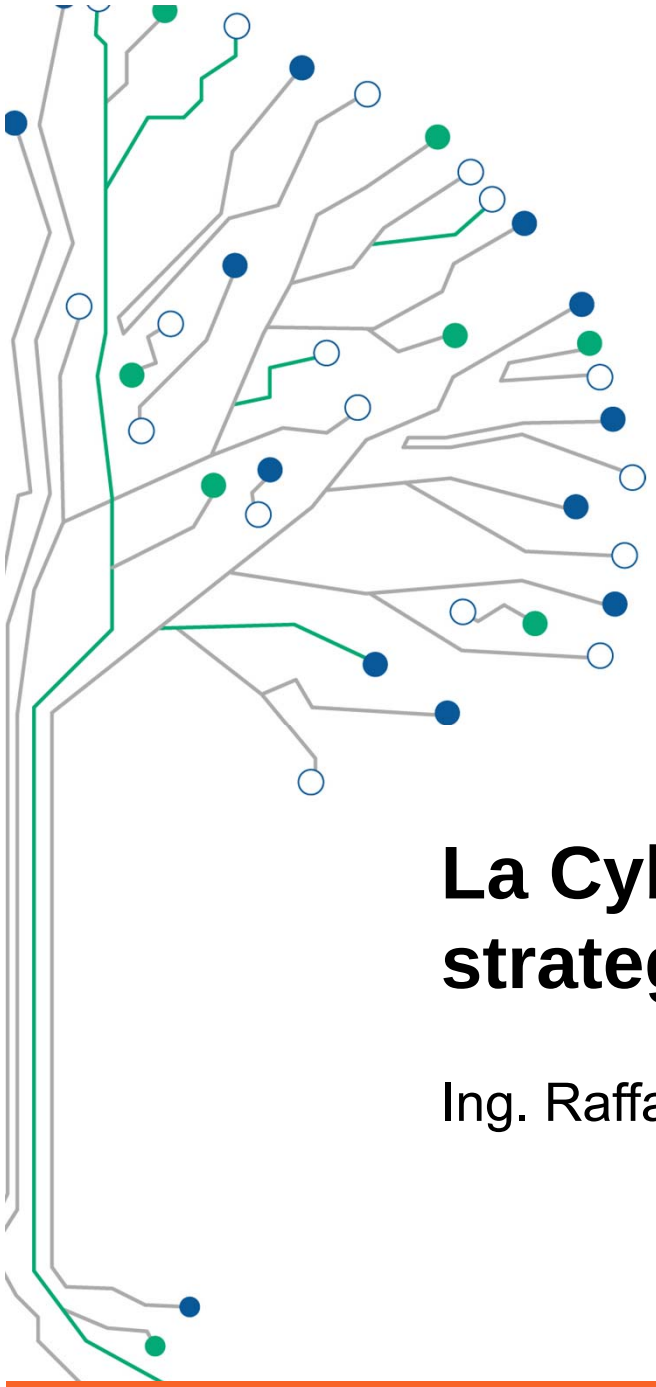


ANIE AUTOMAZIONE

ANIE FEDERAZIONE

CONFINDUSTRIA

La Cyber Security quale elemento strategico dell'approccio Industry 4.0

Ing. Raffaele Esposito

PHOENIX CONTACT

Industry 4.0

Le necessità di flessibilità ed efficienza produttiva sono soddisfatte dal mondo dell'industria attraverso l'uso sempre più ampio e consapevole di tecnologie digitali in senso lato

Tali tecnologie hanno modificato radicalmente approcci, strumenti e modalità operative del mondo industriale con un impatto che può essere assimilato a quelle delle passate Rivoluzioni Industriali

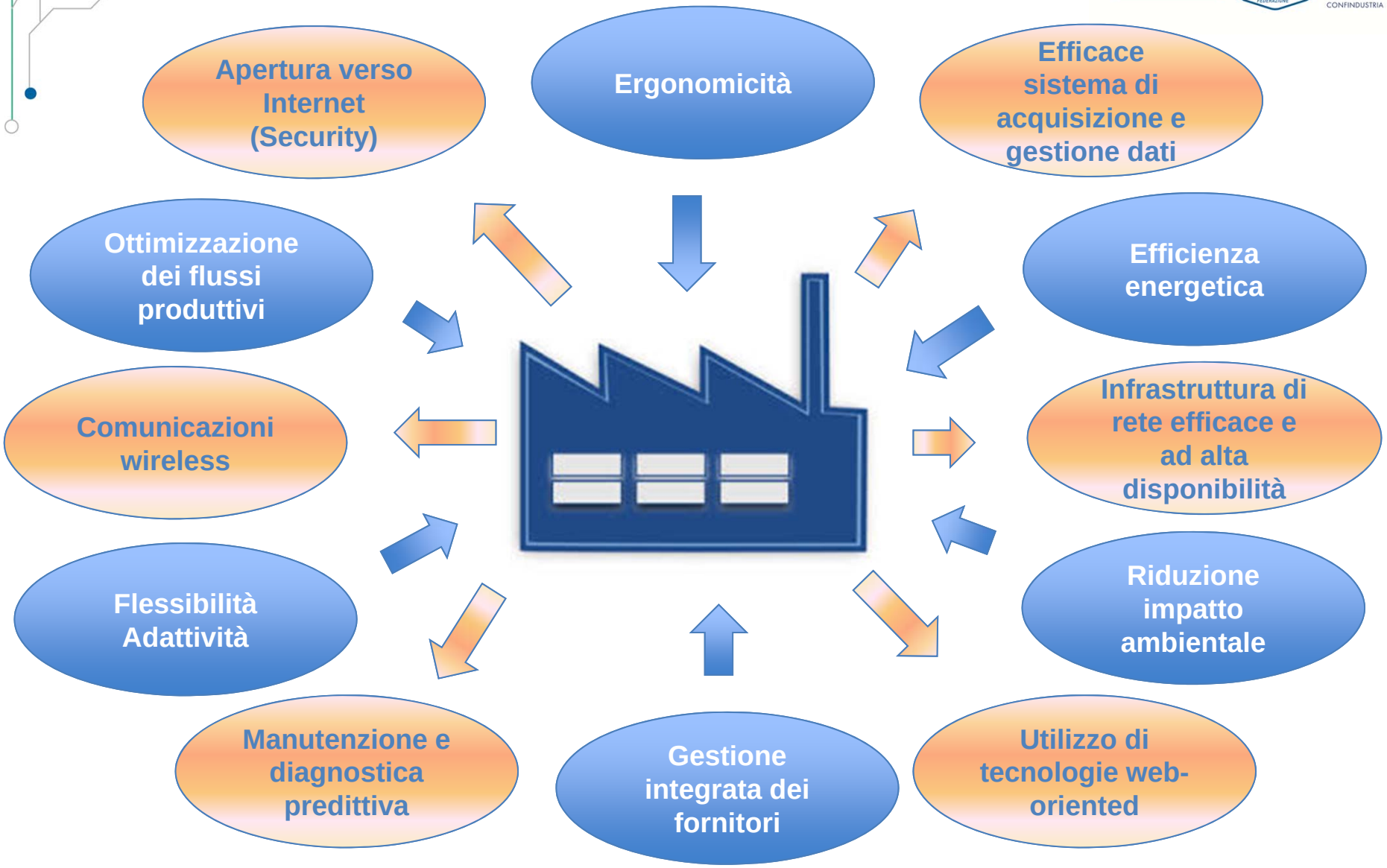
Si tratterebbe della quarta (dopo quelle caratterizzate dall'uso a fini produttivi del vapore, dell'elettricità e dell'energia nucleare), da qui il termine ''Industry 4.0'' utilizzato per la prima volta a livello ministeriale tedesco

Industry 4.0

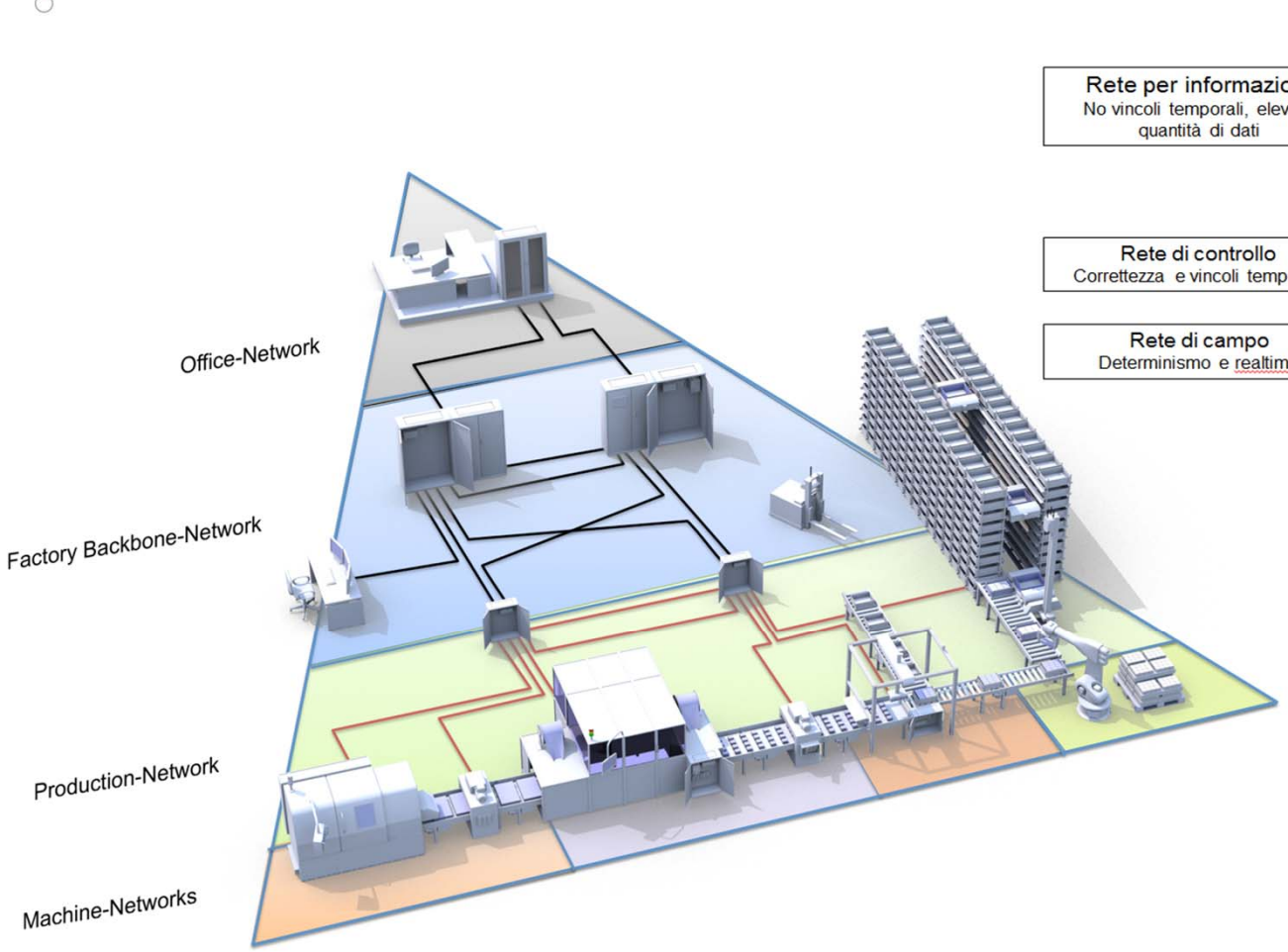
Industry 4.0 si basa sui cosiddetti ‘’sistemi virtuali-reali’’ (Cyber Physical Systems), vale a dire sistemi ad alta complessità costituiti da componentistica intelligente basata su varie tecnologie quali ad esempio la meccanica, l’elettronica, l’informatica e che, in genere, sono posti tra loro in comunicazione attraverso una rete, spesso costituita da Internet

Varie le definizioni utilizzate per identificare soluzioni o concetti tecnologici che costituiscono le colonne portanti di Industry 4.0: si pensi ad esempio ai concetti di Internet of Thing, Smart Factory, Smart Grid, Cloud, …

La Smart Factory



Apertura verso Internet (Security)



Rete per informazioni
No vincoli temporali, elevata quantità di dati

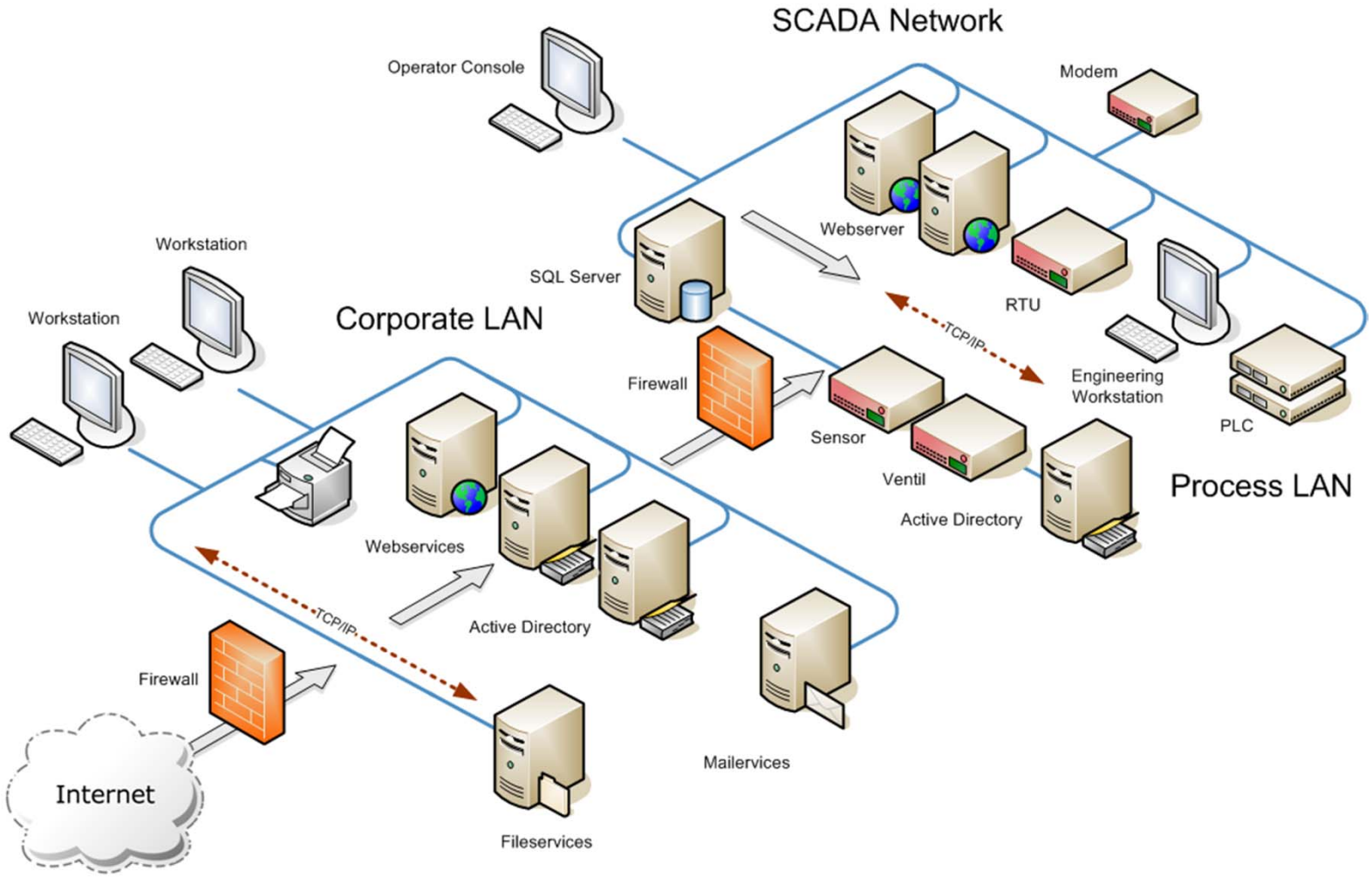
Rete di controllo
Correttezza e vincoli temporali

Rete di campo
Determinismo e realtime

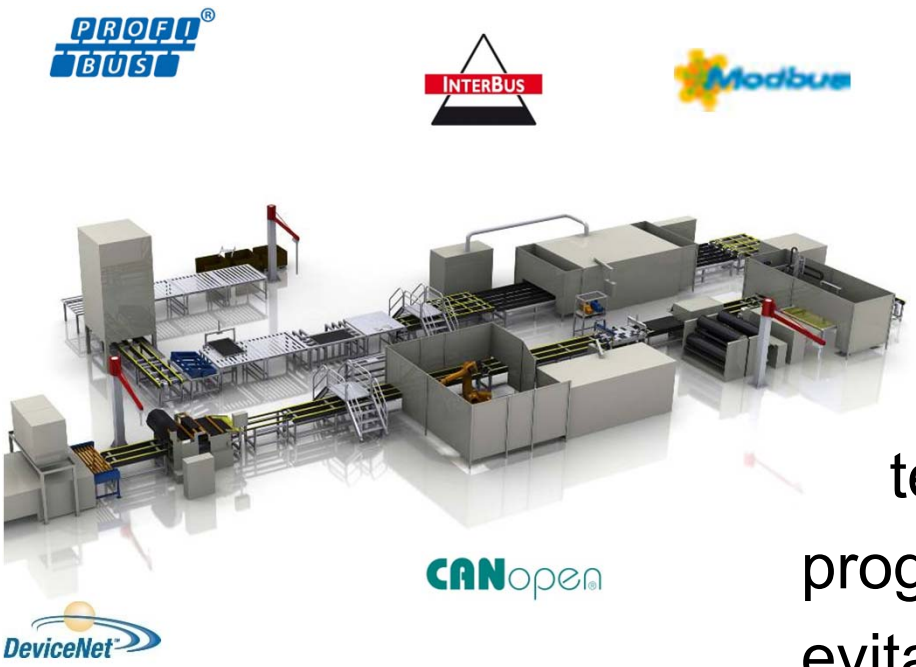
comandi

informazioni

Apertura verso Internet (Security)

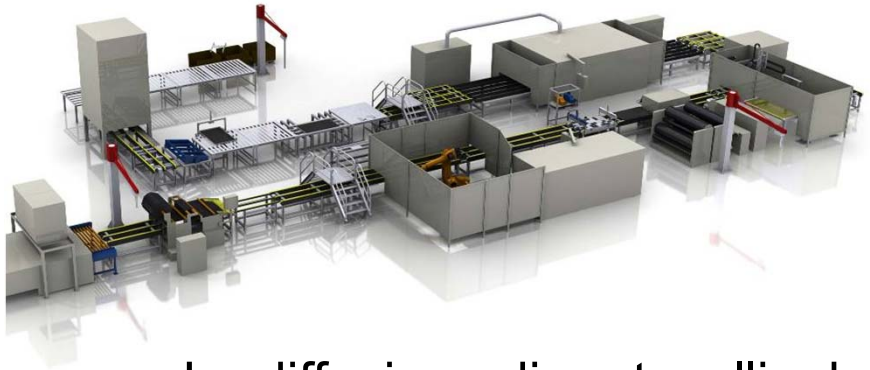


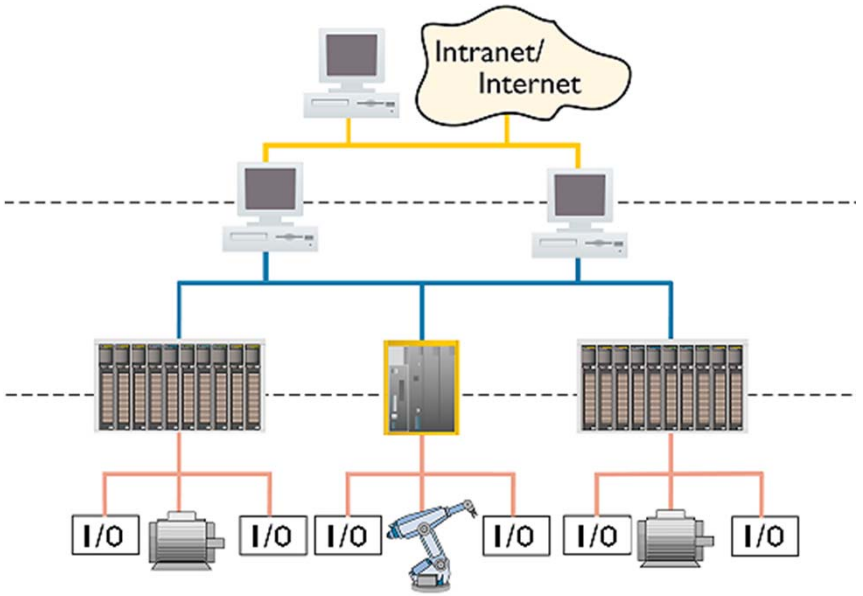
La Security



Con fieldbus strettamente limitato all'applicazione di automazione ci si preoccupava solo di evitare possibili accessi tendenti a modificare il progetto installato al fine di evitare modifiche di responsabilità dell'installatore o del produttore del macchinario

La Security





La diffusione di protocolli a base Industrial Ethernet ha ancor più favorito l'integrazione della rete di macchina nella piramide di comunicazione con scambi da/verso sistemi ERP/MES e con l'accesso a tale rete anche da remoto: la Security diventa un'esigenza imprescindibile anche per i progettisti di automazione industriale

La Security nel Factory

Vantaggi legati all'integrazione:

- Uso di sistemi ERP e MES
- Accesso da remoto (teleassistenza e telecontrollo)

Possibili conseguenze di un attacco:

- Sistemi produttivi non affidabili
- Perdita di produzione
- Danni a persone e a cose
- Perdita di dati sensibili

La Security nel Process

Vantaggi legati all'integrazione:

- Uso di sistemi ERP e MES
- Maggior semplicità nel rispetto di norme e legislazioni
- Accesso al sito da parte di fornitori e sub-contactor

Possibili conseguenze di un attacco:

- Sistemi produttivi non affidabili
- Perdita di produzione
- Danni a persone e a cose con eventuali importanti conseguenze anche all'eco-sistema
- Perdita di dati sensibili

La Security nell'Energy

Vantaggi legati all'integrazione:

- Acquisizione permanente di dati dal campo
- Maggior semplicità nel rispetto di norme e legislazioni
- Accesso al sito da parte di fornitori e sub-contactor

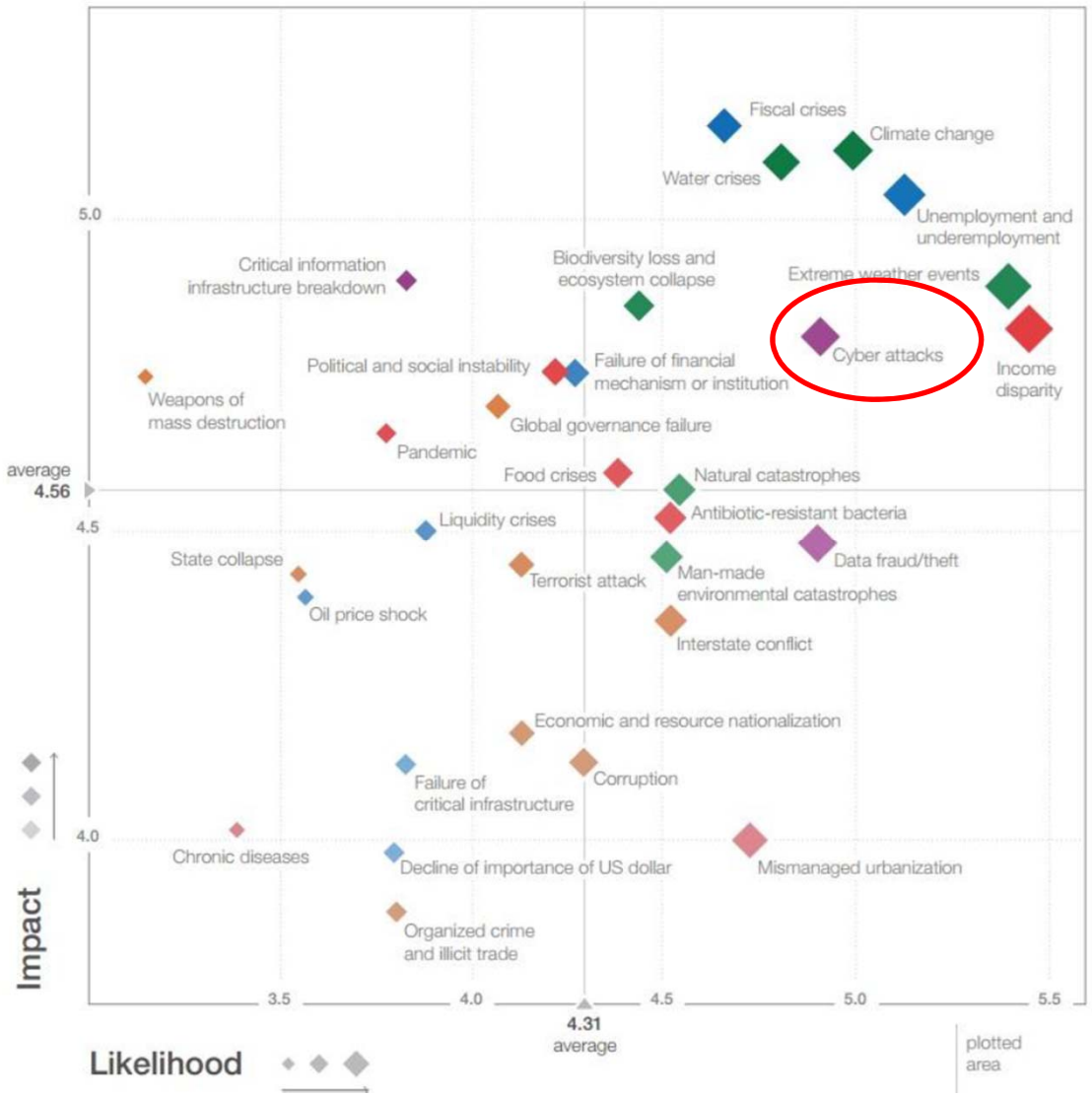
Possibili conseguenze di un attacco:

- Mancata affidabilità di infrastrutture strategiche
- Danni a persone e a cose con eventuali importanti conseguenze anche all'eco-sistema

Security

Al World Economic Forum 2014:

«***Cyber Attacks*** *considerati uno dei* ***rischi più elevati*** *per l'economia in termini di IMPATTO e PROBABILITA'»*



Security: stima dei costi

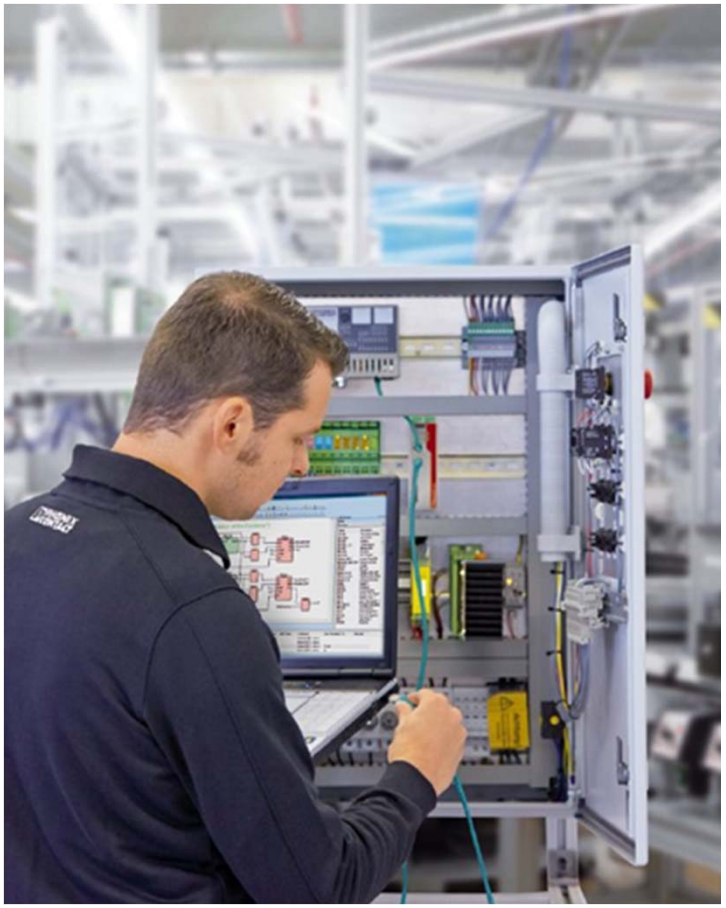
1	**Perdita dei dati:** Improvvisamente tutti vostri dati vengono persi. Quale potrebbe essere il costo della ricostruzione di tali dati?	Euro _____
2	**Perdita di know-how:** Un vostro competitor riesce ad accedere ai vostri dati sensibili (progettazione, ingegnerizzazione, ...). Quanto può economicamente valere il danno?	Euro _____
3	**Fermi di produzione:** A causa di problemi legati alla security, la produzione deve arrestarsi per alcune ore, Quanto può essere il costo di una tale mancata produzione?	Euro _____
4	**Ore lavoro dei vostri dipendenti:** Quante ore lavoro dei vostri dipendenti sarebbe necessario impiegare per risolvere i danni generati da una falla nelle vostre misure di security?	Euro _____
5	**Hijacking dai vostri computer:** Quanto potrebbe costare una campagna di comunicazione per spiegare che una terza parte ha usato i vostri sistemi per spiare o attaccare un'altra società?	Euro _____
6	**Reputazione:** Quanto potrebbe essere importante un danno alla vostra reputazione se i vostri clienti non riponessero in voi la giusta fiducia circa la protezione da Cyber attacchi?	Euro _____

Totale: Euro _____

I rischi

Se la rete Ethernet locale (LAN) non è connessa a Internet molti ritengono che non vi siano motivazioni valide per investire in soluzioni tecnologiche o prodotti atti a garantire la Security

Dipendenti o tecnici esterni che accedono alla rete potrebbero introdurre malware all'interno della stessa per mezzo di memorie USB o attraverso PC di servizio



I rischi

Il ciclo di vita di una macchina o di un'installazione è spesso superiore ai 20 anni

I produttori di sistemi operativi potrebbero dismettere il supporto per tali sistemi prima del termine del ciclo di vita della macchina (si pensi a Windows XP)

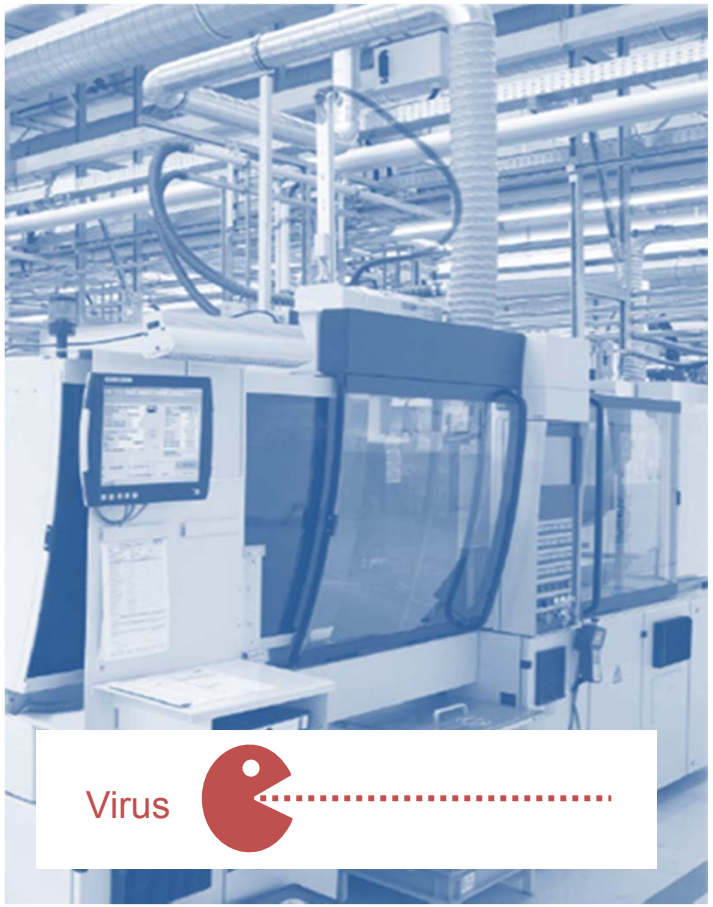
La invulnerabilità dei sistemi non viene più garantita e i rischi associati alla Security aumentano

I rischi

Programmi antivirus (virus scanner) vengono utilizzati dagli IPC per proteggere il sistema produttivo

I programmi antivirus standard possono impattare in modo significativo le proprietà ‘’real time’’ dell’installazione

Il caricamento di archivi per riconoscimento virus cambia permanentemente il sistema



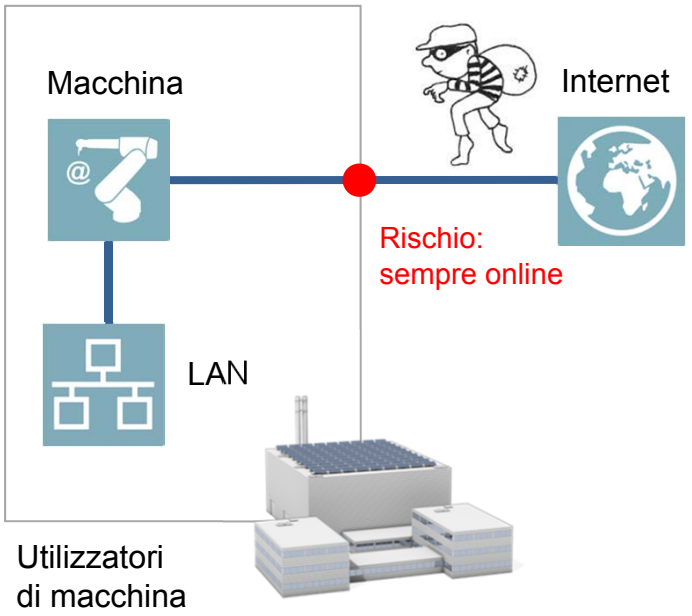
I rischi

In caso di accesso da remoto, i dati spesso vengono trasferiti via Internet senza essere stati preventivamente cifrati (encryption)

In funzione della rete, i pacchetti dati vengono trasferiti via Internet attraverso diversi percorsi e paesi
Pacchetti dati non cifrati possono essere letti e modificati da un qualsiasi soggetto ovunque nel mondo senza che chi invia I dati e chi riceve gli stessi possa avere la percezione di queste azioni

I rischi

Macchine o installazioni vengono spesso mantenute connessa a Internet in modo continuativo (24/7) attraverso un'economica tariffa ''Internet flat''

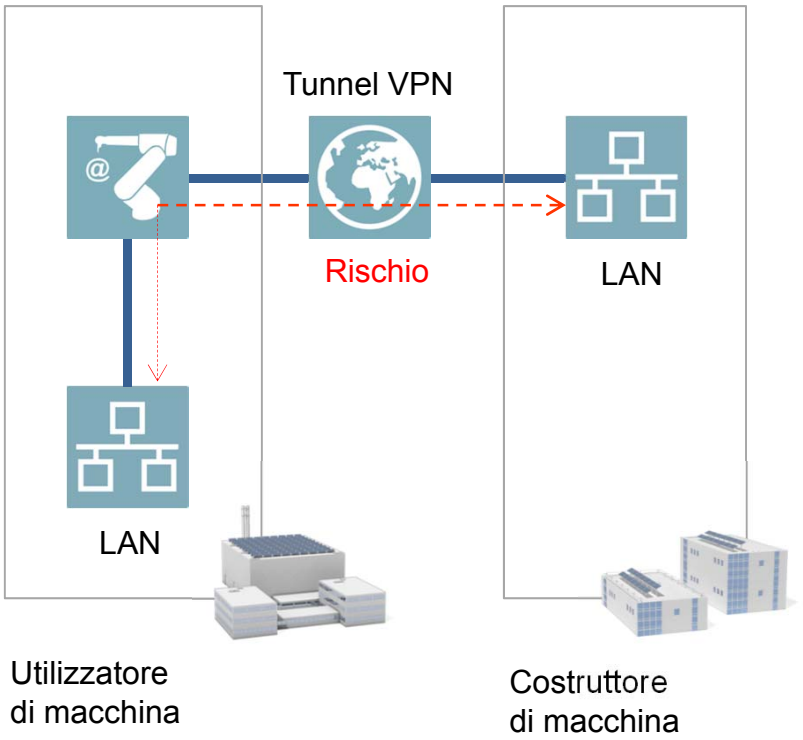


Gli hackers hanno abbastanza tempo per trovare la macchina in Internet e per svolgere svariate tipologie di attacchi alla stessa

I rischi

La comunicazione da remoto viene eseguita attraverso un tunnel VPN sicuro e non vengono quindi adottate ulteriori misure di Security

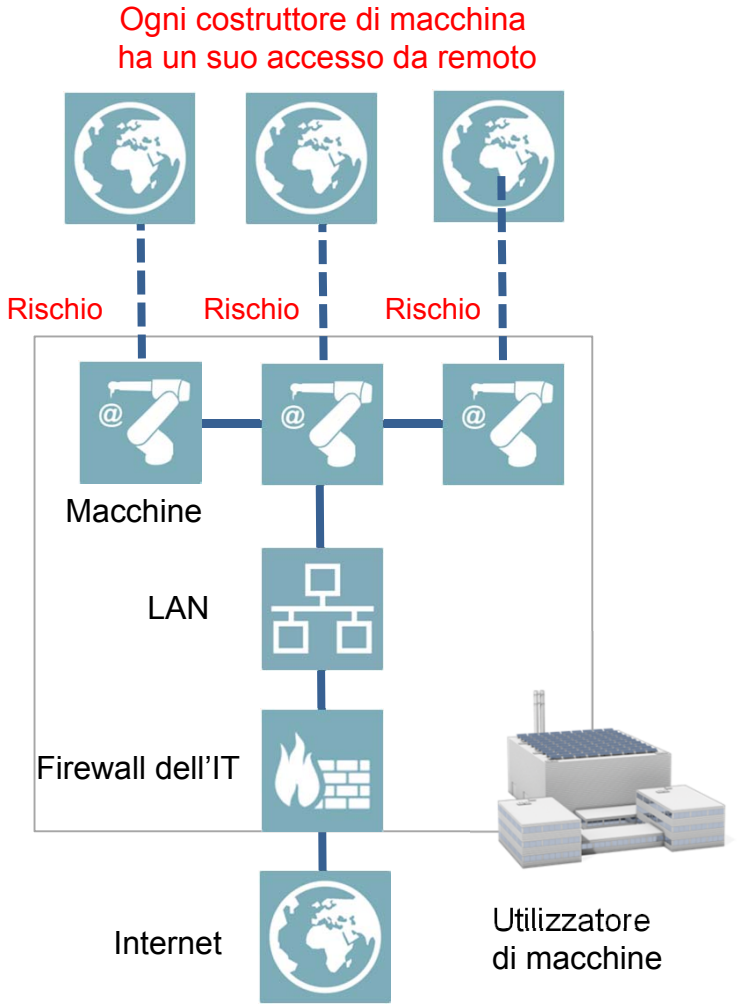
I costruttori di macchine e gli utilizzatori delle stesse sono in comunicazione tra loro attraverso un tunnel VPN ma dei malware potrebbero comunque viaggiare attraverso tale tunnel andando a infettare una delle reti disposte ai due estremi del tunnel stesso



I rischi

L'utilizzatore finale dell'impianto dispone di una rete globale che integra anche le reti disposte su macchine acquistate da diversi fornitori e ogni fornitore ha un accesso da remoto alla ''propria'' macchina

Ogni singola macchina è una potenziale fonte di rischi associati alla Security
Ogni singola rete di macchina può essere infettata o spiata attraverso le reti di tutte le altre macchine



I rischi

I tecnici di assistenza sono in trasferta spesso per alcuni giorni consecutivi

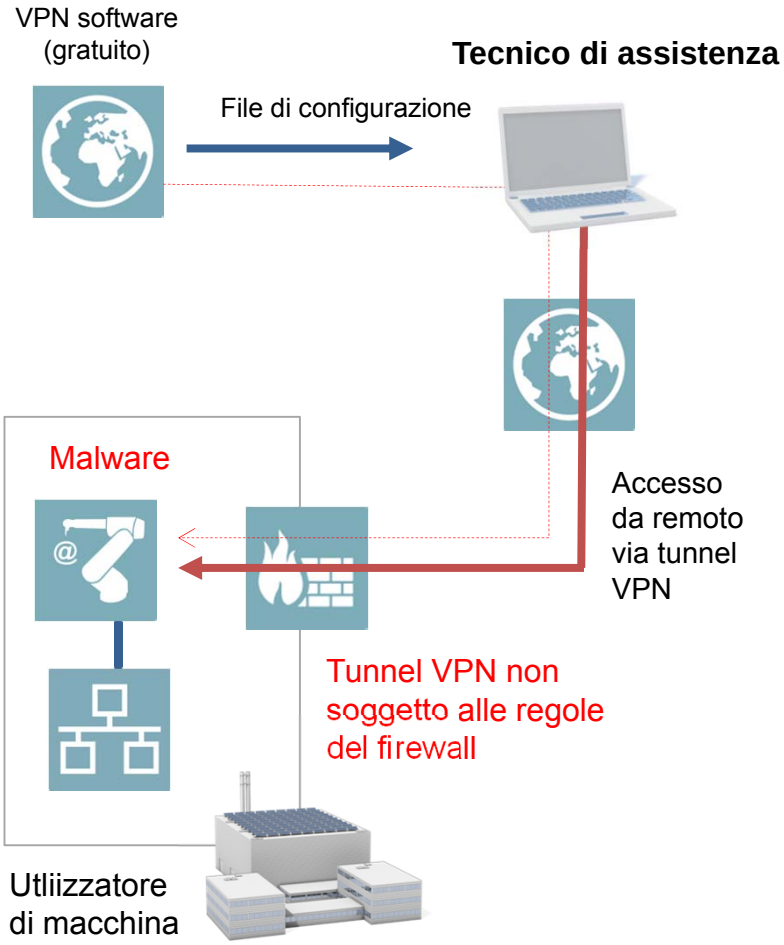
Normalmente usano il loro PC di servizio per collegarsi a Internet la sera in hotel

Il PC di servizio viene di fatto utilizzato molto spesso per fini non professionali
Questo incrementa la possibilità di infezioni del PC che verrebbero a ripercuotersi sull'installazione cui poi il PC verrebbe collegato

I rischi

Spesso i tecnici di assistenza usano VPN software gratuitamente disponibili in Internet per creare una connessione via tunnel VPN dalla macchina

I VPN software disponibili in Internet non possono essere considerati sicuri
Degli Hacker potrebbero servirsi proprio del tunnel VPN così creato per accedere alla rete
Il tunnel VPN non è normalmente soggetto alle regole di firewall



I rischi

I tecnici di assistenza più professionali usano PC dedicati e con VPN software adeguati

Le password per accedere alle varie macchine possono essere salvate all'interno di questi PC

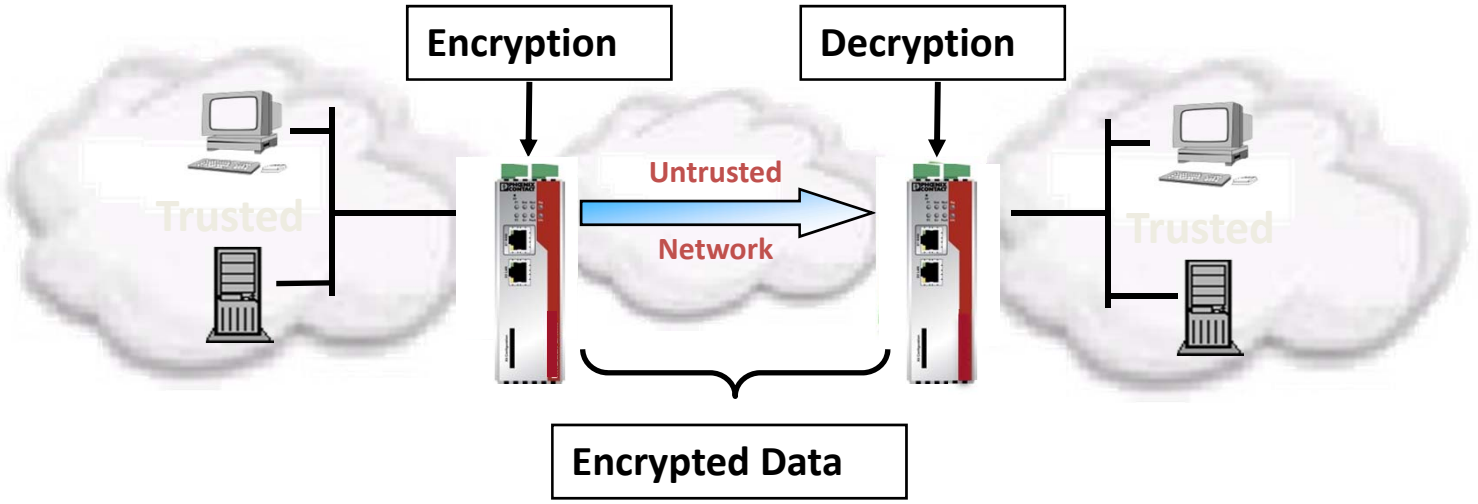
Se il tecnico di assistenza subisce il furto del proprio PC di servizio o se il tecnico cambia lavoro dopo essersi creato una copia di queste password, è necessario cambiare le password di accesso a tutte le macchine potenzialmente coinvolte

Rubato

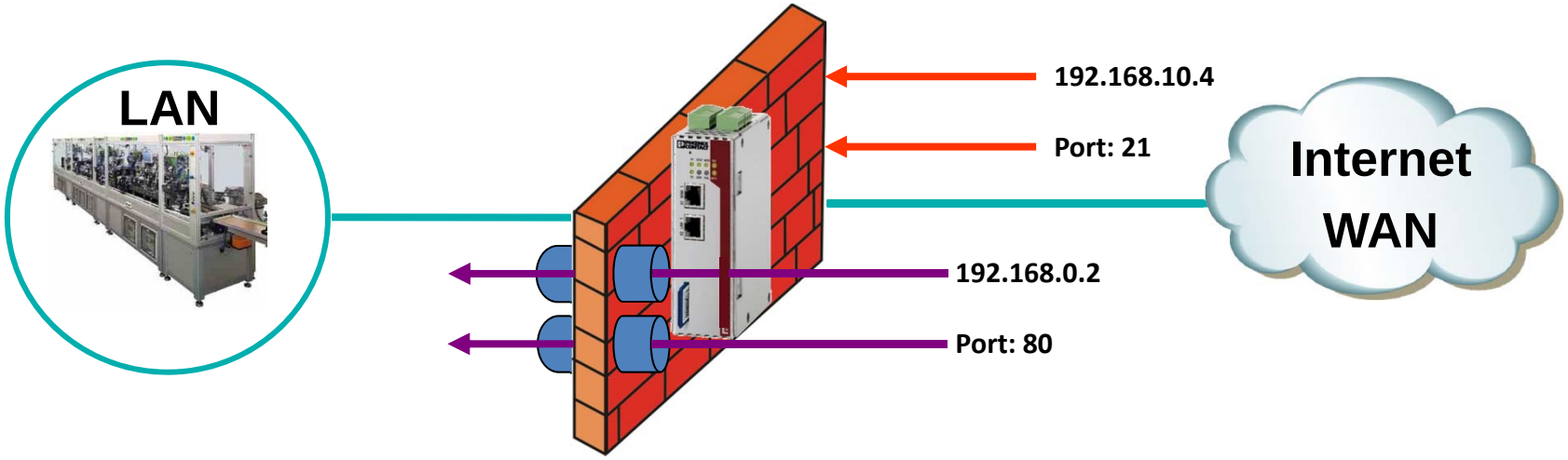
PC con tutti i dati di accesso alle macchine

Le soluzioni:
Security Firewall/Router

Un tunnel VPN consente una comunicazione crittografata e quindi sicura attraverso una rete esterna (WAN) "insicura" (ad esempio Intenet).

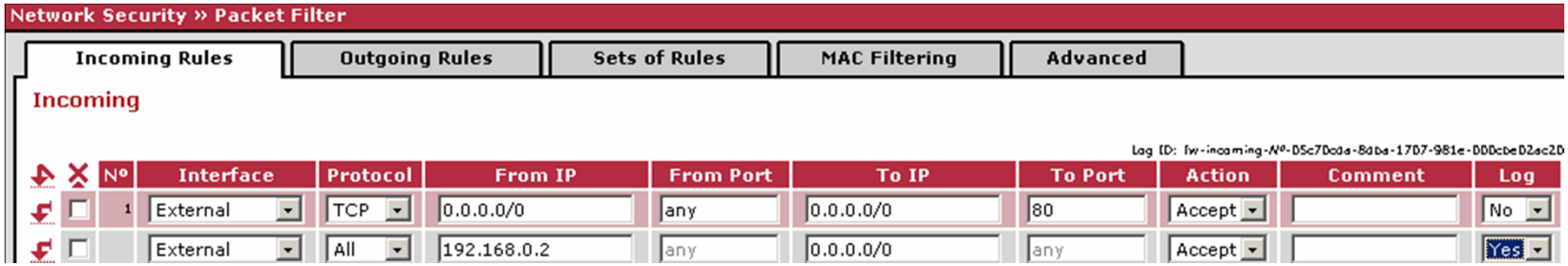


Le soluzioni:
Security Firewall/Router

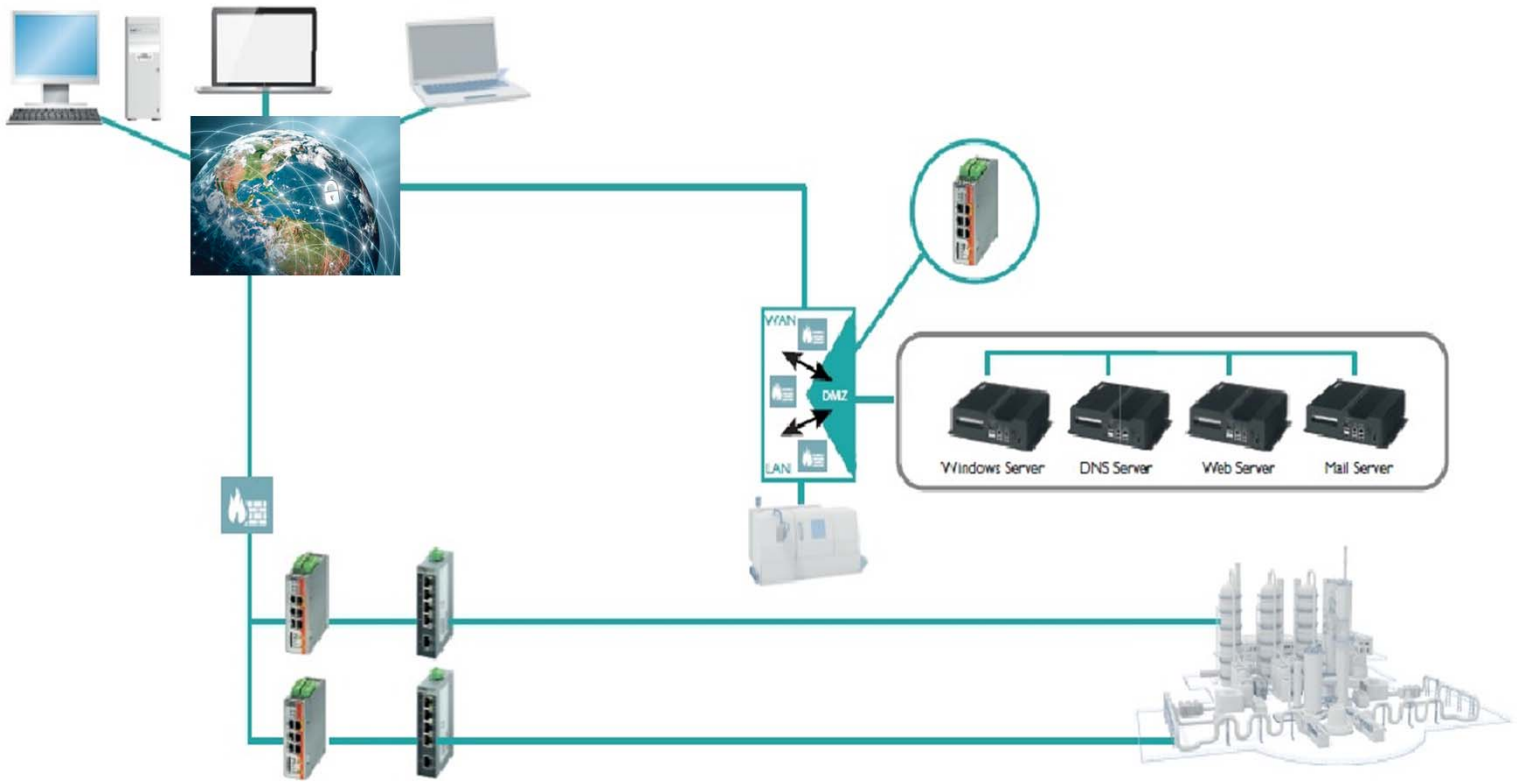


Defined Firewall-Rules:

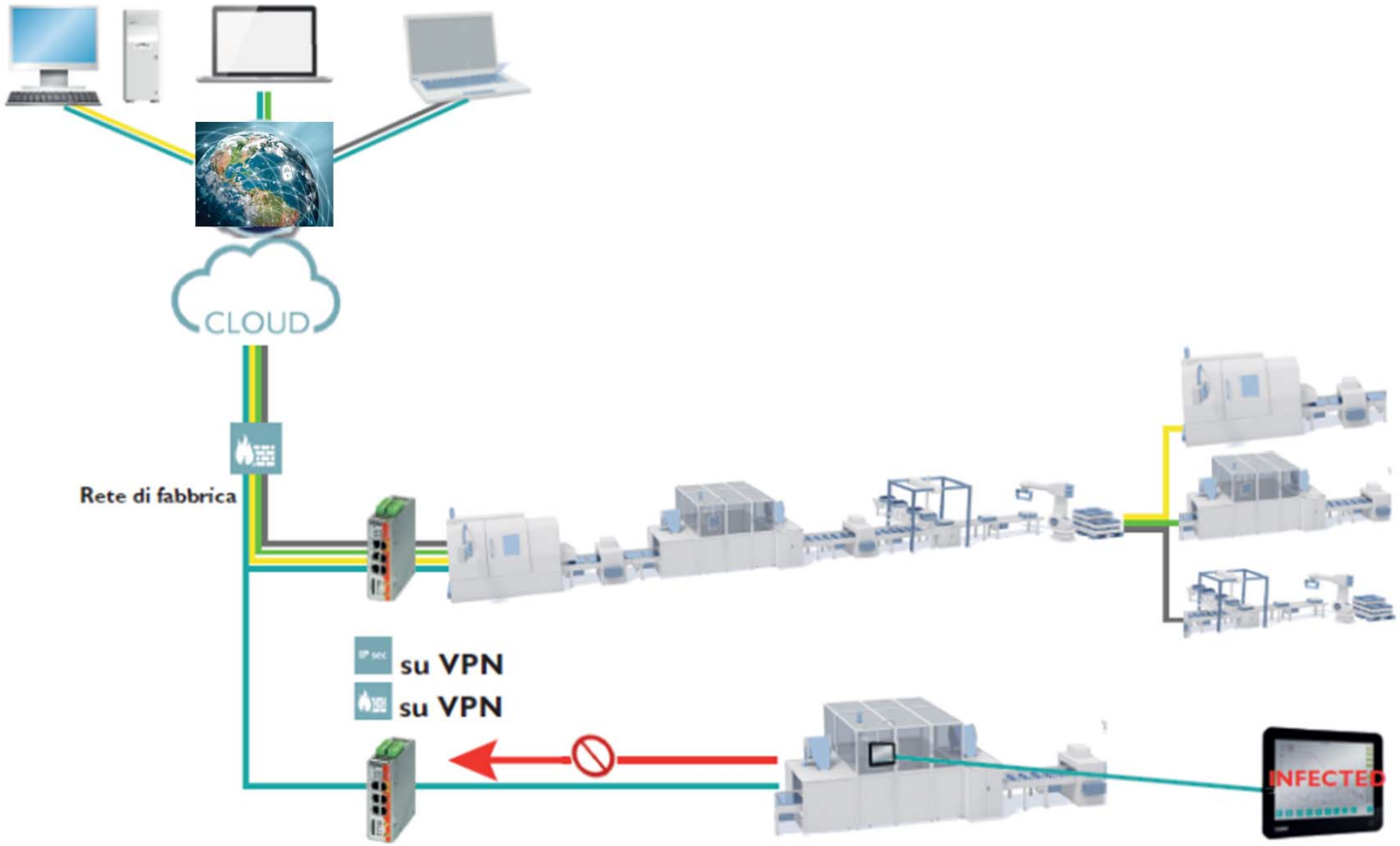
1. **Accept: From TCP - Port 80**
2. **Accept: From IP - Address 192.168.0.2**



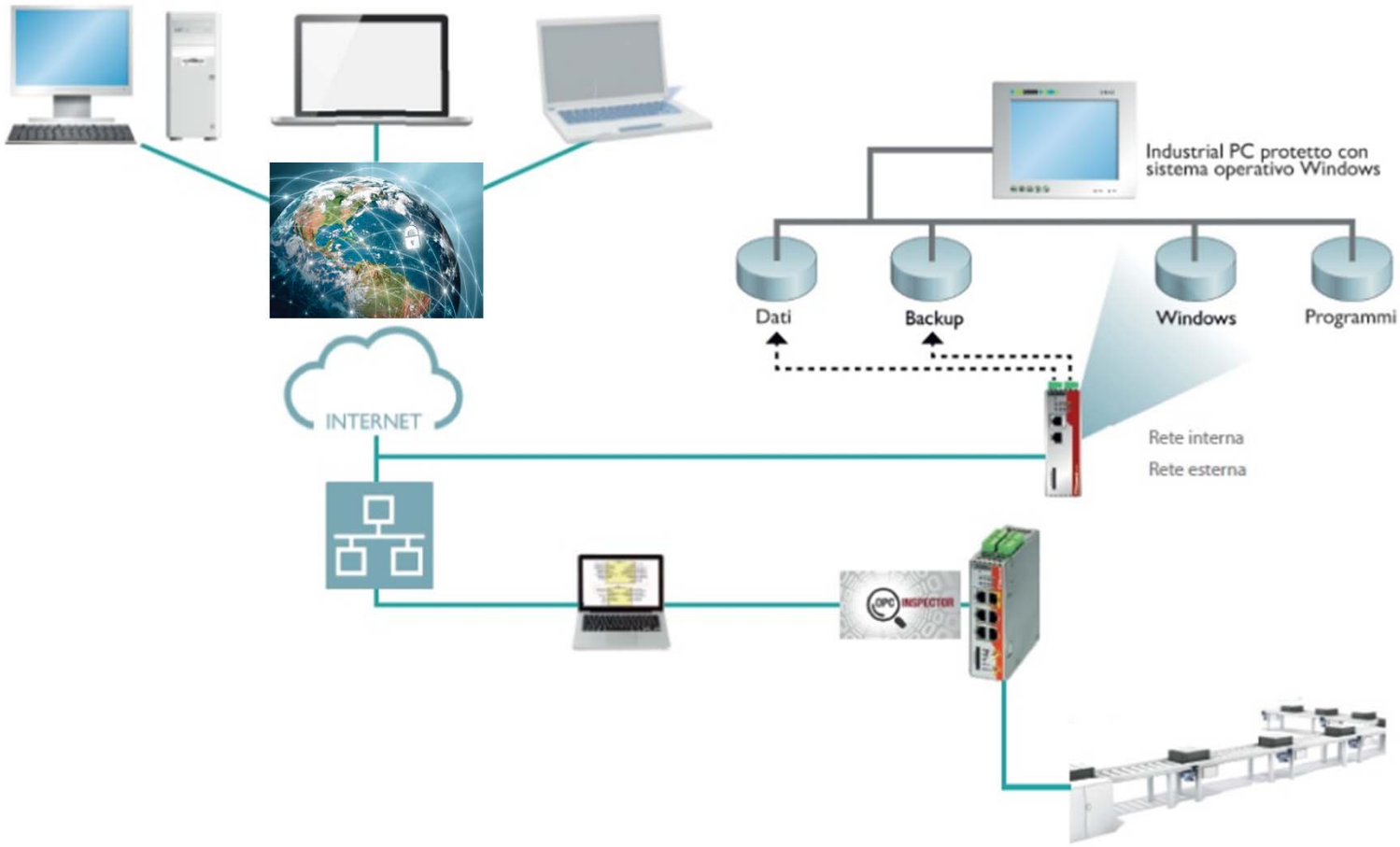
Le soluzioni



Le soluzioni



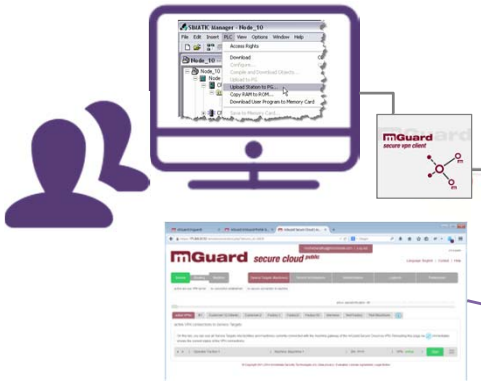
Le soluzioni



Le soluzioni: Secure Cloud

Massima disponibilità per il host

Costruttore di macchina / Tecnico di servizio



VPN-Servizio:
connessione VPN criptata con IPsec dal mGuard Secure VPN Client verso il Gateway servizio

VPN: online

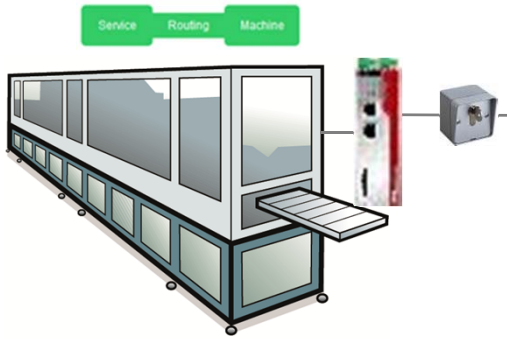
Gateway servizio (virtuale)

Secure Cloud App

Routing & Management

Internet

Macchina presso il cl. finale



VPN: online

Gateway macchina (virtuale)

VPN macchina:
connessione VPN criptata con Psec verso il Gateway macchina

SecurITy made in Germany

Raggungibile tramite il indirizzo IP reale

L'intera gamma di prodotti per la Cyber Security può essere visionata accedendo al sito Internet www.phoenixcontact.it nella sezione ''Prodotti/Industrial Ethernet''