Proteggere il sistema produttivo nell'era di Industry 4.0

Cristian Sartori

SIEMENS

Slide - Save 27 Ottobre 2015

Industrial Security

Attacchi cibernetici sono una realtà…dinamica

Top 10 threats 2012	Top 10 threats 2014
1. Unauthorized use of remote maintenance access	1. Infection with harmful software via the Internet and Intranet (New)
2. Online attacks via office/enterprise networks	2. Introduction of harmful software via removable media and external hardware
3. Attacks against standard components used in the ICS network	3. Social engineering (New)
4. (Distributed) denial-of-service ((D)DOS) attacks	4. Human error and sabotage
5. Human error and sabotage	5. Unauthorized use of remote maintenance access
6. Introduction of harmful code via removable media and external hardware	6. Internet-connected control components (New)
7. Reading and writing messages in the ICS network	7. Technical faults and acts of God
8. Unauthorized access to resources	8. Compromised smartphones in the production environment (New)
9. Attacks on network components	9. Compromised Extranet and cloud components (New)
10. Technical faults and acts of God	10. (Distributed) denial-of-service ((D)DOS) attacks

Source: BSI analysis on cyber security 2012

Source: BSI analysis on cyber security 2014

L’evoluzione della specie…

Top 10 minacce 2014

1. Infezioni malware via Internet e Intranet (p.es. server di posta)
2. Introduzione di malware con supporti di memoria removibili (p.es. USB) o altro hardware
3. Social engineering
4. Errore umano e sabotaggio
5. Uso non autorizzato di accessi per teleassistenza
6. Controllori collegati a Internet
7. Problemi tecnici e “Act of God”
8. Smartphones compromessi in ambienti produttivi
9. Componenti extranet e cloud compromessi
10. Attacchi (Distributed) denial-of-service ((D)DOS))

Source: BSI analysis on cyber security 2014

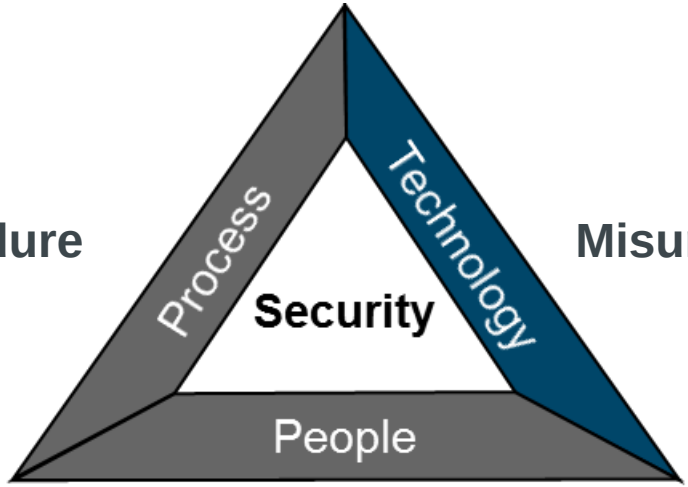
Top 10 minacce 2016

1. Social engineering e (spear)phising — New
2. Introduzione di malware con supporti di memoria removibili (p.es. USB) o altro hardware
3. Infezioni malware via Internet e Intranet (p.es. server di posta)
4. Intrusioni attraverso accessi remoti (p.es. teleassistenza)
5. Errore umano e sabotaggio
6. Controllori collegati a Internet
7. Problemi tecnici e force majeure
8. Componenti extranet e cloud compromessi
9. Attacchi (Distributed) denial-of-service ((D)DOS))
10. Smartphones compromessi in ambienti produttivi

Source: BSI analysis on cyber security 2016

Security è legata a…

Policy e procedure



Misure di security

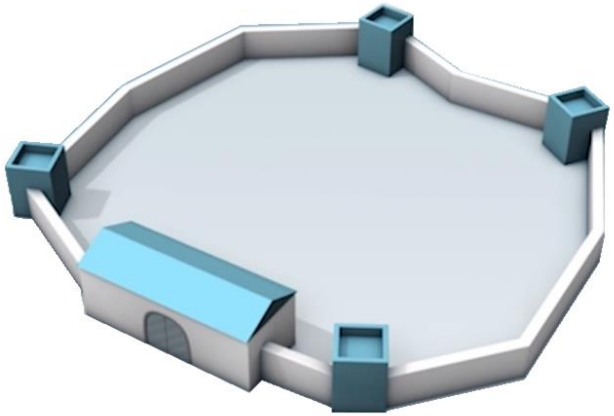
Competenza

Un approccio olistico per la security è un concetto che include: tecnologie, processi e persone

Defense in Depth: la chiave per un’infrastruttura sicura

Singola Barriera

- Muro impenetrabile
- Singolo livello di protezione
- Singolo punto di attacco

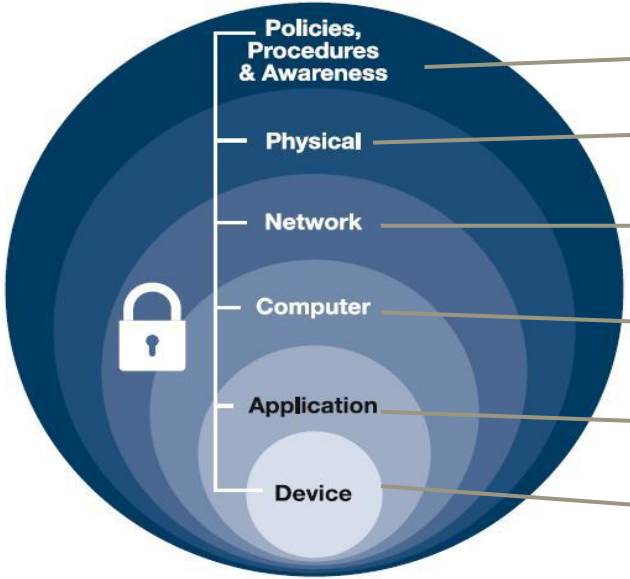


Defense In Depth

- Protezione su più livelli
- Ogni livello protegge gli altri livelli
- Un attaccante deve spendere tempo ed effort per ogni transizione

IEC 62443: Security per l'automazione

IEC 62443: standard security in ambito IACS – Industrial Automation and Control System - basato sul principo "Defense in depth" → protezione su più livelli



- Policies, Procedures, Training
- Access Control Cards, Cameras, Locks
- Firewall, IPSec, Network Intrusion Detection
- System Hardening, Intrusion Detection
- Application Layer FW , Application Hardening
- Access Controls, Encryption, Digital Rights

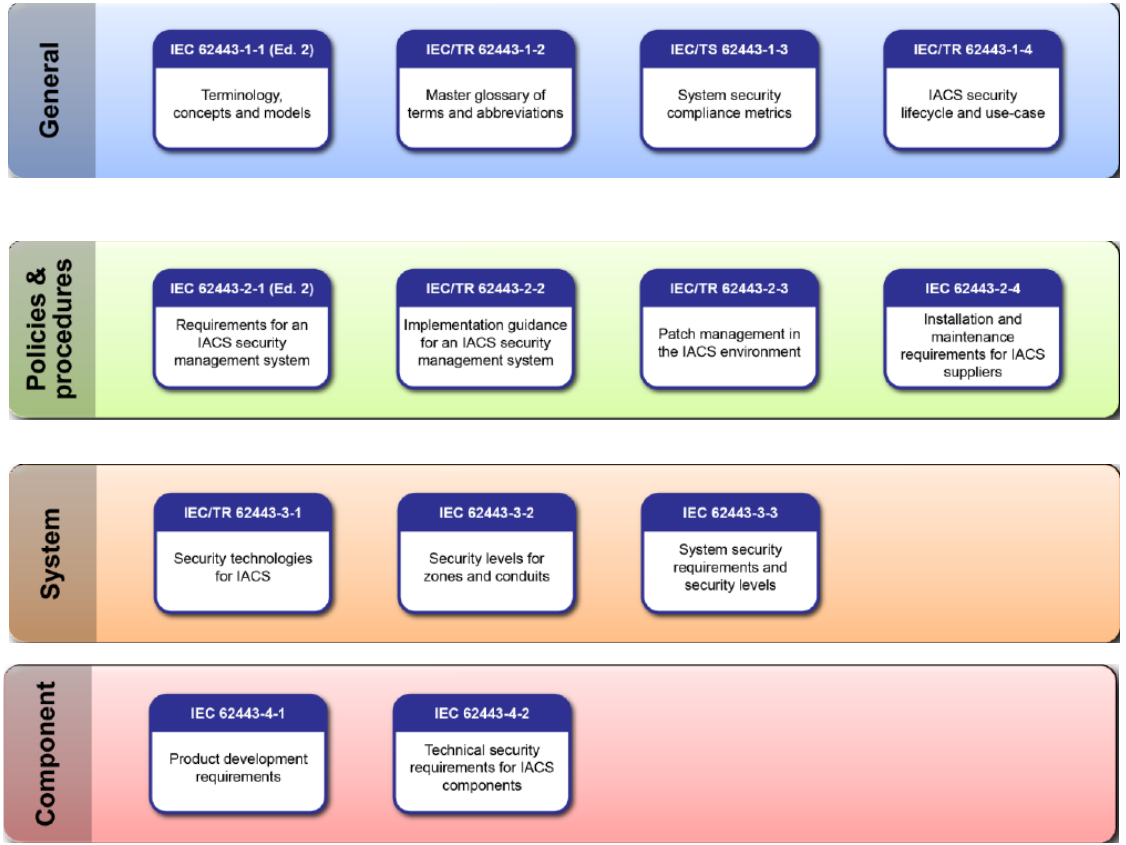
IEC 62443: Framework

62443-1
Terminologia, definizioni e **concetti**

62443-2
Requisiti per la **sicurezza dei processi e organizzazione** dell'end user e integratore

62443-3
Requisiti per raggiungere **una soluzione sicura**

62443-4
Requisiti per ottenere un **componente sicuro**

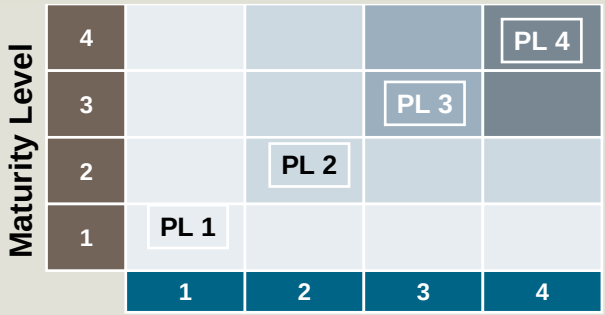


PL: Funzione dei livelli dei processi e funzionalità

Security Level

- Valutazione delle **funzionalità** di security
- Basati su IEC 62443-3-3

Protection Level (PL)



Maturity Level

- Valutazione dei **processi** di security
- Basati su IEC 62443-2-4 and ISO27001

Attacco rete elettrica Ucraina 2015

Spear Phishing

↓

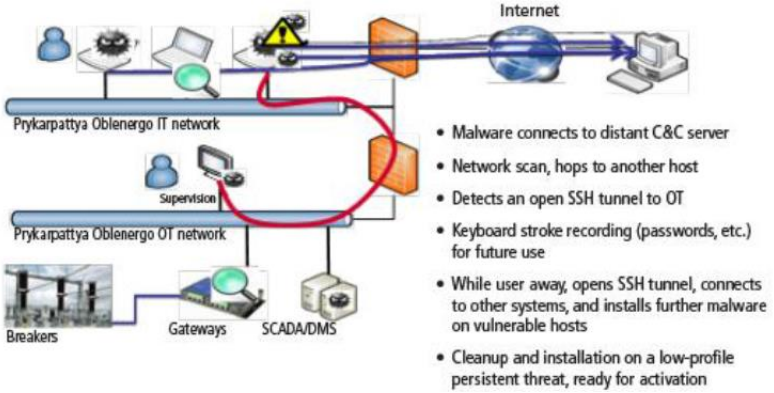
Intrusione nella rete IT

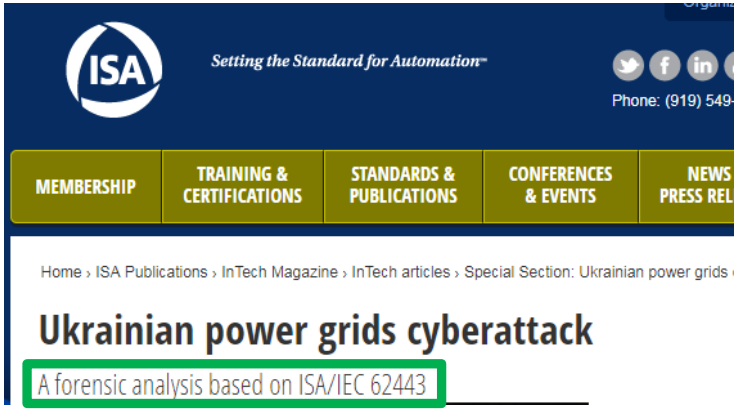
↓

Raccolta di informazioni sulla rete IT e OT

↓

Attacco sullo SCADA





Source
https://www.isa.org/templates/news-detail.aspx?id=152995

Defense in Depth

Plant security

- Meccanismi di protezione fisica per accesso ad aree critiche
- Implementazione processo di security management

Network security

- Protezione di cella, DMZ assitenza remota
- Firewall e VPN

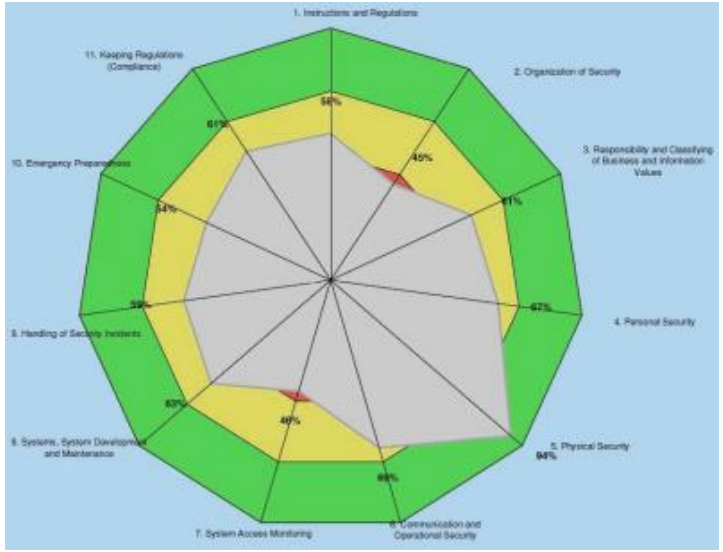
System integrity

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

Defense in Depth

Plant Security

- **Assessment** della sicurezza della fabbrica in funzione dello standard **ISO 27001** e **IEC 62443**



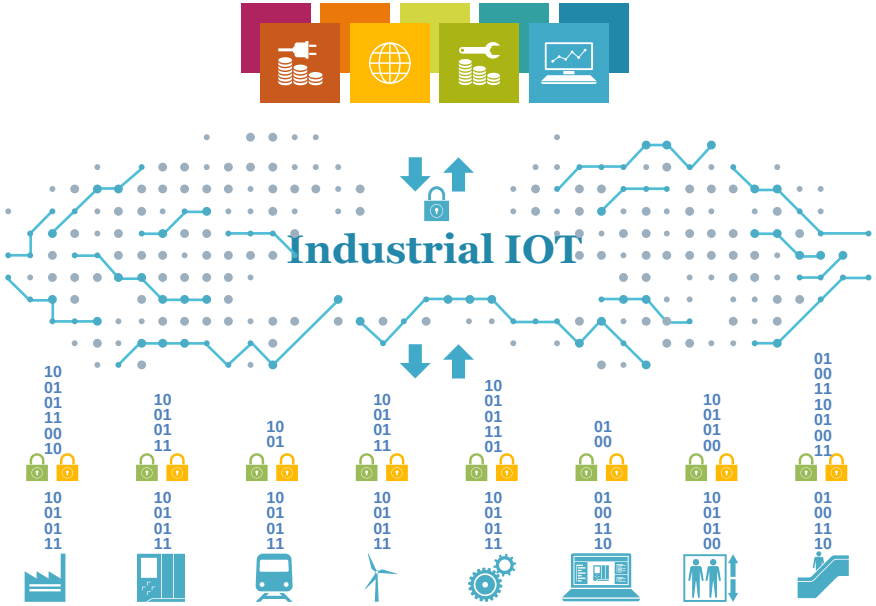
- **Risk & Vulnerability Assessment:** identificazione, classificazione e valutazione per un programma basato sulla metodologia del rischio

Vulnerability	Risk Score
Flat network architecture / No DMZ available	8,1
Flat network architecture / No network segmentation	8,1
Unsecure / Not controlled remote activities	7,4
No system hardening / Unneeded applications and services installed	7,1
Unpatched operating systems	6,8
Obsolete anti-virus database	6,6
Windows firewall not active	5,6
Uncontrolled USB interfaces	4,8

Table 1: Risk Scoring (direct risks) according to CVSS

- Red [7,5-10] – Unacceptable risk; Urgent action is necessary
- Orange [5-7,5] – Unacceptable risk; Action is required
- Yellow [2,5-5] – Acceptable risk; Subject to management approval
- Green [0-2,5] – Acceptable risk; No action required

Industrial Internet of Things - Security



Storage/Processing

Architettura multitenant per proteggere i diversi servizi
Criteri IT per ISO 27001

Transito:

comunicazione HTTPS Transport Layer Security (TLS) 1.2 standard e crittografia TSL a 256 bit

Trasmissione sicura:

Protezione attraverso firewall e Proxy
Black Box: agente di connessione non accessibile per modifica

APP IIOT per la security

✓APP operanti su IIOT come strumento di supporto per la gestione della sicurezza

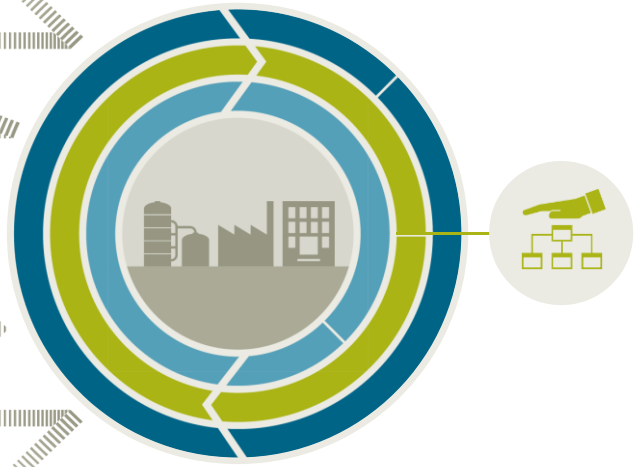
✓Censimento delle versioni SW/HW dei componenti

✓Monitoraggio e segnalazione Patch e nuove versioni applicabili

✓Report su vulnerabilità

Defense in Depth

Defense in Depth



Network security

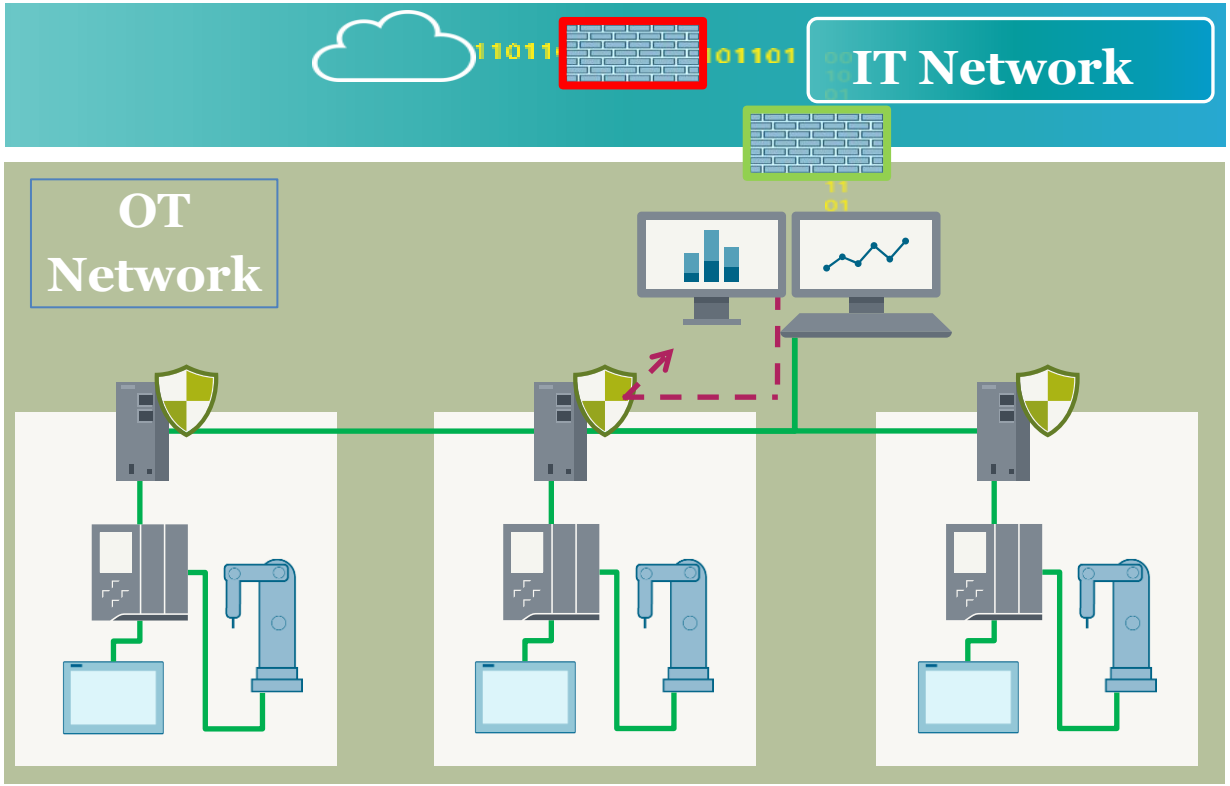
- Protezione di cella, DMZ assitenza remota
- Firewall e VPN

Switch managed - “Go Managed!!!”

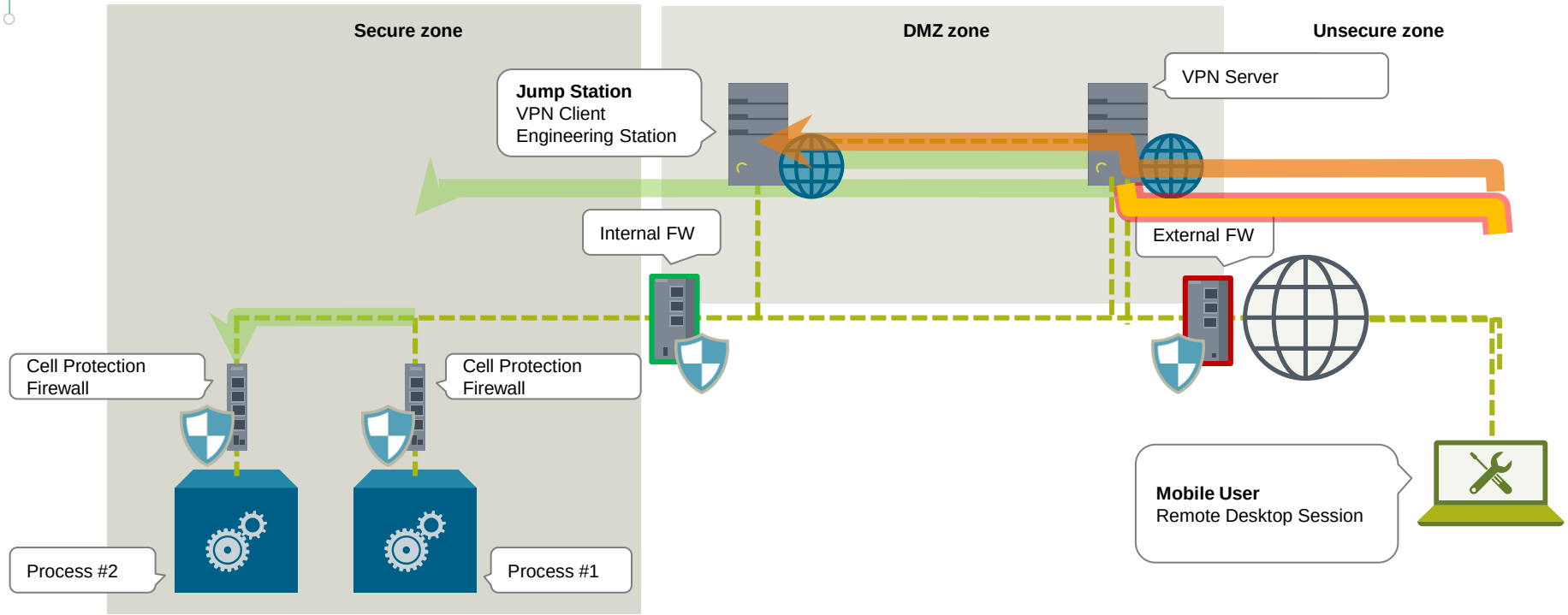
- Sfruttare **protcolli** per **ridondanza**
- Usare **Password**
- Usare **VLAN**
- Abilitare **ACL**
- **Limitare** Broadcast (DoS)
- **Disabilitare porte** non utilizzate e **Loop Detection**
- Abilitare **SNMP V3**

Firewall: Segmentazione - Cell Protection

- Separazione della rete OT in **celle di protezione**
- Connessioni autorizzate tramite **Firewall**



Teleassistenza sicura



System Integrity

Defense in Depth

System integrity

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

RFID - Autenticazione utenti

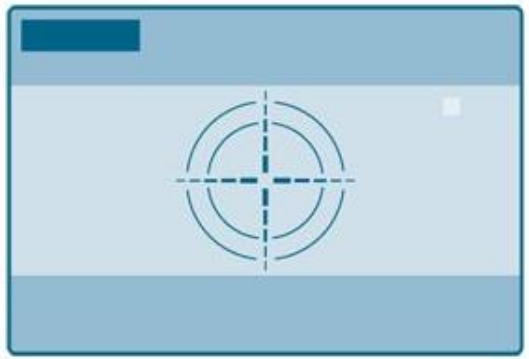
Obiettivo

Controllo di accesso alle macchine e sistemi di automazione in funzione dei diritti dell'utente/operatore tramite utilizzo di badge

Soluzione

Reader RFID che fornisce il controlllo di accesso alla macchina di automazione tramite **badge standard** (ISO 14443A/B e ISO 15693).

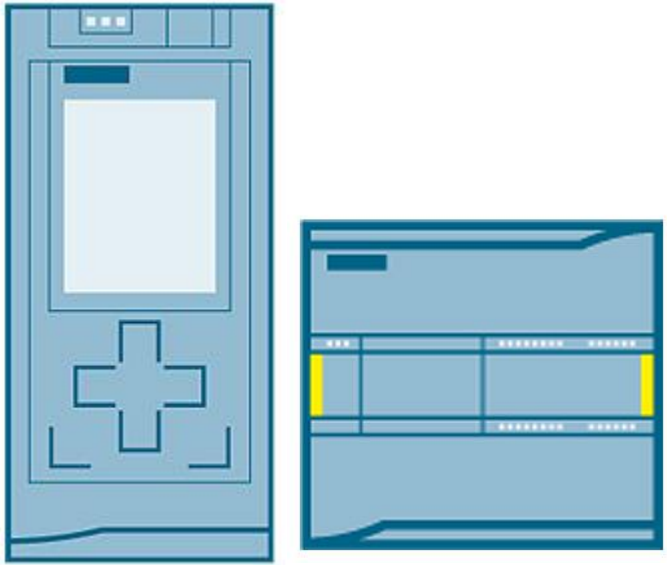
Possibilità di tenere traccia tramite log su base utente



PWD devono essere robuste!

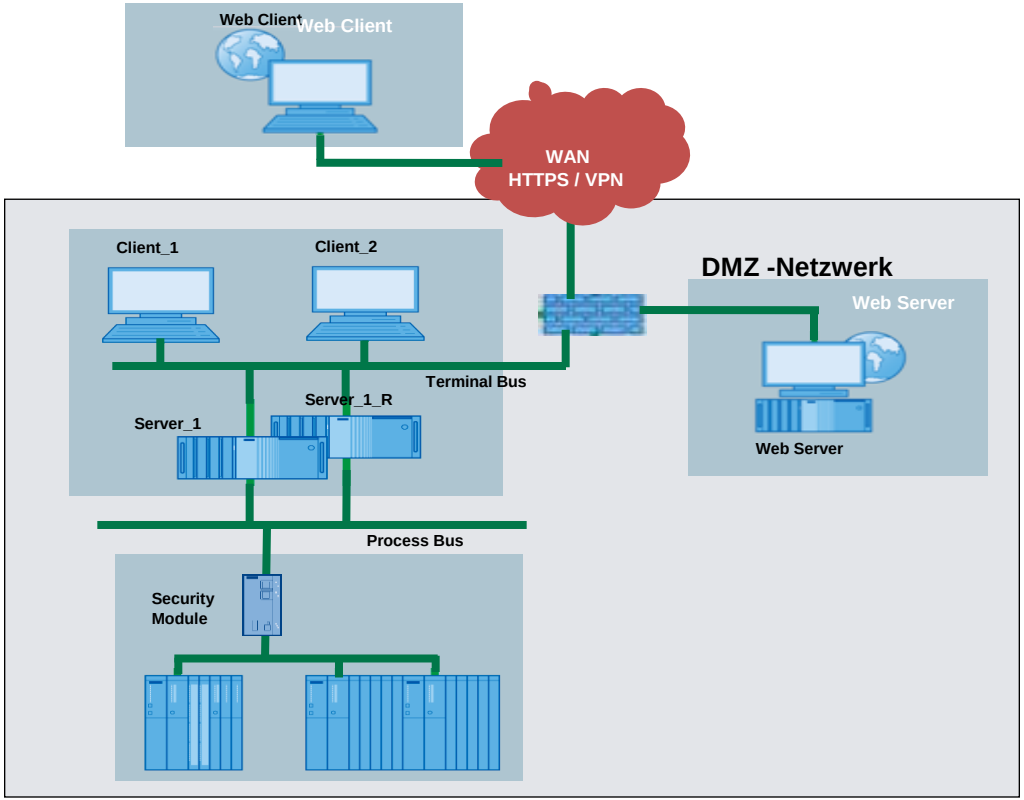
http://calc.opensecurityresearch.com/?pwLen=3&kpsSelect=9250000&charSelect=lalpha-numeric-all-space&charsetLen=77&kps=9250000

PLC



- Protezione dei blocchi con password
- Protezione copia programma con riconoscimento serial number di CPU o Memory Card
- Protezione di accesso con diversi diritti di accesso
- Comunicazione tra PLC, HMI e Engineering con security integrata
- **Supporto certificati secondo standard X.509**
- **Server OPC UA con autenticazione e encryption**
- Web Server con gestione utenti con diversi di diritti di accesso
- **Comunicazione TCP/IP con crittografia**

HMI



- **Supporto di Antivirus testati**
- **Compatibilità con le Security Patches di Microsoft**
- **Comunicazione sicura tra server e client tramite crittografia SSL**
- Utilizzo di Domain Controller e gestione utenti ereditando le policy di sicurezza di Windows
- IPSEC tra i Server e Web Navigator
- Possibilità di configurare la comunicazione HTTPS nei server Web, obbligatoria in WebUX
- Supporto di reti VPN per i client web
- Configurazione dell'accesso in lettura/scrittura ai PLC
- Per l'engineering, Know-how Protection di script, pagine grafiche

In conclusione…

1. Con la digitalizzazione è necessario affrontare il tema della cyber security per proteggere i propri impianti industriali.
2. Non esiste la singola misura di protezione perfetta! La protezione è ottimizzata solo implementando **contemporaneamente** più **misure complementari**
3. **La IEC 62443** è la normativa di riferimento per la cyber security in ambito industriale, basata sul principio – **Defense In Depth**
4. La secuirity è un processo sempre “ongoing”: **assess, implement & manage**
5. Si può collegare l’industria con l’Internet of Things in modo facile, affidabile e sicuro. E anche sfruttarlo per avere lo stato sempre aggiornato,