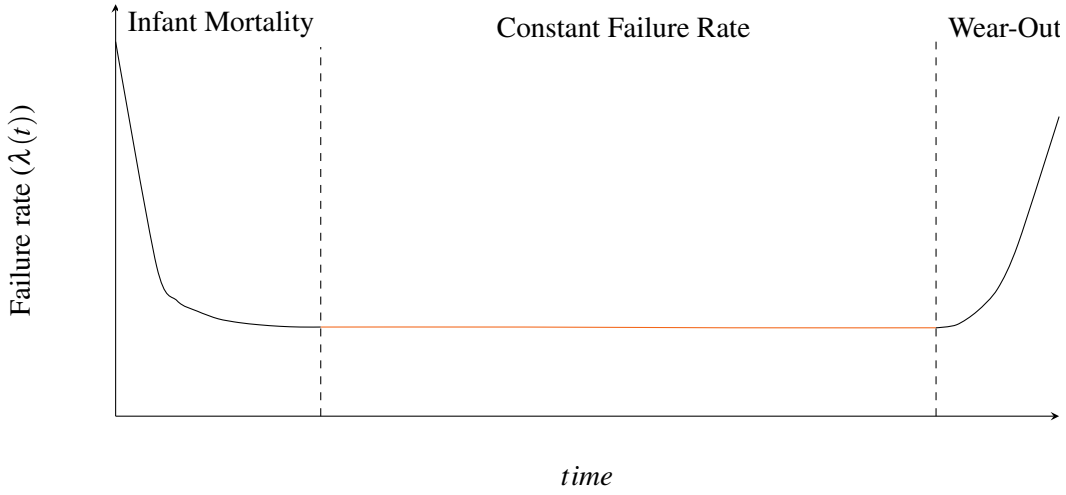


Figure 2.3: Bathtub curve for the failure rate of a system

In engineering and reliability analysis, the failure rate λ of a system or component is the frequency with which it fails, expressed in failures per unit of time. It represents the probability of a failure occurring within a specified time interval. The failure rate is a key metric for understanding

the reliability and lifespan of a system, and it can be used to make informed decisions about maintenance and replacement schedules.

Failure rates can be calculated in different ways, depending on the type of system and the available data. For example, the failure rate of a component may be calculated based on historical data of failures, or it may be estimated using statistical methods or accelerated life tests.

■ **Example 2.1** Usually, failure rate is expressed as a constant and is measured in failures per unit of time. For example, a light bulb might have a measured failure rate of 0.001 failures per hour, a solid-state drive might have 0.000015 failures per hour and a passenger airplane a typical failure rate of 0.000000001 per hour ■

Failure rates can be affected by a number of factors, including the design of the system, the quality of the components, and the operating environment.

The impact of these factors can be expressed through the following empirical failure rate formula:

$$\lambda = \pi_L \pi_Q (C_1 \pi_T \pi_V + C_2 \pi_E) \tag{2.6}$$

where the notations are as follows:

- λ - Failure rate of component.
- π_L - Learning factor, associated with how mature the technology is.
- π_Q - Quality factor, representing manufacturing process quality control (ranging from 0.25 to 20.00).
- π_T - Temperature factor, with values ranging from 0.1 to 1000. It is proportional to $e^{\frac{E_a}{kT}}$, where E_a is the activation energy in electron-volts associated with the technology, k is the Boltzmann constant ($8.6173 \times 10^{-5} eV/K$), and T is the temperature in Kelvin.
- π_V - Voltage stress factor for CMOS devices; can range from 1 to 10, depending on the supply voltage and the temperature; does not apply to other technologies (where it is set to 1).
- π_E - Environment shock factor; ranges from very low (about 0.4), when the component is in an air-conditioned office environment, to very high (13.0) when it is in a harsh environment.
- C_1, C_2 - Complexity factors; functions of the number of gates on the chip and the number of pins in the package.

This formula was taken from MIL-HDBK-217E, MILITARY HANDBOOK: RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT (27 OCT 1986), written by the U.S. Department of Defense to address reliability modeling of their electronic equipment.

In the harsh environment of space, where charged particles abound and extreme temperature fluctuations occur, electronic devices are more prone to malfunctions compared to their counterparts in the controlled climate of air-conditioned offices. Similarly, computers in automobiles, subjected to intense heat and vibrations, and those in industrial settings, exposed to harsh conditions, face elevated failure rates.

Software failure rate usually decreases as a function of time. A possible curve is shown in Figure 2.4. The three phases of evolution are: test/debug (I), useful life (II) and obsolescence (III).

Software failure rate during useful life depends on the following factors:

1. software process used to develop the design and code
2. complexity of software,

3. size of software,
4. experience of the development team,
5. percentage of code reused from a previous stable project,
6. rigor and depth of testing at test/debug (I) phase.

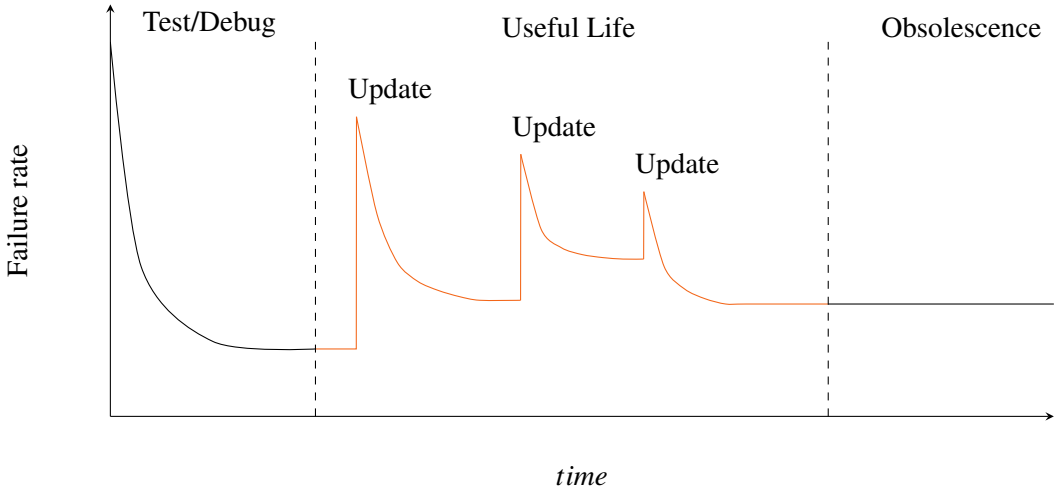


Figure 2.4: The failure rate curve for software versus time

Compared to hardware, software failure curves exhibit two distinct characteristics. Firstly, software's failure rate tends to spike after each feature update during its useful-life phase. This is because upgrades often introduce new functionalities, leading to increased complexity and consequently a higher likelihood of faults. However, following the initial surge in failures, the rate gradually stabilizes, partly due to bug fixes implemented after the upgrades. Secondly, unlike hardware, software does not experience a progressive increase in failure rate during its final phase. In this stage, software approaches obsolescence, and the need for further upgrades or modifications diminishes.

2.1.3 Mean Time Between Failures

Another metric to assess a system's fault tolerance is the *Mean Time Between Failures* (MTBF). This parameter is derived from observing the system's behavior during its operational lifespan. The simplest model incorporating fault tolerance assumes the system transitions between two states: fully operational and completely failed. These transitions occur upon failure or after system repair, as depicted in Figure 2.5.

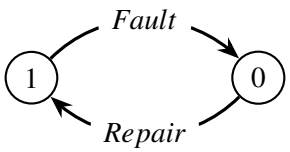


Figure 2.5: Simple state transition graph for a system with failure and repair

This two-state model can be applied to simple systems like light bulbs, which can either illuminate or be burned out, and wires in circuits, which can either be connected or interrupted. It can also be extended to more complex systems like cars and web servers, but the definitions of "operational" and "failed" need to be tailored to the specific context. For instance, an operational web server would

be fully responsive to client requests, while a failed web server could be completely unresponsive due to a crash or undergoing maintenance.

Visualizing the system's behavior over time reveals alternating intervals of operational periods and repair downtime. As depicted in Figure 2.6, the system initially operates until it encounters a failure, marking the end of the first Time-To-Fail (TTF_1) interval. Subsequently, the system transitions into the first Time-To-Repair (TTR_1) interval, representing the time it takes to restore functionality. This pattern of alternating operational and repair intervals persists throughout the system's lifespan.

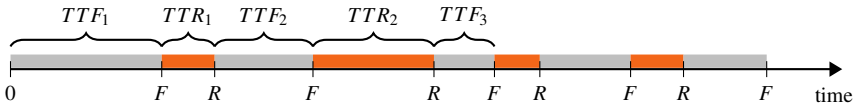


Figure 2.6: The lifetime of a system with consecutive functioning and repair episodes

Measuring these intervals and averaging their values over a long observational period yields two important metrics: the *Mean Time to Failure*, or *MTTF* which is an average of all Time-To-Fail (TTF) intervals, and the *Mean Time to Repair*, or *MTTR*, which is the average of all Time-To-Repair intervals.

$$MTTF = \sum_i \frac{TTF_i}{n} \qquad MTTR = \sum_i \frac{TTR_i}{n} \tag{2.7}$$

Definition 2.1.3 — Mean Time Between Failures. Using the above two notions, we can define the *Mean Time Between Failures, MTBF* as the average expected time between two failures for a repairable system:

$$MTBF = MTTF + MTTR \tag{2.8}$$

2.1.4 Availability

Few systems are designed to run indefinitely without downtime or maintenance. Typically, we care not only about system reliability but also about failure frequency and recovery time. For example, for web servers, we aim to maximize uptime, the proportion of time the system is operational. This metric is captured by *Availability*.

The system's *Availability A(t)* at time t denotes the likelihood that the system is operating correctly at that specific moment. A(t) is alternatively known as point availability or instantaneous availability. This metric is suitable for scenarios where continuous performance is not crucial, yet prolonged system downtime would incur substantial costs. For instance, an airline reservation system requires high availability to avoid customer dissatisfaction and revenue loss due to downtime. However, occasional very brief failures can be tolerable in such a system.

Definition 2.1.4 — Interval Availability. Often it is necessary to determine the *Interval*, or *Mission Availability*. It is defined by:

$$A(T) = \frac{1}{T}\int_0^T A(t)dt \tag{2.9}$$

A(T) is the value of the point availability averaged over some interval of time T. This interval might be the life-time of a system or the time to accomplish some particular task.

Ultimately, it is frequently observed that following an initial transient impact, point availability stabilizes to a time-independent value. In such instances, we refer to it as *Steady-state availability*, alternatively recognized as Long-term Availability denoted by $A(\infty)$.

Definition 2.1.5 — Steady-State Availability.

$$A(\infty) = \lim_{T\to\infty} A(T) = \lim_{T\to\infty} \left(\frac{1}{T} \int_0^T A(t)dt \right) \tag{2.10}$$

The interpretation of $A(\infty)$ lies in its representation as the probability that the system will be operational at a randomly chosen moment, and its relevance is confined to systems incorporating the repair of defective components. In cases where a system is irrepairable, the point availability $A(t)$ aligns with the system's reliability—namely, the probability that the system remains operational from time 0 to t. Consequently, as the time duration T approaches infinity, the steady-state availability of a non-repairable system converges to zero:

$$A(\infty) = 0 \tag{2.11}$$

The long-term availability $A(\infty)$, or more simply written A, can be calculated from MTTF, MTBF, and MTTR as follows:

$$A = \frac{MTTF}{MTBF} = \frac{MTTF}{MTTF + MTTR} \tag{2.12}$$

■ **Example 2.2** A system with low reliability can still exhibit high availability. For example, imagine a communication channel that is down every couple of hours but its takes only 3 seconds to reestablish connection. We can compute the MTBF as 2 hours (7200 seconds) and the MTR as 3 seconds. Even if the reliability of such a communication link is low, its availability is quite high: $A = 7200/7203 = 99.96\%$. ■

Steady-state availability is often specified in terms of downtime per year. Table 2.1 shows examples for some of the values for availability and the corresponding downtime.

Availability(%)	Downtime per year	Downtime per month	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
99% ("two nines")	3.65 days	7.2 hours	1.68 hours
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

Table 2.1: Availability and the corresponding downtime per year.

Availability stands as an essential metric, particularly for systems that can endure short interruptions. Networked systems, such as telephone switching and web servers, provide concrete illustrations of this principle. Telephone users anticipate seamless call completion without disruptions, accepting an annual downtime of up to three minutes. Research indicates that web users' tolerance diminishes if websites take more than eight seconds to display results. Consequently, these websites must maintain continuous availability and swift responsiveness, even amid substantial concurrent user traffic.

The electrical power control system serves as another notable example. Consumers expect an uninterrupted power supply 24/7, regardless of weather conditions. Prolonged power outages can pose health risks, disrupting essential services like water pumps, heating, lighting, and medical care. Industries also face substantial financial losses in the event of power disruptions.

2.2 Failure Rate, Reliability, and Mean Time to Failure for an Exponential Fault Distribution

In this section we will approach the derivation of reliability and Mean Time Between Failures (MTBF) from the fundamental concept of failure rate. We focus on a component operational at t=0 and sustained in operation until encountering a failure. Our consideration involves the assumption that failures adhere to an exponential probability distribution.

Let's now assume that all failures are permanent and irreparable. Let T represent the random variable "lifetime of the component" (indicating the time until failure). Additionally, let f(t) and F(t) denote the probability density function (PDF) of T and the cumulative distribution function (CDF) of T, respectively. As established in the preceding chapter, we determined that these functions are interrelated as follows:

$$f(t) = \frac{dF(t)}{dt} \qquad F(t) = \int_0^t f(\tau)d\tau \quad \forall t \geq 0 \tag{2.13}$$

The PDF f(t) can be understood as the probability the system will fail at time t. For a tiny $\Delta t, f(t)\Delta t \approx Prob(t \leq T \leq t + \Delta t)$. f(t) is a probability density function, therefore the following will be true:

$$\int_0^\infty f(t)dt = 1 \quad f(t) \geq 0, \forall t \geq 0 \tag{2.14}$$

In the context of the random variable defined above as the lifetime of a component, F(t) can be viewed as probability that the system will exhibit a failure anywhere in (0,t]:

$$F(t) = Prob(t \leq T) \tag{2.15}$$

Conversely, R(t) if the inverse of F(t) and can be defined as the probability the system functions without failure until time t:

$$R(t) = Prob(T > t) = 1 - F(t) \tag{2.16}$$

As we defined it in the previous chapter, the *failure rate* of a system $\lambda(t)$ gives us the probability the system will fail at time t:

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \tag{2.17}$$

Since $f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt}$, we can rewrite the expression above:

$$\lambda(t) = -\frac{dR(t)}{dt}\frac{1}{R(t)} \tag{2.18}$$

As previously mentioned, for the active life of a system we can consider the failure rate to be constant, $\lambda(t) = \lambda$. This simplifies the previous equation and makes it trivial to solve:

$$\frac{dR(t)}{dt} = -\lambda R(t) \tag{2.19}$$

We can assume R(0) = 1 and we can solve 2.19 for R(t):

$$R(t) = e^{-\lambda t} \tag{2.20}$$

This equation links the reliability of a system to its constant failure rate λ, if the system is within its normal operational lifetime (the flat constant region of the bathtub curve).

This is the *exponential failure law* and it is plotted in Figure 2.7.

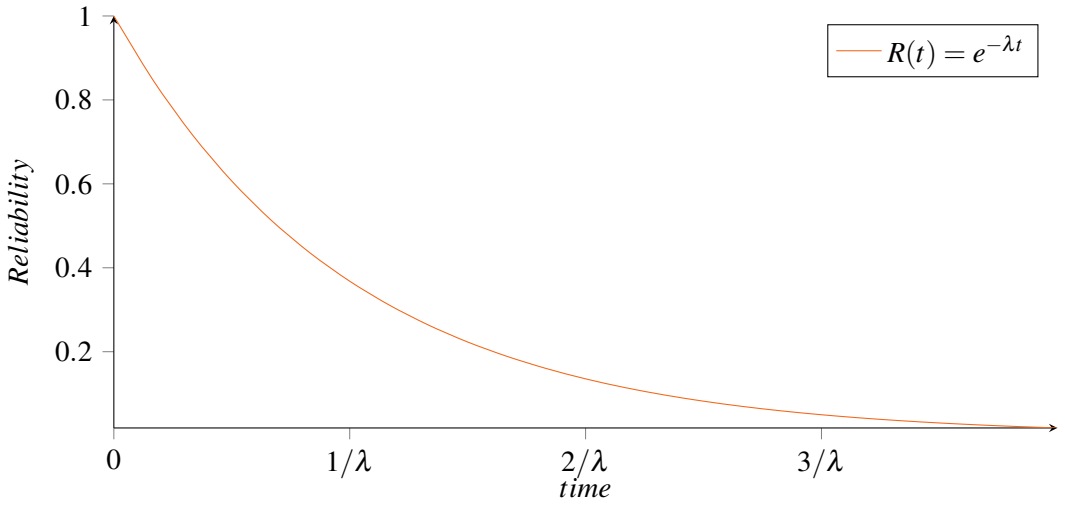


Figure 2.7: Reliability function for an exponential distribution of faults

The exponential failure law is very valuable for the analysis of reliability of components and systems in hardware. However, it can only be used in cases when the assumption that the failure rate is constant is adequate.

To summarize the definitions we have derived above:

$$f(t) = \lambda e^{-\lambda t} \qquad F(t) = 1 - e^{-\lambda t} \qquad R(t) = e^{-\lambda t} \qquad for\ t \geq 0 \tag{2.21}$$

Definition 2.2.1 — MTBF for an exponential fault distribution. By definition, the MTBF of an irreparable component is equal to its expected lifetime, E[T]. As the random variable is time, which is always greater than zero, we can rewrite 1.23 as:

$$MTBF = E[T] = \int_0^\infty t f(t) dt \tag{2.22}$$

Substituting $f(t) = -\frac{dR(t)}{dt}$ we get,

$$MTBF = -\int_0^\infty t\frac{dR(t)}{dt}dt = -tR(t)\,|_0^\infty + \int_0^\infty R(t)dt \tag{2.23}$$

The value of $-tR(t)$ is equal to 0 at $t = 0$ and also to zero at $t \to \infty$, as the reliability of every system asymptotically drops to zero given a long enough time, ($R(\infty) = 0$). Thus, we can write:

$$MTBF = \int_0^\infty R(t)dt \tag{2.24}$$

Given an exponential reliability function with a constant failure rate λ, we can rewrite 2.24 as:

$$MTBF = \int_0^\infty R(t)dt = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda} \tag{2.25}$$

2.2.1 Non-constant Failure Rate

Most reliability calculations imply a constant failure rate $\lambda = ct$. partly due to the fact that the analyzed system is thought to be in its operational lifetime, where failure occurrence is random and partly because a failure rate that is dependant of time will further complicate reliability formulas.

If we would like to model the reliability of a system in its "infant mortality" or its "wear-out" phases from Figure 2.3, we will need to employ the Weibull probability distribution, which models appropriately these states.

As presented in a previous section of this work, the Weibull distribution has two parameters, λ - the shape parameter and β - the scale parameter. We can rewrite equation 1.35 for $t \geq 0$ and get the PDF:

$$f(t) = \lambda\beta t^{\beta-1}e^{-\lambda t^\beta} \tag{2.26}$$

We can derive the failure rate, but in this case it will not be constant:

$$\lambda(t) = \lambda\beta t^{\beta-1} \tag{2.27}$$

By varying the value of β we have the following three cases:

- $\beta > 1$: failure rate is a decreasing function of time (used for modeling infant mortality).
- $\beta = 1$: failure rate is constant λ and we use the reliability formulas derived in the previous section for the exponential distribution.
- $\beta < 1$: failure rate is an increasing function of time (modeling wear-out).

We can also derive the reliability function when using a Weibull distribution by plugging in the new formula for $\lambda(t)$ in equation 2.18 and solving for R(t):

$$R(t) = e^{-\lambda t^\beta} \tag{2.28}$$

Note that reliability now depends also of β and a similar discussion can be made for R(t)'s properties for $\beta < 1$, $beta = 1$ and $beta > 1$.

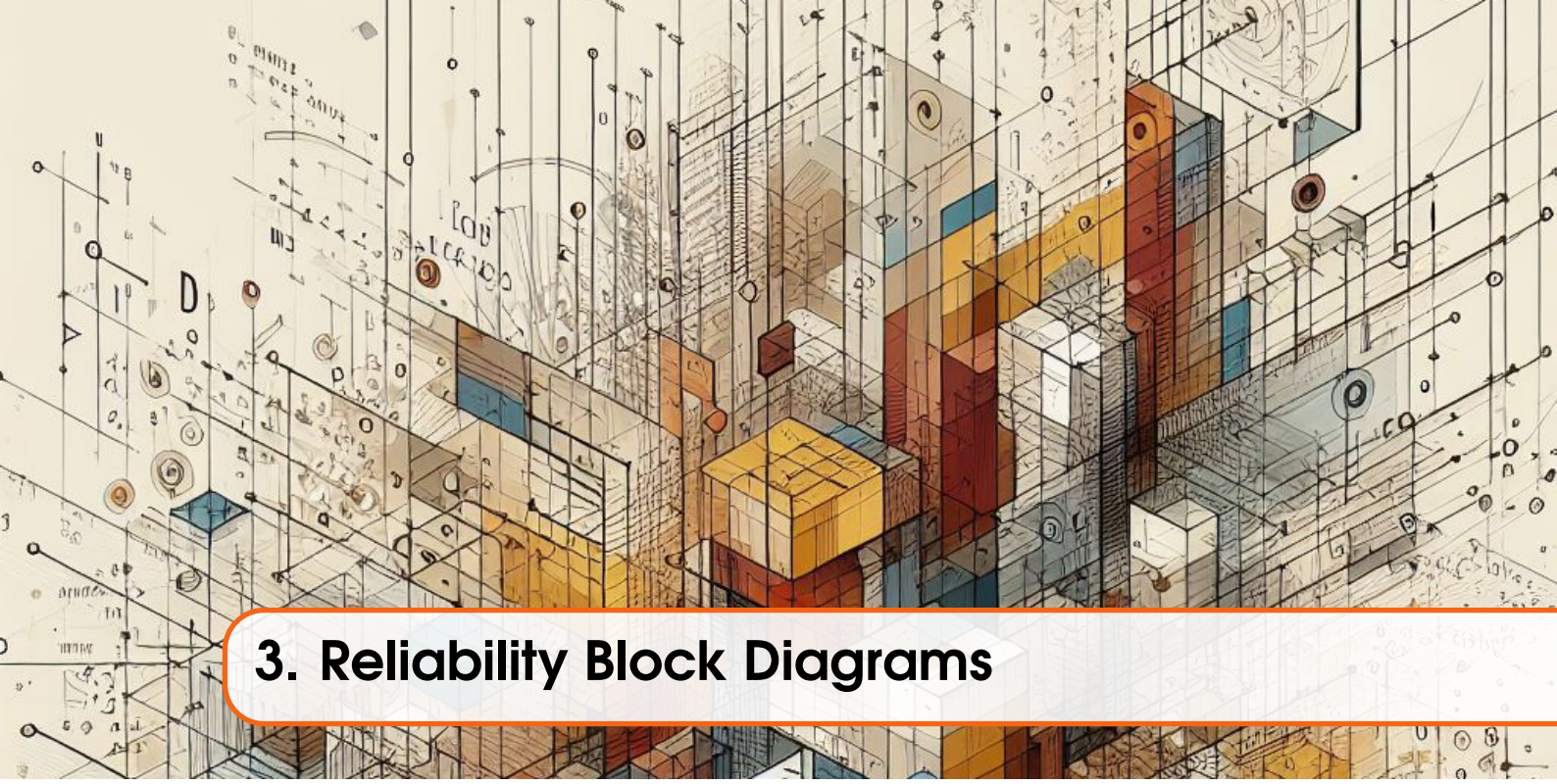
We can also derive the MTBF from this new reliability formula as:

$$MTBF = \int_0^\infty R(t)dt = \frac{\Gamma(\beta^{-1})}{\beta\lambda^{\beta-1}} \tag{2.29}$$

Definition 2.2.2 — Gamma function. $\Gamma(x)$ is the gamma function, which is an extension of the factorial function for real number values. It can be computed that $\Gamma(x) = \int_0^\infty y^{x-1}e^{-y}dy$, and, as a factorial function, it will also satisfy the following:

$\Gamma(0) = \Gamma(1) = 1$
$\Gamma(x+1) = (x)\Gamma(x) \ \ \forall x > 1$
If x is a positive integer, then $\Gamma(x) = (x-1)!$

Part Two



3. Reliability Block Diagrams

3.1 Modeling Reliability Through Blocks

Within the realm of combinatorial reliability models, reliability block diagrams (RBDs) have emerged as the most established and prevalent method for analyzing system reliability. These diagrams offer a simplified representation of a system's structure and component reliability, utilizing blocks to denote individual components and interconnections between blocks to depict the operational dependencies among them.

RBDs provide a clear and intuitive graphical representation of system structure and dependencies, facilitating a straightforward understanding of system behavior. They also enable the calculation of various reliability metrics, such as system availability, reliability, and mean time to failure (MTTF), providing valuable insights into system performance.

Also, RBDs can be applied to a wide range of systems, from simple configurations to complex networks, making them a versatile tool for reliability assessment.

Using RBDs, we can represent, for example, components that are tied in series, as in Figure 3.1 a), components that are linked in parallel, as in Figure 3.1(b) or more complex systems that are combinations of series-parallel connections.

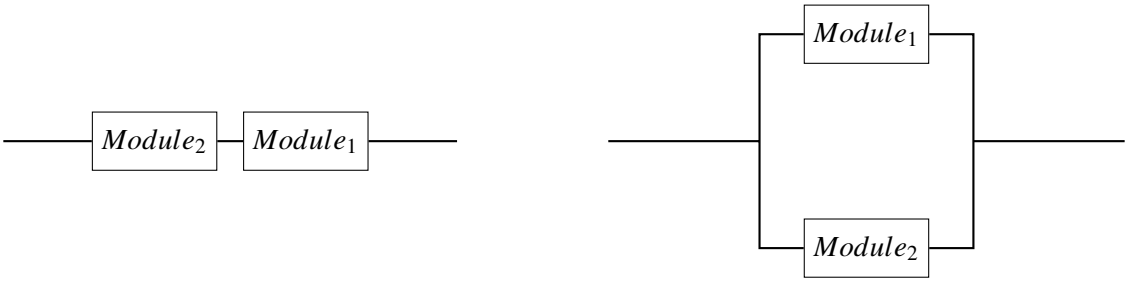


Figure 3.1: Reliability diagrams for a series (a) and a parallel (b) system

For a combination of series, parallel RBD, consider a computing unit that consists of two processor cores that are connected to a shared RAM memory. The reliability block diagram for this system is depicted in Figure 3.2. The processors are arranged in parallel, as only one functioning processor is necessary for system operation. The memory, on the other hand, is connected in series, as its failure would render the entire system inoperable.

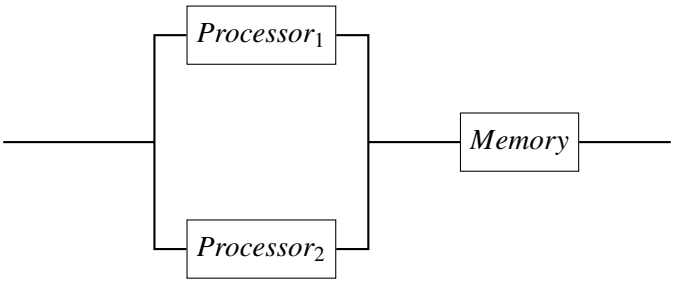


Figure 3.2: Reliability diagram for a three-component system

Despite their widespread use, reliability block diagrams (RBDs) exhibit certain limitations that restrict their applicability in certain situations.

Primarily, RBDs adhere to a simplified assumption that system components can only exist in either an operational or failed state. Additionally, they assume that the system configuration remains constant throughout the mission. These assumptions preclude the modeling of standby components, repair processes, and sophisticated fault detection and recovery mechanisms.

Furthermore, RBDs operate under the assumption of independent component failures. This assumption implies that the sequence in which components fail does not affect the overall system reliability. However, in reality, the order of failures can significantly impact the system's ability to function.

These limitations suggest that RBDs may not be suitable for modeling complex systems where standby components, repair mechanisms, or intricate fault detection and recovery strategies are employed, or where the order of component failures significantly affects system reliability.

In this section, we consider some canonical structures, out of which more complex structures can be constructed.

We start with the basic series and parallel structures, continue with non-series/parallel ones, and then describe some of the many resilient structures that incorporate redundant components (next referred to as modules).

In the next sub-sections, we will use the following notations:

- $R_i = p_i$, the reliability of block i, meaning the probability that functional block i is working properly
- $Q_i = q_i = 1 - p_i$, the probability that functional block i is defective
- R, the reliability of the whole system (i.e. the probability that the whole system is functioning properly)
- $Q = 1 - R$, the probability that the whole system is defective

3.2 Series Structures

A series system consists of N interconnected modules, where the malfunction of any individual module leads to the entire system's failure. It is crucial to note that the diagram in Figure 3.3 represents a reliability diagram, not necessarily an electrical circuit. The output of the first module may not always directly connect to the input of the second module.

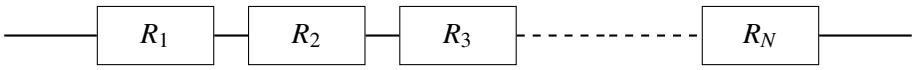


Figure 3.3: Reliability diagram for a series system

For such a system to function properly, all its units must function properly. Assuming that the modules in Figure 3.3 fail independently of each other, the reliability of the entire series system is the product of the reliabilities of its N modules.

Denoting with $R_s(t)$ the reliability of the whole system we can write the following,

$$R_s = P(1 \wedge 2 \wedge 3 \wedge .. \wedge N) = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_N \tag{3.1}$$

If we denote by $R_i(t)$ the reliability of module i, we can rewrite the equation,

$$R_s(t) = \prod_{i=1}^{N} R_i(t) \tag{3.2}$$

Also,

$$Q_s(t) = 1 - R_s(t) = 1 - \prod_{i=1}^{N} (1 - Q_i(t)) \tag{3.3}$$

$$\prod_{i=1}^{N} (1 - Q_i(t)) = 1 - (Q_1(t) + Q_2(t) + .. + Q_N(t)) + (Q_1(t)Q_2(t) + Q_1(t)Q_3(t) + .. + Q_{N-1}(t)Q_N(t)) - .. \tag{3.4}$$

Usually, in order for the whole system to have a high reliability, each block needs to have a high reliability $R_i \geq 0.9$, which means that Q_i is very small, so we can neglect factors that contain a product of at least two Q_i factors. Therefore, we can rewrite Equation 3.4 as,

$$\prod_{i=1}^{N} (1 - Q_i(t)) \approx 1 - (Q_1(t) + Q_2(t) + .. + Q_N(t)) = 1 - \sum_{i=1}^{N} Q_i(t) \tag{3.5}$$

If we input this into Equation 3.3, we get:

$$Q_s(t) = 1 - (1 - \prod_{i=1}^{N} (1 - Q_i(t))) = \sum_{i=1}^{N} Q_i(t) \tag{3.6}$$

If module i has a constant failure rate, denoted by λ_i, then, $R_i(t) = e^{-\lambda_i t}$, and consequently:

$$R_s(t) = \prod_{i=1}^{N} e^{\lambda_i t} = e^{-\sum_{i=1}^{N} \lambda_i t} = e^{-\lambda_s t} \tag{3.7}$$

From 3.7 we see that the series system also follows an exponential repartition and has a constant failure rate equal to λ_s (the sum of the individual failure rates). Using the relation derived in 2.24, the MTBF of the series system is therefore

$$MTBF_S = \frac{1}{\lambda_s} = \frac{1}{\sum_{i=1}^{N} \lambda_i} = \frac{1}{\sum_{i=1}^{N} \frac{1}{MTBF_i}} \tag{3.8}$$

This means that:

$$MTBF_S < MTBF_i, \forall i = \overline{1,N} \tag{3.9}$$

The failure rate of a series system increases with the number of units that are linked in series.

$$\lambda_S = \sum_{i=1}^{N} \lambda_i \tag{3.10}$$

For identical systems, with the same failure rate, $\lambda_i = \lambda$, we can simplify the equation above to:

$$\lambda_S = N\lambda \tag{3.11}$$

■ **Example 3.1** Consider the series structure in Figure 3.4. The four modules in this diagram represent the instruction decode unit (R_{ID}), execution unit (R_{EU}), data cache (R_{DC}), and instruction cache (R_{IC}) in a microprocessor. All four units must be fault-free for the microprocessor to function, although the way they are physically connected does not resemble a series system.

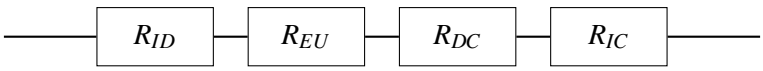


Figure 3.4: Reliability diagram for a series system

Let's assume the modules have the following constant reliabilities: $R_{ID} = 0.9$, $R_{EU} = 0.95$, $R_{DC} = 0.99$, $R_{IC} = 0.89$. Then, the total reliability of the microprocessor is:

$$R_S = R_{ID} \cdot R_{EU} \cdot R_{DC} \cdot R_{IC} = 0.9 \cdot 0.95 \cdot 0.99 \cdot 0.89 \approx 0.75 \tag{3.12}$$

As a general rule, the reliability of a series structure is lower than the reliability of its individual components. This can be explained by the fact there are more states in which two modules can fail when working together than individually. It can be noted that, for the processor to have a 99.9% reliability (which is a common figure for today's PCs), the reliability of each of the four subsystems needs to be at least $R = \sqrt[4]{0.999} \approx 0.9998$ If we increase the number of components that are linked in series even further, the overall reliability will decrease asymptotically towards zero.

For example, if we link together an ever increasing number of systems with reliability $R = 0.9$, we will get the following decrease in overall reliability:

- 2 systems: $R_S = 0.9^2 = 81\%$
- 3 systems: $R_S = 0.9^3 = 72.9\%$
- 4 systems: $R_S = 0.9^4 = 65.61\%$
- 5 systems: $R_S = 0.9^5 = 59.05\%$
- 6 systems: $R_S = 0.9^6 = 53.14\%$

This decrease in reliability is shown in Figure 3.5.

■

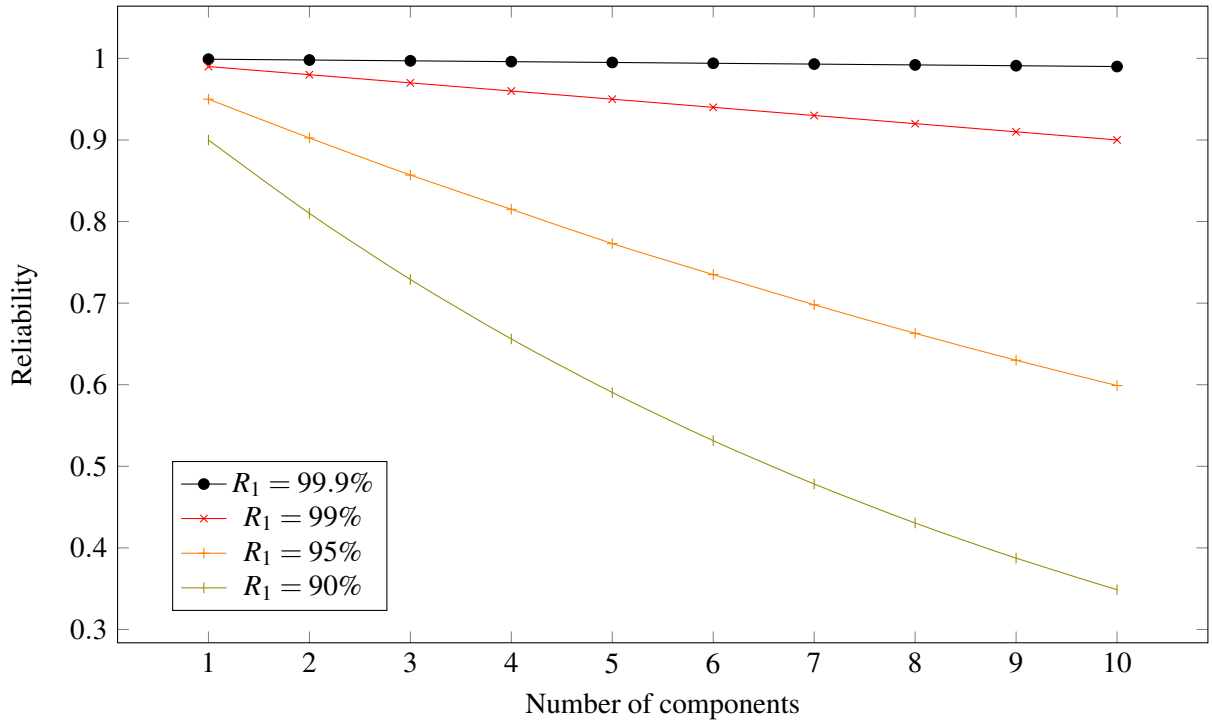


Figure 3.5: Reliability of a series system with increasing number of identical components: single component reliability (R_1) from 90% to 99.9%

3.3 Parallel Structures

A parallel system is defined as a set of N modules connected together so that it requires the failure of all the modules for the system to fail, as in Figure 3.6.

To get to a reliability formula for the parallel structure, we will have to first consider the probability that the whole system will malfunction ($Q_p(t)$). This will happen when all the blocks malfunction, so block 1, block 2 through block N are all defective. We can express that by:

$$Q_P(t) = P(\overline{1} \wedge \overline{2} \wedge .. \wedge \overline{N}) = \prod_{i=1}^{N} Q_i(t) \tag{3.13}$$

where all blocks are independent and $Q_i(t)$ is the probability that block i is faulty.

We can therefore express the reliability of a parallel structure of N modules by:

$$R_P(t) = 1 - Q_P(t) = 1 - \prod_{i=1}^{N} Q_i(t) = 1 - \prod_{i=1}^{N} (1 - R_i(t)) \tag{3.14}$$

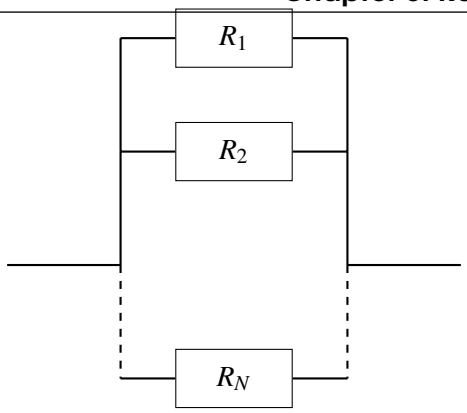


Figure 3.6: Reliability diagram for a parallel system

If every module has a constant failure rate λ_i, then we can write:

$$R_P(t) = 1 - \prod_{i=1}^{N}(1 - e^{-\lambda_i t}) = \sum_{i=1}^{N} e^{-\lambda_i t} - \sum_{i=1, j=1, i\neq j}^{N} e^{-(\lambda_i+\lambda_j)t} + .. + (-1)^{N+1} \prod_{k=1}^{N} e^{-\lambda_k t} \quad (3.15)$$

To calculate the MTBF, we follow the rule derived in Equation 2.24:

$$MTBF_P = \int_0^\infty R_P(t)dt = \quad (3.16)$$

$$= \sum_{i=1}^{N} \int_0^\infty e^{-\lambda_i t} dt - \sum_{i=1, j=1, i\neq j}^{N} \int_0^\infty e^{-(\lambda_i+\lambda_j)t} dt + .. + (-1)^{N+1} \int_0^\infty \left(\prod_{k=1}^{N} e^{-\lambda_k t} \right) dt = \quad (3.17)$$

$$= \sum_{i=1}^{N} \int_0^\infty e^{-\lambda_i t} dt - \sum_{i=1, j=1, i\neq j}^{N} \int_0^\infty e^{-(\lambda_i+\lambda_j)t} dt + .. + (-1)^{N+1} \int_0^\infty \left(e^{-\sum_{k=1}^{N} \lambda_k t} \right) dt \quad (3.18)$$

We can simplify Equation 3.18 by integration:

$$MTBF_P = \sum_{i=1}^{N} \frac{1}{\lambda_i} - \sum_{i=1, j=1, i\neq j}^{N} \frac{1}{\lambda_i + \lambda_j} + .. + (-1)^{N+1} \frac{1}{\sum_{k=1}^{N} \lambda_k} \quad (3.19)$$

If all systems have the same failure rate $\lambda_i = \lambda_j = .. = \lambda_N = \lambda$, we can rewrite Equation (78):

$$MTBF_P = \frac{N}{\lambda} - \frac{N}{2\lambda} + .. + (-1)^{N+1} \frac{1}{N\lambda} = \frac{1}{\lambda} \sum_{i=1}^{N} (-1)^{i+1} \frac{C_N^i}{i} \quad (3.20)$$

We can easily substitute the sum in Equation 3.20 with the partial sum of the harmonic series:

$$\sum_{i=1}^{N} (-1)^{i+1} \frac{C_N^i}{i} = \sum_{i=1}^{N} \frac{1}{i} \quad (3.21)$$

Therefore, we can simplify Equation 3.20 and write the MTBF of a parallel system with N identical components as:

$$MTBF_P = \frac{1}{\lambda}\sum_{i=1}^{N}\frac{1}{i} \approx \frac{ln(2N)}{\lambda} \tag{3.22}$$

Note that the harmonic series is divergent, so a parallel system does not have a constant failure rate. The failure rate decreases with the increase of the systems that are linked in parallel. We can derive the global failure rate of a system with N identical modules with failure rate λ that are connected in parallel using the result in Equation 3.22:

$$\lambda_P = \frac{\lambda}{\sum_{i=1}^{N}\frac{1}{i}} \tag{3.23}$$

■ **Example 3.2** A system consists of two components in parallel, as in Figure 3.7. What is the total reliability, MTBF and the failure rate of the system?

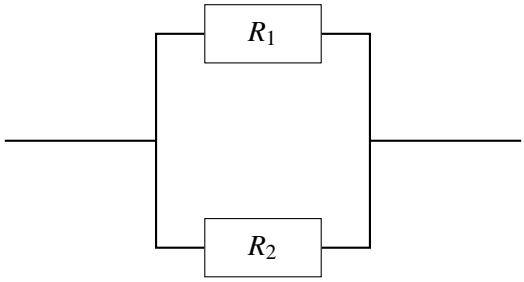


Figure 3.7: Reliability diagrams for a parallel system with two components

We can derive the reliability formula from the general form:

$$R_P(t) = 1 - \prod_{i=1}^{2}(1 - R_i(t)) = 1 - (1 - R_1(t))(1 - R_2(t)) = R_1(t) + R_2(t) - R_1(t)R_2(t) \tag{3.24}$$

Presuming $R_1(t) = e^{-\lambda_1 t}$ and $R_2(t) = e^{-\lambda_2 t}$, the MTBF of the system can be expressed as

$$MTBF_P = \int_0^\infty R_P(t)dt = \int_0^\infty e^{-\lambda_1 t}dt + \int_0^\infty e^{-\lambda_2 t} - \int_0^\infty e^{-(\lambda_1+\lambda_2)t}dt \tag{3.25}$$

$$MTBF_P = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} \tag{3.26}$$

If both modules are identical, meaning $R_1(t) = R_2(t) = R(t)$, then we can simplify the reliability formula to

$$R_P(t) = 2R(t) - R^2(t) \tag{3.27}$$

The MTBF will then be equal to:

$$MTBF_P = \frac{3}{2\lambda} \tag{3.28}$$

and the failure rate of the parallel module will be equal to:

$$\lambda_P = \frac{2}{3}\lambda \tag{3.29}$$

It is worth noting that, as individual reliability functions are $0 \leq R(t) < 1$, $R_P(t)$ will always be greater than $R(t)$, which means that the reliability of the parallel system will always be greater than the reliability of its individual components.

$$R_P(t) = 2R(t) - R^2(t) > R(t), \forall R(t) \in [0,1) \tag{3.30}$$

■

■ **Example 3.3** If the reliability of two individual components is $R_1 = R_2 = 0.9$, then, the total reliability of the parallel system is $R_P = 0.99$. If we increase the number of systems in parallel, as in Figure 3.8, the overall system reliability will also increase:

- 2 systems: $R_P = 1-(1-0.9)^2 = 99\%$
- 3 systems: $R_P = 1-(1-0.9)^3 = 99.9\%$
- 4 systems: $R_P = 1-(1-0.9)^4 = 99.99\%$
- 5 systems: $R_P = 1-(1-0.9)^5 = 99.999\%$
- 6 systems: $R_P = 1-(1-0.9)^6 = 99.9999\%$

■

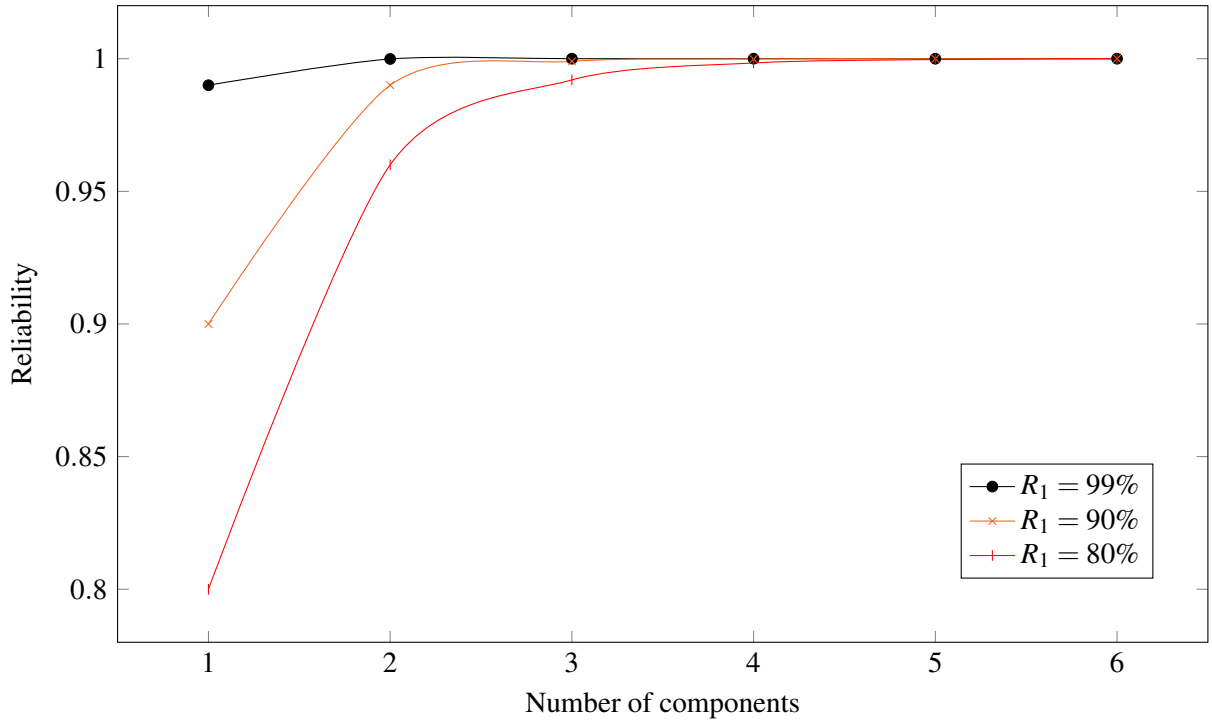


Figure 3.8: Reliability of a parallel system with increasing number of identical components: single component reliability (R_1) of 80%, 90% and 99%

3.4 Combination of Series and Parallel

While many smaller systems can be accurately represented by either a simple series or parallel configuration, there may be larger systems that involve both series and parallel configurations in the overall system. Such systems can be analysed by calculating the reliabilities for the individual series and parallel sections and then combining them in the appropriate manner. Such a methodology is illustrated in the following example.

■ **Example 3.4** Calculating the Reliability for a Combination of Series and Parallel.

Consider a system with three components. Units 1 and 2 are connected in series and Unit 3 is connected in parallel with the first two, as shown in Figure 3.9. This is meant to illustrate a real-life example of a computing structure in which two processor cores are sharing access to a single RAM memory unit. Each unit has its own reliability function, R_1 and R_2 for each processor core and R_3 for the RAM memory.

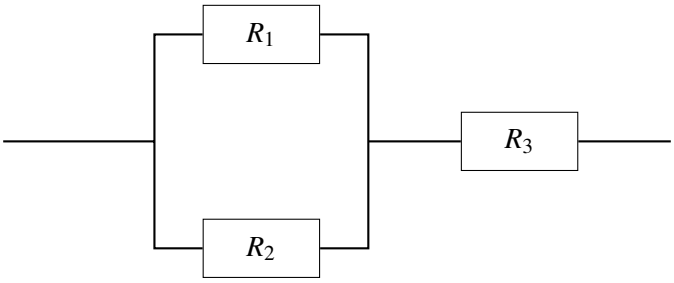


Figure 3.9: Reliability diagram for a simple series-parallel system

What is the reliability of the system if $R_1 = 99.5\%$, $R_2 = 98.7\%$ and $R_3 = 97.3\%$ at 100 hours?

First, the reliability of the parallel segment consisting of Units 1 and 2 is calculated: $R_{12} = 1-(1-R_1)(1-R_2) = 1-(1-0.995)(1-0.987) = 0.999935$

The reliability of the overall system is then calculated by treating Units 1 and 2 as one unit with a reliability of 99.9935% connected in series with Unit 3. Therefore: $R_{123} = R_{12}R_3 = 0.97294$ ■

3.5 k Out of n Systems

The k-out-of-n configuration is a special case of parallel redundancy. This type of configuration requires that at least k components succeed out of the total n parallel components for the system to succeed.

■ **Example 3.5** Consider an airplane that has four engines. Furthermore, suppose that the design of the aircraft is such that at least two engines are required to function for the aircraft to remain airborne. This means that the engines are reliability-wise in a k-out-of-n configuration, where k = 2 and n = 4. More specifically, they are in a 2-out-of-4 configuration.

Now, we can derive the overall reliability of such as system if we assume that all four engines have the same reliability function $R(t)$ as a sum of probabilities.

$$R_{2/4}(t) = R^4(t) + 4R^3(t)(1-R(t)) + 6R^2(t)(1-R(t))^2 \tag{3.31}$$

The first term in the probability sum above $R^4(t)$ denotes the probability of all four engines being operational at a certain time. The second term, $R^3(t)(1-R(t))$, denotes the probability of only three engines being operational at a certain time and, as there are four cases in which a single engine could fail, we multiply this by a factor of 4. The last term in the sum gives the probability of a two-engine failure at a certain time. As in the previous case, since there are six instances in which any two engines could fail (equal to C_4^2), the total probability of a two-engine failure for our airplane is $6R^2(t)(1-R(t))^2$ ∎

Following this example, we can deduce a general formula for k out of n reliability as being:

$$R_{k/n}(t) = C_n^n R^n(t) + C_n^{n-1} R^{n-1}(t)(1-R(t)) + .. + C_n^k R^k(t)(1-R(t))^{n-k}, \forall k < n \tag{3.32}$$

Or, we can express the above sum as:

$$R_{k/n}(t) = \sum_{i=k}^{n} C_n^i R^i(t)(1-R(t))^{n-i}, \forall k < n \tag{3.33}$$

Even though we classified the k-out-of-n configuration as a special case of parallel redundancy, it can also be viewed as a general configuration type. As the number of units required to keep the system functioning approaches the total number of units in the system, the system's behavior tends towards that of a series system. If the number of units required is equal to the number of units in the system, it is a series system. In other words, a series system of statistically independent components is an n-out-of-n system and a parallel system of statistically independent components is a 1-out-of-n system.

This can be easily deduced from the previous equation. if we plug in k = n in the general k-out-of-n reliability formula we get the reliability of a series system:

$$R_{n/n}(t) = \sum_{i=n}^{n} C_n^i R^i(t)(1-R(t))^{n-i} = R^n(t) \tag{3.34}$$

If we plug in k = 1 in the same formula, we get the standard reliability of a parallel system with n identical units:

$$R_{1/n}(t) = \sum_{i=1}^{n} C_n^i R^i(t)(1-R(t))^{n-i} = 1-(1-R(t))^n \tag{3.35}$$

If $R(t) = e^{-\lambda t}$, then k-out-of-n reliability can be written as:

$$R_{k/n}(t) = \sum_{i=k}^{n} C_n^i e^{-i\lambda t}(1-e^{-\lambda t})^{n-i} \tag{3.36}$$

We can also write the MTBF for the k-out-of-n structure:

$$MTBF_{k/n}(t) = \int_0^\infty R_{k/n}(t)dt = \frac{1}{\lambda}\sum_{i=k}^{n}\frac{1}{i} \tag{3.37}$$

■ **Example 3.6** For our airplane model that tolerates a two-engine failure, if we assume the fault distribution to be exponential with a constant failure rate $\lambda = 0.00001/hour$ for each engine, we can calculate the MTBF of the airplane as:

$$MTBF_{2/4}(t) = \frac{1}{\lambda}\sum_{i=2}^{4}\frac{1}{i} = \frac{1}{\lambda}\left(\frac{1}{2}+\frac{1}{3}+\frac{1}{4}\right) = \frac{13}{12}\frac{1}{\lambda} \approx 108333 hours \tag{3.38}$$

■

3.6 Series-Parallel and Parallel-Series Systems

In this section we consider systems which use multiple identical units of a given reliability that can be linked in groups of series and parallel. We present two ways in which we can link these identical units: series-parallel and parallel-series configurations. Assuming each unit has a reliability function $R(t)$ and using series and parallel reliability formulas, we can quickly derive the overall reliability of the structures presented in Figures 3.10 and 3.11.

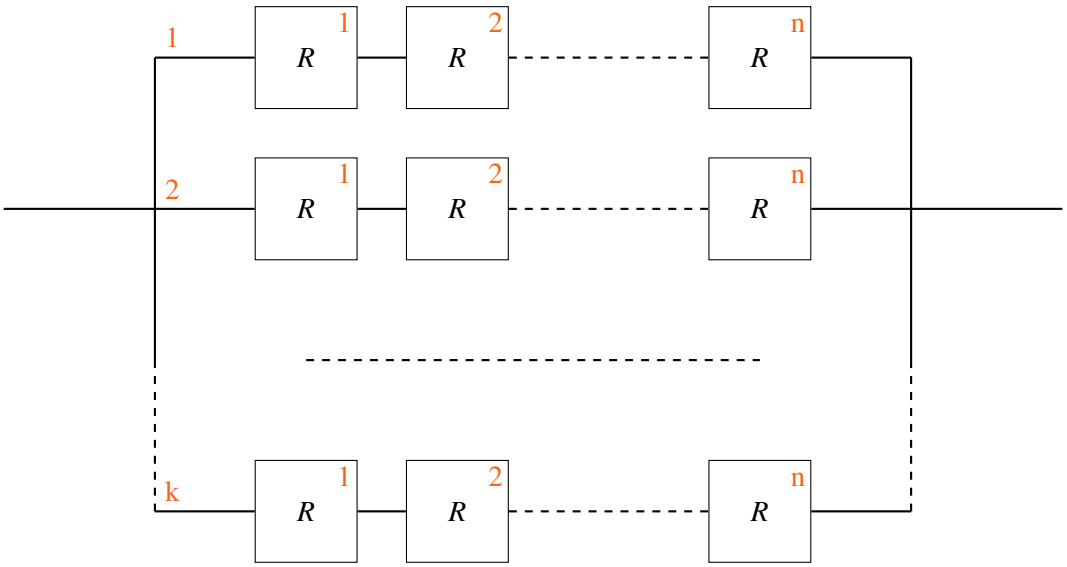


Figure 3.10: Reliability diagram for a $k \times n$ series-parallel system with identical units

For the series-parallel structure, we have n identical units in series on each of the k lines. As such, we can derive the following formula for the series-parallel reliability function $R_{SP}(t)$:

$$R_{SP}(t) = 1 - (1 - R^n(t))^k \tag{3.39}$$

In a similar fashion, for the parallel-series structure in Figure 3.11, we have a group of k identical units in parallel that are connected in series with another group of k-parallel units and so on repeating n times.

We can derive the following formula for the parallel-series reliability function $R_{PS}(t)$:

$$R_{PS}(t) = \left[1 - (1 - R(t))^k\right]^n \tag{3.40}$$

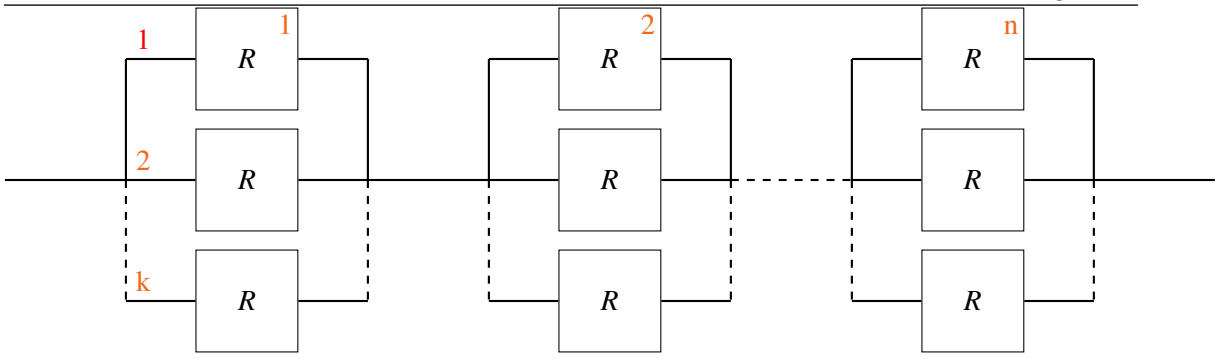


Figure 3.11: Reliability diagram for a $k \times n$ parallel-series system with identical units

Having deduced these formulas, we can plot the two reliability functions as in Figure 3.12. It can be mathematically proven that the reliability of the parallel-series configuration $R_{PS}(t)$ is always greater than the reliability of the series-parallel configuration $R_{SP}(t)$ for any positive integer values of n and k.

What this means is that redundancy at the component level is always more effective than redundancy at the system level in improving system reliability, when using the same number of components.

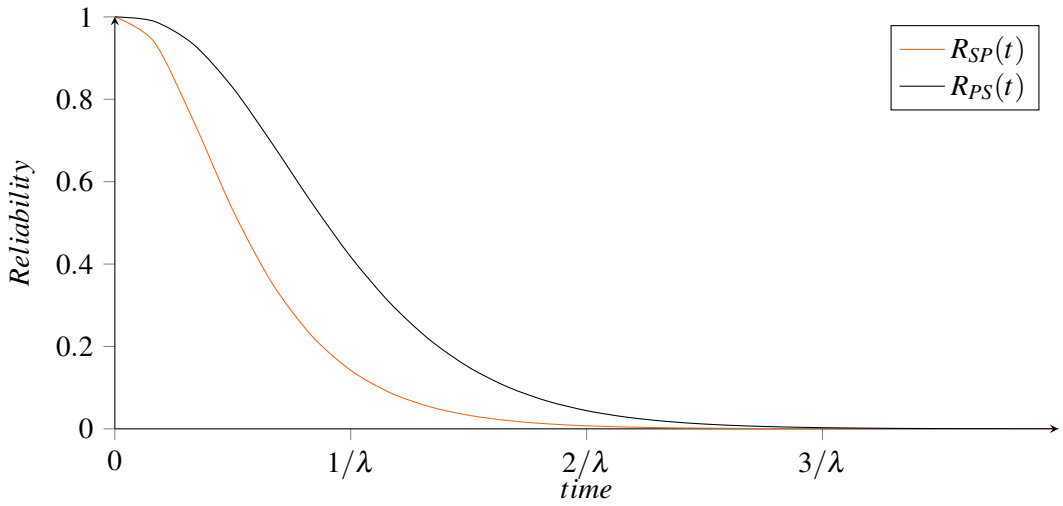


Figure 3.12: $R_{SP}(t)$ versus $R_{PS}(t)$ for n=k=3

■ **Example 3.7** A solar panel is comprised of nine identical solar cells. Each solar cell can have two major failure modes:

- **fail-open**, when the cell or its metallic contacts break due to micro-fissures or bad bonding
- **fail-closed**, when the cell is shorted

In either of these two states the cell's energy production is compromised, but, depending on how the cell is connected to the other cells in the solar panel and the preferred failure mode of the cell, it could have a larger or smaller effect on the overall reliability of the panel.

Given a single solar cell reliability of R=0.9 at a certain time and a fail-open preferred mode of failure, what is the best way to wire the nine cells in the solar panel: series-parallel (Figure 3.13) or parallel-series (Figure 3.14)?

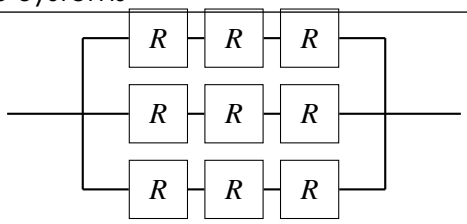


Figure 3.13: Reliability diagram for a 3×3 series-parallel system with identical units

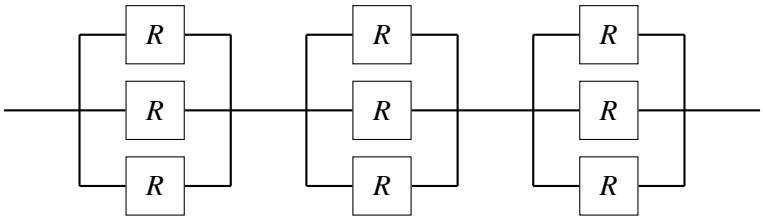


Figure 3.14: Reliability diagram for a 3×3 parallel-series system with identical units

We can compute the 3×3 series-parallel and parallel-series reliability functions as:

- $R_{SP} = 1 - (1 - 0.9^3)^3 = 0.98$
- $R_{PS} = (1 - (1 - 0.9)^3)^3 = 0.997$.

It is evident that $R_{SP} < R_{PS}$.

In conclusion, if the preferred failure mode of a solar cell is fail-open, it is more reliable to wire a solar panel as a parallel-series configuration. ∎

3.7 Non-Decomposable Systems

There are systems that can be described by reliability block diagrams that cannot be decomposed into series or parallel units. An example of such a system is described in Figure 3.15, where the structure does not lead to any type of equivalence to a series or parallel module configuration.

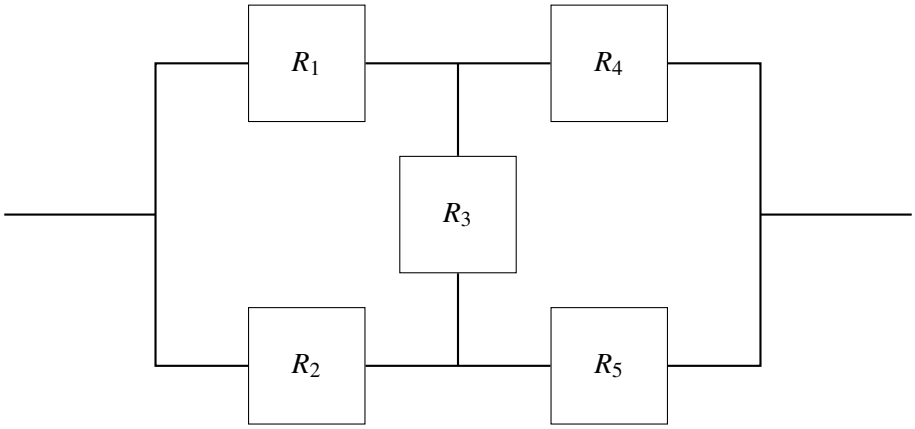


Figure 3.15: Reliability diagram for a non-decomposable system

We can assess the reliability of this type of system by considering the behaviour of one of its constituent modules. Let us pick the module with reliability R_3 and estimate the reliability of the system in the following two situations:

Case 1: module R_3 has failed.

In this case, module R_3 can be represented as open in the system reliability diagram (reliability = 0), as in Figure 3.16.

We can estimate the reliability of the system in this case as:

$$R_{C1} = (R_1R_4)||(R_2R_5) = 1-(1-R_1R_4)(1-R_2R_5) = R_2R_5+R_1R_4-R_1R_4R_2R_5 \tag{3.41}$$

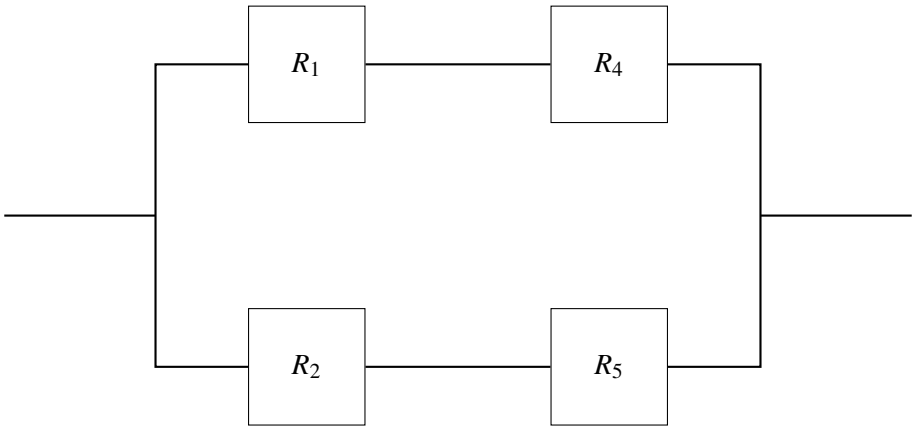


Figure 3.16: Equivalent system reliability diagram for module R_3 failed

Case 2: module R_3 is fully operational.

In this case, module R_3 can be represented as connection in the system reliability diagram (reliability = 1), as in Figure 3.17.

We can also estimate the reliability of the system in this case as:

$$\begin{aligned} R_{C2} &= (R_1||R_2)(R_4||R_5) = (R_1+R_2-R_1R_2)(R_4+R_5-R_4R_5) = \\ &= R_1R_4+R_1R_5-R_1R_4R_5+R_2R_4+R_2R_5-R_2R_4R_5-R_1R_2R_4-R_1R_2R_5+R_1R_2R_4R_5 \end{aligned} \tag{3.42}$$

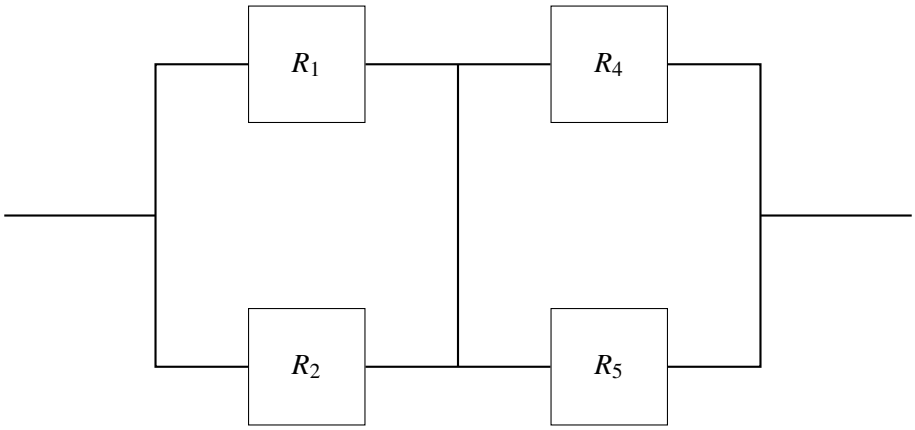


Figure 3.17: Equivalent system reliability diagram for module R_3 fully operational

The reliability of the system in Figure 3.15 is going to be a sum of probabilities of the two cases:

$$R_S = R_3 \times P(system\ works|3\ is\ without\ faults) + (1-R_3) \times P(system\ works|3\ is\ faulty) \tag{3.43}$$

$$\begin{aligned}
&= R_3 R_{C2} + (1-R_3) R_{C1} \\
&= R_3(R_1R_4 + R_1R_5 - R_1R_4R_5 + R_2R_4 + R_2R_5 - R_2R_4R_5 - R_1R_2R_4 - R_1R_2R_5 + R_1R_2R_4R_5) \\
&\quad + (1-R_3)(R_2R_5 + R_1R_4 - R_1R_4R_2R_5) \\
&= R_1R_4 + R_2R_5 + R_1R_3R_5 + R_2R_3R_4 - R_1R_3R_4R_5 - R_2R_3R_4R_5 - R_1R_2R_3R_4 - R_1R_2R_3R_5 \\
&\quad - R_1R_2R_4R_5 + 2R_1R_2R_3R_4R_5
\end{aligned}$$

If $R_1 = R_2 = R_3 = R_4 = R_5 = R$, then we can rewrite 3.43 as:

$$R_S = 2R^2 + 2R^3 - 5R^4 + 2R^5 \tag{3.44}$$

3.8 Majority Voted Redundancy

Majority voted redundancy is a fault-tolerant technique used in computing systems to enhance reliability and protect against component failures. It employs a redundant approach, utilizing multiple identical copies of a hardware component or software module to execute the same task. The outputs of these redundant components are then fed into a voting mechanism, which determines the correct output based on the majority vote.

3.8.1 Triple Modular Redundancy (TMR)

The simplest structure to offer majority voted redundancy is the triple modular scheme in which three identical components, be it hardware or software, are set to simultaneously execute the same function and the results at their outputs are compared by a voter, as in Figure 3.18.

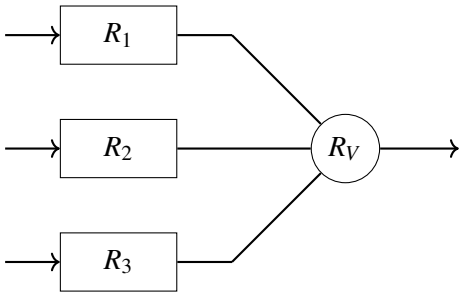


Figure 3.18: Triple modular redundancy majority voting system

The majority voting mechanism determines the correct output based on the majority vote. If two or more components produce the same output, that is considered the correct output. If there is a tie, the system may enter a fail-safe state or attempt to recompute the output.

TMR provides exceptional fault tolerance, as it can withstand one or, in some instances, two component failures while still maintaining system operation. The voting mechanism effectively detects discrepancies among the outputs of the redundant components, enabling error detection and correction.

TMR is widely used in mission-critical systems where reliability is paramount, such as aircraft avionics, medical devices, and industrial control systems. Also, TMR is often employed in data storage systems to protect against data loss due to hardware failures.

The main limitation of TMR comes from its scale, as it introduces additional hardware or software overhead, leading to higher system costs.

The total reliability of a TMR system can be inferred from the fact that it needs at least two of its three modules and its voter to function fault-free in order for the whole system to function properly. As such, we can write:

$$R_{2/3} = [R_1R_2(1-R_3) + R_1(1-R_2)R_3 + (1-R_1)R_2R_3 + R_1R_2R_3]R_V \tag{3.45}$$

Given the three modules are identical, we can assume that $R_1(t) = R_2(t) = R_3(t) = R(t)$. Also, the voter is far simpler in structure than of any other of the three modules, so we can assume that it can be much more reliable $R_V(t) >> R(t)$, $R_V(t) \approx 1$

Therefore, we can rewrite 3.45 as:

$$R_{2/3}(t) = 3R^2(t) - 2R^3(t) \tag{3.46}$$

Given that $R(t) = e^{-\lambda t}$, we can plug in to 3.46:

$$R_{2/3}(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t} \tag{3.47}$$

One interesting question is whether this TMR structure is more reliable than a single module. We can answer this question by solving this simple inequality:

$$R_{2/3}(t) > R(t) \Rightarrow 3R^2(t) - 2R^3(t) > R(t) \Rightarrow 2R^3(t) - 3R^2(t) + R(t) < 0 \Rightarrow R(t)(2R^2(t) - 3R(t) + 1) < 0 \tag{3.48}$$

As $R(t) \geq 0 \ \ \forall t \geq 0$ as a probability function, then:

$$2R^2(t) - 3R(t) + 1 < 0 \Rightarrow \left(R(t) - \frac{1}{2}\right)(R(t) - 1) < 0 \tag{3.49}$$

which is true for $R(t) \geq \frac{1}{2}$.

Therefore, it is advisable to use triple modular redundancy only with modules that operate at an individual reliability greater than 50%, as in Figure 3.19. We can calculate the elapsed mission time at which the triple modular redundancy falls below the reliability of a single module $t = ln(2)/\lambda \approx 0.69/\lambda$. In conclusion, TMR can be used for applications that have mission times less than 69% of MTBF.

We can also calculate the MTBF of a TMR structure as:

$$MTBF_{2/3} = \int_0^\infty \left(3e^{-2\lambda t} - 2e^{-3\lambda t}\right) dt = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6\lambda} = \frac{5}{6}MTBF \tag{3.50}$$

We can see that $MTBF_{2/3} < MTBF$ at any time, which says the TMR structure will fail on average more often than one of its constituent modules.

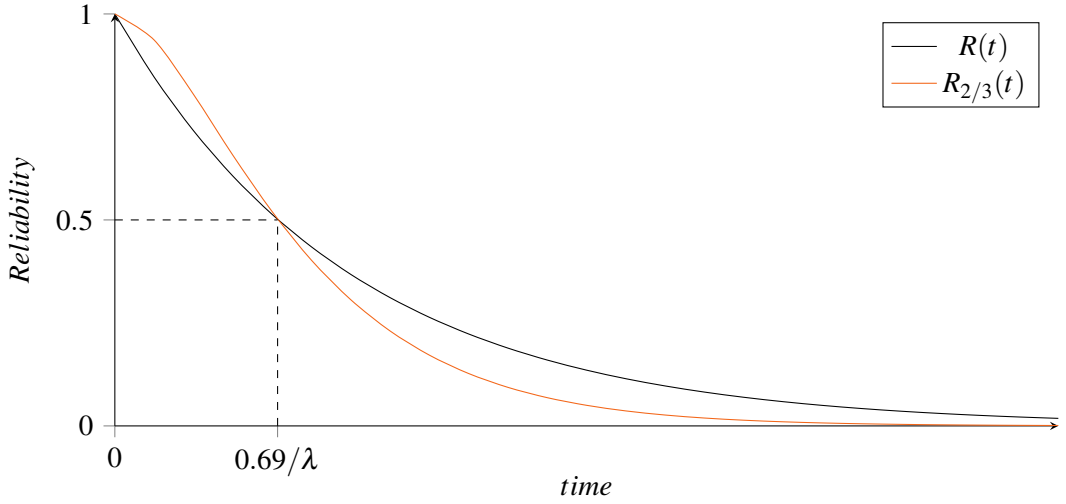


Figure 3.19: $R_{2/3}(t)$ versus $R(t)$ for a TMR system

3.8.2 3-out-of-5 Modular Redundancy

We can further replicate the modules in the TMR scheme and build a two out of five majority voting scheme, as in Figure 3.20.

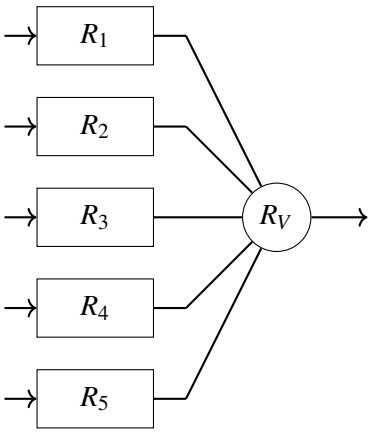


Figure 3.20: 3/5 majority voting system

Operating under the same assumptions that that $R_1(t) = R_2(t) = R_3(t) = R_4(t) = R_5(t) = R(t)$ and $R_V(t) >> R(t)$, $R_V(t) \approx 1$, we can deduce the reliability:

$$R_{3/5}(t) = R^5(t) + 5(1-R(t))R^4(t) + 10(1-R(t))^2R^3(t) = 6R^5(t) - 15R^4(t) + 10R^3(t) \quad (3.51)$$

Given that $R(t) = e^{-\lambda t}$, we can plug in to 3.51:

$$R_{3/5}(t) = 6e^{-5\lambda t} - 15e^{-4\lambda t} + 10e^{-3\lambda t} \quad (3.52)$$

which is also greater than $R(t) \;\; if \;\; R(t) \in (\frac{1}{2}, 1]$

The MTBF of the structure is:

$$MTBF_{3/5} = \int_0^\infty \left(6e^{-5\lambda t} - 15e^{-4\lambda t} + 10e^{-3\lambda t}\right) dt = \frac{6}{5\lambda} - \frac{15}{4\lambda} + \frac{10}{3\lambda} = \frac{47}{60\lambda} = \frac{47}{60} MTBF \quad (3.53)$$

Therefore, $MTBF_{3/5} < MTBF_{2/3} < MTBF$.

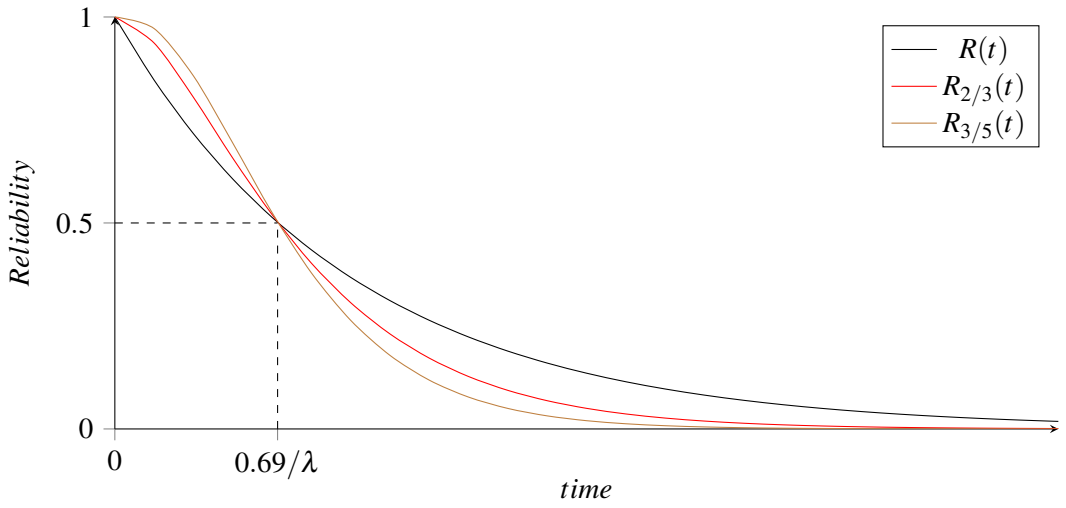


Figure 3.21: $R_{3/5}(t)$ and $R_{2/3}(t)$ versus $R(t)$

3.8.3 n-out-of-(2n-1) Modular Redundancy

Given the previous two examples of majority voting, we can expand to a general case of n out of 2n-1 modular redundancy with voting. This is similar to a k-out-of-n structure, with the particularity that n must be an odd number, to allow majority voting.

The general formula for majority voting structures reliability becomes:

$$\begin{aligned} R_{n/2n-1}(t) &= C_{2n-1}^{2n-1} R^{2n-1}(t) + C_{2n-1}^{2n-2}(1-R(t))R^{2n-2}(t) + .. + C_{2n-1}^{n}(1-R(t))^{n-1}R^{n}(t) \\ &= \sum_{i=n}^{2n-1} C_{2n-1}^{i}(1-R(t))^{2n-1-i}R^{i}(t) \end{aligned} \quad (3.54)$$

If $R(t) = e^{-\lambda t}$, we can rewrite 3.54:

$$R_{n/2n-1}(t) = \sum_{i=n}^{2n-1} C_{2n-1}^{i}(1-e^{-\lambda t})^{2n-1-i}e^{-i\lambda t} \quad (3.55)$$

It can be mathematically proven that $R_{n/2n-1}(t) > R(t)$ when $R(t) > 0.5$, so any majority voting system can be used for mission times shorter than 0.69 of a single unit MTBF.

The MTBF for the entire structure is generally decreasing with the increase in number of redundant modules. While this is counter-intuitive, it can be explained by the increasing probability of a number of redundant modules malfunctioning at any given time.

$$MTBF_{n/2n-1} = \int_0^\infty R_{n/2n-1}(t)dt = \frac{1}{\lambda}\sum_{i=n}^{2n-1}\frac{1}{i} \tag{3.56}$$

It can be proven that, when n increases, $MTBF_{n/2n-1}$ decreases asymptotically to:

$$\lim_{n\to\infty} MTBF_{n/2n-1} = \frac{1}{\lambda}\lim_{n\to\infty}\sum_{i=n}^{2n-1}\frac{1}{i} = \frac{ln(2)}{\lambda} \approx 0.69MTBF \tag{3.57}$$

3.9 Standby-Sparing

Standby-sparing is a fault-tolerant technique used to improve the reliability of systems. It involves having one or more spare components that are inactive until the primary component fails. When the primary component fails, the spare component is activated and takes over its operation.

There are three types of standby-sparing commonly used in computing:

- Cold Sparing: The spare component is not powered on until the primary component fails. This is the simplest form of standby sparing but also the least efficient.
- Warm Sparing: The spare component is powered on but not actively participating in the system operation. This is more efficient than cold sparing but requires additional resource consumption.
- Hot Sparing: The spare component is fully active and ready to take over operation immediately upon primary component failure. This is the most efficient form of standby sparing but also the most complex and expensive.

There are some immediate benefits of standby sparing over the other types of techniques to improve reliability. It is a structure that offers high reliability, as standby sparing can significantly improve the reliability of systems by providing multiple paths for system operation. Another benefit is reduced downtime. When a primary component fails, the standby component can take over immediately, minimizing downtime and improving system availability.

3.9.1 One Spare Reliability

Figure 3.22 describes a one-spare system. There is a primary module with reliability R_1 and a spare R_2. The spare is coupled into operation only when the failure detection module FD detects a failure of the primary module. Note that the diagram does not implicitly differentiate between cold or warm sparing.

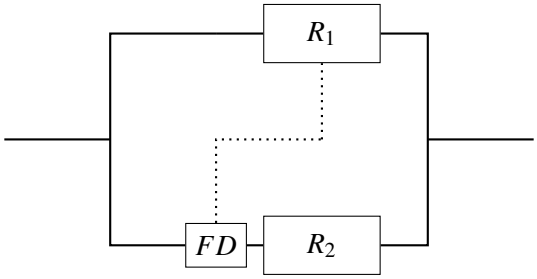


Figure 3.22: One-spare reliability diagram

Cold Sparing

We will analyze the system with the assumption that the spare module is not powered until the primary has completely failed.

As previously stated, we note the reliability of the primary module R_1 and the reliability of the spare R_2. The failure detection module is much simpler in structure than either the primary or the spare, therefore its reliability can be approximated to be $R_{FD} = 1$.

There can be two cases in which this structure successfully completes its mission:

1. The primary module survives for the entire mission duration
2. The primary module shuts down due to a defect at a certain time and the spare switches on for the remainder of the mission duration

If we write P_1 to be the probability of case one happening and P_2 the probability attached to the second case, then, the reliability of the one-spare structure can be written as $R_{1sp} = P_1 + P_2$

P_1 is equal to the reliability of the primary, so $P_1 = R_1$.

To calculate P_2 we need to take into account that there are two events that need to happen: the primary breaking down at a certain time and the spare switching on at this time and continuing the mission. Let's write this moment in time as τ.

The probability of the primary breaking down at time τ is equal to the pdf $f(\tau)$, which, by the relations established in a previous chapter is $f(\tau) = \frac{\mathrm{d}F(\tau)}{\mathrm{d}\tau} = -\frac{\mathrm{d}R_1(\tau)}{\mathrm{d}\tau}$. The probability of the spare switching on at time τ and then continuing to operate until the mission is completed at a certain time t is $R_2(t-\tau)$. However, the malfunction of the primary can happen anytime between 0 and time t, so $P_2 = \int_0^t -\frac{\mathrm{d}R_1(\tau)}{\mathrm{d}\tau} R_2(t-\tau)d\tau$

Therefore, we can write the reliability of a one spare system with cold sparing as:

$$R_{1sp}(t) = P_1 + P_2 = R_1(t) + \int_0^t -\frac{\mathrm{d}R_1(\tau)}{\mathrm{d}\tau} R_2(t-\tau)d\tau \tag{3.58}$$

If $R_1(t) = e^{-\lambda_1 t}$ and $R_2(t) = e^{-\lambda_2 t}$, then we can rewrite 3.58 as:

$$\begin{aligned} R_{1sp}(t) &= e^{-\lambda_1 t} + \int_0^t \lambda_1 e^{-\lambda_1 \tau} e^{-\lambda_2 (t-\tau)} d\tau = e^{-\lambda_1 t} + \lambda_1 e^{-\lambda_2 t} \int_0^t e^{-(\lambda_1 - \lambda_2)\tau} d\tau \\ &= e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_2 - \lambda_1} e^{-\lambda_2 t} \left(e^{-(\lambda_1 - \lambda_2)t} - 1 \right) = \frac{\lambda_2}{\lambda_2 - \lambda_1} e^{-\lambda_1 t} - \frac{\lambda_1}{\lambda_2 - \lambda_1} e^{-\lambda_2 t} \end{aligned} \tag{3.59}$$

We can also calculate the MTBF of this structure as:

$$MTBF_{1sp} = \int_0^\infty R_{1sp}(t)dt = \int_0^\infty \left(\frac{\lambda_2}{\lambda_2 - \lambda_1} e^{-\lambda_1 t} - \frac{\lambda_1}{\lambda_2 - \lambda_1} e^{-\lambda_2 t} \right) dt \tag{3.60}$$

$$= \frac{\lambda_2}{\lambda_2 - \lambda_1} \int_0^\infty e^{-\lambda_1 t} dt - \frac{\lambda_1}{\lambda_2 - \lambda_1} \int_0^\infty e^{-\lambda_2 t} dt = \frac{\lambda_2}{\lambda_2 - \lambda_1} \frac{1}{\lambda_1} - \frac{\lambda_1}{\lambda_2 - \lambda_1} \frac{1}{\lambda_2} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2}$$

Therefore, we can conclude that $MTBF_{1sp} = MTBF_1 + MTBF_2$, which means that, on average, a one-spare system will have a longer lifetime than any one of its two components.

Usually, in one-spare systems, the primary and the spare are similar, if not identical modules (e.g. a compute core taking over when an identical compute core breaks down, or a memory drive that backs up a primary drive with the same capacity or specifications). Therefore, we can assume that $R_1(t) = R_2(t) = e^{\lambda t}$.

We can recalculate 3.59 to take into account we are working with identical modules:

$$R_{1sp}(t) = e^{-\lambda t} + \int_0^t \lambda e^{-\lambda \tau} e^{-\lambda(t-\tau)} d\tau = e^{-\lambda t} + \lambda e^{-\lambda t} \int_0^t d\tau = e^{-\lambda t}(1+\lambda t) \tag{3.61}$$

Similarly, we can infer the MTBF:

$$MTBF_{1sp} = \frac{1}{\lambda} + \frac{1}{\lambda} = 2MTBF \tag{3.62}$$

This shows that the MTBF of a one-spare structure with cold sparing and identical units is twice the MTBF of a single unit.

Warm Sparing

Now, let us assume that the spare is not completely switched off while the primary is operating. Therefore, it will also be affected by degradation, but at a much lover rate than normal. We will note this as a different reliability function for the spare, R_{2n}.

Similar assumptions from the cold sparing case can be applied. The system is considered to be working if:

- The primary operates without interruption for the entire duration of the mission $(P_1 = R_1(t))$.
- The primary breaks down at a certain time τ and the spare takes over, switching from a standby state into full operation (P_2).

The only major difference from cold sparing is for case 2, taking into account that the spare is in a standby state while the primary is fully operational. We can quantify this new reliability as $P_2 = \int_0^t -\frac{dR_1(\tau)}{d\tau} R_{2n}(\tau) R_2(t-\tau) d\tau$

Therefore, the reliability of a one-spare system with warm sparing can be written as:

$$R_{1sp'}(t) = P_1 + P_2 = R_1(t) + \int_0^t -\frac{dR_1(\tau)}{d\tau} R_{2n}(\tau) R_2(t-\tau) d\tau \tag{3.63}$$

If $R_1(t) = e^{-\lambda_1 t}$, $R_2(t) = e^{-\lambda_2 t}$ and $R_{2n}(t) = e^{-\lambda_{2n} t}$, then we can rewrite 3.63 as:

$$\begin{aligned} R_{1sp'}(t) &= e^{-\lambda_1 t} + \int_0^t \lambda_1 e^{-\lambda_1 \tau} e^{-\lambda_{2n} \tau} e^{-\lambda_2 (t-\tau)} d\tau = e^{-\lambda_1 t} + \lambda_1 e^{-\lambda_2 t} \int_0^t e^{-(\lambda_1 + \lambda_{2n} - \lambda_2)\tau} d\tau \\ &= e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 + \lambda_{2n} - \lambda_2} \left(e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_{2n}) t} \right) \end{aligned} \tag{3.64}$$

We can also calculate the MTBF of this structure as:

$$MTBF_{1sp'} = \int_0^\infty R_{1sp'}(t)dt = \frac{1}{\lambda_1} + \frac{1}{\lambda_2}\frac{\lambda_1}{\lambda_1+\lambda_{2n}} = MTBF_1 + MTBF_2\frac{MTBF_{2n}}{MTBF_1+MTBF_{2n}} \quad (3.65)$$

If the primary and the spare are identical we can assume $R_1(t) = R_2(t) = e^{-\lambda t}$, but the standby reliability of the spare will still need to be factored in. We can write this as $R_{2n} = e^{-\lambda_n t}$

We can rewrite 3.64 as:

$$R_{1sp'}(t) = e^{-\lambda t} + \int_0^t \lambda e^{-\lambda\tau} e^{-\lambda_n\tau} e^{-\lambda(t-\tau)} d\tau = e^{-\lambda t}\left[1 + \frac{\lambda}{\lambda_n}\left(1 - e^{-\lambda_n t}\right)\right] \quad (3.66)$$

MTBF in 3.65 can also be simplified as:

$$MTBF_{1sp'} = \frac{1}{\lambda} + \frac{1}{\lambda+\lambda_n} \quad (3.67)$$

From 3.67 we can infer that the MTBF of the warm spare system is lower than one for the cold spare system, due to the lower MTBF of the spare.

3.9.2 Two Spare Reliability

Next, we will focus on the reliability of a two-spare system. There is a primary module of reliability $R_1 = e^{-\lambda_1 t}$ and two spares with reliabilities $R_2 = e^{-\lambda_2 t}$ and $R_3 = e^{-\lambda_3 t}$. We will focus on the cold sparing case, in which both spares are completely switched off when are not used.

We can estimate the reliability of the structure through two iterations: first considering the reliability of the $[R_1, R_2]$ ensemble as a one-spare system R_{12}, and then adding R_3 as a spare to it.

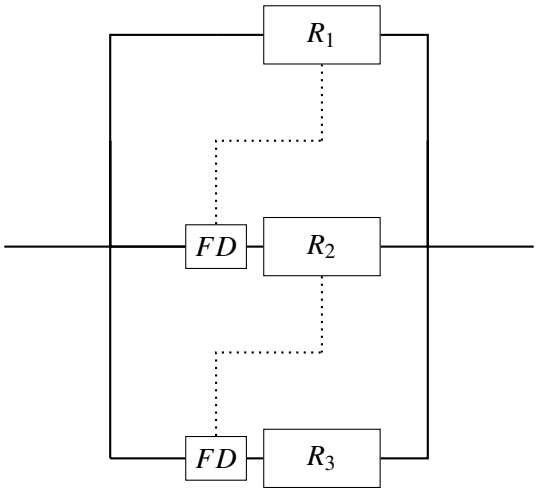


Figure 3.23: Two-spare reliability diagram

We have previously demonstrated in equation 3.59 that:

$$R_{12}(t) = \frac{\lambda_2}{\lambda_2-\lambda_1}e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1-\lambda_2}e^{-\lambda_2 t} \quad (3.68)$$

Factoring the above into the expression for the total system reliability yields the following expression:

$$R_{2sp} = R_{123}(t) = R_{12}(t) + \int_0^t -\frac{\mathrm{d}R_{12}(\tau)}{\mathrm{d}\tau} R_3(t-\tau)d\tau \tag{3.69}$$

After plugging in equation 3.68 in the above expression, we can write:

$$R_{2sp}(t) = \frac{\lambda_2\lambda_3}{(\lambda_2-\lambda_1)(\lambda_3-\lambda_1)}e^{-\lambda_1 t} + \frac{\lambda_1\lambda_3}{(\lambda_1-\lambda_2)(\lambda_3-\lambda_2)}e^{-\lambda_2 t} + \frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_3)(\lambda_2-\lambda_3)}e^{-\lambda_3 t} \tag{3.70}$$

From here it can be easily deduced that MTBF of the two spare structure is:

$$\begin{aligned} MTBF_{2sp} &= \int_0^\infty R_{2sp}(t)dt \qquad (3.71)\\ &= \int_0^\infty \left(\frac{\lambda_2\lambda_3}{(\lambda_2-\lambda_1)(\lambda_3-\lambda_1)}e^{-\lambda_1 t} + \frac{\lambda_1\lambda_3}{(\lambda_1-\lambda_2)(\lambda_3-\lambda_2)}e^{-\lambda_2 t} + \frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_3)(\lambda_2-\lambda_3)}e^{-\lambda_3 t} \right) dt \\ &= \frac{\lambda_2\lambda_3}{(\lambda_2-\lambda_1)(\lambda_3-\lambda_1)}\frac{1}{\lambda_1} + \frac{\lambda_1\lambda_3}{(\lambda_1-\lambda_2)(\lambda_3-\lambda_2)}\frac{1}{\lambda_2} + \frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_3)(\lambda_2-\lambda_3)}\frac{1}{\lambda_3} \\ &= \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} \end{aligned}$$

We can rewrite equation 3.71 as:

$$MTBF_{2sp} = MTBF_1 + MTBF_2 + MTBF_3 \tag{3.72}$$

If all of the three modules are identical, $R_1(t) = R_2(t) = R_3(t) = e^{-\lambda t}$ we can rewrite equation 3.69 as:

$$R_{2sp} = e^{-\lambda t}(1+\lambda t) + \int_0^t -\frac{\mathrm{d}(e^{-\lambda\tau}(1+\lambda\tau))}{\mathrm{d}\tau}e^{-\lambda\tau}d\tau = e^{-\lambda t}\left(1+\lambda t+\frac{\lambda^2 t^2}{2}\right) \tag{3.73}$$

Also,

$$MTBF_{2sp} = \int_0^\infty e^{-\lambda t}\left(1+\lambda t+\frac{\lambda^2 t^2}{2}\right)dt = \frac{3}{\lambda} = 3MTBF \tag{3.74}$$

3.9.3 N Spare Reliability

We can generalize the one spare and two spare examples to a system which has any number of spares.

For ease of calculation, we can make the following assumptions:

- Each spare is identical with the primary unit

- The entire standby-sparing system is operating with cold spares

The reliability of a system with n such spares can be deduced iteratively and be written as:

$$R_{nsp} = e^{-\lambda t}\left(1+\lambda t+\frac{\lambda^2 t^2}{2}+\frac{\lambda^3 t^3}{6}+..+\frac{\lambda^n t^n}{n!}\right) = e^{-\lambda t}\sum_{0}^{n}\frac{\lambda^n t^n}{n!} \tag{3.75}$$

Similarly, the MTBF of an n-spare system is:

$$MTBF_{nsp} = \int_0^\infty e^{-\lambda t}\sum_{0}^{n}\frac{\lambda^n t^n}{n!}dt = n\frac{1}{\lambda} = n\cdot MTBF \tag{3.76}$$

Infinite Spares

An interesting, albeit purely theoretical case is when the system has an infinite amount of spares, because the sum $\sum_0^\infty \frac{\lambda^n t^n}{n!}$ is the Taylor series of $e^{\lambda t}$.

Replacing this into 3.75 for $n = \infty$ we get:

$$R_{\infty sp} = e^{-\lambda t}\sum_{0}^{\infty}\frac{\lambda^n t^n}{n!} = e^{-\lambda t}e^{\lambda t} = 1 \tag{3.77}$$

This is the only example in reliability where a system can achieve 100% reliability. Unfortunately, it is also an unachievable example.