Sistemi HMI e SCADA
Soluzioni industriali per accesso remoto sicuro

Ing. Marco Caliari

La Rete

Gli impianti e le reti sono sempre più una risorsa critica e diventa sempre più importante potere avere accesso alle informazioni da remoto e via web.

In un contesto in cui “funzionamento“ e “manutenzione“ sono sempre più legati a fenomeni di delocalizzazione e globalizzazione del mercato, si rendono necessari servizi per la manutenzione da remoto, con possibilità di estenderli a sistemi di raccolta e analisi dei dati.

Come conseguenza, si è registrata una modifica dei requisiti e dei trend nell’automazione in termini di: decentralizzazione, uso di standard IT aperti, comunicazione via Ethernet, integrazione tra reti di automazione e di organizzazione, monitoraggio e supporto remoti via Internet, sistemi di automazione flessibili.

Ethernet, già utilizzata come rete di alto livello, è oggi sempre più utilizzata fino a livello di campo: un’infrastruttura integrata e flessibile consente di ridurre costi di progettazione e gestione, grazie anche al web server integrato nei dispositivi locali.

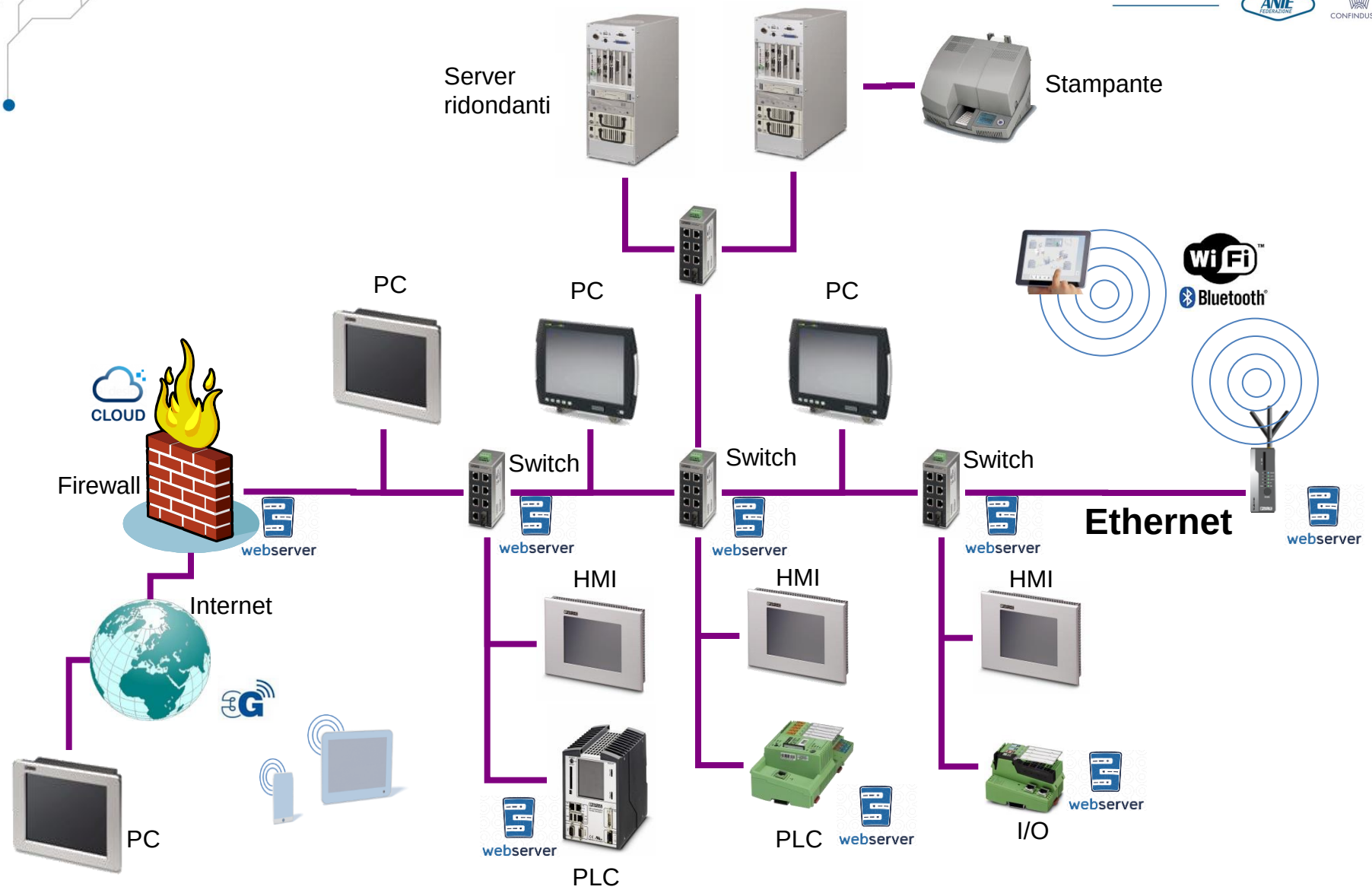
Modbus-IDA the architecture for distributed automation

PROFINET®

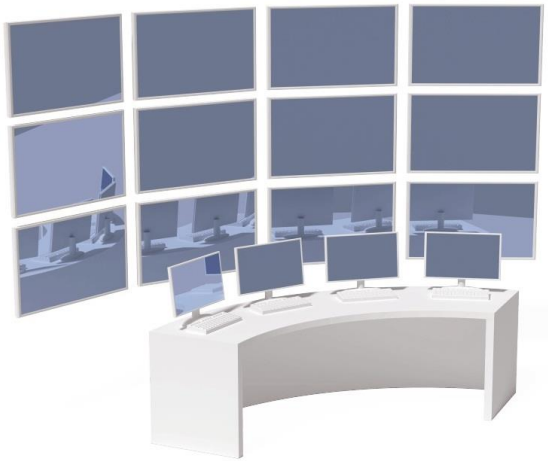
EtherNet/IP™

Industry 4.0

Tali tecnologie hanno modificato radicalmente approcci, strumenti e modalità operative con un impatto assimilabile a quello delle passate Rivoluzioni Industriali.
Si tratterebbe della quarta rivoluzione (dopo quelle caratterizzate dall'uso 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 si basa su sistemi costituiti da componentistica intelligente basata su svariate tecnologie (come, ad esempio, meccanica, elettronica ed informatica) che, in genere, è posta in comunicazione attraverso una rete, spesso costituita da Internet.


Server
ridondanti
Stampante
PC
PC
PC
CLOUD
Firewall
webserver
Switch
webserver
Switch
webserver
Switch
webserver
Ethernet
webserver
Wi Fi
Bluetooth
HMI
HMI
HMI
Internet
3G
PC
webserver
PLC
webserver
PLC
webserver
I/O
webserver

Software per l‘industria

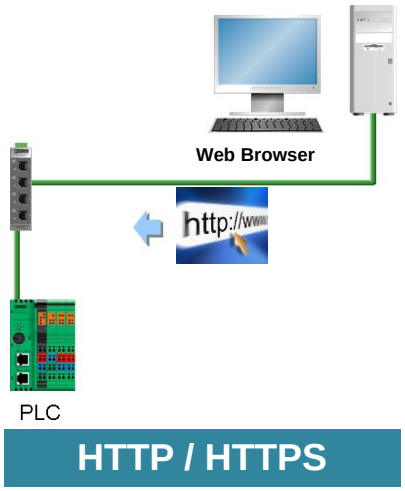


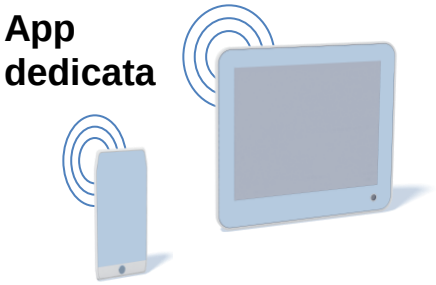
- Visualizzazione;
- Interfaccia Web;
- Gestione utenti;
- Interfacce di processo;
- Storicizzazione (Database);
- Analisi dati, report e valutazione;
- Gestione allarmi;
- Interfaccia per teleassistenza.

HTTP Vs HTTPS

- Hypertext Transfer Protocol (HTTP) viene utilizzato nel World Wide Web per trasferire dati e servizi tra un server e dei client dotati di web browser.
- Hypertext Transfer Protocol Secure (HTTPS) è una versione più sicura di inviare dati tra server e client.

HTTP	HTTPS
URL inizia con “http://”	URL inizia con “https://”
Usa la porta 80 per comunicare	Usa la porta 443 per comunicare
Insicuro	Sicuro
Nessuna crittografia	Crittografia presente
Nessun certificato richiesto	Certificato richiesto





Problematiche:

- Caricamento pagine più lento (necessario caricamento Java VM);
- Gestione (Java security warning);
- Non supportato da piattaforme mobile.

Requisiti minimi:

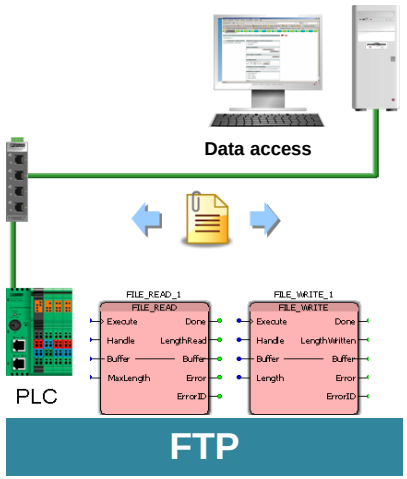
- Firefox 3.5+;
- Google Chrome 3.0+;
- Internet Explorer 9.0+;
- Opera 9.2+;
- Safari 4+.

Vantaggi:

- HTML5 è una tecnologia web „nativa“ (no Plug-In aggiuntivi, supporto anche su piattaforme mobile);
- Caricamento pagine più veloce (caricamento Java VM non più necessario);
- Gestione migliore (no Java security warning).

Un server FTP offre svariate funzioni che permettono al client di interagire con il suo filesystem e i file che lo popolano, tra cui:

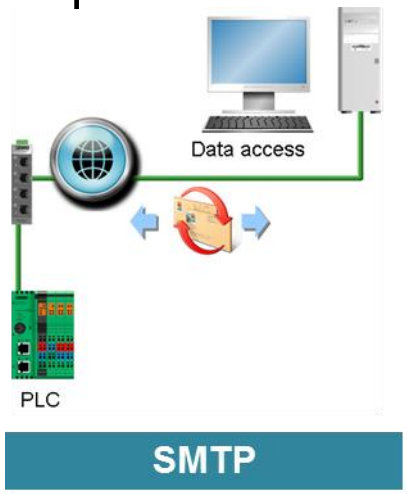
- Download / upload di file;
- Resume di trasferimenti interrotti;
- Rimozione e rinomina di file;
- Creazione di directory;
- Navigazione tra directory.



FTP fornisce inoltre un sistema di autenticazione in chiaro (non criptato) degli accessi e dei relativi privilegi.
La specifica originale di FTP non prevede alcuna cifratura per i dati scambiati tra client e server.

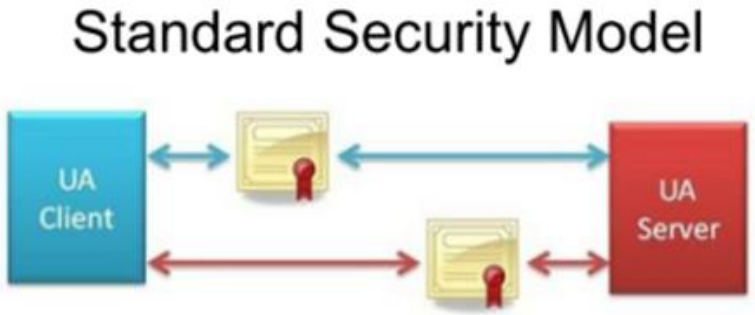
SSL (Secure Sockets Layer):

- Sistema di cifratura molto robusto ed efficace, impiegato da tutte le realtà (banche online, provider di posta elettronica, ecc.) che devono fare transitare in modo sicuro e indecifrabile i dati.
- Lo scopo è quello di fornire sistemi di comunicazione affidabili, riservati ed altamente sicuri.
- Questo sistema di cifratura offre diversi vantaggi, tra i quali:
  - Autenticazione;
  - Confidenzialità dei dati trasmessi (crittografia);
  - Affidabilità.

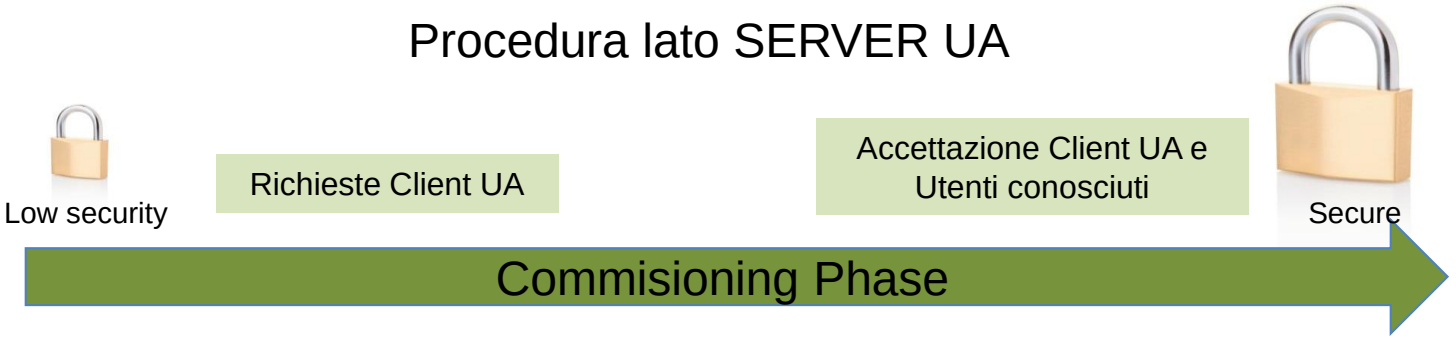


OPC UA
Sicurezza scalabile

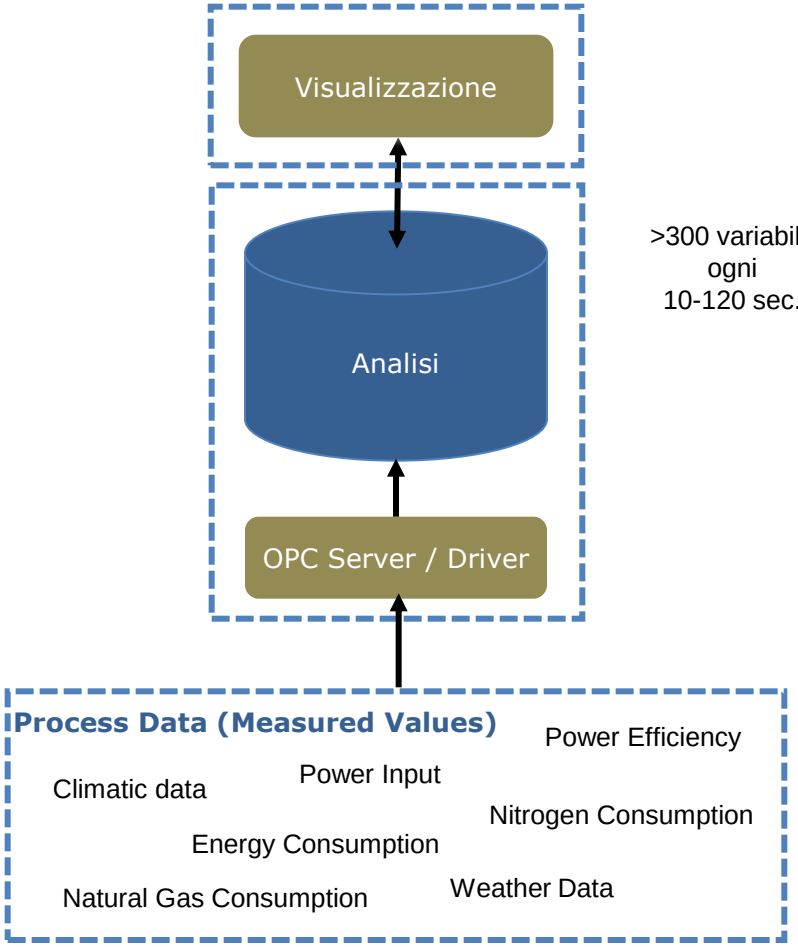
- Basato su certificati X.509;
- Comunicazione sicura tramite openSSL:
  - Certificati firmati;
  - Certificati firmati e crittografati;
- Meccanismi di protezione aggiuntivi tramite nome utente / password.



Procedura lato SERVER UA

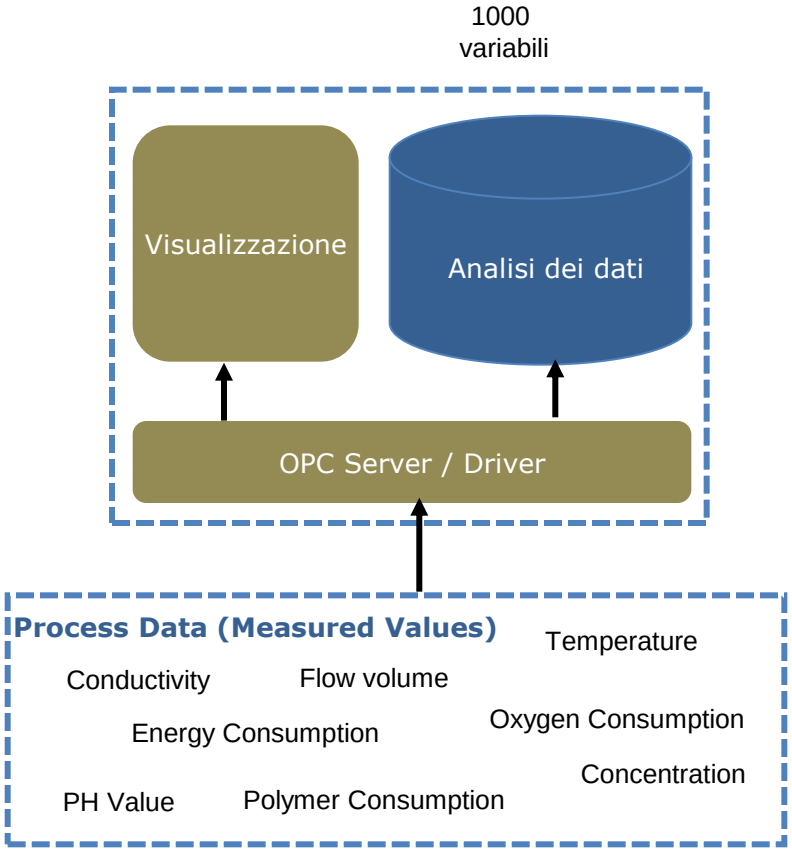


Visualizzaizone e gestione dati

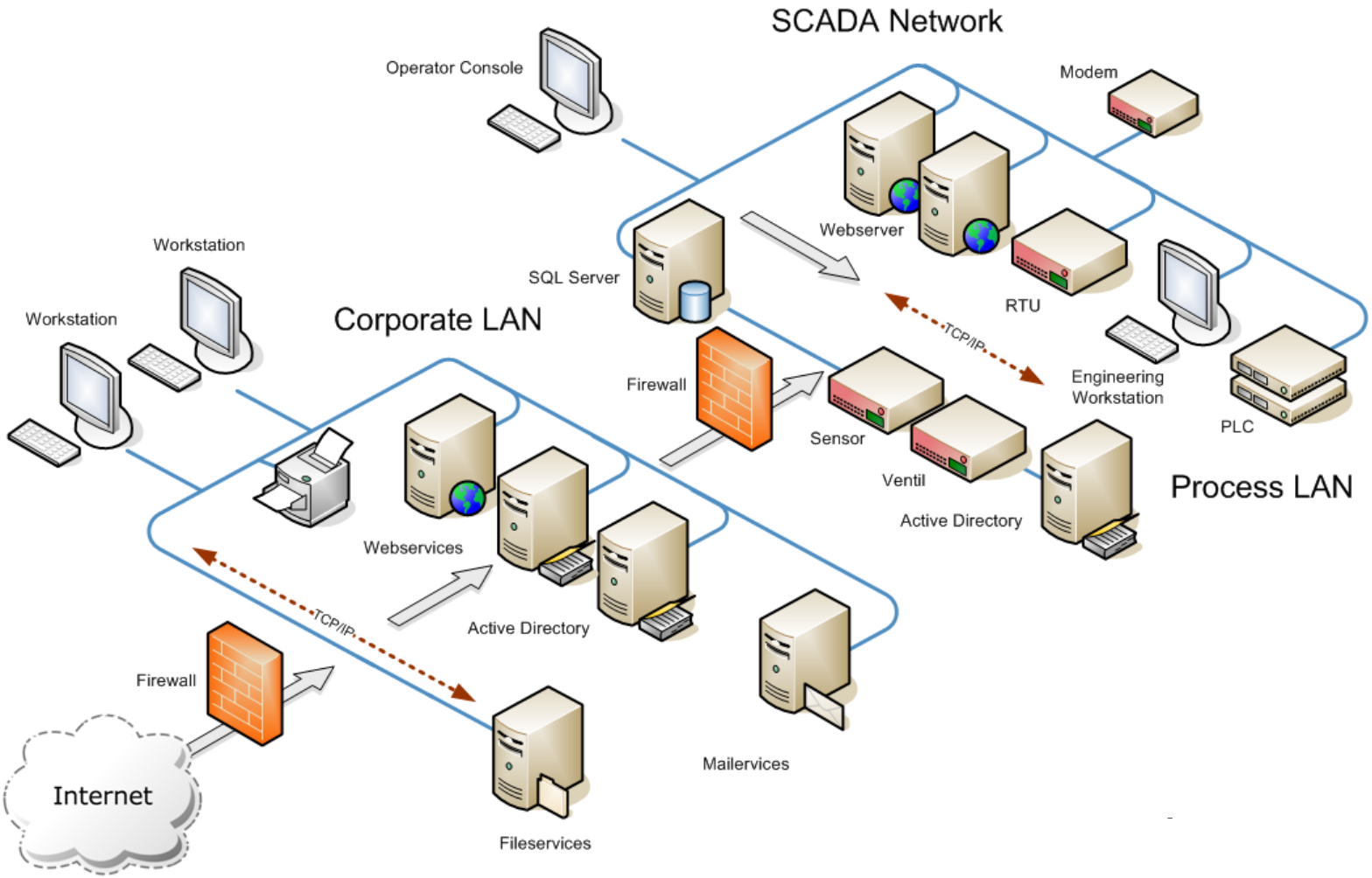


>300 variabili
ogni
10-120 sec.

1000
variabili



Apertura verso Internet (Security)



Security





Vantaggi legati all'integrazione:

- Uso di sistemi ERP e MES;
- Accesso da remoto (teleassistenza e telecontrollo);
- Accesso al sito da parte di fornitori e sub-contactor;
- Acquisizione permanente di dati dal campo;
- Maggior semplicità nel rispetto di norme e legislazioni.

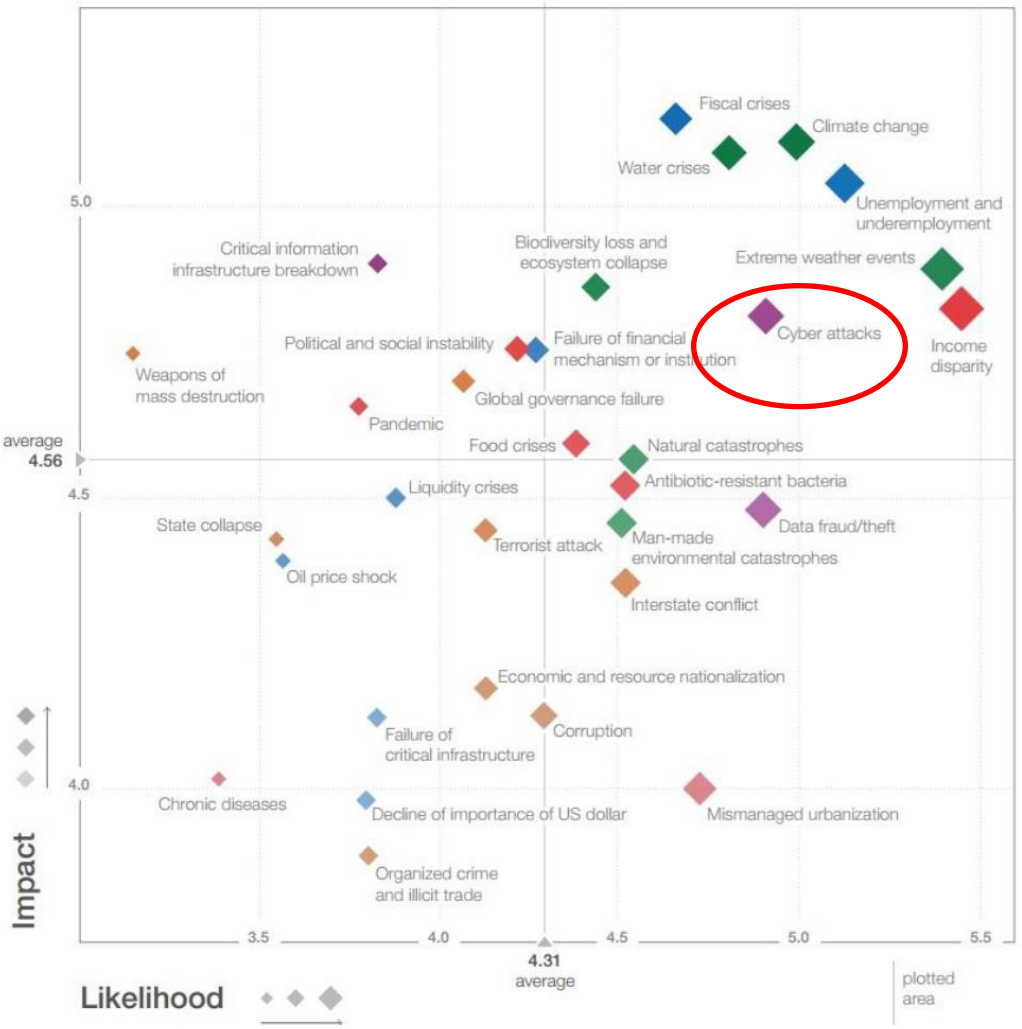
Possibili conseguenze di un attacco:

- Sistemi produttivi non affidabili;
- Perdita di produzione;
- Perdita di dati sensibili;
- Danni a persone e cose (con eventuali importanti conseguenze anche all'ecosistema).

Security

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

(World Economic Forum 2014)



I rischi

«La LAN di impianto non è connessa a Internet, quindi non ci rischi» e non ci sono motivazioni valide per investire in Security.

Il ciclo di vita di un'installazione è anche superiore ai 20 anni ma il supporto per il Sistema Operativo potrebbe terminare prima della fine del ciclo di vita dell'installazione (si pensi a Windows XP).

Dipendenti o tecnici esterni potrebbero introdurre malware per mezzo di memorie USB o attraverso PC di servizio.

L'invulnerabilità dei sistemi non viene più garantita e i rischi associati alla Security aumentano.

I rischi

«Sul PC è presente un programma antivirus» per proteggere il sistema produttivo.

I programmi antivirus standard possono impattare in modo significativo (e negativo) sulle prestazioni ‘’real time’’, dal momento che il caricamento di archivi per riconoscimento virus (soggetto ad aggiornamenti) può cambiare continuamente il sistema.

In caso di accesso da remoto, i dati spesso vengono trasferiti via Internet senza essere stati protetti con meccanismo di cifratura.

I pacchetti dati viaggiano via Internet attraverso diversi percorsi (e Paesi). Pacchetti non cifrati possono essere letti e modificati senza che i diretti interessati ne abbiano la percezione.

I rischi

Le installazioni sono spesso connesse a Internet in modo continuativo (24/7) attraverso un’economica tariffa “Internet flat”.

«La comunicazione da remoto viene eseguita attraverso un tunnel VPN sicuro» e quindi non sono servono ulteriori misure di Security.

Gli hacker hanno abbastanza tempo per “trovare” le apparecchiature in Internet ed attaccarle.

Malware potrebbero comunque viaggiare attraverso il tunnel VPN, infettando una delle reti disposte ai due estremi del tunnel stesso.

I rischi

L’utilizzatore dispone di una rete “globale”, che integra anche le reti di apparecchiature acquistate da fornitori diversi. Ogni fornitore ha un accesso da remoto alla “propria” apparecchiatura.

I tecnici di assistenza sono spesso in trasferta per alcuni giorni consecutivi ed usano il loro PC di servizio per collegarsi a Internet la sera in hotel.

Ogni singola apparecchiatura è una potenziale fonte di rischio in termini di Security, dal momento che ogni singola “sottorete” può essere infettata o spiata.

Il PC di servizio viene di fatto utilizzato per fini non professionali, incrementando la possibilità di infezioni che si andrebbero a ripercuotere sull’installazione cui il PC venisse poi collegato.

I rischi

Spesso vengono usate software VPN disponibili gratuitamente in Internet per creare una connessione VPN.

I tecnici più professionali usano PC dedicati e con software VPN adeguati. Le password per accedere alle reti possono essere salvate all'interno dei PC.

I software VPN gratuiti disponibili in Internet non possono essere considerati sicuri.
Hacker potrebbero servirsi di questo tunnel VPN (normalmente non soggetto a regole di firewall) per accedere alla rete.

Se il PC del tecnico venisse rubato o il tecnico cambiasse lavoro dopo essersi creato una copia delle password, sarebbe necessario cambiare tutte le password di accesso alle reti potenzialmente coinvolte.

Cyber security

Diventa fondamentale la protezione a livello industriale contro accessi non autorizzati alla rete per l'accesso da qualsiasi parte del mondo

- Integrazione di sottositemi in reti di livello superiore (routing, NAT);
- Protezione contro accessi non autorizzati ed attacchi esterni;
- Possibilità di garantire la protezione del sistema monitorarando le modifiche ai file system;
- Possibilità di utilizzare, a seconda delle esigenze:
  - router-firewall;
  - router-firewall con modem integrato (sia per linea cablata che 3G);
- Teleassistenza sicura via Internet tramite tunnel VPN e firewall;
- Funzioni di security integrate, configurabili tramite interfaccia web o portale cloud.

Grazie per l’attenzione!