Sistemi di assistenza da remoto per il monitoraggio e la supervisione

Federico Varotti

Scenario odierno:

Monitoraggio come parte accessoria dell’applicazione

- IP Pubblico
- Router dedicato
- Regole su Firewall

- IP Pubblico
- Router dedicato
- Regole su Firewall

Scenario futuro:

Monitoraggio come parte integrata dell’applicazione

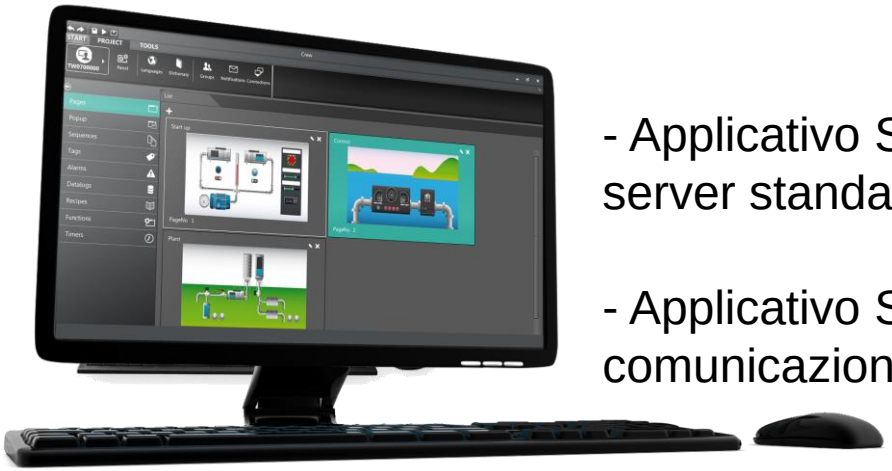
- Nessun IP Pubblico
- Nessun Router dedicato
- Nessuna Regole su Firewall

- Nessun IP Pubblico
- Nessun Router dedicato
- Nessuna Regole su Firewall

Scenario futuro come ottenerlo:

Utilizzando apparati Hw e applicativi Sw che permettano una comunicazione trasparente con il mondo esterno

LATO APPLICATIVO UFFICIO

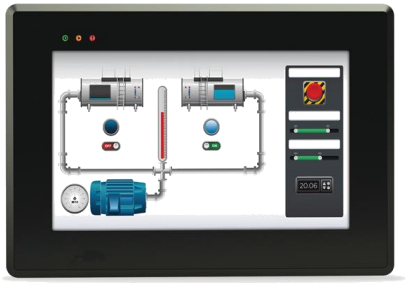


- Applicativo SCADA che esponga pagine su un web server standard

- Applicativo SCADA che utilizzi porte standard per la comunicazione con il mondo esterno

Scenario futuro come ottenerlo:

Utilizzando apparati Hw e applicativi Sw che permettano una comunicazione trasparente con il mondo esterno



LATO APPLICATIVO IMPIANTO

- Applicativo SCADA che esponga pagine su un web server standard

- Applicativo SCADA che utilizzi porte standard per la comunicazione con il mondo esterno

- Trasversalità dell'applicativo rispetto all'Hw

Scenario futuro come ottenerlo:

Utilizzando apparati Hw e applicativi Sw che permettano una comunicazione trasparente con il mondo esterno

TECNOLOGIE

-Applicativo SCADA che si appoggia a porte standard quali ad esempio 80 o 443

-Applicativi basati su HTML5

-Applicativi in grado di funzionare su architetture diverse (Pc e Embedded)

Scenario futuro come ottenerlo:

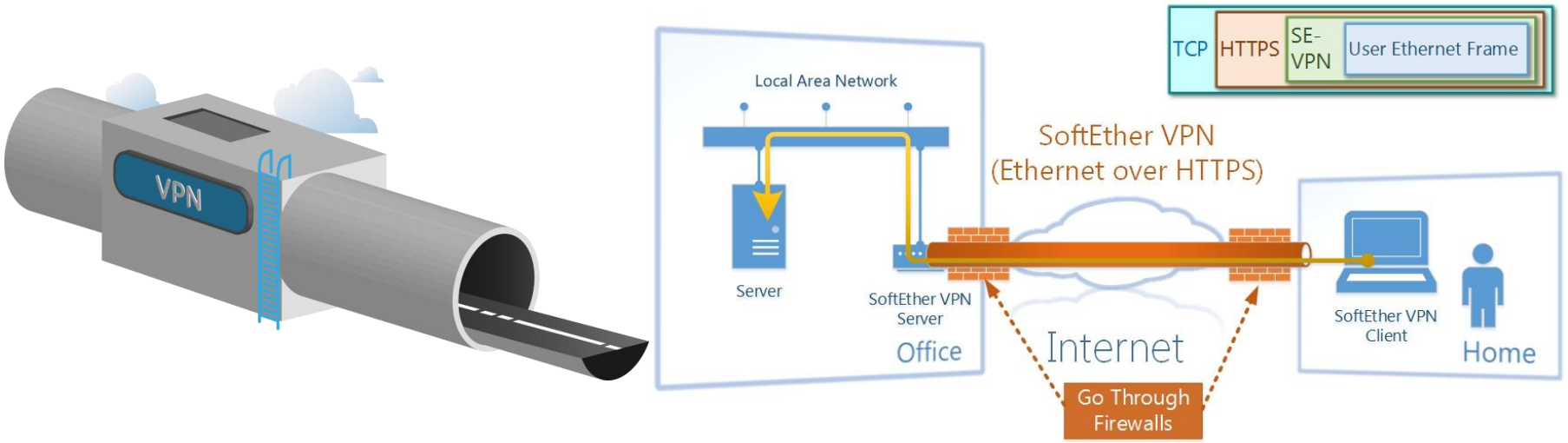
L’interconnessione dei sistemi implica l’esposizione ad attacchi informatici quali:

-Furti d’identità
-Furti di dati sensibili
-Attacchi portati attraverso Trojan o Malware

Scenario futuro come ottenerlo:

Rendere sicure le interconnessioni

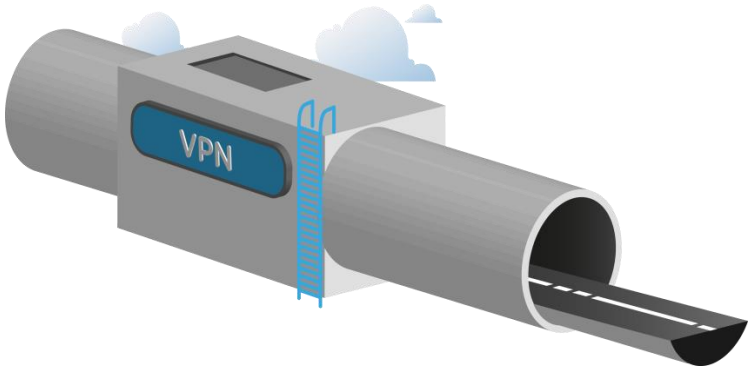
-Utilizzando connessioni VPN over HTPP su porta 80 o over HTTPS su porta 443

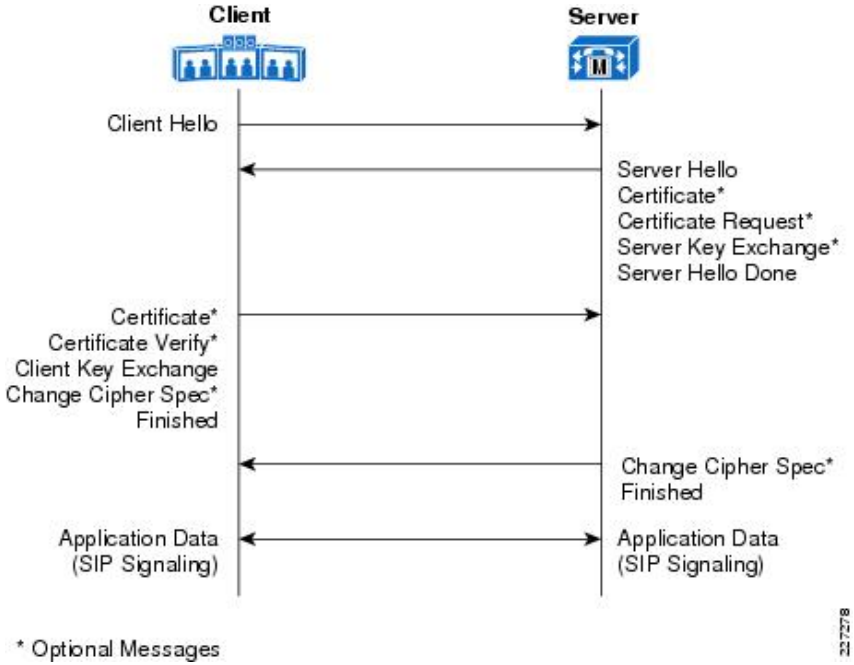


Scenario futuro come ottenerlo:

Rendere sicure le interconnessioni utilizzando indirizzi IP privati per le connessioni

-VPN over HTTP/HTTPS crittografata basata su protocollo TLS





Scenario futuro come ottenerlo:

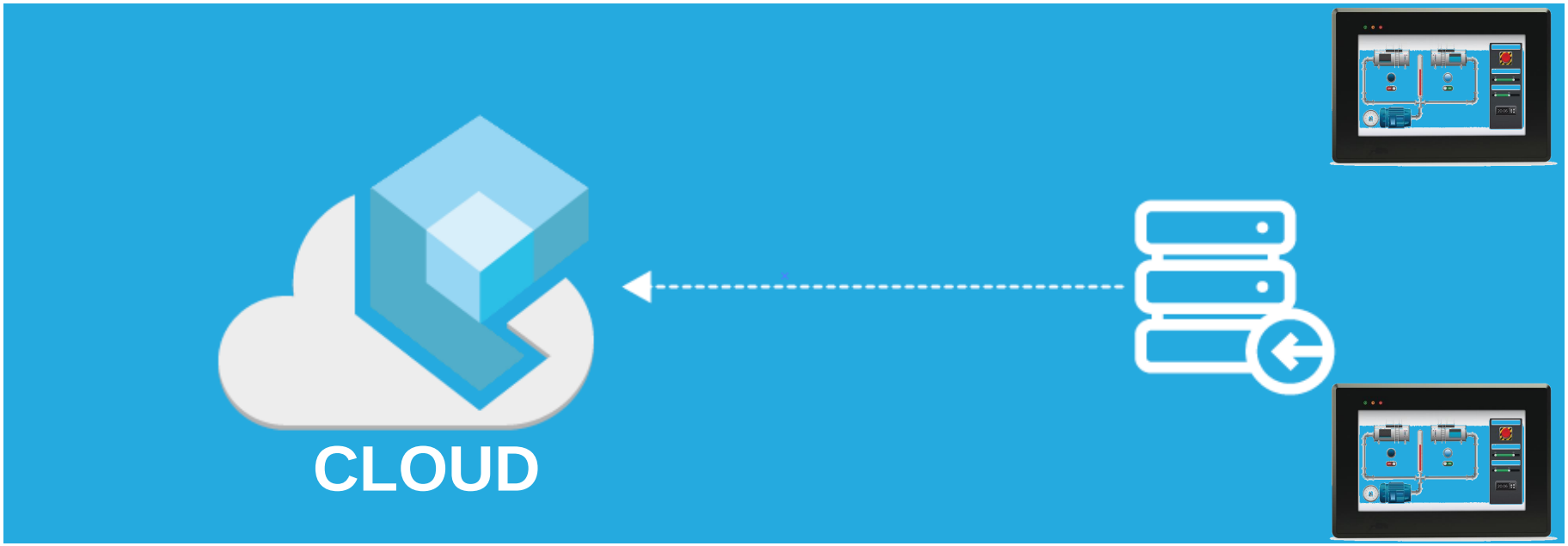
Rendere sicure le interconnessioni

-Accesso alla infrastruttura attraverso l’uso di Username e Password con policy restrittive

Scenario futuro come ottenerlo:

Dove ospitare i Dati e le Applicazioni

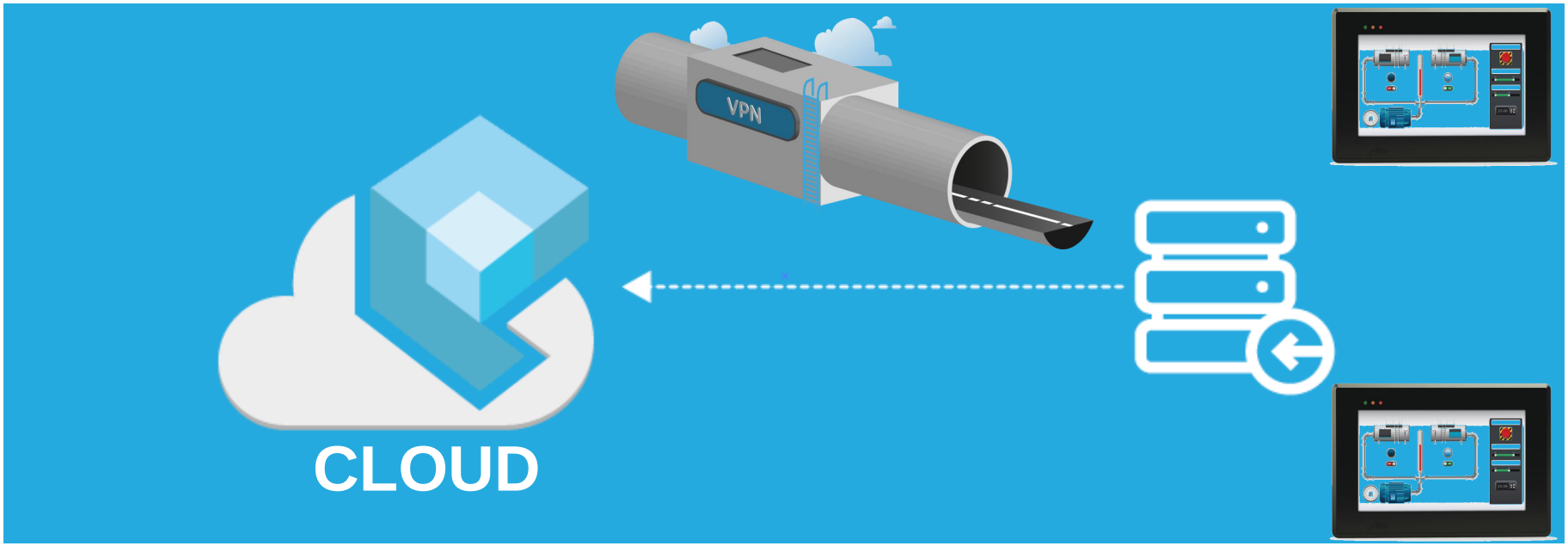
- Utilizzo di una infrastruttura Cloud Standard che ospiti Applicazioni e Dati



Scenario futuro come ottenerlo:

Sicurezza delle connessioni

- Le applicazioni dovranno essere raggiunte attraverso una connessione VPN sicura e crittografata



Scenario futuro come ottenerlo:

Condivisione dei Dati

-L’utente sceglie quali dati raccolti condividere in Cloud, avendo anche la possibilità di mantenere dati localmente.

Scenario futuro come ottenerlo:

Condivisione dei Dati

-Aggiornamento in tempo reale dei dati provenienti dagli apparati installati (Big Data)

Scenario futuro come ottenerlo:

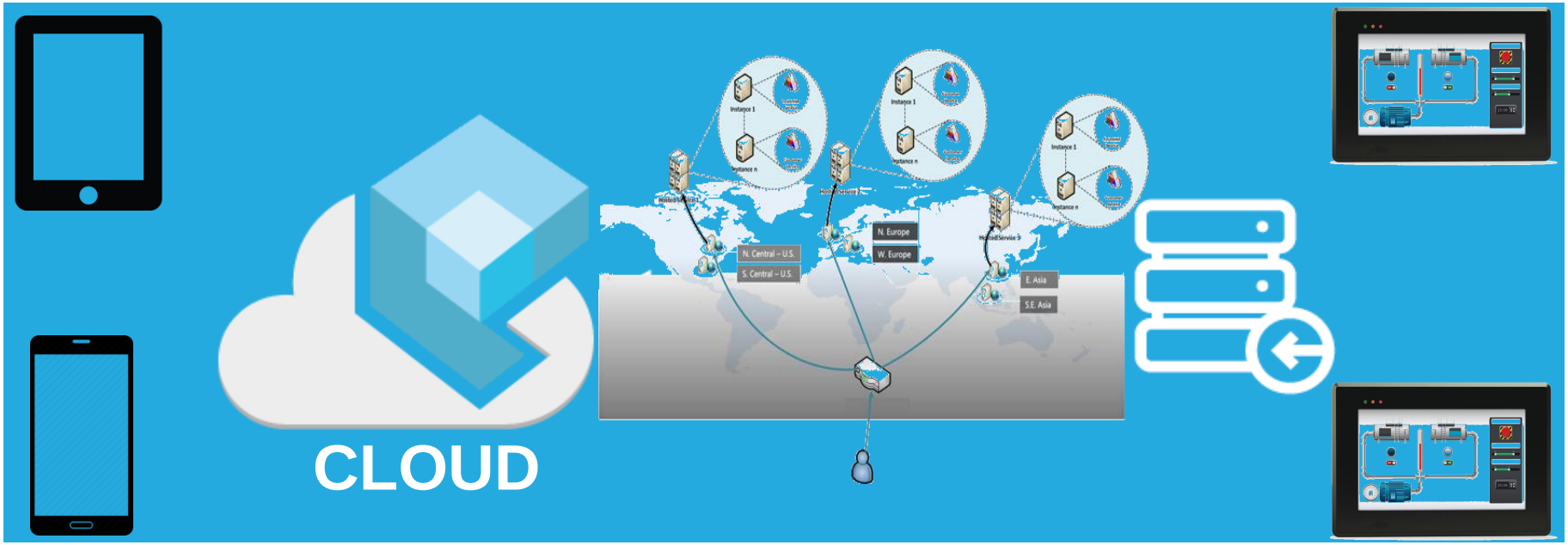
Sicurezza del salvataggio dei Dati

- Ridondanza geografica dei Server

Scenario futuro come ottenerlo:

Velocità delle comunicazioni

- Geolocalizzazione delle connessioni



Scenario futuro come ottenerlo:

Utilizzo di tecnologia standard e Cross-Platform per la parte grafica

Scenario futuro:

Architettura di fabbrica interconnessa

Grazie per l’attenzione