Affidabilità e sicurezza degli schemi di protezione del sistema elettrico: oltre la IEC 61508

Luca Ferrarini, Leonardo Ambrosi, Emanuele Ciapessoni

Questo articolo[1] considera il problema dell'analisi di rischio dei sistemi di protezione e degli schemi di protezione della rete di trasmissione elettrica. In accordo con la norma IEC 61508, è stato sviluppato un modello ibrido per l'analisi di sistemi di protezione. Tale modello consente di valutare, sulla base di opportuni indici di rischio, i requisiti di affidabilità e sicurezza dei sistemi di protezione. L'uso di modelli analitici nell'analisi del rischio permette di valutare il livello di sicurezza associato alle diverse strategie di protezione e consente di identificare specifiche criticità ICT dei sistemi di protezione.

In Italia, come in molti paesi europei e in molti altri ambiti industriali, il settore elettrico ha affrontato la liberalizzazione del mercato elettrico, il che comporta il passaggio da un sistema facilmente prevedibile e regolabile con un unico operatore, ad un sistema multi operatore. In questo quadro lo sviluppo della rete elettrica e dei relativi sistemi d'automazione, costituisce un processo decisionale complesso soggetto a scelte di carattere economico, tecnico e ambientale in uno scenario caratterizzato da persistente *incertezza*. In questo scenario è estremamente importante definire criteri di "qualità", che devono essere rispettati da tutti gli operatori che consentano, tramite una corretta e positiva cooperazione, di garantire un servizio adeguato all'utente. Nonostante l'evoluzione in atto, i classici criteri deterministici per garantire la sicurezza del sistema elettrico, adottati prima della liberalizzazione, sono ancora applicati in sede di libero mercato. Tali criteri sono basati sul fatto che ogni condizione operativa anomala in un set predefinito di contingenze soddisfa criteri di performance predefiniti.

Questa scelta permette di progettare i sistemi di protezione senza prendere in considerazione tutte le combinazioni di configurazioni di stati e tutte le condizioni di esercizio, cosa inattuabile per un sistema così complesso.

Sebbene efficace nella pratica, l'approccio deterministico tende a concentrarsi sugli eventi più severi e credibili, cosa che porta a un sistema di protezione sovradimensionato e poco flessibile, con ovvie conseguenze economiche per gli operatori e per gli utenti. I principali limiti consistono nel non considerare la frequenza e l'impatto delle contingenze, e cioè nel non considerare in modo completo il rischio, inteso come una combinazione della probabilità degli eventi indesiderati con la gravità dei loro effetti (che può essere più o meno "catastrofica").

L'approccio deterministico alla gestione della sicurezza può essere sostituito da un approccio basato sul rischio: molti studi [3,4,6,8] dimostrano i possibili guadagni associati all'uso di un approccio basato sul rischio nell'analisi, valutazione e gestione della sicurezza del sistema elettrico. In questo articolo si propone l'applicazione dell'analisi del rischio nel ciclo di vita di un sistema di protezione o di uno schema di protezione della rete di trasmissione. Il principale riferimento normativo in quest'ambito, è lo standard IEC 61508. Tuttavia, i sistemi elettrici presentano problemi specifici relativamente all'affidabilità e sicurezza, cosa che può portare alla necessità di un'integrazione dello standard stesso, come suggerito nel seguito.

Caratteristiche del sistema elettrico

Interconnessione dei sottosistemi

Il sistema elettrico è essenzialmente caratterizzato dalla sua complessità, dalla sua estensione (è per sua natura *wide area*) e dalla forte interconnessione dei diversi sottosistemi. Il sistema elettrico è, infatti, composto di un numero molto alto di elementi di diversi tipi (linee, sbarre, trasformatori, interruttori ecc.), elettricamente interconnessi con topologie variabili da zona a zona e da paese a paese. Questo fa sì che comportamenti anomali di alcuni elementi possano avere conseguenze inaspettate su altri elementi o sottosistemi, localizzati in altre zone e che operano in condizioni diverse [2]. Inoltre l'interconnessione elettrica

L. Ferrarini, L. Ambrosi - Politecnico di Milano; E. Ciapessoni, CESI Ricerca

[1]Attività finanziata nell'ambito della "Ricerca di Sistema" per il Settore Elettrico (Decreto 28.02. 2003, "Modalità di gestione del Fondo per il finanziamento delle attività di ricerca e sviluppo di interesse generale per il sistema elettrico nazionale", Ministero per le Attività Produttive)

comporta che la propagazione dei fault sia estremamente veloce. In queste condizioni, l'analisi del rischio della rete di trasmissione è molto complessa. Benché gli elementi di rete sono standardizzati, risulta infatti difficile, in fase di progetto, stimare il loro modo di operare quando sono interconnessi in condizioni di esercizio. Queste difficoltà sembrano imporre la necessità di ripensare il concetto stesso di livello d'integrità della sicurezza (*Safety Integrity Level* - SIL) come definito nello standard IEC 61508, essendo questo insufficiente a caratterizzare il livello di sicurezza dei singoli elementi, e non facilmente applicabile a sottosistemi complessi o all'intero sistema.

Scatti indesiderati

Lo standard IEC 61508 si concentra sul fatto che i sistemi di protezione possono non intervenire in caso di *fault*. Dal punto di vista del servizio invece, una delle cause più importanti di indisponibilità è data dagli scatti indesiderati (*undesired trip*), che spesso comportano l'apertura in cascata delle linee elettriche [2] per l'intervento delle protezioni di sovracorrente o per altri fenomeni. Si deve notare che gli scatti indesiderati delle protezioni non dipendono necessariamente da un guasto o un errore delle protezioni stesse, ma da fattori "esterni" (fenomeni wide area), che non consentono di misurare e valutare correttamente lo stato di funzionamento delle linee [9], [Xingbin].

Per trattare questi aspetti è necessario adottare una terminologia ben definita per caratterizzare e valutare le proprietà caratteristiche dei sistemi di protezione. Noi useremo la *fidatezza* come la proprietà principale di un sistema di protezione. La fidatezza consiste nella capacità di operare correttamente ed è definita come la combinazione dell'*affidabilità*, la capacità di un sistema di protezione di intervenire per un fault nella zona di protezione, e della *sicurezza*, la capacità di non intervenire quando non richiesto, ad esempio per un fault esterno alla zona di protezione.

Vincoli dinamici

Un altro aspetto importante dei sistemi elettrici, poco considerato o addirittura ignorato dallo standard IEC 61508, consiste nella dinamicità delle condizioni che il sistema deve soddisfare per essere "sicuro". Una condizione può infatti essere valutata, o meno, come "sicura" a seconda delle condizioni di funzionamento di altri sottosistemi o dell' intero sistema.

L'adozione di un approccio dinamico, che consente un'analisi più efficace del sistema elettrico e in particolare della rete di trasmissione, permette di sviluppare un sistema di protezione più preciso e selettivo, sulla base di specifici indici di rischio [7]. Chiaramente, ciò richiede di considerare questi comportamenti, non solo nella fase di progetto dei sistemi di protezione, ma anche nella fase di valutazione. A tal fine, in alcuni casi può essere necessario sviluppare modelli adatti per le diverse condizioni di esercizio.

Un modello ibrido modulare per la rete di trasmissione

Un metodo per valutare la sicurezza funzionale del sistema elettrico è lo sviluppo di un modello in grado di catturare sia la parte dinamica e probabilistica a tempo continuo del sistema sia la parte ad eventi.

Per ottenere questo risultato è stato sviluppato un modello ibrido e modulare (cfr figura 1). Nella figura si notano gli elementi principali della rete di trasmissione (linee, sbarre, trasformatori, interruttori) con le relative interfacce e connessioni.

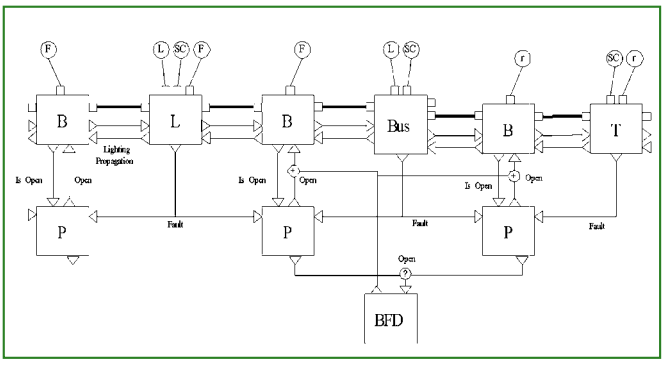

Figura 1 - Schema del modello ibrido della rete di trasmissione

I criteri utilizzati per lo sviluppo del modello sono i seguenti.

Modularità

È sicuramente consigliabile avere una metodologia di modellizzazione e un ambiente di simulazione, in cui l'utente possa comporre i moduli del sistema, che corrispondano direttamente ai componenti fisici, invece che scrivere equazioni. Questo porta a considerare ogni modulo come un generico componente con il suo comportamento e i relativi vincoli. Il modello completo sarà quindi composto dall'aggregazione dei singoli moduli, ciò consentirà all'utente di evitare di scrivere equazioni.

Comportamento ibrido

Dato che il sistema che si sta analizzando si comporta sia in maniera continua per quanto riguarda i fenomeni elettrici, sia in maniera discreta per gli eventi come rotture e guasti, è necessario considerarli entrambi e considerare le interazioni tra le due parti (ovviamente il modello discreto è un'approssimazione di un comportamento continuo estremamente rapido e a livello atomico, è perciò inutile per la trattazione da considerare come tale).

Per ottenere tale risultato, la parte discreta è stata modellizzata utilizzando le Reti di Petri, una tecnica ben nota per rappresentare sistemi ad eventi. Le Reti di Petri ordinarie sono però state estese in modo da generare dei segnali in uscita e accettare degli input dal modello continuo.

Comportamento stocastico

Alcune transizioni delle reti di petri sono state condizionate ad un ritardo, regolato da una variabile stocastica come specificato nel formalismo delle GSPN [1]. Ciò significa che una transizione stocastica è associata ad un valore che rappresenta il rateo medio di accadimento dell'evento, generalmente rappresentato con la lettera λ.

È necessario notare come alcuni di questi parametri λ siano eso-

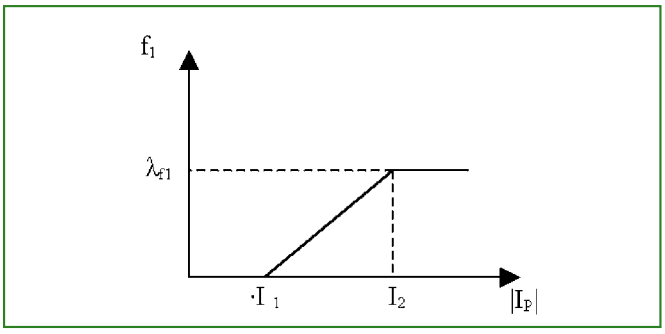

Figura 2 - Dipendenza della frequenza di guasto di un dispositivo elettrico dalla corrente circolante

geni, ovvero rappresentano dei fenomeni fisici esterni al modello, come cadute di alberi sulle linee o la fulminazione di elementi elettrici, ma altri non lo siano. Un tipico esempio è l'effetto a cascata. Si consideri il rateo di guasto di un componente elettrico. Questo può dipendere dalla corrente istantanea che circola al suo interno, come specificato nella figura 2.
Dal punto di vista della modellizzazione e della simulazione, significa che il rateo di guasto di una transizione stocastica della rete di Petri del modello ad eventi del sistema, dipende da un valore che viene calcolato dalla parte continua del modello dello stesso componente. Inoltre anche la stessa parte continua è influenzata da quella discreta per la quale inoltre non è possibile effettuare previsioni deterministiche di evoluzione.
Nel seguito verranno spiegati i dettagli della modellizzazione effettuata per il sistema.

Linea elettrica
La linea è fondamentalmente un elemento di trasmissione. La parte continua del modello prende in considerazione il fatto che la linea può essere interrotta (per lo scatto di un interruttore o per un guasto), può andare in corto circuito (ancora un guasto o per una causa esterna) o può essere colpita da un fulmine. La modellizzazione della fulminazione è stata semplificata ad un comportamento "logico", poiché la modellizzazione fisica dello stesso esula dallo scopo del modello. Il comportamento continuo è presentato nella figura 3.
La parte a tempo discreto descrive invece gli altri comportamenti della rete (cfr figura 4).
Il significato di posti e transizioni è il seguente:

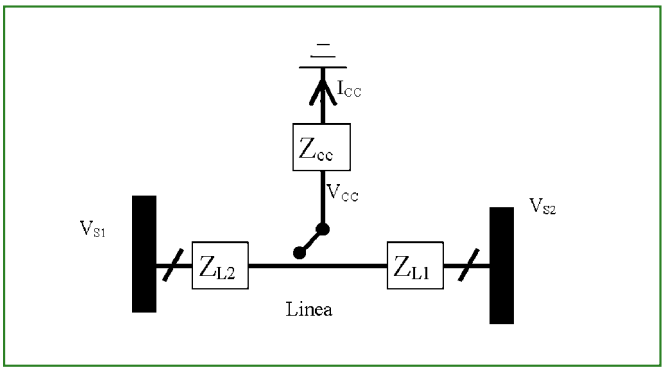

Figura 3 - Modello del comportamento continuo di una linea elettrica

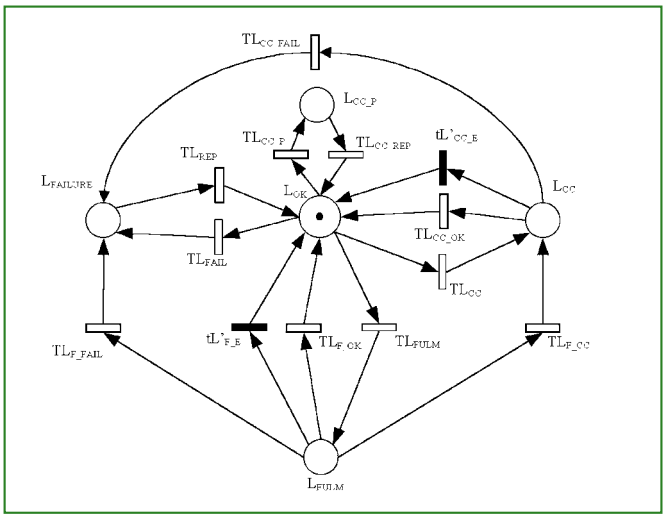

Figura 4 - Rete di Petri che modellizza una linea elettrica

Posti:
- L_{OK} = la linea funziona correttamente.
- L_{CC} = la linea è in corto circuito.
- L_{CC}_P = la linea è in corto circuito permanente.
- L_{FULM} = la linea è fulminata.
- $L_{FAILURE}$ = la linea è guasta.

Transizioni:
- TL_{FULM} = la linea è colpita da un fulmine.
- TL_{F_OK} = il fulmine si estingue autonomamente e la linea ritorna in stato di OK.
- tL'_{F_E} = il fulmine si estingue a causa dell'intervento delle protezioni. Questa transizione immediata è condizionata dal fatto che: $|I_{LINE}|<\varepsilon$.
- TL_{CC} = la linea dallo stato di OK va in corto circuito col terreno.
- TL_{CC_OK} = il corto circuito si estingue autonomamente.
- tL'_{CC_E} = il corto circuito si estingue grazie all'intervento delle protezioni. Questa transizione è condizionata dal fatto che $|V_{LINE}| <\varepsilon$.
- TL_{CC_P} = la linea va in stato di corto circuito permanente.
- TL_{CC_REP} = la linea viene riparata dallo stato di corto circuito permanente.
- TL_{FAIL} = rottura di una linea (normalmente dovuta ad un oggetto esterno).
- TL_{REP} = la linea viene riparata.
- TL_{F_FAIL} = guasto di una linea causato da un fulmine. Gli effetti del fulmine si estinguono autonomamente.
- TL_{F_CC} = la linea va in corto circuito a causa di un fulmine. L'energia del fulmine viene considerata scaricata a terra.
- TL_{CC_FAIL} = la linea si guasta a causa di un cortocircuito.

Il comportamento della rete di Petri può ora essere dedotto abbastanza semplicemente.
Infine si deve considerare l'interazione dei due modelli continuo e discreto. Ad esempio, la caduta di un albero su una linea genera un cortocircuito, ciò può essere assimilato alla chiusura di un interruttore fittizio tra la linea e massa e ciò comporta il fatto che la relativa transizione sulla rete di Petri scatta.

Interruttore
L'interruttore può essere modellato con un approccio simile. Esso possiede quattro stati logici fondamentali: aperto, chiuso, bloccato aperto, bloccato chiuso. Le transizioni tra gli stati sono abbastanza semplici e possono essere dedotte facilmente dal nome assegnato alle transizioni. Il modello a reti di Petri è rappresentato nella figura 5.

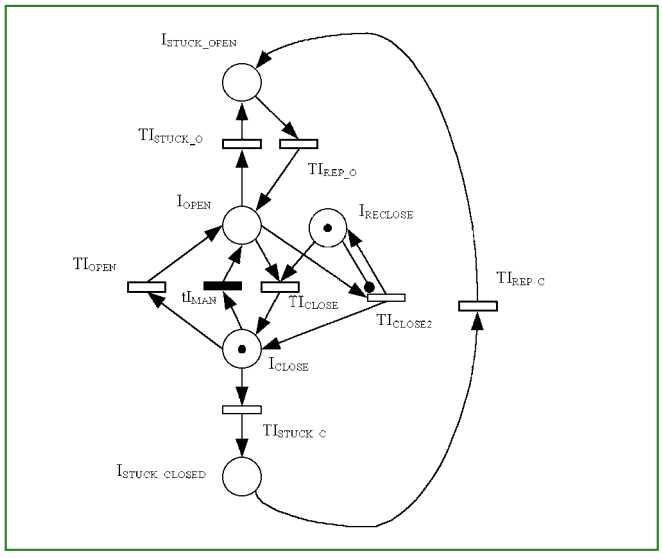

Figura 5 - Rete di Petri che modellizza un interruttore

Come si nota, è stato anche modellata la richiusura automatica. Dopo un'apertura, l'interruttore si può chiudere autonomamente (con una transizione stocastica). Se l'interruttore dovesse aprirsi di nuovo, a questo punto si potrebbe chiudere nuovamente solo con la transizione T_{close2}, questa transizione è condizionata dal fatto che le linee connesse ad esso siano in uno stato funzionante.

Transizioni:
- tI_{MAN} = apertura di un interruttore a seguito di un comando manuale o per l'intervento del BFD (Breaker Failure Device).
- TI_{OPEN} = apertura di un interruttore per l'intervento di una protezione.
- TI_{CLOSE} = richiusura veloce dell'interruttore.
- TI'_{CLOSE2} = richiusura dell'interruttore condizionata al corretto funzionamento degli elementi connessi a desso.
- TI_{STUCK_C} = rottura dell'interruttore da chiuso a bloccato chiuso.
- TI_{STUCK_O} = rottura dell'interruttore da aperto a bloccato aperto.
- TI_{REP_O} = riparazione dell'interruttore da bloccato chiuso.
- TI_{REP_C} = tempo che trascorre tra il guasto di un interruttore ed il momento in cui questo viene individuato. L'interruttore verrà quindi aperto e riparato (transizione TI_{REP_O}).

Sbarre e Trasformatori
Come per gli altri elementi, anche le sbarre e i trasformatori sono state modellate con la stessa procedura. I dettagli sono omessi per semplificare la trattazione.

Simulazione

Al fine di valutare quantitativamente il suddetto modello, deve essere usato un ambiente adatto alla simulazione. Il simulatore dovrebbe essere sufficientemente esatto da poter essere usato in presenza di dinamiche tempo-continue, di dinamiche basate su eventi discreti e di dinamiche stocastiche.
La nostra scelta è caduta sull'ambiente *Modelica/Dymola*. Si tratta di una modellistica e struttura di simulazione orientata agli oggetti, con una descrizione orientata ai componenti di facile comprensione, con porte fisiche e di comunicazione, dotata di un'accurata manipolazione simbolica delle equazioni, che permette sia all'utente di descrivere le equazioni direttamente nel dominio a tempo continuo sia di ottenere un codice ottimizzato di simulazione.
È un simulatore basato sul tempo, il che significa che la parte a eventi discreti deve essere trattata adeguatamente per un'efficiente ed efficace esecuzione. Analogamente, non c'è nessun supporto per comportamenti stocastici, che devono quindi essere introdotti e gestiti esplicitamente. Attualmente, sono stati costruiti i modelli base della linea, della sbarra, del trasformatore, dell'interruttore, del generatore e del carico.
Tali componenti specifici e riutilizzabili sono stati modellati come sistemi ibridi, il cui comportamento interno è dato da una opportuna combinazione del sottomodulo dinamico continuo con un sottomodulo a eventi discreti stocastici.
In particolare, il sottomodulo stocastico della rete di Petri è stato direttamente implementato in *Modelica*, sfruttando la possibilità di usare "le funzioni esterne". Particolare cura è stata messa nella modellistica dei comportamenti di commutazione (dovuti per esempio agli interruttori o a guasti) ed all'interazione reciproca fra la parte di continua e discreta di ogni componente, oltre che alla "trasmissione" di eventi fra componenti. In particolare, il sottomodulo della rete di Petri stocastico è stato direttamente implementato in *Modelica*, come modello a parte, sfruttando la possibilità di usare le funzioni esterne.
Particolare cura è stata messa nella modellistica dei comportamenti di commutazione (dovuti per esempio agli interruttori o a guasti, che determinano una brusca variazione dinamica delle correnti e tensioni, quindi pongono seri problemi di integrazione numerica oltre che concettuale) e all'interazione reciproca fra la parte di continua e discreta di ogni componente, oltre che alla trasmissione di eventi fra componenti.
I due sottomodelli, rispettivamente della parte continua di un componente fisico e della parte logica dello stesso, sono poi stati aggregati in componenti ibridi così da favorire il loro riuso da parte dell'utente. Attualmente, è in fase di ultimazione l'ampia validazione del modello ibrido e stocastico complessivo, sia basata su dati disponibili in letteratura sia da precedenti misurazioni.

Conclusioni

L'applicazione dello standard IEC 61508 al ciclo di vita dei sistemi di E/E/EP per la protezione della rete di trasmissione elettrica mostra i suoi limiti in quanto tale sistema meglio si presta

ad essere controllato con tecniche di analisi del rischio, in grado di gestire meglio la complessità e la vastità geografica della rete e di supportare l'identificazione del livello di sicurezza richiesto.
A questo scopo, l'articolo propone un modello ibrido, basato su semplici estensioni di reti di Petri stocastiche generalizzate integrate con modelli continui, permettendo così l'analisi quantitativa del rischio e la valutazione delle strategie differenti di protezione, sulla base di opportuni indici da definire. L'articolo descrive il modello ibrido, considerando sia le dinamiche a tempo continuo sia quelle ad eventi discreti, per tenere in conto anche fenomeni di rotture, guasti, fenomeni naturali. L'uso dei modelli analitici permette di valutare il livello di sicurezza associato alle differenti strategie di protezione e supportare l'identificazione delle criticità specifiche del sistema di protezione stesso.
Successivi lavori includono l'affinamento del modello e della sua efficienza di calcolo, l'implementazione di opportuni indici di rischio e l'applicazione a casi di benchmark.

Bibliografia

[1] M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli and G. Franceschinis, *Modelling with Generalized Stochastic Petri Nets*, Wiley, New York, 1995.
[2] Z. Bie, X. Wang, *Evaluation of power system cascading outages*, IEEE, 2002
[3] I. Dobson, B. A. Carreras, V. E. Lynch, D. E. Newman, "Complex Systems Analysis of Series of Blackouts: Cascading Failure, Criticality, and Self-organization", *Bulk Power System Dynamics and Control* - VI, Agosto, 2004, Cortina d'Ampezzo.
[4] I. Dobson, B. A. Carreras, D. E. Newman, "A criticality approach to monitoring cascading failure risk and failure propagation in transmission systems", *Electricity transmission in deregulated markets*, Conference at Carnegie Mellon university, Dicembre 2004.
[5] *IEEE Reliability test system*, IEEE transaction on power system, 1999.
[6] D. Lucarella, M. Pozzi, M. Valisi, G. Vimercati, "Un approccio basato sull'analisi di rischio per l'esercizio in sicurezza del sistema elettrico"; *Convegno nazionale valutazione e gestione del rischio negli insediamenti civili ed industriali*; Pisa, Ottobre 2004.
[7] Y. V. Makarov, R. C. Hardiman, "On Risk-based Indices for Transmission Systems"; *Proc. IEEE PES Annual Meeting*, Toronto, Luglio 2003.
[8] J. McCalley, V. Vittal; *Risk Based Security Assessment*, final report for EPRI Project WO8604-01, 2001.
[9] A. Padke, "Hidden failures in protection systems", *Power systems and communications infrastructures for future*, Beijing, 2002.
[10] Yu, Chanan Singh, "A Practical Approach for Integrated Power System Vulnerability Analysis With Protection Failures", *IEEE Transaction on power systems*, vol. 19, no. 4, Novembre 2004.