APPLICAZIONE DEL FT DINAMICO ALLA MANUTENZIONE

Marco Caira*, Alberto Gambellini*
*Dipartimento di Ingegneria Nucleare e Conversione Energetica - Università di Roma "La Sapienza"
Corso Vittorio Emanuele II, 244
M.Caira@qprogetti.it

SOMMARIO

Negli ultimi anni la crescente domanda di sicurezza da parte dell'opinione pubblica ha rinnovato l'interesse verso le analisi di rischio e di sicurezza. Nel mondo anglosassone l'idea che l'analisi di rischio probabilistica fornisca maggiori garanzie di sicurezza ed affidabilità sta prendendo sempre più piede[1]. Studi su numerosi eventi incidentali hanno evidenziato la vulnerabilità dei sistemi in seguito ad eventi manutentivi o non previsti in sede di progetto preliminare. In pratica le situazioni reali che si vengono a creare durante la marcia dell'impianto possono differire anche di molto da quelle riportate nei documenti di valutazione dei rischi determinando così situazioni temporanee di rischio oltre quelle normalmente previste[2]. L'uso di analisi di rischio dipendenti dal tempo possono essere viste come un potente strumento per monitorare lo stato di un sistema in un determinato lasso di tempo. In tal modo essa può costituire uno strumento atto a fornire indicazioni per quei processi decisionali che comportano cambiamenti nell'affidabilità e sicurezza dell'impianto (manutenzione straordinaria, ottimizzazione dello scheduling della manutenzione preventiva ecc). Le analisi di rischio convenzionali devono quindi essere modificate per poter inserire nei modelli il fattore tempo. In questo lavoro si presenterà il modello dell'albero dei guasti dinamico, e se ne spiegheranno le potenzialità ed il funzionamento.

2. INTRODUZIONE

Nel corso di questi ultimi anni vi è stato sempre maggiore interesse da parte degli organi di controllo nello stimolare l'uso dell'analisi probabilistica di rischio allo scopo di incrementare un'attività conoscitiva dell'impianto sia da un punto di vista del controllo del rischio sia come gestione delle risorse e quindi della flessibilità dello stesso. Il concetto fondamentale recepito è che una configurazione di impianto basata su un'analisi probabilistica fornisce maggiori sicurezze dal punto di vista del rischio, rispetto alle analisi deterministiche in uso, dove l'attività di impianto seguivano esclusivamente considerazioni dettate dall'esperienza e da regole di buon senso e non da considerazioni susseguenti ad effettive valutazioni sul rischio introdotto.

I motivi per cui tali considerazioni sono state fatte risiedono nel fatto che ci si è resi conto che le analisi di rischio convenzionali fotografano situazioni statiche. Spesso si è costretti ad eseguire elaborate e costose analisi di sensibilità per ottenere informazioni di impianto che potrebbero risultare utili per la gestione. Un impianto è un sistema dinamico oggetto di cambiamenti, cambiamenti che avvengono anche repentinamente nel tempo e che lo portano in configurazioni sempre più lontane dalle configurazioni nominali studiate della analisi di rischio riportate del documento di valutazione di impatto ambientale.

L'esperienza dimostra che i grandi incidenti verificatesi nel corso degli anni nei settori chimico-nucleari sono da imputarsi ad una cattiva gestione impiantistica, da un punto di vista procedurale (Chernobyl, Three miles Island, Bophal). Molti autori [3] hanno evidenziato il fatto che un impianto, a causa dell'attività di test e manutenzione, quasi mai si troverà in una situazione nominale, per cui un eventuale anomalia può condurre a situazioni non previste in sede di progetto e si può quindi facilmente uscire dal range di affidabilità considerato dai progettisti con un evidente danno sia di rischio sia economico se l'impianto e' soggetto a numerose rotture che ne abbassano la disponibilità[4].

Le linee che si vanno delineando vedono sempre più affermarsi la RCM (Reliabilty Centered Maintenance) o manutenzione incentrata sull'affidabilità di origine statunitense e sviluppata in ambito nucleare ed aeronautico.

Queste nuove esigenze richiedono che lo strumento probabilistico di analisi di rischio utilizzato abbia la capacità di seguire l'impianto nelle sue varie configurazioni e di monitorare l'andamento del rischio nel tempo. Le metodologie convenzionali sono state quindi modificati nel corso di questi ultimi anni allo scopo di introdurre in essi la capacità di seguire l'impianto nei suoi cambiamenti e di monitorare le grandezze probabilistiche di interesse nell'analisi del rischio.

Questo lavoro ha lo scopo di fornire una vista d'insieme delle problematiche e dei vantaggi che un'analisi dinamica comporta. Allo scopo e' stato utilizzato il modello di albero dei guasti dinamico formalizzato in

letteratura pochi anni or sono e sviluppato in alcune sue applicazioni dagli autori successivamente.

3. ALBERO DEI GUASTI DINAMICO

Nel corso degli anni, numerose sono state le modifiche che sono state apportate alla metodologia Fault Tree, si possono ricordare:

- Metodologie atte allo sviluppo di affidabilità di software;
- Valutazione di scenari dinamici che seguono una sequenza di eventi incidentali;
- Modellizzazione delle funzionalità di sistemi ingegneristici .

Tali metodologie hanno implementato lo sviluppo di questo tipo di approccio, ma hanno anche introdotto una complessità nel modello, con l'introduzione di nuove porte logiche[5].

Il Fault tree dinamico utilizzato per questo studio sfrutta invece le capacità di calcolo sempre crescente dei moderni computer, allo scopo di sviluppare un fault tree statico in istanti temporali diversi.

Il principale elemento che costituisce il legame tra statico e dinamico, risulta essere la matrice degli House Event dinamica.

Nell'albero dei guasti statico, la matrice degli house event, è utilizzata per la costruzione di un unico albero dei guasti per ogni sistema oggetto dello studio. Nella PSA (Probabilistic Safety Assessment) classica possono essere necessari numerosi alberi dei guasti per un singolo sistema di sicurezza. Alberi che possono differire a causa di differenti criteri di successo e/o differenti scenari con differenti requisiti. È possibile integrare tutti gli alberi relativi ad un sistema in un albero integrato detto "ombrello"[6]. In questo caso, gli House event blocks sono usati per "accendere e spegnere" rispettive parti del albero integrato.

3.1 House event dinamica e modello

La tabella dell'House event è prodotta per documentare quale house event è acceso, e quale è spento affiché il Top Event di un determinato albero risponda al rispettivo criterio di successo/insuccesso modellato nell'appropriato ramo oggetto dello studio[7].

La matrice degli house events, identifica tutti gli house events del modello del sistema con il suo numero delle righe, mentre identifica i modi di funzionamento tramite il numero delle colonne. Ogni house event in tabella ha un valore definito dal valore logico vero o falso (1 o 0).

La matrice degli House Event dinamica, invece, è una matrice che si presenta con questo aspetto[8]:

$$MH = \begin{Vmatrix} H_{11} & & H_{1,N} \\ H_{21} & & \\ & & \\ H_{m,1} & & H_{MN} \end{Vmatrix} \tag{1}$$

Il numero delle righe rappresenta le differenti configurazioni che un sistema può avere durante il suo funzionamento mentre il numero delle colonne rappresenta il numero degli intervalli di tempo considerati nel modello. Occorre notare che per ogni istante temporale è generata una configurazione dell'albero. Ogni elemento H_{ij} della matrice risulta essere un vettore nei valori logici vero e *falso* (*1* e *0*) dal cui valore dipenderà poi il valore del Top Event mentre la sua lunghezza dipenderà sia dal modello temporale scelto per i basic event sia dal numero di basic event presenti nell'albero integrato.

La valutazione quantitativa tiene conto della probabilità come funzione del tempo e quindi le equazioni fondamentali saranno[9]:

$$MCS_i(t) = \left(H_{i,j}, t\right) = q_1(t) \cdot q_2(t) \cdots q_n(t) \tag{2}$$

dove H rappresenta i valori degli house events associato alla configurazione
le *q(t)* rappresentano i valori di indisponibilità che i basic events assumono al tempo *t*

L'equazione per il calcolo della probabilità del top event risulta essere:

$$TE(t) = \bigcup_i MCS_i(t) \tag{3}$$

Si distinguono due usi separati della matrice degli house events: Il caso di sinistra in figura 1 serve per modellare la messa in fuori servizio del componente mentre il caso a destra serve per modellare più modi di funzionamento del componente o sistema.

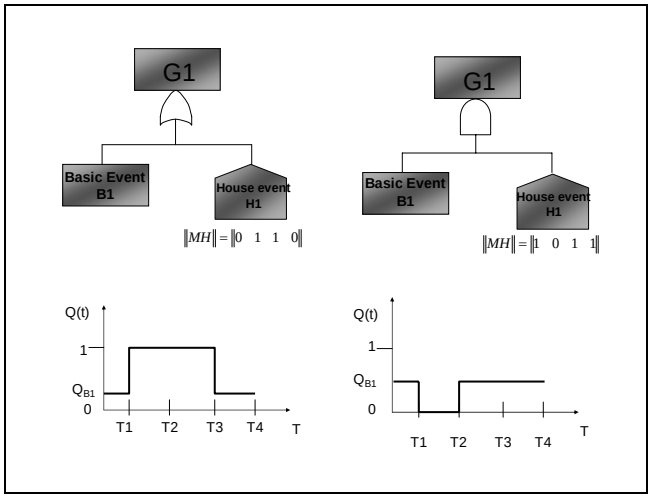

Figura 1. Schema logico di funzionamento degli house events[8].

L'house event H1 sotto una porta logica OR simula la messa in fuori servizio del componente perché quando l'house event è settato ad 1 significa che il valore G1 è sempre il valore unitario, mentre se l'house event è settato zero il valore dipende dal valore del basic event.

L'altra figura mostra che quando un house event è settato a zero G1 è sempre uguale a zero, così un house event sotto la porta AND simula i differenti modi di lavorare di un componente.

3.2 Modello per basic event

Molti modelli temporali per basic event possono trovarsi in letteratura e la scelta di quello giusto dipende dalle seguenti considerazioni:

- Tipologia e precisione dei dati;
- Grado di confidenza dell'analista con i dati e con il modello;
- Livello di dettaglio dell'analisi richiesto;
- Proposito del modello.

I valori dell'indisponibilità come funzione del tempo che sono stati presi in considerazione sono quelli di un componente testato periodicamente. Il modello tiene conto della possibilità di effettuare una manutenzione differita (Staggered maintenance) [10]:

$$\begin{aligned}
&\text{Per } 0 < t < (T_p - T_t f_0); && Q_{Bj}(t) = q + 1 - e^{-\lambda t},\\
&\text{Per } (T_p - T_t f_0) < t < T_p; && Q_{Bj}(t) = 1,\\
&\text{Per } T_p < t < (T_i - T_t f_o - T_r + T_p); && Q_{Bj}(t) = q + 1 - e^{-\lambda(t - T_p)}\\
&\text{Per } (T_i - T_t f_o - T_r + T_p) < t < (T_i - T_t f_o + T_p); && Q_{Bj}(t) = q + 1 - e^{-\lambda T_i} + \left(e^{-\lambda T_i} - q\right)\left(q + 1 - e^{-\lambda(t - T_p)}\right)\\
&\text{Per } (T_i - T_t f_o + T_p) < t < (T_i); && Q_{Bj}(t) = 1
\end{aligned} \tag{4}$$

Con: $Q_{Bj}(t)$ indisponibilità al tempo t; *q* costante (solitamente si usa per tener conto del fallimento sull'interrutore che determina la partenza del componente in stand-by); T_I Intervallo di test; T_T tempo di durata della manutenzione preventiva; T_R tempo di riparazione; T_p tempo di prima manutenzione o time placement; λ rateo di fallimento; f_0 fattore di override (specifica la porzione del tempo T_T in cui il sistema risulta indisponibile).

La prima delle 4 risulta essere il modello del decadimento esponenziale dell'indisponibilità con il rateo di guasto λ costante. La seconda riporta il valore di indisponibilità certa e quindi unitaria che segue alla manutenzione preventiva. La quarta delle 4 tiene conto del fatto che il componente verrà riparato se trovato indisponibile durante la manutenzione: il primo addendo porta in conto la probabilità che il componente si possa rompere durante il periodo di disponibilità; il secondo addendo tiene conto del fatto che il sistema non si sia rotto durante il periodo di disponibilità e che quindi possa ricominciare il decadimento esponenziale dell'indisponibilità.

3. CASO DI STUDIO

Di seguito si riporta il comportamento dell'albero dei guasti su sistemi in serie ed in parallelo. Si considererà un treno costituito da una Valvola motorizzata, una Check Valve ed una Pompa con i rispettivi ratei di guasto dati dalla seguente tabella. La tabella riporta anche i valori delle variabili presenti nel modello per i basic event di cui al punto precedente.

Componente	*Tipo di fallimento*	*Rateo di guasto (eventi/ora)*	*Intervallo di Test*	*MTTR*	*Tempo di outage*
Valvola Motorizzata	Failure to open	$8.8 \times E^{-6}$	720	10	5
Pompa	Failure to start	$3 \times E^{-4}$	720	20	10
Check valve	Failure to open	$1.7 \times E^{-7}$	720	5	5

Tabella 1. Ratei di guasto

3.1 Componenti in serie

L'andamento temporale dell'indisponibilità nell'intervallo di test è dato dalla seguente figura:

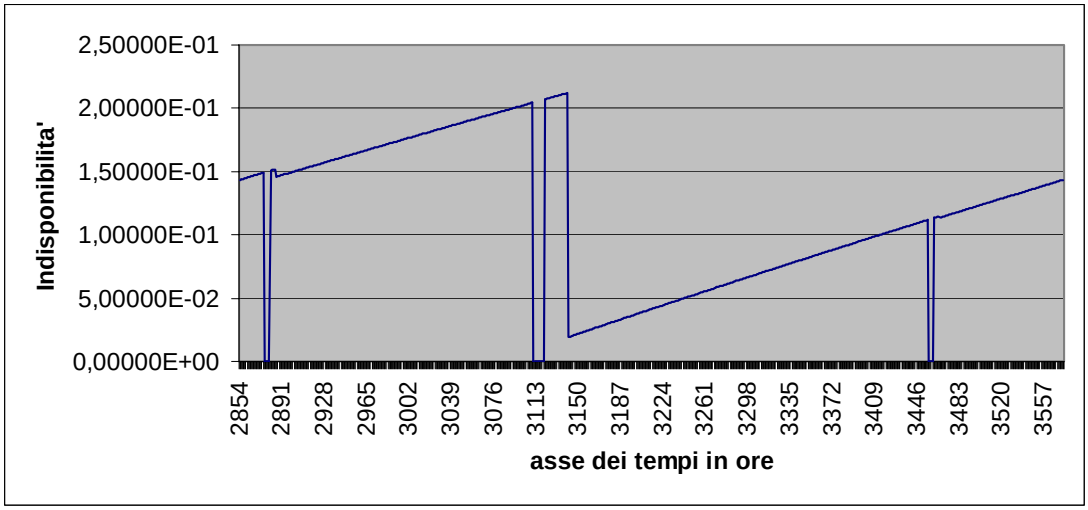

Figura 2. Andamento dell'inaffidabilità nel tempo

Gli istanti di tempo in cui il treno è in fuori servizio (indisponibilità unitaria) sono posti a zero per facilitare la lettura del grafico. Il primo decadimento risulta essere quello della valvola motorizzata, il

secondo quello della pompa ed il terzo quello della check valve. Per confrontare il metodo statico con quello dinamico occorre considerare la media temporale delle indisponibilità puntuali di figura 2 con il valore che si otterrebbe utilizzando metodi statici. Altro nodo da sciogliere è la scelta della tipologia di manutenzione sui componenti. La manutenzione può essere sequenziale o differita nell'intervallo di manutenzione. Se si utilizza la manutenzione differita occorre definire le tempistiche di manutenzione per i singoli componenti. (es. 0; 240; 580 con T_i di 720 ore). Per il confronto si è utilizzata il seguente formulismo che tiene conto dell'indisponibilità temporale dovuto alla manutenzione[11]:

$$Q_{mean} = q + \frac{1}{2}\lambda T_I + \frac{T_T f_0}{T_i} + (q + \lambda T_I)\frac{T_R}{T_I} \qquad (5)$$

La tabella seguente riporta i risultati ottenuti se si sceglie la metodologia di manutenzione differita con tempi [0; 240; 580]:

	Indisponibilità
Metodologia statica	$1.452 \cdot 10^{-1}$
Metodologia dinamica	$1.330 \cdot 10^{-1}$

Tabella 2. Confronto tra metodologia classica e dinamica

Il vantaggio della metodologia dinamica risiede nella possibilità di conoscere gli intervalli temporali in cui il sistema lavora con un'inaffidabilità più alta rispetto a quella ipotizzata utilizzando metodologie statiche. In figura 2 si può vedere come il treno si trova a lavorare per circa otto giorni (tra 3150 e 2971) in condizioni più sfavorevoli rispetto all'ipotizzato. Inoltre risultano agevoli le analisi di sensibilità dato che si dispongono dei valori puntuali dell'inaffidabilità. Si riporta di seguito il risultato ottenuto variando l'intervallo di manutenzione della pompa.

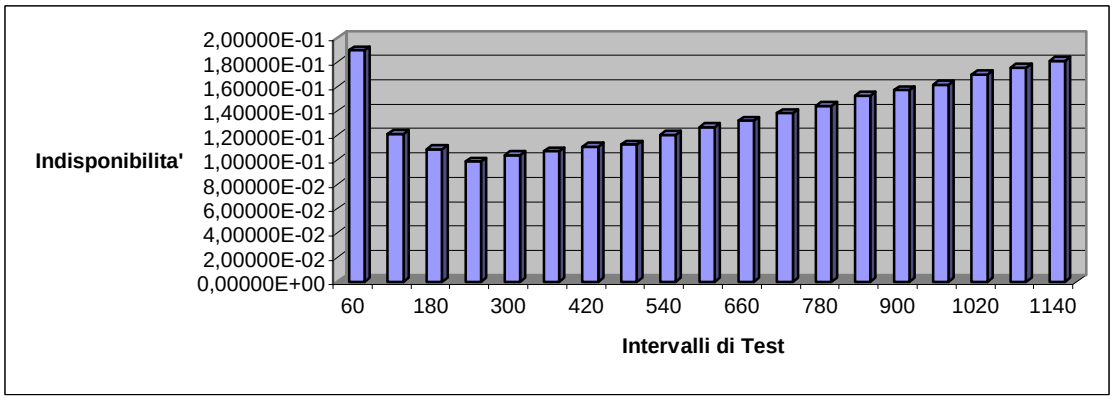

Figura 3. Indisponibilità della pompa al variare dell'intervallo di manutenzione

3.1 Sistemi in parallelo e fattore di copertura CF

Usualmente un sistema in parallelo viene concepito per quelle funzioni che si vogliono assicurare con un certo grado di affidabilità, soprattutto quando tale affidabilità non può essere raggiunta tramite un sistema singolo in serie, specie perché questo e' condizionato dall'affidabilità del componente peggiore.

Se si sceglie una strategia di test sequenziale si ha per entrambi i treni si ha che l'andamento dell'indisponibilità risulta essere:

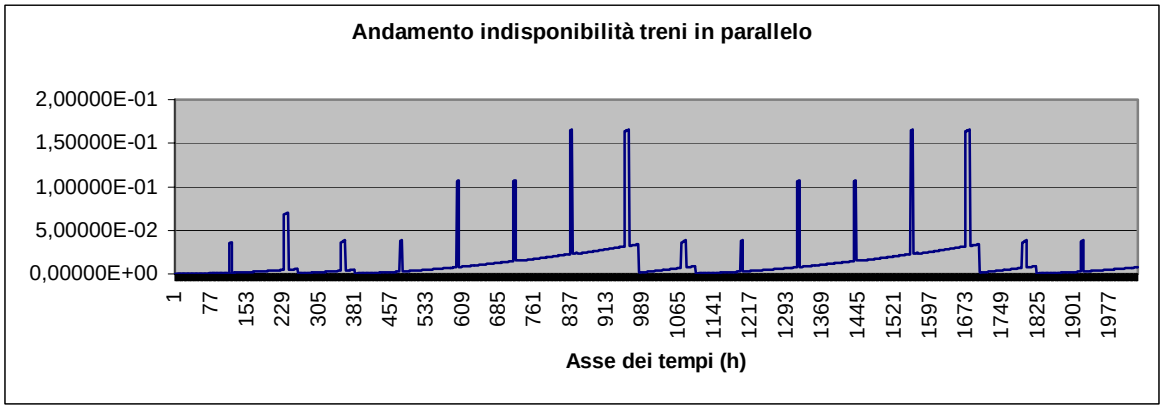

Figura 4. Andamento dell'indisponibilità per parallelo in manutenzione differita

Si è rilevato come l'indisponibilità media per una serie varia al variare delle tempistiche di manutenzione dei vari componenti. Prendiamo due treni identici in parallelo ma con la seguente tempistica di manutenzione [720 240 480] e [120 360 600], che si suppone essere la tempistica che ottimizza l'indisponibilità del singolo treno, e che quindi l'indisponibilità media di entrambi i treni sia 1.3304 E^{-1}. Ci si aspetta un'indisponibilità media di 1.77 E^{-2}. Si ha invece un valore minore di circa 2.6 E^{-4} a causa di una migliore distribuzione dei due treni nel tempo. Sfasando ulteriormente i tempi si trova che il valore dell'indisponibilità del sistema diminuisce progressivamente. Il problema che ci si è posti è stato quindi quello di ricercare quelle tempistiche di manutenzione che minimizzano il valore di picco dell'indisponibilità e che forniscano il valore mediato nel tempo più basso.

A tal proposito si è sviluppato la metodologia del fattore di copertura che permette un'ottimizzazione delle tempistiche di manutenzione evitando così il ricorso a metodologie euristiche per la risoluzione di problemi analoghi[9] .

3.1 Metodo del fattore di copertura

Un metodo molto utile per la scelta della giusta strategia di test (la strategia di test che minimizza l'indisponibilità media) può essere il metodo del fattore di copertura [12] di seguito riportato.

Questo metodo consiste nella minimizzazione di un solo parametro (i.e. il fattore di copertura) per l'intero sistema invece che la ricerca dei tempi di primo test per tutti i componenti il sistema attraverso algoritmi complessi. Esso si adatta ad ogni sistema che consiste di parti ridondanti.

Il concetto base risiede nel fatto che lungo il periodo di tempo preso in considerazione, i treni in parallelo dovrebbero essere manutenuti in modo tale che le rispettive curve di indisponibilità caratteristiche si vadano a disporsi uniformemente nel tempo, senza addensare i propri picchi di disponibilità/indisponibilità in specifici periodi di tempo, determinando quindi elevata affidabilità in taluni momenti ed eccessiva inaffidabilità in altri.

Per ogni treno ridondante si può trovare l'insieme $G_{i,j}$ dove i e' l'indice per ogni singolo treno, mentre j, e' il picco progressivo sulla curva funzione di disponibilità (zona inferiore del picco nel caso si disponesse dell'indisponibilità).

L'insieme dei valori $g_{i,j} \in G_{i,j}$ sarà formato da tutti gli istanti di tempo t che soddisfano la seguente equazione nel periodo considerato e che quindi hanno associato un valore dell'indisponibilità basso:

$$t = g_{i,j} \in G_{i,j} \Rightarrow U(t) - C \cdot U_M < 0 \qquad (6)$$

dove U(t) e' il valore dell'indisponibilità
U_M e' la media nel periodo di funzionamento del sistema
C e' parametro di ampiezza

Il valore del parametro di ampiezza viene stabilito di volta in volta dall'analista per individuare intervalli temporali più o meno stringenti dal punto di vista dell'affidabilità. Maggiore e' il valore di C, maggiore sarà il numero degli elementi nell'insieme $G_{i,j}$ (e quindi criterio meno stringente). Unendo le zone $G_{i,j}$ si ottiene un insieme di tempo G_i che considera il tempo in cui le performance del treno di indice *i* dal punto di vista del rischio risulta essere maggiore del livello di sicurezza posto dall'analista tramite la scelta del fattore C. Per

quanto riguarda il valore di C occorre dire che non potrà mai assumere valori tali da avere:

$$U_{Max} < C \cdot U_M < U_{Min} \tag{7}$$

Il fattore di copertura (CF) e' dato dalla seguente formula:

$$CF = \frac{\bigcup G_i}{T_t} \cdot 100 \tag{8}$$

Dove T_t rappresenta il tempo preso in considerazione e G_i e' ottenuto dall'unione dei $G_{i,j}$. Il valore del fattore di copertura, e' una percentuale indicante la frazione del tempo totale in cui almeno uno dei due treni lavora nelle condizioni di sicurezza migliore; mentre il fattore di debolezza che e' dato da:

$$FD = \overline{CF} \tag{9}$$

dove FD è il complemento a 100 di CF, rappresenta la frazione di tempo in cui il sistema lavora in condizioni minori dal punto di vista dell'affidabilità. Per un sistema formato da treni in parallelo, il fine e' di massimizzare l'indice del fattore di copertura per un assegnato parametro di ampiezza C (o minimizzare quello di debolezza). In questo modo si può trovare la configurazione che sfrutta al meglio le evoluzioni temporali per la disponibilità dei due treni.

3.1 Ottimizzazione di due sistemi in parallelo

Si parte da una situazione (Caso 2) in cui i due treni hanno i seguenti tempi di primo test per i componenti costituenti i treni: P_1 [720 240 480], P_2 [120 360 600]. Si noti il secondo vettore riportante i tempi di primo test è stato ottenuto sfasando il primo di 120 h. Si sceglie poi il parametro di ampiezza C (es. C=1). Ottengo il valore per il fattore di debolezza di *37.12962963.* Per prova sfaso ulteriormente il secondo treno di ulteriori 60 ore ottenendo per il secondo treno il valore P_2 di [180 420 660] procedendo con il calcolo del fattore di debolezza ottengo *29.21296296.* Il fattore di debolezza minore mi indica che la configurazione seconda dei treni è migliore della prima trovata. Iterando il procedimento arrivo ad uno sfasamento di circa 360 h ottenendo un fattore di debolezza *12.14* (Caso 4). Sfasando ulteriormente il secondo treno rispetto al primo, arrivando quindi alla configurazione [370 610 130] che differisce di solo 10 ore rispetto alla precedente, ottengo un valore del fattore di debolezza di *15.27* quindi maggiorato. Si può quindi concludere che il valore ottimo si troverà compreso tra lo sfasamento di 360 h (incluso) e 370 H (escluso).

La prima delle successive tabelle mostra l'andamento del fattore di debolezza per le diverse configurazioni presentate con differenti valori di C, mentre la seconda delle tabelle presentate mostra i valori delle grandezze caratteristiche nelle varie configurazione. Si noti come il caso 1 che corrisponde ad una manutenzione sequenziale dei componenti del primo e del secondo treno risulti essere la peggiore da un punto di vista della sicurezza tra quelle possibili.

Parametro di ampiezza	**Caso 1 (manutenzione sequenziale)**	**Caso 2**	**Caso 3**	**Caso4**
	FD	FD	FD	FD
1.2	35.76388889	26.86342593	19.09722222	1.33
1.1	40.90277778	31.57407407	23.80787037	2.29
1	45.90277778	37.12962963	29.21296296	12.14
0.9	50.90277778	42.12962963	33.66898148	21.72
0.8	55.90277778	47.12962963	38.65740741	31.29
0.7	60.76388889	51.44675926	43.66898148	39.69

Tabella 3. Fattore di debolezza andamento in varie configurazioni

Caso 1 (manutenzione sequenziale)	Tempistiche di primo test			Indisponibilità	Valore massimo
	Motor valve	Pompa	Check valve		
Treno 1	110	130	100	$1.74324\ E^{-2}$	$1.86988\ E^{-1}$
Treno 2	165	185	155		
Caso2					
Treno 1	720	240	480	$1.64336\ E^{-2}$	$1.65846\ E^{-1}$
Treno 2	120	360	600		
Caso3					
Treno 1	720	240	480	$1.55486\ E^{-2}$	$1.81248\ E^{-1}$
Treno 2	180	420	660		
Caso 4					
Treno 1	720	240	480	$1.48927\ E^{-2}$	$1.65846\ E^{-1}$
Treno 2	360	600	120		

Tabella 4. Tempistiche di manutenzione e valori di indisponibilità media e massima

Si vede come la configurazione quattro (sfasamento di 360 h) sia quella ad indisponibilità minore, si è inoltre rilevato che è anche la configurazione che presenta un valore di picco dell'indisponibilità minore (picco che si presenta quando uno dei due treni viene a trovarsi in manutenzione) e varianza minore.

3. Conclusioni

Il metodo discusso, permette di effettuare valutazioni sulla base delle informazioni contenute nella PSA in una maniera relativamente semplice. Possono essere analizzati sistemi che hanno vari modi di funzionamento.

Paragonando questo metodo al metodo classico delle catene di Markov sono state rilevate le seguenti differenze:

- maggiore facilità nel gestire gli aspetti matematici;
- maggiore flessibilità dei modelli;
- possibilità di modellare fallimenti mutuamente indipendenti la cui probabilità può anche non essere casuale;
- minore tempo di elaborazione e valutazione;
- maggiore facilità nella comprensione e gestione del metodo;
- minor precisione nei valori di output.

Riguardo questo ultimo punto, il metodo risulta comunque adatto nel caso che si debba trovare una valutazione approssimativa. L'errore dovuto alla minore precisione matematica, è parzialmente compensato dalla maggiore flessibilità nell'introdurre meno approssimazione durante l'attività di modellizzazione[13].

La facilità di comprensione del metodo, lo rende facilmente disponibile agli operatori, perché i principi su cui è basato sono ampiamente conosciuti.

La possibilità di seguire il trend della disponibilità ed indisponibilità nel tempo permette di ottenere un'immediata visuale dell'impatto che l'outage ha in un sistema complesso quando si verifica in un suo componente elementare.

Il modello risulta molto utile per eventuali algoritmi di ottimizzazione [9,14,15,16].

Data la tipologia di output come stringa di valori di indisponibilità nel tempo, le analisi di sensibilità risultano notevolmente agevolate.

Riguardo all'ottimizzazione di treni in parallelo risulta importante il fattore di copertura. Infatti il processo di ottimizzazione si può suddividere in due passi: si può ottenere una ottimizzazione ad un primo livello usando un appropriato tempo di placement, differenti strategie di test, differenti tempi di riparazione ecc. Il secondo livello consiste in una appropriata distribuzione dei picchi di indisponibilità lungo il tempo.

La possibilità di ottenere una funzione di disponibilità dipendente dal tempo permette di notare che la

mancanza di una adeguata distribuzione temporale dei picchi, potrebbe condurre l'analista a valori sotto o sovrastimati della probabilità di fallimento del sistema specie se questi utilizza il valore mediato. Dal momento che i valori della disponibilità sono di solito forniti come valori medi temporali, questi sbilanciamenti sono nascosti all'interno dei valori medi.

Un valore elevato del fattore di copertura implica un minor valore di varianza e quindi un dato medio maggiormente affidabile.

Le principali caratteristiche di questo tipo di approccio sono:

- Veloce valutazione degli incrementi di indisponibilità dovuti ad un outage;
- Possibilità di ottimizzare le performance del sistema attraverso una analisi di sensibilità di tutte le variabili presenti nel modello scelto per il basic event;
- Possibilità di ottimizzare la strategia di test scelta;
- Per sistemi in parallelo, la possibilità di compiere uno shift temporale dei treni affinché i valori massimi o minimi associati si distribuiscano lungo il tempo preso in considerazione;
- Il metodo risulta utilizzabile in un eventuale event tree dinamico per ottenere il controllo sui principali scenari incidentali ipotizzati;
- Quando si verifica un outage non previsto, la flessibilità del processo decisionale è incrementata.

I modelli statici per il calcolo dell'indisponibilità per componenti in stand-by soggetti a test e manutenzioni sono stati incrementati tenendo conto dell'effettiva tempistica della loro vita temporale. Si rileva infine che il metodo dinamico è totalmente equivalente al metodo classico ai fini dell'individuazione del valore medio dato che i valori del primo risultano identici a quelli che si troverebbero in una analisi classica.

Il fattore di copertura, consente di ottimizzare la tempistica di manutenzione su sistemi in parallelo, se i sistemi sono identici, i tempi di primo test sono ottenuti dalla formula:

$$\Delta S = \frac{T_I}{N} \qquad \text{e} \qquad \begin{cases} T_1 = 0 \\ \Delta T_2 = \Delta S \\ . \\ . \\ \Delta T_N = (n-1)\Delta S \end{cases} \tag{10}$$

Con ΔS il tempo tra lo sfasamento tra un treno e il successivo, N il numero dei treni presenti nel parallelo; T_I il test interval; ΔT_n lo sfasamento tra il primo treno ed il treno n.

Nel caso i treni in parallelo non fossero identici (e.g sistemi di iniezione a bassa ed alta pressione) occorre procedere con un processo iterativo come quello mostrato precedentemente. L'albero dei guasti dinamico potrebbe essere utilizzato per simulare anche sequenze incidentali e transitori. Nella figura seguente è riportato l'andamento dell'affidabilità di un sistema in cui un evento incidentale o un'anomalia di funzionamento va ad incidere sull'affidabilità di uno dei componenti alterandone la prestazione d' aspettata.

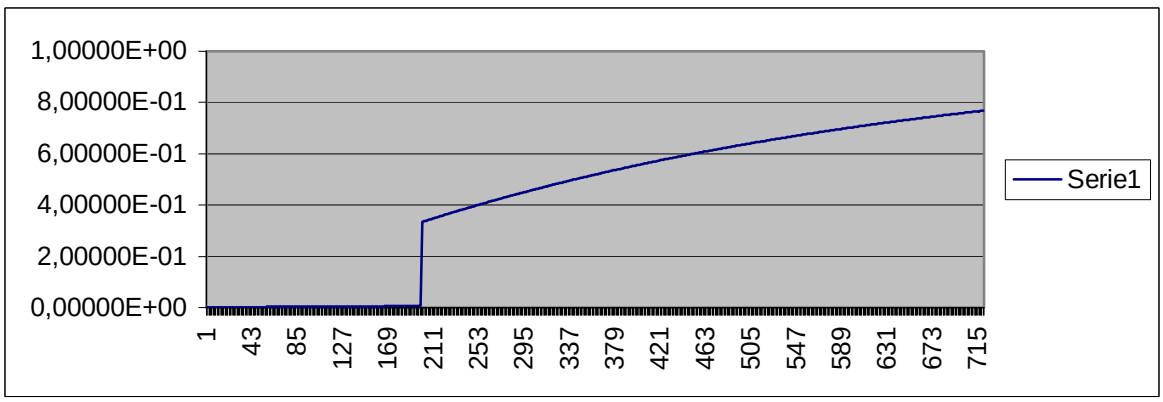

Figura 5. Transitorio di affidabilità per un evento incidentale

Il valore dell'indisponibilità dei basic event, va sostituito con la probabilità che un componente si rompa in un istante ben definito. La probabilità che un componente si rompa tra l'istante *t* e l'istante *t+dt* è data dalla [17]:

$$f(t)dt = \lambda(t)dt\left[1 - Q(t)\right] \tag{11}$$

dove

$f(t)dt$ è la probabilità di fallimento nell'intorno dt di t

$\lambda(t)dt$ è la probabilità di nell'intorno dt di t dato che il componente è sopravvissuto sino all'istante t

1-Q(t) la probabilità che il componente sia sopravvissuto sino al tempo t

Se si conoscono gli andamenti della $\lambda(t)$, si può risalire alla f(t) e quindi si può utilizzare il metodo del fattore di copertura per individuare gli istanti temporali in cui il sistema potrebbe essere soggetto a rotture. Il fattore di copertura assume quindi la funzione di strumento in grado di coadiuvare l'operatore nella scelta del momento opportuno dove fare eseguire una manutenzione o riparazione non programma senza compromettere la sicurezza dell'impianto evitandone la fermata e quindi una perdita da un punto di vista economico.

Se invece si conoscono le influenze che i parametri di processo (pressioni, temperature, ecc) hanno sui ratei di guasto dei componenti fisici dei sistemi si può facilmente utilizzare l'albero dei guasti dinamico non come mezzo per ottimizzare i sistemi bensì strumento per monitorare il transitorio incidentale.

L'albero dei guasti dinamico, si presenta quindi come un valido strumento alternativo ai metodi classici.

4. BIBLIOGRAFIA

[1] E.Borgonovo, G.E. Apostolakis, A new importance measure for risk informed decision making. Reliab Engng Syst Saf 2001; 72 193-212;

[2] Revision to 10CFR 50.65 The maintenance rule, 1999 utility working conference, August 11, 1999;

[3] Dezfuli H. Modarres M. Meyer J., Application of Reveal_W to risk-based configuration control, Reliab Engng Syst Saf 1994; 44 243-263

[4] J.K.Vaurio, Extensions of the uncertainty quantification of common cause failure rates, Reliability Engineering and System Safety, 78 (2002) 63-69

[5] Ravan Manian, Joanne Bechta Dugan, Combining Various Techniques for Dynamic Fault Tree Analysis of Computer Systems, 97RM-047 pages 1-7,1997

[6] M.Cumo, Impianti nucleari 1, UTET 1996

[7] Roberts NH, Vaseley WE, Haasl DF, Goldberg FF. Fault tree Hand-book, NUREG-0492. Washington: US NRC, 198;

[8] Marko Cepin, Borut Mavko, A Dynamic fault tree. Reliab Engng Syst Saf 2002; 75(1):83-91;

[9] M.Cepin, Optimization of safety equipment outages improves safety, Reliability Engineering and System Safety, 77 (2002) 71-80.

[10] Cepin M, Mavko B, Probabilistic safety assessment improves surveillance requirement in technical specifications. Reliab Engng Syst Saf 1997; 56 69-77

[11] Vaurio, J. K. Optimization of test and maintenance intervals based on risk and cost. Reliab Engng Syst Saf 1995; 49 23-36;

[12] Caira M, Gambellini A, Method to optimize test and maintenance activity, PSAM-ESREL 04

[13] Gambellini A, Baratta AJ, Caira M. The Evaluation of Dynamic Fault Tree Analysis to Maintenance Activities on a Simplified ECCS System, International Conference on Nuclear Power Plant 03.

[14] Martorell S. Sanchez A. Carlos S. Serrandel V. Simultaneous and multi-criteria optimization of TS requirements and maintenance at NPPs; Annals of Nuclear Energy 2002; 29 147-168;

[15] Martorell S,Carlos S, SerrandelV, Constrained optimization of test intervals using a stedy-state generic algorithm, Reliab Engng Syst Saf 2000; 67: 215-32

[16] H.Schabe, A new approach to optimal replacement times for complex systems, Microelectron.Reliab, vol 35 No. 8 pp 1125-1130

[17] McCormick, Norman J., Reliability and Risk Analysis Methods and Nuclear Power Applications. Academic Press, INC;