

EVENT TREE ANALISYS DINAMICA

M. Caira, L. Ferroni, M. Minichiello
Università di Roma "La Sapienza"

Dipartimento di Ingegneria Nucleare e delle Conversioni di Energia
Corso V. Emanuele II 244 - 066868095

SOMMARIO

Scopo del presente lavoro è fornire i risultati della prima fase di un'attività di studio e sviluppo di metodologie di analisi di rischio di tipo dinamico, adatte ad analizzare transitori incidentali, seguendo in maniera semplice le variazioni dei diversi parametri di processo. È stato scelto di sviluppare la metodologia utilizzando l'albero degli eventi. La metodologia è finalizzata a collegare le probabilità di funzionamento dei componenti e della risposta umana all'andamento delle variabili di processo durante il transitorio studiato. In funzione della suddivisione funzionale del processo si è proceduto ad applicare un metodo probabilistico ai componenti e sistemi interessati dal transitorio ed un metodo ad indici al comportamento dell'uomo. La metodologia è stata implementata in un programma per l'analisi di rischio basata sull'Event Tree.

INTRODUZIONE

La maggior parte degli esperti di analisi probabilistica di sicurezza sono concordi nel ritenere che l'utilizzo di tecniche classiche (ETA, FTA, HAZOP, ecc) presenta delle lacune in quanto tali tecniche essendo statiche non sono in grado di tener conto dell'evoluzione dell'impianto sia durante la sua vita operativa (per tener conto ad esempio dell'invecchiamento dei componenti o dell'influenza sul loro rateo dei guasti delle periodiche manutenzioni) che durante i transitori incidentali più o meno gravi che possono accadere durante l'esercizio.

Nella operatività degli impianti però gli aspetti dinamici giocano un ruolo importante, infatti i valori assunti dalle variabili di processo influenzano fortemente il comportamento di tutti i sistemi dell'impianto, da cui la necessità di utilizzare metodi che descrivano, appunto, la dinamica dell'impianto; in particolare devono porre l'attenzione sul funzionamento dinamico dei sistemi di controllo e regolazione e sull'influenza che le variazioni delle variabili fisiche di processo che si verificano durante i transitori incidentali hanno sulla probabilità di malfunzionamento dei vari componenti costituenti il sistema analizzato.

Le variazioni delle variabili di processo e la velocità con cui variano influenzano notevolmente anche le azioni degli operatori; ricordiamo infatti che un loro intervento tendente a riportare l'impianto in condizioni di sicurezza è molto importante nello sviluppo di scenari incidentali.

Tra le metodologie di tipo dinamico messe a punto negli ultimi anni ricordiamo i metodi della simulazione con il Montecarlo e le reti neurali. Questi, però, benché metodi molto affidabili, sono anche molto complessi.

Basti pensare che in genere la maggior parte degli studi di affidabilità riguarda problemi di analisi di eventi con bassa probabilità di accadimento e sebbene il Montecarlo, attraverso la simulazione di migliaia di storie, permette di ottenere risultati statisticamente significativi, d'altra parte la maggior parte delle storie non dà nessun contributo all'informazione finale che più ci interessa e comporta solo un notevole dispendio di tempo e di calcolo e di chi va ad analizzare i risultati in uscita dal calcolatore che di mezzi.

Negli ultimi anni sono poi state sviluppate metodologie, che sembra opportuno definire semidinamiche, in quanto seguono la vita dell'impianto tenendo conto dei fenomeni di invecchiamento, della manutenzione periodica, di eventuali riparazioni, ma non lo seguono durante l'evoluzione degli incidenti. D'altra parte hanno il pregio di essere molto meno complessi di quelli dinamici.

La metodologia presentata, l'albero degli eventi dinamico, è ancora una metodologia semplice come l'albero degli eventi classico o semidinamico; tale metodologia oltre a tenere in considerazione l'invecchiamento e la manutenzione di componenti e sistemi, segue, anche, il loro comportamento durante il transitorio incidentale e come questo comportamento sia influenzato dallo stesso scenario incidentale.

IMPIANTO E PROCESSO

Gli impianti sono un insieme di sistemi che interagiscono tra loro per raggiungere una finalità quale quella di produrre beni, energia, ecc.

Ogni sistema assolve ad una funzione specifica ed è a sua volta composto da sottosistemi, i quali lavorano in sinergia per far sì che il sistema da essi composto assolva alla sua funzione, ogni sottosistema può poi ulteriormente suddividersi in componenti per arrivare ad un grado di dettaglio richiesto da uno dei possibili modelli descrittivi scelti per descrivere il sistema impiantistico.

L'impianto dal punto di vista funzionale può essere suddiviso in:

- Produzione
- Misura
- Regolazione

I sistemi e componenti che svolgono le diverse funzioni nell'impianto possono sempre essere semplicemente classificati in base alla loro natura in:

- Meccanici
- Elettrici
- Elettronici
- Umani.

Dal punto di vista della analisi di sicurezza è necessario differenziare concettualmente le modalità di funzionamento e di risposta dei componenti e sistemi meccanici, elettrici, elettronici dal comportamento e risposta dell'uomo; pertanto nella trattazione seguente le due tipologie saranno analizzate separatamente.

La funzione di misura si realizza attraverso i seguenti componenti:

- sensori e trasmettitori della variabile di processo

- Ricevitori del segnale normalizzato proveniente dai trasmettitori (indicatori, registratori, allarmi, ecc.)

La funzione di regolazione avviene invece attraverso i seguenti componenti:

- trasmettitori della variabile di processo
- regolatore della variabile di processo al valore impostato di variabile desiderata, che possono essere del tipo ad azione continua o discontinua
- attuatori che modulano l'energia fornita al processo (valvole, interruttori, azionamenti per motori, ...).

Nell'analisi di sicurezza è importante analizzare le funzioni di misura e regolazione o controllo delle diverse variabili di processo.

Le funzioni di misura e regolazione dell'impianto sono, ovviamente, correlate al processo che vi si sta sviluppando.

Si può ricordare che, secondo la norma internazionale IEC 902 il processo è un insieme di operazioni che seguono una trasformazione fisica o chimica o una serie di tali trasformazioni. E' quindi una entità dinamica, le cui variabili caratteristiche variano nel tempo, da cui la necessità di sistemi di strumentazione e regolazione che ne controllino e regolino l'andamento nel tempo.

E' importante a questo punto definire le variabili del processo e le loro variazioni operazionali o incidentali.

Se indichiamo con A la generica variabile di processo (pressione, temperatura, livello, portata, corrente, ecc.) che caratterizza lo stato fisico di un sistema, questa in seguito ad un evento iniziatore può:

- Aumentare
- Diminuire
- Rimanere costante.

Subirà in generale una variazione che può essere individuata da una funzione $A(t)$ rappresentativa dello scostamento della variabile di processo dal suo valore nelle normali condizioni operative e della velocità con cui si discosta dal valore nominale.

Per la $A(t)$, in prima approssimazione, possiamo supporre i seguenti andamenti:

1) Andamento lineare: $A(t) = a t + b$ con $t \in [0, +\infty)$ e $b \in (-\infty, +\infty)$

2) Andamento quadratico:

- parabola: $A(t) = \frac{1}{2} a t^2 + b$ con $t \in [0, +\infty)$ e $b \in (-\infty, +\infty)$ ed il fuoco in $(0, a/2)$
- iperbole: $A(t) = |b/a (t^2 - a^2)^{1/2}|$ con $t \in [0, +\infty)$ e $b, a \in (-\infty, +\infty)$

3) Andamento cubico: $A(t) = b + a t^3$ con $t \in [0, +\infty)$ e $b, a \in (-\infty, +\infty)$

4) Andamento esponenziale: $A(t) = b + a t^\alpha$.

parametri che caratterizzano tale legame viene in genere indicato come "prestazioni" del componente.

Per una corretta analisi del loro funzionamento ed impiego è necessario quindi conoscere le prestazioni, la maggior parte delle quali si riferisce direttamente alle caratteristiche statiche e dinamiche del dispositivo stesso.

La caratteristica statica esprime in forma analitica o, meglio grafica, la relazione esistente tra l'ampiezza della grandezza di ingresso y e l'ampiezza della grandezza d'uscita y_m .

L'espressione analitica della caratteristica statica corrisponde nel piano y, y_m ad una curva

$$Y_m = C(y)$$

La scelta della forma della $C(\cdot)$ dipende dal dispositivo considerato e dalla precisione desiderata.

Le prestazioni di un componente sono individuate dalle caratteristiche metrologiche del componente stesso: accuratezza, precisione, isteresi, sensibilità, deriva di zero, deriva della sensibilità, intervallo di errore che viene in genere dato in percento di fondo scala per uno strumento, ecc.

L'effetto di alcune grandezze quali la variazione della temperatura di lavoro, della pressione ambiente, della tensione di alimentazione, hanno come effetto sulle caratteristiche metrologiche un aumento l'errore sul guadagno (rapporto tra output (% FS) e l'input (%)), e si traducono nella pratica come un errore nella risposta del dispositivo.

La caratteristica dinamica esprime anch'essa in forma analitica la relazione esistente tra l'ampiezza della grandezza di ingresso y e l'ampiezza della grandezza d'uscita y_m , con riferimento ad una variazione rapida della grandezza all'ingresso; di questa si individua una risposta in ampiezza ed una in fase.

Durante un transitorio di tipo incidentale si ha variazione delle variabili di influenza delle caratteristiche metrologiche e di conseguenza variazione dell'errore della risposta del dispositivo e quindi variazione della sua probabilità di malfunzionamento. Questi errori alla risposta, sono tipici del breve periodo del transitorio.

Per tenere conto della variabile tempo su larga scala (mesi, anni), la caratteristica statica deve essere corretta con un valore che tenga conto dell'aumentare dell'errore relativo col passare del tempo (fenomeni di invecchiamento o correzioni dovute alla manutenzione).

EVENT TREE DINAMICO

L'albero degli eventi dinamico, proposto nel presente lavoro, è una metodologia semplice come il classico event tree, di cui mantiene la struttura, ma considera le probabilità di malfunzionamento come funzioni dipendenti dal tempo e dai fenomeni che influenzano la corretta risposta dei dispositivi nel tempo sia su larga scala che nel breve periodo del transitorio.

Il metodo sviluppato tratta in maniera differenziata le risposte dei dispositivi propriamente detti (meccanici, elettrici, elettronici) da quelle dell'essere umano, per cui si è preferito, in prima analisi, non seguire un approccio probabilistico puro, ma si è scelto di utilizzare un metodo ad indici

RISPOSTA DEI DISPOSITIVI

Ricordiamo che l'affidabilità di un componente viene definita come la probabilità che esso compia correttamente la funzione assegnatagli, senza guastarsi in un dato intervallo di tempo, in determinate condizioni ambientali ed in base alle sollecitazioni cui è normalmente o potrebbe essere in casi particolari sottoposto.

Ciò significa che bisogna stabilire:

- 1) un criterio univoco **C** per giudicare se l'elemento è funzionante oppure no. Per i sistemi bistabili tale criterio è ovvio, altre volte lo stato di guasto è definibile solo con il riconoscimento di un limite massimo o minimo per uno o più parametri, in questi casi è in genere possibile anche individuare stati di funzionamento parziali.
- 2) Le condizioni ambientali di impiego **I**.
- 3) L'intervallo di tempo **t** durante il quale si richiede che il componente funzioni.

Se indichiamo allora con **R** l'affidabilità, questa risulterà essere in generale una funzione delle tre variabili su specificate

$$R = R(C, I, t)$$

Inoltre fissato **C**, poichè in genere $I = I(t)$, l'affidabilità diventa funzione solo del tempo e la $R(t)$ dipenderà allora dalla legge probabilistica con cui il guasto può verificarsi nel tempo. La variabile casuale quindi è il tempo **T** che intercorre tra l'istante iniziale del periodo a cui si riferisce l'analisi di affidabilità e quello in cui avviene il guasto o la rottura del componente. L'affidabilità viene quantificata con un valore che da una probabilità ed è quindi un numero dimensionale compreso tra zero ed uno. Se indichiamo con N_0 il numero dei componenti in funzione al tempo $t=0$ e con $N_g(t)$ ed $N_s(t)$, rispettivamente, i componenti guasti e sopravvissuti al tempo $t>0$, allora

$$N_0 = N_g(t) + N_s(t)$$

Mentre definiamo l'inaffidabilità come la probabilità che un componente si guasti nell'intervallo di tempo 0-t

$$F(t) = N_g(t) / N_s(t)$$

Ossia $F(t) = P(T \leq t)$, dove $F(t)$ è la funzione di distribuzione della variabile casuale T .

Per l'affidabilità invece possiamo scrivere:

$$R(t) = N_s(t) / N_0(t) = 1 - F(t) = P(T > t)$$

La $R(t)$ quindi è la probabilità che il componente funzionante al tempo $t=0$ funzioni ancora al tempo t .

Definiamo inoltre la funzione di densità di probabilità $f(t)$ come

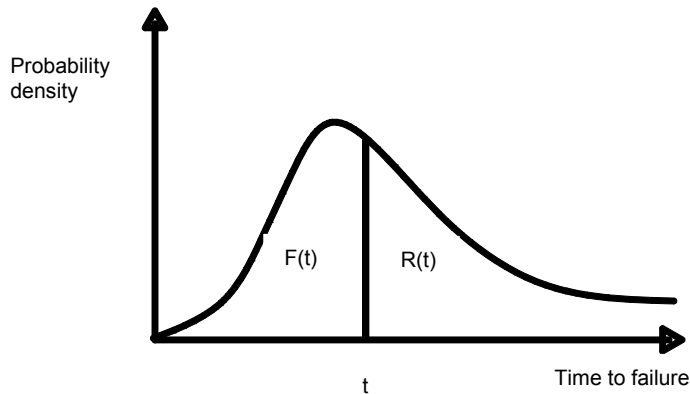
$$f(t) = dF(t)/dt = (1/N_0) * (dN_g/dt) = (1/N_0) [d(N_0 - N_s)/dt] = (-1/N_0) (dN_s/dt)$$

$$f(t) = -dR(t)/dt$$

Inoltre valgono le seguenti relazioni:

$$F(t) = \int_0^t f(x) dx$$

$$R(t) = \int_t^{\infty} f(x) dx$$



Indichiamo con $f(t) dt$ la probabilità che un componente messo in opera al tempo $t=0$ si guasti nell'intervallo $t, t+dt$ e con $\lambda(t)$ il tasso di guasto o failure rate.

Allora $\lambda(t) dt$ rappresenta la probabilità condizionata che il componente si guasti in un tempo compreso tra t e $t+dt$, supponendo che in t sia ancora funzionante.

Mentre la $f(t) dt$ è la frazione di popolazione che si guasta nell'intervallo $t, t+dt$, riferendoci ad una popolazione sana al tempo $t=0$, la $\lambda(t)dt$ è la frazione di popolazione sopravvissuta fino al tempo t e che si guasta poi nell'intervallo $t, t+dt$.

$$P[\text{componente si guasti in } (t, t+dt)]$$

$$\lambda(t)dt = \frac{P[\text{componente non si sia guastato in } (0,t)]}{P[\text{componente non si sia guastato in } (0,t)]}$$

Sappiamo inoltre che la probabilità condizionata che dato l'evento B si verifichi l'evento A è data da $P(A/B)=P(A \cap B)/P(B)=P(B/A)*P(A)/P(B)$, e quindi sviluppando la relazione di sopra:

$$\lambda(t)dt = \frac{P[\text{componente si guasti in } (t,t+dt) \text{ e che non si sia guastato in } (0,t)]}{P[\text{componente non si sia guastato in } (0,t)]}$$

$$\lambda(t)dt = 1/R(t) \times \{ P[\text{componente si guasti in } (0,t+dt)] - P[\text{componente si guasti in } (0,t)] \}$$

$$\lambda(t) = \frac{R(t) - R(t+dt)}{R(t)} = -dR(t)/dt = -d / dt (\ln R(t))$$

Da cui si ottiene : $f(t)=\lambda(t)R(t)$

$$R(t) = \exp - \int_0^t \lambda(x)dx$$

$$F(t) = 1 - R(t)$$

Il tasso di guasto $\lambda(t)$ è una funzione del tempo e a seconda del suo andamento la densità di probabilità di guasto $f(t)$ assumerà diverse configurazioni. Se assumiamo $\lambda(t)=\lambda = \text{cost.}$, allora la $f(t)$ assumerà la forma di una distribuzione esponenziale negativa.

$$R(t) = \exp(-\lambda t)$$

Quando si assume $\lambda = \text{cost.}$ si dice che il componente "non ha memoria", nel senso che il funzionamento non dipende dal particolare istante della sua vita. E' tuttavia possibile definire l'affidabilità d'intervallo relativa al generico intervallo $[(s+t),s]$ e non dall'età s :

$$R(s+t, s) = P[T > s+t / T > s]$$

$$R(s+t / s) = \exp. - \int_s^{s+t} \lambda(t)dt$$

Se $\lambda(t)=\lambda = \text{cost.}$ si ottiene che $R(s+t/s)=\exp.-\lambda(t)=R(t)$, ossia se la durata dell'intervallo $(0,t)$ è uguale a quella dell'intervallo $(s,s+t)$ le due affidabilità coincidono.

Si possono utilizzare anche tassi di guasto variabili nel tempo mediante , ad esempio, il modello di Weibull o rappresentazioni lineari, come quella da noi scelta:

$$\lambda(t) = \lambda_0 + k t + c(\tau, n, s)$$

k= termine di invecchiamento

c(t)= termine di manutenzione

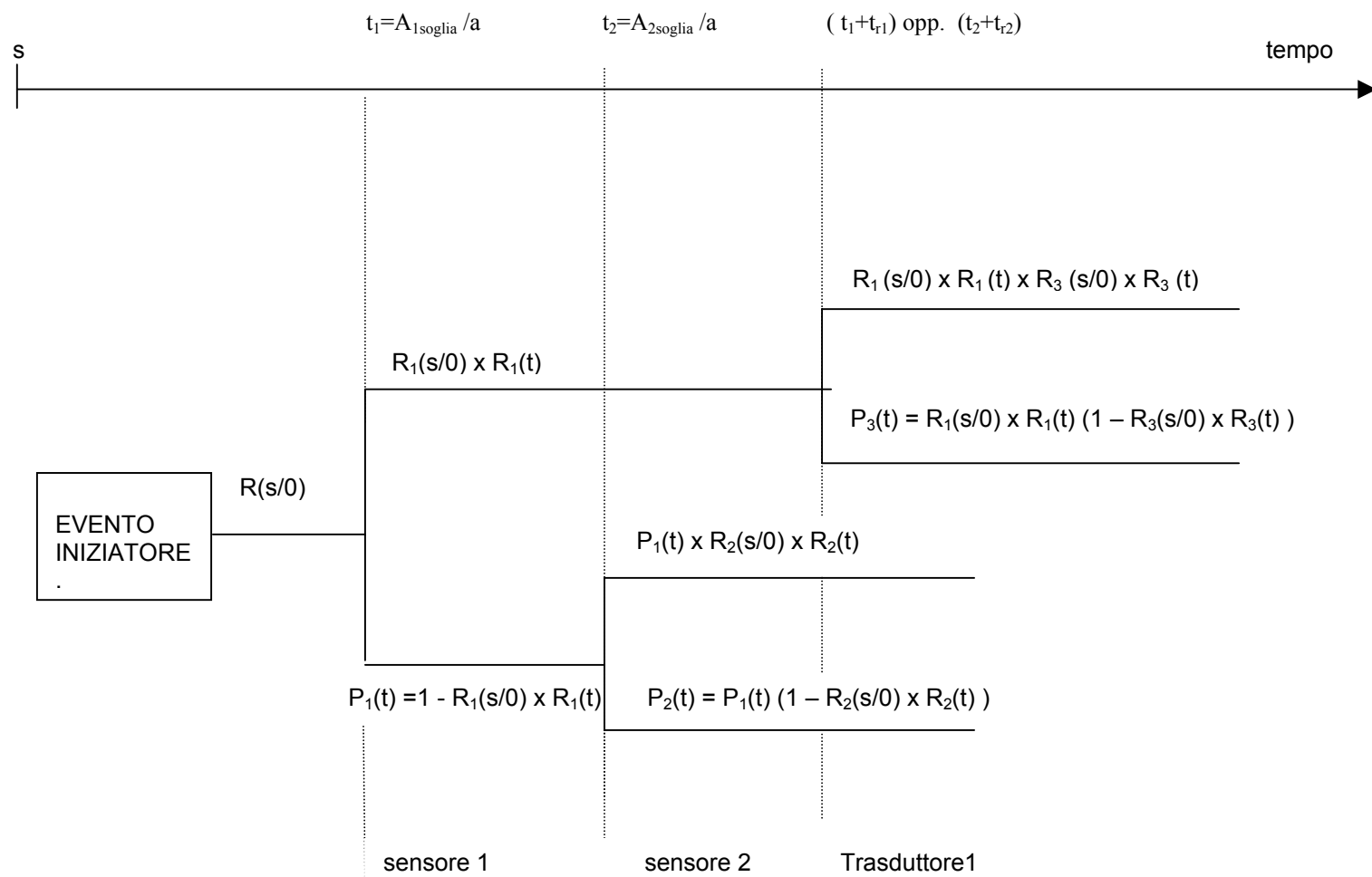
τ = intervallo di tempo previsto tra una manutenzione e l'altra

n= numero delle manutenzioni eseguite sul componente dall'inizio della sua messa in esercizio

s= età del componente.

Nella costruzione dell'albero degli eventi si parte sempre da un evento iniziatore che porta alla situazione incidentale.

Indichiamo con $P(t)$ la probabilità di fallimento e con $R(t)$ la reliability, cioè la probabilità di successo e supponiamo che l'evento iniziatore si verifichi al tempo $t = s$ e che implichi una variazione della variabile di processo con andamento lineare $A(t) = a t$



Dove t_{r1} e t_{r2} sono i tempi di risposta rispettivamente del sensore 1 e del sensore 2.

$$R_1(t) = R_1(s + t/s)R_1^*(t) = \exp\left(-\int_{t_1}^{t_2} \lambda^*(t)dt\right)$$

$$\lambda^*(t) = f[\lambda(s + t, s), f(A(t)), f(\varepsilon\%)]$$

dove: $\varepsilon\%$ = errore relativo percentuale dovuto alla variazione del parametro di processo considerato.

RISPOSTA DELL'UOMO

Per l'applicazione del metodo ad indici si è tenuto in conto che la risposta umana è funzione di diversi parametri, quali interfaccia uomo-macchina, ambiente di lavoro, politiche di sicurezza, ecc..

Preso atto che l'analisi degli errori umani è di vitale importanza non solo per la sicurezza dell'impianto e dell'uomo stesso, ma anche ai fini di una buona ottimizzazione del processo e che quando un operatore commette un errore porta in genere il sistema in uno stato di vulnerabilità o danno latente, che alla fine può portare sia ad un semplice guasto che ad una emergenza, nell'analisi di sicurezza ci troviamo di fronte a diversi tipi di errori umani causate da diverse situazioni :

- a) Inadeguatezza nelle strumentazioni e nelle sale di controllo: riguarda la disposizione dei dispositivi di segnalazione, il numero dei dispositivi di allarme,....
- b) Inadeguatezze nell'ambiente di lavoro : rumore, illuminazione, temperatura, spazi...
- c) Carenze nella politica di sicurezza: training, procedure insufficienti, comunicazione carente, ecc..

In questa fase si è scelto di utilizzare un metodo semplice quale il metodo HCR (Human cognitive Reliability), specifico per l'analisi di compiti o azioni per i quali il tempo a disposizione T è il vincolo principale e il cui corretto svolgimento implichi aspetti cognitivi. Questo metodo fornisce la probabilità di non risposta entro il tempo T , indicata come $P_e(t)$, dovuta ad uno svolgimento troppo lento del compito assegnato e non comprende né l'errore di percezione dell'anomalia, né quello di scelta del provvedimento da prendere, che possono essere a loro volta modellati con un albero degli eventi.

Il metodo si sviluppa secondo i seguenti passi:

- classificazione del compito
- determinazione del valore nominale del tempo mediano $T_{1/2}^*$
- Conversione di $T_{1/2}^*$ con le PSF (fattori modificanti le prestazioni), ottenendo così il $T_{1/2}$
- Determinazione del tempo T a disposizione
- Applicazione del metodo HCR per ottenere $P_e(T)$.

Nel primo punto, stabilito il livello di decomposizione delle azioni per le quali la dipendenza dal tempo è essenziale, occorre fare una

classificazione in base al tipo di processo cognitivo che esso implica, per es. Skill-based (risposta immediata), Rule-based (basato su regole), Knowledge-based (conoscitivo). Poi si passa alla determinazione del tempo mediano nominale $T_{1/2}^*$ (tramite l'esperienza operativa, simulatori, giudizio degli esperti, ecc) che rappresenta il valore del tempo a disposizione per cui si ha esattamente il 50% di probabilità di failure nello svolgere un determinato compito. L'aggettivo nominale sta ad indicare che tale valore si riferisce ad una situazione media, ma per tener conto della specificità del caso in esame si fa ricorso a tre PFS (Performance Shaping Factor): addestramento, stress, qualità della sala di controllo e dell'impianto. Ad ogni PFS è associato un K_i , $i=1,2,3$, ed il tempo mediano è stimato tramite la relazione:

$$T_{1/2} = T_{1/2}^* (1 + k_1)(1 + k_2)(1 + k_3)$$

Il valore dei vari K_i si trova tabellato, mentre per ciascuna situazione occorre determinare il tempo a disposizione T del personale per svolgere l'intervento prima che abbia luogo un significativo e indesiderato cambiamento dello stato del sistema, in base all'esperienza o al giudizio di esperti, ecc.. A questo punto la probabilità di non risposta in funzione del tempo T è data dalla:

$$P_e(t) = \exp - \left(\frac{t / T_{1/2} - \gamma_i}{\eta_i} \right)^{\beta_i}$$

dove t è la variabile indipendente tempo, mentre i parametri β_i , γ_i , η_i si trovano tabellati in base al tipo di processo cognitivo.

A questo punto basterà inserire T nell'espressione di cui sopra e determinare l'ordinata corrispondente a $T/T_{1/2}$ nei grafici delle tre curve del modello(per Skill, Rule e Knowledge) In funzione del tempo normalizzato $t/T_{1/2}$, per ottenere la probabilità di non risposta cercata.

CONCLUSIONI

La prima fase dell'attività di ricerca sull'albero degli eventi di tipo dinamico ha affrontato anche lo sviluppo di un programma di calcolo (ETA2002) che è provvisto di data base di tipologie di transitori, di componenti e sistemi di impianto con le caratteristiche dinamiche e dei parametri relativi alla risposta umana.

La metodologia sviluppata ed il programma saranno applicati a test case qualificati per:

- analizzare le variazioni che scaturiscono dall'applicazione dell'event tree dinamico;
- verificare quale sia nell'analisi dinamica la scala dei valori di influenza sugli incidenti dei dispositivi e dei fattori umani;
- definire quale tipologia di andamento delle variazioni dei parametri di processo sia più corretta per i differenti transitori incidentali da esaminare.

BIBLIOGRAFIA

1. Norman J. McCormick, Reliability and Risk Analysis, Academic Press, Inc., 1981.
2. Massimiliano Peternella, Roberto Vitelli, Strumentazione Industriale, trasduttori e regolatori, UTET, 1981.
3. Oliver Strater, Assesment of Cognitive Errors and Organizational Aspects Based on Evaluation of Plant Experience, Processed Reprint of Paper in ANS_Proceedings of the international topical Meeting on Probabilistic Safety Assesment 1996. Park City, Utah (USA), september 29-October 3, 1996.
4. Oliver Starter, A Method for Human Reliability Data Collection and Assesment, Processed Reprint of Paper from Cacciabue, P. C. & Papazoglou, I. A. (Eds.) (1966) Probabilistic Safety Assesment and Management. Proceedings of ESREL'96/ PSAM-III. Crete, Greece, June 24-25, 1996.
5. Cappa, Sensori e Trasduttori per Misure Meccaniche e Termiche, Borgia Editore, 2000.
6. Brunelli A., Strumentazione di misura e controllo nelle applicazioni industriali, Editore G.S.I., gruppo imprese strumentazione italia, Milano, Aprile 2000.
7. Doebelin Ernest O., Measurement systems: Application and design, New York, McGraw-Hill International Edition, 1990.
8. Hume K. J., Engineering Metrology, second edition, London, Macdonald.
9. M. Marseguerra, E. Zio, Un connubio promettente per l'ottimizzazione di progetto e gestione logistica d'impianto, VGR2k Pisa, ottobre 2000.
10. M. Marseguerra, E. Zio, Affidabilità dinamica con metodo Monte Carlo e reti neurali, VGR1998 Pisa, ottobre 1998.
11. J. Devooght and C. Smidts, Probabilistic Reactor Dynamics-I: The Theory of Continuous Event trees, nuclear science and engineering:111,229-240 (1992).
12. Marko Cepin, Borut Mavko, A dinamic fault tree, Reliability Engineering and Sistem Safety 75 (2002) 83-91.
13. R. Manian, J. B. Dugan, D. Coppit, K. J. Sullivan, Combining Various Solution Techniques for Dynamics Fault Tree Analysis of Computer Systems, VGR2k Pisa, ottobre 2000.
14. Paolo Vespucci, Modelli per la valutazione dell'affidabilità Umana, Franco Angeli libri s.r.l, Milano, 1990.