M. Carcassi

ANNEX B: ELEMENTS OF RELIABILITY THEORY AND APPLICATIONS TO SAFETY ANALYSIS

B.1 INTRODUCTION

The aim of this chapter is to provide the main tools for understanding the application of the techniques of reliability on safety studies. Therefore, after recalling the **definition of the main variables** used in the reliability analysis, the focus will be on assessing **the reliability of components and systems, simple or complex**. It will also briefly examined a crucial aspect for applications: the common causes of failure and human error. Obviously we are not going to do a full discussion of the reliability theory and application techniques to the analysis of complex systems, but only introduce this theme, with sufficient understanding of its use in the safety analysis. For further information and more details, see the books mentioned in the references.

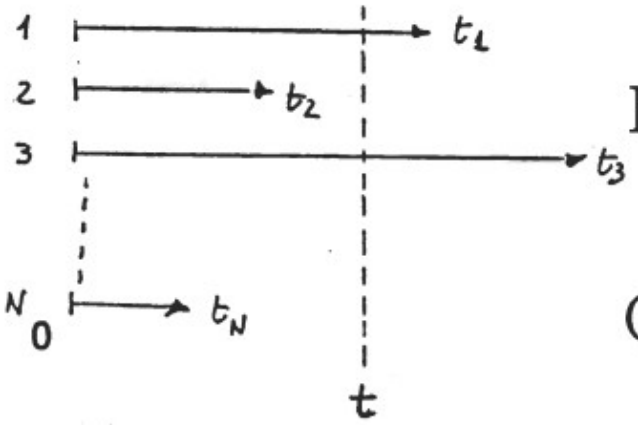
The **reliability** numerically expresses the **probability** of correct operation of of an apparatus for a **certain period of time** under certain environmental conditions for which it was designed

$$A = \text{evento}$$

$$P(A) = \frac{n}{N}$$

$$P(A) = \lim_{N \to \infty} \frac{n}{N}$$

N_0 OGGETTI IN FUNZIONE



$$R(t) = \frac{N_s}{N_0} = \frac{N_s}{N_g + N_s}$$

$$Q(t) = \frac{N_g}{N_0} = \frac{N_g}{N_g + N}$$

$$R + Q = 1$$

$$R(t) = \frac{N_s}{N_g + N_s} = \frac{N_0 - N_g}{N_0} = 1 - \frac{N_g}{N_0}$$

$$\frac{dR}{dt} = \frac{d\left(1 - \frac{N_g}{N_0}\right)}{dt} = -\frac{1}{N_0}\frac{dN_g}{dt}$$

$$\frac{dN_g}{dt} = -N_0\frac{dR}{dt} = -\frac{dN_s}{dt}$$

La probabilità di guasto istantanea di un componente

$$\lambda = \frac{1}{N_s}\frac{dN_g}{dt} = -\frac{N_0 dR}{N_s dt} = -\frac{1}{R}\frac{dR}{dt}$$

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

$$\lambda dt = -\frac{dR}{R}$$

$$\int_0^t \lambda dt = -\int_1^R \frac{dR}{R} = \ln R$$

$$t=0 \quad R=1$$

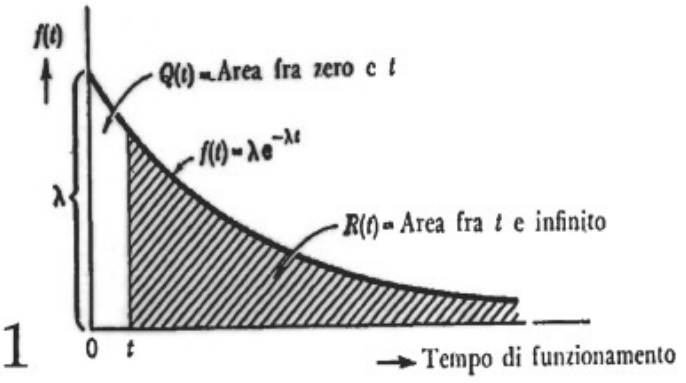
$$R(t) = \exp\left[-\int_c^t \lambda dt\right]$$

Funzione densità di guasto o DISTRIBUZIONE

$$\frac{dR}{dt} = -\frac{1}{N_0}\frac{dN_g}{dt}$$

$$f(t) = \frac{1}{N_0}\frac{dN_g}{dt} = -\frac{dR}{dt}$$

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



$$A = \int_0^\infty f(t)dt = 1$$

$$A = \int_0^t f(t)dt + \int_t^\infty f(t)dt = Q(t) + R(t) = 1$$

$$m = \int_0^\infty R(t)dt$$

B.2 DEFINITIONS

Failure rate λ (t): fraction of components that fail per unit of time;

Reliability R (t): probability that an apparatus performs the task assigned in a specific time interval (0-t), under certain environmental conditions;

Unreliability Q (t): probability that the equipment has failed during the considered time interval (0-t) (it does not carry out the function assigned at the instant t, for a fault occurred at any instant in the interval 0 -t);

Availability A (τ): probability that the system is operating properly during the mission time **τ;**

Unavailability I (τ): probability that the system is not able to perform its function during the mission time **τ**, namely fraction of **τ** for which, an average, the system is defective (Relative Dead Time).

B.3 CLASSIFICATION OF COMPONENTS FAILURES

To determine the reliability of components produced industrially in large quantities (eg. electrical components, such as resistors, capacitors, transistors, etc.), we can do an experiment, putting them into operation simultaneously in a large number N_0 in the same conditions, according to the manufacturer's specifications (see Fig. B.1).

As shown in the upper part of Fig. B.1, the number of components in operation is reduced rapidly in the initial stage of the experiment; then the rate of decrease is stabilized for a long period of time to a minimum value, while it returns to increase towards the end of the life of the components. The graph shows clearly the three periods mentioned above, and their name:

0 - t1, "**trial stage**";
t1 - t2, "**useful life**";
> t2, "**usury**" or "**old age**."

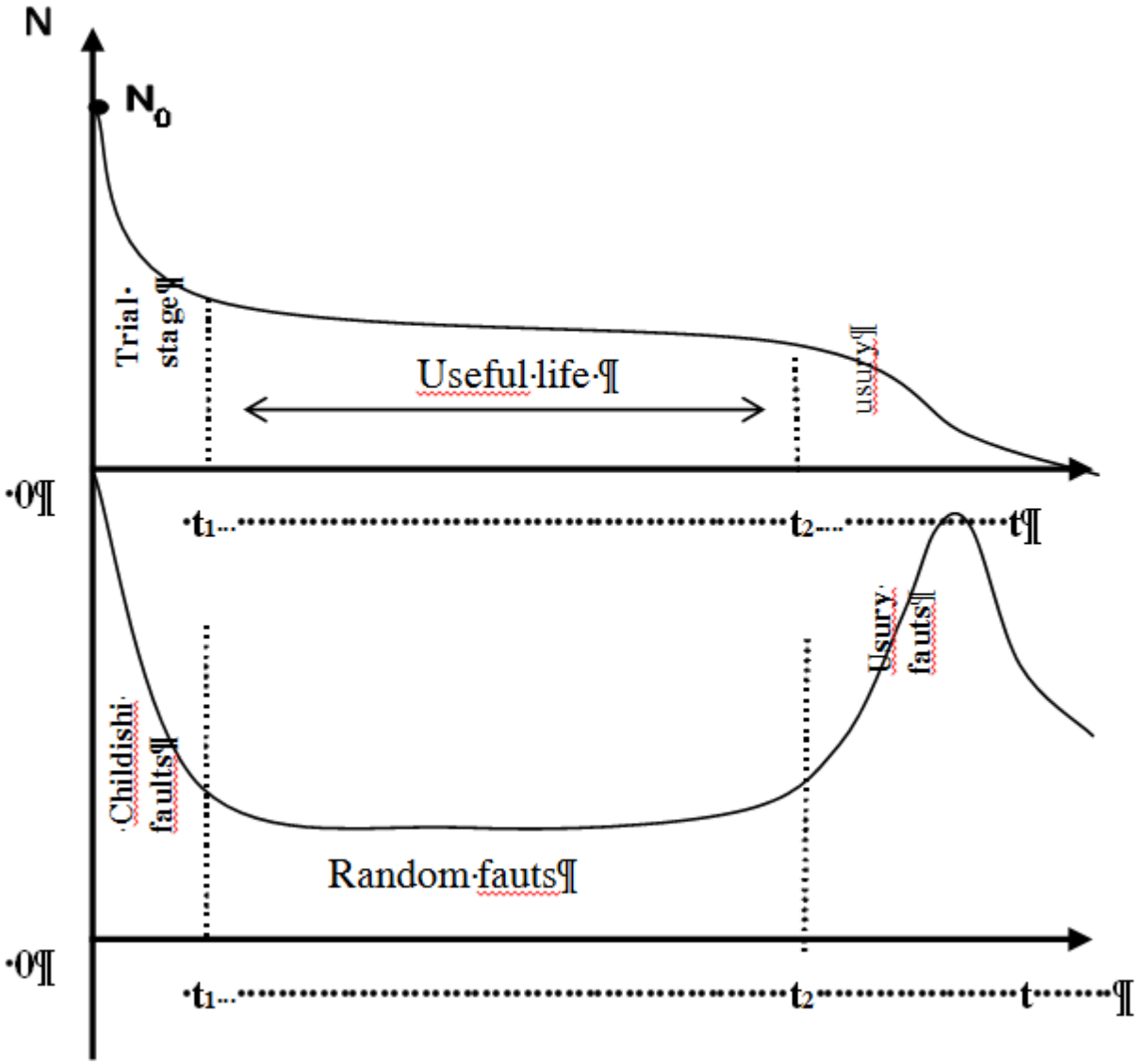


Fig. B.1 Periods characteristic of operation and corresponding failure classification of the components

According to the definition given in the previous paragraph, you can easily draw the trend of the corresponding failure rate λ as a function of time, shown in the lower part of the same Fig. B.1, It is the well-known curve "bathtub", leading to the classification component failures in:
"**childish**", due to defects and imperfections of construction that are evident readily during the break-in period, leading to the exclusion from the use of components that are affected;
"**random**", during the period of useful life, corresponding to a rate of fault minimum and almost constant;
"**usury**", during the corresponding period and due to the deterioration of the characteristics of the component by the stresses to which has been subjected during operation.

Previous observations imply that for optimum reliability, it is necessary to make a proper break-in components, using the same only during the period of useful life; consequently it is also necessary to perform maintenance operations programmed, by replacing the components which have reached the end of their useful life. Only by doing so you can rely on a minimum and also almost constant, in time, failure rate for the components used.

B.4.1 Non repairable components

Assuming, as usual engineering practice, that is possible to approximate the probability with the observed frequency (hypothesis acceptable if the statistical basis is sufficiently wide), the reliability is given by the relation:

$$R(t) = N / N_0 \qquad (B.1)$$

where N is the number of components "survivors" at time t, and N_0 is the initial number of components at the time t=0.

Similarly, the unreliability is expressed by the relation:

$$Q(t) = 1-R(t) = N_g / N_0 \qquad (B.2)$$

where N_g is the number of failed components between the initial instant and the generic time t.

Note that the two relationships listed above are valid for **non-repairable** components, or that, once they faults, remain in a state of failure for the whole duration of the observation.

The definition of the failure rate can be expressed with the relationship:

$$\lambda = \frac{1}{N}\frac{dN}{dt} \qquad \text{(B.3)}$$

from which, according to (1) is immediately obtained:

$$\lambda = -\frac{1}{R}\frac{dR}{dt} \qquad \text{(B.3')}$$

Solving:

$$R = \exp\left(-\int_0^t \lambda dt\right) \qquad \text{(B.4)}$$

and under the assumption that λ is constant over time:

$$R = e^{-\lambda t} \simeq 1-\lambda t \qquad \text{if } \lambda t << 1 \qquad \text{(B.4')}$$

According to the fundamental theorem of probability theory we therefore have:

$$Q(t) = 1 - e^{-\lambda t} \simeq \lambda t \qquad \text{if } \lambda t << 1 \qquad \text{(B.5)}$$

In the study of a system composed of non-repairable components (eg. missile, etc.), the probability that the system fails during the mission time τ will be given by $Q(\tau)$. Furthermore:

$$A(\tau) = R(\tau) \quad \text{and} \quad I(\tau) = Q(\tau) \qquad \text{(B.6)}$$

The assumption of constant (and minimum) failure rate is generally valid for units that have been passed the break-in period (elimination of defects "childish", namely due to defects in the construction, trivial errors, etc.) and are used during the period of "useful life", before they will overtake the usury. Using always process units in the period of useful life (and then by making systematic and scheduled maintenance, with units replacement at the end of their useful life), the mean time between failure period (**MTBF - Mean Time Between Failures**) is:

$$\mathbf{MTBF = 1/\tau} \qquad \text{(B.7)}$$

More generally one can demonstrate the validity of the following relationship:

$$MTBF = \int_0^{\infty} R(t)\,dt \qquad \text{(B.8)}$$

valid whatever the mathematical expression of R (t).

The previous definitions and relationships extends easily to the case of process units with cyclic operation, with the replacement of the MTBF with the average number of cycles of correct operation "c" (to be put in previous relationship (B.7) in place of $1 / \tau$).

B.4.2 Repairable components

Differently from the previous case (and most interest cases for the industry), the failing component is usually repaired (or replaced) and put back into operation. In this case, it becomes important the concept of **Mean Time To Repair (MTTR)**, namely the time interval during which the component remains in a fault state.
Similarly to the failure rate, it can be defined a repair rate m:

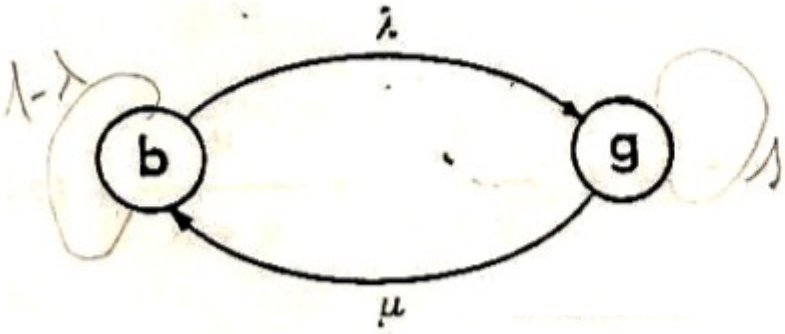
$$\mathbf{m = 1/MTTR} \qquad \text{(B.9)}$$

For repairable components the availability is therefore defined as:

$$A = MTBF / (MTBF + MTTR) \qquad \text{(B.10)}$$

and analogously the unavailability as:

$$\mathbf{I = 1 - A = MTTR / (MTBF + MTTR) = } \frac{\lambda}{\lambda + \mu} \qquad \text{(B.11)}$$



$$\frac{dP_b(t)}{dt} = -\lambda P_b(t) + \mu P_g(t)$$

$$\frac{dP_g(t)}{dt} = \lambda P_b(t) - \mu P_g(t) \qquad (11)$$

Assumendo come condizione iniziale $P_b(0)=1$ (cioè con probabilità 1 il sistema è funzionante a t=0), e risolvendo le equazioni (11), si ottiene:

$$A(t) = P_b(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

$$U(t) = P_g(t) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \qquad (12)$$

(notare che, per ogni valore del tempo t viene rispettata la condizione $P_b(t)+P_g(t)=1$).

We have already mentioned that an incident in a highly dangerous plant occurs only for the concomitant occurrence of a fault in the system process (demand) and the failure of the system for protection and safety. Hence the definition of "**unavailability**" of a safety and protection system such as **probability of non-intervention following a request of the process system**. In this way the probability of occurrence of an accident is given by the product of the probability of failure of the process system for the unavailability of the protection system. For protection system failures "fail to danger" unrevealed, it is easily to demonstrate that the unavailability for a mission time τ (interval between two successive tests, which can reveal the faulted protection system) is given by:

$$I = \frac{1}{\tau}\int_0^{\tau} Q(t)\,dt \qquad \text{(B.12)}$$

B5 RELIABILITY OF PROTECTION AND SAFETY SYSTEMS

For equipment and systems devoted to protection and safety, it is necessary to premise a further classification of types of failure:

- **faults in favor of safety** (fail safe), namely involving the intervention of the unit in the absence of a dangerous situation. In consequence of an intervention "fail safe", the plant changes state from that of normal operation to a situation of greater safety. This automatically reveals the failure of the unit.
- **faults to the detriment of safety** (fail to danger), which involve the non-availability of a unit in the event that it be called to operate as a result of a failure (demand) of the process system.

The faults fail to danger can be **revealed** (and in such case promptly repaired) or **not revealed**; in the latter case they can be detected only by a request of the process system (which cannot be satisfied and therefore result in an incident) or from an ad hoc test at the end of the mission time. Clearly, as the risk of incidents arises mainly from occurrence of faults fail to danger, the designer puts a certain cure in minimizing the relative failure rate, particularly for faults not revealed.

We have already mentioned that an incident in a highly dangerous plant occurs only for the concomitant occurrence of a fault in the system process (demand) and the failure of the system for protection and safety. Hence the definition of "**unavailability**" of a safety and protection system such as **probability of non-intervention following a request of the process system**. In this way the probability of occurrence of an accident is given by the product of the probability of failure of the process system for the unavailability of the protection system. For protection system failures "fail to danger" unrevealed, it is easily to demonstrate that the unavailability for a mission time τ (interval between two successive tests, which can reveal the faulted protection system) is given by:

$$I = \frac{1}{\tau}\int_0^{\tau} Q(t)\,dt \qquad \text{(B.12)}$$

Ultimately this relation expresses the fact that I is the average value of Q (t) within the mission time. I is also equal to the Relative Dead Time, namely the fraction of the time τ for which on average the protection system is broken:

$$I = \frac{1}{\tau}\int_0^{\tau} (\tau - t)\,dQ \qquad \text{(B.13)}$$

In the previous relation dQ is the probability that the protection system fails at a generic instant t, in which case remains faulted for the remaining interval (t-τ).

In the case of a protection system with exponential reliability:

$$Q(t) = 1 - e^{-\lambda t} \simeq \lambda t \qquad \text{if } \lambda t << 1$$

And:

$$I = \frac{1}{\tau}\int_0^{\tau}(1 - e^{-\lambda t})\,dt \simeq \frac{1}{\tau}\int_0^{\tau}\lambda t\,dt = \frac{1}{2}\lambda\tau \quad \text{(B.14)}$$

In the previous expression it is implicitly admitted that the tests are all perfect and of infinitesimal duration (namely negligible compared to τ). With this hypothesis would be sufficient to reduce the time interval between two tests to reduce accordingly, as you want, the unavailability of the protection system, in accordance with (B.14). At the limit, by tending τ to zero, I also tends to zero, against the obvious conclusion that if a system of protection is constantly under test, it is never available to perform its function (and therefore has unavailability equal to 1).

Introducing the test duration τ_t (and including in τ_t the repair time when the test reveals a fault), the previous relationship becomes:

$$I = \frac{1}{2}\lambda\tau + \frac{\tau_t}{\tau} \qquad \text{(B.15)}$$

given the fact that during the test the system is not available and its Q is 1. The latter relationship is suitable to an optimization of the interval between two successive tests; The minimum is obtained deriving equation (B.15) and putting the derivative to 0:

$$\frac{dI}{d\tau} = \frac{1}{2}\lambda - \frac{\tau_t}{\tau^2} = 0 \qquad \text{(B.16)}$$

from which:

$$\tau_0 = \sqrt{\frac{2\tau_t}{\lambda}} \qquad \text{(B.17)}$$

By substituting this optimum mission interval in (B.15), we have:

$$I_m = \lambda\tau_0 = \sqrt{2\lambda\tau_t} \qquad \text{(B.18)}$$

Previous conclusion is consequence of the hypothesis of perfect testing (which do not introduce faults). This hypothesis can be removed, assuming that λ is function of the number of tests and increases by increasing the number of tests:

$$\lambda = \lambda_o \, . \, f(\tau) \qquad \text{(B.19)}$$

The simplest expression for (B.19) is

$$\lambda = \lambda_o . \left(1 + \frac{K}{\tau} \right) \qquad \text{(B.19')}$$

that, by substituting in (B.16), leads to the relationship:

$$I = \frac{1}{2} \lambda_0 \tau + \frac{\tau_t}{\tau} + \frac{K \lambda_0}{2} \qquad \text{(B.20)}$$

To conclude this section we have to treat the case of a system malfunction fail to danger revealed. The solution of the problem is immediate, remembering that unavailability is equal to the Relative Dead Time and therefore the relationship (B.11) holds, already seen in the case of repairable parts. In addition it is implicit the assumption that the plant continues to be operated during the repair time. In the case of installations with a high hazard, this can be admitted only if there are other safety systems capable of carrying out the function performed by the system under repair.