Tecnica biomedica 2

> Affidabilità dei sistemi

- Generalmente l'analisi dei sistemi dal punto di vista dell'affidabilità (capacità di svolgere una determinata funzione) è legata a considerazioni

  > tecniche
  quando è messa in gioco la stessa possibilità di funzionamento, come nel caso del calcolatore a valvole.

  > economiche
  perché il mancato funzionamento si può sempre associare a un costo, come pure ogni collaudo o verifica

- Nel caso di sistemi biomedici destinati a svolgere funzioni per il sostentamento della vita, a questi motivi se ne aggiungono altri di carattere <u>etico</u> e <u>giuridico</u> che entrano a far parte della responsabilità del progettista. (vedi scritta sui manuali riguardo alle funzioni life-support).

- Per parlare di affidabilità occorre capire che cosa è il fenomeno che limita la capacità di svolgere una funzione: il guasto

  - Ogni difformità del comportamento del sistema e del valore dei suoi parametri da quanto stabilito dalle specifiche si può chiamare GUASTO.
  - Esiste una vasta possibilità di classificazione dei guasti, in funzione del modo, delle cause, delle modalità di insorgenza. In particolare si dicono

(1) modo:
- PARAMETRICI: degradazione soft delle specifiche: qualche valore esce dalle tolleranze previste dal progetto
- CATASTROFICI: la funzione non viene svolta affatto

La distinzione può sempre in teoria sottile
Quando è rotta una resistenza da 1kΩ 5%?

0Ω — 500Ω — 1kΩ — 1500Ω — ∞Ω

(2) generi

- SISTEMATICI: si presentano in tutti gli esemplari R1.1b del sistema; praticamente errori di progetto (hw, sw) sfuggiti alla fase di Debug.
- OCCASIONALI: Presenti in una particolare realizzazione, sono dovuti al processo di realizzazione o agli stress durante la vita operativa.

in sogg. (3)

- PERMANENTI: le guasto c'è e ci resta
- TEMPORANEI
  - TRANSITORI: indotti da particolari e eccezionali condizioni operative spariscono senza lasciare tracce (?!?)
  - INTERMITTENTI: vanno e vengono in modo casuale - Generalmente evidenziano una criticità del progetto o una transizione verso il guasto permanente.

- Occorre poi tradurre il problema in termini quantitativi per poter eseguire analisi e adottare strategie corrette di progetto. L'approccio è di tipo STATISTICO.
  - > Viene definita una variabile aleatoria e le sue principali statistiche
    - τ: tempo di vita
    - $y_\tau(t)$: densità di probabilità
    - $Y_\tau(t)$: distribuzione
    - $E\{\tau\}$: aspettazione di vita o
      MTF (tempo medio al guasto)
      MTBF (tempo medio tra guasti, per sistemi ripristinabili)
  - > In particolare si definisce
    - $R(t)$: affidabilità, probabilità di un tempo di vita superiore a t. (tempo di missione)

    Si ha

$$R(t) = \int_t^\infty y_\tau(t)\,dt = 1 - Y(t)$$

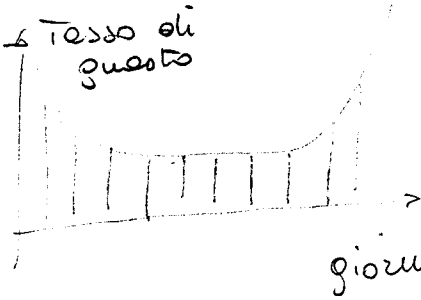
- Come si vede si tratta di parametri probabilistici, che possono essere desunti con metodi statistici da esperimenti reali.

> Un esperimento che per sistemi complessi e articolati porta a un risultato caratteristico è il seguente:

- si individua una popolazione di numerosi esemplari di un certo sistema
- si controlla nel tempo il numero di quelli che si rompono e di quanti continuano a funzionare
- si rapporta il numero di sistemi rotti in un certo periodo con il totale dei funzionanti all'inizio del periodo.

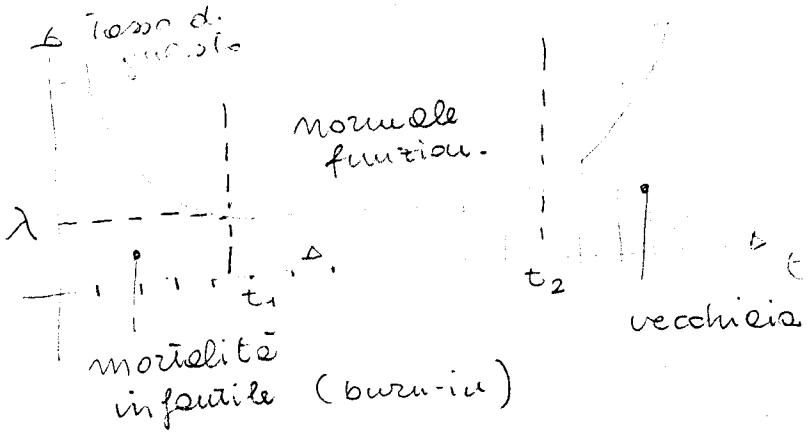
Esempio

giorno	Funzion	Guasti	Tasso di guasto
	100	0	~
1	80	20	20%
2	70	10	12.5%
3	65	5	7.14%
4	61	4	6.15%
5	57	4	6.56%
6	53	3	5.26%
7	50	3	5.66%
8	47	3	6%
9	44	3	6.38%
10	41	2	4.55%
11	39	3	7.32%
12	36	6	15.4%
13	30	10	27.8%
14	20	15	50%
15	5	5	~
16			



- Queste osservazioni danno origine a una curva caratteristica, detta a VASCA da BAGNO dove si riconoscono tre regioni

$S(t, \Delta)$



- L'individuazione di questa curva con la valutazione di t_1, t_2 e soprattutto λ può dare indicazione sul valore dei parametri probabilistici

> Questo è alla base di ogni procedimento statistico, che opera attraverso meccanismi di coerenza interna. I parametri probabilistici "stimati" ci permettono di risalire al grado di probabilità di una certa osservaz. che viene detto "grado di confidenza".

> Nel nostro caso, cosa indica $\Delta S(t, \Delta)$?
Può essere considerato uno "stimatore" dell'evento
{ guasto in $t, t+\Delta$ | dato che in t il dispositivo OK}

La probabilità di questo evento si può scrivere come

$$\frac{Y_z(t+\Delta) - Y_z(t)}{1 - Y_z(t)} = \Delta S(t, \Delta)$$

se l'intervallo Δ è sufficientemente piccolo si può scrivere

$$S(t) = \frac{1}{R(t)} \lim_{\Delta \to 0} \frac{Y_z(t+\Delta) - Y_z(t)}{\Delta} = -\frac{R'(t)}{R(t)}$$

- La conoscenza della curva a vasca, nel tratto di normale funzionamento, ci dice che $S(t)$ è costante per cui possiamo risolvere l'equazione differenziale.

• Si ha

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

$$\frac{dR(t)}{dt} + \lambda R(t) = \emptyset \qquad \text{omogenea. Da cui}$$

$$R(t) = e^{-\lambda t} \qquad \text{per } t \geq 0 \text{ e } 1 \text{ altrove}$$

dovendo essere $R(0) = 1$ per ovvi motivi.

• Immediatamente, in queste ipotesi, si ha

$$\left.\begin{aligned} Y_z(t) &= 1 - e^{-\lambda t} \\ y_z(t) &= \lambda e^{-\lambda t} \end{aligned}\right\} \text{ per } t \geq 0 \text{ e } 0 \text{ altrove}$$

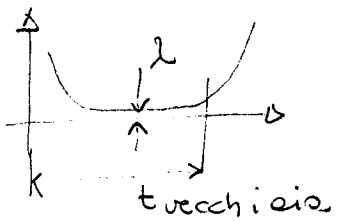
• Interessante valutare l'aspettazione di vita o MTF

$$E\{\tau\} = \int_0^\infty x\, y_z(x)\, dx = \lambda \int_0^\infty x e^{-\lambda x} dx = \qquad \text{per parti}$$

$$= \lambda \left\{ -\frac{x e^{-\lambda x}}{\lambda} \Big|_0^\infty + \int_0^\infty \frac{e^{-\lambda x}}{\lambda} dx \right\} = \frac{1}{\lambda}$$

• È importante ricordare sempre che questo risultato vale solo per il normale funzionamento, quando il tasso di guasto è costante (cioè per $t < t_{vecchiaia}$).

Può accadere che MTF > tvecchiaia : significa solamente che ci sarà un bassissimo numero di guasti accidentali prima del periodo di degenerazione finale



Osservazione: l'aspettazione di vita non mi dice che senz'altro il tale sistema vivrà MTF anni. In fatti

$$R\left(\frac{1}{\lambda}\right) = e^{-1} \qquad 36.8\,\%$$

PS: quando si dice che l'uomo ha una aspettazione di vita di 76 anni, si fa riferimento a una $R(t)$ che COMPRENDE il fenomeno della vecchiaia (sarebbe

- Valutazione dell' MTF di sistemi complessi, ottenuti combinando sottosistemi di cui sia nota l'affidabilità.

> Sistema SERIE : la rottura di un pezzo blocca tutto

$$P\{t>t_0\} = P\{t_1>t_0 \text{ e } t_2>t_0\} = R_1(t)\cdot R_2(t) \quad \text{se indipendenti}$$

caso esponenziale

$$R(t) = e^{-(\lambda_1+\lambda_2)t} \qquad MTF = \frac{1}{\frac{1}{MTF_1}+\frac{1}{MTF_2}} \quad \text{(formula del //)}$$

> Sistema PARALLELO : un pezzo rotto può essere rimpiazzato da un altro che ne svolge la funzione

$$P\{t>t_0\} = 1 - P\{t_1<t_0 \text{ e } t_2<t_0\} = 1 - Y_1(t)\,Y_2(t) = R_1 + R_2 - R_1R_2$$

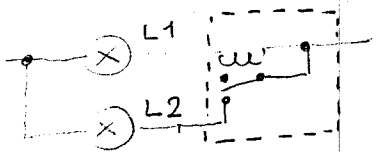
caso esponenziale

$$R(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}$$

$$MTF = MTF_1 + MTF_2 - \frac{1}{\frac{1}{MTF_1}+\frac{1}{MTF_2}}$$

è senz'altro maggiore di ciascuna delle due

ES:



se L1 brucia, L2 viene inserita dal relè (la cui affidabilità si considera ∞)

> Sistemi misti più complessi : le modalità di auto-riconfigurazione possono essere più complesse e non direttamente assimilabili a serie e parallelo. Occorre ricostruire la statistica del tempo di vita globale

componenti indipendenti				Esito
1	2	3	4	
OK	OK	OK	OK	OK
OK	OK	OK	–	OK
OK	OK	–	OK	–

gli eventi sono disgiunti e le relative probabilità note.

- Per i grossi sistemi idraulici (non di supporto alla vita) si può costruire una teoria analoga che però tenga conto della possibilità di riparazione.

  Si ha così la variabile duale

  τ_r : Tempo di riparazione (in cui il sistema resta guasto.)

  $m_\tau(t)$: densità

  $M_\tau(t)$: distribuzione (Manutenibilità)

  > Lo studio delle statistiche di τ e τ_r permette di valutare la DISPONIBILITÀ di una grande apparecchiatura e impostarne efficaci strategie per la manutenzione.

- Progettazione per l'affidabilità. (cenni)

  Non è affatto banale progettare sistemi che siano affidabili - Soprattutto l'affidabilità non è qualcosa che si attacca dopo all'oggetto finito.
  Riguarda tutta la vita del sistema

  > Progettazione
  > Produzione (es: ISO9000)

  Qualità: controllo completo di TUTTO il processo produttivo
  definizione delle procedure
  considerazione del fattore umano
  rilevamento costante dei parametri di qualità

- Torniamo alla progettazione.
  Esistono diverse filosofie, non in alternativa, per affrontare questo tema.

  > Migliorare la collaudabilità
  È un passo ineludibile - Qualsiasi strategia per avere sistemi affidabili prevede una fase di DIAGNOSI.
  Si migliora la collaudabilità di un sistema per due vie

  - Migliorare controllabilità e osservabilità dei singoli sottosistemi
    - Partizionamento in sottoblocchi fisicamente individuabili e accessibili
    - JTAG e simili

- Aggiungere direttamente sul sistema ulteriore HW+SW con l'unico scopo di eseguire test di funzionamento (built-in testing)
  - ☐ Fase iniziale del boot di ogni calcolatore
  - ☐ Verifica dei fine corsa e di ogni elemento dotato di feedback attuatore-sensore.

> Capacità di autodiagnosi (self-checking)

Il successivo passo prevede la capacità del sistema di autoverificare il corretto comportamento DURANTE il normale modo operativo.

Questa capacità si può ottenere

- Con un abbondante "inserimento" del sistema con sensori che verifichino la congruenza dello stato del sistema con quanto impostato
- Con l'uso di codifiche per l'informazione nel sistema ridondanti e "preservate" dalle operazioni eseguite dagli elaboratori previsti (CRC, parità) e dei checker.

> Possibilità di indirizzare il sistema guasto verso un comportamento di "minimo danno"

(fail-safe)

- Per esempio, un interruttore si può rompere in due modi: ① non fa più contatto ② i contatti si incollano e vanno in corto

  L'ipotesi ① è considerata più "safe" della ② e orienta le tecniche costruttive di interruttori e relè.

> Realizzazione di sistemi tolleranti i guasti.

Tali sistemi riescono a compiere la loro missione anche in presenza di uno o più guasti. Perché ciò sia possibile il sistema deve

- Avere capacità di autodiagnosi
- Avere possibilità di autoconfigurarsi (ridondanza hardware)
- Avere possibilità di autocorreggersi (ridondanza nei codici e nel software)

Si può pensare anche a "graceful degradation..."

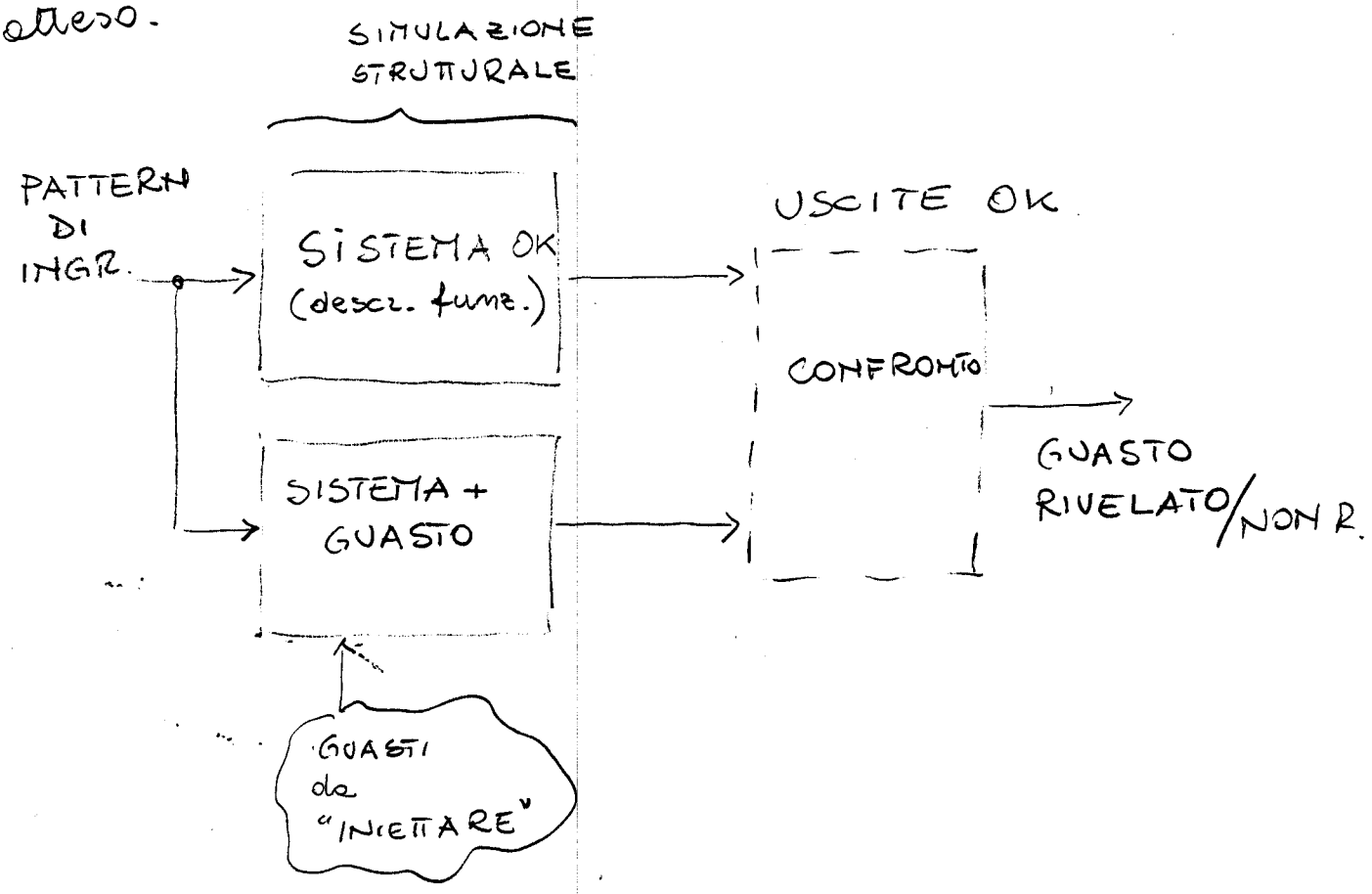
MIGLIORARE LA COLLAUDABILITÀ

> Concetto di MODELLO di guasto

→ Per poter trattare il collaudo in modo rigoroso, occorre avere un modello preciso del guasto che permetta di predirne gli effetti sul sistema.

→ La presenza di un guasto (di ogni guasto potenziale) deve poter essere descritta in modo formale e data in pasto a un SIMULATORE.

→ Rivelare un guasto vuol dire dare una sequenza di ingressi (opportuna) e osservare in uscita un comportamento diverso da quello atteso.



→ Esempio dei circuiti digitali: modello di guasto logico "STUCK AT" (LINEA FISSA)

0

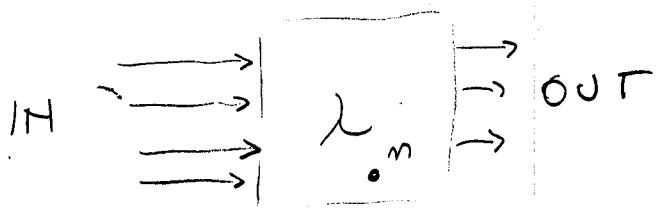
• Vantaggi -

1) Data la descrizione strutturale di un circuito, l'insieme dei guasti è ben definito e limitato
2) Uno STUCK non può creare effetto memoria (cioè una rete COMBINATORIA non può diventare SEQUENZIALE)

• Svantaggi
NON è molto aderente alla realtà fisica degli odierni circuiti CMOS

> OSSERVABILITÀ e CONTROLLABILITÀ in reti combinat.

$OUT = \lambda(IN)$



↑ SINGOLO GUASTO n STUCK at Ø

* è controllabile se $\boxed{\exists\ IN \Rightarrow (n=1)}$ insieme $IN_{n=1}$
la controllabilità sarà $\frac{IN(n=1)}{IN\ totali}$

* Se stacchiamo n da tutte le porte che esso pilota e forziamo questo valore dall'esterno abbiamo

$$OUT' = \lambda_n(IN, n)$$

Sarà

$$OUT = n\,\lambda_n(IN,1) + \bar{n}\,\lambda_n(IN,0)$$

E' osservabile se $\exists\ IN \Rightarrow$

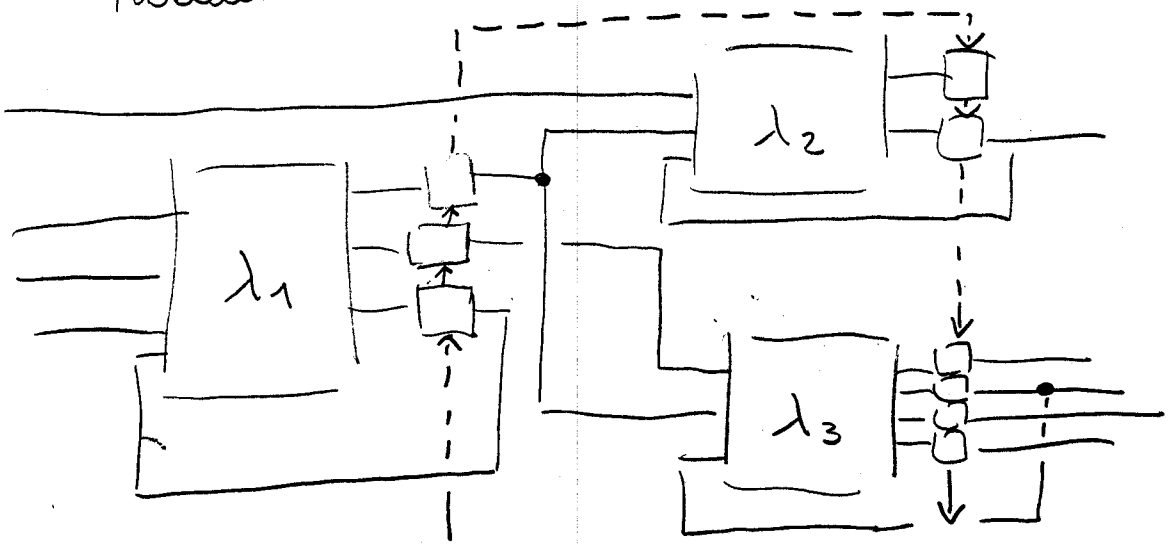
$$\lambda_n(IN,1) \neq \lambda_n(IN,\emptyset)$$

→ Per RIVELARE occorrono entrambe le condizioni.

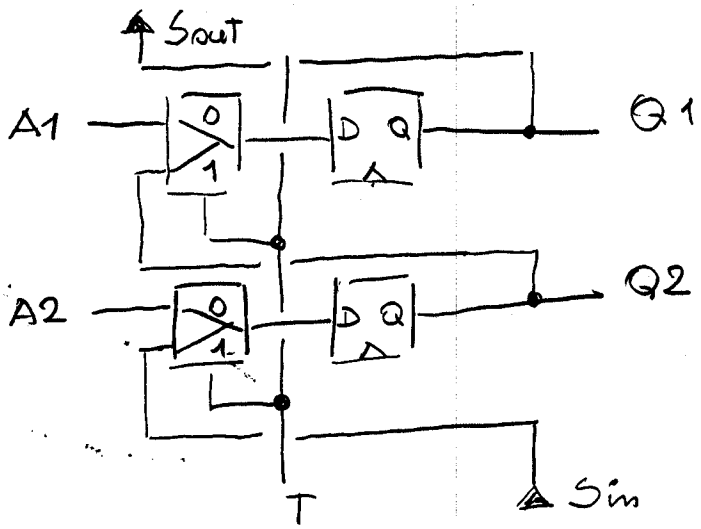
> Come collaudare reti SEQUENZIALI

→ occorre avere accesso allo STATO della macchina
→ interrompere lunghi contatori
→ le concetto di scan-path

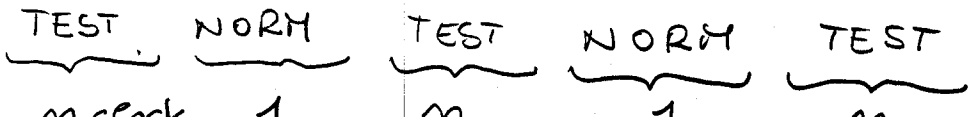
Modello di macchina sequenziale



TUTTI i registri che contengono lo stato interno hanno un collegamento ausiliare (pilotato da un ingresso indipendente T) che li fa diventare un UNICO SHIFT-REGISTER



Il collaudo così può essere riportato a quello dello shift + 3 reti combinatorie



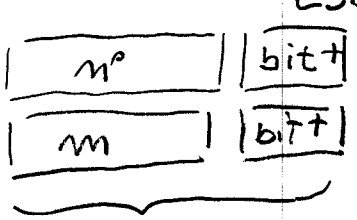
> Altri esempi di BUILT-IN testing

- Presenza di generatori di segnali di prova per la verifica di interi sistemi di misura
- Programmi diagnostici
- Coerenza tra più sistemi collegati alla stessa grandezza

  Es: sistema sensore di posizione accurato (assoluto) + rivelatori di 0 e fine corsa
- Sistemi in grado di eseguire DUMP in caso di eccezioni

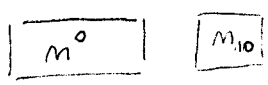
  Es: praticamente tutti i DSP delle ultime generazioni
- Uso di codifiche con ridondanza "chiuse" rispetto alle operazioni di interesse

  Es: parità rispetto alle operazioni di max/min (bit aggiunti come LSB)



$n \leq m$ ⟶ eseguite sul numero complessivo danno lo stesso risultato che fanno su n e m.

- prova del "nove".



(in binario $2^n - 1$)*

3847	4
1294	7 ↓

Somma
Prodotto $+5141 \rightarrow (2)$

$\times 497{,}8018 \rightarrow (1)$

• AUTODIAGNOSI

> Cosa ha oltre il built-in
ATTIVA durante il NORMALE Funzionamento

Simile al mostro "Mi sento male"

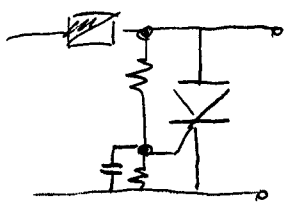
> Esempio dei sistemi con "watch dog":
un sistema INDIPENDENTE osserva il comportamento del sistema principale e intraprende eventuali azioni nel caso rilevi comportamenti anomali.

PACE MAKER

> Il concetto di TIME-OUT per i processi che dovrebbero (se tutto va bene) arrivare a compimento in un tempo noto

• FAIL SAFE esempi

- Fusibile
- Circuiti di crowbar
- Valvole delle caffettiere (fondono a 110°C)
- Semafori → giallo lampeggiante
- Scocche a deformazione progressiva



(Scaricatori di sovratensione)

- FAULT TOLERANT esempi

  - Doppi circuiti frenanti (HW)
  - Doppie euci di stop (HW)
  - Codici a correzione d'errore (SW)
    (dischi o nastri, canali disturbati)

Esempio di codice che rivela e corregge il singolo errore e rivela il doppio in $(m \times n)$ bit utili

x	x	x	x	0
x	x	x	x	0
x	x	x	x	0
x	x	x	x	0
0	0	0	0	0

} n righe +1 di parità in verticale

m colonne +1 di parità in orizzontale

- Reni, polmoni
- Doppia campana nel proiettore ...