

# CAPITOLO 3

## Alberi di guasto

### 1 Introduzione

L'analisi degli alberi di guasto, o FTA (Fault Tree Analysis) come spesso si usa abbreviare, fu introdotta per la prima volta nel 1962 nei Bell Telephone Laboratories in relazione allo studio della sicurezza del sistema di controllo del Missile Minuteman. Negli anni successivi questo metodo fu sviluppato dalla Boeing Company e utilizzato sempre più diffusamente nell'industria aerospaziale e nucleare e in generale per lo studio di sistemi complessi di grosse dimensioni.

Esistono vari metodi per valutare i rischi di un sistema, essi sono classificabili in due categorie: forward e backward, a seconda della metodologia utilizzata. In particolare,

- nelle metodologie forward si parte da un insieme di eventi e si procede in avanti per analizzare quale tipo di malfunzionamento possono generare nel sistema,
- nelle metodologie backward si parte dal malfunzionamento del sistema e si procede a ritroso per individuare i possibili eventi che hanno provocato il malfunzionamento.

Sul primo approccio sono basate metodologie come la FMEA (Failure Mode and Effect Analysis) e la FMECA (Failure Modes Effects and Criticality Analysis), la FTA è invece basata sull'approccio backward.

La FMEA è una tecnica induttiva, per analizzare i malfunzionamenti di un sistema. Il principio basilare su cui si fonda la tecnica è il seguente:

*Per ogni componente si deve effettuare un'identificazione sistematica di tutti i possibili modi di malfunzionamento del sistema ed i loro effetti.*

Ovviamente il termine componente acquisisce vari significati in accordo al significato di sistema. Per effettuare un'analisi di questo tipo FMEA vanno eseguiti i seguenti passi:

1. identificare tutti i possibili malfunzionamenti del sistema,
2. individuare gli effetti e le possibili cause di ogni malfunzionamento,
3. cercare le possibili azioni atte a ridurre gli effetti di ogni malfunzionamento.

La FMEA è uno strumento prettamente qualitativo. Per rendere quantitativa la FMEA si effettua un'analisi di criticità; in questo modo si ottiene la FMECA. La criticità viene introdotta per ogni tipo di malfunzionamento attraverso un "indice di priorità di rischio", denotato con  $IPR$ , determinato come

$$IPR = P_0SD$$

dove  $P_0$  rappresenta la probabilità che si verifichi la causa che provocherà il malfunzionamento,  $S$  e  $D$  sono invece connessi al malfunzionamento,  $S$  quantifica la “severità” degli effetti del malfunzionamento e  $D$  ne misura la rilevanza. In particolare,  $P_0$  va da improbabile a molto probabile,  $S$  da irrilevante a gravissima e  $D$  da certa a improbabile. Per effettuare un’analisi FMECA è necessario aggiungere tre passi all’analisi FMEA:

1. definire le scale di punteggio dei tre parametri che caratterizzano l’ $IPR$ ,
2. calcolare l’ $IPR$  per ogni malfunzionamento;
3. sulla base degli indici  $IPR$  calcolati, definire gli interventi da intraprendere per portare l’ $IPR$  sotto un valore di soglia prefissato.

La FTA è particolarmente adeguata per l’analisi di sistemi altamente ridondanti, mentre per sistemi particolarmente vulnerabili che possono provocare incidenti è preferibile utilizzare tecniche di tipo diverso come la FMEA. La metodologia FTA può essere applicata sia durante la fase di progettazione di un nuovo sistema (impianto) che in fase di verifica del sistema stesso allo scopo di migliorarne la sicurezza. Infatti, la FTA permette di individuare importanti caratteristiche come i punti deboli del sistema, le false ridondanze o gli effetti di un dato componente sull’affidabilità complessiva. Permette inoltre di effettuare predizioni studiando gli stati dei componenti del sistema nonché di effettuare un’analisi diagnostica.

L’uso degli alberi di guasto richiede una conoscenza dettagliata del funzionamento del sistema, dei modi di guasto dei suoi componenti e dei relativi effetti. Dopo che l’analista ha sviluppato l’albero di guasto è necessario che il modello venga esaminato dal personale che ha esperienza operativa con il sistema ed i componenti che lo costituiscono.

Il tempo ed il costo di una FTA dipendono, ovviamente, dalla complessità del prodotto in esame e dal livello di risoluzione dell’analisi.

Per avere un’idea, è sufficiente pensare che un sistema relativo ad un processo semplice può essere risolto in un giorno da un analista, mentre un sistema complesso, che magari richiede lo sviluppo di più alberi di guasto, può impegnare più persone anche per mesi.

Negli ultimi anni la FTA è stata utilizzata anche nel contesto di “Risk Management”. Con questo termine si intende la funzione aziendale che ha il compito di identificare, valutare, gestire e sottoporre a controllo economico i rischi puri dell’impresa che sono collegati ad eventi capaci di ridurre il valore aziendale dando luogo a perdite. L’analisi dei rischi aziendali consiste nel raccogliere ed elaborare informazioni allo scopo di migliorare la conoscenza dei rischi ed aumentare la prevenzione degli interventi.

## 2 Alberi di guasto

La tecnica degli alberi di guasto richiede la decomposizione del sistema in un diagramma logico, detto appunto albero di guasto, in cui certi eventi primari conducono ad uno specifico evento che rappresenta l’avaria totale del sistema, detto Top Event visto che si trova alla radice dell’albero.

In altri termini, un albero di guasto illustra lo stato del sistema (dato dal Top event) in base agli stati (funzionamento o guasto) delle componenti del sistema (basic event). Un esempio di albero di guasto è illustrato in Figura 1. Iniziando dal top event, si costruisce l'albero ramificandolo verso livelli più bassi costituiti da eventi intermedi che potrebbero determinare il top event. Ciò permette di ricostruire la sequenza degli eventi fino ad arrivare agli eventi di base dei quali si conoscono le probabilità di occorrenza. Una volta che l'albero di guasto è stato costruito, si può calcolare la probabilità del top event seguendo un approccio top-down. Le connessioni con gli eventi intermedi sono interpretate come gates, l'output di un gate è ovviamente individuato dai suoi input.

La FTA si articola nei seguenti passi fondamentali:

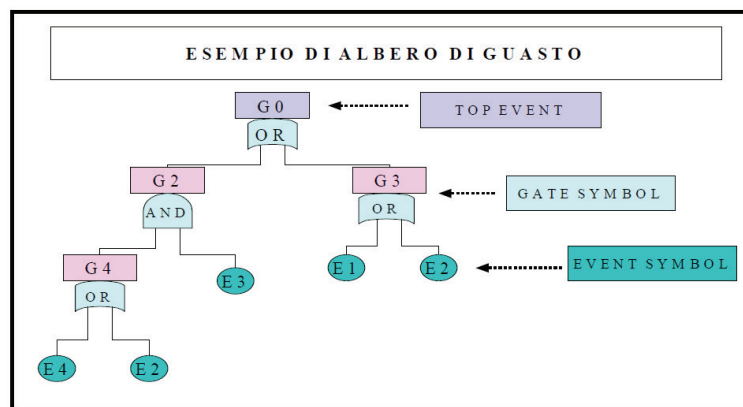


Figure 1: Esempio di albero di guasto.

1. *definizione del top event*, ciò equivale a selezionare il malfunzionamento del sistema che si vuole analizzare;
2. *costruzione dell'albero di guasto*, questo significa identificare gli eventi che contribuiscono direttamente al malfunzionamento del sistema;
3. *analisi qualitativa*, durante questa fase si correlano gli eventi che contribuiscono al malfunzionamento del sistema mediante porte logiche;
4. *eventuali analisi quantitative dell'albero di guasto*, in particolare, per ogni evento individuato al passo 3., che si ritiene non sia stato dettagliato in modo sufficiente, si effettua un'analisi più approfondita individuando le cause che lo scatenano e correlandole all'evento stesso attraverso porte logiche.
5. Il passo 4. può essere iterato fino al livello di dettaglio desiderato.

## 2.1 Definizione del top event

L'albero di guasto è un modello grafico che visualizza combinazioni di eventi che possono provocare un evento finale, il top event, coincidente generalmente con la rottura o il malfunzionamento del

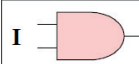
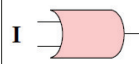
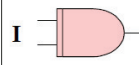
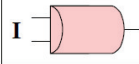
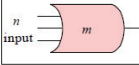
sistema visto nel suo complesso. Per descrivere il top event è necessario descrivere l'evento critico su cui è focalizzata l'analisi (what), dove si verifica (where) e quando (when).

La definizione dell'evento critico è sicuramente una delle fasi più delicate, infatti se si dà una definizione molto precisa si rischia di avere un albero di guasto eccessivamente grande e complesso, non ben focalizzato sul problema da analizzare.

## 2.2 Costruzione dell'albero di guasto

La radice di un albero di guasto è costituita dal top event da qui, scendendo di livello in livello, si giunge alle foglie dell'albero che sono costituite dagli eventi di base (cut set). Su ogni livello dell'albero sono presenti dei gates che rappresentano i nodi dell'albero e descrivono graficamente le relazioni che intercorrono tra i rami che giungono nel nodo. I gates maggiormente utilizzati sono rappresentati in Figura 2.

In questa analisi ogni componente può trovarsi solo in due stati: funzionante e non funzionante.

<u>GATE SYMBOL</u>	<u>GATE NAME</u>	<u>CASUAL RELATION</u>
	<u>AND</u> gate	Il guasto si verifica se tutti gli elementi in input si guastano
	<u>OR</u> gate	Il guasto si verifica se almeno un elemento di input si guasta
	<u>PRIORITY AND</u> gate	Il guasto si verifica se tutti gli eventi di input si guastano seguendo un preciso ordine
	<u>EXCLUSIVE OR</u> gate	Il guasto si verifica se uno, e solo uno, degli eventi di input si guastano
	<u>m-OUT OF-n</u> gate	Il guasto si verifica se m degli n eventi di input si guastano

I = INPUT \ O = OUTPUT

Figure 2: Gates più comuni.

Il fatto che lo stato di ogni elemento sia binario comporta che lo stato dell'intero sistema sarà binario. La simbologia utilizzata è mostrata in Figura 3. Per costruire l'albero di guasto si deve tener conto della struttura logica del sistema piuttosto che della sua organizzazione fisica. L'organizzazione logica segue lo schema di Figura 4 secondo cui una porta OR corrisponde ad una struttura seriale e un gate AND corrisponde ad una struttura parallela, esattamente il contrario di quanto accade negli schemi affidabilistici analizzati nel Capitolo 2 in quanto nella FTA siamo interessati al calcolo della probabilità di guasto piuttosto che a valutare l'affidabilità del sistema.

Durante la fase di definizione dell'albero è importante considerare la presenza di eventuali cause comuni di guasto. Infatti, se il malfunzionamento o la rottura di un componente del sistema comporta la perdita di più funzioni del sistema ne risulta che gli effetti provocati non possono essere considerati indipendenti fra loro la qual cosa può comportare una variazione significativa






EVENT SYMBOL	NOME	SIGNIFICATO
	Cerchio	Basic Event con sufficienti dati
	Diamante	Evento non sviluppato
	Rettangolo	Evento rappresentato da un gate
	Casa	Evento che può occorrere o non occorrere
	Triangolo	Simbolo di trasferimento

Figure 3: Simbologia usata.

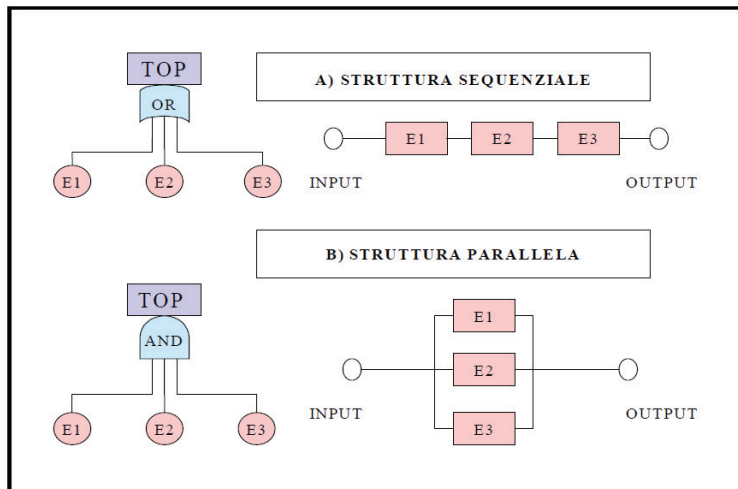


Figure 4: Organizzazione logica.

nella definizione della probabilità del top event rappresentante il guasto totale del sistema. Le regole standard per la costruzione dell'albero di guasto sono le seguenti:

- definire la complessità del sistema che si vuole analizzare;
- definire il top event nel modo più accurato possibile;
- identificare le cause che provocano il top event utilizzando i gates e i simboli di eventi più opportuni per identificare i nodi;
- identificare gli eventi di base, ossia le ultime ramificazioni dell'albero.

Gli errori che si commettono più frequentemente nella costruzione di un albero sono connessi

- ad identificazioni errate che possono condurre a soluzioni ambigue o prive di significato,

- a notazione inappropriata, ciò accade ad esempio quando si usa la stessa componente per la descrizione di componenti simili ma diverse,
- all'uso di sottosistemi significativi per analizzare il sistema nel suo complesso.

## 2.3 Analisi qualitativa

Come più volte sottolineato, l'occorrenza del top event corrisponde al fallimento del sistema ed è causata dal verificarsi, più o meno combinato, di eventi di base. L'albero di guasto fornisce le informazioni riguardanti le combinazioni degli eventi di base.

**Esempio 1** Consideriamo un modello di affidabilità di un routing alternato in una rete telefonica rappresentata dal grafo orientato di Figura 5 i cui nodi rappresentano le locazioni degli uffici e i rami rappresentano i link di comunicazione tra gli uffici.

La misura di interesse è l'affidabilità intesa come l'abilità della rete a mantenere un certo grado

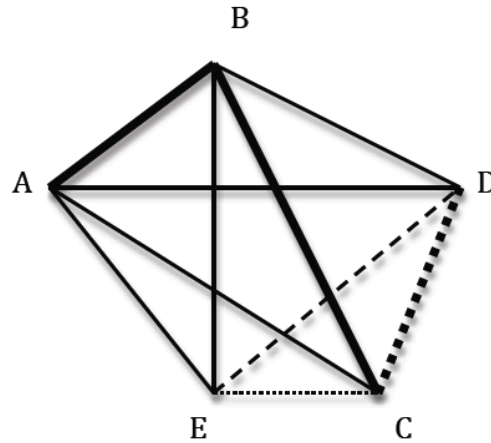


Figure 5: Con riferimento all'Esempio 1.

di connessione. Nello schema proposto la rete è up se le coppie di nodi  $A - B$  e  $C - D$  sono entrambe connesse o direttamente o attraverso una coppia di link. L'affidabilità della rete risulta

$$R_{network} = [1 - (1 - R_{ab})(1 - R_{ac}R_{cb})(1 - R_{ad}R_{bd})(1 - R_{ae}R_{eb})] \\ \times [1 - (1 - R_{cd})(1 - R_{ce}R_{ed})]$$

Dallo schema di Figura 5 è possibile costruire l'albero di guasto e calcolare la probabilità del top event che risulta  $P(T) = 1 - R_{network}$ .

**Esempio 2** Vogliamo studiare il sistema che gestisce la linea di produzione di schede elettroniche. In questo caso il malfunzionamento che si può rilevare corrisponde alla produzione di schede non funzionanti. Definiamo i seguenti eventi:

$$E_1 = \{\text{Prelievo non corretto dei componenti da magazzino}\},$$

$E_2 = \{\text{Errato caricamento delle macchine corrispondente ad un errore umano}\};$

$E_3 = \{\text{Mancata alimentazione dei componenti nella fase di pick and place (montaggio automatico elettronico)}\};$

$E_4 = \{\text{Funzionamento anomalo della saldatrice}\};$

$E_5 = \{\text{Errata predisposizione dei parametri di saldatura}\};$

$E_6 = \{\text{Malfunzionamento della saldatrice}\};$

$E_7 = \{\text{Errata programmazione umana}\};$

$E_8 = \{\text{Mancato funzionamento del sistema di autocontrollo della saldatrice}\}.$

In Figura 6 è mostrato l'albero di guasto relativo al sistema in analisi. Indicando con  $A$  il top event e con  $B$  l'evento "problemi di linea" si ha:

$$A = B \cup E_1 \quad E_4 = E_5 \cup E_6 \quad B = E_2 \cup E_3 \cup E_4 \quad E_5 = E_7 \cap E_8.$$

Quindi, il malfunzionamento del sistema in esame corrisponde al verificarsi dell'evento

$$A = E_1 \cup E_2 \cup E_3 \cup E_6 \cup E_7 \cap E_8$$

e si realizza se e solo se si verifica almeno uno degli eventi

$$E_1, \quad E_2, \quad E_3, \quad E_6, \quad E_7 \cap E_8.$$

Assumendo che le probabilità associate agli eventi sono  $\mathbb{P}(E_1) = \mathbb{P}(E_2) = \mathbb{P}(E_3) = \mathbb{P}(E_6) = 0.01, \mathbb{P}(E_7) = \mathbb{P}(E_8) = 0.1$ , sotto la ragionevole ipotesi di indipendenza di  $E_7$  e  $E_8$ , si ha che la probabilità del top event, ossia la probabilità di errato funzionamento del sistema è  $\mathbb{P}(A) = 0.05$ .

Lo studio dei cut sets permette di effettuare un'analisi più approfondita sugli eventi di base rispetto ad uno studio effettuato sui singoli componenti. Infatti con l'uso dei cut sets è possibile analizzare simultaneamente un certo numero di guasti (quando i cut sets contengono più eventi di base), consentendo un'analisi semplificata delle cause comuni di guasto che comportano il fallimento del sistema.

Ricordiamo la definizione di cut set:

**Definizione** Un cut set in un albero di guasto è un insieme di eventi di base necessari per il verificarsi del top event. Un cut set è detto minimale se non può essere ridotto senza perdere la sua caratteristica.

**Esempio 3** Consideriamo un'operazione di raccolta ordini effettuata ad uno sportello. La Figura 7 mostra l'albero di guasto e i relativi minimal cut sets connessi a questo sistema. In questo schema il top event corrisponde al fallimento dell'operazione "raccolta ed espletamento ordini", inoltre sono stati individuati i seguenti eventi:

1. Contrattazione

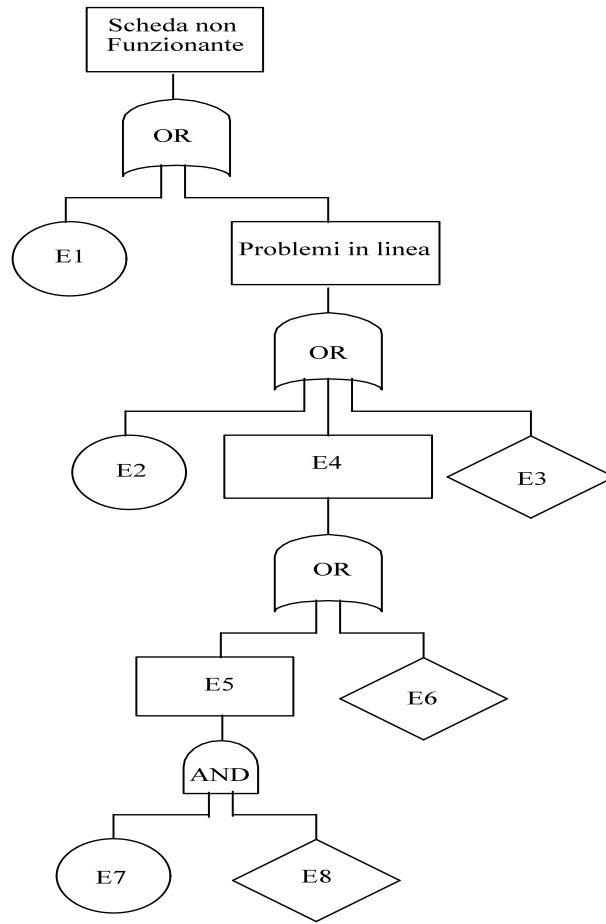


Figure 6: Albero di guasto relativo all'Esempio 2

2. Pricing (assegnazione di prezzi)
3. Data entry (immissione dei dati)
4. Validazione dei dati
5. Esecuzione dell'ordine (Eseguito).

Osserviamo che un guasto al nodo  $G1$  è causato sia da  $E3$ , cioè un errore nella fase di inserimento dei dati, sia da  $E4$ , ossia da un errore nella fase di validazione dei dati. Inoltre, il top event, cioè il fallimento del sistema, si verifica in presenza di un errore nel nodo 1, nel 3, in quello denotato con  $G1$  oppure nel nodo 5. Pertanto, considerando che  $G1$  si verifica in corrispondenza del verificarsi simultaneo di  $E3$  e  $E4$ , si ha che gli insiemi candidati a cut sets sono:  $\{1\}$ ,  $\{2\}$ ,  $\{3, 4\}$ ,  $\{5\}$ . Visto che nessuno di questi insiemi è contenuto in altri si ha che questi sono cut sets minimali.

Il metodo basato sui minimal cut sets può essere applicato sempre che

- tutti i guasti sono di natura binaria,
- la transizione dallo stato di funzionamento allo stato di guasto è istantanea,



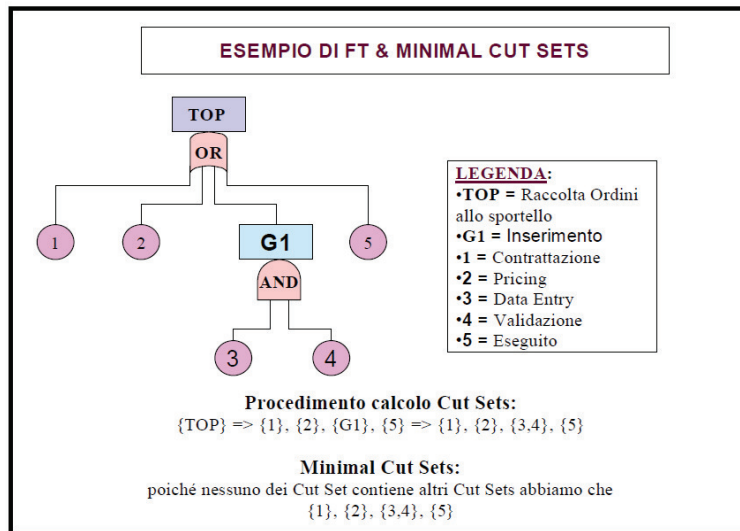


Figure 7: Ad illustrazione dell'Esempio 3.

- i guasti dei vari componenti sono eventi indipendenti,
- il tasso di guasto di ogni componente è costante,
- il tasso di guasto di ogni componente rimane invariato dopo la riparazione.

**Esempio 4** Vogliamo costruire ed analizzare col metodo dei minimal cut sets l'albero di guasto relativo ad un impianto di alimentazione idrica di un'utenza civile il cui schema è dato in Figura 8. Dalla Figura 4, ricordando che per gli schemi logici i gates AND corrispondono a collegamenti in

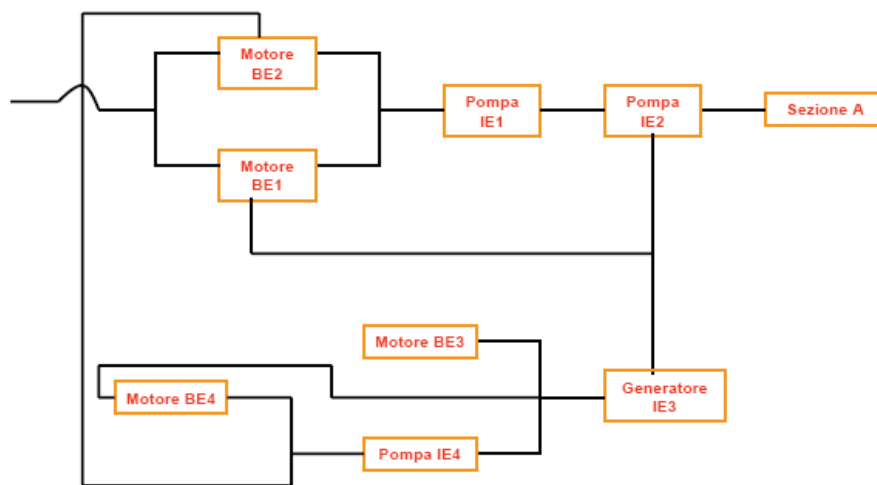


Figure 8: Ad illustrazione dell'Esempio 4.

parallelo mentre le porte di tipo OR corrispondono a collegamenti in serie, si può ricavare l'albero di guasto mostrato in Figura 9. La struttura logica dell'albero di guasto è espressa da relazioni

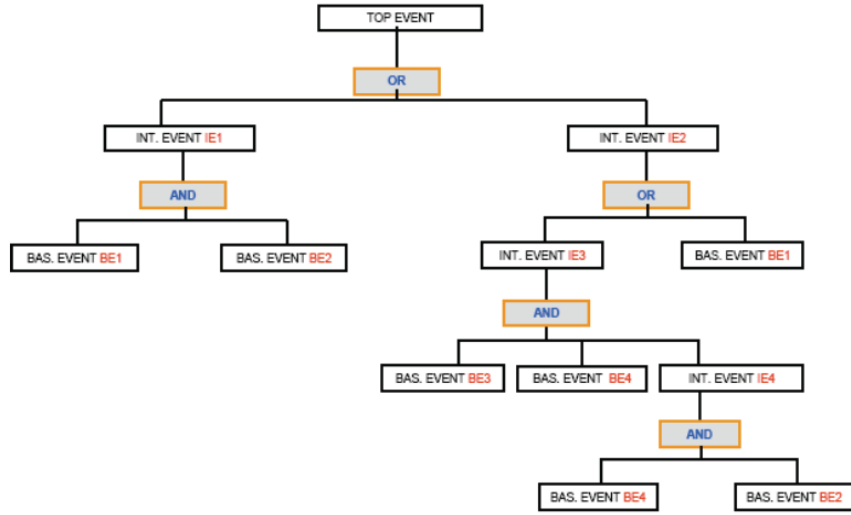


Figure 9: L'albero di guasto relativo all'Esempio 4.

booleane. Inoltre, l'albero deve essere analizzato livello per livello secondo l'approccio top-down. Ricordiamo che condizione necessaria e sufficiente affinché si verifichi il top event è che si verifichi almeno uno dei minimal cut sets che possono essere individuati procedendo come qui di seguito illustrato.

Affinché si verifichi il top event  $T$  deve verificarsi  $E1$  o  $E2$ . L'evento  $E1$  si verifica a patto che simultaneamente si verifichino gli eventi  $BE1$  e  $BE2$ , mentre  $E2$  si verifica in corrispondenza del verificarsi di  $BE1$  o di  $IE3$ . Procedendo in questo modo si ha che  $T = IE1 \cup IE2$  da cui segue:

$$\begin{aligned}
 T &= IE1 \cup IE2 = (BE1 \cap BE2) \cup (BE1 \cup IE3) = (BE1 \cap BE2) \cup (BE1 \cup (BE3 \cap BE4 \cap IE4)) \\
 &= (BE1 \cap BE2) \cup (BE1 \cup (BE3 \cap BE4 \cap (BE4 \cap BE2))) \\
 &= (BE1 \cap BE2) \cup (BE1 \cup (BE3 \cap BE4 \cap BE2)) = BE1 \cup (BE3 \cap BE4 \cap BE2).
 \end{aligned}$$

In questo caso i minimal cut sets sono  $\{BE1\}$  e  $\{BE2, BE3, BE4\}$ , così che la FTA dello schema di Figura 9 può essere effettuata sulla base dell'analisi dello schema di Figura 10.

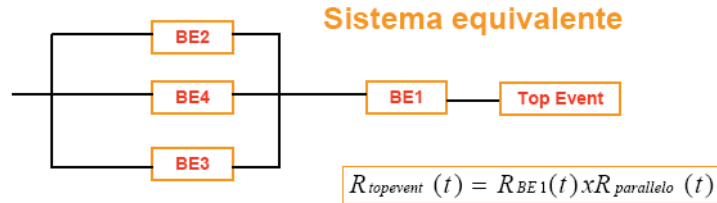


Figure 10: Riduzione dello schema di Figura 9 in termini di insiemi di minimo taglio.

Gli alberi di guasto possono essere analizzati anche utilizzando gli insiemi di cammino minimo.

## 2.4 Analisi quantitativa

Una volta individuati gli insiemi di minimo taglio è possibile calcolare la probabilità che si presentino diversi stati del sistema ottenendo così dei risultati di tipo quantitativo. Per calcolare questi valori si parte dalla probabilità che si presenti un guasto negli eventi di base, poi si individuano le probabilità di guasto negli insiemi di taglio minimo e infine si calcola la probabilità del verificarsi di un guasto nel nodo top event che corrisponde ad un guasto dell'intero sistema. Con la stessa procedura si possono ottenere altre informazioni come l'affidabilità e la disponibilità. Per fare questo si utilizza la funzione di struttura del sistema.

## 3 Funzione di struttura

L'algebra booleana è lo strumento di base per l'analisi di un albero di guasto. Sia  $H = \{0, 1\}$  l'insieme di definizione di una variabile booleana, una funzione booleana è tale che  $\Phi : H^n \rightarrow H$ . La funzione di struttura è una funzione booleana che permette la formalizzazione in termini matematici delle relazioni esistenti tra top event e eventi di base. Il suo scopo essenziale è di descrivere in maniera sintetica il guasto/fallimento del sistema ( $\Phi = 0$ ) o il funzionamento corretto ( $\Phi = 1$ ) per tutti i possibili stati dei suoi componenti.

Generalmente, con il termine fault tree di un sistema si intende sia la funzione  $\Phi$  che la sua rappresentazione grafica. L'albero di guasto mostra, quindi, la struttura logica di come i guasti si ripercuotono sul guasto dell'intero sistema.

L'analisi degli alberi di guasto è di grande interesse nello studio dei rischi operativi; si effettua per scoprire tutte le cause che conducono ad un particolare fallimento/guasto, in modo da poterle identificare e, se possibile, eliminare. Gli insiemi di taglio minimo e l'algoritmo di Enzeman sono modelli utilizzati per analizzare gli eventi di base e determinare la funzione di struttura.

Lo studio di modelli particolarmente complessi avviene, invece, attraverso la modularizzazione. Si tratta di una tecnica che consente una semplificazione dell'albero di guasto ottenuta isolando dei sottoalberi del fault tree, detti moduli del fault tree, che risultano indipendenti l'uno dall'altro.

La modularizzazione parte da un'analisi dei singoli moduli che vengono sostituiti nell'albero di guasto principale con le rispettive variabili di uscita, consentendo, così, una semplificazione della struttura dell'albero principale.

Il Teorema di decomposizione di Shannon e l'algoritmo di Enzeman sono utilizzati per ottenere la funzione di struttura del sistema. In particolare, il teorema di Shannon fornisce la funzione booleana in forma normale disgiuntiva (DNF) perché formata da disgiunzioni di termini composti da congiunzioni di variabili semplici o negate; l'algoritmo di Enzeman fornisce la forma "aritmetica" della funzione di struttura. La funzione di struttura può essere realizzata anche a partire dagli insiemi di taglio.

### 3.1 Teorema di decomposizione di Shannon

Il teorema di decomposizione di Shannon permette di definire in modo appropriato la funzione di struttura di un albero di guasto. Una funzione booleana si dice ridotta in forma normale disgiuntiva (DNF) se è formata da disgiunzioni di termini composti da congiunzioni di variabili semplici o negate.

Il seguente teorema consente di trasformare una qualsiasi funzione booleana in forma semi-polinomiale, ossia in termini di disgiunzione di termini composti da congiunzioni di variabili semplici o negate; una forma di questo tipo si dice polinomiale. In accordo al metodo di Shannon, una funzione Booleana di  $n$  variabili può essere espressa rispetto ad una, due, ...,  $n$  variabili. Quando l'espansione è completa si parla di espansione minterms.

**Teorema di decomposizione di Shannon** Sia  $\Phi : H^n \rightarrow H$  una funzione booleana e sia  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  un vettore di  $H^n$ . Fissato un intero  $i$  minore o uguale di  $n$  si ha che

$$\Phi(x_1, x_2, \dots, x_n) = x_i \wedge \Phi(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \vee (1 - x_i) \wedge \Phi(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$$

La dimostrazione segue banalmente in quanto  $x_i$  è una variabile binaria.

Il procedimento di decomposizione può essere iterato più volte. I termini ottenuti nella decomposizione sono a due a due ortogonali, ossia disgiunti. Notiamo, inoltre, che la negazione e la disgiunzione formano un insieme completo di operazioni nel senso che generano tutte le funzioni  $f : H^n \rightarrow H$ .

### 3.2 Algoritmo di Enzeman

Un metodo alternativo per calcolare la funzione di struttura di un albero di guasto è basato essenzialmente sulla natura booleana della funzione di struttura e utilizza il teorema di unicità della funzione polinomiale che permette di individuare la forma aritmetica di una funzione di struttura. In particolare risulta

**Teorema** Ogni funzione booleana ammette un'unica rappresentazione in forma polinomiale:

$$\Phi(x_1, x_2, \dots, x_n) = a_0 + a_1 x_1 + \dots + a_n x_n + a_{1,2} x_1 x_2 + \dots + a_{1,2,\dots,n} x_1 x_2 \dots x_n.$$

I coefficienti della forma polinomiale possono essere determinati con l'algoritmo di Enzeman qui di seguito brevemente riassunto:

$$\begin{aligned} \Phi(0, 0, \dots, 0) &= a_0, \quad \Phi(1, 0, \dots, 0) = a_0 + a_1, \quad \Phi(0, 1, \dots, 0) = a_0 + a_2, \quad \dots, \quad \Phi(0, 0, \dots, 1) = a_0 + a_n, \\ \Phi(1, 1, \dots, 0) &= a_0 + a_1 + a_2 + a_{1,2}, \quad \dots, \quad \Phi(0, 0, \dots, 1, 1) = a_0 + a_{n-1} + a_n + a_{n-1,n}, \quad \dots, \\ \Phi(1, 1, \dots, 1) &= a_0 + a_1 + \dots + a_n + a_{1,2} + \dots + a_{n-1,n} + \dots + a_{1,2,\dots,n}. \end{aligned}$$

**Esempio 5** Consideriamo un sistema composto da tre componenti e assumiamo che esso sia in funzione se almeno due dei suoi elementi funzionano, si tratta di un sistema 2-out-of-3. La funzione booleana del sistema è

$$\Phi_{2-out-of-3}(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$$

ossia, ricordando che  $(1 + x_3) = 1$ ,

$$\begin{aligned}\Phi_{2-out-of-3}(x_1, x_2, x_3) &= x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3 \\ &= x_1x_2(1 + x_3) + x_1x_3 + x_2x_3 \equiv x_1x_2 + x_1x_3 + x_2x_3.\end{aligned}$$

Facendo uso dell'algoritmo di Enzeman possiamo individuare i coefficienti dell'unica forma polinomiale di  $\Phi_{2-out-of-3}$ . In particolare, ricordando che  $1 \vee 1 \vee 1 = 1$ , risulta:

$$\begin{aligned}\Phi_{2-out-of-3}(0, 0, 0) &= a_0 = 0, \\ \Phi_{2-out-of-3}(1, 0, 0) &= \Phi_{2-out-of-3}(0, 1, 0) = \Phi_{2-out-of-3}(0, 0, 1) = 0 \implies a_1 = a_2 = a_3 = 0, \\ \Phi_{2-out-of-3}(1, 1, 0) &= \Phi_{2-out-of-3}(1, 0, 1) = \Phi_{2-out-of-3}(0, 1, 1) = \Phi_{2-out-of-3}(1, 1, 1) = 1 \\ \implies a_{1,2,3} + a_1 + a_2 + a_3 + a_{1,2} + a_{1,3} + a_{2,3} &= 1 \implies a_{1,2,3} + a_{1,2} + a_{1,3} + a_{2,3} = 1 \\ \implies a_{1,2,3} + 1 &= 1 \implies a_{1,2,3} = 0\end{aligned}$$

In conclusione, la forma aritmetica della funzione di struttura di un sistema 2-out-of-3 è:

$$\Phi_{2-out-of-3}(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3.$$

### 3.3 Insiemi di minimo taglio e cammini minimi

Il principio su cui si basa questo modello è lo stesso di quello presentato nel Capitolo 2. In particolare, denotando con  $\zeta_i(t)$  lo stato della componente  $i$ -esima all'istante  $t$ , si ha  $\zeta_i(t) = 0$  se la componente è down e  $\zeta_i(t) = 1$  se è up. Lo stato del sistema all'istante  $t$  è descritto dal vettore  $n$ -dimensionale  $\mathbf{X}(t) = (\zeta_1(t), \zeta_2(t), \dots, \zeta_n(t))$  ed è caratterizzato dalla funzione di struttura  $\Phi(X(t))$  che vale 1 se il sistema è up e 0 se il sistema è down. In presenza di  $m$  cut sets la funzione di struttura risulta data

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

dove  $C_i$  rappresenta lo  $i$ -esimo cut sets. Osserviamo che tale espressione è caratteristica di  $m$  componenti collegate in serie.

Analogamente, la funzione di struttura può essere ottenuta anche a partire dagli insiemi di cammino minimo. In questo caso, supponendo di avere  $r$  insiemi di cammino minimo si ha:

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

dove  $\Pi_i$  rappresenta un cammino minimo.

**Esempio 6** Con riferimento all'Esempio 3 (cf. anche Figura 11), ridefiniamo gli eventi:

1. Contrattazione
2. Pricing (assegnazione di prezzi)

3. Data entry (immissione dei dati)
4. Validazione dei dati
5. Esecuzione dell'ordine (Eseguito).

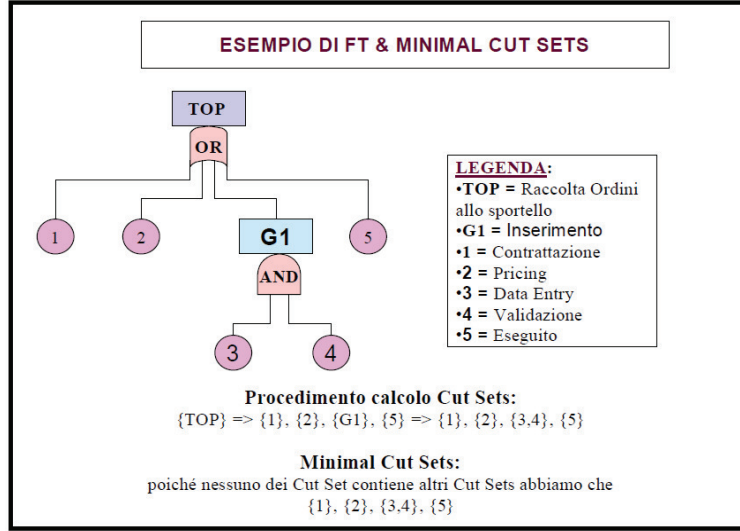


Figure 11: Con riferimento all'Esempio 6.

In questo caso i minimal cut set sono  $\{1\}, \{2\}, \{3, 4\}, \{5\}$ , pertanto la funzione di struttura del sistema è

$$\Phi(\mathbf{X}(t)) = [1 - (1 - x_1)] [1 - (1 - x_2)] [1 - (1 - x_5)] [1 - (1 - x_3)(1 - x_4)] = x_1 \wedge x_2 \wedge x_5 \wedge (x_3 \vee x_4).$$

Applicando l'algoritmo di Enzeman si ha che

$$\Phi(\mathbf{0}) = 0 \implies a_0 = 0$$

$$\Phi(1, 0, 0, 0, 0) = \dots = \Phi(0, 0, 0, 0, 1) = 0 \implies a_i = 0$$

$$\Phi(1, 1, 0, 0, 0) = \dots = \Phi(0, 0, 0, 1, 1) = 0 \implies a_{i,j} = 0$$

$$\Phi(1, 1, 1, 0, 0) = \dots = \Phi(0, 0, 1, 1, 1) = 0 \implies a_{i,j,k} = 0$$

$$\Phi(1, 1, 1, 0, 1) = \dots = \Phi(1, 1, 0, 1, 1) = 1 \implies a_{1,2,3,5} = a_{1,2,4,5} = 1, \quad a_{i,j,k,l} = 0 \text{ altrimenti}$$

$$\Phi(1, 1, 1, 1, 1) = 1 \implies a_{1,2,3,4,5} = 1 - (a_{1,2,3,5} + a_{1,2,4,5}) = 1 - 1 = 0.$$

Pertanto la forma polinomiale della funzione di struttura è

$$\Phi(\mathbf{X}(t)) = x_1 x_2 x_3 x_5 + x_1 x_2 x_4 x_5.$$

Notiamo che lo stesso risultato si ottiene facendo uso di semplici operazioni. Infatti, ricordando che gli insiemi di minimo taglio in questo caso sono  $\{1\}, \{2\}, \{3, 4\}, \{5\}$ , segue che

$$\begin{aligned} \Phi(\mathbf{X}(t)) &= [1 - (1 - x_1)][1 - (1 - x_2)][1 - (1 - x_5)][1 - (1 - x_3)(1 - x_4)] \\ &= x_1 x_2 x_5 (1 - \overline{x_3} \overline{x_4}) = x_1 x_2 x_5 \overline{\overline{x_3} \overline{x_4}} = x_1 x_2 x_5 (x_3 + x_4). \end{aligned}$$

Anche partendo dagli insiemi di cammino minimo che per questo esempio sono  $\{1, 2, 3, 5\}$  e  $\{1, 2, 4, 5\}$  si può costruire la funzione di struttura, infatti si ha:

$$\begin{aligned}
\Phi(\mathbf{X}(t)) &= 1 - (1 - x_1 x_2 x_3 x_5)(1 - x_1 x_2 x_4 x_5) = 1 - \overline{x_1 x_2 x_3 x_5 x_1 x_2 x_4 x_5} \\
&= \overline{x_1 x_2 x_3 x_5 x_1 x_2 x_4 x_5} = \overline{x_1} + \overline{x_2} + \overline{x_3} + \overline{x_5} + \overline{x_1} + \overline{x_2} + \overline{x_4} + \overline{x_5} \\
&= x_1 x_2 x_3 x_5 + x_1 x_2 x_4 x_5.
\end{aligned} \tag{1}$$

Ricordiamo che  $\mathbb{P}(\text{top event}) = \mathbb{P}[\Phi(t) = 0]$ ; pertanto, se supponiamo che ad ogni evento di base siano associate le seguenti probabilità di guasto annuali:

$$p_1 = 0.27, \quad p_2 = 0.13, \quad p_3 = 0.15, \quad p_4 = 0.07, \quad p_5 = 0.17,$$

dalla funzione di struttura ottenuta precedentemente si può ricavare la probabilità di errore nel top event, ossia la probabilità che il sistema fallisca:

$$\begin{aligned}
\mathbb{P}(\text{top event}) &= 1 - \mathbb{P}[\Phi(\mathbf{X}(t)) = 1] \\
&= 1 - (1 - p_1)(1 - p_2)(1 - p_3)(1 - p_5) - (1 - p_1)(1 - p_2)(1 - p_4)(1 - p_5) \\
&\equiv 1 - (1 - p_1)(1 - p_2)(1 - p_5)(2 - p_3 - p_4) = 0.0617033.
\end{aligned}$$