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

L'ACQUEDOTTO MONTESCURO OVEST

G. M. Patti - G. Modica - S. Santagati
Proteo Control Technologies S.r.l.

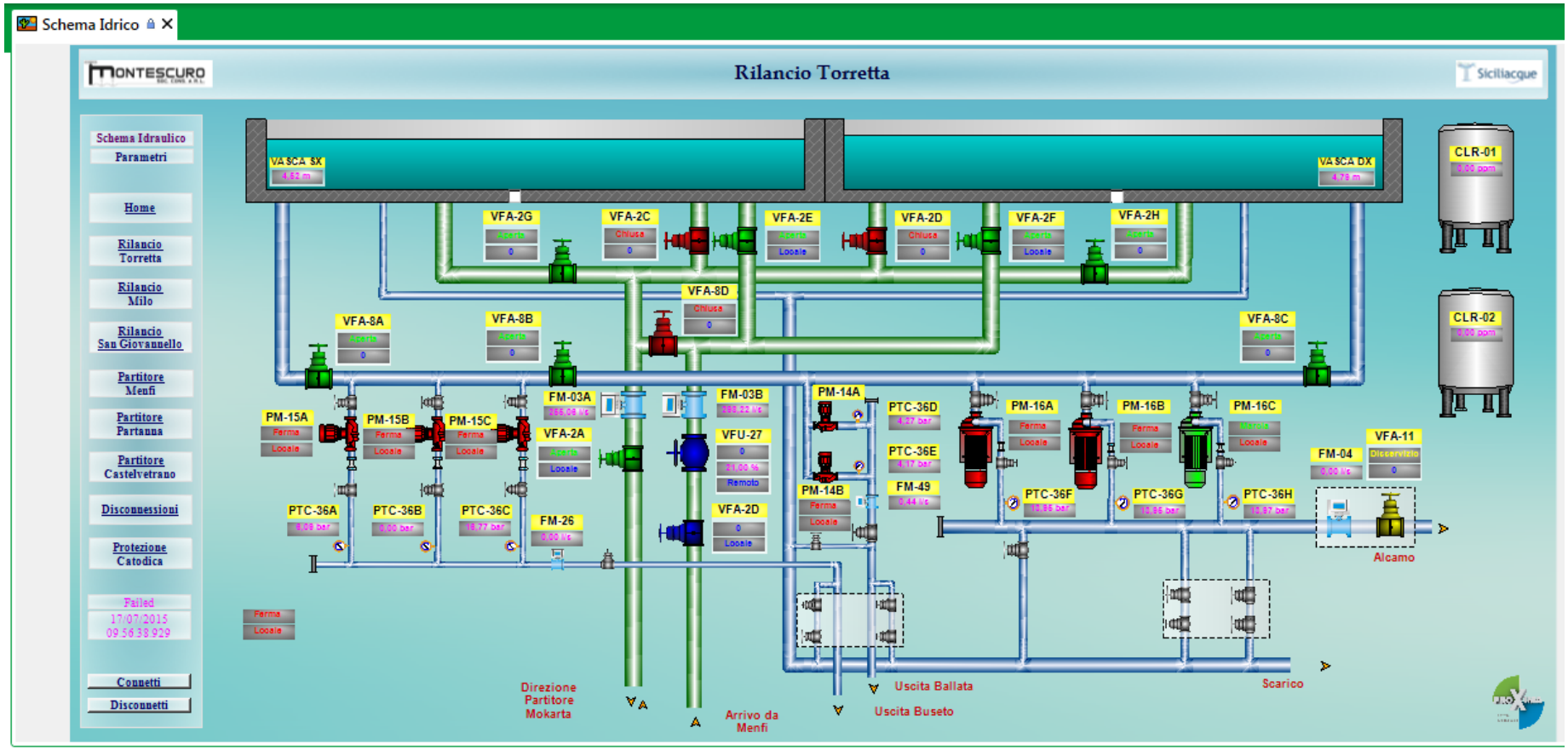
L'ACQUEDOTTO MONTESCURO OVEST

Il progetto, realizzato nel 2014 ed ancora in corso di evoluzione, ha previsto l'implementazione di un sistema di supervisione e controllo di dimensioni significative, realizzato secondo criteri di flessibilità e modularità, ponendo l'attenzione sugli aspetti relativi alla sicurezza.

Il progetto del 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:

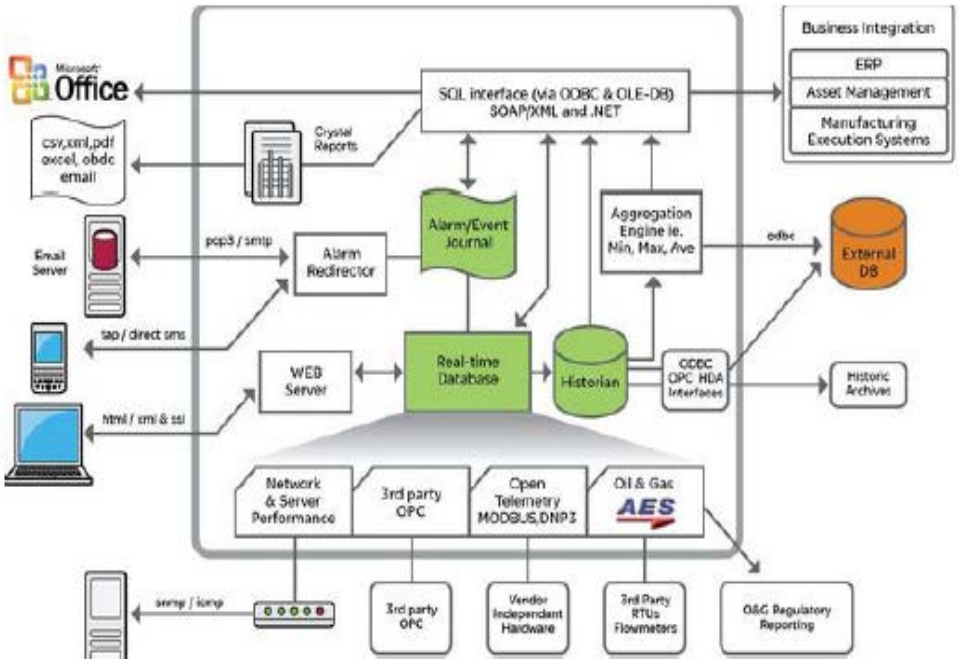
- Serbatoi
- Centrali di pompaggio
- Nodi idrici (partitori, camere di manovra e punti di misura)
- Centraline di Protezione Catodica

IL SISTEMA DI TELECONTROLLO DELL'ACQUEDOTTO MONTESCURO OVEST



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

É stata realizzata una infrastruttura tecnologica in grado di utilizzare informazioni che di norma un sistema di telecontrollo mette a disposizione, 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 che rappresenta l'obiettivo generale di ogni sistema evoluto.



SICUREZZA: I CYBER ATTACK

Nella nuova era dei Cyber Attack, 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, 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, senza che vi possano essere disagi o limitazioni ai gestori del sistema e agli utilizzatori abituali della risorsa.

LA SICUREZZA NEI SISTEMI ACQUEDOTTISTICI
I Precedenti

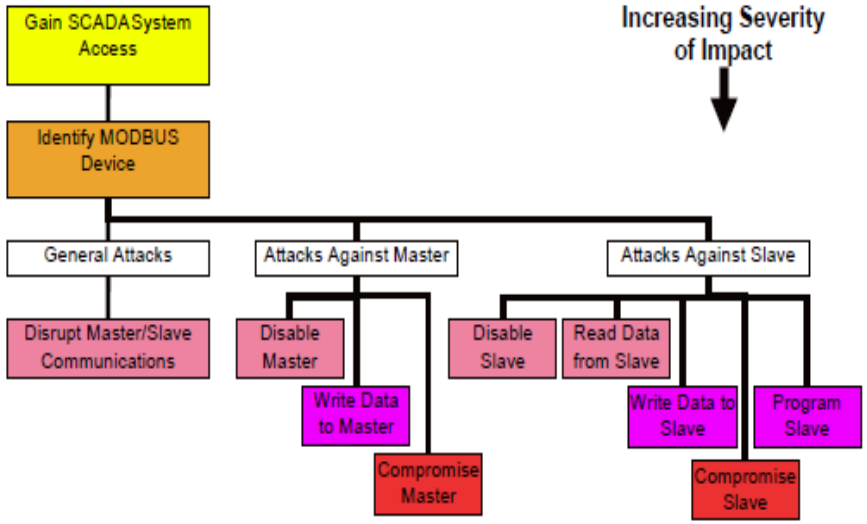
Sin dai tempi degli assiri, gli acquedotti sono stati oggetto di attacco biologico, negli anni recenti a questi si sono affiancati i Cyber-Attacks:

- 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.

LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Possibili Effetti

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 su organi dosatori per alterare la quantità di sostanze immesse per la disinfezione dell'acqua
- Ecc.



LA SICUREZZA NEI SISTEMI DI TELECONTROLLO

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. In tal modo si è aumentato sia l'interesse dei pirati informatici, sia le vulnerabilità del sistema.

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

- L'interconnessione delle reti di telecomunicazioni
- Le modalità di accesso remoto ai sistemi
- La standardizzazione delle tecnologie
- La disponibilità di reperire informazioni tecniche

LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Protocolli di Comunicazione

I Protocolli di comunicazione sono una delle parti più critiche per la sicurezza ed il funzionamento di un sistema di Telecontrollo, 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 sono stati per lungo tempo «proprietari», oggi la tendenza è cambiata e si tende sempre più ad adoperare protocolli «Aperti» e «Standard».

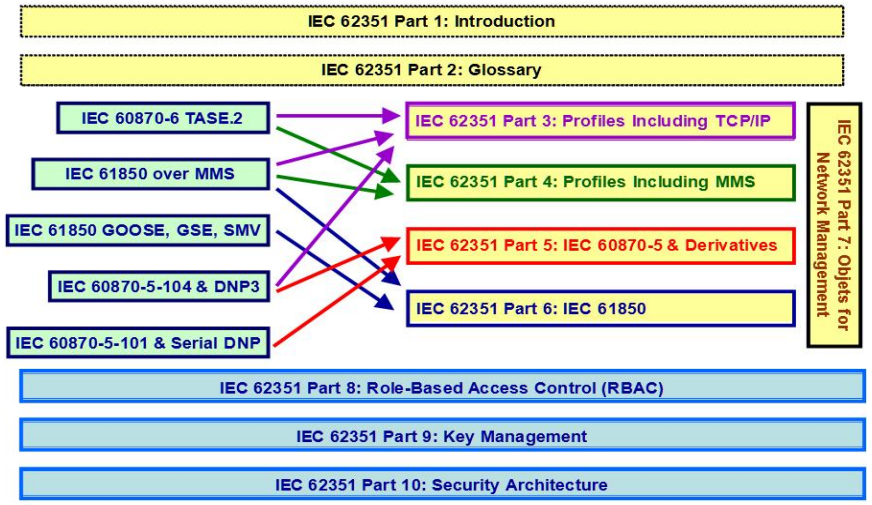
Il rovescio della medaglia è dato dall'ampia documentazione disponibile e di conseguenza una maggiore probabilità di attacco informatico.

LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Misure Adottate

Nello specifico si è scelto di adottare 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.

Tale protocollo assicura altissima protezione tramite:

- Criptaggio dei dati
- Autenticazione avanzata



LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Misure Adottate

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.

LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Misure Adottate

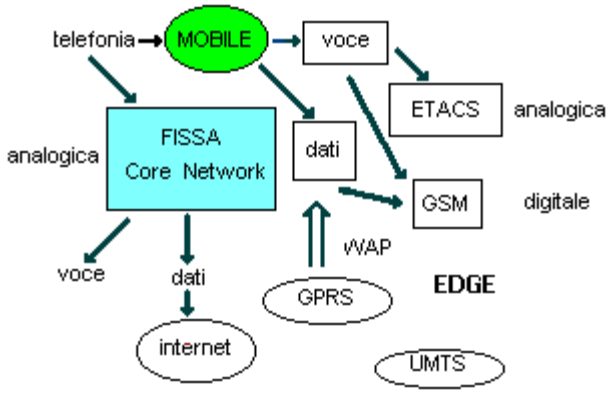
Altro strumento utile è stato creare una copia di backup del progetto da tenere nella nostra Server-Farm o in Cloud, al fine di sopperire ad eventuali blocchi del sistema del cliente o in alternativa da utilizzare per un confronto in caso di dubbi relativi ai dati percepiti.

LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Misure Adottate

Nel futuro prossimo, per le aziende medio-piccole non dotate di un CED o di un amministratore di rete, 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 dei sistemi di telecontrollo ad aziende che adottano tecniche di sicurezza e di Disaster Recovery più evolute ed aggiornate, 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.

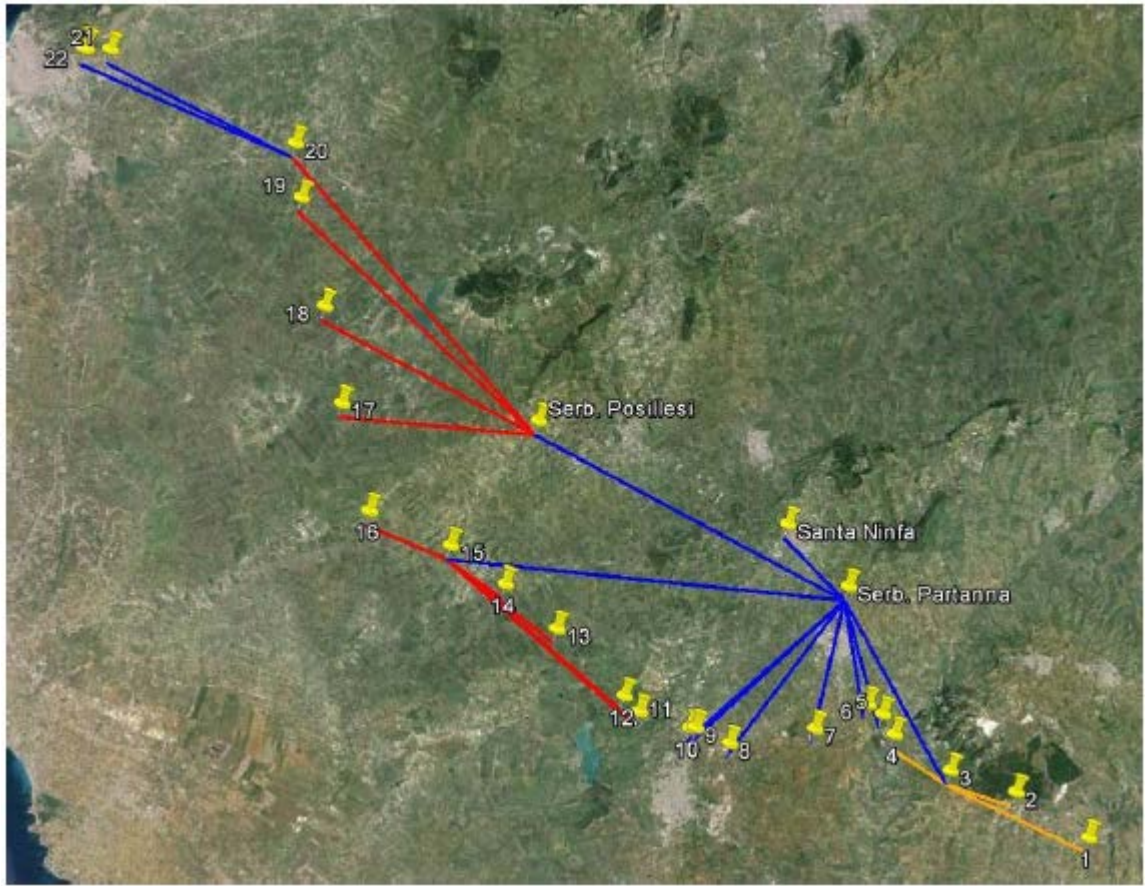
LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Misure Adottate

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.



LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Misure Adottate

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.

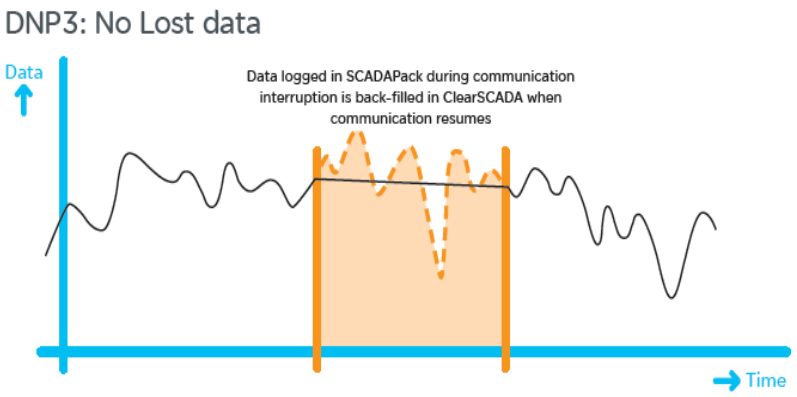


LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Misure Adottate

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:

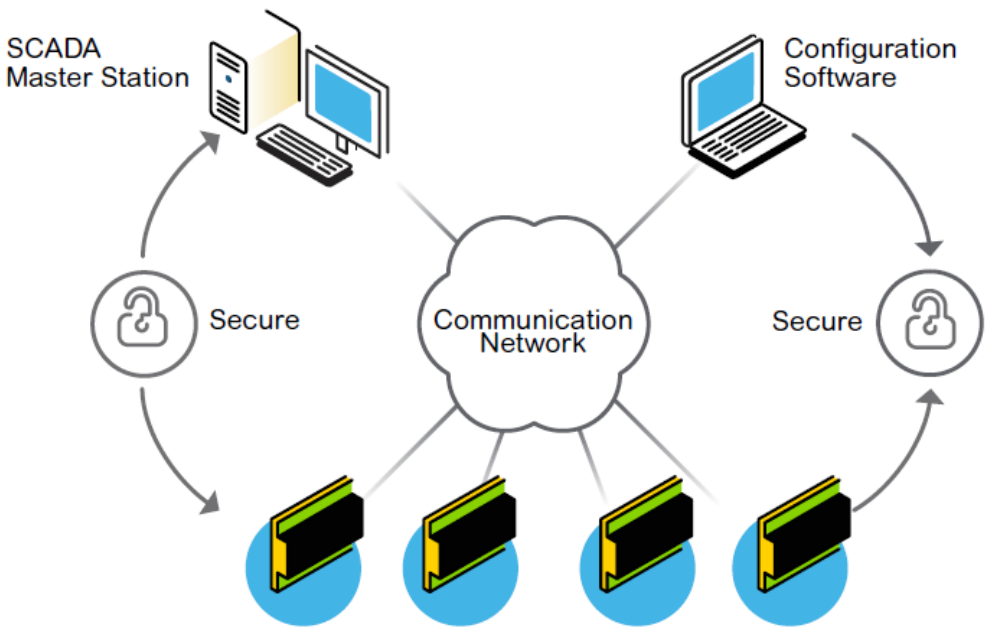
- IEE6189 (AGA12)
- IEC62351

Inoltre è stato adottato il protocollo di comunicazione DNP3 che 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.



LA SICUREZZA NEI SISTEMI DI TELECONTROLLO
Misure Adottate

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.



CONCLUSIONI 1/3

- I Sistemi di distribuzione idrica sono un potenziale obiettivo strategico
- Numerosi soggetti hanno potenzialità e risorse per effettuare attacchi informatici
- Molti sistemi SCADA presentano numerose vulnerabilità, se non aggiornati
- Un attacco ad un Sistema SCADA che sovraintenda 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 generando 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
- Preparare piani di emergenza per il recupero dei dati e per il ripristino delle normali attività.
- Istruire correttamente il personale utilizzatore della risorsa.
- Preparare piani di emergenza, per il Disaster Recovery.

CONCLUSIONI 2/3

Il sistema realizzato dimostra come sia possibile integrare con successo molteplici tecnologie convergenti in un unico sistema integrato di telegestione applicato ad 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 autorizzate, il tutto senza limitare le funzionalità richieste oggi da un sistema di Telecontrollo moderno.

Inoltre si è mostrato come per aziende medio-piccole, che non sempre sono dotate di un CED avente le competenze adeguate, sia più conveniente allocare il sistema di telecontrollo su piattaforme di tipo Cloud, eliminando le componenti di rischio legati all'accesso fisico alla risorsa e demandando l'aspetto sicurezza a strutture ben più attrezzate.

CONCLUSIONI 3/3

Nello 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 tantomeno ricorrere ad una soluzione Cloud, in quanto essendo l'azienda di alto profilo tecnologico ed essendo dotata di un proprio CED che coordina e mantiene le apparecchiature ed i servizi ovvero l'infrastruttura IT dell'azienda, garantisce gli aspetti di sicurezza interna 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

GRAZIE PER L'ATTENZIONE

G. M. Patti - G. Modica - S. Santagati

Proteo Control Technologies S.r.l.

info@proteo.it