Dependable Systems





Theoretical background

Failures and repairs as Stochastic Processes

A *Stochastic Process* is a set of random variables

$$X_1, X_2, \ldots X_n$$

that operates over the same set.

Since the variables might be correlated, the process must be described with the probability of obtaining a given outcome for a variable *i*, conditioned on the values of the previous outcomes:

$$P(X_i = a_i \mid X_1 = a_1, \ldots X_{i-1} = a_{i-1})$$

Things however can be simplified a lot by considering smaller levels of correlations among the random variables.

Failures and repairs as Stochastic Processes

The index *i* of the random variables, can be either discrete or continuous.

$$X_1, X_2, \ldots X_n \quad or \quad X_t$$

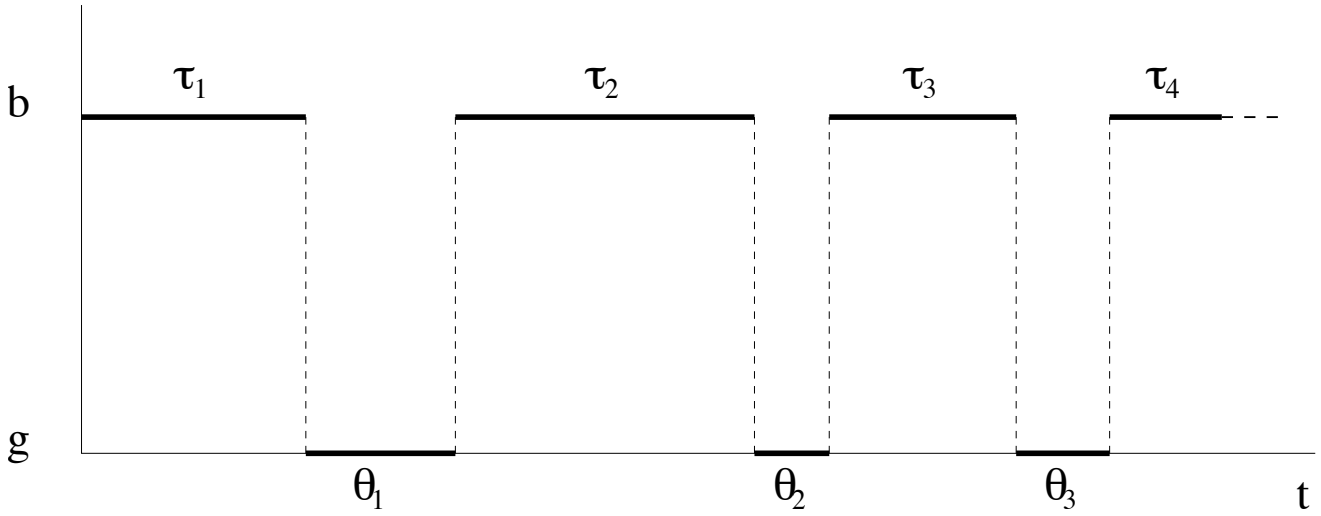
If the index is continuous, it usually corresponds to the time.

The set of outcomes of the random variables can also be discrete or continuous.

In dependability studies, the index is usually continuous (time) and the set of outcomes is discrete (in many cases, composed by only two states – working or failed).

Failures and repairs as Stochastic Processes

As it has been presented, the lifetime of a component is characterized by *Up* times and *Down* times.



The *Up* or *Down* states of a component at a given time instant can be considered as a random variable.

The correlation among these random variables can be described as a *Stochastic Process*.

Introduction

If the *Up* and *Down* times of the components are **not correlated**, they can usually be studied by simply focusing on the distributions.

- ***Studying the system is simpler***
- ***Results can be computed with combinatorial analysis***
- ***The model might be not realistic***

These cases have been considered, for what concerns reliability, in the dependability part of the *Computing Infrastructure* course.

Introduction

If the *Up* and *Down* times of the components are **correlated**, analysis must be performed using stochastic processes.

- ***Studying the system is much harder***
- ***In many cases, simple stochastic models like Marvok Chains can be used***
- ***Models are however more realistic, and results more accurate***

Reliability and failure time distribution

The reliability of a component is defined as R(t):

$$R(t) = Prob\{\text{“The component is not failed at } t\text{”}\}$$

Then, if we define

$$F(t) = 1 - R(t) = Prob\{\text{“The component has failed between 0 and } t\text{”}\}$$

we can see that *F(t)* is a proper random variable, that defines the *failure time distribution*.

Reliability and failure time distribution

In particular we can define the proability density of the failure time *f(t)* as:

$$f(t) = \frac{d\,F(t)}{d\,t} = -\frac{d\,R(t)}{d\,t}$$

From *f(t)*, the MTTF can be computed as the first moment (the average) of the corresponding distribution:

$$m_1 = E[\tau] = MTTF = \int_0^\infty t \cdot f(t)\,d\,t = \int_0^\infty R(t)\,d\,t$$

$$\int_0^\infty t\cdot\left(-\frac{dR(t)}{dt}\right)dt = \left[t\cdot\left(-R(t)\right)\right]_0^\infty - \int_0^\infty 1\cdot\left(-R(t)\right)dt = \left[0-0\right] + \int_0^\infty R(t)\,dt$$

Hazard rate

Starting form the distribution of the failure time of a component, an important characterizing function, called the *hazard rate* (or *failure rate*) can be computed:

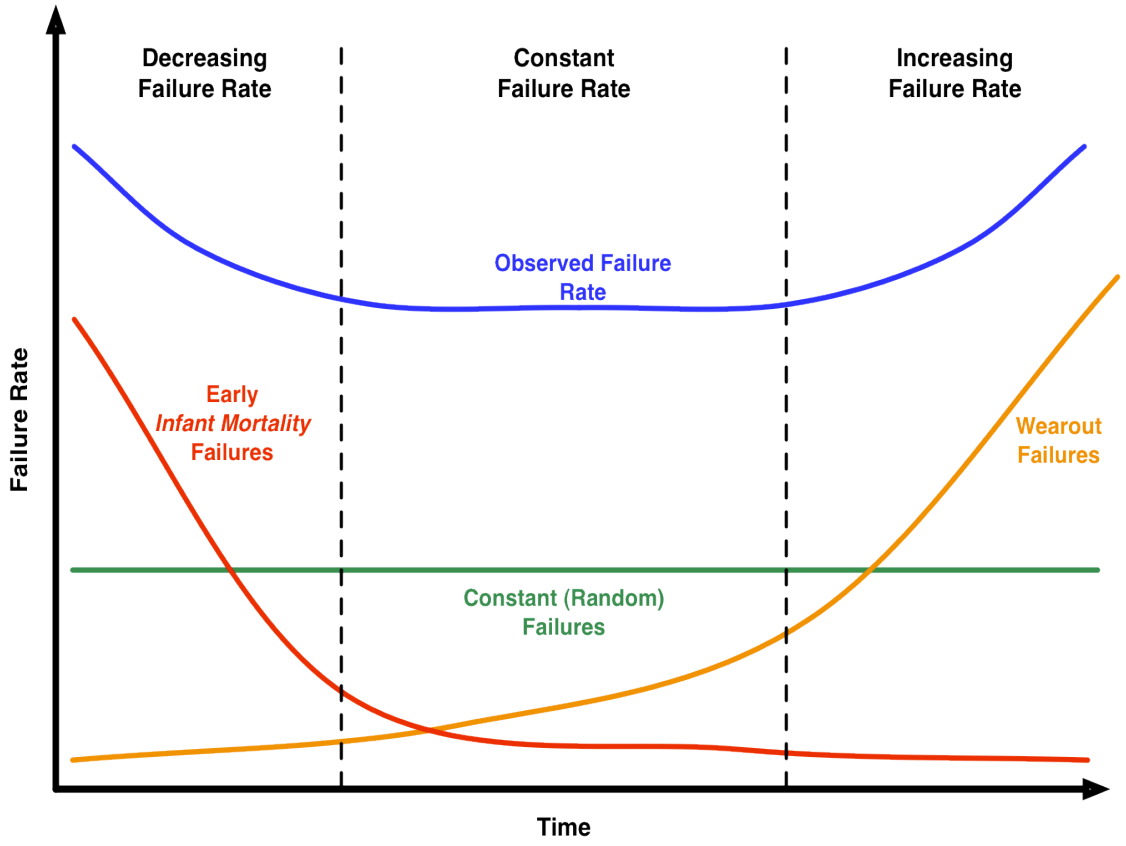
$$h(t) = Prob\{\, t < \tau \leq t + dt \,|\, \tau > t \,\} = \frac{Prob\{\, t < \tau \leq t + dt \,,\, \tau > t \,\}}{Prob\{\, \tau > t \,\}}$$

It represents the probability that the system will fail between time *t* and *t+dt*, given that it has survived until *t*.

In other words, given a time instant *t*, *h(t)* represents the "speed" at which the system can fail in that given time instant.

Hazard rate

The “bathtub” function that was introduced in the previous lessons, is a representation of the *hazard (failure) rate* of the failure distribution of the considered component.



Hazard rate

The failure rate *h(t)* can be obtained directly form the reliability function *R(t)* :

$$h(t) = \frac{f(t)}{R(t)} = -\frac{1}{R(t)}\frac{d\,R(t)}{dt}$$

Conversely, the reliability function *R(t)* can be derived from the failure rate *h(t)* using the following definition:

$$R(t) = e^{-\int_0^t h(x)dx}$$

Hazard rate

The integral inside the exponential represents the *accumulated age* of the component.

$$R(t) = e^{-\int_0^t h(x)dx}$$

We can call *H(t)* the accumulated age up to time t.

$$R(t) = e^{-H(t)} \qquad H(t) = \int_0^t h(x)dx$$

The Exponential distribution

A classical distribution used to characterize the life-time of components is the *Exponential distribution*.

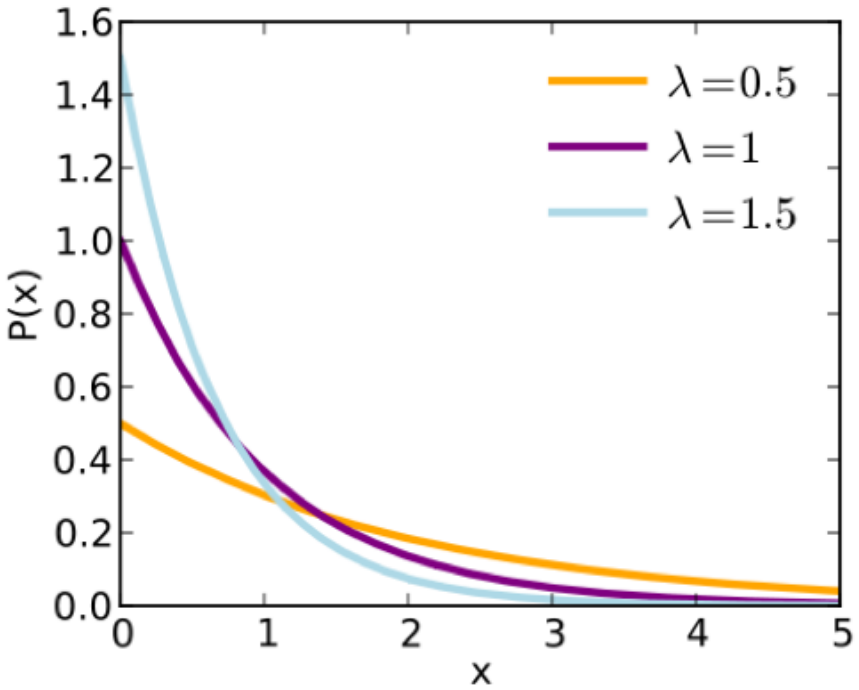
Its mathematical properties are:

$$
\begin{aligned}
F(t) &= 1 - e^{-\lambda t} \\
R(t) &= e^{-\lambda t} \\
f(t) &= \lambda\, e^{-\lambda t} \\
h(t) &= \lambda
\end{aligned}
$$

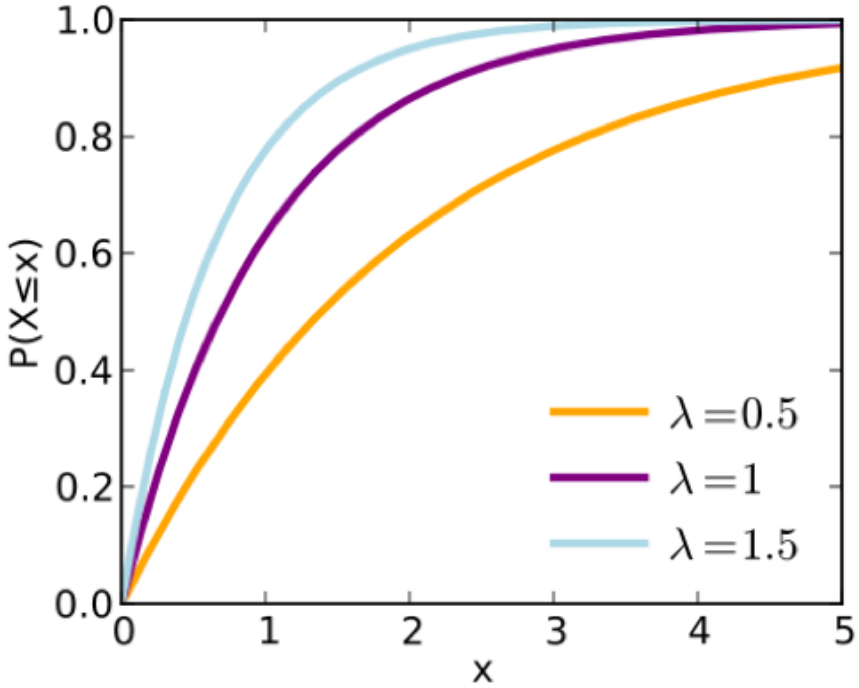
The interest in the exponential distribution in dependability cames from the fact that it has a constant hazard rate: it models a bathtub curve with no burn-in or wear-out phases.

The Exponential distribution

The shape of the exponential distribution is proportional to its parameter:



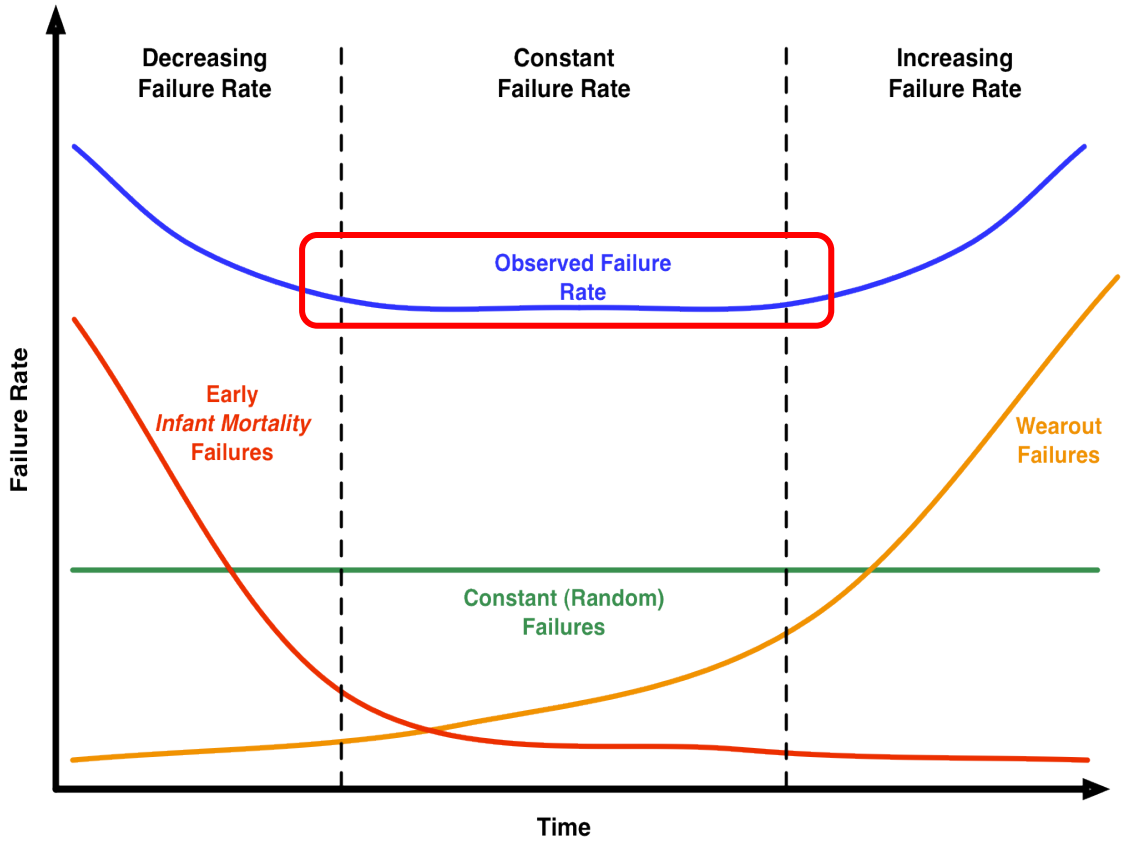
f(t)



F(t)

The Exponential distribution

Since the hazard rate of the exponential distribution is constant, it perfectly captures the constant failure rate part of a classical hazard rate of a component.



The Exponential distribution

The MTTF of a component that follows an exponential distribution of paramter λ, can be simply computed as λ^{-1}.

$$E[\tau] = MTTF = \int_0^\infty t \cdot f(t)\, dt = \lambda \int_0^\infty t \cdot e^{-\lambda t}\, dt$$

$$E[\tau] = \lambda \left[-\frac{t \cdot e^{-\lambda t}}{\lambda} \right]_0^\infty + \lambda \int_0^\infty \frac{e^{-\lambda t}}{\lambda} \cdot dt = \frac{1}{\lambda}$$

The Exponential distribution

The feature of the exponential distribution that greately simplifies its use in dependability studies, is that it exhibits the "memoryless property":

$$R(t+a\,|\,a) = \frac{R(t+a,\,a)}{R(a)} = \frac{e^{-\lambda(t+a)}}{e^{-\lambda a}} = e^{-\lambda t}$$

$$R(t+a\,|\,a) = R(t)$$

In other words, the time to failure does not depend on the life that the component has already been through.

The Weibull distribution

Another distribution that is often used in dependability study is the *Weibull distribution*.

Its mathematical properties are:

$$F(t) = 1 - exp\left[-(t/\eta)^{\beta}\right]$$

$$R(t) = exp\left[-(t/\eta)^{\beta}\right]$$

$$f(t) = \frac{\beta}{\eta^{\beta}} \cdot t^{\beta-1} \cdot exp\left[-(t/\eta)^{\beta}\right]$$

$$h(t) = \frac{\beta}{\eta^{\beta}} \cdot t^{\beta-1}$$

The interest in the Weibull distribution comes from the fact that it can model an increasing or decreasing failure rate by changing one of its parameters.

The Weibull distribution

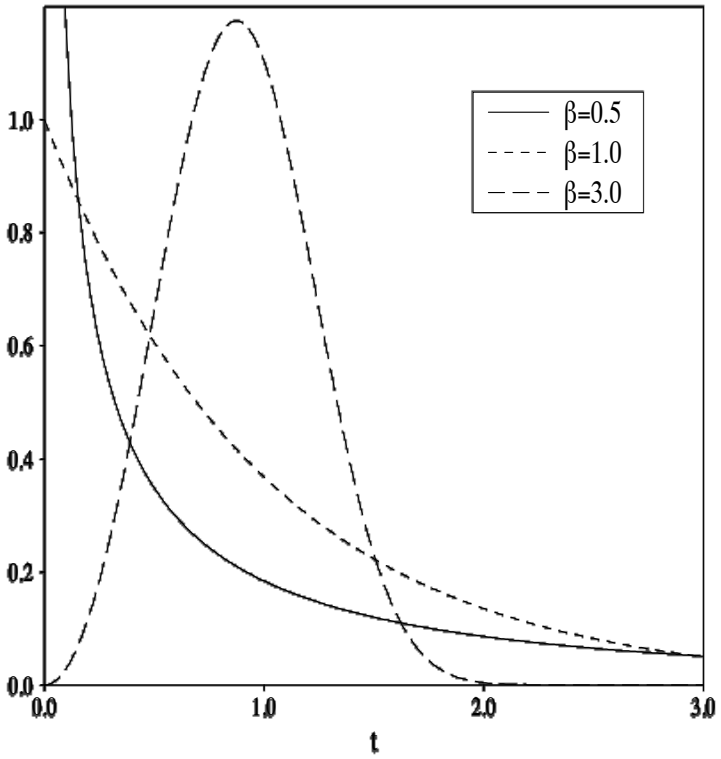
The two parameters of the Weibull distribution are:

$$f(t) = \frac{\beta}{\eta^{\beta}} \cdot t^{\beta-1} \cdot exp\left[-(t/\eta)^{\beta}\right]$$

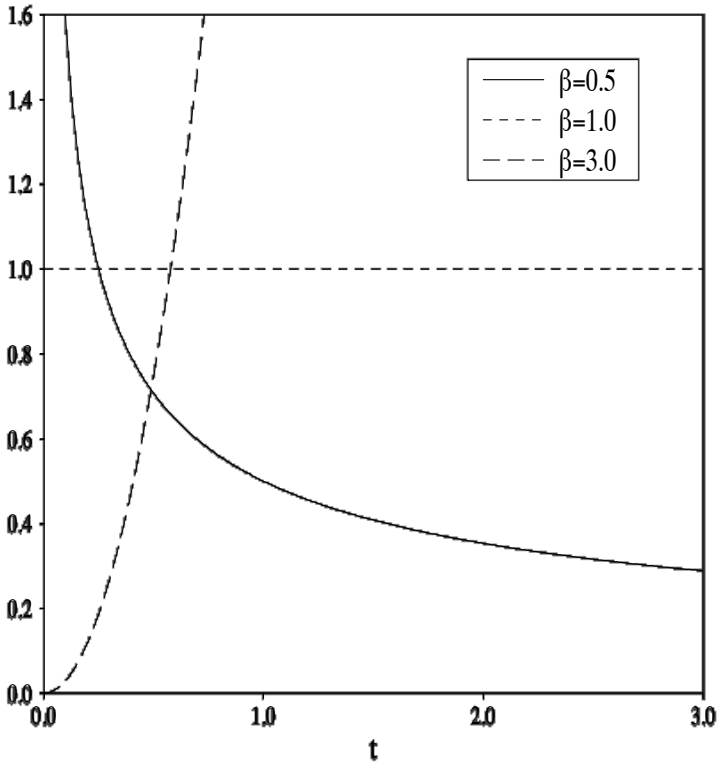
- η is the *scale parameter*, since it determines the height (the speed) of the distribution
- β is *the shape parameter*, that defines the particular shape of the distribution (and of its failure rate)

The Weibull distribution

The shape of the Weibull distribution for different shape parameters is the following:



f(t)



h(t)

The Weibull distribution

The Mean of the Weibull distribution can be expressed using the Gamma function:

$$f(t) = \frac{\beta}{\eta^{\beta}} \cdot t^{\beta-1} \cdot exp\left[-(t/\eta)^{\beta}\right]$$

$$E[\tau] = MTTF = \eta\Gamma\left(1+\frac{1}{\beta}\right)$$

Note that for $\beta=1$, by defining $\lambda=1/\eta$, since $\Gamma(n) = (n-1)!$ for integer numbers, we obtain $E[x]=1/\lambda$ that is the mean of the exponential distribution.

The Weibull distribution

In particular we have that:

- If $\beta < 1$, the failure rate is decreasing (DFR – Decreasing Faiulre Rate)
- If $\beta = 1$, the failure rate is constant (CFR – Constant Faiulre Rate), and the distribution is exponential
- If $\beta > 1$, the failure rate is increasing (IFR – Increasing Faiulre Rate)

For example, studies show that the failure rate of a CPU core, is Weibull distributed, with $\beta > 1$ and η function of the temperature of the core.

MTTR and Availability

As it can be seen, if the system can be repaired, a reasoning similar to the one done for MTTF can be done for MTTR.

In this case, we have defined *M(t)* as the maintainability (also denoted with *G(t)*):

$$G(t) = Pr\{\theta \leq t\}$$

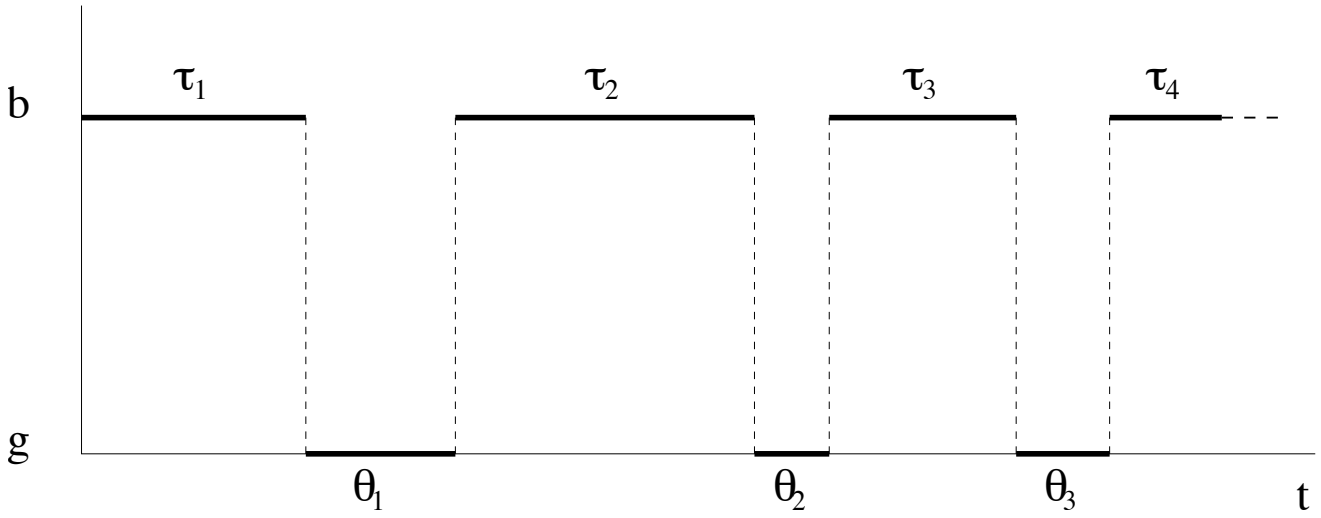
And we have:

$$\begin{aligned} g(t) &= \frac{d\,G(t)}{dt} \\ h_g(t) &= \frac{g(t)}{1 - G(t)} \\ MTTR &= \int_0^\infty t\,g(t)\,dt \end{aligned}$$

MTTR and Availability

Then, if the system continuously alternates between up and down states, we can define the availability *A(t)* as:

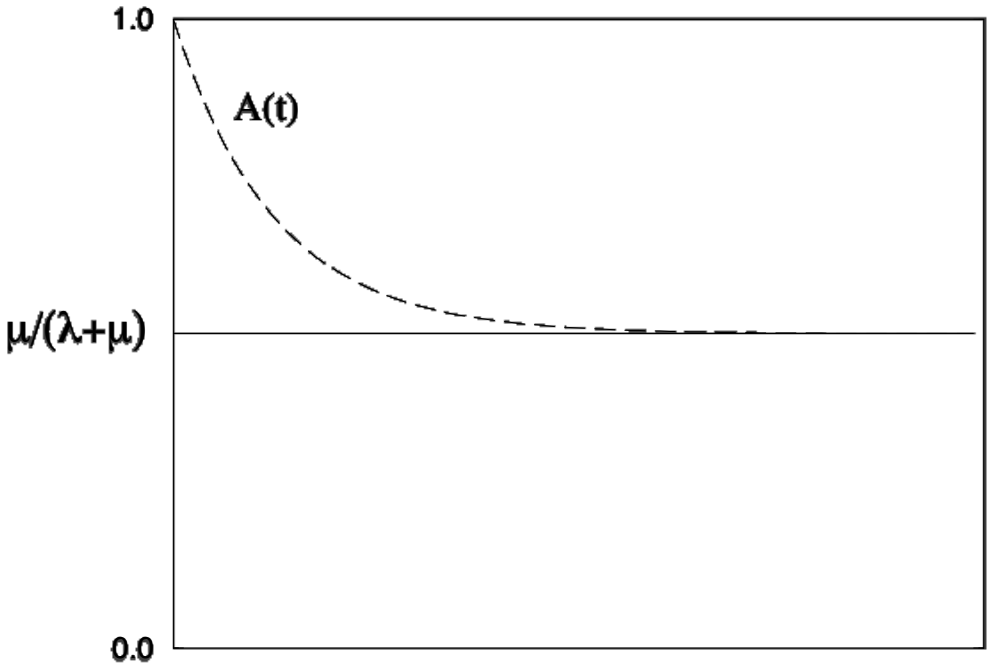
$$A(t) = \text{Prob}\{\text{“The system is working at time t”}\}$$



MTTR and Availability

In particular, under some broad assumptions, it can be shown that *A(t)* tends to a constant value as *t* tends to infinity.

Obviously, if we imagine that the system is initially working we have *A(0) = 1*



MTTR and Availability

We have that:

$$A_\infty = \lim_{t \to \infty} A(t) = \frac{MTTF}{MTTF + MTTR}$$

If both the failure and repair times are exponentially distributed, respectively with parameter λ and μ, we have that:

$$A_\infty = \frac{\mu}{\lambda + \mu} = \frac{1/\lambda}{1/\lambda + 1/\mu} = \frac{MTTF}{MTTF + MTTR}$$

MTTR and Availability

Computing the time dependent availability *A(t)*, from a system for which we know the reliability *R(t)* and the maintainability *M(t)* is not an easy task.

It requires the use of Stochastic Processes: we will se an example when R(t) and M(t) are exponentially distributed after having presented the Markov Chains.

Computing however A_{oo} is much simpler, since it requires just the MTTR and MTTF.

Moreover, in many applications A_{oo} is more meaningful to assess the availability of the system than *A(t)*.