



La tolleranza ai guasti

Concetti generali

Docente:

William Fornaciari

Politecnico di Milano

fornacia@elet.polimi.it

www.elet.polimi.it/~fornacia

Sommario



- Storia
- Concetti fondamentali
- Correttezza ed affidabilità



- 1967. Avizienis: un sistema è FT se i suoi programmi possono essere eseguiti correttamente nonostante l'occorrenza di guasti fisici. Da qui:
 - ▶ Costruzione architetture ridondanti
 - ▶ Introduzione codici di errore, duplicazione e triplicazione con votazione per rilevazione e/o correzione degli errori
 - ▶ Tecniche diagnostiche per individuazione dei guasti
 - ▶ Duplicazione dei principali sottosistemi
- 1971: Jet Propulsion Laboratory (NASA) e IEEE promuovono la prima conferenza sul calcolo della tolleranza ai guasti

Definizioni



- **Ridondanza:** parte del sistema non necessaria per il corretto funzionamento del sistema in assenza di FT
 - ▶ Ridondanza hardware
 - ▶ Ridondanza software
 - ▶ Ridondanza temporale (algoritmi ripetuti nel tempo)
- **Disponibilità:** probabilità in funzione del tempo che il sistema sia correttamente operativo all'istante t
- **Affidabilità:** probabilità in funzione del tempo che il sistema sia correttamente funzionante all'istante t se il sistema stesso era funzionante all'istante 0 . È un parametro più stringente della disponibilità

Definizioni



- **Avaria o insuccesso (failure):** cambiamento fisico nell'hardware
- **Guasto (fault):** stato erroneo di hw o sw derivante da: *avarìa*, errori di progetto, interferenze ambientali, errori umani. Un guasto può essere:
 - ▶ **Permanente:** guasto continuo e stabile
 - ▶ **Intermittente:** guasto o errore occasionale e instabile
 - ▶ **Transiente:** guasto o errore risultato di particolari e temporanee condizioni ambientali (non riparabili)
- **Errore (error):** manifestazione di un *guasto* in un programma
- **Avaria -> Guasto -> Errore**

La classificazione dei guasti



- Guasti per difetti fisici, tipo difetti di fabbricazione di un chip (che si evitano con test di affidabilità delle singole componenti, ma non ci riguarda)
- Guasti per difetti a livello logico
 - ▶ Stuck-at: i valori di una linea, porta o pin sono fissi a 0 o 1.
 - ▶ Bridging: due o più segnali adiacenti sono cortocircuitati (possibile creazione di AND o OR)
 - ▶ Short or open: è presente una connessione in più o in meno
 - ▶ Unidirezionale: a causa della geometria dei circuiti un guasto può avere un *effetto cascata* su più linee.

La classificazione dei guasti



- Guasti dovuti a difetti a livello di sistema. Si hanno quindi dei *modelli di guasto*, basati su distribuzioni probabilistiche (esponenziali e Weibull). È possibile gestire in tal modo
 - ▶ guasti permanenti
 - ▶ alcuni guasti intermittenti
 - ▶ pochissimi guasti transienti
- Esistono algoritmi per il rilevamento automatico dei guasti (AUTOFAIL)

Correttezza ed affidabilità



- Sono quattro i meccanismi che l'architettura di un sistema operativo affidabile deve fornire:
 - ▶ Rilevazione degli errori
 - ▶ Delimitazione e valutazione del danno
 - ▶ Copertura dell'errore
 - ▶ Trattamento dell'errore e ripristino del servizio
- L'ordine di applicazione di quanto sopra può variare, salvo partire dalla rilevazione degli errori



Due diverse metodologie di sviluppo:

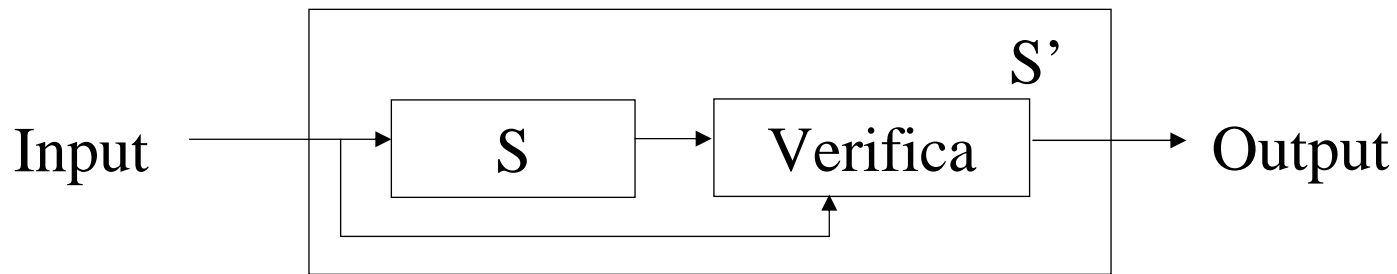
- Bottom-up: si progetta un sistema composto da sottosistemi autonomi, di per sé tolleranti ai guasti, cui aggiungere funzionalità di tolleranza ai guasti globali
- Top-down: si progetta un sistema composto da sottosistemi già esistenti che presentano una minima (al limite nulla) tolleranza ai guasti

Correttezza ed affidabilità

Rilevazione degli errori



- Tanto più efficace è la rilevazione degli errori, tanto più un sistema sarà affidabile
- L'approccio migliore per la rilevazione degli errori è il seguente, basato sulla corrispondenza del comportamento di un sistema ai suoi dati di targa



- Nella realtà è impossibile un controllo così rigoroso. Si controlla solo l'accettabilità dei valori d'uscita

Correttezza ed affidabilità

Delimitazione e valutazione del danno



- Intercorre sempre del tempo tra l'occorrenza del guasto e la sua rilevazione
- Pessimisticamente è bene ritenere che il danno si sia propagato a tutto il sistema
- Bisogna quindi aspettare che si manifestino altri eventuali errori in cascata, non ancora rilevati, prima di qualsiasi intervento di copertura

Correttezza ed affidabilità

Copertura dell'errore



Bisogna riportare il sistema in uno stato non erraneo

- All'indietro (checkpoint): il sistema torna ad uno stato precedente privo di errori
- In avanti: si costruisce uno stato esente da errori a partire da informazioni già esistenti (usualmente ridondanti)
- Due casi particolari di copertura:
 - ▶ Correzione dell'errore: il sottosist. dà risultati attendibili anche in caso di guasto permanente
 - ▶ Mascheratura attraverso ridondanza, senza azioni di copertura. Ad esempio, voting

Correttezza ed affidabilità

Trattamento errore e ripristino servizio



- Assicurarsi che un guasto occorso non si ripresenti
- La rilevazione dell'errore non necessariamente è utile all'identificazione del guasto (diversi guasti possono manifestarsi con lo stesso errore)
- Trovato il sottosistema guasto ho 3 alternative:
 - ▶ Sostituire il sottosistema guasto con uno di riserva
 - ▶ Riconfigurare il sistema affinché funzioni senza il sottosistema guasto
 - ▶ Ignorare il guasto se ritenuto transitorio