PI Italia
PROFIBUS • PROFINET

Workshop

Safety & Security

PROFINET® PROFIBUS® PROFIsafe PROFIenergy PROFIdrive IO-Link FDI

Programma

1. Safety vs. Security
2. Safety in ambiente industriale
3. Safety & Profibus/Profinet: il profilo PROFIsafe
4. Security in ambiente industriale
5. Security & Profinet

Safety vs. Security

Safety vs. Security

Safety: protezione degli uomini dalle macchine

Safety

Definizione tratta dalla Guida ISO/IEC n.51

”Freedom from unacceptable risks”

Calandoci nelle realtà di macchine e impianti industriali possiamo meglio specificare la definizione di ”Safety” come ”capacità di macchine o impianti di svolgere la propria funzione, essere trasportate, installate, regolate, mantenute, smantellate ed eliminate senza provocare lesioni o danni”

Safety vs. Security

Security: protezione delle macchine dagli uomini

Security

Definizione inclusa nella specifica tecnica IEC/TS 62443-1-1:2009 ”Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, concepts and models”:

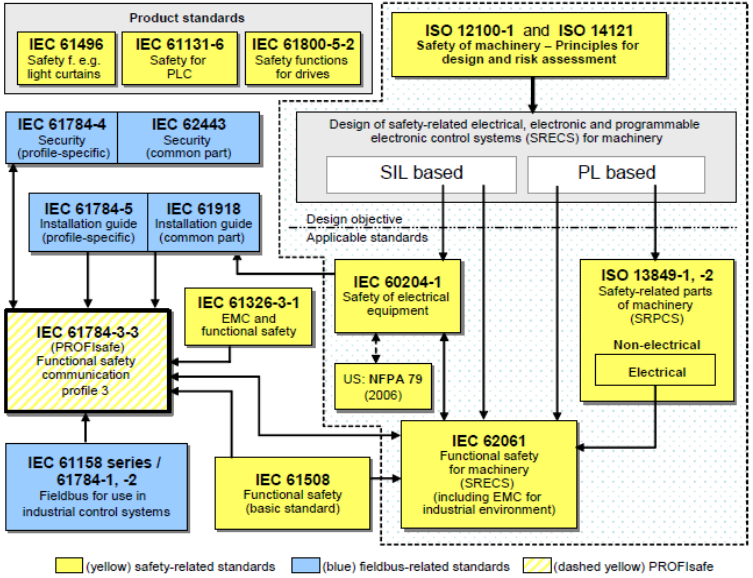
”Prevenzione di accessi illegali o non voluti o di interferenze nello specifico e previsto funzionamento di un sistema di comando e controllo per l’automazione industriale”

Safety in ambiente industriale

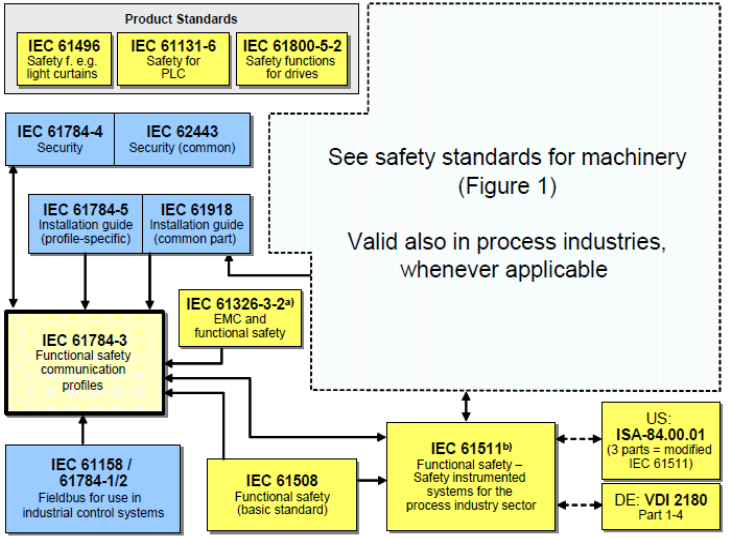
- I requisiti essenziali di sicurezza per applicazioni di tipo industriale sono definiti in leggi specifiche (nella UE spesso costituite dalla trasposizione di Direttive Comunitarie quali ad esempio Direttiva Macchine, Direttiva Bassa tensione, Direttiva Compatibilità Elettromagnetica, ….)
- Al fine di raggiungere gli obiettivi di sicurezza fissati in tali leggi, particolarmente utile risulta il ricorso a Norme Tecniche emesse da Istituti di Certificazione internazionale (IEC, ISO, ….)
- Le “norme armonizzate” conferiscono la cosiddetta “presunzione di conformità”

Safety in ambiente industriale

Norme tecniche attinenti



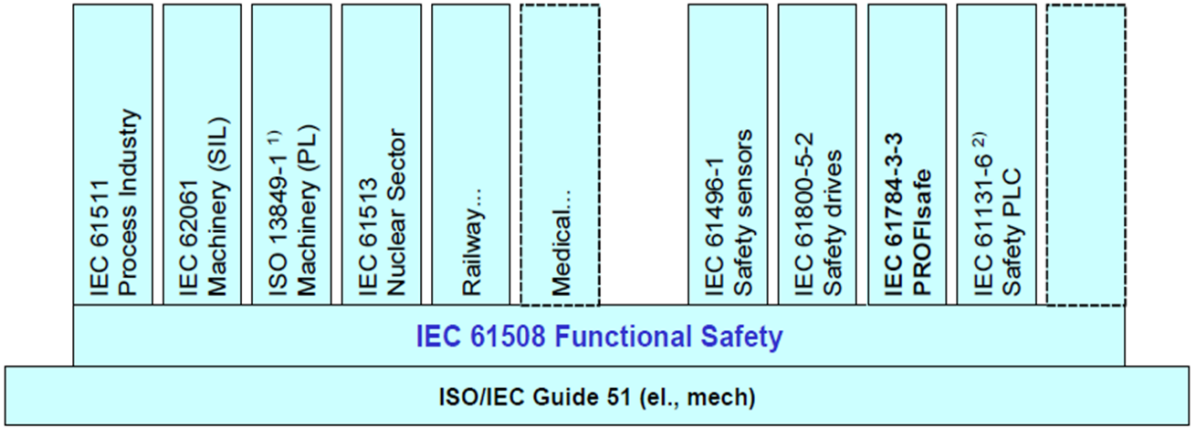
Macchinario



Processo

Safety in ambiente industriale

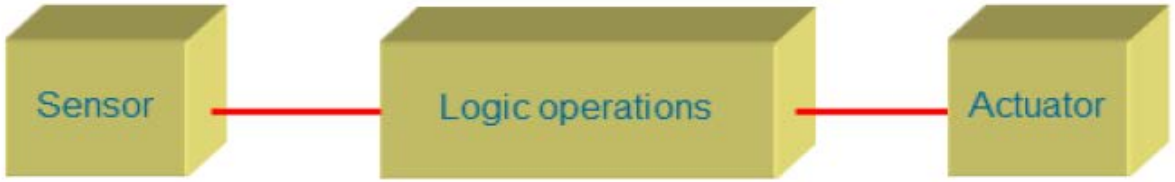
- Le norme di sicurezza che più interessano la gestione di funzioni di sicurezza su reti di automazione industriale sono le norme attinenti la cosiddetta “Sicurezza Funzionale”
- La “Sicurezza Funzionale” è quella parte dell’intera sicurezza che dipende dal corretto funzionamento dei sistemi di sicurezza elettrici, elettronici, programmabili, da altre tecnologie e da strumenti esterni di riduzione del rischio



Safety in ambiente industriale

- All’interno di tali norme si fa riferimento alla cosiddetta "integrità di sicurezza" definita come la probabilità che un sistema di controllo sicuro esegua in modo soddisfacente le funzioni prescritte relative alla sicurezza, in tutte le condizioni dichiarate
- L’integrità di sicurezza viene classificata, a seconda delle norme utilizzate, in Performance Level (PL) o Safety Integrity Level (SIL)
- Più elevato è il valore del PL o del SIL, minore è la probabilità che il sistema di controllo sicuro non esegua correttamente la richiesta funzionalità di sicurezza

Safety in ambiente industriale

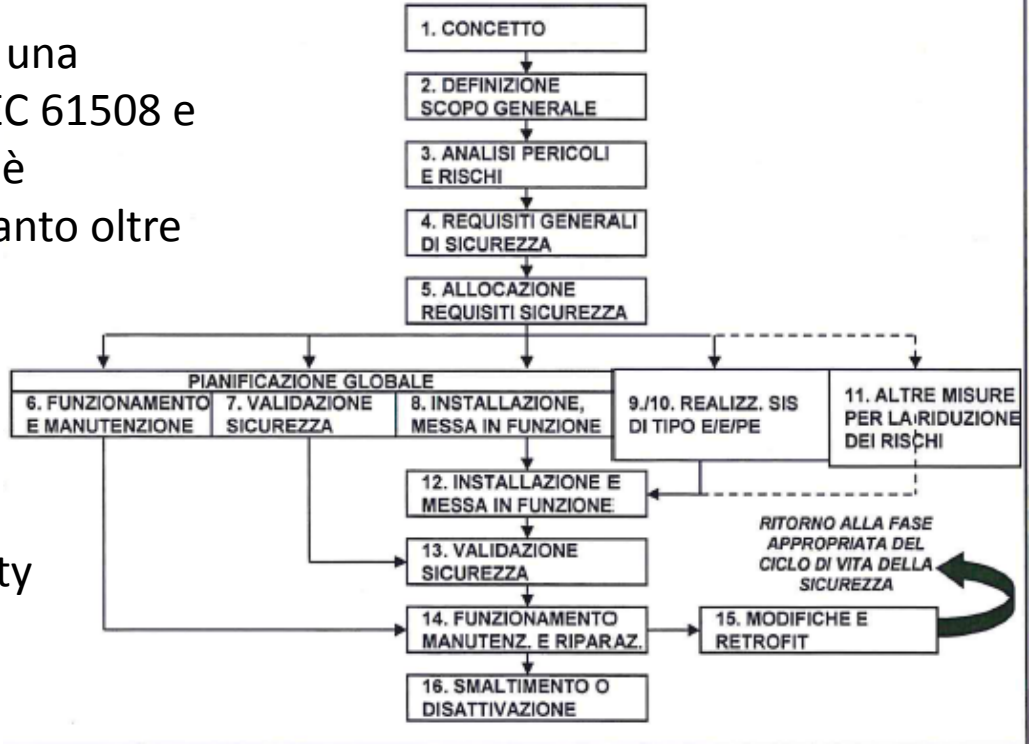


Parametri da considerare per il calcolo del Performance Level di una funzione di sicurezza (norma ISO 13849-1)

- Categorie di Sicurezza (vincoli architetturali)
- Mean Time To Failure dangeorus (MTTFd) del canale di sicurezza (sensore+ logica + attuatore)
- Diagnostic Coverage (DC)
- Common Cause Failure (CCF)

Safety in ambiente industriale

Nel calcolo del Safety Integrity Level di una funzione di sicurezza (serie di norme IEC 61508 e relative norme applicative) la gestione è burocraticamente più complessa in quanto oltre alla medesima valutazione di vincoli architetturali, integrità di sicurezza e probabilità di guasto casuale dell'hardware, la norma richiede la predisposizione di un vero e proprio piano di gestione della Functional Safety a copertura di tutte le fasi del ciclo di vita della sicurezza



Safety in ambiente industriale

La serie di norme base per la gestione della Sicurezza Funzionale (IEC 61508) include anche la definizione delle misure tecnologiche che, se correttamente implementate, permettono la gestione di funzioni di sicurezza anche mediante l'utilizzo di logica elettronica/elettronica programmabile e di bus di campo (reti)

Meas. / Error	Consec. number	Time tag	Time expect.	Echo	S/R detection	Data save	Redun. & comparison.	Data save (S ≠ NS)
Repetition	●	●					●	
Loss	●		cyclic only	●			●	
Insertion	●			●	●		●	
Incorrect seq.	●	●					●	
Corruption (of user data)				●		●	serial bus only	
Delay		●	●					
Coupling of S + NS messages				●	●			●

Safety & Profibus/Profinet: il profilo PROFIsafe

Il profilo per la gestione di segnali attinenti Funzioni di Sicurezza su reti

PROFINET®

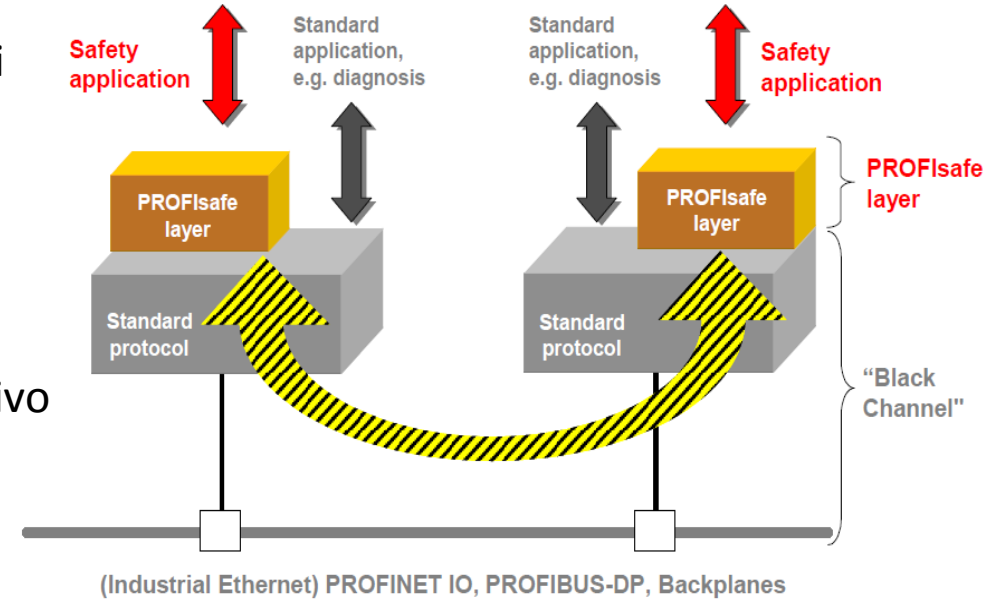
e/o

PROFIBUS®

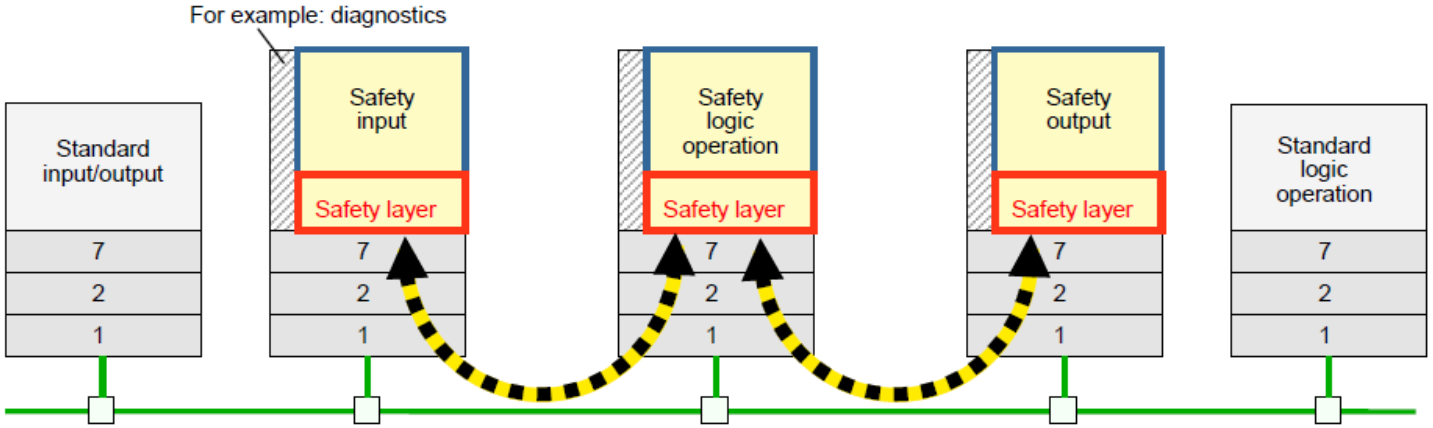
Safety & Profibus/Profinet: il profilo PROFIsafe

PROFIsafe

- Layer aggiuntivo al di sopra dei protocolli PROFIBUS e PROFINET
- Riduce la probabilità di errore di una trasmissione tra dispositivi di sicurezza
- Permette coesistenza di segnali “safety” e “standard” sullo stesso mezzo trasmissivo
- Supporta come mezzi trasmissivi rame, fibra ottica, wireless e backplane
- È certificato fino a SIL3 ai sensi di IEC 61508



Safety & Profibus/Profinet: il profilo PROFIsafe



Key

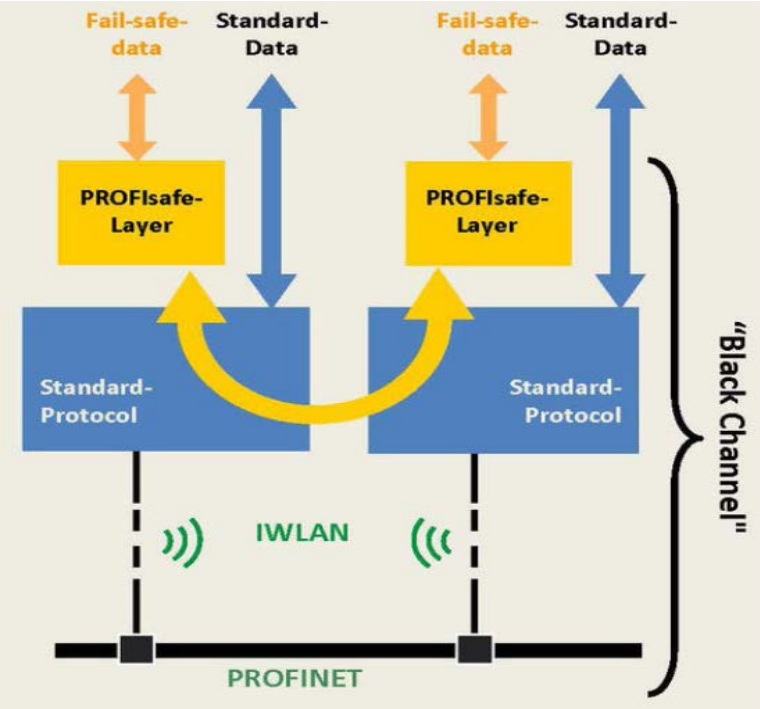
"Black Channel": ASICs, wires, switches, etc. are not safety relevant components

None safety related functions, e.g. diagnostics

FSCP 3/1: the safety related protocol comprises: addressing, watch-dog timing, sequencing, signatures, etc.

The safe IO and safe logic controller functions are safety relevant but not part of the safety profile

Safety & Profibus/Profinet: il profilo PROFIsafe

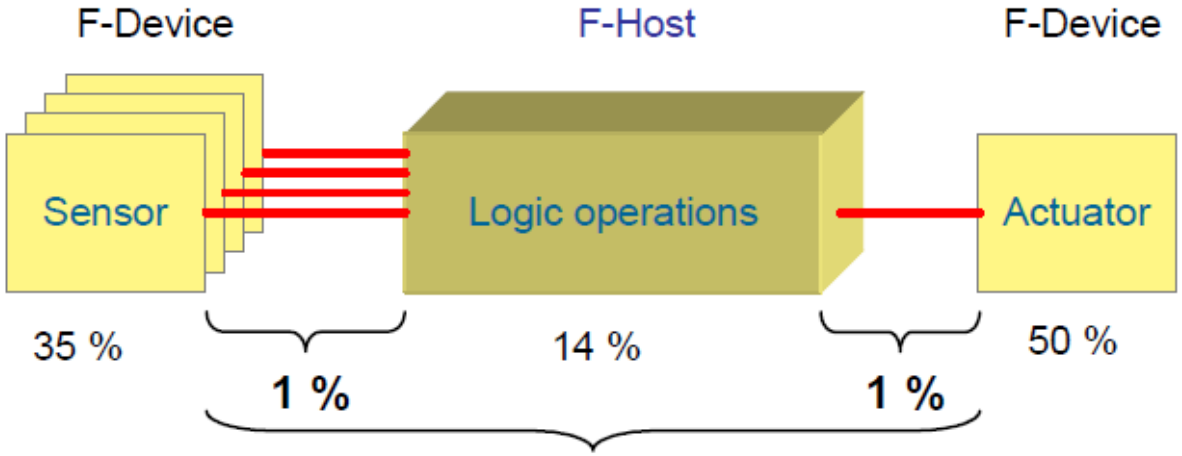


Il fatto che:

- il profilo PROFIsafe sia un layer aggiuntivo al di sopra del protocollo PROFINET
- l'utilizzo della tecnologia ''Black Channel'' rende lo scambio di pacchetti dati indipendente dal mezzo fisico utilizzato
- i pacchetti dati PROFINET possono essere trasferiti in modo trasparente utilizzando le tecnologie wireless Bluetooth o WLAN

consente di veicolare segnali di sicurezza anche in modalità wireless

Safety & Profibus/Profinet: il profilo PROFIsafe

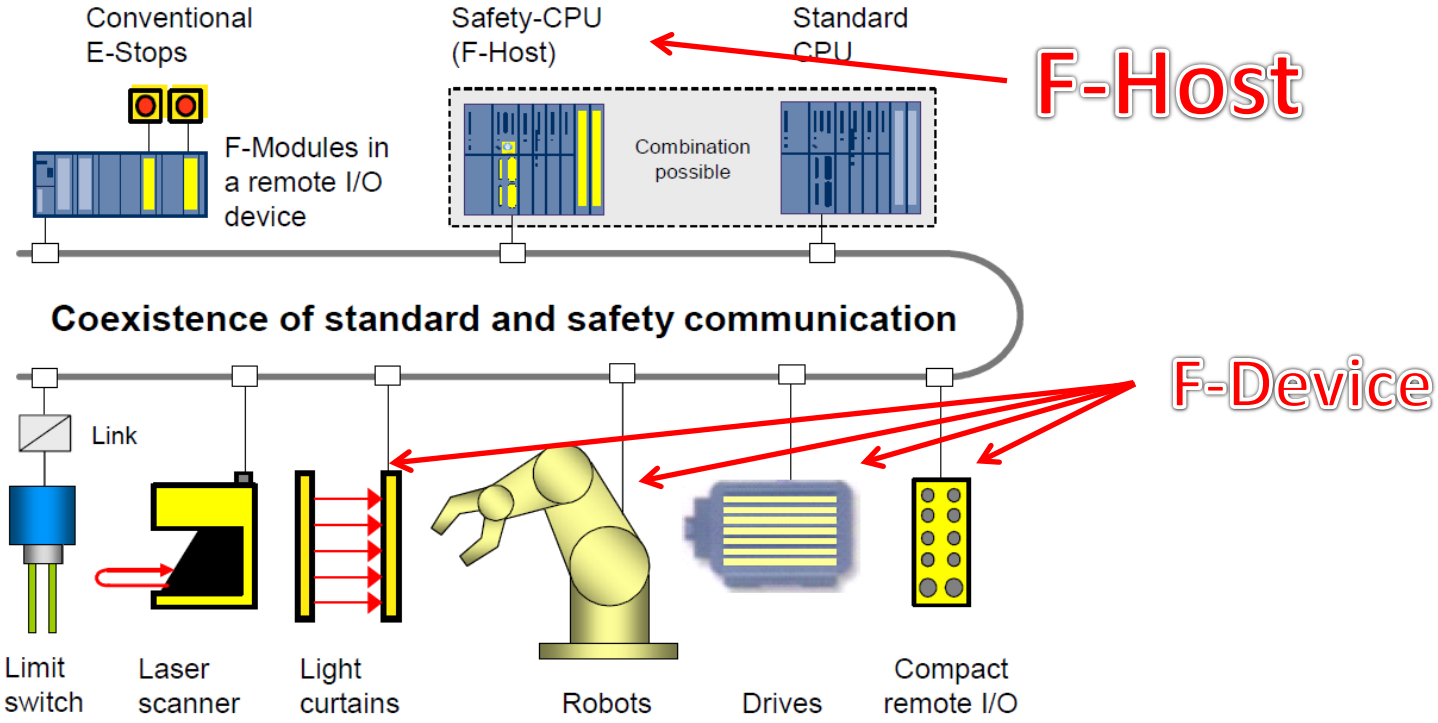


Layer di comunicazione sopra Profibus e Profinet

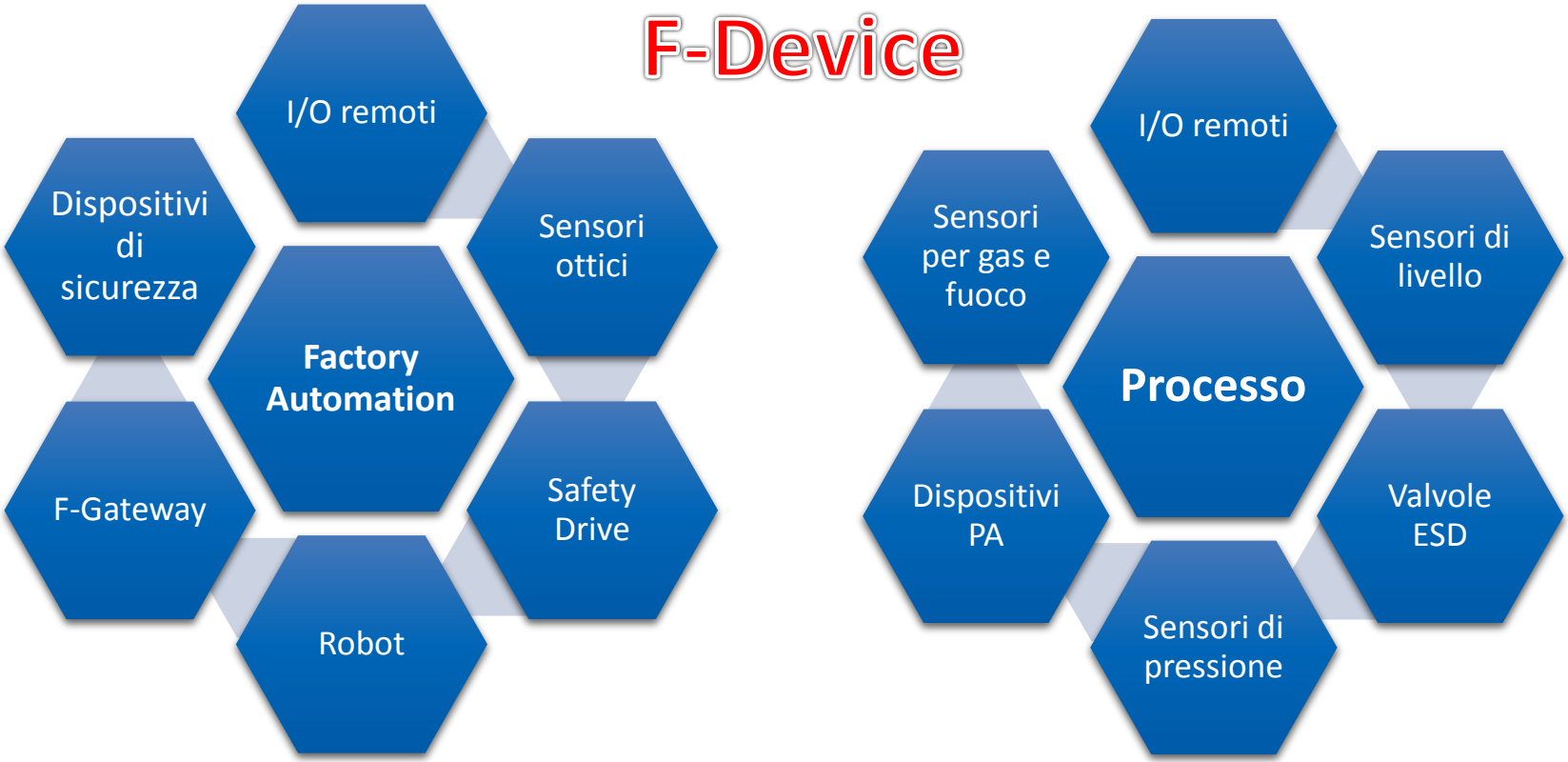
CERTIFICATO SIL 3

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

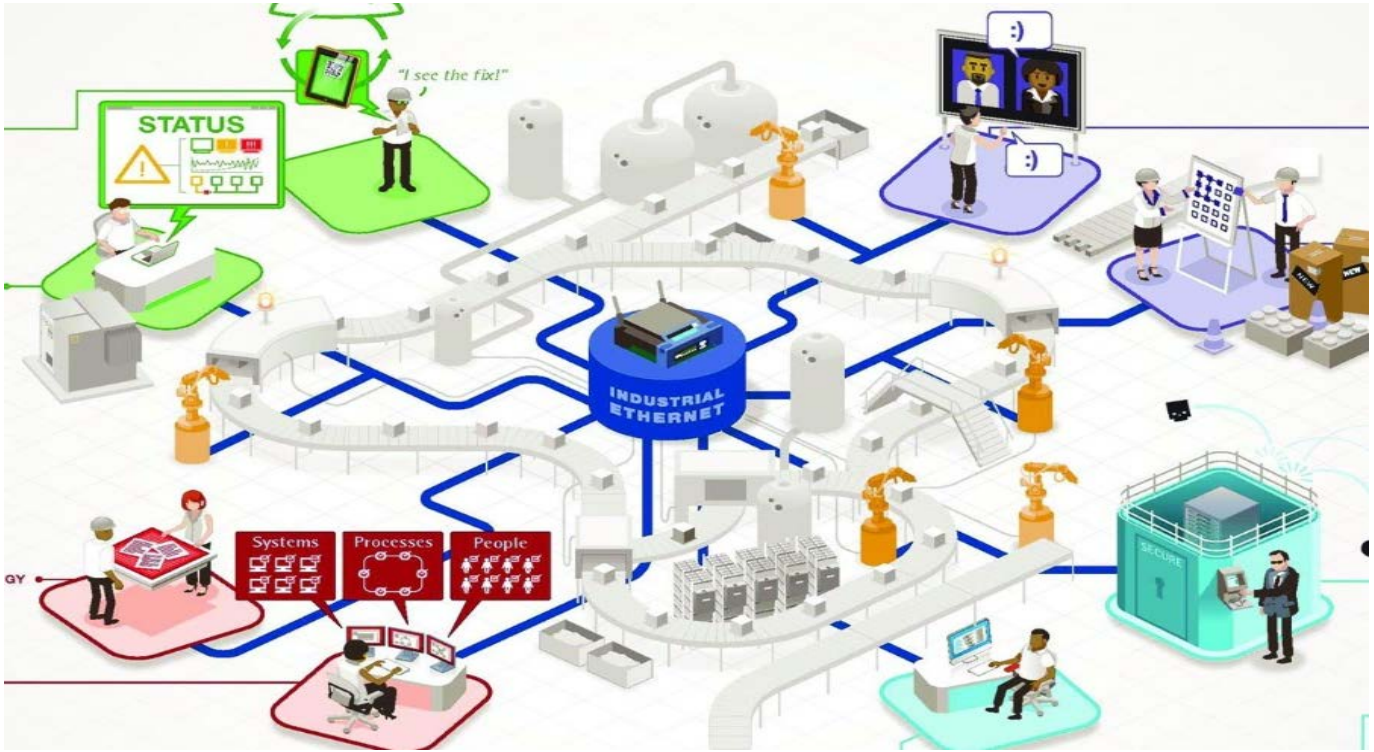
Safety & Profibus/Profinet: il profilo PROFIsafe



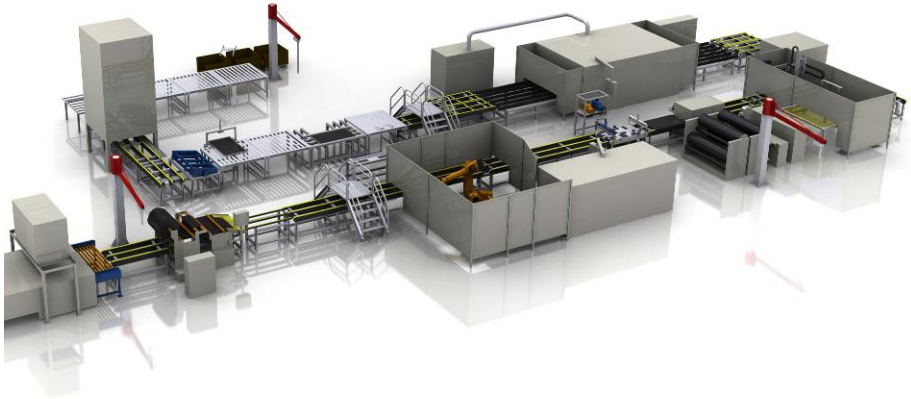
Safety & Profibus/Profinet: il profilo PROFIsafe



Security in ambiente industriale

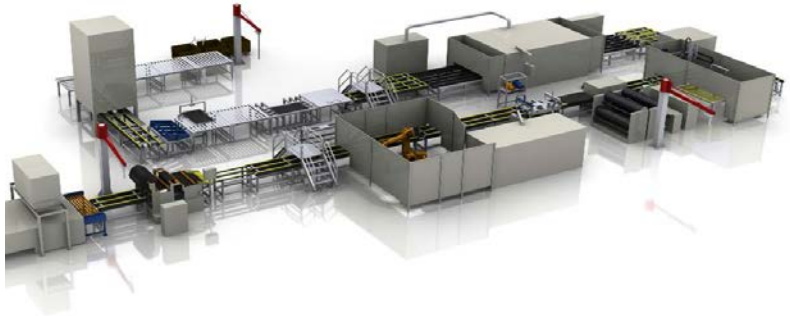


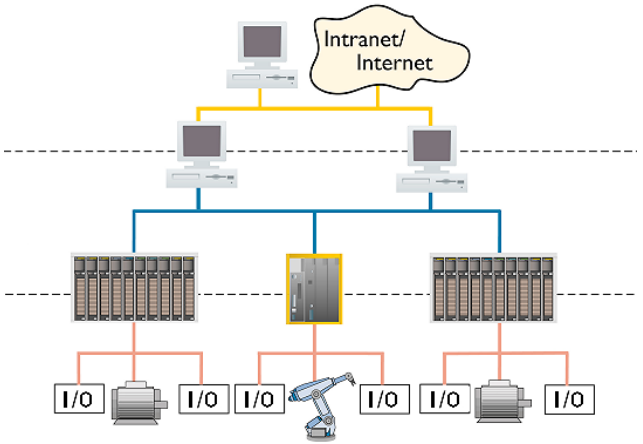
Security in ambiente industriale



- Con fieldbus su base seriale e macchina non interconnessa, le preoccupazioni dei progettisti di automazione nei confronti della security si limitavano al predisporre opportune misure e/o modalità operative tali da evitare accessi al progetto installato sul sistema di controllo
- Questo al fine di evitare modifiche dello stesso con possibili conseguenze che avrebbero potuto coinvolgere la responsabilità dell'installatore o del produttore del macchinario

Security in ambiente industriale





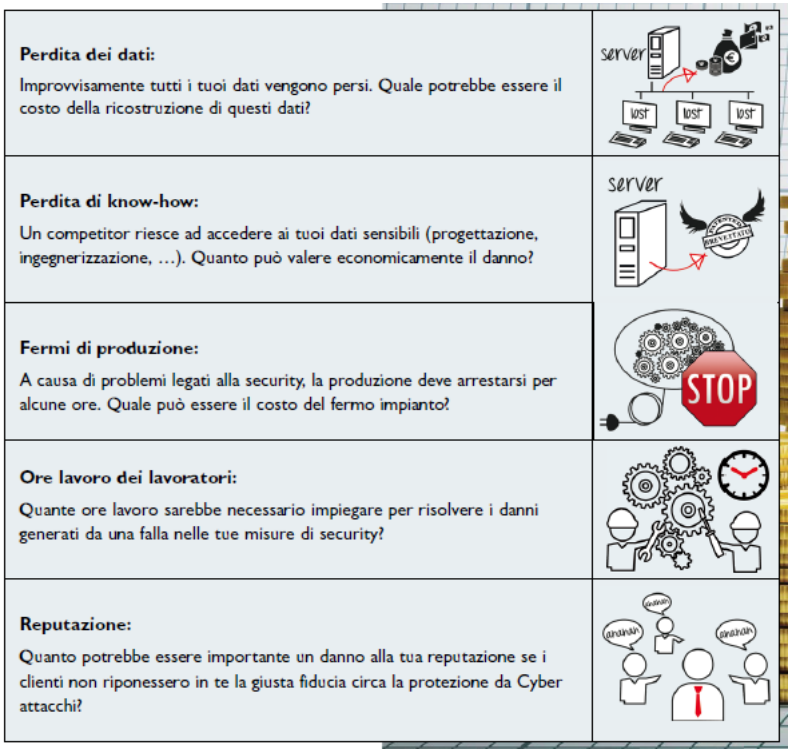
- La diffusione di protocolli a base Industrial Ethernet ha ancor più favorito l'integrazione della rete di macchina nella piramide di comunicazione con scambi da/verso sistemi ERP/MES e con l'accesso a tale rete anche da remoto: la Security diventa un'esigenza imprescindibile anche per i progettisti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

Security in ambiente industriale

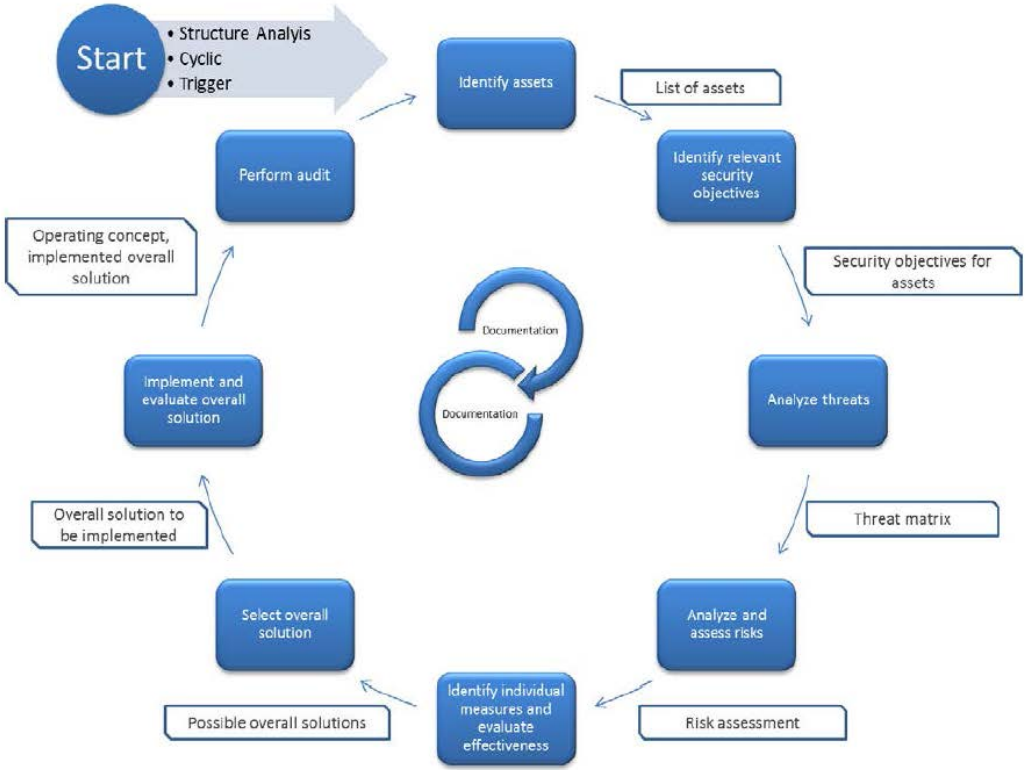
Quali le possibili conseguenze di una non adeguata protezione di una rete Ethernet in ambito industriale?

Qualche esempio ….

Lista (purtroppo) non esaustiva ….

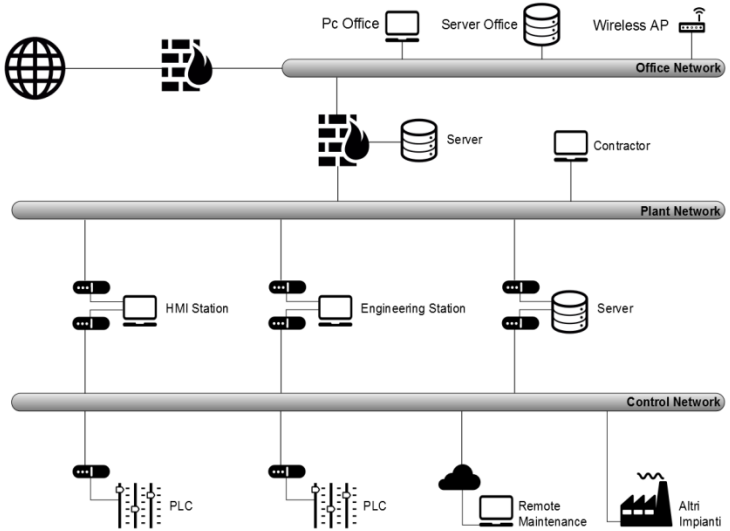


Security in ambiente industriale



Security in ambiente industriale

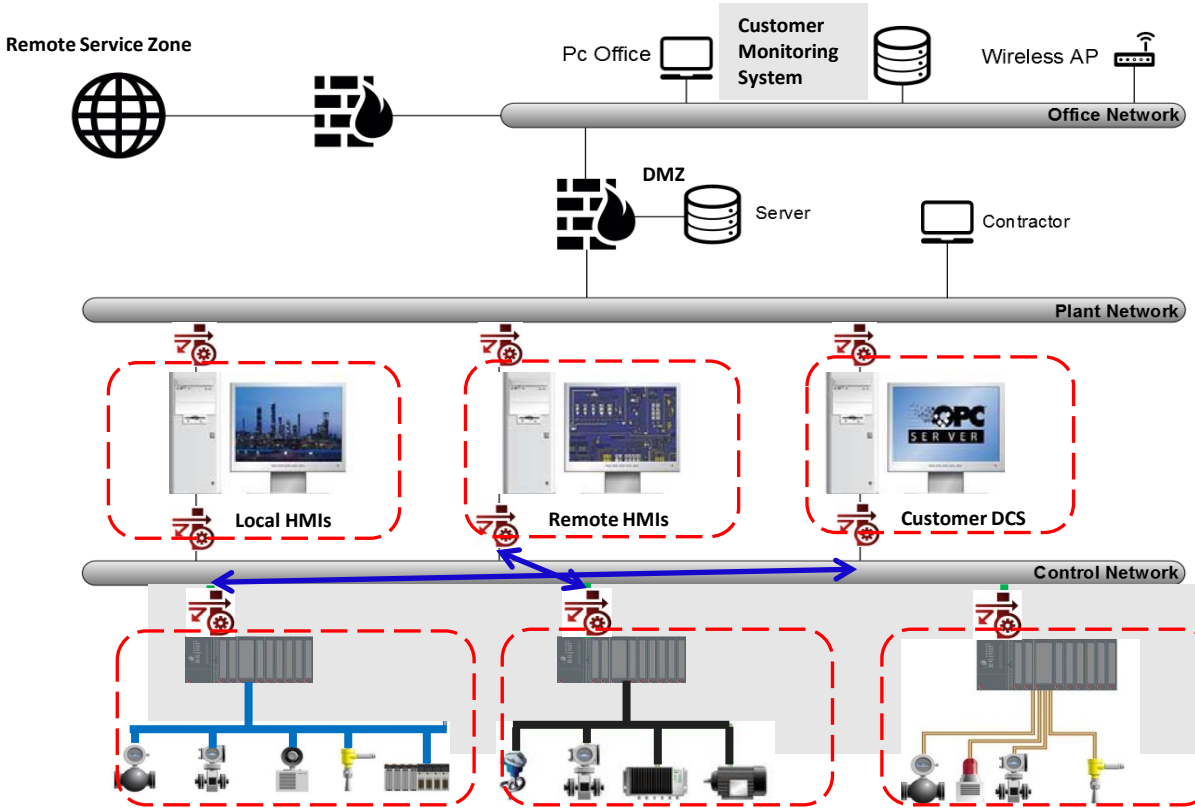
- Misure e soluzioni tecnologiche per garantire un adeguato livello di Security di una rete andranno quindi scelte in funzione delle esigenze specifiche
- Tra tali misure possiamo elencare un'opportuna segmentazione di rete con adeguata protezione (routing/firewall) dei punti di segmentazione, una corretta gestione delle prerogative di accesso locale alla rete e un'efficace protezione degli accessi da remoto (VPN, firewall, security cloud)
- L'utilizzo di strumenti di monitoraggio continuo di rete permetterà anche la rilevazione immediata di tentativi di intrusioni non autorizzate



Security & Profinet

- Come i principi di Security possono trovare applicazione in una rete PROFINET ?
- Per il concetto di segmentazione della rete può essere utile fare riferimento alla serie di norme IEC 62433, all'interno della quale vengono esplicitati i concetti di ''zone'' (anche dette ''celle'' o ''isole'') e ''percorsi''
- Una ''zona'' è definita come un insieme di dispositivi appartenenti a una rete che condividono medesime necessità di security
- Ogni scambio dati tra diverse ''zone'' deve seguire un ben determinato ''percorso''
- Ogni ''percorso'' deve essere adeguatamente protetto (Routing/Firewall/VPN)

Security & Profinet

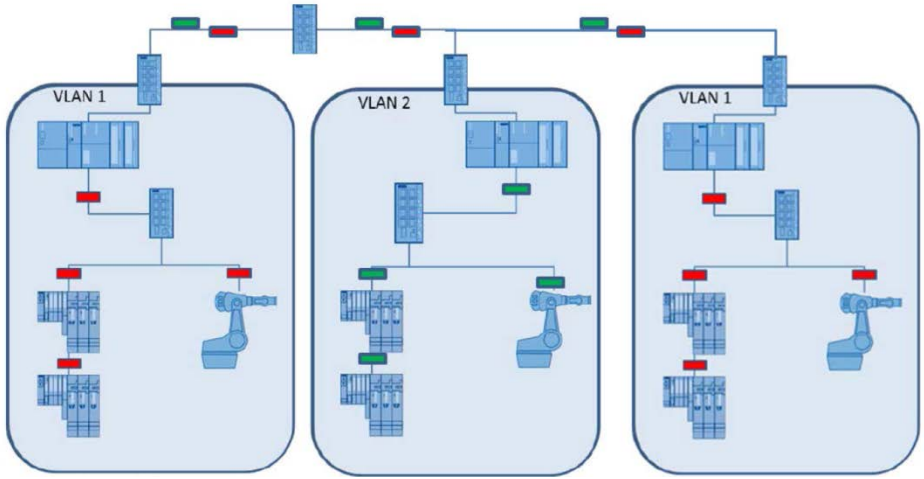


''Zone''

''Percorsi''

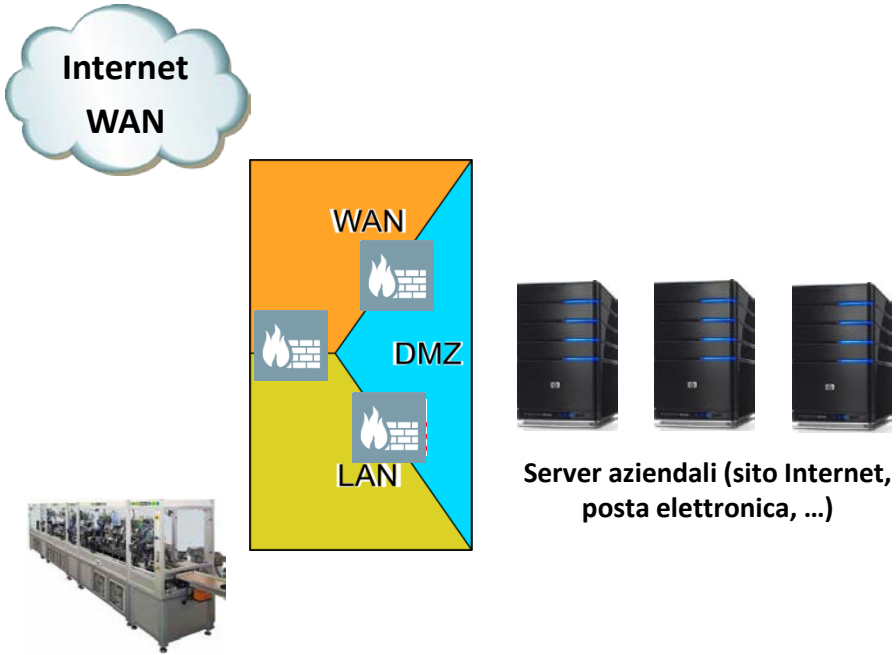
Dispositivi di protezione dei ''percorsi''

Security & Profinet



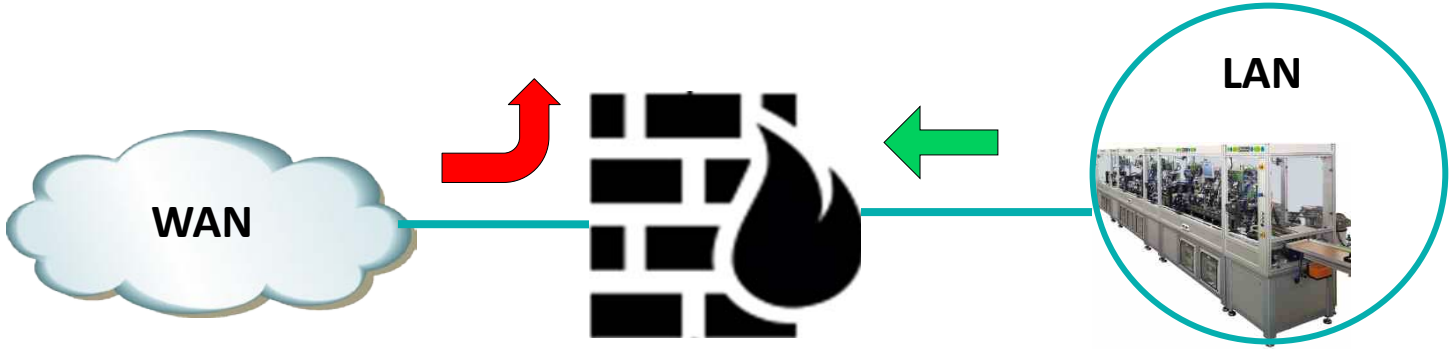
- Per la segmentazione in celle si possono sfruttare le cosiddette Virtual Local Area Network (VLAN)
- Prevedendo nell'infrastruttura di rete PROFINET degli switch di tipo ''managed'' è possibile creare delle sottoreti virtuali (le VLAN)
- Attraverso questa segmentazione sarà possibile definire anche delle adeguate politiche di accesso

Security & Profinet



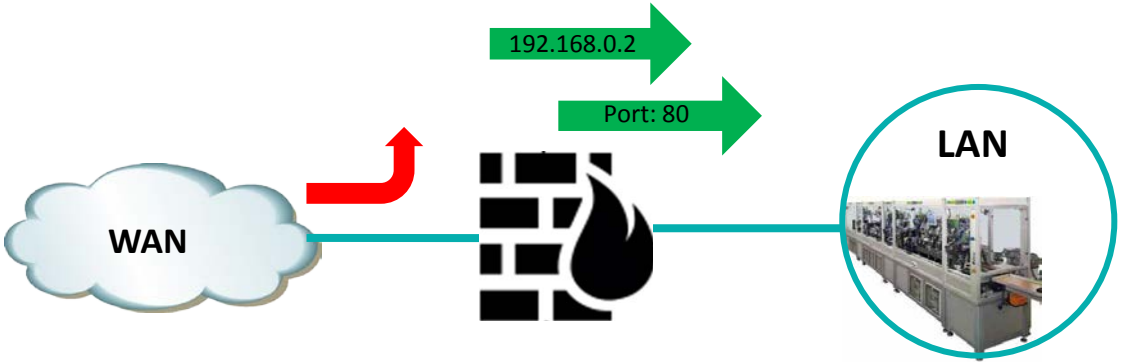
- Un’altra forma di segmentazione è quella che utilizza la cosiddetta Demilitarized Zone (acronimo DMZ)
- Questo consente la creazione di una sottorete separata protetta in accesso da Firewall, all’interno della quale è possibile disporre dispositivi più sensibili dal punto di visto della protezione dei dati
- Classici dispositivi dotati di porta DMZ sono i cosiddetti ‘’security router’’

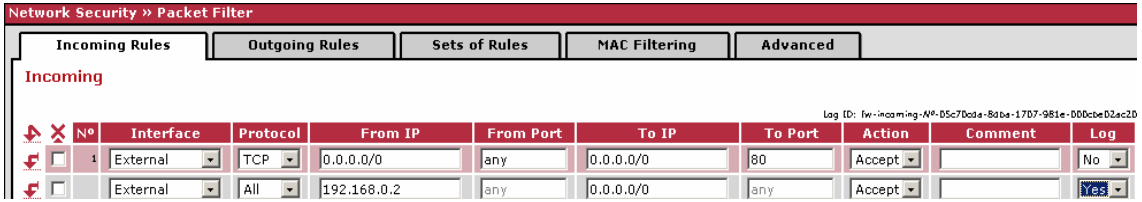
Security & Profinet



- Un Firewall (dispositivo hardware e/o firmware) ideale permette la comunicazione solo da una rete protetta (rete LAN) verso l'esterno (rete WAN, normalmente non sicura), impedendo accessi in senso opposto

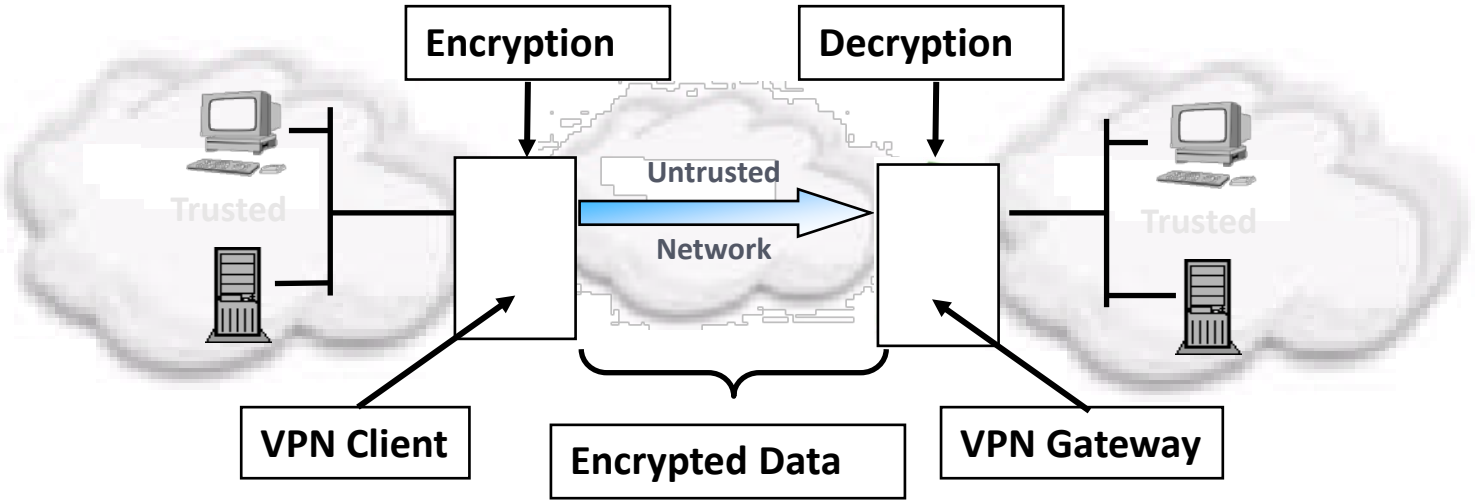
Security & Profinet





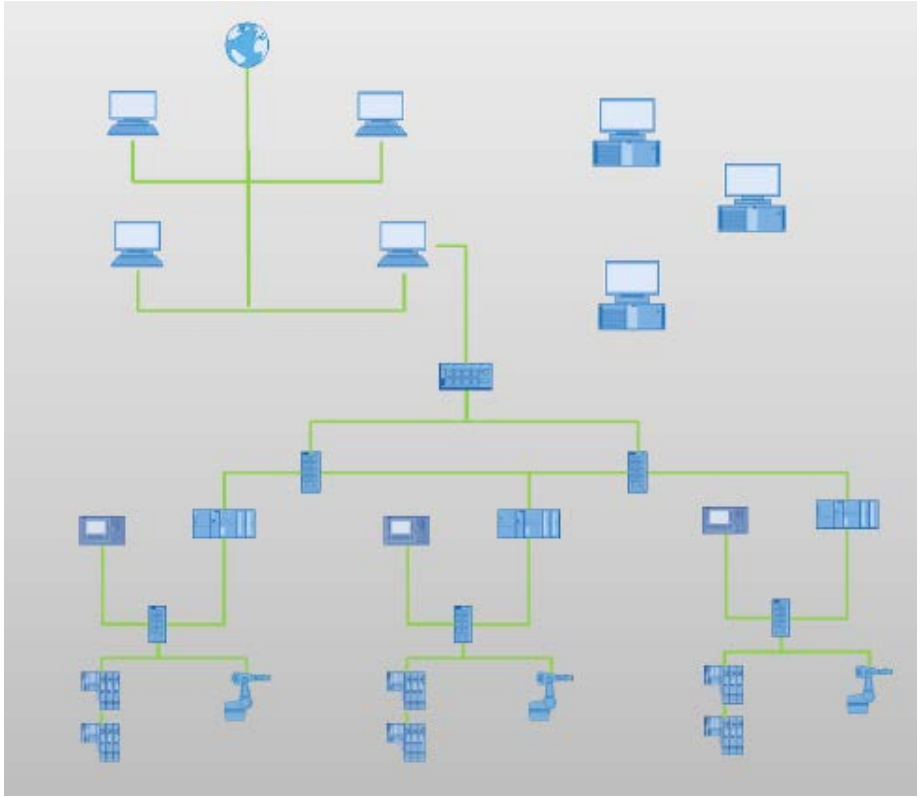
- Dispositivi dotati di Firewall configurabile permettono l'accesso WAN -> LAN solo secondo regole ben precise

Security & Profinet



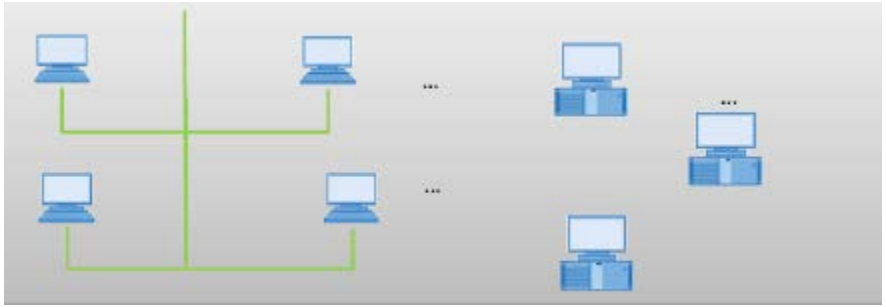
- Un tunnel VPN consente una comunicazione crittografata e quindi sicura attraverso una rete ”insicura” (ad esempio Intenet)

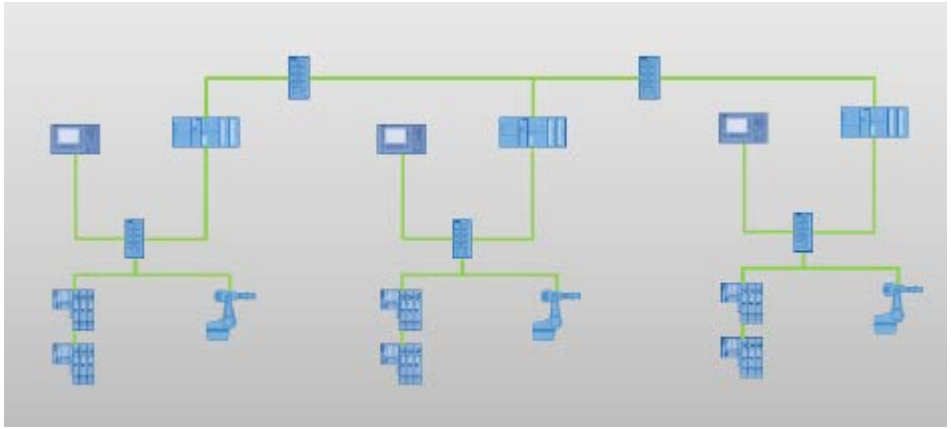
Security & Profinet



- Come proteggere al meglio una rete PROFINET seguendo il concetto di segmentazione della IEC 62433?
- Quali le conseguenze delle scelte decisionali relativamente alle modalità di segmentazione sulla funzionalità della rete?

Security & Profinet



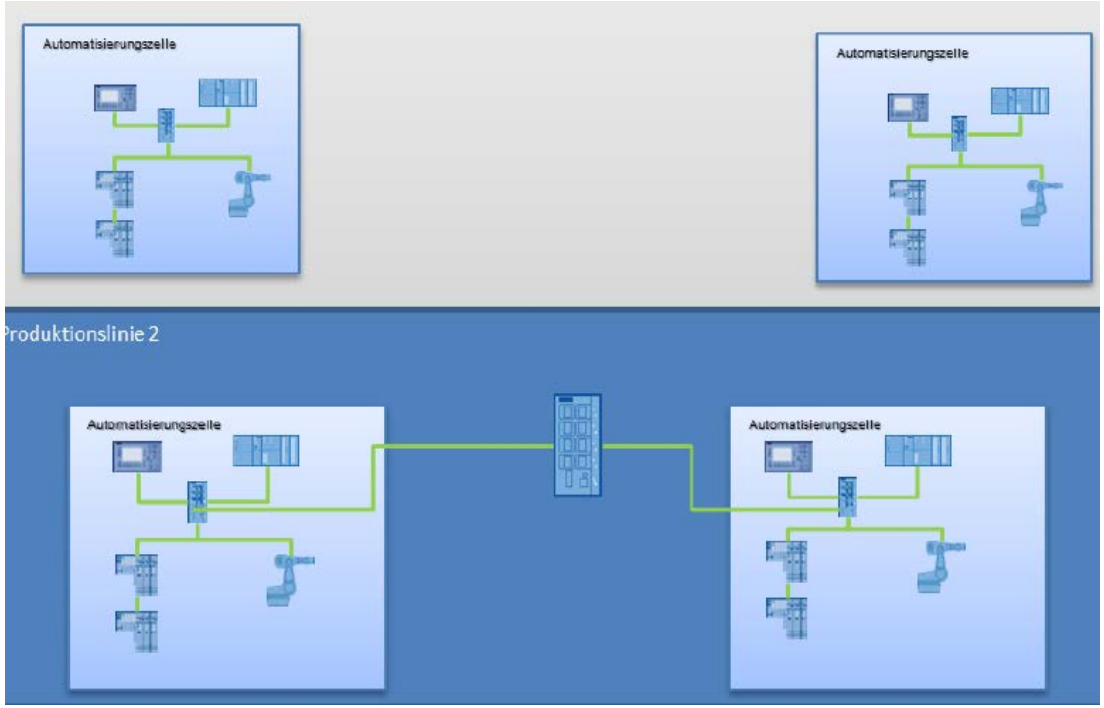


- Separazione tra rete di produzione e rete office
- Il percorso tra le due reti sarà adeguatamente protetto (ad esempio per mezzo di security router con firewall)
- La rete di produzione potrà poi a sua volta essere suddivisa in celle di automazione

Security & Profinet

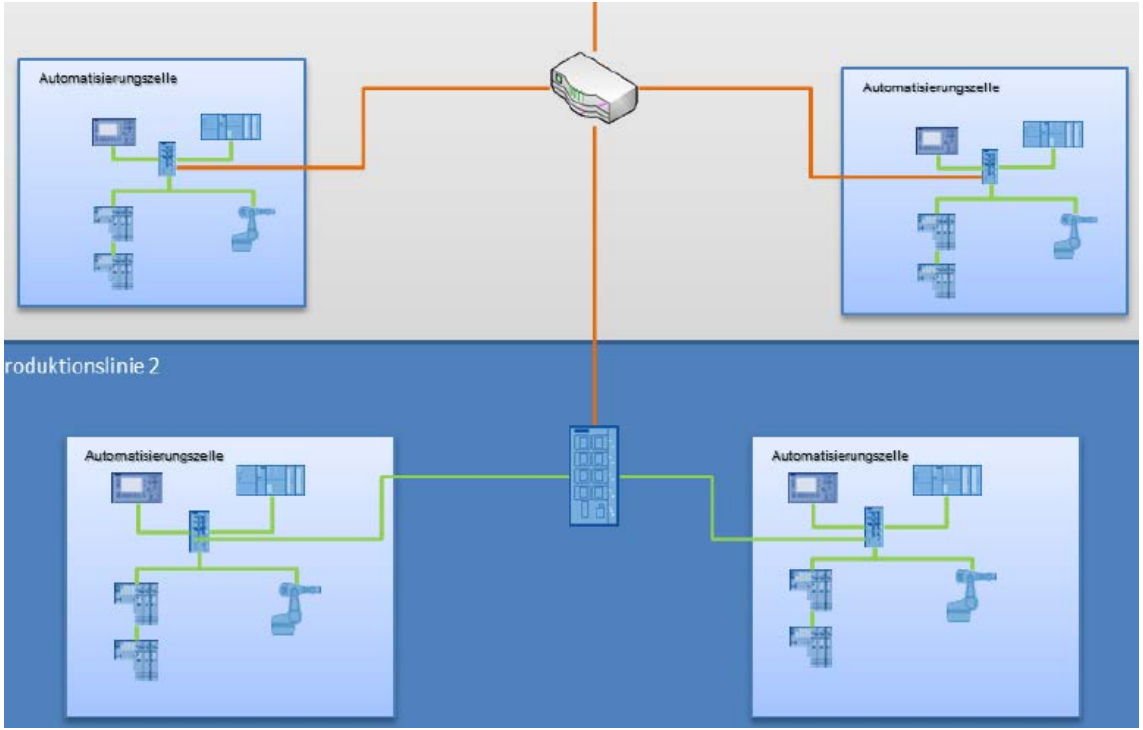
- Esempio di scomposizione in quattro celle, a due a due appartenenti a linee di produzione differenti

Security & Profinet



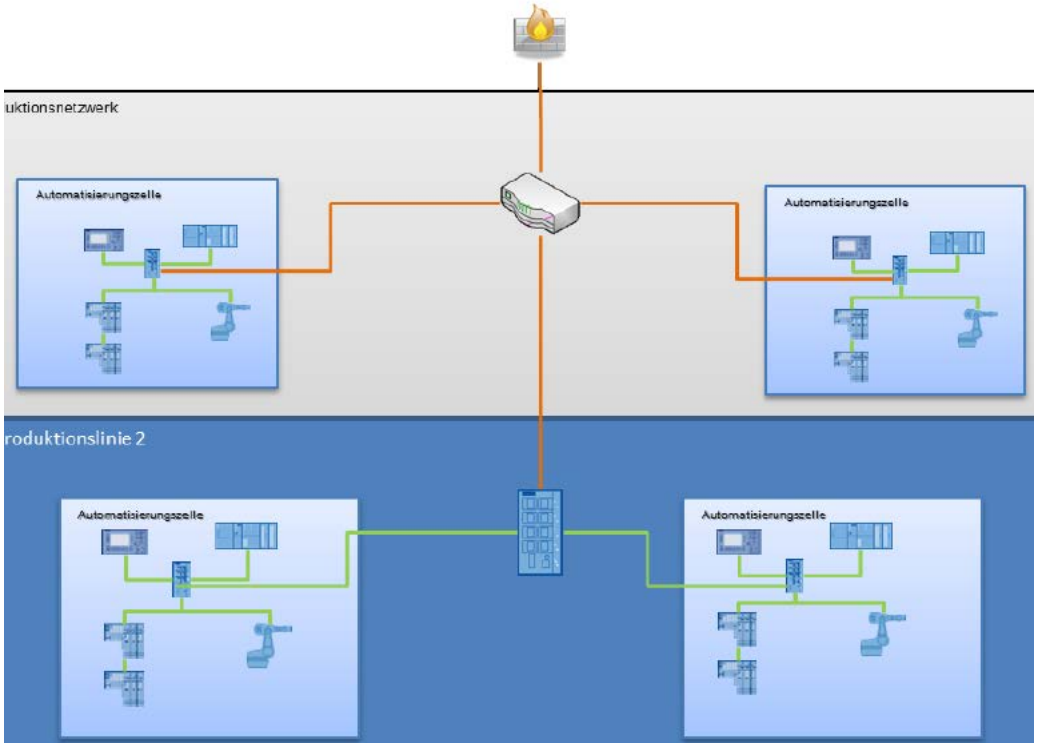
- Se necessaria una comunicazione di Layer 2 tra due celle di una medesima linea (per esempio per assegnare il nome a dispositivi PROFINET), la stessa può essere realizzata mediante l'utilizzo di switch
- Messaggi multicast possono raggiungere dispositivi di entrambe le celle

Security & Profinet



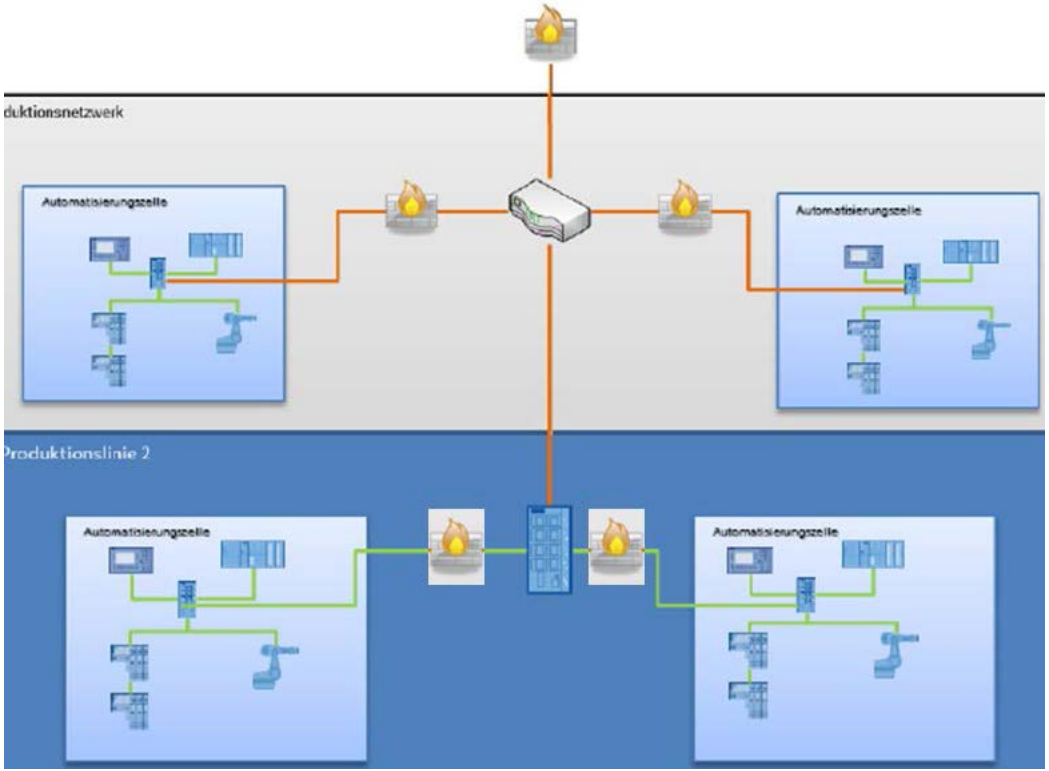
- Se è invece necessaria una comunicazione IP-based (quindi di Layer3), diventa necessario l'utilizzo di un router
- La comunicazione di Layer 2 tra le due linee non è possibile e non è quindi possibile l'uso completo dei servizi PROFINET

Security & Profinet



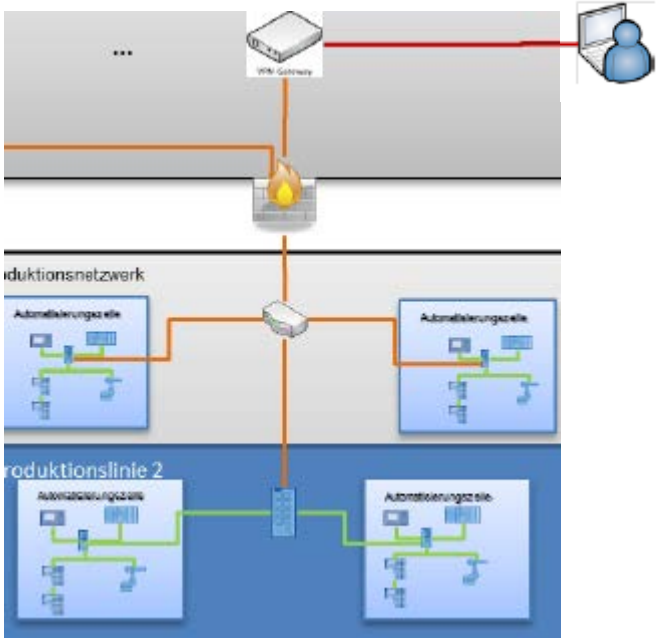
- Per separare in modo efficace la rete di produzione dalla rete IT, può essere utilizzato un Firewall che possa almeno definire delle regole basate su indirizzi IP e numero di porte

Security & Profinet



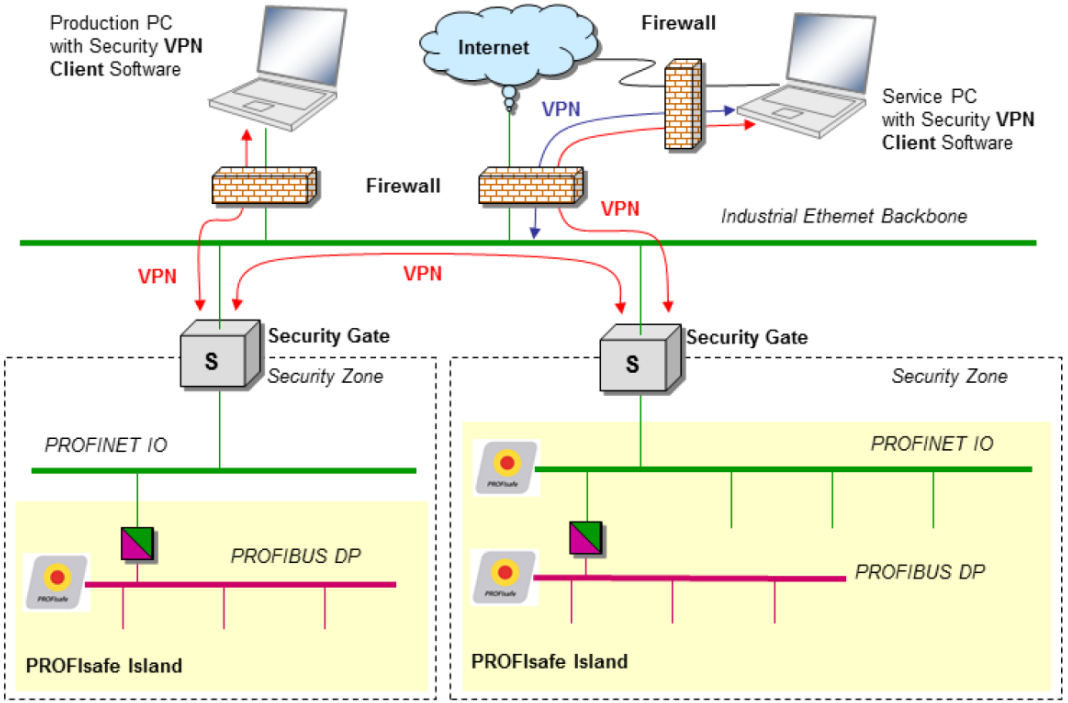
- L’utilizzo di Firewall in ingresso a ogni cella permette una maggiore flessibilità nella definizione delle regole di accesso e accresce, di conseguenza, il livello di protezione della rete

Security & Profinet



- Volendo consentire accessi da remoto, ad esempio per operazioni di teleassistenza, può essere previsto un collegamento via VPN
- Il gateway VPN è a monte del Firewall ci modo che anche il traffico che attraversa il tunnel VPN può accedere o meno alle celle in funzione delle regole di configurazione del Firewall

Security & Profinet



- Se infine sulla rete sono presenti tratti con dispositivi PROFIsafe, questi dispositivi devono essere raggruppati in celle dedicate
- L'accesso a e tra tali celle deve prevedere adeguata protezione (security gate con VPN/Firewall)

GRAZIE

per l‘attenzione