# UNRELMC 1.0: UN CODICE MONTE CARLO PER L'ANALISI DELL' AFFIDABILITA' STATICA O DINAMICA DI UN SISTEMA

M. Marseguerra, E. Zio
Dipartimento di Ingegneria Nucleare -- Politecnico di Milano
Via Ponzio 34/3, Milano 20133
marzio.marseguerra@polimi.it

## SOMMARIO

Nel presente lavoro vengono illustrate le potenzialita' del codice UNRELMC 1.0, un codice fortran per l'analisi Monte Carlo dell'affidabilita' e disponibilita' di sistemi complessi sviluppato presso il Dipartimento di Ingegneria Nucleare del Politecnico di Milano. Particolare cura e' stata rivolta alla flessibililita' del codice che consente cosi' di tener conto di molteplici tra gli aspetti rilevanti che si incontrano nelle analisi di sistemi reali. Questi aspetti dell'analisi possono essere gestiti efficacemente nel contesto della simulazione Monte Carlo, la cui struttura consente di considerare in maniera relativamente semplice le dipendenze tra componenti, i guasti su domanda, gli effetti dell'usura etc.

Il codice prevede l'utilizzo di tecniche di riduzione della varianza per aumentare l'efficacia del calcolo nel caso di sistemi altamente affidabili. Infine, il codice consente di introdurre eventuali dipendenze dall'evoluzione fisica delle variabili di processo per quei sistemi in cui la dinamica giuoca un ruolo importante.

## 1. INTRODUZIONE

L'analisi affidabilistica di un sistema consiste essenzialmente nel calcolare le distribuzioni di probabilita' relative al verificarsi di predefiniti eventi indesiderati, tenendo conto delle incertezze presenti. La composizione del sistema e le sue procedure di operazione e manutenzione possono complicare significativamente l'analisi, introducendo elementi di dipendenza, nonlinearita' e dinamica. Questi aspetti dell'analisi possono essere gestiti efficacemente nel contesto della simulazione Monte Carlo, la cui struttura consente di considerare in maniera relativamente semplice le dipendenze tra componenti, i guasti su domanda, gli effetti dell'usura etc. [1].

Nel presente lavoro vengono illustrate le potenzialita' del codice UNRELMC 1.0, un codice fortran per l'analisi Monte Carlo dell'affidabilita' e disponibilita' di sistemi complessi sviluppato presso il Dipartimento di Ingegneria Nucleare del Politecnico di Milano. Particolare cura e' stata rivolta alla flessibililita' del codice che consente cosi' di tener conto di molteplici tra gli aspetti rilevanti che si incontrano nelle analisi di sistemi reali.

Il codice prevede l'utilizzo di tecniche di riduzione della varianza per aumentare l'efficacia del calcolo nel caso di sistemi altamente affidabili. Per tali sistemi, la probabilita' di un incidente dovuto a un guasto singolo e' assai modesta; in aggiunta, le procedure di intervento e riparazione dei guasti dei componenti vengono tipicamente completate in tempi brevi, relativamente ai tempi di rottura dei singoli componenti, cosicche' il verificarsi di guasti indipendenti multipli e' assai improbabile. Corrispondentemente in un calcolo Monte Carlo analogico (o diretto), la maggior parte delle storie simulate non porterebbe alcuna informazione utile per la stima della probabilita' del guasto di sistema. Da cio' deriva la necessita' di introdurre efficaci tecniche di riduzione della varianza che "forzino" il sistema a rompersi, consentendo cosi' di fare una stima statisticamente significativa delle quantita' di interesse [2].

Infine, il codice consente di introdurre eventuali dipendenze dall'evoluzione fisica delle variabili di processo per quei sistemi in cui la dinamica giuoca un ruolo importante. E' noto, infatti, che i metodi convenzionali per l'analisi di affidabilita' sono considerati in generale statici in quanto si focalizzano principalmente sugli aspetti stocastici dell'analisi, mentre non sono in grado di tener conto in maniera dettagliata dell'evoluzione fisica dell'impianto. D'altra parte, gli impianti reali sono in generale caratterizzati da forti interazioni tra caratteristiche hardware ed evoluzione fisica. In molti casi, per esempio, le proprieta' stocastiche di transizione dei componenti di un sistema dipendono dalle condizioni in cui essi si trovano ad operare, e cioe' dai valori assunti da certe variabili di processo quali la temperatura, la pressione etc. Un altro aspetto dinamico tipico degli impianti reali e' la presenza di sistemi di controllo/protezione il cui funzionamento e' strettamente legato all'evoluzione fisica e puo' influenzare l'analisi con fenomeni tipici quali la *failure on demand*. In situazioni in cui l'impianto in esame presenti forti caratteristiche di dinamica, quali

quelle qui accennate, le analisi classiche di affidabilita' sembrano mostrare delle lacune. Per questo motivo, negli ultimi anni si e' avviato un filone di ricerca per lo sviluppo di un approccio dinamico all'analisi probabilistica di rischio [3].

## 2. METODO MONTE CARLO PER L'ANALISI DI AFFIDABILITA' E DISPONIBILITA'

L'affidabilita' di un sistema puo' essere calcolata in linea di principio con metodi analitici [4-5] ma l'analisi diventa eccessivamente onerosa e al limite impossibile al crescere della complessita' dei sistemi. I metodi deterministici per la valutazione quantitativa dell'affidabilita' di un sistema sono inoltre soggetti a pesanti limitazioni, quali ad esempio quelle derivanti dall'ipotesi, difficilmente rimovibile, che i singoli componenti si comportino indipendentemente gli uni dagli altri. In un calcolo Monte Carlo e' invece possibile adottare un modello piu' realistico, introducendo una vasta gamma di condizioni di dipendenza e correlazioni tra i componenti [6]. La tecnica Monte Carlo ha il vantaggio di essere intuitiva, nel senso che consente di seguire individualmente un gran numero di possibili storie del sistema. Poiche' il metodo Monte Carlo implica la generazione di un grande numero di storie, si comprende come la sua efficacia venga a dipendere da parametri esterni quali il tempo di calcolo e la memoria disponibile, ma va osservato che una simulazione di questo tipo richiede, diversamente da un'analisi svolta secondo metodi deterministici, una minore disponibilita' di memoria della macchina.

Consideriamo un sistema ad $N_C$ componenti ed indichiamo con $\boldsymbol{B}=(b_1, b_2, ..., b_{NC})$ lo stato del sistema, $b_i$ essendo lo stato del componente *i*-esimo. Nello spazio delle fasi, il sistema viene rappresentato da un punto $P=(\boldsymbol{B},t)$. La simulazione Monte Carlo consiste nell'eseguire al calcolatore un gran numero di "storie di vita" del sistema. Ogni storia da' luogo ad una catena di punti di collisione $(P_1 , P_2, ..., P_n)$ che si protrae nel tempo finche' il sistema entra in uno stato assorbente da cui non ha possibilita' di uscire, o finche' non sia raggiunto il tempo di missione. Il cammino casuale (*random walk*) $(P_1 , P_2, ..., P_n )$ che ne deriva rappresenta la storia campionata. Date *N* storie del sistema, e' possibile risalire alle quantita' di interesse relative al comportamento affidabilistico del sistema. Per esempio, definendo per la *j*-esima storia una variabile casuale $h_j(P_1 , P_2, ..., P_n)$ che assume valore 1 se il sistema fallisce prima del tempo di missione e 0 diversamente, la quantita'

$$u = \frac{1}{N}\sum_{j=1}^{N}\eta_j \qquad (1)$$

e' una stima *unbiased* dell'inaffidabilita', cioe' quando $N \to \infty$, *u* converge alla inaffidabilita' del sistema.

Le equazioni che governano le transizioni di sistema vengono costruite a partire da due probabilita': la densita' di probabilita' condizionale $f(t|t',k')$ che il sistema compia una transizione al tempo *t* supposto che sia nello stato *k'* al tempo *t'*, e la probabilita' condizionale $q(k|k')$ che l'effetto della transizione sia che il sistema entri nello stato *k*, sapendo che lo stato prima della transizione era *k'*.

Nel codice UNRELMC1.0 il modello base dei tempi di transizione dei componenti e' quello esponenziale e indichiamo con $\lambda^i_{j\to k}$ il rateo di transizione dell' *i*-esimo componente dallo stato *j* allo stato $k \neq j$. Il rateo di transizione del sistema in uscita dallo stato *k'* , in corrispondenza del quale il componente *i*-esimo sia nello stato *l'*, diventa:

$$\gamma_{k'} = \sum_{i=1}^{NC}\sum_{j=1}^{N_s^i}\lambda^i_{l'\to j} \qquad (2)$$

ove $N^i_S$ e' il numero di stati possibili del componente *i* e $\lambda^i_{j\to j} = 0$.

Per campionare gli intervalli *Dt* tra le transizioni si sfrutta il metodo della trasformata inversa [7]: un numero casuale $r_1$ viene campionato da una distribuzione uniforme in [0,1) e uguagliato alla distribuzione cumulativa:

$$r_1 = 1 - e^{-\gamma_{k'}\Delta t} \qquad (3)$$

che puo' essere facilmente risolta in termini di *Dt*.

Noto l'istante di transizione, occorre campionare lo stato risultante *k*. Nel codice cio' viene fatto in due fasi successive: prima si individua il componente che ha compiuto la transizione e poi il suo stato di arrivo. Per determinare il componente si procede nel seguente modo. Per ogni componente *i* nello stato *j*, si indica con

$\lambda^i_j = \sum_{k=1}^{N^j_c} \lambda^i_{j\to k}$ la densita' di probabilita' di una qualsiasi transizione uscente dallo stato *j*. Si estrae poi il numero casuale $r_2$ ed il componente *i* che subisce la transizione e' quello per cui:

$$\sum_{m=1}^{i-1} \lambda^m_{l'} \le \gamma_{k'} r_2 \le \sum_{m=1}^{i} \lambda^m_{l'} \tag{4}$$

Individuato il componente che ha subito la transizione e procedendo in maniera analoga si determina lo stato di arrivo *l* che e' quello per il quale si abbia:

$$\sum_{m=1}^{l-1} \lambda^i_{l'\to m} \le \lambda^i_{l'} r_2 \le \sum_{m=1}^{l} \lambda^i_{l'\to m} \tag{6}$$

A questo punto la transizione e' completamente definita: lo stato del sistema puo' venire aggiornato e il calcolo puo' continuare a partire dalle nuove condizioni.

## 3. TECNICHE DI RIDUZIONE DELLA VARIANZA

Nella pratica, la maggior parte dei problemi di affidabilita' di sistemi complessi e' costituita da problemi ad evento raro, caratterizzati da una probabilita' di insuccesso del sistema molto piccola. Questo significa che l'evento top si verifica molto raramente e, nella simulazione, la maggior parte delle storie non fornisce alcun contributo all'informazione richiesta. Cio' comporta la necessita' di eseguire un numero di prove molto elevato per poter ottenere risultati statistici significativi, con conseguente eccessivo impiego di tempo di calcolo. Questo aspetto rappresenta una grossa limitazione del metodo Monte Carlo e in questo ambito, diventa indispensabile introdurre tecniche di riduzione della varianza, simili a quelle gia' introdotte per i calcoli di trasporto delle particelle, e piu' in generale, per la valutazione di integrali multidimensionali [7], che consentano di aumentare l'efficienza del calcolo.

Nel codice UNRELMC 1.0 sono implementate due tecniche di forzatura. La prima, comunemente utilizzata, porta il nome di *tecnica delle transizioni a tempi forzati* [2] e consiste nel forzare il verificarsi di transizioni di qualsiasi tipo modificando opportunamente la densita' di probabilita' da cui viene campionato l'istante di successiva transizione. La densita' di probabilita' del tempo di transizione, originalmente di tipo esponenziale, $f(t) = \gamma_k \exp[-\gamma_k (t - t_i)]$, ove $t_i$ e' l'istante dell'ultima transizione, viene forzata in maniera da condizionare il successivo istante di transizione a verificarsi nel rimanente tempo, entro il tempo di missione, $T_M$, ed assume la forma

$$\tilde{f}(t) = \frac{\gamma_k \exp[-\gamma_k (t - t_i)]}{1 - \exp[-\gamma_k (T_M - t_i)]} \tag{7}$$

Al fine di mantenere *unbiased* le stime Monte Carlo, il peso della storia Monte Carlo, inizializzato ad uno, viene aggiornato in corrispondenza del verificarsi di ogni transizione moltiplicandolo per il fattore

$$\frac{f(t)}{\tilde{f}(t)} = 1 - \exp[-\gamma_k (T_M - t_i)] \tag{8}$$

La seconda tecnica di forzatura, nota con il nome di *metodo di forzatura verso i cut set piu' vicini*, e' stata originariamente proposta dagli autori [8] e consiste nell'incoraggiare il sistema a compiere quelle tra le transizioni possibili che portano il sistema ad avvicinarsi ad uno stato di cut set. A partire da una data configurazione del sistema, $\mathbf{B_i}$, si suddividono le possibili transizioni in tre classi, $\aleph$(riparazioni), $\Im$ (transizioni a stati di guasto di componente che fanno parte di un cut set), $\Re$ (transizioni residue). Tipicamente i ratei di riparazione (transizioni in $\aleph$) sono molto piu' grandi di quelli di guasto, mentre e' ovvio che per ottenere informazioni sull'inaffidabilita' del sistema dobbiamo favorire le transizioni in $\Im$. Per un

componente *i* nello stato *j*, si indicano con $\mu^i$, $\varphi^i$, $\lambda^i$, le densita' di probabilita' relative a transizioni contenute rispettivamente in $\aleph$, $\Im$ ed $\Re$ e siano $\Sigma_\mu$, $\Sigma_\varphi$, $\Sigma_\lambda$ le somme di tali densita' su tutti i componenti, con $\Sigma = \Sigma_\mu + \Sigma_\varphi + \Sigma_\lambda$. Senza entrare in eccessivi dettagli di trattazione, la forzatura consiste nell'espandere artificialmente la quota $\Sigma_\varphi$ di $\Sigma$, e ridurre corrispondentemente $\Sigma_\mu$ e $\Sigma_\lambda$ in maniera da mantenere $\Sigma$ costante. Inoltre, tra le gia' favorite transizioni di $\Im$ vengono preferite quelle che portano piu' rapidamente ad una configurazione di cut set, tenendo conto sia del numero di transizioni necessarie per passare dalla presente configurazione ad una di cut set che della probabilita' di tali transizioni. Analogamente a quanto detto per la prima tecnica di forzatura, il peso associato alla storia Monte Carlo va opportunamente aggiornato dopo il verificarsi di ogni transizione, al fine di ottenere una stima *unbiased* delle quantita' di interesse.

Come esempio di applicazione delle tecniche su esposte facciamo riferimento ad un sistema di letteratura [9] il cui albero dei guasti e' riportato in Figura 1. Il sistema e' composto da 10 componenti ognuno dei quali puo' trovarsi in uno stato di funzionamento o di guasto. I ratei di transizione per i diversi componenti sono riportati in Tabella 1. Dall'analisi dell' albero dei guasti si individuano tre configurazioni di cutset minimo di ordine 2 ed una di ordine 3. Tuttavia, poiche' il tempo di missione considerato di 1000 ore e' significativamente piu; grande dei tempi caratteristici di rottura dei componenti, il raggiungimento di una configurazione di cut set rappresenta un evento raro. Cio' e' confermato dai risultati ottenuti (Tabella 2) che mostrano come siano necessarie $10^7$ storie affinche' il Monte Carlo analogico (cioe' con le probabilita' naturali) produca una buona stima dell'inaffidabilita' del sistema. Al contrario, l'applicazione delle tecniche di forzatura di cui sopra ha consentito di ottenere stime piu' accurate in un minor tempo di calcolo, come evidenziato dal confronto delle rispettive cifre di merito $C_m = 1/s^2 t$ ove $s^2$ e' la varianza della stima di inaffidabilita' e *t* il tempo di calcolo in secondi.

| Componente i | $\lambda_i(10^{-5}\ h^{-1})$ | $\mu_i(h^{-1})$ |
|---|---|---|
| 1 | 0.26 | 0.042 |
| 2 | 0.26 | 0.042 |
| 3 | 0.26 | 0.042 |
| 4 | 3.5 | 0.17 |
| 5 | 3.5 | 0.17 |
| 6 | 3.5 | 0.17 |
| 7 | 0.5 | 0 |
| 8 | 0.5 | 0 |
| 9 | 0.8 | 0 |
| 10 | 0.8 | 0 |

Tabella 1. Ratei di transizione per l'esempio di Figura 1; $\lambda$ e $\mu$ indicano rispettivamente i ratei di guasto e di riparazione.

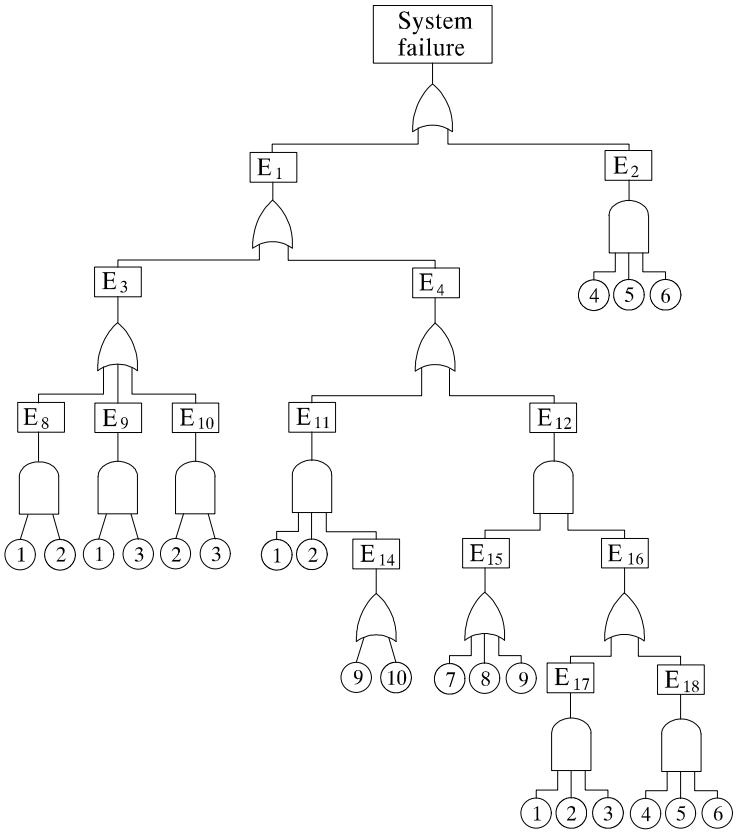


Figura 1. Albero dei guasti per il sistema di riferimento di letteratura [9] con tre cutsets di secondo ordine ed uno di terzo.

| | Analogico | Forzato |
|---|---|---|
| $N$ | $10^7$ | $10^4$ |
| $t$ | $2.19 \cdot 10^3$ | 25.8 |
| $U$ | $(12.0 \pm 2.7) \cdot 10^{-7}$ | $(9.38 \pm 0.31) \cdot 10^{-7}$ |
| $C_M$ | $6.35 \cdot 10^9$ | $4.08 \cdot 10^{13}$ |
| $n_{tr}$ | $(2.505 \pm 0.002) \cdot 10^{-1}$ | $(2.432 \pm 0.035) \cdot 10^{-1}$ |

$N$ = numero storie

$t$ = tempo di calcolo (s)

$U$ = inaffidabilità

$C_M$ = cifra di merito

$n_{tr}$ = numero medio di transizioni

Tabella 2. Stima di inaffidabilita' per l'esempio di Figura 1.

## 4. DIPENDENZE TRA COMPONENTI

Tipicamente i sistemi a rischio sono caratterizzati da un elevato numero di ridondanze che fanno si' che il maggior contributo al profilo di rischio dell'impianto sia dovuto ai guasti dipendenti. Il tener conto di tali dipendenze e', dunque, di fondamentale importanza per un'accurata stima del rischio associato ad un impianto.

Grazie alla sua flessibilita', lo schema Monte Carlo e' in grado di adottare modelli alquanto realistici di dipendenze e correlazioni tra componenti. Per tenere conto delle possibili dipendenze si tratta di specificare come vengono modificate le proprieta' statistiche di transizione dei singoli componenti del sistema.

Nel codice UNRELMC 1.0 e' previsto che dipendenze nel comportamento stocastico dei componenti possano derivare dalla configurazione congiunta di piu' componenti, detti *componenti-padri*. Quando si verifica la coincidenza di piu' componenti-padri in ben determinati stati le probabilita' di transizione di altri componenti, detti *componenti-figli*, vengono modificate. Si noti che la molteplicita' di componenti-padri introduce un elemento di non linearita' nel problema, venendo a mancare la sovrapposizione degli effetti. In termini pratici l'effetto delle dipendenze sulle probabilita' di transizione dei componenti consiste nell'alterare il tasso di transizione del corrispondente componente correlato in uscita da un suo stato ben definito. Nel modello qui proposto si suppone che, a causa di una determinata correlazione, i tassi di transizione del componente correlato, per transizioni che dallo stato j cui si riferisce la correlazione portano ad un qualunque altro suo stato *k*, vengano alterati tramite degli opportuni fattori $R_{j\,\mathbb{R}\,k}$ detti *fattori di correlazione*, che sono specifici della correlazione e che risultano essere diversi a seconda dello stato di arrivo *k*. Il fattore $R_{j\,\mathbb{R}\,k}$ e' maggiore di 1 se la correlazione e' tale da provocare un aumento della probabilita' di transizione dallo stato *j* allo stato *k* del componente correlato ed e' minore di 1 in caso contrario. Nel caso non siano noti tutti i fattori $R_{j\,\mathbb{R}\,k}$ , il modello proposto puo' essere semplificato supponendo che l'effetto della correlazione sia indipendente dello stato di arrivo *k*, cosicche' per tutti i valori $R_{j\,\mathbb{R}\,k}$ si adotta un unico fattore $R_j$. Nel caso generale, a titolo di esempio, consideriamo il sistema di figura 2 che deve consentire il passaggio di una data portata. Le due valvole di controllo abbiano la possibilita' di lavorare in 3 stati: 1) tutta aperta (nominale); 2) parzialmente aperta; 3) tutta chiusa. Ad un certo istante si verifica un malfunzionamento della valvola A che dallo stato nominale 1 passa nello stato 2 di parziale apertura. Poiche' la portata che fluisce nel dispositivo deve rimanere costante, si ha un sovraccarico della valvola B che deve lavorare in condizioni piu' gravose. Conseguentemente la sua probabilita' di passare nella condizione 2 di malfunzionamento viene moltiplicata per un fattore $R^B_{1\,\mathbb{R}\,2} > 1$ e quella di rottura totale (transizione allo stato 3) viene moltiplicata per un $R^B_{1\,\mathbb{R}\,3} > 1$. Se successivamente la valvola B passa effettivamente nello stato 2 la situazione diventa critica ed e' intuibile che cio' comporti un aumento della probabilita' di rottura totale della valvola A, tramite un fattore $R^A_{2\,\mathbb{R}\,3}$ . Se pero' si tiene conto dell'intervento umano nelle operazioni e' lecito pensare che la procedura di riparazione del dispositivo sia organizzata in modo tale che nella situazione descritta diventi molto probabile che la successiva transizione consista nella riparazione della valvola A, per cui la probabilita' che si verifichi tale transizione viene alterata tramite un coefficiente $R^A_{2\,\mathbb{R}\,1}$. Questo significa che quando la valvola B si trova nello stato 2 nasce una correlazione per effetto della quale viene aumentata la probabilita' della valvola A (componente-figlio) di andare dallo stato 2 di malfunzionamento allo stato 3 di guasto completo $R^A_{2\,\mathbb{R}\,3}$ a causa del peggioramento delle condizioni di lavoro, ma aumenta ancora di piu' la sua probabilita' di riparazione, cioe' transizione allo stato nominale 1, grazie all'intervento efficace delle procedure di riparazione ($R^A_{2\,\mathbb{R}\,1} > R^A_{2\,\mathbb{R}\,3}$ ).

Il caso descritto e' esemplificativo di situazioni in cui la configurazione del sistema influenza il comportamento dei suoi componenti in maniera diversa a seconda della transizione considerata. Quando si ha a che fare con correlazioni a componenti-padri multipli, e' necessario far riferimento ad una diversa simbologia. Il fattore che descrive una data correlazione tra uno o piu' componenti-padri ed una transizione di un componente-figlio viene indicato col simbolo:

$$R[(C_1,S_1 + C_2, S_2 + ... + C_n, S_n) \text{ Þ } (C_l, S_l \text{ ® } S^*_l)] \qquad (9)$$

dove,

- la prima parentesi tonda contiene la coppia numero-componente,numero-stato di tutti i componenti-padri;
- la freccia Þ indica la correlazione;
- nella seconda parentesi tonda $C_l$ indica il componente-figlio ed $S_l$ ® $S^*_l$ indica la sua transizione di stato.

Il modello proposto permette anche di tenere conto della possibilita' che piu' correlazioni possano agire contemporaneamente su uno stesso componente-figlio. Supponiamo di avere a che fare con un sistema a tre componenti, ognuno dei quali ha a disposizione tre stati e in cui il componente 3 nello stato 2 sia figlio di tre

correlazioni che hanno come componenti-padre rispettivamente il componente 1 nello stato 4, il componente 2 nello stato 5, e il componente 1 nello stato 4 congiuntamente al componente 2 nello stato 5. Siano:

– *R[(1, 4) Þ (3, 2 ® 1 )]* e *R[(1, 4) Þ (3, 2 ® 3 )]*
– *R[(2, 5) Þ (3, 2 ® 1 )]* e *R[(2, 5) Þ (3, 2 ® 3 )]*
– *R[(1,4+2, 5) Þ (3, 2 ® 1 )]* e *R[(1,4+2, 5) Þ (3, 2 ® 3 )]*

i rispettivi fattori di correlazione. Supponiamo che inizialmente il componente 1 sia nello stato 4, il componente 2 in uno stato che non sia il 5 e il componente 3 in un suo qualunque stato. Gia' a causa della configurazione iniziale i tassi di transizione del componente 3 nello stato 2 vengono alterati per i rispettivi fattori *R[(1, 4) Þ (3, 2 ® 1 )]* e *R[(1, 4) Þ (3, 2 ® 3 )]*.

Supponiamo ora che si verifichi la transizione che porta il componente 2 nello stato 5. Allora i tassi di transizione del componente 3, per transizioni uscenti dallo stato 2, vengono ulteriormente modificati per i fattori *R[(2, 5) Þ (3, 2 ® 1 )]* e *R[(2, 5) Þ (3, 2 ® 3 )]*, *R[(1,4+2, 5) Þ (3, 2 ® 1 )]* e *R[(1,4+2, 5) Þ (3, 2 ® 3 )]*.

Ad ogni transizione si rende dunque necessaria una operazione di *riassestamento* dei tassi di transizione, che ristabilisca la nuova situazione derivante dalle correlazioni che di volta in volta risultano attive. Nell'ipotesi implicita che il processo sia Markoviano, non ci deve essere un accumulo delle alterazioni dovute a correlazioni che si sono attivate in transizioni precedenti. Questo significa che se la transizione e' tale che nella nuova configurazione del sistema alcune correlazioni non hanno piu' effetto, i tassi di transizione da esse alterati devono essere depurati dall'effetto di tali correlazioni. Segue poi il rinnovamento di quei ratei di transizione che sono influenzati dalle correlazioni eventualmente attive nella nuova configurazione del sistema.

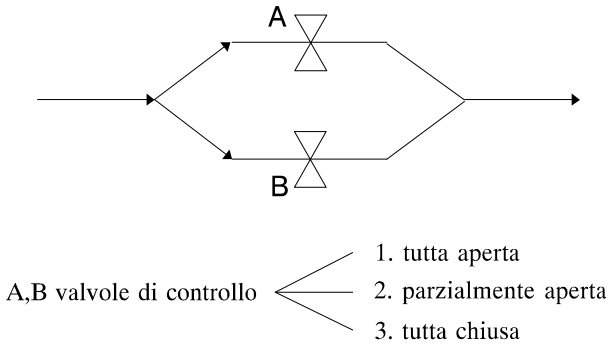


Figura 2. Esempio semplice di sistema con due valvole di controllo

## 5. STRATEGIE DI RIPARAZIONE

Il codice considera una strategia di riparazione alquanto realistica, secondo la quale ogni componente, in relazione alle sue caratteristiche, puo' necessitare di un preciso tipo di riparazione (es., idraulica. elettromeccanica, etc.). Per ogni tipologia di riparazione, il codice prevede la disponibilita' di un numero di squadre di intervento fissato in input dall'utente. Inoltre, a seconda del progetto del sistema e della criticita' dei componenti, l'utente puo' fissare un indice di *priorita'* che determina una "gerarchia" tra i componenti che necessitano dello stesso tipo di intervento di riparazione.

Quando un componente si guasta, se una squadra di riparazione e' disponibile la riparazione ha inizio. Se invece la squadra non e' disponibile, sul componente guastato viene inviata una squadra tra quelle gia' al lavoro, ma su componenti a priorita' inferiore, il cui funzionamento e' meno critico per il sistema. Il componente su cui tale squadra stava lavorando rimane in attesa.

La durata della riparazione e' considerata una variabile casuale di distribuzione assegnata. Quando un componente viene riparato, la squadra che ha terminato il lavoro inizia istantaneamente un intervento di riparazione sul componente a priorita' massima tra quelli che necessitano del tipo di riparazione a cui la squadra e' abilitata. Se non ci sono componenti da riparare, la squadra viene posta in stato di disponibilita'.

## 6. ANALISI DI AFFIDABILITA' PER SISTEMI DINAMICI

Come menzionato nell'introduzione, i metodi convenzionali per l'analisi di sicurezza con approccio probabilistico, PSA (dall'acronimo delle parole inglesi *Probabilistic Safety Assessment*), si basano principalmente sull'utilizzo dell'albero degli eventi ed albero dei guasti. Queste tecniche sono considerate in generale statiche in quanto non sono in grado di descrivere in maniera dettagliata l'evoluzione fisica dell'impianto.

D'altra parte, gli impianti reali sono in generale caratterizzati da forti interazioni tra caratteristiche hardware ed evoluzione fisica. In molti casi, per esempio, le proprieta' stocastiche di transizione dei componenti di un sistema dipendono dalle condizioni in cui essi si trovano ad operare, e cioe' dai valori assunti da certe variabili di processo quali la temperatura, la pressione etc. Un altro aspetto dinamico tipico degli impianti reali e' la presenza di sistemi di controllo/protezione il cui funzionamento e' strettamente legato all'evoluzione fisica e puo' influenzare l'analisi con fenomeni tipici quali la *failure on demand*. In situazioni in cui l'impianto in esame presenti forti caratteristiche di dinamica, quali quelle qui accennate, le analisi classiche di affidabilita' sembrano mostrare delle lacune. Per questo motivo, negli ultimi anni si e' avviato un filone di ricerca per lo sviluppo di un approccio dinamico all'analisi probabilistica di rischio.

Nell' approccio dinamico, un certo numero di stati $N_S^j$ e' possibile per il *j*-esimo componente. Questi stati si differenziano in *stati di guasto* e *stati di funzionamento*: se il componente e' in stato di guasto, il Sistema di Controllo non puo' intervenire sul componente; viceversa, se un componente e' in uno stato di funzionamento, esso puo' cambiare stato su richiesta del Sistema di Controllo.

Ogni componente e' poi caratterizzato da una *uscita* o *erogazione* (ad es., per una pompa, la portata). Gli stati di funzionamento e di guasto si differenziano ulteriormente in relazione al valore che assume la erogazione (ad es., 50%, 75% ...). Per ogni stato deve essere introdotto dall' utente il valore della variabile in uscita. Le transizioni verso uno stato di guasto possono solo essere di tipo stocastico; viceversa, quelle verso gli stati di funzionamento possono essere sia di tipo deterministico -quando dettate dal Sistema di Controllo - che stocastico (riparazioni). Vengono definiti uno stato nominale, introdotto dall' utente verso cui il componente viene riportato in caso di riparazione, ed uno stato iniziale, in cui si trova il componente all' inizio di ogni storia.

Come sopra detto, in un approccio di tipo dinamico e' necessario seguire l'evoluzione delle variabili di processo in gioco Il codice UNRELMC 1.0 consente di seguire un numero qualsiasi (entro il dimensionamento delle corrispondenti matrici o vettori) di variabili di processo. Ad ogni istante, lo stato del sistema e' definito in modo compiuto da un indice *i* caratterizzante la configurazione hardware e dal vettore **x** delle variabili di processo che si muove nello spazio delle fasi seguendo le linee integrali il cui andamento e' definito dalle equazioni della dinamica del processo in esame.

Nella visione dinamica dell'analisi di affidabilita', la condizione di fallimento del sistema (*top event*) e' dovuta al raggiungimento di valori di soglia da parte di una o piu' variabili di processo. Viene cosi' definita nello spazio delle fasi una *banda di funzionamento*, delimitata dai valori minimo e massimo ammissibili per ogni variabile, ai quali si fara' riferimento rispettivamente come *soglia inferiore di top event* e *soglia superiore di top event*.

Al fine di poter modellare anche gli interventi di un Sistema di Controllo viene definita una ulteriore banda delimitata da due valori di soglia per ciascuna variabile di processo, e l' intersezione di queste bande definisce nello spazio delle fasi la regione di funzionamento ottimale. Quando le variabili di processo rimangono entro la regione di funzionamento ottimale, nessuna azione di controllo viene intrapresa. Viceversa, quando le soglie che delimitano la zona di funzionamento ottimale vengono raggiunte e le variabili di processo tendono ad uscire, e' previsto l' intervento del Sistema di Controllo al fine di riportare il sistema ad una condizione di funzionamento ottimale. A questi valori di soglia si fara' riferimento in seguito rispetivamente come ai valori di *soglia di controllo inferiore* e *soglia di controllo superiore*.

Nella simulazione dinamica dunque si verifica una sorta di competizione tra le transizioni stocastiche e quelle deterministiche, con scale temporali tipicamente molto diverse: lunghe per le prime e piu' corte per le seconde. Per quanto riguarda le transizioni stocastiche, l'estrazione dei tempi di transizione segue una logica del tutto simile a quella per il caso statico. Tuttavia, nell'analisi dinamica, il codice UNRELMC 1.0 consente di considerare il caso, molto importante, che i ratei di transizione dei componenti possano dipendere dai valori assunti dalle variabili di processo, con, attualmente, la limitazione che tutti i ratei abbiano la stessa

dipendenza dalle variabili dinamiche. L'intervallo di tempo di successiva transizione viene allora determinato eguagliando un numero casuale *r*, estratto da una distribuzione uniforme *U*[0,1] alla distribuzione cumulativa:

$$r = \int_t^{t+\Delta t} f_k(\tau)d\tau = 1 - \exp[-\int_t^{t+\Delta t} \gamma_k(x(\tau))d\tau] \qquad (10)$$

ove si e' evidenziata la dipendenza di $\gamma_k$ dal vettore delle variabili dinamiche **x**. Ai fini pratici, la (10) non e' analiticamente invertibile; senza entrare in dettagli, per i quali si rimanda alla referenza [10], qui basti dire che UNRELMC 1.0 impiega un algoritmo che utilizza il valore della probabilita' che una transizione stocastica avvenga prima che le variabili dinamiche raggiungano una qualsiasi soglia (istante $t+Dt_{cross}$), cioe' la quantita' $I = 1 - \exp[-\int_t^{t+\Delta t_{cross}} \gamma_k(x(\tau))d\tau]$.

Quando, durante l'evoluzione dinamica, una variabile di processo raggiunge un valore di soglia, il sistema di controllo viene richiesto di effettuare una *transizione dinamica*. Note le condizioni iniziali, il tempo necessario perche' una variabile di processo raggiunga il valore di soglia e' determinato risolvendo le equazioni della dinamica relative alla configurazione data: corrispondentemente la transizione dinamica e' completamente deterministica. In presenza di piu' variabili e piu' valori di soglia, e' possibile ricavare i tempi necessari per ogni transizione dinamica possibile.

Una volta determinate la successiva transizione stocastica e quelle deterministiche, si esegue quella che si verifica per prima. Le rimanenti transizioni vengono tralasciate.

Per quanto riguarda la determinazione del componente che esegue la transizione e lo stato finale che viene raggiunto a seguito di essa, l'aver assunto la medesima dipendenza dei ratei di transizione dalle variabili dinamiche consente di procedere in modo del tutto analogo al caso statico.

Inoltre, la stessa flessibilita' delle correlazioni di comportamento stocastico tra componenti e delle strategie di riparazione viene mantenuta inalterata per il caso dinamico.

Qualche parola in piu' merita la risoluzione delle equazioni che governano l'evoluzione dinamica del sistema. E' evidente che l'estensione dinamica della simulazione Monte Carlo porti ad aumentare ulteriormente i gia' notevoli sforzi computazionali richiesti dall'analisi. Questa situazione deriva dal fatto che si ha a che fare con un problema *stiff* determinato dalla combinazione di lunghe costanti di tempo tipiche dell'analisi probabilistica di affidabilita' (tempi medi di rottura dell'ordine di $10^4$ - $10^5$ h) e delle costanti di tempo molto piu' brevi, caratteristiche dell'evoluzione deterministica delle variabili fisiche di processo (tempi dell'ordine dei secondi, minuti, ore). Per questo motivo, durante la simulazione, UNRELMC 1.0 non risolve le equazioni della dinamica ma opera con una matrice di valori pre-calcolati [10]. In particolare, il codice lavora su una mappatura per punti dello spazio delle fasi. Corrispondentemente ad un numero finito di punti (*punti-griglia*), vertici di un reticolo *n*-dimensionale (essendo *n* il numero di variabili di processo) avente lungo ciascuna dimensione ampiezza stabilita dall' utente, vengono pre-assegnate un certo numero di grandezze di interesse per la simulazione quali la *n*-upla dei valori assunti dalle variabili dinamiche quando la prima soglia dinamica viene incontrata; il tempo necessario a raggiungere la prima soglia dinamica; il tempo necessario ad arrivare alla prima soglia dinamica di top event; la quantita' *I* di cui sopra e che rappresenta la probabilita' che una transizione stocastica si verifichi prima che un qualsiasi valore di soglia dinamica venga raggiunto. In fase di simulazione, le grandezze relative ad un generico punto interno al reticolo vengono valutate tramite interpolazione lineare tra quelle relative ai $2^n$ punti-griglia adiacenti.

Per tener conto dell'attivita' del Sistema di Controllo, il codice prevede che ogni componente possa essere azionato secondo la regolazione di una sola variabile di processo. La domanda di intervento di un dato componente da parte del Sistema di Controllo avviene quando una variabile di processo raggiunge una soglia di controllo. In questo caso, il sistema cerca, tra i componenti abilitati al controllo della variabile in questione, quelli in uno stato di funzionamento. Questi vengono portati, dallo stato dinamico in cui si trovano, a quello caratterizzato dal valore dell' erogazione immediatamente maggiore o minore a seconda che il valore della variabile controllata stia diminuendo o aumentando (in modo cioe' da opporsi all' andamento della variabile stessa). La procedura viene eseguita ripetutamente su tutti i componenti disponibili e su tutti gli stati di questi, fino a che l'andamento della variabile controllata viene invertito. Quando invece, a seguito di riparazione, un componente viene riportato allo stato nominale, istantaneamente, il Sistema di Controllo individua tutti i componenti funzionanti e abilitati al controllo della stessa variabile regolata da quello riparato, e li riporta allo stato nominale, modificandone poi lo stato a seconda dell' andamento risultante della variabile controllata, con la stessa logica di prima, fino all'inversione della tendenza del processo.

La possibilita' di modellare l'intervento del Sistema di Controllo consente anche di tenere conto di possibili *failures on demand* che si verificano quando un componente, chiamato dal Sistema di Controllo ad intervenire non esegue la transizione richiesta ma rimane invece nello stato di funzionamento in cui si

trovava. Il componente non rimane pero' bloccato nel suo stato di funzionamento e ad una successiva chiamata del Sistema di Controllo puo' rispondere correttamente e passare al nuovo stato di funzionamento. Questo fenomeno di failure on demand e' tenuto in conto in UNRELMC 1.0 tramite l'introduzione di un valore di probabilita' di tale evento, per ogni componente e per ogni sua transizione.

UNRELMC modellizza inoltre il fenomeno di usura (*wear out*) dovuto al susseguirsi di domande di intervento su un componente che gradualmente si "affatica" e vede cosi' aumentare la propria probabilita' di failure on demand. Questo effetto di usura viene ottenuto moltiplicando la probabilita' di failure on demand per un coefficiente di usura assegnato dall' utente, specifico rispetto al componente ed alla transizione.

## 7. CONCLUSIONI

In questo lavoro e' stato presentato il codice UNRELMC 1.0 per l'analisi Monte Carlo dell'affidabilita' e disponibilita' di sistemi complessi, sviluppato presso il Dipartimento di Ingegneria Nucleare del Politecnico di Milano.

Il codice mostra una notevole flessibilita' di simulazione che consente di considerare molteplici tra gli aspetti rilevanti che si incontrano classicamente nelle analisi di sistemi reali, quali le dipendenze di comportamento stocastico tra componenti, le strategie di riparazione con logica di intervento gerarchica, etc. Inoltre, il codice consente di introdurre eventuali dipendenze dall'evoluzione fisica delle variabili di processo per quei sistemi in cui la dinamica giuoca un ruolo importante. Per esempio e' possibile considerare la dipendenza delle proprieta' stocastiche di transizione dei componenti dalle condizioni in cui essi si trovano ad operare, e cioe' dai valori assunti da certe variabili di processo quali la temperatura, la pressione etc.; e' possibile modellare l'intervento di sistemi di controllo/protezione il cui funzionamento e' strettamente legato all'evoluzione fisica; e' possibile considerare eventi di *failure on demand* e usura.

Infine, il codice prevede l'utilizzo di tecniche di riduzione della varianza per aumentare l'efficacia del calcolo nel caso di sistemi altamente affidabili. Per tali sistemi, la probabilita' di un incidente dovuto a un guasto singolo e' assai modesta; in aggiunta, le procedure di intervento e riparazione dei guasti dei componenti vengono tipicamente completate in tempi brevi, relativamente ai tempi di rottura dei singoli componenti, cosicche' il verificarsi di guasti indipendenti multipli e' assai improbabile. Corrispondentemente in un calcolo Monte Carlo analogico (o diretto), la maggior parte delle storie simulate non porterebbe alcuna informazione utile per la stima della probabilita' del guasto di sistema. Da cio' deriva la necessita' di introdurre efficaci tecniche di riduzione della varianza che "forzino" il sistema a rompersi, consentendo cosi' di fare una stima statisticamente significativa delle quantita' di interesse.

Attualmente e' in corso un'estensione del codice mirata ad includere effetti di invecchiamento secondo il modello delle riparazioni imperfette di Brown-Proschan e di obsolescenza tecnologica. Inoltre, e' in fase di sviluppo una versione per l'ottimizzazione degli intervalli di manutenzione, secondo un'algoritmo che prevede la minimizzazione di una funzione energia che tiene conto dei costi attivi e passivi dell'impianto.

## 8. BIBLIOGRAFIA


[1] M. Marseguerra, E. Zio: Approaching Dynamic Reliability by Monte Carlo Simulation, Reliability and Safety Assessment of Dynamic Process Systems, NATO ASI Series F, vol. 120, Berlin, Germany, (1993).

[2] E.E. Lewis and F. Bohm, Monte Carlo Simulation of Markov Unreliability Models, *Nuclear Engineering and Design*, **77**, pp. 49-62 (1984).

[3] Special Issue on Reliability and Safety Analysis of Dynamic Process Systems, *Reliability Engineering and System Safety*, , Vol. **52**, (1996).

[4] S. Garribba, Methods for Reliability Analysis of Systems, In *ECSC, EEC, and EAC, Reliability Modelling and Applications*, pp. 1-32 (1987).

[5] N.J. McCormick, *Reliability and Risk Analysis*, Academic Press (1981).

[6] E. Zio, *A Biased Nonlinear Connection Model in Monte Carlo Reliability Analysis of Complex Systems*, CESNEF-FRN-92.01, Dipartimento Di Ingegneria Nucleare, Politecnico di Milano.

[7] M.H. Kalos and P.A. Whitlock, *Monte Carlo Methods Vol. 1: Basics*, J. Wiley, New York (1986).

[8] M. Marseguerra and E. Zio, Nonlinear Monte Carlo Reliability analysis With Biasing Towards Top Event, *Reliability Engineering and System Safety*, **39**, pp. 31-42 (1993).

[9] W.E. Vesely, A Time Dependent Methodology for Fault Tree Evaluation, *Nuclear Engineering and Design*, **13**, pp. 337-360 (1970).

[10] M. Marseguerra and E. Zio, The Cell-To-Boundary Method in Monte Carlo-Based Dynamic PSA, *Reliability Engineering and System Safety*, **49**, pp. 91-99 (1995).