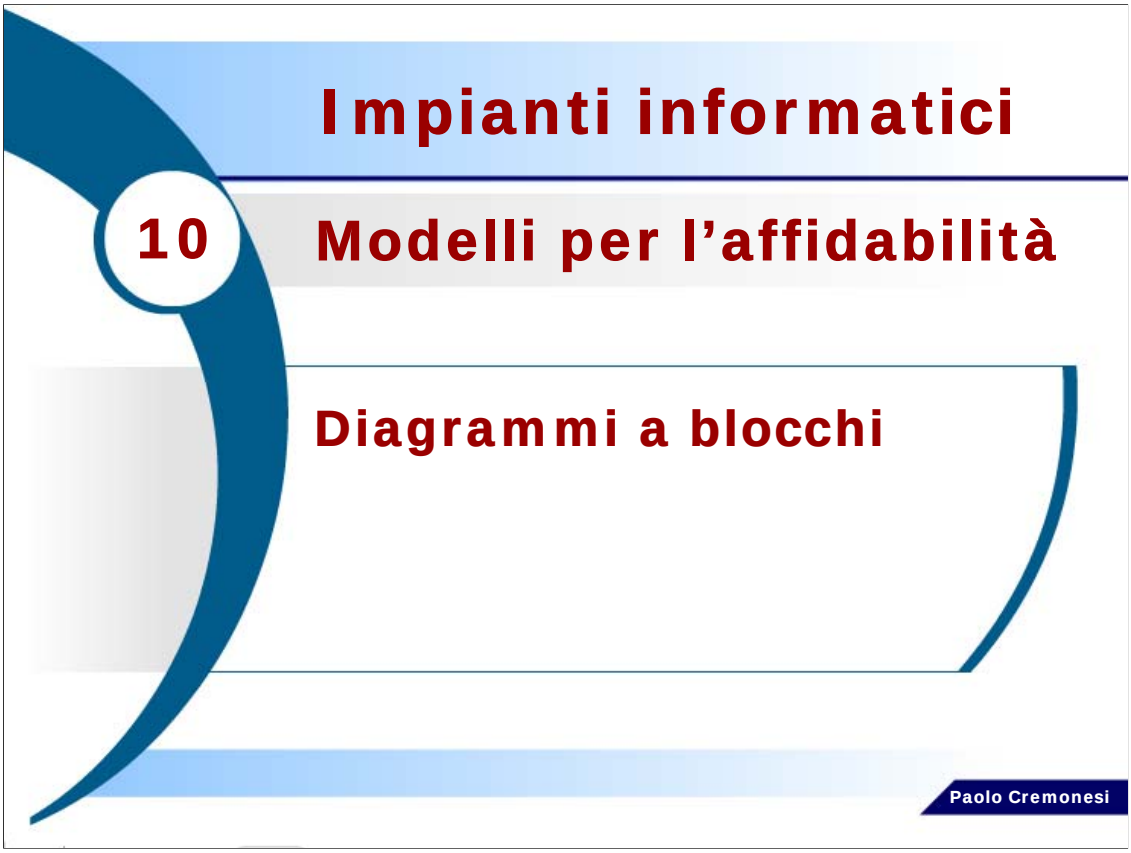
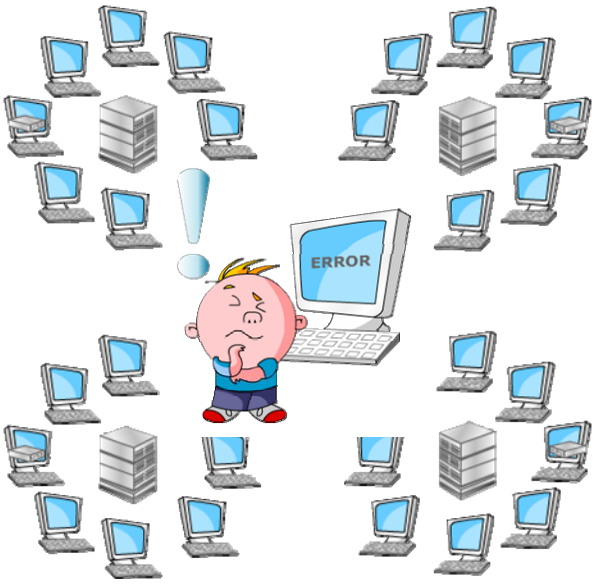


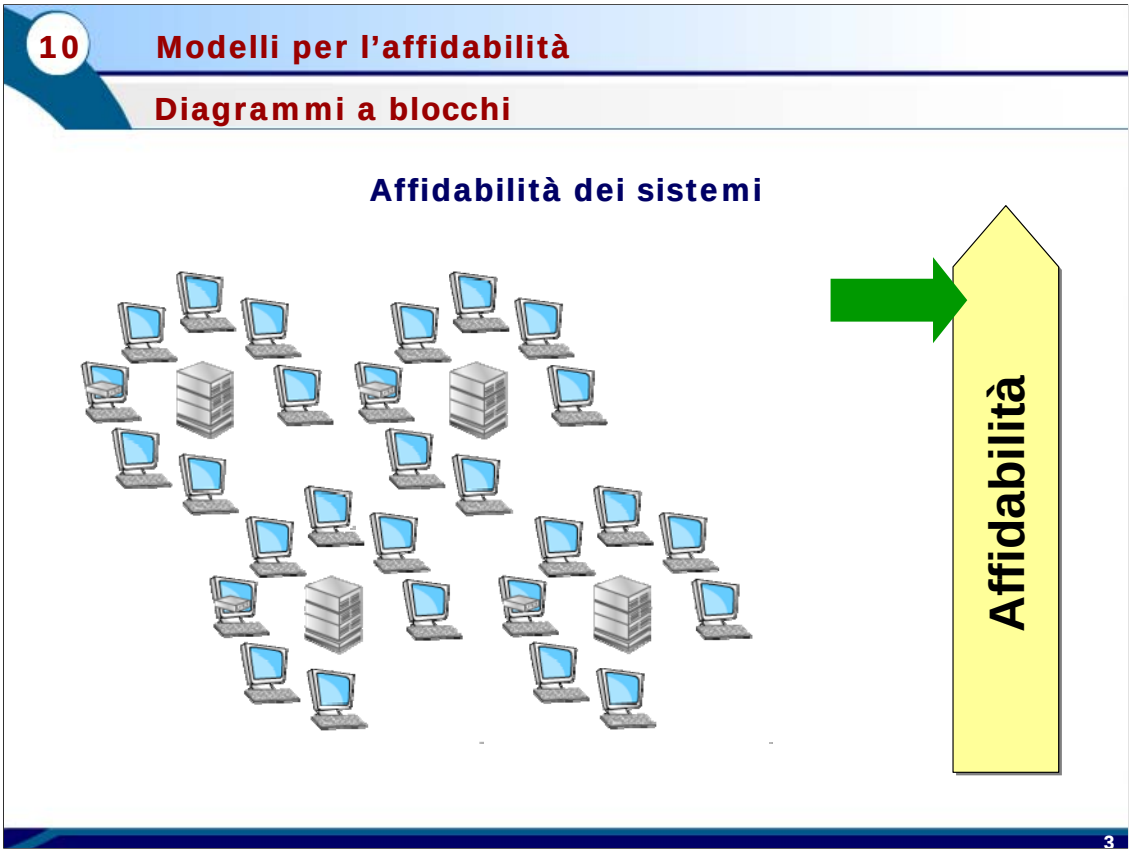
- ridondanza
- sistemi fault-tolerant
- sistemi in stand-by
- elementi in serie
- elementi in parallelo

Introduzione



La costruzione di modelli di affidabilità (in inglese, *reliability modeling*) è il processo che permette di prevedere e di capire l'affidabilità

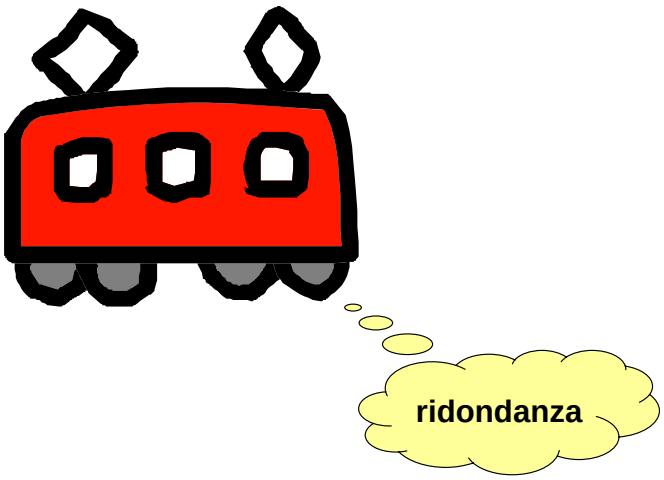
•di un sistema complesso conoscendo l'affidabilità e la funzione delle singole componenti



Come vedremo più avanti, solitamente più un sistema è complesso, minore è la sua affidabilità.

•Questo accade perché. aumentando il numero di componenti di un sistema, aumenta la probabilità che un qualche componente si guasti

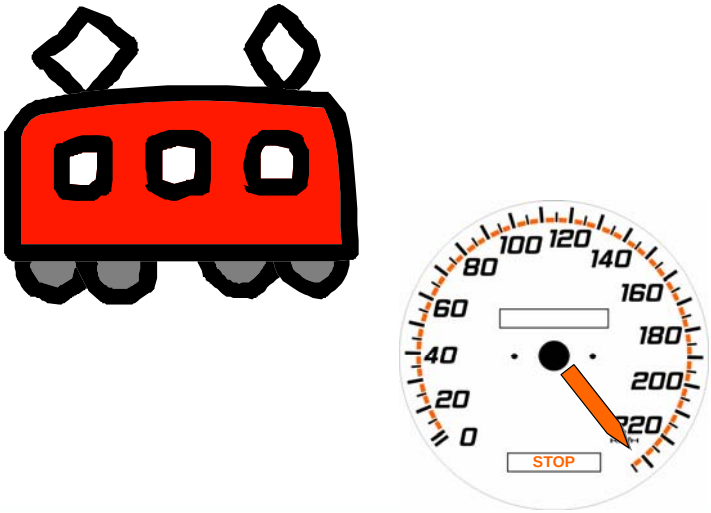
Sistemi fault-tolerant



I sistemi informatici complessi sono spesso progettati in modo da essere tolleranti ai guasti. Un sistema si dice tollerante ai guasti (in inglese, *fault-tolerant*) se è capace di funzionare correttamente anche in presenza di un guasto.

•Il meccanismo di protezione può frequente è quello della "ridondanza", grazie al quale un componente, pur guastandosi, non pregiudica la funzionalità del sistema perché queste funzionalità sono garantite da altre componenti (detti, appunto, ridondanti). Un sistema composto da elementi ridondanti può tollerare un certo numero di guasti ai componenti.

Sistemi fault-tolerant



La tolleranza ai guasti può portare al peggioramento di altre prestazioni, per cui nella progettazione di un sistema è necessario trovare adeguate ottimizzazioni e compromessi

•É importante notare che la tolleranza ai guasti non garantisce l'immunità da tutti i guasti, ma solo da quei guasti per cui è stato progettato un meccanismo di "protezione".

I meccanismi di fault-tolerance variano molto a seconda della tipologia di sistemi a cui vengono applicati.

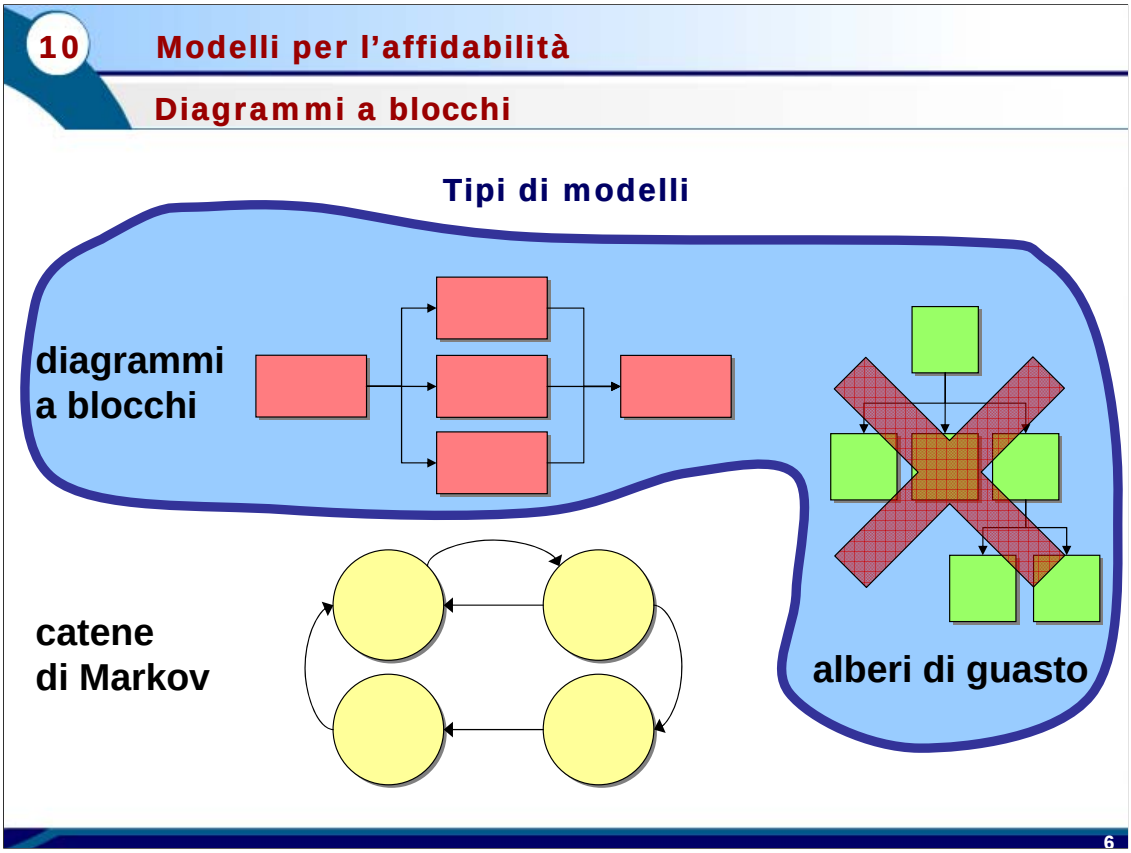
Ad esempio, nel caso dell'alimentazione dei server, si può implementare un semplice sistema di fault-tolerance utilizzando un gruppo di continuità: in caso di assenza della tensione di alimentazione gli apparati continueranno a funzionare per un certo periodo di tempo.

Un sistema più complesso, sempre relativo alle alimentazioni dei server, consiste nella replicazione dell'alimentatore: se l'alimentatore principale si dovesse guastare, l'apparato continuerà a funzionare grazie ad uno o più alimentatori posti in ridondanza.

Nel campo dei processori, è possibile utilizzare più processori contemporaneamente, sfruttando la potenza di calcolo complessiva e, nel caso uno dei processori si dovesse fermare, il funzionamento passerà ai processori ancora in funzione.

Per la protezione dei dati, si può ricorrere a sistemi RAID, nei quali la fault-tolerance è in funzione dello schema RAID adottato e dell'adozione o meno di dischi hot-spare.

Questi aspetti saranno approfonditi nella lezione sui dischi RAID e nella lezione sui sistemi scalabili.



Le tecniche disponibili per creare modelli di affidabilità sono essenzialmente tre.

•La prima tecnica è quella dei diagrammi a blocchi (in inglese, *reliability block diagram*)

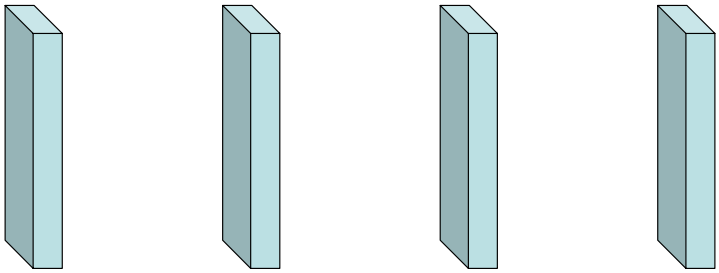
•La seconda tecnica è quella degli alberi di guasto (in inglese, *fault tree*)

•La terza tecnica è quella che si basa sulle catene di Markov

•Le due tecniche dei diagrammi a blocchi e degli alberi di guasto sono molto simili, pertanto in questa lezione affronteremo solo i diagrammi a blocchi.

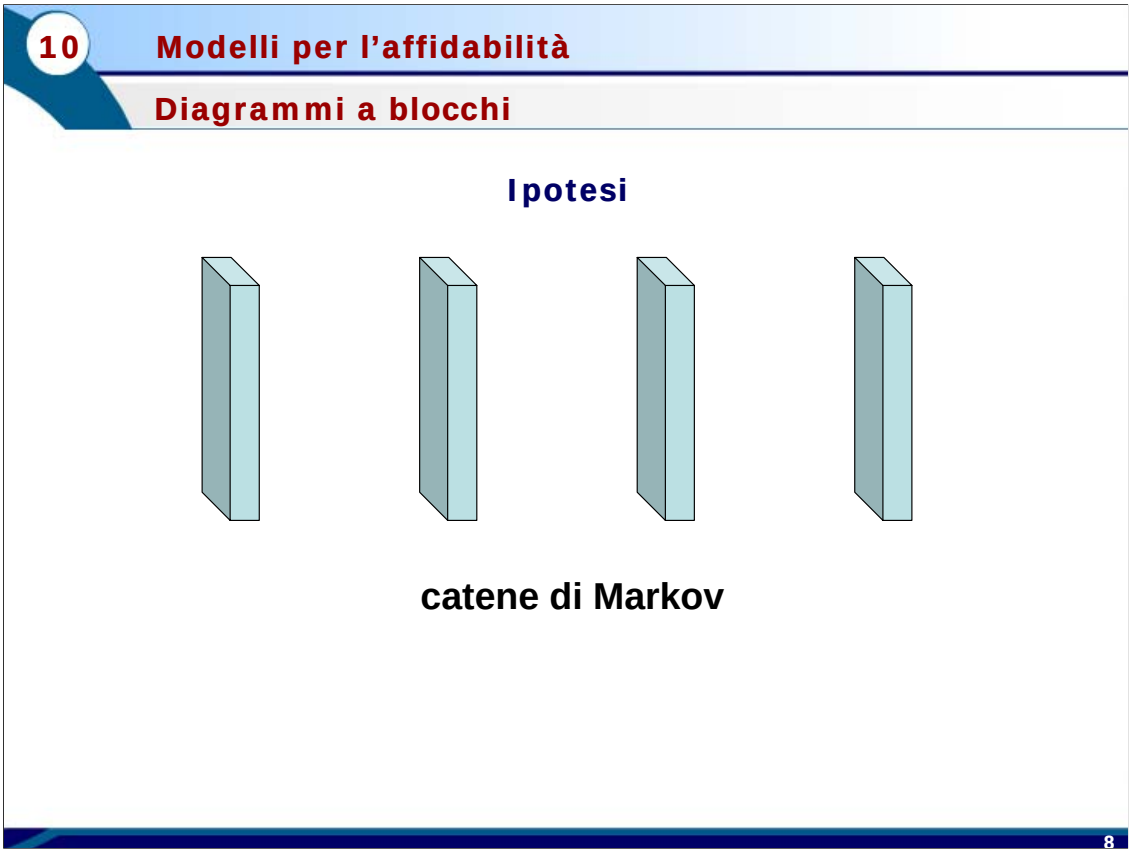
Diagrammi a blocchi

Ipotesi

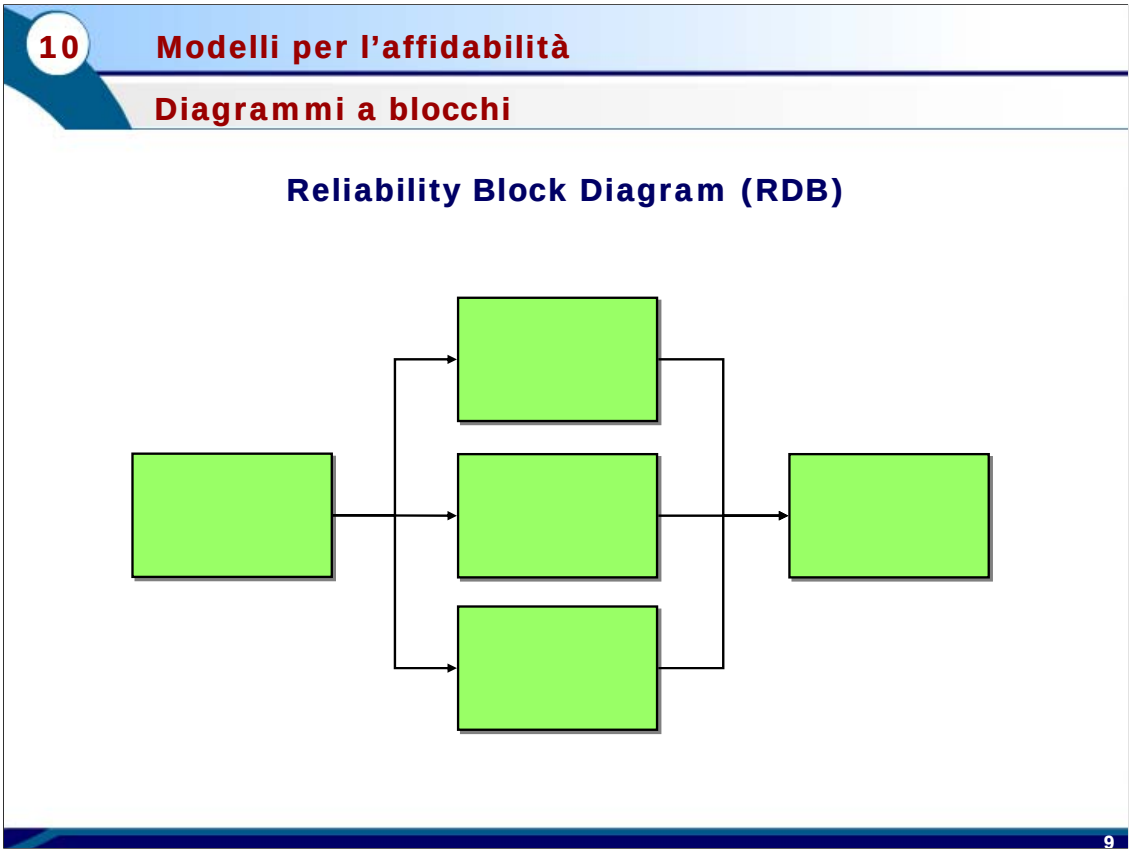


diagrammi a blocchi

I modelli basati sui diagrammi a blocchi si basano sull'ipotesi che gli elementi di un sistema siano statisticamente indipendenti dal punto di vista dell'affidabilità. In altre parole, si ipotizza che un guasto ad un elemento non influenza la probabilità di guasto degli altri elementi. Inoltre, per i sistemi riparabili, si ipotizza che la riparazione di un componente guasto non influenza le riparazioni degli altri componenti guasti



Al contrario, i modelli basati sulle catene di Markov permettono di considerare la reciproca influenza degli elementi, nel caso in cui un guasto ad un componente abbia effetto sulla probabilità di guasto degli altri componenti.



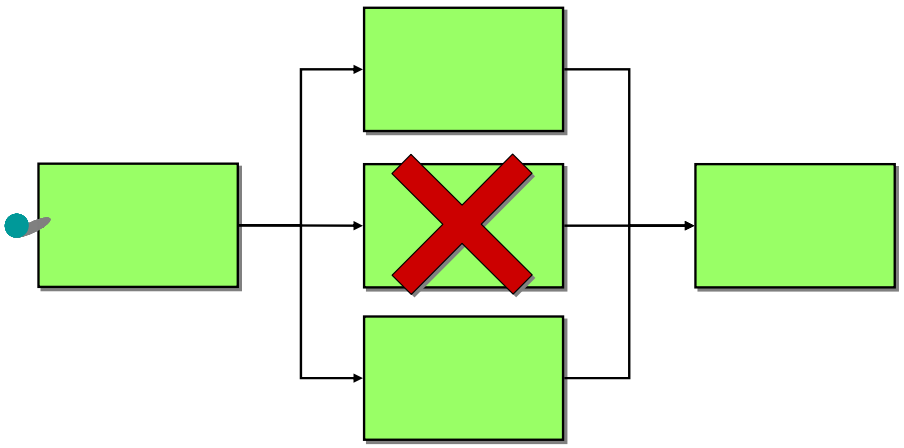
Supponiamo quindi che ogni componente sia indipendente dagli altri per quanto riguarda la possibilità di guasto. Lo stato dell'intero sistema dipende da quali componenti funzionano

Il suo comportamento può essere rappresentato da diagrammi di affidabilità chiamati RDB (in inglese, *Reliability Block Diagram*)

•Ogni componente del sistema è rappresentato da un blocco

•Il comportamento del sistema, in termini di affidabilità, è rappresentato dalle interconnessioni tra i blocchi

Reliability Block Diagram (RDB)

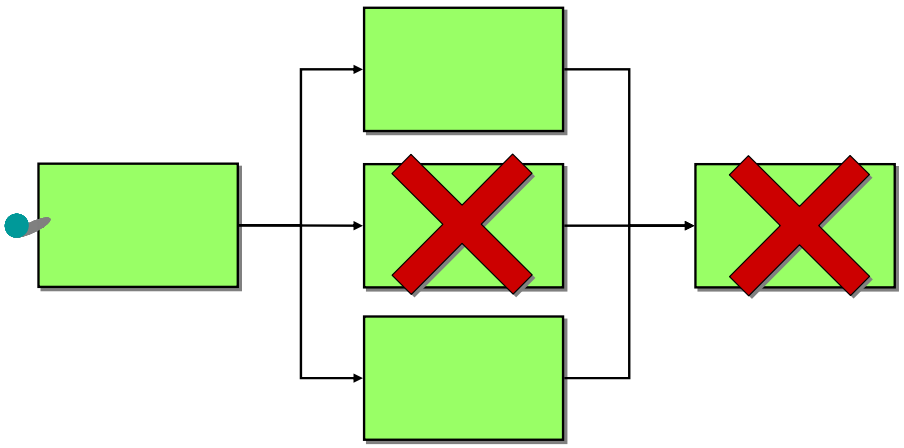


Ogni blocco può essere visto come rubinetto che è aperto quando il componente funziona correttamente

•Quando un componente si guasta (ossia, quando un rubinetto si chiude) il sistema continua a funzionare correttamente fin tanto che esiste un percorso tra l'ingresso e l'uscita

Diagrammi a blocchi

Reliability Block Diagram (RDB)



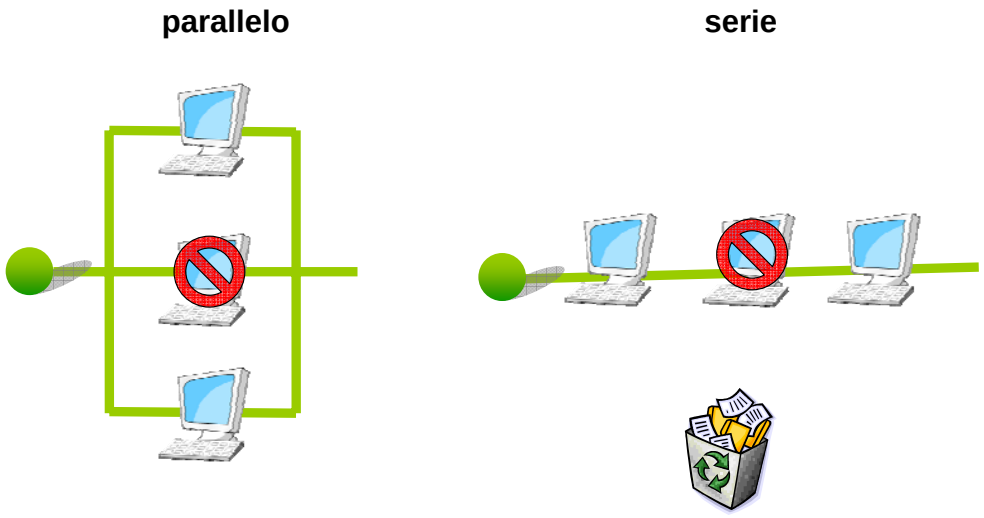
Quando non esite più un percorso "aperto" tra l'ingresso e l'uscita il sistema smette di funzionare.

I diagrammi a blocchi possono essere utilizzati per calcolare:

la reliability di sistemi non riparabili, conoscendo la reliability dei singoli componenti (si assume l'indipendenza statistica dei guasti tra componenti)

l'availability di sistemi riparabili, conoscendo l'availability dei singoli componenti (si assume l'indipendenza statistica dei guasti e delle riparazioni)

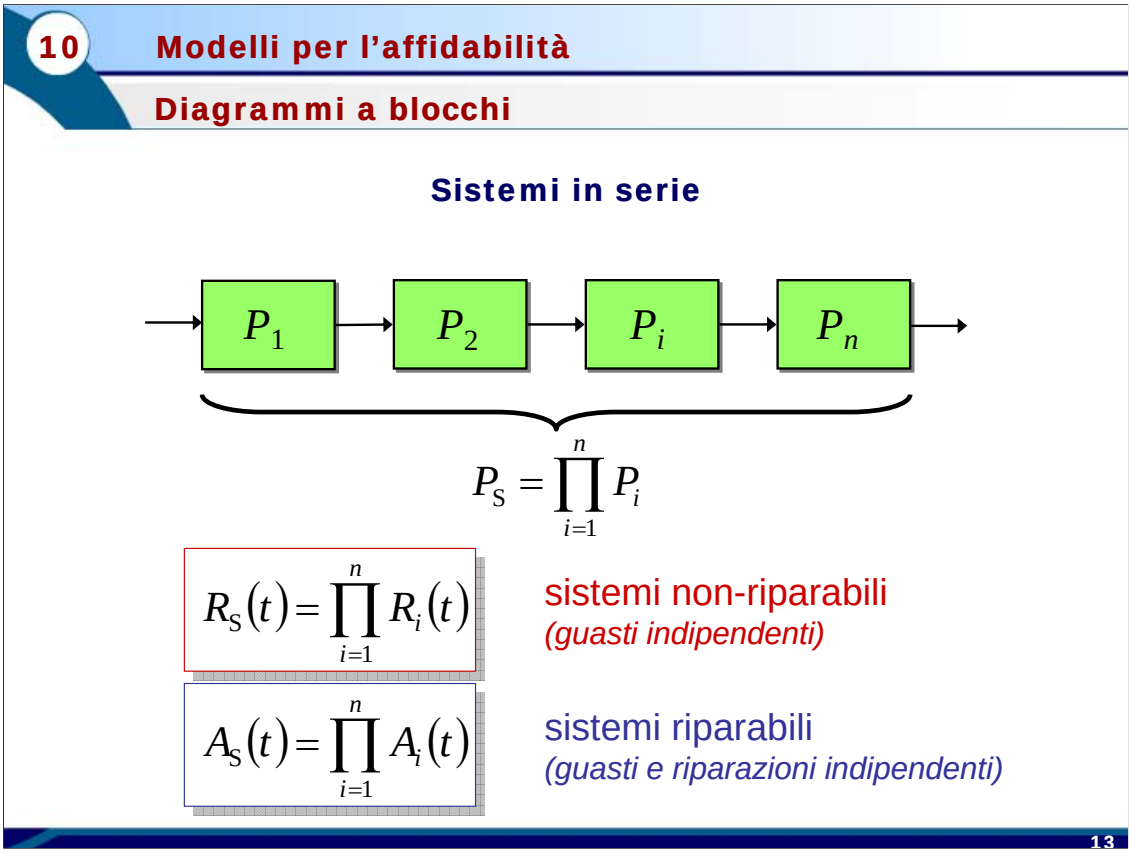
Sistemi in serie e in parallelo



Nei diagrammi a blocchi, i componenti di un sistema, da un punto di vista dell'affidabilità, sono spesso considerati in parallelo od in serie.

•Nel caso in cui tutti i componenti, pur guastandosi, non pregiudicano la funzionalità del sistema, diremo che il sistema è composto da componenti che, da un punto di vista dell'affidabilità, sono collegati tra loro in parallelo.

•Viceversa, nel caso che sia sufficiente l'avaria di un singolo componente per determinare l'avaria del sistema, diremo che tale sistema è composto da componenti connesse in serie.



Supponiamo di avere un sistema composto da *n* componenti in serie.

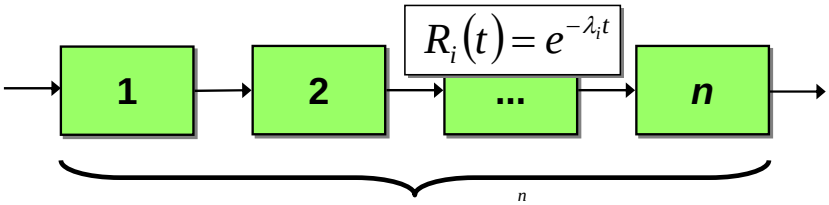
•Vogliamo calcolare la probabilità $\mathbf{P_S}$ che il sistema funzioni correttamente, conoscendo la probabilità $\mathbf{P_i}$ che ciascuno dei componenti funzioni correttamente.

•Perché un sistema in serie funzioni, devono funzionare contemporaneamente tutti i componenti. Rifacendosi al calcolo delle probabilità per eventi indipendenti, si ottiene che la probabilità $\mathbf{P_S}$ è pari al prodotto delle $\mathbf{P_i}$

•Nel caso di sistemi non-riparabili connessi in serie, abbiamo quindi che **l'affidabilità $\mathbf{R_S}$** del sistema è pari al prodotto delle affidabilità $\mathbf{R_i}$ dei singoli componenti

•Nel caso di sistemi riparabili, possiamo invece dire che la **disponibilità $\mathbf{A_S}$** del sistema è pari al prodotto delle disponibilità $\mathbf{A_i}$ dei singoli componenti

Sistemi in serie con failure-rate costante



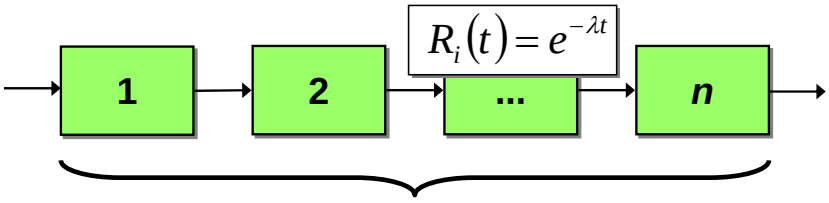
$$R_S(t) = \prod_{i=1}^{n} e^{-\lambda_i t} = e^{-t\sum_{i=1}^{n}\lambda_i} = e^{-t\lambda_S}$$

$$\lambda_S = \sum_{i=1}^{n} \lambda_i$$

Vediamo ora cosa succede nel caso di un sistema in serie in cui i componenti hanno tutti affidabilità esponenziale, ossia, con failure-rate λ_i costante

•In questo caso, anche l'affidabilità complessiva del sistema è di tipo esponenziale, con failure-rate λ_S dato dalla somma dei failure-rate dei singoli componenti

Sistemi in serie con failure-rate uguali



$$\lambda_S = n\lambda \qquad R_S(t) = e^{-t\lambda_S}$$

$$\mathrm{MTTF}_S = \frac{\mathrm{MTTF}}{n}$$

$$\mathrm{MTTF} = \frac{1}{\lambda}$$

$$\mathrm{MTTF}_S = \frac{1}{n\lambda}$$

15

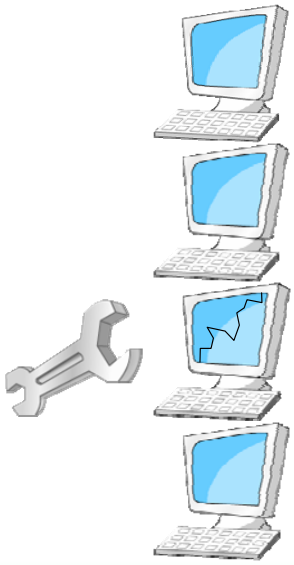
E' interessante vedere cosa succede nel caso in cui i componenti sono, dal punto di vista dell'affidabilità, tutti identici; ossia, nel caso in cui i componenti hanno tutti lo stesso failure-rate λ costante

- In questo caso, anche il failure-rate del sistema è n volte il failure rate dei singoli componenti
- Inoltre, il mean time to failure del sistema è n volte più piccolo rispetto al mean time to failure del componente
- quest'ultima proprietà si può verificare ricordando che il mean time to failure di un componente è pari al reciproco del suo failure rate
- e altrettanto vale per il mean time to failure del sistema

Migliorare l'affidabilità di sistemi in serie

analisi di sensitività

$$\frac{\partial R_S}{\partial R_i} = \frac{R_S}{R_i}$$



E' anche interessante notare che, nel caso di sistemi in serie, il massimo del miglioramento nell'affidabilità (o nella disponibilità) si ottiene migliorando il componente meno affidabile (o meno disponibile)

Vediamone una dimostrazione applicata al caso dell'affidabilità.

•Eseguiamo un'analisi di sensitività dell'affidabilità di un sistema in serie rispetto all'affidabilità delle singole componenti.

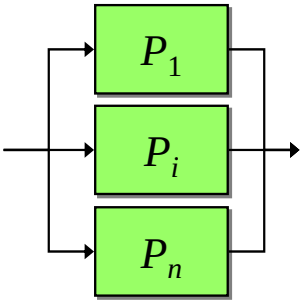
•Per fare questo, calcoliamo le derivate parziali dell'affidabilità del sistema rispetto all'affidabilità delle singole componenti. La dove la derivata assume valori più elevati, maggiore è l'incremento di affidabilità del sistema

•Se eseguiamo alcuni passaggi utilizzando i risultati presentati nei lucidi precedenti, osserviamo che le derivate parziali sono uguali al rapporto tra affidabilità del sistema e affidabilità del componente

•Dato che il numeratore è uguale per tutte i componenti, è chiaro che la derivata maggiore si ha per quel componente con il denominatore più basso, ossia per quel componente con l'affidabilità minore.

Diagrammi a blocchi

Sistemi in parallelo



$$P_S = \prod_{i=1}^{n} P_i$$

$$F_S(t) = \prod_{i=1}^{n} F_i(t)$$

sistemi non-riparabili
(guasti indipendenti)

$$U_S(t) = \prod_{i=1}^{n} U_i(t)$$

sistemi riparabili
(guasti e riparazioni indipendenti)

17

Supponiamo ora di avere un sistema composto da *n* componenti in parallelo.

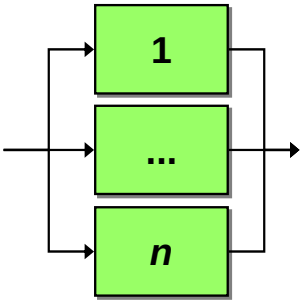
•Vogliamo calcolare la probabilità **P** che il sistema si guasti, conoscendo la probabilità $\mathbf{P_i}$ che si guasti ciascuno dei componenti.

•Un sistema in parallelo si guasta quando tutti i componenti sono guasti. Rifacendosi al calcolo delle probabilità per eventi indipendenti, si ottiene che la probabilità **P** è pari al prodotto delle $\mathbf{P_i}$

•Nel caso di sistemi non-riparabili connessi in parallelo, abbiamo quindi che **l'inaffidabilità $\mathbf{F_S}$** del sistema è pari al prodotto delle inaffidabilità $\mathbf{F_i}$ dei singoli componenti

•Nel caso di sistemi riparabili, possiamo invece dire che la **indisponibilità $\mathbf{U_S}$** del sistema è pari al prodotto delle indisponibilità $\mathbf{U_i}$ dei singoli componenti

Sistemi in parallelo



$$R_S(t) = 1 - \prod_{i=1}^{n} [1 - R_i(t)]$$

sistemi non-riparabili
(guasti indipendenti)

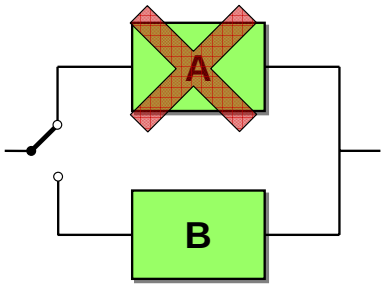
$$A_S(t) = 1 - \prod_{i=1}^{n} [1 - A_i(t)]$$

sistemi riparabili
(guasti e riparazioni indipendenti)

E' possibile riformulare le proprietà precedenti in termini di affidabilità R e disponibilità A

Sistemi in stand-by

- Il componente B non si usura fino a che rimane in stand-by
- L'interruttore agisce istantaneamente in caso di guasto
- L'interruttore non si guasta mai



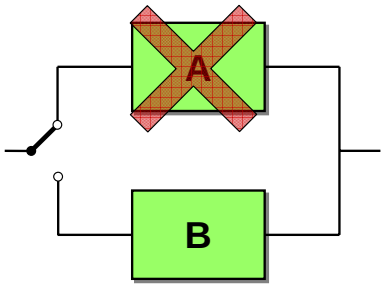
I sistemi in stand-by sono un caso particolare di sistemi in parallelo. Nella loro implementazione più semplice, i sistemi in stand-by sono composti da due componenti, di cui uno è operativo, mentre l'altro componente è in stand-by. I due componenti vengono spesso chiamati "attivo" il primo e "passivo" il secondo.

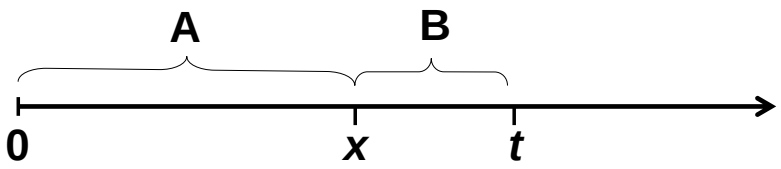
- In caso di guasto del componente attivo, un apposito meccanismo (hardware o software) agisce da interruttore e attiva il componente passivo. Quando questo accade si dice che è avvenuto uno "switch del servizio"
- Per calcolare l'affidabilità di un sistema in stand-by, facciamo alcune ipotesi. La prima ipotesi dice che il componente passivo non si "usura" fin tanto che è in stand-by. In altre parole, ipotizziamo che il componente passivo, nel momento in cui entra in funzione, è come se fosse nuovo.
- La seconda ipotesi è che l'interruttore, in caso di guasto al componete attivo, è in grado di attivare istantaneamente il componente passivo.
- La terza ipotesi prevede che l'interruttore abbia affidabilità sempre pari ad uno (in altre parole, ipotizziamo che l'interruttore non si guasti mai). Queste ipotesi, volendo, possono essere eliminate, complicando però la risoluzione del modello.

Sistemi in stand-by

Il sistema funziona nell'intervallo di tempo 0 — *t* se

a) Il componente A non si è guastato in *0 — t*
b) Il componente A si è guastato nell'istante *x<t* , e il componente B non si è guastato da *x* a *t*





- Vediamo adesso come calcolare la probabilità che il sistema, nell'intervallo di tempo 0 — *t* , non si sia mai guastato. Questa probabilità è l'unione di due eventi disgiunti.
- Può accadere che il componente attivo non si guasti mai nell'intervallo *0 — t*
- Oppure può accadere che il componente attivo si guasti in un istante *x<t* , e che il componente passivo, una volta entrato in funzione, non si è guasti nel periodo da *x* a *t*

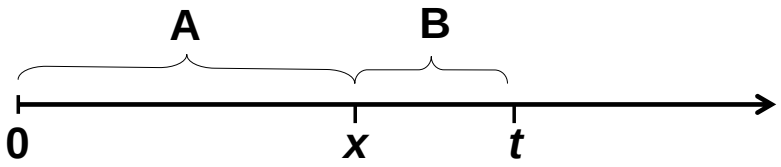
Sistemi in stand-by

$$R_S(t) = P_a(t) + P_b(t)$$

$$P_a(t) = R_A(t)$$

$$P_b(t) = \int_0^t R_B(t-x) f_A(x) \mathrm{d}x$$

$$R_S(t) = R_A(t) + \int_0^t R_B(t-x) f_A(x) \mathrm{d}x$$



21

•L'affidabilità del sistema è data quindi dalla somma delle probabilità che si verifichi uno o l'altro evento

•La prima probabilità e semplicemente l'affidabilità del componente attivo

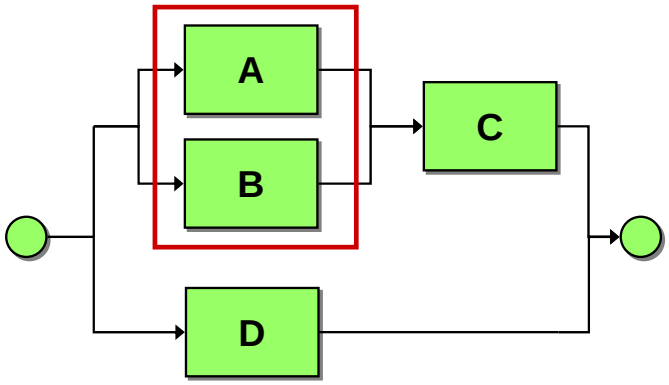
•Il secondo termine è dato dalla probabilità f_A che il componete attivo si guasti nell'istante x, per la probabilità R_B che il componente passivo, una volta entrato in funzione, riesca a funzionare fino all'istante t. Il tutto integrato su tutti i possibili valori di x

•Il risultato è l'affidabilità del sistema

Diagrammi a blocchi

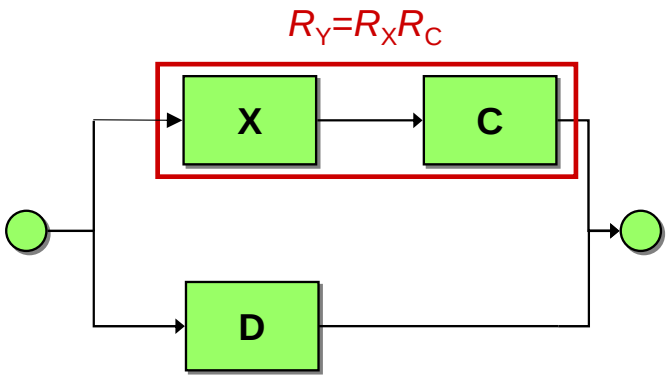
Sistemi serie / parallelo

$R_X = 1-(1-R_A)(1-R_B)$



Molti impianti informatici possono essere rappresentati, per quanto riguarda l'affidabilità, mediante diagrammi a blocchi di tipo serie/parallelo.

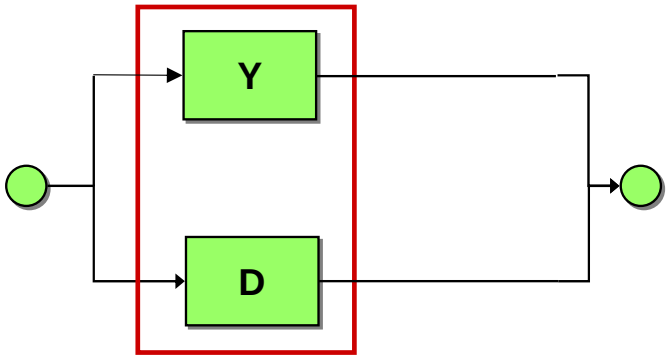
Sistemi serie / parallelo



In questo tipo di diagrammi è sempre possibile individuare sottogruppi di componenti connessi in serie o in parallelo.

Sistemi serie / parallelo

$R_S = 1-(1-R_Y)(1-R_D)$



Applicando le formule per i sistemi in serie e per quelli in parallelo a ciascun sottogruppo, è possibile risolvere in modo ricorsivo l'intero modello