Chapter 3 Reliability & Safety Analysis of Elementary Systems

3.1 Probability Concepts for Failure Analysis

What is a "failure"?

A *failure* can be defined as any deviation between the actual characteristics of a system or component and its expected (or design) characteristics. A failure thus represents a non-conformity with given objectives or specification clauses for the concerned entity.

The failure of a component is generally function not only of its design and quality of construction, but also of the environment in which it is placed. One of the reasons why failure data are sometimes not representative of the actual failure probability is that the operating conditions and environment of the device may not always be the same. It is important to be aware that system reliability is defined as the "*probability of performing a specified function or mission under given conditions for a prescribed time*" [McCormick, 1981].

Failures can be *instantaneous* or by *degradation*. A simple example of an instantaneous failure is for example the sudden axle breakage of a power plant feed pump. An example of degradation failure is the gradual wearing out of bushings, used in lieu of bearings. The second case raises the question of defining when precisely a failure actually takes place. According to the above definition, it is convenient to define the failure of a device undergoing degradation as occurring as soon as performance parameters lie outside the specified limits of tolerance.

In safety or reliability analyses it is not sufficient to know that a failure has occurred, it is in addition necessary to specify the *mode of failure* of the component in question. For example, a valve can fail to open or fail to close; generally, the probability that a component fails to open is different from the probability that it fails to close (another example is failure to start compared to failure to stop, etc.).

Two different types of system operations

Generally speaking, two different types of system operations should be distinguished: systems that operate on demand and systems that operate continuously.

Demand failures occur in systems that operate intermittently or in a repetitive manner. Either the system operates at the *n*th demand, event D_n, or it fails, event $\overline{D}_n$. The probability that the system fails at the *n*th demand, after having successfully responded to the *n*-1 preceding demands, event S_{n-1}, is given by (see Eq.[2.73]):

$$\begin{aligned} P\left(\overline{D}_n \cap S_{n-1}\right) &= P\left(\overline{D}_n \mid S_{n-1}\right) \cdot P\left(S_{n-1}\right) \\ &= P\left(\overline{D}_n \mid D_1 \cap D_2 \cap \ldots D_{n-1}\right) \cdot P\left(D_{n-1} \mid D_1 \cap D_2 \cap \ldots D_{n-2}\right) \cdot \ldots \\ &\quad \ldots P\left(D_2 \mid D_1\right) \cdot P\left(D_1\right) \end{aligned} \qquad [3.1]$$

It is often legitimate to assume that the failures are random (independent); in this case Eq. [3.1] reduces to:

$$P\left(D_1 \cap D_2 \cap \ldots D_{n-1} \cap \overline{D}_n\right) = P\left(\overline{D}\right) \cdot \left[P(D)\right]^{n-1} = P\left(\overline{D}\right) \cdot \left[1 - P\left(\overline{D}\right)\right]^{n-1} \qquad [3.2]$$

Thus, only one value, the failure probability $P\left(\overline{D}\right)$, needs to be known.

Note that the probability that a *repairable* system will fail anytime during *n* demands would be *n* times the value given by Eq. [3.2]. This is nothing else than the expression of a binomial distribution for the particular case x_i =1 (1 failure), with $p = P(\overline{D})$.

Example: a repairable gas circuit breaker has a demand failure probability of 10^{-4} per demand. On the average, this device has to operate 6 times per month. Calculate the probability that it will fail more than one time during one year.

Fig.: Hyosung Corporation

The number of requests in one year will be: 6 ·12 = 72. The probability of more than one failure during the year is given by P(X >1) = 1 – P(0) – P(1), with:

$$P(0) = \left(1-10^{-4}\right)^{72} = 0.992826 \text{ and } P(1) = 72 \cdot 10^{-4} \cdot \left(1-10^{-4}\right)^{71} = 0.007149$$

Thus, P(X > 1) = 1 – 0.992826 – 0.007149 = 2.5 10^{-5}.

For systems in continuous operation, which do not undergo repair, let us define T as the random variable measuring the operating time without failure. The cumulative probability function of the variable T is by definition (see Chap. 2) given by:

$$F_T(t) = P(T \le t) = 1 - P(T > t) = 1 - R(t) \qquad [3.3]$$

where $f_T(t)$ is the failure probability density and R(*t*) is the *reliability* of the device, defined as the probability that fault has not occurred in a system for a given period of time *t* and under specified operating conditions. These different functions are linked by the following relationships:

$$f(t) = \frac{dF(t)}{dt} = \frac{d\overline{R}(t)}{dt} = -\frac{dR(t)}{dt} \qquad [3.4]$$

With these definitions, the analog of Eq. [3.1] takes the form:

$$f_T(t)\,dt = \Lambda(t)\,dt \cdot [1 - F(t)] = \Lambda(t)\,dt \cdot R(t) \qquad [3.5]$$

In this equation:

- f(*t*) d*t* represents the probability for failure in d*t* about *t*,
- Λ(*t*) d*t* represents the conditional probability for failure in d*t* about *t*, given that no failure has occurred to time *t*,
- 1 – F(*t*) = R(*t*) represents the probability the device did not fail up to time *t*.

The *failure rate* Λ(*t*), which has units of inverse time, is also sometimes called the *hazard rate* (the first name is however more appropriate). According to its definition, this parameter can be evaluated as shown in Fig. 3.1.

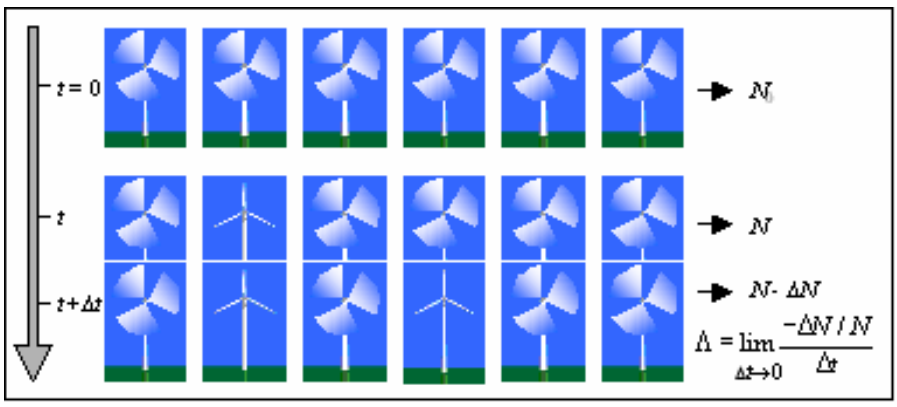


Figure 3.1 ***Failure rate definition and illustration***

The failure rate is directly related to the failure probability of the considered device:

$$\overline{\mathrm{R}}(t) = \frac{N_0 - N(t)}{N_0} = 1 - \frac{N(t)}{N_0} \qquad [3.6]$$

Utilizing moreover the expression given in Fig. 3.1 (to the limit $\Delta t \to 0$), it comes:

$$\frac{\mathrm{d}N(t)}{\mathrm{d}t} = -\,\Lambda(t)\,\mathrm{d}t \qquad [3.7]$$

And therefore, after integration:

$$N(t) = N_0 \cdot \exp\left[-\int_0^t \Lambda(t')\,\mathrm{d}t'\right] \qquad [3.8]$$

which with Eq. [3.6] leads to:

$$\overline{\mathrm{R}}(t) = 1 - \exp\left[-\int_0^t \Lambda(t')\,\mathrm{d}t'\right] \qquad [3.9]$$

This result can also be directly obtained from Eq. [3.5]:

$$\Lambda(t) = \frac{\mathrm{f}(t)}{1 - \mathrm{F}(t)} = \frac{\mathrm{f}(t)}{\mathrm{R}(t)} = -\frac{1}{\mathrm{R}(t)} \cdot \frac{\mathrm{dR}(t)}{\mathrm{d}t} = -\frac{\mathrm{d}\ln \mathrm{R}(t)}{\mathrm{d}t} \qquad [3.10]$$

Thus:

$$\mathrm{R}(t) = 1 - \overline{\mathrm{R}}(t) = \exp\left[-\int_0^t \Lambda(t')\,\mathrm{d}t'\right] \qquad [3.11]$$

If $\Lambda(t) = \lambda$ = constant (often a reasonable assumption, see p.55):

$$\overline{\mathrm{R}}(t) = 1 - \exp(-\lambda t) \cong \lambda t \ \text{(for } \lambda t \text{ small)} \qquad [3.12]$$

Combining Eqs. [3.10] and [3.11] allows us to write the following important result:

$$\mathrm{f}(t) = \Lambda(t) \cdot \mathrm{R}(t) = \Lambda(t) \cdot \exp\left[-\int_0^t \Lambda(t')\,\mathrm{d}t'\right] \qquad [3.13]$$

A summary of formulas relating $\Lambda(t)$, $\mathrm{R}(t)$, $\mathrm{F}(t)$ and $\mathrm{f}(t)$ is given in Table 3.1.

Table 3.1 ***Summary of failure formulas***

Description	Symb.	First form	Second form	Third form
Failure rate	$\Lambda(t)$	$-(1/\mathrm{R})\cdot\mathrm{dR}/\mathrm{d}t$	$\mathrm{f}(t) / [1 - \mathrm{F}(t)]$	$\mathrm{f}(t) / \mathrm{R}(t)$
Reliability	$\mathrm{R}(t)$	$\int_t^\infty \mathrm{f}(t')\,\mathrm{d}t'$	$1 - \mathrm{F}(t)$	$\exp\left[-\int_0^t \Lambda(t')\,\mathrm{d}t'\right]$
Cumulative failure prob.	$\mathrm{F}(t)$	$\int_0^t \mathrm{f}(t')\,\mathrm{d}t'$	$1 - \mathrm{R}(t)$	$1 - \exp\left[-\int_0^t \Lambda(t')\,\mathrm{d}t'\right]$
Failure prob. density	$\mathrm{f}(t)$	$\mathrm{dF}(t) / \mathrm{d}t$	$-\,\mathrm{dR}(t) / \mathrm{d}t$	$\Lambda(t)\cdot\mathrm{R}(t)$

Example: It is assumed that the failure rate for a pressure valve is given by the expression $\Lambda(t) = 1 / (t+2)$. What is the cumulative probability of failure F(t)? What is the probability density for failure at time t, f(t)?

Fig.: Yokota Manufacturing Co., Ltd.

We need first to calculate the integral $\int_0^t \frac{1}{t'+2}\,dt' = \int_2^{t+2} \frac{dx}{x} = \ln x\Big|_2^{t+2} = \ln\left(\frac{t+2}{2}\right)$,

then: $F(t) = 1 - \exp\left[-\int_0^t \frac{1}{t'+2}\,dt'\right] = 1 - \frac{2}{t+2} = \frac{t}{t+2}$

and: $f(t) = \frac{dF(t)}{dt} = \frac{2}{(t+2)^2}$

Reliability indicators

A frequently used indicator to characterize the reliability performance of a device is the *mean time to failure*, or MTTF, which is the first moment of the probability density:

$$MTTF = \int_0^\infty t \cdot f(t)\,dt \qquad [3.14]$$

The mean time to failure can be expressed in terms of the reliability R(t) by replacing f(t) by – dR(t) / dt and then integrating by parts the Eq. [3.14] (assuming that $t \cdot R(t) \to 0$ for $t \to \infty$):

$$MTTF = \int_0^\infty R(t)\,dt \qquad [3.15]$$

The MTTF is particularly simple to calculate in the case of a random failure ($\Lambda(t) = \lambda$ = constant), since:

$$MTTF = \frac{1}{\lambda} \qquad [3.16]$$

It should be noted that the above expressions of the MTTF are only valid for a device that cannot be repaired. If repairs are possible, then the system may remain operable for $t \to \infty$, at least part of the time. In such a case, rather than the reliability it is more meaningful to consider the instantaneous *availability* of the system, A(t), which is defined as "*the probability a system performs a specified function or mission under given conditions at a prescribed time*" [McCormick, 1981]. Obviously, reliability and availability are related by the following inequality:

$$R(t) \le A(t) \le 1 \qquad [3.17]$$

Since, on one hand, A(t) = R(t) for a device that cannot be repaired, and on the other hand, a repairable system may be "available" again some time after a failure had occurred. It follows that, as t becomes large, R(t) approaches zero whereas A(t) reaches some steady-state value.

The MTTF is not the only indicator that can be used to quantify the reliability of a device. Other indicators of this kind, as well as their relationships, are presented in Fig. 3. 2.

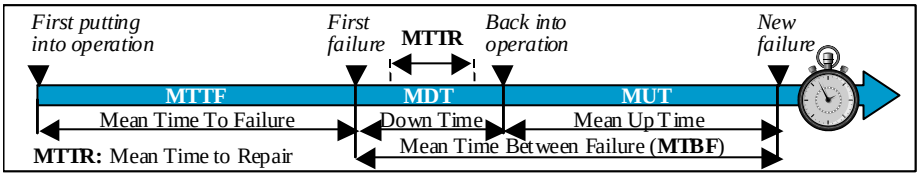


Figure 3.2 ***Different reliability indicators and their relationships***

3.2 Reliability and Availability of Single Components or Units of a System

Repairable versus irreparable units

When analyzing the reliability or availability of a single component or unit of a system, two different cases must be considered:

- the unit cannot be repaired,
- the unit can be repaired; the repair is assumed to begin immediately after the failure has been detected and, at the end of the repair process, the unit is put back into operation "as new".

Note: to make calculations more simple, from now on the failure rates (λ) and, for repairable units, the analog repair rates (μ), will be assumed to be constant

The above assumption is generally well justified for a wide variety of mechanical and electronic components and systems, at least for the useful life part of the product history. This is because the time behavior of the failure rate of such systems typically exhibits what has become widely known as a "bathtub curve" (see Fig. 3.3).

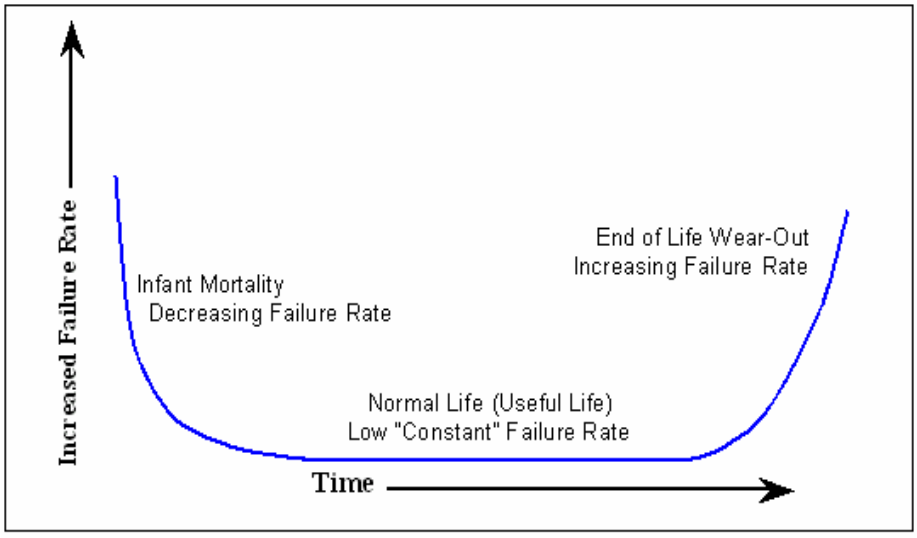


Figure 3.3 ***The "bathtub curve", hypothetical failure rate versus time***

The initial region that begins at time zero when a customer first begins to use the product is characterized by a high but rapidly decreasing failure rate. This region is known as the *Early Failure Period* (also referred to as *Infant Mortality Period*). This decreasing failure rate typically lasts several weeks to a few months. Next, the failure rate levels off and remains roughly constant for (hopefully) the majority of the useful life of the product. This long period of a level failure rate is known as the *Intrinsic Failure Period* (also called the *Stable Failure Period*) and the constant failure rate level is called the *Intrinsic Failure Rate*. Finally, if units from the population remain in use long enough, the failure rate begins to increase as materials wear out and degradation failures occur at an ever increasing rate. This is the *Wearout Failure Period*.

Most technical systems spend most of their lifetimes operating in the flat portion (stable failure period) of the bathtub curve.

The Bathtub Curve also applies (based on much empirical evidence) to repairable systems. In this case, the vertical axis is the repair rate or the rate of occurrence of failures (ROOOF).

Non-repairable units

The reliability of a unit that cannot be repaired is, from Eq. [3.11], given by:

$$R(t) = \exp(-\lambda t) \qquad [3.18]$$

As, by definition, the availability of such a device is equal to its reliability, we have therefore also:

$$A(t) = \exp(-\lambda t) \qquad [3.19]$$

Repairable units

The usual systems consider by a risk analyst can however be repaired; this means that such systems can either be operating or under repair. The determination of $A(t)$ for a system with repairable components is thus more complicate than the analysis of the reliability of a system without repairable parts.

In addition to the failure rate, it is necessary for such systems to define the same way an instantaneous *repair rate* μ (or $\mathcal{M}(t)$ in the general time-dependent case):

$$\mathcal{M}(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} \cdot P(\text{unit is repaired between } t \text{ and } t + dt, \text{ taken that it was out of order during the period } [0, t]) \qquad [3.20]$$

Because the fact that a unit can or cannot be repaired does not change its reliability, the relation [3.18] remains valid here. The situation is different for the availability, which is no more equal to the reliability but responds in this case to the following probability equation:

$A(t + dt) = P(\text{unit is in working order at } t \text{ and does not fail between } t \text{ and } t + dt) +$
$P(\text{unit is out of order at time } t \text{ and is repaired between } t \text{ and } t + dt)$

Using the definitions of the availability as well as of the failure and repair rates, the symbolic expression of the above equation becomes:

$$A(t + dt) = A(t) \cdot (1 - \lambda\, dt) + (1 - A(t)) \cdot \mu\, dt \qquad [3.21]$$

That is to say:

$$\frac{dA(t)}{dt} = \mu - (\lambda + \mu) \cdot A(t) \qquad [3.22]$$

This differential equation can be solved with the help of the Laplace transform (see Appendix 3.1). The Laplace transform of Eq. [3.2] gives:

$$s \cdot \mathcal{L}[A(t)] - A(0) = \frac{\mu}{s} - (\lambda + \mu) \cdot \mathcal{L}[A(t)] \qquad [3.23]$$

Therefore:

$$\mathcal{L}[A(t)] = \frac{A(0)}{s + (\lambda + \mu)} + \frac{\mu}{s \cdot (s + (\lambda + \mu))} \qquad [3.24]$$

Applying the inverse transform approach presented in Appendix 3.1, Eq. [3.24] can be rewritten as follows:

$$\mathcal{L}[A(t)] = \frac{A(0)}{s + (\lambda + \mu)} + \frac{\mu}{s \cdot (s + (\lambda + \mu))} = \frac{q_1}{s} + \frac{q_2}{s + (\lambda + \mu)} \qquad [3.25]$$

with :

$$q_1 = \lim_{s \to 0} \frac{A(0) \cdot s}{s + (\lambda + \mu)} + \frac{\mu}{(s + (\lambda + \mu))} = \frac{\mu}{\lambda + \mu}$$

$$q_2 = \lim_{s \to -(\lambda+\mu)} A_0 + \frac{\mu}{s} = A_0 - \frac{\mu}{\lambda + \mu} \qquad [3.26]$$

The general expression of the availability of a repairable system is thus given by (see Table in Appendix 3.1 for the inverse transforms)

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda \cdot A_0 - \mu \cdot (1 - A_0)}{\lambda + \mu} \cdot e^{-(\lambda+\mu)\cdot t} \qquad [3.27]$$

Two different initial conditions are possible:

a) the unit is in operating order at the time t=0, i.e. $A_0 = 1$; in this case:

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} \cdot e^{-(\lambda+\mu)\cdot t} \qquad [3.28]$$

b) the unit is out of order at the time t=0, i.e. $A_0 = 0$; in this case:

$$A(t) = \frac{\mu}{\lambda + \mu} \cdot \left[1 - e^{-(\lambda+\mu)\cdot t}\right] \qquad [3.29]$$

We observe that for large time the asymptotic value, towards which the availability tends, is the same in both cases:

$$\lim_{t \to \infty} A(t) = \frac{\mu}{\lambda + \mu} \qquad [3.30]$$

This behavior of the availability function of a repairable unit is represented graphically in figure 3.4.

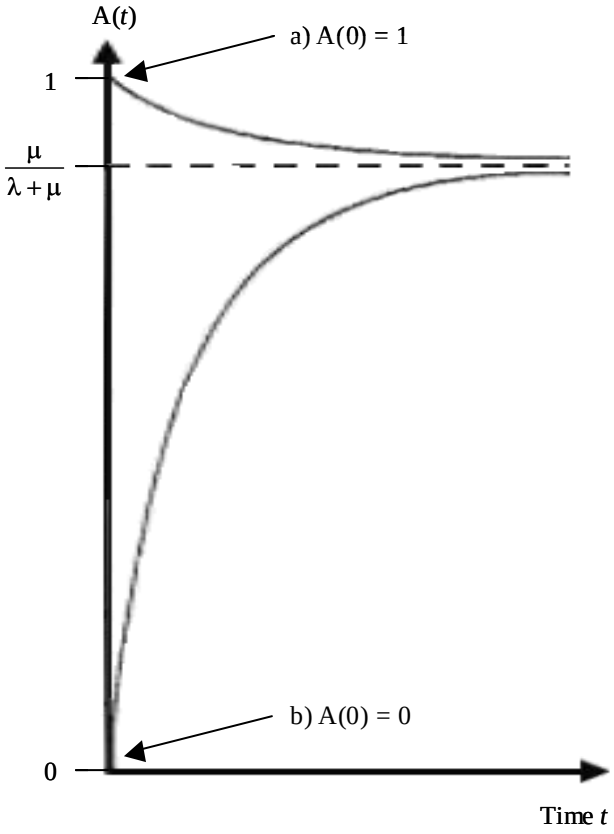


Figure 3.4 ***Time behavior of repairable unit availability***

Taking into account that for constant failure and repair rates:

$$\text{MTTF} = \int_0^\infty \text{R}(t)\,\text{d}t = \int_0^\infty \text{e}^{-\lambda \cdot t}\,\text{d}t = \frac{1}{\lambda} \qquad [3.31]$$

and:

$$\text{MTTR} = \int_0^\infty \left[1 - \text{M}(t)\right]\text{d}t = \int_0^\infty \text{e}^{-\mu \cdot t}\,\text{d}t = \frac{1}{\mu} \qquad [3.32]$$

we deduce that:

$$\lim_{t \to \infty} \text{A}(t) = \text{A}(\infty) = \frac{\mu}{\lambda + \mu} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \qquad [3.33]$$

or

$$\overline{\text{A}}(\infty) = 1 - \text{A}(\infty) = \frac{\text{MTTR}}{\text{MTTF} + \text{MTTR}} \approx \frac{\lambda}{\mu} \qquad [3.34]$$

In Eq. [3.32], M(t) is the cumulative probability function for the random variable characterizing the repair time T_r (i.e. $P(T_r \leq t)$). The corresponding density function will be noted g(t). We have therefore (analogy with Eq. [3.4]):

$$\text{g}(t) = \frac{\text{dM}(t)}{\text{d}t} \qquad [3.35]$$

A summary of the expressions of the main reliability and availability characteristics for the model of constant failure and repair rates is given in Table 3.2

Table 3.2 ***Reliability and availability characteristics for units with const. λ and μ***

Non-repairable unit	**Repairable unit**
$\Lambda(t) = \lambda$ = constant	$\Lambda(t) = \lambda$ = constant
$f(t) = \lambda \cdot \exp(-\lambda \cdot t)$	$f(t) = \lambda \cdot \exp(-\lambda \cdot t)$
$R(t) = \exp(-\lambda \cdot t)$	$R(t) = \exp(-\lambda \cdot t)$
$\overline{R}(t) = 1 - \exp(-\lambda \cdot t)$	$\overline{R}(t) = 1 - \exp(-\lambda \cdot t)$
$A(t) = R(t) = \exp(-\lambda \cdot t)$	$A(t) = \mu/(\lambda+\mu) + [\lambda/(\lambda+\mu)] \cdot \exp[-(\lambda+\mu) \cdot t]$, $A(0)=1$
	$A(t) = \mu/(\lambda+\mu) \cdot \{1-\exp[-(\lambda+\mu) \cdot t]\}$ $A(0)=0$
$\overline{A}(t) = 1 - \exp(-\lambda \cdot t)$	$\overline{A}(t) = \lambda/(\lambda+\mu) \cdot \{1-\exp[-(\lambda+\mu) \cdot t]\}$ $A(0)=1$
	$\overline{A}(t) = 1 - \mu/(\lambda+\mu) \cdot \{1-\exp[-(\lambda+\mu) \cdot t]\}$ $A(0)=0$
$\mathcal{M}(t) = 0$	$\mathcal{M}(t) = \mu$ = constant
$g(t) = 0$	$g(t) = \mu \cdot \exp(-\mu \cdot t)$
$M(t) = 0$	$M(t) = 1 - \exp(-\mu \cdot t)$
$\text{MTTF} = 1/\lambda$	$\text{MTTF} = 1/\lambda$
$\text{MTTR} = \infty$	$\text{MTTR} = 1/\mu$

3.3 Estimation of Reliability Parameters

Reliability estimators

The basic elements of the estimation theory have been presented in section 2.2. We will deal here with the specific question of defining appropriate reliability estimators and calculating their confidence intervals.

Failure rate in continuous operation

Assuming the failure rate constant, an estimator of this parameter for a unit in continuous operation is given by:

$$\hat{\lambda} = \frac{N_f}{T_f} \qquad [3.36]$$

where N_f is the total number of failures observed during the cumulating operating time T_f. Thus means that the mean time between failures, T_f/N_f, will be equal to $1/\hat{\lambda}$, in accordance with the fact that MTTF ≈ MTBF = $1/\lambda$ (Eq.[3.31]).

Failure rate at rest

Similarly, the failure rate of a unit at rest can in principle be calculated as follows:

$$\hat{\lambda}_r = \frac{N_r}{T_r} \qquad [3.37]$$

where N_r is the total number of failures observed at rest and T_r the cumulated rest time. Of course, it could be difficult in practice to become aware that a unit has failed while being at rest.

Failure rate for operation on demand

For units operating on demand, the demand failure probability estimator $\hat{\gamma}$ is given by the ratio of the number N_{df} of observed failures to respond to a demand, to the total number of demands N_d:

$$\hat{\gamma} = \frac{N_{df}}{N_d} \qquad [3.38]$$

Repair rate

The repair rate (in continuous operation or at rest) can be calculated in a similar way as the failure rates in Eqs. [3.36] and [3.37]:

$$\hat{\mu} = \frac{N_{rep}}{T_{rep}} \qquad [3.39]$$

where N_{rep} is the number of repair processes carried out during the cumulated repair time T_{rep}.

Note: if the unit cannot be repaired, it has to be replaced; in such a case, it is more appropriate to use the term *substitution rate* rather than *repair rate*.

Table 3.3 gives a summary of the way reliability indicators can be estimated from observed data.

Table 3.3 *Practical estimation of reliability indicators*

Relative to failure rate	**Relative to repair rate**
$\widehat{\text{MTTF}} \approx \widehat{\text{MUT}} \approx \widehat{\text{MTBF}} \approx 1/\hat{\lambda} = T_\alpha/N_\alpha$	$\widehat{\text{MDT}} \approx \widehat{\text{MTTR}} \approx 1/\hat{\mu} = T_{rep}/N_{rep}$

In most cases, the mean time to repair (MTTR) and the mean down time (MDT) are very small compared to the operating times (MTTF or MTBF). This justifies the approximate relationships used in Table 3.3.

Confidence intervals

The reliability parameters being random variables, as pointed out in section 2.2 a confidence interval must be associated with the estimators given above, in such a way that (for any given parameter p):

$$P\,(p_{inf} \leq \hat{p} \leq p_{sup}) = 1 - \alpha \qquad [3.40]$$

where p_{inf} and p_{sup} are the confidence limits and 1-α is the expected confidence level.

Example: assuming a constant failure rate λ, the number of failures N_f is distributed according to a Poisson law. In this case, the confidence limits are given by:

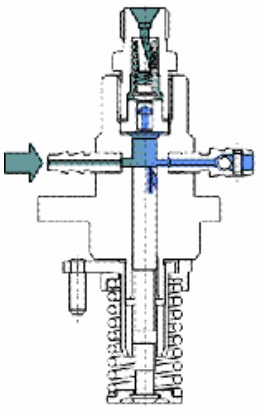
$$\lambda_{inf} = \frac{\chi^2_{\alpha/2}(2N_f)}{2T_f} \quad , \quad \lambda_{sup} = \frac{\chi^2_{1-\alpha/2}(2N_f + 2)}{2T_f} \qquad [3.41]$$

$\chi^2_\alpha(r)$ is deduced from the *chi-square* distribution, a special case of the *gamma distribution*, which obeys the equation:

$$F\left(\chi^2 \middle| r\right) = \frac{\int_0^{\chi^2} t^{(r/2)-1} \cdot e^{-t/2}\, dt}{2^{(r/2)} \cdot \Gamma(r/2)} = \frac{\gamma(r/2, \chi^2/2)}{\Gamma(r/2)} \qquad [3.42]$$

The integer r, with $r \geq 1$, in this distribution is called the "*degree of freedom*". $\chi^2_\alpha(r)$ is the value of χ^2 for which the above expression is equal to α.

As a numerical application, let us consider a set of identical pumps that have registered 2 failures during a cumulated operation time of 10'000 hours. The failure rate of these pumps can thus be estimated as:



$$\hat{\lambda} = \frac{2}{10'000} = 2\,10^{-4}\ \left[h^{-1}\right]$$

The 90% confidence limits are in these conditions given by:

$$\lambda_{inf} = \frac{\chi^2_{0.05}(4)}{20'000} = \frac{0.711}{20'000} = 3.6\,10^{-5}\left[h^{-1}\right]$$

$$\lambda_{sup} = \frac{\chi^2_{0.95}(6)}{20'000} = \frac{12.1}{20'000} = 6.3\,10^{-4}\left[h^{-1}\right]$$

Let us assume now that the set of pumps is observed over a longer cumulated time, for example 70'000 hours and that 14 failures are registered in this case. Obviously, this does not change the estimation of the failure rate, which remains equal to:

$$\hat{\lambda} = \frac{14}{70'000} = 2\,10^{-4}\ \left[h^{-1}\right]$$

This is however not true for the 90% confidence limits, which here become:

$$\lambda_{inf} = \frac{\chi^2_{0.05}(28)}{140'000} = \frac{16.9}{140'000} = 1.2\,10^{-4}\left[h^{-1}\right]$$

$$\lambda_{sup} = \frac{\chi^2_{0.95}(30)}{140'000} = \frac{43.8}{140'000} = 3.1\,10^{-4}\left[h^{-1}\right]$$

The ratio $\lambda_{sup}/\lambda_{inf}$ is thus reduced by a factor greater than six (from 17.5 in the first case to 2.6 in the second case). This narrowing of the limits expresses the gain in confidence obtained thanks to the longer observation time.

Bayesian estimation

The fact that more information leads to improved statistical results is a general observation. It is at the root of the most classical application of the Bayes' theorem (section 2.4) in safety/reliability analyses, i.e. as a means of revising failure data. When applied in this way, it serves as an important link between axiomatic probability and relative frequency probability. Additional information tends to modify axiomatic probabilities to yield posterior probabilities closer to the relative frequency [McCormick, 1981].

Let us note $P(\theta_i|I_g)$ the prior probability of observing, among *n* discrete possible values, the value θ_i of the parameter we are interested in, taking into account "generic" information only (information about the general design and fabrication of the device, about the operating performances of devices of the same kind, etc.).

Now, if after some time experimental data about a specific device become available (information of the I_s type), a revised estimation of the probability of observing the value θ_i of the parameter can be calculated for this *particular* device using Bayes' equation:

$$P\left(\theta_i \middle| I_g, I_s\right) = \frac{P\left(\theta_i \middle| I_g\right) \cdot P\left(I_s \middle| \theta_i, I_g\right)}{\sum_{j=1}^{n} P\left(\theta_j \middle| I_g\right) \cdot P\left(I_s \middle| \theta_j, I_g\right)} \qquad [3.43]$$

with:

$P\left(\theta_i \middle| I_g\right)$: prior estimation of the probability of observing the value θ_i for the parameter of interest, based on generic information only;

$P\left(I_s \middle| \theta_i, I_g\right)$: probability that the information of type I_s will be observed if the value of the parameter is indeed θ_i and given the knowledge of the generic information;

$P\left(\theta_i \middle| I_g, I_s\right)$: posterior estimation of the probability of observing the value θ_i for the parameter of interest, given the knowledge of the generic *and* specific information.

The above expressions can easily be generalized to the case where the possible values of the parameter of interest are given by a continuous function.

The prior probability $P\left(\theta_i \middle| I_g\right)$ is immediately available if the generic law relative to the parameter of interest is fully known for the considered type of device. However, sometimes only the upper and lower values that the parameter θ can possibly take are known. If the type of probability law can be guessed, the parameters of this last one can be estimated assuming that the upper and lower limits define for example a 90% confidence interval.

It remains to calculate the $P\left(I_s \middle| \theta_i, I_g\right)$ probabilities. If we consider for example that the parameter to be estimated is the failure probability on demand γ and that *k* failures had actually been observed on *n* attempts (demands), $P\left(I_s \middle| \gamma_i, I_g\right)$ is given by (binomial distribution):

$$P\left(I_s \middle| \gamma_i, I_g\right) = \frac{n!}{k!(n-k)!} \cdot \gamma_i^k \cdot (1-\gamma_i)^{(n-k)} \qquad [3.44]$$

If the *k* failures are observed during a cumulated operation time of *T* hours, the distribution of the failure rate λ takes this time the form (Poisson distribution):

$$P\left(I_s \middle| \lambda_i, I_g\right) = \frac{(\lambda_i \cdot T)^k}{k!} \cdot \exp(-\lambda_i \cdot T) \qquad [3.45]$$

Example (adapted from [Lemeur, 1988]): the emergency generating unit of a nuclear power plant is assumed to have a prior failure probability on demand distributed according to a lognormal law.

Given that the unit had been found to fail to start 5 times on 227 attempts, give the posterior distribution taking this new information into account.

The details of the required calculations are given in the following table.

Table 3.4 ***Detailed calculations of the posterior distribution of the failure probability on demand for the considered emergency generating unit***

$227!/(5!\cdot 222!)\cdot\gamma_i^{5}\cdot(1-\gamma_i)^{222}$

γ_i	A $P(\gamma_i \mid I_g)$	B $P(I_s \mid \gamma_i, I_g)$	C A * B	$P(\gamma_i \mid I_g, I_s)$
$8.70\ 10^{-3}$	0.048	$3.44\ 10^{-2}$	$1.65\ 10^{-3}$	$1.99\ 10^{-2}$
$1.15\ 10^{-2}$	0.054	$7.41\ 10^{-2}$	$4.00\ 10^{-3}$	$4.83\ 10^{-2}$
$1.54\ 10^{-2}$	0.096	$1.33\ 10^{-1}$	$1.27\ 10^{-2}$	$1.54\ 10^{-1}$
$2.05\ 10^{-2}$	0.134	$1.75\ 10^{-1}$	$2.35\ 10^{-2}$	$2.83\ 10^{-1}$
$2.74\ 10^{-2}$	0.161	$1.56\ 10^{-1}$	$2.50\ 10^{-2}$	$3.02\ 10^{-1}$
$3.65\ 10^{-2}$	0.160	$8.10\ 10^{-2}$	$1.30\ 10^{-2}$	$1.56\ 10^{-1}$
$4.87\ 10^{-2}$	0.141	$2.02\ 10^{-2}$	$2.85\ 10^{-3}$	$3.44\ 10^{-2}$
$6.49\ 10^{-2}$	0.097	$1.88\ 10^{-3}$	$1.82\ 10^{-4}$	$2.20\ 10^{-3}$
$8.66\ 10^{-2}$	0.053	$4.33\ 10^{-5}$	$2.29\ 10^{-6}$	$2.77\ 10^{-5}$
$1.16\ 10^{-1}$	0.051	$1.45\ 10_{-7}$	$7.40\ 10^{-9}$	$8.92\ 10^{-8}$
	Lognormal	Total $\rightarrow$ $8.29\ 10^{-2}$		C/Total

The corresponding graphical representations of the prior and posterior distributions are given in Fig. 3.5.

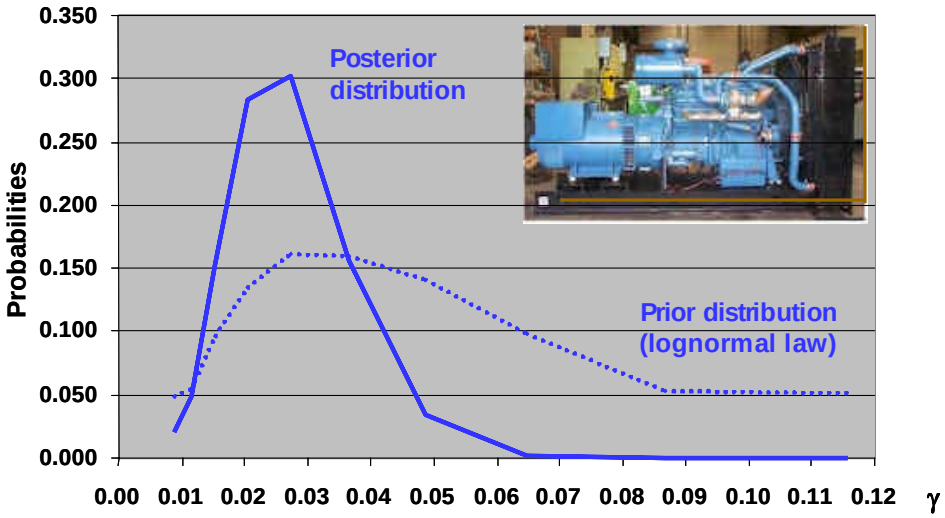


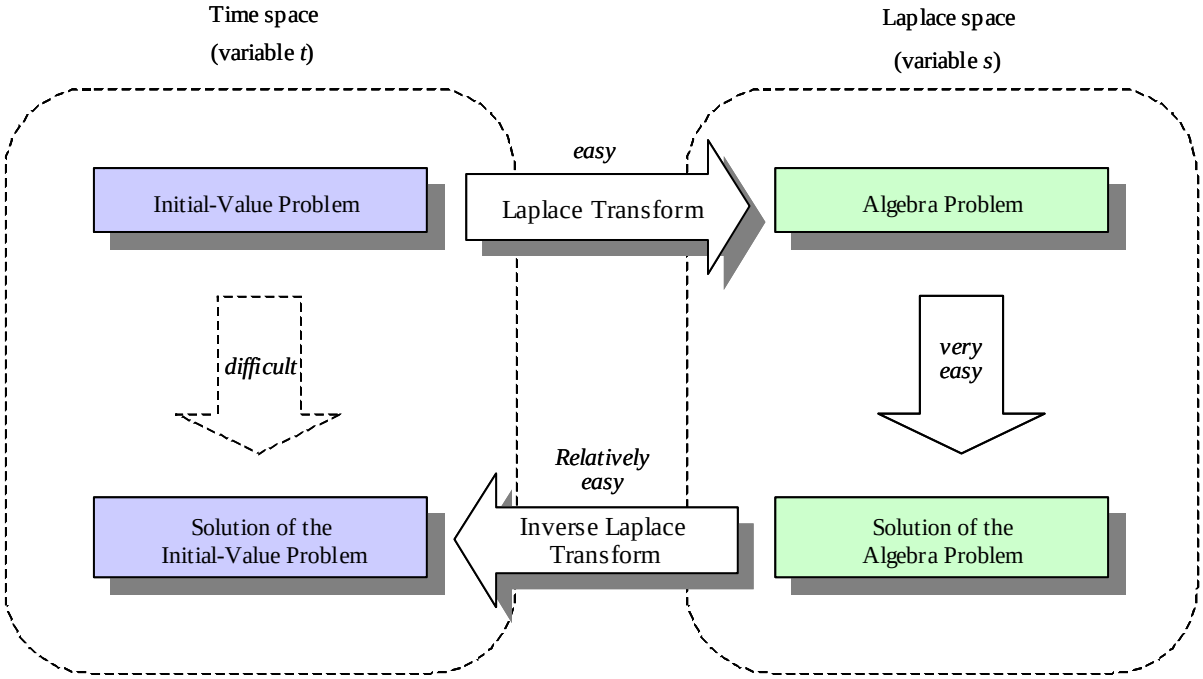
Figure 3.5 ***Prior and posterior distributions of the failure probability on demand***

The figure shows that the prior distribution has been, on one hand, shifted towards lower probabilities and, on the other hand, narrowed (reduction of the distribution dispersion) as could be expected from the use of additional information.

Appendix 3.1 Laplace Transform

• General definition of the Laplace transform:

The *Laplace transform* is a powerful mathematical tool formulated to solve a wide variety of *initial-value* problems. The strategy is to transform the difficult differential equations solving into simple algebra problems where solutions can be easily obtained. One then applies the *Inverse Laplace transform* to retrieve the solutions in the original problem space (usually, time space). This can be illustrated as follows:



• Mathematical definition of the Laplace transform:

The Laplace Transform - denoted F(*s*) - of a function f(*t*) defined on the interval [0, ∞[is given by the following integral:

$$\mathcal{L}\{f(t)\} \equiv F(s) = \int_0^\infty e^{-st} \cdot f(t)\, dt$$

Where *s* is real and $\mathcal{L}$ is called the *Laplace Transform Operator*.

For F(*s*) to exist, it is sufficient (but not necessary) that f(*t*) fulfill the following conditions:

1) f(*t*) is piecewise continuous on $0 \le t < \infty$,
2) f(*t*) is of exponential order as $t \to \infty$; that is, there exist real constant K, a and T such that:

$$|f(t)| \le K \cdot e^{at} \quad , \quad \text{for all } t > T.$$

• Mathematical definition of the Inverse Laplace Transform:

By definition:

$$\mathcal{L}^{-1}\{F(s)\} = f(t)$$

where $\mathcal{L}^{-1}$ is the Inverse *Laplace Transform Operator*.

For the inverse Laplace transform to exist, it is necessary that: 1) $\lim_{s \to \infty} F(s) = 0$ and 2) $\lim_{s \to \infty} s \cdot F(s)$ remains finite.

The table below gives some important Laplace transforms and Laplace transform properties:

Function	Laplace Transform	Function	Laplace Transform
1	$\frac{1}{s}$	t	$\frac{1}{s^2}$
t^n $\quad n \in Z > 0$	$\frac{n!}{s^{n+1}}$	t^a $\quad a > 0$	$\frac{\Gamma(a+1)}{s^{a+1}}$
$H_c(t)$ *Heaviside step function*	$\frac{e^{-cs}}{s}$ $\quad c \geq 0$	e^{at}	$\frac{1}{s-a}$ $\quad s > a$
$\left[\frac{t^{n-1}}{(n-1)!}\right] \cdot e^{-at}$	$\frac{1}{(s+a)^n}$, $n = 1, 2, 3 \ldots$	$1 - e^{-at}$	$\frac{a}{s \cdot (s+a)}$
$\frac{1}{(a-b)} \cdot \left[e^{-at} - e^{-bt}\right]$	$\frac{1}{(s+a)\cdot(s+b)}$ $\quad b \neq a$	$\frac{1}{ab} + \frac{e^{-at}}{a\cdot(a-b)} + \frac{e^{-bt}}{b\cdot(b-a)}$	$\frac{1}{s\cdot(s+a)\cdot(s+b)}$ $\quad b \neq a$
$\frac{1}{(a-b)} \cdot \left[a \cdot e^{-at} - b \cdot e^{-bt}\right]$	$\frac{s}{(s+a)\cdot(s+b)}$ $\quad b \neq a$	$\frac{1}{\sqrt{\pi t}} \cdot e^{-at}$	$\frac{1}{\sqrt{s+a}}$
$\delta(t\text{-}c)$ *Dirac*	e^{-cs} $\quad c > 0$	$\frac{\lambda^\beta \cdot t^{(\beta-1)} \cdot e^{-\lambda t}}{\Gamma(\beta)}$ *Gamma*	$\frac{\lambda^\beta}{(s+\lambda)^\beta}$
$\cos(\omega t)$	$\frac{s}{s^2+\omega^2}$	$\sin(\omega t)$	$\frac{\omega}{s^2+\omega^2}$
$\cosh(\omega t)$	$\frac{s}{s^2-\omega^2}$ $\quad s > \lvert\omega\rvert$	$\sinh(\omega t)$	$\frac{\omega}{s^2-\omega^2}$ $\quad s > \lvert\omega\rvert$
$J_0(at)$ *zero-order Bessel*	$\frac{1}{\sqrt{s^2+a^2}}$	$I_0(at)$ *Modified Bessel*	$\frac{1}{\sqrt{s^2-a^2}}$
$\left(\frac{t}{a}\right) \cdot J_1(at)$	$\frac{1}{\left(s^2+a^2\right)^{3/2}}$	$\left(\frac{t}{a}\right) \cdot I_1(at)$	$\frac{1}{\left(s^2-a^2\right)^{3/2}}$
$\frac{df(t)}{dt}$	$s\cdot F(s) - f(0)$	$\frac{d^k f(t)}{dt^k}$	$s^k \cdot F(s) - s^{k-1} \cdot f(0) - s^{k-2} \cdot \left.\frac{df}{dt}\right\rvert_0 \ldots - \left.\frac{d^{k-1} f}{dt^{k-1}}\right\rvert_0$
$\int_0^t f(t')\,dt'$	$\frac{1}{s} \cdot F(s)$	$\int_0^\infty f(t')\,dt'$	$F(0)$

Function	Laplace Transform	Function	Laplace Transform
f(a*t*) a > 0	$\frac{1}{a} \cdot F\left(\frac{s}{a}\right)$	f(*t* –a)	$e^{-as} \cdot F(s)$
Convolution integral $\int_0^t f(t-\tau) \cdot g(\tau)\, d\tau$	F(s)·G(s)	$e^{at} \cdot f(t)$	F(*s*-a)

The Laplace transform has moreover the following interesting properties:

$$\lim_{t \to \infty} f(t) = \lim_{s \to 0} s \cdot F(s)$$

$$\lim_{t \to 0} f(t) = \lim_{s \to \infty} s \cdot F(s)$$

• **Inverse Laplace Transform of the ratio of two polynomials in *s*:**

Consider the following Laplace transform function:

$$F(s) = \frac{Q(s)}{R(s)}, \qquad \text{with } R(s) = (s\text{-}a_1)\cdot(s\text{-}a_2) \ldots (s\text{-}a_n)$$

Q(*s*) and R(*s*) are two polynomials in s, with degree Q(*s*) < degree R(*s*).

In this case, F(*s*) can be written as follows:

$$F(s) = \sum_{i=1}^{n} \frac{q(a_i)}{s - a_i}, \qquad \text{with } q(a_i) = \lim_{s \to a_i} \frac{Q(s) \cdot (s - a_i)}{R(s)}$$

The inverse transform of $1/(s\text{-}a_i)$ being the function $\exp(a_i t)$ (see Table above), f(*t*) takes thus the form:

$$f(t) = \sum_{i=1}^{n} q_i(a_i) \cdot e^{a_i t}$$

• **Laplace Transforms in the case of the sum of random variables:**

Consider for example two independent random variables X and Y with probability distributions $f_1(x)$ and $f_2(y)$ respectively. If Z is the random variable corresponding to the sum of X and Y, its probability distribution is given by:

$$f_Z(z) = \int_0^z f_1(x) \cdot f_2(z - x)\, dx = \int_0^z f_1(z - x) \cdot f_2(x)\, dx$$

Therefore (see Table):

$$\mathcal{L}[f_Z(z)] = \mathcal{L}[f_1(x)] \cdot \mathcal{L}[f_2(y)]$$

This example can straightforwardly be generalized to the case of the sum of $n > 2$ random variables.