LA METODOLOGIA ASTRA PER L'ANALISI DI AFFIDABILITA' DI SISTEMI COMPLESSI

Sergio Contini[1], Giacomo G.M. Cojazzi[1], Guido Renda[1], Giuseppe de Cola[2]
[1.] Commissione Europea, Centro Comune di Ricerca, Ispra, VA
[2.] Infocon, Lavagna, GE
sergio.contini@jrc.it

SOMMARIO

Il software ASTRA per l'analisi di affidabilità e sicurezza di sistemi complessi, quali ad esempio i sistemi di produzione e distribuzione dell'energia, è stato sviluppato nel 1996-97 e si basa sull'approccio BDD (Binary Decision Diagrams) dimostratosi di gran lunga più efficiente degli approcci precedenti. Recentemente é iniziata una fase di miglioramento del codice sia dal punto di vista metodologico che informatico. Scopo della presente memoria è la descrizione degli aspetti più importanti di alcuni degli algoritmi realizzati e in corso di implementazione e delle caratteristiche più significative dei diversi moduli costituenti ASTRA.

1. INTRODUZIONE

Il software ASTRA, sviluppato presso il CCR nel periodo 96-97 [1, 2] ed in fase di aggiornamento con la realizzazione di nuovi moduli di calcolo, consente di eseguire l'analisi di sistemi complessi mediante la modellizzazione basata su Alberi di Guasto (fault-trees) e di evento (event-trees). Gli algoritmi per l'analisi logica fanno uso dell'approccio BDD (*Binary Decision Diagram*) di gran lunga più efficiente dei precedenti metodi basati sulla manipolazione di combinazioni di guasto [3]. L'aggiornamento delle procedure di analisi probabilistica che, sfruttando le potenzialità della tecnica BDD permettono di effettuare il calcolo esatto delle grandezze probabilistiche di interesse, è attualmente in fase di implementazione e costituisce l'oggetto della presente memoria.

Dopo alcuni richiami della tecnica BDD [4], riportati nella sezione 2, saranno descritti nella sezione 3 i seguenti aspetti metodologici dell'analisi degli Alberi di Guasto (AdG):

- il calcolo dei valori esatti dell'indisponibilità, della frequenza di guasto, del numero atteso di guasti per il *Top event* e per tutti i modi di guasto minimi (*Minimal Cut Sets*) significativi.
- il calcolo dei valori esatti di diversi indici di importanza dei componenti (*Structural Importance, Birnbaum, Risk Achievement Worth, Risk Reduction Worth, Fussell-Vesely, Criticality, Barlow-Proschan, Differential Importance Measure).*

A richiesta, queste grandezze possono essere ottenute in funzione del tempo e rappresentate graficamente con la possibilità di simulare correttamente diverse politiche di test.

Allo scopo di fornire un'idea più precisa della metodologia di analisi con BDD viene illustrato nella sezione 4 un semplice esempio. Viene poi fornita nella sezione 5 una breve descrizione dell'architettura di ASTRA e delle caratteristiche principali dei diversi programmi disponibili ed in corso di aggiornamento o di realizzazione. Le conclusioni sono riportate nella sezione 6.

2. PROCEDURA DI ANALISI LOGICA DI UN ALBERO DEI GUASTI

La funzione di struttura di un albero dei guasti è una funzione logica combinatoria (senza memorie) e come tale può contenere solo gli operatori logici fonsdamentali AND, OR, NOT. Le variabili di ingresso sono i modi di guasto dei componenti (0=funzionante, 1=guasto) e la variabile di uscita corrisponde allo stato del Top event (0=non verificato, 1=verificato). Le funzioni che non contengono la complementazione (NOT) sono dette coerenti in quanto il verificarsi di una variabile, il guasto di un componente, può solo degradare il sistema o far verificare il Top event. Nelle funzioni AND-OR-NOT, dette non coerenti e più complesse da analizzare, anche la riparazione di un componente può contribire al verificarsi del Top event. Ovviamente un sistema che si comportasse in questo modo sarebbe stranordo. Ricordiamoci però che l'albero dei guasti viene costruito per identificare le cause che possono verificare il top event e per calcolarne la probabilità di occorrenza. La funzione di struttura, coerente o non coerente, dipende quindi dalla stecifica definizione del Top event. Per chiarire questo concetto consideriamo ad esempio un semplice sistema formato da due pompe in parallelo P1 e P2 e supponiamo di essere interessati ai seguenti Top events:

1) entrambe le pompe guaste $\Rightarrow$ Top = (P1 guasta) AND (P2 guasta)
2) almeno una pompa guasta $\Rightarrow$ Top = (P1 guasta) OR (P2 guasta)

3) una sola pompa guasta $\Rightarrow$ Top = ((P1 guasta) AND (P2 sana)) OR ((P1 sana) AND (P2 guasta))

Di questi top events il terzo è non coerente. Infatti, con entrambe le pompe guaste il Top non può essere verificato; appena una delle due pompe viene riparata, il Top si verifica. Questo comportamento dipende solo dal fatto che con la terza definizione di Top siamo interessati a calcolare la probabilità di guasto di una sola pompa, non di tutte e due. In altri termini, non abbiamo a che fare con un sistema strano, ma più semplicemente la nostra definizione di Top event introduce l'evento negato allo scopo di scartare la combinazione di due pompe guaste. L'uso di eventi negati (successo), ossia di Top events non coerenti, è molto importante per la modellizzazione completa di sistemi complessi [5, 6,7].

L'analisi di un albero dei guasti si articola in due fasi:

- Analisi logica, per la determinazione dei modi di guasto (minimal cut sets, MCS);
- Analisi probabilistica, per la determinazione della probabilita' di accadimento del Top event e degli indici di importanza o criticita' dei componenti.

Il software ASTRA utilizza l'approccio basato sui Diagrammi Decisionali Binari, (Binary Decision Diagrams, BDD), rivelatasi estrememente superiore ai precedenti approcci basati sulla manipolazione di combinazioni di guasto di componenti. In pratica l'albero da analizzare viene dapprima modularizzato, ossia suddiviso in tanti sottoalberi indipendenti (moduli) e pertanto analizzabili separatamente; successivamente, per ciascun modulo, viene costruito il corrispondente BDD mediante l'applicazione del teorema di espansione di Shannon, secondo il quale una qualsiasi funzione booleana G (x_1, x_2, ..., x_n) di n variabili, x_1, x_2, ... x_i, …x_n può essere scritta nel modo seguente:

$$G(x_1, x_2, ..., x_n) = (x_i \wedge G_1) \vee (\bar{x}_i \wedge G_0) \quad (1)$$

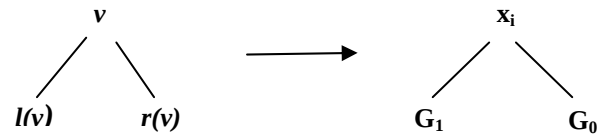
dove:

$$G_1 = G|_{xi=1} = G(x_1, x_2, .. , x_{i-1}, x_i = 1, x_{i+1}, ..., x_n) \quad (2)$$

$$G_0 = G|_{xi=0} = G(x_1, x_2, .. , x_{i-1}, x_i = 0, x_{i+1}, ..., x_n) \quad (3)$$

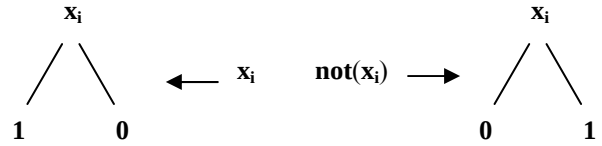
sono i due residui di G ottenuti ponendo rispettivamente $x_i = 1$ e $x_i = 0$; "$\wedge$" rappresenta l'operatore logico AND, "$\vee$" rappresenta l'operatore logico OR, e "–" l'operatore NOT. Spesso si usano i simboli "+" per OR, mentre AND viene sottinteso.

La (1) può essere graficamente rappresentata come albero binario nel modo seguente:



dove al nodo *v* è associata la variabile x_i, al discendente sinistro *l(v)* è associato il residuo G_1 ed al discendente destro *r(v)* il residuo G_0.

I *nodi* dell'albero ai quali sono associate le variabili x_1, x_2, …, sono detti *non-terminali* e i nodi 0, 1, che rappresentano i valori della funzione G per diverse combinazioni di valori delle variabili, sono detti *nodi terminali*. Ad esempio, la rappresentazione BDD delle variabili $\mathbf{x_i}$ e **not**($\mathbf{x_i}$) è la seguente:



Si può notare come la negazione si riconduca all'inversione dei nodi terminali.

Nell'analisi degli alberi di guasto le variabili, o nodi, sono gli eventi primari e la funzione G rappresenta la funzione di struttura, vale a dire l'insieme delle relazioni logiche fra gli eventi di guasto espresse mediante gli operatori logici AND, OR e NOT (Figure 1 e 2).

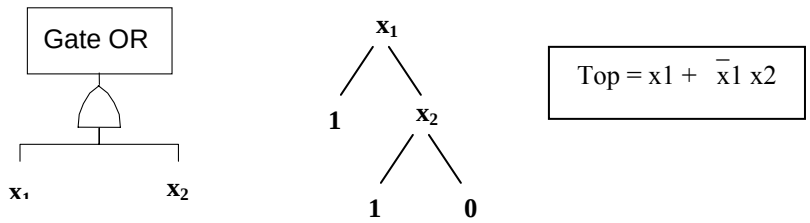


Figura 1. Rappresentazione di un porta logica di tipo OR, del corrispondente BDD e della espressione logica nella quale i modi di guasto sono disgiunti per costruzione.

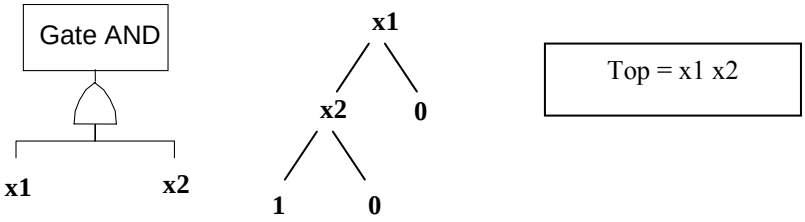


Figura 2. Rappresentazione di un porta AND, del corrispondente BDD e dell' espressione logica.

Si nota facilmente come la procedura di costruzione del BDD, attraverso l'applicazione a tutte le variabili del teorema di Shannon - secondo un ordine prestabilito - fornisca un grafo nel quale i cammini fra i nodi terminali 1 e la radice rappresentano tutti i modi di guasto disgiunti. Ad esempio in figura 1 i cammini da 1 alla radice sono x1, $\bar{x}$1 x2. La variabile è positiva se si giunge al nodo dal ramo sinistro, negata se dal ramo destro. La disgiunzione di questi cammini consente di eseguire l'analisi probabilistica esatta senza dover calcolare i modi di guasto minimi. Il BDD che consente di fare ciò è denominato ROBDD (Reduced Ordered BDD). Da questo grafo si ricava poi il BDD minimo (MOBDD) contenente tutti i MCS del sistema, dal quale è possibile calcolare la distribuzione dei MCS in funzione dell'ordine e della probabilità. Questa informazione agevola la scelta dei valori di soglia (probabilità e ordine degli MCS) per l'estrazione degli MCS più importanti (figura 3).

Diversamente dai programmi basati sulla manipolazione degli insiemi di guasto, con l'approccio BDD è possibile eseguire il taglio non solo in base alla indisponibilità ma anche alla frequenza di guasto ω(t).

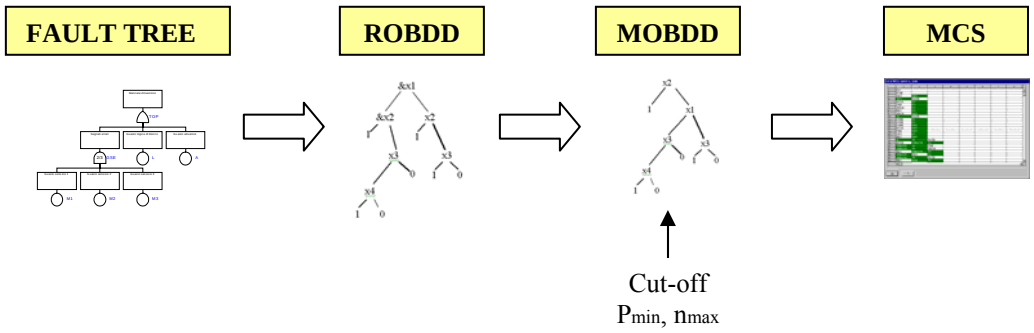


Figura 3. Fasi principali della procedura di analisi degli alberi di guasto mediante l'approccio BDD.

Un altro vantaggio del BDD rispetto ai precedenti approcci è relativo alla possibilità di verificare l'equivalenza logica di due fault trees. In precedenza questo problema veniva risolto solo confrontando un sotto insieme degli MCS, i più significativi, con conseguente margine di errore. Con l'approccio BDD è possibile risolvere questo problema in modo molto semplice, costruendo i BDD dei due alberi utilizzando la stessa sequenza di variabili per l'applicazione della (1). I due fault trees sono uguali se e solo se lo sono i corrispondenti BDD.

Infine, i tempi di calcolo per l'analisi di sistemi complessi con BDD differiscono persino di alcuni ordini di grandezza rispetto ai tempi di calcolo necessari con algoritmi basati sulla manipolazione delle combinazioni di guasto. Diversi fault trees precedentemente non analizzabili sono stati elaborati con ASTRA in alcune decine di secondi su PC [4].

3. PROCEDURA DI ANALISI PROBABILISTICA

Secondo gli approcci basati sulla manipolazione delle combinazioni di guasto l'analisi probabilistica viene eseguita sull'insieme *N* dei modi di guasto significativi, fornendo valori approssimati. Infatti, per la probabilità dell' evento Top, valgono le seguenti disuguaglianze:

$$\sum_{i=1}^{N} P(C_i) - \sum_{i=1}^{N-1}\sum_{j=i+1}^{N} P(C_i \cap C_j) \le P(Top) = P(\bigcup_{i=1}^{N} C_i) \le 1 - \prod_{i}^{N}(1 - P(C_i)) \le \sum_{i=1}^{N} P(C_i) \qquad (4)$$

Dove C_i , $i= 1,\ldots N$, e' il generico insieme minimo di guasto del sistema.
Nella (4), il primo termine della disuguaglianza e' noto come second order (lower) bound mentre l' ultimo termine della disuguaglianza è noto come first order (upper) bound. La (5) riporta anche il cosiddetto Esary Proshan upper bound che da' sempre un risultato meno conservativo del bound di primo ordine.

In un ROBDD i cammini dai nodi terminali 1 alla radice, indicati con $Path_k\ (1 \rightarrow Top)$ rappresentano i modi di guasto del sistema per il top-event in esame (in generale questi non sono minimi). Da notare che tali modi di guasto, per costruzione del BDD, sono mutuamente esclusivi e pertanto la probabilità esatta del Top event è data dalla somma delle probabilità dei cammini che portano dai nodi terminali 1 alla radice (Root):

$$P(Top) = P(\bigcup_k Path_k\ (1 \rightarrow Root)) = \sum_k P\ (Path_k (1 \rightarrow Root)) \tag{5}$$

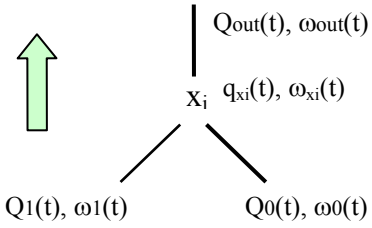
Pertanto la quantificazione di un BDD consente di ottenere i valori esatti di indisponibilità $Q_S(t)$, della frequenza non condizionata di guasto del top event $\omega_S(t)$ e degli indici di importanza dei componenti. Se poi l'analisi viene eseguita in funzione del tempo allora è possibile simulare le diverse politiche di test/ispezione dei componenti. Diversi autori hanno proposto metodi di analisi probabilistica e di calcolo degli indici di importanza applicati o applicabili al BDD [8,9,10]. Nel seguito viene brevemente descritta la procedura di analisi probabilistica in fase di implementazione nella nuova versione di ASTRA per il calcolo delle grandezze affidabilistiche a livello di sistema (Top event, par 3.1) e per la determinazione delle misure di importanza dei componenti (par. 3.2). Quanto segue è limitato alla quantificazione dei fault trees coerenti. La metodologia per l'analisi dei FT non coerenti, appositamente sviluppata per ASTRA e in corso di pubblicazione, è più complessa e non viene descritta per brevità.

3.1 Indisponibilità, Numero atteso di guasti e inaffidabilità

Il calcolo del valore esatto dell'indisponibilità del Top event può essere effettuato visitando il BDD secondo due opposte modalità: partendo dai nodi terminali (Bottom-Up, BU) o dalla radice (Top-Down, TD). Entrambi gli algoritmi sono necessari per il calcolo degli indici di importanza dei componenti. Per brevità riportiamo solo l'algoritmo BU.

Consideriamo il generico nodo del grafo associato alla variabile x_i, con i suoi discendenti sinistro ($x_i = 1$) e destro ($x_i = 0$). Dati $Q_1(t)$, $\omega_1(t)$ per il discendente sinistro e $Q_0(t)$, $\omega_0(t)$ per il discendente destro, si determinano $Q_{out}(t)$, $\omega_{out}(t)$ in funzione dell'indisponibilità $q_{xi}(t)$ e della frequenza di guasto del componente $\omega_{xi}(t) = \lambda(1 - q_{xi}(t))$. Per i nodi terminali, punto di partenza dell'algoritmo, abbiamo:

- nodo 1: $Q_1(t) = 1$ e $\omega_1(t) = 0$
- nodo 0: $Q_0(t) = 0$ e $\omega_0(t) = 0$



$$Q_{out}(t) = Q_1(t)\ q_{xi}(t) + Q_0(t)\ (1- q_{xi}(t)) \tag{6}$$

$$\omega_{out}(t) = Q_1(t)\ \omega_{xi}(t)\ + \omega_1(t)\ q_{xi}(t)\ + \omega_0(t)\ (1- q_{xi}(t)) - Q_0(t)\ \omega_{xi}(t) \tag{7}$$

$Q_S(t)$ e $\omega_S(t)$ sono i valori $Q_{out}(t)$, $\omega_{out}(t)$ risultanti dall'analisi del nodo radice.

Integrando $\omega_S(t)$ fra 0 e T (T tempo di missione) si ottiene $W_{S(T)}$, il numero aspettato di volte che il Top event si verifichi entro T. Per sistemi con componenti riparabli $W_S(T)$ viene spesso utilizzato come estremo superiore per l'inaffidabilità $F_S(T)$, in quanto quest'ultima, a causa della limitazione intrinseca dell'albero dei guasti, non può essere calcolata esattamente [11]. Finché la probabilità di accadimento del Top event si mantiene inferiore a 0,1 l'uso di $W_S(T)$ comporta un errore per eccesso di qualche percento. In caso contrario è preferibile usare la seguente espressione per il calcolo approssimato di $F_S(T)$:

$$F_S(T) \leq 1 - \exp- \{\int_0^T [\omega_S(\tau) / (1 - Q_S(\tau))]\ d\tau\} \tag{8}$$

3.2. Indici di importanza degli eventi primari

Il calcolo delle grandezze affidabilistiche a livello di Top event può considerarsi sufficiente solo nei casi in cui i valori ottenuti siano adeguatamente inferiori ai valori obiettivo prefissati. In caso contrario è

necessario migliorare il sistema con interventi correttivi mirati, non solo migliorando i componenti o i sottosistemi relativamente più deboli, ma anche utilizzando componenti meno affidabili (meno costosi) o riducendo le frequenze di test/manutenzione nei punti in corrispondenza dei quali disponibiltà e affidabilità sono maggiori del necessario. In definitiva questo significa allocare razionalmente le risorse disponibili dove è veramente necessario. L'individuazione dei componenti del sistema da considerare si effettua attraverso il calcolo degli indici di importanza dei componenti. Applicazioni tipiche degli indici di importanza sono:

- in fase di progettazione, per migliorare le caratteristiche affidabilistiche del sistema mediante adeguate modifiche progettuali;
- in fase di manutenzione, per programmare gli interventi mantenendo un adeguato livello di sicurezza;
- in caso di guasto del sistema, per definire la sequenza di verifica dei componenti per la ricerca rapida del guasto e la conseguente riduzione dei tempi di riparazione.

Per il calcolo degli indici di importanza consideriamo di nuovo la (1); passando alle probabilità si ottiene:

$$Qs(t) = q_{xi}(t)\, Qs(t)_{|\, xi\,=\,1} + (1 - q_{xi}(t))\, Qs(t)_{|\, xi\,=\,0} \qquad (9)$$

dove:

$$Qs(t)_{|\, xi\,=\,1} = Pr\,[G_1\,(q_{x1}(t), q_{x2}(t), \ldots, q_{xi-1}(t), 1, q_{xi+1}(t), \ldots, q_{xn}(t))]$$
$$Qs(t)_{|\, xi\,=\,0} = Pr\,[G_0\,(q_{x1}(t)\, q_{x2}(t), \ldots, q_{xi-1}(t), 0, q_{xi+1}(t), \ldots, q_{xn}(t))]$$

Derivando la (9) rispetto alla indisponibilità $q_{xi}(t)$ si ottiene:

$$\partial Qs(t) / \partial q_{xi}(t) = Qs(t)_{|\, xi\,=\,1} - Qs(t)_{|\, xi\,=\,0} \qquad (10)$$

La (10) rappresenta la variazione di indisponibilità nel passaggio del componente dallo stato di funzionamento ($x_i = 0$) allo stato di guasto ($x_i = 1$). Diversi indici di importanza fanno uso della (10) nota come Indice di Birnbaum $I_{Bi}(t)$. Maggiore è il valore di $I_{Bi}(t)$ maggiore è la degradazione che subisce il sistema a seguito del guasto del componente x_i. $I_{Bi}(t)$ può essere anche definito come la probabilità che lo stato del sistema dipenda solo dallo stato del componente, ossia il sistema funziona se il componente funziona, si guasta se il componente si guasta.

Gli indici di importanza degli eventi primari calcolati in ASTRA sono riassunti in tabella 1. Dalla tabella si nota la possibilità di calcolare gli indici di importanza strutturale I_{Si}, da utilizzarsi in mancanza di dati affidabilistic. In pratica questo indice considera più importanti i componenti che formano MCS del primo ordine. Per componenti in MCS di ordine superiore l'importanza è tanto maggiore quanto minore è l'ordine degli MCS in cui si trova e tanto maggiore è il numero di tali MCS.

RAW_i indica invece di quanto aumenta il rischio a seguito del guasto del componente x_i. Peranto componenti con elevato valore di RAW sono critici e la funzione che loro esplicano nel sistema deve essere garantita con elevata probabilità.

L'indice RRW_i (Risk Reduction Worth) indica di quanto si riduce il rischio se si suppone il componente x_i molto affidabile. Maggiore è RRW e maggiore è la convenienza di mantenere il componente in efficienza.

L'indice di criticità $I_{Ci}(t)$ indica di quanto varia percentualmente la probabilità del Top event a seguito di una variazione percentuale della probabilità di guasto del componente. La sua importanza è ovvia.

L'indice di Fussell-Vesely $I_{FVi}(t)$ fornisce il contributo del componente alla probabilità del top event. I valori sono molto simili a quelli forniti da $I_{Ci}(t)$, ed infatti $I_{Ci}(t)$ e $I_{FVi}(t)$ forniscono lo stesso ranking.

Gli ultimi due indici sono utili nel caso di calcolo della frequenza di incidente, il cui integrale fornisce il numero medio aspettato di guasti. $I_{BPi}(t)$ fornisce il contributo alla frequenza di guasto da parte di componenti del sistema di produzione, mentre $I_{Ei}(t)$ fornisce il contributo da parte dei componenti del sistema di protezione. La distinzione fra eventi iniziatori ed eventi relativi a modi di guasto di componenti che svolgono solo azioni di protezione viene eseguita automaticamente in ASTRA a seguito dell'analisi dei gates INH.

Infine l'indice DIM, Differential Importance Measure, fornisce la frazione della variazione totale di $Q_S(t)$ dovuta alla variazione di $q_{xi}(t)$ [12]. Importante è il fatto che questo indice gode della proprietà di additività, molto utile per definire l'importanza di gruppi di eventi.

Dal contenuto della tabella 1 si evince che quasi tutti gli indici di importanza si possono esperimere in funzione di $I_{Bi}(t)$. Ne consegue che informazioni utili possono essere ricavate dall'esame congiunto di due indici [13]. Infatti un valore elevato di un indice può essere dovuto alla elevata probabilità di guasto del componente oppure ad un elevato valore di $I_{Bi}(t)$. Ad esempio, valori elevati di $I_{Bi}(t)$ e di $I_{FVi}(t)$ indicano che il componente deve essere migliorato, mentre bassi valori di questi due indici indicano che il componente può essere sostituito con un altro meno affidabile e meno costoso. Quest'ultima situazione potrebbe non essere identificabile se l'analisi probabilistica venisse effettuata sugli MCS più significativi. Infatti bassi valori degli indici sono ricavabili dagli MCS poco significativi e generalmente questi hanno probabilità inferiore ai valori di soglia. Questo inconveniente non si verifica con l'uso dei BDD, in quanto gli indici di importanza sono calcolati su tutti gli MCS [14].

Indice di importanza	Definizione	Espressione
Indice di Birnbaum $I_{Bi}(t)$	Probabilità che il componente in esame si trovi in uno stato critico per il guasto del sistema. Questo indice non dipende dalla probabilità di guasto del componente.	$I_{Bi}(t) = \partial Qs(t) / \partial q_{x_i}(t)$
Importanza strutturale $I_{Si}(t)$	Indica l'importanza di un componente dovuta solo alla sua posizione nella funzione di struttura. Utilizzato quando non sono disponibili dati probabilistici di guasto dei componetni. Possibile classificare ulteriormente gli eventi in base al tipo (errori umani, componenti attivi, componenti passivi)	$I_{Si}(t) = I_{Bi}(t)$ con $q_{x_i} = 0.5$ per tutti gli eventi
RAW_i (Risk Achievement Worth)	Indice di aumento potenziale del rischio. RAW rappresenta l'aumento del livello di rischio a seguito del guasto del componente. Componenti con elevato valore di RAW sono critici e la funzione da loro esplicata nel sistema deve essere garantita con elevata probabilità.	$Qs(t)_{\mid x_i = 1} / Qs(t) = 1 + (1 - q_{x_j}(t)) I_{Bi}(t) / Qs(t)$
RRW_i (Risk Reduction Worth)	Indice di riduzione potenziale del rischio. Indica la riduzione potenziale del rischio nel caso in cui si supponga il componente x_i perfettamente funzionante. Valori elevati di RRW indicano componenti critici la cui affidabilità deve esere mantenuta.	$Qs(t) / Qs(t)_{\mid x_i = 0} = [1 + q_{x_i}(t) I_{Bi}(t) / Qs(t)]^{-1}$
Fussel Vesely $I_{FVi}(t)$	Contributo del componente x_i alla proabilità di guasto del sistema.	$Qs_{xi}(t) / Qs(t)$
Criticality $I_{Ci}(t)$	Indica la variazione relativa di Qs(t) per una variazione relativa di $q_{xi}(t)$.	$(\Delta Qs(t) / \Delta q_{x_i}(t)) \; Qs(t) / q_{x_i}(t) = I_{Bi}(t)\, q_{x_j}(t\tau) / Qs(t)$
Barlow-Proschan per eventi iniziatori, $I_{BPi}(t)$	Contributo del componente x_i al numero medio aspettato di guasti del sistema. Il numeratore rappresenta la frazione del numero medio di guasti dovuta al guasto di xi.	$\dfrac{\int_0^t I_{Bi}(t)\; \omega_{x_i}(\tau) d\tau}{Ws(t)}$
Importanza degli eventi protezione, $I_{Ei}(t)$	Contributo al guasto del sistema di componenti che svolgono solo azione protettiva (enabler events). Il numeratore rappresenta la frazione del numero medio di guasti dovuta al guasto di xi a seguito del verificarsi dell'evento iniziatore xj.	$\dfrac{\int_0^t [Qs(\tau)_{\mid xj = 1, xi = 1} - Qs(\tau)_{\mid xj = 1, xi = 0}] \omega_{x_j}(\tau) q_{x_i}(\tau) d\tau}{Ws(t)}$
Differential Importance Measure, DIM	Fornisce la frazione della variazione totale di Qs(t) dovuta ad una variazione della indisponibilita' degli eventi. DIM $(x_1, x_2, ..., x_n)$ = DIM)(x_1) + DIM(x_2) + ….+ DIM(x_n). DIM puo' essere calcolato, sotto opportune condizioni, in funzione di $I_{Bi}(t)$.	$DIM_i = \dfrac{dQ_{Sxi}}{dQ_S} = \dfrac{\dfrac{\partial Qs}{\partial q_i} dq_i}{\sum_k \dfrac{\partial Qs}{\partial q_k} \partial q_k}$

Tabella 1. Indici di importanza considerati nella nuova versione di ASTRA

4. ESEMPIO ILLUSTRATIVO

Allo scopo di rendere più chiari i vantaggi relativi all'analisi degli alberi di guasti secondo l'approccio BDD si farà uso di un semplice esempio.

Consideriamo il sistema semplificato di blocco automatico rappresentato in figura 4, formato da tre sensori in logica 2/3 (M1, M2, M3), dalla logica di blocco (L) e dall'attuatore (A). L' Evento Top considerato è la mancata attuazione su domanda. L' Albero dei Guasti (AdG) per l' evento Top è rappresentato in fig. 5.

L' espressione logica dell' evento Top per il sistema è la sguente:

$$Top = A \vee L \vee (M \wedge M2) \vee (M1 \wedge M3) \vee (M2 \wedge M3) \qquad (11)$$

Dove "$\wedge$" rappresenta l'operatore logico AND e "$\vee$" rappresenta l'operatore logico OR. I modi di guasto minimi, o Minimal Cut Sets (MCS) sono: A, L, M1 $\wedge$ M2, M1 $\wedge$ M3 e M2 $\wedge$ M3

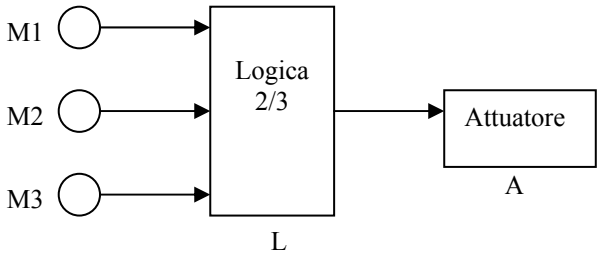


Figura 4. Sistema semplificato di attuazione automatica.

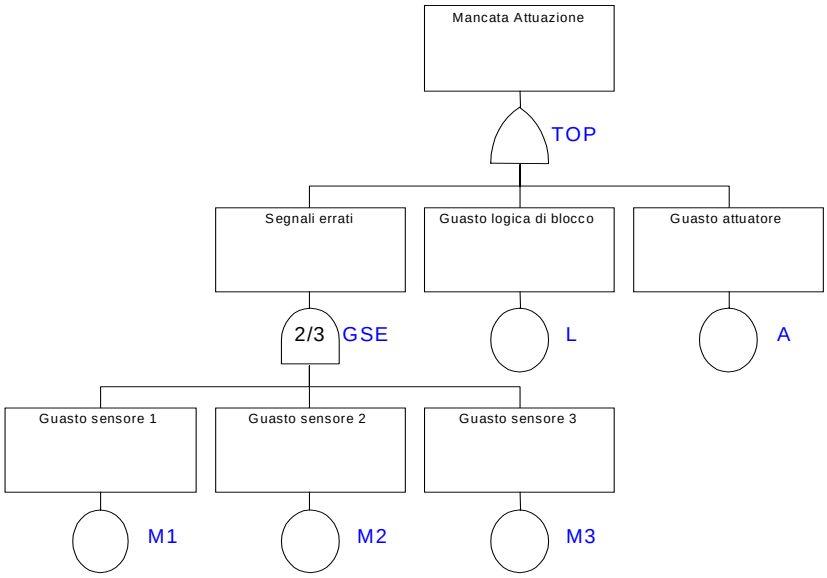


Figura 5. Albero dei guasti per il sistema semplificato di attuazione automatica di figura 4.

Senza entrare nei particolari delle regole di costruzione dei BDD, per i quali si rimanda a [4], ci si limita a mostrare in figura 6 il BDD relativo all'albero di guasto di figura 5. Il valore di indisponibilità per il sistema di figura 4 può essere calcolato sul BDD di figura 6 applicando ricorsivamente la (6). I calcoli sono riportati in Tabella 2 dove q_{M1}, q_{M2}, q_{M3}, q_L e q_A, sono le indisponibilità su domanda dei componenti. Il numero in grassetto accanto ad ogni nodo dell'ROBDD indica la sequenza di esame delle variabili.

Ipotizzando che tutti i componenti abbiano pari valore di indisponibilità alla domanda q, l'indisponibilità del sistema è data da:

$$Q_S = 2q + 2q^2 - 8q^3 + 7q^4 - 2q^5$$

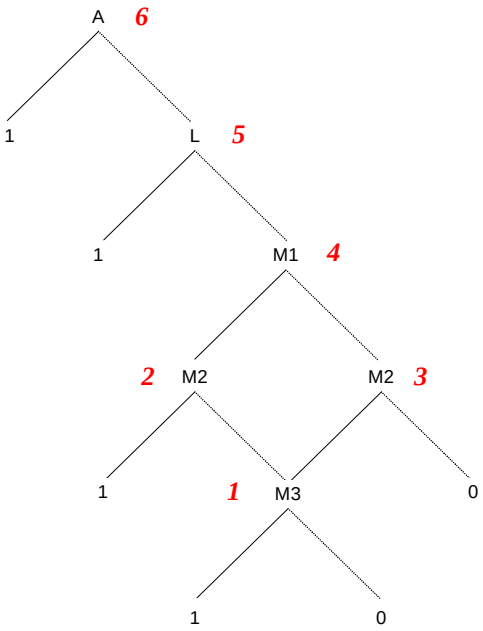


Figura 6. ROBDD dell'albero di figura 5.

Rif.	Evento	Discendente sinistro, $Q_1(t)$	Discendente destro, $Q_0(t)$	$Q_{out}(t)$ associata al nodo
1	M3	1	0	q_{M3}
2	M2	1	q_{M3}	$q_{M2} + (1- q_{M2})\, q_{M3}$
3	M2	q_{M3}	0	$q_{M2}\, q_{M3}$
4	M1	$q_{M2} + (1- q_{M2})\, q_{M3}$	$q_{M2}\, q_{M3}$	$(q_{M2} + (1- q_{M2})\, q_{M3})\, q_{M1} + q_{M2}\, q_{M3}(1- q_{M1})$
5	L	1	$(q_{M2} + (1- q_{M2})\, q_{M3})\, q_{M1} + q_{M2}\, q_{M3}(1- q_{M1})$	$q_L + [(q_{M2} + (1- q_{M2})\, q_{M3})\, q_{M1} + q_{M2}\, q_{M3}(1- q_{M1})]\, (1- q_L)$
6	A	1	$q_L + [(q_{M2} + (1- q_{M2})\, q_{M3})\, q_{M1} + q_{M2}\, q_{M3}(1- q_{M1})]\, (1- q_L)$	$q_A + \{[(q_{M2} + (1- q_{M2})\, q_{M3})\, q_{M1} + q_{M2}\, q_{M3}(1- q_{M1})]\, q_L + [(q_{M2} + (1- q_{M2})\, q_{M3})\, q_{M1} + q_{M2}\, q_{M3}(1- q_{M1})]\, (1- q_L)\}\, (1- q_A)$

Tabella 2. Calcolo della indisponibilità con approccio BDD per il sistema di figura 4

Con l'approccio MCS (eq. 4) si avrebbero invece le seguenti espressioni analitiche per l' indisponibilita':

- Upper Bound (Primo bound): $Qs_{-UB} = q + 3q^2$
- Lower Bound (Secondo bound): $Qs_{-LB} = 2q + 2q^2 - 9q^3$
- Esary-Proschan bound: $Qs_{-EP} = 2q + 2q^2 - 6q^3 + 6q^5 - 2q^6 - 2q^7 + q^8$

In figura 7 sono riportati i grafici della indisponibilità (eq. 6, curva continua) calcolati da ASTRA con la tecnica BDD. I grafici sono effettuati per valori crescenti delle indisponibilità dei componenti e nell'ipotesi che tutte le indisponibilità abbiano il medesimo valore. Sono inoltre riportati i valori dei bounds (Upper-Bound, Lower-Bound ed Esary-Proschan bound, eq. 4) che si applicano normalmente effettuando l'analisi probabilistica sui minimal cut sets. Come si può vedere, solo per valori dell'ascissa minori di 0.1, l'analisi probabilistica effettuata con la tecnica dei bounds fornisce valori accettabili. Il primo bound dà valori uguali a 1 per $q > 0.32$. Fa eccezione il solo bound di Esary-Proshan, che nel semplice caso studio considerato dà risultati particolarmente buoni.

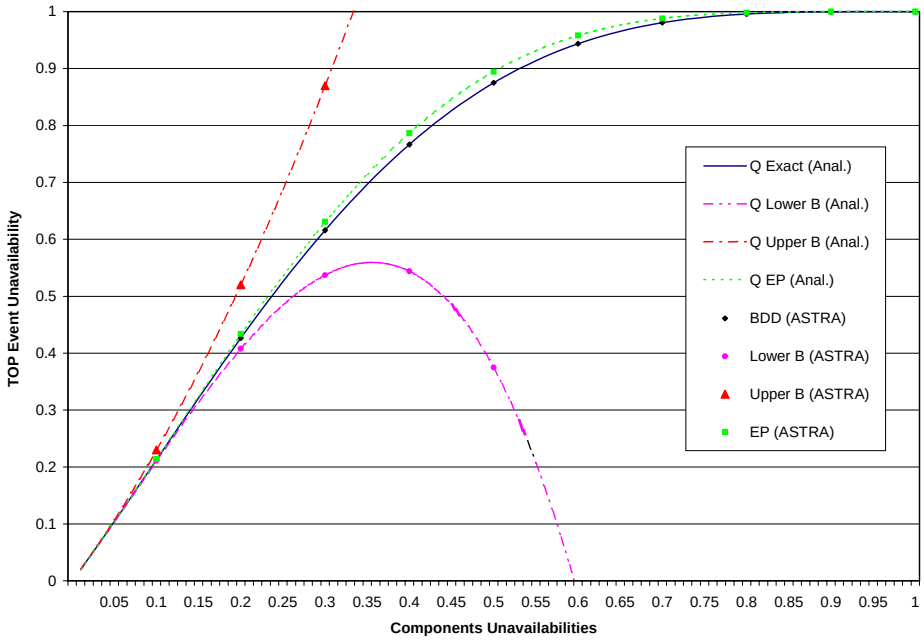


Figura 7. Calcolo dell' indisponibilità del sistema di figura 4, nell'ipotesi di valori uguali di indisponibilità dei componenti.

5. IL SOFTWARE ASTRA

ASTRA e' un pacchetto software utilizzabile su Personal Computers sotto diverse versioni del sistema operativo Windows, e contiene diversi programmi come schematizzato in figura 8.

- **ASTRA-FTA** e' il pacchetto base. Esso contiene il DESKTOP dal quale possono essere lanciate tutte le applicazioni. Un editore grafico, supportato da Windows permette la costruzione interattiva dell'albero di guasto. ASTRA–FTA considera i seguenti operatori logici: AND, OR, NOT, XOR, INH e K/N. Possono essere considerate le condizioni al contorno per calcolare la probabilità del TOP event condizionata allo stato di alcuni componenti. L'albero di guasto può poi essere disegnato in formato A4/A3 tramite un modulo grafico (Fault Tree Drawer). L'analisi di un albero di guasto e' suddivisa in due fasi, l'analisi logica e l'analisi probabilistica. La prima, basata sull'uso della tecnica BDD, permette il calcolo del grafo che contiene di tutti gli insiemi minimi di guasto (MCS). In aggiunta, l'uso opzionale di soglie di tipo logico e probabilistico permette l'estrazione degli MCS più significativi ed il calcolo dell'errore di troncamento associato. L'analisi probabilistica, cioè la determinazione dell'indisponibilità e del numero atteso di guasti dell'evento top e degli MCS è effettuata al tempo di missione. Si possono considerare sia componenti non riparabili (caratterizzati sia da probabilità costante che da ratei di guasto costanti) che componenti riparabili on–line (caratterizzati dal tempo medio di riparazione). E' altresì possibile modellizzare componenti testati sequenzialmente. Le importanze dei componenti (secondo le misure di Fussel Vesely e Barlow Proschan) sono anch' esse calcolate al tempo di missione. La stampa dei risultati dell'analisi e' possibile grazie al modulo Report Writer che genera un file ASCII. Nella nuova release di ASTRA, la gestione dei moduli e dei progetti sarà migliorata, ad esempio sarà possibile lavorare contemporaneamente su diversi alberi di uno stesso progetto nell'ambito della medesima sessione di lavoro. L'editore grafico sarà migliorato e sarà, ad esempio possibile individuare dei sotto-alberi per l' analisi logica e probabilistica evidenziandoli direttamente tramite l' editore stesso. La tecnica delle condizioni al contorno verrà estesa ai sottoalberi permettendo il calcolo dell'evento top condizionato al successo od al fallimento certo di intere parti del sistema analizzato. Sarà poi possibile effettuare, a richiesta dell'utente, un'analisi completa dell'albero, senza dovere necessariamente effettuare l'analisi logica e probabilistica in due fasi distinte. Il modulo di Report Writer verrà potenziato, reso in grado di produrre rapporti direttamente editabili in MS Word e verrà reso in grado di documentare i risultati di tutte le analisi.
- **ASTRA-FTA Plus** costituisce una versione sperimentale di ASTRA-FTA che comprende tutti i moduli della versione base a differenza dell' editore dell' albero di guasto di tipo grafico che è sostituito da una versione più potente. L'editore grafico di ASTRA-FTA Plus è poi interfacciato con una banca dati di componenti realizzata in MS ACCESS dalla quale i dati affidabilistici dei componenti dell'albero da

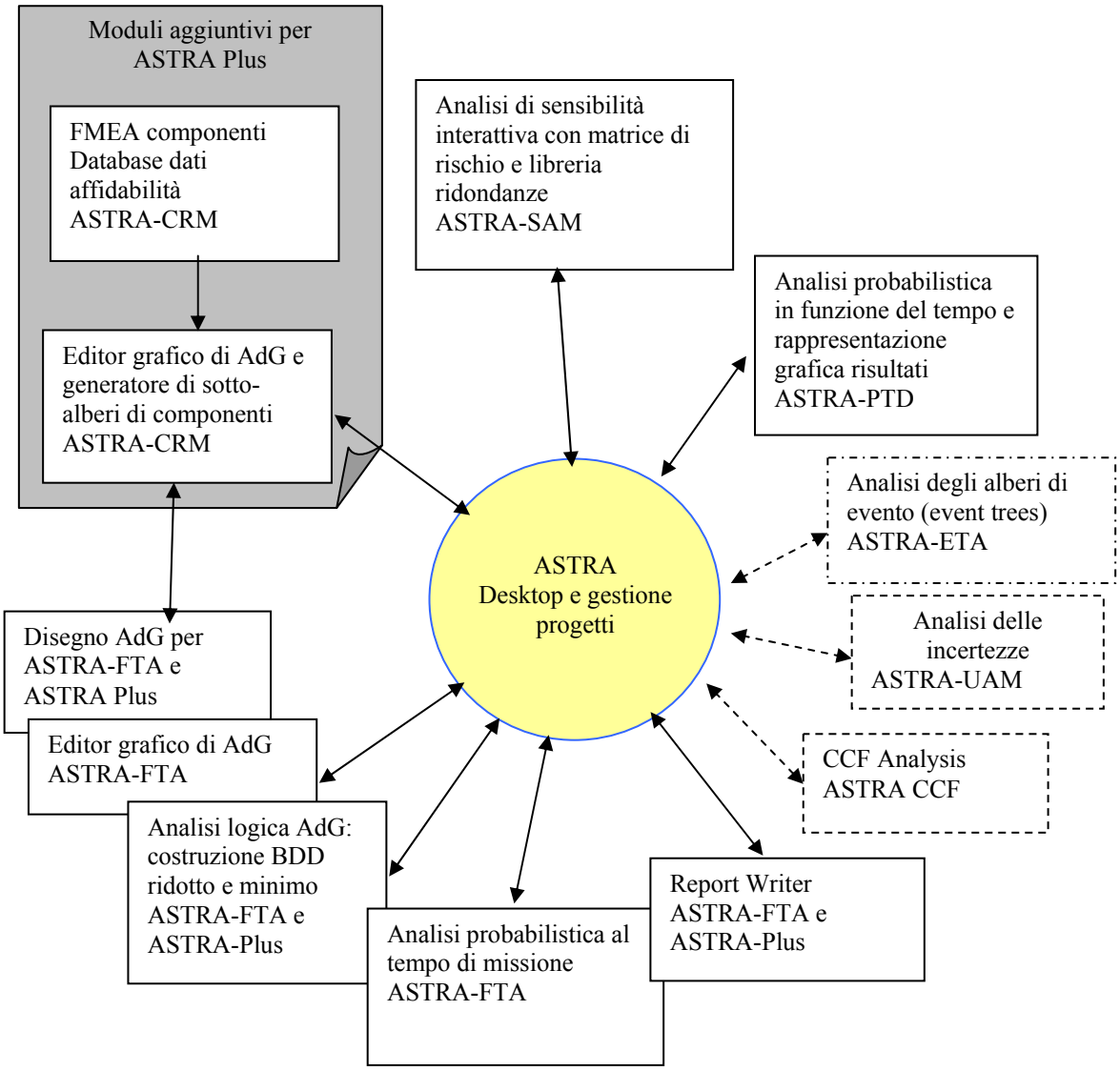


Figura 8. Schema dei diversi moduli costituenti il pacchetto ASTRA.

analizzare possono essere direttamente caricati nell'albero stesso. Nella nuova versione di ASTRA tool set, ASTRA-FTA Plus package sarà reso completamente operativo e dotato anch' esso della nuove caratteristiche del software ASTRA-FTA base (e.g. analisi diretta di sotto-alberi, condizioni al contorno etc.). Inoltre il data base di componenti verrà dotato di una tassonomia di esempio.

- **ASTRA-PTD**. Questo modulo aggiuntivo sia per ASTRA-FTA che per ASTRA-FTA Plus permette il calcolo in funzione del tempo sia della indisponibilità che del numero atteso di guasti dell'evento Top. Il calcolo in funzione del tempo permette anche di tenere in conto di componenti con diverse politiche di ispezione e di test, sia di tipo sequenziale che di tipo differito (staggered). Gli indici di importanza (Fussell-Vesely, aumento e riduzione potenziale del rischio, etc.) sono anch'essi calcolati in funzione del tempo. Tutte le grandezze calcolate sono rappresentabili in funzione del tempo. Attualmente il modulo PTD lavora sugli insiemi minimi di taglio significativi forniti dall'analisi logica e permette ad esempio il calcolo in funzione del tempo dell'upper bound (first bound e bound di Esary Proshan) e del lower bound della indisponibilità del TOP event. Nella nuova versione di ASTRA, il modulo PTD implementerà anche il calcolo probabilistico esatto, mediante la tecnica BDD, della system unavailability, del numero atteso di guasti e degli indici di importanza di tabella 1. Sarà anche possibile salvare i risultati in formato EXCEL per ulteriori analisi o rappresentazioni.
- **ASTRA-SAM**. E' il modulo aggiuntivo di ASTRA-FTA per l'analisi di sensibilità interattiva. Il calcolo degli indici di criticità consente di individuare rapidamente i punti relativamente più deboli dell'impianto sui quali deve indirizzarsi l'attenzione dei progettisti per il miglioramento delle caratteristiche

affidabilistiche dell' impianto, qualora la probabilità degli stati critici, corrispondenti a conseguenze non accettabili, fossero troppo elevate. A tale scopo è necessario definire un livello accettabile di probabilità del top event in funzione della gravità delle conseguenze. La relazione fra gravità delle conseguenze dei potenziali incidenti e i corrispondenti valori di frequenza è definita mediante una matrice di rischio. L'analisi può essere effettuata in modo concorrente su tutti i diversi alberi di guasto contenenti un componente del quale si vuole studiare l'effetto sull'accadimento dell'evento TOP [15]. ASTRA-SAM contiene inoltre una libreria di configurazioni ridondanti comprendente tra l'altro esempi di stand-by di tipo caldo e freddo. L'analisi probabilistica è effettuata al tempo di missione direttamente sulla struttura BDD e supporta l'uso di tecniche di cut-off sia di tipo logico sia probabilistico. Nella nuova versione di ASTRA-SAM, l'interfaccia utente verrà completamente aggiornata e il programma verrà reso operativo per entrambe le versioni ASTRA-FTA ed ASTRA-Plus, con la possibilità, in questo secondo caso, di essere interfacciato con il data-base di componenti. Sarà possibile effettuare delle analisi in funzione del tempo allo scopo di tenere in conto delle politiche di test dei componenti e l' utente potrà definire una matrice di rischio di default che potrà essere richiamata ed opportunamente modificata.

In figura 8 sono riportati i moduli precedentemente descritti e, in tratteggio, i moduli ETA e CCF, già esistenti ma che richiedono una fase di test e validazione. La realizzazione eventuale di un modulo di propagazione delle incertezze dipenderà dalle necessità e dalle sinergie con i programmi istituzionali del CCR.

Per quanto concerne il modulo ETA, sono stati messi a punto nuovi algoritmi basati sull'approccio *Fault tree linking,* ossia sulla rappresentazione in termini di AdG equivalente di ciascuna sequenza. Il metodo d'analisi sviluppato crea una differenziazione della tipologia di eventi tale da ridurre i tempi di calcolo, dal momento che generalmente la semplice applicazione dell'approccio *Fault tree linking* trasforma una sequenza dell'AdE in un albero dei guasti molto complesso. E' stato quindi sviluppato un algoritmo di pre processamento, sempre basato su BDD, che consente di ridurre la complessità dell'albero di guasto risultante prima di passare all'analisi logica e probabilistica.

6. CONCLUSIONI

La presente memoria ha illustrato la metodologia ASTRA per l' analisi di affidabilità di sistemi complessi. Dopo un richiamo della metodologia BDD, alla base di ASTRA, si e' illustrato in dettaglio come la tecnica BDD permetta di effettuare un' analisi probabilistica esatta del Top-event e degli indici di criticità. Il calcolo esatto effettuato con ASTRA del valore di indisponibilità dell' evento Top di un caso studio e' stato confrontato con il risultato analitico e con i valori dei bounds, e per valori crescenti di probabilità di guasto degli eventi primari mostrando così i limiti di un calcolo probabilistico approssimato.

La possibilità di effettuare un calcolo probabilistico esatto del Top event è fondamentale per l'analisi di importanza dei componenti e per i casi in cui la probabilità dell'evento di successo (negato) non può considerarsi molto prossima all'unità. In un lavoro precedente [16] relativo al campo delle salvaguardie nucleari, alcuni dei presenti autori hanno, ad esempio, indagato le possibilità di proliferazione nucleare in un dato ciclo del combustibile (rappresentata mediante degli alberi di successo) ed effettuato mediante ASTRA il calcolo della probabilità di successo data la volontà di proliferare del paese ospitante. Un altro campo, attualmente di grande attualità, dove un'analisi probabilistica esatta con elevati valori di probabilità degli eventi primari è richiesta, è quello dello studio della vulnerabilità dei sistemi tecnologici complessi ad eventi esterni o ad azioni di sabotaggio [17]. In tale caso le probabilità da associare agli eventi sono le probabilità condizionate di guasto dei componenti stessi all'azione di sabotaggio considerata.

RINGRAZIAMENTI

Il presente lavoro è stato effettuato nell'ambito dell'attività di *analisi dei sistemi applicata alla salvaguardia nucleare,* svolta presso l'unità di Salvaguardie Nucleari e non Proliferazione del CCR. Ringraziamo i capi unità A. Poucet e J. Gonçalves per il sostegno al lavoro. ASTRA e' il risultato di programmi quadro di ricerca diretta del CCR, di contratti terzi e di re-investimenti derivanti dalla commercializzazione. Ringraziamo J. Bonnin della DG-RTD, precedentemente alla DG-JRC, e G. Barry, T. Gering e V. Koutsiouris della DG-JRC per il supporto finanziario dato all'attività di aggiornamento di ASTRA.

ELENCO DEI SIMBOLI

C_i	Generico MCS
N	Numero di MCS
N	Ordine MCS
x_i	i-esima variabile booleana, stato guasto componente i-esimo
$q_{xi}(t)$	Indisponibilta' del componente i-esimo al tempo t
λ	Component failure rate
$\omega_{xi}(t)$	Unconditional failure frequency of a component
Qs(t)	Indisponibilta' del systema (top event) al tempo t
$Qs(t)_{\mid xi=1}$	Indisponibilta' del systema (top event) al tempo t con xi guasto
$Qs(t)_{\mid xi=0}$	Indisponibilta' del systema (top event) al tempo t con xi funzionante
T	Tempo di missione
Ws(T)	Numero medio atteso di guasti del sistema
$F_S(T)$	Upper bound per l'inaffidabilità del sistema al tempo di missione
$\omega_S(t)$	Frequenza non condizionala di guasto del sisetma
I_{Si}	Indice di importanza strutturale dell'evento xi
$I_{FVi}(t)$	Indice di Fussell-Vesely dell'evento xi
$I_{Ci}(t)$	Indice di Criticità dell'evento xi
$I_{BPi}(t)$	Indice di Barlow-Proschan per l'evento iniziatore xi
$I_{Ei}(t)$	Indice di importanza evento protezione xi

BIBLIOGRAFIA

[1] S. Contini, S. Scheer; M. Wilikens, G. De Cola; G. Cojazzi. ASTRA, an Integrated Tool Set for Complex Systems Dependability Studies, in *Tool Support for System Specification, Development and Verification, Advances in Computing Science,* R. Berghammer, Y. Lakhnech (Eds.), SpringerWienNewYork, pp 77-89, 1999.

[2] ASTRA-FTA, Fault Tree Analysis Module, User Manual, EC-JRC, S.P.I.98.64.

[3] S. Contini, G. De Cola, A top down approach to fault tree analysis using binary decision diagrams, *Journal Europèen des Systèmes Automatisès*, 1996.

[4] S. Contini, Recenti sviluppi metodologici nell'analisi degli alberi di guasto, *VGR '98*, Pisa, 1998.

[5] A. Amendola, C. Clarotti, S. Contini, F. Spiozzichino, Analysis of Complete Logical Structures in System Reliability Assessment, EUR report, JRC-Ispra, 1980.

[6] B.D. Johnston, R.H. Matthews, Non-coherent Structure Theory: A Review and its Role in Fault Tree Analysis, SRD Report R 245, 1983.

[7] J.D. Andrews, "To not or not to not", *Proc. Int.l System Safety Conference*, Fort Worth, 2000.

[8] A. Rauzy, New Algorithms for Fault Trees Analysis, *Reliability Engineering and System Safety*, Vol 40 Issue 3, 203-211, 1993.

[9] R.M. Sinnamon, J.D. Andrews, Quantitative fault tree analysis using Binary Decision Diagrams, *Journal Europèen des Systèmes Automatisès*, 1996.

[10] J. Liu, Z.J. Pan, An improved Algorithm of kinetic tree theory, *Rel. Eng. System Safety*, Vol 23, 1988.

[11] C. Clarotti, Limitations of minimal cut set approach in evaluating reliability of systems with repairable components. *IEEE Trans. Reliability*, Vol. R-30, (1981).

[12] E. Borgonuovo, G.E. Apostolakis, A new importance measure for risk-informed decision making, *Rel. Eng. and System Safety,* Vol. 72, (2001).

[13] M. van der Borst, H. Schoonakker, An overview of PSA importance measures, *Rel. Eng. and System Safety,* Vol . 72, (2001).

[14] Y. Dutuit, A. Rauzy, Efficient algorithms to assess component and gate importance in fault tree analysis, *Rel. Eng. and System Safety,* Vol 72, (2001).

[15] S. Contini, S. Scheer, M. Wilikens, Sensitivity Analysis for System Design Improvement, *International Conference on Dependability of Systems and Networks*, New York, 2000.

[16] G.G.M. Cojazzi, G. Renda, S. Contini, Qualitative and Quantitative Analysis of Safeguards Logic Trees, C. Spitzer et al. (eds.) *Proc. PSAM 7 ESREL'04*, June 14-18, 2004, Berlin.

[17] D.E. Peplow, C.D. Sulfredge, R.L. Sanders, R.H. Morris, T.A. Hann, Calculating Nuclear Plant Vulnerability Using Integrated Geometry and Event/Fault-Tree Models, *Nuclear Science and Engineering,* Vol. 146, 2004.