



*Valutazione comparata dell'affidabilità degli UPS con flywheel integrato
e degli UPS a doppia conversione con batterie*

Libro bianco 103

2128 W. Braker Lane, BK12

Austin, Texas 78758-4028

www.activepower.com

OBIETTIVO

Questo documento fornisce l'analisi quantitativa comparata dell'affidabilità in servizio dei sistemi UPS (gruppi di continuità) Active Power CleanSource® basati su flywheel e dei tradizionali sistemi UPS a doppia conversione alimentati a batteria. L'analisi è stata condotta applicando il metodo di valutazione probabilistica del rischio.

RISULTATI PRINCIPALI

- MTechnology ha riscontrato che la probabilità di mancata alimentazione al carico delle unità CleanSource UPS durante brevi buchi di tensione è sette volte inferiore a quella degli UPS a doppia conversione con batterie.
- MTechnology ha riscontrato che “ la mancata alimentazione al carico è estremamente improbabile nei sistemi ad immagazzinaggio di energia cinetica mediante l'utilizzo di flywheel. Infatti, se operativo al momento della mancanza di alimentazione, il flywheel funzionerà con quasi assoluta certezza.”
- Lo switch di ridondanza, presente in entrambi i sistemi, è il componente che da solo causa la maggior parte dei guasti di sistema, essendo infatti responsabile del 95 per cento dei guasti di sistema contemplati, seguito da vicino dal mancato avvio del gruppo di comando principale e del generatore.
- La modalità di guasto più frequente in un UPS a doppia conversione con batterie riguarda i guasti non rilevabili della batteria (assenze di carico)
- Lo studio ha utilizzato un ottimistico tasso di guasti non rilevabile pari all'uno per cento, di per sé molto prudente, presupponendo inoltre che le batterie siano sottoposte a regolari interventi manutentivi e di collaudo. L'esperienza di MTechnology suggerisce fortemente che sarebbe difficile ottimizzare il funzionamento delle batterie oltre quanto predetto dal modello.
- Facendo riferimento a un tasso di guasto non rilevabile delle batterie del 10 per cento, la probabilità che un'unità CleanSource UPS possa guastarsi durante un breve buco di tensione (10 secondi massimo) è 52 volte inferiore a quello di un UPS a doppia conversione.
- In un UPS a doppia conversione con batterie, i guasti rilevabili delle batterie con sistema in modalità bypass sono secondi nella categoria dei guasti più frequenti.

INTRODUZIONE

Active Power, Inc. si è servita nuovamente di MTechnology, Inc. (MTech), una società con sede nel Massachusetts, per eseguire l'analisi comparativa sull'affidabilità delle proprie unità CleanSource UPS da 300 kVA/240 kW e degli UPS a doppia conversione con batterie.

MTechnology, Inc. (MTech) applica dal 1996 la scienza della valutazione probabilistica del rischio al problema dell'alta disponibilità di energia elettrica per sostenere computer, collegamenti Internet e altre installazioni mission critical. Tra i clienti di MTech si annoverano produttori, studi di progettazione e proprietari e utenti di installazioni mission critical. I servizi MTech sono rivolti ad un'ampia gamma di settori, compresi data center aziendali, impianti per la generazione di energia nucleare e di produzione di gas naturale liquefatto, laboratori di ricerca biomedica e per la terapia protonica del cancro e centri di sviluppo di celle a combustibile.

Lo studio comprende due classi di guasti di rete:

- Interruzioni di rete superiori ai 10 secondi in cui la fonte CA viene trasferita sul generatore, che presuppongono l'operatività dello switch di ridondanza e l'azionamento del generatore stesso.
- Interruzioni di rete inferiori ai 10 secondi in cui l'energia immagazzinata dall'UPS deve bastare per sostenere il carico in attesa del ripristino del servizio, senza il trasferimento su generatore. Ciò amplia le differenze fondamentali in termini di affidabilità tra i due sistemi UPS.

MTech ha sviluppato un modello ad albero dei guasti per entrambi i sistemi. Il modello ad albero dei guasti abbina quanto noto sulle combinazioni guasti di rete e componentistica UPS che provocano un avaria di sistema e le nozioni relative alla frequenza dei guasti della componentistica e relativa durata delle riparazioni previste. I dati concernenti i guasti della componentistica sono stati prelevati dagli standard industriali, tra cui pubblicazioni quali il Gold Book di IEEE e, dove possibile, dall'esperienza maturata sul campo attraverso il parco installato CleanSource UPS Active Power.

DESCRIZIONE DEI SISTEMI

CleanSource UPS

L'unità CleanSource UPS Serie 300 è un sistema UPS trifase che si serve della tecnologia flywheel per immagazzinare energia. Il sistema propone caratteristiche di condizionamento della rete, quali regolazione della tensione e compensazione delle armoniche. Accoppiando un'unità CleanSource UPS e un generatore di standby, è possibile creare un sistema di alimentazione continua che protegge i carichi mission critical sia durante brevi buchi di tensione, sia in caso di interruzioni di rete prolungate.



FIGURA 1: CLEANSOURCE UPS SERIE 300

Il flywheel accumula energia cinetica sotto forma di massa rotante. Durante il normale esercizio, il flywheel gira a velocità costante. Il sistema distribuisce l'energia dalla rete al carico protetto. Quando si verifica un'interruzione sulla rete, il sistema converte in energia elettrica l'energia cinetica accumulata nel flywheel. Una volta ripristinato il servizio, il sistema restituisce il carico alla rete. Per ulteriori informazioni, consultare il libro bianco n. 108 ("Funzionamento e prestazioni di un sistema UPS basato su Flywheel").

Tecnologia flywheel

Active Power produce sistemi integrati di alimentazione con UPS e in CC basati su tecnologia flywheel, quale alternativa efficace all'uso di batterie chimiche. Il parco di unità CleanSource conta più di 40 milioni di ore esercizio con installazioni in tutto il mondo.



FIGURA 2: FLYWHEEL DI PRODUZIONE PER APPLICAZIONI UPS

Il rotore del flywheel è supportato dalla tecnologia a cuscinetti magnetici Active Power. Con questa tecnologia, il cuscinetto a cartuccia meccanica, sostituibile in loco, non è costretto a sopportare la maggior parte del peso del flywheel. Una pompa da vuoto svuota la camera d'aria, riducendo la resistenza cui è sottoposto il flywheel rotante. Con il trasferimento della potenza sul carico, il flywheel decelera. La corrente regolata viene distribuita alle bobine di eccitazione per garantire un'uscita di tensione costante per tutta la durata della scarica.

Il sistema esegue il condizionamento della rete e garantisce autonomia durante gli abbassamenti e i picchi di tensione. Inoltre, esso colma i buchi di tensione che intercorrono tra l'interruzione di rete e il passaggio all'alimentazione con generatore. La figura 3 illustra lo schema unifilare dell'unità CleanSource UPS semplificato per il modello ad albero dei guasti.

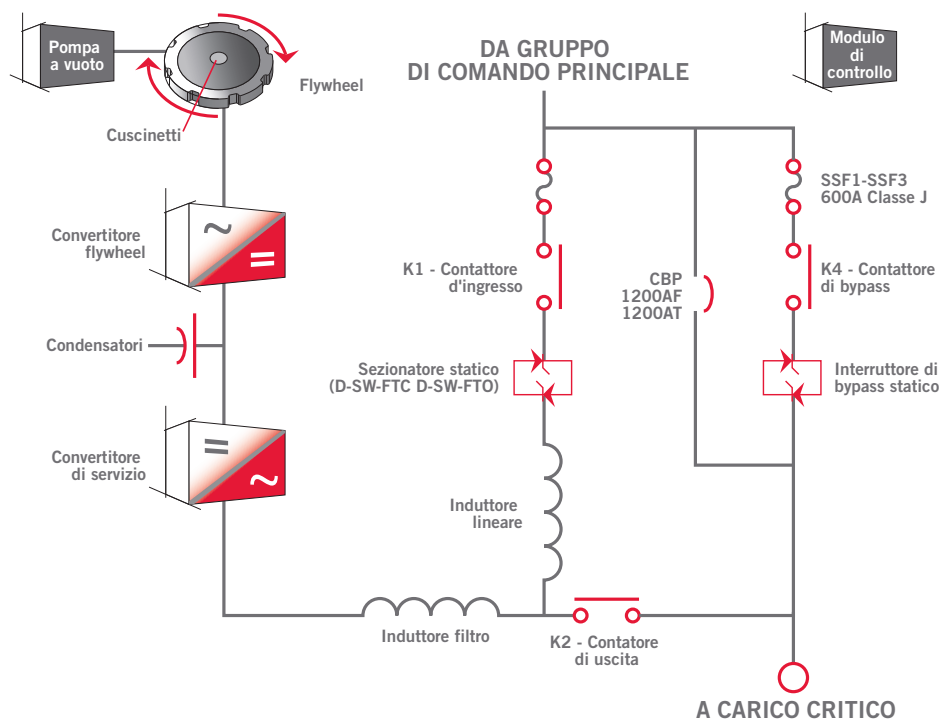


FIGURA 3: SCHEMA UNIFILARE DELL'UNITÀ CLEANSOURCE UPS

Gruppo di continuità Double Conversion

Il sistema UPS a doppia conversione utilizza un raddrizzatore e un inverter, accumulando energia mediante batterie chimiche o altri metodi e utilizzando un collegamento in CC tra le due fasi di conversione. In un sistema UPS a doppia conversione tradizionale, il raddrizzatore carica la batteria e alimenta in CC l'inverter. L'inverter a sua volta alimenta il carico con CA continua. Quando si verifica un'interruzione della tensione all'ingresso principale dell'UPS, l'energia viene prelevata dalla batteria in attesa che venga ripristinata la potenza in ingresso. Il raddrizzatore quindi ricarica la batteria, alimentando al contempo l'inverter in CC. Quando il sistema funziona secondo quanto prescritto, questo processo si verifica senza interruzioni sull'uscita dell'UPS.

Sebbene efficace, gli svantaggi di un sistema a doppia conversione sono vari: minore efficienza operativa a causa di un processo a due fasi che prevede la conversione dell'energia di rete da CA a CC e quindi nuovamente da CC a CA. Inoltre, le batterie piombo-acido sono voluminose e pesanti, ricolme di sostanze chimiche corrosive e materiale pericoloso da smaltire con cautela. Queste batterie richiedono in genere un ambiente controllato. In una situazione tipo, un aumento della temperatura ambiente di 10 gradi Celsius dimezza la vita utile prevista della batteria.

Per prevenire reazioni avverse tra i filtri d'ingresso dell'UPS e i generatori diesel è necessaria un'attenta progettazione, soprattutto nel caso di sistemi UPS a doppia conversione con carico leggero. I generatori hanno un fattore di potenza nominale in anticipo limitato rispetto alle capacità del fattore di potenza in ritardo di cui sono dotati. Un generatore collegato a un carico con fattore di potenza in anticipo eccessivamente ampio può subire un'autoeccitazione, con conseguente aumento della tensione in uscita, anche con corrente di campo ridotta al minimo. Questa condizione è pericolosa e prevede l'immediato arresto del generatore e del motore primo, con conseguente perdita del carico critico. I modelli utilizzati per lo studio non hanno tenuto conto di questa modalità di guasto, poiché si è partiti dal presupposto che, secondo un esame informato dei possibili carichi imposti sul generatore, essa sarebbe stata progettata esternamente al sistema.

Un ulteriore svantaggio dei sistemi tradizionali a batteria è rappresentato dall'assenza di carico su richiesta. La batteria si compone di un ampio numero di celle a due volt collegate in serie. Il guasto di una cella o di un collegamento tra celle comporta il guasto dell'intera batteria. Di solito, tali guasti si evidenziano solo quando il carico viene applicato alla batteria durante una reale assenza di alimentazione. Il modello aveva presupposto l'esecuzione di un collaudo mensile della batteria, con la conseguente alta probabilità di rilevare eventuali celle guaste che potevano così essere riparate. La figura 4 illustra lo schema unifilare dell'UPS a doppia conversione semplificato per il modello ad albero dei guasti.

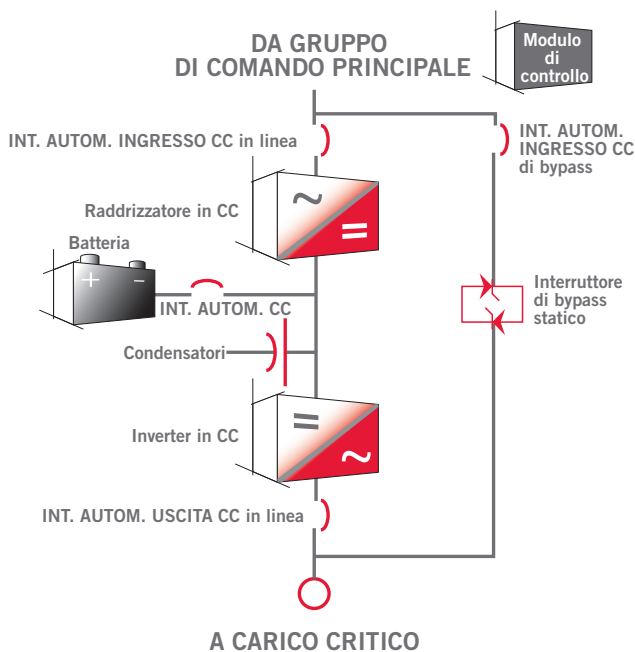


FIGURA 4: SCHEMA UNIFILARE DELL'UPS A DOPPIA CONVERSIONE

Rete e generatore

I due sistemi hanno in comune un'unica alimentazione di rete in ingresso e un generatore di standby, entrambi collegati agli ingressi dell'UPS attraverso il gruppo di comando e lo switch di ridondanza. La figura 5 illustra lo schema unifilare che collega rete, generatore, switch di ridondanza e gruppo di comando all'ingresso dell'UPS.

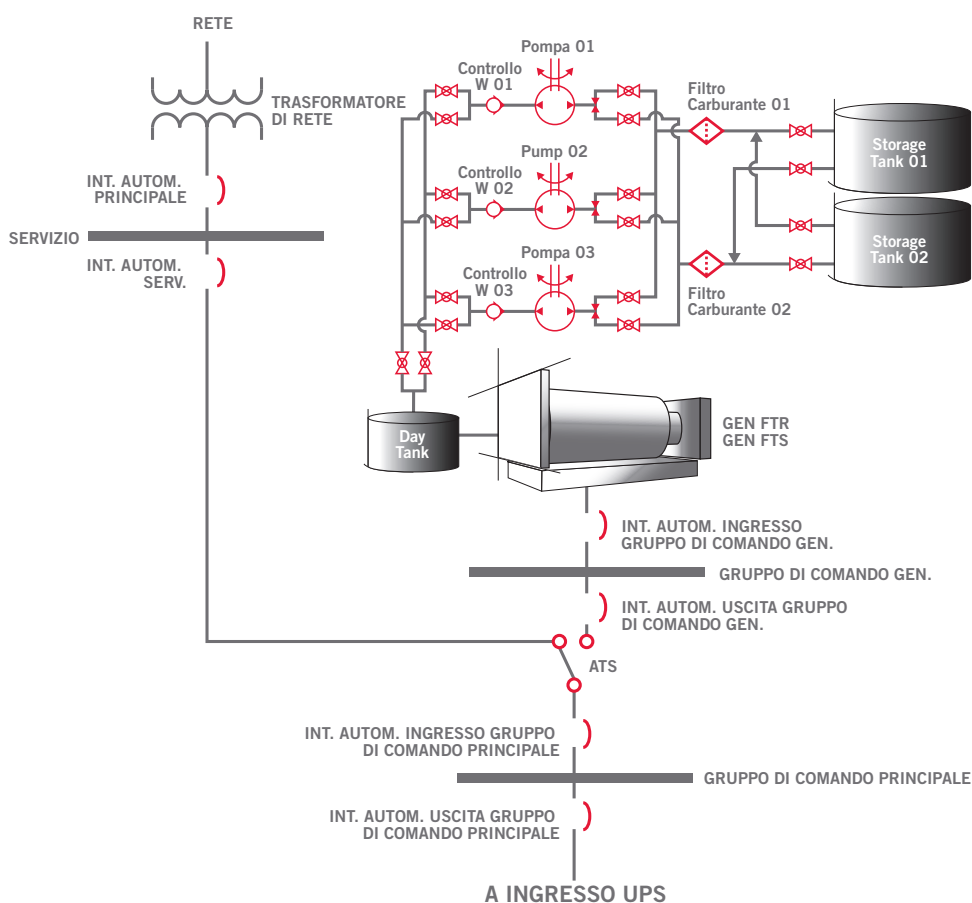


FIGURA 5: SCHEMA UNIFILARE PER RETE, GENERATORE D'EMERGENZA, SWITCH DI RIDONDANZA E GRUPPO DI CONTROLLO PRINCIPALE UTILIZZATI NEL SISTEMA PER IL MODELLO AD ALBERO DEI GUASTI

VALUTAZIONE PROBABILISTICA DEL RISCHIO

La valutazione probabilistica del rischio è una raccolta di tecniche formali utilizzate per determinare l'affidabilità e la disponibilità di sistemi complessi. I motivi che spingono ad utilizzare questa metodologia per studiare sistemi ad alta affidabilità sono due, entrambi molto importanti:

- Le limitazioni intrinseche degli studi sull'affidabilità condotti mediante la mera osservazione dei guasti di sistema
- La necessità di quantificare il rischio per l'allocazione razionale ed efficace di risorse scarse

In questo campo sono frequentissime le affermazioni di disponibilità “a sei nove”, cioè del 99,9999 per cento di tempo medio di disponibilità. Eppure sottoponendo a una breve analisi matematica tali affermazione ci si rende conto che si riferiscono a una durata media prima di un'avaria (MTTF, mean time to failure) di oltre 1.200 anni. È pertanto impossibile appurare la veridicità di tali affermazioni attraverso la sola osservazione di impianti il cui ciclo di vita in termini economici è al massimo di qualche decennio. Infatti, la vita del progettista e del proprietario non è sufficientemente lunga per appurare la verità. Allo stesso modo, affermazioni del tipo “30 anni d'esperienza” equivalgono a dichiarare che per tutta la carriera il progettista non ha fatto altro che ripetere gli stessi errori.

Le tecniche di valutazione probabilistica del rischio agevolano lo sviluppo di stime credibili e giustificabili sull'affidabilità dei sistemi, combinando dati noti sui tassi di guasto dei componenti più semplici in un modello matematico formale. Il volume di dati disponibile sul tasso di guasto della maggior parte di componenti elettronici, elettrici e meccanici, è considerevole. I calcoli effettuati dalla valutazione probabilistica del rischio consentono di integrare i dati concernenti l'interazione dei componenti in un particolare sistema con le conoscenze in materia acquisite dagli esperti, per generare stime utili sui tassi di guasto dei sistemi complessi. Il tutto ancor prima di passare alla fase di costruzione dei sistemi.

La capacità di questa metodologia di stimare i tassi di guasto di un sistema consente a progettisti e produttori di valutare l'affidabilità dei design concorrenti prima di costruire il prototipo iniziale. La capacità di predire gli effetti dei miglioramenti proposti è anch'essa uno strumento molto potente. I sistemi ad alta affidabilità utilizzano invariabilmente componenti ridondanti, sistemi di backup e altre tecniche. Tali tecniche comportano la creazione di progetti complessi, contrari a ciò che intuitivamente sarebbe progettualemente più opportuno.

La valutazione probabilistica del rischio è necessaria al fine di determinare l'affidabilità dei sistemi in cui i guasti sono così rari che rendono impraticabile la misurazione diretta. Questa metodologia è anche utile quando i guasti devono essere evitati a ogni costo, come ad esempio nel caso degli impianti nucleari. Il secondo motivo e forse il più importante per utilizzare la metodologia di valutazione probabilistica del rischio è rappresentato dalle implicazioni per i responsabili in fase decisionale.

I risultati di una buona analisi probabilistica dei rischi sono molto più significativi dei valori di MTTF o di disponibilità. I risultati sono presentati sia sotto forma di probabilità di guasto (esaminati di seguito), sia di valutazione quantitativa del contributo apportato da ciascun componente al rischio complessivo di guasto. È appunto questa quantificazione del rischio che giustifica più che mai l'impiego della valutazione probabilistica del rischio nella realizzazione di sistemi estremamente affidabili.

I risultati conseguiti dall'unità CleanSource UPS e dall'UPS a doppia conversione sono coerenti con i primi studi condotti sui data center aziendali e con i prodotti UPS della concorrenza. Modelli con dozzine o anche migliaia di componenti evidenziano invariabilmente una prevalenza del rischio di guasto concentrata solo su alcuni componenti. Senza queste informazioni sul contributo relativo dei componenti all'avaria, le società di progettazione e relativi responsabili non potrebbero in alcun modo allocare le scarse risorse disponibili in maniera efficace. Armati della nozione che solo determinati componenti provocano la maggior parte dei guasti di sistema, le risorse possono essere ivi allocate e rimosse da componenti, pratiche di manutenzione e altri sforzi il cui contributo all'affidabilità del sistema è palesemente minimo o nullo.

Ricapitolando, la valutazione probabilistica del rischio fornisce informazioni concernenti l'affidabilità di un sistema difficili se non addirittura impossibili da ottenere con altri mezzi. Tali informazioni consentono l'allocazione razionale e giustificabile di risorse al fine di migliorare l'affidabilità durante tutte le fasi di progettazione, messa in servizio, manutenzione e ottimizzazione.

DISPONIBILITÀ E PROBABILITÀ DEL GUASTO

MTech riporta i propri risultati principalmente in termini di probabilità di guasto, piuttosto che di disponibilità. La disponibilità è il parametro tecnicamente corretto per i sistemi riparabili, ma non è necessariamente il più utile per comprendere i rischi o le differenze tra sistemi concorrenti.

Il motivo principale per adottare il parametro probabilità di guasto è che i clienti lo considerano molto più utile. Sono poche le aziende che possono vantare una sostanziale esperienza con le tecniche di calcolo per la valutazione probabilistica del rischio, nonostante funzionari e direttori si destreggino con regolarità tra più proposte concorrenti, tutte con vari livelli di rischio. Molti acquistano prodotti quali assicurazioni o programmi di disaster recovery in base alla propria valutazione del rischio, che corrisponde alla probabilità di subire una perdita moltiplicata per l'importo del danno previsto da una tale perdita. Molte aziende che gestiscono data center sono destinate a subire notevoli perdite anche con una sola interruzione di rete e, pertanto, devono conoscere la probabilità del verificarsi di un tale evento per poter formulare una decisione informata relativamente ad eventuali investimenti aggiuntivi o ad altri mezzi volti a mitigare il rischio.

Un altro motivo per utilizzare la probabilità di guasto, piuttosto che la disponibilità, è che il primo di questi parametri è una funzione del tempo. I metodi di analisi quali la catena di Markov e la riduzione di rete si limitano a considerare tassi di guasto costanti e i risultati, spesso denominati MTTF, sono ottenuti per inversione da un tasso di guasto costante pari a 1:

$$\text{MTTF} = 1/\lambda.$$

Sebbene ciò sia vero per un componente o un sistema con tassi di guasto costante, non si può dire lo stesso di elementi ridondanti con tassi di guasto costanti che producono sistemi con tassi di guasto variabili. In questo caso è fuorviante caratterizzare sistemi composti da elementi ridondanti come aventi un tasso di guasto costante.

MODELLO AD ALBERO DEI GUASTI

L'analisi dell'albero dei guasti è una tecnica utilizzata per monitorare gli effetti di un guasto di un componente o di un sottosistema. L'analisi inizia con l'avaria del sistema, quindi determina quali sottosistemi si sono dovuti guastare per provocare l'avaria del sistema. Con la stessa tecnica, si passa a valutare ciascun sottosistema, finché, avendo raggiunto un numero ben definito di guasti, denominati eventi scatenanti, l'analisi si ferma. I modelli ad albero dei guasti sono modelli logici di avarie di sistema combinati con i tassi di guasto e riparazione degli eventi scatenanti. Le combinazioni dei guasti dei componenti sufficienti a provocare l'avaria del sistema sono noti come Minimal Cut Set (MCS).

Gli alberi dei guasti e gli strumenti di analisi a essi associati rappresentano la prima tecnica per la definizione di un modello adatto a determinare gli MCS. I tassi di guasto e riparazione per ciascun evento preso in considerazione sono utilizzati per definire il contributo relativo di ciascun evento, all'avaria complessiva del sistema. Il prodotto di questa analisi è un elenco di MCS e relativo contributo alla probabilità totale di avaria del sistema. Giacché anche modelli semplici in genere evidenziano migliaia di MCS quasi tutti riconducibili a solo pochi elementi di base (CS, Cut Set), MTech non riporta il contributo di ogni singolo CS. Il modello per il confronto delle unità CleanSource UPS e degli UPS a doppia conversione è stato realizzato utilizzando lo strumento per l'analisi dell'albero dei guasti denominato SAPHIRE.

L'avaria del sistema viene definita come la mancata distribuzione di potenza dal percorso in linea o di standby al carico critico. La rete e il generatore di standby sono fonti in CC. Il modello effettua il confronto tra entrambi i sistemi UPS: l'unità CleanSource UPS/modulo di bypass e l'UPS a doppia conversione/modulo di bypass. L'avaria si verifica se si guastano entrambi i tipi di UPS. Questo approccio consente di condividere alcuni elementi comuni dell'albero dei guasti, quali rete, generatore e così via. Il modello ad albero dei guasti può selezionare per l'analisi sia un'unità CleanSource UPS che un UPS a doppia conversione, impostando la probabilità dell'avaria dell'altro sistema su zero.

ANALISI DELL'ALBERO DEI GUASTI

MTech utilizza molte fonti per reperire i tassi di guasto dei componenti, tra cui i database relativi agli standard di affidabilità degli impianti a energia nucleare, i dati dei produttori e la propria esperienza nel settore degli UPS. Nei casi in cui Active Power ha fornito dati derivati dall'esperienza sul campo, come ad esempio quelli derivati dalle esperienze con il parco di unità CleanSource UPS, detti dati sono stati utilizzati per ispirare stime sui tassi di guasto dei componenti e le modalità di avaria.

MTech ha realizzato gli alberi dei guasti per le unità CleanSource UPS utilizzando schemi unifilari con i chiarimenti forniti da Active Power, secondo necessità. L'avaria di un sistema è definita come l'impossibilità del carico di distribuire potenza dal percorso in linea o di standby, ovvero l'"evento superiore" dei modelli combinati dell'albero dei guasti. Eventi modello che rappresentano eventi di base simili sono stati introdotti per gestire con efficienza gli eventi di base del guasto di un componente.

CLASSI DI INTERRUZIONI DI RETE

Ai fini di questo studio sono state prese in considerazione due tipologie di interruzioni di rete.

- Interruzioni di rete superiori ai 10 secondi, in cui la fonte CA viene trasferita sul generatore, necessitando l'operatività dello switch di ridondanza e l'azionamento del generatore stesso.
- Interruzioni di rete inferiori ai 10 secondi in cui l'energia immagazzinata dall'UPS deve bastare per sostenere il carico in attesa del ripristino del servizio, senza il trasferimento su generatore. Ciò amplia le differenze fondamentali in termini di affidabilità tra i due sistemi UPS.

Interruzioni di rete lunghe: > 10 secondi con trasferimento al generatore

Nel caso di un'interruzione di rete prolungata, l'energia accumulata dell'UPS alimenta il carico critico per il breve periodo necessario all'avviamento del generatore di standby che si assumerà il carico trasferito dallo switch di ridondanza. È utile notare che le interruzioni di rete più lunghe di 10 secondi sono poco frequenti nei paesi sviluppati. Infatti, l'Istituto per la ricerca sull'energia elettrica (Electric Power Research Institute, EPRI) stima che la probabilità che l'utenza subisca cali di tensione è 10 volte superiore a quella di una completa interruzione di rete. Delle interruzioni di rete, meno del 4 percento superano i 10 secondi.

I 18 Cut Set superiori per un UPS a doppia conversione con batteria e per le unità CleanSource UPS sono riprodotti nella figura 6. Ciascuna voce rappresenta uno specifico guasto all'interno dell'architettura, la cui concatenazione ha comportato la perdita di potenza nelle apparecchiature di prima necessità. Ogni evento è ponderato e ha una probabilità o frequenza propria di guasto, stabilite in base ai dati divulgati dal settore, al Gold Book di IEEE o ad argomenti tratti dall'esperienza maturata sul campo dai produttori di UPS.

CLEANSOURCE UPS

INTERRUZIONE DI RETE SUPERIORE				
Cut N.	Cut Set %	Prob./Freq.	Evento	Probabilità
1	94,7	8,20E-02	GUASTO DELLO SWITCH DI RIDONDANZA	8,20E-02
2	1,2	1,10E-03	INTERRUTTORE DI POTENZA D'INGRESSO DEL GRUPPO DI COMANDO PRINCIPALE	1,10E-03
3	1,2	1,10E-03	INTERRUTTORE DI POTENZA D'USCITA DEL GRUPPO DI COMANDO PRINCIPALE	1,10E-03
4	1,2	1,00E-03	GUASTO DEL BUS DEL GRUPPO DI COMANDO PRINCIPALE	1,00E-03
5	1,2	1,00E-03	MANCATO AVVIO DEL GENERATORE	1,20E-03
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
6	0,5	4,30E-04	MANCATO FUNZIONAMENTO DEL GENERATORE - NON ASSOCIATO AL CARBURANTE	5,10E-03
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
7	0,1	8,80E-05	CAUSA COMUNE DI GUASTO DEL MODULO DI CONTROLLO	8,80E-05
8	0,1	8,40E-05	MANCATA COMMUTAZIONE DELLO SWITCH DI RIDONDANZA	1,00E-03
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
9	0,1	4,70E-05	GUASTO DEL CONDENSATORE	5,60E-04
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
10	0	3,90E-05	GUASTO DEL CONDENSATORE	5,60E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
11	0	3,80E-05	GUASTO DEL CONVERTITORE FLYWHEEL	4,50E-04
			INTERRUZIONE LUNGA DI RETE	8,40E-02
12	0	3,80E-05	GUASTO DEL CONVERTITORE IMPIANTO	4,50E-04
			INTERRUZIONE LUNGA DI RETE	8,40E-02
13	0	3,10E-05	GUASTO DEL CONVERTITORE FLYWHEEL	4,50E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
14	0	3,10E-05	GUASTO DEL CONVERTITORE IMPIANTO	4,50E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
15	0	1,80E-05	GUASTO DEL DAY TANK	2,20E-04
			INTERRUZIONE LUNGA DI RETE	8,40E-02
16	0	6,00E-06	GUASTO DELLA POMPA DA VUOTO	7,20E-05
			INTERRUZIONE LUNGA DI RETE	8,40E-02
17	0	5,90E-06	MANCATO AVVIO DEL GENERATORE	1,20E-02
			GUASTO DEL TRASFORMATORE DI RETE	4,90E-04
18	0	5,00E-06	INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
			GUASTO DELLA POMPA DA VUOTO	7,20E-05

UPS A DOPPIA CONVERSIONE

INTERRUZIONE DI RETE SUPERIORE				
Cut N.	Cut Set %	Prob./Freq.	Evento	Probabilità
1	93,8	8,20E-02	GUASTO DELLO SWITCH DI RIDONDANZA	8,20E-02
2	1,2	1,10E-03	INTERRUTTORE DI POTENZA D'INGRESSO DEL GRUPPO DI COMANDO PRINCIPALE	1,10E-03
3	1,2	1,10E-03	INTERRUTTORE DI POTENZA D'USCITA DEL GRUPPO DI COMANDO PRINCIPALE	1,10E-03
4	1,2	1,00E-03	GUASTO DEL BUS DEL GRUPPO DI COMANDO PRINCIPALE	1,00E-03
5	1,2	1,00E-03	MANCATO AVVIO DEL GENERATORE	1,20E-03
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
6	0,7	5,90E-04	GUASTO DELLA BATTERIA NON RILEVABILE	5,80E-04
			INTERRUZIONE DI RETE BREVE NON RIPARABILE	1,00E+00
7	0,5	4,30E-04	MANCATO FUNZIONAMENTO DEL GENERATORE - NON ASSOCIATO AL CARBURANTE	5,10E-03
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
8	0,2	2,00E-04	GUASTO DELLA BATTERIA - RILEVABILE	2,40E-03
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
9	0,2	1,70E-04	GUASTO DELLA BATTERIA - RILEVABILE	2,40E-03
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
10	0,1	8,80E-05	CAUSA COMUNE DI GUASTO DEL MODULO DI CONTROLLO	8,80E-05
11	0,1	8,40E-05	MANCATA COMMUTAZIONE DELLO SWITCH DI RIDONDANZA	1,00E-03
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
12	0,1	4,90E-05	GUASTO DELLA BATTERIA - NON RILEVABILE	5,80E-04
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
13	0,1	4,70E-05	GUASTO DEL CONDENSATORE	5,60E-04
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
14	0,1	4,10E-05	GUASTO DELLA BATTERIA - NON RILEVABILE	5,80E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
15	0	3,90E-05	GUASTO DEL CONDENSATORE	5,60E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
16	0	3,10E-05	GUASTO DELL'INVERTER SUL PERCORSO IN LINEA - DOPPIA CONVERSIONE	4,50E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
17	0	1,80E-05	GUASTO DEL DAY TANK	2,20E-04
			INTERRUZIONE PROLUNGATA DI RETE	8,40E-02
18	0	5,90E-06	MANCATO AVVIO DEL GENERATORE	1,20E-02
			GUASTO DEL TRASFORMATORE DI RETE	4,90E-04

FIGURA 6: PRIMI 18 CUT SET PER UNITÀ CLEANSOURCE UPS (TABELLA IN ALTO) E UPS A DOPPIA CONVERSIONE CON BATTERIE (TABELLA IN BASSO)

L'analisi dell'albero dei guasti dimostra come l'avaria dello switch di ridondanza sia la causa principale del guasto dei gruppi di continuità di backup. I guasti dello switch di ridondanza in servizio partecipano al 95 per cento circa delle avarie di sistema contemplate. Lo switch di ridondanza è un componente comune sia all'unità CleanSource UPS che all'UPS a doppia conversione, quindi la differenza in termini di affidabilità tra i due sistemi illustrati nella figura 7 è irrisoria.

Il risultato non ha lo scopo di condannare lo switch di ridondanza. I dati del Gold Book di IEEE utilizzati nel modello riportano un tasso di guasto di circa 10-5 l'ora o oltre 100.000 ore (11+ anni) di durata media tra guasti, un valore che rappresenta una buona performance per un componente elettromeccanico complesso in servizio continuo. Lo switch di ridondanza partecipa alla maggior parte delle avarie di sistema, poiché è un punto singolo di concentrazione dei guasti. La conseguenza di un guasto dello switch di ridondanza è quasi invariabilmente l'avaria del sistema.

Architettura del sistema: cadute di tensione della rete sul sistema	Probabilità di avaria del sistema*	Probabilità relativa
CleanSource UPS con Flywheel	8,69E-02	1,00
UPS a doppia conversione con batterie	8,77E-02	1,01

*L'avaria del sistema è definita come l'impossibilità di alimentare il carico critico.

FIGURA 7: AFFIDABILITÀ DEI SISTEMI

I dati dimostrano che le probabilità di avaria del sistema, comprese le unità CleanSource UPS, siano inferiori per uno stretto margine, a causa della preponderanza dei tassi di guasto di switch ridondante, gruppo di comando principale e generatore. Il modello dei buchi di tensione è stato basato sul presupposto che sono 100 volte più frequenti delle interruzioni di rete lunghe. Aumentando il tasso di guasto durante le interruzioni brevi, i risultati succitati subiscono notevoli cambiamenti.

Buchi di tensione: < di 10 secondi con trasferimento al generatore

Nel caso di un'interruzione di rete breve, l'energia accumulata offre sufficiente autonomia per affrontare un qualsiasi disturbo di potenza. Considerato che il 96 per cento di tutti i cali di tensione o interruzioni di rete durano 10 secondi o meno, questo parametro diventa molto importante nel determinare l'affidabilità delle singole architetture UPS. La presente analisi dell'albero dei guasti non tiene in considerazione lo switch ridondante, il gruppo di comando e il generatore. La figura 8 illustra la probabilità di eventi di guasto per i due sistemi UPS e relativi dati riepilogativi nella figura 9.

CLEANSOURCE UPS

Guasto dell'UPS durante buchi di tensione < di 10 secondi				
Cut N.	Cut Set %	Prob./Freq.	Evento	Probabilità
1	31,5	3,90E-05	GUASTO DEL CONDENSATORE	5,60E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
2	25,3	3,10E-05	GUASTO DEL CONVERTITORE FLYWHEEL	4,50E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
3	25,3	3,10E-05	GUASTO DEL CONVERTITORE IMPIANTO	4,50E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
4	4,1	5,00E-06	GUASTO DELLA POMPA DA VUOTO	7,20E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
5	3,2	4,00E-06	GUASTO DELL'INDUTTORE DEL FILTRO	5,80E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
6	3,2	4,00E-06	GUASTO DELL'INDUTTORE DI LINEA	5,80E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
7	2	2,50E-06	GUASTO DEL CONTATTORE D'INGRESSO K1	3,60E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
8	2	2,50E-06	GUASTO DEL CONTATTORE D'USCITA K2	3,60E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
9	1,9	2,40E-06	GUASTO FUSIBILI (F1-F3)	3,40E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
10	0,5	6,70E-07	MANCATA APERTURA DEL SEZIONATORE	1,50E-04
			MANCATA APERTURA DEL CONTATTORE D'INGRESSO K1	4,40E-03
			INTERRUZIONE DI RETE BREVE NON RIPARABILE	1,00E+00
11	0,4	5,00E-07	GUASTO DEL CUSCINETTO	7,20E-06
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
12	0,4	5,00E-07	GUASTO DEL FLYWHEEL	7,20E-06
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
13	0,1	8,80E-08	MANCATA CHIUSURA DEL COMMUTATORE STATICO	1,30E-06
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02

UPS A DOPPIA CONVERSIONE

Guasto dell'UPS durante buchi di tensione < di 10 secondi				
Cut N.	Cut Set %	Prob./Freq.	Evento	Probabilità
1	66,9	5,90E-04	GUASTO DELLA BATTERIA - NON RILEVABILE	5,80E-04
			INTERRUZIONE DI RETE BREVE NON RIPARABILE	1,00E+00
2	19,4	1,70E-04	GUASTO DELLA BATTERIA - RILEVABILE	2,40E-03
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
3	4,7	4,10E-05	GUASTO DELLA BATTERIA - NON RILEVABILE	5,80E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
4	4,4	3,90E-05	GUASTO DEL CONDENSATORE	5,60E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
5	3,6	3,10E-05	GUASTO DELL'INVERTER SUL PERCORSO IN LINEA - DOPPIA CONVERSIONE	4,50E-04
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
6	0,4	3,00E-06	GUASTO DELL'INTERRUTTORE AUTOMATICO DEL SEZIONATORE IN CC	4,40E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
7	0,3	2,60E-06	GUASTO DEL RADDRIZZATORE SUL PERCORSO IN LINEA - DOPPIA CONVERSIONE	3,70E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
8	0,2	2,00E-06	GUASTO DELL'INTERRUTTORE AUTOMATICO D'INGRESSO SUL PERCORSO IN LINEA - DOPPIA CONVERSIONE	2,80E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02
9	0,2	2,00E-06	GUASTO DELL'INTERRUTTORE AUTOMATICO D'USCITA SUL PERCORSO IN LINEA - DOPPIA CONVERSIONE	2,80E-05
			INTERRUZIONE DI RETE BREVE DURANTE IL BYPASS	6,90E-02

FIGURA 8: PROBABILITÀ DI EVENTI DI GUASTO PER SISTEMI UPS

L'analisi dell'albero dei guasti dimostra che i guasti della batteria rilevabili e non rilevabili sono responsabili di almeno il 90 per cento di tutti i guasti nelle architetture UPS a doppia conversione. Il tasso di guasto presunto per le batterie è basso e si basa su batterie ben tenute, sottoposte a manutenzione e collaudo regolari. Secondo MTechnology, l'esperienza suggerisce che sarebbe difficile ottimizzare il rendimento delle batterie oltre quanto predetto dal modello.

Sistema	Probabilità di guasto dell'UPS durante buchi di tensione	Probabilità relativa di guasto
CleanSource UPS con Flywheel	1,24E-04	1,0
UPS a doppia conversione con batterie	8,74E-04	7,0

FIGURA 9: DATI RIEPILOGATIVI

L'analisi dimostra che la probabilità che un'unità CleanSource UPS si guasti è sette volte inferiore rispetto a un UPS a doppia conversione.

“Uno dei vantaggi del sistema CleanSource è che le assenze di carico da parte del sistema di accumulo energia con flywheel sono estremamente improbabili; infatti, se operativo al momento della mancanza di alimentazione, il flywheel funzionerà con quasi assoluta certezza.”

ANALISI DELLA SUSCETTIBILITÀ A GUASTI NON RILEVABILI DELLA BATTERIA

Il tasso di guasti non rilevabili della batteria è un parametro importante nell'analisi degli UPS a doppia conversione nell'ambito dei buchi di tensione. Il caso base stima il tasso di guasto nell'ordine dell'1% in termini di tasso di guasti rilevabili della batteria. MTech ha calcolato altri casi aggiuntivi, con stime diverse comprese tra il 10 e il 20 per cento.

Guasto non rilevabile della batteria	Probabilità di avaria del sistema	Probabilità di guasto dell'UPS durante buchi di tensione	% di avaria del sistema **	% di guasto dell'UPS durante buchi di tensione **
1% *	8,76E-02	8,74E-04	100 %	100%
10%	9,32E-02	6,48E-03	106 %	741%
20%	9,94E-02	1,27E-02	113 %	1453%

*CASO BASE: RAPPRESENTA IL TASSO DI GUASTO NON RILEVABILE DELLA BATTERIA STIMATO NELL'ORDINE DELL'1 PERCENTO DEI GUASTI RILEVABILI DELLA BATTERIA.

**QUESTA RAPPRESENTA LA PERCENTUALE DI OGNI CASO MESSO A CONFRONTO CON IL CASO BASE.

FIGURA 10

Dove la probabilità di guasto dell'unità CleanSource UPS durante un buco di tensione è sette volte inferiore rispetto all'UPS a doppia conversione, e ciò in base a un tasso molto ottimistico di guasti non rilevabili della batteria dell'1 per cento dei guasti rilevabili, il divario aumenta, con una probabilità di guasto 52 volte inferiore qualora si consideri una percentuale di guasti non rilevabili della batteria del 10 per cento.

Architettura del sistema	Guasti non rilevabili della batteria	Probabilità di avaria del sistema	Probabilità relativa	Probabilità di guasto dell'UPS durante buchi di tensione	Probabilità relativa
CleanSource UPS con Flywheel	N/D	8,69E-02	1,00	1,24E-04	1,0
UPS a doppia conversione con batterie	1%	8,77E-02	1,01	8,74E-04	7,0
UPS a doppia conversione con batterie	10%	9,32E-02	1,07	6,48E-03	52,3
UPS a doppia conversione con batterie	20%	9,94E-02	1,14	1,27E-02	102,4

FIGURA 11

Allo stesso modo, se implementato nell'ambito di un sistema progettato per proteggere da interruzioni di rete brevi e lunghe, le probabilità di guasto dell'unità CleanSource UPS sono marginalmente inferiori rispetto a un UPS a doppia conversione con l'ottimistico tasso di guasto non rilevabile della batteria dell'1 per cento, tuttavia il divario prestazionale del primo sistema sul secondo aumenta sostanzialmente con il crescere dei tassi di guasto della batteria.

CONCLUSIONE

I modelli ad albero dei guasti hanno valutato due classi diverse di guasti di rete: buchi di tensione con durata inferiore ai 10 secondi, e interruzioni lunghe con durata superiore ai 10 secondi.

Per garantire il funzionamento durante interruzioni di rete prolungate, il generatore deve azionarsi e lo switch ridondante deve essere operativo. In base alla valutazione probabilistica del rischio, la probabilità di guasto di un'unità CleanSource UPS è di solo 1/7 di quelle di un UPS a doppia conversione durante buchi di tensione di 10 secondi o meno. EPRI riporta che il 96 per cento di tutti i cali di tensione e le interruzioni di rete avvengono in questo arco di tempo. Questo scenario è 100 volte più frequente delle interruzione di rete prolungate, il che equivale a dire che il rischio delle strutture per questa classe di interruzioni di rete è sostanzialmente più elevato. Ciò rende ancora più importante il tasso di guasto degli UPS durante i buchi di tensione.

Se implementati nell'ambito di un sistema che prende in considerazione interruzioni di rete lunghe di minimo 10 secondi e più, le differenze in affidabilità tra i due sistemi sono praticamente irrilevanti. I guasti di switch di ridondanza, generatori e gruppi di comando sono responsabili di oltre il 90 per cento dei guasti contemplati. In questo caso, la differenza nei tempi di autonomia tra batterie e flywheel è irrilevante, giacché il guasto di switch di ridondanza, generatore e gruppo di comando sono sia:

1. un punto singolo di concentrazione dei guasti che non può essere riparato (ad esempio, perdita immediata del carico e così via), oppure
2. guasti riparabili con tempi di riparazione previsti che superano i tempi di autonomia sia del flywheel che delle batterie.

In un UPS a doppia conversione con batterie, la modalità di guasto più frequente è relativa a guasti non rilevabili della batteria. Come è stato provato in altre circostanze, è estremamente difficile identificare le celle delle batterie destinate a guastarsi alla prossima richiesta di carico. Pur presupponendo ottimisticamente che con collaudi mensili della stringa di batterie dell'UPS a doppia conversione sia possibile identificare la maggior parte dei guasti della batteria, l'unità CleanSource UPS risulta comunque più affidabile. Stime realistiche di guasti non rilevabili della batteria si risolvono in un chiaro vantaggio per l'unità CleanSource UPS.

La modalità di guasto più probabile per un'unità CleanSource UPS si verifica durante un'interruzione di rete mentre l'UPS è in bypass, in attesa di riparazione o in manutenzione programmata. Tuttavia, riducendo di un terzo il tempo medio di riparazione (MTTR) e il periodo in cui l'UPS è in bypass, l'affidabilità migliora di quasi 10 volte.

Il beneficio chiave di un sistema elettromeccanico dinamico come l'unità CleanSource UPS è che le assenze di carico su richiesta sono altamente improbabili. Lo stato regolare dell'unità CleanSource UPS è con il flywheel in rotazione costante che immagazzina energia cinetica. Eventuali cambiamenti nei valori che influiscono sull'integrità del sistema sono immediati e offrono un'immagine accurata del proprio stato prima che si verifichi un'interruzione di rete. Al contrario, un sistema basato su batteria è un processo elettromeccanico che, anche con i controlli e le manutenzioni consigliate, evidenzia un elevato livello di guasti non rilevabili.

APPENDICE - CASI A SOSTEGNO

Caso 1

Il 23 maggio 2008, il servizio di hosting Host Dime ha pubblicato la seguente descrizione di un'interruzione di rete verificatasi presso il loro centro. La causa alla radice della perdita di tensione fu attribuita a un guasto delle batterie. Questo è un caso di assenza di carico su richiesta descritto nello studio condotto da MTechnology. I risultati principali sono evidenziati.

Ai nostri clienti e partner commerciali,

non esistono parole per descrivere quanto siamo costernati per l'interruzione del servizio verificatosi venerdì 23 maggio 2008. Per l'attaccamento e la dedizione nutriti dal nostro team per l'intera comunità, l'incidente ha provocato un diffuso malcontento nella nostra azienda, sia a livello mentale che emotivo. A tutto ciò si aggiunge la consapevolezza della gravità del danno provocato da questo incidente. Siamo consci che né denaro né parole possono sostituire la perdita subita da ognuno di voi. La nostra azienda resterà per sempre in debito con tutti voi per la frustrazione e sconforto subiti. Nelle situazioni d'emergenza non è mai facile, eppure molti di voi ci hanno dimostrato il loro sostegno mentre lavoravamo alacremente per ripristinare la normalità. Desideriamo ringraziare tutti voi per la pazienza, la comprensione e il sostegno dimostrati durante questo difficile momento. In ogni caso desideriamo, come è giusto, fornirvi la relazione formale sull'incidente redatta dai nostri investigatori. A tal fine, di seguito si riporta il riepilogo dettagliato della successione degli eventi. Nota: non tutti i clienti sono stati colpiti ed è pertanto probabile che alcuni di voi non abbiano subito alcuna interruzione; malgrado ciò desideriamo che tutti siano informati.

L'accaduto:

Alle 8.00 circa, il nostro data center sulla costa occidentale degli Stati Uniti ha subito un picco di tensione cui ha fatto seguito un'interruzione di rete durata diversi minuti, entrambi provocati dalla società elettrica Progress Energy. Il picco di tensione ha disinnescato l'interruttore automatico principale della struttura, progettato con un certo livello di sensibilità per disinnescarsi nel caso di un grave picco di tensione, ciò al fine di proteggere il carico (server e apparecchiature essenziali) da incendio. Immediatamente dopo questo evento, il generatore è intervenuto in pochi secondi, avviandosi automaticamente. Con l'ausilio dello switch di ridondanza, l'alimentazione del nostro carico (server e apparecchiature) è passata automaticamente dalla rete non più disponibile al generatore. Nel frattempo, il nostro gruppo di continuità (UPS) alimentato a batteria avrebbe dovuto sostenere la tensione continua del carico. Tuttavia ciò sembra non essere avvenuto come previsto. L'indagine ha altresì confermato che il generatore era immediatamente disponibile trascorsi pochi minuti dalla mancanza di alimentazione.

Subito dopo l'interruzione, i nostri tecnici ed elettricisti si sono recati al sito. **La diagnosi ha rivelato che si era verificato un guasto nella stringa di batterie collegata all'UPS. Questo guasto ha impedito all'UPS di sostenere a pieno la tensione continua per il carico.** mentre si stava eseguendo la commutazione tramite lo switch di ridondanza dall'alimentazione di rete all'alimentazione fornita dal generatore. In questo arco di tempo, una grossa porzione del data center ha subito un'improvvisa perdita di tensione che ha provocato lo spegnimento e la riaccensione di una miriade di server. Purtroppo, a volte alcuni sistemi non si riavviano automaticamente e richiedono l'intervento manuale dell'amministratore che ne ripristini la piena funzionalità. Dopo l'interruzione di rete, il nostro team si è messo subito a lavoro controllando i sistemi e tutti i server sui quali l'evento ha potuto sortire effetti negativi.

Azioni correttive implementate:

Il nostro tecnico di pronta reperibilità addetto alla manutenzione dell'UPS e i nostri tecnici e ingegneri si sono tutti immediatamente recati in sede per condurre una diagnosi attenta e definire un piano d'azione per correggere tutte le problematiche possibili.

Durante tale riunione si optò per la sostituzione completa del gruppo batterie, nonostante l'età delle batteria utilizzate fosse ben entro i limiti di durata prevista dal produttore. Inoltre, l'UPS fu sottoposto a una ispezione approfondita: ogni singolo componente fu controllato e ricondizionato. Infine, le batterie e l'UPS furono collaudate a pieno carico prima di essere reimpiegate nel sistema di alimentazione di backup, per garantirne la completa affidabilità. Tutto ciò fu completato alcune ore dopo l'incidente.

Conseguenze:

L'interruzione di rete subita è stata intermittente. Tuttavia, anche dopo il ripristino dell'alimentazione completa del centro è stato necessario controllare il file system (FSCK) di numerosi server, sostituire alcuni alimentatori e alcuni dischi rigidi per l'eccessivo numero di errori di I/O. Purtroppo, a seconda dello spazio occupato dal sistema sul disco, il runtime della procedura di FSCK ha impiegato da un minimo di 30 minuti fino ad un massimo di nove ore (circa 200 server). I sistemi che hanno subito maggiori conseguenze erano quelli in cui si è riscontrato un numero eccessivo di errori di I/O e per cui è stata necessaria la sostituzione del disco rigido (circa 12 server in tutto). Inoltre, le sostituzioni dei dischi rigidi hanno richiesto dalle 4 alle 12 ore a seconda dello spazio occupato su ciascun disco. I server che hanno subito le conseguenze minori erano quelli in cui si è resa necessaria la sostituzione dell'alimentatore (circa 60 server).

Il prolungato tempo di fermo di alcuni server non era imputabile alla mancanza di alimentazione, piuttosto alle conseguenze negative descritte dianzi e subite dopo l'improvvisa perdita di tensione.

Misure preventive adottate:

Tutti gli impianti di alimentazione nel nostro data center e i carichi critici continuano a essere ispezionati e mantenuti con regolarità. Tra questi sono inclusi generatore, UPS, interruttori automatici e così via. Il nostro UPS era stato sottoposto a ispezione e servizio di manutenzione la settimana del 12 maggio 2008. La relazione di servizio rilasciata dimostra che l'UPS era in buone condizioni operative, così come la batteria. Il solo consiglio proposto è stato di prendere in esame la possibile sostituzione della serie di batterie, giacché si era prossimi all'ultimo anno di vita utile prevista dal produttore. Si optò di seguire il suggerimento del tecnico della manutenzione, ordinando immediatamente un nuovo gruppo batterie la cui installazione è prevista per martedì 27 maggio 2008.

Al termine delle indagini, il gruppo batterie è risultato responsabile del guasto ed è con rammarico che si osserva che prima dell'evento era già stato programmato l'intervento di manutenzione che avrebbe provveduto alla sostituzione. È difficile affermare cosa si sarebbe potuto fare per prevenire tutto ciò, considerato che le batterie erano nei limiti della durata prevista dal produttore e che, nonostante ciò, non hanno funzionato. Purtroppo eventi di tale portata non sono prevedibili. Infatti la sostituzione del gruppo batterie era stato programmato a puro titolo cautelativo e non perché se ne prevedeva il guasto. Tuttavia, è stato adottato un nuovo standard che prevede l'aumento dei collaudi di affidabilità delle batterie a una volta al mese. Ciò dovrebbe consentirci di intercettare anticipatamente tutti possibili problemi della batteria, riducendo in maniera sostanziale la probabilità di un guasto nei momenti critici.

Il nostro data center utilizza un UPS da 500 KVA e un generatore da 500 KW. Questo fatto è ulteriormente confermato dalle recenti immagini e filmati ripresi ieri pomeriggio. Qualora dovessero sussistere dubbi a questo riguardo, vi chiediamo di concederci cortesemente l'opportunità di dissiparli. Le immagini e i video proposti sotto sono relativi ai nostri sistemi di backup che ci hanno protetto con successo durante precedenti casi di mancanza di alimentazione dell'intero centro. Con esse riveliamo a chi ancora non ne fosse a conoscenza che il nostro centro era dotato fin dal primo giorno di attività delle misure di protezione necessarie e che i vostri servizi sono al sicuro con noi.

Operiamo nel settore da quasi 8 anni e abbiamo sempre fatto del nostro meglio per garantire a tutti tempi di attività del 100%. Dalla nostra apertura, questo è il primo caso di un'interruzione di rete con conseguenze così gravi. Offrirvi il migliore servizio possibile non è solo il nostro lavoro, ma anche la nostra passione. Non vogliamo servirvi della sventura di una situazione imprevedibile come questa come scusante per il tempo di fermo subito. A prescindere dalla natura della situazione, ci assumiamo la piena responsabilità per l'interruzione del servizio e siamo pronti a compensarvi in qualsiasi modo riteniate opportuno. La relazione commerciale che sussiste con voi è preziosa, così come il livello di fiducia di cui ci onorate. Siamo consci che molti di voi desiderano cancellare il loro impegno con noi per le perdite subite, mettendo in dubbio l'integrità dei nostri sistemi. Poiché comprendiamo il grado d'importanza che ciò assume per ognuno di voi, vi invitiamo a contattare la direzione prima di prendere la vostra decisione. Operiamo in un mercato estremamente volatile in cui qualunque cosa può accedere a noi, così come ai nostri concorrenti; tuttavia, promettiamo di essere sempre a vostra disposizione al primo insorgere di un qualsiasi problema, tendendovi una mano per risolverlo il più presto possibile. Tutti possiamo essere soggetti ad eventi sfortunati, ma è come li gestiamo che fa la differenza. Se esiste una qualunque cosa che possiamo fare per aiutarvi a minimizzare le vostre perdite, vi preghiamo di chiedere e consideratelo come fatto. Il livello di consapevolezza e impegno da parte nostra è triplicato e voi potete essere certi che questo evento ci ha resi molto più forti ed esperti. Non sempre si trovano persone o aziende che possono superare problemi di una tale portata e continuare a godere del sostegno e della fedeltà concessaci da tanti di voi. Se desiderate contattarmi personalmente con dubbi, raccomandazioni, suggerimenti, oppure per sfogarvi o comunicarmi modi in cui possiamo compensarvi, inviatemi un'e-mail direttamente all'indirizzo e.v.@hostdime.com. Sarò lieto più che lieto di discuterne con voi.

(Fonte: <http://www.hostdime.com/about/5232008/>)

Discussione

Interruzioni di rete come quella qui descritta sono disastrose e si verificano molto più frequentemente di quanto le aziende ammettano. Nonostante l'interruzione di rete fosse durata solo pochi minuti, il tempo di fermo del sistema è durato da un minimo di 30 minuti fino a diverse ore. I data center parlano di disponibilità delle proprie strutture, valore calcolato come tempo di disponibilità diviso per il tempo di disponibilità più il tempo di fermo, eppure ciò che si evince chiaramente da questa analisi è che la disponibilità ha definizioni diverse a seconda se l'interlocutore sia una società elettrica o i clienti a cui questa nota era indirizzata. MTechnology asserisce che la probabilità di guasto costituisce un parametro migliore per giudicare i data center, giacché include la possibilità del verificarsi di eventi come quelli descritti.

Host Dime afferma "Purtroppo, eventi di tale portata non sono prevedibili...". In realtà lo studio condotto da MTechnology prevede esattamente uno scenario di guasto di questo tipo, dimostrando che esso è, assieme ai guasti dello switch di ridondanza, del gruppo di comando principale e del generatore, una delle cause più probabili di avaria del sistema. Dato che non si fa alcun cenno a un UPS ridondante, si presume che l'architettura dell'impianto di alimentazione di Host Dime sia di I o di II livello, in linea con l'architettura analizzata dallo studio di MTechnology. L'affidabilità di un sistema può essere giudicata solo in base al suo collegamento più debole e in questo caso quel collegamento era l'assenza di carico da parte della batteria.

L'approccio di Host Dime nel dare prova dell'attuale affidabilità del proprio impianto di alimentazione consiste nell'aumentare la frequenza dei collaudi delle batterie portandoli a una volta al mese. Questa è una pratica comunemente accettata come valida, eppure presenta due nei:

- Le batterie piombo-acido hanno un ciclo di vita finito. Aumentando la frequenza dei collaudi, si aumenta potenzialmente l'intervallo tra interventi di manutenzione preventiva per la sostituzione del componente, una proposta costosa. MTechnology ha presentato dati sull'ottimizzazione delle manutenzioni preventive basati sull'analisi dell'affidabilità durante il proprio corso di formazione intitolato "Real Availability" (Disponibilità reale).
- Il collaudo mensile lascia comunque una finestra aperta di 12 x 730 ore per il verificarsi di un guasto non rilevabile. In pratica, non esiste un modo affidabile per rilevare guasti della batteria tra collaudi sul carico e tali periodi di incertezza costituiscono un rischio per le operazioni dei data center. I flywheel sono diversi. Fintanto che tensione viene assorbita dal flywheel e questi continua a ruotare, la probabilità che esso sia in grado di commutare passando alla modalità generatore su richiesta è molto elevata. Per questo motivo, le ragioni che giustificano l'esecuzione di collaudi del carico con il flywheel sono pochi e quando è necessario il sistema di monitoraggio evidenzia prontamente segnali dei componenti che richiedono attenzione, quali velocità del flywheel e così via.

Caso 2

Il 24 giugno 2008, il servizio di hosting Adhost ha pubblicato la seguente descrizione di un'interruzione di rete verificatasi presso il loro centro. La causa all'origine della perdita di tensione fu inizialmente attribuita al guasto delle batterie, che aveva provocato la conseguente avaria dell'UPS. Successivamente, questa fu identificata come una causa comune di guasto per sistemi UPS ridondanti. I risultati principali sono evidenziati.

Aggiornamento sull'evento UPS del Plaza East di Adhost Pubblicato sul Bollettino aziendale (pubblicato da Will R. alle 19:50 del 24 giugno 2008)

Alle 4:35 circa, ora della costa occidentale degli Stati Uniti, di sabato 21 giugno 2008, un gruppo di continuità (UPS) che serve il 20% circa dei server del nostro data center del Plaza East ha subito una significativa avaria. L'unità UPS in questione è ubicata in un locale appositamente adibito a tale scopo e separato dall'Adhost Plaza East Data Center. **Le prime indicazioni suggeriscono che alla base del guasto ci sia un significativo calo di amperaggio nelle stringhe di batterie,** fatto che per motivi ancora da determinare potrebbe aver provocato una situazione di sovratensione innescata dal tentativo spontaneo dell'unità di compensare il calo di tensione. Con molta probabilità, l'analisi completa di questo evento richiederà diverse settimane. In ogni caso, l'esito finale dell'evento è stato un considerevole danno provocato all'unità UPS da calore e fumo.

Con l'attivarsi dell'allarme antincendio, si sono mobilitati gli uomini del reparto dei vigili del fuoco di Seattle che, assistiti dai tecnici in sede, sono stati in grado di scollegare l'UPS in questione e l'unità accanto, impedendo così il propagarsi di danni a persone e struttura. I circuiti "A e B", che alimentano i due UPS e servono la porzione succitata del data center nel Plaza East, sono stati arrestati alle 4:52 (ora degli Stati Uniti occidentali). Nessun altro sistema UPS sul piano o altrove nel Plaza East ha subito conseguenze da questo arresto, compresi i sistemi UPS ubicati all'interno dell'Adhost Plaza East Data Center e gli altri sistemi UPS di proprietà e gestiti da Fisher Plaza presenti sul piano.

L'alimentazione di bypass ai circuiti colpiti nell'Adhost Plaza East Data Center e in altre parti del Fisher Plaza East è stata ripristinata dai team di progettazione di Adhost e Fisher Plaza alle 6:15 circa (ora degli Stati Uniti Occidentali). In seguito, il personale Adhost ha dato inizio il processo di riavvio dei sistemi, coadiuvando al contempo la clientela nel ripristino della piena funzionalità dei propri sistemi colpiti dall'interruzione del servizio.

Perché sono stati arrestati entrambi gli UPS? Queste due unità sono posizionate molto vicine tra loro nel locale adibito a ospitarle. Il secondo UPS, inizialmente senza conseguenze, ha cominciato ad aspirare una notevole quantità di fumo e corpi estranei attraverso la presa d'aria e le ventole di raffreddamento. L'unità è stata probabilmente sottoposta anche a notevole calore che ne ha compromesso i componenti interni. In queste condizioni i tecnici e il produttore rifiutano di certificarne la funzionalità.

Nella nostra prima comunicazione ai clienti avevamo definito questo incidente come un incendio, giacché di questo si era trattato inizialmente. Tuttavia, sono stati verificati un eccesso di calore e fumo e l'assenza di fiamme e, tranne per i due UPS, apparentemente vi sono stati danni irreparabili a lungo termine. L'edificio è stato presidiato da una società di ristrutturazione edile che ha lavorato alacremente per porre rimedio alle tracce di fumo e all'odore. Stiamo esaminando non solo il data center in questo edificio, ma anche gli uffici ubicati sullo stesso piano e finora sono state rilevate tracce minime o completa assenza di danni, eccezion fatta ovviamente per lo stato dell'alimentazione.

A che punto siamo? I carichi colpiti sono attualmente alimentati da un generatore di backup. Ciò significa che, qualora si verifici un'interruzione del servizio fornito dalla società elettrica Seattle City Light, il carico rimarrà privo di alimentazione per un tempo compreso tra 30 e 60 secondi, in attesa dell'intervento del generatore che ripristinerà l'alimentazione. I nostri tecnici hanno una linea diretta con Seattle City Light che è al corrente della nostra situazione e ha accettato di ridurre al minimo, e se possibile sospendere completamente, qualsiasi intervento sul loro impianto di distribuzione che potrebbe avere un impatto negativo sul nostro servizio. Ringraziamo Seattle City Light per la comprensione e la collaborazione dimostrata.

Ora qualche buona notizia. Di norma, la sostituzione di unità UPS come queste richiede molte settimane o addirittura dei mesi. Tuttavia, disponiamo di due nuove unità UPS recentemente installate sul piano. Stiamo collaborando con i responsabili della manutenzione dell'edificio e i nostri fornitori per definire un piano per spostare il carico su questi UPS il più velocemente possibile. Non possiamo ancora prevedere la durata di questo processo, poiché vi sono numerose variabili quali l'esatta disponibilità dei materiali, l'ottenimento dei permessi e l'organizzazione delle ispezioni, solo per nominarne alcune, tuttavia stiamo esercitando quanta più pressione possibile per portare a termine rapidamente questo lavoro pur attenendoci ai criteri di massima sicurezza e legalità. Speriamo di fissare come data obiettivo questo fine settimana. Solo dopo aver precisato la data invieremo una comunicazione ai clienti colpiti. Ovviamente, siamo a disposizione dei nostri clienti per ridurre al minimo l'impatto che questo trasferimento potrebbe avere sul nostro servizio.

Ci scusiamo con i nostri clienti e con i loro clienti per le eventuali conseguenze dovute a questo evento. Al contempo li ringraziamo per la comprensione dimostrata mentre continuiamo a lavorare per risolvere la situazione. Desideriamo inoltre ringraziare i tanti che si sono adoperati in questo momento difficile, tra cui il team di progettazione di Fisher Communications, il team di progettazione Egis, i team di progettazione e amministrazione sistemi di Adhost, Prime Electric, il Dipartimento dei vigili del fuoco di Seattle e Seattle City Light. Grazie al loro sforzo collettivo e alla loro competenza, una situazione potenzialmente molto pericolosa è stata notevolmente migliorata.

Siamo inoltre molto grati che nessuno abbia subito danni personali durante questo evento.

(Rif: <http://www.adhost.com/blog/2008/06/24/plaza-east-ups-event-update/>)

Discussione

In questa particolare situazione, l'esito finale delle indagini non è stato pubblicato. Tuttavia, in base alla valutazione preliminare, possiamo dedurre che sia stata compromessa l'impedenza del circuito della batteria (interno o esterno), innescando così un guasto secondario sull'UPS. Adhost non afferma perché l'UPS aveva effettuato una commutazione per passare all'alimentazione a batteria, forse dovuta a un'interruzione o per un collaudo dei carichi, limitandosi ad affermare che le batterie stavano sostenendo un carico e che avevano subito un repentino calo dell'ampereaggio. All'interno delle batterie, la solfatazione delle piastre può comportare l'aumento dell'impedenza interna e in genere la graduale perdita di capacità. Uno scenario più probabile di guasto interno è la perdita totale o parziale dell'interconnessione tra le piastre. Le stringhe di batterie sono formate da numerose celle da 2 volt in serie. Un tipico UPS trifase con bus in CC nominale da 480 V contiene 240 celle in serie, ciascuna suscettibile a guasti che possono provocare l'eventuale avaria dell'intera stringa. Esternamente, le stringhe di batterie sono composte da numerosi cavi di interconnessione, e ognuno di questi può essere soggetto alla perdita del contatto con i terminali della batteria. In questo caso i cavi mantengono la capacità di sostenere una carica a basso potenziale, ma non il pieno carico.

MTechnology esamina le cause comuni dei guasti nel proprio corso "Real Availability" (Disponibilità reale) tenuto periodicamente nell'ambito di congressi che vertono sul tema dell'affidabilità dei data center. Il fatto che l'avaria del primo UPS abbia influito su un sistema ridondante rappresenta una di quelle circostanze insidiose molto difficili da prevedere senza un'ampia esperienza nel settore. Ad esempio, molte società presuppongono che, disponendo di una doppia alimentazione di rete, sia quasi possibile annullare la probabilità un guasto di mandata. In realtà è vero che il rischio di un guasto dell'apparecchiatura rispetto a una rete ad alimentazione singola risulta mitigato; è però altrettanto vero che questo impianto è affidabile solo fino a quando non si incontra un punto di interconnessione comune, senza contare che di norma esso non protegge dalle interruzioni su rete regionale, note per avere un intervallo medio tra avarie di dieci anni.

In questo caso, con molta probabilità la causa alla base dell'interruzione è stata un'assenza di carico sulla batteria che, unita al guasto dell'UPS, hanno innescato un guasto per causa comune dell'UPS ridondante. Ai fini di questo documento, ciò che si deve desumere dalla dissertazione presentata è che le assenze di carico della batteria si verificano con sufficiente regolarità, potendone infatti documentare due casi nel breve periodo di un mese.

RIFERIMENTI

- » IEEE Gold Book
 - IEEE 493-2007 (Gold Book) Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems, 2007
- » NRC
 - Houghton e altri, Review of Operational Experience with Molded Case Circuit Breakers in US Commercial Nuclear Power Plants, AEOD/S92-03, Nuclear Regulatory Commission, 1992
- » Grant
 - Grant e altri, Emergency Diesel Generator Power System Reliability 1987 – 1993
- » RIAC
 - RIAC 217Plus™ Integrated Circuit and Inductor Failure Rate Models, J Reliability Information Analysis Center, 2007
- » OREDA
 - OREDA 2002, Offshore Reliability Data Handbook, 4ª ed, SINTEF, Norvegia, 2002
- » JET/TLK
 - Pinna e altri, Collection of data related to JET and TLK operational experience and component failure, http://nuclear.inl.gov/fusionsafety/meetings/iea-task-5-2003/docs/pinna_pppl-jet_data.pdf