EVOLUZIONE DI UN SISTEMA DI TELECONTROLLO CON PARTICOLARE ATTENZIONE ALLA VULNERABILITÀ E SICUREZZA INFORMATICA DEI SISTEMI SCADA CONNESSI ALLA RETE INTERNET:

L'ACQUEDOTTO MONTESCURO OVEST

1 PREMESSA

La memoria si inserisce nell'ambito della gestione ottimizzata delle risorse idriche attraverso un utilizzo "intelligente" del telecontrollo. Nell'esperienza proposta il sistema di telecontrollo è inquadrato in un contesto olistico costituito da: strumentazione, attuatori di campo, sistemi di supervisione e controllo e strumenti software evoluti di analisi di flussi informativi.

A tal proposito negli ultimi anni la lunga fase di start-up degli Ambiti Territoriali Ottimali ed il conseguente notevole aumento in termini di complessità e dimensioni della gestione, ha portato i soggetti gestori ad investire gran parte delle proprie risorse nel miglioramento del livello di conoscenza dei sistemi idrici gestiti. Tale fase è stata altresì accompagnata dallo sviluppo e/o dal potenziamento di sistemi software (Sistemi Informativi Territoriali SIT/GIS, Supervisory Control And Data Acquisition System SCADA, Sistemi di Supporto alle Decisioni DSS) in grado di gestire le informazioni raccolte durante le fasi di miglioramento della conoscenza degli impianti e delle reti, consentendo di rendere fruibili tali informazioni alle diverse strutture operative distribuite sul territorio. Questi singoli sistemi, essendo progettati e strutturati per la gestione di determinate informazioni, risultano indispensabili per la gestione operativa ma insufficienti ai fini del controllo strategico se non utilizzati in maniera connessa e coordinata.

L'incremento dell'impiego di tali sistemi e della loro interconnessione, e la loro fruibilità dall'esterno (accessibilità WEB) ha aumentato di molto la vulnerabilità dei sistemi informatici, attirando le attenzioni di possibili pirati informatici, con possibili gravi conseguenze sul corretto funzionamento complessivo del sistema idrico e sugli utenti serviti.

Occorre quindi porre particolare attenzione all'aspetto concernente la "sicurezza informatica" al fine di prevenire, intervenire o ripristinare i sistemi informatici da eventuali attacchi informatici.
In quest'ottica è stato realizzato il progetto del "Sistema di telecontrollo dell'Acquedotto Montescuro Ovest" per conto di Siciliacque S.p.A.

2 DAL DATO ALLA CONOSCENZA: L'EVOLUZIONE DEI SISTEMI DI TELECONTROLLO

Un sistema di supervisione e controllo consente tipicamente di acquisire una serie di grandezze caratteristiche del funzionamento del sistema, di impartire comandi e segnalare allarmi. In particolare i moderni impianti di telecontrollo non possono prescindere dal contributo che può fornire la tecnologia d'automazione per assicurare gli standard richiesti di efficienza e di affidabilità, nel rispetto dei vincoli normativi e di servizio.

Nel presente progetto si è andati oltre tali requisiti di base, in ogni caso implementati allo stato dell'arte ed attivi in misura massiccia nel sistema dell'Acquedotto Montescuro Ovest, è infatti stata realizzata una infrastruttura tecnologica in grado di utilizzare tali informazioni, unitamente ad altri domini di dati, per generare una base di conoscenza in grado di tradurre tali input in corrispondenti azioni finalizzate all'ottimizzazione della gestione e dei processi produttivi, obiettivo generale di ogni sistema evoluto.

È stata utilizzata una piattaforma di applicazioni commerciali software (SCADA in primo luogo ma anche, GIS, DSS, …), componenti specificamente progettati per rappresentare il processo di distribuzione idropotabile.

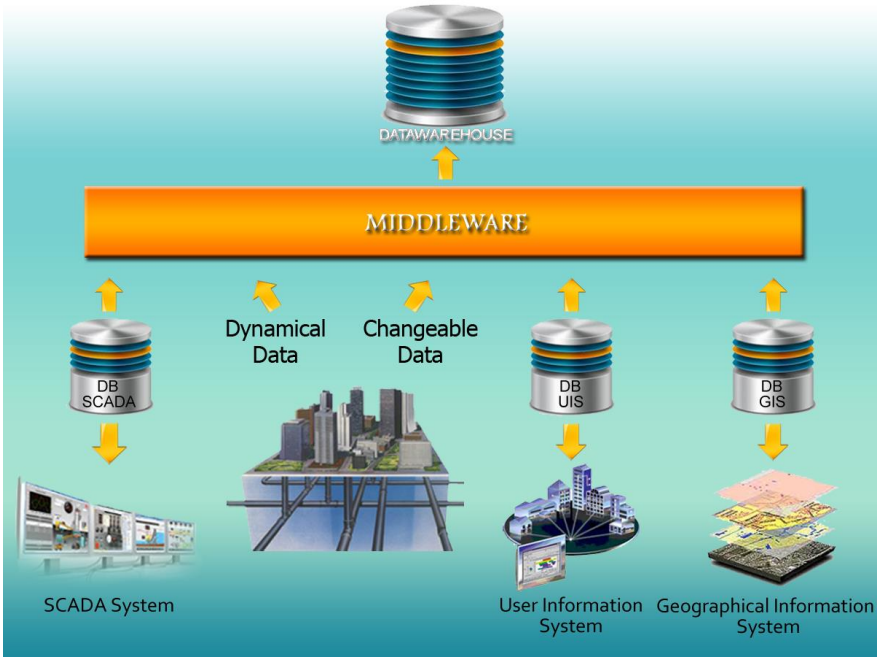
Autori: Giuseppe Modica (Proxima S.r.l.), Giuseppe Mario Patti, Salvatore Santagati (Proteo Control Technologies S.r.l.)

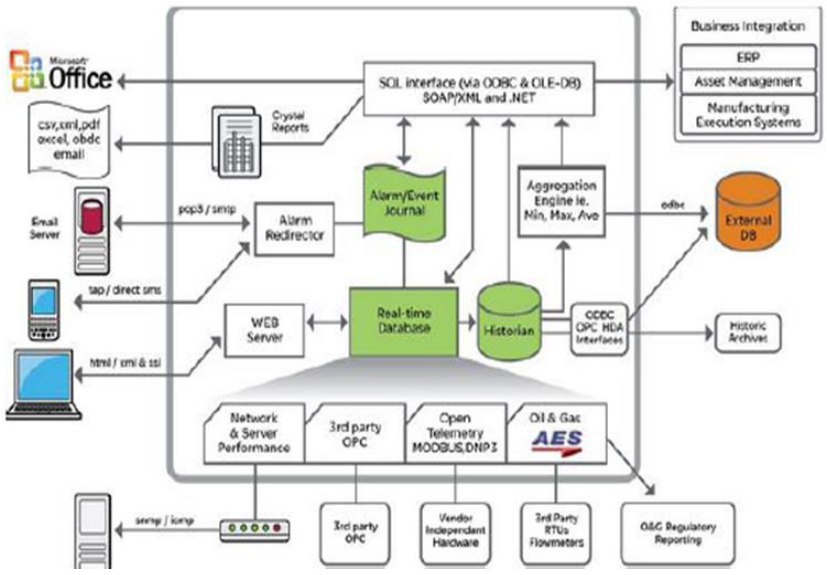
Con un tale approccio tutti i componenti e gli applicativi del sistema sono cooperanti e utilizzano banche dati centralizzate, a cui tutti gli utenti possono avere accesso, per l'elaborazione dei dati e delle informazioni di interesse. Alla piattaforma informativa e operativa SCADA si integrano i flussi informativi provenienti dal GIS, dal sistema DSS.

Tale tipo di integrazione dati, comporta uno scambio di informazioni e più genericamente uno scambio di interazioni con reparti aziendali non legati strettamente al telecontrollo, con un incremento delle potenziali vulnerabilità sulla sicurezza, per via dell'esistenza di punti di accesso ed interazione prima inesistenti.

Per eliminare tali vulnerabilità e consentire all'utilizzatore di fruire ugualmente dei servizi evoluti che il nuovo sistema offre, sono state adottate una serie di accorgimenti che saranno meglio esplicitati in seguito.

L'integrazione delle basi di conoscenza del sistema in oggetto è di seguito rappresentata:





3 Il SISTEMA DI TELECONTROLLO DELL'ACQUEDOTTO MONTESCURO OVEST

Il progetto, realizzato nel 2014 ed ancora in corso di evoluzione, ha previsto l'implementazione di un sistema di supervisione e controllo di significative dimensioni, distribuito su un territorio esteso e variegato, caratterizzato dall'utilizzo di molteplici supporti trasmissivi (Ponti Radio, rete GPRS/UMTS, altro) e dalla presenza di un'architettura strutturata con centralizzazione dei dati .

Il sistema di Telecontrollo dell'acquedotto Montescuro Ovest si estende su un territorio molto vasto e montuoso nella Sicilia Occidentale e controlla, per mezzo di un sistema trasmissivo dei dati basato su radio digitali, circa 90 impianti tra cui:

- Serbatoi
- Centrali di pompaggio
- Nodi idrici lungolinea (partitori, camere di manovra e punti di misura)
- Centraline di Protezione Catodica

Il progetto è stato realizzato secondo criteri di flessibilità e modularità così da consentire di adattare e modificare il sistema, secondo l'evoluzione delle esigenze del gestore, salvaguardando le apparecchiature esistenti e permettendo di inserire in rete nuove unità di controllo, nuovi segnali relativi a nuove strumentazioni e/o nuove apparecchiature o inserire il sistema in una rete di supervisione ancora più complessa.

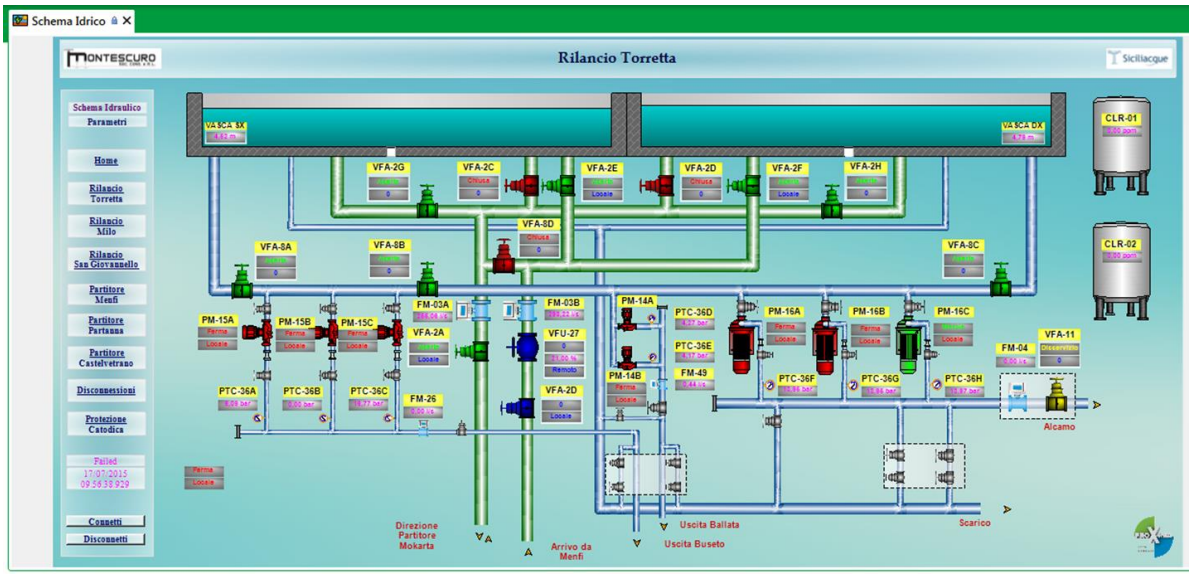
L'architettura adottata consente di impiegare al meglio ogni unità del sistema, in particolare scaricando l'elaboratore centrale dai compiti di automazione locale per dedicarlo esclusivamente alla supervisione dell'impianto ed all'elaborazione e gestione delle informazioni.

La struttura è gerarchica con un unico centro strategico direzionale per l'intero ambito, strutturata come di seguito indicato:

- Livello 2 Centro di Supervisione Direzionale (Sede di Santa Ninfa)
- Livello 1 Unità periferiche in campo (PLC/RTU/PC)
- Livello 0 Strumentazione elettronica di misura e apparecchiature elettromeccaniche esistenti in campo

La struttura gerarchica per livelli del sistema di controllo è intrinsecamente fault-tolerant perché le logiche relative al corretto funzionamento degli impianti sono codificate nei livelli più bassi della gerarchia degli elementi di supervisione. E' responsabilità dei livelli più alti di supervisione il coordinamento dei sottosistemi idrici affinché la gestione complessiva risulti ottimale.

Nel caso in cui un evento accidentale renda impossibile la comunicazione tra il centro di controllo e la periferia e quindi non sia possibile coordinare le attività dei sottosistemi idrici e dei singoli impianti, comunque i livelli inferiori del sistema di controllo ne assicureranno il corretto funzionamento e la messa in sicurezza a scapito esclusivamente del rendimento complessivo.



4 LA SICUREZZA NEI SISTEMI DI TELECONTROLLO

Nella nuova era dei Cyber Attacchi, ci sono numerosi motivi per cui i sistemi di telecontrollo (SCADA, PLC e altre apparecchiature) delle Public Utilities possano risultare di interesse per gruppi terroristici, organizzazioni criminali o anche semplicemente giovani in cerca di notorietà nell'ambiente degli Hacker.



L'approccio è finalizzato al conseguimento del prelievo, del trasporto e della distribuzione di un grande sistema acquedottistico a livello regionale gestito da Siciliacque S.p.A., ponendo particolare attenzione agli aspetti legati alla sicurezza, riducendo al minimo le probabilità di essere soggetti ad un attacco informatico che possa permettere l'accesso ai dati e soprattutto impedire l'interazione con gli organi di manovra presenti in campo, in modo che non vi siano disagi, limitazioni o danni ai gestori del sistema e agli utilizzatori abituali della risorsa.

Sin dai tempi degli assiri, gli acquedotti sono stati oggetto di attacco biologico, negli anni recenti a questi si sono affiancati i Cyber-Attacks:

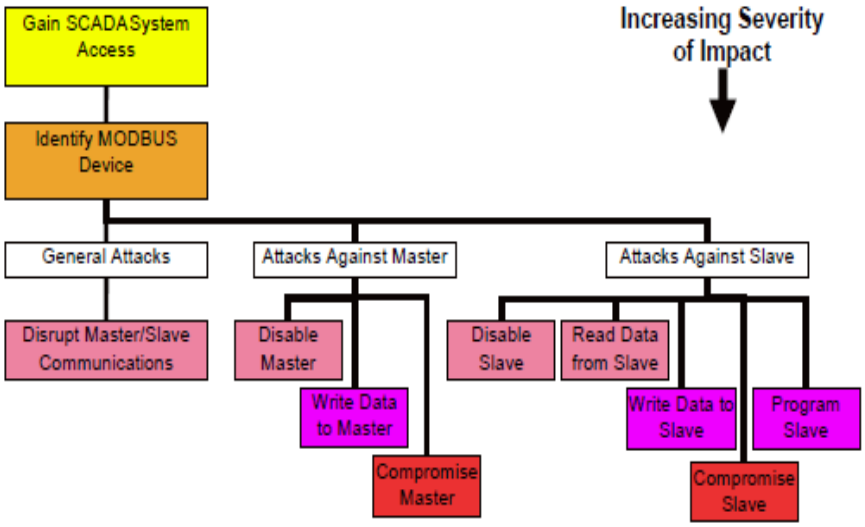
- 1994 – Salt River Project water dept., Arizona
- 2000 – Maroochy Water System, Australia
- 2006 – Harrisburg, PA water treatment plant
- 2007 – Tehema Colusa Canal Authority, California
- 2004 - 2009 – Gli attacchi informatici nei sistemi idrici hanno avuto un incremento del 300%, cosi come riportato dal RISI (Repository of Industrial Security Incidents)
- 2010 – Diffusione di Stuxnet, primo worm ad attaccare direttamente i PLC industriali.

I problemi non riguardano esclusivamente il settore dell'acqua, ma qualunque tipo di sistema che sia connesso e dipendente da un sistema di telecontrollo.

I potenziali effetti di un attacco informatico ai danni di un sistema SCADA possono così essere riassunti:

- Interferire con le operazioni
- Effettuare delle modifiche non autorizzate alle logiche dei programmi
- Cancellare o modificare dati
- Inviare false informazioni
- Cambiare le soglie di allarme

- Comandare organi di manovra
- Agire sugli organi dosatori per alterare la quantità di sostanze immesse per la disinfezione dell'acqua
- Ecc.



Per lungo tempo i sistemi SCADA sono rimasti nascosti all'interno della rete aziendale, dando ai gestori una sensazione di «sicurezza» ed inaccessibilità alle risorse, se non dall'interno. Tuttavia, gli SCADA moderni, si sono evoluti verso soluzioni standardizzate a basso costo e di facile manutenzione ed accessibilità, comportando una diffusione su larga scala di conoscenze sui sistemi SCADA e della sua importanza in termini di potenziale, incrementando in questo modo l'interesse dei malintenzionati, diminuendo la segretezza e sicurezza degli stessi.

I principali fattori che hanno contribuito ad un aumento della vulnerabilità dei sistemi di telecontrollo sono:

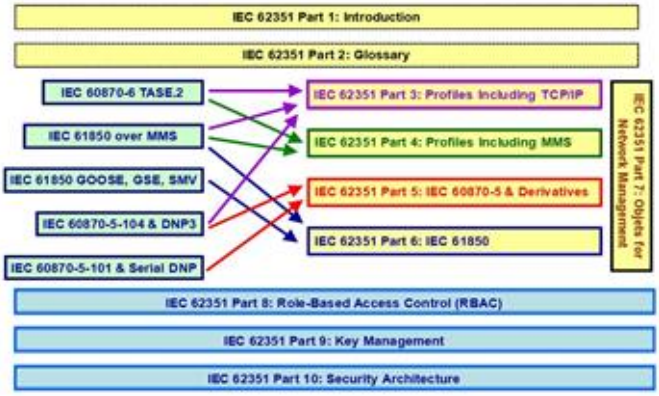
- L'interconnessione delle reti di telecomunicazioni
    - Le utility del settore, si ritrovano spesso a gestire la convergenza della rete informatica interna, centralizzando le diverse aree aziendali su un'unica rete. Se non vengono adottate le opportune precauzioni di sicurezza su tutte le sottoreti che la compongono, il risultato è un potenziale punto di accesso, dove malintenzionati possono agire per attaccare il sistema di telecontrollo.
- Le modalità di accesso remoto ai sistemi
    - Punti di accesso come, router, modem e moduli wireless, sono utilizzati per la diagnostica, la manutenzione e la verifica dello stato del sistema, da remoto. Se i dati non sono opportunamente criptati e se non viene utilizzato un dovuto meccanismo di autenticazione, l'integrità delle informazioni trasmesse sono altamente vulnerabili.
- La standardizzazione delle tecnologie
    - Le organizzazioni hanno sempre più la tendenza ad utilizzare sistemi e tecnologie standardizzate, questo comporta notevoli benefici in termini economici e di espandibilità, per contro il risultato di questo processo è l'incremento delle persone che abbiano il potenziale di conoscenza e strumenti necessari ad effettuare attacchi, incrementando la percentuale di rischio.
- La disponibilità di reperire informazioni tecniche
    - Le specifiche tecniche sui sistemi adottati, sono spesso facilmente reperibili su internet, agevolando il compito di eventuali hacker.

Un aspetto fondamentale della sicurezza in ub sistema d telecontrollo, sono i protocolli di comunicazione in quanto rappresentano il mezzo con cui le informazioni vengono recuperate dalle apparecchiature in campo e allo stesso tempo l'invio di comandi di controllo.

I protocolli utilizzati sono stati per lungo tempo «proprietari», adottando l'approccio "Security By Oscurity", oggi la tendenza è cambiata e la quasi totalità dei nuovi impianti è orientata ad adoperare protocolli «Aperti» e «Standard».
Il rovescio della medaglia è dato dall'ampia documentazione disponibile e di conseguenza una maggiore probabilità di attacco informatico.
Il protocollo di comunicazione che nello specifico si è scelto di adottare è il «DNP3 Secure Authentication» basato sullo standard IEC62351, uno dei pochi standard aperti disponibile per le comunicazioni SCADA, che soddisfi i principali requisiti di sicurezza.

Tra i vari obiettivi di sicurezza che lo standard ricerca, troviamo:

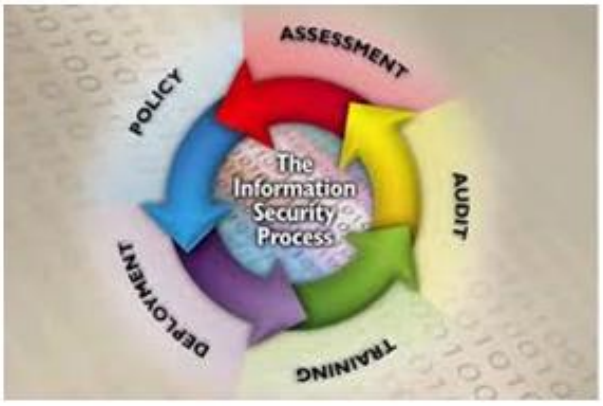
- L'autenticazione del processo di trasferimento di dati tramite firma digitale
- La garanzia di accessi esclusivamente dopo autenticazione
- La garanzia della confidenzialità dei dati trasmessi tramite la prevenzione dell'eavesdropping, ossia la possibilità che le comunicazioni vengano intercettate
- La prevenzione di attacchi di spoofing (intromissione nella rete sostituendo una degli elementi della rete)
- Criptaggio dei dati (al fine di nascondere il contenuto dei messaggi a chi dovesse intercettare le comunicazioni senza avere la chiave di cifratura)



Altro strumento molto utile per il ripristino a seguito di un attacco è mantenere una copia di backup del progetto nella Server-Farm del realizzatore dell siIstema ed in Cloud, al fine di sopperire ad eventuali blocchi del sistema del cliente, (dovute non solo a cyber attacchi, ma anche a eventuali situazioni di Disaster Event) o in alternativa da utilizzare per un confronto in caso di sospetto relativamente ai dati percepiti.

Nel futuro prossimo, per sopperire alle possibili carenze tecniche dei clienti che non sempre sono dotati di un propria organizzazione per la manutenzione delle reti interne, la tendenza sarà sempre più di realizzare sistemi di telecontrollo allocando le risorse necessarie su sistemi Cloud, al fine di demandare gli aspetti legati alla sicurezza del centro di controllo ad aziende fornitrici di tali piattaforme che adottano tecniche di sicurezza e di Disaster Recovery più evolute di quanto si possa trovare in un gestore di servizi di piccole-medie dimensioni, eliminando inoltre, le componenti di rischio di attacco dall'interno che risultano le più pericolose, in quanto il malintenzionato dispone di un punto di accesso fisico al sistema, agevolandosi di molto nelle possibilità di riuscita di un attacco.

Ovviamente alle misure sopra citate, vanno comunque affiancati i metodi classici di protezione di una rete di telecomunicazioni (firewall, antivirus, policy, etc etc) che tuttavia da soli non sono più sufficienti a garantire adeguata protezione.



Tali protezioni sono comunque necessarie al fine di prevenire gli attacchi di base quali:

- **Denial of Service:** Occupare le risorse (una rete intranet o un Web server) con migliaia di false richieste al fine di mandare in crash il sistema o di rendere la risorsa inutilizzabile al cliente.
- **Spyware:** per monitorare le attività dell'utilizzatore della macchina.
- **Trojan Horse:** programmi o file dannosi che si camuffano da programmi regolari per infettare i computer.
- **Virus:** Attacca i programmi esistenti per diffondersi anche su altri computer
- **Worm:** File infetto che replica se stesso al fine di infettare tutti i computer della rete
- **Sniffer:** Effettua il monitoraggio della rete per sottrarre dati sensibili trasmessi
- **Key Loggers:** Registra e trasmette ciò che viene digitato sulla tastiera dall'utente, anche in questo caso per poter sottrarre dati sensibili, quali: password, numeri di carta di credito, informazioni, altro.
- **Phishing:** Finti siti web o E-mail per sottrarre dati sensibili agli ignari utilizzatori.

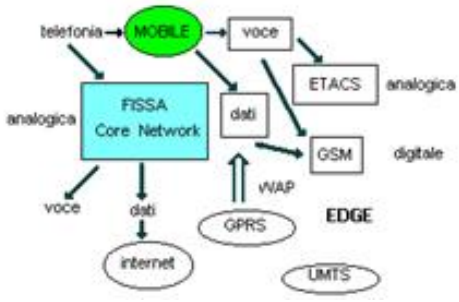
Le linee guida per contrastare il genere di attacchi sopra elencato, possono essere cosi riassunte:

- Limitare il più possibile il numero di persone autorizzate ad accedere fisicamente ai nodi cruciali della rete.
- Aggiornare regolarmente tutti i software, in quanto le case produttrici rilasciano periodicamente delle nuove Patch di sicurezza, proprio per essere aggiornati con le nuove tecniche adottate dagli hacker.
- Utilizzare delle password secondo gli standard di sicurezza, quindi che contengano maiuscole, minuscole, numeri e caratteri speciali ove possibile.
- Istruire il personale sulle policy aziendali, relative ai software da installare o se possibile evitare che personale non qualificato possa avere le autorizzazioni per installare e/o modificare programmi.
- Installare software Antivirus, AntiSpyware, AntiMalware che oltre a rilevare eventuali software dannosi, possano offrire anche una protezione real-time.
- Introdurre dei firewall oltre che di tipo software anche di tipo hardware
- Separare la rete interna per aree di interesse isolando i reparti che non hanno necessità di essere connessi tra di loro, come ad esempio potrebbe essere il reparto amministrativo con il reparto di Telecontrollo.

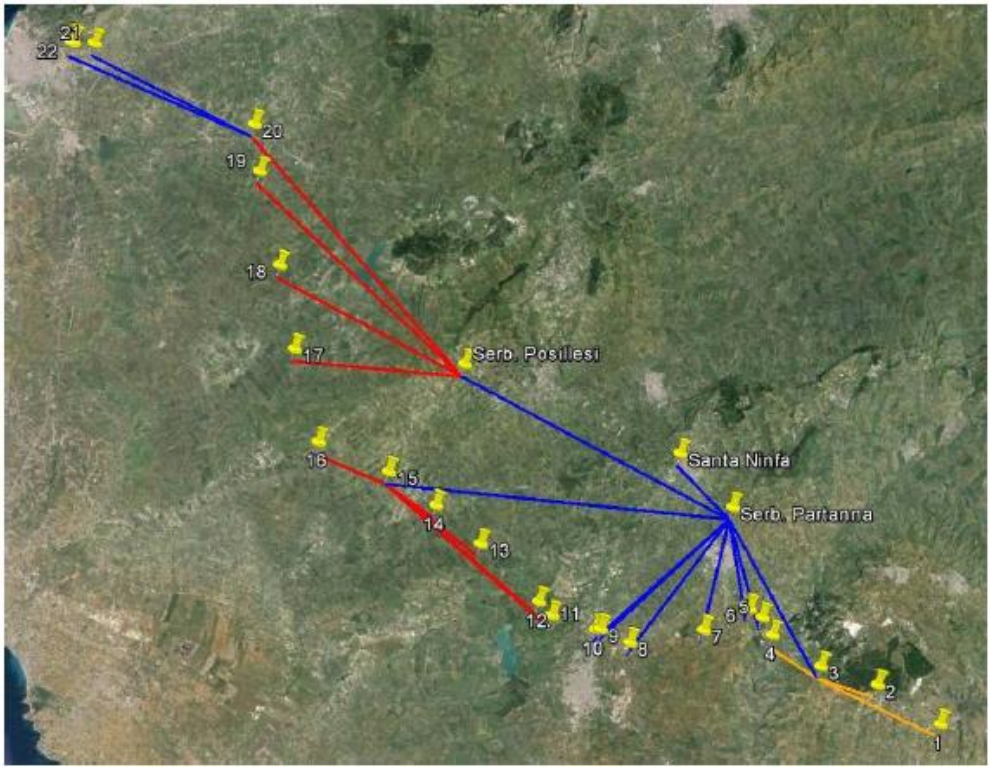
TRASMISSIONE DATI

La scelta del supporto di trasmissione da utilizzare ha tenuto conto di vincoli tecnici, geografici ed economici. In particolare partendo dal presupposto di garantire la sicurezza di trasmissione dei dati, sono state considerate le distanze reciproche tra gli impianti, la presenza di stazioni isolate o di difficile accesso, la possibilità di installazione delle linee telefoniche, i costi dei dispositivi di trasmissione (modem, etc...), i costi di installazione dei collegamenti, i costi di esercizio e l'utilizzo di mezzi trasmissivi già esistenti.

Come detto uno dei principali fattori che hanno contribuito ad un aumento della vulnerabilità è l'interconnessione delle reti di telecomunicazioni.
Spesso si tende ad adoperare soluzioni economiche quali il GPRS o il GSM, tuttavia ciò espone le periferiche di controllo ad una maggiore esposizione di rischio.



Per tale motivo si è scelto di adottare un sistema di comunicazione basato su sistema Radio Digitale, operante su frequenze licenziate, avente sistemi di criptazione dei dati a 256Bit ed altre funzionalità per la gestione tramite accesso remoto sicuro.

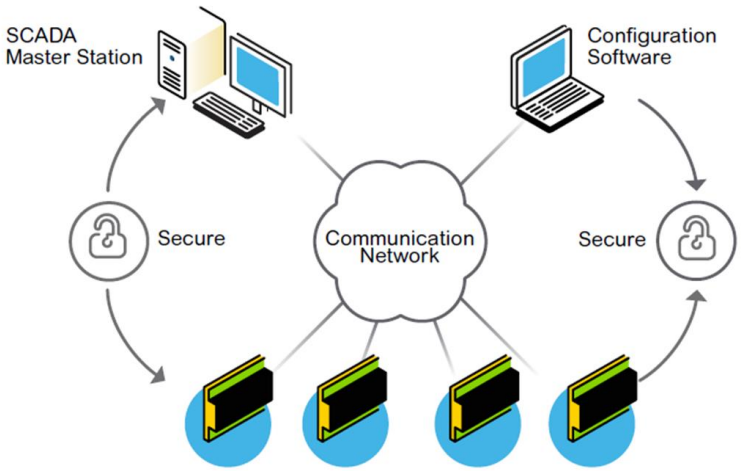


Operando su frequenze licenziate, si elimina la possibilità di disservizi legati ad interferenze e si possono adottare protocolli di comunicazione proprietari, garantendo capacità di affidabilità enormemente superiori rispetto ai sistemi in banda libera o collettiva.

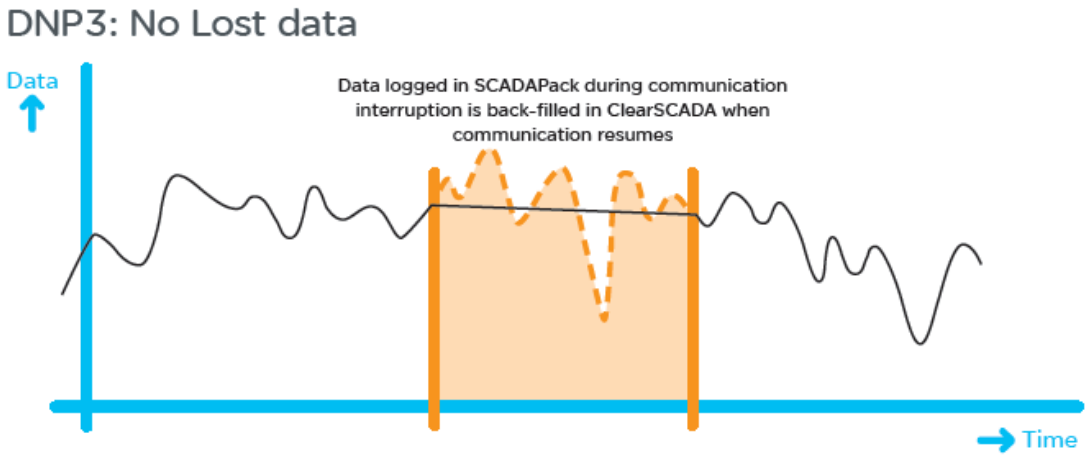
Il sistema implementato permette la criptazione dei dati trasmessi ed immagazzinati e possiede sistemi di autenticazione, basati sui più elevati standard di sicurezza internazionale quali:

- IEE6189 (AGA12)
- IEC62351

I dati originali, vengono combinati con una chiave di sicurezza per criptare il messaggio, rendendo illeggibile la comunicazione a chiunque non possegga la chiave originale. Le misure di sicurezza relative all'autenticazione, risolvono i problemi su possibili attacchi che possano modificare il controllo e/o la configurazione del sistema, attraverso la sequenza Richiesta-Contesa-Risposta.



Inoltre il protocollo di comunicazione DNP3, oltre a possedere i requisiti di sicurezza già citati, possiede altre importanti qualità di affidabilità e robustezza, consentendo di recuperare i dati anche in caso di temporanea assenza di comunicazione.



5 CONCLUSIONI

- I Sistemi di distribuzione idrica sono un potenziale obiettivo strategico.
- Numerosi soggetti hanno le potenzialità e le risorse per effettuare attacchi informatici.
- Molti sistemi SCADA presentano numerose vulnerabilità.
- I sistemi SCADA sono connessi ad internet e ciò li rende potenzialmente attaccabili da qualunque parte del mondo.
- Un attacco ad un Sistema SCADA che sovrintenda ad un sistema idrico, può alterare la qualità dell'acqua, modificare dei processi di esercizio, inviare false informazioni ed anche provocare danni meccanici che possono creare disservizi più o meno lunghi, creando danni economici, funzionali e sulla salute delle persone.

Occorre quindi:

- Non trascurare l'aspetto sicurezza nella realizzazione dei sistemi di telecontrollo.
- Utilizzare SCADA che posseggano le più moderne tecnologie di criptaggio ed autenticazione.
- Porre attenzione ad ogni singolo componente del sistema di telecontrollo (mezzi trasmissivi, protocolli, accessibilità remota, etc) in quanto ognuno di essi, può rappresentare una Backdoor di accesso per potenziali attacchi informatici.
- Effettuare periodicamente procedure di Penetration-Test, aggiornate alle nuove minacce.
- Istruire correttamente il personale utilizzatore della risorsa.
- Preparare piani di emergenza per il recupero delle informazioni e per il ripristino delle normali attività.

Il sistema realizzato dimostra come sia possibile integrare con successo molteplici tecnologie convergenti in un unico sistema integrato di telegestione applicato per un sistema acquedottistico di grandi dimensioni.

Allo stesso tempo sono state adottate diverse politiche per garantire al sistema robustezza nella ricezione del dato e sicurezza globale di non accesso alle informazioni o ai comandi da parte di persone non autorizzate, il tutto senza limitare le funzionalità richieste oggi da un sistema di Telecontrollo moderno.

Inoltre si è mostrato come, specialmente per le aziende medio-piccole, sia più conveniente demandare la questione sicurezza del proprio centro di controllo a soluzioni con piattaforme di tipo Cloud, eliminando i rischi da attacco interno e quelli legati alle competenze dei tecnici di manutenzione della rete che non sempre hanno gli skill necessari per proteggere un sistema di telecontrollo.

Nel caso specifico del progetto di Telecontrollo di Montescuro Ovest per Siciliacque S.p.A., non si è reso necessario agire sugli aspetti generali di "Sicurezza delle reti informatiche aziendali" né tanto meno ricorrere ad una soluzione CLOUD, in quanto in quanto l'azienza di alto profilo tecnologico, è dotata di un CED (Centro Elaborazione Dati) che coordina e mantiene le apparecchiature ed i servizi ovvero l'infrastruttura IT dell'azienda assicurando la sicurezza dei sistemi gestiti.

Gli aspetti sui quali si è agito, per limare il più possibile i rischi di attacchi informatici, sono quelli legati strettamente alla filiera del telecontrollo, quindi:

- Mezzo Trasmissivo
- Protocolli di Comunicazione
- Autenticazione Avanzata
- Backup & Disaster Recovery