CONSORZIO OPERATIVO GRUPPO MPS

Il Disaster Recovery oggi, a seguito delle più recenti innovazioni tecnologiche

V. Giardina - Staff Continuità Operativa
C. Degani – Ufficio Change Management

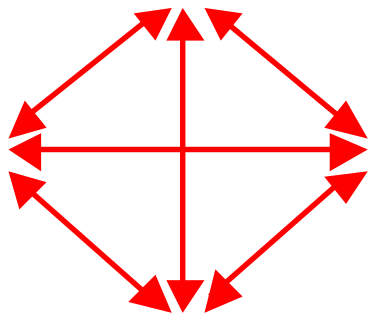
GRUPPO MPS

Gli "asset" del Gruppo al 30/9/2003:

- ✓ 27.040 dipendenti
- ✓ 1.835 filiali Italia
- ✓ 38 filiali e rappr. Estero
- ✓ 4.425.000 clienti

Le linee strategiche:

- ✓ modello di business: **centralità del cliente**
- ✓ modello organizzativo: **ottica divisionale**



Banca MPS
Banca Agricola Mantovana
Banca Toscana
Banca Steinhauslin
Banca 121 Promozione Finanziaria

4 Banche estere

MPS Finance
MPS Banca Verde
MPS Merchant
Consum.it
MPS Leasing & Factoring
MPS Asset Mngmt SGR
Ticino Assicurazioni
Ticino Vita
Montepaschi Vita
Grow Life
Web Sim
MPS Net
MPS Gest. Crediti Banca

Amministrazioni Immobiliari
Paschi Gestioni Immobiliari

Consorzio Operativo Gruppo MPS

I Consorziati

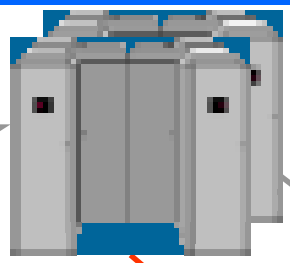
- Banca Monte dei Paschi di Siena
- Banca Toscana
- Banca Agricola Mantovana
- Banca Steinhauslin
- Banca 121 P.F.
- MPS Finance
- MPS Merchant
- MPS Banca Verde
- MPS Gestione Crediti Banca
- MPS Leasing & Factoring

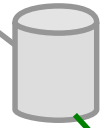
CONSORZIO OPERATIVO GRUPPO MPS

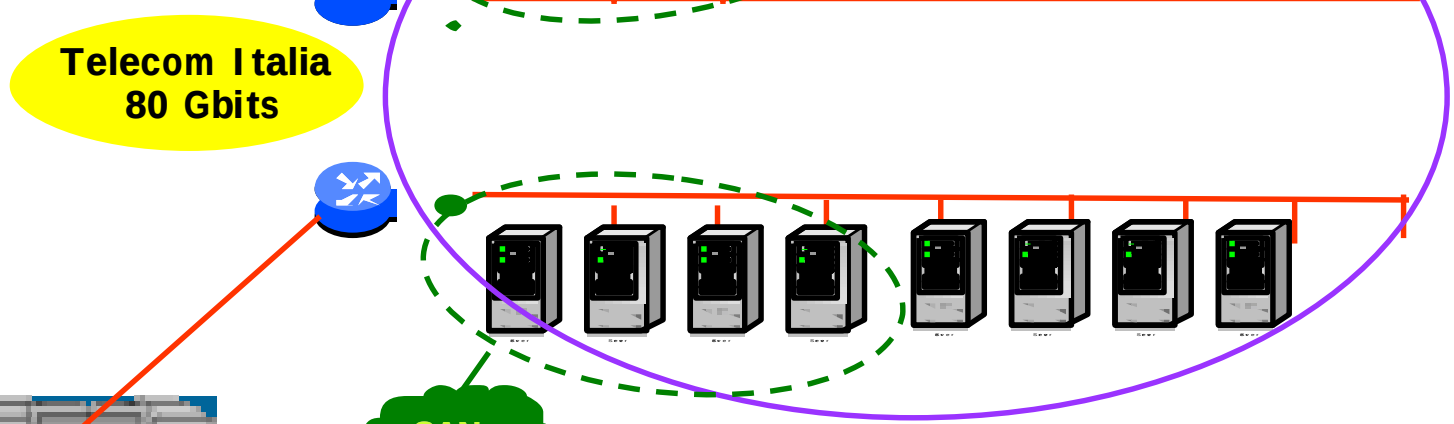
Le infrastrutture tecnologiche centrali

- BT
- MPS Merchant
- Banca Verde
- Steinhauslin
- Banca 121 PF
- MPS Leasing & Factoring
- MPS Gestione Crediti
- Esattorie
- MontePaschiVita

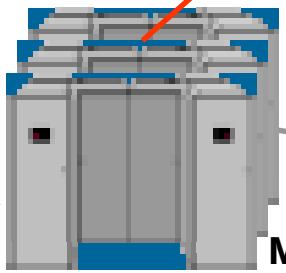
- BMPS
- BAM
- MPS Finance
- SGR
- Ambienti di test e collaudo





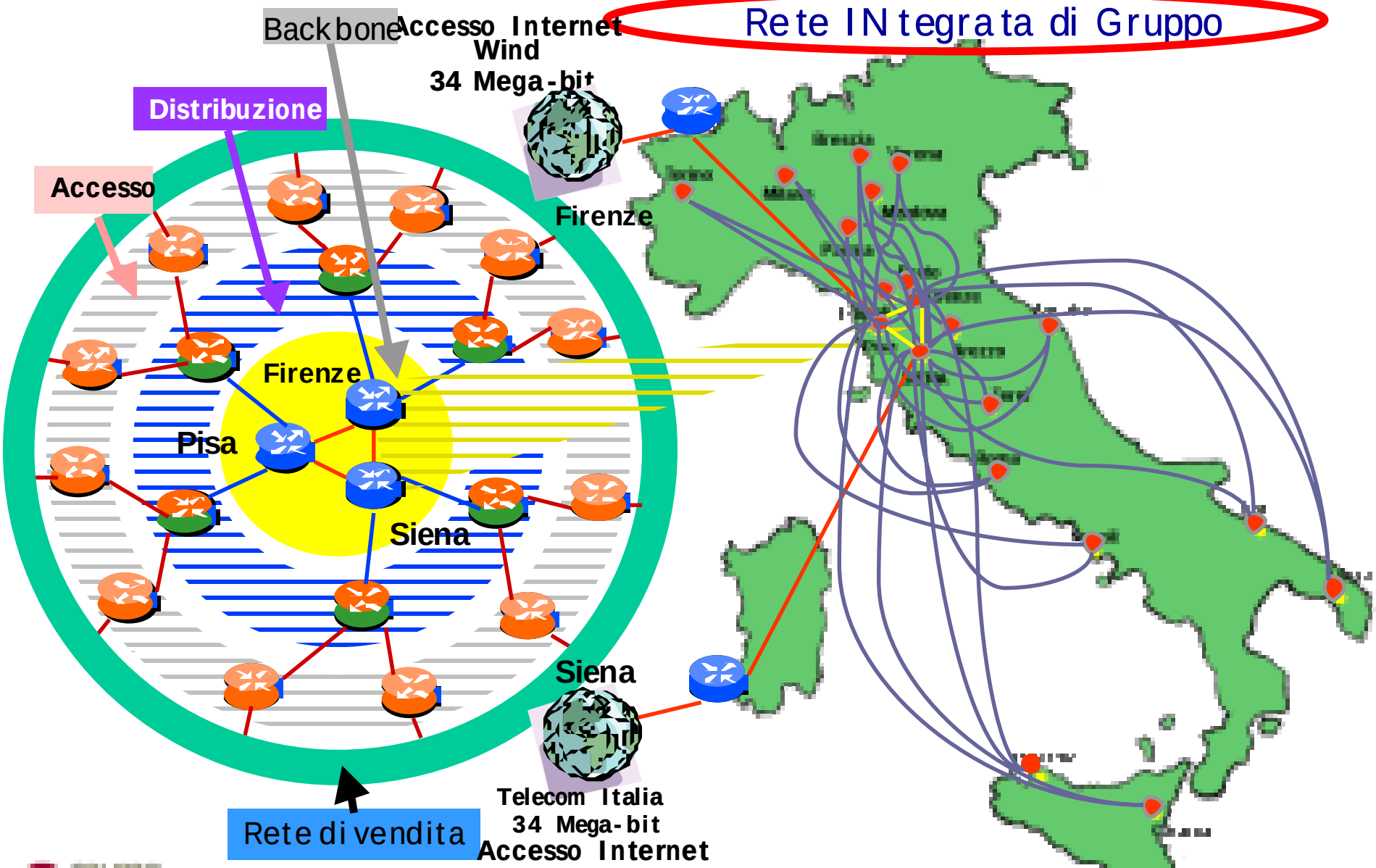


Telecom Italia
80 Gbits

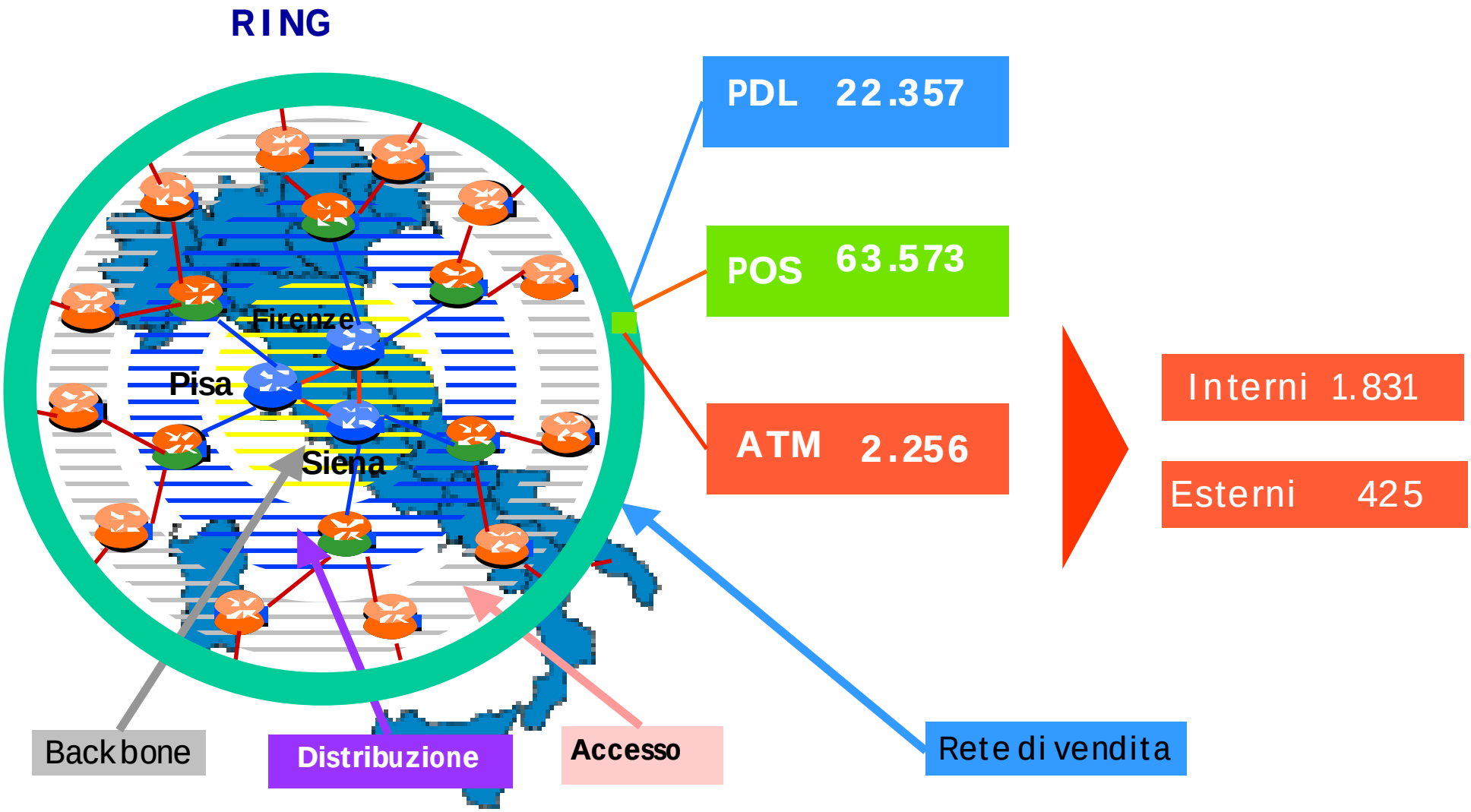


Totale MIPS 14.000; Totale GBYTE 63.000

Le infrastrutture tecnologiche di telecomunicazione



Le infrastrutture tecnologiche periferiche



Considerazioni Preliminari

- *i processi aziendali devono essere riconsiderati in logica di business continuity*

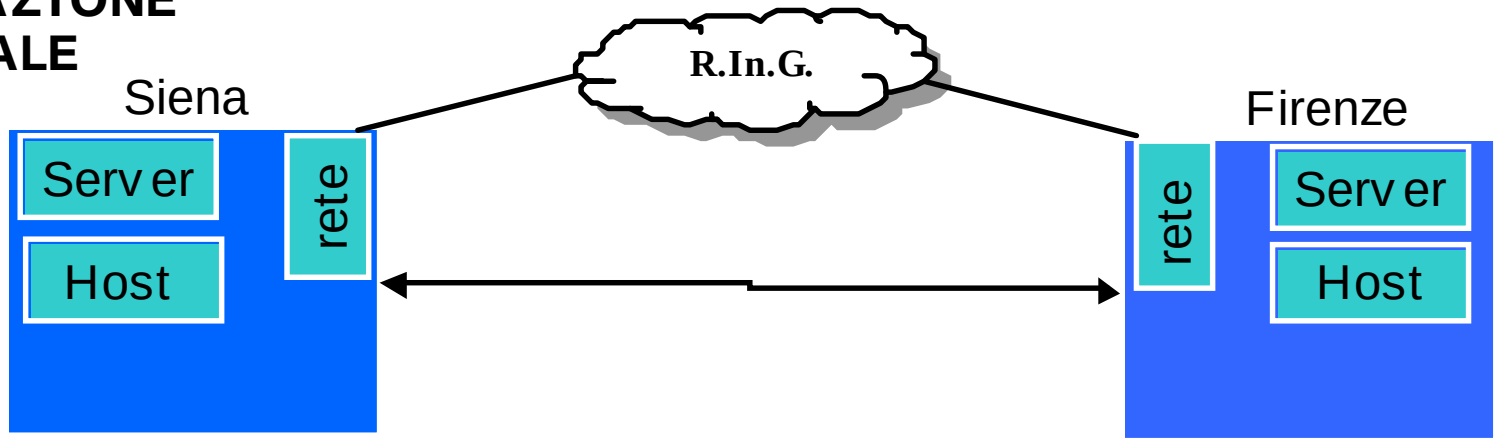
- *ogni processo, sia interno sia di relazione verso l'esterno, deve essere rivisitato pesando per ciascuno le priorità e l'impatto che eventi "disastrosi" possono avere sia sul singolo processo sia sui processi a monte ed a valle dello stesso.*

- *un Gdl interfunzionale provvederà alla definizione di ruoli, responsabilità e tempi per il coordinamento di tutta la problematica, sia in fase di sviluppo sia a regime.*

- *nell'individuazione dei processi critici, a garanzia dell'integrita' del "sistema, si dovrà tener conto delle Linee Guida emanate dalla Banca d'Italia e delle indicazioni provenienti dal gdl ABI.*

- *le cosiddette "utilities" devono prioritariamente dare "garanzia di sicurezza" nella continuità dei servizi di fatto "indispensabili" e la cui mancanza verrebbe a vanificare qualunque misura messa in atto.*

SITUAZIONE ATTUALE



Due CED con architetture HW e SW identiche

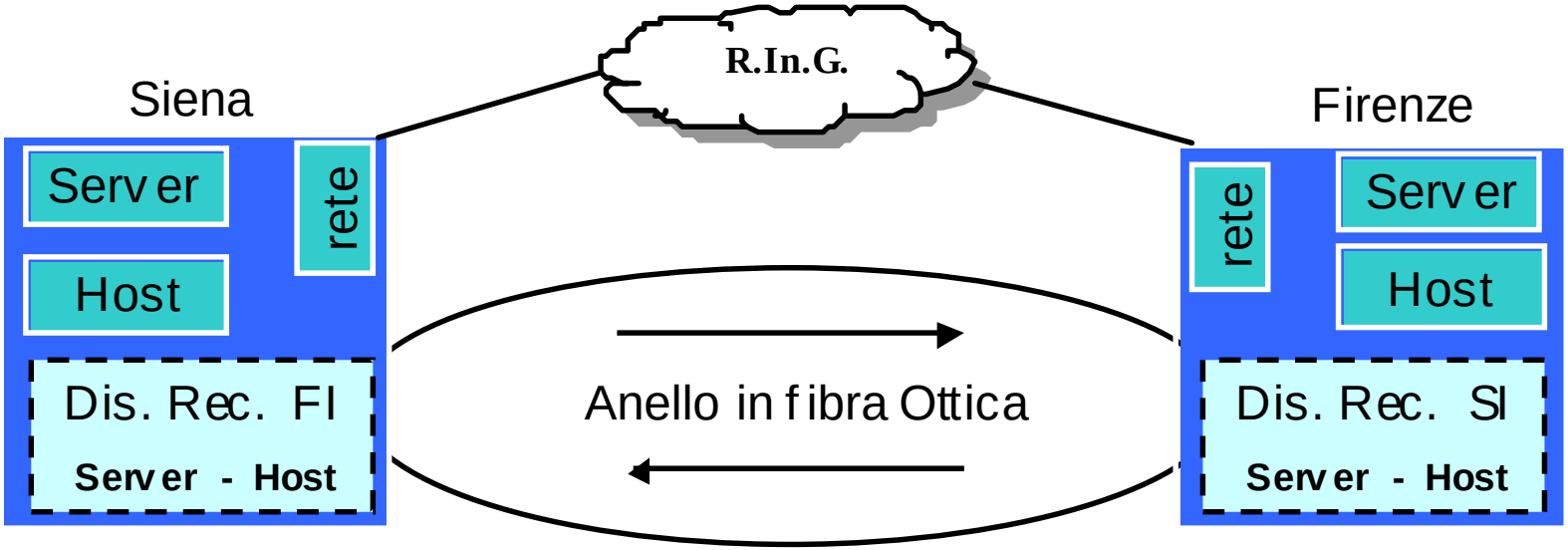
Unico sistema informativo replicato per tutte le Banche Consorziate

Connettività di rete con percorsi ridondanti e alternativi

Le filiali possono collegarsi ai due CED

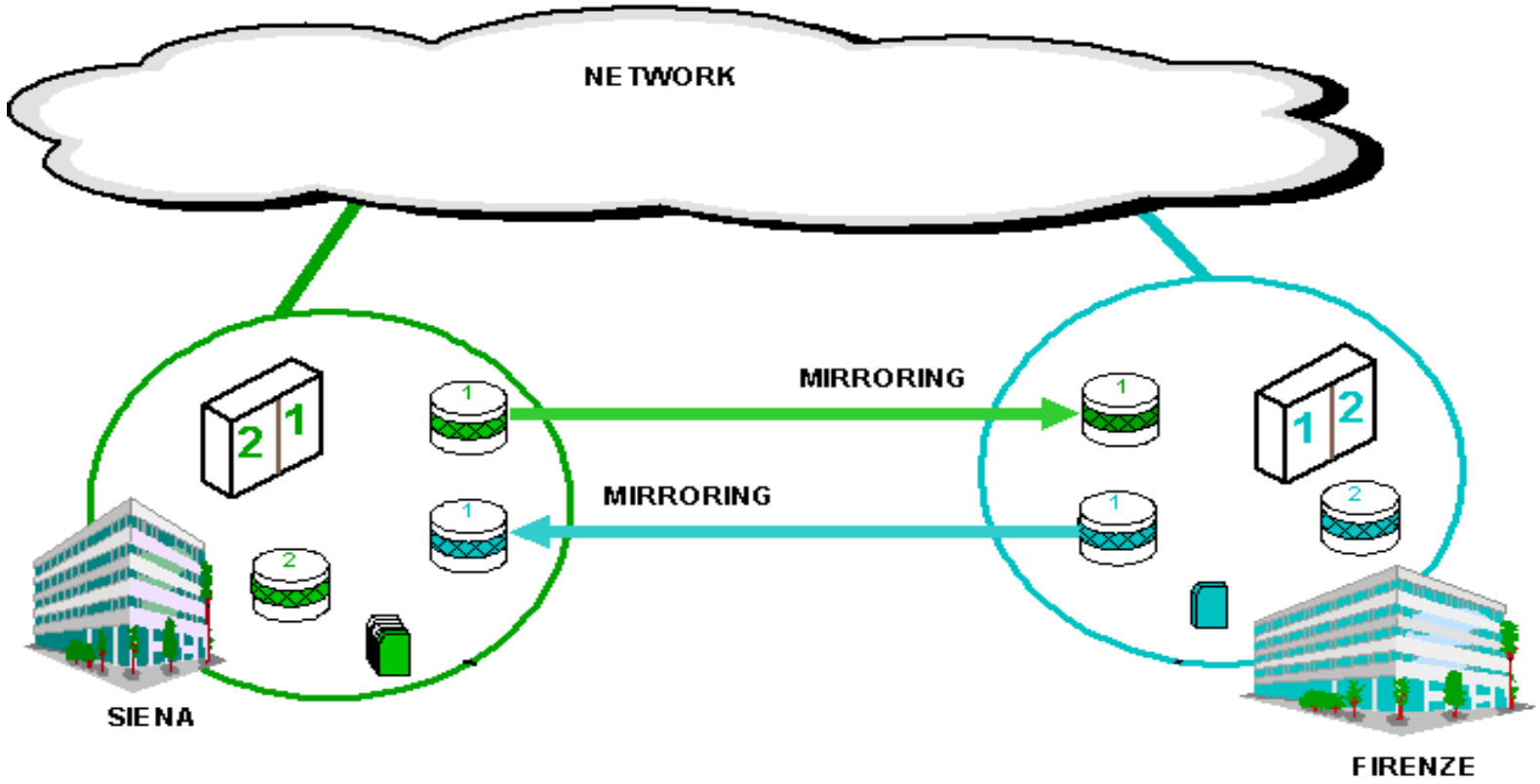
Operatività svolta da personale di tutti i Poli (SI, FI, MN, LE), anche remotamente, rispetto

Linee guida per l'EVOLUZIONE

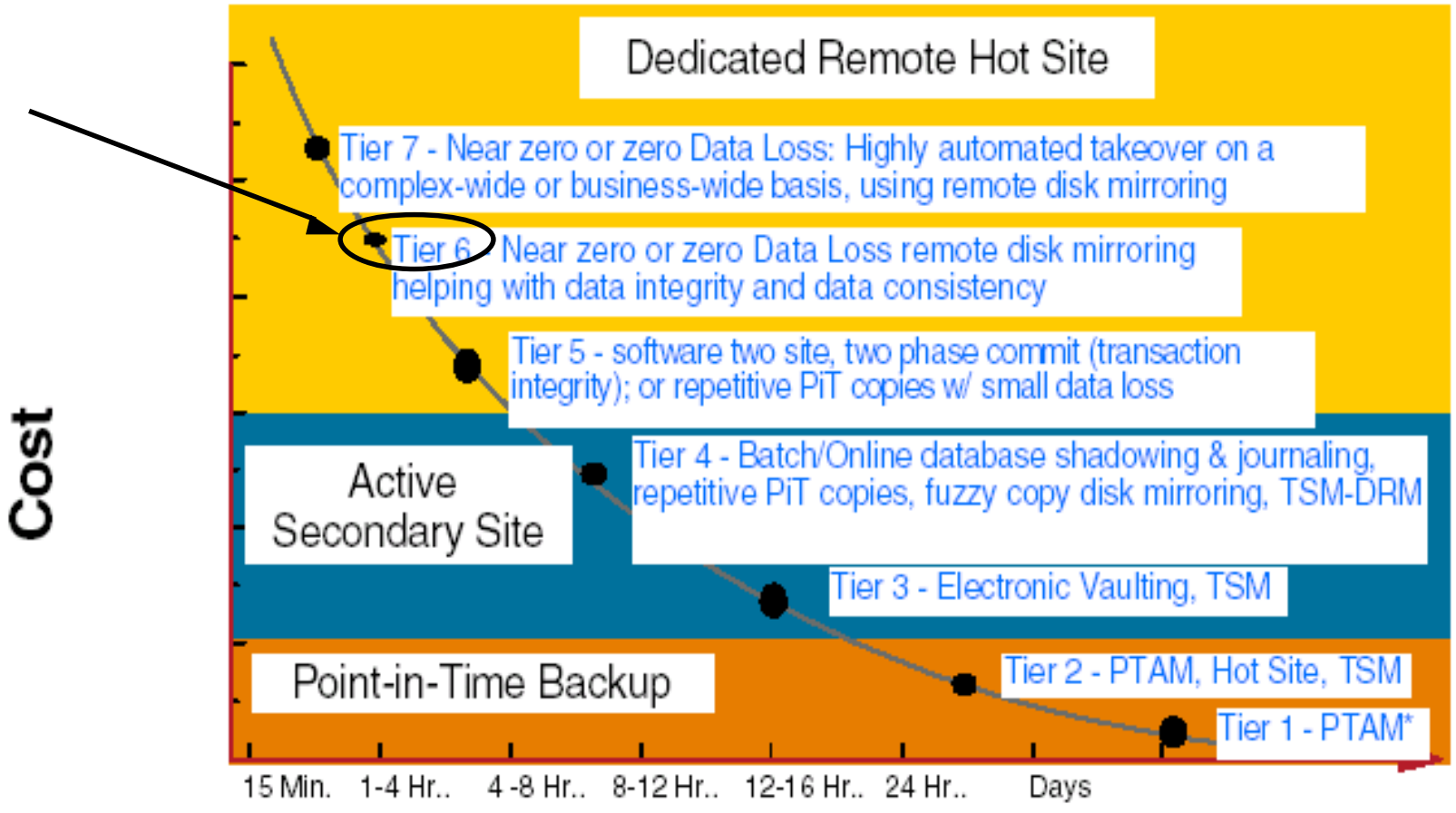


- **Sistema trasmissivo ad ampia capacità e velocità**
- **Ridondanza dei componenti, finalizzati al singolo servizio, distribuita fra i due Poli**
- **Copia continua di tutta la base dati (componente legacy e dipartimentale accentrata)**
- **Ogni CED funge da centro secondario di backup all'altro (visione "active-active" con possibilità di specializzare i Poli)**

La distanza tra i due CED, pari su percorso terreno a 90 KM circa, configura il progetto come uno dei più avanzati dal punto di vista della protezione al rischio…ma anche della **complessità esecutiva**.



Possibili livelli verso la business continuity ….



La soluzione ipotizzata si colloca per i processi "business critical" su un **TIER 6** e si basa sui seguenti obiettivi:

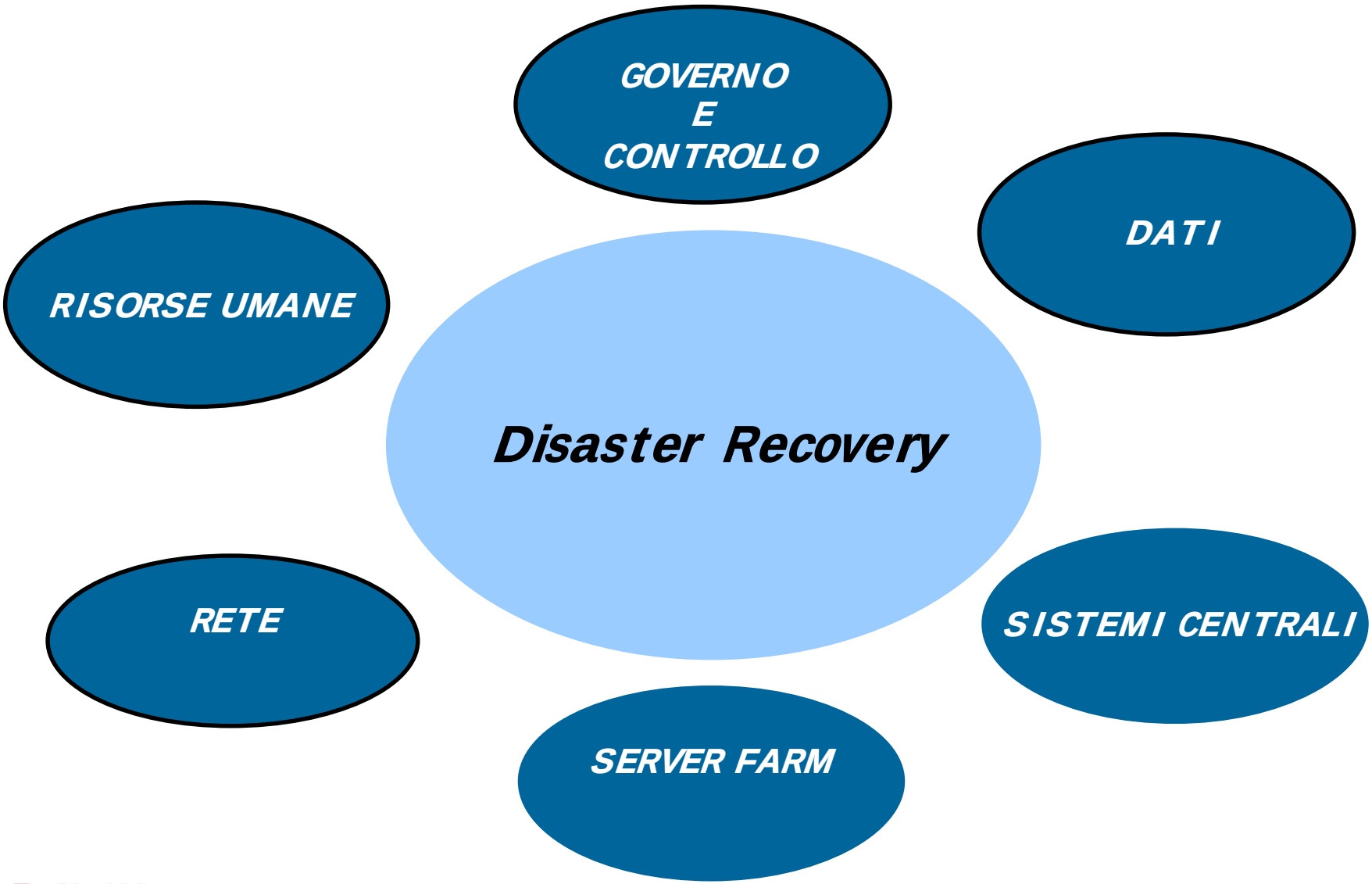
- utilizzo di un meccanismo di remotizzazione dei dati di tipo sincrono (aggiornamento in tempo reale sul sito primario e secondario) che garantisce il minimo valore di **RPO** (***Recovery Point Objective***) cioè minimizza (*teoricamente* annulla) i dati persi al momento del disastro.

RPO → 0

- un tempo di ripartenza per i sistemi IT a supporto delle applicazioni "**business critical**" e di riconfigurazione della rete tendente alle **due ore**. Questi valori, denominati **RTO** (***Recovery Time Objective***) e **NRO** (***Network Recovery Objective***), da valutare nei termini di "quanto tempo posso permettermi di restare con i processi critici "offline", sono, unitamente all'RPO, strettamente correlati con i costi connessi con la soluzione.

RTO e NRO → 2 ore

Le aree del Disaster Recovery



Piano di Disaster Recovery

- Integrazione con **Piano di Emergenza** per la Continuità Operativa dei Processi
- Valutazione rischi
- Struttura organizzativa / comitato di crisi
- Attività di ripristino per fasi e gruppi di lavoro

DATI

– Definizione e determinazione dei "***DATI VITALI***"

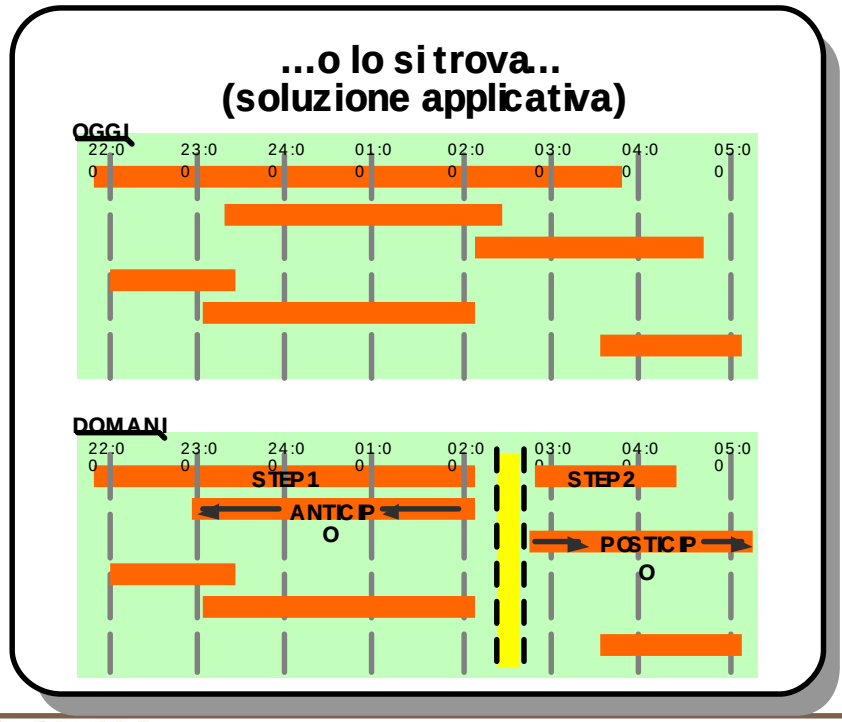
È da ritenersi *Dato Vitale* qualunque dato (archivio o applicazione) essenziale per la ripartenza dei servizi per i quali si garantisce la continuità attraverso il Disaster Recovery.

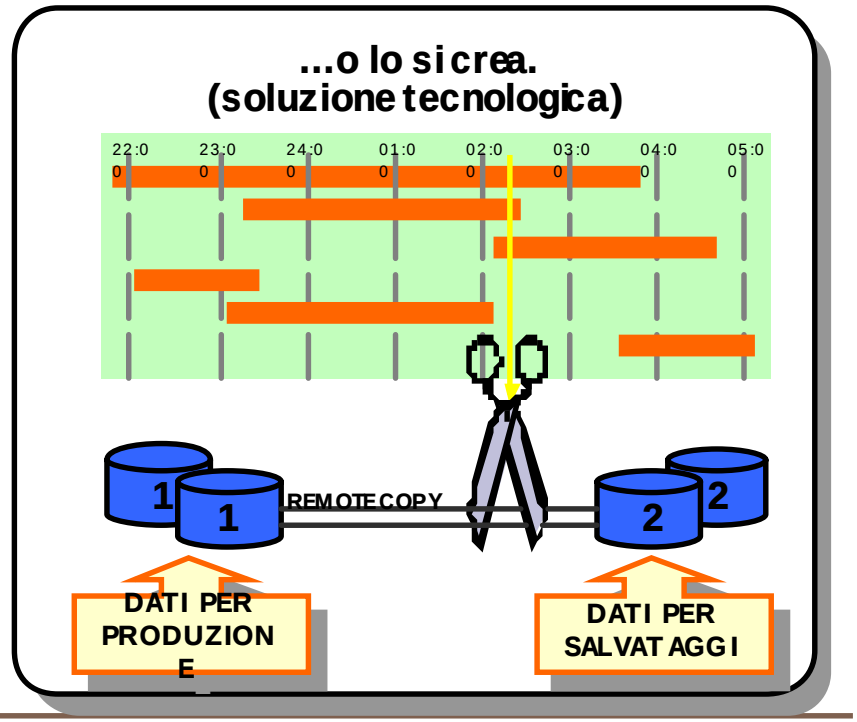
– Copia sincrona dei dati vitali (***MIRRORING***)

Si deve prevedere il mirroring di tutti i dati ritenuti vitali, secondo le modalità proprie dell'ambiente su cui risiedono (host – dipartimentale) garantendo l'ottenimento della **consistenza**.

Dati – Punto di consistenza

Il salvataggio dei dati "ideale" per disaster recovery deve essere prodotto con tutti i dati nello stesso istante, senza aggiornamenti in corso: questo momento viene chiamato convenzionalmente "PUNTO DI CONSISTENZA"
Soddisfare il "punto di consistenza" in un ambiente complesso è difficile (mole dei dati, ampiezza della "finestra" necessaria, esigenze di continuità applicativa, eterogeneità delle piattaforme) e si ricorre di conseguenza alla soluzione tecnologica….





DATI SU SISTEMI CENTRALI

- Insieme degli archivi e delle librerie sia di sistema che dei programmi applicativi
- Per la complessità dell'ambiente e l'interrelazione esistente tra i servizi/processi, si considerano come **Dati Vitali** ***la totalità dei dati di produzione***
- Per rispettare l'ipotesi di perdita di dati minima o nulla (RPO → 0), utilizzeremo per questi dati una modalità di duplicazione remota di tipo **sincrono** (PPRC).
- Si rende necessario adottare software di automazione, quale ad esempio il GDPS, che garantisca la consistenza complessiva dei dati remotizzati, permettendo in tal senso una ripartenza indolore all'atto dell'attivazione dei sistemi sul sito di recovery

DATI SU SISTEMI DIPARTIMENTALI

- Si considerano **Dati Vitali**, in questa fase del progetto, i dati (archivi e applicazioni) che si riferiscono ai servizi legati al ***TP di sportello, Internet, Intranet.***

Archivi

- Gli archivi ritenuti vitali collocati sulla SAN (Storage Area Network) aziendale e trattati alla stessa stregua dei dati centrali (utilizzo di un meccanismo di remotizzazione dei dati di tipo **sincrono**) garantendo la loro consistenza.
- Per quelli meno "critici", che sono su dischi interni (DAS) o sulla NAS, backup (snapshot) periodici FI⇔SI.

SISTEMI CENTRALI

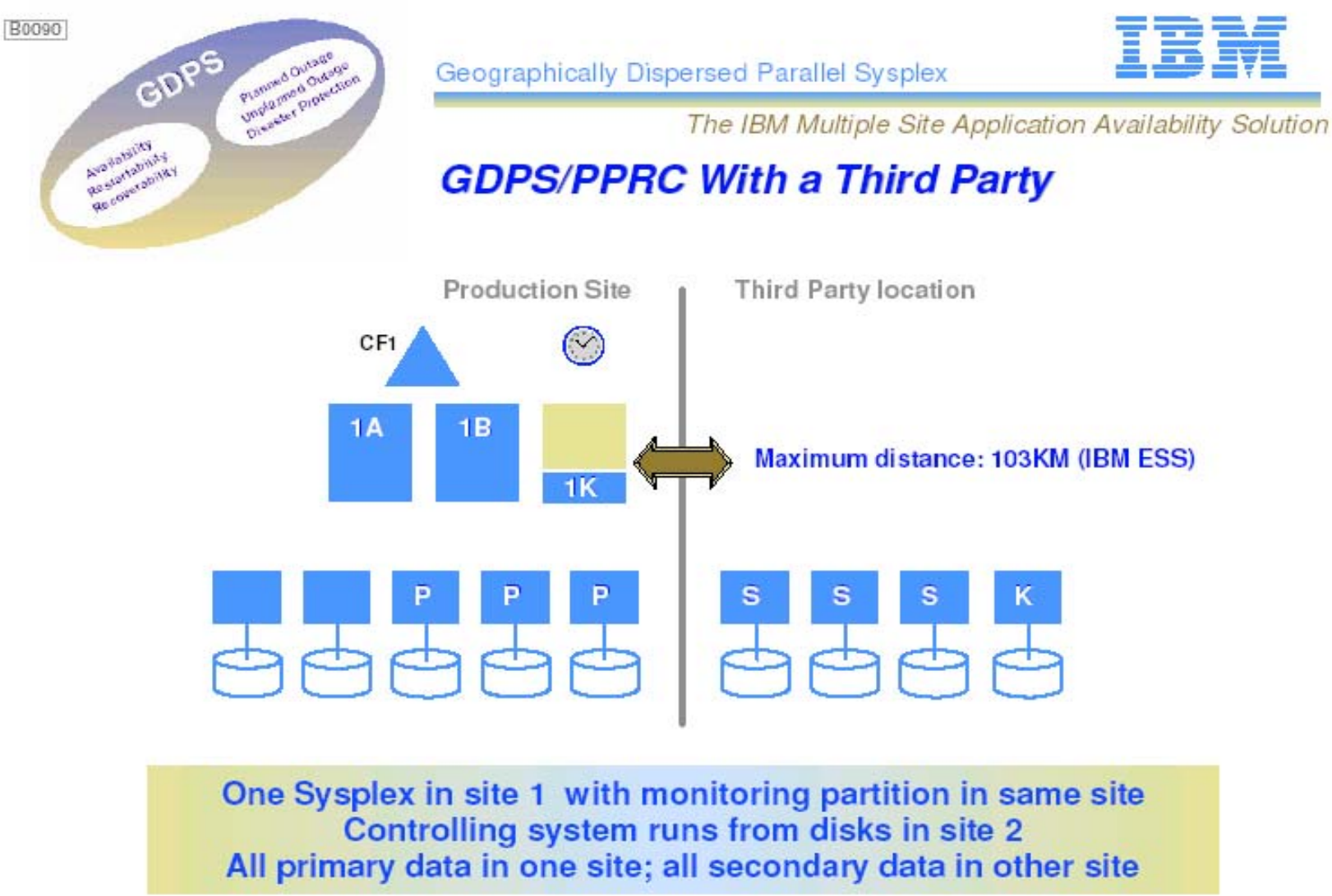
• I sistemi centrali dei due Poli dovranno prevedere le risorse infrastrutturali necessarie per la ripartenza degli ambienti elaborativi delle aziende che hanno subito l'evento catastrofico.

- ***spazio disco sul polo di recovery per la copia, in sincrono, della base dati sul polo primario***
- ***mips e memoria disponibili all'atto delle prove e del recovery effettivo***
- ***configurazioni, collegamenti a canale e altre infrastrutture già predisposti e pronti***

• Adozione, dove possibile, di soluzioni "**dormienti**", nelle quali cioè le risorse vengono rese disponibili solo nel momento del bisogno;

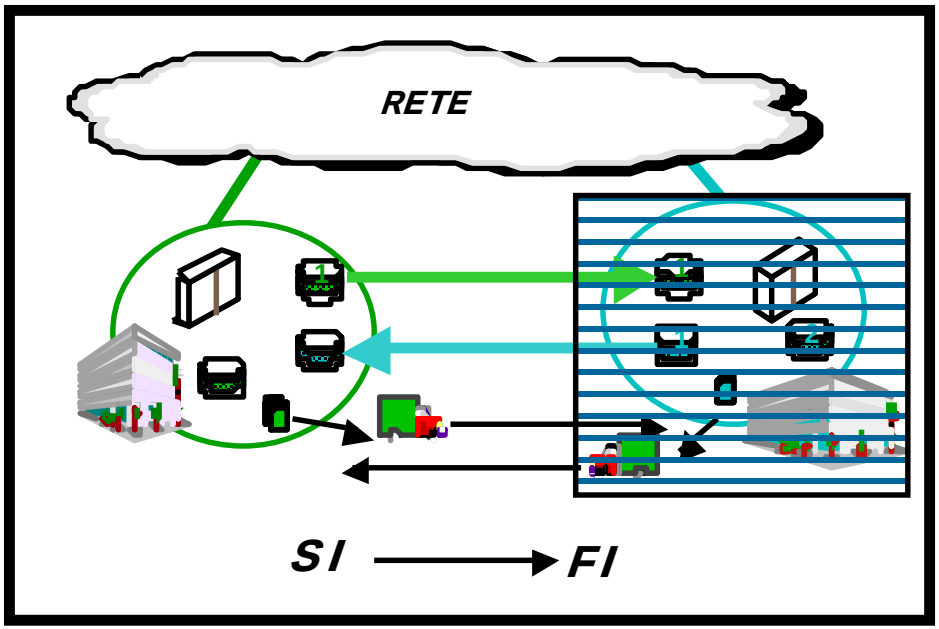
•Per evitare interferenze sul polo di recovery fra le aziende in produzione e quelle in recovery, è opportuno prevedere una "separazione" fra le risorse;

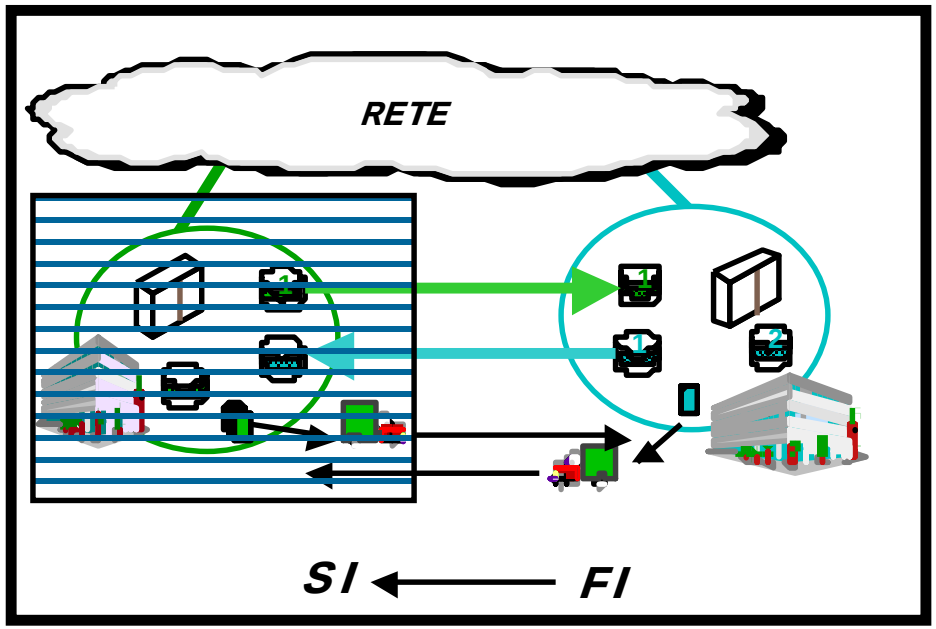
• Adozione del software di controllo e automazione (GDPS)


B0090
GDPS
Planned Outage
Unplanned Outage
Disaster Protection
Availability
Restartability
Recoverability
Geographically Dispersed Parallel Sysplex
IBM
The IBM Multiple Site Application Availability Solution
GDPS/PPRC With a Third Party
Production Site
Third Party location
CF1
1A
1B
1K
Maximum distance: 103KM (IBM ESS)
P
P
P
S
S
S
K
One Sysplex in site 1 with monitoring partition in same site
Controlling system runs from disks in site 2
All primary data in one site; all secondary data in other site

Deve essere privilegiata la **SEPARAZIONE INFRASTRUTTURALE** tra il mondo di produzione presente nei due siti come "primari" e quello caratteristico degli stessi ambienti con funzione di recovery (dormiente) come siti "secondari".

Questo al fine di minimizzare l'impatto della generazione degli ambienti recoverati all'atto del disastro sui sistemi normalmente attivi.





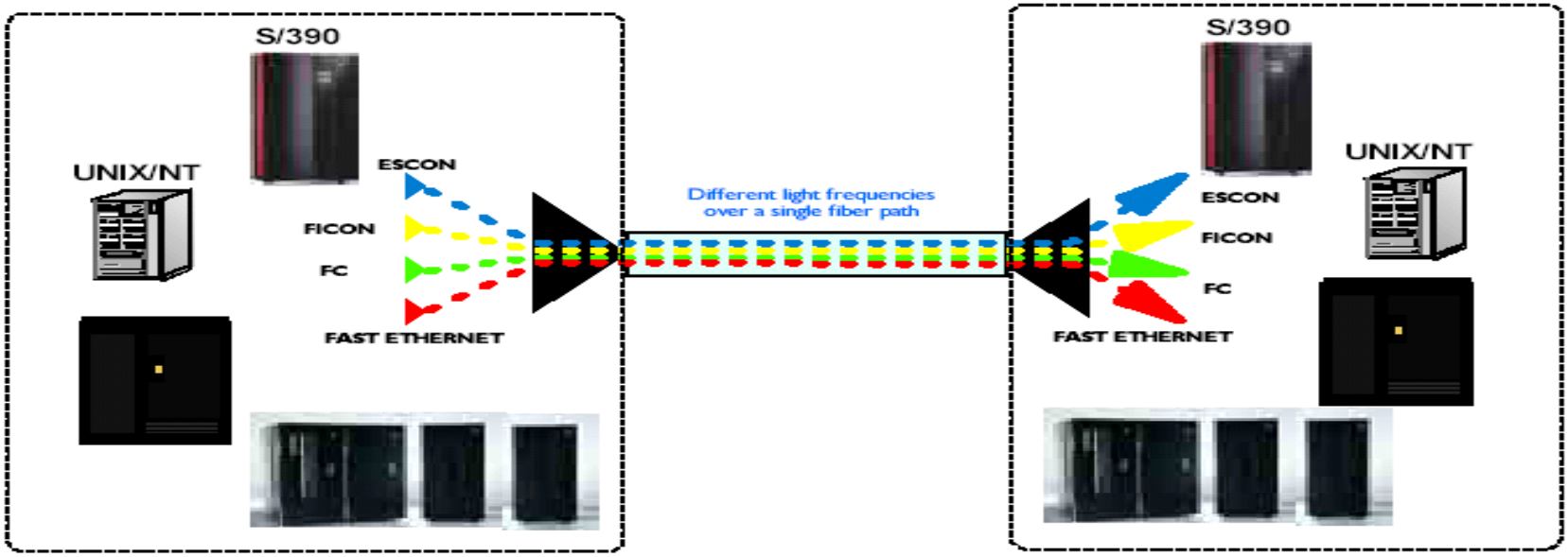
SERVER FARM

- Completamento del processo di "consolidation" su piattaforma SAN degli archivi di applicazioni vitali
- Attivazione di procedure di backup "ad hoc" per altri archivi
- Rimozione dei vincoli che legano parte della server farm dipartimentale al polo elaborativo
- Completamento della distribuzione, sui due poli, dei server applicativi

RETE

Collegamento in **fibra ottica** dedicato (dark fiber) e ridondato (anello) tra i siti di Siena e Firenze illuminato ad onde multiple tramite apparati di terminazione DWDM (Dense Wave Division Multiplexer).

Il collegamento permette di disporre di una notevole banda trasmissiva (32 lambda a 2,5 Gbps per ogni fibra) che garantisce i livelli di connettività richiesti e le prestazioni necessarie per la remotizzazione dei dati host e dipartimentali.



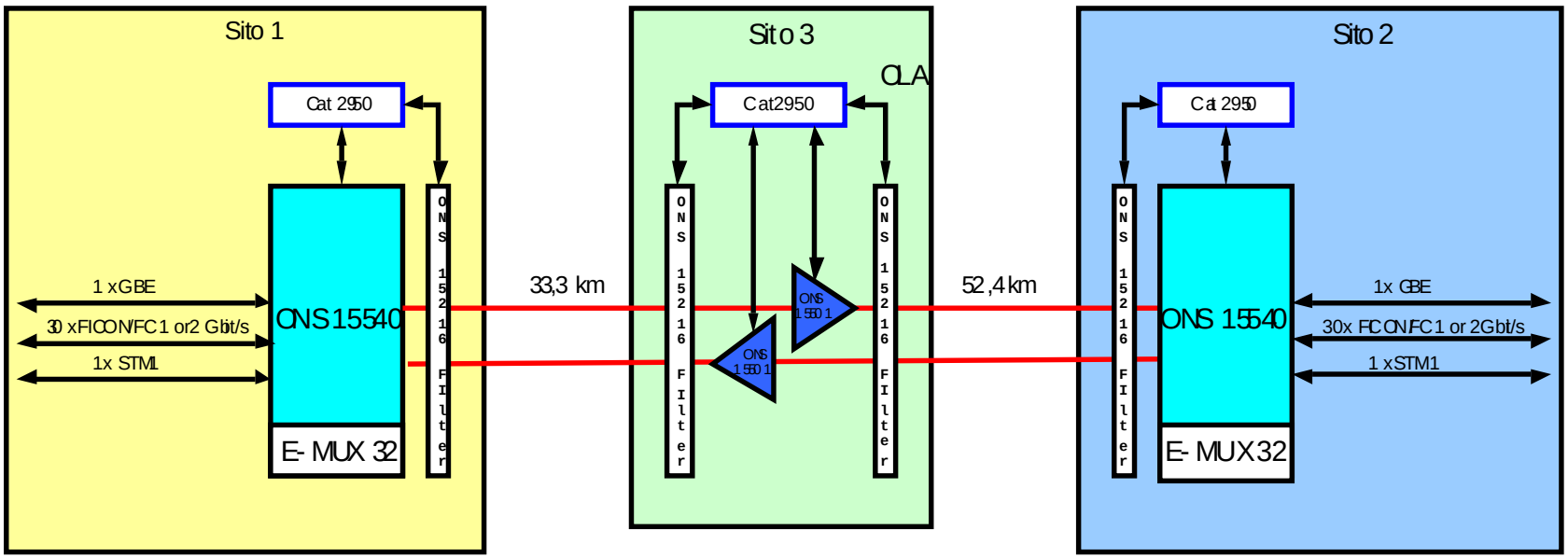
Siena – Via Ricasoli

Firenze – Via Panciatichi

Rete - Architettura Sistema Trasmissivo

- Fibra ottica monomodale ITU-T G.652
- Apparati DWDM (Dense Wavelenght Division Multiplexing) Cisco ONS 15540

- Trasporto su un'unica fibra di 32 segnali "accordati" su differenti lunghezze d'onda



RISORSE UMANE

- Disponibilità di personale tecnico su entrambi i Poli Elaborativi per sovrintendere alla normale gestione dei 2 CED (immediatamente attivabile per le attività di recovery sull'ambiente di back-up).

- Presidio sui sistemi di ogni CED, centrali e dipartimentali, tramite consolles remote (CED attivo ma non agibile).

- Personale di gestione delle elaborazioni presente su tutti i Poli del Consorzio (Siena, Firenze, Mantova, Lecce)

- Personale di Application Management e di Back Office distribuito su tutti i Poli del Consorzio

ATTIVITA' 2003 (PILOT)

- Pianificazione e coordinamento attività
- Impostazione architettura di rete (prima fibra) per mirroring dei dati SI-FI
- Acquisizione e predisposizione di risorse infrastrutturali "minime necessarie"
- Test della soluzione su un campione di dati
- Inizio predisposizione della server farm (duplicazione e ridistribuzione server, accentramento base dati)
- Impostazione Piano di Emergenza

ATTIVITA' 2004 →

- Completamento architettura di rete (seconda fibra) per mirroring bidirezionale dei dati SI-FI
- Acquisizione e predisposizione di risorse infrastrutturali necessarie al recovery completo
- Completamento architettura server farm dipartimentale in ottica di business continuity
- Consolidamento e mantenimento piano di emergenza
- Prime prove di recovery di ambienti effettivi e completi

Grazie per l'attenzione