Automazione “Security Integrated”

Cristian Sartori

SIEMENS

“Un bug non è mai solo un errore. Rappresenta qualcosa di più. Un errore nel modo di pensare”.

Industrial Security

Agenda

- Introduzione
- Industrial Security
  - Plant
  - Networking
  - System
- Soluzioni per la Network Security
  - Switch managed
  - Firewall
  - DMZ
  - VPN e Teleassistenza
- Conclusioni

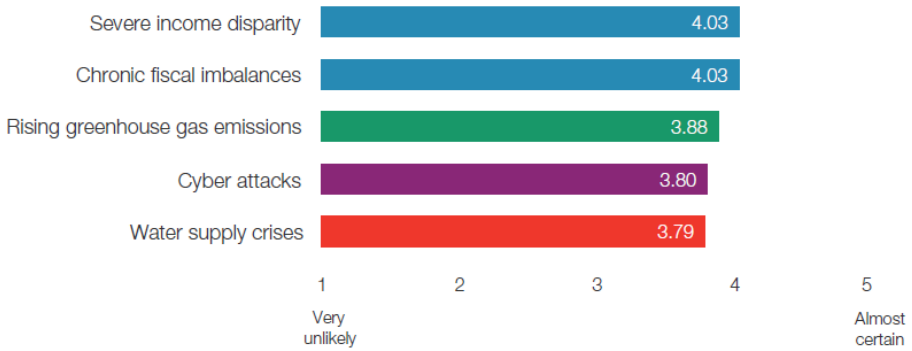
Industrial Security

Introduzione – Cosa stiamo osservando?

Trend che impattano la Security

- Incremento uso Smart Phone
- Approccio Cloud Computing
- Tecnologia Wireless
- Smart Grid
- IoT (Internet of Things)
- Industry 4.0
- Teleassistenza per accesso ad aree remote

5 rischi più probabili



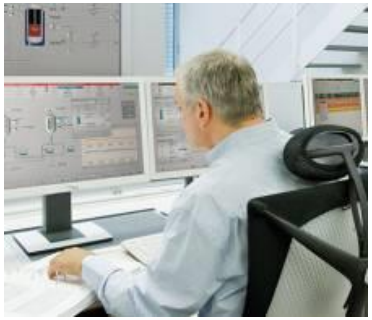
Source: World Economic Forum 2014, 50 Global Risks

Industrial Security

Introduzione – quali rischi corriamo?

Motivi per aumentare la sicurezza a causa delle vulnerabiltà

- Perdita della proprietà intellettuale
- Segreti industriali
- Sabotaggio impianto di produzione
- Indisponibilità di produzione causati da virus e malware
- Manipolazione dei dati e/o di applicazioni SW
- Uso non autorizzato di funzioni di sistema




Industrial Security

La securezza aziendale è forte come il suo anello più debole

La sicurezza potrebbe fallire

- Dipendenti
- Smarphone
- Workstation
- PC e laptop
- Infrastruttura di rete
- Policy aziendali
- Ambiente di produzione

Industrial Security

Cosa vuol dire proteggere?

Minimizzare il rischio

1 Disponibilità

Prevenzione e riduzione dei malfunzionamenti causati da attachi cibernetici per aumentare la disponibilità di produzione

2 Integrità

Protezione di sistema e integrita dei dati per ridurre problemi di malfunzionamento, errori in produzione e downtime

3 Confidenzialità

Protezione e confidenzialità dei dati e della proprietà intelletuale

Industrial Security

Attacchi cibernetici sono una realtà…dinamica

Top 10 threats 2012

1. Unauthorized use of remote maintenance access
2. Online attacks via office/enterprise networks
3. Attacks against standard components used in the ICS network
4. (Distributed) denial-of-service ((D)DOS) attacks
5. Human error and sabotage
6. Introduction of harmful code via removable media and external hardware
7. Reading and writing messages in the ICS network
8. Unauthorized access to resources
9. Attacks on network components
10. Technical faults and acts of God

Source: BSI analysis on cyber security 2012

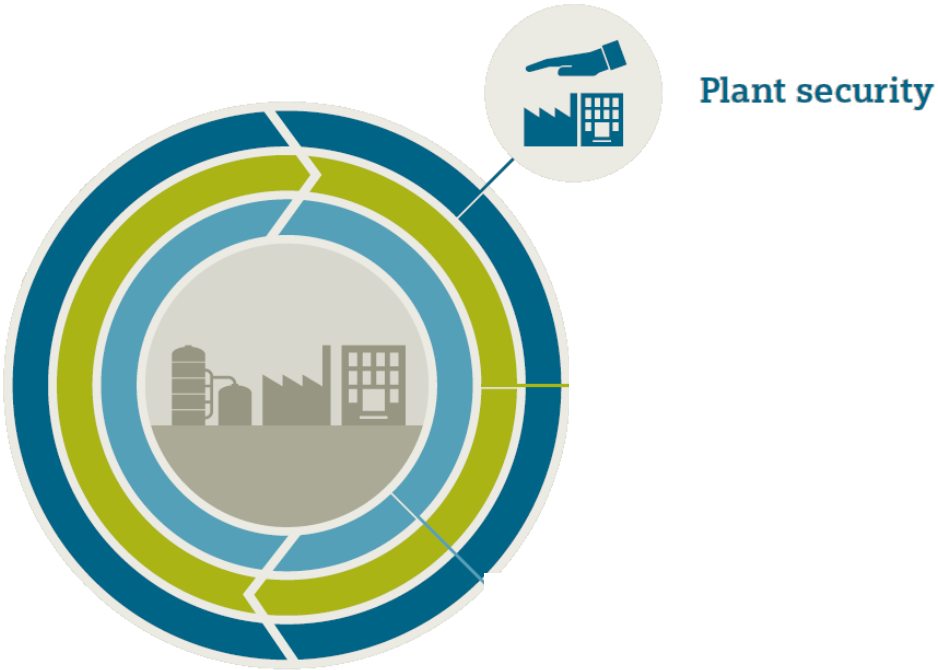
Top 10 threats 2014

1. Infection with harmful software via the Internet and Intranet — New
2. Introduction of harmful software via removable media and external hardware
3. Social engineering — New
4. Human error and sabotage
5. Unauthorized use of remote maintenance access
6. Internet-connected control components — New
7. Technical faults and acts of God
8. Compromised smartphones in the production environment — New
9. Compromised Extranet and cloud components — New
10. (Distributed) denial-of-service ((D)DOS) attacks

Source: BSI analysis on cyber security 2014

Industrial Security

Concetto “Defense in Depth” – ISA 99 / IEC 62443



- Meccanismi di protezione fisica per accesso ad aree critiche
- Nomina del Security Manager

- Interfacce definite tra mondo office e area di automazione
- Segmentazione dell’area di automazione in celle protette

- Piano di aggiormanto software permessi e antivirus
- Autenticazione riservata a gruppi di operatori

1. Plant Security

Concetto “Defense in Depth”

- Analisi vulnerabilità
- Analisi rischio
- Gap Analysis
- Analis minacce

- Corsi cyber security
- Sviluppo strategia di security
- Implementazione di tecnolgie per la cyber security

- Operazioni continue
- Rilevamento e gestione di incidenti legati alle cyber security
- Dinamicità nell’adotaare strategia contro le vulnerabilità

2. Network Security

Concetto “Defense in Depth”

Network Security

Network Access Control

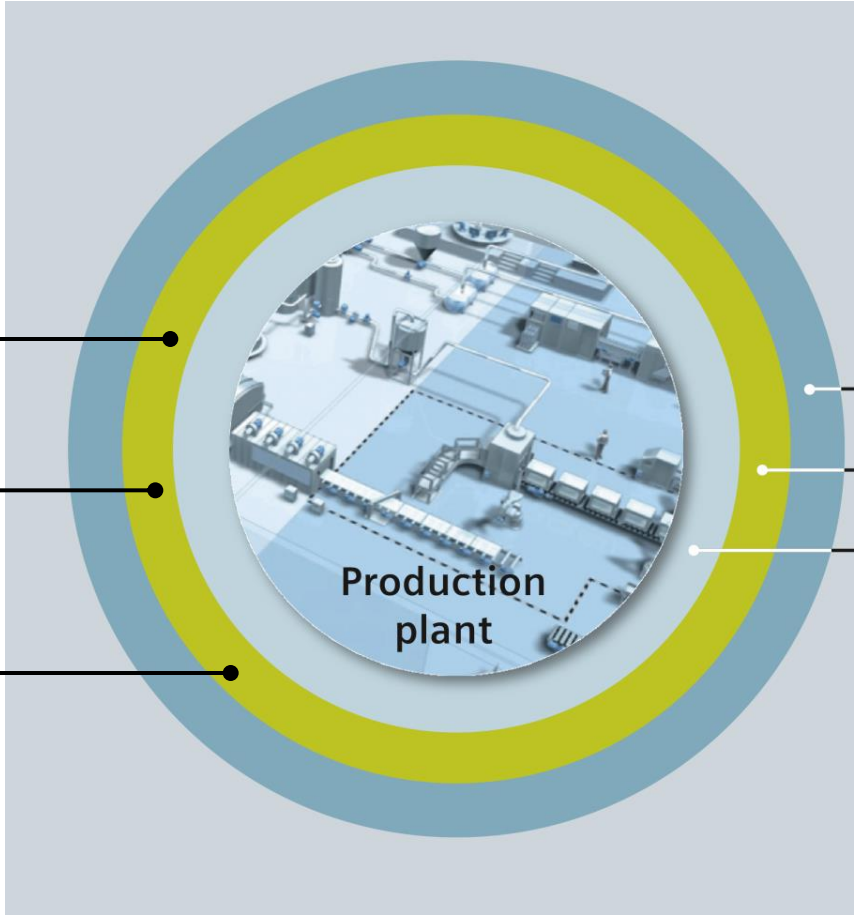
- Architettura sicura tra IT e automazione con DMZ
- Accesso sicuro attraverso Internet per VPN
- Autenticazione di utente e sicurezza di porta con Firewall

Redundancy

- Implementazione di concetti di ridondanza sia a livello di topologia di rete che di connessioni sicure

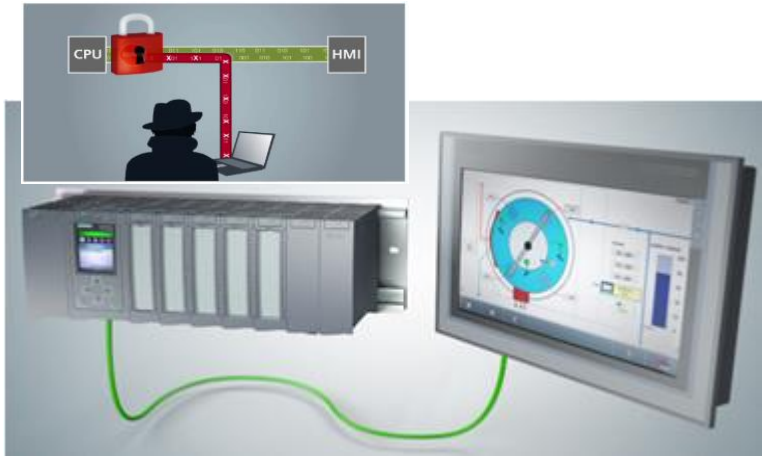
Cell Protection

- Mitigazione del rischi tramite segmentazione delle celel di automazione
- Utilizzo di comunicazione sicura (ad esempio https) per prevenire rischioi di spionaggio e manipolazione



3. System Security

Concetto “Defense in Depth”



- Sistemi basati su PC devono gestire la identificazione dell’utente
- System Hardening

- Gestione di SW antivirus e Malware
- Gestione e update delle patch

Soluzioni per la Network Security

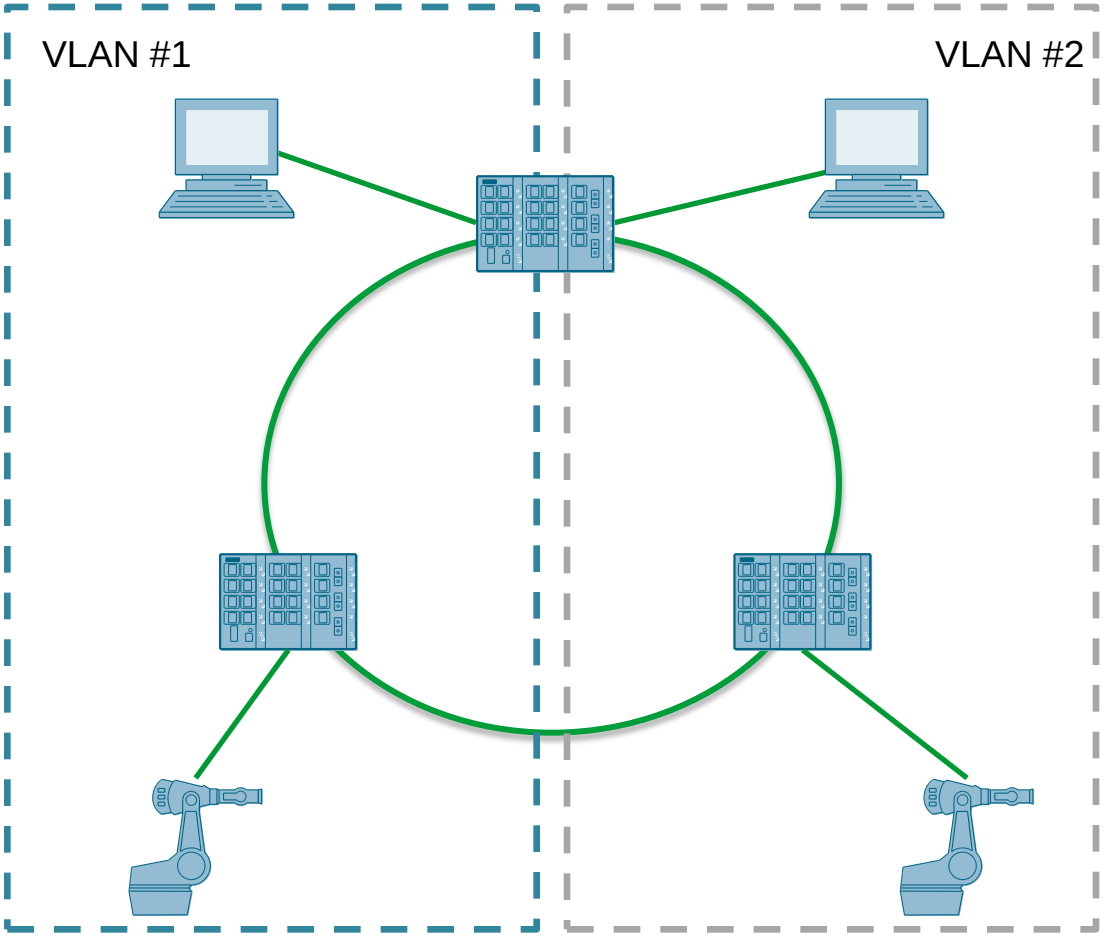
Switch managed e ridondanza di anello

Obiettivo

Implementazione di aree logiche separate, collegamenti ridondati e dispositivi per diagnostica avanzata

Soluzione

Utilizzo di switch managed per implementazione di VLAN, MRP (Media Redunandancy Protocol) e protocollo SNMP per la diagnostica



Soluzioni per la Network Security

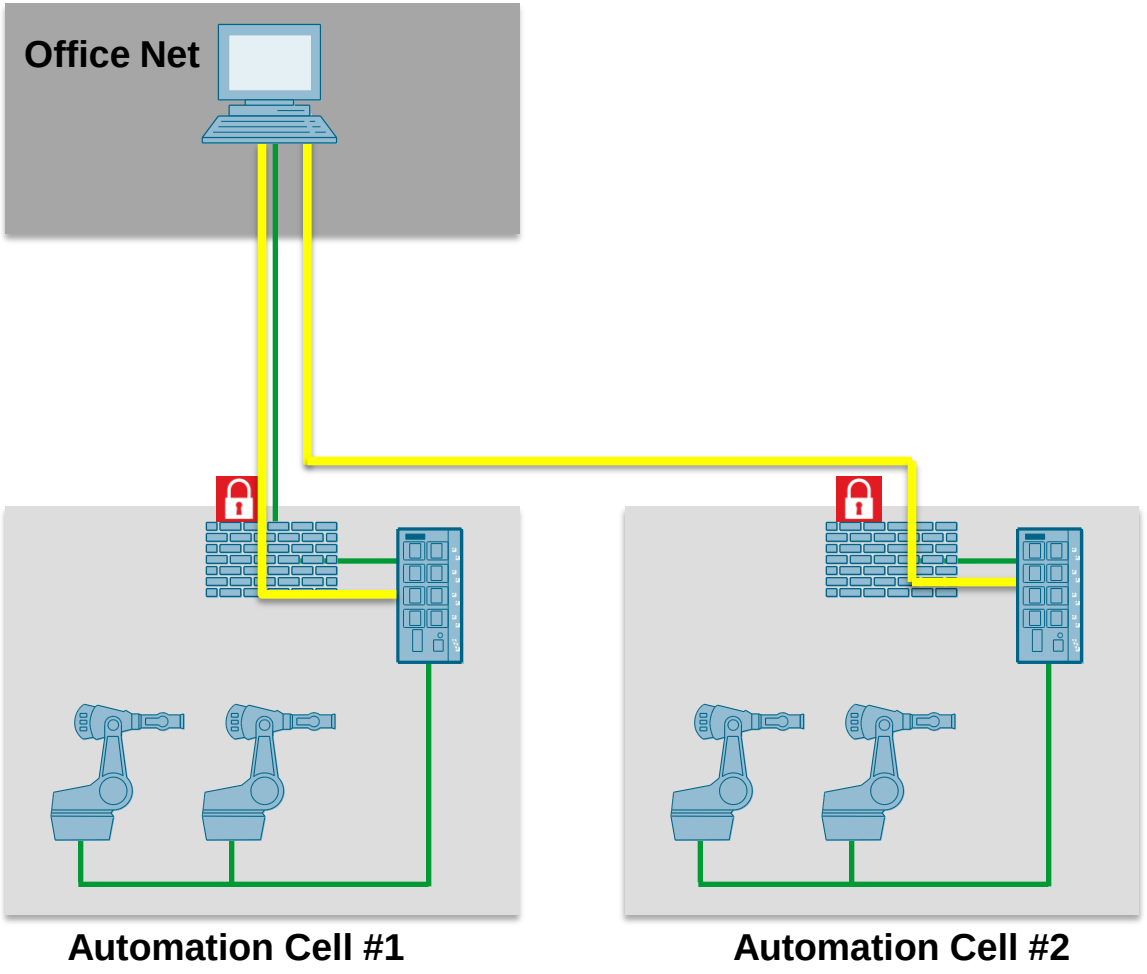
Firewall

Obiettivo

Solo connessioni autorizzate possono accedere ad aree riservate (celle di automazione)

Soluzione

Firewall per ogni cella di automazione con accesso per autenticazione



Soluzioni per la Network Security

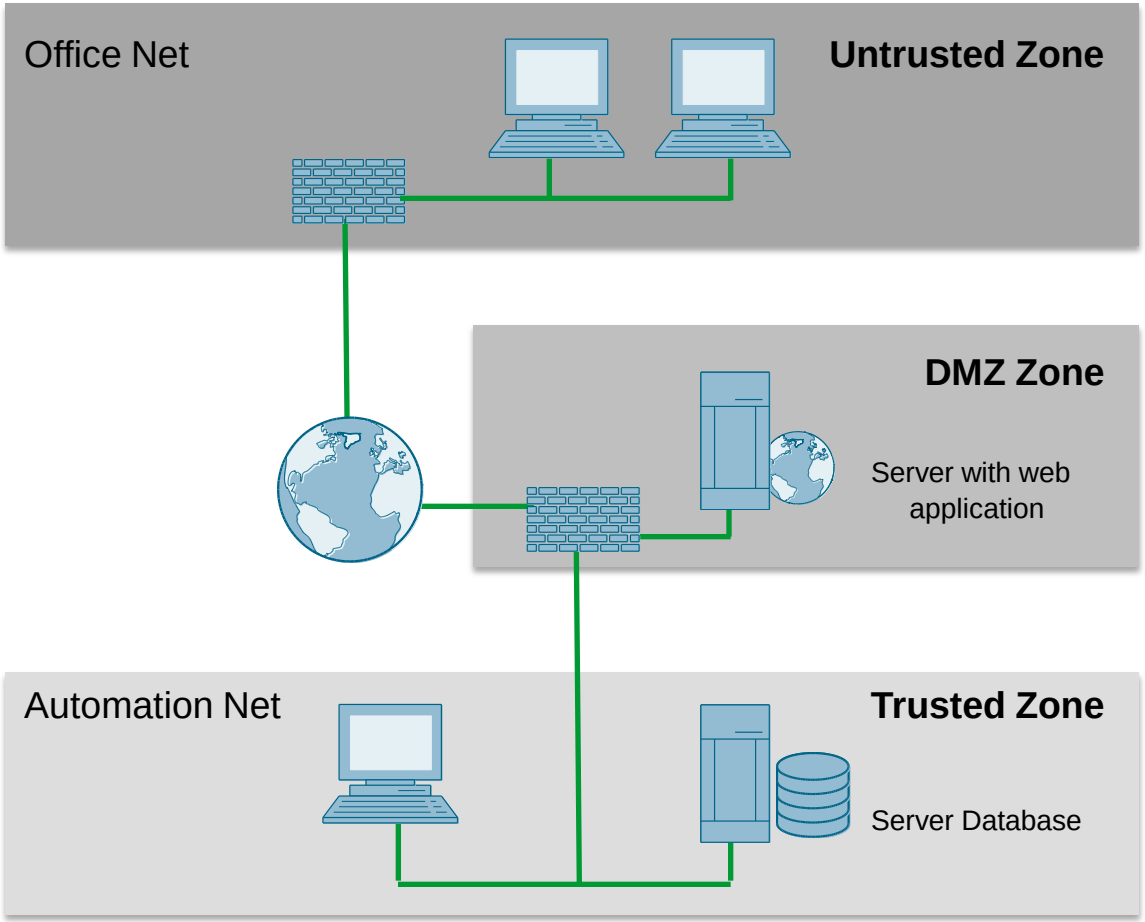
DMZ

Obiettivo

Utenze come il MES devono essere accessibili sia da rete non-sicura che sicura (automazione) evitando un canale diretto tra le due reti

Soluzione

Si implementa una rete DMZ (demilitarizzata) separando il server con applicazione web e il server con database su aree separate tramite firewall



Soluzioni per la Network Security

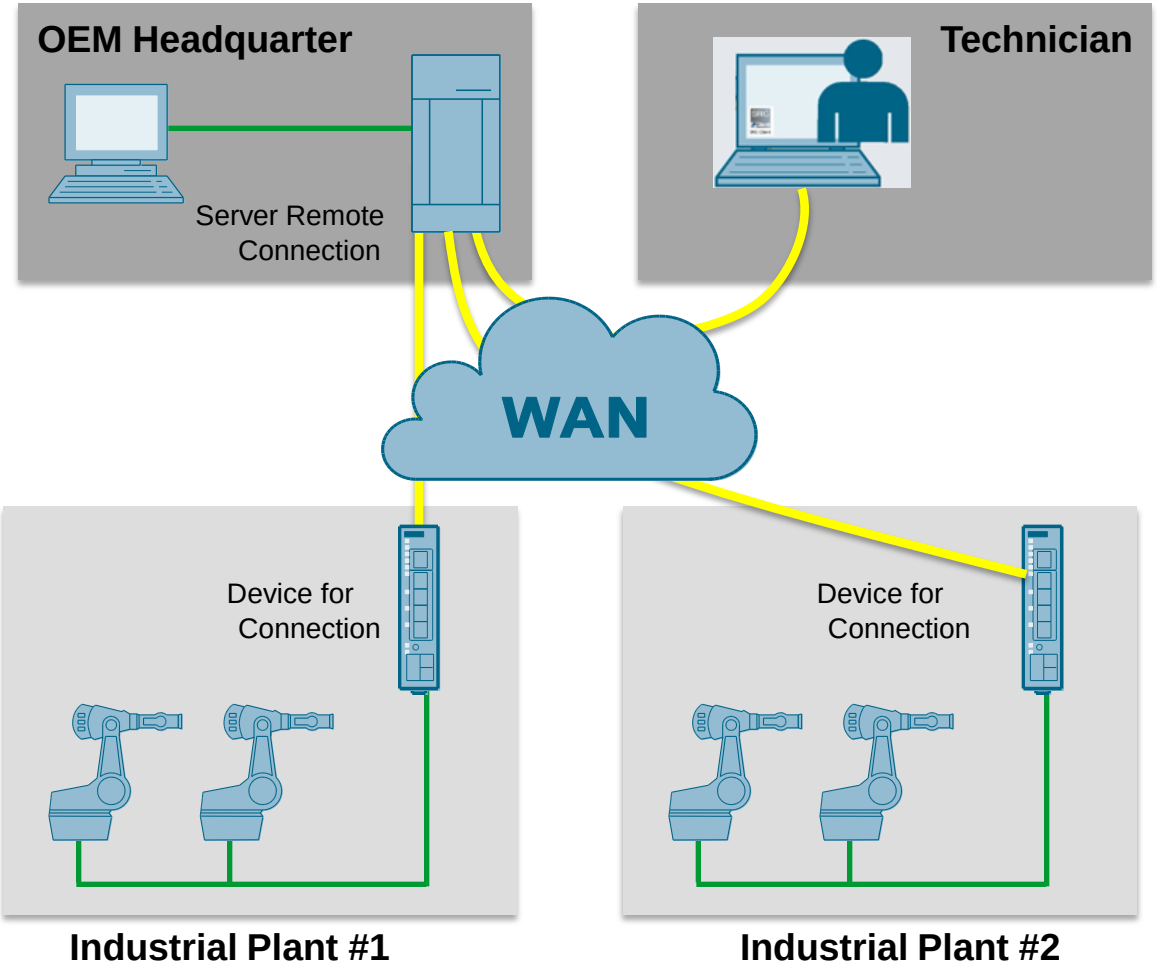
Teleassistenza

Obiettivo

Accesso sicuro ed autenticato a macchine remote installate in tutto il mondo per telassistenza (diagonsitica e upgrade del SW) e possibilità di configurazione dellle porte VPN

Soluzione

Utilizzo di un server installato nell'ufficio del produttore di macchine e di n dispositivi per stabilire il tunnel VPN di tipo sicuro con Open VPN



Industrial Security

Conclusioni

Defense in Depth

Grazie per l‘attenzione