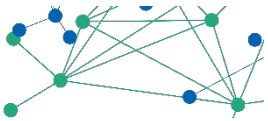
PI Italia
PROFIBUS • PROFINET

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

© 2017 PROFIBUS e PROFINET Italia

Safety vs. Security

© 2017 PROFIBUS e PROFINET Italia

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″

© 2017 PROFIBUS e PROFINET Italia

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″:

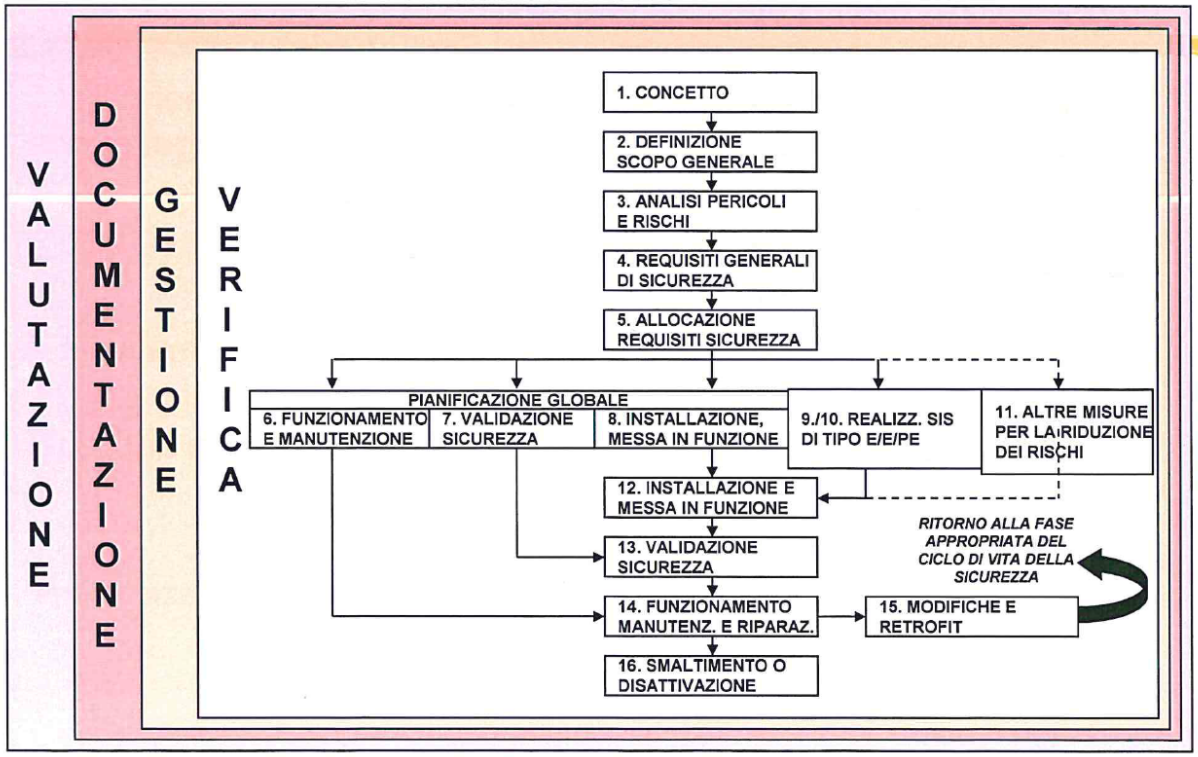
″Prevenzione di accessi illegali o non voluti o di interferenze nello specifico e previsto funzionamento di un sistema di comando e controllo per l'automazione industriale"

© 2017 PROFIBUS e PROFINET Italia

I campi di applicazione della safety

Protezione macchine	Processo	Trasporti
■Nastri ■Presse ■Macchine di produzione ■Controlli	■Bruciatori ■Industria petrolifera ■Chimica ■Farmaceutica	■Funivie ■Ascensori ■...

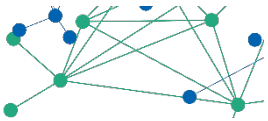
Safety in ambiente industriale



- La safety interessa l'intero ciclo di vita del macchinario/processo
- Impatta anche sul sistema di gestione
- Definizione dell'organizzazione
- Definizione delle responsabilità
- Individuazione della documentazione di riferimento

© 2017 PROFIBUS e PROFINET Italia

Legislazione di riferimento per la safety macchine



- Qualsiasi dispositivo o macchinario, per essere liberamente commercializzato all'interno dei paesi della Comunità Europea, deve soddisfare le prescrizioni delle direttive comunitarie. Esse stabiliscono i principi generali affinché i costruttori mettano in commercio prodotti che non siano pericolosi per gli operatori.
- I pericoli derivanti dal funzionamento dei macchinari sono trattati dalla Direttiva Macchine 2006/42/EC.
- La conformità alle direttive viene certificata mediante l'emissione della Dichiarazione di Conformità da parte del costruttore e dall'apposizione della marcatura CE sulla macchina stessa.

© 2017 PROFIBUS e PROFINET Italia

Legislazione di riferimento per la safety Processo

- Lato processo non esiste una Direttiva Europea
- Esistono le norme tecniche specifiche di settore e generiche per il mondo safety
- Esiste la legislazione generale di sicurezza sul lavoro (DLgs. 81/08)

Cogente

© 2017 PROFIBUS e PROFINET Italia

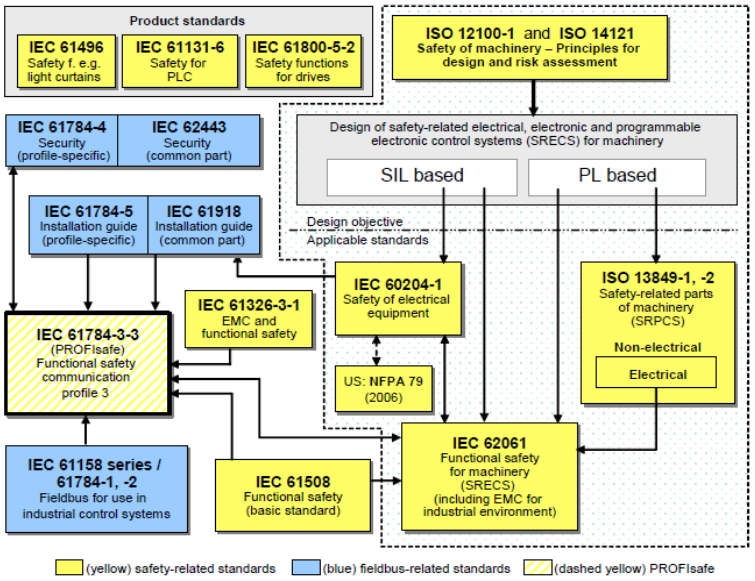
Normativa di riferimento per la safety

- Per la valutazione dei rischi che la macchina presenta e per la realizzazione dei sistemi di sicurezza atti a proteggere l'operatore da detti rischi gli enti normatori europei CEN e CENELEC hanno emanato una serie di norme che traducono in indicazioni tecniche il contenuto delle direttive.
- Una norma diventa armonizzata quando viene pubblicata negli Stati membri della comunità
- Un prodotto costruito in conformità ad una norma armonizzata europea (EN), il cui riferimento è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea per una specifica Direttiva e che risponde ad uno o più dei requisiti essenziali di sicurezza e di tutela della salute, è presunto conforme ai requisiti essenziali di tale Direttiva

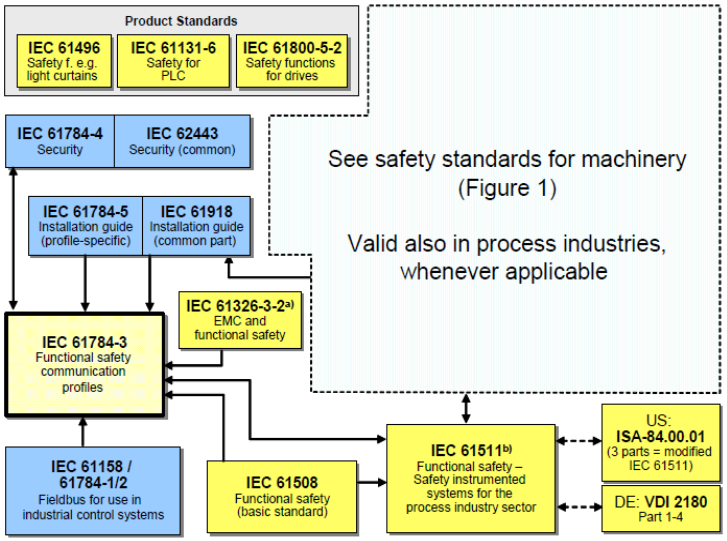
© 2017 PROFIBUS e PROFINET Italia

Safety in ambiente industriale

Norme tecniche attinenti



Macchinario

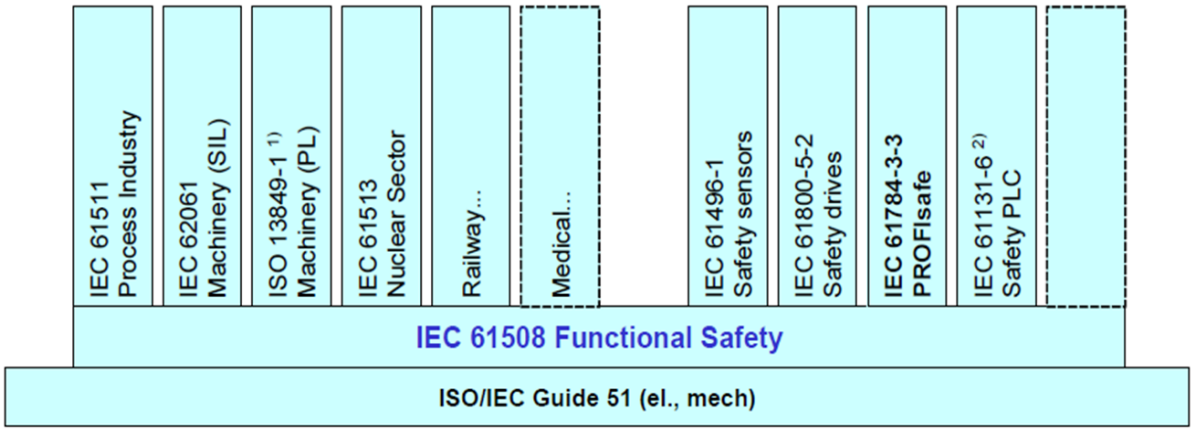


Processo

© 2017 PROFIBUS e PROFINET Italia

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



© 2017 PROFIBUS e PROFINET Italia

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

© 2017 PROFIBUS e PROFINET Italia

Safety Integrity Level (SIL)

- Livello di Integrità di Sicurezza (SIL): è un livello discreto (da 1 a 4) per specificare i requisiti di integrità di sicurezza delle funzioni di sicurezza che devono essere assegnate ai SIS, dove il livello 4 rappresenta il livello più alto di integrità di sicurezza ed il livello 1 il livello più basso di integrità di sicurezza.

Safety Integrity Level (SIL)	Probabilità di fallimento	Risk Reduction Factor (RRF)
SIL 4	$\geq 10^{-5} \ldots < 10^{-4}$	>10000 ... ≤100000
SIL 3	$\geq 10^{-4} \ldots < 10^{-3}$	>1000 ... ≤10000
SIL 2	$\geq 10^{-3} \ldots < 10^{-2}$	>100 ... ≤1000
SIL 1	$\geq 10^{-2} \ldots < 10^{-1}$	>10 ... ≤100

Relazione tra Riduzione del Rischio, probabilità di Fallimento e SIL di una Funzione di Sicurezza

© 2017 PROFIBUS e PROFINET Italia

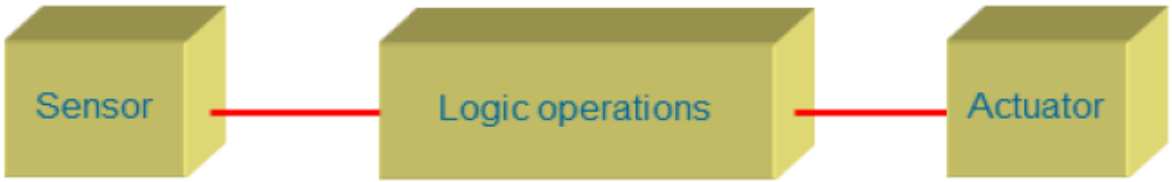
Performance Level (PL)

- Performance Level (PL): è un livello discreto (da 1 a 5) a, b, c, d, e. PL è il livello di affidabilità per realizzare la riduzione richiesta di rischio per ogni funzione di sicurezza, ovvero la capacità di un sistema di comando e controllo di svolgere una funzione di sicurezza sotto determinate condizioni, al fine di ottenere la prevista riduzione dei rischi.

Performance level (PL)	Average probability of a dangerous failure per hour [1/h]
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

© 2017 PROFIBUS e PROFINET Italia

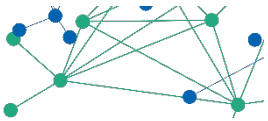
Safety in ambiente industriale



- Catena di sicurezza a cui si applica la definizione di SIL o di PL
- Probabilità di guasto a budget diversi per i singoli componenti

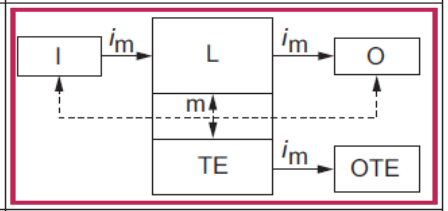
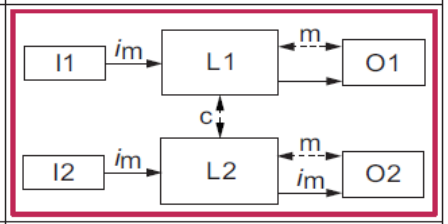
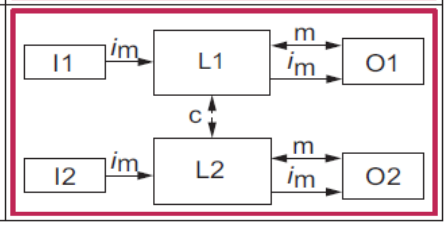
© 2017 PROFIBUS e PROFINET Italia

Parametri di interesse per i due standard



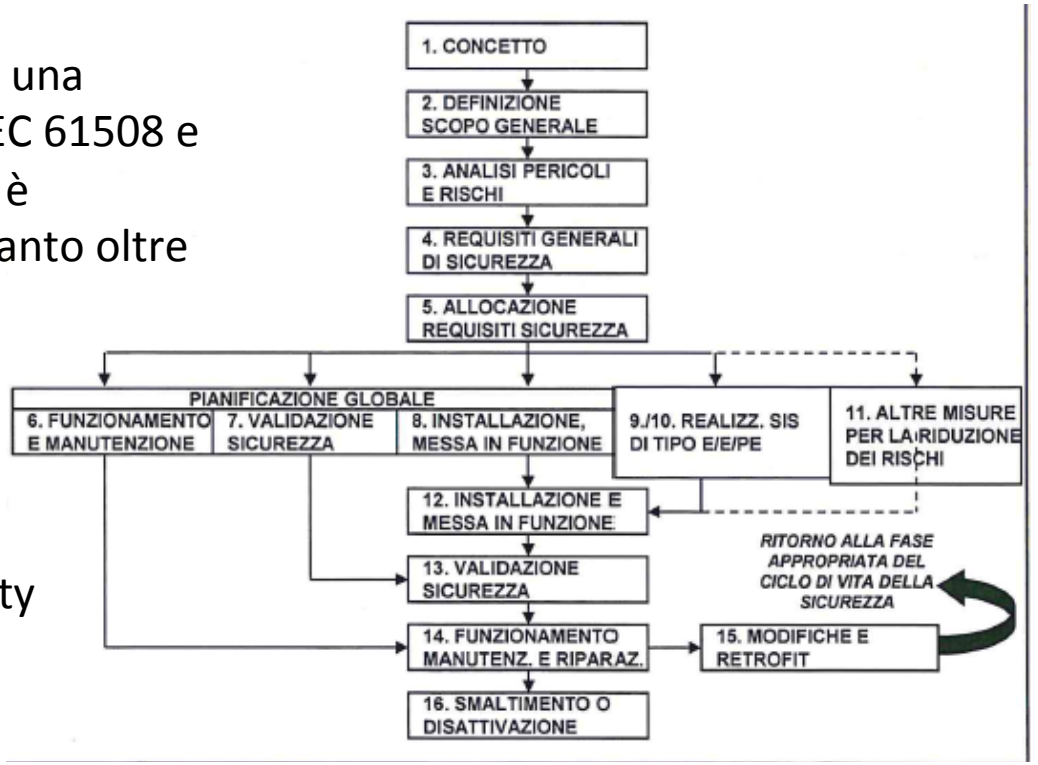
‘Parametri ISO’	‘Parametri IEC’
PL: Performance Level	SIL: Safety Integrety Level
Categorie delle funzioni di sicurezza	Tipo di sottosistema: A,B,C, D
MTTF: Mean TimeTo Failure	Failure rate
DC: Copertura Diagnostica	DC: Copertura Diagnostica
CCF: guasti di modo comune	CCF: guasti di modo comune

Vincoli archietturali per il sistema PL

Cat.	System behaviour	Designated architectures
B	A fault can lead to loss of the safety function	
1	As for category B but the probability of this occurence is lower than for the category B	
2	A fault can lead to loss of the safety function between two periodic inspections and loss of the safety function is detected by the control system at the next test.	
3	For a single fault, the safety function is always ensured. Only some faults will be detected. The accumulation of undetected faults can lead to loss of the safety function.	
4	When faults occur, the safety function is always ensured. Faults will be detected in time to prevent loss of the safety function	

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



© 2017 PROFIBUS e PROFINET Italia

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)

Error \ Meas.	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				●	●			●

© 2017 PROFIBUS e PROFINET Italia

Safety & Profibus/Profinet: il profilo PROFIsafe

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

PROFINET®

e/o

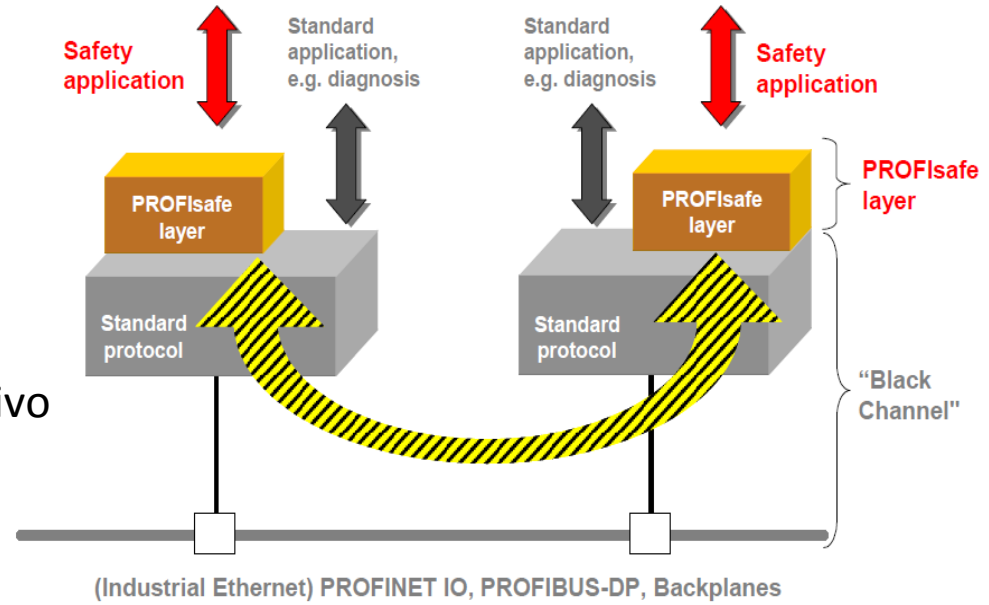
PROFIBUS®

© 2017 PROFIBUS e PROFINET Italia

Safety & Profibus/Profinet: il profilo PROFIsafe

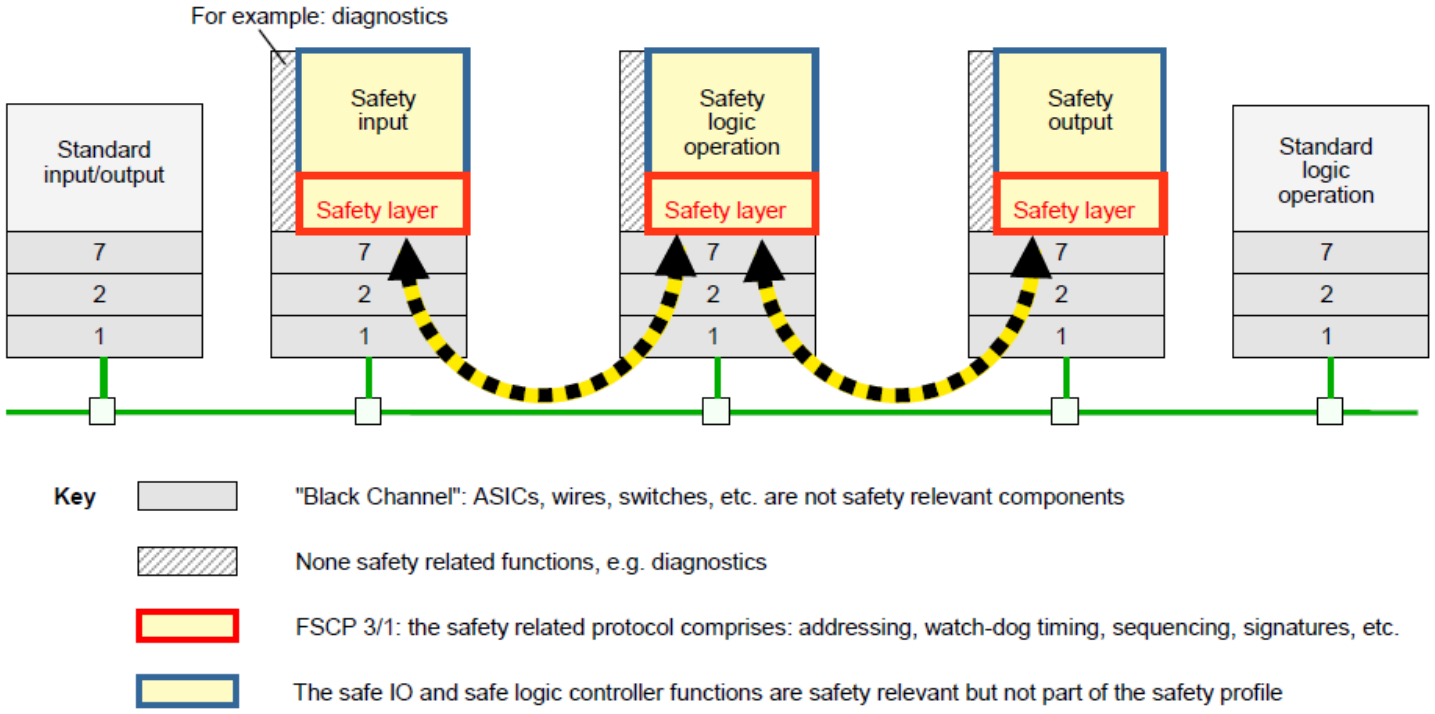
PROFIsafe

- 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



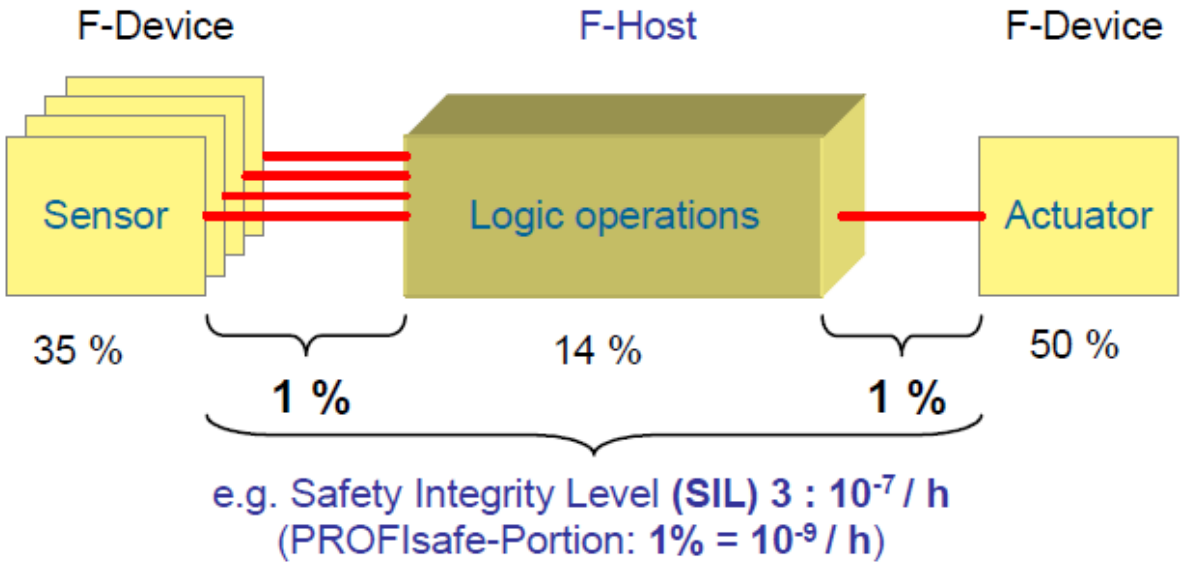
© 2017 PROFIBUS e PROFINET Italia

Safety & Profibus/Profinet: il profilo PROFIsafe



© 2017 PROFIBUS e PROFINET Italia

Safety & Profibus/Profinet: il profilo PROFIsafe



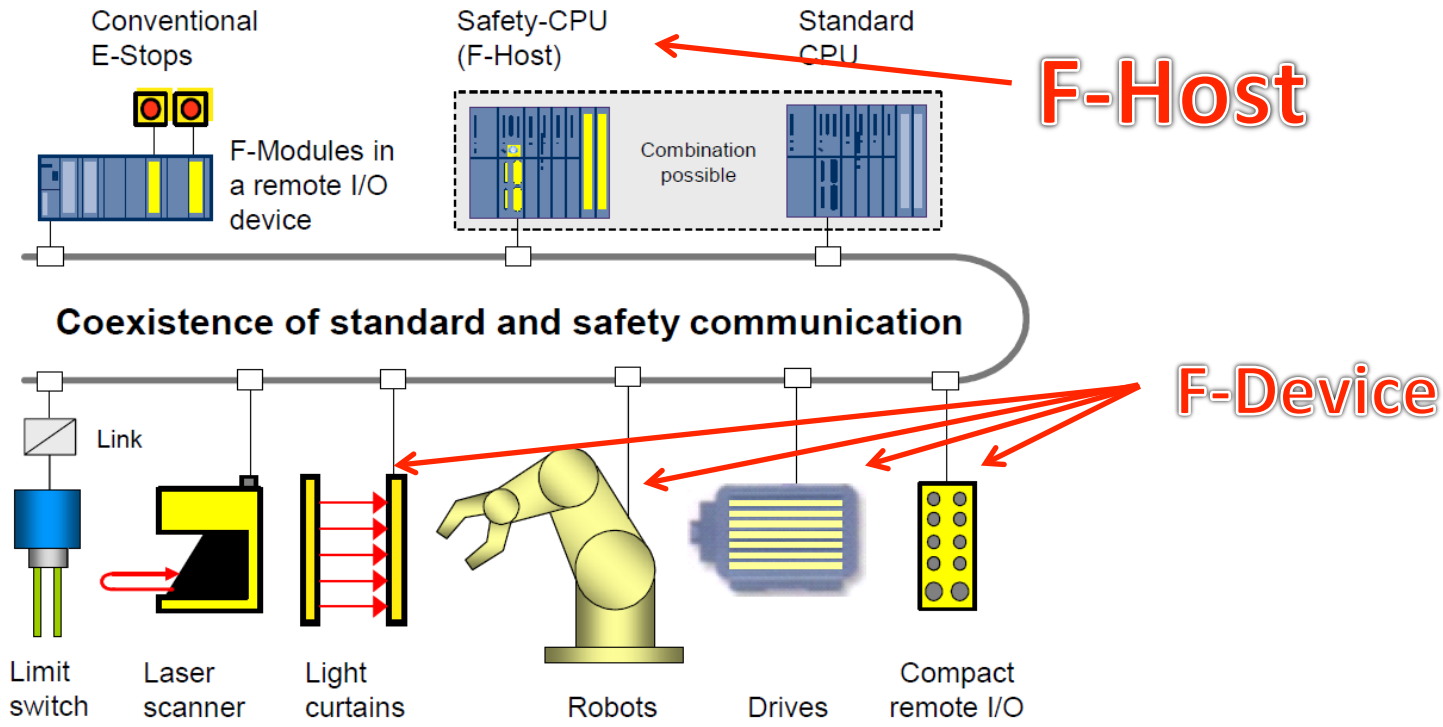
Layer di comunicazione sopra Profibus e Profinet

CERTIFICATO SIL 3

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

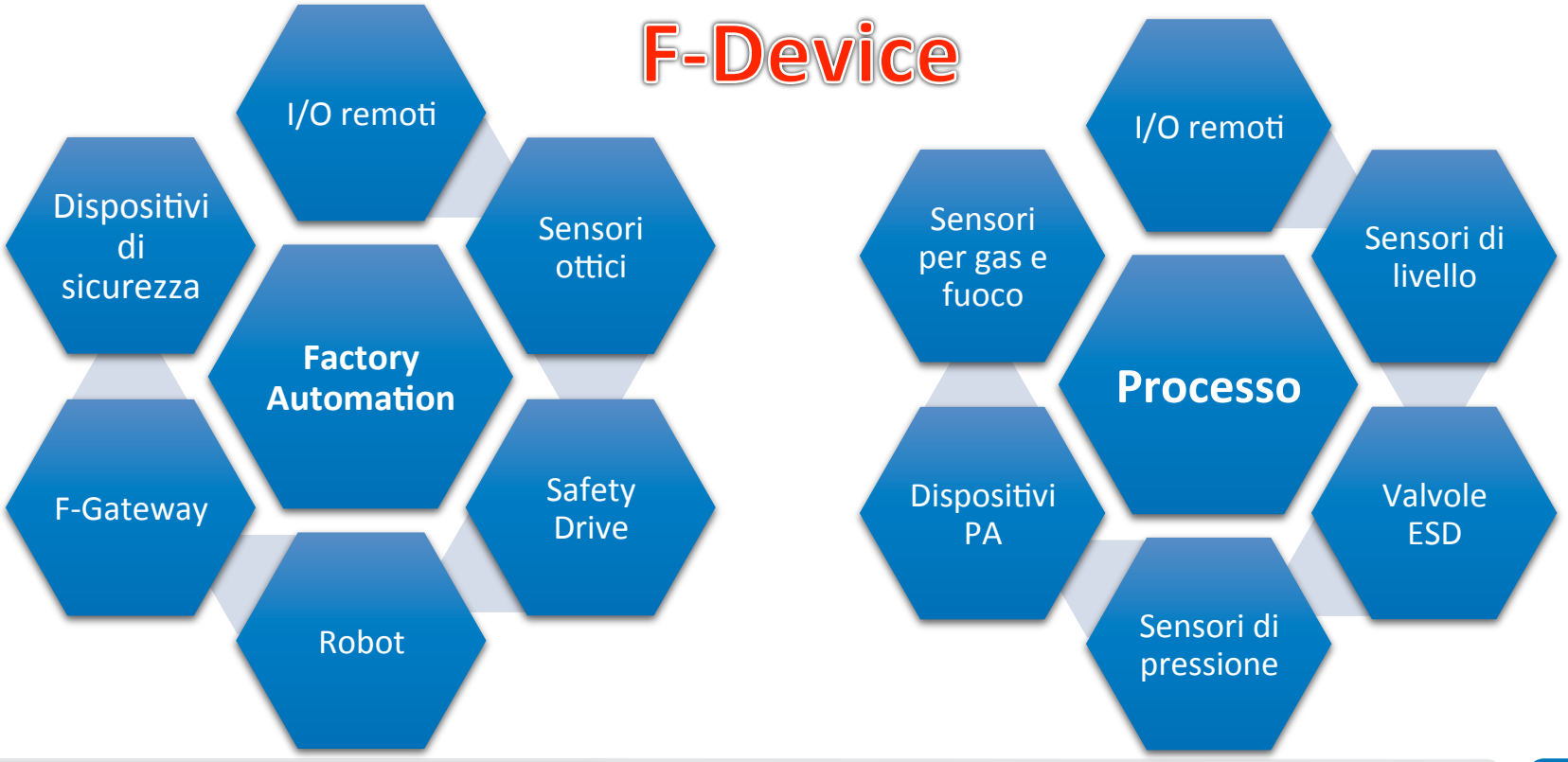
© 2017 PROFIBUS e PROFINET Italia

Safety & Profibus/Profinet: il profilo PROFIsafe



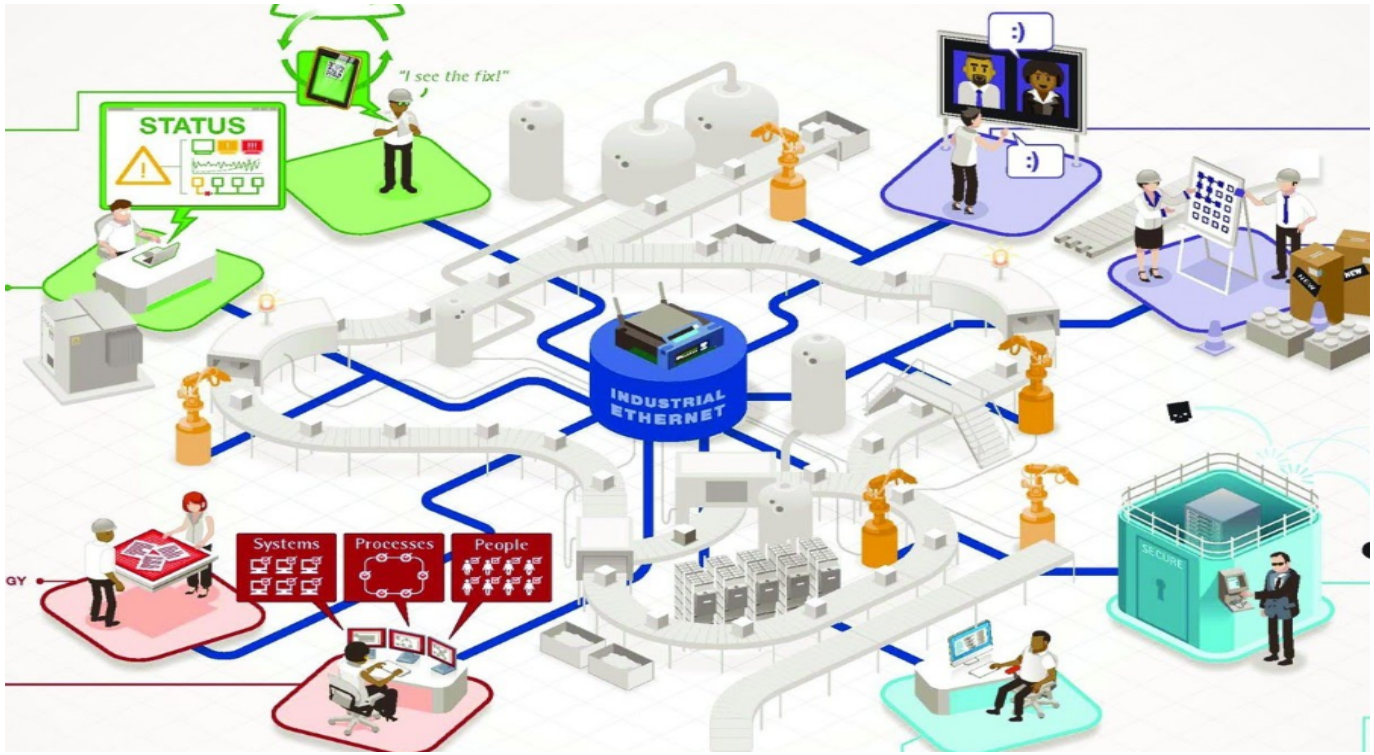
© 2017 PROFIBUS e PROFINET Italia

Safety & Profibus/Profinet: il profilo PROFIsafe



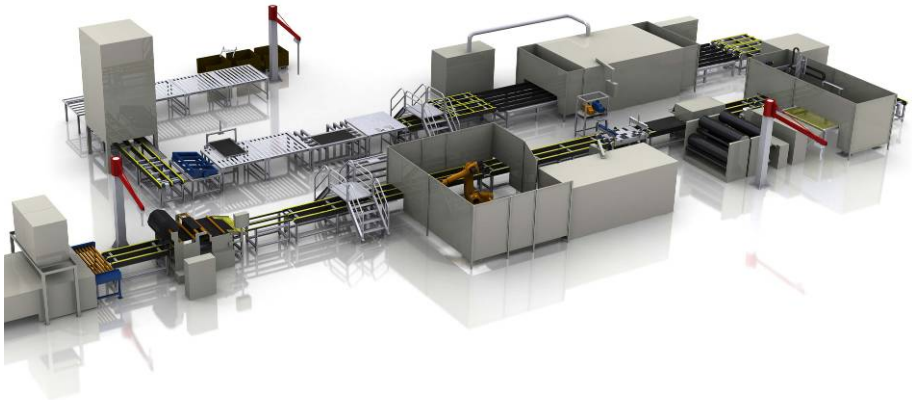
© 2017 PROFIBUS e PROFINET Italia

Security in ambiente industriale



© 2017 PROFIBUS e PROFINET Italia

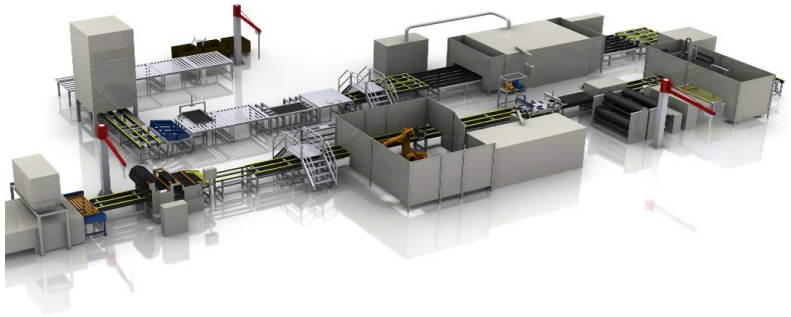
Security in ambiente industriale

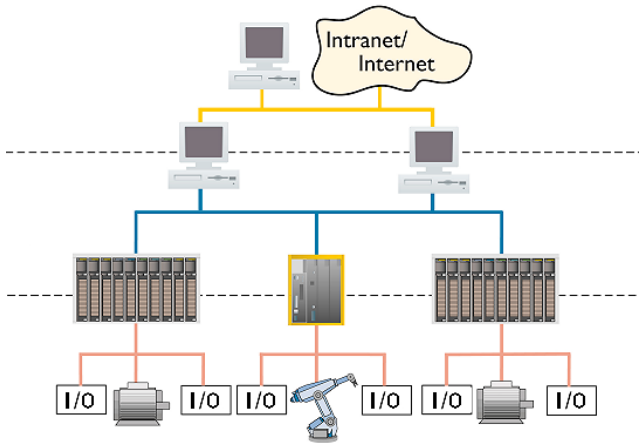


- Con fieldbus su base seriale e macchina non interconnessa, le preoccupazioni dei progettisti di automazione nei confronti della security si limitavano al predisporre opportune misure e/o modalità operative tali da evitare accessi al progetto installato sul sistema di controllo
- Questo al fine di evitare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

© 2017 PROFIBUS e PROFINET Italia

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

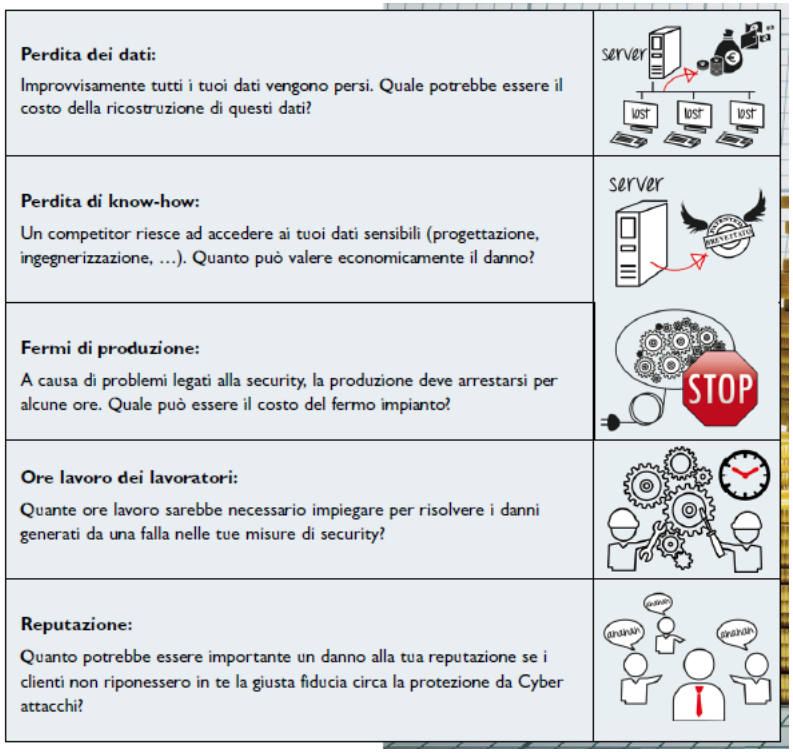
© 2017 PROFIBUS e PROFINET Italia

Security in ambiente industriale

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

Qualche esempio ….

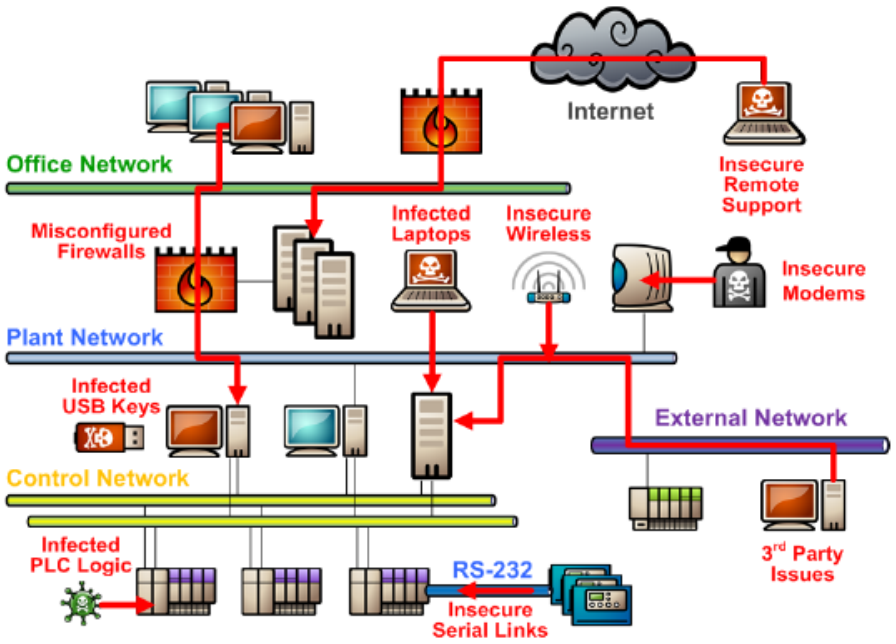
Lista (purtroppo) non esaustiva ….



© 2017 PROFIBUS e PROFINET Italia

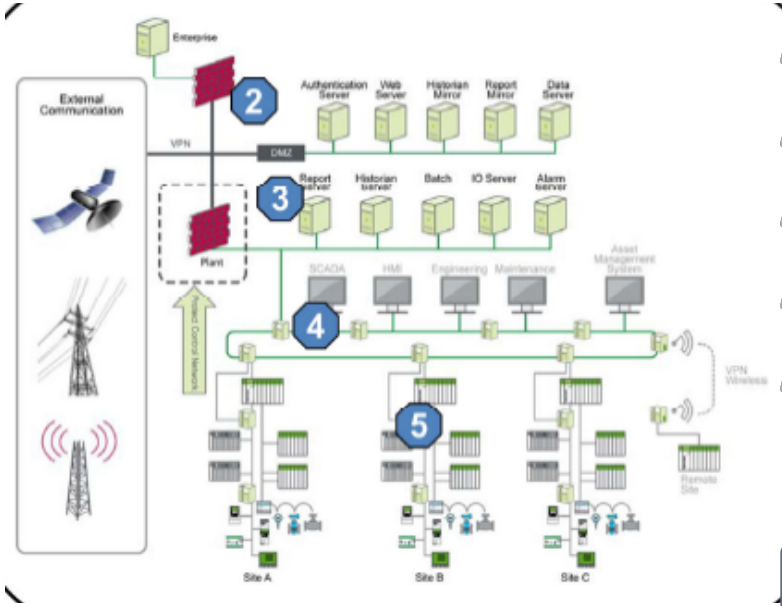
Security in ambiente industriale

- Connessioni remote per diagnostica
- MES in condivisione con utenti office
- Modem di accesso remoto
- Sistemi wireless
- Porte UBS
- PC portatili
- Scambio di file



© 2017 PROFIBUS e PROFINET Italia

Security in ambiente industriale



- Security plan
- Separazione delle reti
- Protezione del perimetro
- Segmentazione della rete
- Device hardening
- Monitoring and updating

Defense in depth

© 2017 PROFIBUS e PROFINET Italia

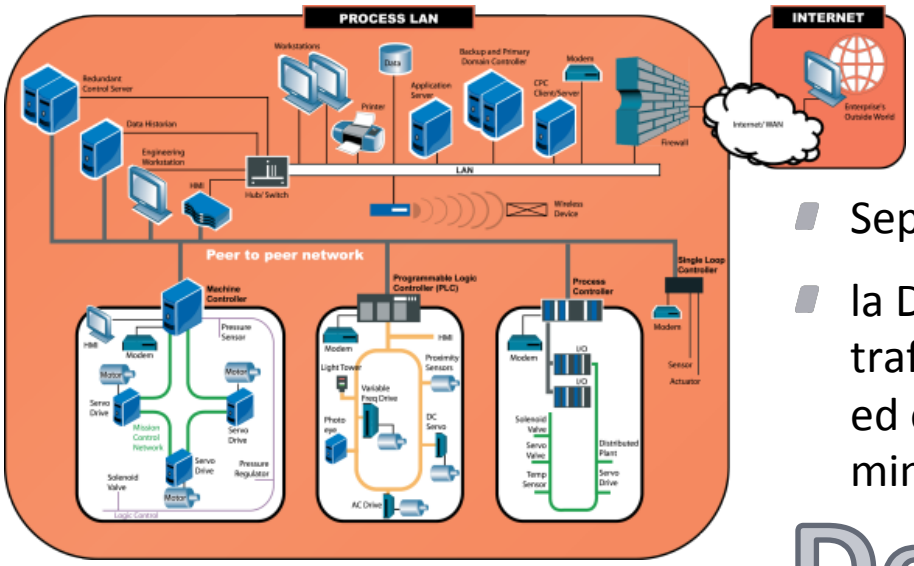
Security in ambiente industriale

- Security plan
- Procedure e policies aziendali che si occupano di
  - Valutazione del rischio
  - Gestione del rischio
  - Riduzione del rischio
  - Strategie per il disaster recovery

Defense in depth

© 2017 PROFIBUS e PROFINET Italia

Security in ambiente industriale



- Separazione delle reti
- Separazione delle reti per mezzo di una DMZ
- Separazione del mondo IT dal mondo OT
- la DMZ è un'area pubblica protetta, dove il traffico è strettamente regolato da entrambi i lati ed è utile per pubblicare servizi verso l'esterno minimizzando i rischi per la rete interna.

Defense in depth

© 2017 PROFIBUS e PROFINET Italia

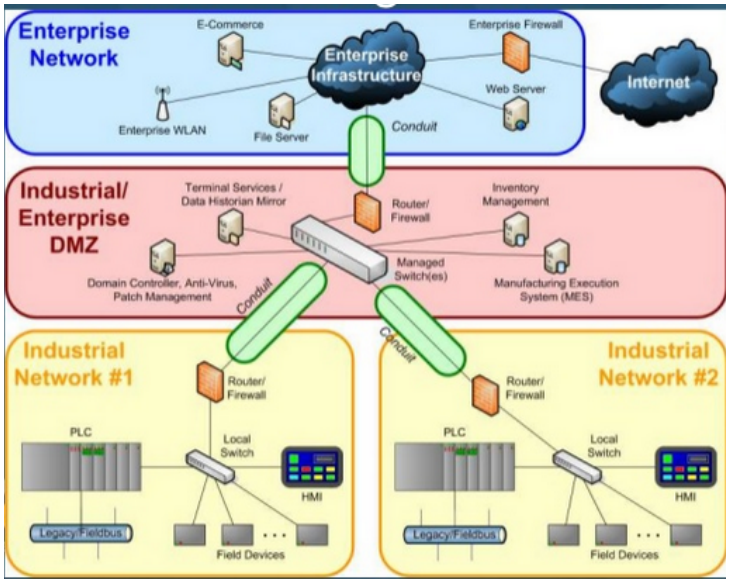
Security in ambiente industriale

- Protezione del perimetro
- Protezione del contenuto della rete per mezzo di policies e metodi di autenticazione per l'accesso
  - Firewallls
  - Autenticazione
  - VPN
  - Antivirus

Defense in depth

© 2017 PROFIBUS e PROFINET Italia

Security in ambiente industriale



- Segmentazione della rete
- Contenimento del potenziale problema di security solo entro un certo segmento
- Utilizzo di switches
- Utilizzo di VLAN
- Suddivisione della rete in sotto reti

Defense in depth

© 2017 PROFIBUS e PROFINET Italia

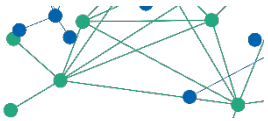
Security in ambiente industriale

- Device hardening
- Gestione delle password
- Definizione del profilo user
- Disattivazione dei servizi non impiegati

Defense in depth

© 2017 PROFIBUS e PROFINET Italia

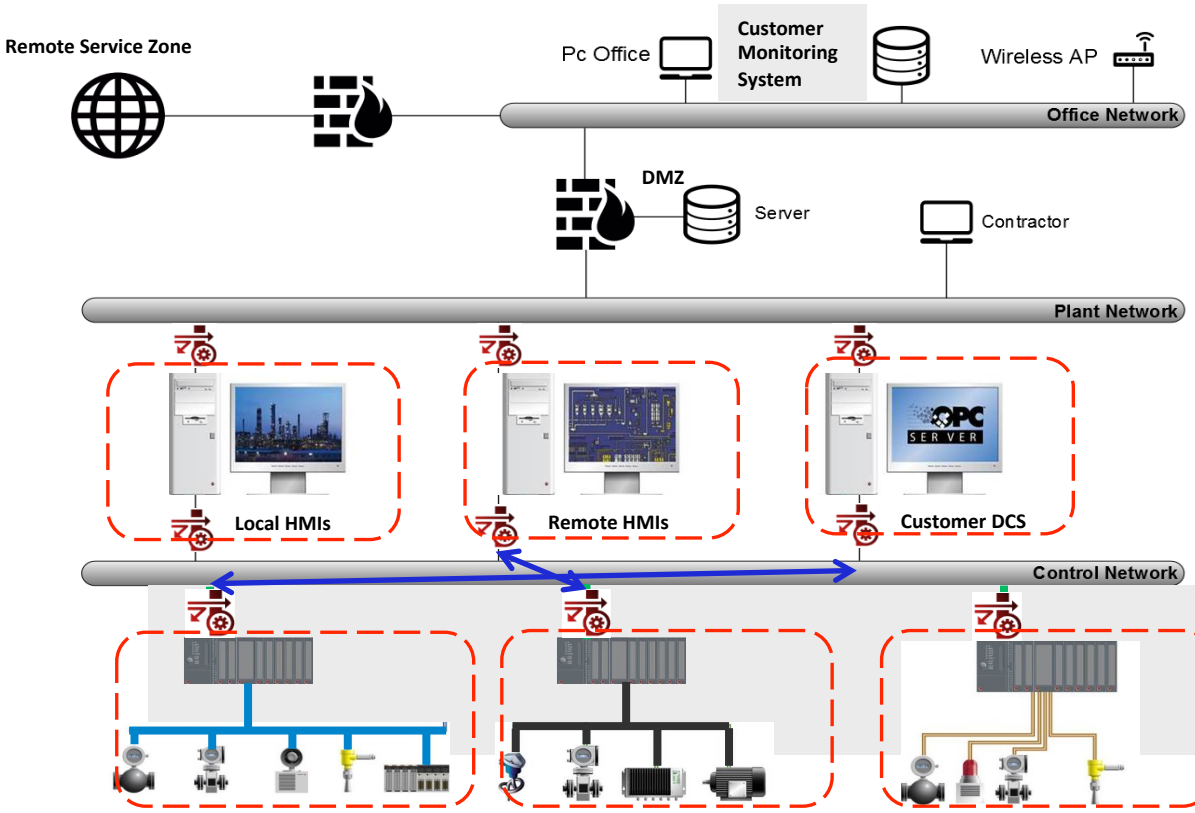
Security & Profinet



- 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)

© 2017 PROFIBUS e PROFINET Italia

Security & Profinet



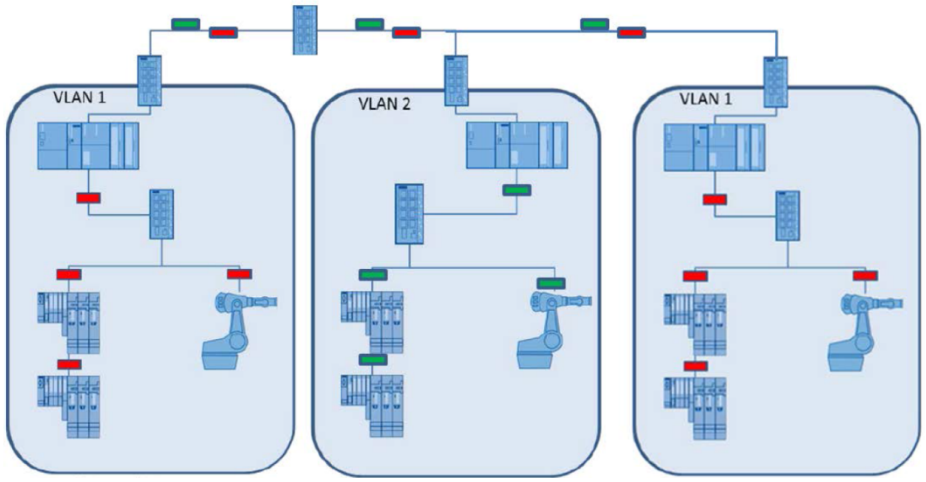
''Zone''

''Percorsi''

Dispositivi di protezione dei ''percorsi''

© 2017 PROFIBUS e PROFINET Italia

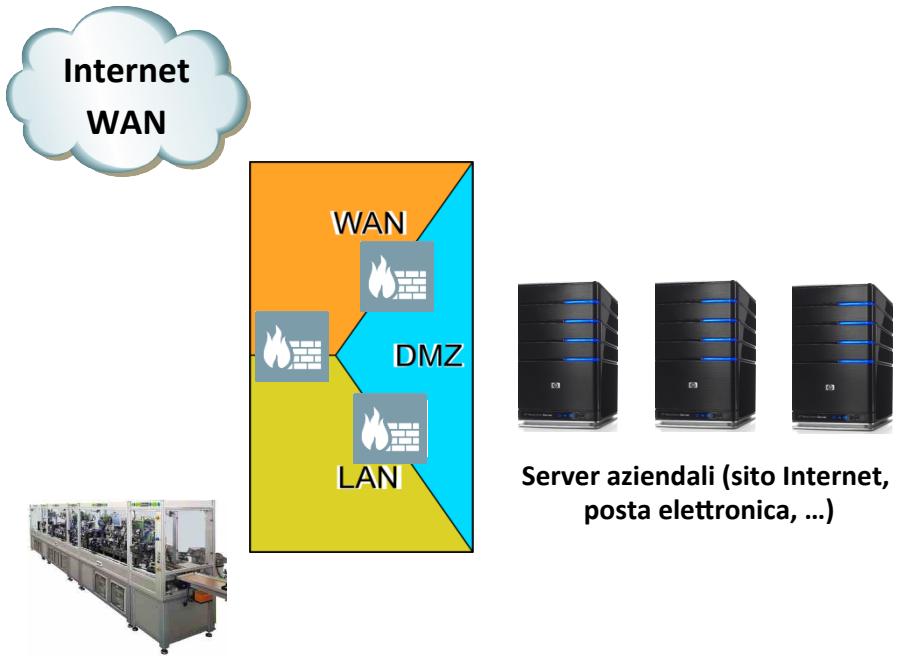
Security & Profinet



- 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

© 2017 PROFIBUS e PROFINET Italia

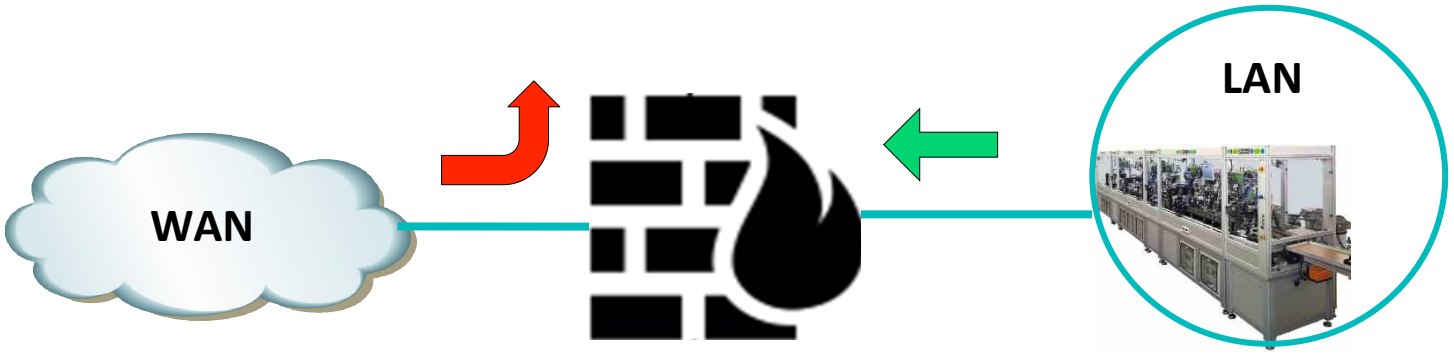
Security & Profinet



- 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''

© 2017 PROFIBUS e PROFINET Italia

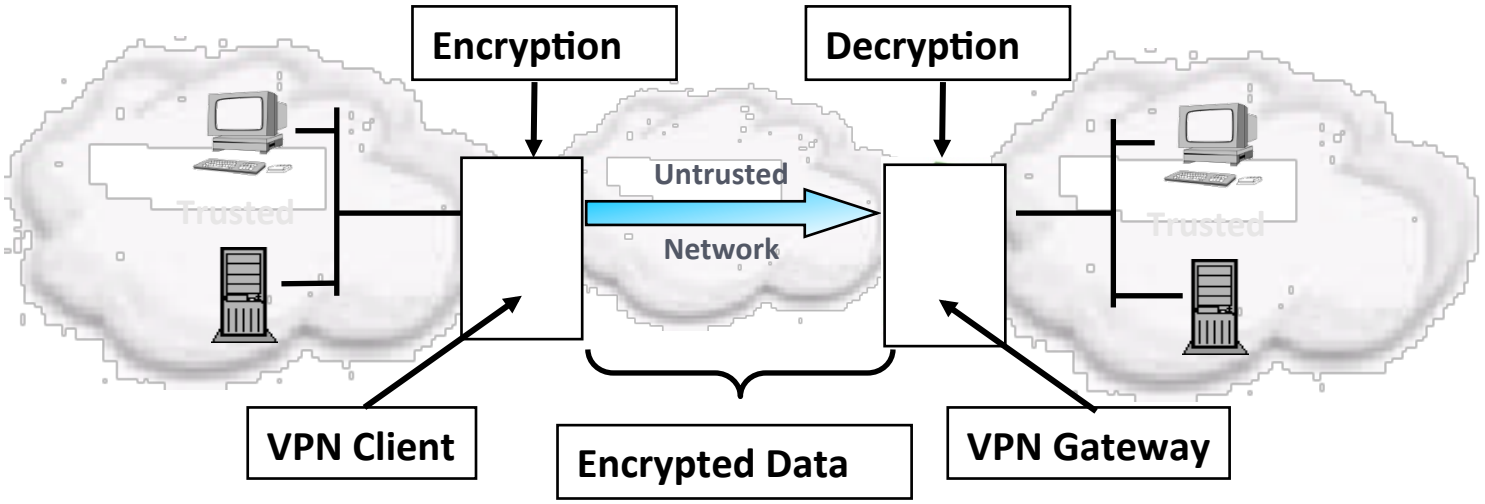
Security & Profinet



- 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

© 2017 PROFIBUS e PROFINET Italia

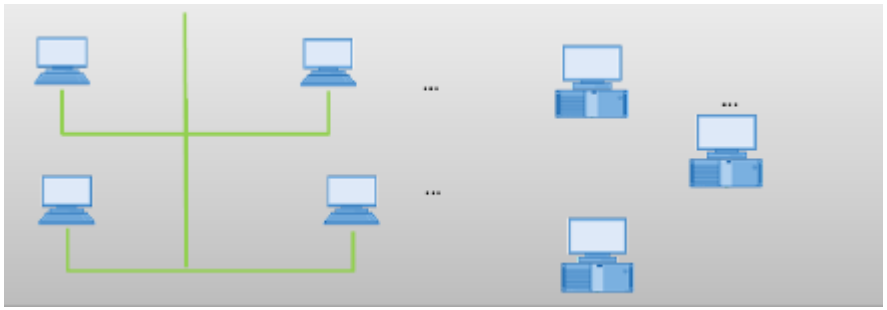
Security & Profinet

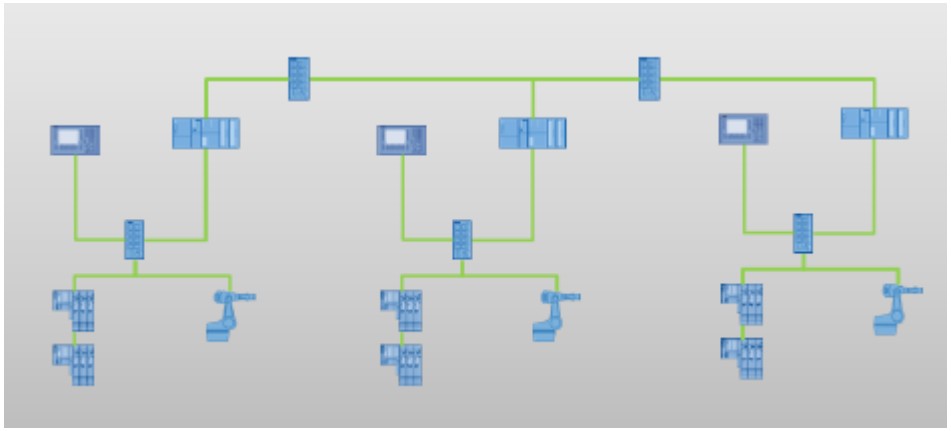


- Un tunnel VPN consente una comunicazione crittografata e quindi sicura attraverso una rete ″insicura″ (ad esempio Intenet)

© 2017 PROFIBUS e PROFINET Italia

Security & Profinet

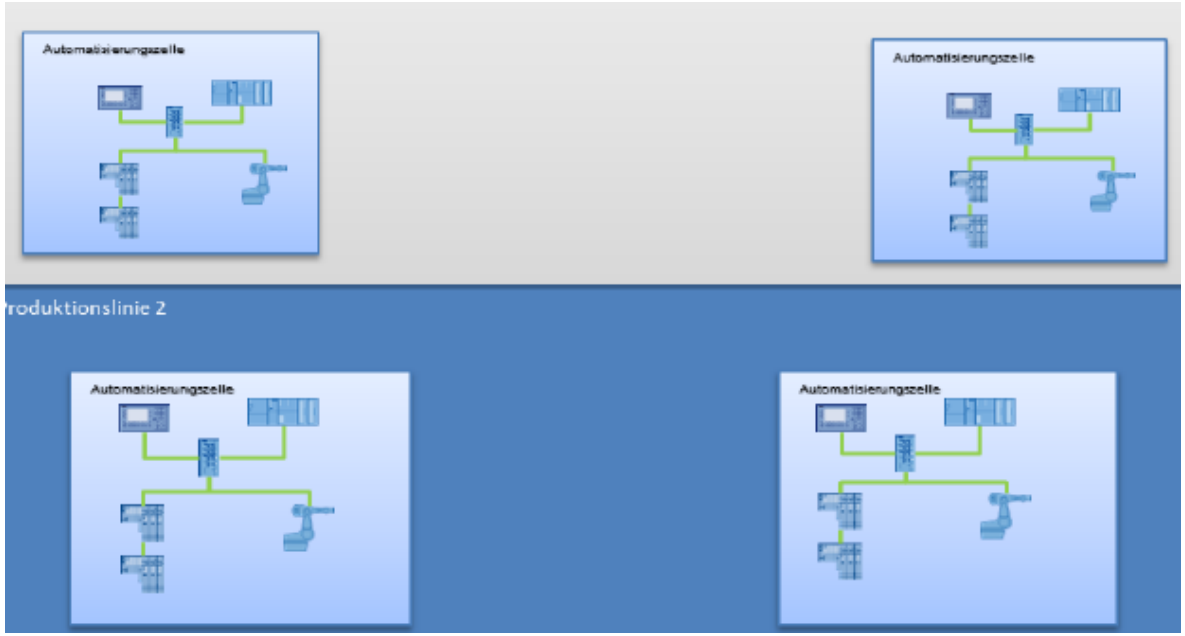




- Separazione tra rete di produzione e rete office
- Il percorso tra le due reti sarà adeguatamente protetto (ad esempio per mezzo di security router con firewall)
- La rete di produzione potrà poi a sua volta essere suddivisa in celle di automazione

© 2017 PROFIBUS e PROFINET Italia

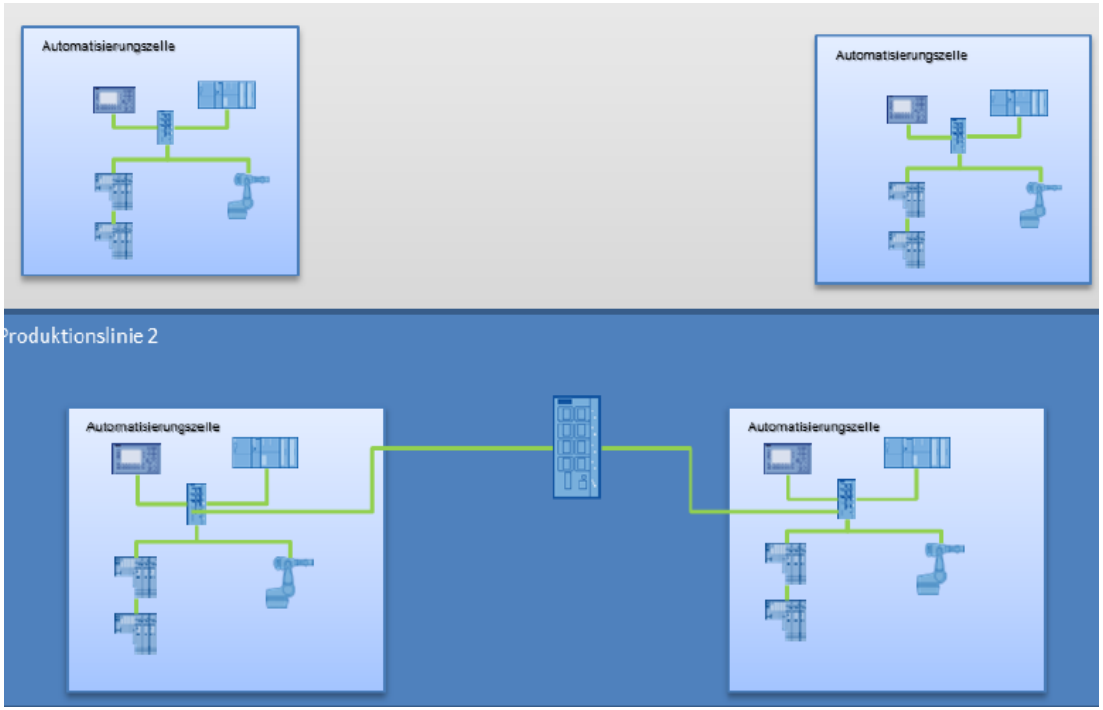
Security & Profinet



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

© 2017 PROFIBUS e PROFINET Italia

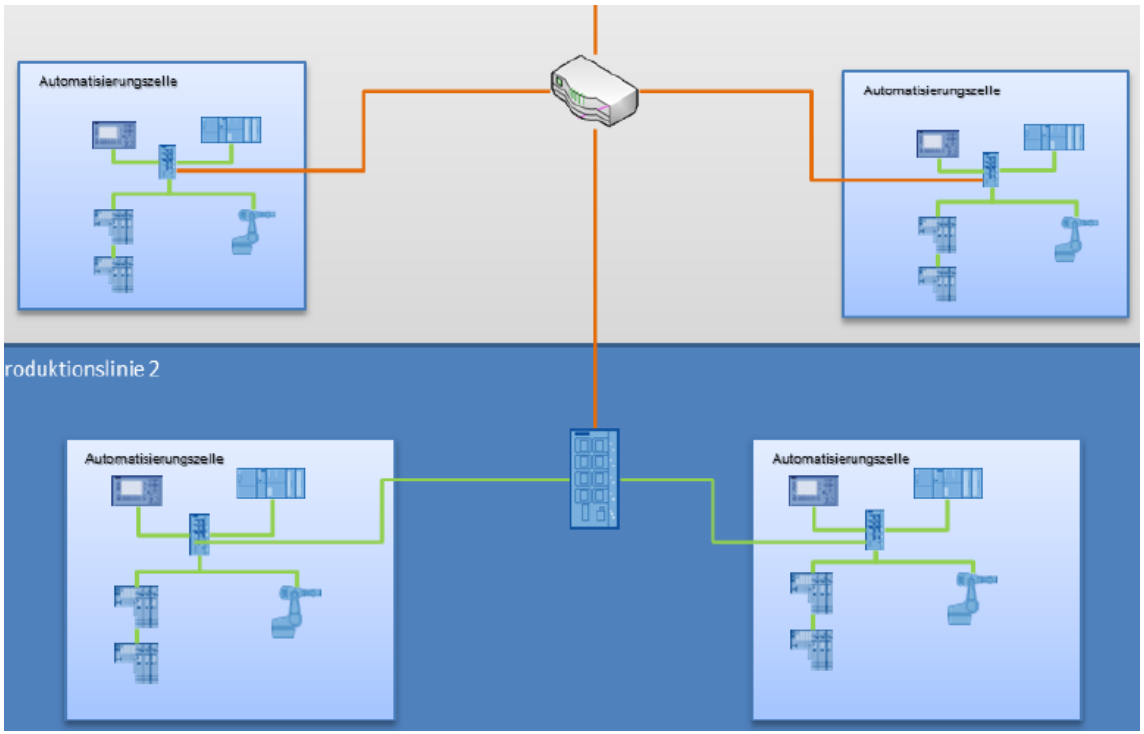
Security & Profinet



- 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

© 2017 PROFIBUS e PROFINET Italia

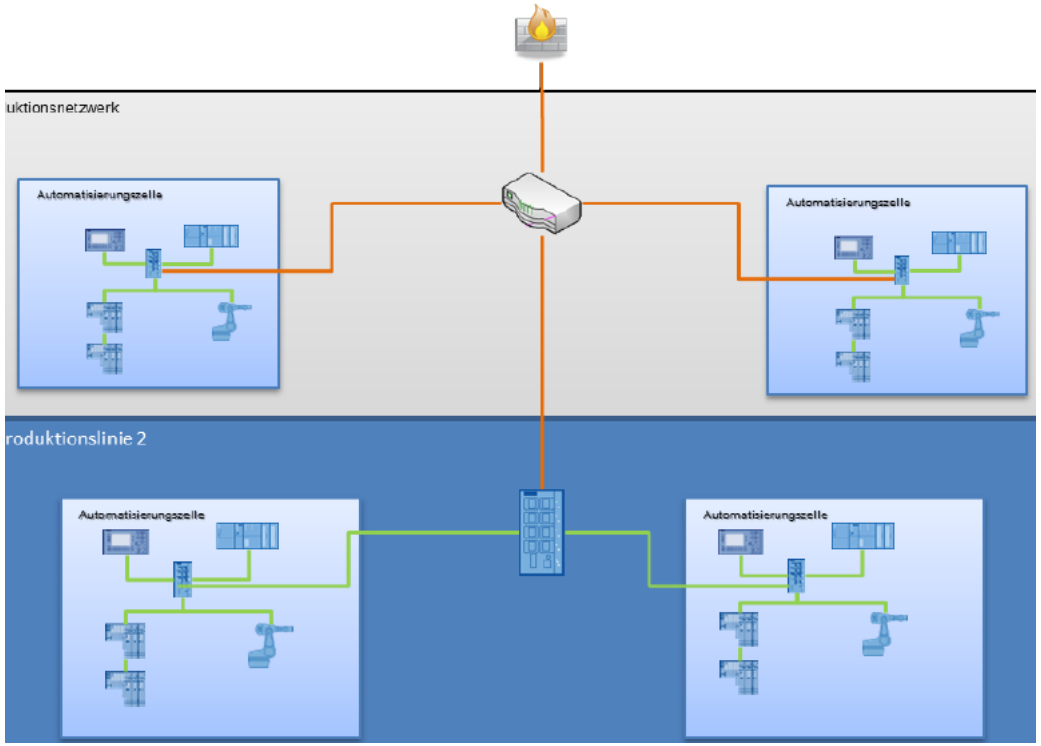
Security & Profinet



- 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

© 2017 PROFIBUS e PROFINET Italia

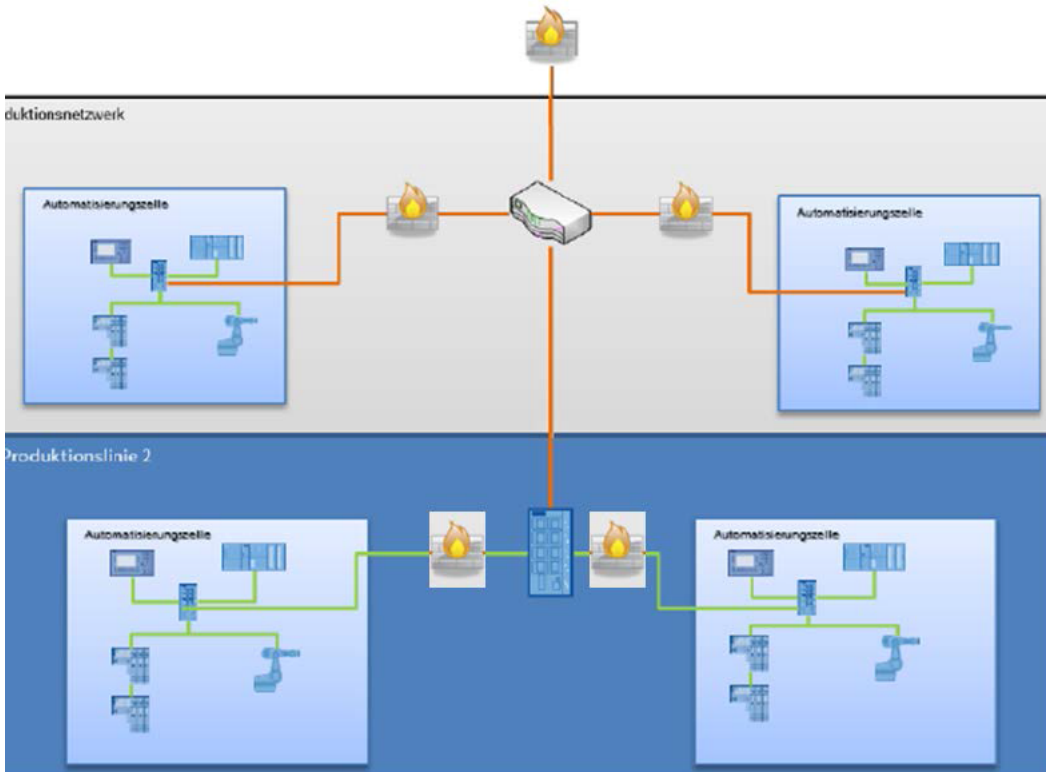
Security & Profinet



- 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

© 2017 PROFIBUS e PROFINET Italia

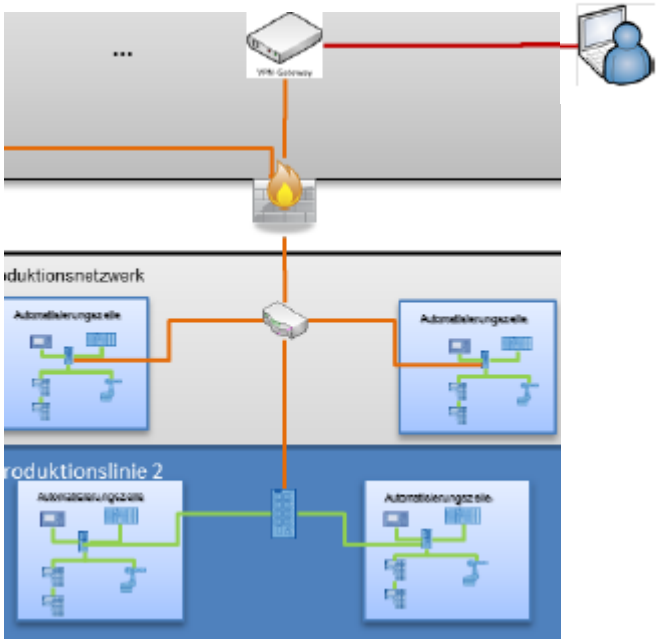
Security & Profinet



- 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

© 2017 PROFIBUS e PROFINET Italia

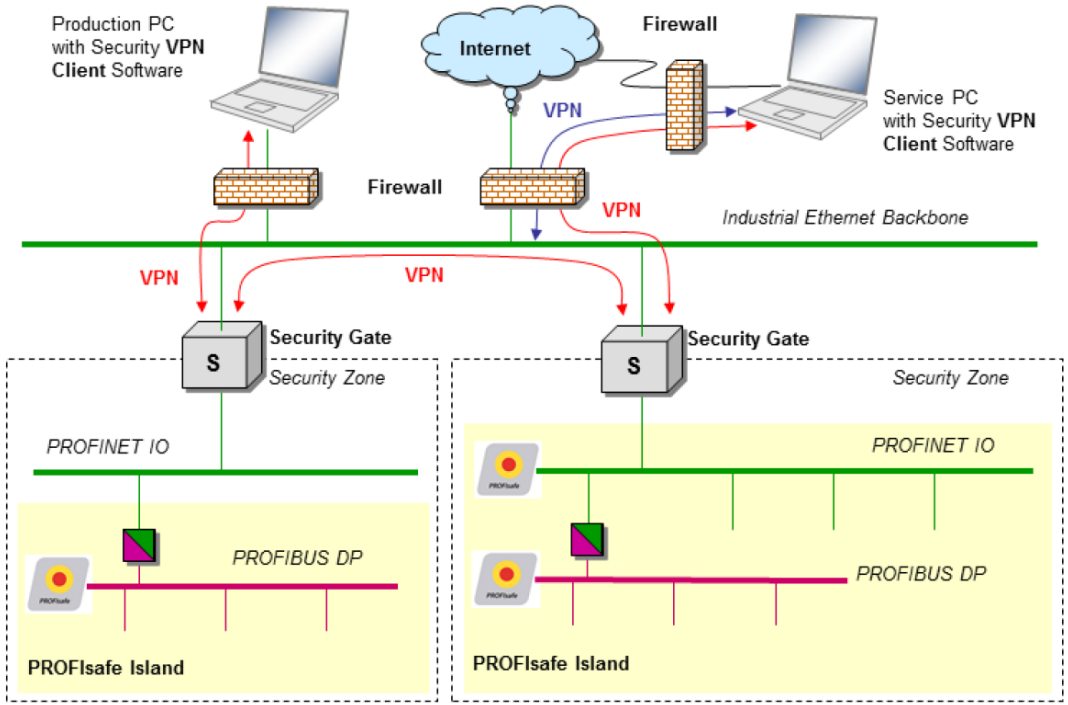
Security & Profinet



- 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

© 2017 PROFIBUS e PROFINET Italia

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)

© 2017 PROFIBUS e PROFINET Italia

PI Italia
PROFIBUS • PROFINET

GRAZIE

per l'attenzione

PROFINET® PROFIBUS® PROFIsafe PROFIenergy PROFIdrive IO-Link FDI