

# CAPITOLO 2

## Concetti di base

### 1 Affidabilità, funzione di distruzione e densità di probabilità dei tempi di rottura

L'affidabilità di un prodotto può essere definita come la capacità di compiere il lavoro richiesto in determinate condizioni di esercizio e per un periodo di tempo stabilito. Ragionando in questo modo, si deduce che l'affidabilità può essere definita in termini di frequenza di interventi di riparazione richiesti in assistenza tecnica espressa, ad esempio, ogni 100 prodotti.

**Esempio 1** Vogliamo stabilire l'affidabilità su un certo intervallo di tempo. Come procedimento sottoponiamo ad un test dieci prodotti identici. Il test consiste nel verificare se i prodotti scelti nel campione funzionano correttamente nell'intervallo di tempo considerato. Supponiamo che si siano verificate le tre situazioni rappresentate in Figura 1. Nella prima situazione l'affidabilità è massima in quanto tutti gli elementi testati funzionano, nella seconda situazione c'è un solo elemento che non supera il test e questo ci porta a pensare che l'affidabilità sia abbastanza elevata, nella terza situazione, invece, il prodotto testato non è abbastanza affidabile visto che quattro elementi su dieci non superano il test.

Denotando con  $N^*$  il numero di prodotti testati nell'intervallo di tempo  $(0, t)$  e con  $N(t)$  il numero



Figure 1: Risultati di tre test effettuati per stabilire l'affidabilità di un prodotto.

di prodotti ancora funzionanti all'istante  $t$  si può concludere che

$$\text{Affidabilità misurata in } (0, t) = \frac{N(t)}{N^*}.$$

Pertanto nel primo caso l'affidabilità è 1, nel secondo caso è 0.9 e nel terzo caso risulta  $3/5 = 0.6$ . Dall'esempio appena discusso si deduce che l'affidabilità, almeno da un punto di vista intuitivo, si può pensare come la frequenza relativa di oggetti che funzionano correttamente in uno specificato

intervallo di tempo. Pertanto, ricordando che, per la legge empirica del caso, la frequenza relativa del verificarsi di un evento converge alla probabilità dell'evento stesso al crescere della taglia del campione, si giunge alla seguente definizione formale.

**Definizione 1** L'affidabilità è data dalla probabilità che un sistema o una componente (non riparabile) lavori in maniera soddisfacente (senza guasti) in un intervallo di tempo  $(0, t)$  sotto determinate condizioni ambientali.

Per poter definire quantitativamente l'affidabilità è necessario introdurre un parametro che permetta di stabilire se in un certo istante di tempo il dispositivo esibisce un funzionamento soddisfacente (senza guasti). A tal fine si utilizza un vettore  $X(t)$  che rappresenta lo stato di funzionamento del dispositivo. Le componenti di tale vettore sono in generale variabili in un intervallo di numeri reali e potrebbero contenere i valori dei parametri più significativi del dispositivo. In una situazione molto semplice  $X(t)$  può diventare unidimensionale e fornire un'informazione di tipo binario:  $X(t) = 1$  se il dispositivo funziona e zero altrimenti.

Introduciamo una funzione  $g(X)$  che fornisce un valore per ogni stato di funzionamento del dispositivo che può essere legato a considerazioni di carattere economico se, ad esempio, si pensa alla finalità a cui il dispositivo è destinato. Infatti, nel caso di funzionamento insoddisfacente  $X = 0$  si avrebbe una perdita economica mentre per  $X = 1$  si verificherebbe un guadagno inteso come mancanza di perdita. Facendo riferimento alla variabile aleatoria unidimensionale sopra definita si ha che  $g(X)$  è una variabile discreta avente valore medio:

$$G(t) = \mathbb{E}[g(X)] = g(0) \mathbb{P}[X(t) = 0] + g(1) \mathbb{P}[X(t) = 1].$$

Se supponiamo che  $g[X(t)]$  è una funzione binaria definita come  $g[X(t)] = 1$  quando il dispositivo funziona correttamente all'istante  $t$  e  $g[X(t)] = 0$  altrimenti, allora risulta:

$$G(t) = \mathbb{E}[g(X)] \equiv \mathbb{P}[X(t) = 1].$$

Considerando che la definizione data di affidabilità si riferisce ad un intervallo di tempo, si può concludere che l'affidabilità coincide con  $G(t)$  se si assume che un dispositivo che funziona correttamente ad un certo istante di tempo  $t$  ha funzionato correttamente dall'istante iniziale fino all'istante  $t$ . Tale situazione non è sempre verificata; infatti riguarda una particolare categoria di dispositivi detti non riparabili per i quali non è possibile (o economicamente svantaggioso) effettuare operazioni di riparazione o sostituzione delle componenti danneggiate. Più precisamente possiamo distinguere le seguenti due situazioni:

1. Sistemi non riparabili: costituiti da oggetti o componenti non ripristinabili; il passaggio dallo stato di funzionamento a quello di guasto per questi sistemi è irreversibile. In questo caso si parla di affidabilità in senso stretto;
2. Sistemi riparabili: costituiti da oggetti o componenti riparabili; in questo caso si ha l'alternanza di intervalli di tempo di durata casuale in cui il sistema passa dallo stato di funzionamento a quello di guasto e viceversa.

Per dispositivi riparabili, oltre al concetto di affidabilità, si introduce quello di disponibilità (Availability). Intuitivamente la disponibilità è la capacità che un dispositivo ha di funzionare correttamente nell'istante in cui viene richiesto il suo utilizzo. Questa quantità può essere misurata come il rapporto tra la somma degli intervalli di tempo in cui il dispositivo funziona e l'ampiezza dell'intervallo di tempo totale in cui si sono effettuate le osservazioni. Questo rapporto rappresenta la frequenza relativa dei tempi di funzionamento; così che, se si assume che l'intervallo di tempo in cui si effettuano le osservazioni sia sufficientemente ampio, allora la legge empirica del caso consente di interpretare tale frequenza come una probabilità. Si giunge così alla seguente definizione.

**Definizione 2** La disponibilità di un dispositivo riparabile è la probabilità che si trovi in condizioni operative soddisfacenti ad un determinato istante di tempo. In altri termini, la disponibilità di una componente è la probabilità che essa funzioni senza guastarsi in un determinato e stabilito istante di tempo  $t$  con riferimento a ben precisate condizioni ambientali.

Il verificarsi di molti guasti comporta una diminuzione dell'affidabilità del sistema, comunque, se i guasti possono essere riparati facilmente (in tempi brevi) la disponibilità del sistema rimane alta. Diversamente dall'affidabilità, per la disponibilità si fa riferimento ad un istante temporale ben preciso piuttosto che ad un intervallo di tempo. Infatti, quello che interessa è che il dispositivo funzioni all'istante  $t$  sebbene sia possibile che si sia potuto guastare in qualche istante precedente. Questa definizione si riferisce a dispositivi riparabili. Anche in questo caso possiamo considerare una variabile aleatoria  $X(t)$  che definisce lo stato del dispositivo ed una funzione guadagno  $g[X(t)]$  definita come in precedenza il cui valor medio risulta:

$$G(t) = \mathbb{E}[g(X)] = \mathbb{P}[X(t) = 1].$$

Possiamo quindi concludere che in un dispositivo non riparabile la definizione di affidabilità si identifica con quella di disponibilità.

Da quanto detto fin'ora si evince che l'affidabilità di un dispositivo non è direttamente misurabile; per poter ottenere elementi utili ad una definizione formale è necessario far riferimento all'evento "guasto" ossia al complemento dell'evento "funzionamento corretto".

Sia  $T$  la variabile aleatoria che rappresenta l'istante di rottura di una componente, l'affidabilità della componente nell'intervallo di tempo  $(0, t]$  è quindi

$$R(t) = \mathbb{P}(T > t).$$

L'affidabilità è detta anche funzione di sopravvivenza, risulta essere una funzione decrescente che vale sempre 1 per  $t = 0$  e 0 per  $t \rightarrow \infty$ . L'affidabilità è connessa alla funzione di distribuzione della variabile aleatoria  $T$  in quanto si ha:

$$R(t) = 1 - \mathbb{P}(T \leq t) = 1 - F(t).$$

La funzione  $F(t)$  rappresenta la probabilità che la componente si guasti prima dell'istante  $t$ . Essendo la funzione di ripartizione della variabile aleatoria  $T$ ,  $F(t)$  risulta non negativa e non

decescente, continua da destra, vale 0 per  $t \rightarrow 0$  e 1 se  $t \rightarrow \infty$ . Dal punto di vista della teoria dell'affidabilità,  $F(t)$  rappresenta, in un certo senso, l'inaffidabilità del prodotto in esame.

**Osservazione** Supponiamo di aver testato  $N^*$  prodotti su un fissato intervallo di tempo di ampiezza  $t$ . Supponendo che di tali prodotti  $N(t)$  risultano ancora funzionanti all'istante  $t$  si ha che

$$R(t) = \frac{N(t)}{N^*}, \quad F(t) = 1 - R(t).$$

In Figura 2 sono confrontate le funzioni  $R(t)$  e  $F(t)$ . È evidente che mentre la prima è non crescente, la seconda è non decrescente. Inoltre, risulta che  $R(t) = F(t)$  se e solo se  $R(t) = 1 - R(t)$ , ossia se e solo se  $R(t) = 0.5$ . Sia  $f(t)$  la funzione densità di guasto, ossia la funzione densità di

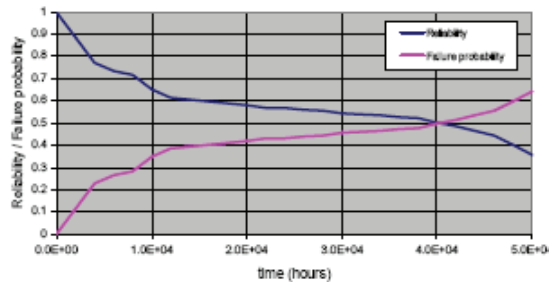


Figure 2: Confronto tra la funzione di distribuzione e l'affidabilità di un dispositivo

probabilità dell'istante di rottura  $T$ , risulta che

$$\mathbb{P}(t_1 \leq T \leq t_2) = \int_{t_1}^{t_2} f(t) dt$$

La densità di probabilità di una variabile aleatoria è sempre non negativa ed è integrata ad 1 sull'asse reale. In particolare, poiché  $T$  rappresenta un tempo il suo insieme di definizione è  $\mathbb{R}_+$  e quindi

$$\int_0^\infty f(t) dt = 1,$$

ciò significa che la probabilità che prima o poi la componente si rompa deve raggiungere l'unità. La funzione densità di probabilità è quasi ovunque data dalla derivata della funzione di distribuzione; d'altra parte la funzione di distribuzione di  $T$  è ottenibile come l'integrale calcolato sull'intervallo  $(0, t)$  della funzione densità di probabilità. Risulta inoltre che

$$\mathbb{P}(t_1 \leq T \leq t_2) = \int_{t_1}^{t_2} f(t) dt = F(t_2) - F(t_1)$$

**Definizione 3** Per tutti gli istanti  $t$  per i quali  $F(t) < 1$  la funzione frequenza istantanea di rischio (hazard rate), detta anche frequenza istantanea di guasto o **failure rate** (tasso di rottura) è:

$$r(t) = \lim_{h \rightarrow 0} \frac{1}{h} \frac{F(t+h) - F(t)}{R(t)} = \frac{f(t)}{R(t)}.$$

Per dare un'interpretazione probabilistica del failure rate osserviamo che per piccoli valori di  $h$  vale la seguente approssimazione:

$$r(t)h \simeq \frac{F(t+h) - F(t)}{R(t)} = \mathbb{P}(t \leq T < t+h | T \geq t) = \frac{f(t)}{R(t)}h.$$

Notiamo esplicitamente che il failure rate e la funzione densità di probabilità sono confrontabili, l'Esempio 2 mostra quantitativamente in cosa differiscono.

**Esempio 2** Un test di affidabilità su 16 lampadine ha dato i risultati riportati in Figura 3. Con riferimento all'intervallo di tempo  $(2,3)$ , si ha che

$$R(2) = \mathbb{P}(T > 2) = \frac{(16-5)}{16} = \frac{11}{16}, \quad f(2)\Delta t = f(2)1 = \frac{4}{16} = 0.25 \quad \text{se } 2 < t < 3$$

visto che in ogni istante di tempo appartenente all'intervallo  $(2,3)$  ci sono 4 componenti non funzionanti. Il prodotto  $f(t)\Delta t = f(t)1$  rappresenta la probabilità che una lampadina si fulmini nell'intervallo di tempo  $(2,3]$ . Dalla definizione segue quindi che  $r(t)1 = f(t)1/R(t)$  e quindi

$$r(2)1 = \frac{f(2)1}{R(2)} = \frac{4}{11} = 0.3625 \quad \text{se } 2 < t < 3.$$

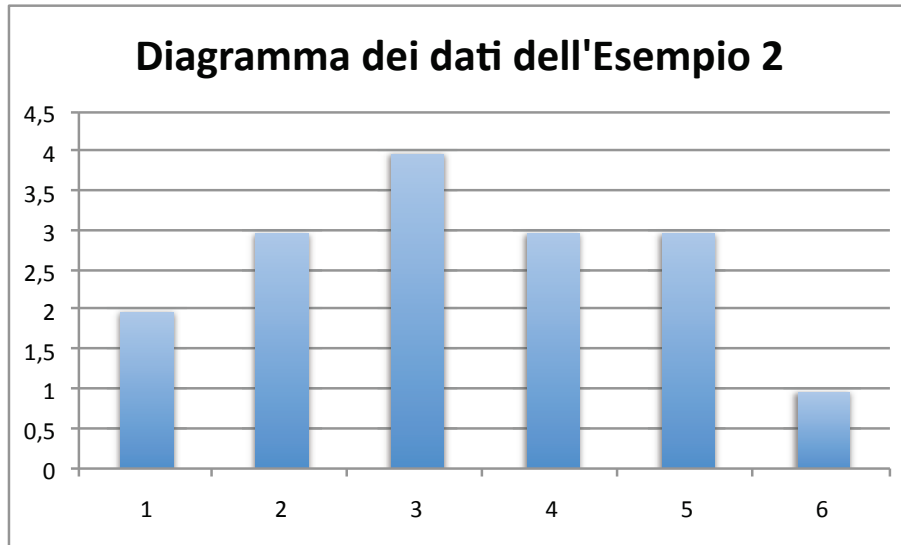


Figure 3: Risultato di un test effettuato su 16 lampadine.

Osserviamo che mentre  $f(t)\Delta t$  rappresenta la probabilità che si verifichi un guasto nell'intervallo di tempo  $(t, t + \Delta t)$  assumendo che le osservazioni siano fatte a partire dall'istante iniziale  $t = 0$ ,  $r(t)\Delta t$  approssima la probabilità che il guasto si verifichi nell'intervallo  $(t, t + \Delta t)$  supponendo che fino all'istante  $t$  non si siano avuti guasti. Quindi,  $r(t)\Delta t$  si riferisce ad una popolazione in generale meno numerosa. Ovviamente, se  $t$  tende a zero  $r(t)\Delta t$  tende a  $f(t)\Delta t$ .

In Figura 4 sono mostrati i grafici della densità di probabilità  $f(t)$  e della funzione frequenza istantanea di guasto. È possibile osservare che

- La curva relativa a  $f(t)$  è in ogni istante sottesa dalla curva  $r(t)$ , ciò deriva dalla definizione di  $r(t)$ . Infatti, il failure rate è definito in termini di  $1/R(t)$  e risulta che  $0 < R(t) < 1$
- La funzione di ripartizione  $F(a)$  rappresenta l'area sottesa da  $f(t)$  nell'intervallo  $(0, a)$ , per ogni  $t < a$
- La funzione di sopravvivenza  $R(a)$  assume un valore pari all'area sottesa alla curva  $f(t)$  e delimitata a sinistra dalla retta  $t = a$ , per ogni fissato  $t = a$ .

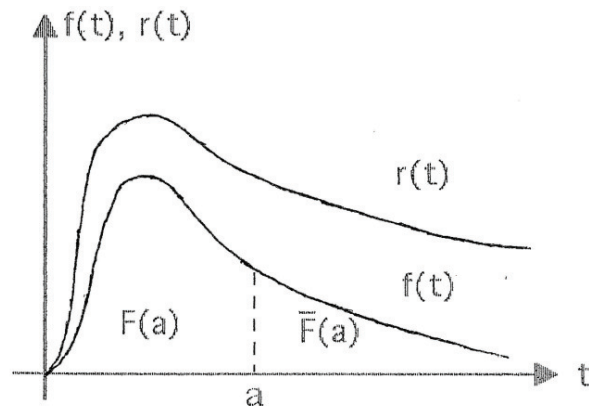


Figure 4: Grafico della densità di probabilità e del failure rate.

**Esempio 3** Un test di affidabilità è stato effettuato su 72 lampadine ed ha fornito i risultati mostrati nell'istogramma di Figura 5. Vogliamo graficare le funzioni  $f(t)$  e  $r(t)$ .

Dall'istogramma possiamo ottenere le informazioni statistiche riportate nelle prime tre colonne della Tabella 1 di Figura 6. La quarta e la quinta colonna possono essere ricavate a partire da tali informazioni. In particolare,  $f(t)$  è data dal rapporto tra il numero di guasti e 72,  $r(t) \equiv \lambda(t)$  è il rapporto tra il numero di guasti e il numero di lampadine funzionanti. Ad esempio,  $3/72 \simeq 0.0417$  e  $3/70 \simeq 0.429$ . Il grafico di Figura 6 è stato tracciato sulla base dei dati della quarta e della quinta colonna.

**Teorema 1** La densità di probabilità di guasto, l'affidabilità e il failure rate sono funzioni del tempo legate dalle seguenti relazioni:

$$R(t) = \exp\left\{-\int_0^t r(\tau) d\tau\right\}, \quad r(t) = -\frac{d}{dt} \log R(t), \quad f(t) = r(t)R(t) = r(t) \exp\left\{-\int_0^t r(\tau) d\tau\right\}.$$

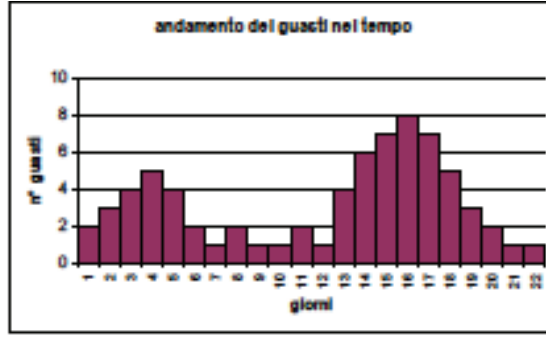


Figure 5: Istogramma del test di affidabilità dell'Esempio 3.

**Dimostrazione** Osserviamo che il failure rate è definito come una densità di probabilità condizionata, pertanto risulta non negativo ed è integrato a 1 su  $\mathbb{R}_+$ . Inoltre, si ha:

$$r(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{\mathbb{P}(T > t)} = \frac{1}{1 - F(t)} \frac{dF(t)}{dt}. \quad (1)$$

Da ciò segue in primo luogo che la densità di probabilità di guasto all'istante  $t$  si può esprimere in termini dell'affidabilità e del failure rate all'istante  $t$  essendo  $f(t) = r(t)R(t)$ . In secondo luogo, possiamo notare che  $F(t)$  si può ottenere integrando in  $t$  l'equazione differenziale (1), così facendo si ha che

$$-\ln[1 - F(t)] = \int_0^t r(\tau) d\tau \quad \Rightarrow \quad F(t) = 1 - \exp\left\{-\int_0^t r(\tau) d\tau\right\},$$

da ciò segue che l'affidabilità e il failure rate sono strettamente legate dalla seguente relazione:

$$R(t) = \exp\left\{-\int_0^t r(\tau) d\tau\right\}.$$

Osserviamo che nei casi in cui il failure rate è costante si può facilmente calcolare l'istante di tempo in cui si raggiunge un prefissato livello di affidabilità. Infatti, sotto tale ipotesi si ha che

$$R(t) = e^{-rt} = c \quad \Rightarrow \quad -rt = \ln c \quad \Rightarrow \quad t = -\ln c / r$$

che risulta sicuramente non negativo visto che  $c$  deve essere una probabilità e come tale deve appartenere all'intervallo  $[0, 1]$ .

**Esempio 4** Consideriamo una componente caratterizzata da failure rate costante  $r = 15 \cdot 10^{-6}/h$ . Vogliamo calcolare l'istante di tempo in cui si dimezza l'affidabilità di tale componente. Si desidera quindi calcolare l'istante  $t$  tale che  $R(t) = 1/2$ . Dato che  $r$  è costante si ha

$$\begin{aligned} R(t) = e^{-rt} = 1/2 & \Rightarrow \exp\{-15 \cdot 10^{-6}t\} = 1/2 \Rightarrow \ln(1/2) = \ln(\exp\{-15 \cdot 10^{-6}t\}) \\ & \Rightarrow \ln(1/2) = -15 \cdot 10^{-6}t \Rightarrow t = \ln 2 / 15 \cdot 10^{-6} \text{ ore,} \end{aligned}$$

da cui segue che all'istante  $t = 46210$  ore l'affidabilità si dimezza. Possiamo calcolare anche l'istante in cui si raggiunge un livello di affidabilità pari al 99.5%. Infatti, in tal caso si ha

$$t = -\frac{\ln 0.995}{15 \cdot 10^{-6}} = 334 \text{ ore.}$$

giorni	guasti	non guasti	$f(t)$	$\lambda(t)$
1	2	72	0,0278	0,0278
2	3	70	0,0417	0,0429
3	4	67	0,0596	0,0597
4	5	63	0,0694	0,0794
5	4	58	0,0556	0,0690
6	2	54	0,0278	0,0370
7	1	52	0,0139	0,0192
8	2	51	0,0278	0,0392
9	1	48	0,0139	0,0204
10	1	48	0,0139	0,0208
11	2	47	0,0278	0,0426
12	1	45	0,0139	0,0222
13	4	44	0,0556	0,0909
14	6	40	0,0833	0,1500
15	7	34	0,0972	0,2059
16	8	27	0,1111	0,2963
17	7	19	0,0972	0,3684
18	5	12	0,0694	0,4167
19	3	7	0,0417	0,4286
20	2	4	0,0278	0,5000
21	1	2	0,0139	0,5000
22	1	1	0,0139	1,0000

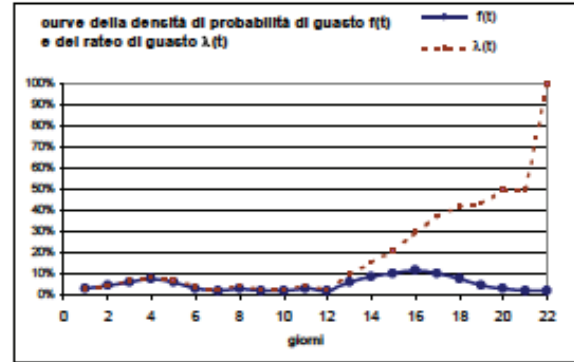


Figure 6: Nella Tabella sono mostrati i dati relativi all'Esempio 3; il grafico mostra la densità di probabilità e il failure rate per i dati mostrati nella Tabella

**Definizione 4** Il tempo medio di guasto, o vita media della componente, è definita come la media della variabile aleatoria  $T$ :

$$m = E(T) = \int_0^{\infty} t f(t) dt = - \int_0^{\infty} t R'(t) dt = -tR(t) \Big|_0^{\infty} + \int_0^{\infty} R(t) dt \equiv \int_0^{\infty} R(t) dt.$$

La vita media  $m$  costituisce un parametro significativo dell'affidabilità di una componente e viene spesso indicata con la sigla MTTF (mean time to failure). Nel caso di sistemi riparabili si distinguono due tempi medi:

- MTTF (mean time to first failure) che rappresenta il tempo medio intercorrente fra la messa in funzione e il verificarsi del primo guasto
- MTBF (mean time between failure) che rappresenta il tempo medio che intercorre fra due guasti successivi.

Se il sistema riparte dallo stato iniziale dopo ogni riparazione allora i due tempi medi MTBF e MTTF coincidono.



**Definizione 5** Si definisce vita media residua di una componente il rapporto

$$m(t) = \frac{\int_t^\infty R(\theta) d\theta}{R(t)}.$$

La funzione  $m(t)$  permette di valutare quanto tempo possa ancora mediamente durare una componente di età  $t$ , cioè che ha funzionato ininterrottamente dall'istante iniziale fino all'istante  $t$ . A differenza di  $m$ , che si riferisce all'istante iniziale,  $m(t)$  permette di effettuare delle stime sul guasto futuro di una componente in qualsiasi istante di tempo  $t$  sempre che la componente sia ancora funzionante in quell'istante. Osserviamo che pur essendo  $T$  la durata di vita iniziale della componente, nel caso in questione visto che è già trascorso un tempo  $t$ , rimane una durata di vita residua

$$T_t = T - t.$$

La funzione  $m(t)$  è il valor medio di  $T_t$ . Infatti, la funzione di ripartizione di  $T_t$  è data da

$$F_{T_t}(x) = \mathbb{P}(T_t \leq x) = \mathbb{P}(T - t \leq x | T > t) = \frac{\mathbb{P}(t < T \leq t + x)}{\mathbb{P}(T > t)} = \frac{F(t + x) - F(t)}{R(t)},$$

da cui segue che l'affidabilità residua è

$$R_{T_t}(x) = 1 - F_{T_t}(x) = \frac{R(t) - F(t + x) + F(t)}{R(t)} = \frac{1 - F(t + x)}{R(t)} = \frac{R(t + x)}{R(t)}.$$

Quindi, la vita media residua risulta:

$$m_t = E(T_t) = \int_0^\infty R_{T_t}(x) dx = \frac{\int_t^\infty R(\theta) d\theta}{R(t)} \equiv m(t).$$

## 2 Eventi casuali nella teoria dell'affidabilità

La teoria dell'affidabilità può essere studiata seguendo due approcci: quello basato sugli eventi casuali e quello basato sulle variabili aleatorie. In particolare, per poter studiare l'affidabilità di sistemi formati da più componenti collegate tra loro è necessario tener presente i concetti di unione e intersezione di eventi, nonché il concetto di indipendenza. A tale scopo consideriamo il seguente esempio.

**Esempio 5** Consideriamo un sistema di trasporto di fluidi su cui sono state installate due pompe (una vecchia e una più nuova) che lavorano indipendentemente l'una dall'altra e dalle altre componenti del sistema. L'affidabilità della pompa vecchia in uno specificato intervallo di tempo è 0.6 mentre per la pompa nuova, misurata sullo stesso intervallo di tempo è 0.8. Vogliamo valutare le probabilità che in uno specificato intervallo di tempo si verifichino i seguenti eventi:

- $E_1 = \{\text{ci sarà un completo rifornimento}\}$
- $E_2 = \{\text{ci sarà un rifornimento}\}$

- $E_3 = \{\text{non ci sarà alcun rifornimento}\}$
- $E_4 = \{\text{ci sarà un rifornimento insufficiente}\}.$

Formalizziamo il problema introducendo due eventi

- $A = \{\text{la pompa vecchia lavora ancora alla fine dell'intervallo di tempo}\},$
- $B = \{\text{la pompa nuova lavora ancora alla fine dell'intervallo di tempo}\}.$

Risulta:

$$\mathbb{P}(E_1) \equiv \mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B) = 0.6 \cdot 0.8 = 0.48$$

$$\mathbb{P}(E_2) \equiv \mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B) = 0.92$$

$$\mathbb{P}(E_3) \equiv \mathbb{P}(\bar{A} \cap \bar{B}) = [1 - \mathbb{P}(A)] [1 - \mathbb{P}(B)] = 0.4 \cdot 0.2 = 0.08$$

$$\mathbb{P}(E_4) \equiv \mathbb{P}[(A \cap \bar{B}) \cup (\bar{A} \cap B)] = \mathbb{P}(A \cap \bar{B}) + \mathbb{P}(\bar{A} \cap B) = \mathbb{P}(A)\mathbb{P}(\bar{B}) + \mathbb{P}(\bar{A})\mathbb{P}(B) = 0.44.$$

### 3 Affidabilità di componenti logicamente collegate in serie o in parallelo

Una componente si trova solitamente a dover operare all'interno di un sistema e questo comporta la sua interazione con tanti altri elementi, che concorrono al compimento di una missione. L'affidabilità di strutture costituite da una sola componente può essere calcolata come mostrato precedentemente. L'interazione della componente in analisi con il resto del sistema avviene attraverso connessioni fisiche e connessioni logiche. Strutture più complesse possono essere considerate come costituite da varie componenti collegate. Le connessioni fisiche dipendono da come è strutturato il sistema. Le connessioni logiche si fondano sulle risposte che le varie componenti forniscono durante le diverse fasi operative; in tal senso, per la ricerca dell'affidabilità di un sistema, occorre analizzare l'influenza che un guasto di una componente ha sulla funzionalità di quelle che la circondano e/o sull'intero sistema.

L'analisi di affidabilità combinatoria fornisce modelli per lo studio di strutture basate su varie forme di connessioni.

#### 3.1 Sistemi senza ridondanza

Dal punto di vista dell'affidabilità, un sistema si dice senza ridondanza se tutte le componenti che lo costituiscono devono lavorare correttamente per assicurare il pieno svolgimento della funzione richiesta. Si tratta di sistemi in cui la rottura o il fallimento di una sola delle componenti porta alla crisi dell'intero sistema. Per avere un'idea possiamo pensare ad una serie di lampadine di quelle che si usano per addobbare gli alberi di Natale: in questo caso è sufficiente che una sola lampadina sia fulminata perché l'insieme non si accenda. Una connessione in serie può essere rappresentata attraverso uno schema di flusso, detto *Reliability Block Diagram* (RBD), come mostrato in Figura 7 in cui con  $x_i$  sono state denotate le componenti funzionanti e con  $x'_i$  quelle

non funzionanti. Come mostrato in Figura 7, il diagramma a blocchi in questo caso è costituito dalla connessione in serie delle componenti che formano il sistema. Per semplificare la discussione assumiamo che ogni componente sia funzionante o meno indipendentemente l'una dall'altra. Per sistemi collegati in serie quest'assunzione non deve essere necessariamente verificata in quanto il primo guasto si presenta come guasto di sistema.

Consideriamo ora un sistema composto da  $n$  componenti indipendenti organizzate in serie. Defi-

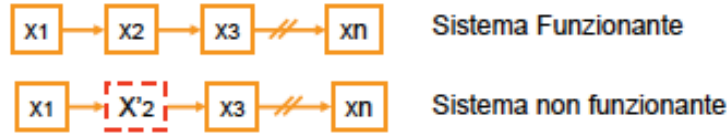


Figure 7: Esempio di RBD per componenti collegate in serie.

niamo i seguenti eventi:

$$S = \{\text{Il sistema lavora nell'intervallo } (0, t)\},$$

$$C_k = \{\text{La componente } k\text{-esima lavora nell'intervallo } (0, t)\}.$$

Per componenti collegate in serie l'evento  $S$  si realizza se e solo se tutti gli eventi  $C_k$  si realizzano. Pertanto, a causa dell'indipendenza del funzionamento di ciascuna componente, si avrà:

$$\mathbb{P}(S) = \mathbb{P}(C_1 \cap C_2 \cap \dots \cap C_n) = \mathbb{P}(C_1)\mathbb{P}(C_2) \dots \mathbb{P}(C_n). \quad (2)$$

Sia  $R_S(t) = \mathbb{P}(S)$  l'affidabilità del sistema e sia  $R_k(t) = \mathbb{P}(C_k)$  l'affidabilità della componente  $k$ -esima. Dalla (1) concludiamo che l'affidabilità di un sistema costituito da componenti collegate in serie è data dal prodotto delle affidabilità delle singole componenti.

Il tasso di rottura di un sistema senza ridondanza, ossia composto da componenti collegate in serie, costituito da elementi indipendenti è dato dalla somma dei singoli tassi di rottura. Infatti, ricordando la definizione di failure rate e facendo uso delle proprietà dei logaritmi segue che

$$r_S(t) \equiv -\frac{d}{dt} \log R_S(t) = -\frac{d}{dt} \log \prod_{i=1}^n R_{C_i}(t) = -\frac{d}{dt} \sum_{i=1}^n \log R_{C_i}(t) = -\sum_{i=1}^n \frac{d}{dt} \log R_{C_i}(t) \equiv \sum_{i=1}^n r_i(t).$$

Inoltre, se i singoli elementi hanno un tasso costante allora risulta che l'affidabilità del sistema è quella relativa alla distribuzione esponenziale caratterizzata da tasso costante così che il tempo medio che intercorre dall'istante iniziale a quello in cui si verifica il primo guasto è pari a  $1/r_S$ . In conclusione, nel caso di failure rates costanti, si ha:

$$r_S(t) \equiv r_S = \sum_{i=1}^n r_i, \quad R_S(t) = \exp\{-r_S t\}, \quad MTBF_S \equiv MTTF_S = \frac{1}{r_S}.$$

**Esempio 6** Consideriamo un sistema costituito da una pompa e da un filtro collegati in serie come mostrato in Figura 8. Assumiamo che i failure rates siano costanti; in particolare supponiamo che

$$r_{pompa} = 1.5 \cdot 10^{-4}/h, \quad r_{filtro} = 3 \cdot 10^{-5}/h.$$



Figure 8: Sistema pompa - filtro di cui all'Esempio 6.

Visto che i failure rates sono costanti possiamo calcolare il failure rate del sistema considerando la somma di  $r_{pompa}$  e  $r_{filtro}$ ; in questo modo risulta che

$$r_S = r_{pompa} + r_{filtro} = 1.5 \cdot 10^{-4} + 3 \cdot 10^{-5} = 1.8 \cdot 10^{-4}/h.$$

Pertanto, il tempo medio di guasto è

$$MTTF = MTBF = 1/r_S = 10^4/(1.8) h = 5.5555h.$$

Inoltre, la densità dei tempi di guasti, la distribuzione dei tempi di guasti e la funzione affidabilità per l'intero sistema risultano dati da

$$\begin{aligned} f_S(t) &= r_S \exp\{-r_S t\} = 1.8 \cdot 10^{-4} \exp\{-1.8 \cdot 10^{-4} t\}/h, \\ F_S(t) &= 1 - \exp\{-1.8 \cdot 10^{-4} t\}, \quad R_S(t) = \exp\{-1.8 \cdot 10^{-4} t\}. \end{aligned} \quad (3)$$

In particolare, se  $t = 8760 h$  ( $8760 = 365 \cdot 24$ ) si ha:

$$\begin{aligned} f_S(8760) &= 1.8 \cdot 10^{-4} \exp\{-1.8 \cdot 10^{-4} \cdot 8760\}/h = 3.7 \cdot 10^{-5}/h, \\ F_S(8760) &= 1 - \exp\{-1.8 \cdot 10^{-4} \cdot 8760\} = 0.7934, \\ R_S(8760) &= \exp\{-1.8 \cdot 10^{-4} \cdot 8760\} = 0.2066. \end{aligned}$$

Riconsideriamo ora una situazione generale. Osserviamo che se al sistema in esame si collega una nuova componente, si ottiene un nuovo sistema meno affidabile di quello originale; ciò è dovuto al fatto che le probabilità sono minori di 1.

Inoltre, sempre a causa del fatto che le probabilità di corretto funzionamento delle singole componenti sono minori dell'unità, segue che l'affidabilità di ogni singola componente è maggiore dell'affidabilità dell'intero sistema. Questa osservazione porta a concludere che l'affidabilità di un'organizzazione in serie non può essere migliorata a meno che non si migliora l'affidabilità di almeno una componente.

A parità di costo se si vuole migliorare l'affidabilità del sistema si deve intervenire sull'elemento caratterizzato da minore affidabilità; in altri termini, per migliorare l'affidabilità di un sistema composto da componenti organizzate in serie si deve aumentare l'affidabilità di quelle componenti "più deboli" e non di quelle che sono caratterizzate già da alta affidabilità.

Senza venir meno a generalità, supponiamo che le componenti siano state organizzate in ordine decrescente rispetto alle corrispondenti affidabilità in modo che risulti  $R_1 > R_2 > \dots > R_n$ .

Assumiamo, inoltre, che l'affidabilità della componente  $R_n$  sia aumentata a quella della componente più affidabile ( $R_n = R_1$ ). Ora l'affidabilità del nuovo sistema è minore dell'affidabilità della componente  $R_{n-1}$  che risulta la meno affidabile, miglioriamo anche la componente  $(n-1)$ -esima aumentando la sua affidabilità fino ad  $R_1$ .

Procedendo in questo modo si ottiene alla fine un sistema la cui affidabilità è pari a  $R_S = R_1^n$ . Questo è il massimo che possiamo ottenere.

**Esempio 7** Consideriamo un sistema costituito da due componenti caratterizzate da alta affidabilità  $R_c$  prossima ad 1 connesse da un'interfaccia la cui affidabilità  $r$  è molto minore di  $R_c$  (cf. Figura 9). Da quanto detto l'affidabilità di questo sistema è  $R_S = R_c^2 r \simeq r$ : Per migliorare il



Figure 9: Due componenti con affidabilità  $R_c$  sono connesse da un'interfaccia con affidabilità  $r$ .

sistema si deve migliorare l'affidabilità dell'interfaccia.

Un modo alternativo per indicare l'affidabilità di un sistema costituito da  $n$  componenti indipendenti ed identiche collegate in serie è

$$R_S = (1 - p)^n = \exp[n \ln(1 - p)] \quad (4)$$

dove  $p$  è la probabilità di fallimento della singola componente nell'intervallo  $(0, t)$ . A partire da questa espressione possiamo fornire una connessione tra la complessità di un sistema e la sua affidabilità. Infatti, dall'ultima espressione data in (2) notiamo che per valori di  $p \ll 1$  risulta che

$$\ln(1 - p) \simeq -p \quad (p \ll 1),$$

così che l'affidabilità diventa:

$$R_S \simeq \exp\{-pn\} \quad (p \ll 1),$$

questo permette di concludere che se il numero di componenti nel sistema aumenta da  $n$  a  $nk$ , per mantenere il sistema alle stesse prestazioni è necessario diminuire la probabilità di fallimento di ogni singola componente dello stesso fattore  $k$ .

Osserviamo esplicitamente che in un sistema costituito da un gran numero di componenti collegate in serie l'errore associato all'affidabilità predetta, data dalla (2), può essere significativo. Infatti, supponiamo che ogni componente sia caratterizzata da affidabilità predetta  $r$  così che l'affidabilità dell'intero sistema è  $R = r^n$ . Un errore relativo  $\Delta r/r = (r' - r)/r$  nella valutazione dell'affidabilità  $r$  conduce ad un errore relativo significativo nella valutazione dell'affidabilità predetta dell'intero

sistema  $\Delta R/R \simeq n\Delta r/r^1$ .

**Esempio 8** Consideriamo un sistema costituito da 35 componenti identiche e indipendenti connesse in serie. Sia  $r$  l'affidabilità stimata di una singola componente tale che  $0.96 < r < 0.98$ . Se  $r = 0.96$  allora l'affidabilità dell'intero sistema è  $R_S = 0.96^{35} \simeq 0.24$ , mentre se  $r = 0.98$  risulta  $R_S \simeq 0.49$ .

È possibile fornire una diversa interpretazione di quanto fin'ora detto. A tale scopo supponiamo che una componente possa rompersi a causa di  $n$  tipi indipendenti di rottura. L'evento  $S = \{\text{la componente funzionerà fino all'istante } t\}$  è uguale all'intersezione degli eventi  $S_i = \{\text{la componente sopravvive al tipo di rottura } i\text{-esimo}\}$ . La probabilità  $\mathbb{P}(S)$  è l'affidabilità  $R(t)$  della componente associata all'intervallo  $(0, t)$ , data dal prodotto

$$R(t) = \mathbb{P}(S_1) \mathbb{P}(S_2) \dots \mathbb{P}(S_n) = R_1(t) R_2(t) \dots R_n(t),$$

dove  $R_k(t)$  rappresenta la probabilità che la componente sopravviva al  $k$ -esimo guasto. Le probabilità di rottura prima dell'istante  $t$  associate ai singoli tipi di rottura sono  $F_k(t) = 1 - R_k(t)$ , così che la probabilità che la componente si rompa prima di  $t$  è

$$F(t) = 1 - R(t) = 1 - \prod_{k=1}^n [1 - F_k(t)]. \quad (5)$$

Osserviamo che, in generale, le cause di rottura possono non essere indipendenti. In questi casi l'affidabilità si esprime come prodotto di probabilità condizionate:

$$R(t) = \mathbb{P}(S_1) \mathbb{P}(S_2|S_1) \mathbb{P}(S_3|S_1 S_2) \dots \mathbb{P}(S_n|S_1 S_2 \dots S_{n-1}), \quad (6)$$

dove  $\mathbb{P}(S_k|S_1 S_2 \dots S_{k-1})$  denota la probabilità che la componente sopravviva alla  $k$ -esima causa di guasto dato che né la prima, né la seconda,  $\dots$  né la  $(k-1)$ -esima causa di guasto ha prodotto la rottura della componente. Due cause di rottura dipendenti possono essere:

- i) rottura causata da un guasto individuale
- ii) rottura dovuta ad un gruppo di difetti che si verificano all'interno di una zona critica.

Osserviamo infine che il tempo di funzionamento di un sistema costituito da  $n$  elementi collegati in serie è dato dal minimo dei tempi di funzionamento di ciascun elemento.

### 3.2 Sistemi con ridondanza

Molto spesso livelli di affidabilità più o meno alti possono essere raggiunti solo aggiungendo ridondanza al sistema. Un sistema ridondante è costituito da più componenti adibite allo svolgimento

---

<sup>1</sup>Osserviamo che

$$\frac{R' - R}{R} = \frac{1}{R} \left[ \sum_{k=0}^n \binom{n}{k} r^{n-k} (\Delta r)^k - r^n \right] = \frac{1}{r^n} \left[ \sum_{k=0}^n \binom{n}{k} r^{n-k} (\Delta r)^k - r^n \right] = \sum_{k=1}^n \binom{n}{k} \left(\frac{r}{r}\right)^{n-k} \left(\frac{\Delta r}{r}\right)^k \simeq n \frac{\Delta r}{r}$$

della stessa funzione. La ridondanza non implica necessariamente la duplicazione di hardware in quanto questa può essere implementata anche a livello di software o si può trattare di ridondanza temporale. Per evitare rotture nei singoli punti, gli elementi ridondanti dovrebbero essere realizzati, ossia progettati e costruiti, indipendentemente l'uno dall'altro. Tecnicamente la ridondanza può essere implementata considerando due o più elementi che lavorano parallelamente.

In Figura 10 è mostrato uno schema con due componenti collegate in parallelo. Più in generale, date due o più componenti, queste si dicono connesse in parallelo se si può garantire la funzionalità dell'intero sistema anche quando risulta attiva una sola delle componenti. Per avere un'idea

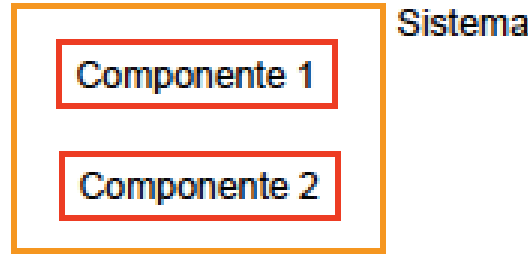


Figure 10: Schema con due componenti collegate in parallelo.

possiamo pensare ad una stanza illuminata da varie lampadine collegate in parallelo: in questo caso è sufficiente che una sola lampadina sia in funzione perché sia assicurata l'illuminazione della stanza.

**Osservazione** Consideriamo un sistema costituito da due componenti che lavorano in parallelo indipendentemente l'una dall'altra come mostrato nelle Figure 10 e 11. Definiamo i seguenti eventi

$A = \{\text{la componente A funziona fino all'istante } t\}$

$B = \{\text{la componente B funziona fino all'istante } t\}.$

Affinché il sistema in esame funzioni in  $(0, t]$  è necessario che in tale intervallo funzioni almeno una delle due componenti, questo si verifica con probabilità

$$\mathbb{P}(A)\mathbb{P}(B) + \mathbb{P}(A)[1 - \mathbb{P}(B)] + \mathbb{P}(B)[1 - \mathbb{P}(A)] = 1 - [1 - \mathbb{P}(A)][1 - \mathbb{P}(B)] = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A)\mathbb{P}(B).$$

Pertanto, l'affidabilità del sistema è:

$$R_S(t) = R_A(t) + R_B(t) - R_A(t)R_B(t).$$

Nel caso particolare in cui le due componenti sono identiche con failure rate costante pari ad  $r$  si ha che  $R_A(t) = R_B(t) = e^{-rt}$ , così che

$$R_S(t) = e^{-rt} + e^{-rt} - e^{-2rt} = 2e^{-rt} - e^{-2rt}.$$

Quindi, in questo caso il tempo medio di guasto è

$$MTTF_S = MTBF_S = \int_0^\infty R_S(t)dt = \int_0^\infty 2e^{-rt}dt - \int_0^\infty e^{-2rt}dt = \frac{2}{r} - \frac{1}{2r} = \frac{3}{2r},$$

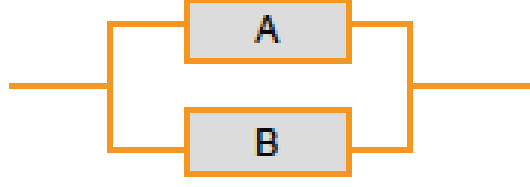


Figure 11: Sistema costituito da due componenti collegate in parallelo.

così che il failure rate del sistema è  $r_S = 1/MTTF_S = 2r/3$ .

**Esempio 9** Consideriamo due generatori elettrici dello stesso modello caratterizzati dalla stessa capacità ognuno dei quali funziona alla metà della propria capacità massima (cf. Figura 12). Supponiamo che il failure rate di ciascun generatore sia  $r_{generatore} = 9 \cdot 10^{-6}/h$ . Osserviamo

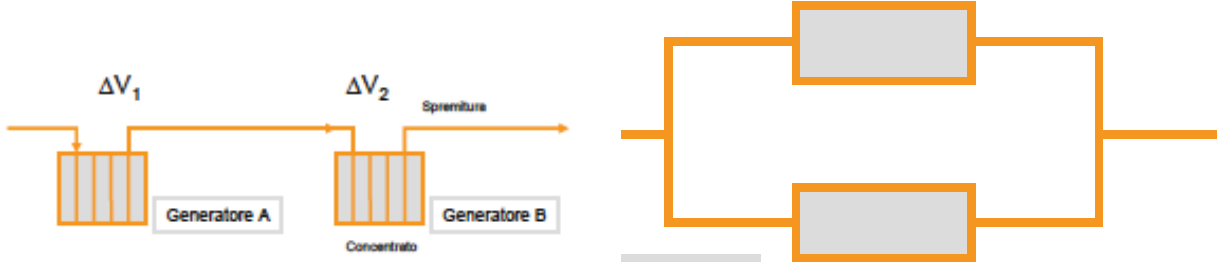


Figure 12: Ad illustrazione dell'Esempio 9, a sinistra è mostrato lo schema fisico e a destra lo schema affidabilistico.

in primo luogo che  $r_S = 2r_{generatore}/3 = 2 \cdot 9 \cdot 10^{-6}/3 = 6 \cdot 10^{-6}/h$ , ciò permette subito di affermare che il tempo medio di guasto del sistema è  $MTTF_S = 1/r_S = 166.667h$ .

Inoltre, l'affidabilità del sistema nell'intervallo  $(0, 8760]$  (8760 sono le ore in un anno) è

$$R_S(8760) = 2 \exp\{-9 \cdot 10^{-6} \cdot 8760\} - \exp\{-2 \cdot 9 \cdot 10^{-6} \cdot 8760\} = 0.99425,$$

da ciò segue immediatamente che

$$\begin{aligned} F_S(8760) &= 1 - R_S(8760) = 1 - 0.99425 = 5.75 \cdot 10^{-3}, \\ f_S(8760) &= r_S R_S(8760) = 6 \cdot 10^{-6} \cdot 0.99425 = 5.966 \cdot 10^{-6}. \end{aligned}$$

Una connessione parallela può essere rappresentata attraverso un RBD come indicato in Figura 13 in cui con  $x_i$  sono state indicate le componenti elementari che funzionano correttamente e con  $x'_i$  quelle fuori servizio. Assumiamo quindi che il sistema sia costituito da  $n$  componenti indipendenti organizzate in parallelo (cf. Figura 13). Consideriamo i seguenti eventi

$$S = \{\text{Il sistema lavora fino all'istante } t\}$$

$$C_k = \{\text{La componente } k\text{-esima lavora fino all'istante } t\}.$$



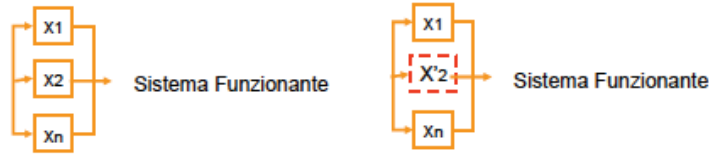


Figure 13: Esempio di RBD per componenti collegate in parallelo.

Per componenti collegate in parallelo l'evento  $S$  si realizza se e solo se almeno uno degli eventi  $C_k$  si realizza. In questo caso è preferibile ragionare sugli eventi complementari; a tal proposito ricordiamo che vale la seguente implicazione:

$$S = C_1 \cup C_2 \cup \dots \cup C_n \quad \Rightarrow \quad \bar{S} = \bar{C}_1 \cap \bar{C}_2 \cap \dots \cap \bar{C}_n.$$

Inoltre, se gli eventi  $C_i$  sono indipendenti risultano indipendenti anche gli eventi complementari così che risulta:

$$\mathbb{P}(\bar{S}) = \mathbb{P}(\bar{C}_1) \mathbb{P}(\bar{C}_2) \dots \mathbb{P}(\bar{C}_n).$$

Pertanto, segue che l'affidabilità di un sistema costituito da  $n$  componenti collegate in parallelo è data da

$$R = \mathbb{P}(S) = 1 - \mathbb{P}(\bar{S}) = 1 - [1 - \mathbb{P}(S_1)] \dots [1 - \mathbb{P}(S_n)] \equiv 1 - [1 - R_1] \dots [1 - R_n], \quad (7)$$

dove  $R_i$  rappresenta l'affidabilità della componente  $i$ -esima. Da questa relazione possiamo trarre due importanti conclusioni.

In primo luogo osserviamo che maggiore è il numero di componenti e maggiore risulta l'affidabilità complessiva del sistema. Infatti, se al sistema in esame si collega una nuova componente,  $C_{n+1}$ , si ottiene un nuovo sistema più affidabile di quello originale; ciò è dovuto al fatto che le probabilità sono minori dell'unità così che risulta:

$$\begin{aligned} [1 - R_1] \dots [1 - R_n] &> [1 - R_1] \dots [1 - R_n] [1 - R_{n+1}] \Rightarrow \\ &\Rightarrow 1 - [1 - R_1] \dots [1 - R_n] < 1 - [1 - R_1] \dots [1 - R_n] [1 - R_{n+1}]. \end{aligned}$$

Inoltre, possiamo osservare che l'affidabilità di un sistema organizzato in parallelo è maggiore dell'affidabilità di ogni singola componente; infatti risulta:

$$1 - [1 - R_1] \dots [1 - R_n] > R_i$$

visto che vale la seguente disuguaglianza

$$(1 - R_i) [1 - (1 - R_1) \dots (1 - R_{i-1}) (1 - R_{i+1}) \dots (1 - R_n)] > 0. \quad (8)$$

A riguardo di quest'ultima disuguaglianza possiamo osservare che  $(1 - R_i) > 0$ , perché rappresenta la probabilità che la componente  $i$ -esima si rompa prima dell'istante  $t$  così che la parentesi quadra che compare in (8) rappresenta l'affidabilità di un sistema costituito da  $n - 1$  componenti (le  $n$  originarie meno la  $i$ -esima), pertanto è anch'essa un termine positivo.

Osserviamo che il tempo di funzionamento di un sistema costituito da  $n$  elementi collegati in parallelo coincide con il massimo dei tempi di funzionamento di ciascun elemento.

In particolare, se  $R_i(t) = e^{-rt}$  si ha:

$$R_S(t) = 1 - (1 - e^{-rt})^n.$$

Inoltre, poiché risulta che

$$\sum_{k=1}^n \binom{n}{k} \frac{(-1)^{k+1}}{k} = \sum_{j=1}^n \frac{1}{j},$$

(la dimostrazione può essere effettuata per induzione) si ha che

$$\begin{aligned} MTTFS &= \int_0^\infty R_S(t) dt = \int_0^\infty [1 - (1 - e^{-rt})^n] dt = - \sum_{k=1}^n \binom{n}{k} (-1)^k \int_0^\infty e^{-rkt} dt \\ &= \sum_{k=1}^n \binom{n}{k} \frac{(-1)^{k+1}}{rk} = \frac{1}{r} \left[ 1 + \frac{1}{2} + \dots + \frac{1}{n} \right]. \end{aligned}$$

Quest'ultima relazione conferma ciò che ci si aspetta intuitivamente: più componenti colleghiamo in parallelo maggiore è la ridondanza e maggiore risulta il tempo medio di guasto.

Possiamo fornire una generalizzazione di quanto discusso finora. In particolare, consideriamo un sistema costituito da  $n$  elementi in parallelo ognuno caratterizzato da affidabilità  $R(t)$ . Assumiamo che il sistema funzioni se almeno  $k$  dei suoi elementi funzionano; un sistema di questo tipo si dice  $k$ -out-of- $n$  redundancy. Quindi, in un sistema  $k$ -out-of- $n$  redundancy non possono esserci più di  $n - k$  componenti non funzionanti. L'affidabilità dell'intero sistema può essere interpretata come la probabilità di osservare almeno  $k$  successi in  $n$  prove ripetute di Bernoulli caratterizzate da probabilità di successo  $p \equiv R(t)$ . In questo modo, facendo riferimento allo schema binomiale, risulta che

$$R_S(t) = \sum_{i=k}^n \binom{n}{i} R^i(t) [1 - R(t)]^{n-i}. \quad (9)$$

La (9) coincide con la (7) se  $R_i = R$ .

In letteratura, in aggiunta ai sistemi  $k$ -out-of- $n$  redundancy sono stati considerati dei sistemi il cui funzionamento è assicurato se non più di  $n - k$  elementi consecutivi falliscono. Strutture di questo tipo sono dette *consecutive*  $k$ -out-of- $n$  systems e risultano teoricamente più affidabili dei corrispondenti sistemi  $k$ -out-of- $n$  redundancy. Per un *consecutive*  $k$ -out-of- $n$  system costituito da  $n$  componenti identiche e indipendenti ognuna caratterizzata da affidabilità  $R$  risulta che

$$\begin{aligned} R_S &= Pr\{\text{non ci sono blocchi con più di } n - k \text{ elementi consecutivi in fallimento}\} \\ &= \sum_{i=0}^n g(n, i) R^{n-i} (1 - R)^i \end{aligned}$$

dove

$$\begin{aligned} g(j, i) &= \binom{j}{i} \quad \text{se } 0 \leq i \leq n - k, \quad g(a, a) = 0 \quad \text{se } a \geq n - k + 1, \\ g(a, b) &= g(a - 1, b) + g(a - 2, b - 1) + \dots + g(a - n + k - 1, b - n + k) \quad \text{altrove.} \end{aligned}$$

**Esempio 10** Consideriamo un sistema costituito da  $n = 5$  componenti identiche collegate in parallelo che lavorano indipendentemente l'una dall'altra caratterizzate ciascuna da affidabilità costante  $R$ . Supponiamo che il sistema sia funzionante se almeno  $k = 3$  elementi funzionano. Se il sistema è  $k$ -out-of- $n$  redundancy si ha che

$$R_S = R^5 + 5R^4(1 - R) + 10R^3(1 - R)^2.$$

Se invece si tratta di un sistema *consecutive*  $k$ -out-of- $n$  system, poiché risulta che

$$\begin{aligned} g(5, 0) &= 1, \\ g(5, 1) &= \binom{5}{1} = 5, \quad g(5, 2) = \binom{5}{2} = 10, \quad g(5, 4) = g(4, 4) + g(3, 3) + g(2, 2) = 0 + 0 + 1 = 1, \\ g(5, 3) &= g(4, 3) + g(3, 2) + g(2, 1) = g(3, 3) + g(2, 2) + g(1, 1) + \binom{3}{2} + \binom{2}{1} \\ &= g(2, 2) + g(1, 1) + 3 + 2 = \binom{2}{2} + \binom{1}{1} + 3 + 2 = 7, \end{aligned}$$

segue che

$$R_S = R^5 + 5R^4(1 - R) + 10R^3(1 - R)^2 + 7R^2(1 - R)^3 + R(1 - R)^4.$$

È evidente che l'affidabilità di questo secondo schema è maggiore dell'affidabilità del primo schema di un termine pari a  $7R^2(1 - R)^3 + R(1 - R)^4$ . Osserviamo esplicitamente che per i applicazioni di questo tipo si dovrebbe verificare accuratamente l'assunzione di indipendenza tra le componenti.

### 3.3 Sistemi con componenti collegate in serie e in parallelo

Il comportamento di un sistema con componenti logicamente collegate in serie e in parallelo può essere analizzato applicando in successione le considerazioni per i sistemi con componenti in serie o in parallelo. Per illustrare la procedura consideriamo alcuni esempi.

**Esempio 11** Un sistema costituito da 7 elementi collegati in serie e in parallelo (cf. Figura 14) che lavorano indipendentemente l'uno dall'altro. Assumiamo che la componente  $E_i$  sia caratterizzata da affidabilità  $R_i(t)$  e da failure rate costante  $r_i$ .

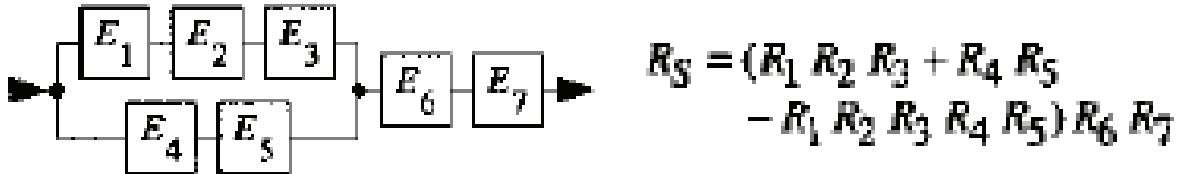


Figure 14: Sistema con componenti collegate in serie e in parallelo (Esempio 11).

*Passo 1:* Il gruppo di elementi  $E_1$ ,  $E_2$  e  $E_3$ , che risultano collegati in serie, è sostituito dall'elemento  $E_8$ , inoltre la coppia di elementi  $E_4$  e  $E_5$  è sostituita da  $E_9$  e la coppia  $E_6$  e  $E_7$  con  $E_{10}$ . Così facendo si ottiene lo schema di Figura 15. Osserviamo che i nuovi elementi sono caratterizzati

dalle seguenti affidabilità

$$R_8(t) = R_1(t)R_2(t)R_3(t), \quad R_9(t) = R_4(t)R_5(t), \quad R_{10}(t) = R_6(t)R_7(t)$$

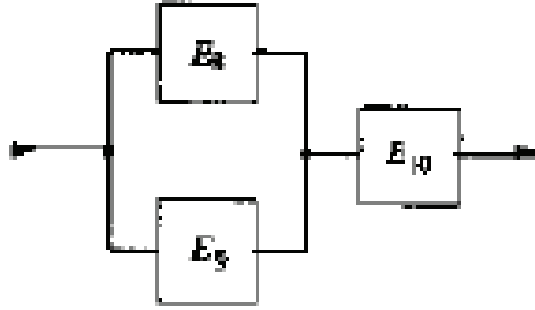


Figure 15: Riduzione dello schema mostrato in Figura 14 (Esempio 11).

*Passo 2:* Il gruppo di elementi  $E_8$  e  $E_9$ , che risultano collegati in parallelo, è sostituito dall'elemento  $E_{11}$  caratterizzato da affidabilità  $R_{11}(t) = R_8(t) + R_9(t) - R_8(t)R_9(t)$ .

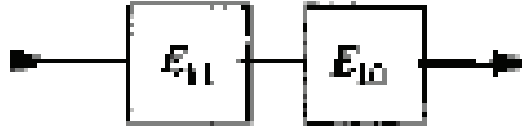


Figure 16: Riduzione dello schema mostrato in Figura 15 (Esempio 11).

*Passo 3:* Dai passi 1 e 2 deriviamo l'affidabilità del sistema:

$$\begin{aligned} R_S(t) &= R_{11}(t)R_{10}(t) = [R_8(t) + R_9(t) - R_8(t)R_9(t)]R_6(t)R_7(t) \\ &= [R_1(t)R_2(t)R_3(t) + R_4(t)R_5(t) - R_1(t)R_2(t)R_3(t)R_4(t)R_5(t)]R_6(t)R_7(t), \end{aligned} \quad (10)$$

cioè

$$R_S(t) = R_1(t)R_2(t)R_3(t)R_6(t)R_7(t) + R_4(t)R_5(t)R_6(t)R_7(t) - R_1(t)R_2(t)R_3(t)R_4(t)R_5(t)R_6(t)R_7(t).$$

Visto che abbiamo assunto che i failure rate dei singoli elementi sono costanti, possiamo scrivere che

$$R_S(t) = \exp\{-(r_1+r_2+r_3+r_6+r_7)t\} + \exp\{-(r_4+r_5+r_6+r_7)t\} - \exp\{-(r_1+r_2+r_3+r_4+r_5+r_6+r_7)t\}$$

così che risulta:

$$MTTF = \int_0^\infty R(t) dt = \frac{1}{r_1 + r_2 + r_3 + r_6 + r_7} + \frac{1}{r_4 + r_5 + r_6 + r_7} - \frac{1}{r_1 + r_2 + r_3 + r_4 + r_5 + r_6 + r_7}.$$

**Esempio 12** Consideriamo il sistema di Figura 17 costituito da 8 elementi collegati in serie e in parallelo che lavorano indipendentemente l'uno dall'altro. Assumiamo che la componente  $E_i$  sia caratterizzata da affidabilità  $R_i(t)$  e da failure rate costante  $r_i$ . Per prima cosa riduciamo

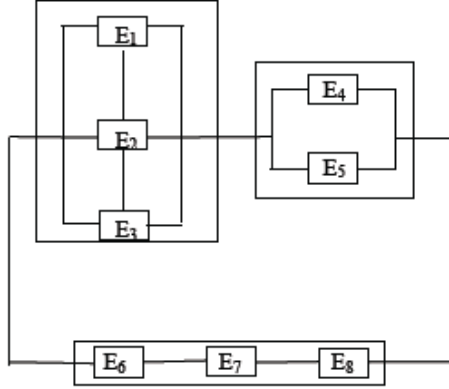


Figure 17: Sistema con componenti in serie e in parallelo dell'Esempio 12.

le componenti in parallelo ad una sola componente avente affidabilità data dall'affidabilità del sottosistema corrispondente; allo stesso tempo riduciamo le tre componenti collegate in serie ad una sola componente caratterizzata dalla corrispondente affidabilità. Così facendo avremo un nuovo sistema costituito da tre componenti, come mostrato in Figura 18, aventi rispettivamente affidabilità:



Figure 18: Riduzione dello schema di Figura 17

$$R_{123} = 1 - (1 - R_1)(1 - R_2)(1 - R_3), \quad R_{45} = 1 - (1 - R_4)(1 - R_5), \quad R_{678} = R_6 R_7 R_8.$$

Più precisamente si ha:

$$R_{123} = R_1(t) + R_2(t) + R_3(t) - R_1(t)R_2(t) - R_1(t)R_3(t) - R_2(t)R_3(t) + R_1(t)R_2(t)R_3(t)$$

$$R_{45}(t) = R_4(t) + R_5(t) - R_4(t)R_5(t), \quad R_{678}(t) = R_6(t)R_7(t)R_8.$$

Procedendo nella riduzione, si possono “assemblare” le due componenti in serie producendo una nuova componente di affidabilità

$$R_{12345}(t) = R_{123}(t)R_{45}(t) = [R_1(t) + R_2(t) + R_3(t) - R_1(t)R_2(t) - R_1(t)R_3(t) - R_2(t)R_3(t) + R_1(t)R_2(t)R_3(t)][R_4(t) + R_5(t) - R_4(t)R_5(t)]. \quad (11)$$

Quest'ultimo passo riduce il sistema a due componenti collegate in parallelo di cui è facilmente calcolabile l'affidabilità che risulta essere:

$$R_S(t) = 1 - [1 - R_{12345}(t)][1 - R_{678}(t)] = R_{12345}(t) + R_{678}(t) - R_{12345}(t)R_{678}(t).$$

**Esempio 13** Consideriamo un sistema costituito solo da 2 componenti collegate in serie come mostrato in Figura 19. È possibile aumentare l'affidabilità del sistema in due modi diversi:



Figure 19: Due componenti collegate in serie (Esempio 13).

- i) aggiungendo ridondanza sull'intero sistema (cf. Figura 20 caso i))
- ii) includendo ridondanza sulle singole componenti (cf. Figura 20 caso ii)).

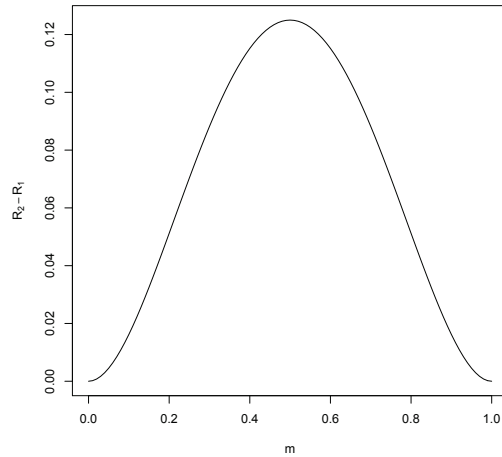


Figure 20: Due diversi modi per aumentare la ridondanza; grafico della differenza tra le affidabilità calcolate nei due casi (Esempio 13).

Confrontiamo l'affidabilità delle due riorganizzazioni.

Nel caso i) abbiamo due componenti collegate in parallelo e ognuna di esse è costituita da due componenti collegate in serie ognuna caratterizzata da affidabilità  $m^2$ . Pertanto, l'affidabilità dell'intero sistema è

$$R_1 = 1 - (1 - m^2)(1 - m^2) = 1 - (1 - 2m^2 + m^4) = m^2(2 - m^2).$$

Nel caso ii) abbiamo due componenti collegate in serie, ognuna di esse è costituita da due componenti collegate in parallelo per le quali l'affidabilità è  $1 - (1 - m)(1 - m) = m(2 - m)$ . Pertanto, l'affidabilità dell'intero sistema è

$$R_2 = m^2(2 - m)^2.$$

Osserviamo che

$$R_2 - R_1 = m^2(2 - m)^2 - m^2(2 - m^2) = m^2(4 - 4m + m^2 - 2 + m^2) = 2m^2(1 - 2m + m^2) = 2m^2(1 - m)^2 > 0.$$

Quindi, l'affidabilità nel caso i) è minore dell'affidabilità nel caso ii). In Figura 20 è mostrato anche il grafico della differenza  $R_2 - R_1$ .

L'Esempio 13 mostra un principio generale:

*La ridondanza a livello di singole componenti è più efficiente della ridondanza a livello di sistema.*

**Esempio 14** Consideriamo il sistema di Figura 21 e supponiamo che ad un certo istante di tempo fissato le affidabilità delle singole componenti siano  $R_1 = 0.95$ ,  $R_2 = 0.99$ ,  $R_3 = 0.70$ ,  $R_4 = 0.75$ ,  $R_5 = 0.9$ . L'affidabilità dell'intero sistema allo stesso istante di tempo risulta data da

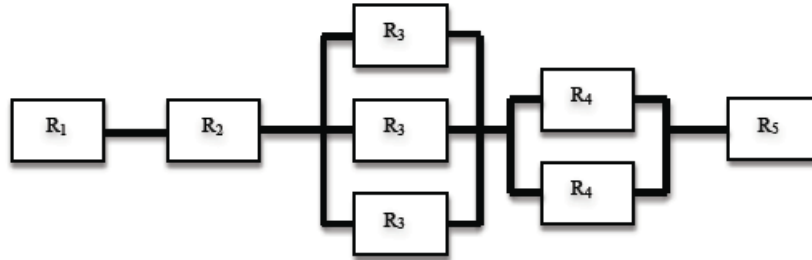


Figure 21: Sistema con componenti collegate in serie e in parallelo (Esempio 14).

$$R_S = 0.95 \cdot 0.99 \cdot [1 - (1 - 0.7)^3] \cdot [1 - (1 - 0.75)^2] \cdot 0.9 = 0.772.$$

### 3.4 Ridondanza a maggioranza

La ridondanza a maggioranza è un caso particolare della  $k$ -out-of- $n$  redundancy che si usa frequentemente nei circuiti digitali con ridondanza, ma non solo in essi. Supponiamo che  $2n + 1$  output vadano ad alimentare un dispositivo, detto voter (elettore), il cui output è dato dalla maggioranza dei suoi  $2n + 1$  segnali. L'analisi di un dispositivo di questo tipo è basata sulla procedura descritta precedentemente per le strutture organizzate in serie-parallelo. Queste strutture realizzano in modo semplice una metodologia di "tolleranza di errori" senza l'uso di dispositivi di controllo.

**Esempio 15** Consideriamo il sistema di Figura 22. In questo caso il voter è l'elemento  $E_v$  ed è alimentato dai tre segnali in input provenienti dai dispositivi  $E_1$ ,  $E_2$  ed  $E_3$ . Una struttura

di questo tipo può essere utilizzata come dispositivo di allarme. In questo caso l'affidabilità del sistema è

$$R_S(t) = [1 - (1 - R_1(t))(1 - R_2(t))(1 - R_3(t))]R_\nu(t) \\ = [R_1(t) + R_2(t) + R_3(t) - R_2(t)R_3(t) - R_1(t)R_2(t) - R_1(t)R_3(t) + R_1(t)R_2(t)R_3(t)]R_\nu(t).$$

Assumendo che  $R_i(t) = R(t)$ , si ha che

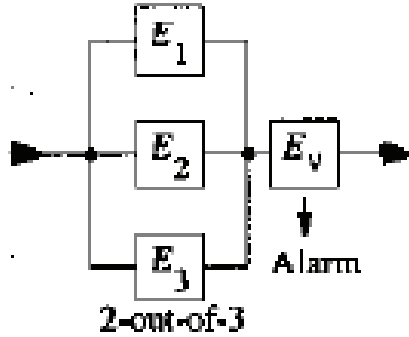


Figure 22: Esempio di dispositivo con ridondanza a maggioranza (Esempio 15).

$$R_S(t) = [3R(t) - 3R^2(t) + R^3(t)]R_\nu(t).$$

Se inoltre assumiamo che il sistema, costituito da elementi con la stessa affidabilità, sia 2-out-of-3, allora, scegliendo  $k = 2$  e  $n = 3$  nella (9) segue che

$$R_{\tilde{S}}(t) = [3R^2(t) - 3R^3(t) + R^3(t)]R_\nu(t) = [3R^2(t) - 2R^3(t)]R_\nu(t).$$

Notiamo che se tutte le componenti sono caratterizzate dalla stessa affidabilità  $R(t)$ , dalle ultime due relazioni si ottiene:

$$R_S(t) - R_{\tilde{S}}(t) = R_\nu(t) [3R(t) - 3R^2(t) + R^3(t) - 3R^2(t) + 2R^3(t)] = 3R(t)R_\nu(t)[1 - R(t)]^2.$$

Una ridondanza a maggioranza può essere realizzata tramite software. In particolare si può usare *N-version programming* (NVP), nota anche con il nome *multiversion programming*. Si tratta di un metodo o un processo dell'ingegneria del software in cui i programmi multipli funzionalmente equivalenti sono generati indipendentemente a partire dalle stesse specifiche iniziali. Il concetto di *N-version programming* fu introdotto nel 1977 da Liming Chen e Algirdas Avizienis con la principale congettura che l'indipendenza di programmi si sforza di ridurre fortemente la probabilità di software identico che si presenta in due o più versioni del programma. Lo scopo dell'NVP è quello di assicurare l'affidabilità delle operazioni software costruendo sistemi fault tolerance.

## 4 Affidabilità di sistemi con strutture complesse

Nel presente contesto, consideriamo complesso un sistema che ha un diagramma a blocco di affidabilità che non si può ridurre ad una struttura in serie-parallelo costituita da componenti



indipendenti; ciò può accadere o perché non ci riusciamo o perché non esiste un simile diagramma. Ad esempio, non esiste un diagramma a blocco quando si devono considerare più di due stati (in funzione/non in funzione) per ogni elemento, oppure quando esiste più di uno stato per stabilire il fuori uso di una componente. Comunque, lo schema in serie/parallelo in generale non funziona nei sistemi distribuiti o quando gli elementi compaiono nel sistema più di una volta. L'espressione "elementi indipendenti" si riferisce all'indipendenza per quanto riguarda l'effetto della componente sulla rottura del sistema. L'analisi di strutture complesse può diventare difficile e richiedere tempo. Comunque, esistono metodologie ben sviluppate che possono essere utilizzate quando il diagramma a blocco esiste e il sistema soddisfa i seguenti requisiti:

- solo un tipo di ridondanza (quella parallela) è considerata
- gli elementi possono comparire più di una volta nel diagramma di affidabilità, ma elementi diversi sono indipendenti
- le operazioni di on/off sono affidabili al 100% altrimenti il loro effetto deve essere considerato nel diagramma a blocco di affidabilità con le restrizioni precedenti.

Sotto queste assunzioni l'analisi può essere sviluppata con un modello booleano. Ai fini pratici sono efficienti anche metodi euristici come il *key item method* e il *successful path method*.

## 4.1 Key Item Method

Questo metodo è basato sul teorema delle alternative. Infatti, in questo caso si verifica la situazione in cui l'evento "il sistema funziona senza rotture nell'intervallo  $(0, t)$ " o, più brevemente "il sistema è on in  $(0, t)$ " si può scomporre in due eventi complementari:  $\{\text{l'elemento } E_i \text{ è up e il sistema è up in } (0, t)\}$ ,  $\{\text{l'elemento } E_i \text{ fallisce e il sistema è up in } (0, t)\}$ .

Cominciamo col definire un insieme di alternative.

**Definizione** Sia  $(\Omega, \mathcal{A}, \mathbb{P})$  uno spazio di probabilità<sup>2</sup> e sia  $B$  un evento di  $\mathcal{A}$ . Una famiglia  $\{B_n; n = 1, 2, \dots, k\}$  di eventi di  $\mathcal{A}$  costituisce un insieme di alternative per  $B$  se sono soddisfatte le seguenti proprietà:

- (i)  $B_i \cap B_j = \emptyset \quad (i, j = 1, 2, \dots, k; i \neq j)$ ;
- (ii)  $\bigcup_{n=1}^k B_n = B$ ;
- (iii)  $\mathbb{P}(B_n) > 0$  per  $n = 1, 2, \dots, k$ .

Se  $B = \Omega$ , le condizioni (i), (ii) e (iii) si dicono individuare un "insieme completo" di alternative.

In particolare la (i) afferma che gli eventi  $B_1, B_2, \dots, B_k$  sono incompatibili, e quindi alternativi, mentre la (ii) esprime la circostanza che tali eventi sono anche necessari per  $B$ .

---

<sup>2</sup>A partire da un esperimento casuale avente spazio campione  $\Omega$  si può costruire uno spazio di probabilità dato dalla terna  $(\Omega, \mathcal{A}, \mathbb{P})$ , dove  $\mathcal{A}$  è la minima sigma-algebra costruita su una classe di sottoinsiemi di  $\Omega$  e  $\mathbb{P}$  è una misura di probabilità definita su  $\mathcal{A}$ .

**Legge delle alternative** Sia  $\{B_n; n = 1, 2, \dots, k\}$  un insieme completo di alternative e sia  $A$  un evento di  $\mathcal{A}$ . Risulta:

$$\mathbb{P}(A) = \sum_{n=1}^k \mathbb{P}(A|B_n) \mathbb{P}(B_n). \quad (12)$$

**Dimostrazione** Poiché per ipotesi gli eventi dell'insieme  $\{B_n; n = 1, 2, \dots, k\}$  sono a due a due incompatibili, tali sono anche gli eventi dell'insieme  $\{A \cap B_n; n = 1, 2, \dots, k\}$ . Inoltre, poiché  $\bigcup_{n=1}^k B_n = \Omega$ , si ha:

$$\mathbb{P}(A) = \mathbb{P}(A \cap \Omega) = \mathbb{P}\left(A \cap \bigcup_{n=1}^k B_n\right) = \mathbb{P}\left(\bigcup_{n=1}^k (A \cap B_n)\right) = \sum_{n=1}^k \mathbb{P}(A \cap B_n),$$

da cui, facendo uso della regola moltiplicativa segue la (12).

La legge delle alternative permette di calcolare la probabilità a priori di  $A$  conoscendo le probabilità  $\mathbb{P}(B_n)$  delle alternative e le probabilità condizionate  $\mathbb{P}(A|B_n)$ .

**Esempio 16** Data un'urna contenente biglie numerate con gli interi da 1 a 9 si estragga con equiprobabilità una biglia e successivamente, senza reinserire la prima biglia nell'urna, se ne estragga una seconda. Si calcoli la probabilità che la seconda biglia estratta abbia numero pari.

Si considerino gli eventi  $A_i = \{\text{la } i\text{-esima biglia estratta ha numero pari}\}$  ( $i = 1, 2$ ). Dalla legge delle alternative segue:

$$\mathbb{P}(A_2) = \mathbb{P}(A_1) \mathbb{P}(A_2|A_1) + \mathbb{P}(\overline{A_1}) \mathbb{P}(A_2|\overline{A_1}) = \frac{4}{9} \cdot \frac{3}{8} + \frac{5}{9} \cdot \frac{4}{8} = \frac{4}{9}.$$

**Esempio 17** Supponiamo che quotidianamente vengano esaminate le condizioni metereologiche in una prefissata regione. Si consideri l'evento  $A_j = \{\text{il } j\text{-esimo giorno in esame non è piovoso}\}$  ( $j = 1, 2, \dots$ ) e si supponga che  $\mathbb{P}(A_{j+1}|A_j) = \beta$  e  $\mathbb{P}(A_{j+1}|\overline{A_j}) = \alpha$  con  $\alpha$  e  $\beta$  numeri arbitrari interni all'intervallo  $(0, 1)$ . Si intende calcolare  $\mathbb{P}(A_j)$  ( $j = 1, 2, \dots$ ).

Dalla legge delle alternative segue:

$$\mathbb{P}(A_{j+1}) = \mathbb{P}(A_j) \mathbb{P}(A_{j+1}|A_j) + \mathbb{P}(\overline{A_j}) \mathbb{P}(A_{j+1}|\overline{A_j}) = \mathbb{P}(A_j) \beta + [1 - \mathbb{P}(A_j)] \alpha,$$

da cui si ha:

$$\mathbb{P}(A_{j+1}) = (\beta - \alpha) \mathbb{P}(A_j) + \alpha \quad (j = 1, 2, \dots).$$

Abbiamo ottenuto un'equazione ricorsiva, la cui soluzione, ricavata in modo iterativo, è la seguente:

$$\begin{aligned} \mathbb{P}(A_j) &= (\beta - \alpha)^{j-1} \mathbb{P}(A_1) + \alpha \sum_{i=0}^{j-2} (\beta - \alpha)^i \\ &= (\beta - \alpha)^{j-1} \mathbb{P}(A_1) + \alpha \frac{1 - (\beta - \alpha)^{j-1}}{1 - (\beta - \alpha)} \quad (j = 1, 2, \dots). \end{aligned}$$

Si noti che il limite

$$\lim_{j \rightarrow +\infty} \mathbb{P}(A_j) = \frac{\alpha}{1 - \beta + \alpha}$$

non dipende da  $\mathbb{P}(A_1)$ ; ciò indica che con il trascorrere dei giorni la probabilità di non avere pioggia tende a non dipendere dalla probabilità con cui ha piovuto il primo giorno.

Il teorema delle alternative permette di calcolare l'affidabilità del sistema. Infatti denotando con  $R_i(t)$  l'affidabilità dell'elemento  $E_i$ , si ha:

$$R_S(t) = R_i(t)P\{\text{il sistema è up in } (0, t)|E_i \text{ è up in } (0, t)\} \\ + [1 - R_i(t)]P\{\text{il sistema è up in } (0, t)|E_i \text{ fallisce in } (0, t)\}.$$

I seguenti esempi mostrano due situazioni tipiche

**Esempio 18 (Struttura bridge)** In Figura 23 è mostrato il diagramma di affidabilità di una struttura bridge con una connessione bidirezionale. L'elemento  $E_5$  può lavorare rispetto alla sua

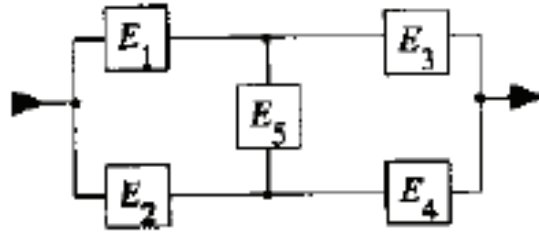


Figure 23: Diagramma di affidabilità di una struttura bridge bidirezionale (Esempio 18).

funzione in entrambe le direzioni: da  $E_1$  a  $E_4$  via  $E_5$  e da  $E_2$  a  $E_3$  via  $E_5$ . L'elemento  $E_5$  si trova quindi in una posizione chiave. Questa proprietà permette di applicare la metodologia precedentemente illustrata. Pertanto, si devono analizzare le situazioni: a)  $E_5$  è up e b)  $E_5$  è down, che danno luogo agli schemi mostrati in Figura 24. L'affidabilità del sistema è pertanto



Figure 24: Due alternative per il diagramma di affidabilità della struttura bridge di Figura 23 (Esempio 18).

$$R_S(t) = R_5(t)[R_1(t) + R_2(t) - R_1(t)R_2(t)][R_3(t) + R_4(t) - R_3(t)R_4(t)] \\ + [1 - R_5(t)][R_1(t)R_3(t) + R_2(t)R_4(t) - R_1(t)R_3(t)R_2(t)R_4(t)].$$

Lo stesso procedimento si applica alla struttura bridge di Figura 25 anche se in questo caso l'elemento chiave deve essere diverso da  $E_5$ . Scegliendo  $E_4$  o  $E_1$  come elemento chiave possiamo applicare il teorema delle alternative.

Assumiamo che l'elemento chiave sia  $E_4$ . Se  $E_4$  è up il sistema di Figura 25 è costituito da due componenti collegate in parallelo (cf. Figura 26), segue che l'affidabilità è:

$$R_S(t) = R_4(t)\{R_2(t) + R_1(t)[R_3(t) + R_5(t) - R_3(t)R_5(t)] - R_1(t)R_2(t) \\ \times [R_3(t) + R_5(t) - R_3(t)R_5(t)]\} + [1 - R_4(t)]R_1(t)R_3(t).$$

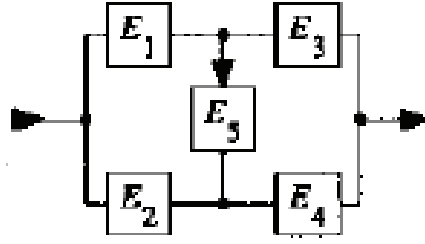


Figure 25: Diagramma di affidabilità di una struttura bridge unidirezionale (Esempio 18).

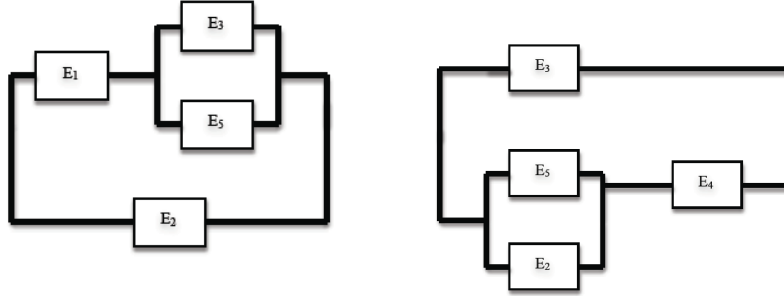


Figure 26: Con riferimento alla Figura 25, a sinistra è stato scelto  $E_4$  come elemento chiave, a destra l'elemento chiave scelto è  $E_1$ .

Assumendo che l'elemento chiave sia  $E_1$  si perviene allo stesso risultato. Infatti, anche in questo caso quando  $E_1$  è up il sistema di Figura 25 si interpreta come costituito da due componenti collegate in parallelo (cf. Figura 26), così che la sua affidabilità è:

$$R_S(t) = R_1(t) \{ R_3(t) + R_4(t) [R_2(t) + R_5(t) - R_2(t)R_5(t)] - R_3(t)R_4(t) \times [R_2(t) + R_5(t) - R_2(t)R_5(t)] \} + [1 - R_1(t)] R_2(t)R_4(t).$$

**Esempio 17** Consideriamo il sistema di Figura 27. Analizziamo come cambia l'affidabilità dal primo caso al secondo caso assumendo che gli elementi siano indipendenti e caratterizzati da affidabilità  $R_{E_1}(t) = R_{E_1'}(t) = R_{E_1''}(t) = R_1(t)$  e  $R_{E_2}(t) = R_{E_2'}(t) = R_2(t)$ .

Nel primo caso l'elemento  $E_1'$  è in posizione chiave così che risulta:

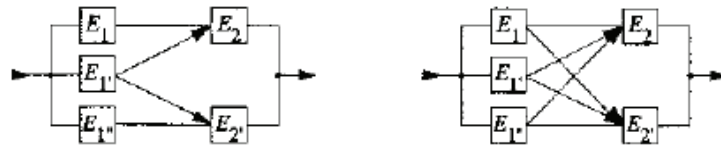


Figure 27: Diagrammi di affidabilità relativo all'Esempio 17.

$$R_a(t) = R_1(t) \{ 2R_2(t) - [R_2(t)]^2 \} + [1 - R_1(t)] \{ 2R_1(t)R_2(t) - [R_1(t)R_2(t)]^2 \}.$$

Infatti, se  $R_1 = 1$  allora l'affidabilità del sistema 1-out-of-3 è  $1 - (1 - R_1)^3 \equiv R_1 + R_1 + 1 + R_1^2 - R_1^2 - R_1 - R_1 = 1$ . Lo schema del secondo caso rappresenta una connessione in serie di un

1-out-of-3 redundancy con un sistema 1-out-of-2 redundancy; pertanto si ha:

$$\begin{aligned} R_b(t) &= \{3R_1(t)[1 - R_1(t)]^2 + 3[R_1(t)]^2[1 - R_1(t)] + [R_1(t)]^3\} \{2R_2(t)[1 - R_2(t)] + [R_2(t)]^2\} \\ &= R_1(t)R_2(t) \{3 - 3R_1(t) + [R_1(t)]^2\} [2 - R_2(t)]. \end{aligned}$$

Osserviamo che

$$\begin{aligned} R_b(t) - R_a(t) &= R_1(t)R_2(t) \{3 - 3R_1(t) + [R_1(t)]^2\} [2 - R_2(t)] - R_1(t) \{2R_2(t) - [R_2(t)]^2\} \\ &\quad + [1 - R_1(t)] \{2R_1(t)R_2(t) - [R_1(t)R_2(t)]^2\} = 2R_1(t)R_2(t)[1 - R_2(t)][1 - R_1(t)]^2. \end{aligned}$$

La differenza  $R_b(t) - R_a(t)$  diventa massima per  $R_1(t) = 1/3$  e  $R_2(t) = 1/2$ ; in questo caso  $R_b(t) = 57/108$  e  $R_a(t) = 49/108$  così che la differenza massima è

$$\max[R_b(t) - R_a(t)] = \frac{57}{108} - \frac{49}{108} = \frac{2}{27}.$$

Quindi, in termini di affidabilità la soluzione proposta nel secondo caso è vantaggiosa anche se di poco.

**Esempio 18** Un dispositivo di confronto è costituito da 4 dispositivi di misurazione (termometro, manometro, voltmetro, ...) e 2 dispositivi di controllo (cf. Figura 28). I dispositivi di misurazione misurano una specifica caratteristica (temperatura, pressione, voltaggio, ...) in due zone separate del sistema denotate con A e B. I dispositivi di controllo sono identici e confrontano la lettura dei dispositivi di misura; essi spediscono un segnale quando si registra una differenza significativa tra le misure rilevate nelle due zone. Per registrare una differenza critica nelle quantità registrate nelle due zone è richiesto solo un dispositivo di controllo  $p$ . Una volta che è stata registrata una differenza critica viene spedito un segnale. Si utilizza anche un trasmettitore per trasmettere i dati da un dispositivo di controllo all'altro. Supponiamo che l'affidabilità di ogni dispositivo di misurazione sia  $m$  e assumiamo che l'affidabilità del trasmettitore di dati sia  $c$ . Vogliamo calcolare la probabilità con cui verrà spedito un segnale nel caso di una differenza critica tra le quantità misurate nelle zone A e B.

Questo tipo di dispositivo di confronto è ampiamente utilizzato nelle applicazioni. Infatti, se

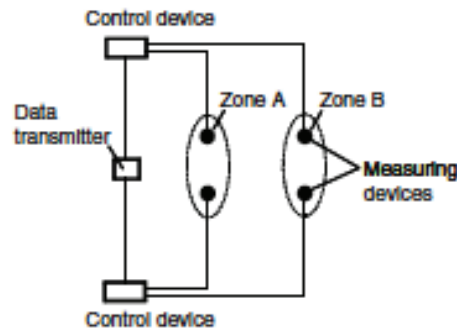


Figure 28: Un diagramma funzionale di un dispositivo di confronto (Esempio 18).

per esempio le misure effettuate indicano un gradiente di concentrazione critica tra le due zone, il

segnale può azionare un dispositivo che elimina questo gradiente. Nel caso di una differenza critica di pressione, il segnale può azionare l'apertura di una valvola che livelli la pressione; nel caso di una differenza significativa di temperatura, il segnale può fermare il riscaldamento/raffreddamento per limitare l'ampiezza dello sforzo termico indotto dal gradiente termico; infine, nel caso di una differenza critica di misure del potenziale nelle due zone di un circuito, il segnale può azionare un interruttore di sicurezza che protegge il circuito.

L'organizzazione logica nel generico dispositivo di confronto è rappresentata dal diagramma a blocco mostrato in Figura 29. Nel diagramma  $m$  denota l'affidabilità dei dispositivi di misurazione,

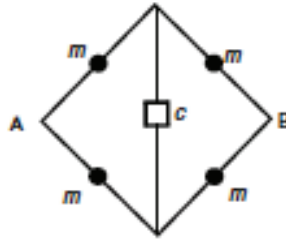


Figure 29: Blocco di affidabilità di un dispositivo di confronto (Esempio 18).

mentre  $c$  è l'affidabilità del dispositivo di trasmissione dei dati. La probabilità che il dispositivo di confronto invii un segnale nel caso esista una discrepanza significativa tra le misurazioni effettuate è uguale alla probabilità che esista un cammino tra i nodi A e B del grafo. Consideriamo gli eventi  $S = \{\text{il dispositivo di confronto sta lavorando su una richiesta}\}$  e  $C = \{\text{il trasmettitore di dati sta lavorando su una richiesta}\}$ . L'affidabilità del diagramma a blocchi si può calcolare considerando separatamente i casi in cui il trasmettitore è in funzione o non lo è (cf. Figura 30).

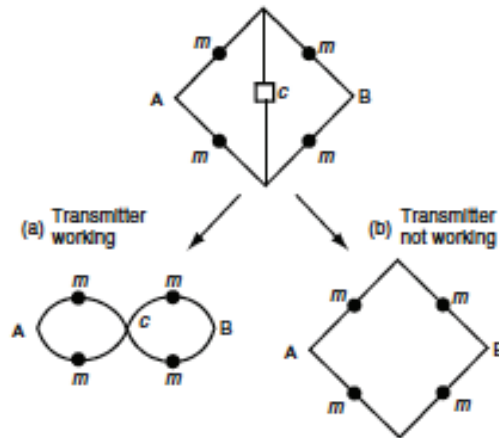


Figure 30: Diagramma a blocchi derivato dalla Figura 29.

Dall'Esempio 13 (Paragrafo 3) si ha:

$$\mathbb{P}(S|C) = m^2(2 - m)^2, \quad \mathbb{P}(S|\overline{C}) = m^2(2 - m^2),$$

così che, dalla formula delle alternative, risulta:

$$\mathbb{P}(S) = \mathbb{P}(S|C) \mathbb{P}(C) + \mathbb{P}(S|\bar{C}) \mathbb{P}(\bar{C}) = c [m^2(2 - m)^2] + (1 - c) [m^2(2 - m^2)].$$

Osserviamo che la probabilità  $\mathbb{P}(S)$  è lineare rispetto all'affidabilità  $c$  del trasmettitore. In particolare, l'affidabilità del dispositivo di confronto decresce linearmente dal valore  $m^2(2 - m)^2$ , quando  $c = 1$ , al valore  $m^2(2 - m^2)$  corrispondente a  $c = 0$ . Il caso  $c = 1$  corrisponde alla situazione di un trasmettitore perfetto, che si può approssimare bene considerando come dispositivo di trasmissione un semplice cavo. Il caso  $c = 0$  corrisponde invece alla situazione in cui il trasmettitore è sconnesso. Per tutti gli altri valori di  $c$ , l'affidabilità del dispositivo di confronto è un valore compreso tra i due casi limite illustrati.

## 4.2 Blocco di affidabilità con componenti ripetute

Spesso si incontrano situazioni in cui il diagramma a blocco per il calcolo dell'affidabilità è caratterizzato dal fatto che qualche componente compare più di una volta. Queste situazioni possono essere analizzate col metodo dell'elemento chiave analizzato prima.

**Esempio 19** Consideriamo il diagramma di Figura 31. In questo caso possiamo assumere

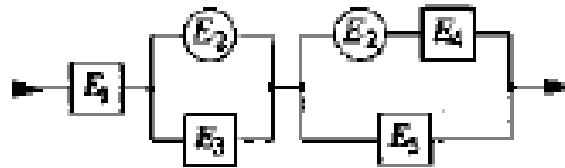


Figure 31: Diagramma di affidabilità per l'Esempio 19.

che l'elemento  $E_2$  sia in posizione chiave; così che, denotando con  $R_i(t)$  l'affidabilità di  $E_i$  nell'intervallo  $(0, t)$  si ha che

$$R_S(t) = R_1(t)R_2(t)[R_4(t) + R_5(t) - R_4(t)R_5(t)] + R_1(t)[1 - R_2(t)]R_3(t)R_5(t).$$

Notiamo esplicitamente che per il sottosistema costituito dalla composizione di  $E_2$  e  $E_3$  collegate in parallelo; se  $E_2$  funziona l'affidabilità è  $R_2 + R_3 - R_2R_3 = 1 + R_3 - R_3 = 1$ .

**Esempio 20** Consideriamo il diagramma di Figura 32. In questo caso possiamo applicare il

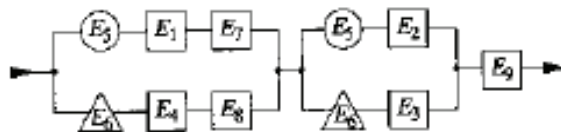


Figure 32: Diagramma di affidabilità per l'Esempio 20.

metodo precedente in successione scegliendo come elemento chiave prima  $E_5$  e poi  $E_6$ , o viceversa. Così facendo si ottiene:

$$\begin{aligned}
R_S(t) = & R_5(t)R_9(t)\{R_6(t)[R_1(t)R_7(t) + R_4(t)R_8(t) - R_1(t)R_7(t)R_4(t)R_8(t)] \\
& \times [R_2(t) + R_3(t) - R_2(t)R_3(t)] + [1 - R_6(t)]R_1(t)R_2(t)R_7(t)\} \\
& + [1 - R_5(t)]R_3(t)R_4(t)R_6(t)R_8(t)R_9(t).
\end{aligned}$$

### 4.3 Successful Path Method

In questo paragrafo e nel prossimo introduciamo due metodi generali. Per fissare le idee consideriamo il blocco di affidabilità di Figura 33, notiamo che gli elementi  $E_3$  ed  $E_4$  compaiono due volte. Il metodo del cammino di successo si basa sul seguente principio intuitivo:

*Il sistema esegue la funzione richiesta se esiste almeno un cammino tra l'input e l'output i cui elementi espletano tutti la loro funzione.*

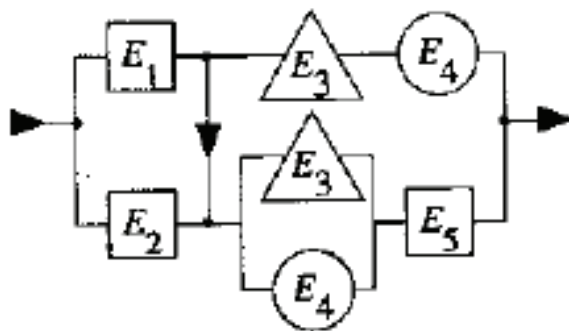


Figure 33: Diagramma di affidabilità di una struttura complessa.

I cammini devono essere orientati da sinistra a destra e non devono contenere cicli. Inoltre, se le connessioni sono orientate si devono rispettare gli orientamenti.

**Esempio 21** L'affidabilità del sistema di Figura 33 può essere calcolata come la probabilità dell'unione di tutti i cammini che portano dall'input all'output. Così, denotando con  $A_i = \{l'elemento E_i \text{ è up in } (0, t)\}$ , si ha:

$$R_S(t) = P\{(A_1 \cap A_3 \cap A_4) \cup (A_1 \cap A_3 \cap A_5) \cup (A_1 \cap A_4 \cap A_5) \cup (A_2 \cap A_3 \cap A_5) \cup (A_2 \cap A_4 \cap A_5)\},$$

da cui, ricordando il principio di inclusione-esclusione, segue che l'affidabilità del sistema in  $(0, t)$  è:

$$\begin{aligned} R_S(t) = & R_1(t)R_3(t)R_4(t) + R_1(t)R_3(t)R_5(t) + R_1(t)R_4(t)R_5(t) + R_2(t)R_3(t)R_5(t) + R_2(t)R_4(t)R_5(t) \\ & - 2R_1(t)R_3(t)R_4(t)R_5(t) - R_1(t)R_2(t)R_3(t)R_5(t) - R_1(t)R_2(t)R_4(t)R_5(t) \\ & - R_2(t)R_3(t)R_4(t)R_5(t) + R_1(t)R_2(t)R_3(t)R_4(t)R_5(t). \end{aligned}$$



#### 4.4 Metodo basato sullo spazio degli stati

Per definire lo stato del sistema all'istante  $t$  assegniamo ad ogni componente  $E_i$  del sistema un indicatore  $\zeta_i(t)$  tale che  $\zeta_i(t) = 1$  finché  $E_i$  non fallisce e  $\zeta_i(t) = 0$  altrimenti. Il vettore costituito dalle componenti  $\zeta_i(t)$  definisce lo stato del sistema all'istante  $t$ . Per ipotesi nell'intervallo  $(0, t]$  ogni elemento del sistema fallisce o meno indipendentemente l'uno dall'altro, ciò comporta che all'istante  $t$  un sistema costituito da  $n$  elementi può trovarsi in uno dei  $2^n$  possibili stati. Dopo aver elencato tutti i  $2^n$  possibili stati in cui può trovarsi il sistema, si evidenziano quelli in cui il sistema può espletare le funzioni richieste, la probabilità che il sistema si trovi in uno di questi ultimi stati costituisce l'affidabilità del sistema considerato.

**Esempio 22** Consideriamo il sistema descritto dal diagramma a blocco di Figura 33. Questo sistema è costituito da 5 componenti così che il sistema può trovarsi in uno dei  $2^5 = 32$  possibili stati elencati nell'ultima riga della tabella in Figura 34. Un "1" in questa tabella indica che l'elemento corrispondente (o il sistema nel caso dell'ultima riga) è up nell'intervallo di tempo  $(0, t]$ . Osserviamo esplicitamente che le informazioni contenute nella tabella di Figura 33 possono

$E_1$	10101010101010101010101010101010
$E_2$	11001100110011001100110011001100
$E_3$	11110000111100001111000011110000
$E_4$	11111111000000001111111100000000
$E_5$	11111111111111110000000000000000
$S$	11101110111000001010000000000000

Figure 34: Spazio degli stati del sistema di Figura 32.

essere espresse anche in termini di unioni di intersezioni di eventi. Infatti, denotando con  $E_i$  l'evento  $\{\text{il componente } C_i \text{ è up}\}$ , dal diagramma di Figura 33 segue che l'evento  $E = \{\text{il sistema è up}\}$  si realizza se e solo se risulta:

$$\begin{aligned} & (E_1 \cap E_2 \cap E_3 \cap E_4 \cap E_5) \cup (\bar{E}_1 \cap E_2 \cap E_3 \cap E_4 \cap E_5) \cup (E_1 \cap \bar{E}_2 \cap E_3 \cap E_4 \cap E_5) \cup \\ & \cup (E_1 \cap E_2 \cap \bar{E}_3 \cap E_4 \cap E_5) \cup (\bar{E}_1 \cap E_2 \cap \bar{E}_3 \cap E_4 \cap E_5) \cup (E_1 \cap \bar{E}_2 \cap \bar{E}_3 \cap E_4 \cap E_5) \cup \\ & \cup (E_1 \cap E_2 \cap E_3 \cap \bar{E}_4 \cap E_5) \cup (\bar{E}_1 \cap E_2 \cap E_3 \cap \bar{E}_4 \cap E_5) \cup (E_1 \cap \bar{E}_2 \cap E_3 \cap \bar{E}_4 \cap E_5) \cup \\ & \cup (E_1 \cap E_2 \cap E_3 \cap E_4 \cap \bar{E}_5) \cup (E_1 \cap \bar{E}_2 \cap E_3 \cap E_4 \cap \bar{E}_5), \end{aligned}$$

da cui, dopo qualche semplificazione, si ottiene:

$$\begin{aligned} & (E_2 \cap E_3 \cap E_5) \cup (E_1 \cap E_3 \cap E_4 \cap \bar{E}_5) \cup (E_1 \cap \bar{E}_2 \cap E_3 \cap \bar{E}_4 \cap E_5) \cup \\ & \cup (E_1 \cap \bar{E}_2 \cap E_4 \cap E_5) \cup (E_2 \cap \bar{E}_3 \cap E_4 \cap E_5). \end{aligned}$$

Pertanto si può concludere che l'affidabilità del sistema di Figura 32 è:

$$\begin{aligned} R_S(t) = \mathbb{P}\{ & (E_2 \cap E_3 \cap E_5) \cup (E_1 \cap E_3 \cap E_4 \cap \bar{E}_5) \cup (E_1 \cap \bar{E}_2 \cap E_3 \cap \bar{E}_4 \cap E_5) \cup \\ & \cup (E_1 \cap \bar{E}_2 \cap E_4 \cap E_5) \cup (E_2 \cap \bar{E}_3 \cap E_4 \cap E_5) \} \end{aligned}$$

che, svolgendo i calcoli, conduce al risultato ottenuto con il metodo del Successful Path Method. Osserviamo esplicitamente che, a differenza di quanto è accaduto con il metodo Successful Path Method, in questo caso tutti gli eventi coinvolti nella valutazione dell'affidabilità sono incompatibili.

#### 4.5 Metodo della funzione booleana

Il metodo della funzione booleana formalizza e generalizza i due metodi precedenti (del cammino di successo e dello spazio degli stati). Per questa analisi oltre alle assunzioni già fatte, ossia

- solo un tipo di ridondanza (quella parallela) è considerata
- gli elementi possono comparire più di una volta nel diagramma di affidabilità, ma elementi diversi sono indipendenti
- le operazioni di on/off sono affidabili al 100% altrimenti il loro effetto deve essere considerato nel diagramma a blocco di affidabilità

è necessario richiedere che il sistema sia coerente, ossia:

- lo stato del sistema dipende dallo stato di tutti i suoi elementi, in particolare il sistema è up se tutti i suoi elementi sono up ed è down se tutti i suoi elementi sono down;
- se il sistema è down nessun fallimento aggiuntivo può riportare il sistema in uno stato up (si tratta di una forma di monotonia).

Nel caso di sistemi riparabili l'ultima di queste assunzioni deve essere estesa diventando:

- se il sistema è up rimane in questo stato se un qualche elemento è riparato.

Nella realtà la maggior parte dei sistemi è coerente. Nel seguito useremo up per indicare che il sistema è in uno stato operativo e down per indicare il sistema è in uno stato di fallimento o in riparazione se il sistema è riparabile.

Sia

$$\Phi = \Phi(\zeta_1, \zeta_2, \dots, \zeta_n) = \begin{cases} 1 & \text{se il sistema è up} \\ 0 & \text{se il sistema è down,} \end{cases}$$

dove  $\zeta_i = \zeta_i(t)$  è la funzione indicatrice dell'elemento  $i$ -esimo che vale 1 se  $C_i$  è up e zero altrimenti. Inoltre risulta che  $\Phi$  dipende da tutte le variabili  $\zeta_i$  ed è non decrescente così che vale 1 se tutte le  $\zeta_i = 1$  e vale zero se  $\zeta_i = 0$  per  $i = 1, 2, \dots, n$ .

Osserviamo che  $R_i(t) = \mathbb{P}[\zeta_i(t) = 1]$ , inoltre, visto che le  $\zeta_i$  sono funzioni binarie si ha che

$$R_i(t) = \mathbb{P}[\zeta_i(t) = 1] = \mathbb{E}[\zeta_i(t)] \quad \text{con} \quad R_i(0) = 1.$$

Un ragionamento analogo si applica anche a  $\Phi$  perché è anch'essa una funzione binaria, pertanto si ha:

$$R_S(t) = \mathbb{P}\{\Phi[\zeta_1(t), \zeta_2(t), \dots, \zeta_n(t)] = 1\} = \mathbb{E}\{\Phi[\zeta_1(t), \zeta_2(t), \dots, \zeta_n(t)]\}.$$

Osserviamo esplicitamente che spesso calcolare  $\mathbb{E}[\Phi]$  è più semplice che calcolare  $\mathbb{P}(\Phi = 1)$ . Quindi, per calcolare l'affidabilità del sistema è necessario determinare la funzione booleana  $\Phi$ . Per fare questo, sono disponibili due metodi molto intuitivi:

**Metodo minimal path set** Un insieme  $\Pi_i$  di elementi è un minimal path set se il sistema è up quando  $\zeta_j(t) = 1$  per tutti gli elementi  $E_j$  che appartengono a  $\Pi_i$  e  $\zeta_k(t) = 0$  per tutti gli elementi  $E_k$  che non appartengono a  $\Pi_i$ , ma questo non si applica ai sottoinsiemi di  $\Pi_i$ .

Ad esempio, per il sistema di Figura 35 segue che  $\{1, 3\}$ ,  $\{2, 4\}$ ,  $\{1, 5, 4\}$ ,  $\{2, 5, 3\}$  sono insiemi di minimo cammino. Gli elementi  $E_j$  in  $\Pi_i$  formano un sistema con componenti collegate in serie la cui funzione di sistema è

$$\Phi_{\Pi_i} = \prod_{j: E_j \in \Pi_i} \zeta_j.$$

Se nel sistema ci sono  $r$  minimal path sets allora questi insiemi costituiscono un sistema con

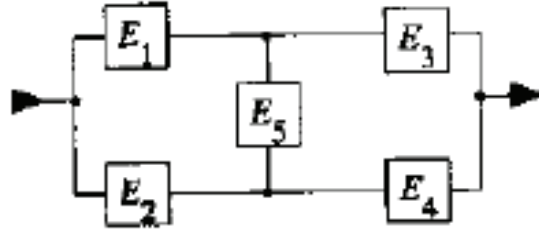


Figure 35: Diagramma di affidabilità di una struttura bridge

componenti collegate in parallelo così che risulta:

$$\Phi = \Phi(\zeta_1, \zeta_2, \dots, \zeta_n) = 1 - \prod_{i=1}^r (1 - \Phi_{\Pi_i}) = 1 - \prod_{i=1}^r \left( 1 - \prod_{j: E_j \in \Pi_i} \zeta_j \right)$$

**Metodo minimal cut set** Un insieme  $C_i$  è un minimal cut set se il sistema è down quando  $\zeta_j(t) = 0$  per tutti gli elementi  $E_j$  che appartengono a  $C_i$  e  $\zeta_k(t) = 1$  per tutti gli elementi  $E_k$  che non appartengono a  $C_i$ , ma questo non si applica ai sottoinsiemi di  $C_i$ .

Ad esempio, per il sistema di Figura 35 segue che  $\{1, 2\}$ ,  $\{3, 4\}$ ,  $\{1, 5, 4\}$ ,  $\{2, 5, 3\}$  sono insiemi di minimo taglio. Gli elementi  $E_j$  in  $C_i$  formano un sistema con componenti collegate in parallelo; pertanto, il sistema funziona se esiste almeno una componente  $E_j \in C_i$  tale che  $\zeta_j = 1$  ne segue che relativamente al taglio  $C_i$  la funzione di sistema è

$$\Phi_{C_i} = 1 - \prod_{E_j \in C_i} (1 - \zeta_j).$$

Quando nel sistema ci sono  $m$  minimal cuts possiamo dedurre che ci sono  $m$  componenti collegate in serie, pertanto il sistema funziona se in ogni taglio funziona almeno un elemento, quindi si ha:

$$\Phi = \Phi(\zeta_1, \zeta_2, \dots, \zeta_n) = \prod_{i=1}^m \Phi_{C_i} = \prod_{i=1}^m \left( 1 - \prod_{E_j \in C_i} (1 - \zeta_j) \right).$$

Osserviamo esplicitamente che un sistema con  $n$  elementi collegate in serie ha un unico path set mentre i cut sets sono  $n$  così come un sistema con  $n$  componenti collegate in parallelo ha un unico cut set e  $n$  path sets.

Esistono algoritmi che individuano sia insiemi di minimo taglio che gli insiemi di cammino minimo. Comunque, individuata la funzione di sistema possiamo calcolare l'affidabilità del sistema. Infatti, da quanto fin'ora detto si deduce che

$$\begin{aligned} R_S(t) &= \mathbb{P}\{\Phi_{\Pi_1} = 1, \text{ oppure } \dots, \Phi_{\Pi_r} = 1\} = \mathbb{P}\{\Phi_{C_1} = 1, \text{ e } \dots, \Phi_{C_m} = 1\} \\ &= 1 - \mathbb{P}\{\Phi_{C_1} = 0, \text{ oppure } \dots, \Phi_{C_m} = 0\}, \end{aligned}$$

con la condizione iniziale  $R_S(0) = 1$ . Osserviamo che, facendo uso della disuguaglianza di Boole, si ricavano i seguenti limiti:

$$1 - \sum_{i=1}^m \mathbb{P}\{\Phi_{C_i} = 0\} \leq R_S(t) \leq \sum_{i=1}^r \mathbb{P}\{\Phi_{\Pi_i} = 1\}.$$

In particolare, se gli insiemi di minimo taglio sono mutualmente esclusivi la disuguaglianza di sinistra è soddisfatta con l'uguaglianza così come quando gli insiemi di minimo cammino sono disgiunti la disuguaglianza di destra è soddisfatta con l'uguaglianza. Inoltre, si può dimostrare che

$$1 - \sum_{i=1}^m \mathbb{P}\{\Phi_{C_i} = 0\} \leq R_S(t) \leq 1 - \left(1 - \frac{(m-1)q}{2}\right) \sum_{i=1}^r \mathbb{P}\{\Phi_{C_i} = 1\},$$

dove  $q = \max\{1 - R_1(t), \dots, 1 - R_n(t)\}$ . Quest'ultima relazione può essere utilizzata per fornire una buona approssimazione dell'affidabilità di sistemi complessi.

**Esempio 23** Con riferimento all'Esempio 21, l'evento individuato per valutare l'affidabilità del sistema, ossia

$$\{(A_1 \cap A_3 \cap A_4) \cup (A_1 \cap A_3 \cap A_5) \cup (A_1 \cap A_4 \cap A_5) \cup (A_2 \cap A_3 \cap A_5) \cup (A_2 \cap A_4 \cap A_5)\},$$

è formato dagli insiemi di cammino minimo per il diagramma di affidabilità di Figura 36. Pertanto, facendo uso del metodo qui illustrato si ottiene

$$\Phi(\zeta_1, \dots, \zeta_5) = 1 - (1 - \zeta_1\zeta_3\zeta_4)(1 - \zeta_1\zeta_3\zeta_5)(1 - \zeta_1\zeta_4\zeta_5)(1 - \zeta_2\zeta_3\zeta_5)(1 - \zeta_2\zeta_4\zeta_5)$$

che conduce al risultato ottenuto nell'Esempio 21, infatti si ha::

$$\begin{aligned} R_S(t) &= R_1(t)R_3(t)R_4(t) + R_1(t)R_3(t)R_5(t) + R_1(t)R_4(t)R_5(t) + R_2(t)R_3(t)R_5(t) + R_2(t)R_4(t)R_5(t) \\ &\quad - 2R_1(t)R_3(t)R_4(t)R_5(t) - R_1(t)R_2(t)R_3(t)R_5(t) - R_1(t)R_2(t)R_4(t)R_5(t) \\ &\quad - R_2(t)R_3(t)R_4(t)R_5(t) + R_1(t)R_2(t)R_3(t)R_4(t)R_5(t) \end{aligned}$$

Anche il metodo degli insiemi di cammino minimo può essere applicato al diagramma di Figura 36. In generale, sistemi con molte componenti in serie possono essere trattati facilmente con gli insiemi di cammino minimo, sistemi con molte componenti collegate in parallelo possono essere studiati più agevolmente con gli insiemi di minimo taglio.

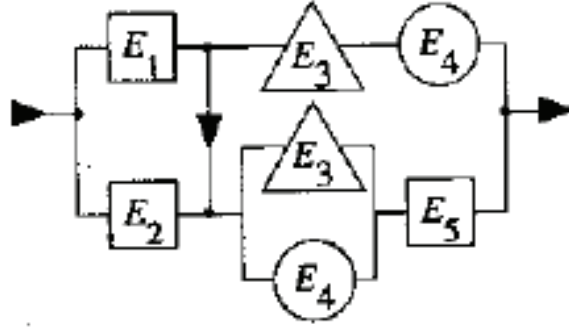


Figure 36: Con riferimento all'Esempio 23.

**Esempio 24** Calcoliamo l'affidabilità del sistema descritto dal diagramma di Figura 37 facendo uso del metodo degli insiemi di cammino minimo e del metodo degli insiemi di taglio minimo. Assumiamo che i singoli elementi del sistema siano indipendenti. Osserviamo che esistono due

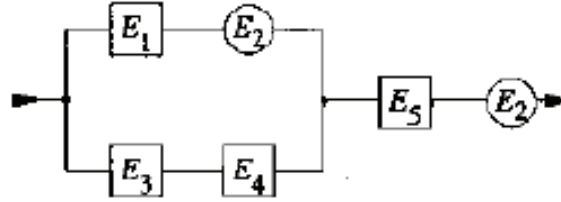


Figure 37: Ad illustrazione dell'Esempio 24.

insiemi di cammino minimo  $\Pi_1$  e  $\Pi_2$  e quattro insiemi di minimo taglio  $C_1$ ,  $C_2$ ,  $C_3$  e  $C_4$ , come mostrato in Figura 38. Con riferimento agli insiemi di cammino minimo, la funzione di sistema è

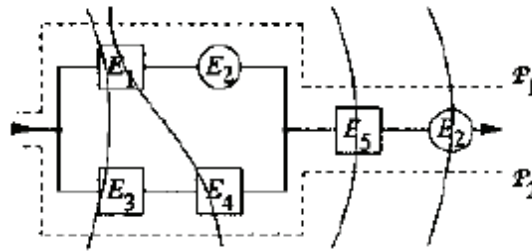


Figure 38: Insiemi di cammino minimo  $\Pi_i$  e insiemi di minimo taglio  $C_i$  per il diagramma di Figura 36.

$$\Phi(\zeta_1, \dots, \zeta_5) = 1 - (1 - \zeta_1 \zeta_2 \zeta_5)(1 - \zeta_2 \zeta_3 \zeta_4 \zeta_5) = \zeta_1 \zeta_2 \zeta_5 + \zeta_2 \zeta_3 \zeta_4 \zeta_5 - \zeta_1 \zeta_2 \zeta_3 \zeta_4 \zeta_5.$$

Invece, considerando gli insiemi di minimo taglio si ha:

$$\begin{aligned} \Phi(\zeta_1, \dots, \zeta_5) &= [1 - (1 - \zeta_1)(1 - \zeta_3)][1 - (1 - \zeta_1)(1 - \zeta_4)][1 - (1 - \zeta_5)][1 - (1 - \zeta_2)], \\ &(\zeta_1 + \zeta_3 - \zeta_1 \zeta_3)(\zeta_1 + \zeta_4 - \zeta_1 \zeta_4) \zeta_2 \zeta_5 = \zeta_1 \zeta_2 \zeta_3 + \zeta_2 \zeta_3 \zeta_4 \zeta_5 - \zeta_1 \zeta_2 \zeta_3 \zeta_4 \zeta_5. \end{aligned}$$

Pertanto, assumendo che elementi diversi lavorino indipendentemente l'uno dall'altro, segue che l'affidabilità del sistema nell'intervallo  $(0, t)$  è:

$$R_S(t) = R_1(t)R_2(t)R_5(t) + R_2(t)R_3(t)R_4(t)R_5(t) - R_1(t)R_2(t)R_3(t)R_4(t)R_5(t).$$

Osserviamo che lo stesso risultato può essere ottenuto col metodo dell'elemento chiave scegliendo come chiave l'elemento  $E_2$ ; così facendo si ottiene:

$$\begin{aligned} R_S(t) &= R_2(t)[R_1(t) + R_3(t)R_4(t) - R_1(t)R_3(t)R_4(t)]R_5(t) + [1 - R_2(t)] \cdot 0 \\ &= R_2(t)[R_1(t) + R_3(t)R_4(t) - R_1(t)R_3(t)R_4(t)]R_5(t). \end{aligned}$$

Riassumendo per sistemi con elementi indipendenti non riparabili la funzione affidabilità  $R_S(t) = \mathbb{E}\{\Phi[\zeta_1(t), \zeta_2(t), \dots, \zeta_n(t)]\}$  si può ottenere direttamente dalla funzione di sistema individuata tramite una delle due espressioni:

$$\begin{aligned} \Phi &= \Phi(\zeta_1, \zeta_2, \dots, \zeta_n) = 1 - \prod_{i=1}^r (1 - \Phi_{\Pi_i}) = 1 - \prod_{i=1}^r \left( 1 - \prod_{j: E_j \in \Pi_i} \zeta_j \right) \\ \Phi &= \Phi(\zeta_1, \zeta_2, \dots, \zeta_n) = \prod_{i=1}^m \Phi_{C_i} = \prod_{i=1}^m \left( 1 - \prod_{E_j \in C_i} (1 - \zeta_j) \right) \end{aligned}$$

## 5 Teorema di Bayes

Introduciamo ora un teorema di particolare rilievo che riguarda le probabilità condizionate; questo riveste grande importanza sia concettuale che applicativa, ma la sua utilizzazione, se non correttamente effettuata può dar luogo ad equivoci e risultati paradossali come spesso è avvenuto. Si tratta del teorema di Bayes che trovò la sua prima e chiara formulazione ad opera di Thomas Bayes nel 1763. Questo teorema consente di interpretare gli eventi in un legame logico come cause ed effetti la qual cosa dà luogo ai concetti di probabilità a priori e a posteriori connesse dalle probabilità probative o verosimiglianze.

**Teorema di Bayes** Sia  $\{B_n; n = 1, 2, \dots, k\}$  un insieme di eventi incompatibile di una sigma-algebra  $\mathcal{A}$  tali che  $\mathbb{P}(B_n) > 0$  per  $n = 1, 2, \dots, k$  e sia  $A \in \mathcal{A}$  un evento con  $\mathbb{P}(A) > 0$ . Se  $A \subset \cup_{n=1}^k B_n$ , allora per  $n = 1, 2, \dots, k$  si ha:

$$\mathbb{P}(B_n|A) = \frac{\mathbb{P}(B_n)\mathbb{P}(A|B_n)}{\sum_{i=1}^k \mathbb{P}(B_i)\mathbb{P}(A|B_i)}.$$

**Dimostrazione** Poiché  $\mathbb{P}(A) > 0$  e  $\mathbb{P}(B_n) > 0$ , dalla definizione di probabilità condizionata segue che

$$\mathbb{P}(B_n|A) = \frac{\mathbb{P}(A \cap B_n)}{\mathbb{P}(A)} = \frac{\mathbb{P}(B_n)\mathbb{P}(A|B_n)}{\mathbb{P}(A)}.$$

Facendo uso del teorema delle alternative segue la tesi.

**Esempio 25** Supponiamo che la probabilità di contaminazione con un particolare agente nocivo sia 0.01. Esiste un test di laboratorio per identificare l'agente che non è perfettamente affidabile. In particolare, è noto che il 90% dei campioni contaminati risulterà positivo al test e il 10% dei campioni non contaminati risulterà positivo al test. Vogliamo conoscere con che probabilità un campione che risulta positivo al test è realmente contaminato.

Denotiamo con  $A = \{\text{il campione è positivo al test}\}$  e con  $B = \{\text{il campione è contaminato}\}$ . Risulta:

$$\mathbb{P}(B|A) = \frac{\mathbb{P}(A|B)\mathbb{P}(B)}{\mathbb{P}(A|B)\mathbb{P}(B) + \mathbb{P}(A|\bar{B})\mathbb{P}(\bar{B})} = \frac{0.90 \times 0.01}{0.90 \times 0.01 + 0.01 \times 0.99} = 0.083.$$

Notiamo che solo l'8% dei campioni che risultano positivi al test sono realmente contaminati!

**Esempio 26** Il fornitore A produce componenti ad alta resistenza mentre il fornitore B produce componenti a bassa resistenza. Una componente del fornitore A supera un test meccanico con probabilità 0.9, la componente proveniente dal fornitore B supera il test con probabilità 0.6. Supponiamo che i fornitori abbiano uguale divisione di mercato, vogliamo calcolare la probabilità con cui una componente che ha superato il test provenga dal fornitore A.

Visto che la divisione di mercato è uguale per i due fornitori, la probabilità che la componente provenga da A o da B è  $\mathbb{P}(A) = \mathbb{P}(B) = 0.5$ . Sia  $E = \{\text{la componente supera il test}\}$ , risulta:

$$\mathbb{P}(E) = \mathbb{P}(E|A)\mathbb{P}(A) + \mathbb{P}(E|B)\mathbb{P}(B) = 0.9 \times 0.5 + 0.6 \times 0.5 = 0.75$$

da cui, facendo uso della formula di Bayes, segue

$$\mathbb{P}(A|E) = \frac{\mathbb{P}(E|A)\mathbb{P}(A)}{\mathbb{P}(E)} = \frac{0.9 \times 0.5}{0.75} \simeq 0.6.$$

## 6 Organizzazione fisica e logica di componenti

È necessario notare che esiste differenza tra l'organizzazione fisica e logica delle componenti. Ricordiamo che l'organizzazione fisica rappresenta un'organizzazione funzionale. In Figura 39 è mostrato un diagramma funzionale di un sistema che effettua degli impacchettamenti attraverso due sistemi di chiusura che inseriscono dei sigilli. Il sistema è costituito da due dispositivi che fisicamente sono collegati in serie anche se logicamente i due dispositivi sono collegati in parallelo. Infatti visto che la finalità del sistema è quella di sigillare delle confezioni si può dedurre che la sua funzione, che consiste nel non disperdere materiale nell'ambiente, è espletata se almeno uno dei due dispositivi di chiusura svolge la sua funzione correttamente ma questo significa che i due dispositivi sono collegati logicamente in parallelo. Viceversa, componenti che sono fisicamente organizzate in parallelo possono avere un'organizzazione logica in serie come illustrato in Figura 40. In questo caso, sebbene l'organizzazione fisica dei sigillatori sia in parallelo, la loro organizzazione rispetto al guasto "perdita nell'ambiente" è di tipo logico in quanto la perdita nell'ambiente si verifica se almeno uno dei dispositivi presenta una perdita.

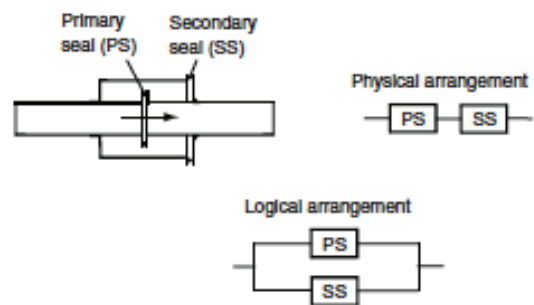


Figure 39: Elementi collegati fisicamente in serie ma logicamente in parallelo.

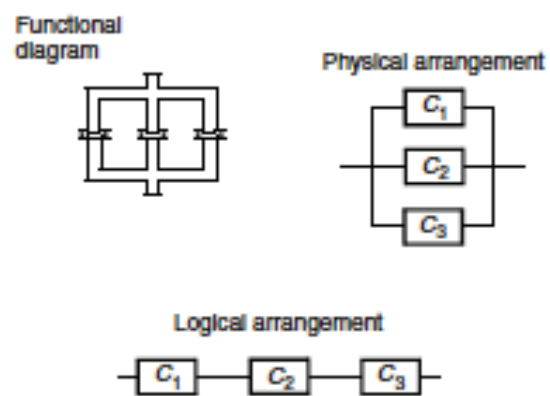


Figure 40: Elementi collegati fisicamente in parallelo ma logicamente in serie.