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:

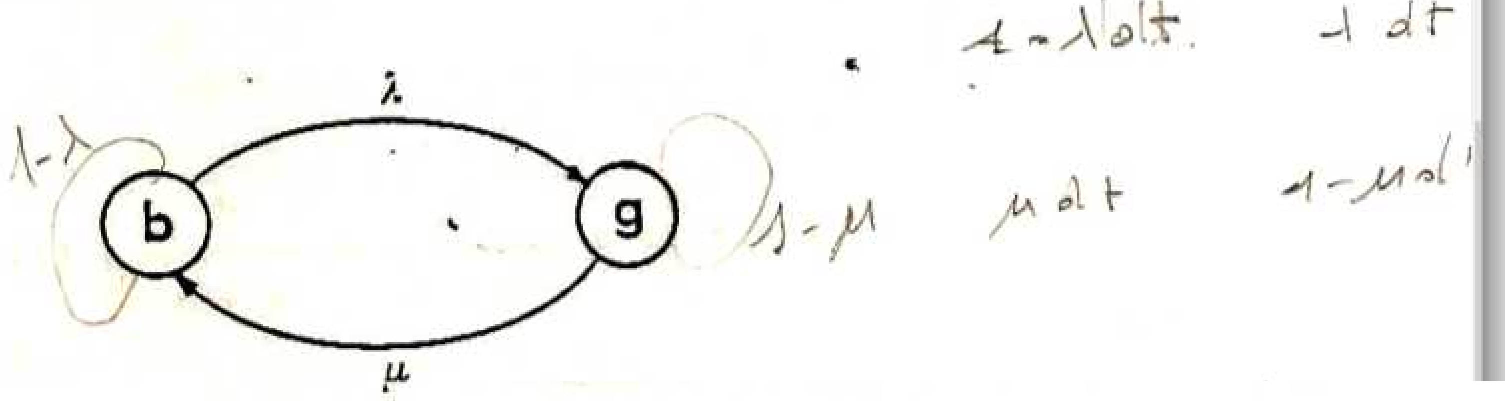
$$\mathbf{m = 1/MTTR} \tag{B.9}$$

For repairable components the availability is therefore defined as:

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

and analogously the unavailability as:

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



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

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

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).

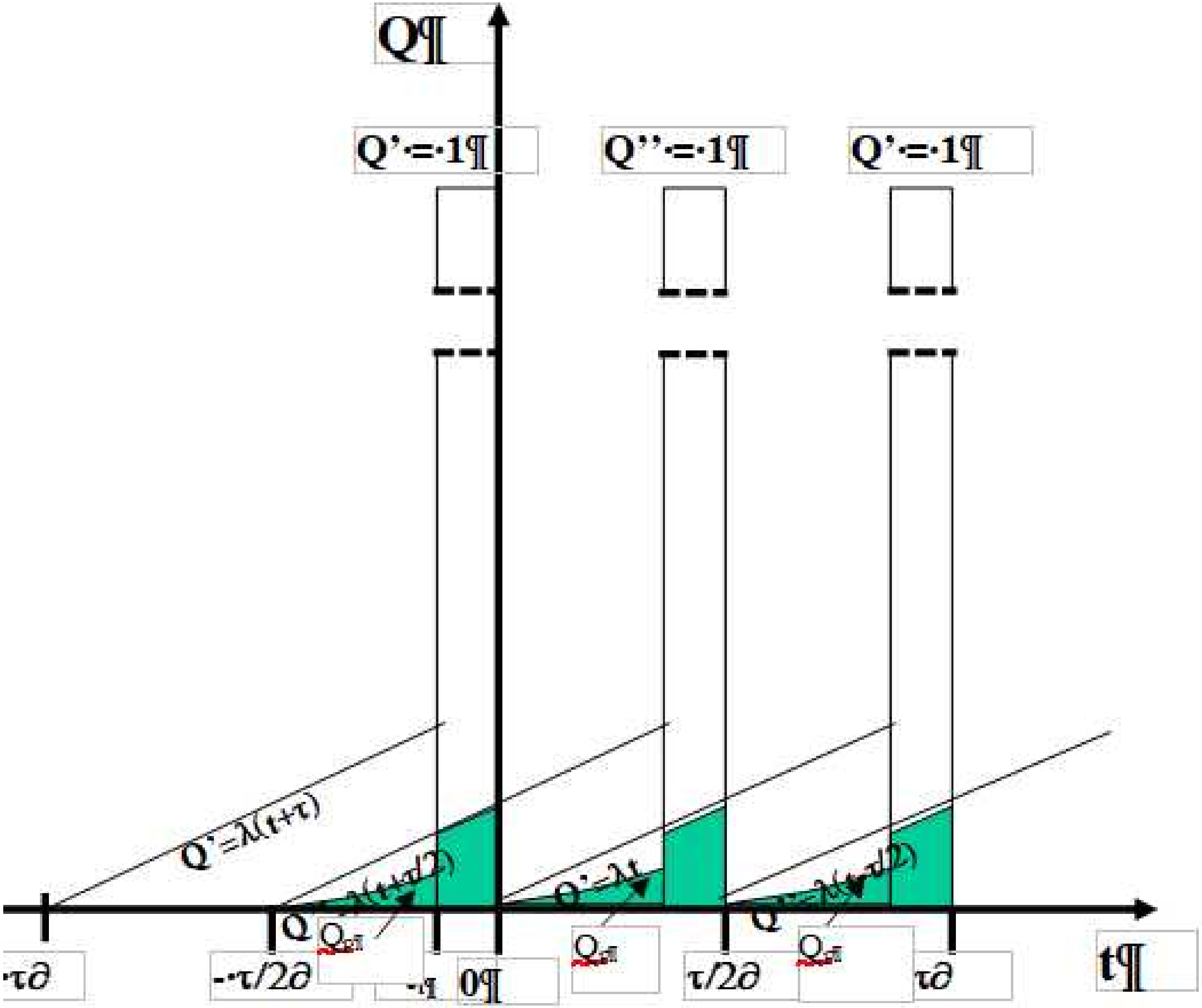
In the case of a protection system with exponential reliability:

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

And:

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

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).


Q¶
Q'=·1¶
Q''=·1¶
Q'=·1¶
Q'=λ(t+τ)
Q'=λ(t+τ/2)
Q'=λt
Q'=λ(t-τ/2)
Q
Q
Q
Qo¶
Qo¶
Qo¶
·τ∂
-·τ/2∂
-·¶
0¶
τ/2∂
τ∂
t¶

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:

$$\lambda = \lambda_{0\ .\ f\ (\tau)} \qquad \text{(B.19)}$$

The simplest expression for (B.19) is

$$\lambda = \lambda 0 . \left(1 + \frac{K}{\tau}\right) \qquad \text{(B.19')}$$

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.