# Tecniche di tolleranza ai guasti

M. Favalli

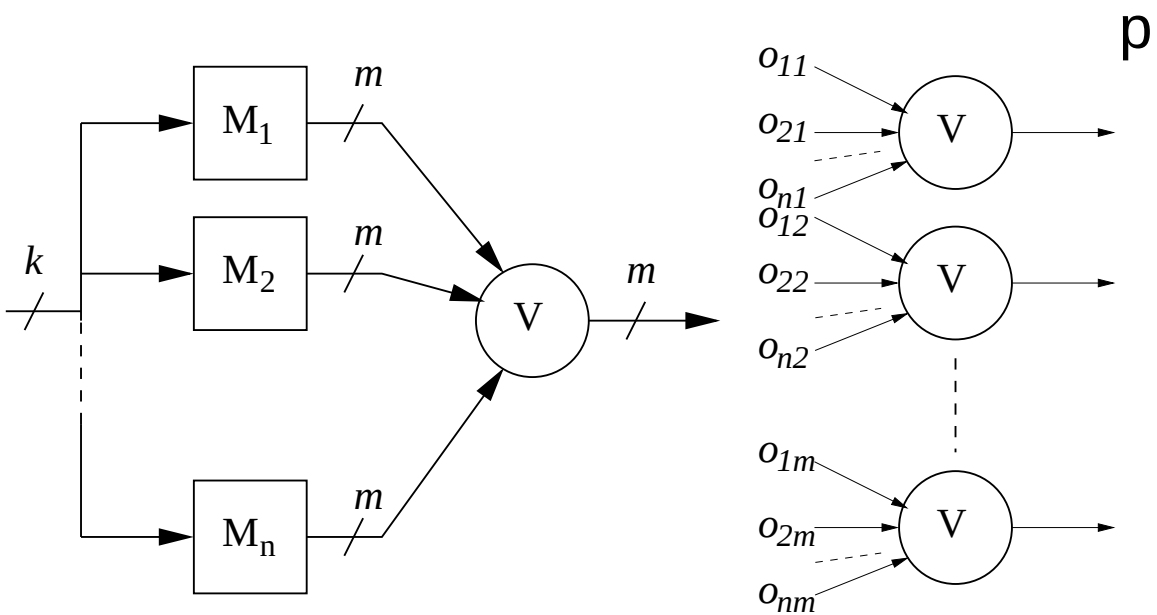
Engineering Department in Ferrara

# Ridondanza hardware

- Ridondanza modulare
  - sistemi *n*MR
- On-line testing e error-recovery

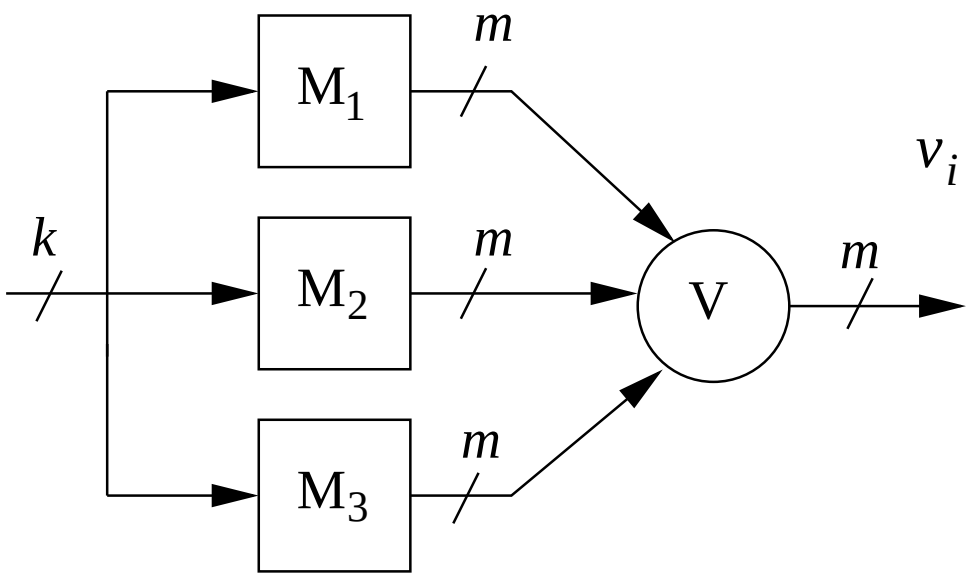
# Ridondanza modulare

- Un modulo é replicato $n$ volte ($n$MR, $n$ times modular redundancy)
- Ciascuna uscita di ciascuna replica va in ingresso a un voter che produce in uscita il valore assunto dalla maggioranza degli ingressi
- Possono essere tollerate fino a $\lceil (n-1)/2 \rceil$ copie malfunzionanti



# TMR - Triple Modular Redundancy

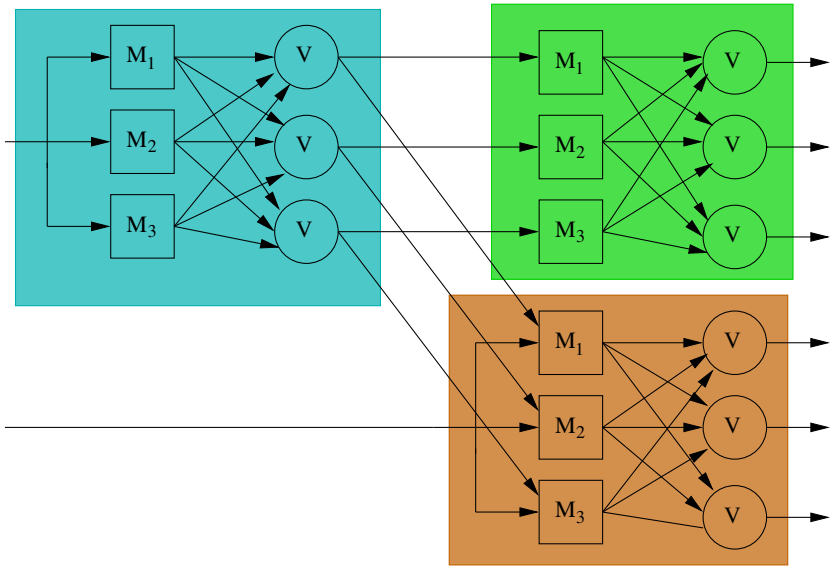
- É il caso piú semplice e piú largamente utilizzato




$$v_i = v_{1i}v_{2i} + v_{1i}v_{3i} + v_{2i}v_{3i}$$

# Applicazioni

- La ridondanza modulare puó essere applicata a qualsiasi livello di astrazione, da quello gate a quello di CPU
- TMR a livello di sottosistema




- La soluzione ottima di un problema dipende dall'affidabilitá dei singoli componenti

# Problemi

- Valutazione dell’affidabilitá
- Sistemi riconfigurabili
- Collaudabilitá e diagnosi

# Affidabilitá

- Ipotesi:
  - probabilitá di malfunzionamenti del voter trascurabile
  - modalitá di malfunzionamento indipendenti fra i vari moduli (common mode errors)
- L'affidabilitá é data da:

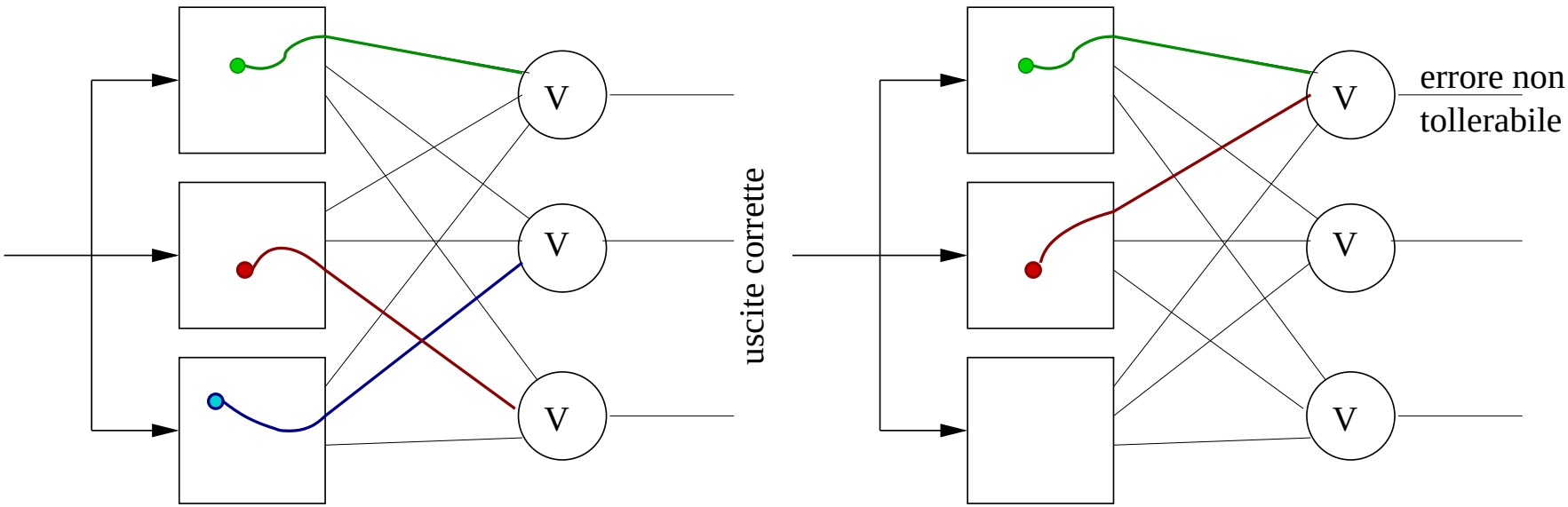
$$R_{TMR} = \sum_{i=0}^{\lceil (n-1)/2 \rceil} \binom{n}{i} (1 - R_M)^i R_M^{(n-i)}$$

- Nel TMR il significato probabilistico é piuttosto chiaro:

$$R_{TMR} = 3R_M^3 + 3R_M^2(1 - R_M)$$

# Affidabilitá

- Questa assunzione é pessimistica



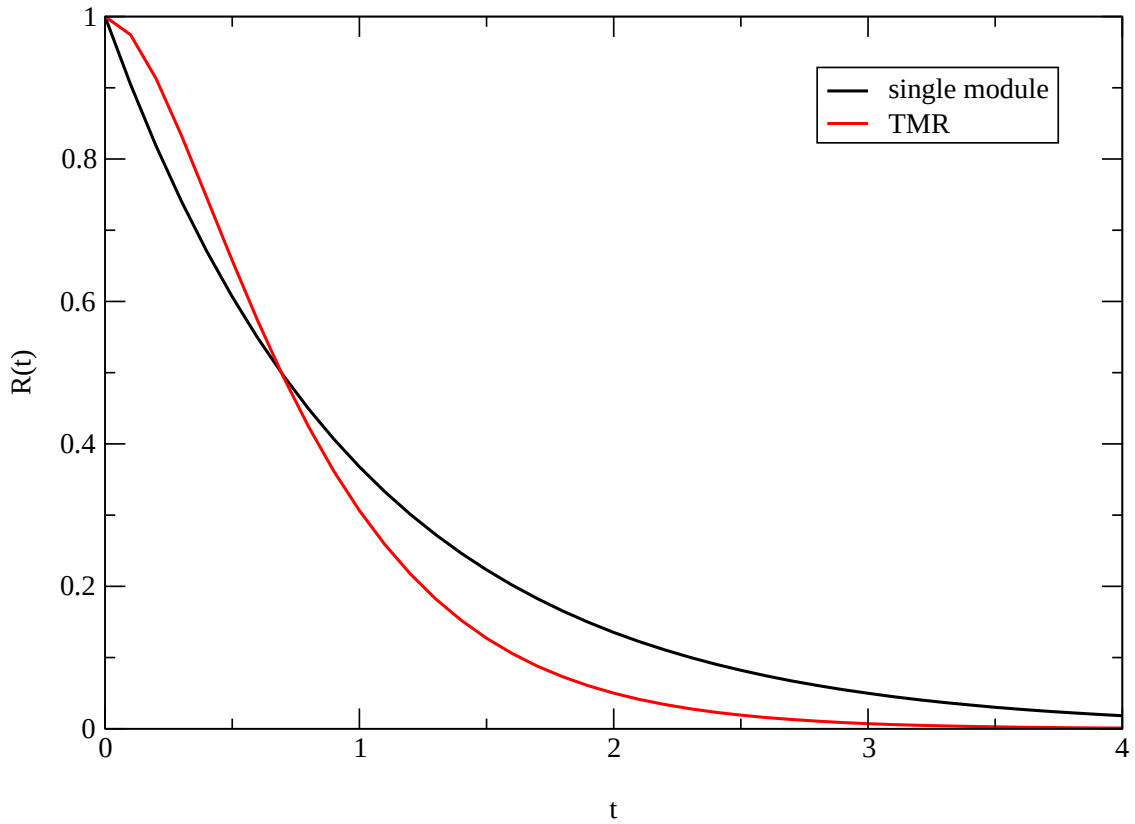
# Affidabilitá

- Nel caso in cui valga l'ipotesi di constant failure rate, si ha $R_M = e^{-\lambda t}$ da cui $R_{TMR} = 3e^{-2\lambda t} - 2e^{-3\lambda t}$
- Integrando si ottiene:

$$\int_0^\infty R_{TMR} dt = \frac{5}{6\lambda}$$

- Sorprendentemente questa quantitá é minore del MTBF $(1/\lambda)$ di un singolo componente
- Questo risultato é dovuto al fatto che l'MTBF considera il comportamento a $t = \infty$, mentre i sistemi vengono progettati per uno specifico tempo di missione

# Evoluzione nel tempo dell'affidabilitá in sistemi singoli e TMR

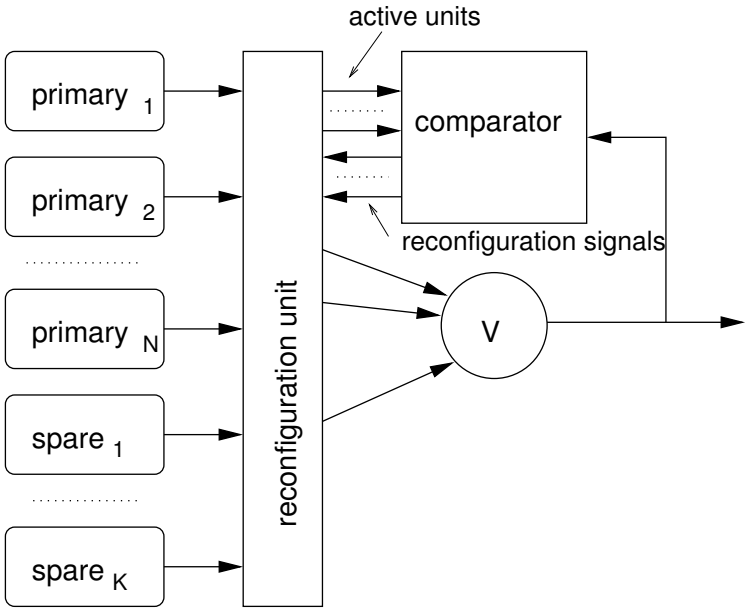


# Utilizzo di spare

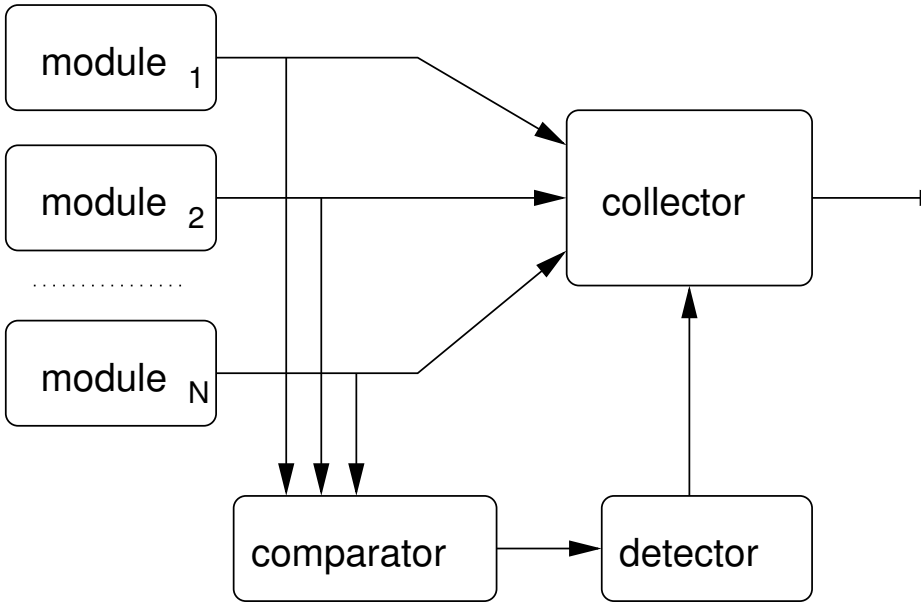
- Per evitare che l'affidabilitá del sistema si degradi nel tempo si possono utilizzare copie di riserva (spare)
- Si possono avere diverse tecniche di riconfigurazione, fra cui:
- Ridondanza ibrida
  - $N$ copie attive e $K$ spare, non appena si presenta un malfunzionamento, la copia guasta viene sostituita da una di riserva
- Ridondanza di tipo *sift*
  - tutte e $N$ le copie sono attive, non appena si verifica un errore, una copia viene spenta e il voting avviene solo sulle rimanenti $N - 1$ ....
- La scelta dipende da diversi parametri oltre all'affidabilitá. In particolare, i meccanismi di guasto nei circuiti spenti vanno considerati con cura

# Sistemi fault tolerant riconfigurabili

## Ridondanza ibrida




## Ridondanza sift



# Collaudabilitá e diagnosi

- Problemi di osservabilitá per i guasti interni ai moduli, in quanto il voter ne maschera gli effetti
- Problemi di controllabilitá per gli ingressi del voter (il voter contiene guasti non rivelabili)
- Possibili soluzioni: a) rendere controllabili indipendentemente gli ingressi dei blocchi funzionali; b) rendere osservabili le uscite dei blocchi funzionali

# Collaudo di sistemi TMR