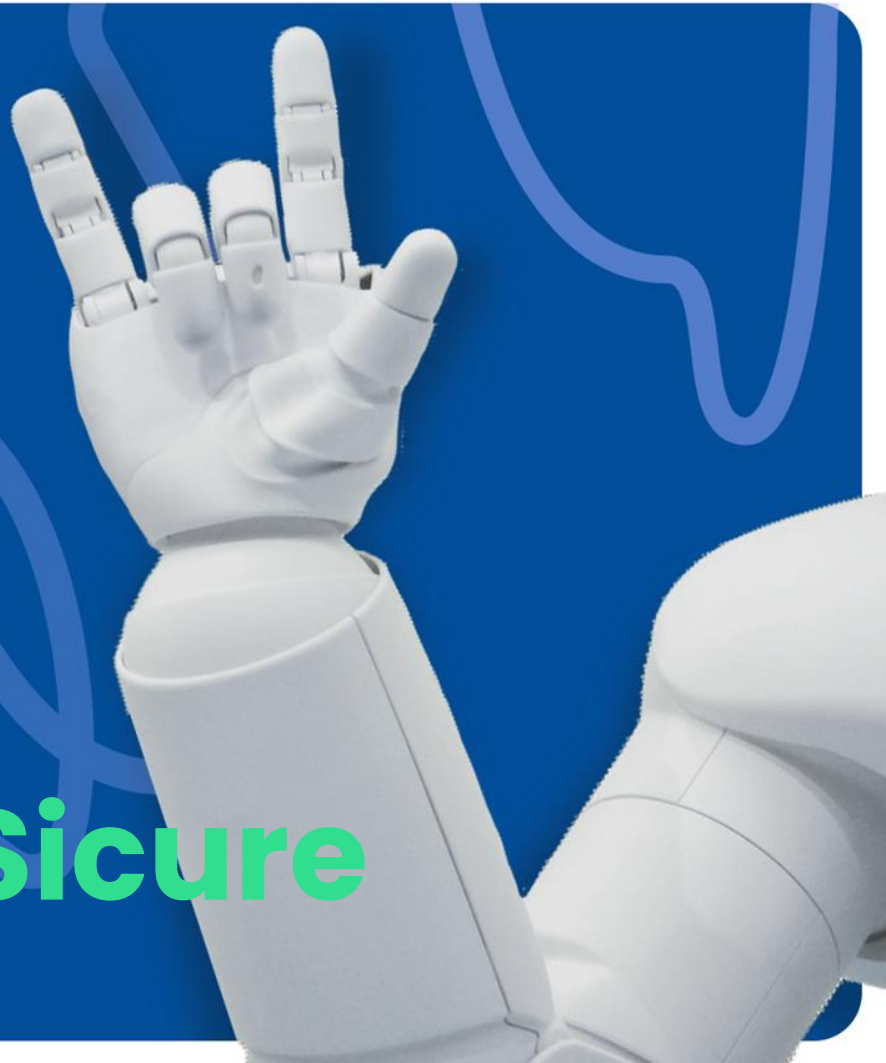
bi-rex SIEMENS

Tre partner leader per ridisegnare sistemi industriali in sicurezza e infrastrutture affidabili e performanti.

Industrie Sicure&CyberSicure



Agenda

15.00 – 15.15	**Introduzione e apertura lavori** Saluti BI-REX (Stefano Cattorini – BI-REX)
15.15 – 15.45	**Cybersecurity & Infrastrutture Industriali** Analisi del contesto (Stefano Talami – FTP) Come nasce il servizio Industrie Sicure & CyberSicure (Andrea Graglia – SIEMENS)
15.45 – 16.30	**Presentazione del servizio** Focus BI-REX (Francesco Meoni - BI-REX) Focus FTP (Stefano Talami - FTP) Focus Siemens (Laura Baccini - SIEMENS)
16.45 – 17.30	**Tour guidato della Linea Pilota**

bi-rex Big Data Innovation & Research Excellence SIEMENS FTP

INTRODUZIONE E APERTURA LAVORI

SALUTI BI-REX (Stefano Cattorini)

CHI SIAMO

BI-REX è uno degli 8 **Competence Center** nazionali istituiti dal **Ministero dello Sviluppo Economico** nel quadro del piano governativo **Industria 4.0**.

Il nostro **Consorzio pubblico-privato**, nato nel 2018 e con sede a Bologna, riunisce in partenariato 60 player tra Università, Centri di Ricerca ed Imprese di eccellenza e ha un focus specializzato sul tema Big Data.

BI-REX è l'unico Competence Center a guida industriale.

LA NOSTRA MISSION

Supportare le aziende nei loro processi di digitalizzazione e innovazione e nell'adozione delle tecnologie abilitanti in ottica Industria 4.0.

Facilitare lo scambio di "best practices", il Trasferimento Tecnologico, l'innovazione aperta

IL CONSORZIO 60 Partner AZIENDE DA 7 FILIERE

12 ENTI

27 END USERS

21 TECHNOLOGY SERVICE PROVIDER

bi-REX

I SERVIZI

Test Before Invest

- Accesso a casi d'uso
- Sviluppo di Prof of Concept
- Progetti integrati
- Equipment-as-a service
- Coaching, temporary management

Networking

- Tech Scouting Open Innovation & Hackathon
- Technology Transfer
- Matchmaking
- Location & Coworking

bi-rex
Big Data Innovation & Research Excellence

Formazione e Orientamento

- +90 corsi di formazione
- Formazione personalizzata
- Valutazione sul gap competenze
- Funding 4 Training
- E-Learning

Supporto per ricerca

- Progetti MISE, Regionali, UE
- Ingegneria Finanziaria
- Gestione incentivi fiscali
- Start-up e SME

I CORSI DI FORMAZIONE

1. Big Data: Big Data e Analytics, Intelligenza Artificiale, Machine e Deep Learning, Visual Computing;

2. ICT e Sistemi avanzati per gestione processi produzione: Industrial IoT, Tecnologie 5G, Edge e Cloud Computing, Revamping digitale;

3. Security & Blockchain;

4. Additive & Advanced Manufacturing: Additive Manufacturing, Digital Twinning, Diagnostica predittiva, Supply Chain, Realtà Virtuale e Aumentata, Human-Machine Interface, tecnologie di Smart Plant;

5. Robotica collaborativa, warehousing e AMR: Automazione industriale, robot collaborativi (COBOT), AMR;

6. Sostenibilità e responsabilità sociale;

7. Trasversali: temi manageriali, organizzativi, finanziari, strettamente correlati all'introduzione di tecnologie I4.0.

CYBERSECURITY & INFRASTRUTTURE INDUSTRIALI

ANALISI DEL CONTESTO (Stefano Talami)

Ad oggi ormai è una necessità
monitorare e assicurare la
sicurezza dei sistemi industriali

© 2022 F.T.P. S.r.l.

UN OSTACOLO CHE NON SI PUÒ PIÙ SOTTOVALUTARE

GLI ATTACCHI CRESCONO IN QUANTITÀ E IN “QUALITÀ”

Nel 2021 gli attacchi nel mondo sono **aumentati del 10%** rispetto al 2020, e sono sempre più gravi.

In Italia i settori più colpiti si confermano il Finance/Insurance e la Pubblica Amministrazione.

A seguire l’**Industria** che ha presentato l’aumento più significativo, **dal 7% del 2020 al 18% del 2021**.

79% sono gli attacchi gravi con effetti molto importanti di livello **Critical** e **High**, contro il 50% del 2020.

La stima delle perdite causate da questa situazione ci dovrebbe far riflettere molto seriamente.

6 trilioni di $

fonte: clusit – Rapporto 2022

© 2022 F.T.P. S.r.l.

UN OSTACOLO CHE NON SI PUÒ PIÙ SOTTOVALUTARE

Le **tecniche di attacco evolvono** in direzioni più difficili da monitorare, da quantificare e anche da intercettare.

Malware e botnet sono in continua crescita con un **+58%** di server compromessi.

Le **vulnerabilità** scoperte **nei sistemi OT nel 2021** sono **più che raddoppiate** rispetto al 2020.

Il **ransomware** è diventato il vettore numero uno per attacchi **ai danni dell'industria**; il settore manifatturiero è quello maggiormente preso di mira con il **60%** di cyber attacchi.

LE MINACCE SONO SEMPRE PIÙ SUBDOLE

Le organizzazioni devono assolutamente restare al passo con l'evoluzione delle tecniche di attacco le quali seguono una naturale evoluzione verso lo **sfruttamento dei punti di ingresso più deboli, inclusi gli individui**.

fonte: clusit – Rapporto 2022

© 2022 F.T.P. S.r.l.

PIU' TECNOLOGIA, PIU' ESPOSIZIONE

Oleodotto americano paga un riscatto di 5 milioni di dollari per ripartire

75 miliardi

numero di device connessi nel 2025, quindi maggiore superfice d'attacco

© 2022 F.T.P. S.r.l.

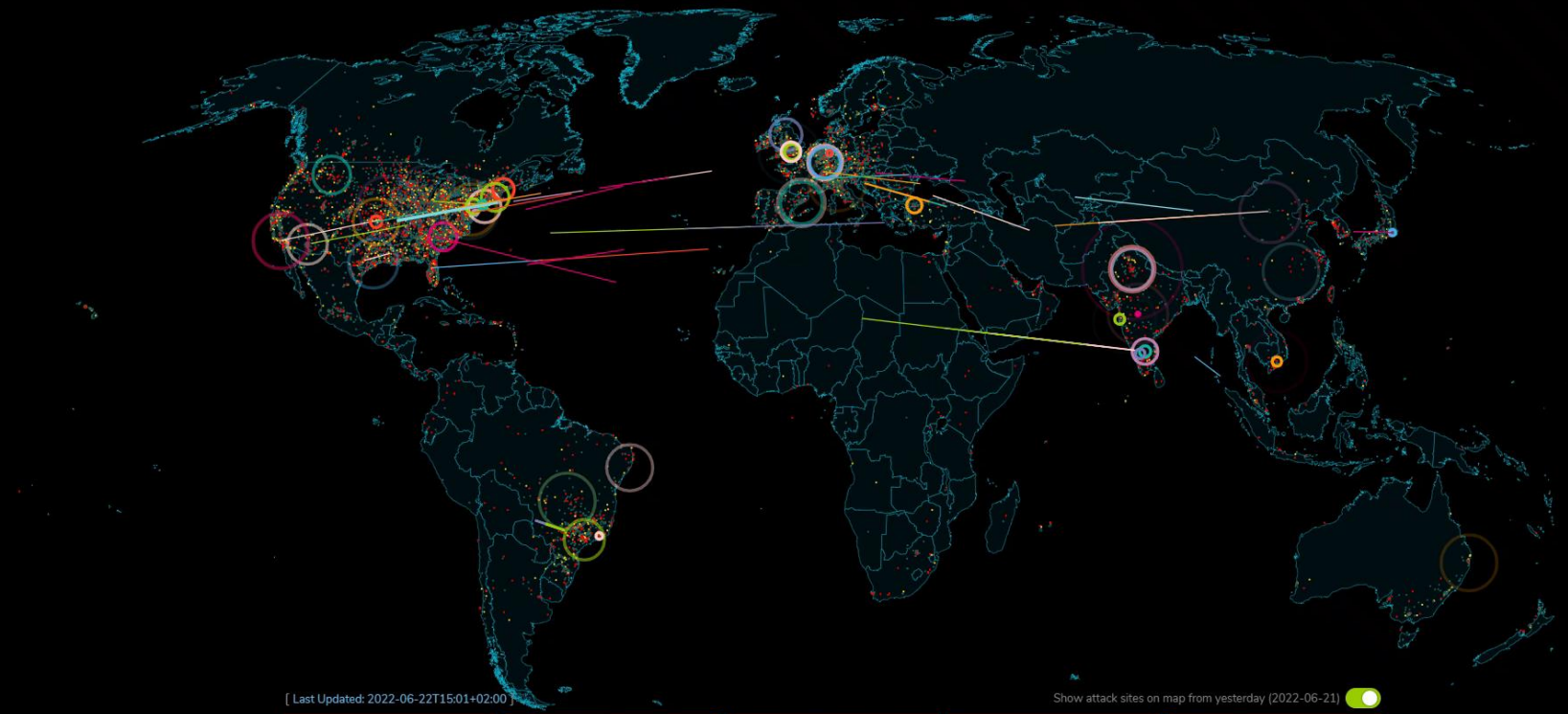
LA PORTA D'INGRESSO DI UN HACKER POTREBBE TROVARSI IN UN INFRASTRUTTURA DATATA, OBSOLETA O DANNEGGIATA

Ecco un esempio di alcuni punti di debolezza

- CONVERGENZA ACCIDENTALE
- DEVICE E ASSET OBSOLETI
- DIPENDENTI DISATTENTI
- MANCANZA DI VISIBILITA' RETI OT
- CONTROLLERS NON PROTETTI

© 2022 F.T.P. S.r.l.

WORLDWIDE ATTACKS



[Last Updated: 2022-06-22T15:01+02:00]

Show attack sites on map from yesterday (2022-06-21)

TOP 3 ATTACK ORIGINS		TOP 3 ATTACK TARGETS		TOP ATTACK TYPES		TOP 3 ATTACKER IP ADDRESS		ATTACK SITE STATISTICS ON JUN 21	
3.79M	United States	2.30B	United States	73.1M	Intrusion	2.01M	103.145.*.*	5,775	> 100 Attacks/Site
2.14M	Austria	1.58B	United Kingdom	17.1M	Malware	1.49M	103.145.*.*	2,388	> 50 < 100 Attacks/Site
394K	Denmark	1.26B	India			1.40M	193.46.*.*	10.9K	< 50 Attacks/Site

fonte: SonicWall 2022

© 2022 F.T.P. S.r.l.

I FALSI MITI

1. NON HO DATI ESPOSTI

2. NON HO NULLA CHE VALGA LA PENA DI RUBARE

3. BASTA IL FIREWALL

4. GLI HACKER NON SI INTERESSANO ALLA MIA AZIENDA

© 2022 F.T.P. S.r.l.

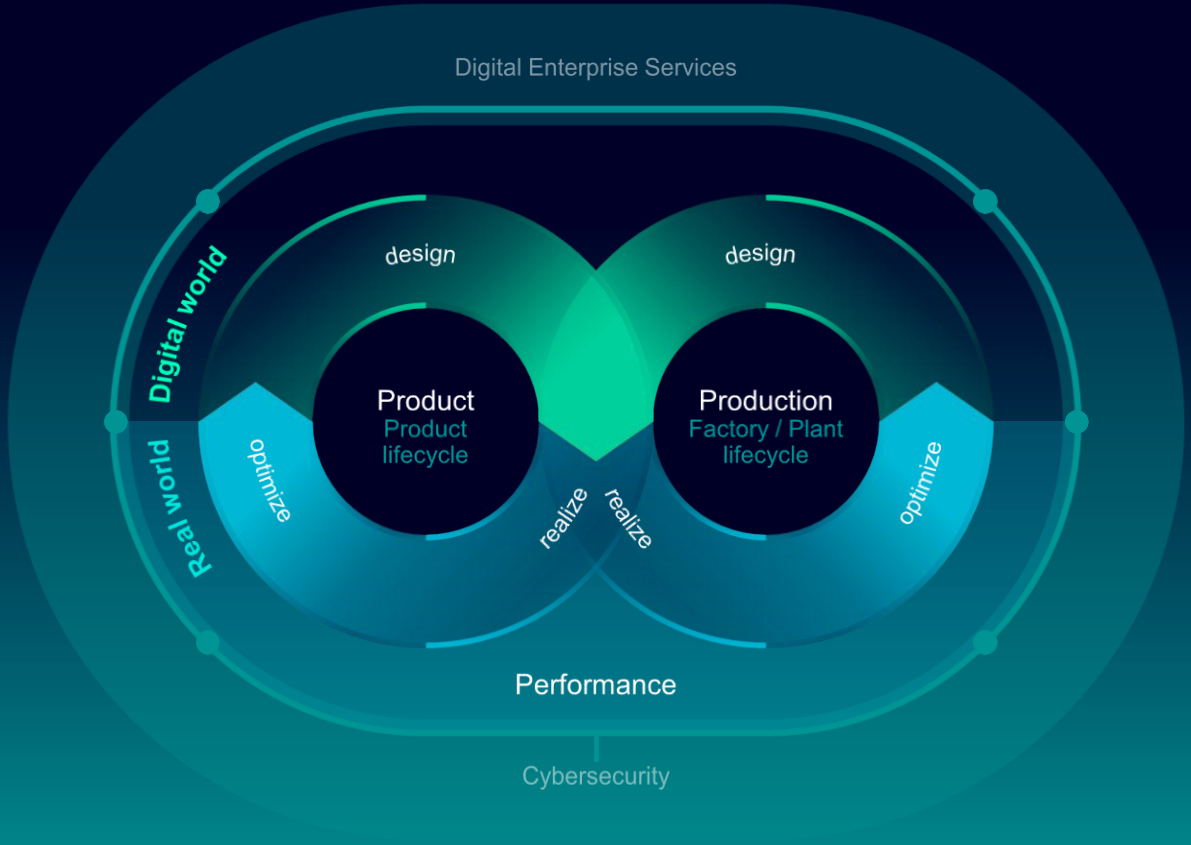
“Everyone has a plan until they get punched in the mouth.”

bi-rex Big Data Innovation & Research Excellence SIEMENS

© 2022 F.T.P. S.r.l.

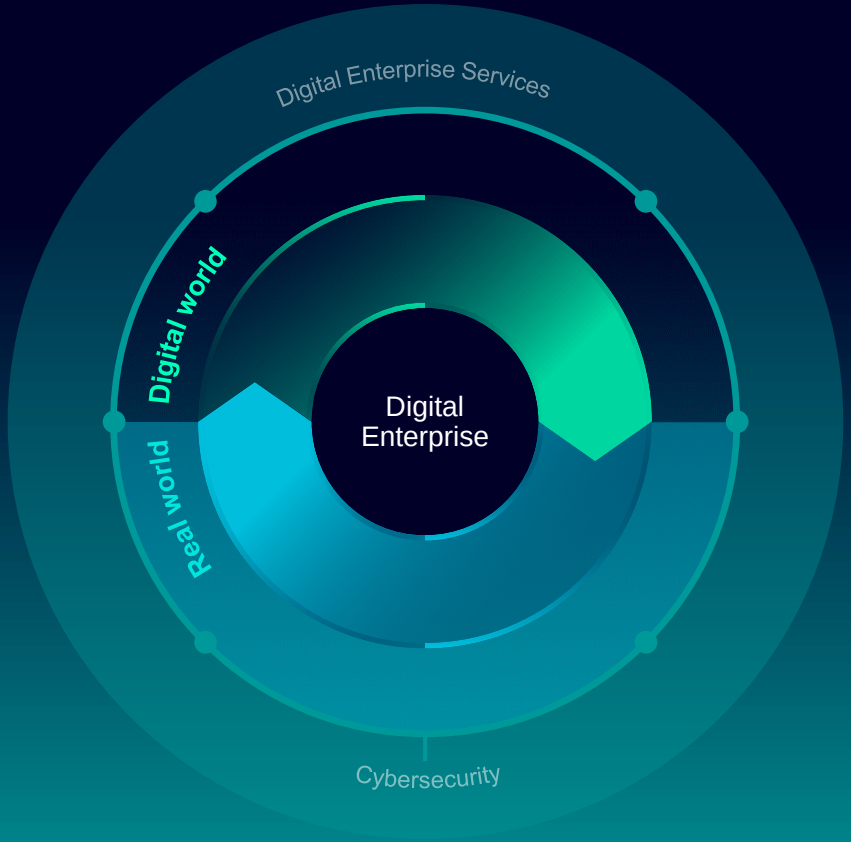
CYBERSECURITY & INFRASTRUTTURE INDUSTRIALI

COME NASCE IL SERVIZIO INDUSTRIE SICURE & CYBERSICURE (Andrea Graglia)



© Siemens 2022

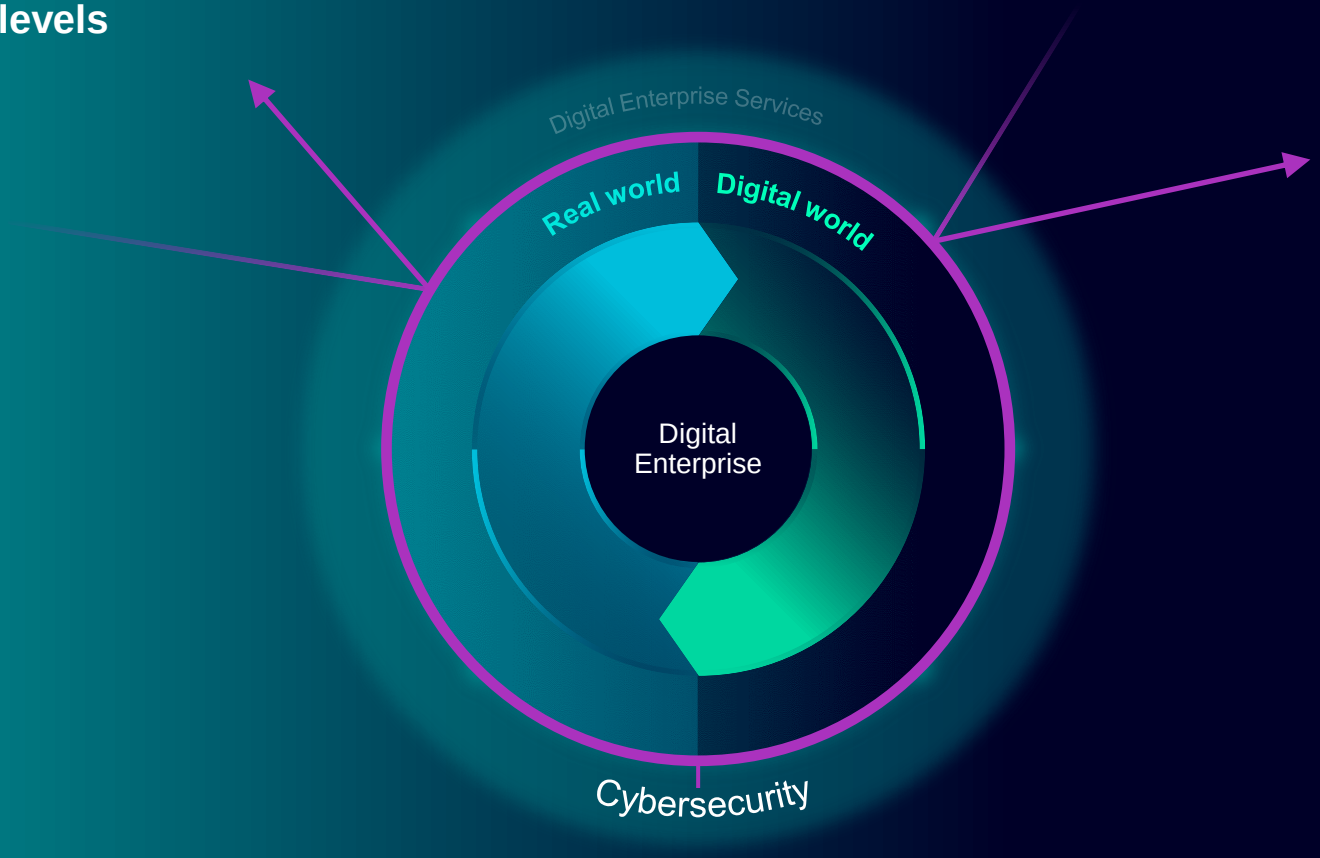
SIEMENS



© Siemens 2022

SIEMENS

Multi-layered security across all levels

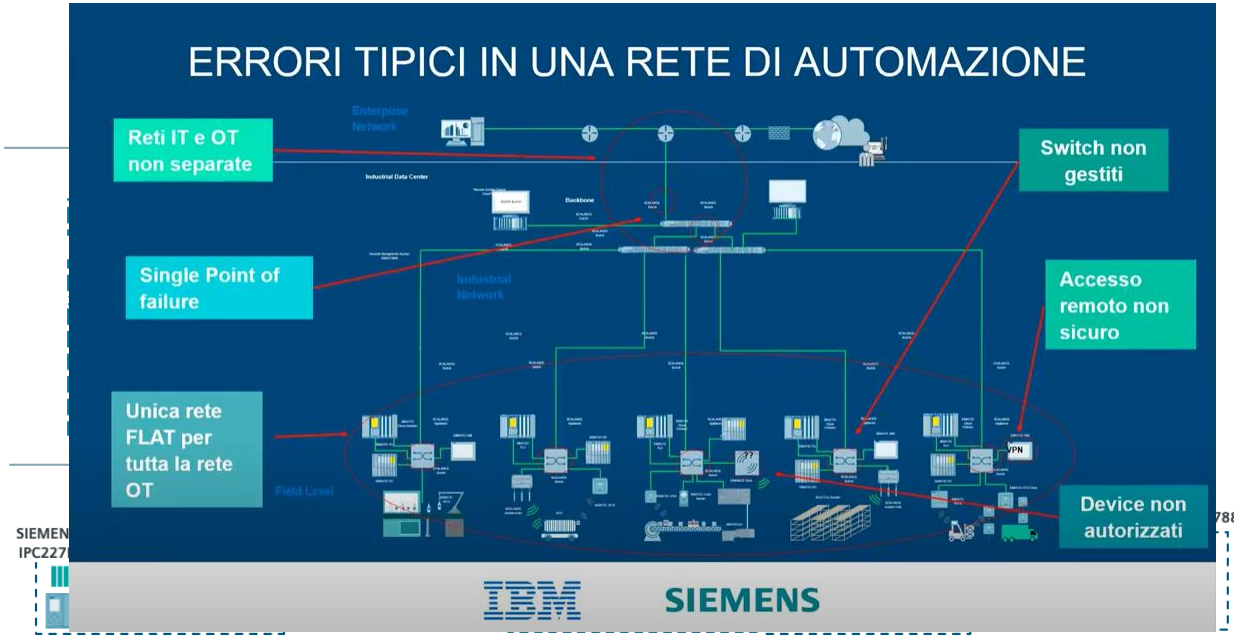


© Siemens 2022

SIEMENS

Network & cybersecurity

The original Bi-rex net architecture was implemented with typical mistakes in the OT systems.
Siemens has developed the new industrial network system of the line: the machines are all connected together and each of them can communicate the data to IoT systems.
The cybersecurity functionalities, developed in collaboration with IBM, are in conformity of the security requirements, in according to IEC62443



Advantages				
	Separation of the IT/OT networks thanks to DMZ zones with firewalls. **Secure remote access**	**Anomaly inspection for checking communication's, trough Rugged Com switch with NOZOMI**	**Segregation of the machines in cells can isolate occurring problems**	**Switch managed can provide diagnostics** **Wi-fi stations**

Webinar Bi-rex:
https://youtu.be/veBKUN-qt6c

© Siemens 2022
SIEMENS

Siemens approach in competence center

bi-rex
Big Data Innovation & Research Excellence

Pilot line

Project of innovation

Training & seminars

Communication and media

Services to customers

Test before invest

Use of operational environment without risk of interruption of productivity

Reduced costs for digital transformation (licenses, hardware, human resources, training…)

Co-creation with other technology partners

SIEMENS

PRESENTAZIONE DEL SERVIZIO

FOCUS BI-REX (Francesco Meoni)
FOCUS FTP (Stefano Talami)
FOCUS SIEMENS (Laura Baccini)

I 4 STEP DEL SERVIZIO

La sfida è **mettere in sicurezza** i sistemi industriali e **ridisegnare le infrastrutture** per rendere affidabili e performanti le reti evitando fermi produttivi.

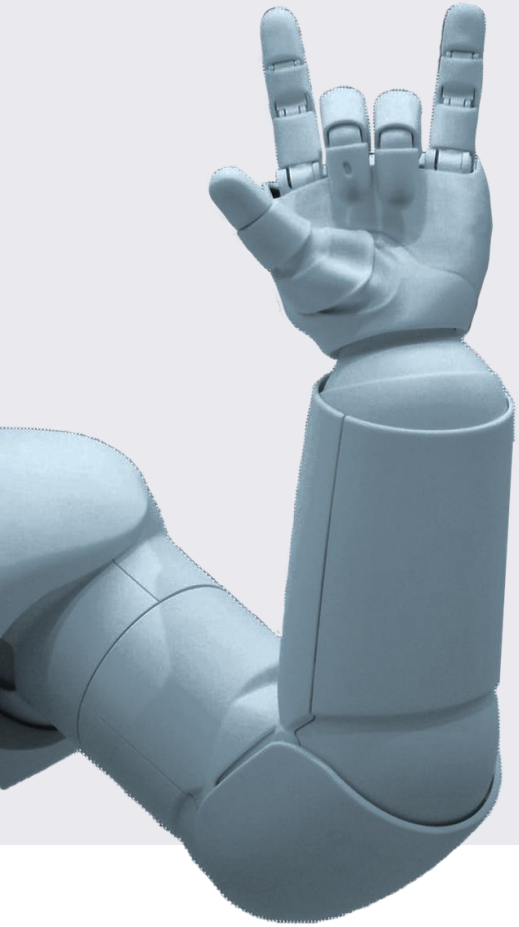
La possibilità di realizzare attività di Test-Before-Invest nella Linea Pilota e la centralità della digitalizzazione dell'industria nel Piano Nazionale di Ripresa e Resilienza (PNRR) hanno dato vita al **servizio Industrie Sicure&CyberSicure** nato dalla **collaborazione tra BI-REX, Siemens e FTP**.

bi-rex SIEMENS FTP

bi-rex Big Data Innovation & Research Excellence

SIEMENS

Explore.



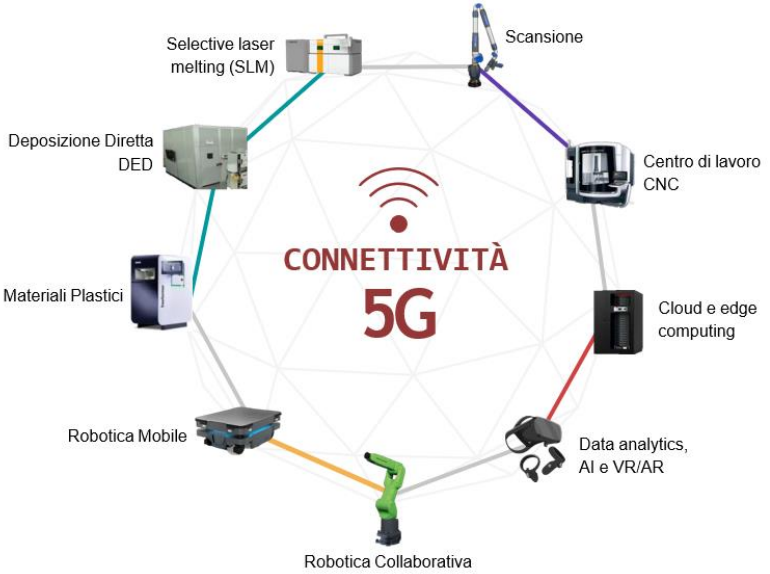
STEP 1
EXPLORE BI-REX

MEZZA GIORNATA PRESSO LA LINEA PILOTA E IDENTIFICAZIONE DEI NEEDS

· **Analisi delle soluzioni di integrazione** IT-OT in BI-REX, realizzate con il supporto di Siemens-FTP e IBM;
· **Accesso all'area Big Data & IoT**;
· Concetto di **Defense in Depth** e **compliance con gli standard** di sicurezza, rischi strutturali e perimetrali;
· Opzioni tecnologiche **hardware e software** per la gestione della sicurezza;
· Opportunità formative e di accesso ai **Crediti d'Imposta 4.0**.

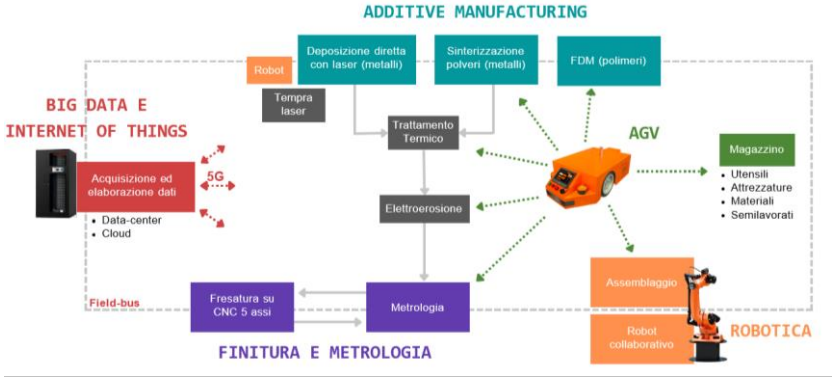
bi-rex Big Data Innovation & Research Excellence SIEMENS FTP

LINEA PILOTA, OPPORTUNITÀ E SERVIZI



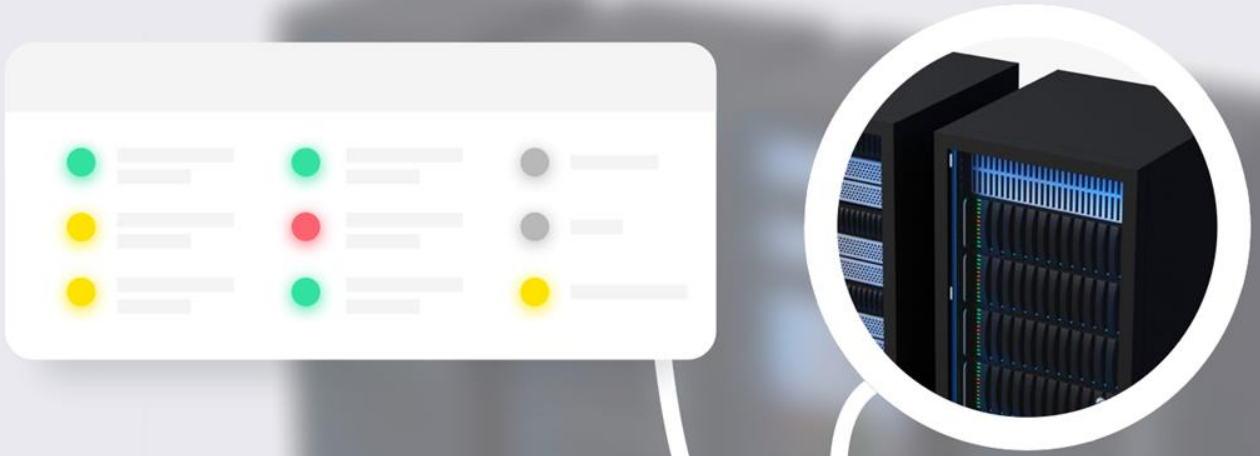
Unique Infrastructure :

· Smart Factory 4.0
· Rete private NSA 5G mmWave
· Accesso a CINECA per HPC
· Un framework di SW 4.0 per le imprese
· Federated Lab & Manufacturing

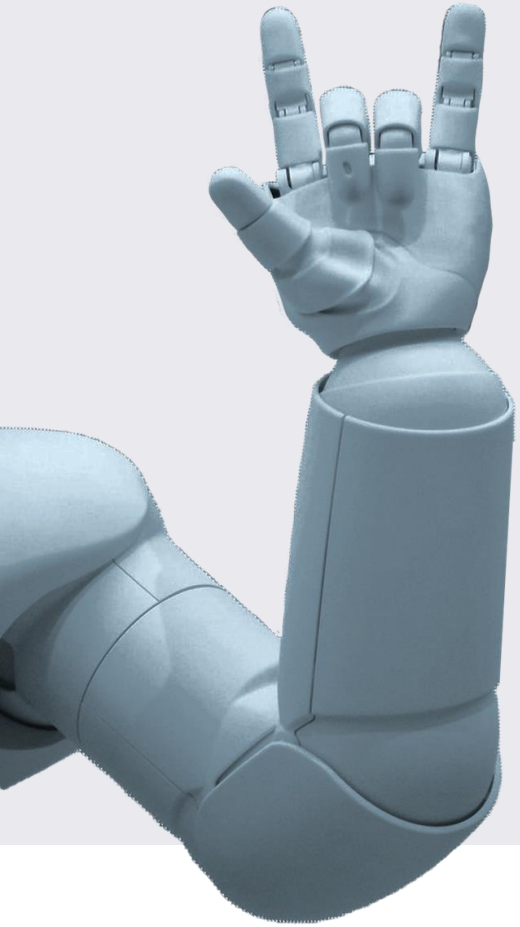


bi-rex
Big Data Innovation & Research Excellence

SIEMENS



Analyze.



STEP 2
GENERAL INFRASTRUCTURE ASSESSMENT

STUDIO DEL CASO

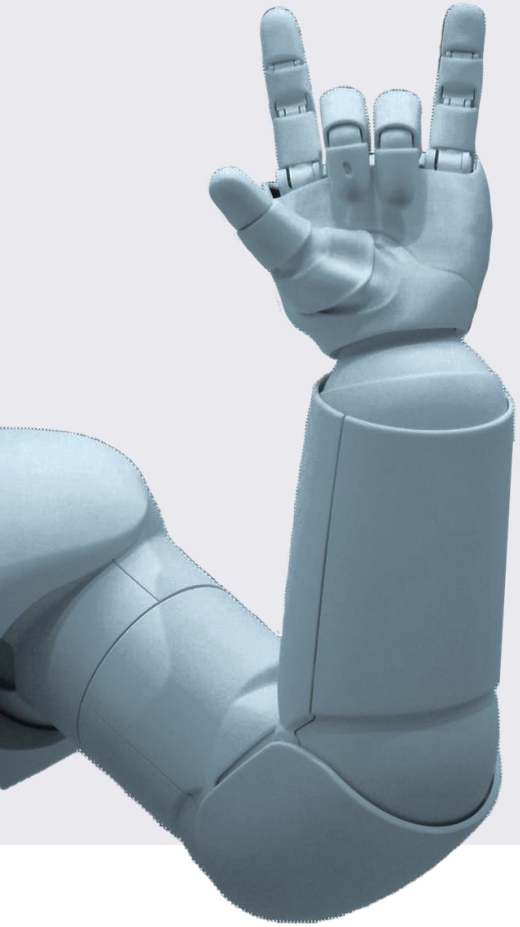
· Tecnici specialisti certificati vengono coinvolti in un' **Infrastructure OT Analysis sull'impianto esistente** ed una valutazione dei rischi tramite un sopralluogo fisico;
· Scopriamo i punti deboli ed eventuali criticità dell'ambiente **verificando il livello di difesa globale dell'infrastruttura OT e il livello di rischio** a cui è esposto il sistema industriale.

bi-rex Big Data Innovation & Research Excellence SIEMENS

bi-rex
Big Data Innovation & Research Excellence

SIEMENS

Design.



STEP 3

DESIGN NUOVA SOLUZIONE

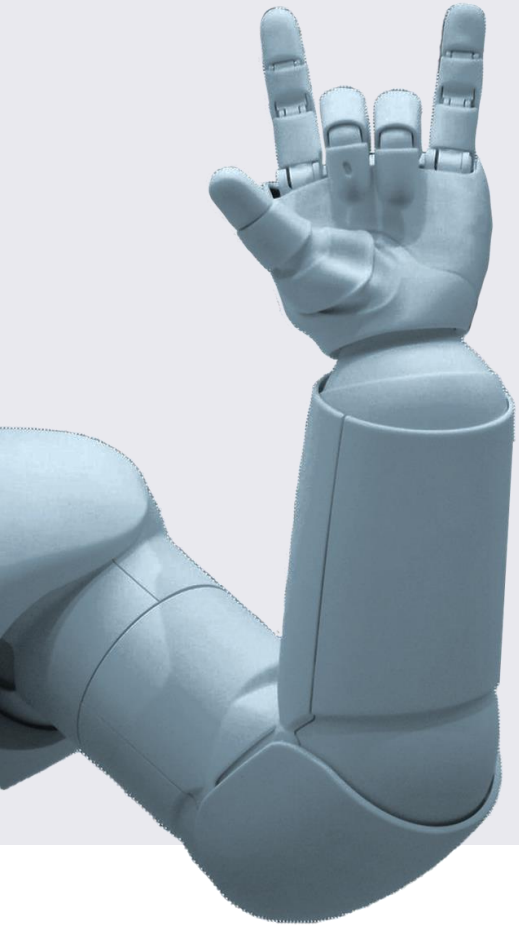
STESURA ARCHITETTURA E LAYOUT DI RETE

· Attiviamo il team di esperti di design infrastrutturale per **progettare un'infrastruttura di networking industriale flessibile e "secure by design"**, correggendo eventuali imprecisioni strutturali e disegnandola secondo gli standard di sicurezza richiesti.

bi-rex
Big Data Innovation & Research Excellence

SIEMENS

Build.



STEP 4
IMPLEMENTAZIONE ARCHITETTURA DI RETE

· **Realizzazione del progetto di nuova architettura di rete OT** applicando le migliori tecnologie idonee per l'ambiente industriale;
· Attività di network e security specifiche che richiedono alta competenza tecnica ed un' accurata gestione nella realizzazione del progetto.

> ANALISI RISCHI E MESSA IN SICUREZZA DELLA RETE OT

CENTRO DI COMPETENZA

CHALLENGE

Protezione dei sistemi industriali: garantire il controllo in real time, l'adattabilità, la disponibilità e la continuità di funzionamento,
la confidenzialità e l'integrità dei dati.

SIEMENS

bi-rex
Big Data Innovation & Research Excellence

© 2022 F.T.P. S.r.l.

POTENZIAMENTO E PROTEZIONE DEI SISTEMI INDUSTRIALI

INDUSTRIA FOOD & BEVERAGE

CHALLENGE

Difesa della rete OT: garantire l'adattabilità, la disponibilità e la continuità di funzionamento, e di produzione nonché la confidenzialità dei dati e la prevenzione dell'intrusione nei sistemi.

SIEMENS

© 2022 F.T.P. S.r.l.

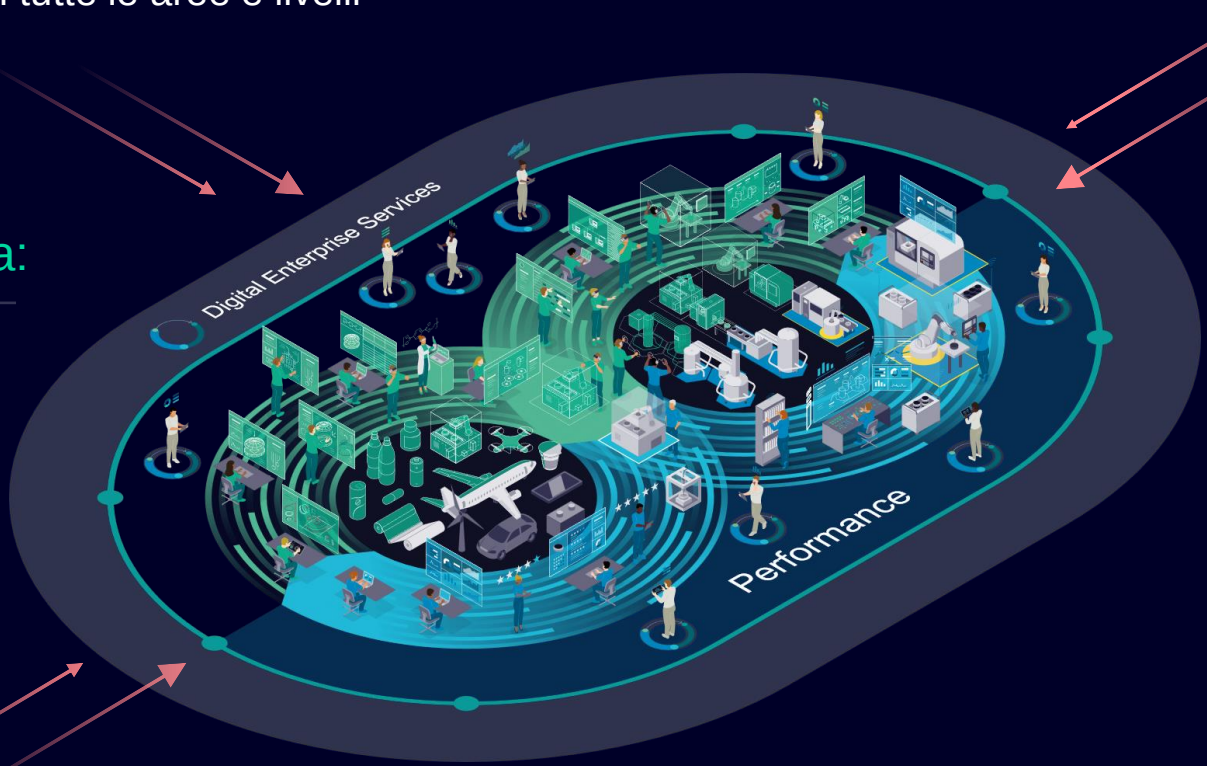
bi-rex Big Data Innovation & Research Excellence SIEMENS dfki

Technologies.

Le machine ed I sistemi di automazione sono interconnessi tramite IoT
Ciò significa integrazione OT/IT in tutte le aree e livelli

Convergenza OT/IT significa:

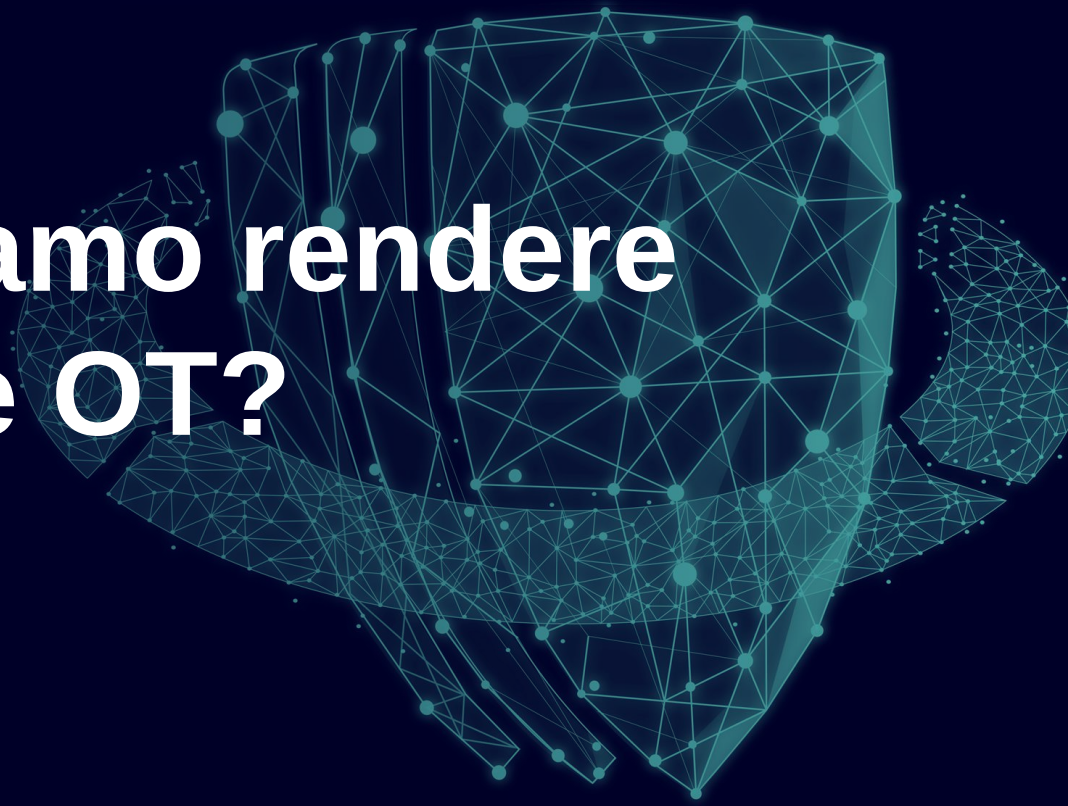
- **Maggiore connettività**
- **Più dati**
- **Nessun rischio al livello di cybersecurity**



Unrestricted | © Siemens 2022

SIEMENS

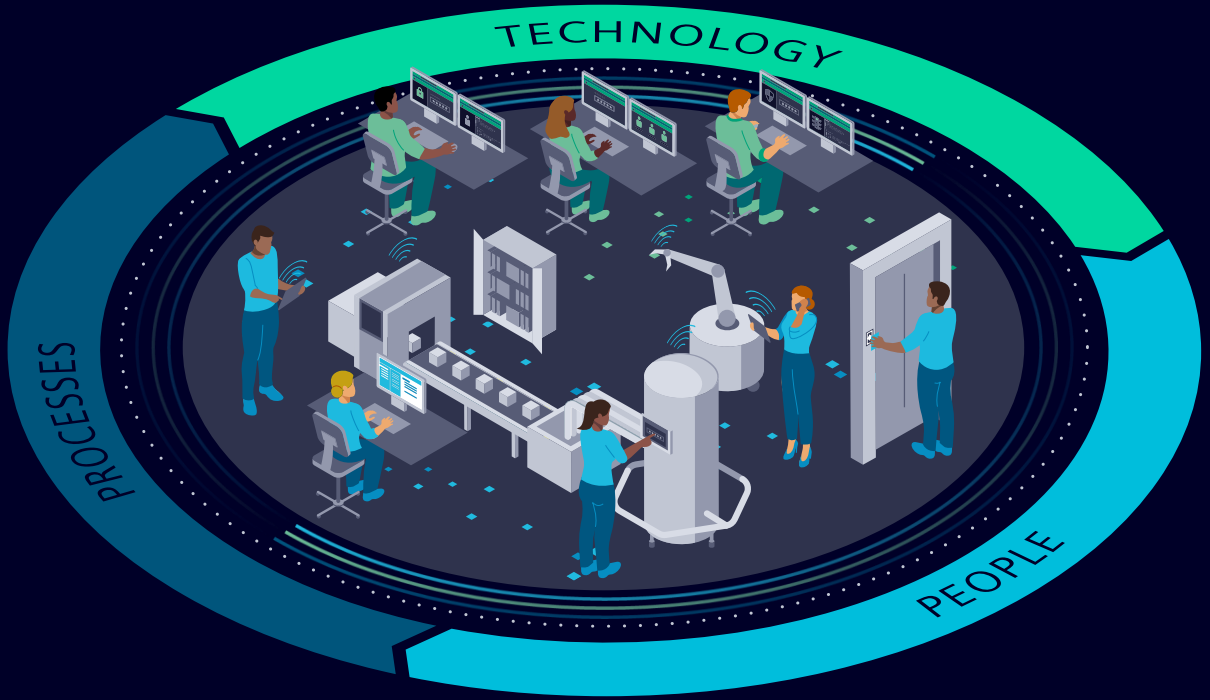
Come possiamo rendere sicura la rete OT?



Unrestricted | © Siemens 2022

SIEMENS

Un approccio olistico alla sicurezza informatica è guidato da tre pilastri principali Persone, Tecnologia e Processi



Policies e procedure

Misure di sicurezza

Competenze

Unrestricted | © Siemens 2022

SIEMENS

Solo un concetto di sicurezza globale basato sul principio della defense in depth può fornire una protezione efficace

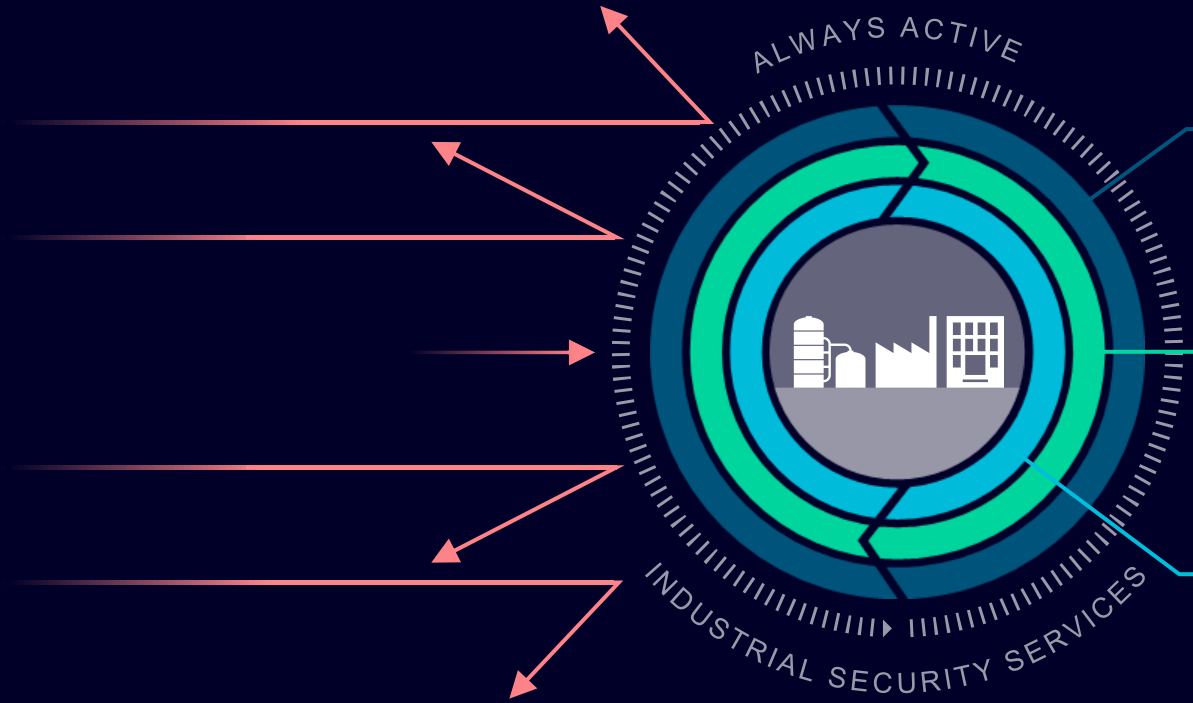
Concetto multi-layer per la sicurezza industriale

Instrinseco in un ecosistema in crescita

Unrestricted | © Siemens 2022

SIEMENS

Solo un concetto olistico di sicurezza industriale può essere efficace contro le minacce informatiche



Plant security

- Protezione dell'accesso fisico
- Politiche di sicurezza
- Monitoraggio della sicurezza

Network security

- Protezione di cella, rete perimetrale e zone attendibili
- Firewall e VPN

System integrity

- System Hardening
- Gestione delle patch
- Autenticazione e protezione dell'accesso

Unrestricted | © Siemens 2022

SIEMENS

Network Security

Unrestricted | © Siemens 2022

SIEMENS

Overview: Network Security

Misure adatte alla produzione:

Network access control

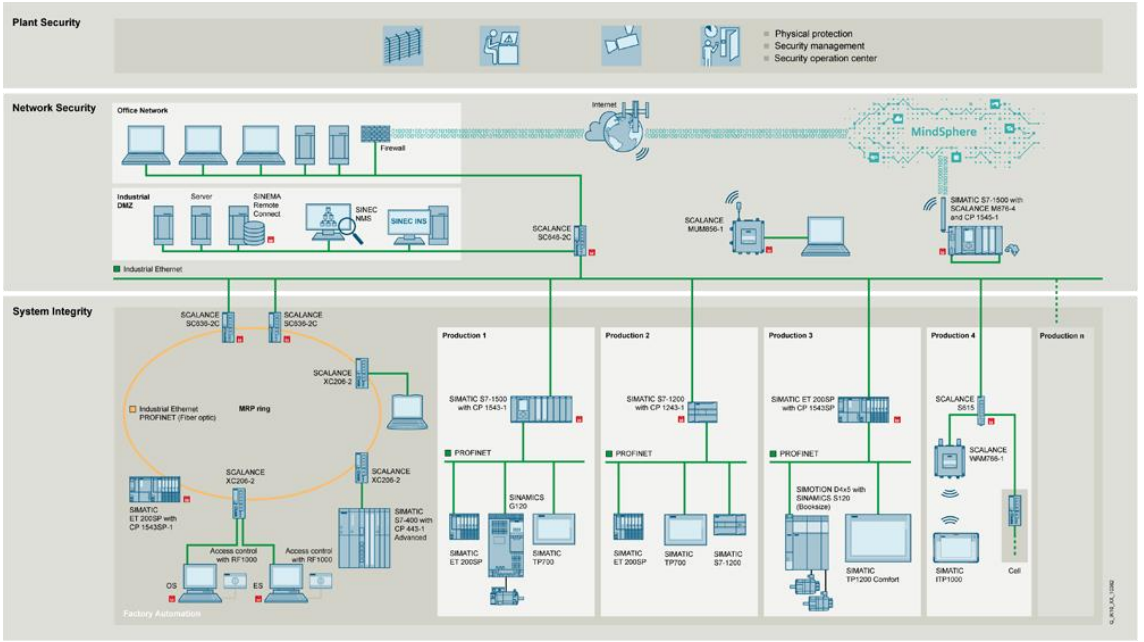
- Interfaccia sicura alle reti IT
- Architettura sicura con DMZ
- Accesso remoto sicuro tramite Internet
- Proteggi l'accesso alla rete locale (sicurezza della porta) tramite l'autenticazione del dispositivo e dell'utente
- Connessione cloud sicura

Ridondanza

- Protezione delle topologie di rete ridondate

Protezione di Cella

- Mitigazione del rischio attraverso la segmentazione della rete
- Estensione del concetto di protezione cellulare mediante:
    - Processori di comunicazione di sicurezza
    - Configurazione VLAN flessibile



Products with firewall or VPN functionality

Unrestricted | © Siemens 2022

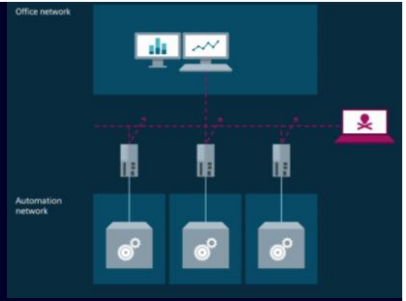
SIEMENS

Network Security- esempi applicativi

Protezione di cella

I dispositivi possono essere protetti all'interno di una cella di automazione utilizzando un firewall.

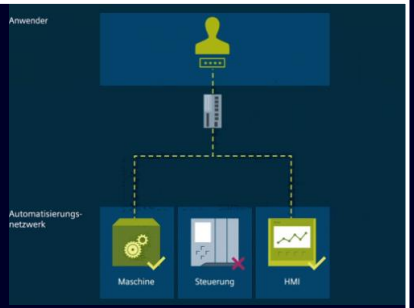
➔ SCALANCE S utilizzato come firewall di cella



Impostazione delle regole di firewall

L'accesso alle aree della rete e ai terminali è limitato a seconda delle persone e dei ruoli

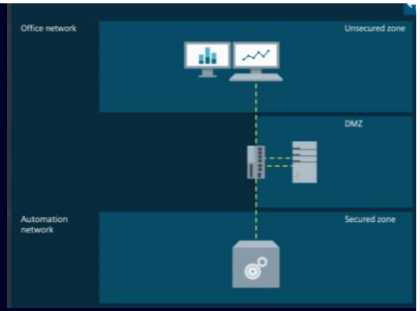
➔ Con i dispositivi di sicurezza industriale SCALANCE S vengono applicate temporaneamente regole firewall specifiche per l'utente.



Demilitarized zone (DMZ1[1])

La DMZ viene realizzata per assicurare la sicurezza della connessione tra rete office e di automazione

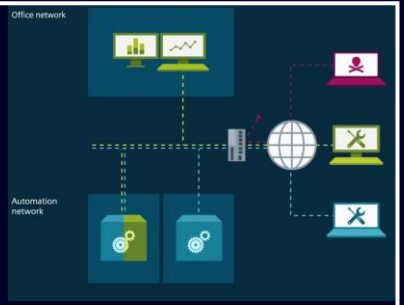
➔ Lo SCALANCE S permette di interconnettere in modo sicuro le due rete e la DMZ[1].



Accesso remoto

L'accesso remoto viene reso sicuro grazie alla gestione degli utenti ed i relativi diritti.

➔ Crittografia della comunicazione dati e controllo accessi a terminali dedicati.



1) Demilitarized zone

SIEMENS

Network Security
Proteggere le reti industriali con lo SCALANCE S

SCALANCE S615

Funzionalità

Configurazione flessibile di zone sicure:

- Assegnazione delle porte a specifiche VLANs

Funzionalità di sicurezza integrate:

- Stateful Inspection Firewall
- User Specific Firewall
- Virtual Private Network (VPN)
- Network Address Translation (NAT)

Data **throughput adatti all'industria**:

- 100 Mbps for firewall and routing
- 035 Mbps for IPsec-VPN

Ingegneria integrate tramite:

- TIA portal e SINEC NMS

Integrato nel **SINEMA Remote Connect**

Benefici

Segmentazione di cella, creando anche DMZ

Protezione di rete contro:

- Accessi non autorizzati
- Manipolazione dei dati

Configurazione centralizzata e possibilità di monitoraggio

Amministrazione centralizzata e facilità di configurazione

Unrestricted | © Siemens 2022

SIEMENS

Network Security
Accesso 3G/4G tramite SCALANCE M

M876-3 **M876-4**

Funzionalità

Connessione sicura tramite comunicazione mobile:

- 3G / HSPA+
- 4G / LTE

Funzionalità di sicurezza **integrate**:

- Stateful Packet Inspection Firewall
- User Specific Firewall
- Virtual Private Network (VPN)
- Network Address Translation (NAT)

Configurabile da Web Page o ingegnerizzabile tramite:

- SINEC NMS

Integrato in **SINEMA Remote Connect**

Implementazione di un concetto flessibile di zona sicura

Benefici

Segmentazione di cella, creando anche DMZ

Protezione di rete contro:

- Accessi non autorizzati
- Manipolazione dei dati

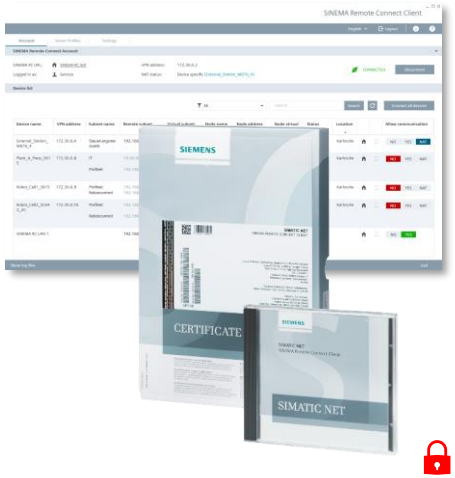
Configurazione centralizzata e possibilità di monitoraggio

Amministrazione centralizzata e facilità di configurazione

Unrestricted | © Siemens 2022

SIEMENS

Network Security
Gestione dell’accesso da remoto: SINEMA Remote Connect



SINEMA Remote Connect

Funzionalità

Gestione sicura delle connessione tra I tecnici in teleassistenza da remote e l’impianto

Funzionalità di sicurezza integrate:

- Virtual Private Network (VPN)
- Dedicated Device Access (DDA)
- Accesso tramite PKI al SINEMA RC Client
- Gestione degli utenti tramite UMC

Concetto di sicurezza integrato:

- SIMATIC Security CPs
- Router industriale 4G/3G SCALANCE M
- Router industriale con rete cablata SCALANCE S

Benefici

Gestione centralizzata degli accessi da remoto

Protezione di rete contro:

- Accessi non autorizzati
- Diritti di accesso specifici dell'utente per verso indirizzi IP e device specificati

Comunicazione gestita in modo centralizzato da un unico server e scambio certificati

[1] Active Directory

SIEMENS

Network Security
SCALANCE LPE9403 – local processing engine

Funzionalità

- 2x RJ45 10/100/1000 Mbps
- 1x Combo-Port – 10/100/1000 Mbps RJ45 o 100/1000 Mbps SFP
- Abilita la collaborazione remota basata su **Zero Trust** con ambienti OT in combinazione con fornitori di terze parti
- Implementazione in ambienti dismessi basati sulla «Defense in Depth»
- Sistema aperto basato su Linux
- Alimentazione ridondata
- Approvazioni complete: ATEX, IECEx, cULus HazLoc, FM, cantieristica

Benefici

L'elevata velocità di trasmissione dei dati consente un'elaborazione rapida dei dati. Comunicazione e trasferimento di informazioni su lunghe distanze tramite cavo in fibra ottica.

Piattaforma hardware Siemens per l'installazione in loco di connettori Zscaler per la comunicazione Uomo-Macchina.

Configurazione dell'accesso personalizzabile in "Zscaler Zero Trust Exchange" e integrazione perfetta nelle infrastrutture di rete esistenti.

Protezione dei dispositivi legacy e accesso remoto sicuro tramite la combinazione di protezione perimetrale con Zero Trust.

I connettori Zscaler stabiliscono breakout Internet diretti e crittografati su Zscaler Zero Trust Exchange. Non sono richieste ulteriori regole del firewall in entrata.

Funzionamento affidabile anche in caso di interruzione dell'alimentazione.

Utilizzo in varie applicazioni, ad es. nella Zona Ex 2 in base alle omologazioni.

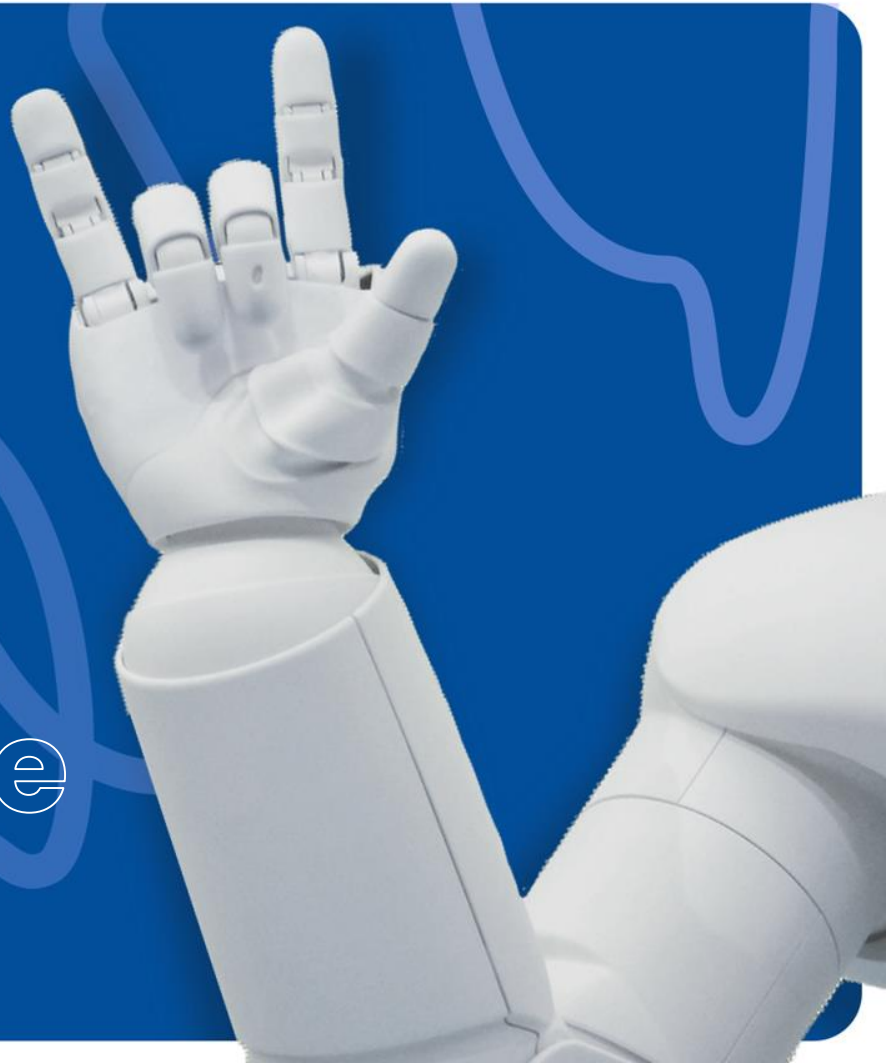
Unrestricted | © Siemens 2022

SIEMENS

TOUR GUIDATO DELLA LINEA PILOTA

BI-REX (Francesco Meoni e Gianmarco Moretti)

bi-rex
Big Data Innovation & Research Excellence

SIEMENS

Grazie
per l'attenzione