Introduzione ai sistemi tolleranti ai guasti

M. Favalli

Engineering Department in Ferrara

Tolleranza ai guasti

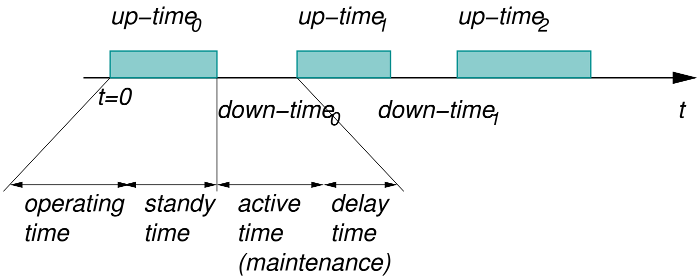
La tolleranza ai guasti é uno dei principali strumenti per risolvere i problemi di affidabilitá che gli attuali sistemi digitali presentano sia dal punto di vista delle tecnologie che delle applicazioni
In questa parte del corso vedremo inizialmente un modello dell'affidabilitá per poi illustrare le diverse tecniche di tolleranza ai guasti

Utilizzo della tolleranza ai guasti

- Applicazioni (aerospaziale, trasporti, biomedico, telecomunicazioni) che richiedono elevati livelli di dependability
- *Dependability*:
  - *reliability*: continuitá di servizio
  - *availability*: prontezza di utilizzo
  - *safety*: capacitá di evitare conseguenze catastrofiche
  - *security*: capacitá di preservare l'integritá e la confidenzialitá dei dati

Operazioni di un sistema digitale

- Vita operativa di un sistema digitale:



- Ipotesi: *stand-by time*=0 e *delay-time*=0
- Caratterizzazione statistica considerando valori medi nel tempo delle diverse grandezze in un insieme di campioni del sistema
- Si noti che esistono sistemi (ad esempio un singolo IC) che non sono riparabili

Availability istantanea

- Probabilitá ($A(t)$) che il sistema sia operativo al tempo t
- É una misura utilizzata nel valutare sistemi le cui operazioni possono essere interrotte per brevi periodi
- I sistemi commerciali rientrano in questo ambito
- Come stimarla? Supponiamo di avere un insieme di n campioni del sistema digitale e sia $X_s(t) \in \{0, 1\}$ una variabile binaria che vale 1 se il campione s del sistema é up e 0 altrimenti

$$A(t) = \sum_{s=0}^{n-1} X_s(t)$$

- Se ne puó anche definire un valore asintotico

Valore medio dell'availability

- Frazione di tempo in cui il sistema é disponibile nell'intervallo $[0, t]$

$$\overline{A(t)} = \frac{1}{t}\int_0^t A(u)du$$

- É utile per avere un idea della disponibilitá del sistema in un certo intervallo di missione
- Si puó stimare utilizzando $A(t)$, oppure si puó stimare anche su un singolo campione come:

$$\overline{A_s(t)} = \frac{1}{t}\int_0^t X_s(u)du$$

MTTF e MTBF

- Quantitá largamente utilizzate per caratterizzare i sistemi dal punto di vista dell'affidabilitá
- MTTF (*Mean Time To Failure*) é il tempo atteso (medio) a un malfunzionamento del sistema
    - é utile per singoli componenti che vengono scartati in caso di malfunzionamenti (MTTFF *Mean Time To First Failure*)
    - nel caso di sistemi riparabili puó essere considerata come il tempo medio di up-time
- Nel caso di sistemi piú complessi che possono avere un processo di riparazione conviene usare MTBF: *Mean Time Between Failures*, ovvero il tempo atteso fra due malfunzionamenti (in alcuni casi si considera MTTF=MTBF)

MTTF e MBTF

- In entrambi i casi si puó scrivere:

$$MTTF = MTBF = \int_0^{\infty} tf(t)dt$$

  ove $f(t)$ é la funzione di densitá di probabilitá dei malfunzionamenti
- MTBF e MTTF non hanno molto significato se la densitá di probabilitá dei malfunzionamenti non é costante

Availability

- Puó risultare interessante esprimere l'availability come una singola quantitá numerica
- L'espressione usata é

$$A = \frac{up - time}{total - time} = \frac{up - time}{up - time + down - time}$$

- Esistono diverse opzioni (A inerente, operativa) che possono essere ricondotte a:

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{MTBF}{MTBF + MTTR}$$

- Se il sistema é affidabile ($MTTF \gg MTTR$) allora $A \to 1$

Critiche

- Quale é il significato di *MTTF*?
- Nel caso in cui il sistema non é riparabile il significato é chiaro
- Cosa succede se il sistema é riparabile?
- *MTTF* risulta ambiguo a meno che non si faccia l'ipotesi che la riparazione oltre a ripristinare il corretto funzionamento ripristini le stesse caratteristiche di affidabilitá del sistema originario
- L'*availability* puó caratterizzare sistemi piuttosto diversi e non fornisce alcuna informazione su quanto un sistema puó funzionare

Esempio

- Un esempio tipico é dato dalla mitragliatrice e dal motore di una torpediniera
- La mitragliatrice ha un valore di A pari a 0.983 con $MTTF = 600s$ e $MTTR = 10s$
- Il motore ha invece un valore di A pari a 0.952 con $MTTF = 200h$ e $MTTR = 10h$

Reliability

- Probabilitá ($R(t)$) che il sistema funzioni dal tempo $t = 0$ al tempo t senza malfunzionamenti (condizionata al fatto che sistema risulti operativo a $t = 0$)
- Capacitá di fornire il servizio con continuitá
- Risulta una specifica per sistemi real-time (aerei ....)

Misure di Reliability

- Anche in questo caso $R(t)$ é misurabile sperimentalmente con un adeguato campione di componenti
- In presenza di eventuali guasti, R puó essere espressa come

$$R = Prob\{no\ fault\} + Prob\{correct\ operation \mid fault\} \cdot Prob\{fault\}$$

  - $Prob\{no\ fault\} = 1 - Prob\{fault\}$: probabilitá che non ci sia alcun guasto nel sistema
    - puó essere massimizzata mediante tecniche di fault avoidance
  - $Prob\{correct\ operation \mid fault\}$: probabilitá condizionale che il sistema funzioni nonostante la presenza di un guasto
    - puó essere massimizzata utilizzando tecniche di fault tolerance
    - si puó osservare che il termine é pesato su $Prob\{fault\}$ e quindi conviene considerare i guasti piú probabili

Utilizzo della fault tolerance nei sistemi digitali

- Le tecniche di fault avoidance (scelta dei materiali, testing) non sono in generale sufficienti a garantire sufficienti livelli di affidabilitá
- La fault-tolerance ha un impatto significativo sull'affidabilitá dei sistemi digitali
- Questo impatto puó essere analizzato da due punti di vista differenti (anche se correlati):
  - produzione: massimizzare la resa (yield)
  - applicazione: massimizzare l'affidabilitá delle operazioni

Problemi di affidabilitá delle tecnologie per circuiti integrati digitali

- La comprensione delle modalitá di guasto é chiaramente il punto di partenza per lo studio delle tecniche di fault-tolerance
- Nelle tecnologie attuali, le dimensioni sempre piú piccole dei componenti elementari (transistori e interconnessioni) e l'aumento delle frequenze di utilizzo portano con sé diversi problemi:
  - difficoltá nel controllare i processi produttivi $\rightarrow$ elevate probabilitá di difetti e aumenti nelle fluttuazioni statistiche dei parametri circuitali (ritardo)
  - riduzione delle capacitá caratteristiche e dei margini di immunitá ai disturbi $\rightarrow$ sensibilitá delle operazioni dei circuiti a disturbi interni (rumore sull'alimentazione, crosstalk) ed esterni (effetti di radiazioni)

Conseguenze

- Impatto sulla resa
- Difficoltá di collaudo
- Problemi dovuti alle radiazioni
  - si tratta di un problema tradizionale per i circuiti integrati in ambiente spaziale a causa dell'assenza dell'effetto schermante dell'atmosfera
  - ora le dimensioni tipiche delle tecnologie sono tali da rendere i circuiti sensibili all'impatto dei neutroni $\Rightarrow$ problemi anche a livello suolo

Guasti di tipo transitorio

- Sono indotti da disturbi interni o esterni
- Diversamente da stuck-at, bridging etc., gli effetti di tali guasti sono transitori
- A causa di una radiazione incidente (α, *n*, *p*), una quantitá di carica viene mossa dando luogo a un iniezione di corrente in una giunzione che da a sua volta luogo a un impulso in uscita al gate che contiene la giunzione
- Se il gate é contenuto in un latch o FF é possibile che lo stato del latch o FF venga cambiato (Single Event Upset, SEU)
- Se il gate é contenuto nella logica combinatoria, é possibile che l'impulso si propaghi nella rete fino all'ingresso di un elemento di memoria ove viene campionato (Single Event Transient, SET)

Utilizzo della fault tolerance

- La fault tolerance puó essere utilizzata per:
    - aumentare la resa rendendo disponibili risorse hardware ridondanti (questa é una pratica comunemente utilizzata ad esempio nella produzione di memorie)
    - rendere piú affidabili le operazioni dei sistemi digitali in presenza di disturbi

Approcci alla fault tolerance

La tolleranza ai guasti viene ottenuta aggiungendo qualche forma di ridondanza al sistema

- Ridondanza hardware
- Ridondanza software
- Ridondanza di informazioni
- Ridondanza nel tempo

Ciascun tipo di ridondanza presenta specifiche caratteristiche dal punto di vista dei guasti tollerabili, dei costi e delle prestazioni

Reliability e failure rate

- L'affidabilitá dei componenti elettronici é una funzione del tempo
- Si supponga di realizzare un esperimento di invecchiamento a partire da N campioni di un sistema digitale
- Sia $S(t)$ il numero di componenti che funzionano ancora al tempo t: $S(t) = N - F(t)$ ove $F(t)$ é il numero di componenti che si sono guastati
- Reliability:

$$R(t) = \frac{S(t)}{N}$$

- Unreliability:

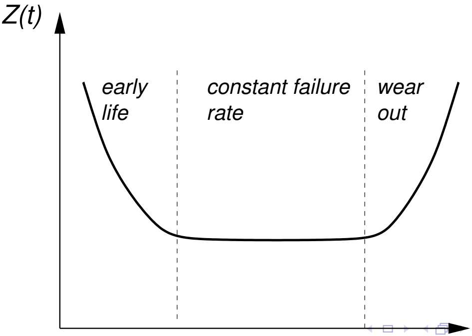
$$Q(t) = 1 - R(t) = 1 - \frac{S(t)}{N} = 1 - \frac{N - F(t)}{N} = \frac{F(t)}{N}$$

Failure rate

Il *failure rate* é il rateo con cui si guastano i componenti al tempo t normalizzato al numero di componenti ancora operativi al tempo t

$$Z(t) = \frac{1}{S(t)} \frac{dF(t)}{dt}$$

Nel caso dei circuiti integrati $Z(t)$ ha un caratteristico andamento detto a vasca da bagno



Constant failure rate

- La maggior parte della vita operativa di un circuito integrato avviene in questa condizione (i componenti destinati a guastarsi nel periodo di early life possono essere individuati con prove accellerate (burn-in))
- Si supponga che sia $Z(t) = \lambda$ e ricordando che:

$$R(t) = \frac{S(t)}{N} = \frac{N - F(t)}{N} = 1 - \frac{F(t)}{N} \; ,$$

si puó esprimere la derivata dell'affidabilitá

$$\frac{dR(t)}{dt} = -\frac{1}{N}\frac{dF(t)}{dt}$$

da cui per la definizione di failure rate ($Z(t) = \lambda = \frac{1}{S(t)}\frac{dF(t)}{dt}$) si ha:

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

Constant failure rate

- L'equazione precedente puó essere scritta come:

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

- E facilmente integrata

$$\int_0^t \lambda d\tau = -\int_1^{R(t)} \frac{dR}{R}$$

- Da cui

$$\lambda\,[\tau]_0^t = -\,[ln(R)]_1^{R(t)}$$

- Infine

$$\lambda t = -ln(R(t))$$

- Andamento di $R(t)$

$$R(t) = e^{-\lambda t}$$

Mean time between failures

- $R(t)$ é una quantitá che evolve nel tempo e quindi non é facilmente utilizzabile per caratterizzare un sistema
- Si utilizza solitamente il tempo medio fra due malfunzionamenti (MTBF)

$$MTBF = \int_0^{\infty} tf(t)dt = \int_0^{\infty} R(t)dt$$

- In caso di failure rate costante si ha:

$$MTBF = \int_0^{\infty} e^{-\lambda t} = -\frac{1}{\lambda}\left[e^{-\lambda t}\right]_0^{\infty} = \frac{1}{\lambda}$$

- Invertendo tale relazione e inserendo λ nell'espressione di $R(t)$, si ottiene:

$$R(t) = e^{-t/MBTF}$$

Relazione fra MTBF e availability

$$\begin{aligned}
A &= \frac{up - time}{up - time + down - time} & (1)\\
&= \frac{up - time}{up - time + no.\, of\ failures \cdot MTTR} & (2)\\
&= \frac{up - time}{up - time + \lambda \cdot up - time \cdot MTTR} & (3)\\
&= \frac{1}{1 + \lambda \cdot MTTR} & (4)
\end{aligned}$$

Utilizzando la relazione fra λ e MTBF

$$A = \frac{1}{1 + \frac{MTTR}{MTBF}} = \frac{MTBF}{MTBF + MTTR}$$

Affidabilitá dei sistemi serie e parallelo

- Ipotesi: i componenti del sistema si guastano in maniera indipendente fra loro (senza common mode failures)
- Serie: $R_s(t) = \prod_{i=1}^{N} R_i(t)$
- Se $R_i(t) = e^{-\lambda_i t}$ (failure rate costante), $R_s(t) = e^{-\sum_{i=1}^{N} \lambda_i t}$
- Parallelo: $R_p(t) = 1 - \prod_{i=1}^{N}(1 - R_i(t))$
- Sistemi piú complessi richiedono diverse metodologie o formule approssimate