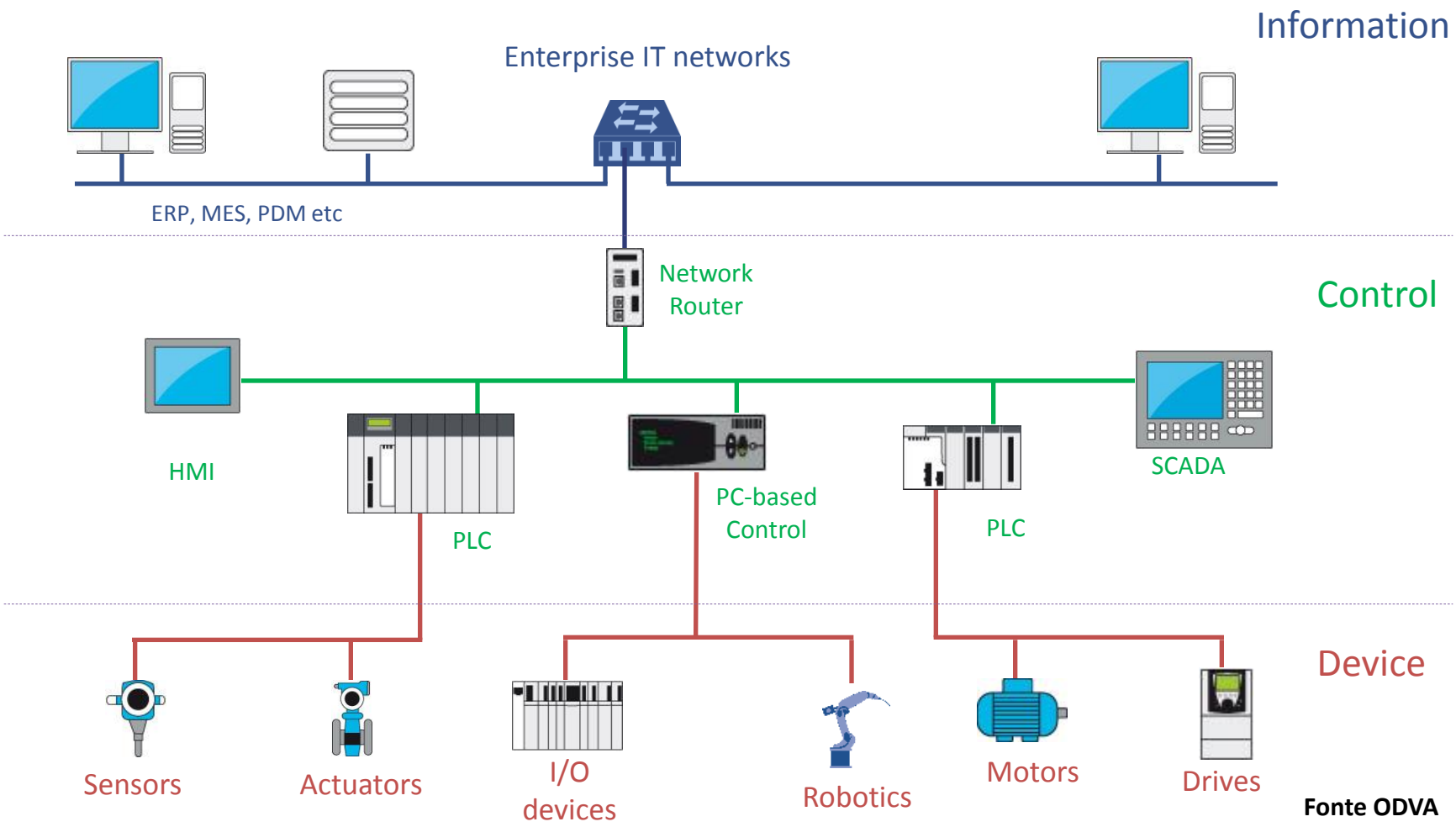
ePAC & Cyber Security verso un nuovo modello di IT/OT nell'Industry 4.0

Carlucci Giancarlo
Business Development & Product Expert
PlantSolution

Convergenza tra IT/OT nell'Industry 4.0

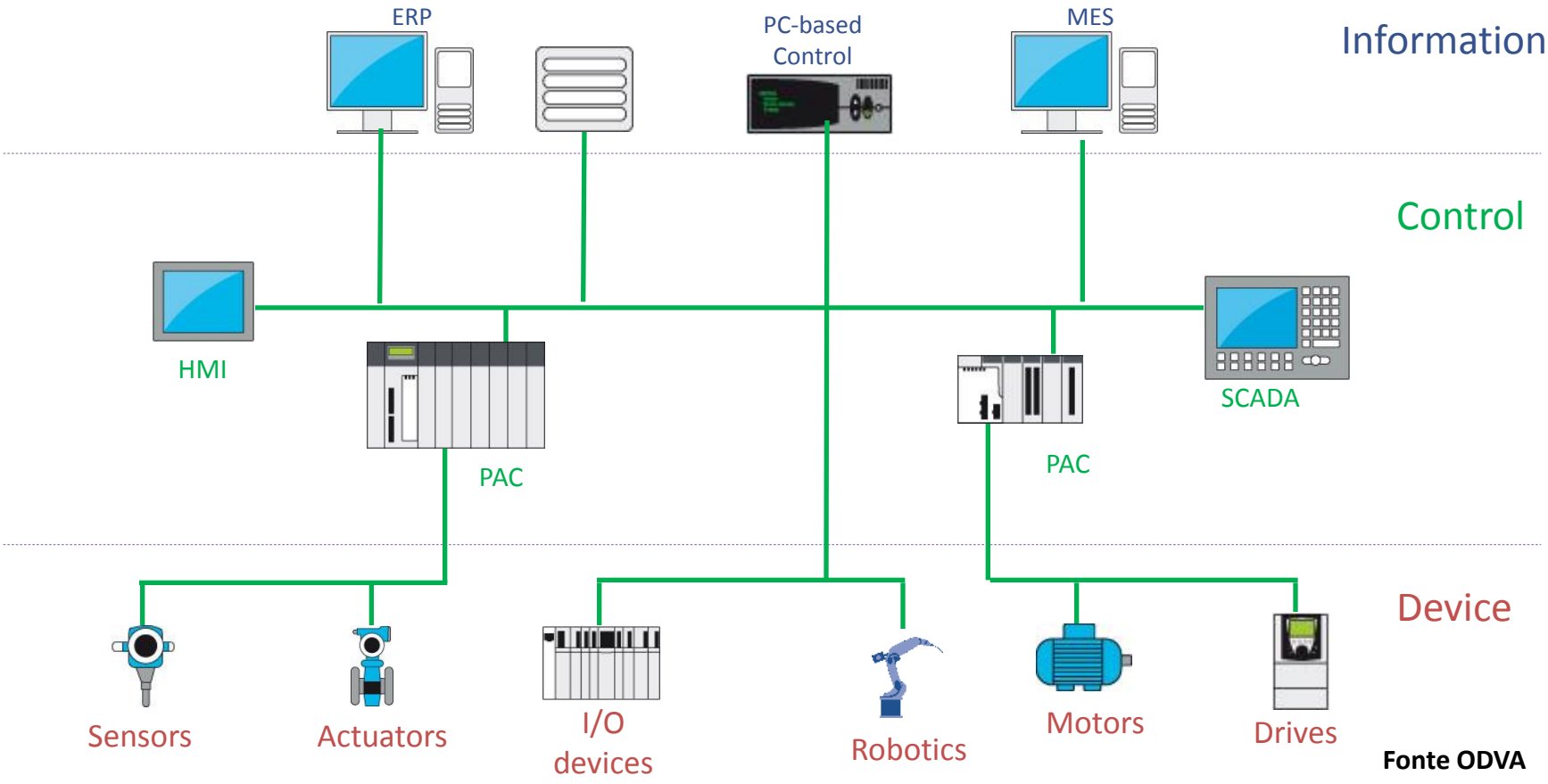
Architettura di rete Tradizionale



Fonte ODVA

Convergenza tra IT/OT nell'Industry 4.0

Architettura di rete Unificata



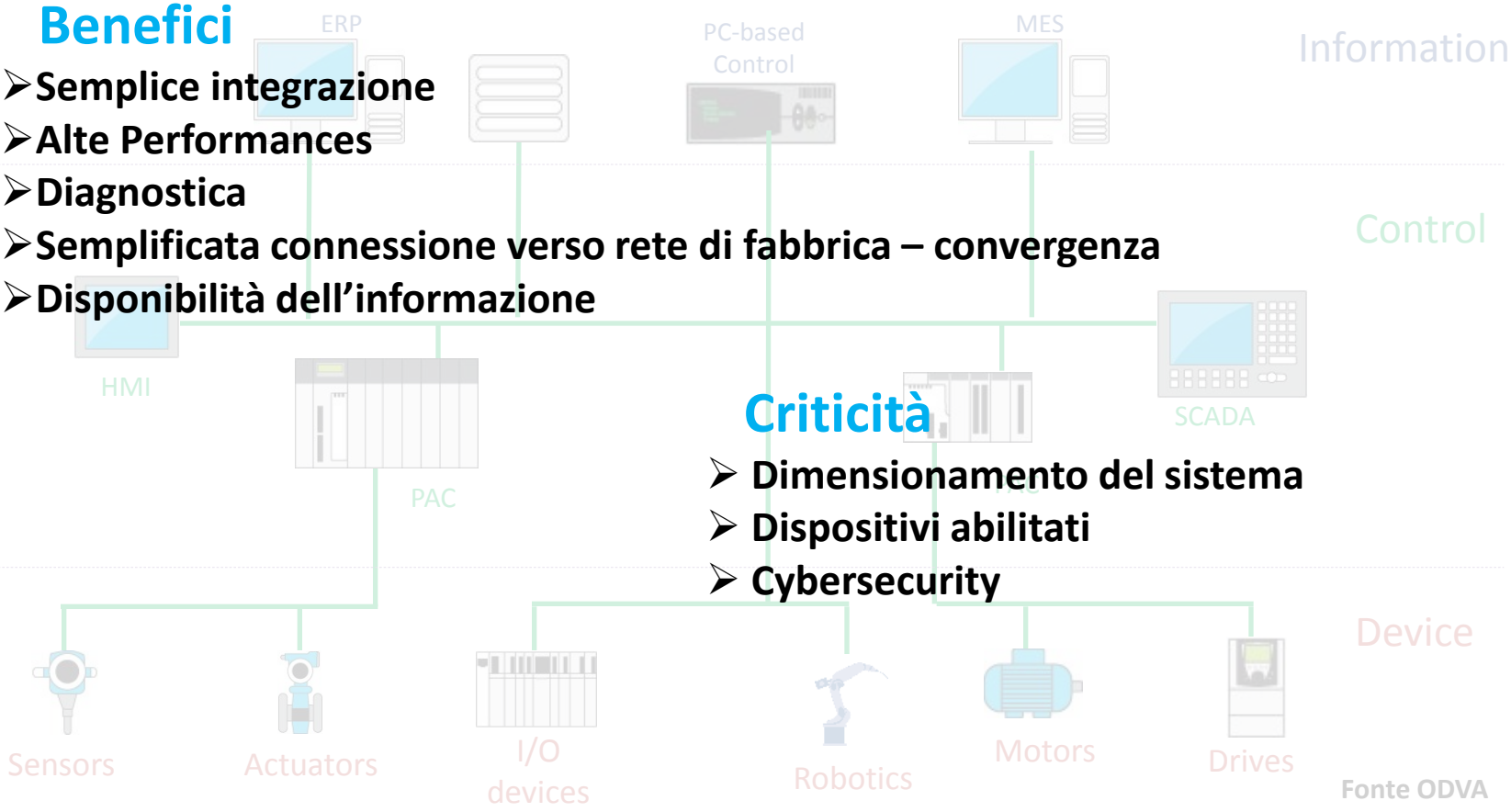
Fonte ODVA

Convergenza tra IT/OT nell'Industry 4.0

Architettura di rete Unificata

Benefici

- **Semplice integrazione**
- **Alte Performances**
- **Diagnostica**
- **Semplificata connessione verso rete di fabbrica – convergenza**
- **Disponibilità dell'informazione**



Criticità

- **Dimensionamento del sistema**
- **Dispositivi abilitati**
- **Cybersecurity**

Fonte ODVA

Industry Cybersecurity Strategy

Sicurezza del sito

Infrastruttura di rete sicura

Offerta prodotti sicuri

Standard di Sicurezza

Sicurezza come processo in continua evoluzione

Industry Cybersecurity Strategy

Sicurezza del sito

Servizi di sicurezza e di protezione avanzata - **Defense-in-Depth**

Analisi tolleranza al Fault

Architetture raccomandate -TVDA

Infrastruttura di rete sicura

Firewall/Router/Switch Managed

SCADA

ePAC

Offerta prodotti sicuri

Standard di Sicurezza

Sicurezza come processo in continua evoluzione

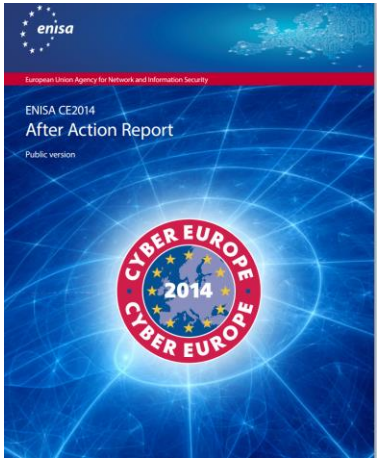
Raccomandazioni e Standard

Unione Europea

Dic 2009, ENISA

Portato in evidenza la problematica raccomandando gli Stati membri circa la necessità di proteggere le Infrastrutture critiche e sistemi Industriali.

ENISA organizza workshop per armonizzare le necessità e creare una piattaforma di lavoro.



www.enisa.europa.eu/

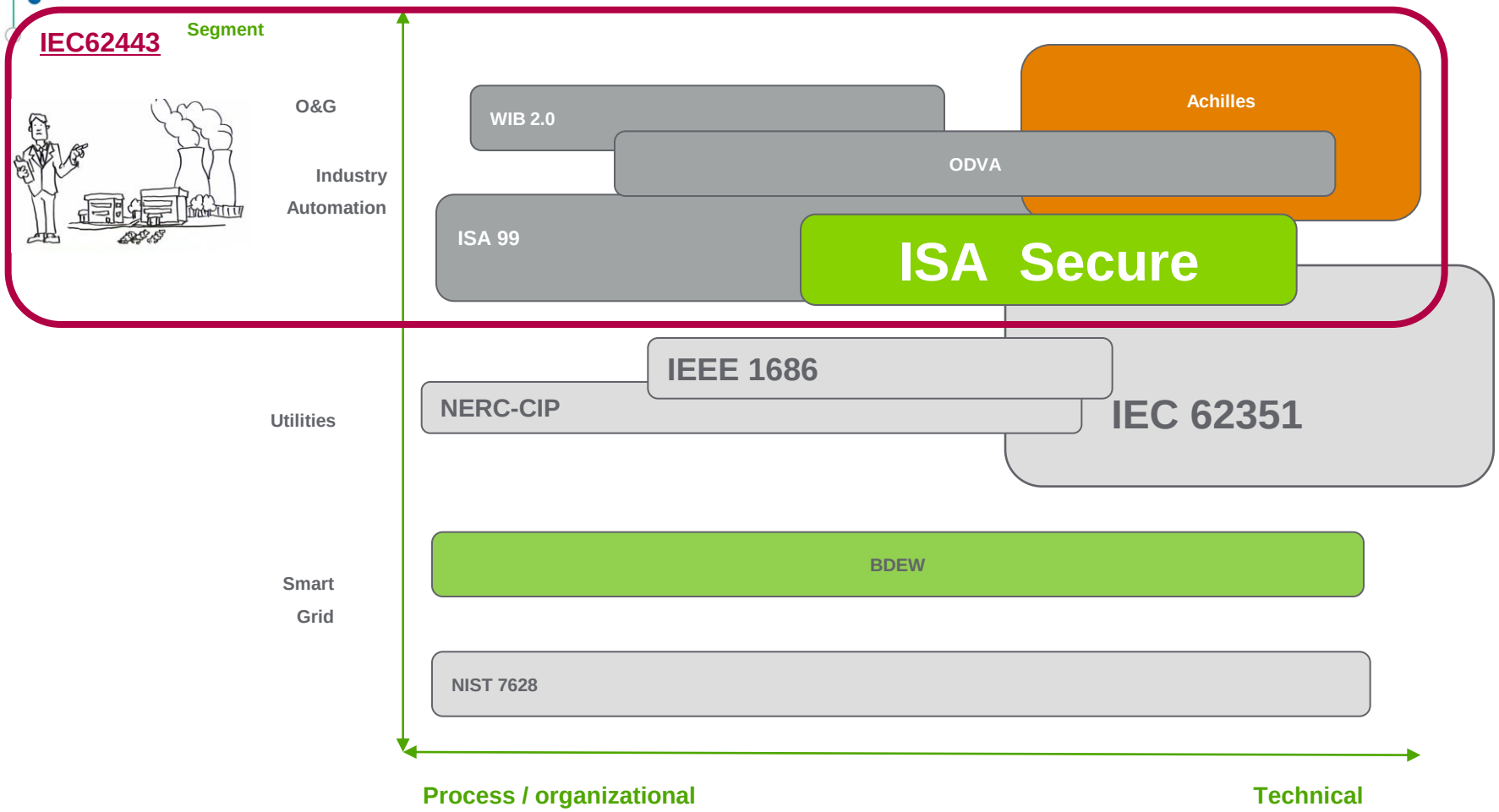
Report workshop orientati ad indicare linee guida

Italia

Marzo 2013, Decreto sulla sicurezza Informatica (Cybersecurity) è stato pubblicato sulla Gazzetta Ufficiale. Il decreto obbliga gli Operatori che gestiscono Infrastrutture critiche Nazionali ed Europee ad utilizzare le pratiche migliori per evitare violazioni a banche dati o corruzione dei processi nei sistemi industriali.

Feb2014, è stato pubblicato sulla Gazzetta Ufficiale il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", con annesso il "Piano nazionale per la protezione cibernetica e la sicurezza informatica". – "sviluppare la capacità per anticipare e prevenire eventi rari e inattesi, assicurando la continuità delle reti e dei sistemi"

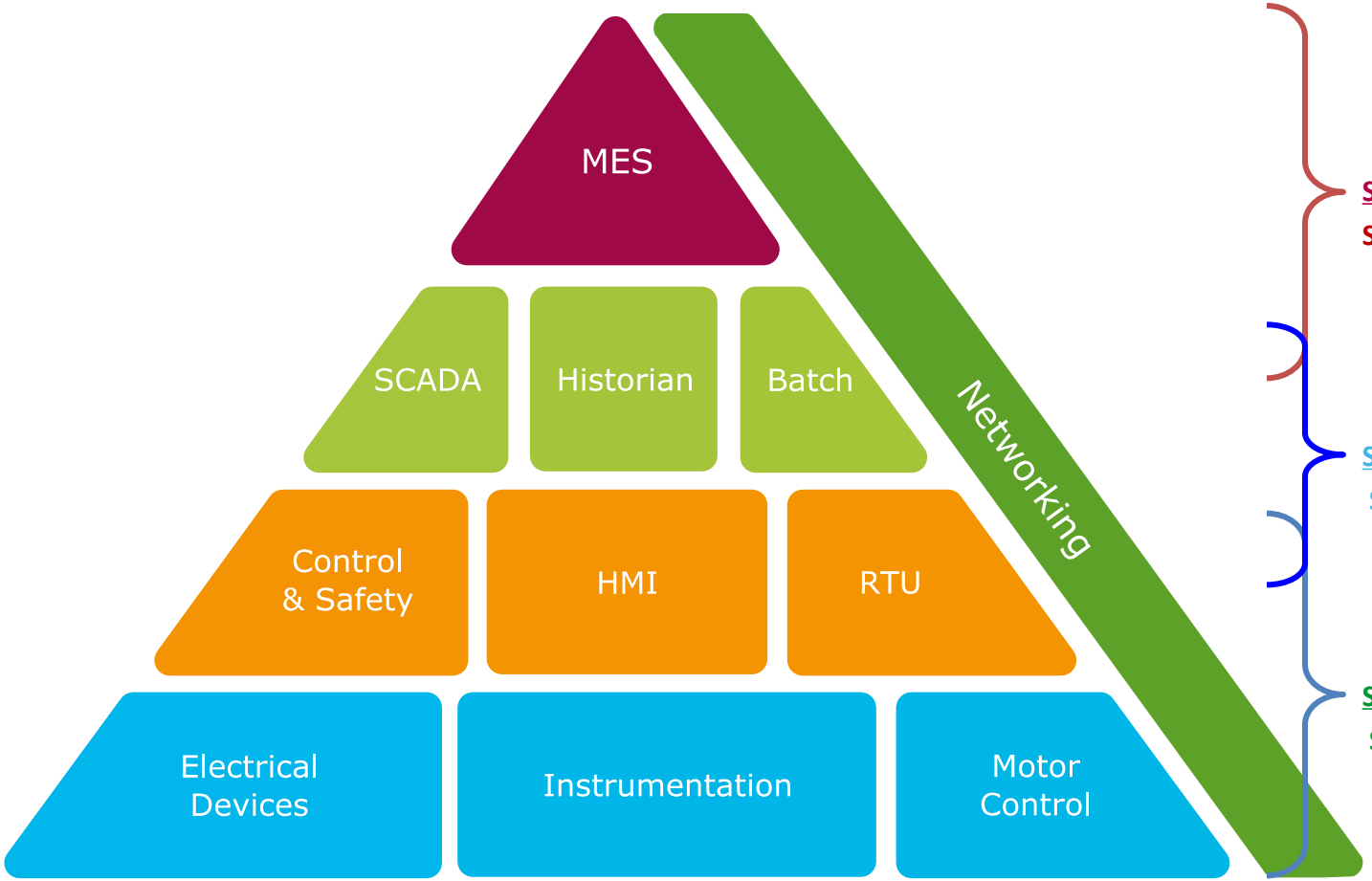
Raccomandazioni e Standard



IEC 62443

Network and system security for industrial-process measurement and control

Definizione **SAL (Security Acceptance Level)**



Security Level 3/4

Sicurezza contro attacchi intenzionali utilizzando strumenti complessi

Security Level 2

Sicurezza contro attacchi intenzionali utilizzando semplici strumenti

Security Level 1

Sicurezza contro gli errori non intenzionali

Quali i tipici attacchi intenzionali?

Attacchi su VLAN

VLAN Hopping → cattura dei dati su VLAN diverse

Double tagging VLAN → incapsulamento nascosto del tag VLAN 802.1Q

SQL Injection su SCADA → query SQL non autorizzate sfruttando la vulnerabilità del db

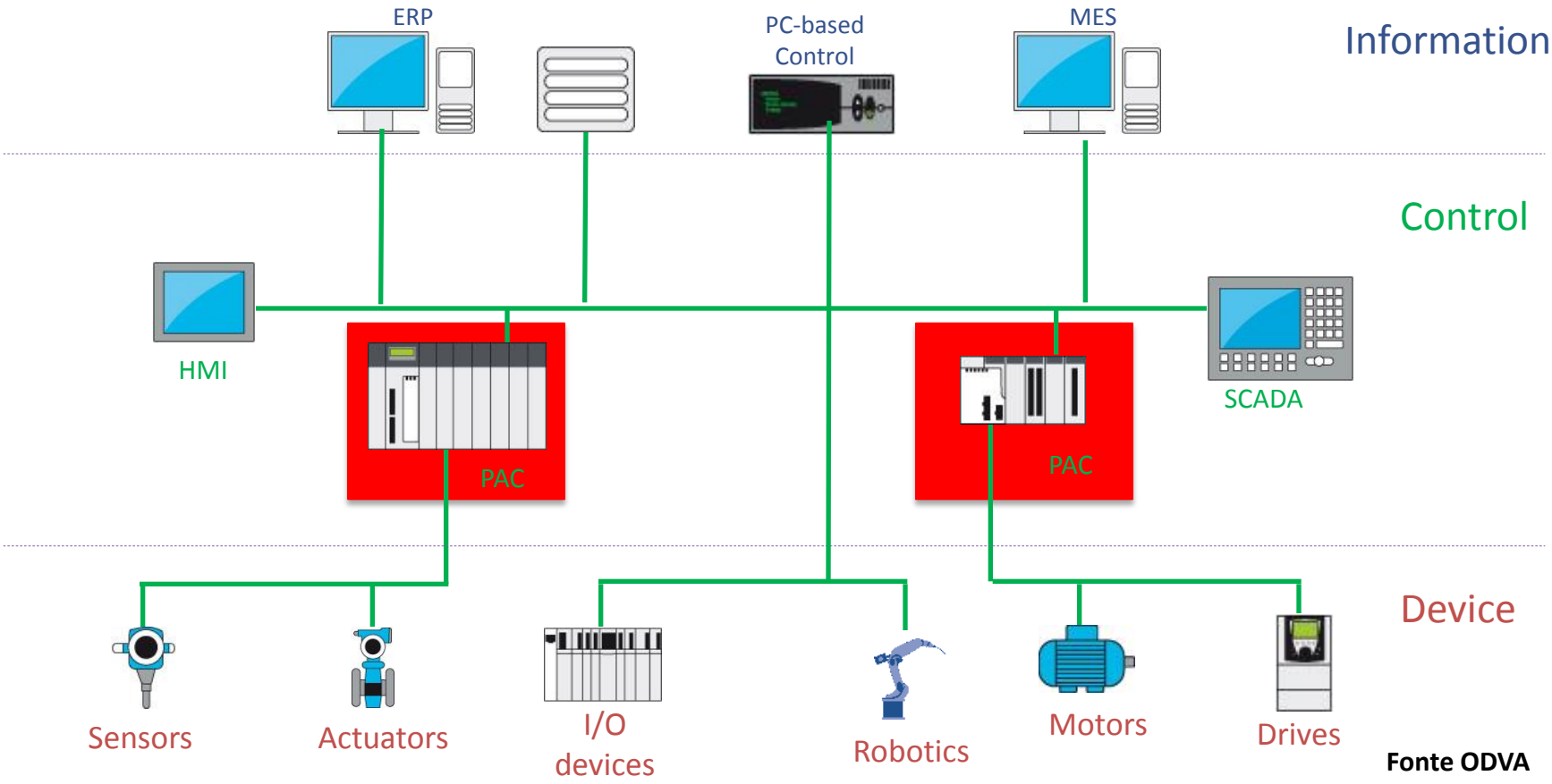
IP Spoofing → falsificazione dell'indirizzo IP del mittente

Denial of Service → saturazione deliberata delle risorse di sistema

- TCP SYN flood
- Land
- ARP spoofing
- ICMP smurf
- Ping of death
- UDP flood
- Teardrop

Il PLC come punto di contatto tra IT/OT

Architettura di rete Unificata

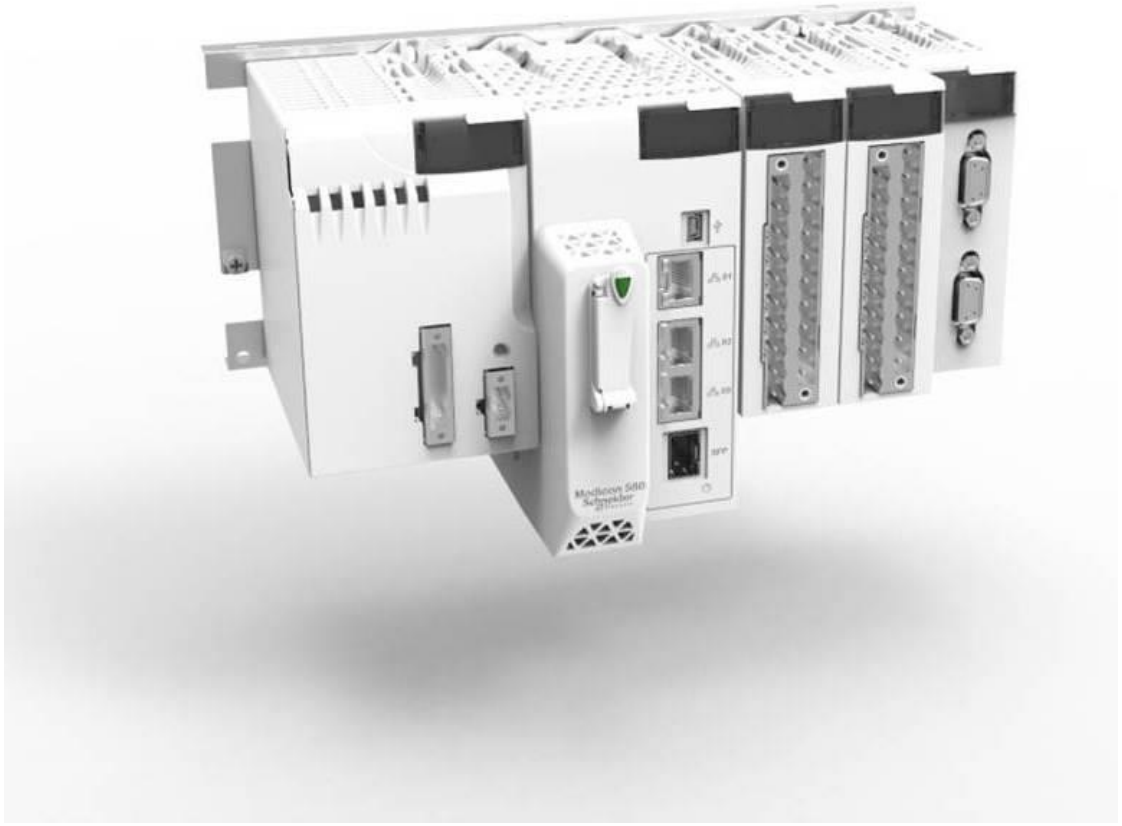


Fonte ODVA

ePAC concept

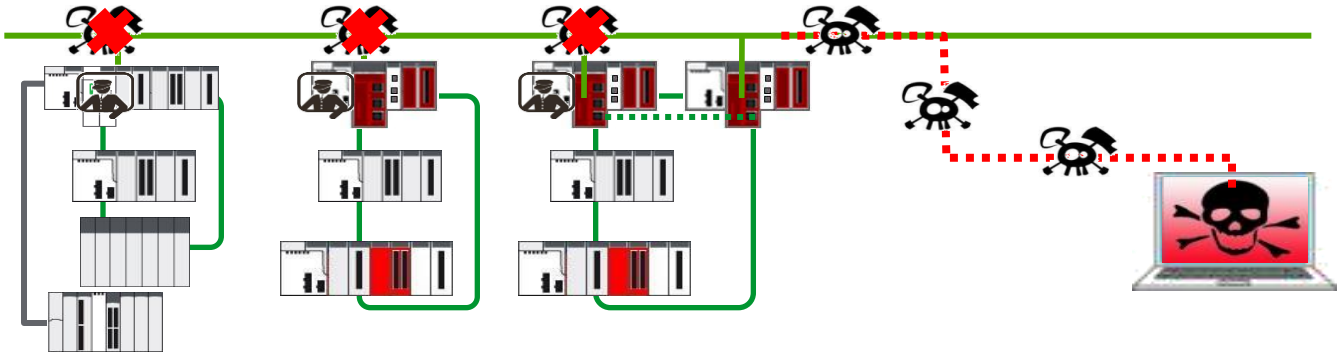
Ricordi quando esistevano…

Adesso basta il nuovo ePAC



L’ ePAC come strumento di sicurezza

PAC certificato per essere CyberSicuro



ISASecure®

achilles wurldtech

Certificazione di robustezza delle comunicazioni ed integrità di sistema

L’ ePAC cybersecurity ready

Sicura modalità di funzionamento del PLC

Modifiche di programma o di configurazione del PLC protette da password a livello PLC
RUN/STOP remoto può essere controllato da un input fisico cablato
Meccanismo di protezione della Memoria controllata tramite input fisico per prevenire qualsiasi modifica

Controllo FTP / HTTP

Disattivazione servizi quando non utilizzati anche dinamicamente da applicazione.

Integrità del firmware e dei files eseguibili

Firmware con firma digitale criptata
Integrità firmware verificata prima che venga scaricato su PLC e allo startup del controllore
Algoritmi crittografici affidabili (SHA256 – RSA4096 – AES256)
Firma elettronica (X509 =S= certificati) dei file eseguibili, delle ddl di OFS e dello strumento di sviluppo Unity PRO
Controllo integrità su richiesta o allo startup

Tracciabilità degli eventi

PLC implementa un SYSLOG client

Ogni evento di sicurezza su ogni PLC vengono rilevati e inviati ad un server SYSLOG

Esempi di eventi sicuri :

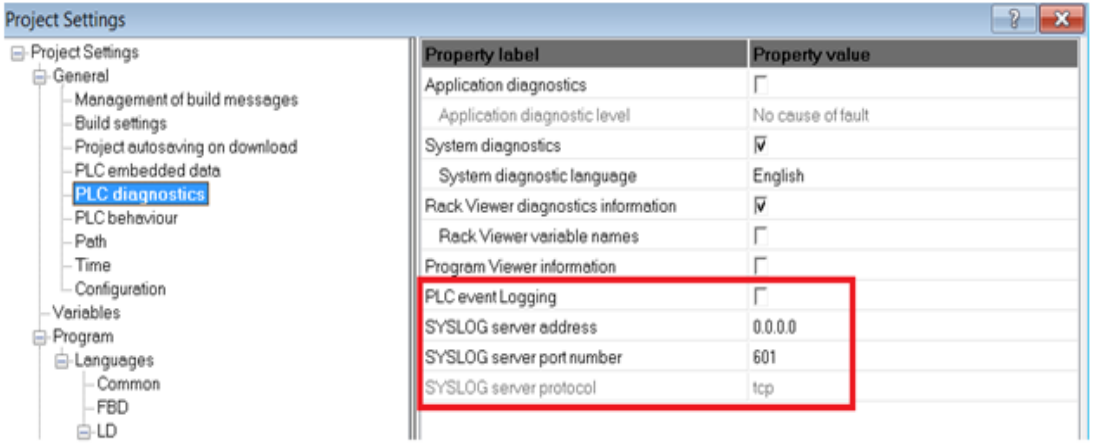
Tutte le connessioni riuscite o non riuscite

Tutte le pricipali modifiche al sistema

Applicazione PLC, Configurazione , reboot , run, stop . . . . .

. . . .

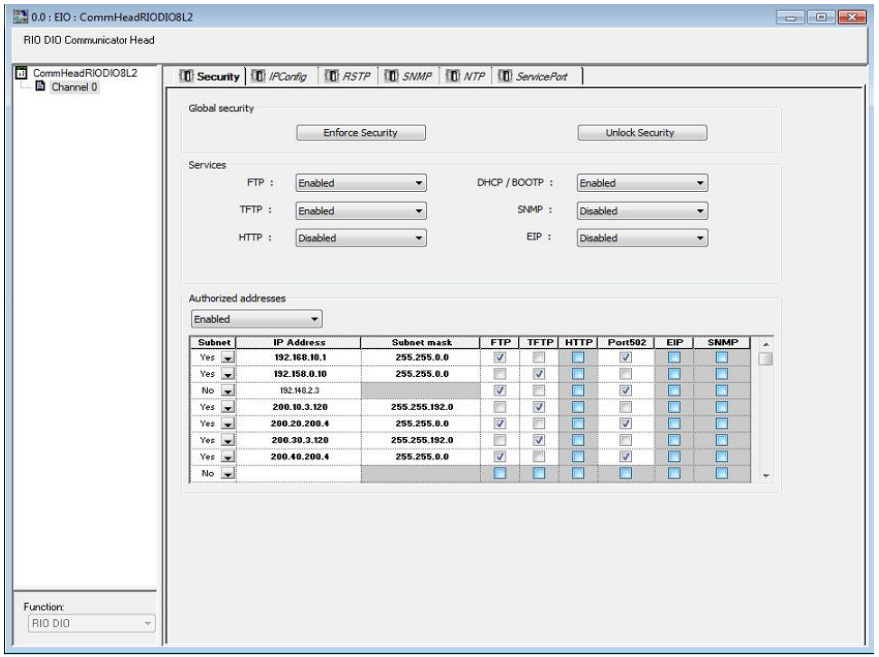
Compatibilità con i tipici SYSLOG server - Formato dell'evento sicuro: date/time/type of event / @IP



Controlli di Accesso severi

Abilitare/Disabilitare I servizi non necessari

I Servizi interessati sono:
File Transfer Protocol (FTP)
Trivial File Transfer Protocol (TFTP)
HyperText Transfer Protocol (HTTP)
Richieste DHCP/BOOTP
Simple Network Management Protocol (SNMP)



Controllo dei servizi via software associati al singolo IP

Comunicazione sicura

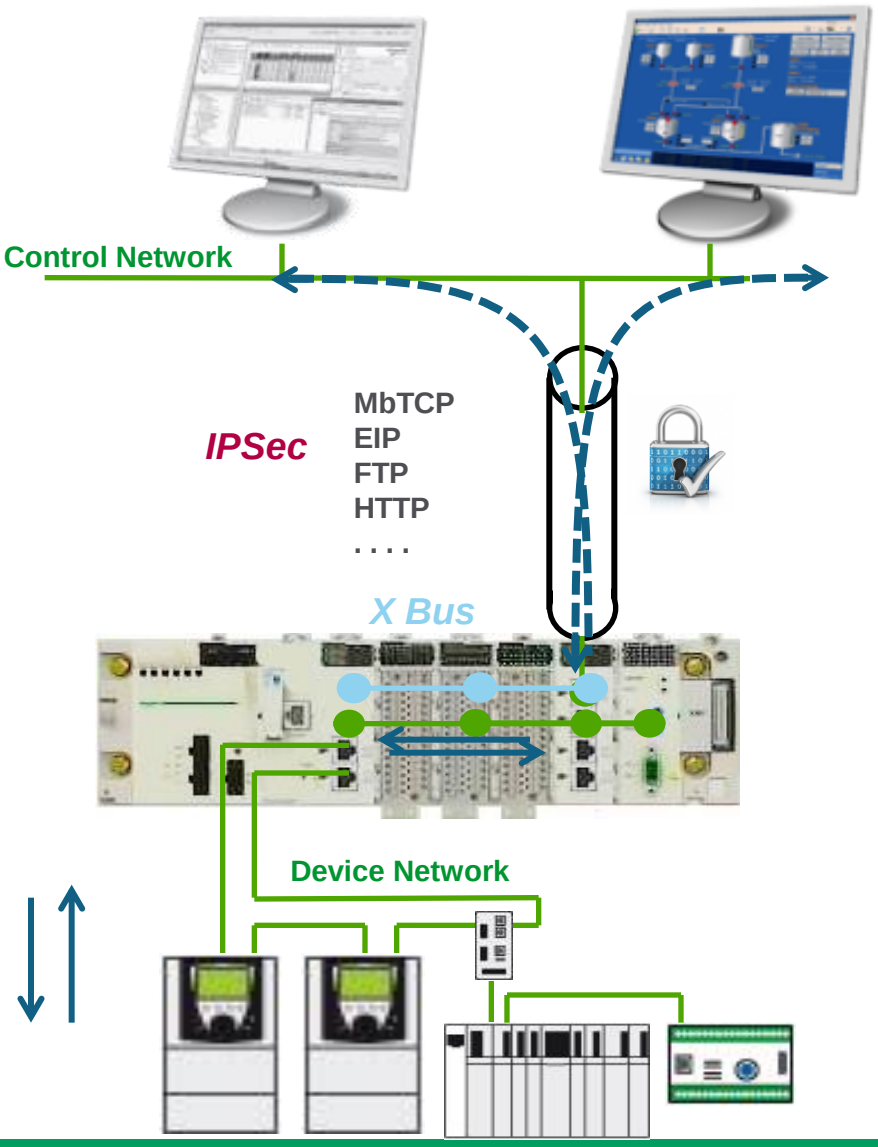
Comunicazione sicura tra Control Network e rete PLC / dispositivo garantita da protocollo IPSec

Implementato sui moduli di comunicazione

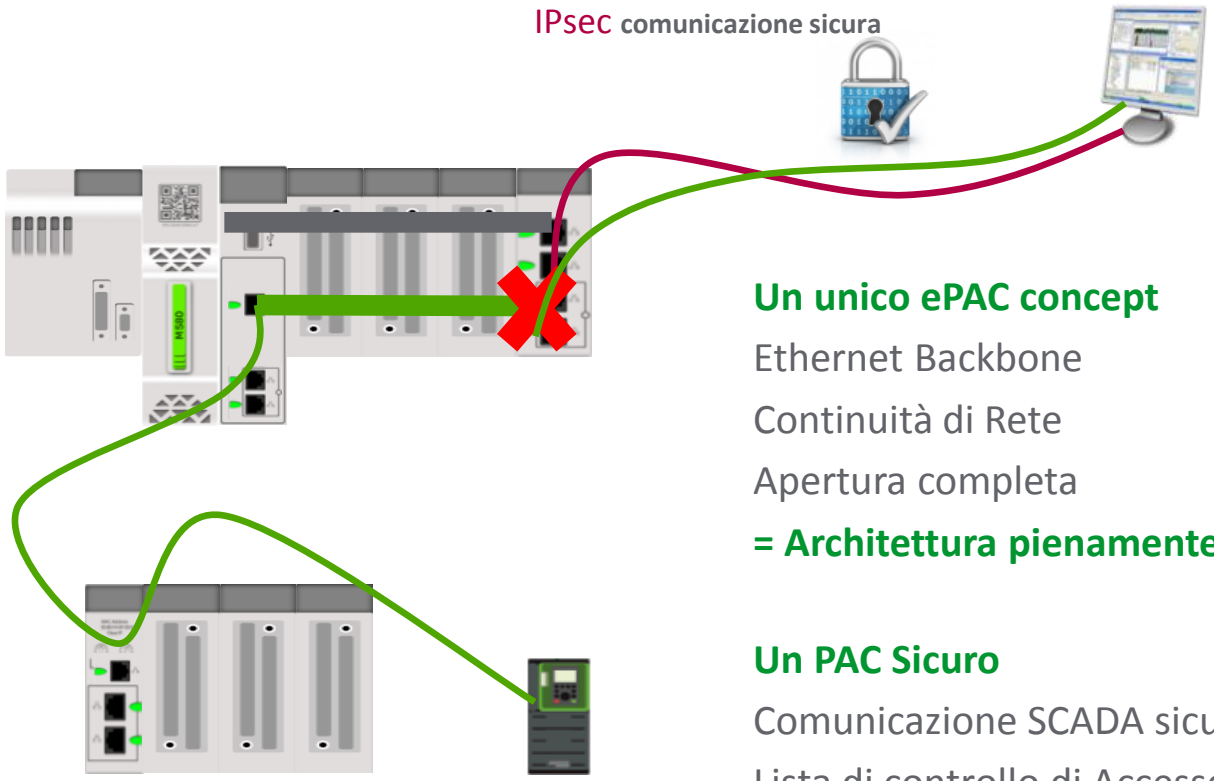
Il protocollo IPSEC fornisce protezione contro la riproduzione - autenticazione dell'origine e controllo dell'integrità dei dati (AH) - La riservatezza non è gestita

Nessun software da installare lato client: possibilità di appoggio al servizio IPSec di Windows (da definire come strategia di politica di sicurezza)

Impatto misurato sulle performances di comunicazione dello SCADA :
+ 10ms per leggere 10000 variabilli



Dualismo tra Transparenza e Sicurezza



Un unico ePAC concept

Ethernet Backbone

Continuità di Rete

Apertura completa

= Architettura pienamente Trasparente

Un PAC Sicuro

Comunicazione SCADA sicura

Lista di controllo di Accesso Access per indirizzo IP & servizio

Password di sicurezza Applicazione

Firma digitale e crittografia per Firmware e software

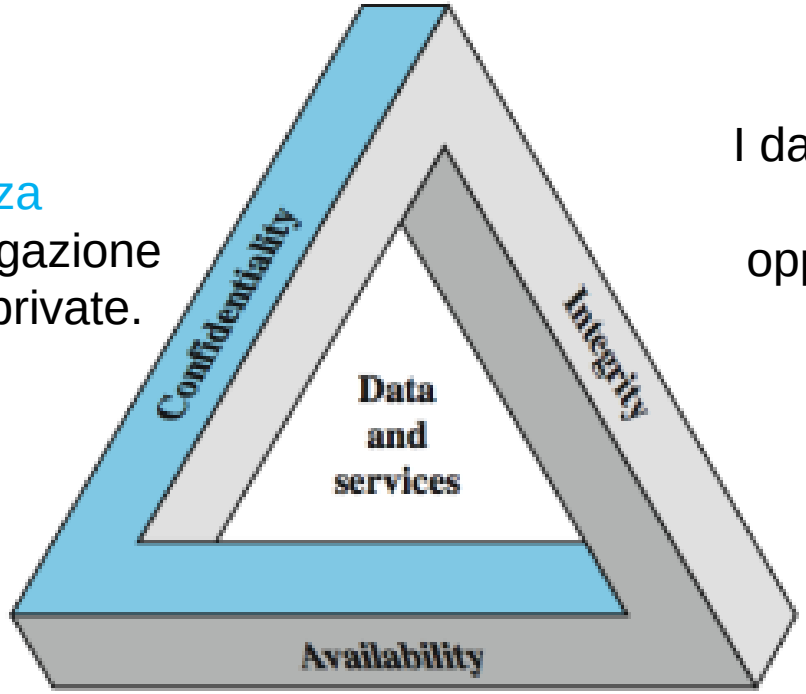
= Architettura pienamente Sicura

Cyber Security?

Quali sono i KPI per proteggere i beni e le attività economiche attraverso la protezione delle informazioni?

Riservatezza

Impedire la divulgazione di informazioni private.



Integrità

I dati non possono essere modificati senza opportune autorizzazioni

Disponibilità

L'informazione sempre disponibile quando necessaria.

Conclusioni

Nessun singolo componente fornisce una adeguata difesa.
Solo una combinazione di prodotti sicuri e giuste pratiche sono in grado di mitigare il rischio.