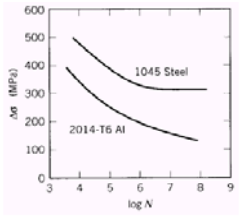
Affidabilità

Si parla di affidabilità (*reliability*) riferendosi a un sistema o a un suo componente o anche a una persona. Essa è associata al concetto di buon funzionamento.

L'affidabilità può essere definita come la probabilità che un sistema o un suo componente funzioni per un certo tempo, se usato in condizioni normali (predefinite).

Negli anni trenta il concetto di affidibilità era essenzialmente intuitivo, soggettivo e qualitativo. Forse la sola eccezione a questo esisteva in ingegneria meccanica ove i fenomeni di fatica dei materiali metallici cominciavano ad essere compresi quantitativamente.
(diagrammi S – N, o di Wöhler)



$S-N$ curves for aluminum and low-carbon steel

La formulazione rigorosa e probabilistica inizia negli anni quaranta, spinta dall'industria aeronautica, dai militari e, più tardi, dall'industria dell'energia nucleare.

Funzione di affidabilità (*Reliability function*)

Se la variabile aleatoria T rappresenta il tempo dopo il quale un elemento cessa di funzionare e $f(t)$ è la densità di probabilità di T, la probabilità che l'elemento abbia cessato di funzionare al tempo t è definita da

$$Pr(T \le t) = \int_0^t f(x)\,dx = F(t)$$

$F(t)$ è la funzione di distribuzione che rappresenta la **non affidabilità**

La funzione di affidabilità (***reliability function***) è definita da

$$R(t) = Pr(T > t) = \int_t^\infty f(x)\,dx = 1 - F(t)$$

Mean Time To Failure, MTTF

Tempo durante il quale ci si aspetta che l'elemento funzioni:

$$E(T) = \int_0^\infty t\, f(t)\,dt$$

Se il sistema è l'oggetto di controlli e riparazioni regolari si parla di ***M**ean operating **T**ime **B**etween **F**ailures. **MTBF***

Failure Rate, FR

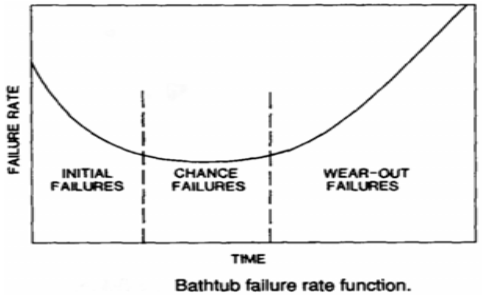
Probabilità che ci sia un guasto per unità di tempo nell'intervallo $[t_1, t_2]$, nell'ipotesi che non ci siano stati guasti prima di t_1

$$FR[t_1, t_2] = \frac{R(t_1) - R(t_2)}{R(t_1)} \frac{1}{t_2 - t_1}$$

Quando l'intervallo è breve la *FR* diventa una funzione

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

L'utilità della funzione di *FR* è che indica le variazioni di tendenza ai guasti durante la vita di una popolazione di sistemi.



Bathtub failure rate function.

Supponiamo che una lampadina debba essere sempre accesa e cerchiamo di capire come avvengono i guasti, facendo l'ipotesi che una lampadina guasta possa esser subito sostituita da una nuova, dello stesso tipo.

In seguito definiamo una **strategia di riparazione o servizio**.

I modelli più comuni sono:

Modello esponenziale
Il tempo tra guasti successivi ha una distribuzione esponenziale di parametro λ

$$f(t;\lambda)=\lambda e^{-\lambda} \qquad t\geq 0 \quad \lambda>0$$

ove λ è la *failure rate,* costante.

Modello di Weibull
Il tempo tra guasti successivi ha una distribuzione a due parametri e una *failure rate* proporzionale a una potenza di t .

Si possono scegliere diverse strategie per assicurare un buon funzionamento e controllare i costi, per esempio:

- **sostituire** la lampadina **subito** appena si guasta
- **sostituire** la lampadina ad **intervalli regolari**
- **verificare** il funzionamento della lampadina ad **intervalli regolari** e sostituirla se necessario
- **verificare** il funzionamento della lampadina ad **intervalli aleatori** (con distibuzioni di probabilità adeguate) e sostituirla se necessario

Le tecniche di previsione possono essere molto sofisticate e si basano sulla conoscenza delle caratteristiche del materiale e su stime probabilistiche, in particolare sulla teoria del rinnovamento (*renewal theory*).

Rinnovamento

Ritornando alla lampadina, supponiamo che le vite delle lampadine $L_1, L_2, L_3, \ldots$ siano independenti e abbiano la stessa distribuzione di probabilità.

Indichiamo con $N(t)$ il numero di sostituzioni, chiamati **rinnovamenti** (*renewals*), avvenute fino al tempo t . L'insieme delle variabili aleatorie $N(t)$ per $t\geq 0$ descrive un **processo di rinnovamento**.

Le quantità $R_i=L_1+L_2+\ldots+L_i$ sono i tempi di rinnovamento.

Il processo possiede la proprietà che si ricomincia a contare il tempo ad ogni rinnovamento, dimenticando il passato, proprietà tipo catena markoviana.

Qualunque sia la distribuzione di probabilità della vita L , quando si osserva una lampadina ad un certo momento durante la sua vita, si può definire una sua **età** e stimare una **vita residua**: si dimostra che età e vita residua hanno la stessa distribuzione di probabilità collo stesso valor medio

$$E[eta']=E[vita\,residua]=\frac{E[L^2]}{2E[L]}=\frac{\sigma_L^2}{2E[L]}+\frac{E[L]}{2}$$

La somma dei valori medi di età e vita residua $\frac{\sigma_L^2}{E[L]}+E[L]$

è **superiore** al valor medio $E[L]$ della vita L , salvo se $\sigma_L=0$

Questa incongruenza apparente è dovuta al fatto che si interviene in una vita che è già trascorsa in parte e quindi non può essere brevissima: si favoriscono vite più lunghe. (*length biasing, inspection paradox, bus paradox*)

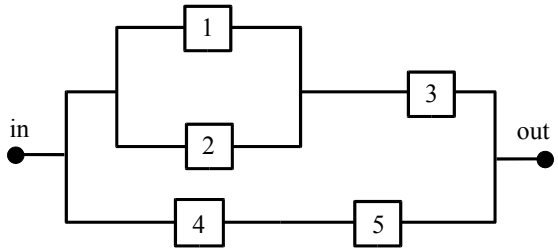
Nel caso di un sistema composto da tanti elementi, l'affidabilità dipende anche dalla topologia delle interconnessioni.

Le affidabilità di elementi in serie (4 e 5) si moltiplicano:

$$R_{45} = R_4 R_5$$

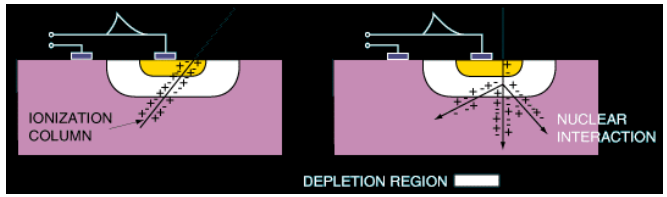
Le affidabilità di elementi in parallelo (1 e 2) si compongono:

$$R_{12} = 1 - (1 - R_1)(1 - R_2)$$



Single Event Upset (SEU)

L'impatto di una particella ionizzante su un circuito elettronico può provocare un impulso cambiando la forma dei segnali analogici o lo stato dei circuiti digitali (***single event upset***).
Può anche indurre un percorso di conduzione che provoca un corto circuito interno (***single event latch-up***) e eventualmente un danno permanente (***single event burnout***).



Ognuno di questi incidenti ha un effetto sull'affidabilità e si devono trovare accorgimenti per ridurre i danni.

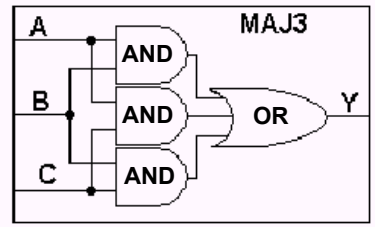
E' necessario analizzare l'importanza dei danni a:

- segnali analogici, es. carica in un pixel sbagliata
- segnali digitali, es. un bit in una memoria cambiato
- valori di controllo dell'elettronica, es. tensione di soglia cambiata, momentaneo o permanente
- programmi dei processori locali, es.programma in un FPGA alterato

Rimedi:

- Mettere gli elementi critici fuori portata (costo, latenza etc.)
- Progettare circuiti più tolleranti ai SEU a livello degli ASIC
- Progettare sistemi intrinsecamente più sicuri

L'accorgimento più comune per neutralizzare i **SEU** in circuiti digitali è il ***voting***: il segnale è triplicato e mandato in un circuito a maggioranza che richiede almeno 2 su 3.



L'accorgimento per limitare *single event latch-up* e *burnout* è di misurare la corrente di alimentazione con un circuito indipendente e spegnere momentaneamente l'alimentazione quando la corrente diventa eccessiva.

Single event chip burnout

Referenze

Teoria del **rinnovamento**

- R. Nelson, Probability, Stochastic Processes and Queuing Theory, Springer Verlag, 1995

- A. Berger, Discrete Stochastic Processes, MIT course 6.692, spring 1999
http://lids.mit.edu/~awberger/6.262/schedule-lectures.html

SEU, SEL etc.

- G. Anelli, A. Marchioro, The future of rad-tol electronics in HEP, Snowmass 2001
http://snowmassserver.snowmass2001.org/Working_Group_E7/www/talks/marchioro.pdf

- G. Anelli, Radiation-hard circuits in deep submicron CMOS technology, BNL Seminar 2004
https://www.inst.bnl.gov/seminars/PDF/04212004.pdf