Disaster Recovery per infrastrutture critiche: mirroring tra due DSO

Lorenzo Camerini
SIEMENS Spa

Paolo Manià
AcegasApsAmga Spa

Alberto Zironi
Inrete Dist. Energia Spa

1. Business Continuity e Disaster Recovery

2. Progetto AcegasApsAmga e Inrete

    - Architettura AS-IS
    - Architettura TO-BE
    - Il Disaster Recovery

3. Punti di Attenzione

4. Conclusioni

Obiettivi principali delle società di Distribuzione Elettrica

- Garantire la continuità del Servizio Elettrico
- Supportare i processi di gestione della Rete
- Garantire il calcolo degli indici di qualità del Servizio
- Garantire la trasmissione dei dati richiesti dal TSO (Terna)
- Scambio dati con altri DSO

↓

Sistemi di Controllo e Gestione

↓

Business Continuity e Disaster Recovery

Resilienza / Affidabilità / Disponibilità

Business Continuity e Disaster Recovery

Metriche

RTO (Recovery Time Objective)

l'intervallo temporale ammissibile di indisponibilità dei sistemi in seguito ad un disastro.

RPO (Recovery Point Objective)

l'ammontare massimo di dati che possono essere persi in seguito ad un disastro

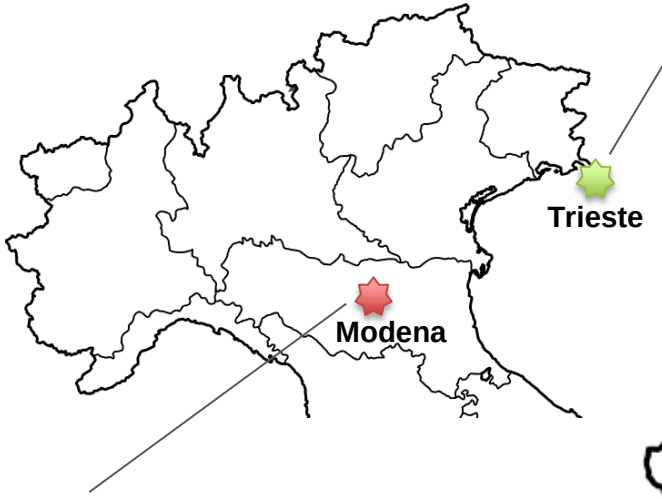
Obiettivi

RTO di minuti

RPO tendente a zero

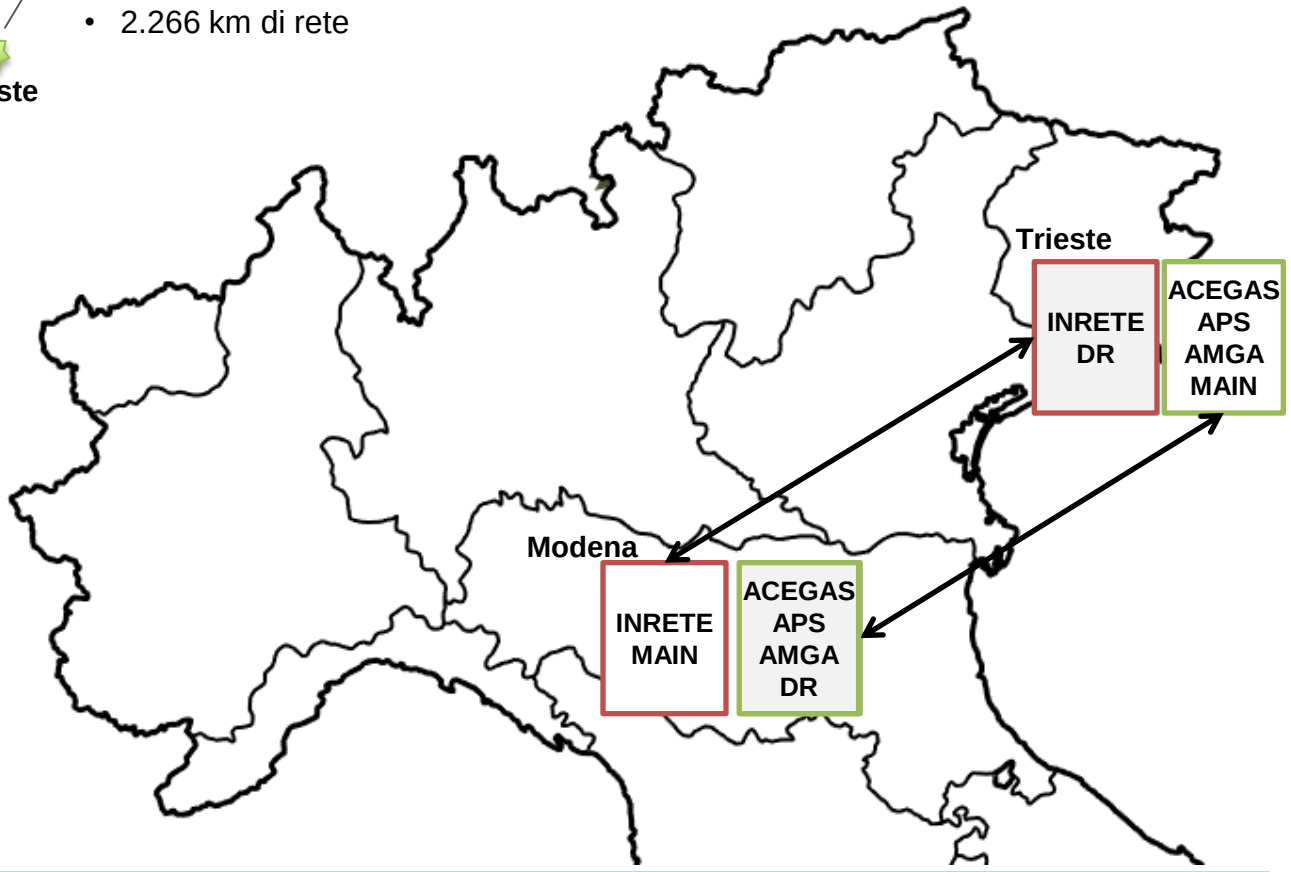
Progetto: AcegasApsAmga e Inrete

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.

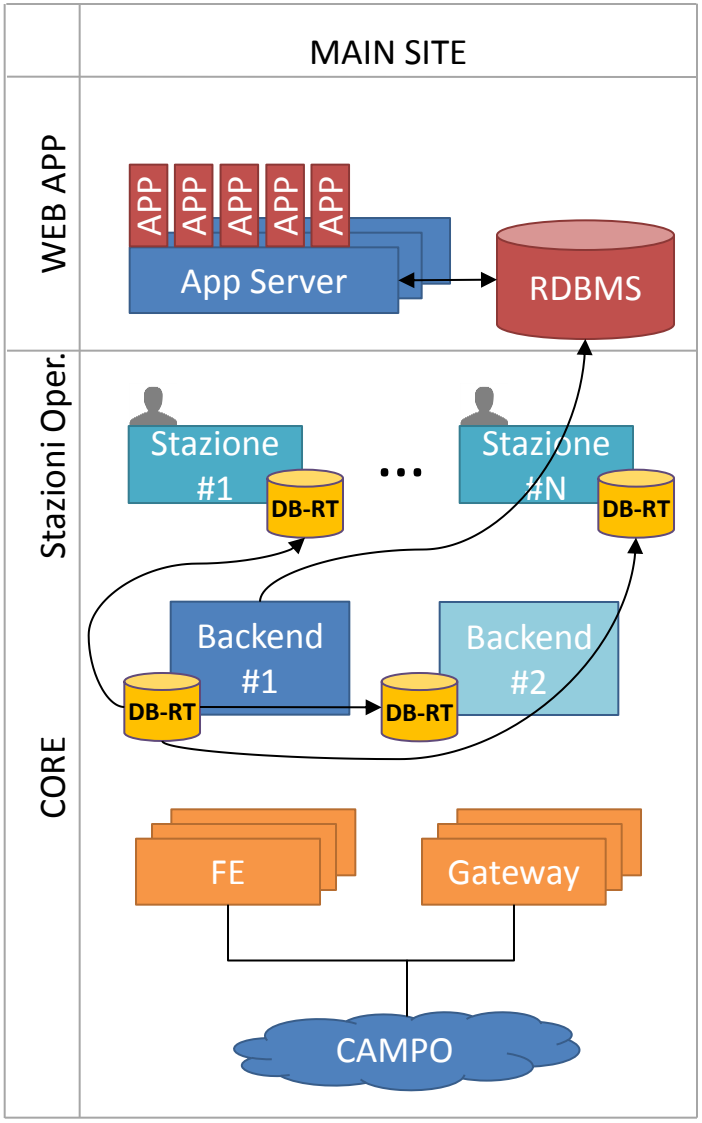


AcegasApsAmga
- Comuni di Trieste e Gorizia
- 163.000 clienti attivi
- 2.266 km di rete

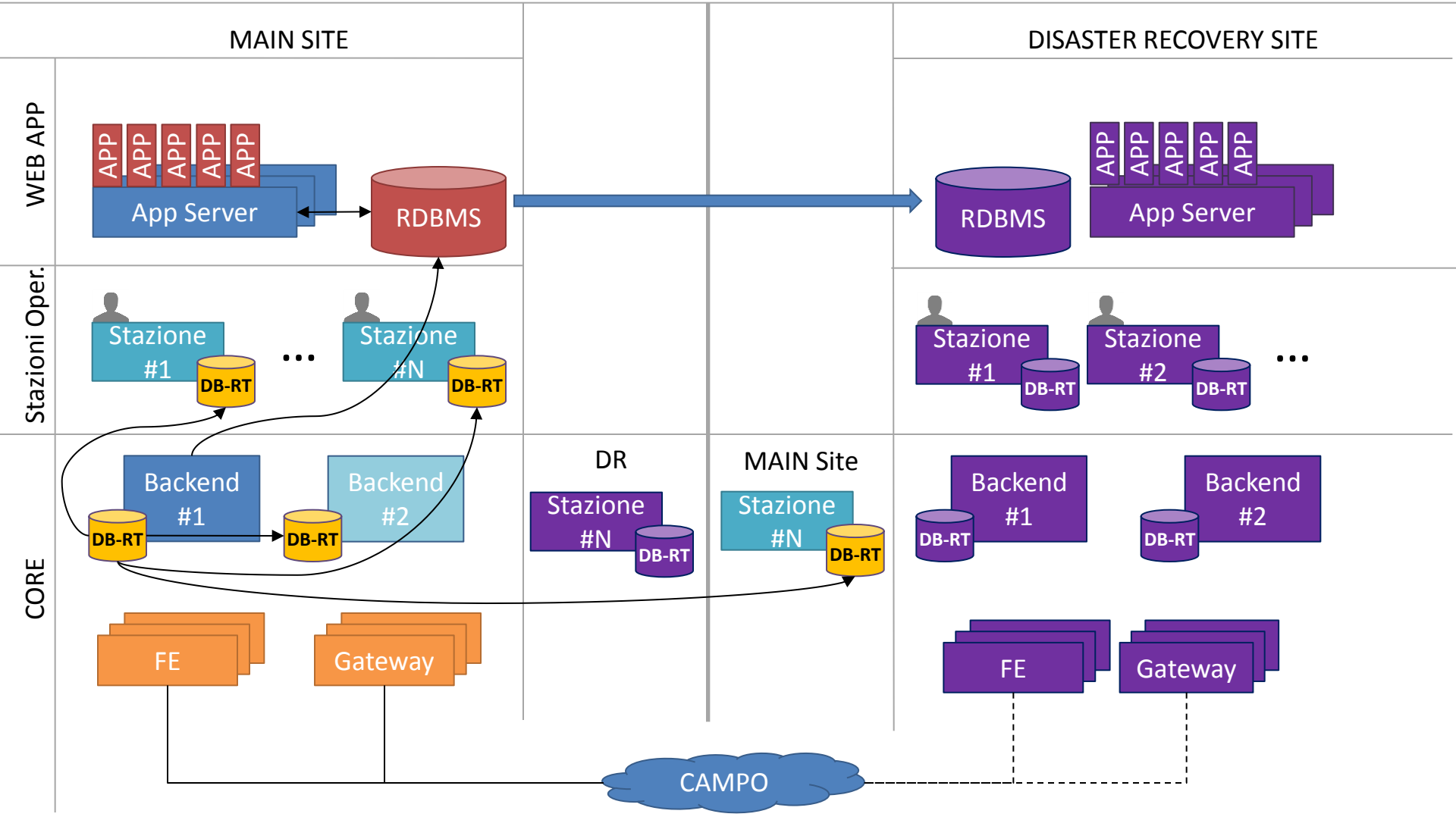
Inrete
- 24 Comuni fra Modena, Bologna e Ravenna
- 260.000 clienti attivi
- 10.155 km di rete



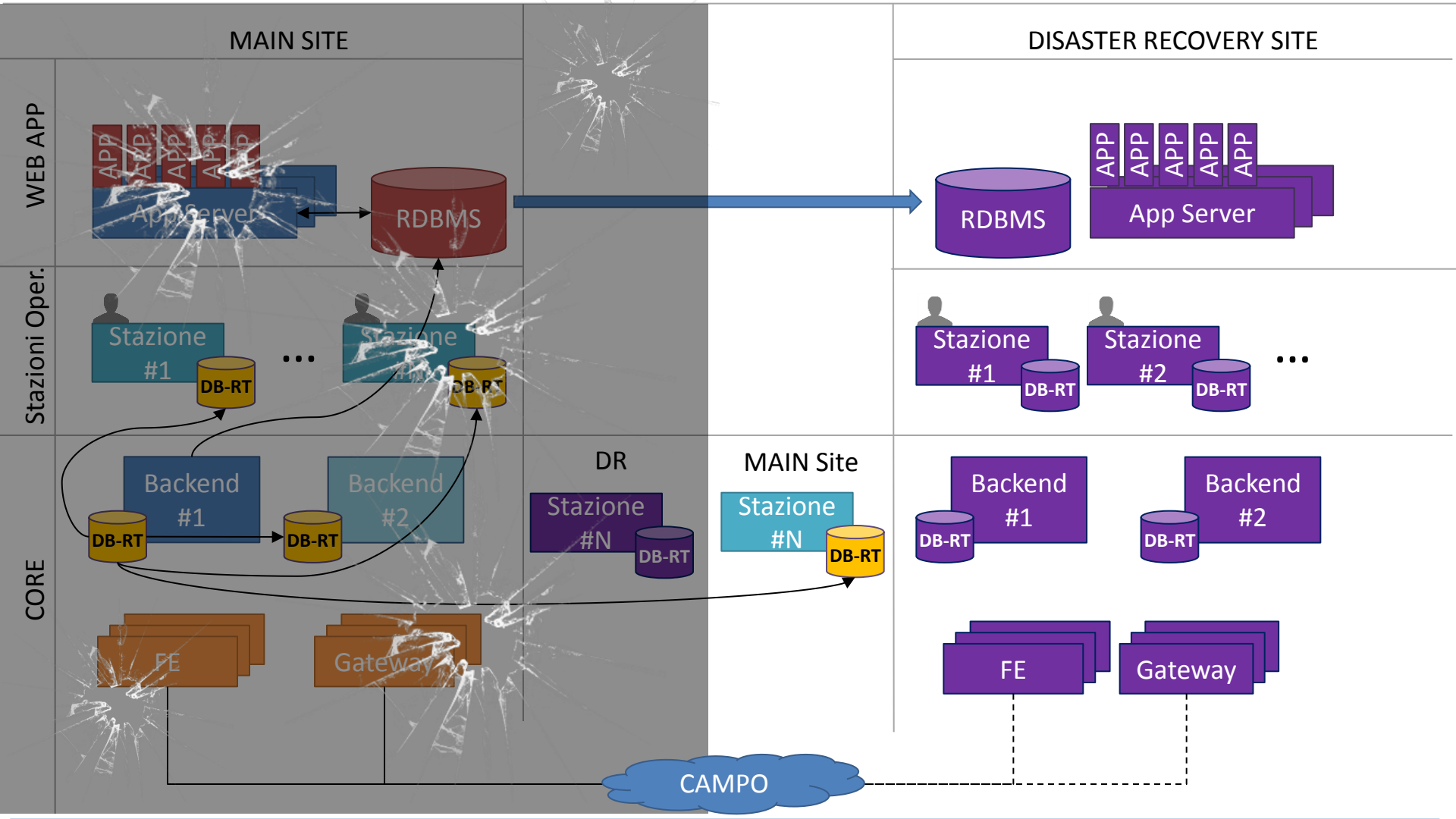
Architettura: AS-IS



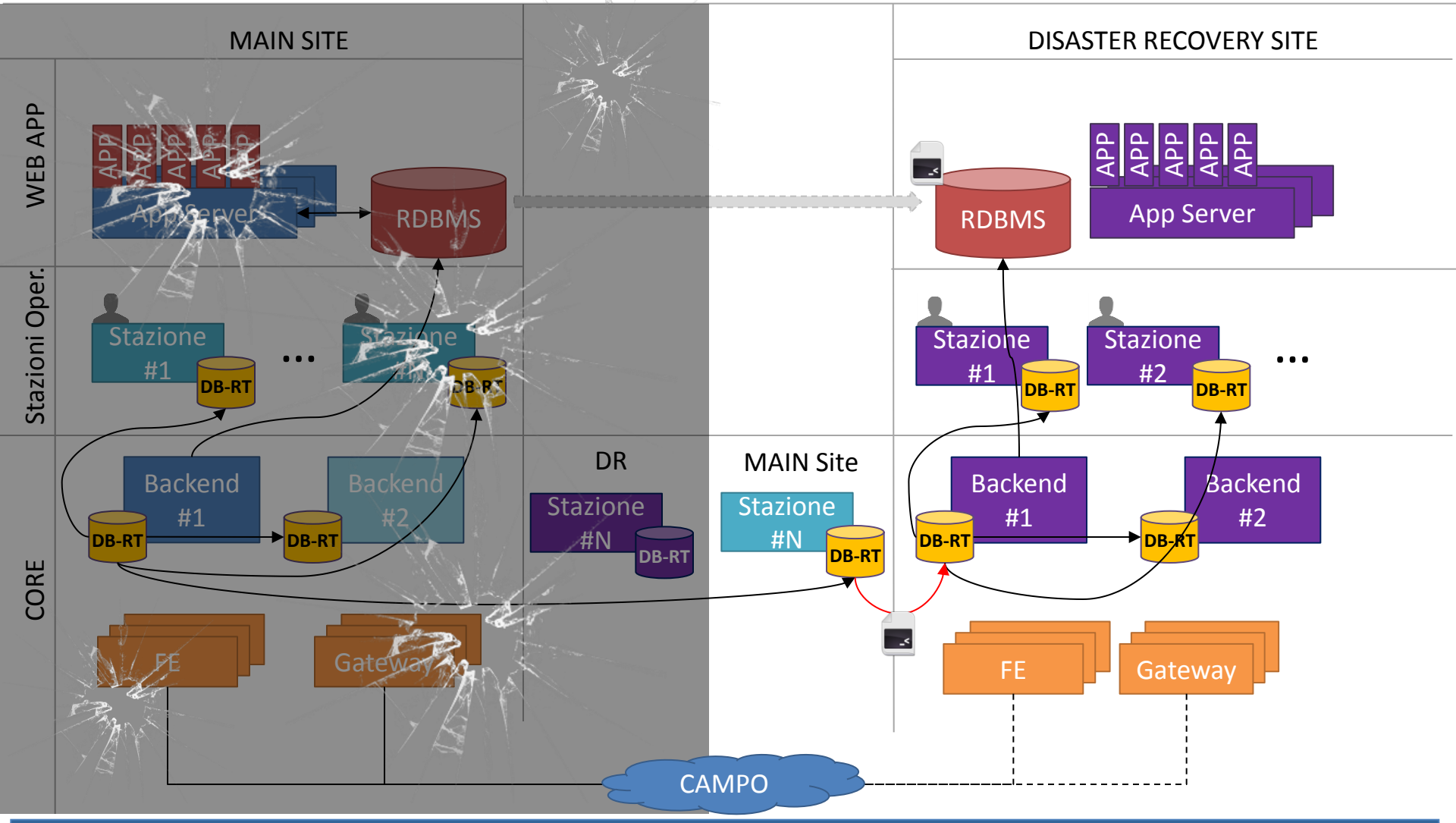
Architettura: TO-BE



Architettura: TO-BE (In caso di disastro)

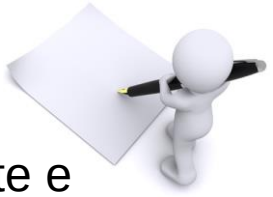


Architettura: TO-BE (In caso di disastro)



Punti di attenzione

- Le Server Farm di ciascun sito devono essere adeguatamente dimensionate per ospitare due sistemi: il sistema MAIN e sistema di Disaster Recovery dell'altro sito.
- La rete di comunicazione e la larghezza di banda che unisce i due siti devono essere adeguati per permettere l'allineamento costante dei due sistemi.
- Il dimensionamento dei dischi delle Server Farm deve essere sufficiente a supportare una disconnessione della rete di comunicazione fra i siti di almeno 24 ore.
- Entrambi i siti devono essere connessi/connettibili alle periferiche di campo.
- Necessità prove periodiche di switch-over
- Cambiano i processi di lavoro, quindi le procedure vanno standardizzate e condivise.



Conclusioni

RTO e Tecnologie

Back-up su Tape off-site (RTO di giorni)
Electronic Tape Vaulting (RTO di parecchie ore)
Back-up Disk to Disk (RTO di alcune ore)
Remote DB Logging (RTO di alcune ore)
Remote Disk Copy Asincrono(RTO di poche ore)
Remote Disk Copy Sincrono (RTO di minuti)

RPO e Tecnologie

Back-up (RPO di circa 24 ore)
Remote DB Logging (RPO di ore/minuti)
Remote Disk Copy Asincrono (RPO di minuti/secondi)

ANIE AUTOMAZIONE

FORUM TELECONTROLLO 2017
RETI DI PUBBLICA UTILITÀ

Grazie per l'attenzione

SIEMENS

Lorenzo Camerini
SIEMENS Spa

lorenzo.camerini@siemens.com

AcegasApsAmga

Paolo Manià
AcegasApsAmga Spa

p.mania@acegasapsamga.it

INRETE DISTRIBUZIONE ENERGIA

Alberto Zironi
Inrete Dist. Energia Spa

alberto.zironi@inretedistribuzione.it

Disaster Recovery per infrastrutture critiche: mirroring tra due DSO

Alberto Zironi
Inrete Dist. Energia Spa

Paolo Manià
AcegasApsAmga Spa

Lorenzo Camerini
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 e 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 servizio 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: RTO (Recovery Time Objective) e RPO (Recovery Point Object).

Lo 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 avesse avuto luogo) mentre il secondario di Modena era gestito come un Warm 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 definisce 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 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 le funzionalità non Real Time (gli archivi di misure ed eventi, interruzioni, 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 necessarie per gestire eventi accidentali non catastrofici (ad esempio il caso di timeout per la connessione tra due siti).

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

INTRODUZIONE

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 e 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.).

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 servizio di ampie porzioni di rete.
Un apporto rilevante alla gestione di tale eventi è il telecontrollo della Rete, realizzato tramite apparati di campo e Sistemi Informatici.

Se l'obiettivo principale di qualunque società di Distribuzione elettrica è la continuità del servizio ~~di distribuzione~~, non meno importanti sono altri aspetti del servizio elettrico, quali:

- la costante trasmissione in tempo reale di informazioni all'Operatore di Trasmissione (in Italia, Terna)
- il calcolo degli indici di qualità, richiesti dai Regolatori per monitorare il servizio
- il supporto ai processi di gestione della rete, quali la ricerca dei guasti e i piani di lavoro necessari per ripristinare il servizio o per modificare strutturalmente la rete
- lo scambio di dati con altri Distributori

Tutti questi processi sono basati su Sistemi Informatici, le cui architetture devono essere adeguate a garantire la necessaria Business Contituity e quindi essere realizzate con tecniche di Disaster Recovery.

BUSINESS CONTINUITY E DISASTER RECOVERY

Per **Business Continuity** (o *Continuità Operativa*) si intende la capacità di un'organizzazione di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente.
Si tratta quindi del processo strategico e tattico che permette ad un'organizzazione di avere una risposta a qualunque avvenimento che può avere impatto sul "core business" aziendale, garantendo un livello di servizio minimo accettabile predefinito.

Il **Disaster Recovery** (o Recupero dal Disastro), in informatica ed in particolare nell'ambito della sicurezza, è l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business, a fronte di gravi emergenze che ne intacchino la regolare attività.
Un disastro è la conseguenza dell'attuarsi di una minaccia non dovuta ad una aggressione intenzionale, come i disastri naturali (terremoto, alluvione, etc.) o i disastri dovuti all'uomo e alla tecnologia (incendio, esplosione, mancanza di linee di telecomunicazione, etc.).

Le metriche del Disaster Recovery sono definite da due indici, di seguito descritti:

RTO (Recovery Time Objective) = esprime in unità di tempo, l'intervallo temporale ammissibile di indisponibilità dei sistemi in seguito ad un disastro.
RPO (Recovery Point Objective) = esprime in unità di tempo, l'ammontare massimo di dati che possono essere persi in seguito ad un disastro.

In Figura 1 sono esemplificati i due indici. L'RTO è l'intervallo di tempo che intercorre dalla notifica del disastro alla ripresa del servizio, passando attraverso l'attivazione della soluzione di Disaster Recovery. L'RPO è l'intervallo di tempo ammissibile all'interno del quale i dati possono essere persi.

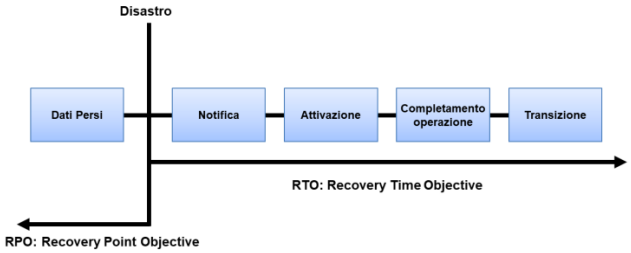


Figura 1 RTO e RPO

E' inoltre importante correlare i costi dell'indisponibilità delle applicazioni con il costo delle soluzioni di recovery.
In Figura 2 si evidenzia come il costo dell'indisponibilità delle applicazioni real-time cresca esponenzialmente dopo pochi minuti, mentre il costo dell'indisponibilità delle applicazioni di back-office cresca dopo ore/giorni.
Ovviamente i costi delle soluzioni di recovery diminuiscono all'aumentare del tempo di indisponibilità accettabile.
Nel caso dei Sistemi di Telecontrollo e Gestione Rete, che informatizzano applicazioni real-time, l'RTO deve essere nell'ordine di minuti.
Il grafico di Figura 2 può essere applicato anche nel caso di RPO.
Anche in questo caso è quindi importante puntare a soluzioni che mantengano l'RPO nell'ordine di minuti.
Ne consegue che è necessario avvalersi di soluzioni di Disaster Recovery di costo adeguato.

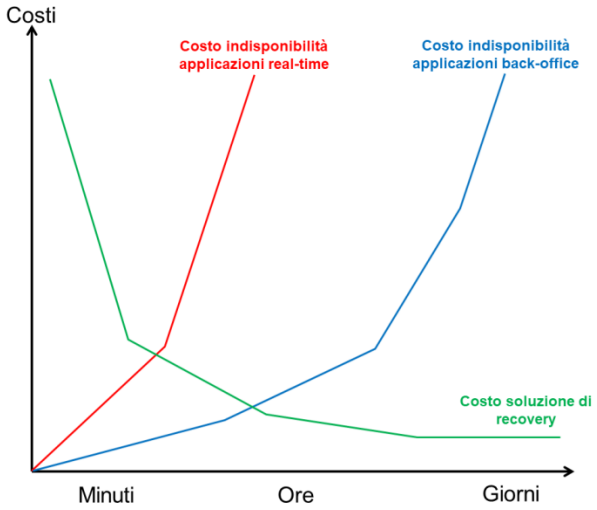


Figura 2 RTO e Costi

Tradizionalmente le funzioni critiche del telecontrollo sono identificate con quelle real-time, mentre le funzioni di supervisione e archiviazione sono considerate non critiche. Nel progetto descritto in questa memoria questo aspetto viene meno, infatti un requisito innovativo è stato quello di estendere il concetto di funzioni critiche anche a tutte le funzionalità non real-time (archiviazione di misure ed eventi, interruzioni, piani di lavoro, etc).

Nel seguito viene riportato uno schema che illustra come RTO e RPO possono variare in funzione delle tecnologie impiegate.

RTO e Tecnologie:

- Back-up su Tape off-site (RTO di giorni)
- Electronic Tape Vaulting (RTO di parecchie ore)
- Back-up Disk to Disk (RTO di alcune ore)
- Remote DB Logging (RTO di alcune ore)
- Remote Disk Copy Asincrono (RTO di poche ore)
- Remote Disk Copy Sincrono (RTO di minuti)

RPO e Tecnologie:

- Back-up (RPO di circa 24 ore)
- Remote DB Logging (RPO di ore/minuti)
- Remote Disk Copy Asincrono (RPO di minuti/secondi)

Nella memoria verrà descritto il progetto di Disaster Recovery in corso di realizzazione per Inrete e AcegasApsAmga.
L'obiettivo del progetto è quello di definire un'architettura che possa portare ad un RTO dell'ordine di minuti e un RPO tendente a zero.

ARCHITETTURA AS IS

Lo 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.
Inoltre era presente un'asimmetria infrastrutturale. Il centro di telecontrollo secondario di Trieste era gestito come un Cold Site, vale a dire che, in caso di evento dannoso, l'hardware necessario per la realizzazione dell'architettura di recovery doveva essere portato all'interno del sito.

Figura 3 Siti Modena e Trieste

Il secondario di Modena, invece, era gestito come un Warm Site vale a dire che il sito conteneva già tutta l'infrastruttura hardware e software con la configurazione aggiornata; i dati, invece, dovevano essere allineati all'ultimo backup proveniente dai sistemi primari.

Per entrambi i centri di controllo l'architettura del sistema è quella descritta in Figura 4.

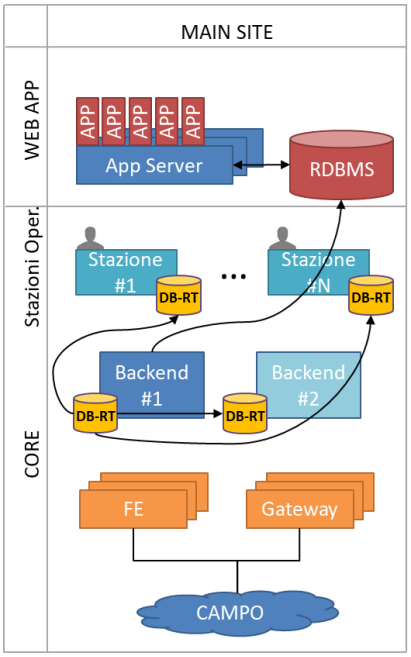


Figura 4 Architettura Telecontrollo AS-IS

Si tratta di un'architettura a tre livelli funzionali: acquisizione da campo, elaborazione centrale e applicazioni web di supporto ai processi aziendali.
Le periferiche di campo sono connesse a front-end di acquisizione dati in grado di gestire diversi protocolli di comunicazione. Le elaborazioni core vengono effettuate da server di backend ridondati, tramite applicazioni che si basano su un database real-time proprietario. La caratteristica di questo database è quella di essere distribuito, replicato su server e stazioni operative e costantemente aggiornato. Infine le applicazioni di processo (archiviazione misure,

eventi, interruzioni, piani di lavoro, etc.) sono allocate su Application Server e si basano su un database relazionale commerciale.

ARCHITETTURA TO BE

Il progetto di integrazione fra Inrete e AcegasApsAmga definisce uno step evolutivo importante, identificando ciascuno dei centri di telecontrollo come Mirror Site dell'altro.
Come si può vedere in Figura 5 la soluzione mira a sfruttare i due siti esistenti al fine di ospitare ciascuno il sistema di Disaster Recovery dell'altro.

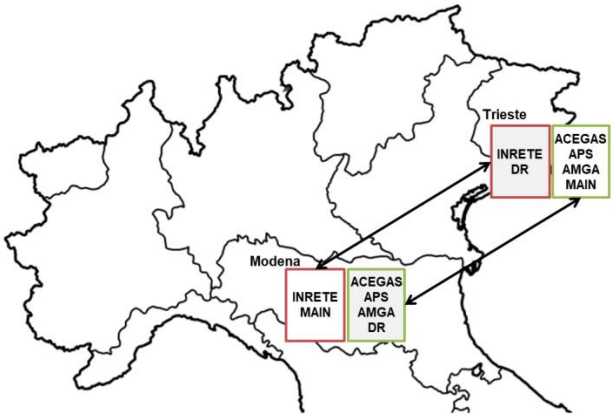


Figura 5 Mirroring fra Modena e Trieste

Dal punto di vista della pertinenza elettrica è stato definito il requisito di segregazione territoriale delle reti. Operativamente, ad esempio, gli impianti dislocati sul territorio di Modena afferiranno al backend di Inrete, indipendentemente che questo sia attivo presso la sede di Modena (sito primario) o presso la sede di Trieste (sito di Disaster Recovery).

Affinché ciò sia possibile, il primo passo realizzativo è quello di passare da un sistema su hardware dedicato a un sistema virtualizzato, operante su un hardware di ultima generazione, opportunamente dimensionato per ospitare due sistemi di Telecontrollo.

La virtualizzazione e il consolidamento dei server permette di aumentare l'affidabilità, la flessibilità, l'efficacia e la convenienza economica della soluzione.

In Figura 6 viene mostrata l'architettura del Disaster Recovery. Per ottenere l'allineamento costante dei dati vengono adottate soluzioni diverse, a seconda si tratti delle funzionalità di real-time o delle funzionalità di archiviazione e back-office.
Per ottenere una replica del database real-time nel sito di Disaster Recovery è stato sufficiente installare una stazione operativa del Sistema di Telecontrollo collegata al sito primario e quindi costantemente aggiornata.
Grazie alla replica del database real-time su questa stazione remotizzata è possibile, come illustrato nel seguito, ripristinare in tempi brevi i dati su tutti i nodi del sistema di Disaster Recovery.
Per ottenere l'aggiornamento del database relazionale si è invece utilizzata una soluzione commerciale. Il meccanismo scelto supporta sia un allineamento sincrono che uno asincrono dei dati. La soluzione sincrona garantirebbe un RPO pari a zero ma richiederebbe un'elevata banda e alta affidabilità della connessione. La soluzione asincrona, invece, garantisce un RPO nell'ordine dei minuti, ma non necessita di un canale di comunicazione ad alte prestazioni.
In base ai requisiti di progetto, alla tipologia di dati e alla rete di comunicazione disponibile, la soluzione asincrona è stata ritenuta la scelta ottimale. In futuro, qualora la rete di comunicazione venisse potenziata, sarebbe possibile considerare il passaggio ad un meccanismo sincrono.

Per quanto riguarda le periferiche di campo è necessario che tutti i periferici siano raggiungibili da entrambi i siti (primario e Disaster Recovery) e quindi che siano connessi tramite una rete WAN o GSM/GPRS. Inoltre è opportuno che ogni apparato periferico usi lo stesso protocollo verso entrambe le istanze.

Nel caso di Inrete e AcegasApsAmga la presenza di periferiche di tipo diverso ha comportato uno studio e un impegno specifico per l'adeguamento di alcune di esse.

L'architettura di Disaster Recovery fin qui descritta si configura come un DR in STANDBY, dove i dati sono costantemente aggiornati e le applicazioni sono dormienti.

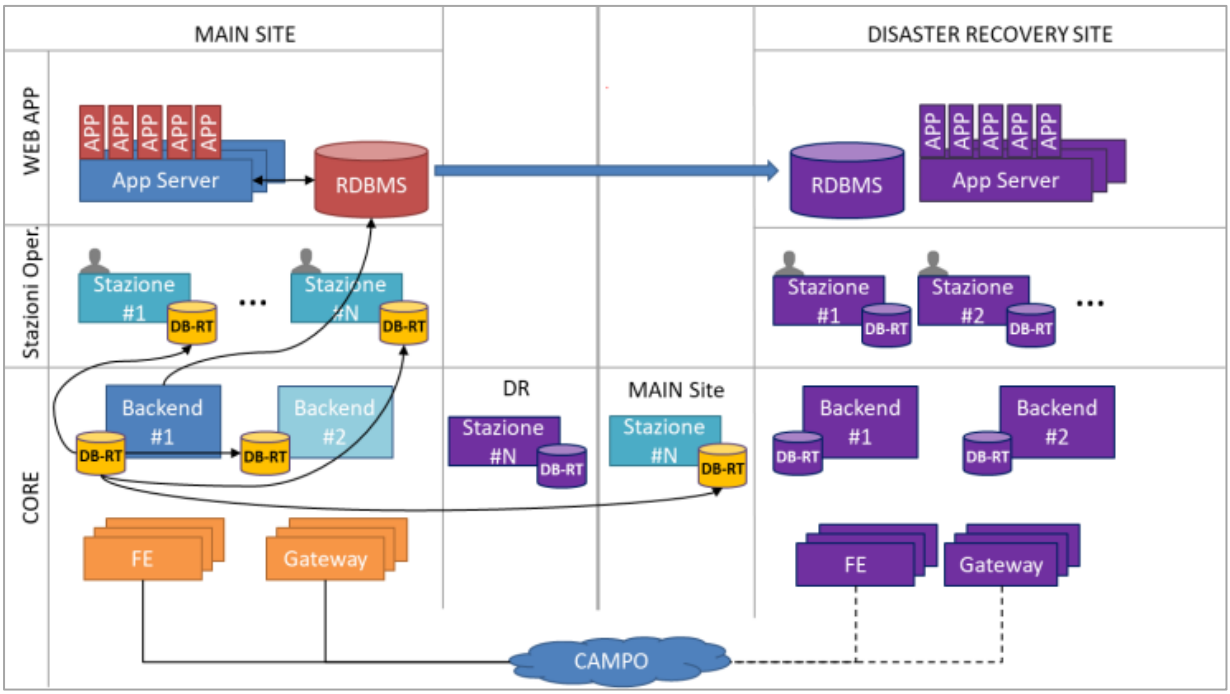


Figura 6 Architettura di Disaster Recovery

In caso di disastro è stata predisposta una procedura operativa che deve essere attivata volontariamente dalla persona preposta, la quale, grazie all'esecuzione di script, attiva il sistema secondo la seguente sequenza (Figura 7):

1. Il database real-time viene copiato dalla stazione aggiornata al backend del Disaster Recovery.
2. Il database relazionale passa dalla modalità standby a quella operativa.
3. Vengono attivati tutti i nodi: frontend, backend, stazioni operative e application server.
4. All'attivazione dei nodi, tutte le stazioni allineano il proprio database con quello del backend aggiornato, ripristinando di fatto le funzionalità real-time che precedentemente erano operative sul sito principale.
5. I frontend prendono in carico il campo.
6. Le applicazioni di archiviazione e backend ripartono, trovando gli stessi dati del sistema primario e rendendo nuovamente disponibili le interfacce web utilizzate dal business.

Quanto sopra descritto viene definito "procedura di ripristino per failover", in quanto applicata quando la transizione fra sito primario e sito Disaster Recovery è conseguenza di un grave problema, che rende il sito primario non raggiungibile o non disponibile.
Nel caso in cui la transizione venga effettuata come simulazione periodica del recovery e verifica dell'efficacia della soluzione, si parlerà di "ripristino per switchover", dove i due siti cambiano semplicemente ruolo: il sito di

Disaster Recovery diventa primario, mentre il primario diventa di Disaster Recovery.

PUNTI DI ATTENZIONE

Nel seguito vengono elencati alcuni punti chiave da prendere in considerazione progettando una soluzione di Disaster Recovery analoga a quella descritta.

- Le Server Farm di ciascun sito devono essere adeguatamente dimensionate per ospitare due sistemi: il sistema principale e il sistema di Disaster Recovery.
- La rete di comunicazione e la larghezza di banda fra i due siti devono essere adeguati a permettere l'allineamento dei sistemi in funzione dell'RPO definito. A tal scopo è opportuno considerare soluzioni ridondate con connettività ben separate e servizi forniti da provider diversi.
- Il dimensionamento dei dischi delle Server Farm deve essere sufficiente a supportare una disconnessione della rete di comunicazione, evento non trascurabile e che può avere impatto rilevante sulla continuità dei dati. Nel progetto presentato tale dimensionamento supporta una disconnessione fra i siti di almeno 24 ore.
- Entrambi i siti devono essere connessi/connettibili alle periferiche di campo e ciò può comportare interventi di ammodernamento, armonizzazione e richiede una analisi specifica.

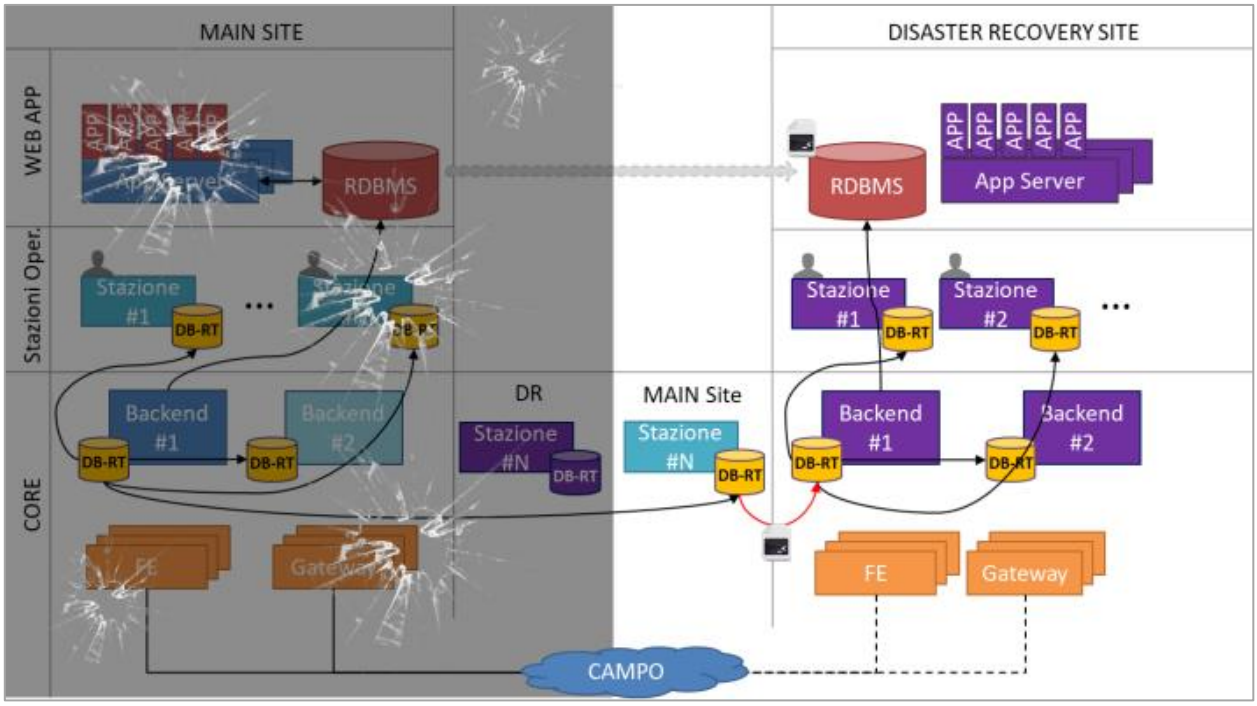


Figura 7 Attivazione del Disaster Recovery

Infine si ricorda che una soluzione di Disaster Recovery non va intesa come un intervento "una tantum" ma come un processo operativo/gestionale continuo che deve essere

monitorato, adeguato e aggiornato in base alle esigenze del business e alle evoluzioni tecnologiche.

CONCLUSIONI

Grazie all'architettura illustrata e alle soluzioni tecnologiche adottate, Inrete e AcegasApsAmga disporranno a breve di una soluzione up-to-date di Disaster Recovery, che consentirà ai due distributori di garantire la Business Continuty nell'ambito di un processo critico quale è la distribuzione dell'energia elettrica.

Il progetto è stato una importante occasione per l'ammodernamento e potenziamento dell'hardware che supporta i sistem, aumentandone l'affidabilità.

Un aspetto innovativo è stata l'inclusione nei processi di Disaster Recovery di tutte le applicazioni non real-time, ma legate al Telecontrollo: ciò permetterà di salvaguardare anche processi di analisi, calcolo e backoffice.

La soluzione è economicamente sostenibile in quanto sfrutta siti e locali esistenti ed è attuabile anche con una rete di connessione limitatamente performante.

Infine è importante sottolineare che la resilienza della rete elettrica si basa non solo su interventi mirati agli asset fisici della rete (manutenzione, pianificazione, ammodernamento), ma deve prendere in considerazione anche i sistemi informatici. E le soluzioni di Disaster Recovery non possono essere più considerate un lusso, ma una reale inderogabile necessità.