Fault Tree Analysis:

Concetti introduttivi:

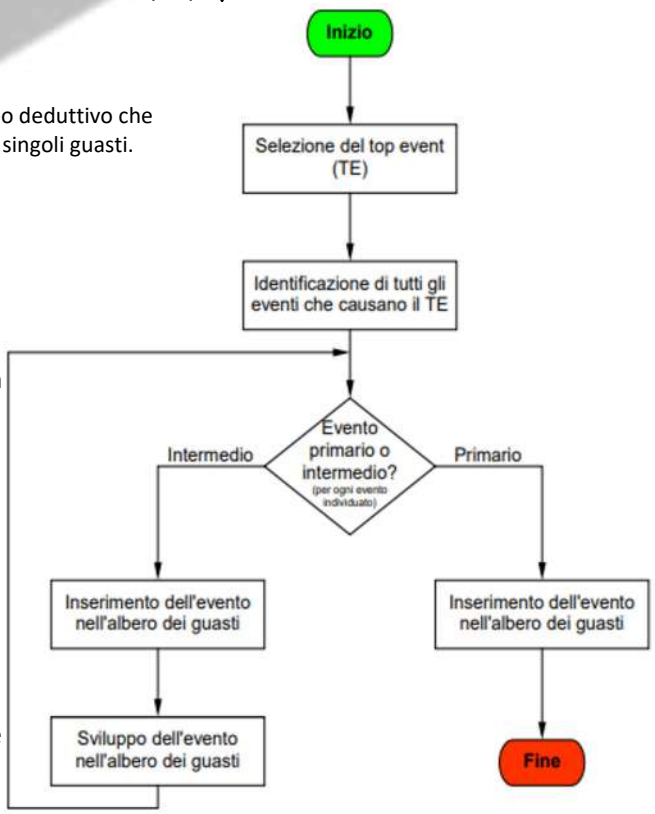
FAULT TREE ANALYSIS (FTA): procedimento di tipo deduttivo che permette da un analisi "generale" di individuare i singoli guasti.
-> Come?

Procedimento:

1. Individuazione Top event;
2. Indagare combinazione di cause.

-> Definizioni:

- **Evento indesiderato o "Top Event"**: È il guasto del sistema da esaminare: ha un numero n di eventi (nodi del sistema) che lo precedono e lo determinano ma nessun evento che lo segue;
- **Combinazione di cause**: Accadimento simultaneo di guasti degli elementi funzionali che portano all'evento indesiderato;
- **Unità esaminata:** È l'oggetto da esaminare, identificato dalle sue caratteristiche funzionali e costruttive (sistemi, componenti ed elementi funzionali);
- **Componente:** È l'unità esaminata di livello più basso alla quale possono essere assegnati uno o più elementi funzionali



Risultati conseguibili:

- È in grado di fornire **informazioni qualitative** e **quantitative** riguardanti l'analisi di affidabilità del sistema;
- Permette di **descrivere il sistema** e il suo comportamento di insuccesso funzionale come una catena causale di effetti
- Permette di **riconoscere** sistematicamente i **percorsi critici** di guasto (analisi causa/effetto)
- Permette di **identificare** tutte le **combinazioni** degli **eventi** che conducono al top event
- Permette di identificare le **combinazioni minime** di eventi di un sistema che conducono al top event (Minimal Cut Set – MCS)

Strumenti per l'applicazione della FTA:

Algebra booleana

"Sintassi" e porte logiche

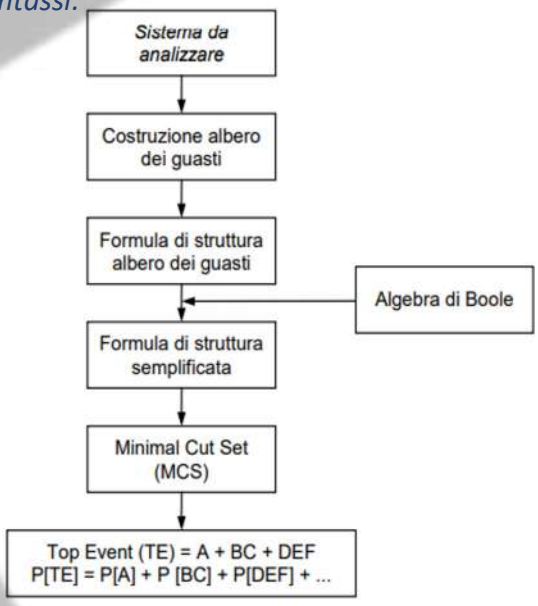
Minimal Cut Set (MCS)

1.Algebra booleana:

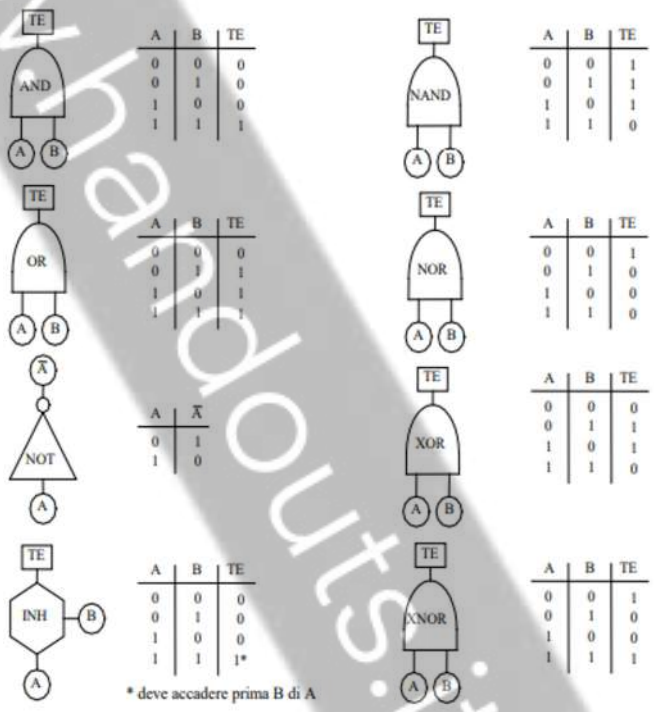
Proprietà	Espressione
commutativa	$AB = BA$ $A + B = B + A$
associativa	$A(BC) = (AB)C$ $A + (B + C) = (A + B) + C$
distributiva	$A(B + C) = AB + AC$
idempotenza	$AA = A$ $A + A = A$
assorbimento	$A + AB = A$

2.Sintassi & Porte logiche:

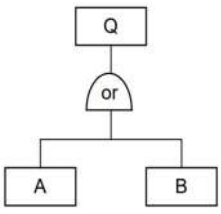
Regole di costruzione e sintassi:



Porte logiche:

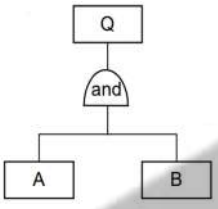


1. Porta OR:



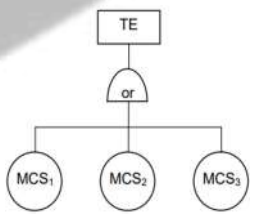
- **Rappresenta l'unione** degli eventi $P[Q] = P[A] + P[B] - P[B \cap A] = P[A] + P[B] - P[A] \cdot P[B|A]$;
- Tipologia di eventi:
  - Eventi mutuamente esclusivi $P[Q] = P[A] + P[B]$;
  - Eventi indipendenti $P[Q] = P[A] + P[B] - P[A] \cdot P[B]$

2. Porta AND:



- **Rappresenta l'intersezione** degli eventi $P[Q] = P[A] \cdot P[B|A] = P[B] \cdot P[A|B]$
  - Eventi indipendenti $P[Q] = P[A] \cdot P[B]$;

Minimal Cut Set (MCS):



TE = MCS1 + MCS2 + MCS3
MCS1 = E1
MCS2 = E2, E4, E5
MCS3 = E3, E4

-> **DEF**: rappresentano le strutture al di sotto dei quali non posso andare nell'albero, il numero minimo di eventi per definire un guasto;
-> **Procedimento**:

1. Dallo schema grafico di un albero dei guasti si ricava formula di struttura dell'albero;
2. Con le regole dell'algebra booleana si ricava la formula di struttura semplificata dell'albero;
3. Si identificano i MCS relativi all'albero dei guasti

Un MCS rappresenta la più piccola combinazione di eventi primari che, se avvengono, causano il Top Event (TE)

↓

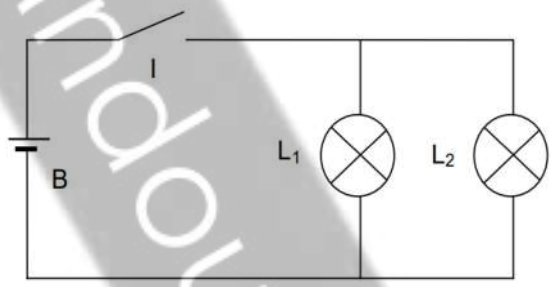
I MCS definiscono i failures modes del TE

↓

Il TE è dato dalla somma (unione) dei MCS

=> Dato un guasto, grazie ai MCS, posso definire, per ogni componente, la quota di partecipazione.

Esercizio 1:



Costruire l'albero dei guasti e **determinarne la formula** di struttura per il Top Event "mancanza di luce". Calcolare inoltre la probabilità che al tempo T = 10.000 ore il sistema sia guasto (ossia che si verifichi il Top Event).

1. Che cosa vuol dire che manca la luce? È data dalla contemporanea indisponibilità di entrambi i componenti o dalla mancanza di uno solo?

Componente	λ [ore^{-1}]	μ [ore^{-1}]	ϑ [ore]	Q
B	10^{-5}	0,1	-	10^{-4}
I	10^{-7}	0,1	-	10^{-6}
L_1	10^{-3}	0,5	-	$2{\cdot}10^{-3}$
L_2	10^{-3}	0,5	-	$2{\cdot}10^{-3}$

-> Nell'esercizio l'indisponibilità dei componenti a T = 10.000 ore è calcolata con la formula approssimata $Q(t) = \lambda/\mu$. Tuttavia, ove possibile, è in genere sempre meglio applicare la formula esatta o quanto meno calcolare il valore asintotico.
=> **Calcolare** infine il **numero atteso di guasti** W(TE) nel tempo T = 10.000 ore.

Soluzione:

1. Scelgo il Top Event:
   -> Sono io a scegliere il Top Event. Solitamente è qualcosa di abbastanza grave, sotto il quale non ha senso andare a vedere.
   => TOP EVENT: niente luce;
2. Indagare le cause:
   -> Le cause della mancanza di luce sono l'unione della luce guasta di entrambi le componenti.
   - Utilizzo un'and;

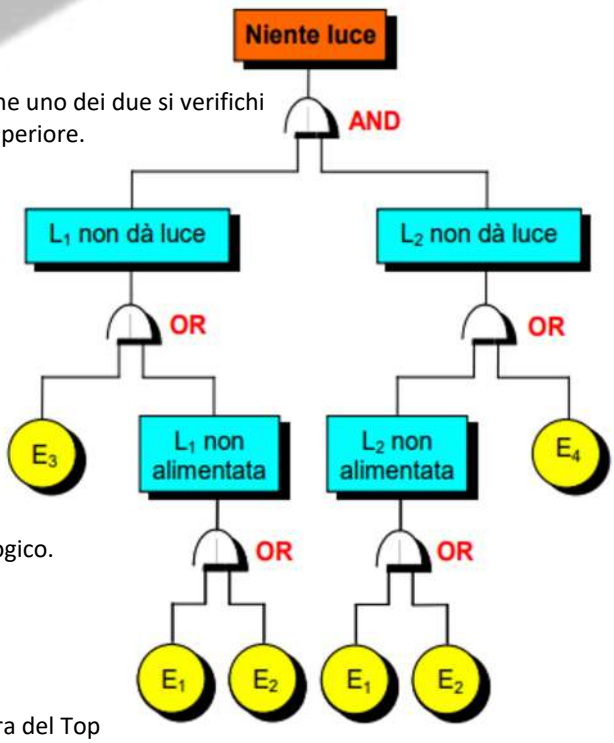
-> Continuo ad indagare:
-> Perché non c'è luce? Perché
- La luce è guasta;
- La luce non è alimentata.

-> Inseriamo un OR perché basta che uno dei due si verifichi per far si che si verifichi l'evento superiore.

-> Perché la luce non è alimentata?
- Perché l'interruttore I è guasto;
- Perché la pila B è scarica.

Eventi primari (*basic event*)

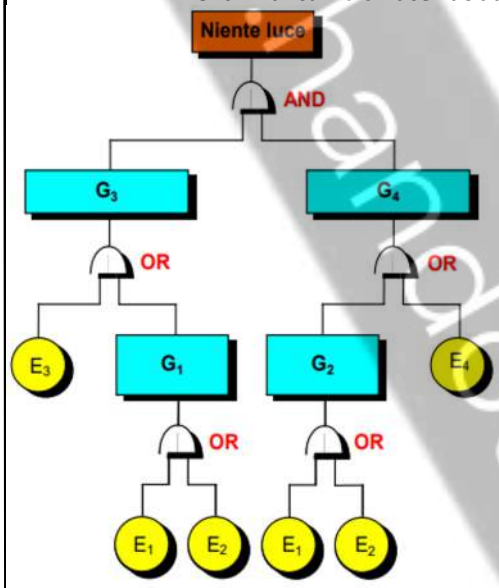
E_1 = B scarica
E_2 = I guasto
E_3 = L_1 guasta
E_4 = L_2 guasta



-> Traduciamo il problema in linguaggio logico.

3. **Semplificazione albero**:
-> Per ricavare la formula di struttura del Top Event "Mancanza di luce" dobbiamo semplificare l'albero:

Regole di logica booleana:
A+A = A;
A+AB = A



$G_1 = E_1 + E_2$
$G_2 = E_1 + E_2$
$G_3 = E_3 + G_1 = E_1 + E_2 + E_3$
$G_4 = E_4 + G_2 = E_1 + E_2 + E_4$

$TE = G_3 \cdot G_4 = (E_1 + E_2 + E_3)\cdot(E_1 + E_2 + E_4)$

=> Semplificando grazie alle regole dell'algebra booleana:

$TE = (E_1+E_2)\cdot(E_1+E_2) + (E_1+E_2)\cdot E_4 + E_3\cdot(E_1+E_2) + E_3\cdot E_4 =$
$= (E_1+E_2) + (E_1+E_2)\cdot(E_3+E_4) + E_3\cdot E_4 = E_1 + E_2 + E_3\cdot E_4$
MSC_1 MSC_2 MSC_3

-> Si possono costruire alberi con strutture diverse ma equivalenti.

$TE = MSC_1 + MSC_2 + MSC_3$

-> La probabilità che al tempo T = 10.000 ore il sistema sia guasto consiste nel calcolare l'indisponibilità relativa al Top Event:

$Q(TE) = Q(E) + Q(I) + Q(L_1 L_2) = 10^{-4} + 10^{-6} + (2\cdot10^{-3}\cdot 2\cdot10^{-3})$
$\simeq 1{,}05\cdot10^{-4}$

CAUSE COMUNI DI GUASTO: possono esistere delle cause comuni di guasto, imprevedibili (come ad esempio un incendio/ il professore che prende a fiondate le lampadine). Noi ipotizziamo l'assenza di queste.

Risultati della FTA:

Probabilità di accadimento del TE (p oppure Q):

a) MCSi mutuamente esclusivi:
p(TE) = p(MCS1) + p(MCS2) + p(MCS3) + …

b) In generale (r = numero di MCS):
p(TE) = S1 – S2 + S3 – … (-1)r-1 ·Sr
S1 = p(MCS1) + p(MCS2) + p(MCS3) + ...
S2 = p(MCS1)·p(MCS2) + p(MCS1)·p(MCS3) + …
S3 = sommatoria dei prodotti del terzo ordine
...
N.B. La probabilità di accadimento del TE corrisponde all'indisponibilità del TE
-> Sommare MSC porta a trascurare minimi cambiamenti, positivi/negativi, e questo ci porta a trascurare ???

Numero atteso di guasti del TE (W):

NUMERO ATTESO DI GUASTI (W): numero atteso di volte che si verifica il TE in seguito all'accadimento degli eventi che costituiscono il MCS.

In un intervallo di tempo, W indica il numero atteso di volte che si verifica il TE in seguito all'accadimento degli eventi che costituiscono il MCS. Se, ad esempio, MCS = {A, B} e l'intervallo di tempo è pari a T:

$$W(AB) = \int_0^T (\lambda_A Q_B + \lambda_B Q_A)dt$$ ← Porta AND

$$W(AB) = \int_0^T (\lambda_A Q_B)dt$$ ← Porta INH

TASSO DI GUASTO

Nel caso di MCS con un solo evento (MCS = {C} con tempo = T):
$W(C) = \lambda_c \cdot T$

-> Le regole con cui si calcola W(TE) sono le stesse viste per p(TE) a proposito dell'unione dei MCS: W(TE) = S1 – S2 + S3 – …

Limite superiore e limite inferiore:

- Il termine S1 corrisponde al limite superiore (upper bound);
- Il termine S1 – S2 rappresenta il limite inferiore (lower bound);
- Il valore esatto di P(TE) o di W(TE) è compreso tra questi due limiti

-> Presenza componente in Stand-By

Riprende Esercizio 1:

Nell'ipotesi che il componente L2 sia in stand-by (ovvero normalmente in attesa quindi pronto ad attivarsi nel caso di guasto di L1) e trascurando la probabilità di fallimento del passaggio da uno all'altro, con gli stessi dati precedenti ad eccezione di quelli relativi a L2 (si pone λ = 10-4 guasti/ora in quanto cambia la condizione di funzionamento e ϑ = 500 ore anziché μ) si ha:

$Q(L_2) = \frac{\lambda * \theta}{2} = \frac{10^{-4} * 500}{2} = 2{,}5 * 10^{-2}$;

da cui: Q(L1L2) = Q(L1)Q(L2) = 2·10-3·2,5·10-2 = 5·10-5
e quindi: Q(TE) ≈ 1,51·10-4

=> Quando ho un componente di sicurezza, la probabilità di indisponibilità di un sistema aumenta di circa il 50%.

-> Il numero atteso di guasti W(TE) nel tempo T = 10.000 ore (approssimando al limite superiore) è:
W(TE)sup = W(B) + W(I) + W(L1L2)
W(B) = λ_B*T
W(I) = λ_I*T
=> Se i due componenti L1 e L2 sono attivi (porta AND):

$$W(L_1L_2) = \int_0^T (\lambda_{L_1} Q_{L_2} + \lambda_{L_2} Q_{L_1})dt$$

=> Se il componente L2 è di sicurezza (porta INH):

$$W(L_1L_2) = \int_0^T (\lambda_{L_1} Q_{L_2})dt$$

→ In valori numerici:

$W(TE) = W(B) + W(I) + W(L_1 L_2) = \lambda_B \cdot T + \lambda_I \cdot T + W(L_1 L_2) =$
$= \int_0^T (\lambda_{b_1} Q_1 + \lambda_{b_2} Q_2)\, dt$

↳ $W(B) = \lambda_B \cdot T = 10^{-5} \cdot 10^4 = 0.1$

↳ $W(I) = \lambda_I \cdot T = 10^{-7} \cdot 10^4 = 0.001$

↳ $W(L_1 L_2) = \int \lambda_I \frac{\lambda_2}{\mu_2} + \lambda_2 \cdot \frac{\lambda_1}{\mu_1}\, dt = 2 \int_0^{T_2} \frac{\lambda^2}{\mu} dt = 2 \frac{\lambda^2}{\mu} T = 0.04$

Dato che le ridondanze sono uguali, possiamo fare x2

-> Nel caso la luce due si trattasse del componente di sicurezza =>

INH: Componente di sicurezza

→ $W(L_1 L_2) = \int_0^T \lambda_1 \cdot \frac{\lambda_2 \Theta}{2}\, dt = \frac{\lambda \cdot \lambda \Theta}{2} T = 0.25.$

↳ Coef. di sicurezza

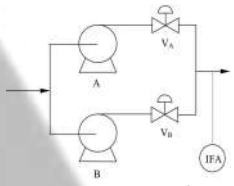
=> $W(TE)_{SUP\ AND} = 0.1 + 0.001 + 0.04 = 0.141$

$W(TE)_{AND} = 0,136864$ → non approssimato

=> $W(TE)_{SUP\ INH} = 0.1 + 0.001 + 0.25 = 0.351$ ← Errore di margine (ci piace)

$W(TE)_{INH} = 0.325675$ → non app.

Esercizio 2:



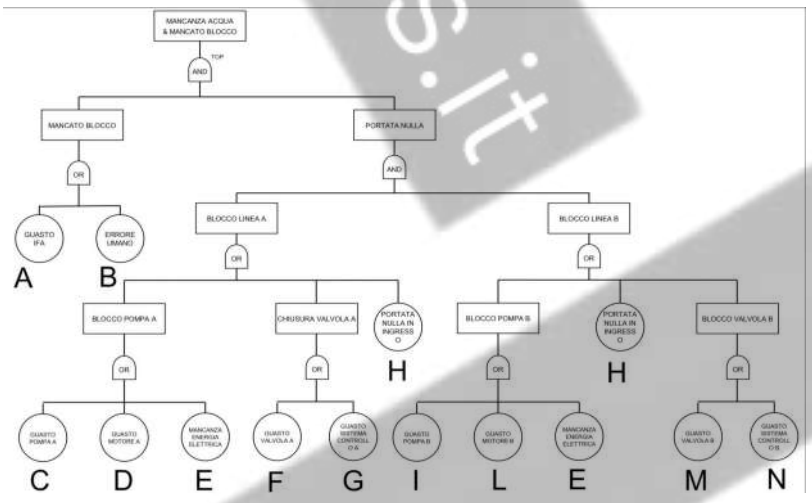
Le pompe A e B funzionano con continuità e sono in grado di fornire ognuna il 100% del fabbisogno. Le valvole VA e VB sono automatiche, controllate da un loop non riportato nello schema. In caso di mancanza di portata, l'allarme IFA allerta l'operatore che ha il tempo di mettere in sicurezza l'impianto. Si studi il Top Event"mancanza completa di acqua e mancata messa in sicurezza dell'impianto".

-> Entrambi i rami d'acqua riescono a fornire il 100% => Le cause per cui non arrivi l'acqua sono:

- Chiuse entrambe la valvole;
- Non funzionano entrambe le pompe.
- Non arriva acqua di alimentazione => Non vanno entrambe => Causa comune di guasto (non ci garba quando si fanno i calcoli);

-> Non funziona l'allarme.

Soluzione:

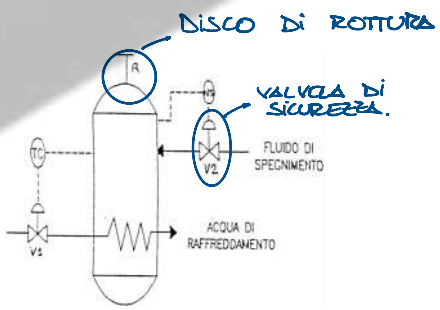


BASIC EVENTS: sono gli eventi alla fine dell'albero (le foglie).

-> Come si stimano i dati dei "Basic Events"?

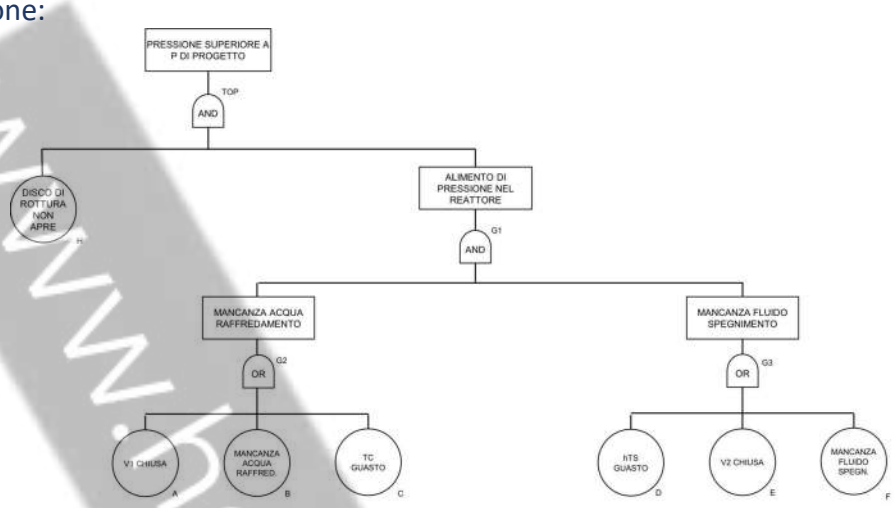
- Grazie ad analisi;
- Grazie allo storico;
- Grazie ai dati del costruttore.

Esercizio 3:



La temperatura nel reattore è regolata da TC e dalla valvola V1. In caso di alta temperatura, il sensore hTS apre la valvola V2 del fluido di spegnimento. In caso di mancato spegnimento, il disco di rottura R apre.
Si studi il Top Event "pressione nel reattore superiore a quella di progetto".

Soluzione:



→ Definiamo gli eventi:
- $G_2 = A + B + C$
- $G_3 = D + E + F$

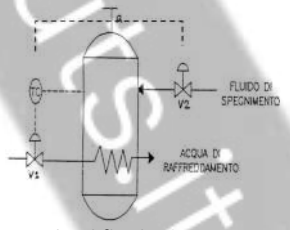
$\Rightarrow G_1 = G_2 \cdot G_3 = (A+B+C)(D+E+F)$

=> Top Event:

$TE = H \cdot G_1$

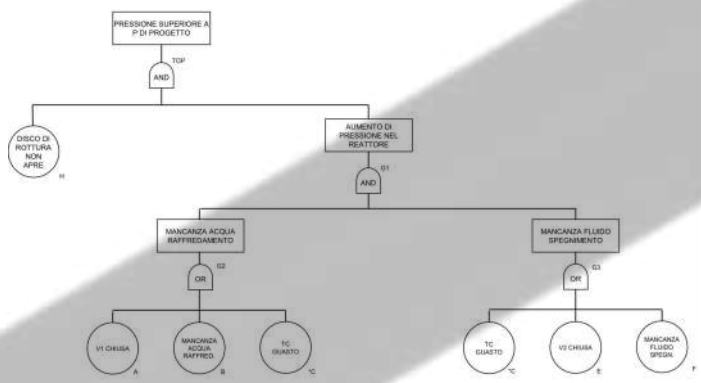
=> Qualsiasi altra cosa che accade assieme all'evento " non si apre il disco di rottura" => Abbiamo un problema.

Esercizio 4:



In questo caso sia l'acqua di raffreddamento che il fluido di spegnimento sono controllati da TC.
Si analizzi lo stesso Top Event dell'esercizio precedente ("pressione nel reattore superiore a quella di progetto").

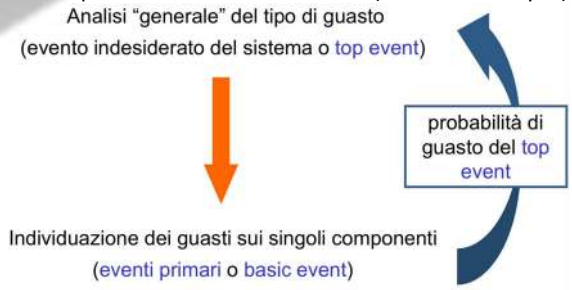
Soluzione:



Nota Bene:

- Alberi differenti devono essere per forza logicamente equivalenti, se ridotti agli stessi MCS.

-> Torniamo all'inizio e cerchiamo di capire bene il modello della FTA (Fault Tree Analysis):



-> Definizione TE:

- Può essere definito a scelta;
- Viene definito come un legame funzionale logico;

Per cosa può essere utilizzato:

- È uno strumento di analisi e aiuto di scelta decisionale.
- Analisi di sensitività: cambiare un parametro e vedere quanto pesa sul totale.

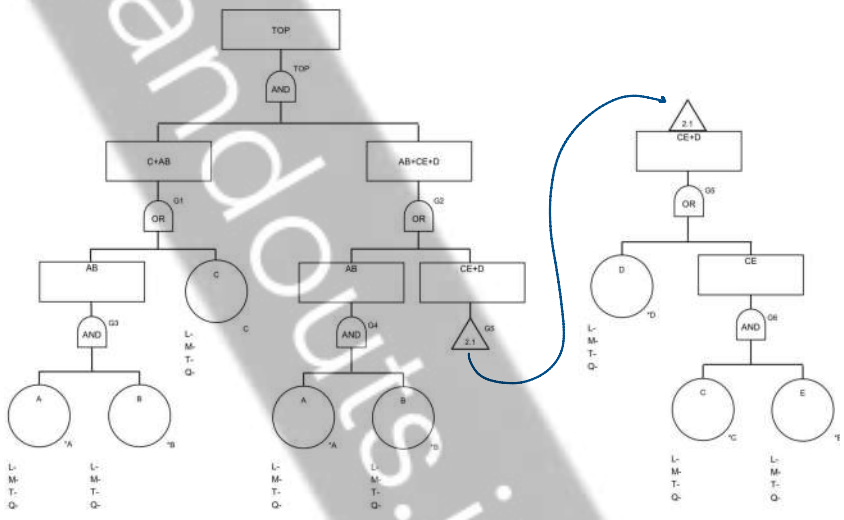
Esercizio autonomo 6:

Si calcoli il numero atteso di guasti del Top Event per un tempo T = 10.000 ore.

Componente	λ [ore^{-1}]	μ [ore^{-1}]
A	10^{-5}	0,01
B	10^{-5}	N.R.
C	10^{-4}	0,005
D	10^{-4}	0,05
E	10^{-5}	N.R.

N.R. = non riparabile => NON SO CALCOLARE Q.

Soluzione:



... | 2.1 = 2.1 : È UN LINK | ...

-> CALCOLO TE:

- G3 = G4 = A + B
- G6 = C + D
- G1 =

} NO => I QUADRATONI INDICANO IL VALORE DI CIÒ CHE STA SOTTO.

$$\Rightarrow TE = (C+AB)(AB+CE+D) = CAB + CCE + CD + AB \cdot AB + ABCE + ABD = AB + CE + CD$$

(CE, AB; ABCE + ABD → ASSORBITI)

$$W(TE) = W(AB) + W(CE) + W(CD)$$

$$W(AB) = \int_0^T (\lambda_A Q_B + \lambda_B Q_A)\,dt \quad (\text{IN GENERALE}, \; Q_B \to \lambda T) = \int_0^T \left(\lambda_A \cdot \lambda_B \cdot T + \lambda_B \cdot \frac{\lambda_A}{\mu_A}\right) dt \quad (\text{DATO } Q_B \text{ N.R.})$$

-> Se un componente è N.R. => non posso calcolarmi disponibilità/indisponibilità:

aff < $R = e^{-\lambda t} \to 1-R = Q$; $A = \ldots \to 1-A = \frac{\lambda}{\mu}$ > => TRATTIAMO L'INAFFIDABILITÀ : $1 - e^{-\lambda t} = \lambda t$

INFATTIBILE SE COMPON. N.R. (NON ABBIAMO μ)

$\Rightarrow W(AB) = \lambda_A \cdot \lambda_B \frac{T^2}{2} + \frac{\lambda_B \lambda_A}{\mu_A} T_A = 5,1 \cdot 10^{-3}$

-> Fare attenzione a N.R.: non riparabile. Q in questo caso non lo otteniamo come disponibilità, ma come inaffidabilità.

- In questa formula l'importante è che Q sia un numero compreso tra 0 e 1.

-> RIPETIAMO X ALTRI DUE COMPONENTI:

-> $W(CE) = \lambda_C \lambda_E \frac{T^2}{2} + \frac{\lambda_E \lambda_C}{\mu_C} T = 5,2 \cdot 10^{-2}$

-> $W(CD) = \left(\lambda_C \frac{\lambda_D}{\mu_D} + \lambda_D \frac{\lambda_C}{\mu_C}\right) T = 2,2 \cdot 10^{-2}$

-> Individuare il numero minimo di MCS che mi individui il guasto => sommo tutti i W calcolati per individuare la probabilità di trovare un errore => il numero dei MCS:

-> Esempio: Continuando il caso prec.: $W(TE) = 5,1 \cdot 10^{-3} + 5,2 \cdot 10^{-2} + 2,2 \cdot 10^{-2} = 7,91 \cdot 10^{-2}$

-> Calcolo numero guasti:

- $W(AB) = \frac{5,1 \cdot 10^{-3}}{7,91 \cdot 10^{-2}} = 6,45\%$
- $W(CE) = \frac{5,2 \cdot 10^{-2}}{7,91 \cdot 10^{-2}} = 65,74\%$
- $W(CD) = \frac{2,2 \cdot 10^{-2}}{7,91 \cdot 10^{-2}} = 27,81\%$

-> Si indichi il numero di MCS che permetta di individuare l'X% del numero di guasti => sommiamo i W (i) calcolati, ottenendo un numero ≥ X%. Contiamo quanti i abbiamo sommato per ottenere il numero minimo.

Esercizio 7:

Calcolare il numero di guasti atteso in un tempo di missione di 10.000 ore. Il componente E ha una probabilità di guasto (indisponibilità) costante e pari a 0,001. E e D sono componenti di protezione/sicurezza.

	λ tasso di guasto [ore^{-1}]	$\tau = \mu^{-1}$ tempo di riparazione [ore]	θ intervallo tra due test [ore]
A	10^{-5}	10	-
B	10^{-4}	2	-
C	10^{-6}	100	-
D	10^{-4}	-	720
E	-	-	-
F	10^{-9}	-	-

Albero: