Criteri di progettazione della sicurezza per la gestione delle reti locali nelle applicazioni industriali

Roberto Motta

Rockwell Automation

La Security secondo IEC 62443-1-1

- Prevenzione di accessi illeciti o non voluti o di interferenze nello specifico e normale funzionamento di un sistema di comando e controllo per l’automazione industriale

Un’affermazione imbarazzante ...

"La mia macchina non è connessa alla rete di fabbrica o ad Internet, dunque la Security non mi riguarda"

- Un PC con un sistema operativo per il quale non sono più fornite patch di aggiornamento (p.e. Windows XP) o un PC su cui non sono state installate le patch di aggiornamento messe a disposizione dal fornitore, sono altre possibili situazioni di rischio

- Chiunque acceda alla macchina potrebbe introdurre un malware attraverso una «pennetta USB» o attraverso il proprio PC di servizio

- La mancata segmentazione della rete di fabbrica potrebbe dare accesso «ovunque» a «chiunque»

Perchè si parla tanto di Security?

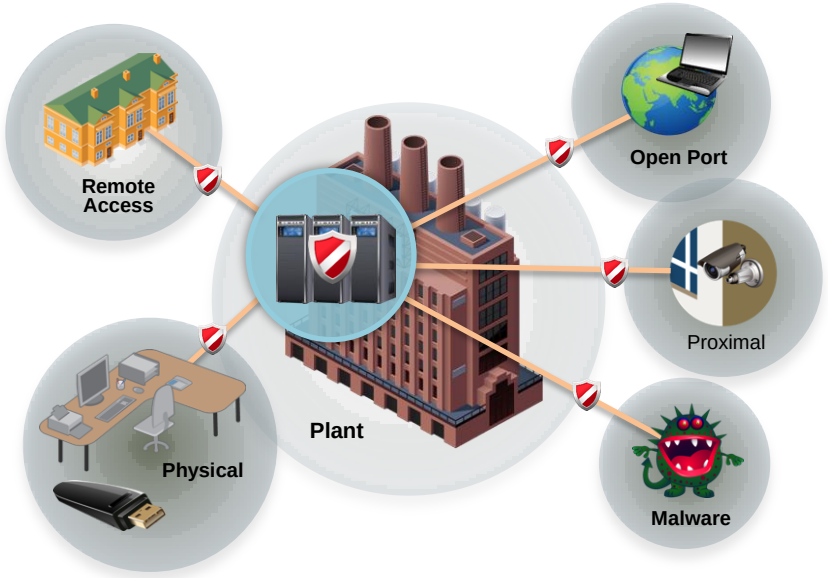
	IERI	OGGI
Sistemi Operativi:	Proprietari	Aperti
Comunicazioni:	Proprietari	Protocolli e tecnologie standard
Flusso delle Informazioni:	Isolato (Silos)	Integrato
Soluzioni Informatiche:	"Monolitiche"	Modulari & Remote
Architetture:	Proprietarie	Aperte
Utenti:	"Interni"	Interni & Esterni (Remoti)

Dobbiamo garantire:

- **Disponibilità / Integrità / Riservatezza**
- **Autenticazione / Autorizzazione / «Accounting»**
- Accessi Remoti sicuri
- Protezione delle informazioni

Le sfide per l'industria aumentano

- Oggi gli ambienti di controllo hanno nuovi punti di accesso in cui possono essere "violati"
- Abbiamo avuto un trend crescente di interruzione di controlli critici dopo Stuxnet (via USB)
- La maggior parte delle reti industriali oggi non è protetta contro queste minacce



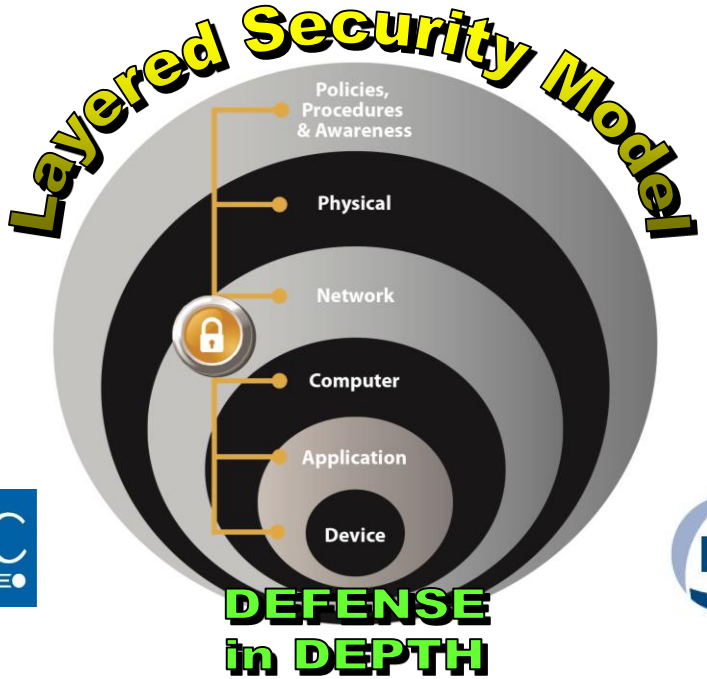
Facciamo degli esempi

Protezione e rilevamento delle **manomissioni** e **intrusioni**

- Come posso accertarmi che la configurazione del mio sistema di controllo non sia cambiata?
- Come posso assicurare l'accesso ad un controllore attraverso un percorso di connessione sicuro?
- Quanto modifiche accidentali al sistema di controllo possono influenzare il corretto funzionamento della mia applicazione ed interferire con la sicurezza degli operatori?

Il modello “difesa in profondità”

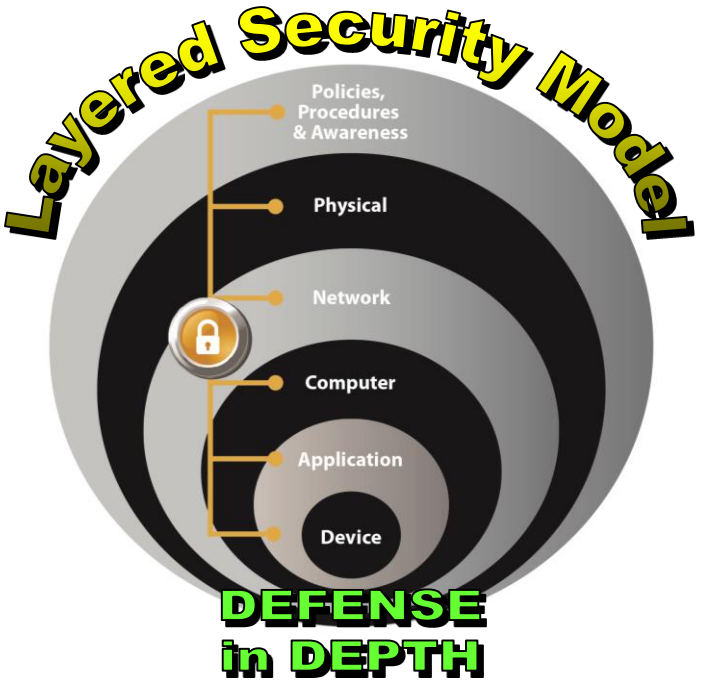
Non bastano un unico prodotto, tecnologia o metodologia per garantire al 100% la sicurezza dei sistemi di controllo industriale



- Modello di Security su più Livelli:
  - Schermare potenziali “bersagli” dietro livelli multipli di protezione per ridurre i rischi
- Difesa in profondità:
  - Utilizzare più contromisure di sicurezza per proteggere l'integrità di componenti e sistemi
- Apertura:
  - Soluzioni disponibili da vari fornitori
- Flessibilità:
  - Per soddisfare «Politiche» e Procedure specifiche
- Coerenza:
  - Soluzioni che si allineano a direttive governative e degli organismi internazionali di normazione

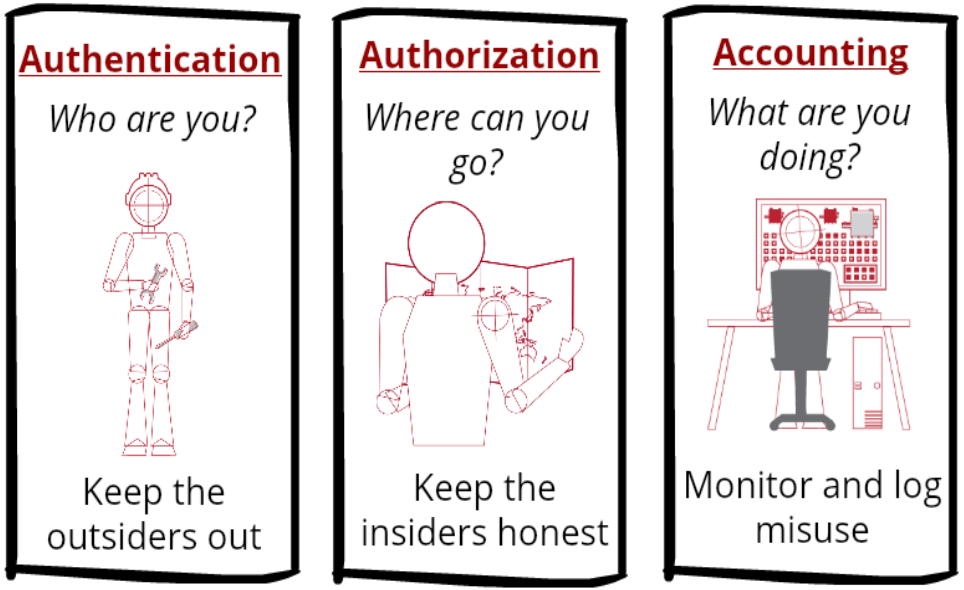
Come applichiamo questo modello?

1. «Autentichiamo» l'identità di tutti gli utenti che richiedono di accedere ad un sistema di automazione
2. «Autorizziamo» l'accesso di un utente ad una specifica risorsa di un sistema rispetto all'insieme di "permission" definiti nel suo profilo
3. «Tracciamo» (Accounting) quanto fatto da un utente che ha avuto accesso a quella specifica risorsa
4. «Aggiorniamo» le patch dei S. O. «disinstalliamo» i componenti software e le porte USB o altre interface poco usate
5. «Segreghiamo» e «Segmentiamo» le reti di automazione anzichè creare reti «piatte»
6. «Limitiamo» l'accesso *fisico* ai dispositivi di automazione p.e. limitiamo l'accesso alle porte di uno switch ad indirizzi MAC specifici



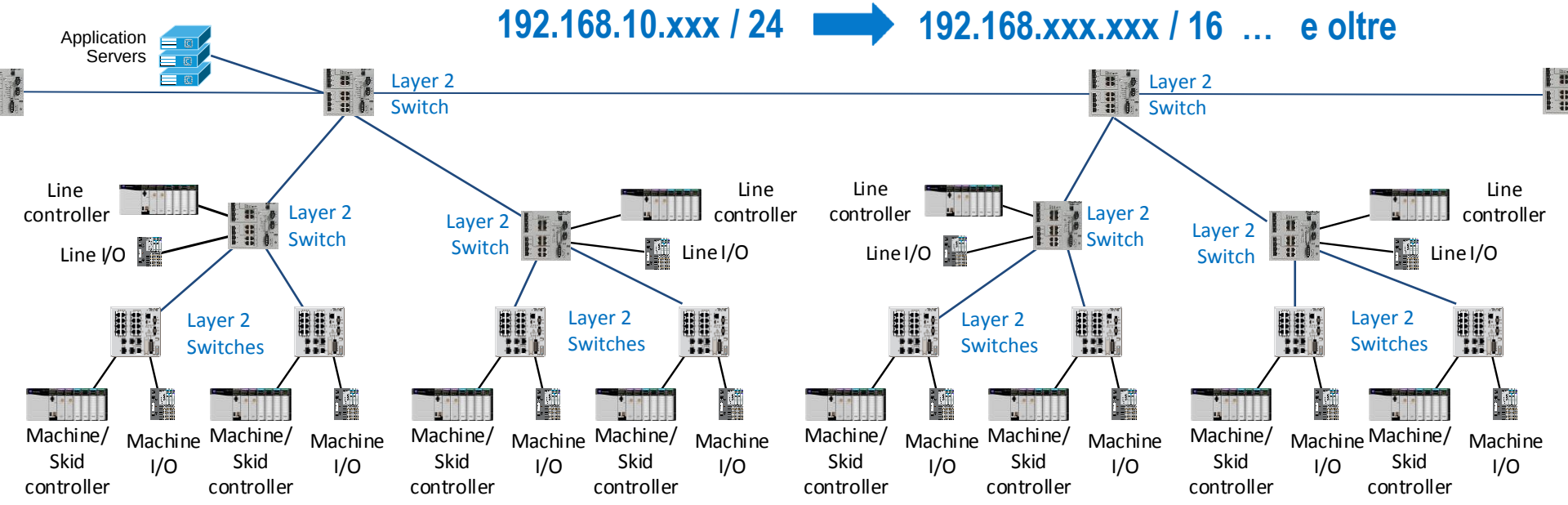
Le politiche di accesso sono varie

- ***Product policies:***
  - Definiscono a quali funzioni (p.e. Frimware update) ha accesso uno specifico utente
- ***System policies:***
  - Definiscono le regole che governano il modo di protezione (p.e. le scadenze delle password)
- ***Computer policies:***
  - Per definire ad esempio quali computer hanno accesso ad uno specifico sistema di automazione
- ***Permission policies:***
  - Lo stesso livello di Permission può essere attribuito ad un utente per un singolo dispositivo, per tutti o per gruppi



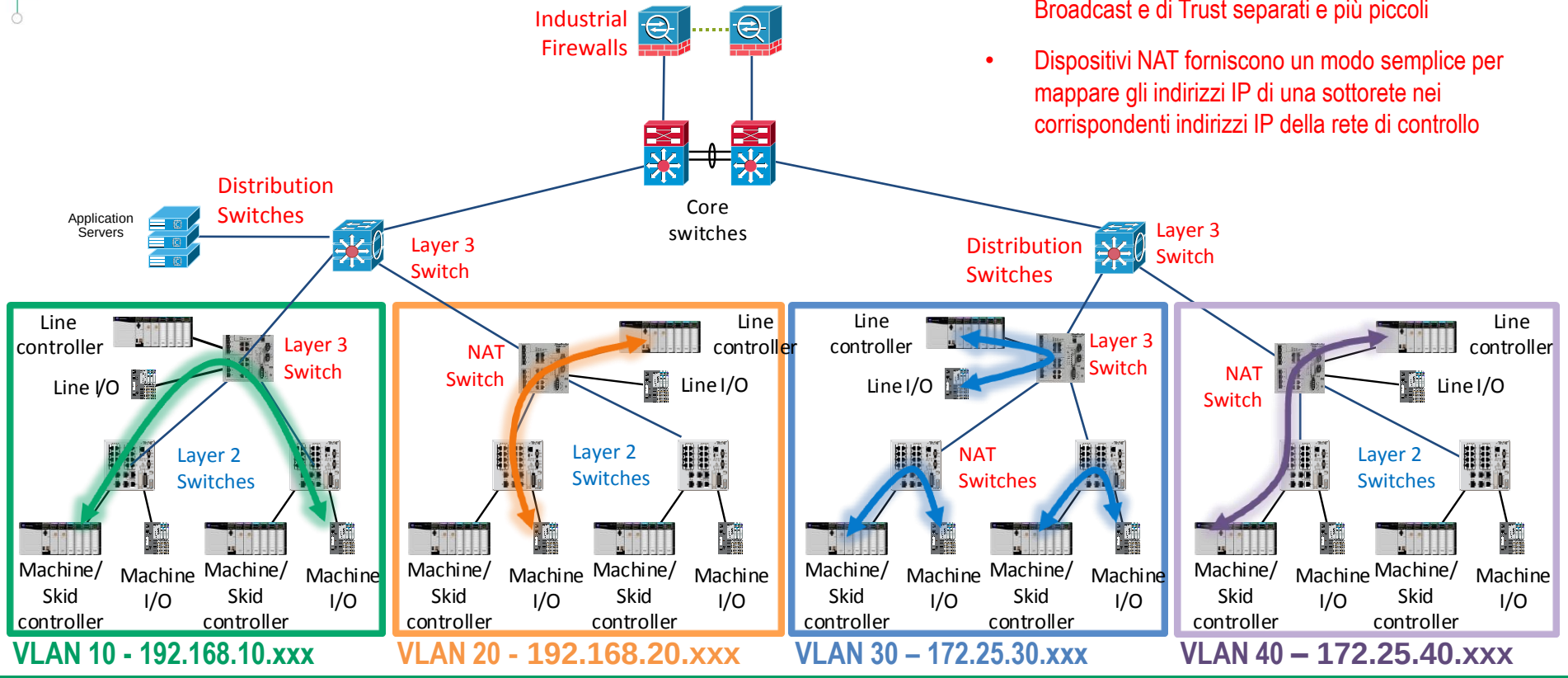
Una rete “piatta” non ha confini “sicuri”

- I Domini di Fault (Layer 2 loops), di Broadcast e di Trust rischiano di crescere a dismisura senza controllo
- Peggio se le reti sono «unamanged»

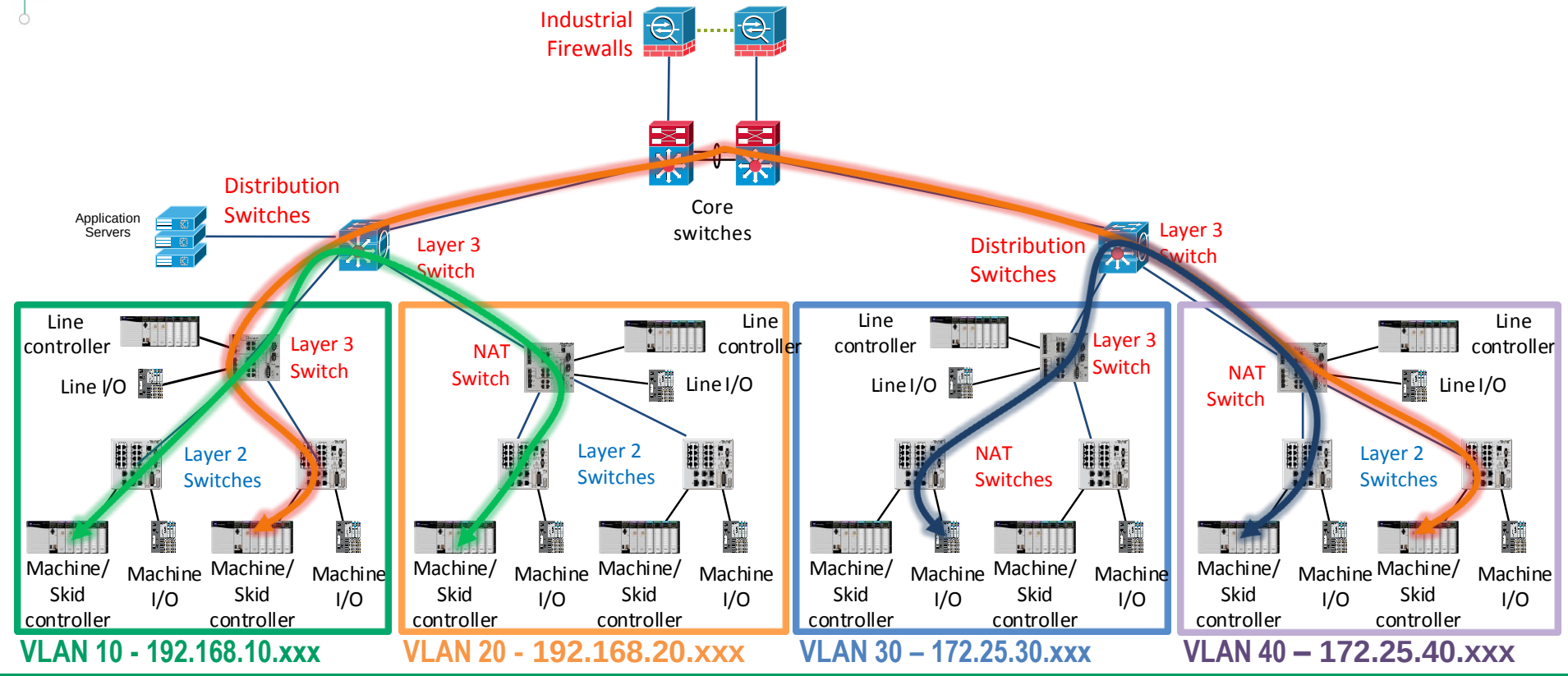


Possiamo creare confini “sicuri” …

- Dispositivi di Layer 3 creano Domini di Fault, di Broadcast e di Trust separati e più piccoli
- Dispositivi NAT forniscono un modo semplice per mappare gli indirizzi IP di una sottorete nei corrispondenti indirizzi IP della rete di controllo



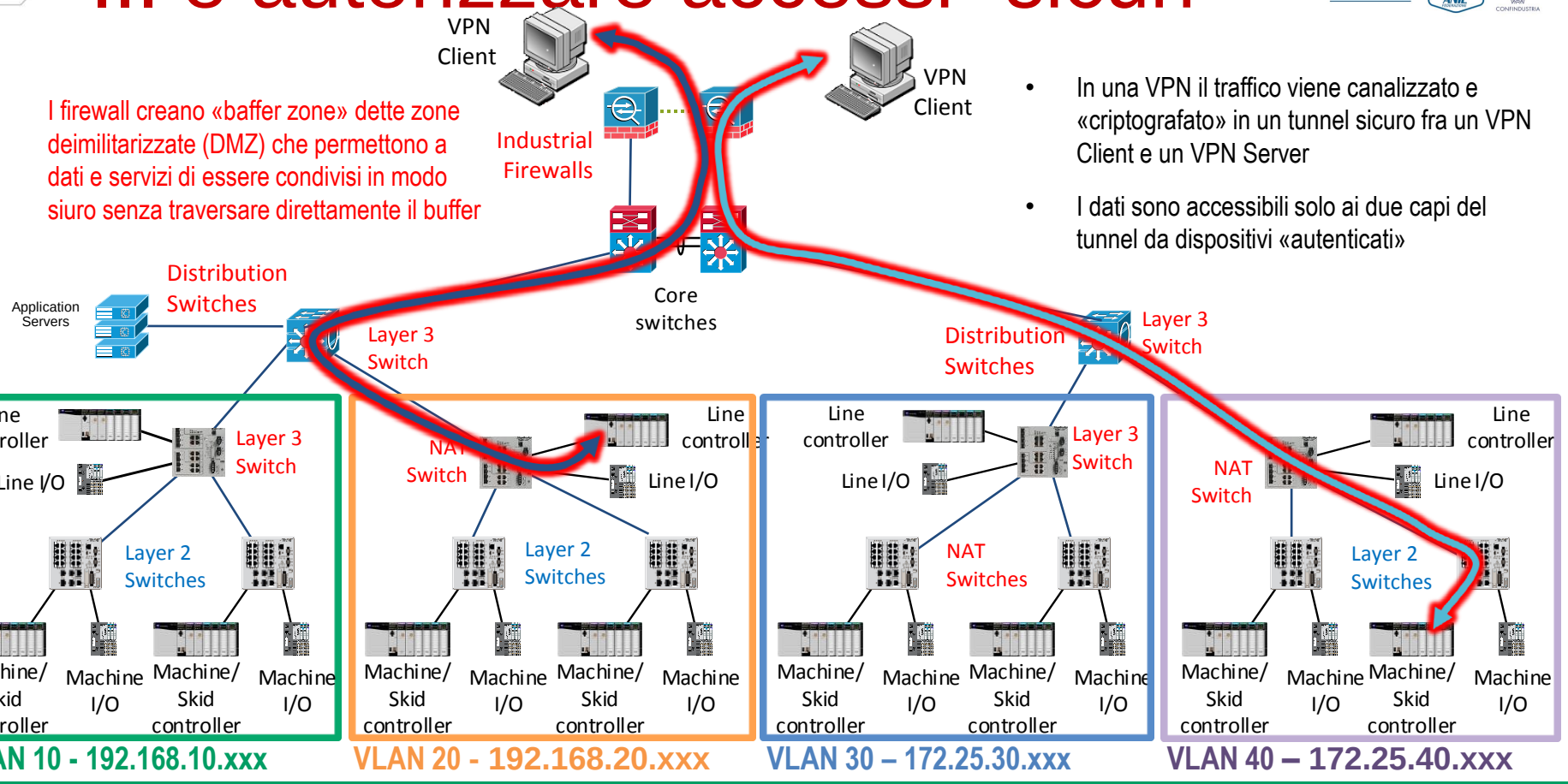
... controllare il traffico fra domini,



… e autorizzare accessi “sicuri”

I firewall creano «baffer zone» dette zone deimilitarizzate (DMZ) che permettono a dati e servizi di essere condivisi in modo siuro senza traversare direttamente il buffer

- In una VPN il traffico viene canalizzato e «criptografato» in un tunnel sicuro fra un VPN Client e un VPN Server
- I dati sono accessibili solo ai due capi del tunnel da dispositivi «autenticati»



Grazie per l’attenzione