UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA INDUSTRIALE

CORSO DI LAUREA MAGISTRALE IN INGEGNERIA DELLA SICUREZZA CIVILE E INDUSTRIALE

Tesi di Laurea Magistrale in

Analisi del rischio nell'industria di processo

Albero dei guasti dinamico: metodologie e applicazione a un caso studio

Relatore: Dott. Ing. Chiara Vianello

Laureando: Matteo Soardo

ANNO ACCADEMICO 2018 – 2019

Riassunto

Lo scopo della seguente trattazione è quello di analizzare una metodologia prevista dall'analisi del rischio per l'individuazione di rischi all'interno di un sistema produttivo, chiamata Albero dei Guasti, discostandosi dall'applicazione tradizionale che segue un modello statico che utilizza parametri medi reperibili in letteratura.

In tale direzione viene scelto di analizzare ed applicare ad un caso studio l'approccio definito di tipo dinamico utilizzando parametri tempo dipendenti, con lo scopo di ottenere informazioni e dati che più si avvicinano alle situazioni che possono presentarsi nella realtà di un impianto produttivo, per il quale viene condotto uno studio di sicurezza parallelamente alla sua progettazione.

Definito il Top Event oggetto di valutazione, viene quindi effettuata la costruzione dell'albero sia per l'analisi di tipo statica, sia per quella di tipo dinamica.

Quando la probabilità di errore definisce il verificarsi dell'evento incidentale, vengono attuati i piani di manutenzione che permettono, dopo un periodo di intervento adeguato, di ristabilire il funzionamento dell'impianto andando ad intervenire sui componenti danneggiati presenti nel processo considerato.

Infine, vengono confrontati i risultati andando a commentare ed evidenziare le differenze dei parametri considerati, ottenuti operando metodologicamente nello stesso ordine durante il processo di analisi, ma applicando i due diversi approcci.

Indice

Introduzione

Durante la progettazione di un impianto produttivo, la sicurezza è uno degli aspetti più importanti e deve essere sviluppata e integrata con la progettazione.
Durante lo studio di sicurezza, una delle fasi fondamentali è quella legata alla valutazione del rischio: deve riguardare tutti i rischi per la sicurezza e la salute dei lavoratori, da questa analisi emergono quali sono le parti più critiche dell'insieme produttivo dal punto di vista del funzionamento, delle interferenze che possono provenire dall'esterno e problematiche legate dalla presenza del fattore umano, infine è fondamentale per identificare quali sono le misure idonee da adottare per ridurre il rischio durante l'attività lavorativa in impianti e sistemi complessi.
Per identificare il rischio si utilizzano più metodologie che possono portare ad analisi qualitative o quantitative a seconda del risultato che si vuole ottenere, una metodologia utile per ricavare informazioni, come per esempio la probabilità di accadimento di un evento, le condizioni alle quali tale evento dipende e il modo in cui tale probabilità di accadimento può essere influenzata, è la tecnica dell'Albero dei Guasti (Fault Tree Analysis - FTA).

Nel primo capitolo si introduce il quadro legislativo per quanto riguarda l'analisi del rischio in Italia e le principali nozioni dell'analisi del rischio, la metodologia dell'Albero dei Guasti, da cosa è composto e la sua costruzione. Viene introdotto il concetto di dinamicità applicata a FTA tradizionale attraverso la distribuzione di Weibull a due parametri: il fattore di scala α e il fattore di forma β.
Nel secondo capitolo si presenta lo stato dell'arte dell'albero dei guasti dinamico attraverso la ricerca di vari studi che trattano l'applicazione di questa metodologia in studi di affidabilità di interi sistemi o più specificatamente a parti di essi.
Nel terzo capitolo viene messa in pratica la metodologia FTA dinamica applicandola a un Minimal Cut Sets (MCS) di un caso studio affrontato durante il corso di Analisi del rischio: si sperimenta così la sua applicazione e si osservano i risultati di tassi di guasto h(t), frequenze di guasto e probabilità di accadimento nel tempo sia analiticamente che sotto forma grafica.
Una volta raggiunto la probabilità di guasto e quindi l'avvenimento incidentale, si procede con l'applicazione dei piani di manutenzione al componente danneggiato, successivamente a questa operazione si controlla come variano i parametri precedentemente ricavati.
Nel quarto capitolo si affronta l'applicazione vera e propria della metodologia tempo dipendente, al caso studio che riguarda il Top Event individuato all'interno di una raffineria, ovvero il superamento della pressione di progetto in una colonna di distillazione.

Viene eseguito inoltre un confronto tra i risultati ottenuti applicando l'approccio di analisi tradizionale e quello dinamico.

Nel capitolo 5 vengono riportate le conclusioni e alcune osservazioni riguardo l'utilizzo della metodologia di analisi dell'Albero dei Guasti con approccio dinamico rispetto al metodo tradizionale durante uno studio di sicurezza che riguarda un impianto produttivo. Vengono infine riportati alcuni spunti per una futura continuazione della ricerca.

Capitolo 1

L'analisi del rischio in Italia

Il capitolo introduce il quadro normativo e le nozioni fondamentali dell'analisi del rischio.

1.1 Quadro normativo

Il quadro normativo nazionale fa riferimento principalmente a due normative: il Testo Unico sulla salute e sicurezza sul lavoro e la direttiva Seveso per le industrie soggette ad incidente rilevante.

1.1.1 Testo Unico sulla salute e sicurezza sul lavoro

La legislazione nazionale dal punto di vista della tutela del lavoro, attraverso il D.Lgs 81/2008 ("Testo unico sulla salute e sicurezza sul lavoro"), in Titolo I, riporta che il processo di valutazione dei rischi è uno dei compiti non delegabili[1] del Datore di Lavoro attraverso il quale egli riesce a fornire un primo strumento di tutela per la salute e sicurezza dei lavoratori nei luoghi di lavoro[2].

Con questo strumento normativo quindi, è possibile stabilire e garantire ai lavoratori alcuni elementi base per la loro tutela durante l'attività lavorativa, vengono inoltre stabiliti dei punti guida che il datore di lavoro, al fine di poter garantire la tutela dei diritti dei suoi lavoratori, deve seguire.

Il processo di valutazione dei rischi e i conseguenti risultati, sono contenuti all'interno del documento di valutazione dei rischi, con la redazione e sottoscrizione di esso da parte del datore di lavoro[3], vengono poi implementati, attraverso una specifica programmazione, dei sistemi per la prevenzione dai pericoli individuati e ove non sia possibile preventivamente, poiché permane del rischio residuo, adozione di misure protettive.

[1] Art 17 co. 1 lett. a
[2] Art 15 co. 1 lett. a
[3] DVR deve essere firmato anche da RSPP, MC ed RLS. Art 28 co. 2

1.1.2 Direttiva Seveso

Con il D.Lgs 105/2015 l'Italia recepisce la Direttiva 2012/18/UE, (Seveso III), essa rappresenta uno strumento utile per la tutela della sicurezza dei lavoratori dagli incidenti di tipo rilevante.

La definizione di incidente rilevante[4] viene fornita dalla precedente versione di tale Direttiva oggi in vigore, chiamata Seveso II (D.Lgs. 334/99 in recepimento della direttiva 96/82/CEE), in Capo I:

> "un evento quale un'emissione, un incendio o un'esplosione di grande entità, dovuto a sviluppi incontrollati che si verificano durate l'attività di uno stabilimento di cui all'articolo 2, comma 1, e che dia luogo ad un pericolo grave, immediato o differito, per la salute umana o per l'ambiente, all'interno o all'esterno dello stabilimento, e in cui intervengano una o più sostanze pericolose".

L'esigenza di normazione per la tutela della sicurezza in ambito industriale è stata evidenziata con l'accadimento dell'evento disastroso avvenuto nel 1976 nell'azienda ICMESA di Meda che vede la successiva nascita della Direttiva 85/501/CEE "Seveso" (in Italia la prima versione del suo è il DPR 17 maggio 1988).

L'incidente sopra citato è avvenuto in seguito all'apertura di una valvola di sicurezza che causò la fuoriuscita di una nube di diossina TCDD, sostanza chimica tossica.

La nube arrivò a colpire vari comuni limitrofi lo stabilimento e in particolare quello di Seveso, non ci furono conseguenze mortali ma parte della popolazione fu colpita da cloracne, in seguito alcuni terreni furono asportati per contaminazione con la sostanza e degli animali furono abbattuti.

[4] Art 3 c. lett. f

1.2 L'analisi del rischio

La valutazione del rischio deve riguardare tutti i rischi per la sicurezza e la salute dei lavoratori, compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari[5].

L'analisi del rischio è fondamentale per identificare i rischi potenziali di un processo e quindi adottare misure idonee atte alla riduzione del rischio durante l'attività lavorativa in impianti e sistemi complessi.

Essa accompagna la fase di progettazione ed evolve con essa, è normalmente applicata negli impianti chimici dove è importante la conoscenza del processo chimico per quanto riguarda qualsiasi fattore che lo caratterizza:

- componenti, parti meccaniche, meccanismi di funzionamento, fascicoli tecnici, manuali di uso e manutenzione propri del sistema;
- manutenzione ordinaria e straordinaria;
- azioni a livello organizzativo e procedurale;
- contesto ambientale interno ed esterno lo stabilimento.

Per quanto riguarda le sostanze chimiche impiegate durante il processo, nella valutazione dei rischi è importante che il datore di lavoro indichi la presenza di agenti chimici pericolosi sul luogo di lavoro ed effettui quindi una valutazione dei rischi per la salute e sicurezza dei lavoratori derivanti dalla presenza di tali agenti, prendendo in considerazione le loro proprietà pericolose, le informazioni sulla salute e sicurezza comunicate dal fornitore tramite la relativa scheda di sicurezza[6] (SDS), livello modo e durata dell'esposizione, circostanze in cui viene svolto il lavoro in presenza di tali agenti tenuto conto della quantità delle sostanze e delle miscele che li contengono o che li possono generare, valori limite di esposizione professionale o i valori limite biologici[7], gli effetti delle misure preventive e protettive adottate o da adottare.

Dall'analisi del rischio emergono quali sono le parti più critiche dell'insieme produttivo dal punto di vista del funzionamento, delle interferenze che possono provenire dall'esterno e problematiche legate dalla presenza del fattore umano.

In art. 28 co. 2 lett. A del D.Lgs. 81/08 il legislatore riporta che la valutazione del rischio è redatta specificando i criteri adottati e che tale scelta di redazione del documento è rimesso al datore di lavoro, egli garantisce che sia redatto con criteri di semplicità, brevità e comprensibilità, in modo da

[5] D.Lgs. 81/08, art 28 co 1

[6] Le SDS sono predisposte ai sensi del regolamento CE n.1907/2006 del Parlamento europeo e del Consiglio

[7] I limiti sono riportati in allegato XXXVIII e XXXIX del D.Lgs 81/2008

garantirne la completezza e l'idoneità come strumento operativo di pianificazione degli interventi aziendali e di prevenzione.
Nei seguenti paragrafi a seguire viene descritta la metodologia per la valutazione del rischio.

1.2.1 Identificazione del rischio

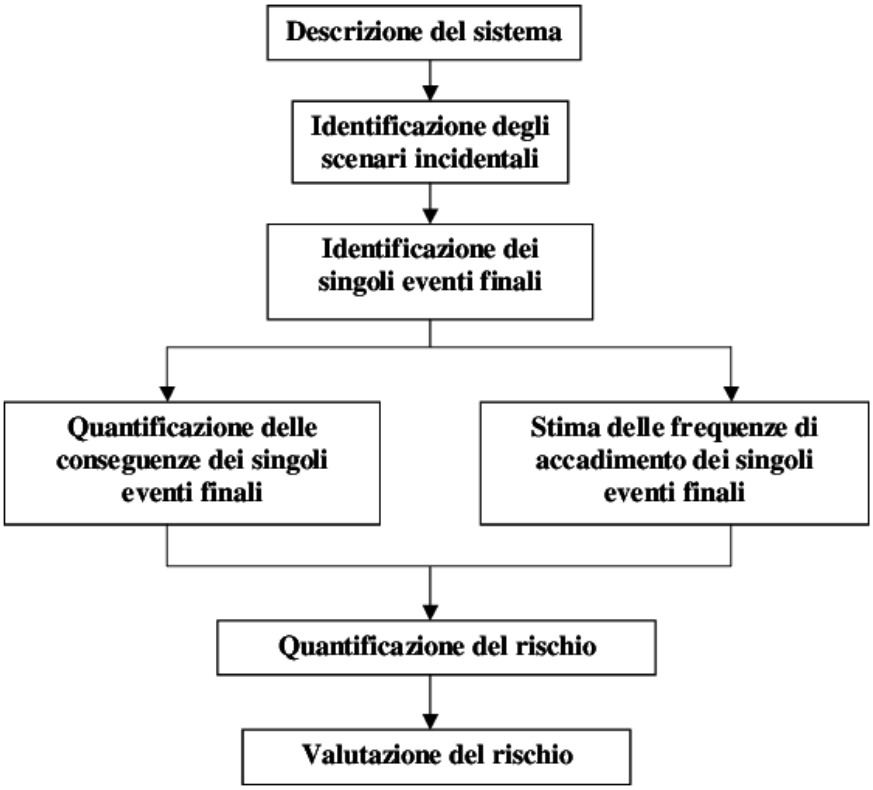


Figura 1.2.1 - *Schema riportante le fasi dell'analisi del rischio*

L'identificazione del rischio segue diverse fasi (Center for Chemical Process Safety, 2010):

- definizione dello scenario incidentale: TOP EVENT;
- valutazione delle frequenze di accadimento;
- valutazione delle conseguenze;
- calcolo del rischio: $R = f\ x\ M$[8]; (1.2.1)

Lo step finale è valutare se il risultato ottenuto dalla valutazione del rischio è accettabile o non accettabile.

[8] R= rischi, f= frequenza di accadimento, M= magnitudo

Nel caso non sia accettabile si devono prevedere delle misure di prevenzione e/o mitigazione del rischio per riportarlo ad una condizione di accettabilità.

Le misure che si possono applicare sono:

- misure di mitigazione del rischio preventive vengono adottate per abbassare la frequenza di accadimento;
- misure protettive dal rischio sono adottate per limitare il danno causato dall'evento negativo.

Per identificare il rischio si utilizzano più metodologie che possono portare ad analisi qualitative o quantitative a seconda del risultato che si vuole ottenere.

Una metodologia utile per ricavare informazioni, quali ad esempio probabilità di accadimento di dell'evento, le condizioni alle quali tale evento dipende e il modo in cui tale probabilità di accadimento può essere influenzata, è la tecnica dell'Albero dei Guasti.

Questo tipo di analisi si basa su un modello qualitativo che attraverso l'utilizzo di frequenze di guasto e logiche derivante dall'algebra booleana può essere valutato quantitativamente.

1.3 Albero dei guasti

1.3.1 Storia della metodologia

FTA è una metodologia il cui utilizzo è previsto dall'analisi del rischio, essa nasce all'inizio degli anni '60 dall'esigenza di dover analizzare sistemi produttivi complessi come ad esempio quelli che riguardano l'ambito nucleare, oggi trova sempre più occasioni di applicazione nell'industria manifatturiera o dei servizi poiché è un metodo semplice ed efficace per testare l'affidabilità e la sicurezza di questi sistemi.

Di seguito viene riportato la diffusione e l'uso che ha avuto negli anni questa metodologia (Clifton, 1999).

- 1961-1970 (esordio)

  1961 – H. Watson of Bell Labs, along with A. Mearns, la tecnica viene sviluppata e applicata alla valutazione del sistema di controllo per il lancio dei Minuteman;

  1963 – Dave Haasl di Boeing assume la metodologia come significativo strumento di analisi della sicurezza del sistema;

  1964-1967, 1968-1969 – periodo di maggiore utilizzo per la valutazione della sicurezza a partire dalla prima applicazione effettuata da Boeing sull'intero sistema Minuteman;

  Giugno 1965 – in occasione della prima conferenza sulla sicurezza tenutasi a Seattle vengono presentati i primi documenti tecnici dell'analisi FTA;

  1966 – Boeing inizia a utilizzare FTA per la progettazione e la valutazione degli aerei ad uso commerciale;

  In questo periodo, Boeing sviluppa un programma di simulazione dell'analisi composto da 12 fasi e un software per la costruzione dell'albero dei guasti adottato dall'industria aerospaziale.

  1969 – La metodologia ha notevole sviluppo in campo nucleare, viene pubblicata in questo anno la teoria probabilistica Kinetic Tree Theory (KITT). Questa teoria consente di calcolare gli "upper bounds" per l'indisponibilità, frequenza di guasto, numero medio di guasti ed indici di importanza per i componenti. La sua applicazione richiede la conoscenza di Minimal Cut

Sets, sono stati così studiati diversi metodi per la loro determinazione basati su diversi approcci: riduzione dell'albero Top-down, Bottom-up e Ibrida, pattern recognition ed altri.

- 1971-1980

  La metodologia viene adottata nel settore dell'energia nucleare e dell'industria energetica, vengono elaborati codici e algoritmi avanzati.

- 1981-1990

  L'impiego di tale metodologia nel campo della sicurezza diventa internazionale, la documentazione tecnica aumenta e vengono sviluppati ulteriori algoritmi e codici di valutazione.

- 1991-1999

  L'analisi FTA si diffonde sempre di più e vengono elaborati codici informatici commerciali di alta qualità adottati dall'industria robotica e dei software.

- 2000 in poi

  Negli ultimi vent'anni per quanto riguarda lo sviluppo ed applicazione di questa metodologia di analisi, la direzione è sempre più quella di seguire l'approccio di tipo dinamico, tema principale di questa trattazione.

  Alcuni esempi a supporto della tesi sono riportati a seguire nel capitolo 2 in cui, negli articoli riportati, sono spiegate delle applicazioni di FTA tempo dipendente.

1.3.2 Costruzione e interpretazione (Stoffen, 1997)

La costruzione dell'albero dei guasti comincia in fase di progettazione del sistema produttivo quando esso non è ancora fisicamente esistente, lo scopo principale è quello di individuare qualsiasi punto critico e di debolezza ed intervenire per eliminarlo o contenerlo, si interviene sul progetto attraverso la ricerca di modifiche e soluzioni alternative che possono evitare spiacevoli sorprese successivamente (ad esempio il verificarsi di incidentali gravi) e di dover effettuare in fase troppo avanzata della progettazione, o durante l'utilizzo vero e proprio del sistema produttivo, di interventi di miglioramento troppo costosi.

Introducendo modifiche durante la progettazione del sistema, la rappresentazione iniziale dell'albero non è definitiva, è quindi importante che la sua costruzione segua parallelamente questa fase.

Esso così deve essere continuamente aggiornato con le dovute variazioni ed integrazioni poiché possono presentarsi nuovi rischi che devono essere ridotti o evitati.

La procedura per ricavare l'albero dei guasti segue un preciso ordine a seconda del risultato che si vuole ottenere.

Per l'analisi qualitativa:

- conoscenza del sistema: conoscere in dettaglio come funziona il sistema e quali modalità di guasto devono essere prese in considerazione.
  Definizione dell'evento principale e costruzione dell'albero dei guasti. Se disponibile, si può seguire il Process Flow Diagram (PFD) del processo produttivo per la sua costruzione;
- determinazione di Minimal Cut Sets.

Per l'analisi quantitativa:

- raccolta di tutti i dati relativi a guasti, riparazioni, test e manutenzione;
- quantificazione MCS;
- valutazione dei risultati.

L'approccio seguito è di tipo deduttivo e parte dal Top Event individuato in una fase precedente a quella dell'analisi del rischio (fasi in riferimento allo schema di Figura 1.2.1)

Procedendo dalla cima dell'albero e andando verso il fondo (metodologia top-down) le diramazioni sottostanti si aggiungono andando ad analizzare le possibili cause che possono aver portato all'evento sfavorevole in analisi, le ramificazioni rappresentano i collegamenti delle catene di guasti e malfunzionamenti (failures) che colpiscono le componenti primarie del sistema analizzato utilizzando porte logiche.

Le porte logiche sono elementi che servono a consentire o contrastare il propagarsi del guasto, mostrando le relazioni degli eventi necessari per il verificarsi del Top Event (Tabella 1.3.2).

Lo scopo del procedere nella costruzione dall'alto verso il basso è quello di ricercare gli eventi primari che hanno dato inizio alla catena di failures arrivando fino all'evento finale, una volta ricavati gli eventi primari (base) è possibile determinare o stimare una probabilità di accadimento.

Alcuni eventi base interessano:

- componenti meccanici del sistema;
- guasti degli hardware facenti parte dei componenti;
- sistemi di sicurezza;
- mancate verifiche di manutenzioni o test;
- fattori legati al comportamento umano e a circostanze ambientali.

Tabella 1.3.2 - *Simboli Albero dei Guasti*

SIMBOLO	PORTA LOGICA	DESCRIZIONE
	evento intermedio	Un evento di errore che si verifica a causa di una o più cause antecedenti che agiscono attraverso porte logiche
	and gate	È necessario che tutti i guasti abbiano luogo e simultaneamente per determinare il guasto risultante.
	or gate	È sufficiente che almeno uno dei guasti abbia luogo per determinare il guasto risultante.
	evento base	Un evento di base che non richiede ulteriori sviluppi perché è stato raggiunto il limite di risoluzione appropriato
	trasferimento	un triangolo indica che l'albero si sviluppa ulteriormente al verificarsi del corrispondente simbolo di trasferimento
	evento non sviluppato	un diamante è usato per definire un evento che non è ulteriormente sviluppato o perché ha conseguenze insufficienti o perché l'informazione è irrinunciabile

1.3.3 Minimal Cut Sets

Attraverso l'individuazione dei MCS si possono ottenere risultati qualitativi, essi rappresentano la più piccola combinazione di eventi base sufficienti a causare l'evento principale.

I MCS sono determinati attraverso l'applicazione dell'algebra booleana.

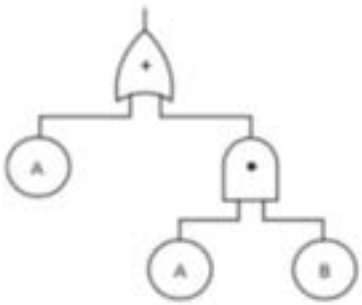
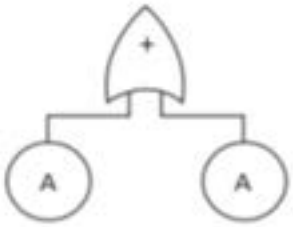
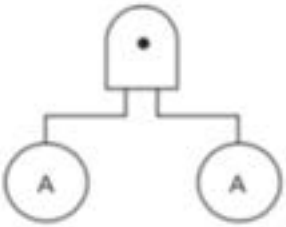
1.3.4 Algebra di Boole

Utilizzando l'algebra booleana si può tradurre la rappresentazione grafica dell'albero dei guasti in un insieme equivalente di equazioni booleane, alcune informazioni base per la comprensione delle espressioni riguardano:

- "+" interpretato come "o";
- "." Interpretato come "e".

L'utilizzo di tale metodologia permette di quantificare il top event dell'albero dei guasti.

Tabella 1.3.4 - Esempi di regole dell'algebra booleana

TERMINE DI SINISTRA FT	REGOLA	TERMINE DI DESTRA FT
	A+A=A	
	A.A=A	
	A+A.B=A	

1.4 Fallimenti correlati al tempo

1.4.1 Definizioni (Stoffen, 1997)

Il concetto di tasso di fallimento viene introdotto durante l'analisi del rischio e di affidabilità per poter valutare guasti legati al tempo. Esso viene utilizzato per descrivere la probabilità di guasto del componente a causa di fenomeni legati al tempo.

Si identificano due parametri di interesse che dipendono dal tempo e hanno dimensioni all'ora (Stoffen, 1997):

- tasso di guasto;
- densità di guasto.

La differenza tra questi due parametri è che sono applicabili a diverse popolazioni di componenti.

Tasso di guasto $\boldsymbol{\lambda(t)}$

Il tasso di guasto è applicabile ai componenti che sono sopravvissuti fino al tempo t.
$\lambda(t)dt$ è la probabilità che il componente abbia un guasto nell'intervallo t e t + dt, dato che il esso è sopravvissuto al tempo t.

$$\lambda(t)dt = P[l'errore\ si\ verifica\ tra\ t\ e\ t + dt | nessun\ guasto\ precedente]$$

Densità di guasto $\boldsymbol{f(t)}$

$f(t)dt$ è la probabilità che il componente subisca un primo guasto durante la sua vita nell'intervallo t e t + dt, quando per t=0 esso non ha mai subito alcun errore.

$$f(t)dt = P[primo\ errore\ tra\ t\ e\ t\ +\ dt\ |\ nessun\ guasto\ al\ tempo\ zero]$$

La densità di guasto è applicabile all'intera popolazione di componenti (sopravvissuti o meno), a differenza del tasso di errore, che è applicabile solo ai componenti che non hanno fallito.
La densità di guasto è normalizzata in termini di dimensioni della popolazione originale dei componenti e il tasso di guasto è normalizzato rispetto al numero medio di componenti funzionanti con successo al tempo t.
Questo può essere espresso con le seguenti formule in cui n(t) rappresenta il numero di componenti funzionanti al tempo t:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{n(t) - n(t + \Delta t)}{n(t)\Delta t}$$

$$f(t) = \lim_{\Delta t \to 0} \frac{n(t) - n(t + \Delta t)}{n(t = 0)\Delta t}$$

1.4.2 Bathtube curve (Stoffen, 1997)

Le definizioni riportate in precedenza non sono costanti nel tempo, l'andamento del tasso di guasto in funzione del tempo può essere classificato in tre periodi nella vita del componente come riportato graficamente dalla Bathtube curve in Figura 1.4.2.

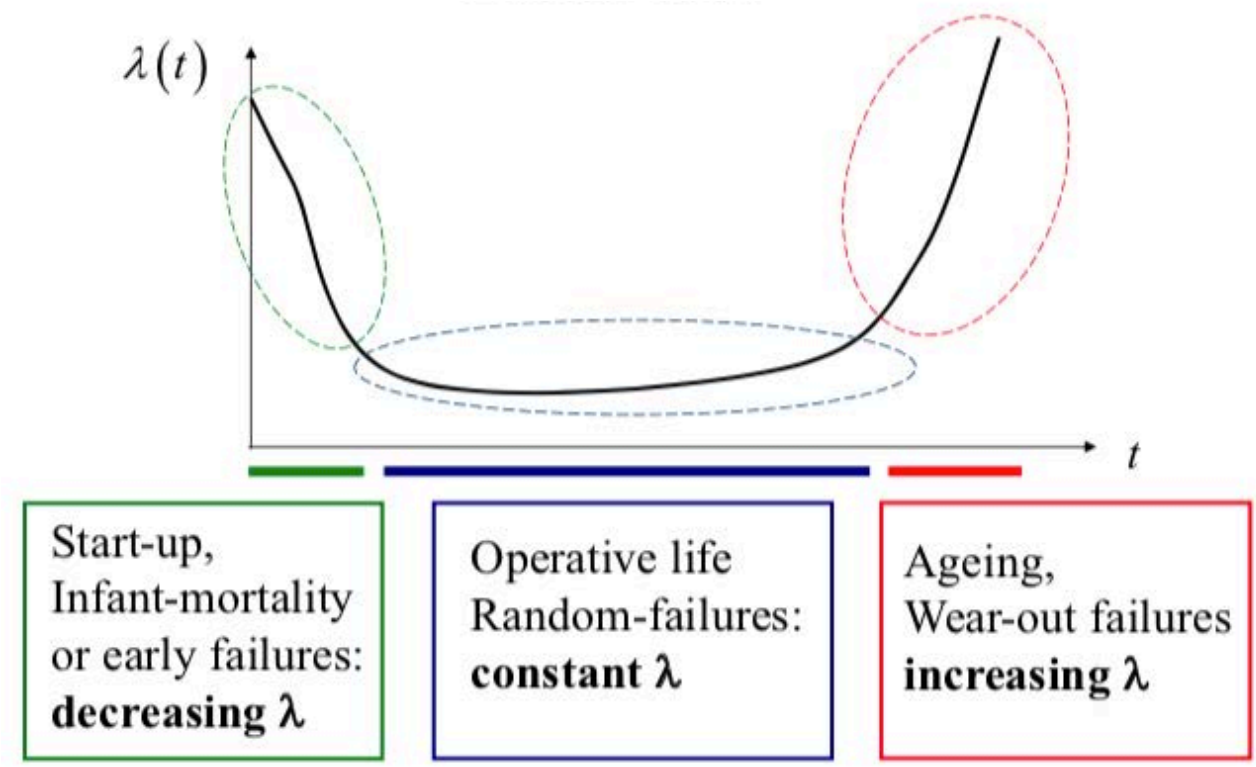


Fig 1.4.2 - *Bathtube curve (Leonardo Bertini, n.d.)*

La curva si suddivide in (Stoffen, 1997):

- **Periodo di insuccesso anticipato (riduzione del tasso di guasto)**

  Dopo l'avvio di un componente si entra nella prima fase di vita denominata anche rodaggio. In questo lasso di tempo normalmente si possono verificare diversi guasti a causa di errori di progettazione e di fabbricazione, errori di installazione, guasti durante l'avviamento e di funzionamento. Tipicamente tali cause vengono eliminate e corrette in questo primo periodo di vita così da far diminuire il tasso di insuccesso che inizialmente è elevato.

- **Periodo di errore casuale (tasso di guasto costante)**

  Nel periodo di "vita utile" dei componenti, i guasti che si presentano riguardano solamente cause accidentali: cause di guasto esterne o errori operativi, guasti durante la manutenzione o per sovraccarico occasionale.

  L'andamento del tasso di fallimento che caratterizza questo periodo della vita del componente è il più lungo tra tutti.

- **Periodo di fallimento dell'usura (aumento del tasso di guasto)**

  Nella fase finale di vita del componente si presentano le seguenti tipologie di cause: usura, corrosione, affaticamento e creep.

  Queste, influiscono in particolar modo sulla riduzione di resistenza e altre caratteristiche materiali del componente che caratterizzano un aumento della probabilità di fallimento.

1.5 Legge di Weibull

La rappresentazione attraverso la curva denominata "Bathtube curve" presenta un'immagine idealizzata della realtà. Per costruire questa curva per un determinato tipo di componente è necessario raccogliere molti dati di quella parte costitutiva durante la sua intera vita poiché durante il suo impiego il tasso di guasto non è costante.
La distribuzione rappresentata dalla Legge di Weibull, permette di rappresentare il modello probabilistico di certe grandezze che possono assumere valori causali sull'intero semiasse positivo, attraverso l'uso di due parametri: alfa e beta.

$$f_x(t) = \alpha\beta t^{\beta-1} e^{(-\alpha t^{\beta})} \qquad (1.5)$$

$$0 \leq t \leq +\infty;\ \propto, \beta\ \in\ \mathcal{R}$$

- fattore di forma (densità) β;
- fattore di scala α.

La densità β è il valore più significativo e definisce la forma della distribuzione di Weibull, a seconda del valore di β (Riccardo, n.d.):

- $\beta < 1$ tratto della curva ad andamento della curva decrescente;
- se $\beta = 1$ tratto della curva ad andamento costante "vita utile";
- $\beta > 1$ tratto della curva ad andamento crescente.

Il parametro $\alpha > 0$ (Riccardo, n.d.) è il fattore di scala che concentra su bassi valori di x (oppure disperde sul semiasse positivo) le masse di probabilità della distribuzione stessa, come si può osservare in Figura 1.5.

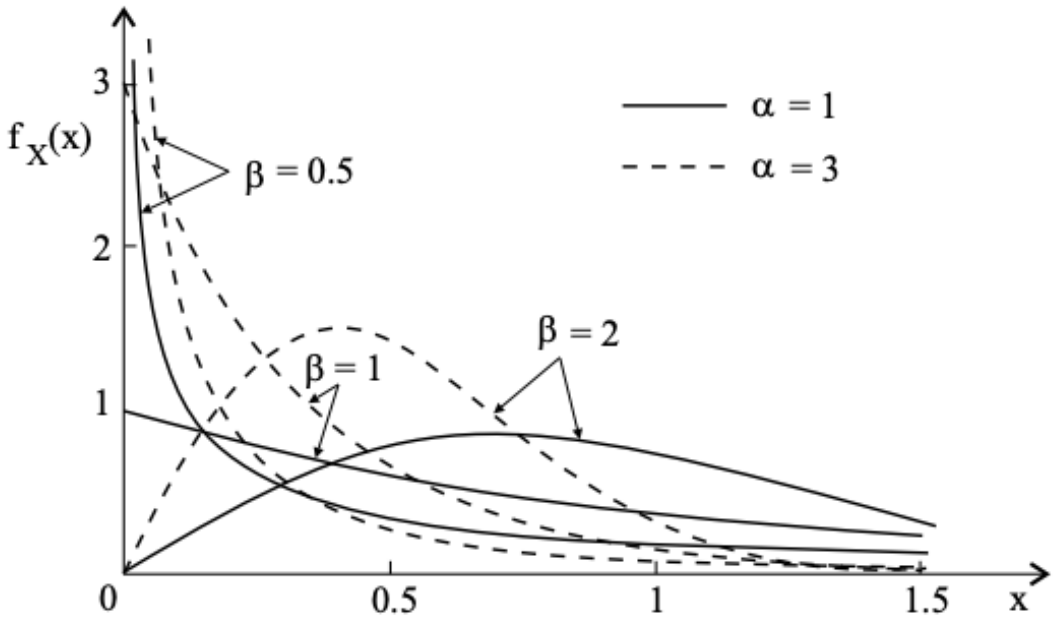


Figura 1.5 - *Distribuzione di Weibull $W(\alpha, \beta)$ al variare del parametro β e per $\alpha = 1$ e $\alpha = 3$ (Riccardo, n.d.)*

L'uso di questa distribuzione, rappresentante l'andamento nel tempo del tasso di guasto, essa assume un ruolo importante negli studi di affidabilità di materiali.

Assegnata la funzione:

$$h(t) = \alpha\beta(\alpha t)^{\beta-1} \qquad (1.5.1)$$

t= tempo di attesa del guasto

Individuati i parametri α e β, l'affidabilità del materiale diventa la seguente funzione del tempo di attesa:

$$R(t) = 1 - H(t) = e^{-\alpha t^{\beta}} \qquad (1.5.2)$$

$H(t)$ è la funzione di distribuzione cumulata di $W(\alpha, \beta)$, ossia la primitiva di $h(t)$ che si annulla per t=0.

1.5.1 Esempio: applicazione della distribuzione di Weibull nel caso statico $\beta = 1$[9]

In riferimento all'analisi FT di tipo statico viene riportato un esempio applicativo riferito al tratto di curva della vita di un componente di un sistema ad andamento costante in cui si possono manifestare errori di tipo casuale.

[9] L'applicazione riportata fa riferimento a slide introdotte durante il corso di Analisi del Rischio

In base alla distribuzione che caratterizza questo periodo si ricavano i parametri di seguito riportati.
Frequenza di guasto [accadimenti/anno] di un componente attraverso la distribuzione di Weibull:

$$f(t) = \beta\mu(\mu t)^{\beta-1}e^{-(\mu t)^{\beta}} \qquad (1.5.1.1)$$

μ=tasso di guasto medio calcolato, presente in letteratura.

t= tempo di attesa del guasto.

Per il calcolo della frequenza di guasto nel tratto di "vita utile" della curva, $\beta = 1$, *f(t)* si semplifica a:

$$f(t) = \mu e^{-\mu t} \qquad (1.5.1.2)$$

Successivamente dalla frequenza di guasto è possibile ricavare la probabilità di guasto *P(t)* e l'affidabilità *R(t)* in funzione del tempo di attesa:

$$P(t) = 1 - e^{-\mu t} \qquad (1.5.1.3)$$

P(t) indica la probabilità che un componente si guasti nell'intervallo [0,t].

$$R(t) = e^{-\mu t} \qquad (1.5.1.4)$$

R(t) indica la probabilità che un componente non si guasti nell'intervallo [0,t].

Come descritto in precedenza, questo tipo di risoluzione è applicabile solamente ad un'analisi di tipo statico comunemente uutilizzata nello studio della valutazione del rischio, in cui non si valuta l'influenza del tempo nella variazione dei tassi di guasto.
Esistono diversi studi in letteratura che si occupano della risoluzione di FTA dal punto di vista dinamico, nel prossimo capitolo ne vengono proposti alcuni con lo scopo di fornire un'idea generale di questo differente tipo di approccio.

Capitolo 2

Stato dell'arte: Albero dei Guasti Dinamico

Nel capitolo si presenta lo stato dell'arte dell'argomento preso in esame attraverso la ricerca di alcuni studi, essi al loro interno presentano applicazioni riguardanti l'approccio dinamico dell'analisi albero dei guasti in studi di affidabilità di interi sistemi di impianti o più in specifico, a singole componenti di essi.

2.1 Ricerche precedenti e loro conclusioni

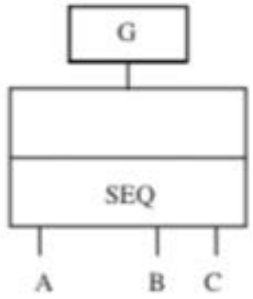
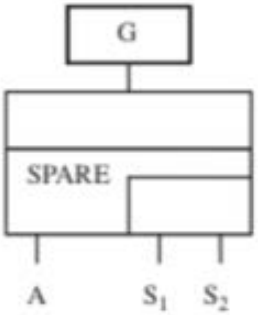
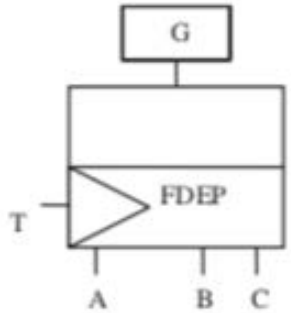
La metodologia FTA tradizionale non tiene conto della dinamicità dei sistemi produttivi oggetti di analisi, le tradizionali porte logiche (AND, OR) non possono acquisire il comportamento dinamico caratteristico dei meccanismi di un sistema che possono comprendere: errori del sistema, eventi dipendenti dalla sequenza di funzionamento, parti di ricambio e gestione dinamica della ridondanza, priorità degli eventi di errore.
Attraverso lo studio dinamico di un sistema considerando questi fattori, è possibile ottenere frequenze di accadimento degli eventi incidentali a partire da tassi di guasto molto più rappresentativi della realtà, soprattutto per quanto riguarda sistemi produttivi complessi.
In letteratura, è spesso affrontato questo tipo di problema ed è quindi possibile ricavare da essa e approfondire, l'utilizzo di varie metodologie integrative della tradizionale FTA di tipo statico per le considerazioni di tipo dinamico:

1. "A new approach to solve Dynamic Fault Trees" (Amari, Dill, & Howald, 2003);
2. "Dynamic Fault Tree Analysis using Monte Carlo simulation in Probabilistic Safety Assessment" (Durga Rao et al., 2009);
3. "Hybrid Faut Tree Analysis using Fuzzy Sets" (Lin & Wang, 1997).

Negli studi analizzati, "A new approach to solve Dynamic Fault Trees" (Amari et al., 2003) e "Dynamic Fault Tree Analysis using Monte Carlo simulation in Probabilistic Safety Assessment" (Durga Rao et al., 2009), vengono analizzati errori di sistema dipendenti dall'ordine dei guasti dei componenti e dalla loro combinazione (Dugan, Bavuso, & Boyd, 1992), vengono introdotti quindi cancelli logici dinamici(Dugan et al., 1992) (Dugan, Sullivan, & Coppit, 2000) che, diversamente da quelli impiegati in FTA tradizionale, con il loro utilizzo è possibile specificare il comportamento del sistema dipendente dalla sequenza di errore, ottenendo FT più compatti e facilmente comprensibili.

L’introduzione di gate dinamici nell’analisi FTA permette di evitare di convertire FT statici in modelli Markov, questa traduzione, risulta particolarmente complessa nel caso in cui i cancelli logici utilizzati siano troppo numerosi, l’individuazione di tali modelli inoltre non è facile per riuscire ad esprimere nel modo migliore l’albero dei guasti analizzato.
Di seguito vengono riportate le definizioni cancelli di tipo dinamico che vengono utilizzati in entrambi gli studi citati.

Tabella 2.1 – *Simboli albero dei guasti dinamico*

SIMBOLO	PORTA LOGICA	DESCRIZIONE
	**Priority-AND gate (PAND)**	Si considerano due componenti A e B, A è il componente attivo in condizioni di funzionamento normale del sistema. Il gate raggiunge lo stato di errore se tutte le componenti di input falliscono in un ordine preassegnato, da sinistra a destra.
	**Sequence-Enforcing gate (SEQ)**	Questo tipo di gate è simile al PAND, il suo stato di errore è raggiunto quando tutte le componenti di input falliscono in un ordine preassegnato (da sinistra verso destra), ma il verificarsi dell'evento è forzato in un modo particolare. Deve guastarsi per forza il primo componente e successivamente tutti gli altri per il verificarsi del guasto.
	**SPARE gate**	Questo tipo di gate viene applicato a uno o più componenti principali che possono essere sostituiti in caso di guasto dai componenti di ricambio. Il componente attivo è indicato con A e i componenti di ricambio con la lettera B. Lo stato di errore è raggiunto solamente quando il numero di pezzi di riserva disponibili è inferiore al minimo richiesto . I ricambi possono guastarsi anche quando sono inattivi , il tasso di guasto di un componente non alimentato però, è inferiore al tasso di guasto del corrispondente alimentato . Definito λcome tasso di fallimento di un componente attivo , $\alpha\lambda$ rappresenta invece il tasso di guasto di un ricambio α è il fattore di dormienza ed ha un valore compreso nell'intervallo [0,1]. I pezzi di ricambio sono chiamati "caldi" se α=1 e "freddi se α=0.
	**Functional Dependency gate (FDEP)**	L'output ottenuto è fittizio poiché non viene preso in considerazione durante il calcolo delle probabilità di errore del sistema. Il fattore di innesco T porterà al verificarsi dell'evento dipendente A o B.

Nell'articolo "Dynamic Fault Tree Analysis using Monte Carlo simulation in Probabilistic Safety Assessment" (Durga Rao et al., 2009), l'analisi di simulazione Monte Carlo ha lo scopo di simulare il funzionamento reale durante un intero ciclo di vita di vari componenti facenti parte di un sistema produttivo, a seconda degli input immessi, si otterranno poi diversi tipi di scenari incidentali.
Nel terzo articolo "Hybrid Faut Tree Analysis using Fuzzy Sets" (Lin & Wang, 1997), viene applicata la teoria degli insiemi tipo Fuzzy per l'elaborazione di un FT tipo ibrido che contiene eventi di guasti di tipo hardware con tassi di fallimento facilmente reperibili in letteratura, e guasti dovuti al fattore umano non noti e non direttamente calcolabili.

2.1.1 "A new approach to solve Dynamic Fault Trees" (Amari et al., 2003)

L'applicazione di questa metodologia per la risoluzione di FT dinamici, risulta rapida e al tempo stesso precisa, viene così utilizzata non solo in progetti orientati alla ricerca ma anche ad applicazioni commerciali, come ad esempio Relex Fault Tree.

L'albero dei guasti che viene sviluppato, è caratterizzato da moduli definiti dinamici contenenti sottosezioni o sottoalberi, con la risoluzione di questi si arriva al calcolo della probabilità di accadimento del Top Event nel sistema analizzato.

I sottoalberi individuati sono indipendenti dal sistema se essi non hanno eventi di base in comune (ci possono essere eventi ripetuti all'interno di ogni sottostruttura ma non devono essere comuni a più sottosezioni).

Le sottosezioni individuate all'interno dei sottoalberi si possono classificare in un (Gulati & Dugan, 1997) modulo dinamico che è caratterizzato dalla seguente struttura:

- Parte superiore con cancello logico dinamico PAND, SEQ e SPARE;
  - -sottoalberi all'interno del modulo indipendenti dal sistema;
  - -sottoalberi all'interno del modulo dipendenti dal sistema.
- Parte superiore con cancello logico statico AND o OR;
  - -sottoalberi dipendenti dal sistema.

La sottosezione è considerata dipendente dal sistema se almeno un evento contenuto in essa è ripetuto tra i sottoalberi del modulo e uno dei sottoalberi coinvolti è dinamico.

Nel caso in cui in un sottoalbero, la variabile casuale sia dipendente dal sistema, il metodo per trovare la distribuzione è semplice se tutti gli input di variabili casuali sono indipendenti, viceversa se l'input dato di una variabile casuale è dipendente dal sistema si possono usare probabilità condizionali così da riportare queste variabili da dipendenti a indipendenti.

In Figura 2.1.1.a è riportato un esempio di modulo dinamico composto da PAND gate superiore e sottostanti AND e OR gate.

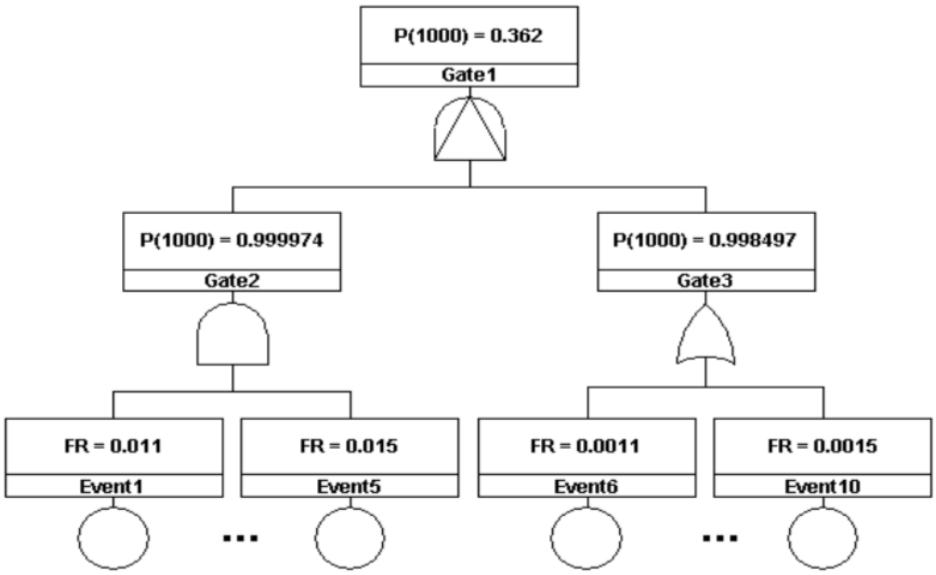


Figura 2.1.1.a – *Esempio 1 albero modulo dinamico*

L'esempio di albero (Figura 2.1.1.b) rappresenta un modulo dinamico con PAND gate superiore e due sottoalberi, uno è composto dallo schema rappresentato in Figura 2.1.1.a, l'altro è composto da SEQ gate superiore al di sotto del quale si trovano 4 gate in input di cui uno SPARE e gli altri AND o OR.

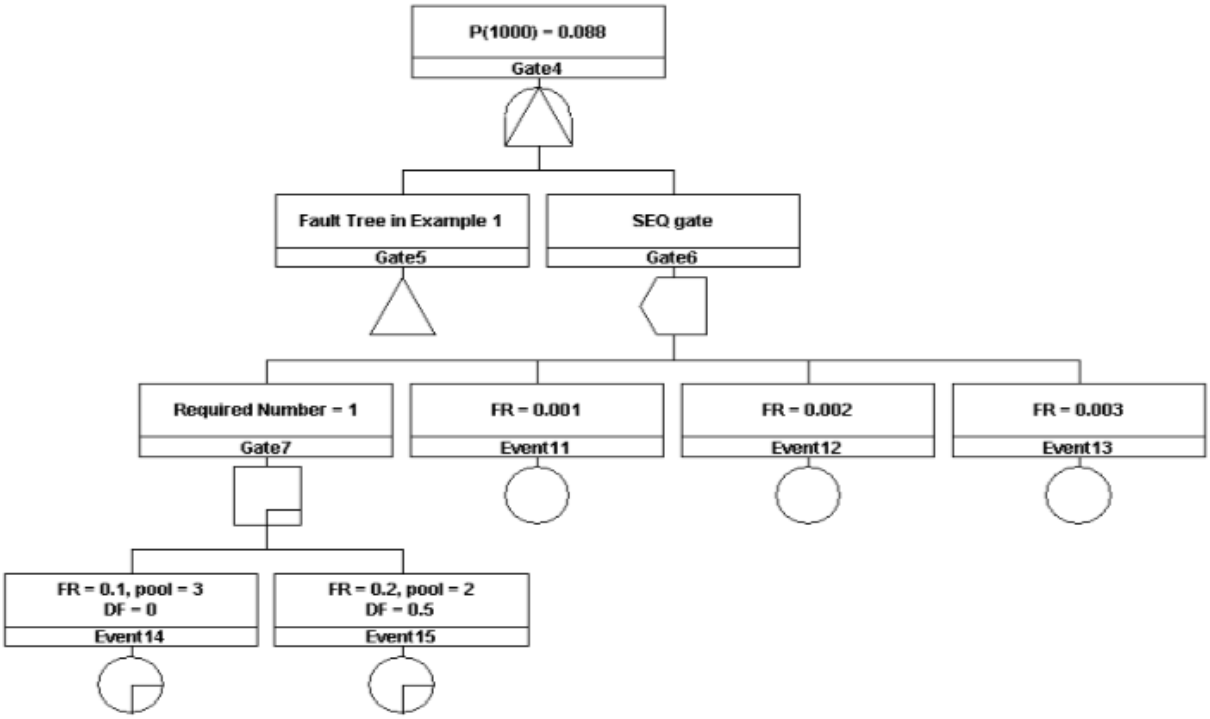


Figura 2.1.1.b – *Esempio 2 modulo dinamico*

2.1.2 "Dynamic Fault Tree Analysis using Monte Carlo simulation in Probabilistic Safety Assessment" (Durga Rao et al., 2009)

L'applicazione dell'approccio di simulazione Monte Carlo viene utilizzata per evitare i limiti introdotti dall'utilizzo di altre metodologie troppo specifiche, per la risoluzione di alberi dei guasti dinamici e quindi poco generalizzabili.

Questo metodo, grazie alla simulazione del processo reale e il comportamento casuale del sistema, può eliminare l'incertezza nella modellazione dell'affidabilità (Suresh, Babar, & Raj, 1996) (Keene, 1994).

Dalla simulazione si possono ottenere indici di affidabilità simulando il processo effettivo e il comportamento casuale del sistema, in un modello computerizzato al fine di creare uno scenario di vita realistico: il problema viene affrontato come una serie di esperimenti reali condotti in tempo simulato, la probabilità e altri indici vengono valutati contando il numero di volte in cui un evento si verifica durante la simulazione.

Alcuni parametri di input richiesti dall'analisi comprendono: funzioni di densità di probabilità per il time to failure (PDF) e riparazione di tutti i componenti base, politiche di manutenzione, intervallo e durata delle prove, manutenzione preventiva.

Porte dinamiche

L'albero dei guasti è costruito con l'utilizzo dei seguenti gate dinamici:

- Priority-AND gate (PAND);
- Sequence-Enforcing gate (SEQ);
- SPARE gate;
- FDEP gate.

PAND gate

Al raggiungimento dello stato di errore segue il processo di riparazione il cui tempo dipende dal PDF del tempo di riparazione.

Questo ciclo è continuato fino a quando viene raggiunto il tempo di missione predeterminato del sistema. Per il secondo componente attivo vengono sviluppato diagrammi analoghi.

Per generare il diagramma temporale dello stato del gate PAND, vengono confrontati entrambi i profili temporali dei componenti, lo stato di insuccesso è raggiunto dal gate se tutti i suoi componenti di input hanno fallito in un ordine preassegnato (solitamente da sinistra verso destra).

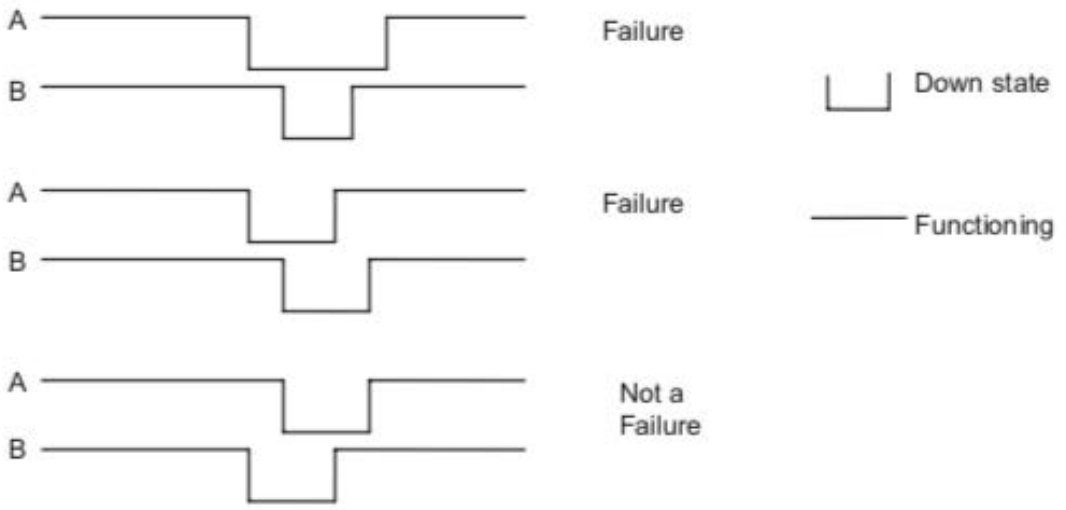


Figura 2.1.2.a – *Diversi stati nel tempo di PAND gate*

Nelle prime due situazioni rappresentate in Figura 2.1.2.a, quando entrambi i componenti A e B falliscono si raggiunge lo stato di guasto del sistema e viene preso in considerazione il tempo di fermo simultaneo.
Nella terza situazione viene mostrato che ancora una volta entrambi i componenti falliscono, B però fallisce per primo e così il sistema non si considera guasto.

SPARE gate

Per i componenti attivi, i tempi di guasto e di riparazione in base ai rispettivi PDF, vengono generati alternativamente fino al momento del tempo termine di missione.
Le componenti di ricambio quando non sono richieste, potrebbero essere indisponibili nel caso in cui: siano in attesa, si trovino fuori uso per un guasto, siano sottoposte a test o manutenzione pianificata.
Occorre modellare uno scenario che preveda tutte le possibili alternative dello stato in cui può trovarsi il componente di ricambio rappresentativo del suo stato reale.
Il motivo di mancato intervento rimane sconosciuto fino a quando il sistema per necessità, deve ricorrere ai componenti di ricambio in sostituzione del componente attivo, il tempo di fallimento in questo caso è assunto pari a tempo morto ed è ottenuto sommando il tempo di attesa al mancato funzionamento del PDF e il tempo di riparazione del PDF.
È necessario verificare inoltre che, il componente in stand-by sia in grado di soddisfare la propria missione, tale funzione viene incorporata ottenendo il tempo di errore in base al PDF di guasto operativo e viene verificato con il tempo di missione, ovvero il tempo di inattività del componente attivo. Se il primo componente in stand-by non riesce ad intervenire per il ripristino del componente attivo, la domanda verrà trasferita al componente di riserva successivo.

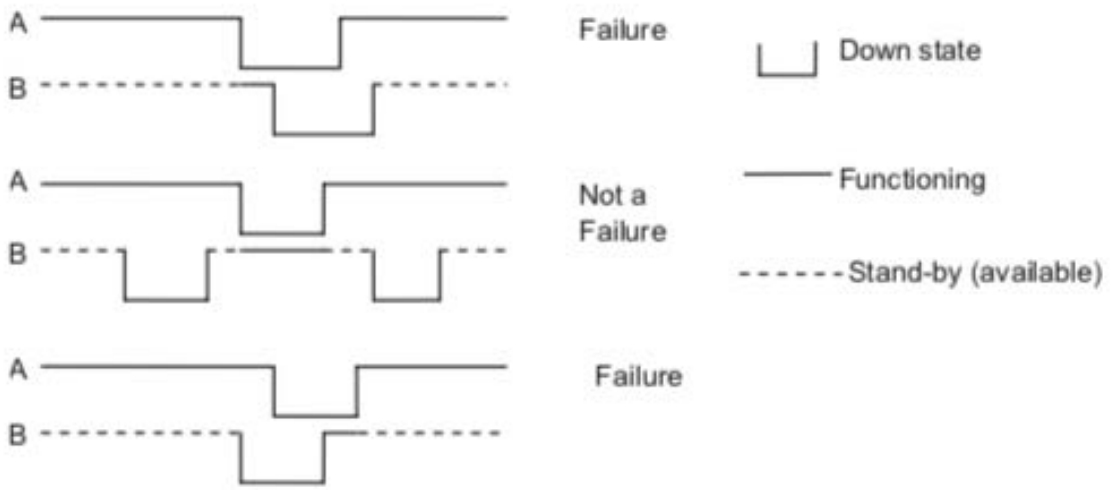


Figura 2.1.2.b – *Diversi stati nel tempo di SPARE gate*

Nella Figura 2.1.2.b il primo caso riporta la situazione in cui la domanda che segue al guasto del componente attivo è soddisfatta dal componente di ricambio, esso però fallisce prima del ripristino del componente attivo.
Nel secondo caso invece, la domanda viene soddisfatta dal componente di ricambio che fallisce due volte quando si trova in modalità dormiente, in conclusione però, tale situazione non comporta nessun effetto sul sistema.
Nell'ultimo caso, il componente in stand-by, essendo fuori uso, non può soddisfare la domanda nel momento in cui essa arriva, in seguito col suo recupero si riduce il tempo di inattività complessiva.

FDEP gate

In Figura 2.1.2.c il primo caso rappresenta, a seconda del PDF dell'evento iniziatore T, la generazione del tempo di errore e di riparazione. Durante il tempo di inattività dell'evento T di attivazione, gli elementi dipendenti si troveranno virtualmente in stato di errore sebbene essi funzionino.
Nel secondo scenario, le singole occorrenze degli eventi dipendenti, non influenzano l'evento di innesco T.

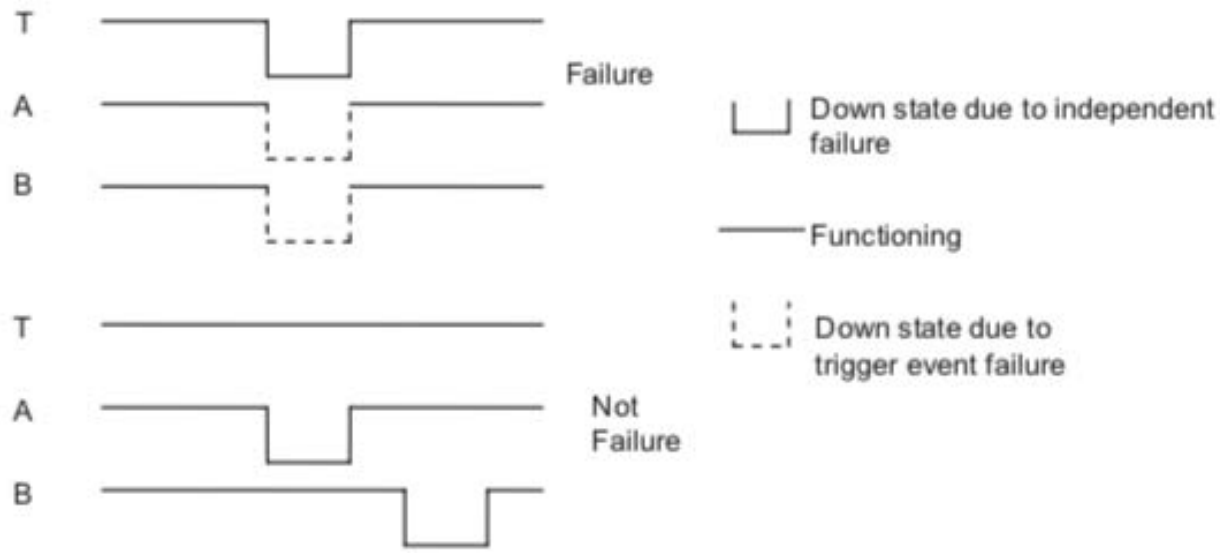
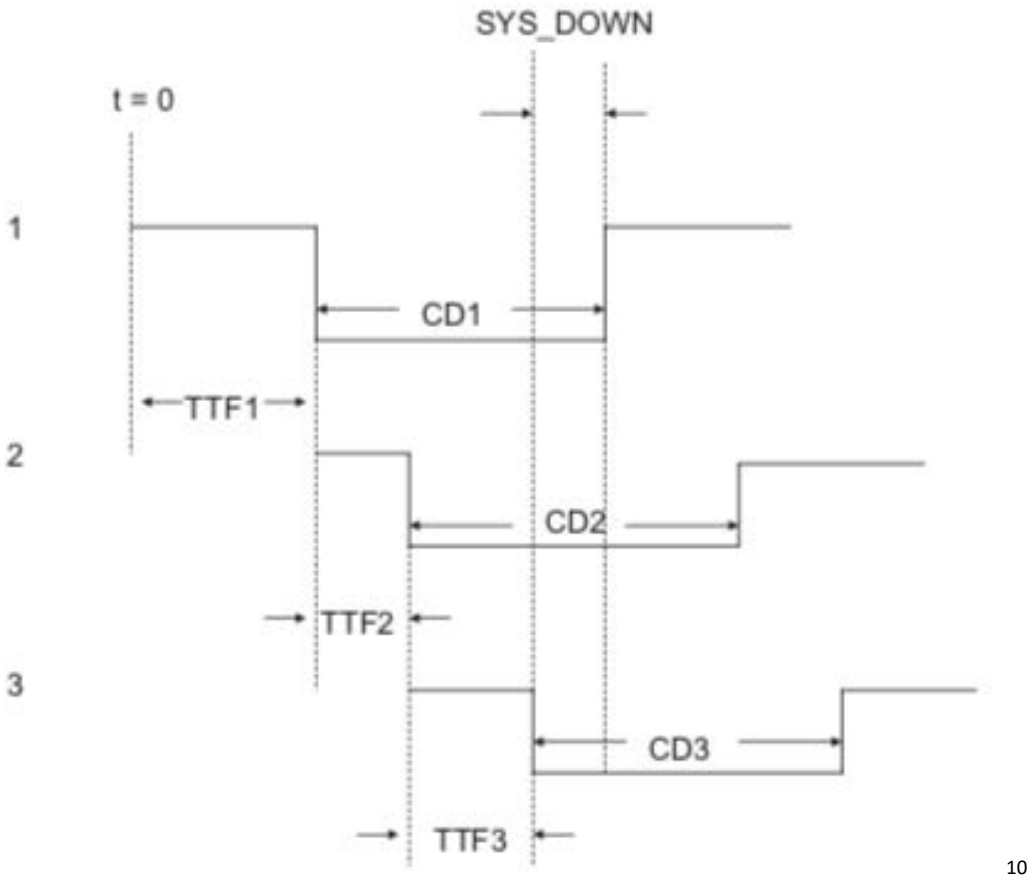


Figura 2.1.2.c – *Diversi stati nel tempo di FDEP gate*

SEQ gate

Considerando SEQ gate avente tre ingressi con componenti riparabili, applicando l'utilizzo dell'approccio Monte Carlo:

1. Il profilo temporale che definisce lo stato del componente, viene generato in base al suo guasto e alla velocità di riparazione. Il tempo della sua inattività è il tempo di missione per il secondo dispositivo. Allo stesso modo, il tempo di fermo del secondo componente è il tempo di missione per il terzo.
2. Nel caso in cui il primo componente si guasti, si passa all'avviamento del secondo. Questa situazione rappresenta t=0 per il secondo componente. Il time to failure TTF2 e il tempo di riparazione CD2 sono generati per il secondo componente.
3. In caso di guasto del secondo componente, si avvia il funzionamento del terzo. Il momento in cui si ha stato di guasto del secondo componente, la situazione rappresenta t=0 per il terzo. Il tempo di guasto TTF3 e il tempo di riparazione CD3 vengono generati per il terzo componente.
4. Il tempo in cui tutti i componenti sono in stand-by è considerato il tempo di inattività della porta SEQ;
5. Il processo è ripetuto per tutti gli stati di non funzionamento del primo componente.



[10]

Figura 2.1.2.d – *Diversi stati nel tempo di SEQ gate.*

[10] TTFi - time to failure dell'i-esimo componente;

CDi – tempo di fermo del componente i-esimo;

SYS_DOWN – tempo di fermo dell'intero sistema.

2.1.3 "Hybrid Faut Tree Analysis using Fuzzy Sets" (Lin & Wang, 1997)

Nei sistemi altamente automatizzati, la presenza dell'uomo è ancora molto rilevante (Mital, Motorwala, Kulkarni, Sinclair, & Siemieniuch, 1994): è evidente così che i metodi FTA convenzionali che considerano solo il tasso di guasto dell'hardware sono impraticabili nelle situazioni reali.

Il fattore umano è responsabile del 20%-90% dei guasti al sistema, la sua presenza va ad unirsi a quella conosciuta (attraverso dati tabulati) negli studi di FTA per la ricerca degli eventi primari che possono portare al verificarsi del Top Event.

In questo articolo è stato proposto un approccio ibrido all'analisi dell'albero dei guasti basato sulla teoria degli insiemi fuzzy.

Questa teoria è adatta a situazioni in cui sono presenti e necessarie sia valutazioni di tipo probabilistico sia di tipo linguistico (Liang & Wang, 1933) (Keller & Kara-Zaitri, 1989) (Page & Perry, 1994). Invece di stimare direttamente la probabilità di fallimento, il tasso di errore fuzzy viene utilizzato per caratterizzare il verificarsi di guasti di sistema che coinvolgono informazioni imprecise come ad esempio gli errori umani.

Si semplifica così il modo in cui gli ingegneri della sicurezza (Walker & Cavallaro, 1996) (Liang & Wang, 1933) (Preyssl, 1995) (Cai, 1996) (Wang, Yang, & Sen, 1995) (Suresh et al., 1996) (Keene, 1994) possono valutare in modo semplice ed efficace il tasso di insuccesso del Top Event efficacemente in un ambiente non definito, adottando sia modelli linguistici sia probabilistici senza restrizioni.

Numeri di Fuzzy

I numeri di fuzzy sono usati per gestire dati imprecisi come quelli rappresentati dai valori linguistici ("vicino a 5", "alta affidabilità"), e si dividono in numeri di tipo triangolari e trapezoidali.

Questi due tipi di numeri sono usati perché, se considerate alcune ipotesi, queste funzioni di appartenenza specifiche soddisfano immediatamente i criteri di ottimizzazione rilevanti (Wang et al., 1995) (Pedryez, 1994) e sono intuitivamente facili da valutare.

Variabili linguistiche

Una variabile linguistica utilizza valori come parole o frasi per rendere più chiaro il concetto che si vuole esprimere, per trattare situazioni che sono troppo complesse o mal definite e tradurle in espressioni quantitative convenzionali, un valore linguistico può essere rappresentato da un numero fuzzy.

Vengono riportati in Figura 2.1.3 i seguenti valori per le espressioni linguistiche: Molto Basso (Very low), Basso (Low), Abbastanza Basso (Fairly low), Medio (Medium), Abbastanza Alto (Fairly high), Alto (High), Molto Alto (Very height).

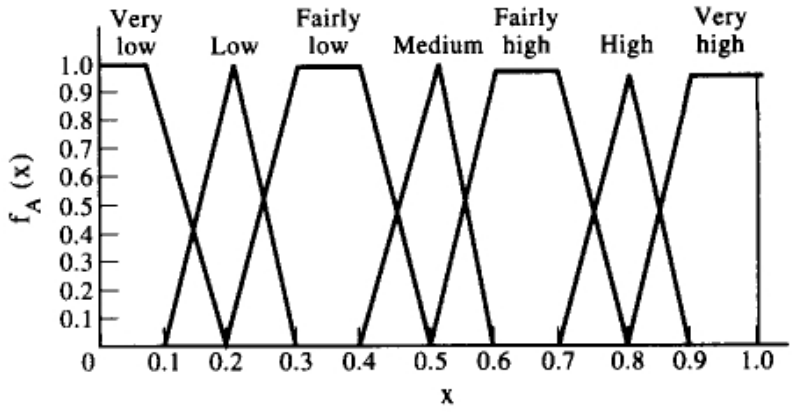


Figura 2.1.3 - *Variabili linguistiche rappresentate da numeri fuzzy*

2.1.3.1 Fasi applicative del metodo ibrido

1. Individuazione Top Event e costruzione FTA;
2. Divisione degli elementi dell'albero dei guasti in analisi di probabilità oggettiva e di valutazione linguistica soggettiva delle prestazioni umane ed eventi poco noti;
3. Selezione delle probabilità di guasto per la stima dei tassi di errore hardware, da letteratura o banche dati;
4. Valutazioni linguistiche per prestazioni umane ed eventi poco noti;
5. Trasformazione delle espressioni linguistiche in numeri fuzzy e aggregazione delle opinioni degli analisti coinvolti nell'analisi, in un unico numero fuzzy;
6. Conversione dei numeri fuzzy in punteggi di probabilità fuzzy FPS;
7. Trasformazione dell'FPS in tasso di fallimento fuzzy FRR;
8. Sintetizzazione del tasso di fallimento dell'evento principale aggregando i tassi di fallimento umano e degli hardware;
9. Analisi dei risultati, studio e adozione di contromisure.

Aggregazione di numeri fuzzy

Al fine di ottenere un unico numero fuzzy, vengono aggregati i singoli risultati ottenuti dal processo di analisi.

Per l'aggregazione esistono vari metodi: media, massimo, minimo e operatori misti.

Solitamente il metodo più utilizzato è quello della media.

Convertire il numero fuzzy in punteggio fuzzy

Con il passaggio da numero fuzzy a punteggio di probabilità FPS è possibile ottenere un punteggio chiaro, FPS rappresenta la probabilità maggiore che un evento possa verificarsi.

La conversione del punteggio finale fuzzy FPS avviene attraverso l'applicazione del metodo di classificazione fuzzy sinistro e destro di Chen e Hwang (1992) (Chen & Hwang, 1992)[17].

Ottenimento del tasso di fallimento fuzzy FRR da punteggio di probabilità FPS

Per garantire la confrontabilità tra il tra il tasso di fallimento di componenti del sistema e il punteggio di probabilità fuzzy FPS, è possibile ottenere il tasso di fallimento fuzzy come:

$$FFR = \frac{frequenza\ di\ un\ errore}{probabilità\ totale\ che\ un\ evento\ abbia\ un\ errore} \qquad (2.1.3.1)$$

2.1.3.2 Esempio di applicazione FTA con metodo ibrido

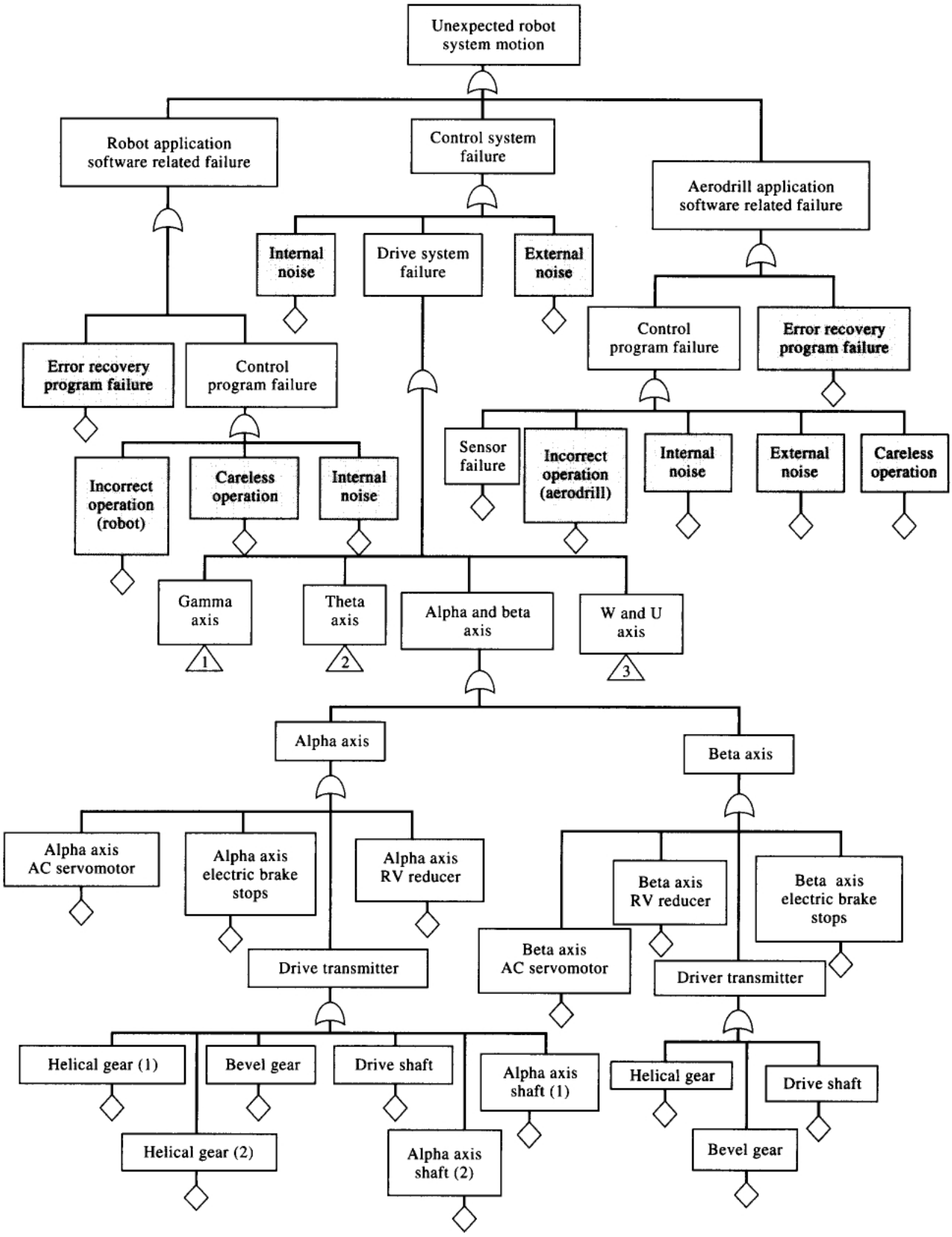


Figura 2.1.3.2 – *Esempio di rappresentazione grafica dell'applicazione del metodo ibrido*

La costruzione di questo albero (Figura 2.1.3.2) riguarda l'analisi di un sistema automatizzato che ha come compito quello di eseguire alcune perforazioni su ali di aeromobili (progetto sviluppato a Tawain da Aerospace Industrial Development Corporation, AIDC).
Secondo i registri di manutenzione, le problematiche più comune di questo sistema sono causati da movimenti imprevisti del robot che esegue le operazioni di perforazione: movimenti fuori sincronia e irregolari, arresto improvviso e movimenti improvvisi.
Il Top Event utilizzato riguarda il movimento inaspettato del robot: nelle due sezioni di FT, una riguarda l'analisi probabilistica oggettiva dei guasti hardware e l'altra la valutazione linguistica fuzzy per le prestazioni umane e degli eventi poco chiari.
Per eventi poco chiari si intendono: funzionamento incauto ed errato, cause interne, cause esterne.
Gli eventi di valutazione linguistica fuzzy sono rappresentati nei blocchi in grassetto.

Capitolo 3
Albero dei guasti dinamico: caso semplificato

Il capitolo introduce l'applicazione dell'analisi FT dal punto di vista dinamico utilizzando per il calcolo dei tassi di guasto la distribuzione di Weibull a due parametri, facendo quindi riferimento ai tratti di Bathtube curve inziale e finale.

3.1 Il tratto iniziale e finale della Bathtube curve

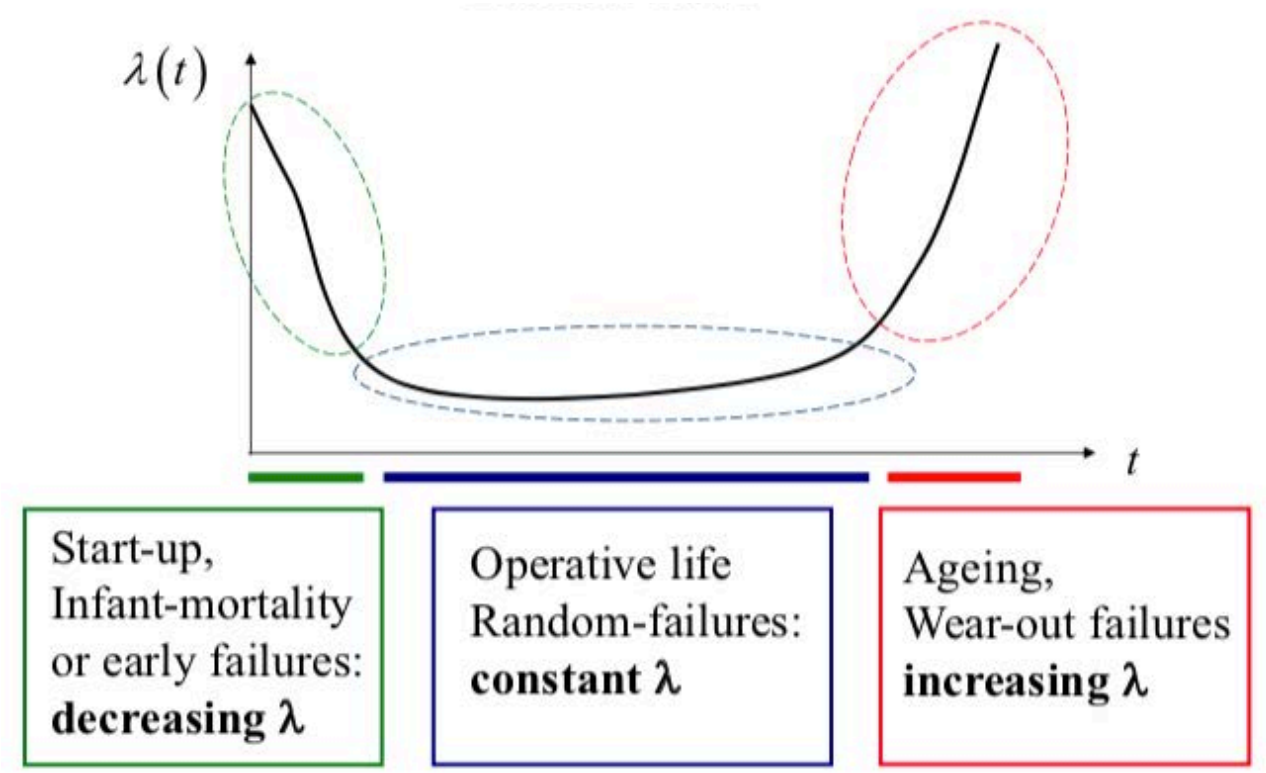


Figura 3.1 – *Bathtube curve (Leonardo Bertini, n.d.)*

Per l'analisi FTA di tipo dinamico ci si concentra sui tratti iniziale e finale della Bathtube curve poiché la frequenza in queste zone è variabile in funzione del tempo. Quindi viene tralasciato il tratto centrale in cui il tasso di guasto essendo medio e costante e risulta facilmente reperibile dalla letteratura.

Nel periodo iniziale e finale della curva è possibile calcolare il tasso di guasto *h(t)* attraverso l'applicazione della distribuzione di Weibull:

$$h(t) = \alpha\beta t^{\beta-1} e^{(-\alpha t^{\beta})} \qquad (3.1)$$

Nell'equazione:

$$\alpha = fattore\ di\ scala$$

Il fattore di scala è un coefficiente che viene utilizzato in riferimento alla vita caratteristica del componente ed è riportato secondo dati di funzionamento tabellati.
Il valore è un dato quantitativo espresso ad esempio sotto forma di numero di cicli di lavoro, distanze o tempo.

$$\beta = fattore\ di\ forma$$

Il valore del fattore di forma (numero puro) è scelto in base al periodo di vita a cui fa riferimento l'analisi FT, generalmente è compreso tra 0,5 e 5(Ierace, n.d.).

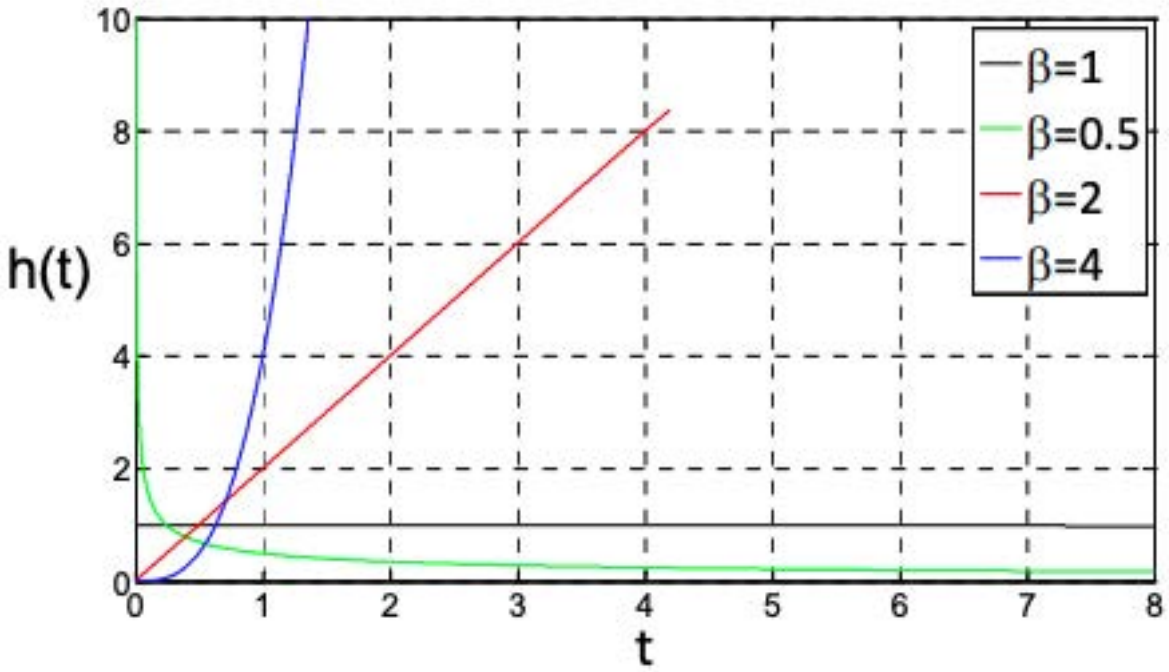


Figura 3.1.a – *Variazione della forma della funzione tasso di guasto h(t) al variare di β, ($\alpha = 1$ s cost) (Distribuzione Weibull, n.d.)*

- Quando $\beta < 1$ (paragrafo 1.4.2), la curva ha andamento monotono decrescente, essa descrive il periodo della vita del componente in cui si ha mortalità infantile (fase di rodaggio).
  Gli errori che si manifestano in questa fase, avvengono principalmente per carenze o sviste avvenute in fase di progettazione e fabbricazione, le azioni conseguenti intraprese, una volta manifestatisi tali errori, sono la loro correzione in vista del funzionamento ottimale previsto nel periodo di vita utile del componente (tratto ad andamento costante della curva).
  Gli errori che avverranno nella seconda fase saranno dovuti a casualità (rotture istantanee, aumento della probabilità di guasto a seguito del guasto di altri componenti, combinazione di più cause).

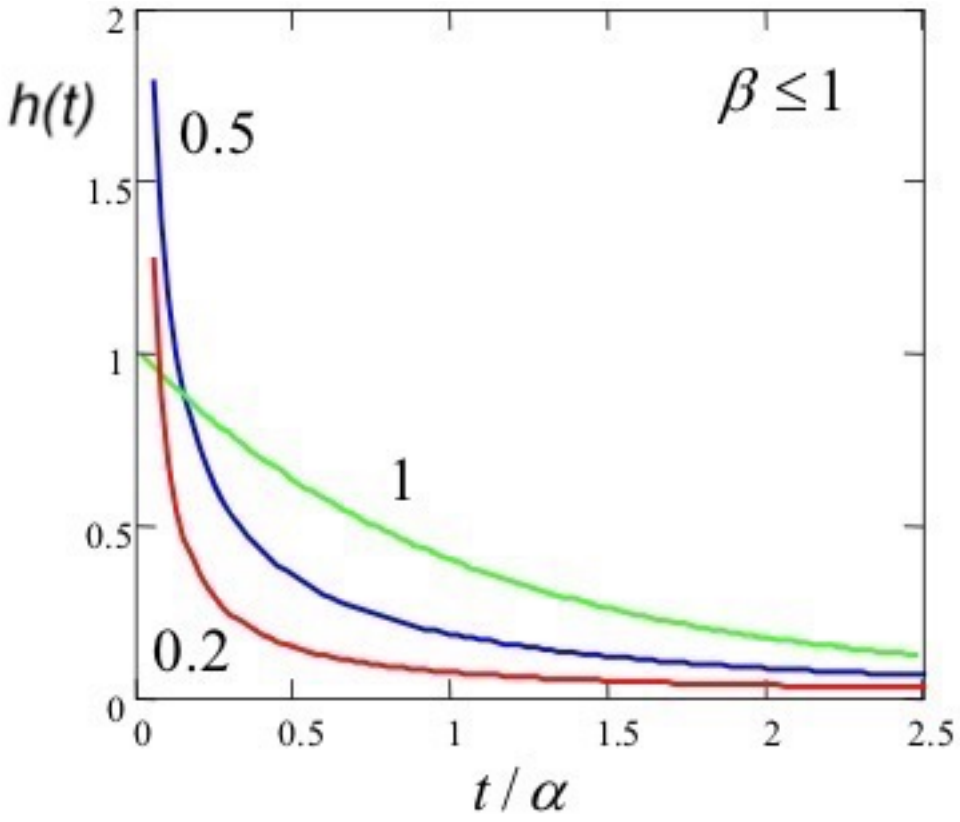


Figura 3.1.b - *Bathtube curve per β<1 (Leonardo Bertini, n.d.)*

- Quando $\beta > 1$ (paragrafo 1.4.2), la parte di curva descritta è quella finale in cui il componente oggetto d'esame è ormai alla fine del suo utilizzo.
  La curva assume andamento crescente e poi decrescente, indicazione del fatto che il tasso di guasto è in aumento per l'usura del componente fino alla sua completa dismissione e sostituzione.

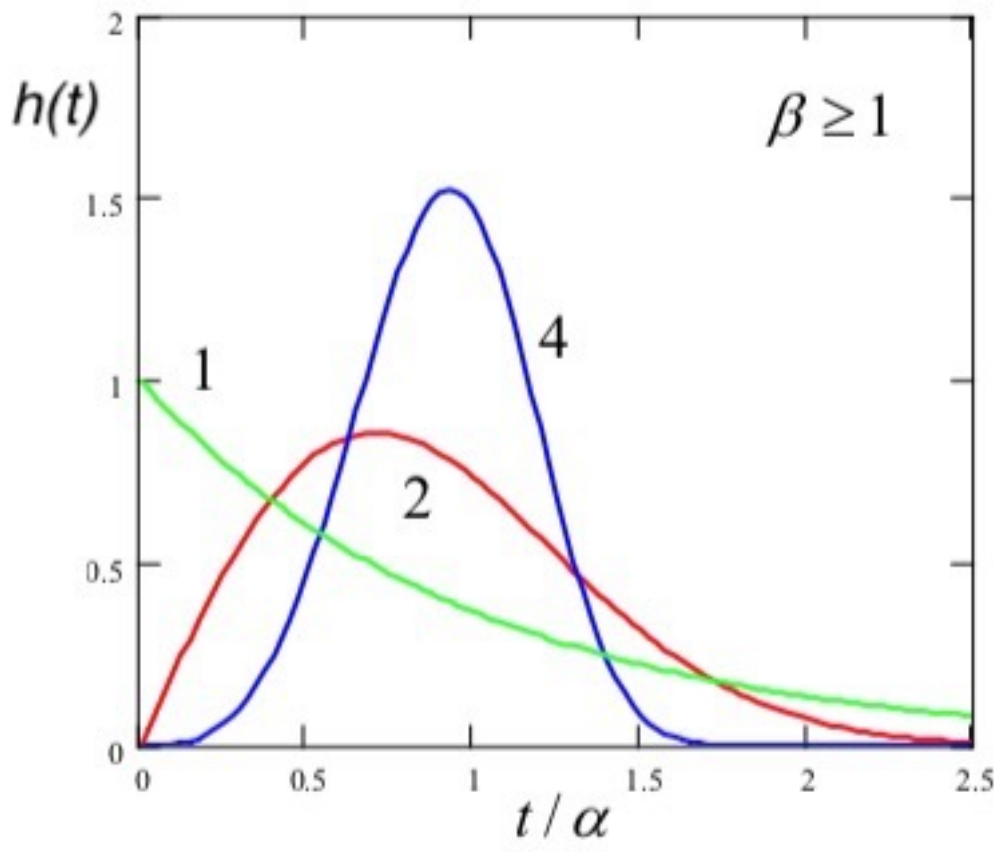


Figura 3.1.c – *Bathtube curve per β>1 (Leonardo Bertini, n.d.)*

3.2 Il tasso di guasto tempo dipendente

Per il calcolo del tasso di guasto tempo dipendente, come descritto nel paragrafo precedente, si applica la distribuzione di Weibull (3.1) e, a seconda del tratto considerato, si inseriscono al suo interno gli opportuni parametri α e β.
Per il calcolo dei fattori α e β si utilizza la metodologia trattata all'interno del manuale "Oreda" (SINTEF, 2002), il tasso di guasto riportato nelle tabelle è ottenuto tramite il calcolo dei fattori con l'applicazione della Distribuzione Gamma.
All'interno del manuale i paramentri ricercati, si ottengono applicando il seguente procedimento:

$$\beta = \frac{\theta^*}{\sigma^2} \tag{3.2}$$

$$\alpha = \beta * \theta^* \tag{3.2.1}$$

$\theta^* =$ rappresenta la media dei valori tra il minimo e il massimo del tasso di guasto, il calcolo è effettuato per l'intervallo di tempo tra l'inizio e la fine della sorveglianza dei dati per un particolare componente;
$\sigma =$ SD, rappresenta la deviazione standard.

Attraverso l'elaborazione dei dati con il supporto di un foglio di calcolo Excel, una volta ottenuti i due parametri di interesse, si procede alla determinazione del tasso di fallimento *h(t)*.
Successivamente si utilizza il valore del tasso di fallimento ottenuto, per ricavare la frequenza di guasto (densità di guasto):

$$f(t) = \beta\, h(t)\, (h(t)\, t)^{\beta-1} e^{-(h(t)\, t)^{\beta}} \tag{3.2.2}$$

Altre informazioni utili per la costruzione dell'albero dei guasti che si possono ricavare sono:

- Probabilità di guasto:

$$P(t) = 1 - e^{-\alpha t^{\beta}} \tag{3.2.3}$$

- Affidabilità:

$$R(t) = e^{-\alpha t^{\beta}} \text{ (3.2.4)} \tag{3.2.4}$$

3.3 Esempio applicativo

L'applicazione della metodologia, per l'analisi dell'albero dei guasti con approccio di tipo dinamico, comincia selezionando un caso semplificato rispetto a quello che sarà trattato nel prossimo capitolo. Viene quindi preso come esempio dello studio della distribuzione di Weibull, un MCS individuato nel corso dell'esercitazione svolta durante il corso di Analisi del Rischio a.a. 2017-2018.
L'esercitazione riguarda l'analisi di sicurezza svolta su di un impianto chimico per la produzione di dimetiletere (DME) ed il Top Event individuato è un qualsiasi rilascio dovuto a guasti che coinvolgeva i vari componenti che formavano il sistema.

3.3.1 MCS: guasto pic

Succesivamente alla costruzione dell'albero dei guasti, in esso vengono individuati i MCS e vengono analizzati nello specifico con lo scopo di ottenere le sequenze di guasti che possono portare all'evento finale, individuando gli eventi di base.
Partendo dal MCS precedentemente individuato, ovvero quello che coinvolge il guasto del controllo di un indicatore di pressione (PIC), si determinano i valori di interesse per l'analisi.

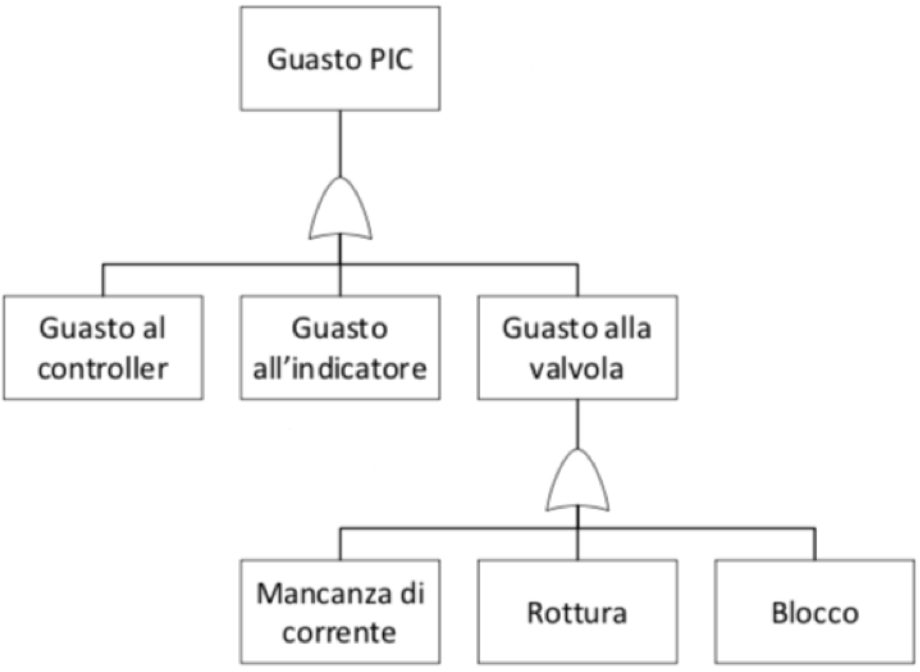


Figura 3.2 - *MCS guasto pic*[11]

[11] Esempio albero dei guasti presente all'interno dell'esercitazione del corso di Analisi del Rischio a.a. 2017-2018

3.3.2 Risultati

Attraverso l'ausilio del foglio di calcolo Excel è possibile ottenere i risultati ricercati: si procede con l'inserimento all'interno delle celle del foglio delle formule necessarie all'analisi, andando a riempire una tabella (Tabelle 3.3.2-a-b-c-d) che mostra anno per anno i risultati ottenuti.

È possibile poi riportare i dati in forma grafica, ottenendo un grafico in cui sull'asse delle ordinate si trova il tasso di guasto e sull'asse delle ascisse gli anni in cui l'analisi è svolta.

Nelle tabelle sotto riportate (Tabelle 3.3.2-a-b-c-d), vengono riportati i risultati dei parametri ricercati.

Il calcolo di frequenza, probabilità ed affidabilità è effettuato seguendo l'ordine di guasto e applicando le regole dell'algebra booleana, in riferimento al MCS in Figura 3.2.

Essendo l'operatore logico inserito all'interno del MCS del tipo "OR", per il calcolo del Top Event viene eseguita l'operazione di produttoria delle diverse probabilità di guasto ottenute.

Il tempo di riferimento assunto per il calcolo dei paramentri di interesse, a partire dall'applicazione della distribuzione di Weibull è di 5 anni[12].

[12] Tempo di calcolo assunto arbitrariamente ai fini dell'applicazione.

Tabella 3.3.2 – *Dati riferiti a 1 anno di funzionamento del componente*

1 anno	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	2,52832E-05	-2,89E-07	0,320059396	0,679940604
rottura	2,63646E-05	-3,05635E-07	0,31787158	0,68212842
blocco	2,52832E-05	-2,89054E-07	0,320059396	0,679940604
guasto alla valvola			0,967437866	0,032562134
guasto controller	2,52832E-05	-2,89054E-07	0,320059396	0,679940604
guasto indicatore	2,63646E-05	-3,05635E-07	0,31787158	0,68212842
GUASTO PIC			0,901575014	0,098424986

Tabella 3.3.2.a – *Dati riferiti a 2 anni di funzionamento del componente*

2 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	1,34647E-05	-1,47716E-07	0,297177435	0,702822565
rottura	1,40599E-05	-1,56057E-07	0,294521293	0,705478707
blocco	1,34647E-05	-1,47716E-07	0,297177435	0,702822565
guasto alla valvola			0,973989521	0,026010479
guasto controller	1,34647E-05	-1,47716E-07	0,297177435	0,702822565
guasto indicatore	1,40599E-05	-1,56057E-07	0,294521293	0,705478707
GUASTO PIC			0,914751487	0,085248513

Tabella 3.3.2.b – *Dati riferiti a 3 anni di funzionamento del componente*

3 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	9,31387E-06	-9,96519E-08	0,283927605	0,716072395
rottura	9,73335E-06	-1,05216E-07	0,281009255	0,718990745
blocco	9,31387E-06	-9,96519E-08	0,283927605	0,716072395
guasto alla valvola			0,977346471	0,022653529
guasto controller	9,31387E-06	-9,96519E-08	0,283927605	0,716072395
guasto indicatore	9,73335E-06	-1,05216E-07	0,281009255	0,718990745
GUASTO PIC			0,922021156	0,077978844

Tabella 3.3.2.c – *Dati riferiti a 4 anni di funzionamento del componente*

4 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	7,17069E-06	-7,53376E-08	0,274601911	0,725398089
rottura	7,49791E-06	-7,95065E-08	0,271503795	0,728496205
blocco	7,17069E-06	-7,53376E-08	0,274601911	0,725398089
guasto alla valvola			0,979526928	0,020473072
guasto controller	7,17069E-06	-2,89054E-07	0,320059396	0,679940604
guasto indicatore	2,63646E-05	-7,53376E-08	0,274601911	0,725398089
GUASTO PIC			0,913910435	0,086089565

Tabella 3.3.2.d – *Dati riferiti a 5 anni di funzionamento del componente*

5 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	5,85424E-06	-6,06287E-08	0,267416933	0,732583067
rottura	6,12408E-06	-6,39583E-08	0,264183348	0,735816652
blocco	5,85424E-06	-6,06287E-08	0,267416933	0,732583067
guasto alla valvola			0,981107769	0,018892231
guasto controller	5,85424E-06	-6,06287E-08	0,267416933	0,732583067
guasto indicatore	6,12408E-06	-6,39583E-08	0,264183348	0,735816652
GUASTO PIC			1	0

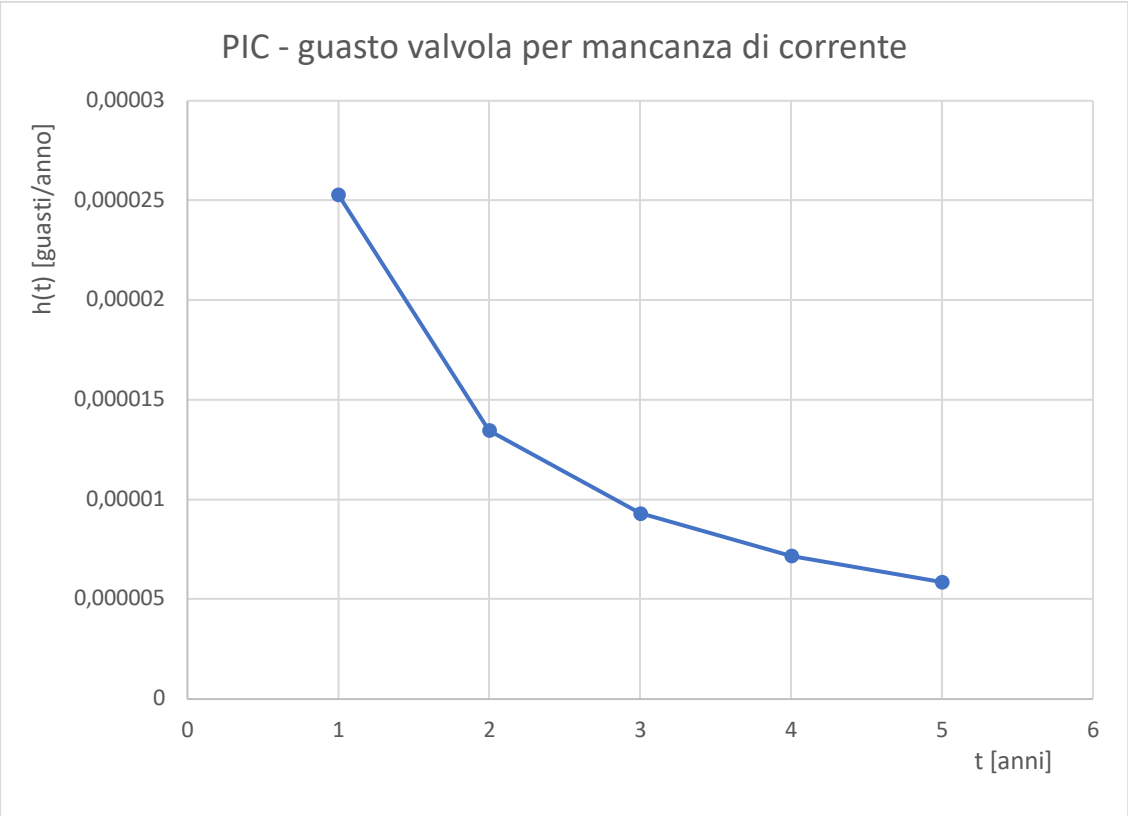


Figura 3.3.2 – *Grafico h(t)-t guasto valvola per mancanza di corrente*

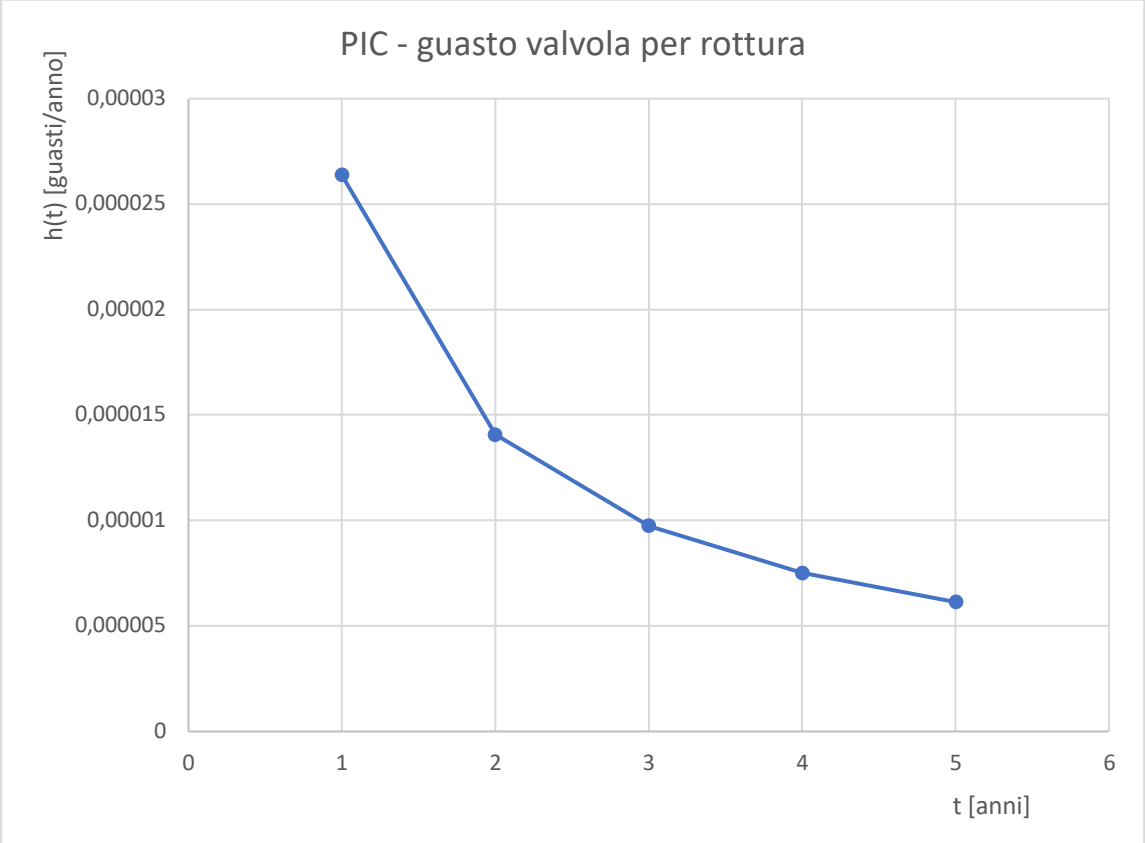


Figura 3.3.2.a – *Grafico h(t)-t guasto valvola per rottura*

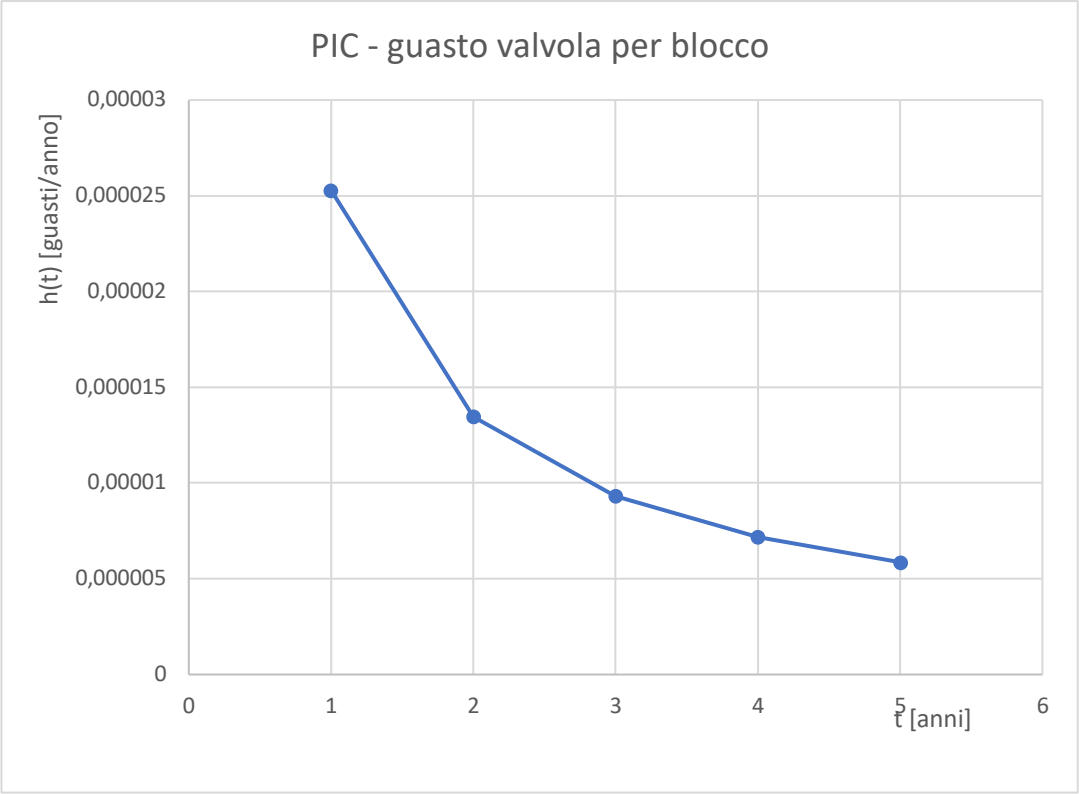


Figura 3.3.2.b – *Grafico h(t)-t guasto valvola per blocco*

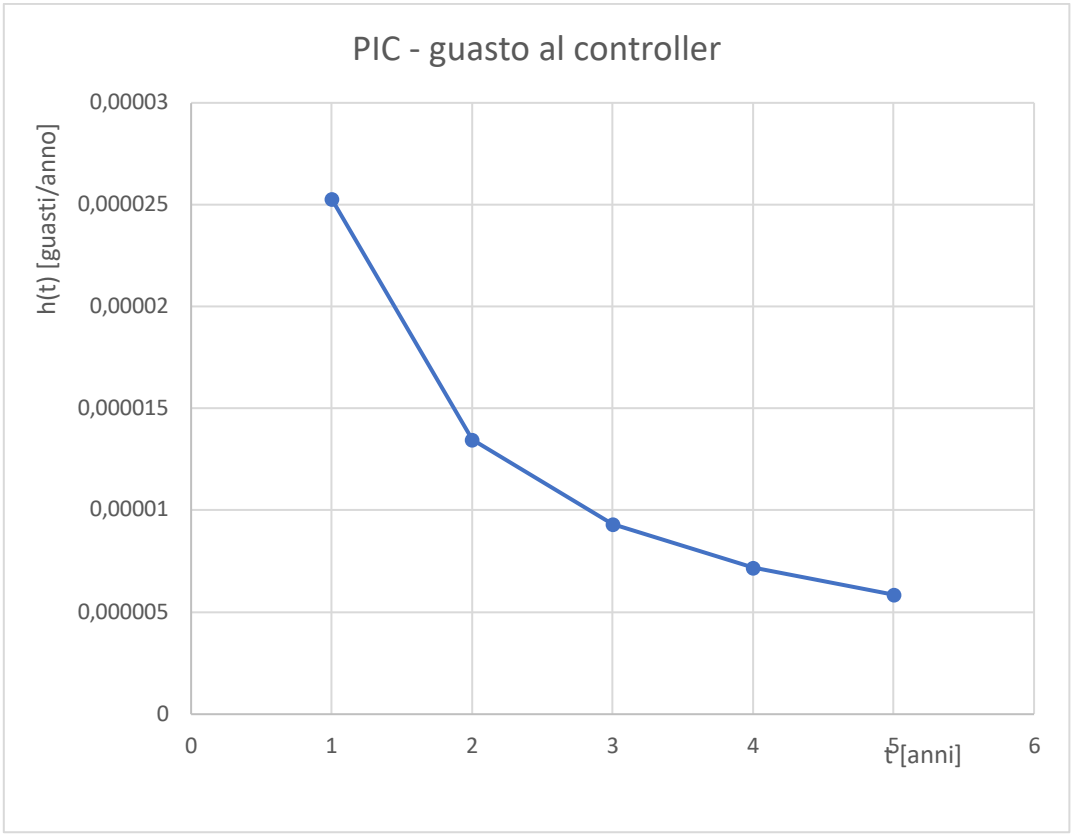


Figura 3.3.2.c – *Grafico h(t)-t guasto PIC per guasto al controller*

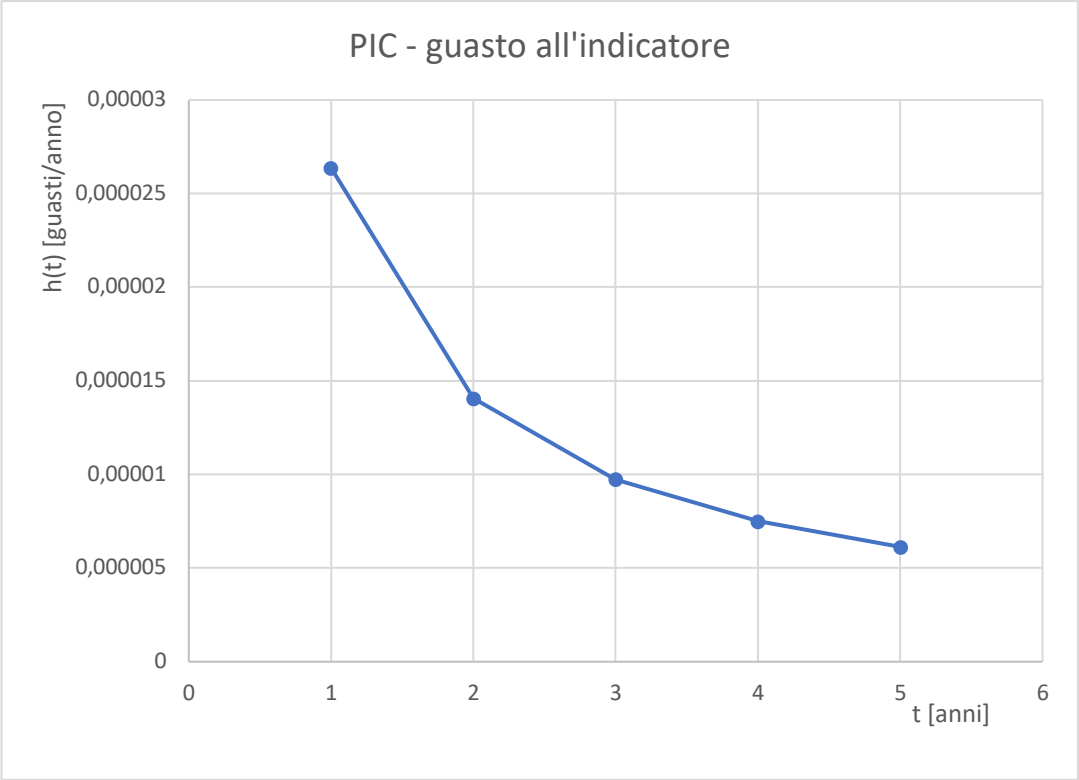


Figura 3.3.2.d – *Grafico h(t)-t guasto PIC per guasto all'indicatore*

Dalle figure sopra riportate (Figure 3.3.2-a-b-c-d) che riguardano l'andamento dei tassi di guasto dei vari componenti che formano il PIC, si nota come il tasso di guasto diminuisce con l'aumentare degli anni in cui il dispositivo opera, questo andamento è quindi coerente con il periodo di vita considerato del PIC, la fase iniziale della Bathtube curve nel periodo di mortalità infantile.

In riferimento alle Tabelle 3.3.2-a-b-c-d, si ricava come la probabilità di accadimento finale dell'evento individuato, nel caso dell'esempio riportato considera il guasto del PIC, aumenta di anno in anno fino al suo verificarsi, ovvero quando P(t)=1.

3.3.3 Introduzione piani di manutenzione

A partire dal risultato indicato nel precedente paragrafo, a seguito del verificarsi dell'evento incidentale, guasto PIC, l'analisi procede introducendo nello studio l'intervento di un piano di manutenzione che prevede la riparazione/sostituzione del componente.

Il manuale Oreda (SINTEF, 2002), fornisce dati riguardo il tempo di riparazione in ore lavorative dei componenti di interesse.

Nel MCS oggetto di analisi (Figura 3.2), la catena di guasti è collegata tramite l'utilizzo di porte logiche "OR", si prendono in considerazione quindi, in fase di preparazione alla reale applicazione per la costruzione FTA dinamica trattata nel prossimo capitolo, solo alcuni dei guasti possibili inseriti nel MCS.

3.3.3.1 Analisi guasto PIC per mancanza di corrente

Viene scelto di applicare il guasto del PIC al caso in cui venisse a mancare la corrente.

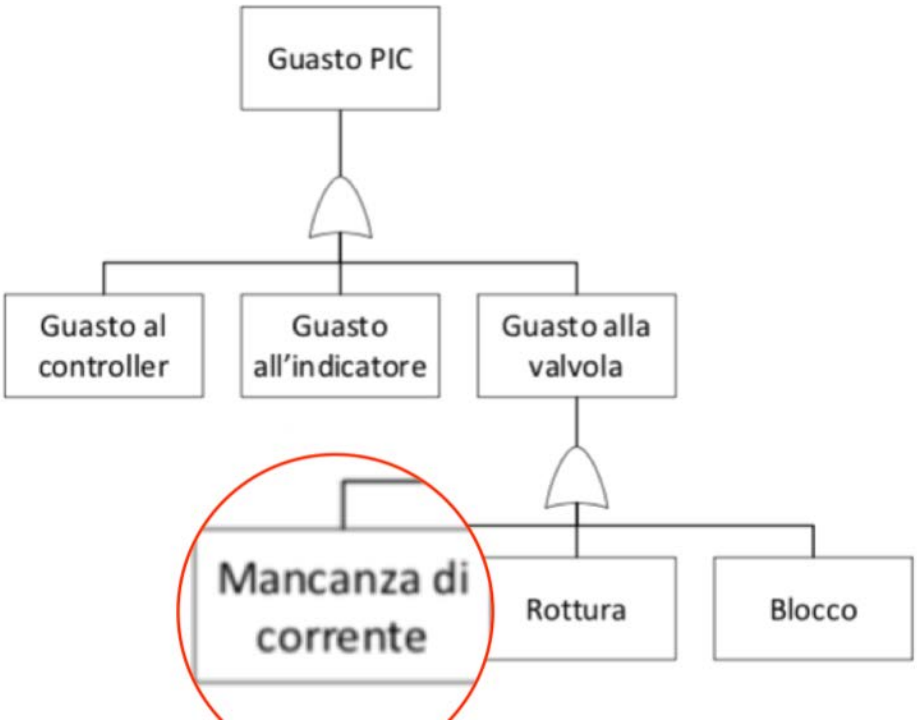


Figura 3.3.3.1 – *MCS guasto pic con evento incidentale in evidenza*

Secondo il manuale Oreda (SINTEF, 2002), il tempo di riparazione per un guasto di questo tipo, corrisponde a 5,3 ore lavorative, approssimate a 6 ore[13] per comodità nell'eseguire i calcoli.

[13] 6 ore= 0.0006849315068493151 anni

Successivamente al periodo di manutenzione, si riprende l'analisi nella ricerca dei parametri di interesse e si esegue infine il confronto con i dati ottenuti prima del guasto a 1 ora dalla riparazione e ripresa del sistema, ipotizzando che la ripresa sia immediatamente successiva alla riparazione.

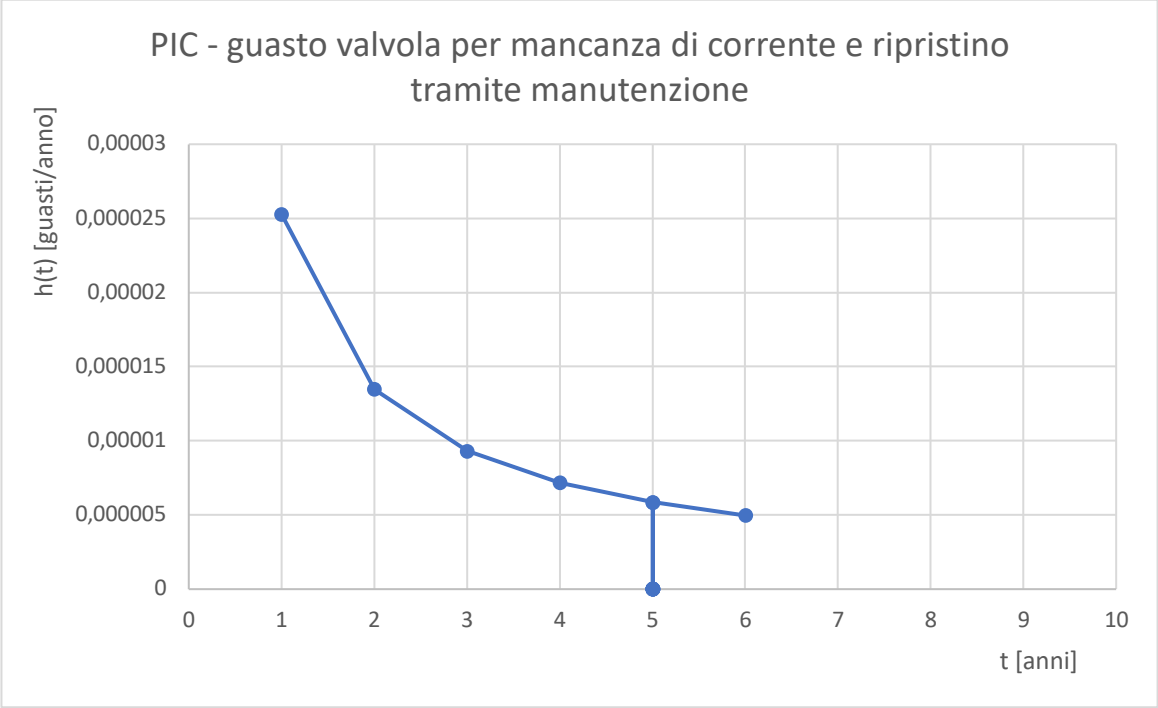


Figura 3.3.3.1 - *Grafico h(t)-t guasto valvola per mancanza di corrente*

Il grafico in Figura 3.3.3.1 mostra l'andamento del tasso di guasto fino all'anno 5, momento in cui avviene il guasto del PIC per mancanza di corrente. Conseguentemente a questo, viene messo in atto il processo di manutenzione previsto per tale componente, dal grafico questo tipo di operazione si nota dal tratto ad andamento differente rispetto a quello precedente il guasto.

Essendo l'intervento stimato di 6 ore (SINTEF, 2002) (dato medio), il tratto in questione è assunto con tasso di guasto costante pari a 0 guasti/anno, poiché l'uso del componente è sospeso per favorire l'intervento di manutenzione.

Nel grafico, trattandosi di poche ore di intervento, la durata della manutenzione è rappresentata da un picco verso il basso, questo è dovuto alla scelta della scala temporale annuale su cui è impostato l'asse delle ascisse nella rappresentazione.

Successivamente alla riparazione, l'andamento della curva riprende coerentemente con il tratto precedente al guasto, il tasso di guasto continua così a diminuire.

Tabella 3.3.2.d - *Dati riferiti a 5 anni di funzionamento del componente*

5 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	5,85424E-06	-6,06287E-08	0,267416933	0,267416933
rottura	6,12408E-06	-6,39583E-08	0,264183348	0,264183348
blocco	5,85424E-06	-6,06287E-08	0,267416933	0,267416933
guasto alla valvola			0,981107769	
guasto controller	5,85424E-06	-6,06287E-08	0,267416933	0,267416933
guasto indicatore	6,12408E-06	-6,39583E-08	0,264183348	0,264183348
GUASTO PIC			1	0

Tabella 3.3.3.1 - *Dati riferiti a 5 anni di funzionamento del componente + 6 ore di manutenzione per guasto per mancanza di corrente*

5,0007991 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	5,85339E-06	-6,06192E-08	0,267411804	0,732588196
rottura	6,12319E-06	-6,39483E-08	0,264178123	0,735821877
blocco	5,85424E-06	-6,06287E-08	0,267416933	0,732583067
guasto alla valvola			0,981108505	0,018891495
guasto controller	5,85424E-06	-6,06287E-08	0,267416933	0,732583067
guasto indicatore	6,12319E-06	-6,39483E-08	0,264178123	0,735821877
GUASTO PIC			0,930688899	0,069311101

Dal confronto dei dati riportati in Tabella 3.3.2.d e 3.3.3.1 si nota come al termine della riparazione, la probabilità di guasto si sia abbassata grazie all'intervento di ripristino del componente.

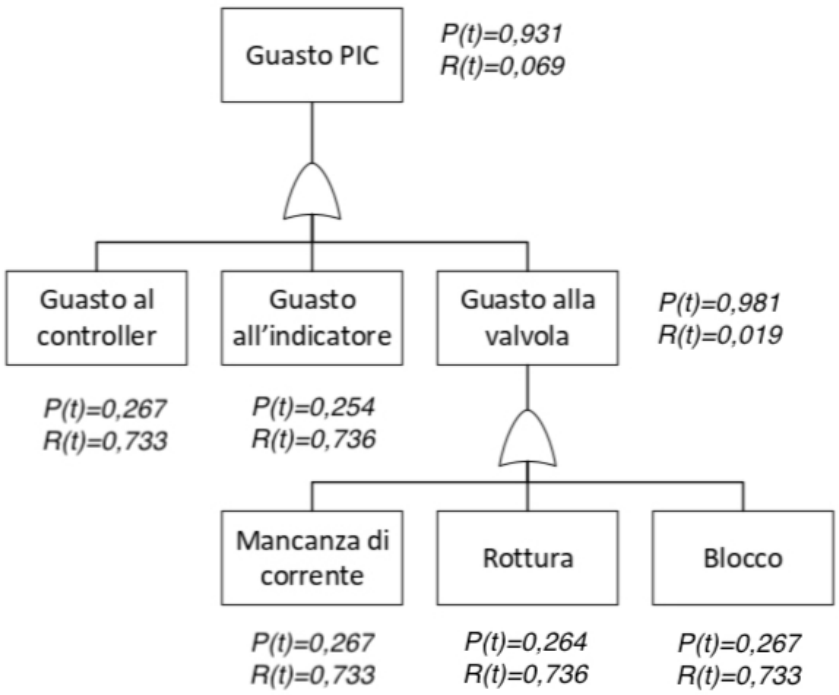


Figura 3.3.3.1.a - *MCS guasto pic con valori relativi a P(t) e R(t)*

3.3.3.2 Analisi guasto PIC per guasto dell'indicatore

In questo paragrafo viene viene simulato il caso in cui il guasto del PIC avvenga per guasto dell'indicatore.

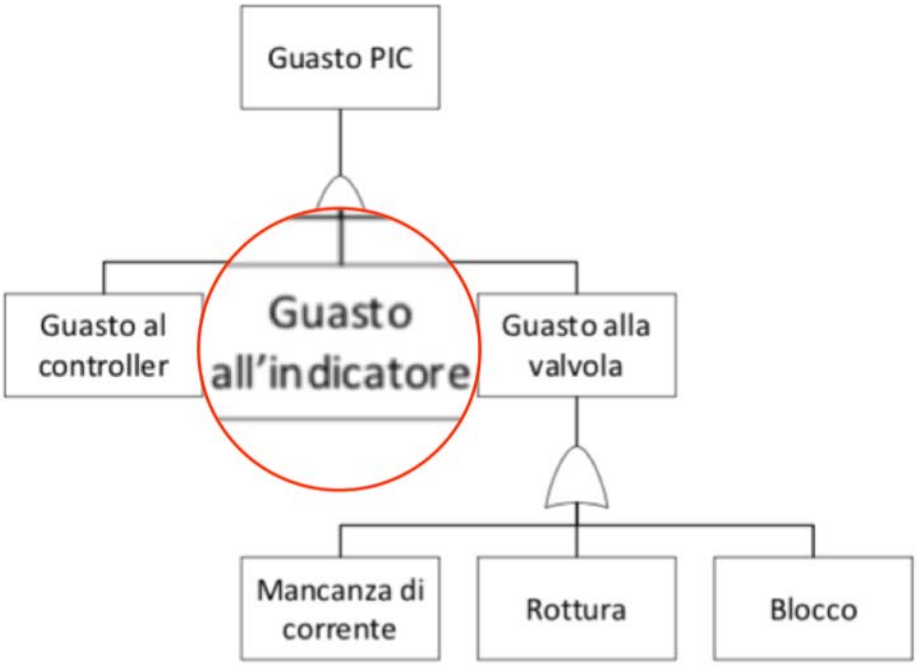


Figura 3.3.3.2 – *MCS guasto pic con evento incidentale in evidenza*

Anche in questo caso, seguendo i dati riportati dal manuale Oreda (SINTEF, 2002), il tempo di riparazione per questo tipo di guasto corrisponde a 5,3 ore lavorative, approssimate a 6 ore per comodità nell'eseguire i calcoli.

Successivamente al periodo di manutenzione, si riprende l'analisi nella ricerca dei parametri di interesse e si esegue infine il confronto con i dati ottenuti prima del guasto a 1 ora dalla riparazione e ripresa del sistema, ipotizzando che la ripresa sia immediatamente successiva alla riparazione.

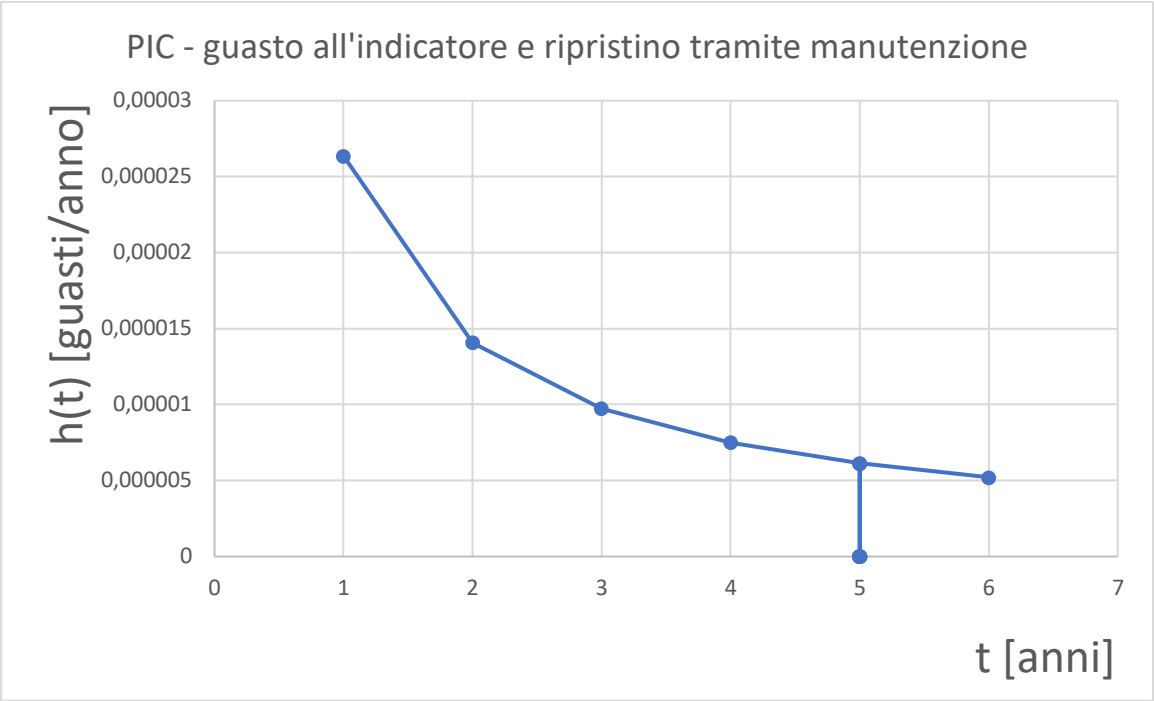


Figura 3.3.3.2 - *Grafico h(t)-t guasto valvola per guasto all'indicatore*

Il grafico in Figura 3.3.3.2 mostra l'andamento del tasso di guasto fino al momento in cui all'anno 5, si ha il guasto del PIC per guasto dell'indicatore. Conseguentemente a questo, viene messo in atto il processo di manutenzione previsto per tale componente, dal grafico questo tipo di operazione si nota dal tratto ad andamento differente rispetto a quello precedente il guasto.

Essendo l'intervento stimato di 6 ore (SINTEF, 2002) (dato medio), il tratto in questione è assunto con tasso di guasto costante pari a 0 guasti/anno, poiché l'uso del componente è sospeso per favorire l'intervento di manutenzione.

Nel grafico, trattandosi di poche ore di intervento, la manutenzione è rappresentata da un picco verso il basso, questo è dovuto alla scelta della scala temporale annuale su cui è impostato l'asse delle ascisse nella rappresentazione.

Successivamente alla riparazione, l'andamento della curva riprende coerentemente con il tratto precedente al guasto, il tasso di guasto continua anche in questo caso a diminuire.

Tabella 3.3.2.d - *Dati riferiti a 5 anni di funzionamento del componente*

5 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	5,85424E-06	-6,06287E-08	0,267416933	0,267416933
rottura	6,12408E-06	-6,39583E-08	0,264183348	0,264183348
blocco	5,85424E-06	-6,06287E-08	0,267416933	0,267416933
guasto alla valvola			0,981107769	
guasto controller	5,85424E-06	-6,06287E-08	0,267416933	0,267416933
guasto indicatore	6,12408E-06	-6,39583E-08	0,264183348	0,264183348
GUASTO PIC			1	0

Tabella 3.3.3.2 - *Dati riferiti a 5 anni di funzionamento del componente + 6 ore di manutenzione per guasto all'indicatore*

5,0007991 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)
mancanza di corrente	5,85339E-06	-6,06192E-08	0,248719464	0,751280536
rottura	6,12319E-06	-6,39483E-08	0,264178123	0,735821877
blocco	5,85424E-06	-6,06287E-08	0,267416933	0,732583067
guasto alla valvola			0,982429038	0,017570962
guasto controller	5,85424E-06	-6,06287E-08	0,267416933	0,732583067
guasto indicatore	6,12319E-06	-6,39483E-08	0,264178123	0,735821877
GUASTO PIC			0,930595609	0,069404391

Dal confronto dei dati riportati in Tabella 3.3.2.d e 3.3.3.1, si nota come al termine della riparazione la probabilità di guasto si sia abbassata successivamente alla ripresa del servizio post intervento di rispristino del componente.

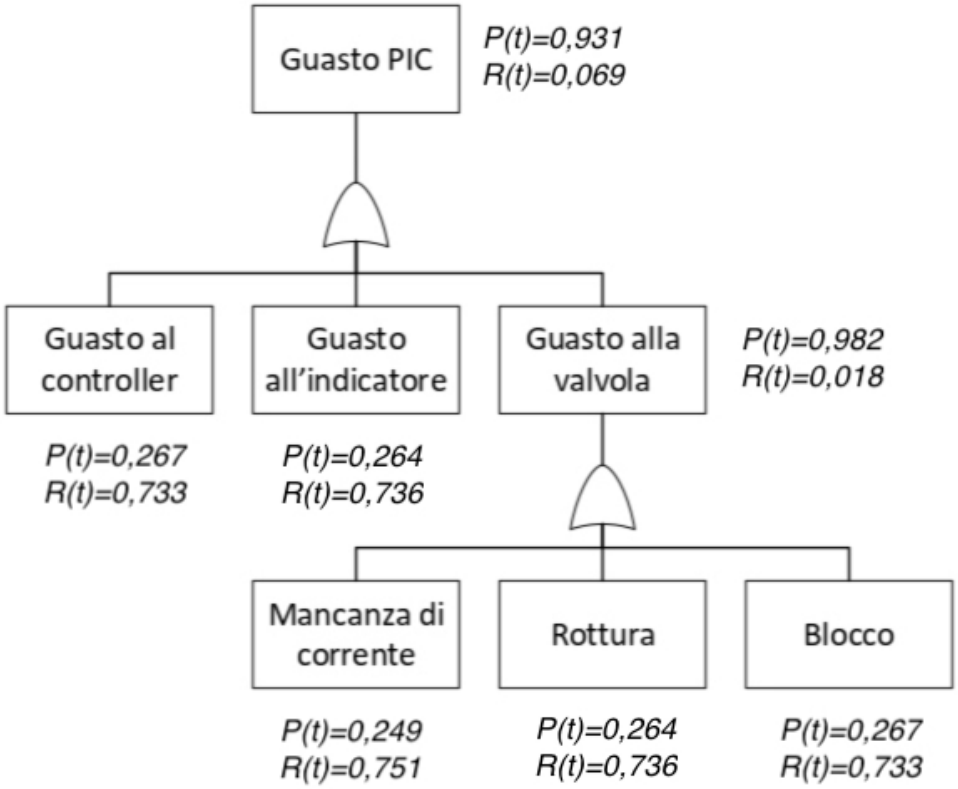


Figura 3.3.3.2.a - *MCS guasto pic con valori relativi a P(t) e R(t)*

Capitolo 4

Albero dei guasti dinamico: caso complesso

Il seguente capitolo riporta lo studio applicativo della metodologia FTA di tipo dinamico applicandolo a un Top Event individuato all'interno dello studio di sicurezza per una raffineria: il superamento della pressione di progetto di una colonna di distillazione.

4.1 Il processo di distillazione

All'interno di una raffineria, il processo di distillazione primaria costituisce la prima fase di lavorazione del petrolio greggio per l'ottenimento dei seguenti semilavorati:

- GPL;
- benzina leggera carica isomerizzazione;
- benzina pesante carica reforming;
- nafta;
- kerosene;
- gasolio leggero atmosferico;
- gasolio pesante atmosferico;
- gasolio leggero da vuoto;
- gasolio pesante da vuoto;
- residuo vuoto.

La proprietà fisica che viene sfruttata è il punto di ebollizione di ogni componente di una miscela che viene immessa all'interno della colonna in esame.
Le operazioni fondamentali che avvengono in un impianto di distillazione sono:

- vaporizzazione per flash: essa avviene tramite i vapori sviluppatisi fino all'entrata della miscela nella colonna di frazionamento, essi devono restare in contatto con il liquido da cui derivano;
- frazionamento e condensazione: entrambi i processi avvengono nella colonna a piatti, con il contatto di questi e i vapori che salgono mentre il liquido scende, si ha l'arricchimento del vapore in frazioni leggere e del liquido in frazioni pesanti per effetto di condensazioni e di evaporazioni successive.

All’interno della colonna si stabilisce un regime termico in cui ogni piatto assume una determinata temperatura e su di esso vi sarà solo quel liquido che in quelle condizioni di pressione si trova al suo punto di ebollizione.
La temperatura dei piatti decresce dal basso verso l’alto e si avranno così liquidi a punto di ebollizione decrescente man mano che si sale verso l’alto nella colonna.
La condensazione avviene per sottrazione continua di calore. La temperatura di testa viene mantenuta costante riflussando in colonna parte del prodotto di testa, condensato e raffreddato opportunamente in appositi scambiatori e refrigeranti.

4.2 Definizione Top Event

Lo studio di sicurezza che porta all'individuazione dei Top Event che possono verificarsi all'interno di una raffineria è condotto in accordo al D.P.C.M. 31/03/89 (Capitolo 2 allegato III), alcune delle fasi di interesse utili per eseguire l'analisi sono:

- analisi storica;
- Metodo ad indici;
- identificazione degli eventi incidentali, in base alle evidenze dell'analisi storica, delle liste di controllo per le lavorazioni in essere nello Stabilimento e dei risultati derivanti dall'Analisi di Operabilità (HazOp) per le aree critiche degli impianti.

I Top Event individuati sono riportati in Tabella 4.2, l'evento incidentale scelto per l'analisi FTA dinamica è il primo tra quelli riportati: il superamento della pressione di progetto di una colonna.

Tabella 4.2 - *Top Event impianto*

N	TOP EVENT
1	Superamento della pressione di progetto della colonna
2	Rilascio di miscela di idrocarburi per perdita di una tubazione a monte del forno
3	Rilascio di miscela di idrocarburi per perdita da tubazione sul treno di preriscaldo carica dalla colonna
4	Superamento della pressione di progetto nella colonna
5	Rilascio della linea di fondo nella colonna stabilizzatrice
6	Rilascio di GPL per perdita della tubazione di fondo dell'accumulatore
7	Trafilamento della tenuta delle pompe a servizio della colonna

4.3 Calcolo della probabilità di accadimento del Top Event con metodo statico FTA

Il seguente paragrafo ha lo scopo di ottenere dei risultati dall'analisi FTA di tipo statico da poter comparare con l'analisi FTA di tipo dinamico che verrà affrontata nel paragrafo a seguire, a tale scopo viene utilizzato l'albero dei guasti[14] riportato in Figure 4.3 e 4.3.a, per risolvere l'analisi verranno utilizzati i tassi di guasto che in esso sono riportati.

[14] FTA presente nel materiale informativo riguardante lo studio di sicurezza della raffineria fornito dal docente.

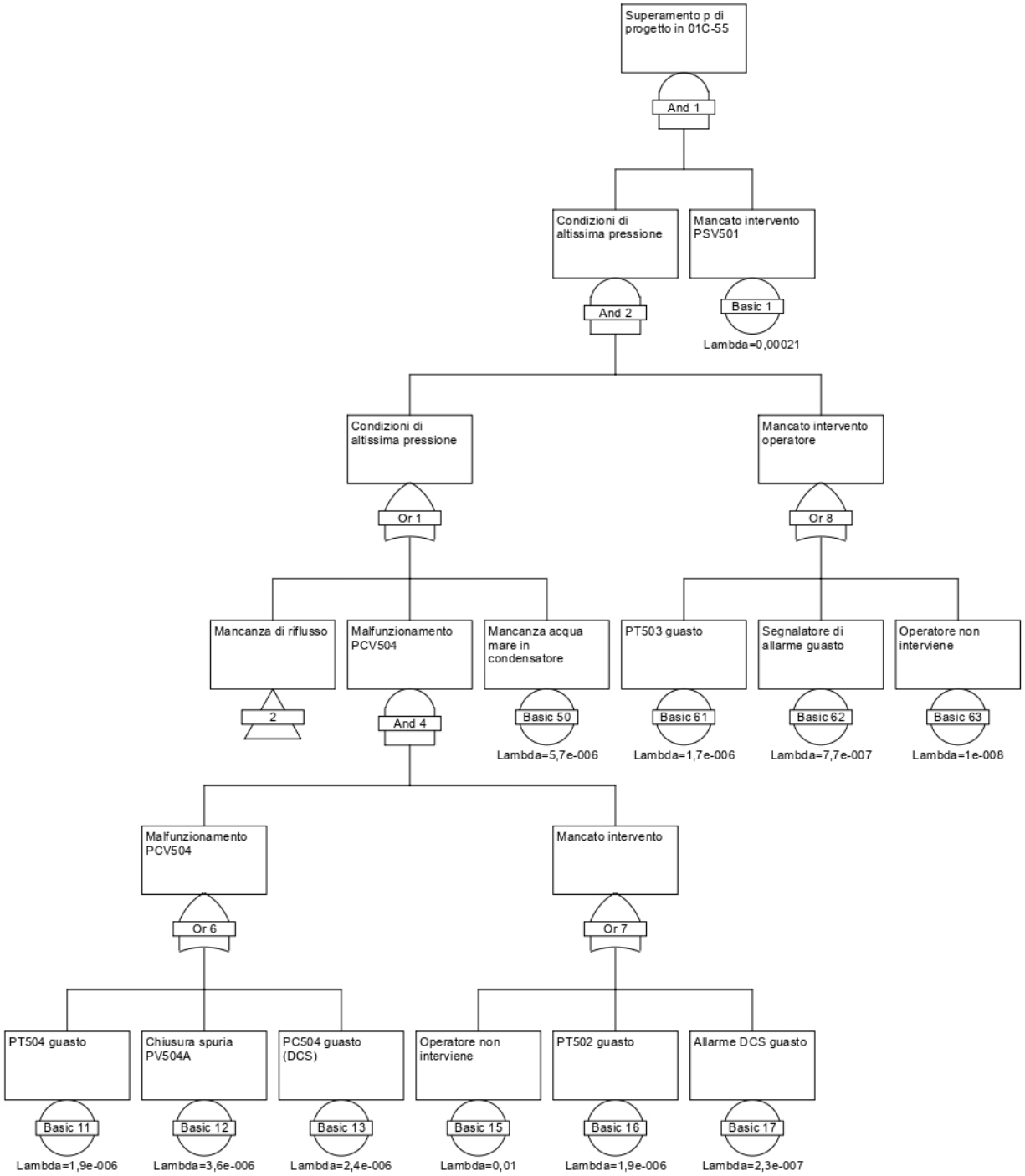


Figura 4.3 – *FTA statico*

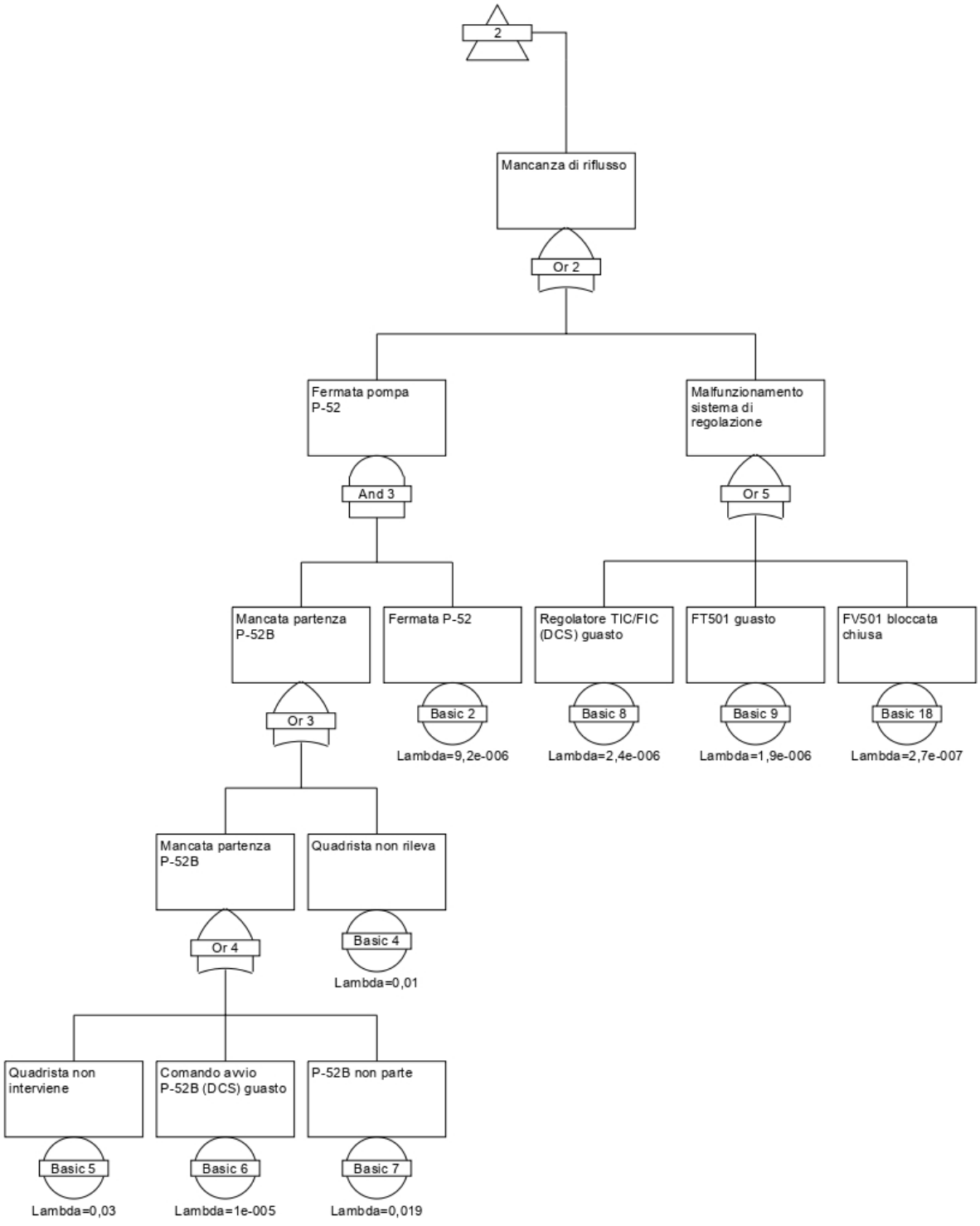


Figura 4.3.a – *FTA statico*

I dati riportati sono ottenuti facendo riferimento al procedimento che si trova all'interno del paragrafo 1.5.1: frequenza di guasto (1.5.1.2), probabilità di guasto (1.5.1.3), affidabilità (1.5.1.4).

Dalla risoluzione dell'albero risulta che la frequenza di guasto corrispondente al Top Event è di $3{,}82026*10^{-6}$ [15] occorrenze/anno.

Dalla frequenza è possibile ottenere quando si verificherà l'avvenimento incidentale dal momento in cui il sistema è messo in funzione, esso avviene a circa 262 anni dall'inizio, considerando la vita media di un impianto, (40-50 anni), si può facilmente assumere che tale evento incidentale non potrà mai accadere durante il corso della sua vita.

[15] Dati presenti all'interno del materiale informativo riguardante lo studio di sicurezza della raffineria fornito dal docente.

4.4 Calcolo della probabilità di accadimento del Top Event con metodo dinamico FTA

In riferimento al Capitolo 3, nel seguente paragrafo vengono riportati i dati riferiti all'analisi FTA di tipo dinamico, coerentemente al procedimento indicato in precedenza (paragrafo 3.1 e 3.2), a partire dalla distribuzione di Weibull (3.1) viene calcolato il tasso di guasto tempo dipendente, successivamente vengono poi ricavati frequenza di guasto (3.2.2), probabilità di accadimento dell'evento incidentale (3.2.3) e affidabilità (3.2.4).

Nella Tabella 4.4 sotto riportata, vengono riportati i risultati dei parametri ricercati.

Il calcolo di frequenza, probabilità ed affidabilità è effettuato seguendo l'ordine di guasto e applicando le regole dell'algebra booleana, in riferimento all'albero dei guasti in Figura 4.3 e 4.3.a.

I dati ricercati vengono determinati per un periodo di tempo di 22 anni, anno in cui si verifica l'evento incidentale scelto (Tabella 4.4) P(t)=1.

Tabella 4.4 – *Dati riferiti all'anno 22 di funzionamento dell'impianto*[16]

22 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)	Probabilità di guasto P(t)
PT504 guasto	0,006016608	-9,47118E-05	0,518475776	0,481524224	0,481524224
chiusura spuria PV504A	2,9220369	9,56361E-32	0	1	1
PC504 guasto (DCS)	0,006016608	-9,47118E-05	0,518475776	0,481524224	0,481524224
malfunzionamento PCV504			1	0	
operatore non interviene	0,01	0,008025188	0,802518798	0,197481202	0,197481202
PT502 guasto	0,005838444	-8,94625E-05	0,516491037	0,483508963	0,483508963
allarme DCS guasto	2,9220369	9,56361E-32	0	1	1
mancato intervento			1	0	
mancanza di riflusso			0,079596131	0,920403869	
malfunzionamento PCV504			1	0	
mancanza acqua mare in condensatore	0,0000057	5,69929E-06	0,999874608	0,000125392	0,000125392
condizioni di altissima pressione			1	0	
PT503 guasto	0,005838444	-8,94625E-05	0,516491037	0,483508963	0,483508963
segnalatore di allarme guasto	2,9220369	9,56361E-32	0	1	1
operatore non interviene	0,00000001	1E-08	0,999874608	0,000125392	0,000125392
mancato intervento operatore			1	0	
Condizioni di altissima pressione			1	0	
mancato intervento PSV501	0,364345247	0,001629806	1	1,97153E-10	1
Superamento p di progetto			1	1,97153E-10	

[16] DCS=controllo di sicurezza della densità/peso specifico;

FT =trasmettitore di portata;

PC=controllo di pressione;

PCV=valvola di controllo di pressione;

PSV=valvola di sicurezza della pressione;

PT=trasmettitore di pressione;

PV=valvola di pressione.

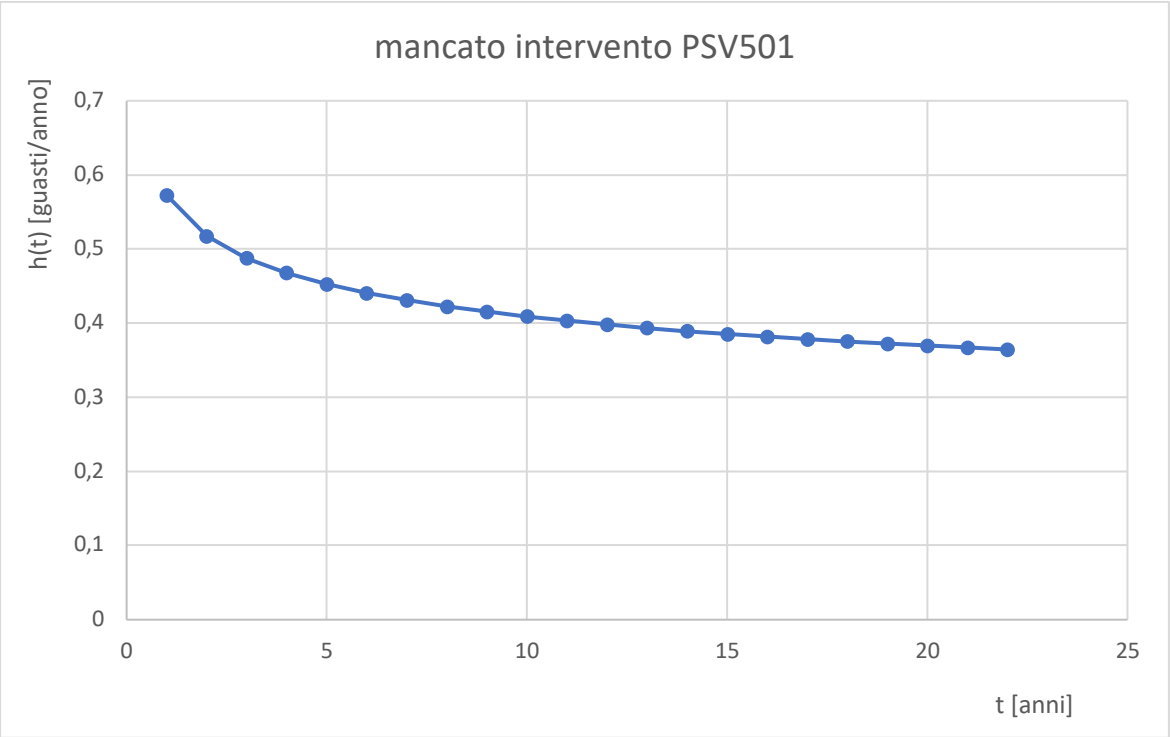


Figura 4.4.1 – *Grafico h(t)-t mancato intervento PSV501*

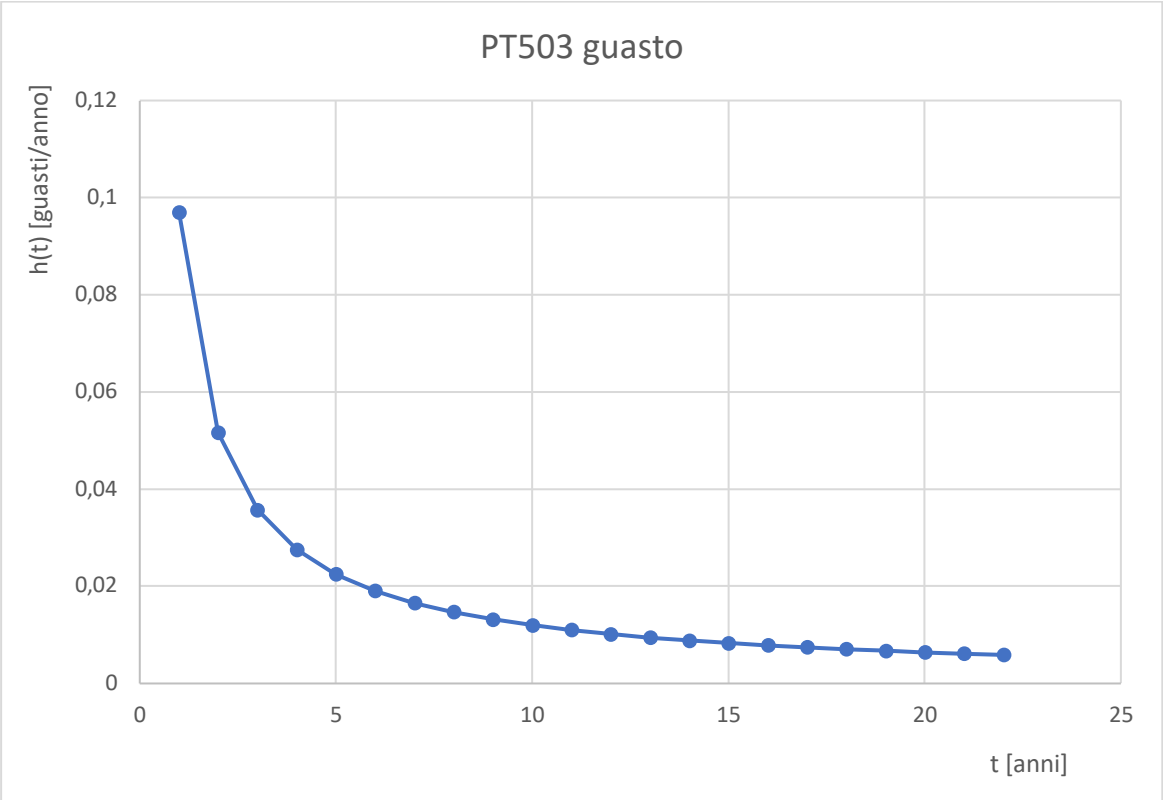


Figura 4.4.1.a – *Grafico h(t)-t PT503 guasto*

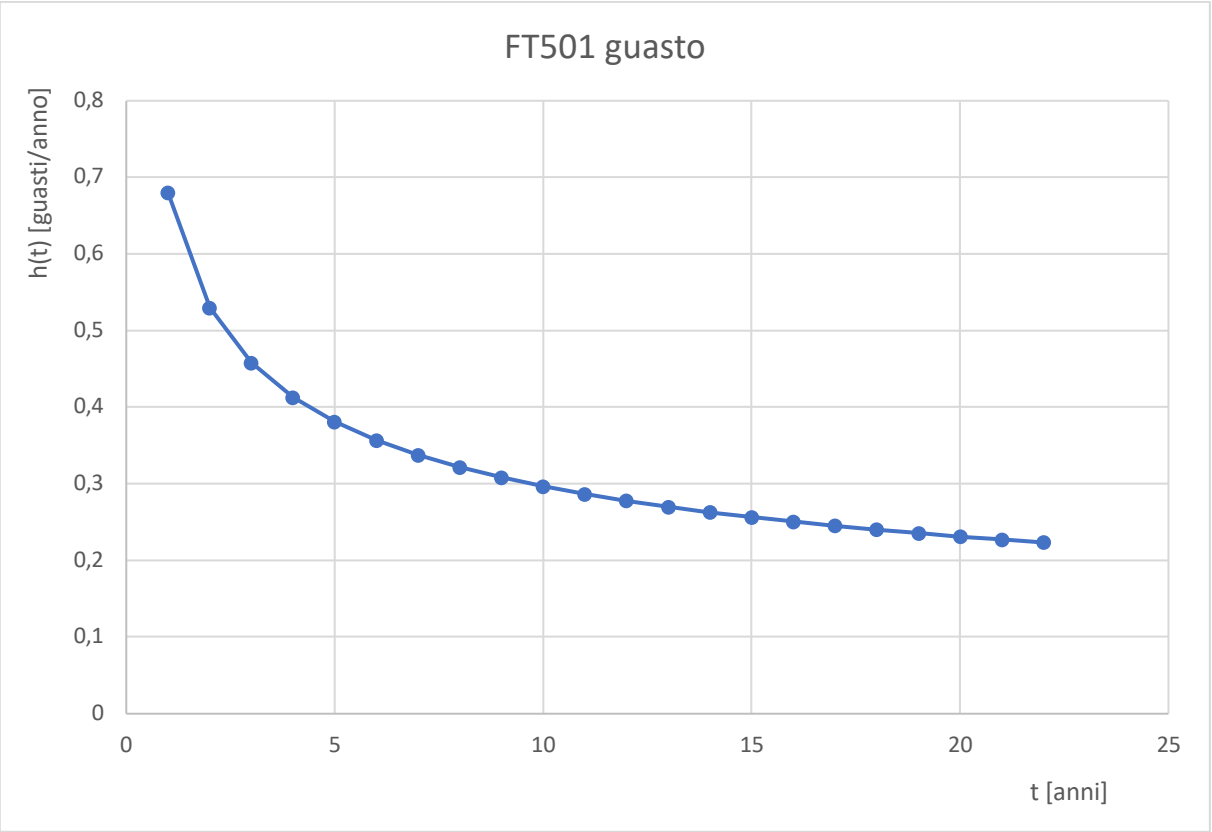


Figura 4.4.1.b – *Grafico h(t)-t FT501 guasto*

Affinché si raggiunga l'evento incidentale individuato, ovvero il superamento della pressione di progetto della colonna, entrambi gli eventi precedenti devono essere verificati poiché essi sono collegati dal cancello logico tipo "AND": condizioni di altissima pressione e mancato intervento PSV501.

L'evento intermedio che corrisponde alle condizioni di altissima pressione è verificato se al di sotto, gli eventi di altissima pressione e mancato intervento operatore si verificano, per quest'ultimo, affinché esso avvenga si considera l'evento base di PT503 guasto.

L'evento intermedio di altissima pressione si verifica se, risalendo all'evento di mancanza di riflusso, esso avviene per malfunzionamento del sistema di regolazione dovuto a un guasto di FT501.

Nelle Figure 4.4.1, 4.4.1.a e 4.4.1.b sono riportati i grafici con gli andamenti dei tassi di guasto h(t) e tempo dei componenti che portano al verificarsi dell'evento incidentale, anche in questo caso come nel precedentemente capitolo (paragrafo 3.3.2), per ogni componente si nota come il tasso di guasto diminuisce con l'aumentare degli anni in cui il sistema opera, l'andamento è quindi coerente con il periodo di vita considerato, ovvero la fase iniziale della Bathtube curve nel tratto di mortalità infantile.

4.5 Confronto dati ottenuti dalle due analisi

A partire dalla FTA di tipo statico si ricava che l'accadimento del Top Event oggetto di analisi, avviene ogni 262 anni circa.

Alla luce di tale risultato, nello studio di sicurezza tale evento non viene considerato per un'ulteriore sviluppo della stessa valutazione, esso ha una frequenza di accadimento di $3{,}82026*10^{-6}$ eventi/anno quindi minore a $5*10^{-6}$ eventi/anno ($5*10^{-7}$ eventi/anno in caso di un evento che coinvolga potenzialmente aree esterne alla Raffineria)[17], è dichiarato non credibile per cui non si individuano scenari incidentali legati ad esso e non viene effettuata la stima della loro frequenza di accadimento come ad esempio attraverso lo sviluppo dell'albero degli eventi.

Nel caso in cui l'analisi venga condotta con parametri tempo dipendenti (Dynamic FTA), il superamento della pressione di progetto avviene nell'anno 22 di funzionamento del sistema.

Con questo risultato, nello studio di sicurezza l'evento incidentale risulterebbe credibile contrariamente al risultato ottenuto nell'analisi FTA condotta in modo statico, nello studio sarebbe quindi ulteriormente sviluppato per quanto riguarda i possibili scenari incidentali che potrebbero verificarsi all'interno della raffineria.

[17] Dati presenti all'interno del materiale informativo riguardante lo studio di sicurezza della raffineria fornito dal docente

4.6 Introduzione dei piani di manutenzione

In analogia a quanto riportato nel paragrafo 3.3.3, a seguito del verificarsi dell'evento incidentale, l'analisi procede introducendo nello studio l'intervento dei piani di manutenzione che possono prevedere la riparazione o la sostituzione del componente.
Anche in questo caso si fa utilizzo del manuale Oreda (SINTEF, 2002) per quanto riguarda il tempo di riparazione in ore lavorative dei componenti di interesse.

4.6.1 Piani di manutenzione dei componenti

Secondo il manuale Oreda (SINTEF, 2002), il tempo di riparazione per i guasti indicati nel paragrafo 4.4 che riguardano il mancato intervento PSV501, guasti a PT503 e FT501, corrisponde a 7 ore lavorative.
Una volta ultimate le operazioni di manutenzione, si riprende l'analisi nella ricerca dei parametri di interesse e si esegue infine il confronto con i dati ottenuti prima del guasto a 1 ora dalla riparazione e ripresa del sistema, ipotizzando che la ripresa sia immediatamente successiva alla riparazione.

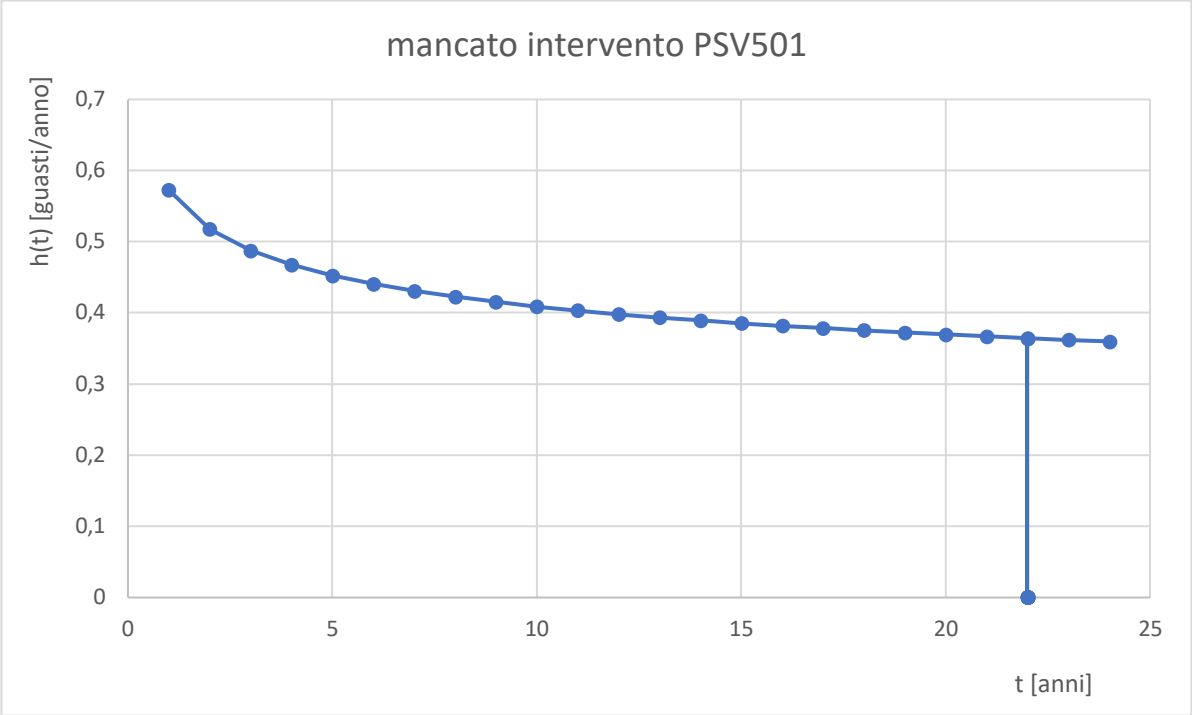


Figura 4.6.1 - *Grafico h(t)-t mancato intervento PSV501*

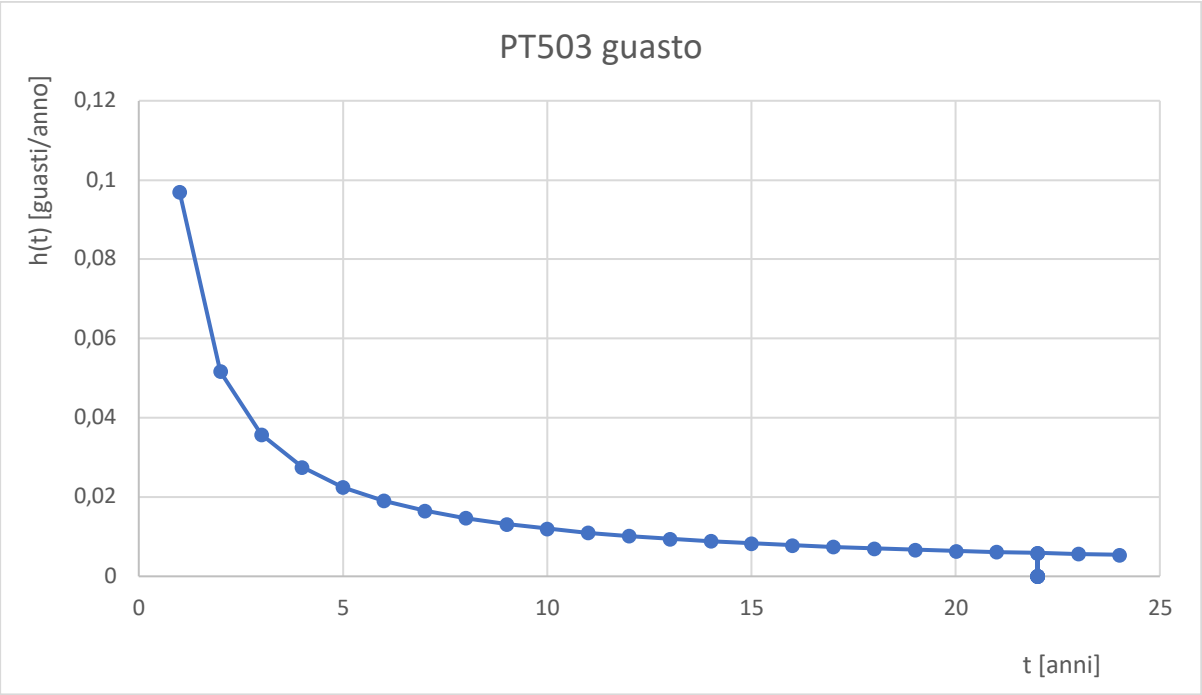


Figura 4.6.1.a - *Grafico h(t)-t PT503 guasto*

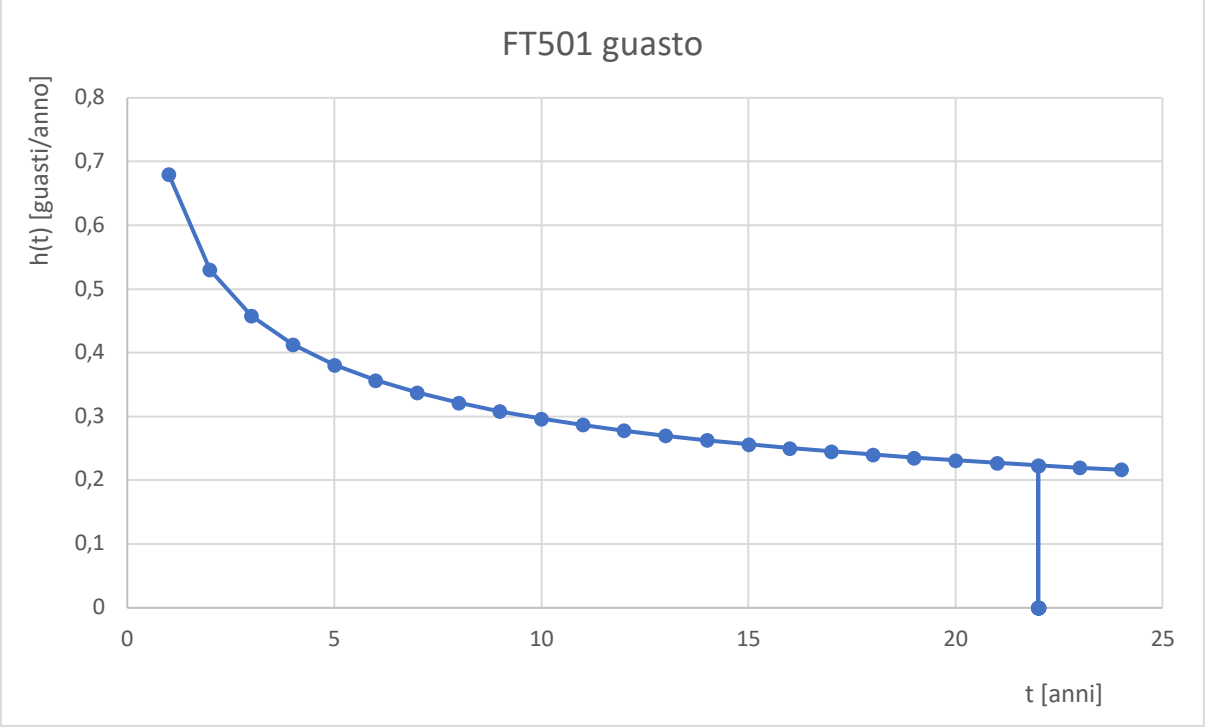


Figura 4.6.1.b - *Grafico h(t)-t FT501 guasto*

I grafici riportati nelle Figure 4.6.1-a-b mostrano l'andamento del tasso di guasto fino al momento in cui all'anno 22, si ha il superamento della pressione di progetto della colonna di distillazione. Conseguentemente a questo, viene messo in atto il processo di manutenzione previsto per le componenti guaste, dai grafici questo tipo di operazione si nota dal tratto ad andamento differente rispetto a quello precedente il guasto.

Essendo l'intervento della durata di 7 ore (SINTEF, 2002) (dato medio), il tratto in questione è assunto con tasso di guasto costante pari a 0 guasti/anno, poiché l'uso del componente è sospeso per favorire l'intervento di manutenzione.

Nei grafici, trattandosi di poche ore di intervento, la durata della manutenzione è rappresentata da un picco verso il basso, questo è dovuto alla scelta della scala temporale annuale su cui è impostato l'asse delle ascisse nella rappresentazione.

4.6.2 Conseguenze introduzione piani di manutenzione dei componenti

Successivamente alla riparazione, l'andamento della curva dovrebbe riprendere coerentemente con il tratto precedente al guasto, il tasso di guasto continuerebbe così a diminuire.

In questo caso si presentano due possibilità:

1. Riparazione di tutti i componenti danneggiati

   In questo caso, successivamente alla completa effettuazione dei piani di manutenzione dei componenti guasti, il sistema non può riprendere il suo normale funzionamento poiché è ancora affetto da guasto come mostrato in Tabella 4.6.2.

Tabella 4.6.2 - *Dati riferiti all'anno successivo la rimessa in funzione del sistema*

23,00091264 anni	tasso di guasto h(t)	frequenza di guasto f(t)	Probabilità di guasto P(t)	Affidabilità R(t)	Probabilità di guasto P(t)
PT504 guasto	0,005778644	-9,0792E-05	0,51706594	0,481524224	0,48293406
chiusura spuria PV504A	2,949320219	1,40637E-33	0	1	1
PC504 guasto (DCS)	0,005778644	-9,0792E-05	0,51706594	0,481524224	0,48293406
malfunzionamento PCV504			1	0	
operatore non interviene	0,01	0,007945264	0,794526351	0,197481202	0,205473649
PT502 guasto	0,005607033	-8,57583E-05	0,515108437	0,483508963	0,484891563
allarme DCS guasto	2,949320219	1,40637E-33	0	1	1
mancato intervento			1	0	
mancanza di riflusso			0,035319058	0,920403869	
malfunzionamento PCV504			1	0	
mancanza acqua mare in condensatore	0,0000057	5,69925E-06	0,999868903	0,000125392	0,000131097
condizioni di altissima pressione			1	0	
PT503 guasto	0,005607033	0,005607033	0,515108437	0,483508963	0,484891563
segnalatore di allarme guasto	2,949320219	1,40637E-33	0	1	1
operatore non interviene	0,00000001	1E-08	0,999868903	0,000125392	0,000131097
mancato intervento operatore			1	0	
Condizioni di altissima pressione			1	0	
mancato intervento PSV501	0,361981798	0,001291663	1		1
Superamento p di progetto			**1**	1,97153E-10	

2. Riparazione dei componenti PT503 e FT501
   Sostituzione PSV501
   Con questo tipo di intervento la probabilità di accadimento dell'evento incidentale si abbassa (Tabella 4.6.2.a), tale scelta può essere conveniente nel momento in cui risulta più semplice e meno oneroso procedere con una sostituzione del componente PSV501 al posto della sua manutenzione.

Tabella 4.6.2.a - *Dati riferiti all'anno successivo la rimessa in funzione del sistema*

23,00091264 anni	**tasso di guasto h(t)**	**frequenza di guasto f(t)**	**Probabilità di guasto P(t)**	**Affidabilità R(t)**	**Probabilità di guasto P(t)**
PT504 guasto	0,005778644	-9,0792E-05	0,51706594	0,481524224	0,48293406
chiusura spuria PV504A	2,949320219	1,40637E-33	0	1	1
PC504 guasto (DCS)	0,005778644	-9,0792E-05	0,51706594	0,481524224	0,48293406
malfunzionamento PCV504			1	0	
operatore non interviene	0,01	0,007945264	0,794526351	0,197481202	0,205473649
PT502 guasto	0,005607033	-8,57583E-05	0,515108437	0,483508963	0,484891563
allarme DCS guasto	2,949320219	1,40637E-33	0	1	1
mancato intervento			1	0	
mancanza di riflusso			0,035319058	0,920403869	
malfunzionamento PCV504			1	0	
mancanza acqua mare in condensatore	0,0000057	5,69925E-06	0,999868903	0,000125392	0,000131097
condizioni di altissima pressione			1	0	
PT503 guasto	0,005607033	0,005607033	0,515108437	0,483508963	0,484891563
segnalatore di allarme guasto	2,949320219	1,40637E-33	0	1	1
operatore non interviene	0,00000001	1E-08	0,999868903	0,000125392	0,000131097
mancato intervento operatore			1	0	
Condizioni di altissima pressione			1	0	
mancato intervento PSV501	0,572631877	-0,113550835	0,797388798	0,202611202	0,797388798
Superamento p di progetto			**0,797388798**	1,97153E-10	

In questo caso il grafico riportato in Figura 4.6.1 si modifica in quello rappresentato in Figura 4.6.2, la rappresentazione dell'andamento del tasso di guasto h(t) in funzione del tempo di funzionamento corrisponderebbe a quella di un PSV nuovo dal momento in cui l'intero sistema riprende il ciclo di funzionamento.

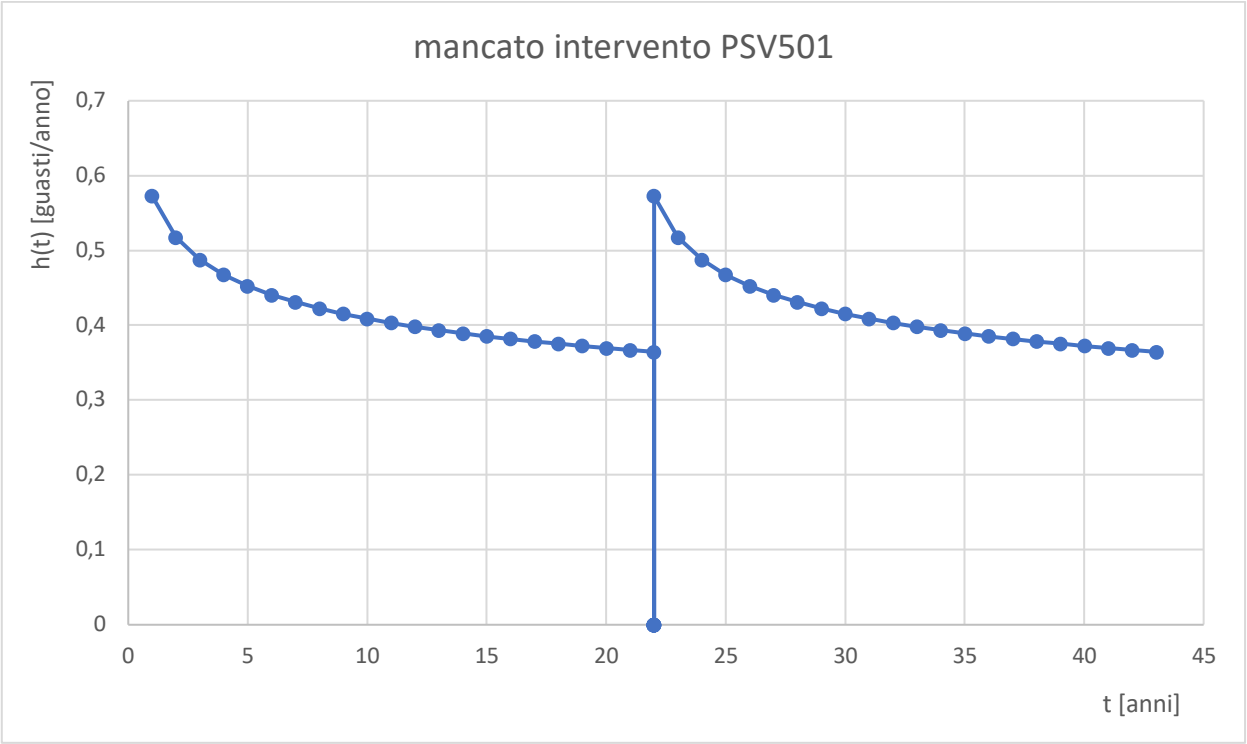


Figura 4.6.2 - *Grafico h(t)-t mancato intervento PSV501*

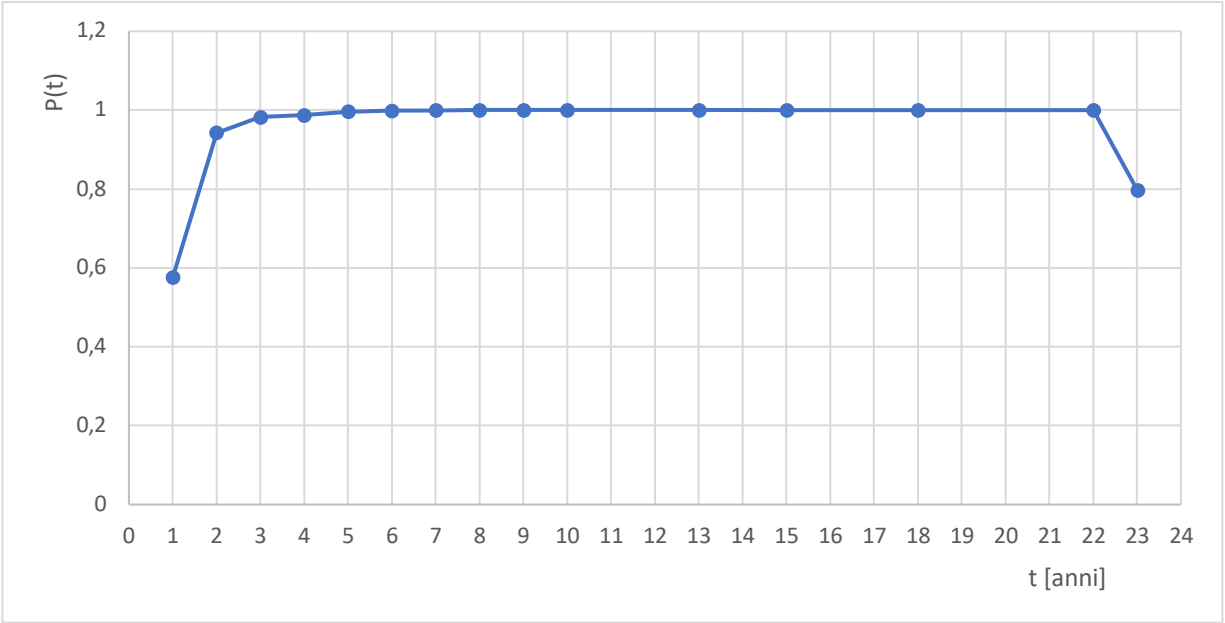


Figura 4.6.3 - *Grafico P(t)-t*

Il grafico in Figura 4.6.3 riporta la probabilità di accadimento del Top Event in funzione degli anni di funzionamento del sistema.
In analogia con quanto indicato in precedenza, l'andamento della probabilità è crescente dal primo anno di funzionamento dell'impianto fino all'anno 22 quando P(t)=1, ovvero quando il Top Event si verifica, durante il fermo dell'impianto successivamente all'evento incidentale viene eseguito un intervento di manutenzione e una volta passato il tempo necessario, il sistema riprende il ciclo produttivo con probabilità di accadimento corrispondente a circa 0,8.

4.6.3 Confronto probabilità di accadimento

In Tabella 4.6.3 viene messa in evidenza la variazione della probabilità di superamento della pressione di progetto, una volta effettuate le manutenzioni ai componenti guasti e ripreso il ciclo di funzionamento del sistema.

Tabella 4.6.3 – *Confronto probabilità di accadimento*

P(t=1)	P(t)=23 anni
0,576	0,797

Dalla tabella sopra riportata la P(t), una volta ripreso il ciclo produttivo del sistema, subisce una variazione del 38,43% in più rispetto all'anno 1, quindi la sua affidabilità è inferire rispetto al primo anno di installazione.

Capitolo 5
Conclusioni e osservazioni

Lo scopo principale di questa tesi è stato quello di analizzare ed applicare il metodo di analisi dell'albero dei guasti dinamico in alternativa all'approccio tradizionale di tipo statico.
In particolare, grazie all'applicazione di questa metodologia a un caso studio, è stato maggiormente possibile evidenziare e confrontare le differenze tra i due tipi di analisi.
L'utilizzo dell'analisi di tipo statico, non permette di poter adattare l'analisi FTA specificatamente al sistema analizzato non ottenendo una valutazione creata su misura del sistema, in alcuni casi infatti, dai risultati delle valutazioni riguardanti frequenze di accadimento degli eventi incidentali individuati, a causa della loro bassa incidenza ($<5*10^{-6}$ eventi/anno), essi verrebbero automaticamente esclusi dallo studio di sicurezza in vista di una possibile valutazione sotto forma di conseguenze di uno scenario incidentale a loro associato.
All'interno della trattazione, questo confronto è affrontato nel Capitolo 4 in cui, dai risultati delle frequenze di accadimento ottenuti dall'analisi statica e successivamente quelli individuati nella valutazione di tipo dinamica, si evince che dall'analisi statica la frequenza di accadimento del Top Event (superamento di pressione di progetto di una colonna di distillazione in una raffineria) è di $3{,}82026*10^{-6}$ eventi/anno, ovvero un accadimento incidentale ogni 262 anni, questo intervallo supera di molto la durata della vita media di un impianto produttivo.
Con questo risultato, l'evento incidentale verrebbe così escluso nel proseguimento dello studio e non verrebbe valutato più in specifico attraverso analisi qualitative o quantitative, definendo eventuali scenari incidentali.
A differenza della prima, applicando l'analisi di tipo dinamico, questo evento incidentale presenta il raggiungimento della probabilità di verificarsi in un intervallo di 22 anni che, considerando una durata media di vita di un impianto di 45 anni, vedrebbe il verificarsi dell'evento al suo interno.
Procedendo nello studio scegliendo i risultati ottenuti quindi con la valutazione di tipo statico, la frequenza di guasto ottenuta non avrebbe così comportato la considerazione dell'evento poiché non credibile.
A differenza della FTA tradizionale, quella dinamica riporta un risultato che riduce di molto l'intervallo di tempo dell'accadimento rispetto al primo risultato.
Procedendo nello studio di sicurezza e quindi nella progettazione del sistema escludendo tale avvenimento, si creerebbe quindi una situazione di pericolo non considerata e adeguatamente trattata nella progettazione.

Con la sua presenza, il pericolo una volta raggiunta la probabilità di accadimento creerebbe danni dal punto di vista produttivo e in maniera più grave, ai lavoratori all'interno dell'area a stretto contatto con esso.
Risulta quindi indispensabile che, durante la progettazione di un impianto e di redazione dello studio di sicurezza, la fase di valutazione del rischio debba essere effettuata quanto più su misura ad esso, i metodi di calcolo utilizzati devono rispecchiare e considerare tutti i possibili eventi di malfunzionamento, guasto ed incidenti, così da poter simulare successivamente, tutti i possibili scenari che con il loro verificarsi possono scaturire.
È utile quindi avvalersi della metodologia FTA dinamica e abbandonare lo studio dal punto di vista statico, considerando tassi di guasto tempo dipendenti a differenza di quelli medi ampiamente presenti in letteratura che poco si adattano a rappresentare situazioni reali.

Un ulteriore sviluppo della ricerca finora riportata, potrebbe essere rappresentato da uno studio degli scenari di aggravio che potrebbero comparire nella vita utile dell'apparecchiatura, come ad esempi fenomeni di corrosione e assottigliamento delle pareti di un'apparecchiatura. Tali fenomeni potrebbero essere inseriti all'interno della struttura dell'Albero dei Guasti e successivamente essere quantificati con una valutazione dipendente dal tempo.

Bibliografia

Amari, S., Dill, G., & Howald, E. (2003). A new approach to solve dynamic fault trees. *Annual Reliability and Maintainability Symposium, 2003.*, 374–379. https://doi.org/10.1109/rams.2003.1182018

Cai, K. Y. (1996). *System failure engineering and fuzzy methodol- ogy an introductory overview. Fuzzy Sets and Systems*.

Center for Chemical Process Safety, C. (2010). *Guidelines for Chemical Process Quantitative Risk Analysis CCPS guidelines series* (J. Wiley & Sons, Ed.).

Chen, S. J., & Hwang, C. L. (1992). *Fuzzy multiple attribute decision making methods and applications*.

Clifton, A. (1999). Fault Tree Analysis.

Distribuzione Weibull. (n.d.). Retrieved from http://www.costruzionedimacchine.com/dispense/affidabilita/distr_weibull.pdf

Dugan, J. B., Bavuso, S. J., & Boyd, M. A. (1992). *Dynamic fault-tree models for fault-tolerant computer system*.

Dugan, J. B., Sullivan, K. J., & Coppit, D. (2000). *Developing a low-cost high-quality software tool for dynamic fault-tree analysis*.

Durga Rao, K., Gopika, V., Sanyasi Rao, V. V. S., Kushwaha, H. S., Verma, A. K., & Srividya, A. (2009). Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. *Reliability Engineering and System Safety*, pp. 872–883. https://doi.org/10.1016/j.ress.2008.09.007

Gulati, R., & Dugan, J. B. (1997). *A modular approach for analyzing static and dynamic fault trees*.

Ierace, S. (n.d.). Affidabilità, Manutenibilità e Disponibilità. Retrieved July 15, 2019, from

http://www00.unibg.it/dati/corsi/22028/46050-L9 - 01 - Affidabilita e Disponibilita.pdf

Keene, S. J. (1994). *Comparing hardware and software reliability. Reliability Review*.

Keller, A. Z., & Kara-Zaitri. (1989). *Further application of fuzzy logic to reliability assessment safety analysis*.

Leonardo Bertini, M. B. (n.d.). Costruzione di macchine. Retrieved June 30, 2019, from http://www.dimnp.unipi.it/leonardo-bertini/Corsi/CMM/Materiale Didattico/2013-14/Lez5_Funzioni_Variabili_aleatorie.pdf

Liang, G. S., & Wang, M. J. (1933). *Fuzzy fault-tree analysis using failure possibility. Microelectron*.

Lin, C. T., & Wang, M. J. J. (1997). Hybrid fault tree analysis using fuzzy sets. *Reliability Engineering and System Safety*, *58*(3), 205–213. https://doi.org/10.1016/S0951-8320(97)00072-0

Mital, A., Motorwala, A., Kulkarni, M., Sinclair, M., & Siemieniuch, C. (1994). *Allocation of functions to humans and machines in a manufacturing environment: part I. Guidelines for the practitioner*.

Page, L. B., & Perry, J. E. (1994). *Standard deviation as an alternative to fuzziness in fault tree models*.

Pedryez, W. (1994). *Why triangular membership functions?*

Preyssl, C. (1995). *Reliability Engineering and System Safety*.

Riccardo, R. (n.d.). Elementi di probabilità e statistica. Retrieved April 25, 2019, from http://calvino.polito.it/~riganti/Prob_Stat_teoria_esercizi.pdf

SINTEF, I. M. (2002). *OREDA - Offshore Reliability Data Handbook*.

Stoffen, G. (1997). *Methods for determining and processing probabilities (red book)*.

Suresh, P. V., Babar, A. K., & Raj, V. V. (1996). *Uncertainty in fault tree analysis: a fuzzy approach. Fuzzy Sets and Systems*.

Walker, I. D., & Cavallaro, J. R. (1996). *Failure mode analysis for a hazardous waste clean-up manipulator. Reliability Engineering and System Safety*.

Wang, J., Yang, J. B., & Sen, P. (1995). *Safety analysis and synthesis using fuzzy sets and evidential reasoning*.