1

The Basics of Reliability Engineering

1.1 The Birth of Reliability Engineering

> ***[EN 764-7] [20] 3 Terms and definitions***
> ***3.14 Reliability.*** *Ability of a system or component to perform a required function under specified conditions and for a given period of time without failing.*

The first Reliability models appeared during World War I, and they were used in connection with **airplane performances**: the Reliability was measured as the number of **accidents per hour** of flight time.

In the 1930s, the Reliability concepts and statistical methods were used for **quality control** of industrial products and, in the 1940s, to analyze the missile system during World War II. At that time, Robert Lusser, a mathematician, established the so-called "Product probability law of series components."

Lusser discovered that the **Reliability of a system** is equal to the product of the reliabilities of the individual components which make up the system. If the system has many components, the system Reliability may therefore be rather low, even though the individual components have high Reliability values.

After the war, the interest in the United States was concentrated on intercontinental ballistic missiles and space research; this led to the creation of an association for engineers working with Reliability. The first journal on the subject, "IEEE Transactions on Reliability" came out in 1963, and several textbooks on the subject were published in that decade. The famous military standard MIL-STD-781 was created at that time. Around that period, also the much-used predecessor to military handbook 217 was published by RCA, Radio Corporation of America, and was used for the **prediction of failure rates of electronic components**.

In the following years, more pragmatic approaches were developed and used in the consumer industries. Reliability tools and tasks became more closely tied to the **engineering design process**.

Today, the study of Reliability engineering permits not only the **evaluation of the conformity** of a device over time but also **to compare different design solutions** with the same **functional characteristics**. It can also identify, inside an apparatus, subsystems or **critical elements** that could cause a failure or malfunction of the apparatus itself, needing corrective actions. For this reason, Reliability has an important role in modern design and constitutes a competitive element, even in the light of stricter **safety requirements**.

Functional Safety of Machinery: How to Apply ISO 13849-1 and IEC 62061, First Edition. Marco Tacchini.

1.1.1 Safety Critical Systems

A part of the Reliability studies deals with **Safety Critical Systems.** Those are systems whose failure could result in the loss of lives or significant damage to properties or to the environment [58].

In the 1970s, the design principles of safety-critical systems, both in Machinery and in the process Industry, were the following:

- **Single-channel system** (no redundancy). This architecture would be regarded as a basic design having minimum safety performance.
- **Dual-channel system** (redundancy) applicable to sensors, for example pressure switches, logic units, and final elements, like contactors and valves.
- **2 out of 3 voting systems (2oo3).** Those systems were used originally in the petrochemical industry: they give a good level of both Reliability and of Availability. **Reliability** measures the ability of a system to function correctly, whereas **Availability** measures how often the system is available for use, even though it may not be functioning correctly. For example, a server may run forever and so have ideal Availability, but may be unreliable, with frequent data corruption.
- All systems were using the concept of **Fail Safe**: a failure in any part of the system would lead to a safe state of the process or the machinery under control.

In the 1990s, a part of the Reliability of Critical System studies became known as **Functional Safety** and focussed on Electrical, Electronic, and Programmable Electronic (E/E/PE) systems. The reference standard became the IEC 61508 series.

1.2 Basic Definitions and Concepts of Reliability

According to IEC 60050-191, **Reliability is the ability of the item to remain functional**, to perform a required function, the item's task, **under given conditions for a given time interval**. The concept of "**performing a required function**" is complementary to that of a "**failure**."

A numerical statement of Reliability must be specified by the definition of the required function, the operating conditions, and the mission duration.

Both the required function and the operating conditions can be time dependent, and this is the reason why it's important to define a **mission profile** related to the Reliability of the item's life. If the Mission Time is considered as a parameter of time, the Reliability function is then defined by the **time-dependent function** $R(t)$.

$R(t)$ is the probability that no failure, at item level, will occur in the interval $(0, t]$.

Reliability is based upon mathematical models, and it can be estimated thanks to the **observation** of items during their lifetime. That is done thanks to **measurements and statistical parameters** such as failure rate (λ), mean time to failure (MTTF), and mean time between failures (MTBF), which are presented in the following paragraphs.

1.3 Faults and Failures

One of the first concepts that needs to be clearly understood, for someone approaching the field of Functional Safety, is **the difference between a Fault and a Failure**.

1.3.1 Definitions

Hereafter are the definitions taken from IEC 61508-4 [8]:

> ***[IEC 61508-4] 3.6 Fault, failure and error***
> ***3.6.1 Fault****. Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.*

In other words, a Fault is the situation where a system cannot perform anymore its required function. Figure 1.1 shows the two statuses where a control system can be: an "OK" state, where it works correctly and a "FAULT" state.

Bottom line, it is important not to confuse the concept of failure (event) with the concept of fault (associated with a particular state of a system).

When the system has a failure, it may stop working properly, and therefore it may move to a FAULT state. Here is the definition of Failure:

> ***[IEC 61508-4] 3.6 Fault, failure and error***
> ***3.6.4 Failure****. Termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required.*

Reliability theory classifies failures in various ways [51], among which are **Primary Failure** (not due to other failures), **Secondary Failure**, **Early life Failure**, **Random Failure**, and **Wear out Failure**.

This can also be classified in: **Total failure** (when variations in the characteristics of the element are such to completely compromise its function) or **Partial failure** (when the variations of one or more characteristics of the element do not impede its complete functioning).

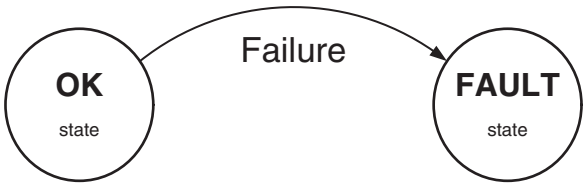
1.3.2 Random and Systematic Failures

In Functional safety, Failures are classified as either **random** (in hardware) or **systematic** (in hardware or software).

> ***[IEC 61508-4] 3.6 Fault, failure and error***
> ***3.6.5 Random Hardware Failure****. Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.*

> ***[IEC 61508-4] 3.6 Fault, failure and error***
> ***3.6.6 Systematic Failure****. Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.*

Figure 1.1 Fault vs failure.



Random Failures are therefore normally attributed to hardware. They are failures, occurring at a random time, which result in one or more of degradation of the component capability to perform its scope. There are many degradation mechanisms occurring at different rates, in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of total equipment, comprising many components, occur **at predictable rates but at unpredictable** (i.e. random) **times**. Based upon historical data, Random Failures can be characterized by a parameter called **Failure Rate** λ. In other words, a random hardware failure involves only the equipment; random failures can occur suddenly without warning or be the outcome of slow deterioration over time. These failures can be characterized by a single reliability parameter, the device failure rate, which can be controlled and managed using an asset integrity program.

Systematic failures can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, or other relevant factors. Examples of causes of systematic failures include human error in the design, manufacture, installation, and operation of the hardware. If, **for example**, a product is not used correctly or it is used in the wrong environment, the risk of systematic failures exists. A systematic failure involves both the equipment and a human error; systematic failures exist from the time that human errors were made and continue to exist until they are corrected. A systematic failure can be eliminated after being detected, while random hardware failures cannot.

Failures are therefore either random or systematic; the latter can be hidden in the hardware or in the software program. A **major difference between random hardware failures and systematic failures** is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy, while systematic failures, by their very nature, cannot be accurately predicted. That means system failure rates arising from random hardware failures can be quantified with reasonable accuracy, while those arising from systematic failures cannot be statistically quantified because the events leading to them cannot easily be predicted. In other words, the reliability parameters of random hardware failures can be estimated from field feedbacks, while it is very difficult to do the same for systematic failures: a qualitative approach is preferred for systematic failures.

In high demand mode functional safety standards, IEC 62061 and ISO 13849-1, the issue of the presence of Systematic Failures is addressed by requiring a systematic approach to product development, engineering, manufacturing, and maintenance, the so-called **Management of Functional Safety**, and the application of the so-called **Basic and Well-tried Safety Principles** (§ 4.13).

When analyzing the Reliability of a Safety System, **all causes of failure,** both systematic and random, **that lead to an unsafe state, should be included**. Some of these failures, in particular the Random hardware failures, can be quantified using the **average frequency of failure in dangerous mode** or the **probability** of a safety-related protection system **failing to operate on demand**.

1.3.2.1 How Random is a Random Failure?

It cannot be stressed enough **the importance of a correct design, installation, and maintenance,** to avoid systematic failures: it often happens that **many failures that we consider to be random are preventable, to a large extent**. Please consider that failures occurring at a random time, which results from one or more degradation mechanisms in the hardware, may be treated as random to the extent that the failures cannot reasonably be prevented.

Only purely random failures can be characterized by a failure rate, including the surrogated failure rate, explained further on in the book. Purely random failures are sudden and complete failures that occur without warning. They are impossible to forecast by examining the item. Constant in time, random failures are usually limited to electronic devices; for electromechanical components, a constant **surrogated failure rate** is used (also referred to as **substitute failure rate**). Hardware failures that are related to deterioration mechanisms may be characterized by failure rates as if they were random, but failure rates depend heavily on the operating environment and on the effectiveness of preventive maintenance. Failure rates will vary by at least an order of magnitude between different applications and different maintenance organizations.

1.4 Probability Elements Beyond Reliability Concepts

We defined $R(t)$ as the probability that no failure, at item level, occurs in the interval $(0, t]$, where t is a random variable.

A **random variable** is a function able to assign a real number to each outcome in the sample space of a random experiment. It can be **continuous or discrete**. Continuous when it has an interval, finite or infinite, of real numbers for its range; discrete when it has a finite range of values.

The probability that a **random variable *X*** assumes a **well-defined value *x*** is described mathematically by the **probability distribution**, which can be continuous or discrete with respect to the random variable considered.

To better understand the Reliability concepts, a brief summary of the **axioms of probability by Kolmogorov (1933)** is reported:

Let (Ω, A) be a measurable space of events. Any event E is a subset of Ω. Assume that the set of all events is represented by a particular family of sets over Ω denoted A.

A probability measure is a real-value function mapping $\mathbb{P} : A \rightarrow \mathbb{R}$ satisfying:

1. *for any event, $E \in A$, $\mathbb{P}(E) \geq 0$*
2. $\mathbb{P}(\Omega) = 1$
3. *for any countably sequence of events $(E_i)_{i \geq 1}$ that are mutually exclusive ($E_i \cap E_j = 0$ if $i \neq j$),*

$$\mathbb{P}\left(\bigcup_{i=1}^{\infty} E_i\right) = \sum_{i=1}^{\infty} \mathbb{P}(E_i)$$

1.4.1 The Discrete Probability Distribution

Discrete probability distribution is usually indicated with $p(x)$, and it can be seen as the relationship between the possible values for the variable and the probability of each value. In this case, the probability distribution can be drawn as shown in Figure 1.2.

This distribution has the following property:

$$\sum_{i} p(x_i) = 1 = \mathbb{P}(\Omega)$$

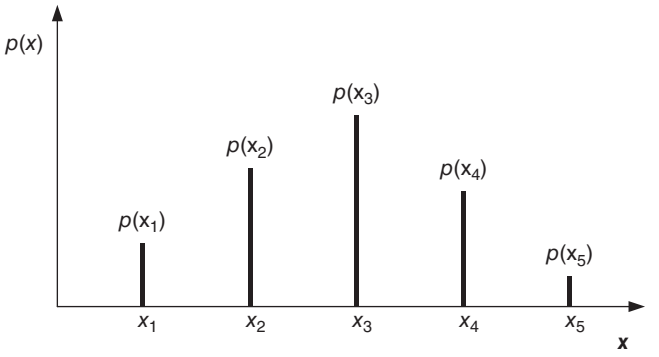


Figure 1.2 Discrete probability distribution.

1.4.1.1 Example: 10 Colored Balls

Let's suppose that a box contains 10 balls:

- Five of the balls are **red**
- Two balls are **green**
- Two balls are **blue**
- One ball is **yellow**

Suppose we take one ball out of the box. Let X be the random variable that represents the ball color. As 5 of the balls are red, and there are 10 balls, the probability that a red ball is drawn from the box is $p(x = \text{red}) = 5/10 = 1/2$.

Similarly, there are two green balls, so the probability that x is green is 2/10. Similar calculations for the other colors yield the probability density function given by Table 1.1 and Figure 1.3.

Table 1.1 Example of a discrete probability distribution.

Ball color	Probability
Red	5/10
Green	2/10
Blue	2/10
Yellow	1/10

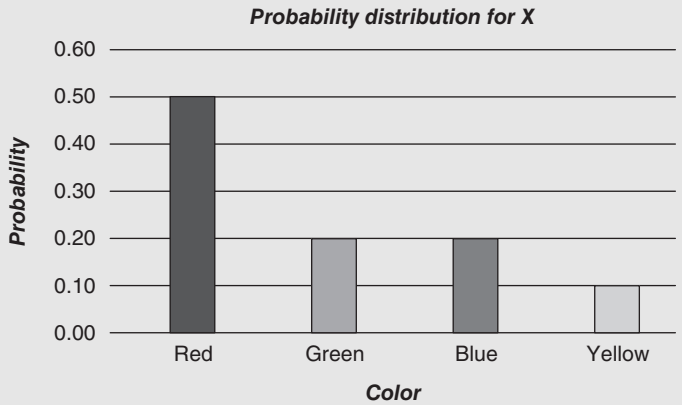


Figure 1.3 Example of a discrete probability distribution.

1.4.1.2 Example: 2 Dice

Let's now suppose that we have two fair six-sided dice. We roll both dice at the same time and add the two numbers that are shown on the upward faces. The discrete probability density function (PDF) is given in Table 1.2 and Figure 1.4.

Table 1.2 Example of a discrete probability distribution for two dice.

Outcome	Sum	Probability
(1.1)	2	1/36
(1.2), (2.1)	3	2/36
(1.3), (2.2), (3.1)	4	3/36
(1.4), (2.3), (3.2), (4.1)	5	4/36
(1.5), (2.4), (3.3), (4.2), (5.1)	6	5/36
...		
(6.6)	12	1/36

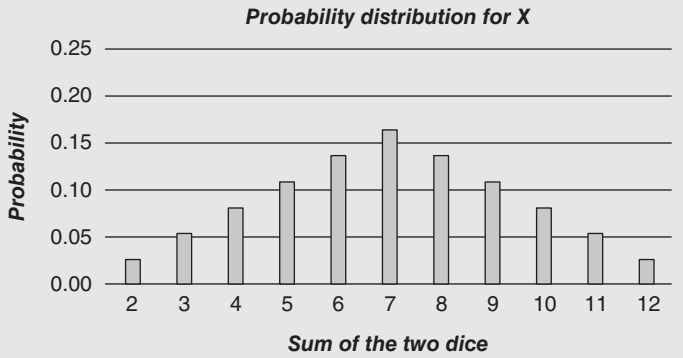


Figure 1.4 Example of a discrete probability distribution for two dice.

1.4.2 The Probability Density Function *f*(*x*)

A continuous probability distribution is indicated with $f(x)$ and is usually called **PDF**. It is expressed by a function, and it can be represented as in Figure 1.5. The bell curve is just an example of a possible PDF.

The main property of a PDF is that:

$$\int_{-\infty}^{+\infty} f(x)dx = 1 = \mathbb{P}(\Omega)$$

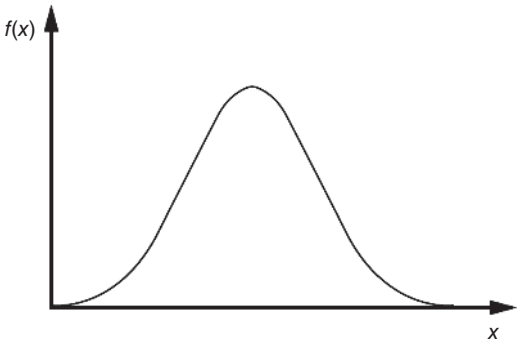


Figure 1.5 Probability density function.

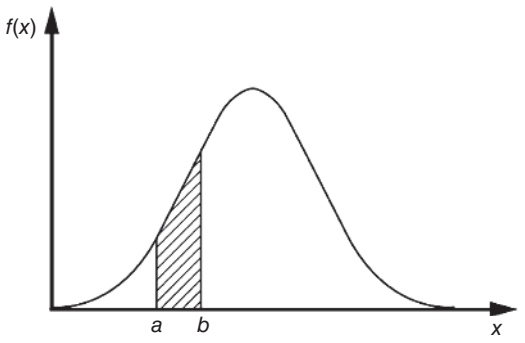


Figure 1.6 The area under the probability density function represents the probability that x assumes values between a and b.

The probability that x assumes values between a and b is evaluated as the following integral of the **PDF:**

$$\int_a^b f(x)dx = \mathbb{P}\{a \leq X \leq b\}$$

This probability is shown in Figure 1.6.

The PDF is also called **Failure Density** or also **Life Distribution.**

1.4.2.1 Example

A uniform PDF over the interval 0–1 for a random variable x is given by $f(x) = 1$ in the range between 0 and 1, and 0 otherwise.

The function $f(x)$, shown in Figure 1.7, is a valid PDF, since it is non-negative and integrates to one. What is the probability of an outcome in the range 0.2–0.8?

$$PDF(0.2 \text{ to } 0.8) = \int_{0.2}^{0.8} 1 \cdot dx = 0.8 - 0.2 = 0.6$$

Meaning that the probability of failure is 60%.

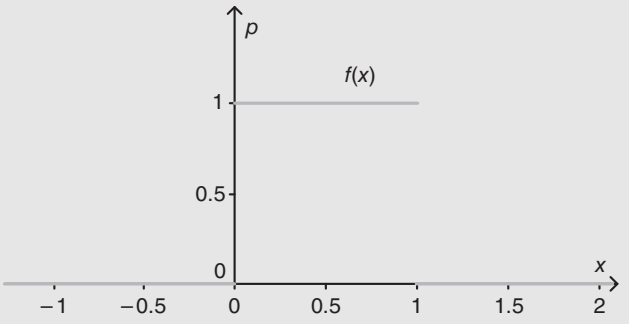


Figure 1.7 Example of a PDF.

1.4.3 The Cumulative Distribution Function *F(x)*

The distribution of a continuous variable can be described by the **Cumulative Distribution Function** as well. That gives the probability that the random variable will assume a value smaller or equal to x. Its expression is:

$$F(x) = \mathbb{P}(X \leq x) = \int_{-\infty}^{x} f(\xi)d\xi$$

For $-\infty < x < +\infty$.

$F(x)$ is a non-decreasing function: $F(-\infty) = 0$ and $F(+\infty) = 1$, thus:

$$\int_{-\infty}^{+\infty} f(\xi)d\xi = 1$$

The derivative of the cumulative distribution function is the **PDF** (or failure density) of the random variable x:

$$f(x) = \frac{dF(x)}{dx}$$

The relationship between the **Cumulative distribution function *F(x)*** and the **PDF *f(x)*** is in Figure 1.8.

These definitions for $F(x)$ allow to express $\mathbb{P}\{a \leq X \leq b\}$ as follows:

$$\mathbb{P}\{a \leq X \leq b\} = \int_{a}^{b} f(x)dx = F(b) - F(a)$$

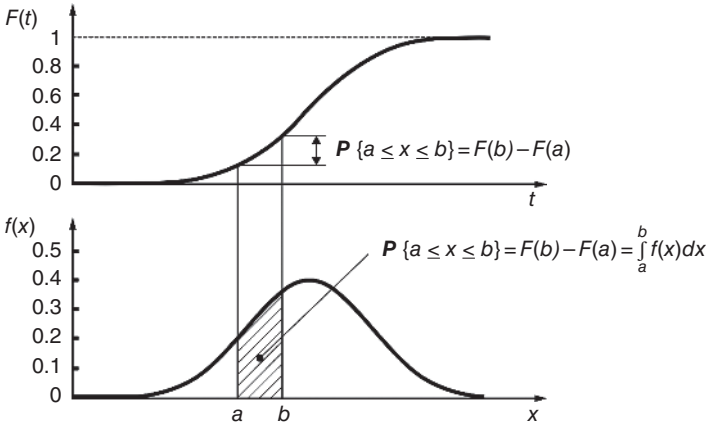


Figure 1.8 *F*(*t*) and *f*(*t*).

Since **we reason in terms of time** and time is a positive random variable failure time, the **Cumulative Distribution Function** can be written in the following way:

$$F(t) = \int_0^t f(x)dx$$

It is represented graphically as in Figure 1.9.

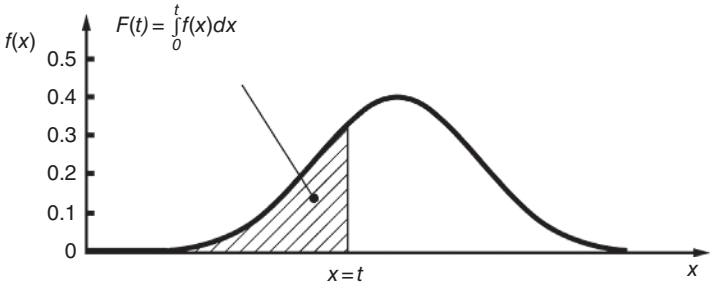


Figure 1.9 *F*(*t*) and *f*(*t*) for a continuous random variable.

and please consider that

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

1.4.4 The Reliability Function *R*(*t*)

R(*t*) is the probability that no failure of the item occurs in the interval (0, *t*]. It is represented in Figure 1.10.

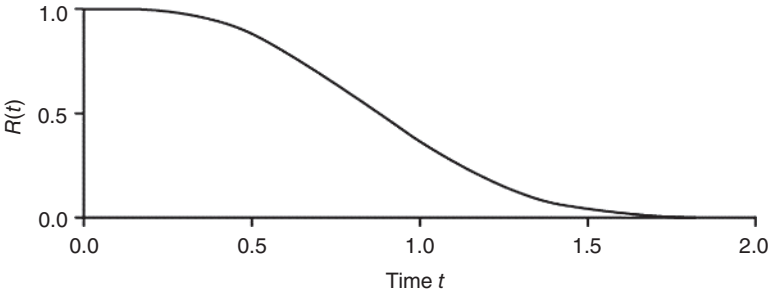


Figure 1.10 The reliability function $R(t)$.

In other terms, $R(t)$ is the probability that an item will operate "failure-free" in time interval $(0, t]$, while the failure will occur in $(t, +\infty)$. Known the PDF $f(x)$ can be represented graphically as in Figure 1.11, we have:

$$R(t) = \int_{t}^{+\infty} f(x)dx$$

$R(t)$ can be represented graphically as the area under $f(x)$ starting from $x = t$, as in Figure 1.11.

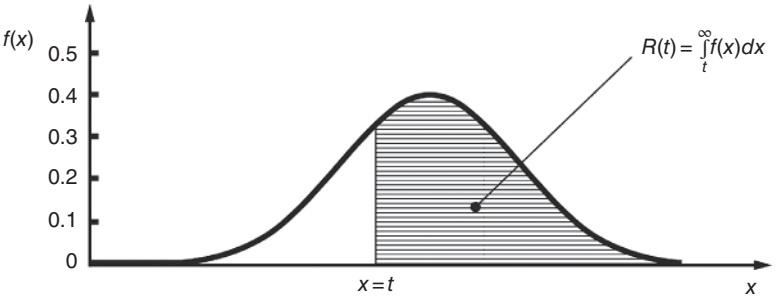


Figure 1.11 $R(t)$ for a continuous random variable.

If the system can be found in two states only, either correct functioning or failure, we can define the function of unreliability $F(t)$ as complementary to $R(t)$, that means:

$$F(t) = 1 - R(t) = \int_{0}^{t} f(x)dx$$

The density function $f(t)$ can now be expressed as:

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \qquad \text{[Equation 1.4.4]}$$

1.5 Failure Rate λ

The failure rate is the basis of the Functional Safety theory.

> ***[IEC 61508-4] 3.6 Fault, failure and error***
>
> ***3.6.16 Failure Rate****. Reliability parameter $\lambda(t)$ of an entity (single components or systems) such that $\lambda(t)dt$ is the probability of failure of this entity within $[t, t + dt]$ provided that it has not failed during $[0, t]$*

Mathematically, $\lambda(t)$ is the conditional probability of failure per unit of time over $[t, t + dt]$. It is possible to demonstrate that the instantaneous failure rate is:

$$\lambda(t) = \frac{f(t)}{R(t)}$$

Using the Equation 1.4.4, it is possible to obtain:

$$\lambda(t) = \frac{-dR(t)/dt}{R(t)} = -\frac{d}{dt}\ln R(t)$$

Integrating the upper equation in time:

$$R(t) = exp\left(-\int_0^t \lambda(\tau)d\tau\right)$$

Failure rates and their uncertainties can be estimated from field feedback using conventional statistics.

The most diffuse and widely known model for the failure rate is the "bathtub" curve, represented in Figure 1.12. In the **initial phase** of the component lifetime, $\lambda(t)$ decreases rapidly with time; this fact derives from the existence of a "weak" fraction of the population whose defects cause a failure within a short period of time from the moment they are produced.

In the period called **useful life**, $\lambda(t)$ is approximately constant, in case for example, of electronic components. For electromechanical components, $\lambda(t)$ is a function of time and, in this interval, it constantly increases.

The last period is characterized by **wear out**, with a rapidly increasing failure rate $\lambda(t)$ caused by wearing out, aging, and fatigue.

During the useful life of a component with a **constant failure rate**, considering as an initial condition that Reliability at time 0 is at a maximum and it is equal to 1, we have:

$$R(t) = exp\left(-\int_0^t \lambda d\tau\right) = e^{-\lambda t}$$

The Reliability function $R(t)$ is shown in Figure 1.13a and the PDFs $f(t)$ in Figure 1.13b, in the case $\lambda =$ constant.

Table 1.3 shows a summary of the four functions described so far.

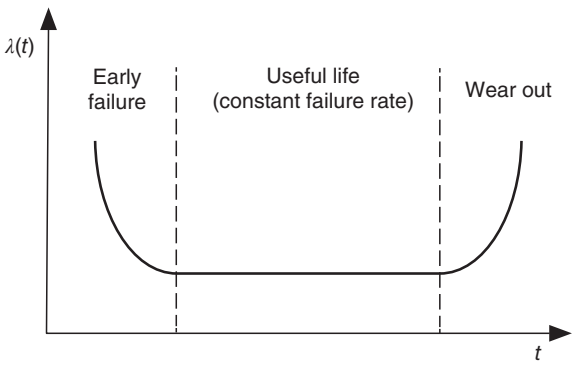


Figure 1.12 The bathtub graph.

Figure 1.13 (a) $R(t)$ and (b) $f(t)$.

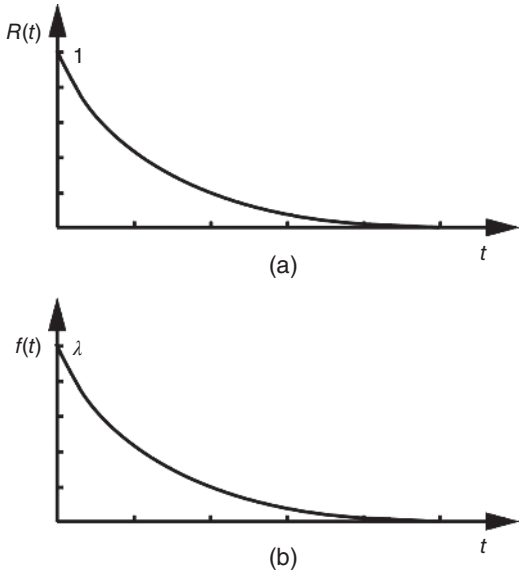


Table 1.3 Summary of the key functions used in Reliability theory.

	$F(t)$	$f(t)$	$R(t)$	$\lambda(t)$	λ = constant
$F(t)$	—	$\int_0^t f(\tau)d\tau$	$1-R(t)$	$1-exp\left(-\int_0^t \lambda(\tau)d\tau\right)$	$1-e^{-\lambda t}$
$f(t)$	$\frac{d}{dt}F(t)$	—	$-\frac{d}{dt}R(t)$	$\lambda(t)\cdot exp\left(-\int_0^t \lambda(\tau)d\tau\right)$	$\lambda \cdot e^{-\lambda t}$
$R(t)$	$1-F(t)$	$\int_t^{+\infty} f(\tau)d\tau$	—	$exp\left(-\int_0^t \lambda(\tau)d\tau\right)$	$e^{-\lambda t}$
$\lambda(t)$	$\frac{dF(t)/dt}{1-F(t)}$	$\frac{f(t)}{\int_t^{+\infty} f(\tau)d\tau}$	$-\frac{d}{dt}\,ln\,(R(t))$	—	—

Figure 1.14 shows the relationship between $F(t)$ and $R(t)$.

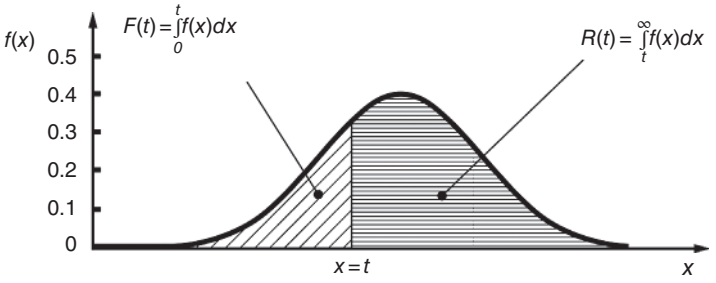


Figure 1.14 $R(t)$ and $F(t)$.

1.5.1 The Maclaurin Series

Mathematically, it can be shown that certain functions can be approximated by a series of other functions. In particular, e^x can be developed as a so-called Maclaurin series:

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$$

In case $x \ll 1$,

$$e^x \approx 1 + x$$

That means the Reliability $R(t)$ and Unreliability $F(t)$ functions can be approximated to

$$R(t) = e^{-\lambda t} \approx 1 - \lambda t$$
$$F(t) = 1 - R(t) \approx \lambda t$$

1.5.2 The Failure in Time or FIT

The failure rate λ has a unit of inverse time: it is a common practice to use the unit of "failures per billion (10^9) hours". This unit is known as **FIT: Failure in Time**.

1.5.2.1 Example

A component has a failure rate of 1000 FITs (10^{-6} h^{-1}).

Question: What is its probability of failure after 10^5 hours (about 11 years)?

$$F(t) = 1 - e^{-\lambda t} = 1 - e^{-10^{-6} t} \Rightarrow F\left(10^5\right) = 1 - e^{-10^{-6} \cdot 10^5} = 1 - e^{-0.1} \cong 0.095$$

By using the approximated formula

$$F\left(10^5\right) = 1 - e^{-\lambda t} \approx \lambda t = 10^{-6} \cdot 10^5 = 0.1$$

Answer: the probability of failure after approximately 11 years is 10%.

1.6 Mean Time to Failure

In case of **non-repairable devices**, for example an incandescent lamp, it is common to define the MTTF as an indication of its Reliability.

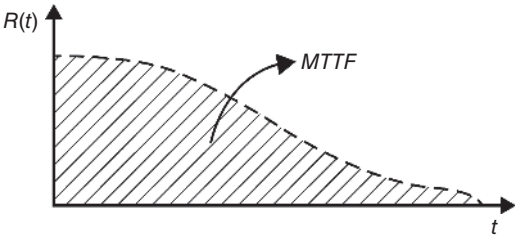
We need to find the expression of the mean of the continuous random variable t_f with density $f(t)$. Defining E, the mean operator, MTTF is:

$$MTTF = E(t) = \int_{-\infty}^{+\infty} t \cdot f(t) dt$$

Since the time is a positive random variable, the previous equation can be reduced to:

$$MTTF = E(t) = \int_{0}^{+\infty} t \cdot f(t) dt$$

Figure 1.15 MTTF and $R(t)$.



$$MTTF = \int_0^{+\infty} t\frac{dF(t)}{dt}dt = \int_0^{+\infty} -t\frac{dR(t)}{dt}dt = -[t \cdot R(t)]_0^{\infty} + \int_0^{+\infty} R(t)dt = \int_0^{+\infty} R(t)dt$$

MTTF represents the area under the Reliability function $R(t)$, as shown in Figure 1.15.

Based upon the previous considerations and assuming a **constant failure rate,** it follows that:

$$MTTF = \int_0^{+\infty} R(t)dt = \int_0^{+\infty} e^{-\lambda \cdot t} = \frac{1}{\lambda}$$

1.6.1 Example of a Non-Constant Failure Rate

A component has the following Reliability function:

$$R(t) = \frac{1}{(0.2t+1)^2}$$

where t represents the months. The PDF is:

$$f(t) = -\frac{dR(t)}{dt} = \frac{0.4}{(0.2t+1)^3}$$

The failure rate is a function of time:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{0.4}{0.2t+1}$$

All three functions are represented in Figure 1.16. MTTF can be calculated as:

$$MTTF = \int_0^{+\infty} R(t)dt = \int_0^{+\infty} \frac{1}{(0.2t+1)^2}dt = 5 \text{ months}$$

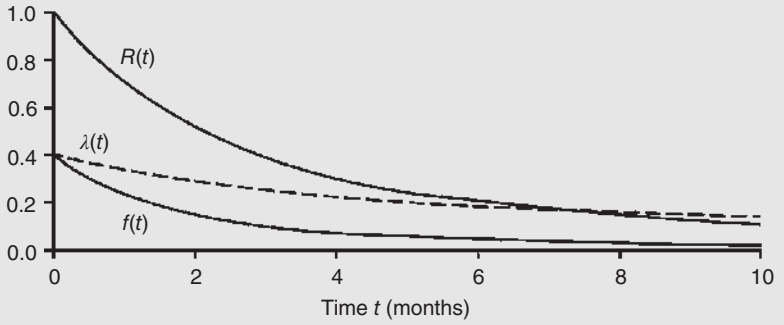


Figure 1.16 $R(t)$, $f(t)$ and $\lambda(t)$.

1.6.2 The Importance of the MTTF

The MTTF is one of the most important parameters used in Functional Safety. Let's look at the value of unreliability $F(t)$ of a component with constant failure rate when it reaches its MTTF value.

$$F(t) = 1 - e^{-\lambda t} \Rightarrow F(t = MTTF) = F\left(t = \frac{1}{\lambda}\right) = 1 - e^{-\lambda \cdot \frac{1}{\lambda}} = 1 - e^{-1} \cong 0.63$$

Therefore, when a component **having a constant failure rate** reaches its MTTF time, its unreliability is about 63% or, in other terms, its Reliability is 37%.

1.6.3 The Median Life

The MTTF is just one way of representing what is also called a "life distribution $f(t)$." Another method is the **Median Life** t_m defined as

$$R(t_m) = 0.5$$

The median divides the distribution in two halves. The component will fail before time t_m with 50% probability.

1.6.4 The Mode

The **Mode** t_{mode} of a life distribution $f(t)$ is the most likely failure time; in other terms, it is the time when the probability density $f(t)$ attains its maximum.

$$f(t_{mode}) = \max_{0 \le t \le \infty} f(t)$$

Figure 1.17 shows the location of the three parameters for a distribution skewed to the right.

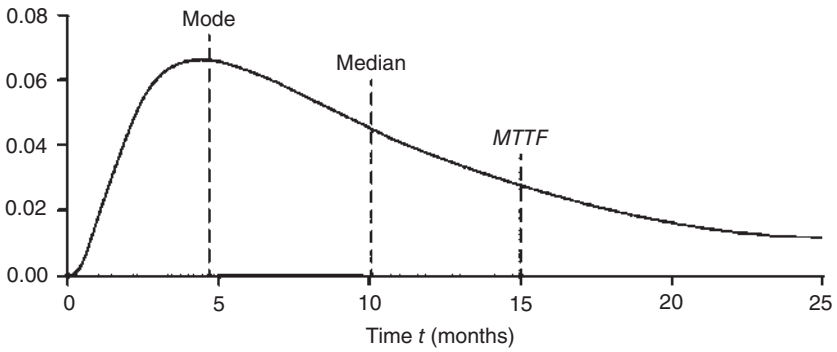


Figure 1.17 Graphical representation of mode, median and MTTF.

1.6.4.1 Example

A component has a constant failure rate $\lambda = 2.5{\cdot}10^{-5}\ \mathrm{h}^{-1}$

1. What is the probability that it survives a period of two months, without failures?

$$R(t) = e^{-\lambda t} \Rightarrow R(t = 1460) = e^{-2.5 \cdot 10^{-5} \cdot 1460} = e^{-0.0365} = 0.96$$

which means **96**%

2. What is its MTTF value?

$$MTTF = \frac{1}{\lambda} \cong 4.6 \text{ years}$$

3. What is the probability the component will survive till its MTTF?

$$R(t) = e^{-\lambda t} \Rightarrow R\left(t = \frac{1}{\lambda}\right) = e^{-1} \cong 0.37$$

which means **37**%

1.6.4.2 Example

A hydraulic solenoid valve, with constant failure rate λ, will survive a period of two years without failure, with a probability of 90%.

1. Calculate the valve MTTF

$$R(t) = e^{-\lambda t} \Rightarrow 0.9 = e^{-\lambda \cdot 17\,520}$$

Therefore $\lambda = 6.01{\cdot}10^{-6}$; that means ***MTTF* = 19 years**

2. Find the probability that the valve will have a failure during the time of 10 years.

$$F(t) = 1 - e^{-\lambda t} \Rightarrow F(t = 10 \text{ years}) = 1 - e^{-\lambda t} = 1 - e^{-6.01 \cdot 10^{-6} \cdot 87\,600} = 0.40$$

which means **40**% failure probability (or 60% survival probability).

3. What is the probability that the valve will fail after 10 years, knowing that it did not fail after 5 years?

Let's first calculate the survival probability

$$\frac{R(t_1 + t_2)}{R(t_1)} = \frac{e^{-(6.01 \cdot 10^{-6} \cdot 87\,600)}}{e^{-(6.01 \cdot 10^{-6} \cdot 43\,800)}} \cong \frac{0.6}{0.77} \cong 0.78$$

which means a survival probability of 78% and therefore a failure probability of 22%.

Please notice that the fact that being 5 years in the way, with the valve that did not fail, gives a higher probability of survival in the 10 years period.

1.7 Mean Time Between Failures

Considering an item or a system that, following a failure, can be **restored**, (these are called **Repairable systems**), the MTBF is the parameter normally used to indicate its level of Reliability.

The MTBF **is defined as the average time period of a Failure + Repair cycle**. It includes the time to failure, any time required to detect the failure, and the actual **repair or restoration time**.

Hereafter the key definitions

> ***[ISO 13849-1] 3 Terms, definitions, symbols and abbreviated terms***
> ***3.1.33 Mean Time Between Failures (MTBF)***
> *Expected value of the operating time between consecutive failures.*
>
> ***[IEC 61508-4] 3.6 Fault, failure and error***
> ***3.6.21 Mean Time to Restoration (MTTR)**. Expected time to achieve restoration.*

MTTR encompasses (please see Figure 1.18):

a) the time to detect the failure and,
b) the time spent before starting the repair and,
c) the effective time to repair and,
d) the time before the component is put back into operation.

The sum of the b + c + d time is called **Mean Repair Time** (MRT).

The relationship then becomes:

$$MTBF = MTTF + MTTR$$

If a system is non-repairable, $MTBF = MTTF$. That is the reason why, where only MTBF values are available, **if** the RDF (Ratio of Dangerous Faults) is assumed as 50% of all failures, a conversion to $MTTF_D$ values can be done by

$$MTTF_D \approx 2^{*} MTBF$$

Otherwise, the worst case is supposing all failures to be dangerous, in that case:

$$\boldsymbol{MTTF_D \approx MTBF}$$

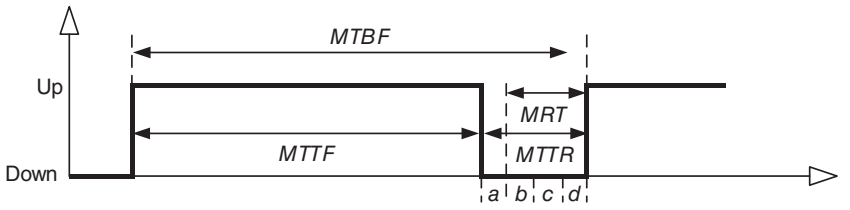


Figure 1.18 Relationship between MTTF and MTBF.

1.8 Frequency Approach Example

In order to make it clear what the Reliability and Unreliability functions stand for, hereafter a simple example. Using the concept of probability based on **relative frequency**, the probability of any event E is defined as:

$$P(E) = \frac{number\ of\ elements\ of\ E}{number\ of\ all\ possible\ outcomes} = \frac{n_E}{n}$$

Combining the $P(E)$ frequency approach with the following formula (§ 1.4.2)

$$\mathbb{P}\{a \leq X \leq b\} = \int_a^b f(x)dx$$

It is possible to define the experimental histogram of relative frequency:

$$f(x) \cdot \Delta x = \frac{n(x)}{n}$$

From a practical point of view, this means that after repeating the experiment n times and after counting the tests $n(x)$, the relationship $x \leq X \leq x + \Delta x$, involving the random variable X is valid. Thinking in histogram terms, Δx represents the width of the classes.

With all these considerations there is an **empirical definition** of Reliability, Unreliability, Density function, and Failure rate, extracted from the **observation and analysis of failure data**.

1.8.1 Initial Data

Let's consider $n = 172$ identical elements, which are statistically independent. We put them into operation under same conditions at time $t = 0$. We obtain the experimental data reported in the table

Time interval (h)	No. of failures at the end of interval
0–1000	59
1000–2000	24
2000–3000	29
3000–4000	30
4000–5000	17
5000–6000	13
Total	**172**

1.8.2 Empirical Definition of Reliability and Unreliability

We will try to arrive at a definition of Reliability and Unreliability in "empirical" terms.

$n_h(t)$ indicates the subset of elements n which have not yet failed at time t, while $n_f(t)$ indicates the number of elements that have failed in time t, considering that $n_h(t) + n_f(t) = n$.

It is now possible to obtain the following definitions:

$$R(t) = \frac{n_h(t)}{n}$$

$$F(t) = \frac{n_f(t)}{n} = \frac{n - n_h(t)}{n} = 1 - R(t)$$

Considering the experimental data, we can evaluate $R(t)$ and $F(t)$ both numerically and graphically (please refer to Figures 1.19 and 1.20).

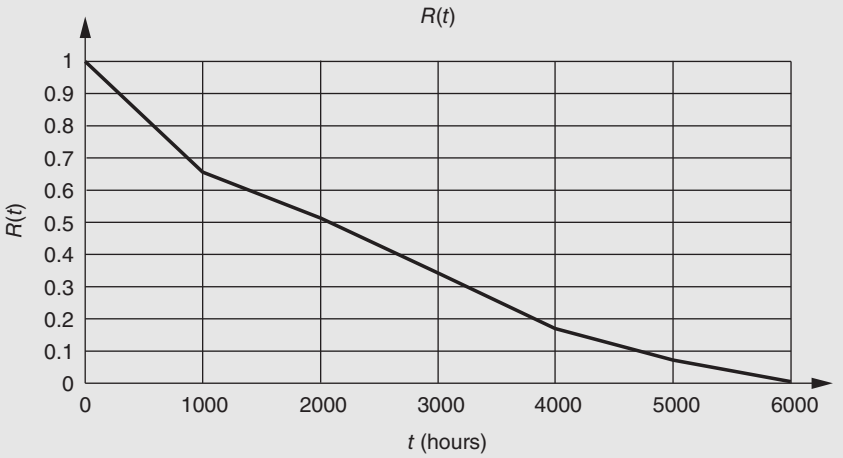


Figure 1.19 $R(t)$.

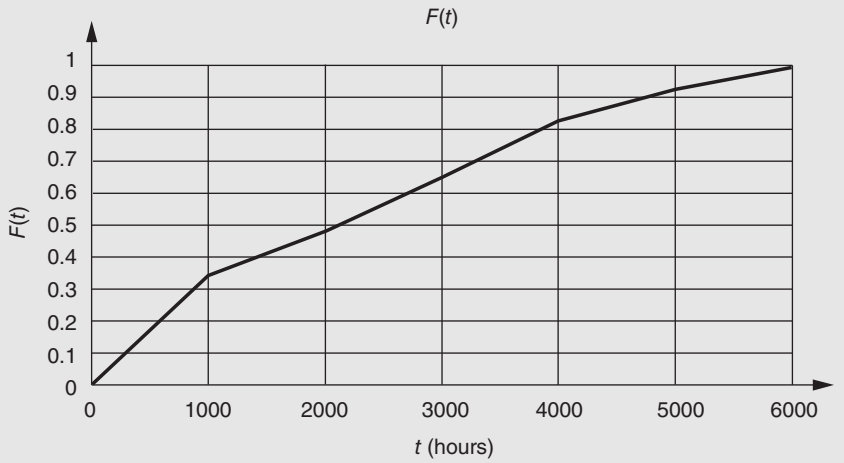


Figure 1.20 $F(t)$.

t (h)	n_h (t)	$R(t)$	n_f (t)	$F(t)$
0	172	1.000	0	0.000
1000	113	0.657	59	0.343
2000	89	0.517	83	0.483
3000	60	0.349	112	0.651
4000	30	0.174	142	0.826
5000	13	0.076	159	0.924
6000	0	0.000	172	1.000

In this case, the experimental histogram of relative frequency can be expressed in the following terms:

$$f_N(t) = \frac{n_f(t+\Delta t) - n_f(t)}{n}\frac{1}{\Delta t} = \frac{F_N(t+\Delta t) - F_N(t)}{\Delta t}$$

We also have the possibility to express the failure rate as the ratio between elements that have broken down in the interval $(t, t+\Delta t]$ and the number of elements functioning at time t, that is:

$$\lambda_N(t) = \frac{n_f(t+\Delta t) - n_f(t)}{n_h(t)}\frac{1}{\Delta t} = f_N(t)\frac{n}{n_h(t)} = \frac{f_N(t)}{R_N(t)}$$

Time interval (h)	f (time interval) 10^{-3}	λ (time interval) 10^{-3}
0–**1000**	0.343	0.343
1001–**2000**	0.140	0.212
2001–**3000**	0.169	0.326
3001–**4000**	0.174	0.500
4001–**5000**	0.099	0.567
5001–**6000**	0.076	1.000

The $f(t)$ and $\lambda(t)$ presented in the above table, can be represented graphically in Figures 1.21 and 1.22.

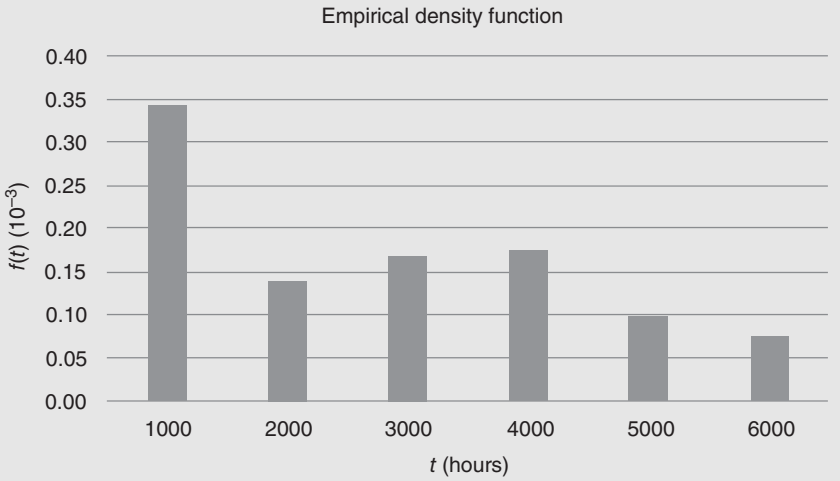


Figure 1.21 $f(t)$.

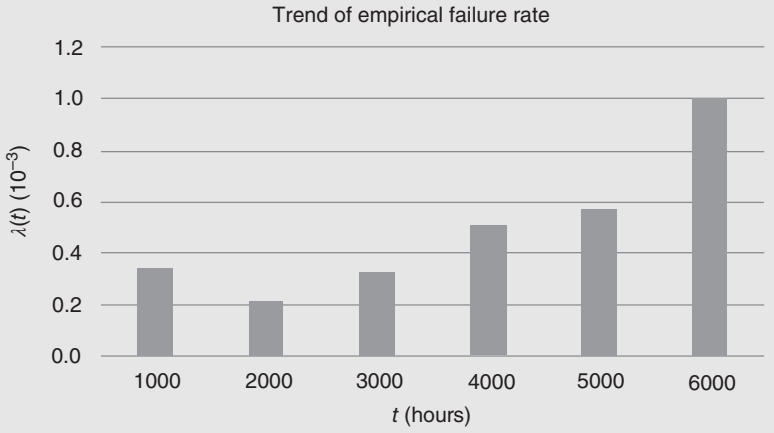


Figure 1.22 $\lambda(t)$.

1.9 Reliability Evaluation of Series and Parallel Structures

1.9.1 The Reliability Block Diagrams

A Reliability block diagram (RBD) illustrates the state of a system with several items. The diagram is made up of **functional blocks**, represented as rectangles, connected by lines. The RBD has a single starting point (a) and a single ending point (b), as shown in Figure 1.23.

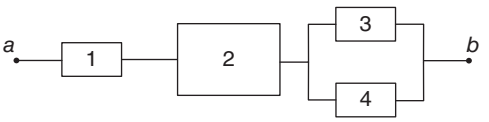


Figure 1.23 Example of a safety function.

In the book, a slightly different graphic will be used: the one shown in Figure 1.24. Normally the biggest block represents the logic unit.

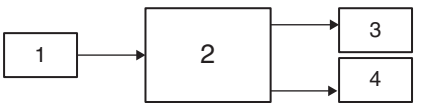


Figure 1.24 Example of a safety function.

In general, each functional block can have two different states, a **functioning state and a failed state**. A functional block may represent an item or a specific function of an item. When the function of the item is **available**, we can pass through the functional block. If we can pass through enough functional blocks to go from (a) to (b), we say that the system is functioning correctly, with respect to its specified function. Guidance to RBD construction and analysis is given in IEC 61078 [26].

Note: Throughout the book, the term Safety-related Block Diagram instead of Reliability Block Diagram will be used.

1.9.2 The Series Configuration

The series functional configuration, whose block diagram is shown in Figure 1.25, represents the simplest and most common Reliability model: a system *S*, composed of n elements, each one with Reliability $R_i(t)$.

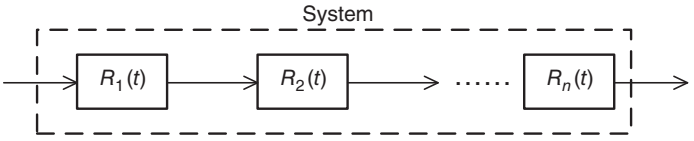


Figure 1.25 RBD for the series configuration.

In the simplified hypothesis of independent events, for which we can assume that the performance of every element, in terms of correct functioning or failure, does not depend on the condition assumed by other elements, the Reliability of the system corresponds to the product of the Reliability of single blocks:

$$\boldsymbol{R_s(t) = R_1(t) \cdot R_2(t) \cdots R_n(t) = \prod_{i=1}^{n} R_i(t)}$$

Assuming:

$$\boldsymbol{R_i(t) = e^{-\lambda_i t}}$$

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = e^{-\left(\sum_{i=1}^{n} \lambda_i\right) t}$$

Therefore, the failure rate of the system λ_S is the sum of the failure rates of the constituent elements λ_i (Figure 1.26). Consequently, the MTTF for the system, in hours, is:

$$MTTF_s = \int_0^{+\infty} R(t)dt = \left[\frac{e^{-\left(\sum_{i=1}^{n} \lambda_i\right) t}}{-\left(\sum_{i=1}^{n} \lambda_i\right)} \right]_0^{\infty} = \frac{1}{\sum_{i=1}^{n} \lambda_i} = \frac{1}{\lambda_s}$$

$$\lambda_s = \sum_{i=1}^{n} \lambda_i$$

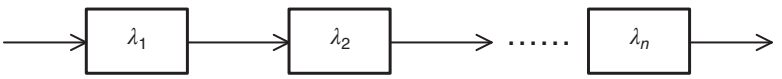


Figure 1.26 The failure rates of reliability functions $R_i(t)$.

In case of **two systems in series** have the same failure rate:

$$\lambda_s = 2\lambda$$

$$MTTF_s = \frac{1}{\lambda_s} = \frac{1}{2\lambda}$$

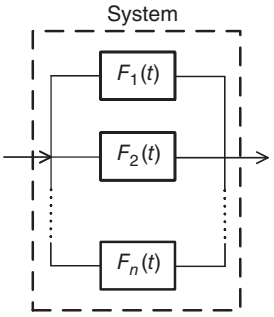


Figure 1.27 RBD for the parallel configuration.

1.9.3 The Parallel Configuration

The parallel function configuration, also called **redundant configuration**, is important when it is necessary to increase the Reliability of a system. The RBD for such a configuration is shown in Figure 1.27.

The system is not functioning when all the elements are faulty, therefore the unreliability of a system corresponds to the product of the unreliability of the constituting elements.

$$\boldsymbol{F_s(t)} = F_1(t) \cdot F_2(t) \cdots F_n(t) = \prod_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{F_i(t)}$$

The Reliability function is, therefore

$$R_s(t) = 1 - F_s(t) = 1 - \prod_{i=1}^{n} F_i(t) = 1 - \prod_{i=1}^{n} \left(1 - e^{-\lambda_i \cdot t}\right)$$

Considering two systems in parallel:

$$R_s(t) = 1 - \left(1 - e^{-\lambda_1 \cdot t}\right) \cdot \left(1 - e^{-\lambda_2 \cdot t}\right) = e^{-\lambda_1 \cdot t} + e^{-\lambda_2 \cdot t} - e^{-(\lambda_1 + \lambda_2) \cdot t}$$

The MTTF for the system, in hours, is:

$$MTTF_s = \int_0^{+\infty} R(t)dt = \left[\frac{e^{-\lambda_1 \cdot t}}{-\lambda_1}\right]_0^{\infty} + \left[\frac{e^{-\lambda_2 \cdot t}}{-\lambda_2}\right]_0^{\infty} - \left[\frac{e^{-(\lambda_1 + \lambda_2) \cdot t}}{-(\lambda_1 + \lambda_2)}\right]_0^{\infty} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

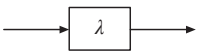
In case the two systems have the same failure rate:

$$MTTF_s = \frac{3}{2 \cdot \lambda}$$

which is a 50% improvement compared with the single element. However, in the parallel case λ_s is a function of time.

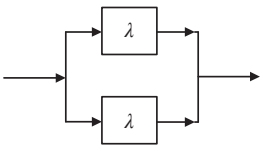
1.9.3.1 Two Equal and Independent Elements

Let's consider an element having a constant failure rate λ

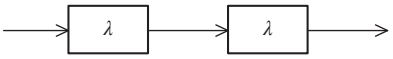


$$R_E(t) = e^{-\lambda t}$$

Let's now compare the configurations with two equal and independent elements functioning in series and in parallel, and plot the Reliability with a single element having the same constant failure rate.



$$R_P(t) = 1 - \left(1 - e^{-\lambda t}\right)^2 = 2e^{-\lambda t} - e^{-2\lambda t}$$



$$R_s(t) = \left(e^{-\lambda t}\right)^2 = e^{-2\lambda t}$$

In Figure 1.28 the three functions are compared.

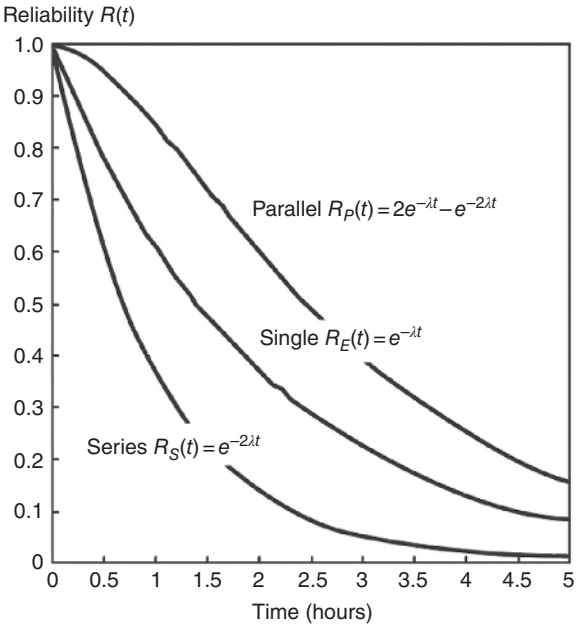


Figure 1.28 Comparison among basic configurations with the same failure rate.

Example 1 Elements in Series.
Please refer to Figure 1.29.

If the values of Reliability of each element, at generic time t, are 0.4, 0.7, and 0.9, respectively, the probability of the system functioning at time t is equal to:

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = 0.4 \cdot 0.7 \cdot 0.9 = 0.252$$

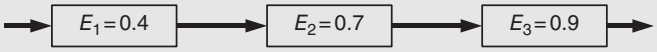


Figure 1.29 RBD for a system made of three elements in a series configuration.

Example 2 Elements in Parallel.

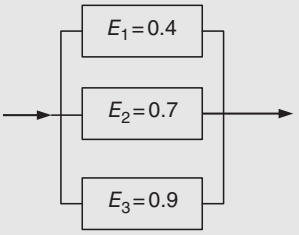


Figure 1.30 RBD for a system made of three elements in a parallel configuration.

Please refer to Figure 1.30.

If the values of Reliability of each element, at time t, are 0.4, 0.7, and 0.9, respectively, the probability of the system functioning at the time t becomes:

$$R_s(t) = 1 - F_s(t) = 1 - \prod_{i=1}^{n} F_i(t) = 1 - (0.6 \cdot 0.3 \cdot 0.1) = 0.982$$

Example 3 Elements Both in Parallel and in Series.

Please refer to Figure 1.31.

Applying the preceding relations in which active redundancy is positioned on the element E_1, with a Reliability value of 0.4, we obtain:

$$R_{S_{PARALLEL}}(t) = 1 - F_s(t) = 1 - \prod_{i=1}^{n} F_i(t) = 1 - (0.6 \cdot 0.6) = 0.64$$

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = 0.64 \cdot 0.7 \cdot 0.9 = 0.4032$$

It is possible to note that redundancy of the less reliable element (E_1) increases the Reliability of the entire system. The Reliability of the entire system is now equal to 0.4, with an increase of 60% with respect to the value of 0.252 in the first example.

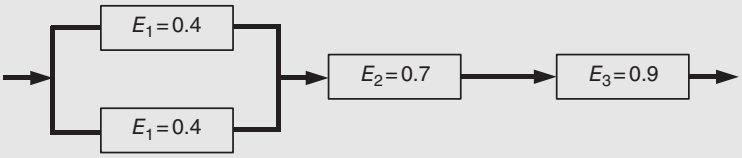


Figure 1.31 RBD for a system made of both parallel and serial configurations.

1.9.4 *M* Out of *N* Functional Configurations

A particular configuration is represented by a system where **at least *M* number of elements, out of a total of *N*, are functioning normally**. The configuration is also called *M*-out-of-*N* redundancy with $M \leq$ N or MooN. Here is the definition according to [16].

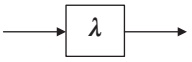
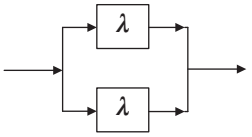
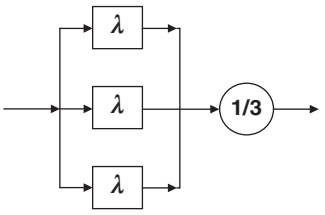
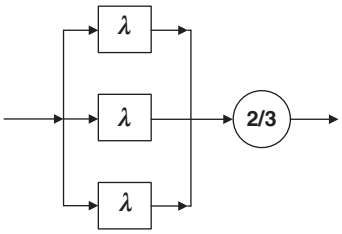
> ***[IEC 61511-1] 3.2 Terms and definitions***
> ***3.2.41 MooN****. SIS, or part thereof, made up of "N" independent channels, which are so connected, that "M" channels are sufficient to perform the SIF.*

For this configuration, we can assume a structure in which M elements are in active redundancy and the remaining elements (N–M) are in stand-by. A typical example is **a steel cable** formed of N strands that can withstand foreseen stress if at least M numbers of strands are intact.

When the concept is applied to a safety system:

- a **1oo1** is a single channel subsystem, for example a low pressure switch. When the sensor detects low pressure, it shuts down the process.
- a **1oo2** is a subsystem with redundant channels; for example, two pressure switches both detecting a low value. In case one triggers, the safety function will trigger.
- A **1oo3** is a subsystem with three channels; again, in case of a risk given by low pressure, each of the sensors have the same setting; as soon as one of the three detects low pressure, the safety system shuts down the process or the machine.
- In a **2oo3** subsystem, instead, we need two of the three sensors to trigger, in order to trigger the safety function.

The following table summarizes the main configurations used in Functional Safety.

Configuration	RBD	Reliability model	$MTTF_S$
Single element **(1oo1)**		$R(t) = e^{-\lambda t}$	$\frac{1}{\lambda}$
1-out-of-2 **(1oo2)**		$R(t) = 2e^{-\lambda t} - e^{-2\lambda t}$	$\frac{9}{6 \cdot \lambda}$
1-out-of-3 **(1oo3)**		$R(t) = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$	$\frac{11}{6 \cdot \lambda}$
2-out-of-3 **(2oo3)**		$R(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$	$\frac{5}{6 \cdot \lambda}$

1.10 Reliability Functions in Low and High Demand Mode

Functional safety was born having in mind the Reliability aspects of Safety-related Control Systems, designed to be activated upon hazardous process deviations; the latter is a process demand generating a Demand Rate of the safety system that protects people, the environment, and material assets.

The parameter used to indicate the Reliability of a Safety-related Control System is the **Unreliability function $F(t)$**. More precisely, there are two functions used, depending if the safety system is working in Low or in High demand mode. Just to give an example, the car airbag safety system is operating in low demand mode since it may remain inactive for years, until a demand occurs (due to a car crash).

In low demand mode, the parameter used to indicate the (un)reliability of a safety function is PFD_{avg}, while in high demand it is PFH(T).

> ***[IEC 61508-4] 3.6 Fault, failure and error***
> ***3.6.18 Average probability of dangerous failure on demand*** *(PFD_{avg}). Mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.*

$$\boldsymbol{PFD_{avg}} = \frac{1}{T_i}\int_0^{T_i} PFD(t)dt$$

In high demand mode safety systems, the parameter used is PFH(t):

> ***[IEC 61508-4] 3.6 Fault, failure and error***
> ***3.6.19 Average frequency of a dangerous failure per hour*** *(PFH). Average frequency of a dangerous failure of an E/E/PE safety related system to perform the specified safety function over a given period of time.*

$$\boldsymbol{PFH}(\boldsymbol{T}) = \frac{1}{T}\cdot\int_0^{T} w(t)dt$$

1.10.1 The PFD

The PFD(t) is the unreliability function $F(t)$ used in low demand mode. Hereafter its definition, supposing a constant failure rate λ:

> ***[IEC 61508-4] 3.6 Fault, failure and error***
> ***3.6.17 Probability of dangerous failure on demand*** *(PFD). Safety unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.*

$$\boldsymbol{PFD} = 1 - e^{-\lambda t} \qquad \text{[Equation 1.10.1]}$$

Therefore, the instantaneous unreliability PFD(t) describes the probability that a safety system is not in a state to perform its required function, under given conditions, at a given instant of time, assuming that the required external resources are provided. Again, it is what we called so far ***F(t).***

$$PFD = 1 - e^{-\lambda t}$$

Considering, for example, a valve with a $\lambda = 50.000$ FIT, its PFD(t) is shown in Figure 1.32. As you can see, the unreliability increases with time; after two years (17 520 hours), $PFD \approx 58\%$. After four years (35 040 hours), $PFD \approx 83\%$.

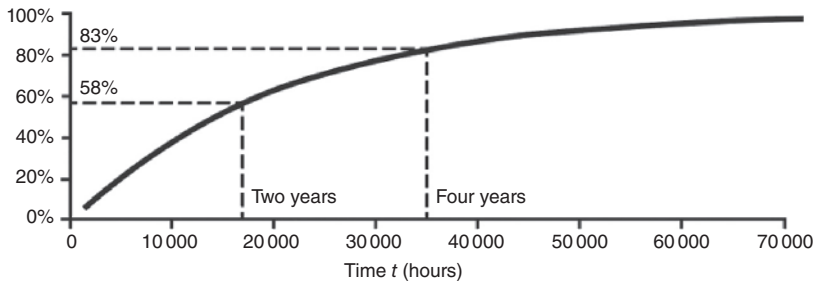


Figure 1.32 PFD over eight years for λ = 50 000 FIT.

Considering a $\lambda = 5.000$ FIT, a more realistic value, its PFD(t) is shown in Figure 1.33. First of all, the PFD has improved: after two years, PFD $\approx 8\%$ and after four years, PFD $\approx 16\%$. **Moreover**, the function can be approximated to a linear one, in case $\lambda \cdot t \ll 1$.

$$PFD = PFD(t) = 1 - e^{-\lambda t} \approx \lambda \cdot t$$

As it can be seen from both graphs, the System unreliability increases with time. Going back to the example of the airbag, that means its probability of failure will be very low when the car is new, and it will increase month by month. That is valid for all the elements of a **Safety Instrumented System** (SIS), that is made by one or more sensors, a logic unit, and one or more actuators.

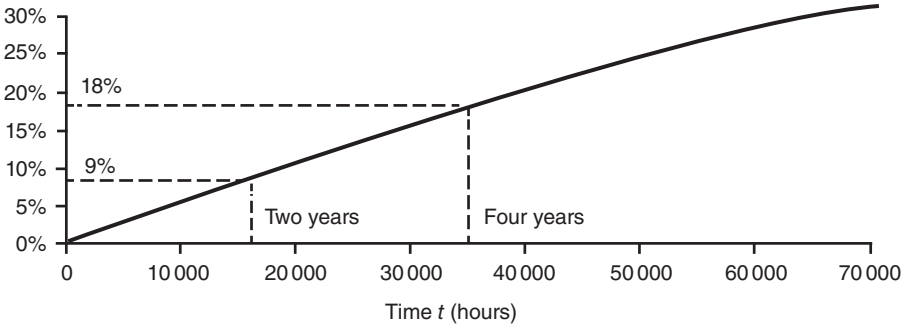


Figure 1.33 PFD over eight years for λ = 5000 FIT.

1.10.1.1 The Protection Layers

A SIS may fail while in passive state and the failure may remain hidden until a demand occurs from the process or until the system is tested.

Let's suppose the pressure in a vessel is controlled by a pressure transmitter and the process control system has to keep the value around a certain set point.

In case the pressure increases above a certain threshold (PSH), an alarm is generated (PAH). In case the value goes "out of control," a safety pressure switch, set at PSHH, shuts down the process (Figure 1.34).

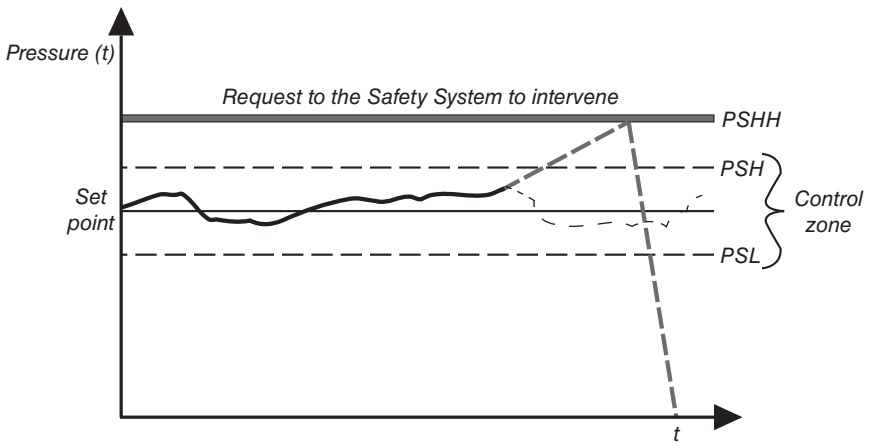


Figure 1.34 Request upon the safety system.

Figure 1.35 EUC, the process control system, and safety system.

We see that there are two protection layers: a Control one and a Safety one. They normally do not share the same field components. In our example, the pressure transmitter belongs to the Control Layer, while the safety pressure switch to the Safety Layer.

Normally, the process control system keeps the pressure around the set point. Very rarely the pressure goes out of control, and at that moment the Safety System intervenes: the issue is that it may have failed in the meantime. A SIS is so-called an **independent protection layer.** It is installed to mitigate the risk associated with the operation of a process that is normally hazardous, and it is called the **Equipment Under Control or EUC** (Figure 1.35).

A Safety Instrumented Function (SIF) is implemented with a SIS that is intended to achieve or maintain a safe state for the EUC with respect to a specific process demand (a high pressure for example). A SIS may consist of one or more SIFs.

1.10.1.2 Testing of the Safety Instrumented System

SISs are normally dormant and their failure may remain undetected, or hidden, until there is a demand upon them (a high temperature or pressure, for example) or until the system is tested if it is still working properly.

There are two types of tests that can be done on such systems.

Diagnostic Testing. They are done automatically by the component itself, or by the logic solver, or by other elements of the safety system. The extent to which this automatic testing reveals a failure is called Diagnostic Coverage (DC). The failures that can be detected in this way are defined as Detectable, the remaining failures are called Undetectable.

Function Testing. The objective of the function testing is especially to reveal the **undetectable failures** and to verify that the system is still able to perform its required function, in case a process demand occurs. Function testing, defined in IEC 61508 as **Proof Test**, is normally done manually, or initiated manually. The time interval between two function tests is indicated as T_i and, in case of a **perfect Proof Test**, the item is considered "as new," after such a test. Please refer to Chapter 3 for the definition of Proof Test and further details.

Do not get confused between Function Test and Functional Test. In literature, you may find that the Proof test is defined as a Function Test, as well as Periodic Test, while the DC is also defined as a Functional Test.

1.10.2 The PFD_{avg}

For a single channel subsystem, the Average PFD is defined as

$$\boldsymbol{PFD_{avg}} = \frac{1}{T_i}\int_0^{T_i} PFD(t)dt = \frac{1}{T_i}\int_0^{T_i}\left(1-e^{-\lambda\cdot t}\right)dt \cong \frac{1}{T_i}\int_0^{T_i}\lambda\cdot t dt = \frac{\lambda\cdot T_i^2}{2\cdot T_i} = \boldsymbol{\frac{\lambda\cdot T_i}{2}}$$

[Equation 1.10.2]

T_i is the time when the system is function tested. The PFD(T) of a SIF, that is periodically tested, is represented by a saw tooth curve, with a probability ranging from low, just after a test, to a maximum, just before the next test.

Its average value, or $\mathbf{PFD_{avg}}$, is represented in Figure 1.36.

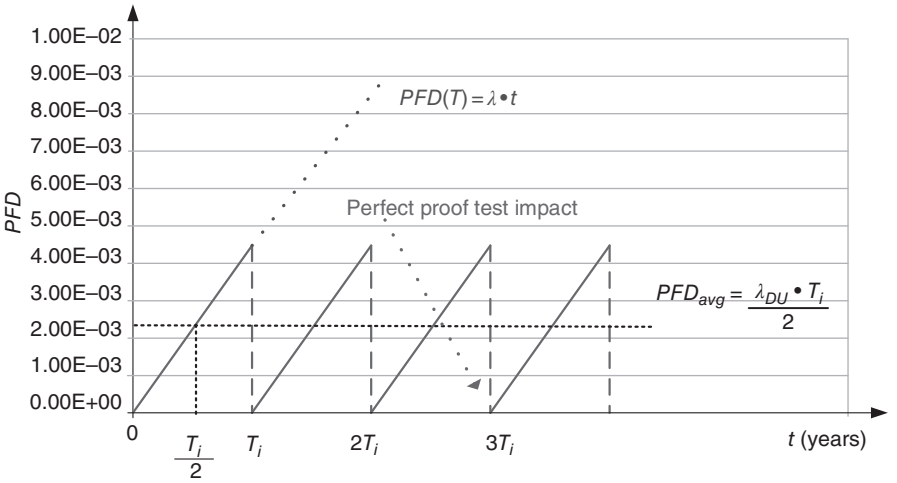


Figure 1.36 PFD(t).

1.10.2.1 Dangerous Failures

When dealing with **Safety Critical Systems**, the important failures are the dangerous ones. Those can be divided into Dangerous Detectable by the Diagnostic tests and Dangerous Undetectable.

Dangerous Undetected Failures (DU) prevent the activation, on demand, of the safety system and are also called **dormant failures**.

Dangerous Detected Failures (DD) may be found immediately when they occur, for example, by an automatic built-in self-test. A short circuit on a normally closed free voltage contact can be revealed with the so-called "trigger" function, now available in almost all Safety-related Control Systems (Chapter 3).

1.10.2.2 How to Calculate the $\mathbf{PFD_{avg}}$

In low demand mode, **Dangerous Detected failures** do not play a role in the Unreliability of a Safety System, since, often, they are detected as soon as they appear, and the process is immediately shut down. Therefore, the only significant failures that influence the value of the PFD_{avg} are the DU failures. Therefore, Equation 1.10.2 can be written as:

$$\boldsymbol{PFD_{avg} = \frac{\lambda_{DU} \cdot T_i}{2}} \qquad \text{[Equation 1.10.3]}$$

The test interval T_i is decided based upon the demand rate, so that there is a fair chance that a Dangerous Undetected fault is revealed and corrected before a demand occurs, such that a hazardous event is avoided.

1.10.3 The PFH

The starting point for the calculation of the PFH is the **Failure Frequency**. Hereafter its definitions [29]:

> ***[ISO/TR 12489] 3.1 Basic Reliability concepts***
> ***3.1.22 Failure Frequency*** *(or Unconditional Failure Intensity) w(t). Conditional probability per unit of time that the item fails between t and t + dt, provided that it was working at time 0.*

In high demand mode, the unreliability value used is the **Average Failure Frequency**. Here its definitions [29]:

> ***[ISO/TR 12489] 3.1 Basic Reliability concepts***
> ***3.1.23 Average Failure Frequency*** $\overline{w}(t_1, t_2)$,$\overline{\boldsymbol{w}}(\boldsymbol{T})$,$\overline{w}$. *Average value of the time-dependent failure frequency over a given time interval.*

$$\overline{w}(T) = \frac{1}{T} \cdot \int_0^T w(t)dt$$

The average failure frequency is also called "**Probability of Failure per Hour**" (PFH) by the standards related to functional safety of safety-related instrumented systems:

$$PFH = PFH_D = \overline{w}(T)$$

However, the correct term for PFH is **Average Failure frequency**. That is the reason why, in the new edition of IEC 62061, PFH is defined as the following [12]:

> ***[IEC 62061] 3.2 Terms and definitions***
> ***3.2.29 Average Frequency of a Dangerous Failure Per Hour PFH or*** $\boldsymbol{PFH_D}$. *Average frequency of dangerous failure of an SCS to perform a specified safety function over a given period of time.*

$$PFH(T) = \frac{1}{T} \cdot \int_0^T w(t)dt$$

Don't be confused by the fact the PFH_D is sometimes written without the subscript *D*. **IEC 62061 uses PFH while ISO 13849 uses** $\boldsymbol{PFH_D}$**, but they mean exactly the same thing.**

Moreover, ISO 13849-1 kept the old terminology: **Probability of Failure per hour**, even if it is not properly correct.

1.10.3.1 Unconditional Failure Intensity *w(t)* vs Failure Density *f(t)*

The average of the **unconditional failure intensity** $\boldsymbol{w(t)}$ is different from the **failure density** $\boldsymbol{f(t)}$**.** Let's now understand what the difference is.

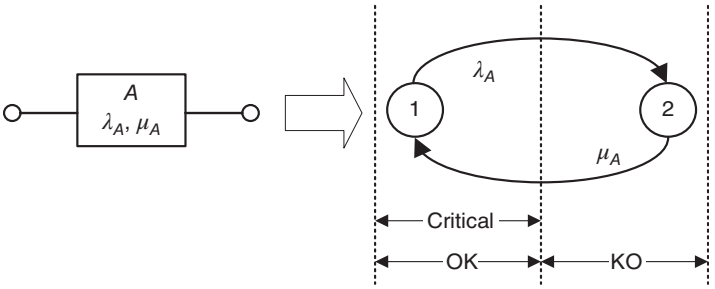


Figure 1.37 Single repairable component.

Please consider a single component that can be in two possible states: OK (1) and KO (2). Figure 1.37 represents the situation and the corresponding Markov Graph failure rate.

where:

- $\boldsymbol{\lambda_A}$: is the failure rate of the component.
- $\boldsymbol{\mu_A}$: is the component restoration rate. Please consider that the restoration rate has the same mathematical properties of the failure rate.

Since the model includes the restoration transition, the system is considered repairable; in other terms, it can be brought to an "as new status" after a repair or a Proof Test. In general, the unconditional failure intensity $w(t)$ is a saw-teeth curve while $f(t)$ is decreasing and goes to 0 when t goes to infinity.

Considering the following data (example taken from [29] annex C):

- $\boldsymbol{\lambda_A} = 5{\cdot}10^{-4}$ (h^{-1})
- $\boldsymbol{\mu_A} = 0.01$ (h^{-1})
- $\boldsymbol{\tau} =$ 2160 hours

the graphs are shown in Figure 1.38:

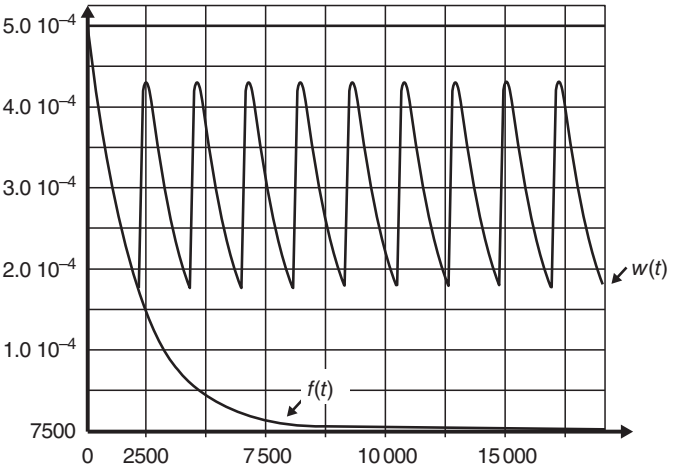


Figure 1.38 Comparison between $w(t)$ and $f(t)$.

1.10.3.2 Reliability Models Used to Estimate the PFH

In high demand mode, the two standards, ISO and IEC, use different models to come to the estimation of the unreliability function.

IEC 62061 uses the RBD method and it assumes the systems (Architectures) as **non-repairable**. **ISO 13849-1** uses Markov Chains and it assumes the systems (Categories) as **repairable**; please refer to § 6.2.5.

That seems a major difference that makes the two approaches irreconcilable. In reality that is not the case and the reason is that in high demand, normally, **the safety control system is the ultimate safety layer:** that is the assumption in both ISO 13849-1 and IEC 62061. Where a safety-related control system is working in high demand or in continuous mode, and it is the ultimate safety layer then, the overall safety-related control system failure **will lead directly to a potentially hazardous situation,** regardless if it is considered repairable or non-repairable.

In case the safety-related control system is the ultimate safety layer $w(t) = f(t)$; that means:

$$PFH(T) = \frac{1}{T} \cdot \int_0^T f(t)dt = \frac{F(T)}{T}$$

Therefore, PFH(T) is the average unavailability of $F(t)$.

Supposing a constant failure rate λ and $\lambda \cdot t \ll 1$:

$$PFH = \frac{F(T)}{T} = \frac{1-R(T)}{T} = \frac{1-e^{\left(-\int_0^T \lambda(t)dt\right)}}{T} = \frac{1-e^{-\lambda t}}{T} \approx \frac{\lambda \cdot T}{T} = \lambda = \frac{1}{MTTF}$$

1.11 Weibull Distribution

It is now clear that, in Functional Safety, **the failure rate of any component has to be constant:** the issue are components subject to wear, like contactors and solenoid valves, since their failure rates are usually not constant. Therefore, **the exponential curve is not helpful to model their life distribution: that is where the Weibull distribution comes in**.

The Weibull distribution [28] is one of the most widely used Life Distributions in Reliability analysis. The distribution is named after the Swedish professor Waloddi Weibull (1887–1979), who developed the distribution for modeling the strength of materials.

The Weibull distribution is very flexible and can, through an appropriate choice of parameters, model many types of failure rate behaviors. **It is therefore used to model the failure behavior of electromechanical components.**

1.11.1 The Probability Density Function

The Weibull **PDF** is the following:

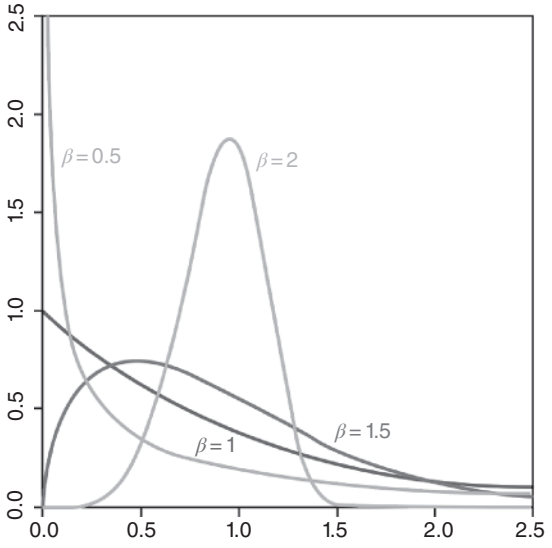
$$f(t) = \beta \cdot \frac{t^{\beta-1}}{\eta^{\beta}} \cdot e^{-\left(\frac{t}{\eta}\right)^{\beta}}$$

- η is called the **Life Characteristics**
- β is referred as the **shape** parameter

Please notice that when $\beta = 1$, the Weibull becomes the Exponential distribution,

In Figure 1.39, the Weibull distribution is plotted for $\eta = 1$ and for some values of β.

Figure 1.39 Weibull *f*(*t*).



1.11.2 The Cumulative Density Function

The Weibull **Cumulative Density Function** is the following:

$$F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}}$$

Please notice that when $t = \eta$

$$F(\eta) = 1 - e^{-\left(\frac{\eta}{\eta}\right)^{\beta}} = 1 - e^{-(1)^{\beta}} = 1 - e^{-1} = 0.63$$

Therefore, regardless of the distribution shape parameter β, when $t = \eta$, the Probability of unavailability $F(t)$ of the component = 63%.

The parameter $\boldsymbol{\eta}$ is defined as the **characteristic** lifetime of the distribution. Please refer to Figure 1.40.

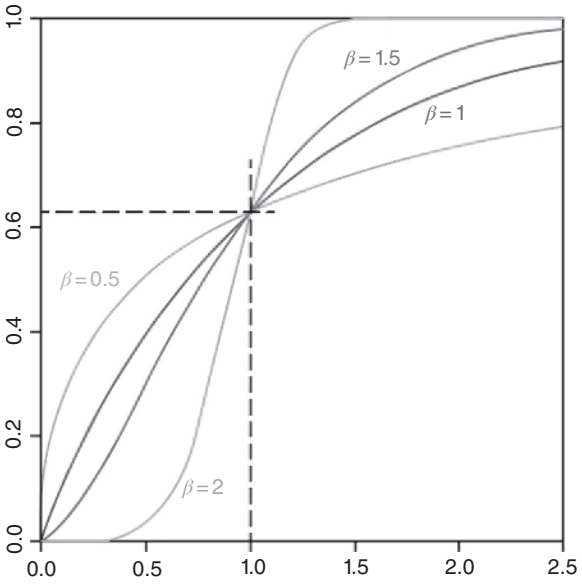


Figure 1.40 Weibull *F*(*t*).

1.11.3 The Instantaneous Failure Rate

Finally, the **Instantaneous Failure Rate** is the following:

$$\lambda(t) = \frac{f(t)}{1-F(t)} = \beta \cdot \frac{t^{\beta-1}}{\eta^{\beta}}$$

When $\beta = 1$, the failure rate is constant and equal to:

$$\lambda = \frac{1}{\eta}$$

In this case, the Weibull distribution is identical to the exponential one. Please refer to Figure 1.41.

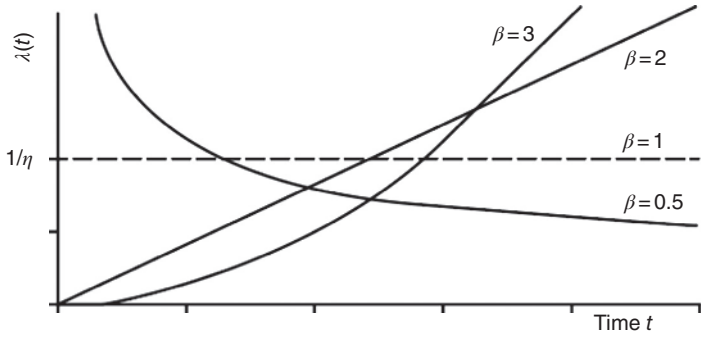


Figure 1.41 Weibull $\lambda(t)$.

When $\beta < 1$, the failure rate decreases with time. Both electronic and mechanical systems may initially have high failure rates. Manufacturers conduct production process control, production acceptance tests, "burn-in," or reliability stress screening (RSS) to prevent early failures before delivery to customers. Therefore, shape parameters of less than one indicate the following:

- lack of adequate process control;
- inadequate burn-in or stress screening;
- production problems, dis-assembly, poor quality control;
- overhaul problems;
- mixture of populations;
- run-in or wear-in.

Many electronic components during their useful life show a decreasing instantaneous failure rate, thus featuring shape parameters less than 1. Preventive maintenance on such a component is not appropriate, as old parts are better than new. Please refer to Figure 1.42.

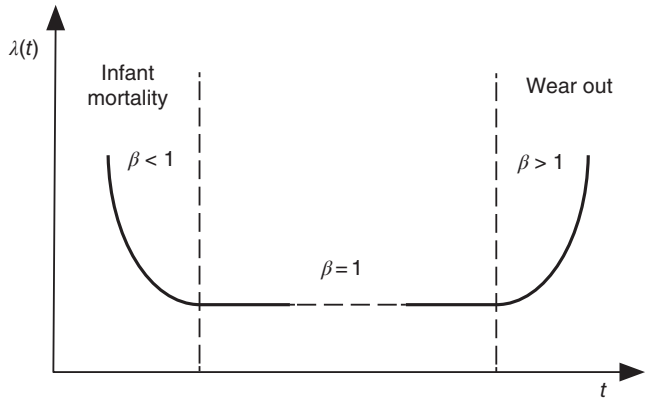


Figure 1.42 Weibull and the bathtub.

When $\beta > 1$, the failure rate increases with time. That behavior is attributed, first of all, to components in the wear-out, or end-of-life, phase. Some typical examples of these cases are:

- wear;
- corrosion;
- crack propagation;
- fatigue;
- moisture absorption;
- diffusion;
- evaporation (weight loss);
- damage accumulation.

Design measures have to ensure that those phenomena do not significantly contribute to the probability of product failure during the expected operational life; however, that is typically the behavior of Contactors and Solenoid valves during their entire life.

1.11.4 The Mean Time to Failure

The MTTF of Weibull distribution is not an easy function. It can be demonstrated that:

$$MTTF = \int_0^{+\infty} R(t)dt = \eta \cdot \Gamma\left(\frac{1}{\beta} + 1\right)$$

where Γ is the **Gamma Function,** whose parameters are shown in Table 1.4.

$\Gamma(1+x) = x \cdot \Gamma(x)$ and $\Gamma(x) \approx \frac{1}{x} + \sum_{k=0}^{7} b_k \cdot x^k$

where $0 \leq x \leq 1$.

Table 1.4 Parameters of gamma function.

Coeff	Value
b_0	−0.577 191 652
b_1	0.988 205 891
b_2	−0.897 056 937
b_3	0.918 206 857
b_4	−0.756 704 078
b_5	0.482 199 394
b_6	−0.193 527 818
b_7	0.035 868 343

1.11.4.1 Example

Let's consider a choke valve, the example is taken from [57], that is assumed to have a Weibull distribution with:

- shape parameter $\beta = 2.25$ and
- scale parameter $1/\eta = 1.15\ 10^{-4}\ \mathrm{h}^{-1}$.

The probability that the valve survives six months (4380 hours) in continuous operation is:

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}} = e^{-(1.15\cdot 10^{-4}\cdot 4380)^{2.25}} \cong 0.81$$

Which means 81% probability. The **MTTF** is

$$MTTF = \eta \cdot \Gamma\left(\frac{1}{\beta} + 1\right) = \frac{\Gamma\left(\frac{1}{2.25} + 1\right)}{1.15\cdot 10^{-4}} = \frac{\Gamma(1.44)}{1.15\cdot 10^{-4}} = \frac{0.886}{1.15\cdot 10^{-4}} \cong 7704 \text{ hours}$$

If the shape parameter $\beta \neq 1$, the MTTF is not equal to η and the MTTF of Weibull distribution is not the time when 63% of the component under test has failed. In case $\beta = 1$, the MTTF is equal to η and the MTTF of Weibull distribution is the time when 63% of the component under test has failed.

$$MTTF = \eta \cdot \Gamma\left(\frac{1}{1} + 1\right) = \eta \cdot \Gamma(2) = \eta \cdot 1! = \eta$$

The Median Life (50% failure probability) is

$$t_m = \eta \cdot (\ln 2)^{\frac{1}{\beta}} \cong 7389 \text{ hours}$$

A Valve that has survived the first six months, will again survive six months with a probability of:

$$\frac{R(t_1 + t_2)}{R(t_1)} = \frac{e^{-(1.15\cdot 10^{-4}\cdot 8760)^{2.25}}}{e^{-(1.15\cdot 10^{-4}\cdot 4380)^{2.25}}} \cong \frac{0.36}{0.81} \cong 0.44$$

which means 44% probability, which is significantly less than the probability that a new valve would survive six months, of course. That fact the failure rate is increasing plays an important role!

1.12 B_{10D} and the Importance of T_{10D}

Once a Safety-related block diagram has been defined, for each safety-related system, the technique used to calculate the probability of hardware failure is based upon specific Markovian formulae obtained from Taylor's series and slightly conservative underlying hypotheses, among which **a constant failure rate**.

The starting point of the analysis is a probabilistic model of the Safety-related control system. That consists in:

- Identifying all the states of the system.
- Analyzing the transitions of the system from state to state, according to events that may arise during its life, like failures, repairs, and tests.

One of the advantages of the Markov models is that they can be modeled with equations.

1.12.1 The $B_{X\%}$ Life Parameter and the B_{10D}

For components having mechanical wear, a straight MTTF cannot be defined. That is the reason why the concept of **$B_{X\%}$ Life** was introduced.

The $B_{X\%}$ life metric originated in the ball and roller bearing industry but has become a product lifetime metric used across a variety of industries. The $B_{X\%}$ life is the lifetime metric that takes to fail X% of the units in a population. For example, if an item has a B_{10} life of 1000 km, this means that 10% of the population will have failed by the time it reached 1000 km in operation. Other percentages can be defined; however, in high demand mode applications, B_{10} is the one used.

B_{10D} is the mean number of cycles until 10% of the components failed dangerously and is used for components having mechanical wear.

If only the B_{10} of a component were available, B_{10D} can be estimated as twice the B_{10} (50% dangerous failure).

Sometimes, the component manufacturer provides the B_{10} value and the **Ratio of dangerous failures** (RDF). The relation among those parameters is the following.

$$B_{10D} = \frac{B_{10}}{RDF}$$

Linked to B_{10} is the **number of operations** a component does **in a year**: n_{op}

The lower the RDF, the higher is the B_{10D}, and therefore the longer is the T_{10D}. However, both ISO 13849-1 and IEC 62061 limit such a value; in particular, if the ratio of dangerous failure is estimated to be less than 0.5 (50% dangerous failure), the T_{10D} of the component **is limited to $2 \times T_{10}$**.

T_{10D} is linked to the number of operations n_{op} by the following formula:

$$T_{10D} = \frac{T_{10}}{RDF} = \frac{B_{10}}{RDF \cdot n_{op}} = \frac{B_{10D}}{n_{op}}$$

The ratio of dangerous failure is estimated as 50% of dangerous failures if no information is available.

1.12.1.1 Example

Let's assume a component has a $B_{10} = 10^6$, an RDF = 30%, and is used six times per hour ($n_{op} = 6 \cdot 8 \cdot 240 = 11\,520$).

$$T_{10} = \frac{B_{10}}{n_{op}} = 87 \text{ years}$$

$$B_{10D} = \frac{B_{10}}{RDF} = 3.3 \cdot 10^6$$

Therefore T_{10D}:

$$T_{10D} = \frac{B_{10D}}{n_{op}} = 286 \text{ years}$$

However, given the standard limitation, T_{10D} is limited to $87 \cdot 2 = 174$ years.

1.12.2 How λ_D and $MTTF_D$ are Derived from B_{10D}

In Functional Safety and, in particular, in high demand Mode of Safety-related Control Systems, **B_{10D} is used to indicate the Reliability of components that do not have a constant failure rate.**

As it will be described later in the chapter, since an "approximated" constant failure rate will be associated to those components, in order to limit the error on the calculation of the PFH_D of the safety Function, **the usage of the component will be limited to when it reaches the B_{10D} number of operation**. That means the component must be replaced when B_{10D} is reached, or earlier, if its Mission Time is shorter.

Since the cycle duration corresponds to the reciprocal of the operating frequency $\boldsymbol{n_{op}}$, the point in time $\boldsymbol{T_{10D}}$, at which the element has completed B_{10D} cycles is:

$$T_{10D} = \frac{B_{10D}}{n_{op}}$$

Given a component with the unreliability function $F(t)$,

$$F(t) = 1 - e^{-\lambda \cdot t}$$

the probability of dangerous failures that a component has, when T_{10D} is reached is

$$F(t = T_{10D}) = 1 - e^{-\lambda_D \cdot T_{10D}}$$

But we know that the probability $F(t = T_{10D}) = 10\%$, therefore:

$$\frac{1}{10} = 1 - e^{-\lambda_D \cdot T_{10D}}$$

$$\lambda_D = \frac{1}{T_{10D}} \cdot ln\,\frac{10}{9} \cong \frac{1}{10 \cdot T_{10D}} = \frac{n_{op}}{10 \cdot B_{10D}}$$

In case of a constant failure rate,

$$\lambda = \frac{1}{MTTF}$$

Therefore, the following is the formula to be used to calculate the $MTTF_D$ from B_{10D}:

$$MTTF_D = \frac{B_{10D}}{0.1 \cdot n_{op}} \qquad \text{[Equation 1.12.2]}$$

1.12.3 The Importance of the Parameter T_{10D}

If a component has a B_{10D}, that means its failure rate is not constant over time. The B_{10D} was chosen not by chance! It can be demonstrated that by limiting the product life to T_{10D}, there is no significant error in the estimation of the PFH_D by assuming a constant failure rate, compared to the use of a Weibull distribution.

Let's calculate the error, comparing three Weibull distributions: with $\beta = 1$ (constant failure rate), $\beta = 2$, and with $\beta = 3$. Please refer to Table 1.5.

Table 1.5 Parameters comparison for three Weibull distributions.

	$\beta = 1$	$\beta = 3$	$\beta = 4$
$F(t)$	$1 - e^{-\frac{t}{\eta}}$	$1 - e^{-\left(\frac{t}{\eta}\right)^3}$	$1 - e^{-\left(\frac{t}{\eta}\right)^4}$
$F(T_{10D}) = 0.1$	$\eta = \frac{T_{10D}}{0.1}$ (Note 1)	$\eta = \frac{T_{10D}}{\sqrt[3]{0.1}}$ (Note 2)	$\eta = \frac{T_{10D}}{\sqrt[4]{0.1}}$ (Note 3)
$\lambda_D(t)$	$\frac{0.1 \cdot n_{op}}{B_{10D}} = constant$	$\beta \cdot \frac{t^{\beta-1}}{\eta^\beta}$	$\beta \cdot \frac{t^{\beta-1}}{\eta^\beta}$
$\boldsymbol{\lambda_D(t)}$	$\boldsymbol{\frac{0.1 \cdot n_{op}}{B_{10D}} = \frac{1}{\eta}}$	$\boldsymbol{3 \cdot \frac{t^2}{\eta^3}}$	$\boldsymbol{4 \cdot \frac{t^3}{\eta^4}}$
$\lambda_D(t)$ with η as per Note 1, 2 or 3	$\frac{0.1}{T_{10D}}$	$3 \cdot \frac{t^2}{\left(\frac{T_{10D}}{\sqrt[3]{0.1}}\right)^3}$	$4 \cdot \frac{t^3}{\left(\frac{T_{10D}}{\sqrt[4]{0.1}}\right)^4}$
$T_{10D} \cdot \lambda_D(t)$	0.1	$3 \cdot \frac{t^2}{\left(\frac{T_{10D}}{\sqrt[3]{0.1}}\right)^3} \cdot T_{10D}$	$4 \cdot \frac{t^3}{\left(\frac{T_{10D}}{\sqrt[4]{0.1}}\right)^4} \cdot T_{10D}$
$\boldsymbol{T_{10D} \cdot \lambda_D(t)}$	**0.1**	$\boldsymbol{0.3 \cdot \left(\frac{t}{T_{10D}}\right)^2}$	$\boldsymbol{0.4 \cdot \left(\frac{t}{T_{10D}}\right)^3}$

Hereafter, in the three Notes, the detailed calculations of "η":

Note 1: $\beta = 1$ → $F(t = T_{10D}) = 0.1 \Rightarrow 1 - exp\left[-\left(\frac{t}{\eta}\right)^1\right] = 0.1 \Rightarrow exp\left[-\left(\frac{t}{\eta}\right)^1\right] = 0.9 \Rightarrow \left[-\left(\frac{t}{\eta}\right)^1\right] = -0.1 \Rightarrow$

$t = \boldsymbol{0.1\,\eta = T_{10D}}$

Note 2: $\beta = 3$ → $F(t = T_{10D}) = 0.1 \Rightarrow 1 - exp\left[-\left(\frac{t}{\eta}\right)^3\right] = 0.1 \Rightarrow exp\left[-\left(\frac{t}{\eta}\right)^3\right] = 0.9 \Rightarrow \left[-\left(\frac{t}{\eta}\right)^3\right] = -0.1 \Rightarrow$

$t = \boldsymbol{\sqrt[3]{0.1}\,\eta = T_{10D}}$

Note 3: β = 4 → $F(t = T_{10D}) = 0{,}1 \Rightarrow 1 - exp\left[-\left(\frac{t}{\eta}\right)^4\right] = 0{,}1 \Rightarrow exp\left[-\left(\frac{t}{\eta}\right)^4\right] = 0{,}9 \Rightarrow \left[-\left(\frac{t}{\eta}\right)^4\right] = -0{,}1 \Rightarrow$

$t = \boldsymbol{\sqrt[4]{0{,}1}\,\eta = T_{10D}}$

Figures 1.43 and 1.44 show the three dangerous failure rates, standardized at T_{10D}.

$$\lambda_D(t) = \frac{0.1 \cdot n_{op}}{B_{10D}} = constant$$

$$\lambda_D(t) = 3 \cdot \frac{t^2}{\eta^3}$$

$$\lambda_D(t) = 4 \cdot \frac{t^3}{\eta^4}$$

At the beginning, the "surrogate" failure rate (the one with $\beta = 1$) is greater but then the "real" failure rate (the one with $\beta = 3$ or with $\beta = 4$) becomes greater. At the point $t = T_{10D}$ the area under both curves is equal and its value is **0.1**: it means that the two failure rates in the interval from $t = 0$ to $t = T_{10D}$ provide the same estimation.

That also shows that for $t > T_{10D,}$ the estimation no longer works. If the component is used longer than T_{10D}, then the surrogate $MTTF_D$ does not reflect the real behavior, and the failure rate would be under-estimate in a dangerous way.

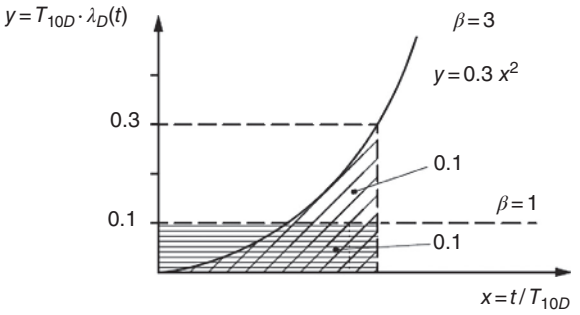


Figure 1.43 Different failure rate functions for β = 3.

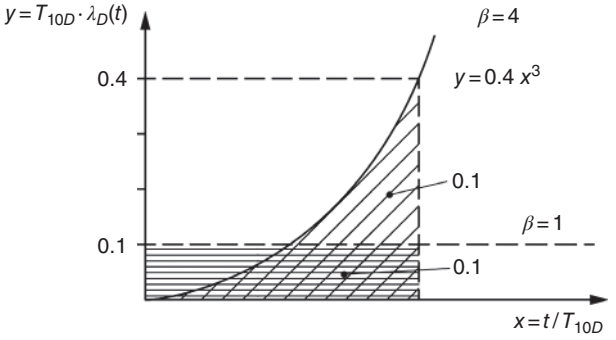


Figure 1.44 Different failure rate functions for β = 4.

That is the meaning of the following note in IEC 62061:

> ***[IEC 62061] 7.3.4 Failure rate of subsystem element***
> ***7.3.4.2 Relationship of relevant parameters*** *[...]*
>
> ***Note 4:*** *For electronic systems, the exponential distribution is applicable. For non-electronic systems, the exponential distribution is not applicable. The Weibull distribution (see also IEC 61649) is more appropriate, but parameters and calculations are difficult to apply. However, when using exponential distribution for non-electronic components within the limits of T_{10D}, then the results of the calculations are pessimistic and the formula with $1 - e^{-\lambda t}$ could be applied as a simplified method.*

1.12.4 The Surrogate Failure Rate

Since Markov only works with a constant failure rate, a **Surrogate failure rate** (also called **Substitute failure rate**) is defined for components subject to wear that do not show such characteristics.

Actually, the first step is to use the Weibull distribution to estimate the best fit value of B_{10}. Examples of those methods are given in standards like ISO 19973-1 [21] and ISO 19973-2 [50], valid for pneumatic components.

The useful life of a component is represented in Figure 1.45 whereby, even if the component has a failure rate that increases with the time, since its lifetime is limited to T_{10D}, its failure rate can be assumed as constant during this period.

Please refer to IEC 60947-1 annex K [78] for further insights.

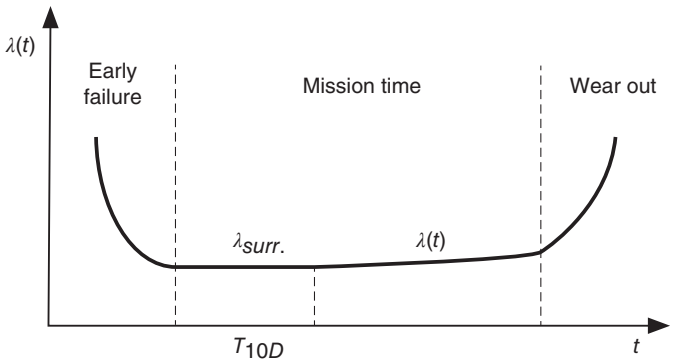


Figure 1.45 Surrogate failure rate.

1.12.5 Markov

The Markov approach is one of the recommended approaches in IEC 61508-6 for Reliability assessment of a Safety Instrumented System, and it is used to analyze **how the state of a system changes with time**.

It is applicable to **Stationary systems** only. That means their behavior must be the same at any moment under consideration, and consequently, the probability of a transition between two states must remain the same during the specific time interval: λ **= constant**.

Finally, the systems must be **without memory**: the future random behavior of a system depends only on its actual state and not on preceding states or the way in which the actual state has occurred.

With those assumptions, the transition probability due to random failures is given by

$$P_f = \lambda \cdot \Delta t$$

where λ is the failure rate, and Δt is the time interval the transition probability is related to. The Markov model for this simple failure process is shown in Figure 1.46:

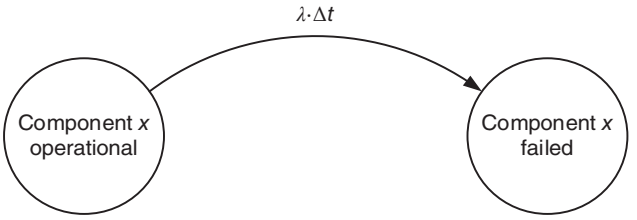


Figure 1.46 Failure of a component with constant failure rate.

In practice, the time is omitted from the graph. Markov processes used in Functional Safety have a finite number of states, for example:

- **State 0:** Functioning State
- **State 1:** Fault state
- λ is the failure rate of the component
- μ is the repair rate of the component

Please refer to Figure 1.47.

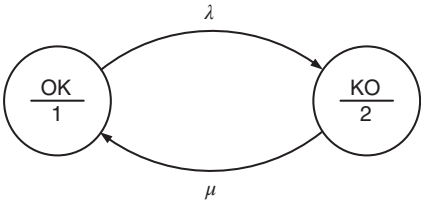


Figure 1.47 A two states transition model.

This Markov model is described by the following differential equation system:

$$\dot{P_1}(t) = -\lambda \cdot P_1(t) + \mu \cdot P_2(t)$$
$$\dot{P_2}(t) = \lambda \cdot P_1(t) - \mu \cdot P_2(t)$$

with the initial conditions:

- Probability that the system is in state 1 at time 0: $P_1(0) = 1$
- Probability that the system is in state 2 at time 0: $P_2(0) = 0$

The solution is as follows:

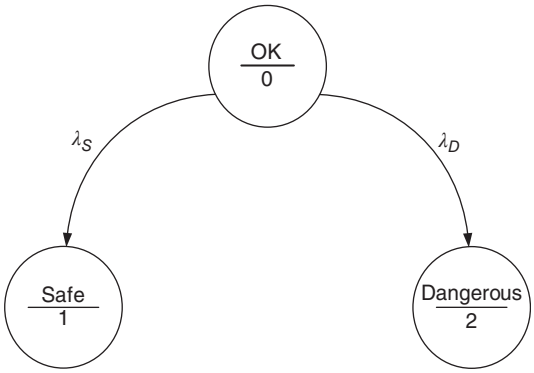
$$P_1(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} \cdot e^{-(\lambda + \mu)t}$$
$$P_2(t) = \frac{\lambda}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} \cdot e^{-(\lambda + \mu)t}$$

That was a simple example. A transition model may have three states like in Figure 1.48:

- **State 0:** the channel is functioning correctly
- **State 1:** the channel has a safe fault
- **State 2:** the channel has a dangerous fault

Supposing the components are non-repairable, the transition model is described in Figure 1.48.

Figure 1.48 Three state transition diagram.



1.13 Logical and Physical Representation of a Safety Function

The Blocks used to represent a Safety Function are a **logical view** of the subsystem architectures.

Blocks can be in a **Series configuration** (i.e. any failure of a block causes the failure of the relevant safety function) or in a **Parallel configuration** (i.e. coincident block failures are necessary for the relevant safety function to fail). However, they do not necessarily represent a specific physical connection scheme.

A Hardware Fault Tolerance of 1 is represented by parallel subsystem elements or blocks, but the corresponding physical connections will depend upon the application of the subsystem.

1.13.1 De-energization of Solenoid Valves

As a first example, we consider an output subsystem whose **mission is to remove power** from a pneumatic cylinder.

Let's suppose the removal of air from the pneumatic cylinder is the safe state condition. In order to implement a redundant pneumatic subsystem ($HFT = 1$), two pneumatic valves (A and B) must be connected in series (Figure 1.49).

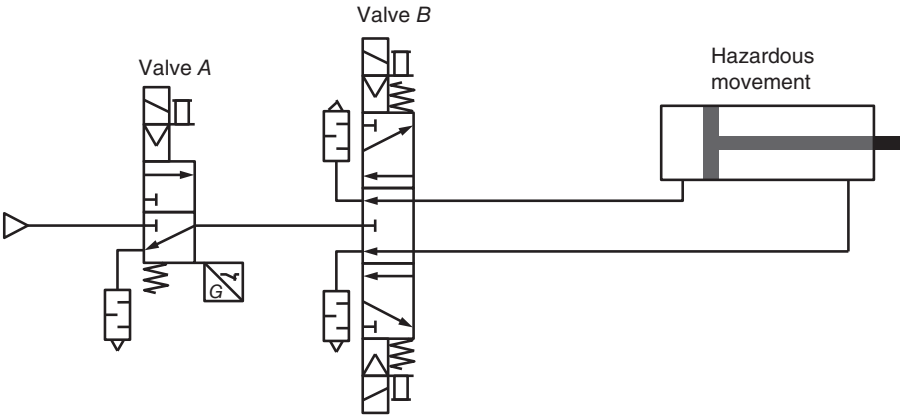


Figure 1.49 Physical representation of a safety output subsystem.

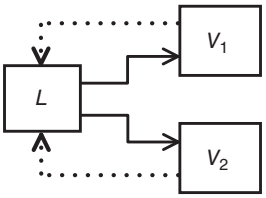


Figure 1.50 Logical representation of a safety 1oo2D output subsystem.

While the physical architecture has two valves in series, the logical one shows the two elements in parallel (Figure 1.50) since we are dealing with a so-called **redundant system** (*HFT* = 1 or 1oo2D).

1.13.2 Energization of Solenoid Valves

Let's consider a continuous casting line. The ladle is positioned above the tundish. At the bottom of the ladle, there is a drawer. When the drawer is opened, the steel flows into the tundish, and the continuous casting can produce steel.

A safe state of the system is when the ladle drawer is closed. The drawer movement is guaranteed thanks to a hydraulic cylinder that is attached to the cylinder stem.

The cylinder is moved thanks to a Solenoid valve that is normally de-energized. Its energization closes the drawer and places the continuous casting machine into a safe state.

In order to implement a redundant subsystem (*HFT* = 1 or 1oo2D), two hydraulic valves in parallel must be installed. The valves must be energized in order to close the drawer. The way they are installed, if one fails, the second one can guarantee the cylinder stem movement and, therefore, the drawer closure.

While the logical system is the same as in Figure 1.50, the physical one is shown in Figure 1.51 two valves in parallel (*A* and *B*) are installed, so that, in case one fails, the other guarantees oil to the cylinder and therefore the drawer closure. Please consider that the circuit was simplified compared with the real one implemented in a continuous casting plant.

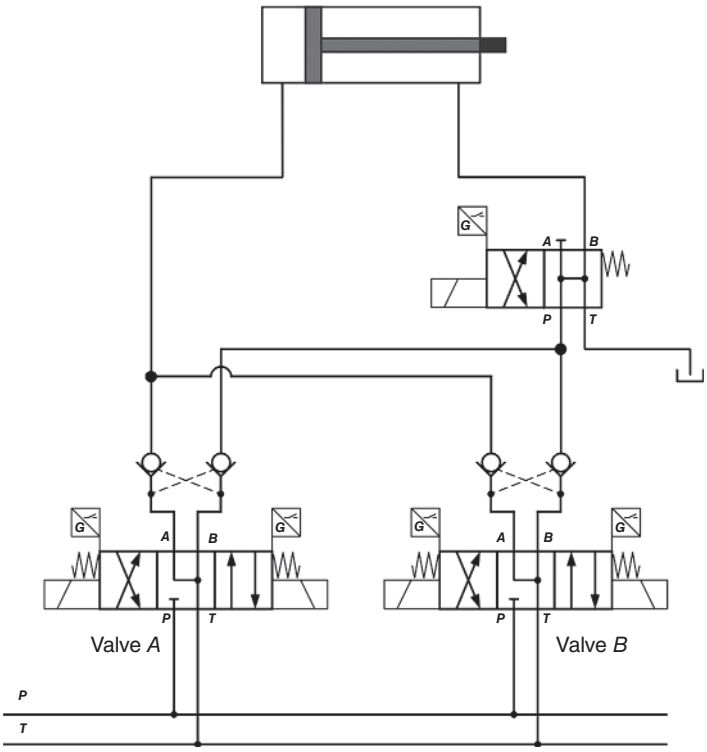


Figure 1.51 Physical representation of a safety output subsystem (with the cylinder as shown in the figure, the drawer is open).