Disaster Recovery per infrastrutture critiche: mirroring tra due DSO

Alberto Zironi
Inrete Dist. Energia Spa

Paolo Manià
AcegasApsAmga Spa

Damiano Manocchia
SIEMENS Spa

L'economia globale, l'esplosiva crescita di dati, l'automazione sempre più avanzata dei processi, i nuovi requisiti normativi insieme ad un'attenzione sempre maggiore verso eventi eccezionali hanno contribuito ad accrescere l'importanza degli aspetti di Business Continuity ed di Disaster Recovery.

La continuità del servizio rappresenta la capacità di un'azienda di mantenere costantemente disponibili i processi vitali e/o critici, a fronte di eventi potenzialmente catastrofici (disastri naturali, interventi umani dolosi e colposi, errori, etc.). Riferendosi ad un sistema informativo, la Business Continuity indica la continuità operativa di tutte le attività di natura critica delle tecnologie informatiche e telematiche messe a disposizione dall'organizzazione stessa.
Nel mondo della distribuzione elettrica, i tavoli di discussione sulla resilienza si sono focalizzati sugli aspetti fisici della rete elettrica e sull'aleatorietà di eventi meteorologici avversi, severi ed estesi che causano il fuori di ampie porzioni di rete; nel mondo dell'informatica la resilienza si declina col concetto di Disaster Recovery.

Il telecontrollo pur recependo il processo di gestione della rete viene realizzato mediante tecnologie informatiche, pertanto anche in questo ambito gli aspetti di resilienza vengono realizzati attraverso il Disaster Recovery. In realtà, data la natura critica del contesto applicativo, è necessario predisporre un piano di Disaster Recovery che tenga conto anche delle specificità del servizio elettrico e della territorialità del DSO.

La presente memoria ha lo scopo di descrivere il percorso evolutivo dei sistemi di telecontrollo elettrico dei due distributori afferenti al Gruppo Hera volto a rafforzare la sinergia già consolidata tra Inrete e AcegasApsAmga.

La prima fase del piano di Disaster Recovery è data dalla raccolta delle informazioni e dall'analisi delle stesse. Successivamente è stata avviata la fase di progettazione della soluzione di continuità con la definizione di opportune metriche: disponibilità, RTO (Recovery Time Objective) e RPO (Recovery Point Object).

La scenario iniziale era caratterizzato da due infrastrutture di telecontrollo disgiunte, ubicate a circa 300 km di distanza (Modena e Trieste), afferenti a due situazioni impiantistiche distinte dislocate in vaste aree geografiche non adiacenti.
Oltre all'integrazione del sistema di telecontrollo elettrico è stato avviato un piano di armonizzazione dei processi esteso a numerosi aspetti organizzativi.
Inoltre era presente un'asimmetria infrastrutturale: il centro di telecontrollo secondario di Trieste era gestito come un Cold Site (l'hardware necessario per la realizzazione dell'architettura di recovery doveva essere portato all'interno del sito dopo che l'evento dannoso ha avuto luogo) mentre il secondario di Modena era gestito come un Hot Site (contenente tutta l'infrastruttura hardware e software con la configurazione aggiornata; i dati dovevano essere allineati all'ultimo backup proveniente dai sistemi primari).

Il progetto di integrazione ha sancito uno step evolutivo molto importante identificando ciascuno dei centri di telecontrollo come Mirror Site dell'altro.

Il primo requisito è stato quello di incrementare l'affidabilità complessiva dei due sistemi di telecontrollo elettrico.

Dal punto di vista della pertinenza elettrica è stato definito il requisito di segregazione territoriale delle reti, pertanto ciascun impianto è telecontrollato dal centro afferente alla sua area indipendentemente da contesto (Primario/Secondario). Operativamente gli impianti dislocati sul territorio di Modena afferiscono al Back End di Inrete indipendentemente che stia girando presso la sede di Modena (come primario o MAIN o LIVE) o presso la sede di Trieste (come secondario o DR).

Tradizionalmente le funzioni critiche del telecontrollo sono identificate con quelle real time, mentre le funzioni di supervisione e archiviazione non sono considerate non critiche. In questo progetto questo dogma viene meno, infatti un terzo requisito del progetto è stato quello di estendere il concetto di funzioni critiche anche a tutte funzionalità non Real Time (gli archivi di misure ed eventi, i piani di lavoro, etc).

L'allineamento tra il sito MAIN e il sito di DISASTER RECOVERY è garantito da due procedure diverse, una per il sistema di telecontrollo in tempo reale e una per il database relazionale e le applicazioni Web.
In questa memoria verranno illustrate le architetture e le tecnologie adottate, nonché le procedure di allineamento, di ripristino per swichover, di ripristino per failover. Inoltre verranno presentate tutte le accortezze neessarie per gestire eventi accidentali non catastrofici (ad esempio il caso di timeout per la connessione tra due siti).

Il progetto di DR ha permesso di ottimizzare le due infrastrutture di telecontrollo in termini di affidabilità e robustezza senza intaccare le procedure operative dei due DSO.