NIER

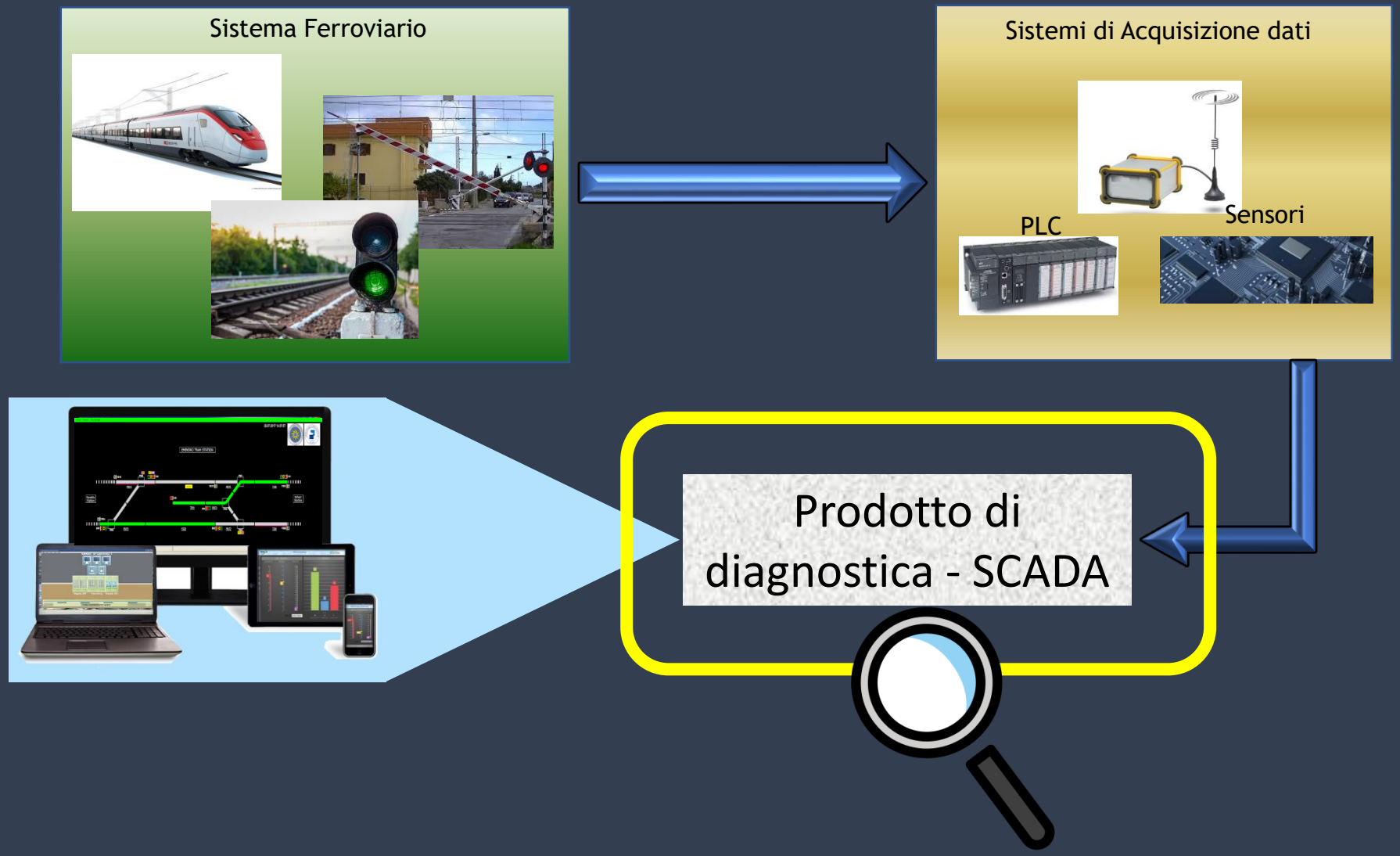
MAKING CHANGE HAPPEN. MAKING LIFE BETTER.

CYBER Security su Sistemi SCADA

Paolo Pizi
Responsabile SW Design Unit
NIER Ingegneria

N .

CONTESTO


Sistema Ferroviario
Sistemi di Acquisizione dati
PLC
Sensori
Prodotto di diagnostica - SCADA

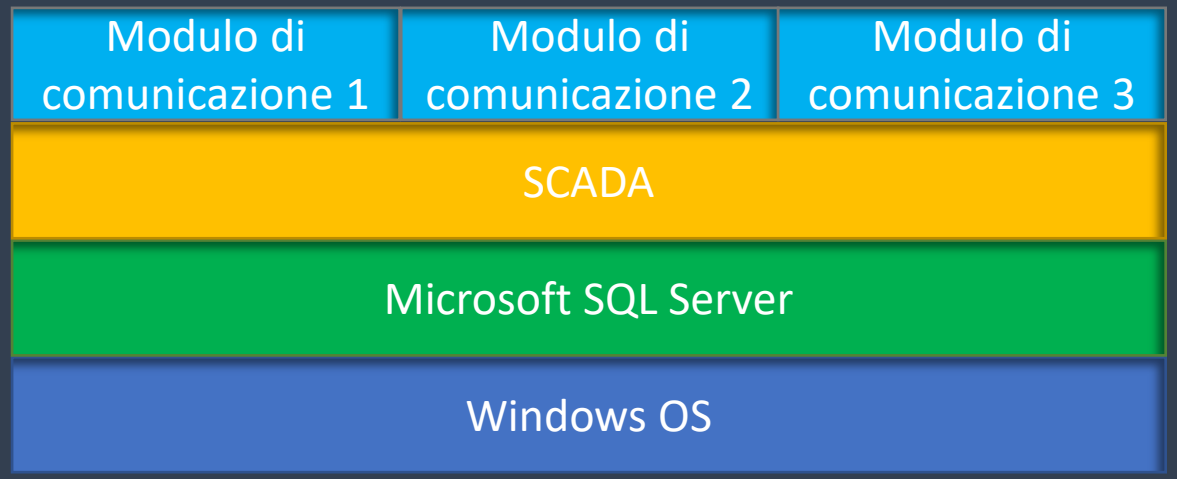
ANALISI ARCHITETTURALE

Moduli SW di comunicazione con gli apparati esterni

Installazione del software SCADA proprietario del cliente

Utilizzo di Microsoft SQL Server per le configurazioni e il salvataggio delle informazioni

Prodotto SW basato su sistemi operativi Windows



CRITICITA’ RISCONTRATE - 1

Per i sistemi operativi Windows:

- Stesso utente (e amministratore) per tutte le macchine
- Password semplice e senza regole di sicurezza
- Accesso alle macchine tramite VNC con password semplice

- Sistema operativo non aggiornato (no aggiornamenti di Windows)

Per Microsoft SQL Server:

- utente “sa” password vuota

Praticità operativa in fase di Installazione e Manutenzione

Per avere sempre le stesse condizioni operative durante le fasi di sviluppo/validazione e la fase di installazione in campo

CRITICITA’ RISCONTRATE - 2

Prima dell’avvento della Cyber Security, tale modus operandi era ritenuto corretto, in quanto i prodotti sviluppati con tecnologia SCADA non presentavano, in questo modo, problemi di «funzionamento».

Ma oggi sappiamo, o meglio siamo più consapevoli, che questo porta il prodotto (e il sistema di cui ne fa parte) ad essere vulnerabile.

Finché questi prodotti sono «in casa», in ambienti isolati, rimangono comunque al sicuro, ma quando vengono installati in campo vengono, per necessità, «esposti al mondo esterno»

CYBER SECURITY: PRIMI STEP

PROTEZIONE AI «MORSETTI»

Analizzato lo stato dell'arte si è proceduto al rafforzamento delle piattaforme su cui il prodotto, basato su SCADA, viene installato:

- Aggiornamento del Sistema Operativo alle ultime patch di sicurezza fornite da Microsoft
- Abilitazione delle policy per le password degli utenti e conseguente rafforzamento delle stesse
- Definizione degli utenti specifici
- Abilitazione dei Firewall
- Rimozione di connessioni remote non sicure come VNC
- Installazione Antivirus

Applicando «alla cieca» tutte le regole facenti parte lo «Standard Cyber», si rende al primo colpo il prodotto inusabile, in quanto totalmente isolato dal mondo esterno di cui i sistemi da diagnosticare fanno parte

CYBER SECURITY: APPROFONDIMENTO

- Abbiamo capito fin da subito che il problema non era quello di individuare ed eliminare le vulnerabilità, ma farlo lasciando il prodotto funzionante «come prima».

- E’ facile individuare quello che non va. E’ meno facile applicare le soluzioni senza alterare il prodotto su cui queste vengono applicate.

- La soluzione Cyber deve essere modellata sul prodotto, sulle sue comunicazioni, sulle sue possibili configurazioni, ed è un lavoro lungo che chiede di entrare in merito ad ogni necessità

CYBER SECURITY: SOLUZIONI TAILOR-MADE

Azioni fatte:

- Aggiornato il Sistema Operativo 

- Abilitati i firewall con definizione delle regole di connessione 
- Abilitato il trasferimento dati FTPS 

- Abilitata la connessione desktop remoto per utenti specifici 
- Attività di Verifica e Validazione 

LAVORI IN CORSO

Dopo aver agito ai morsetti, ora il lavoro è sui protocolli interni usati dall'applicazione SCADA:

- Passaggio da OPC-DA a OPC-UA
- Applicazione DTLS sui protocolli proprietari
- Supporto agli sviluppi e alla fase di V&V

Insieme al cliente, il lavoro che richiede più tempo, è il cambio di mentalità per gli utilizzatori

www.niering.it