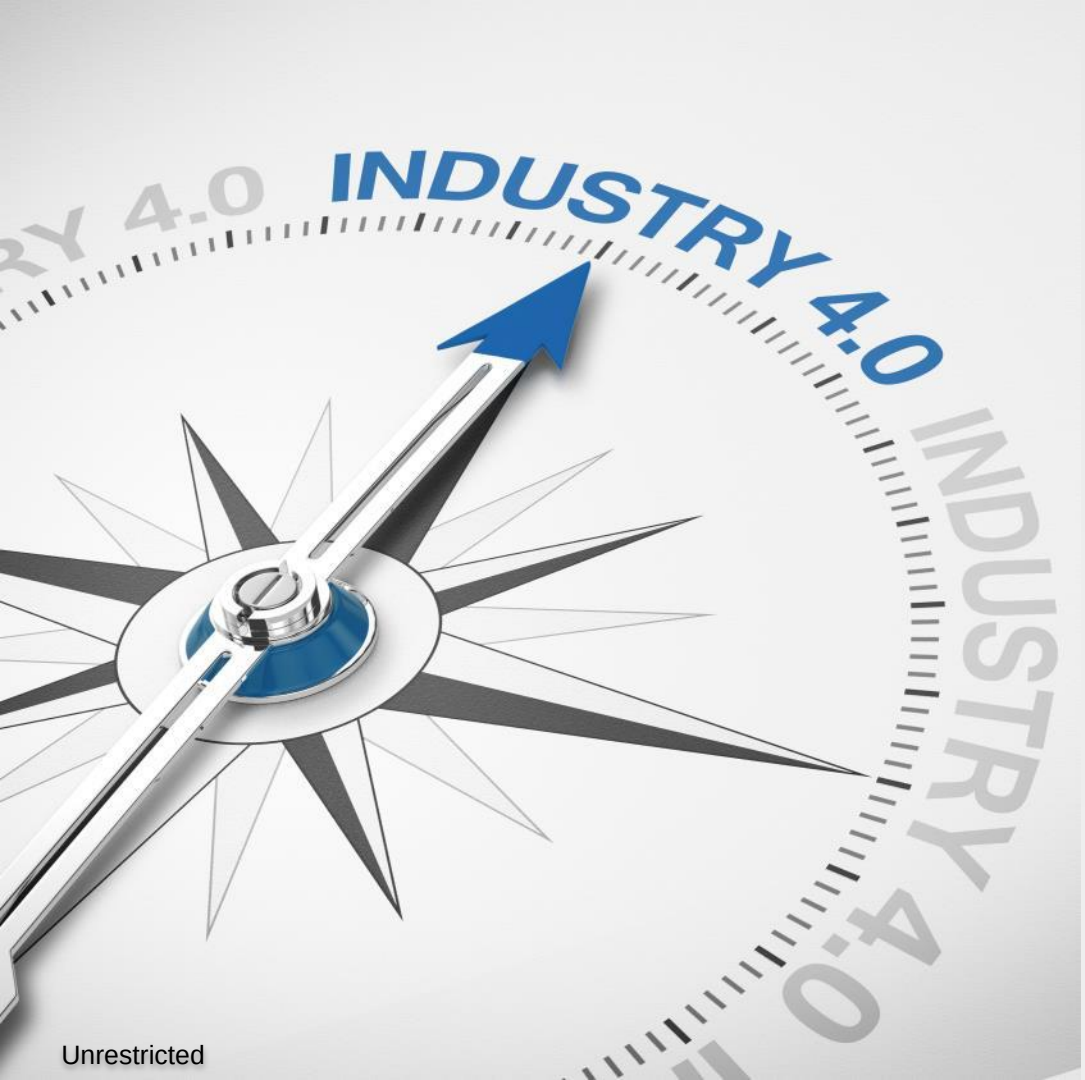


Realizzare l'interconnessione sicura e affidabile tra reti OT e IT

SIEMENS
Ingenuity for life

Organizzato da

La Digitalizzazione abilita la crescita dell'Industria

+ 3300%

growth of data volume from 2000 -2025[1)]

+ 526 %

market growth of industrial robots from 2000 – 2025[1)]

Digitalization changes everything

+ 1250 %

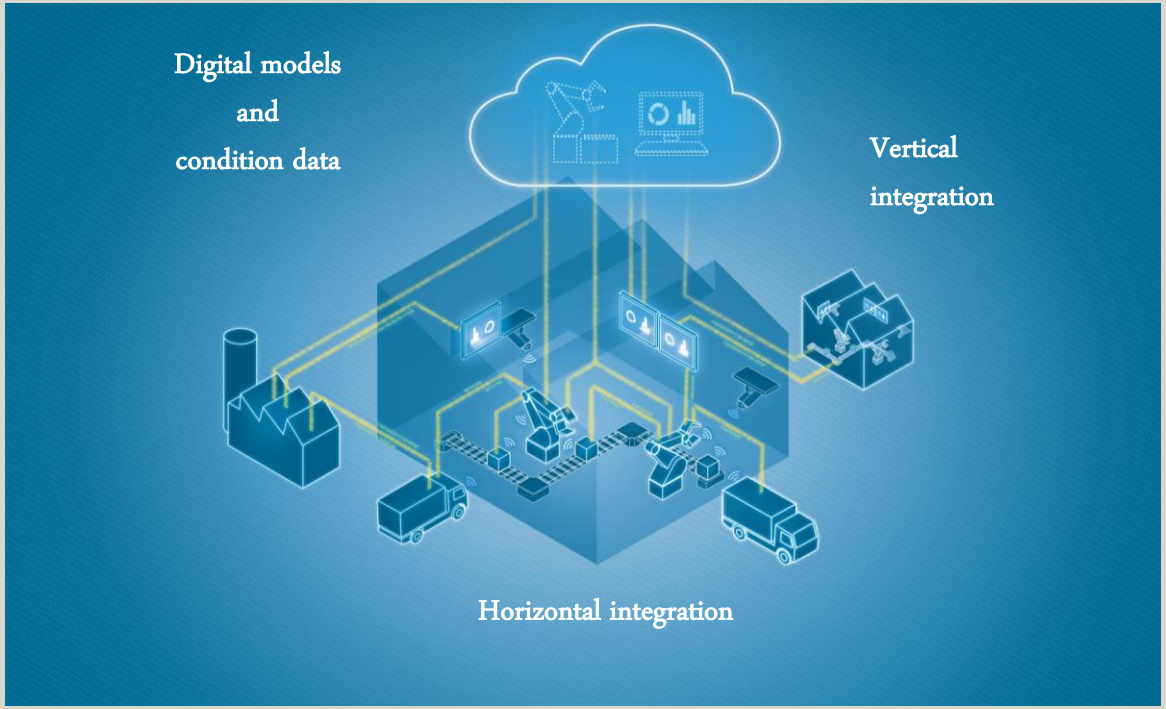
Increase of connected machines from 2000 – 2025[1)]

1200

of G2000 manufacturers rely on digital platforms by 2020[2)]

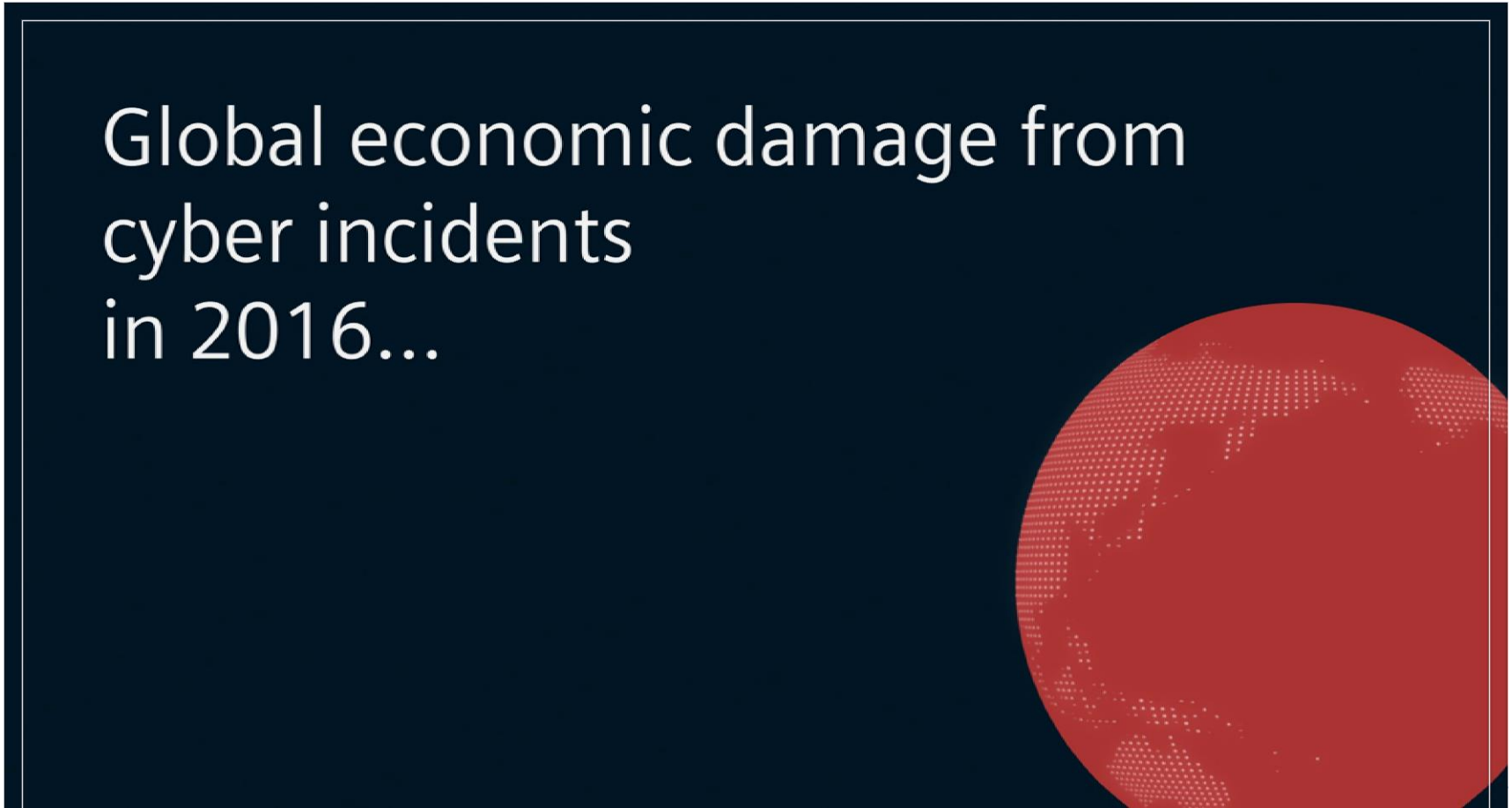
* Sources: 1) Weinländer: Industrielle Kommunikation – Basistechnologie für die Digitalisierung der Industrie. Berlin. Beuth/VDE, 2017
2) IDC FutureScape: Worldwide manufacturing 2018

E’ necessaria un’integrazione completa del sistema di produzione



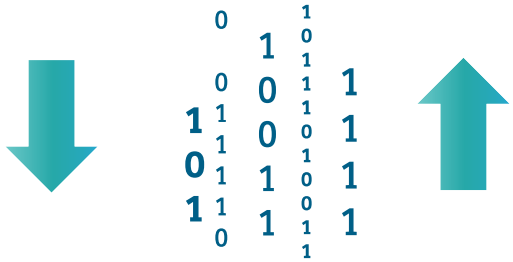
Potenti reti di comunicazione per gestire una quantità imponente di dati

- **Alta velocità**: Comunicazione Real-time
- **Alti volumi di dati**: Ampia larghezza di banda
- **Protezione contro spionaggio e attacchi**: Comunicazione Sicura
- **Connettività garantita**: Componenti e reti robusti e affidabili
- **Flessibilità**: componenti Plug’n’play, facili da riconfigurare


Global economic damage from
cyber incidents
in 2016...

Le Reti di produzione (OT) e le Reti enterprise (IT) si integrano

IT: Information Tecnology



OT: Operational Tecnology

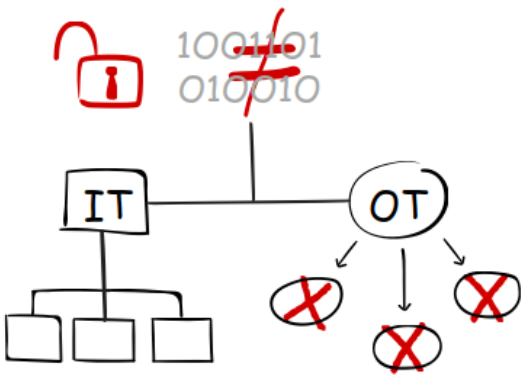
Necessità di definire modelli opportuni per l'interconnessione tra OT e IT

Trasparenza
Security

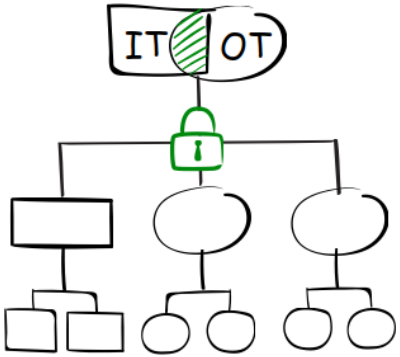
Big Data
Industrial IOT

Flessibilità
Uptime

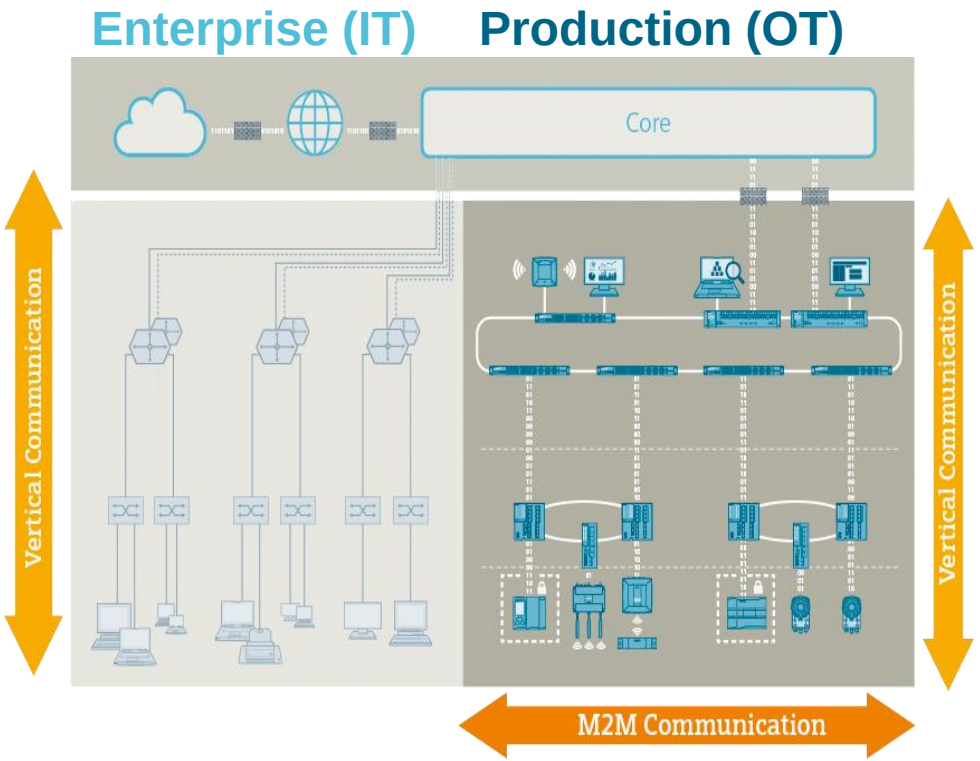
Convergenza



Collaborazione

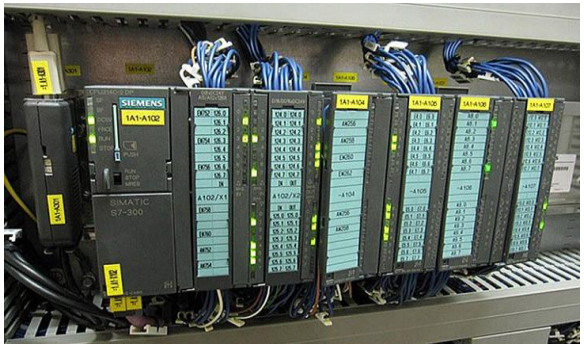


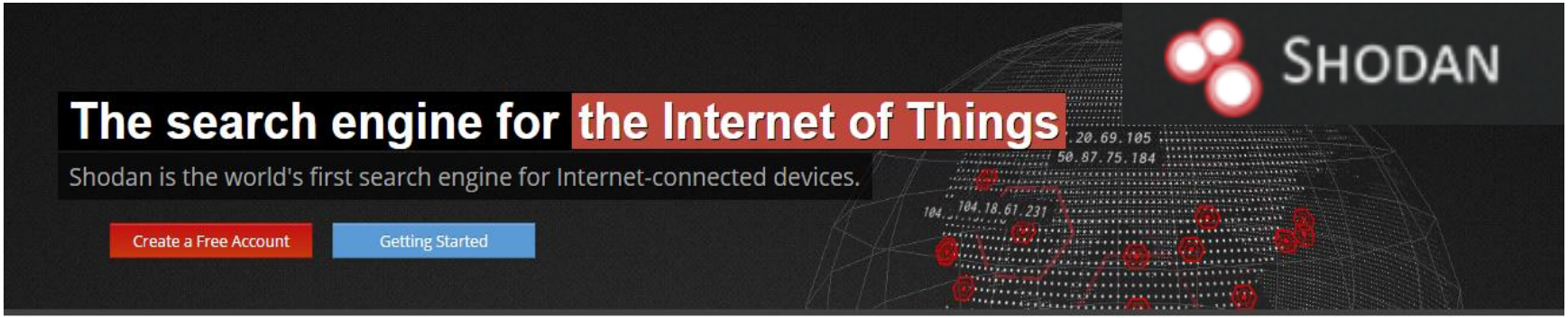
I requisiti specifici delle Reti di produzione!



- Alta Disponibilità
- Robustness
- Flessibilità
- Determinismo
- Security
- Safety

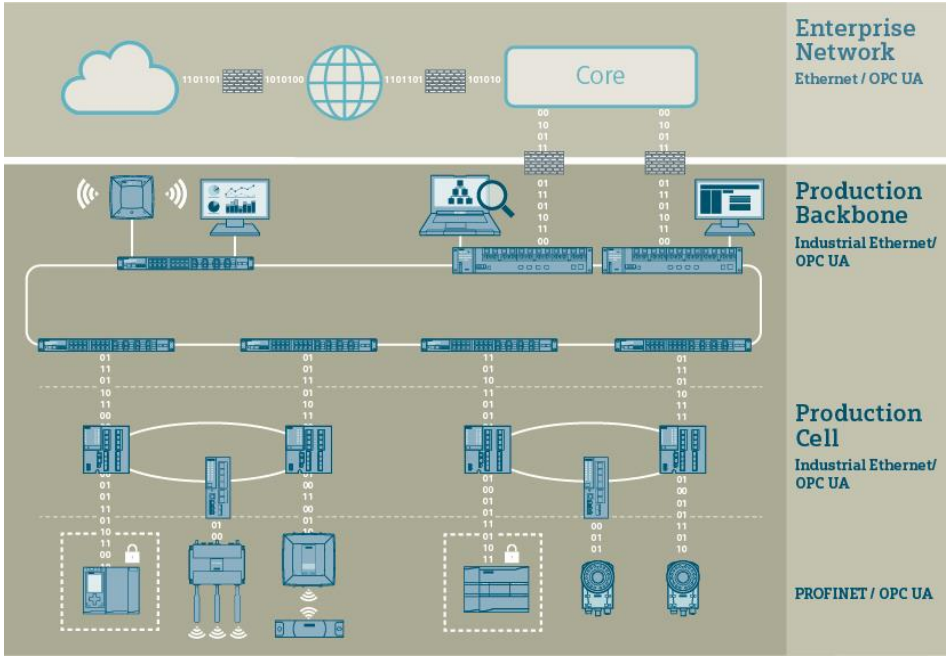
Certe “cose” non sono fatte per essere collegate “as is” ad Internet…





https://www.shodan.io/

Infrastruttura per l'interconnessione tra OT e IT



Aspetti di produzione relativi al networking

Network structure

Architettura ridondata e segmentata per una rete di comunicazione affidabile e sicura, scalabile e aperta. Integrata con il cloud

Mobile applications

Semplice e veloce accesso dei dati tramite **dispositivi Wireless industriali** e grazie alla tecnologia **RTLS**

Network Management

Massima trasparenza delle reti industriali e dei relativi dispositivi collegati

Network security

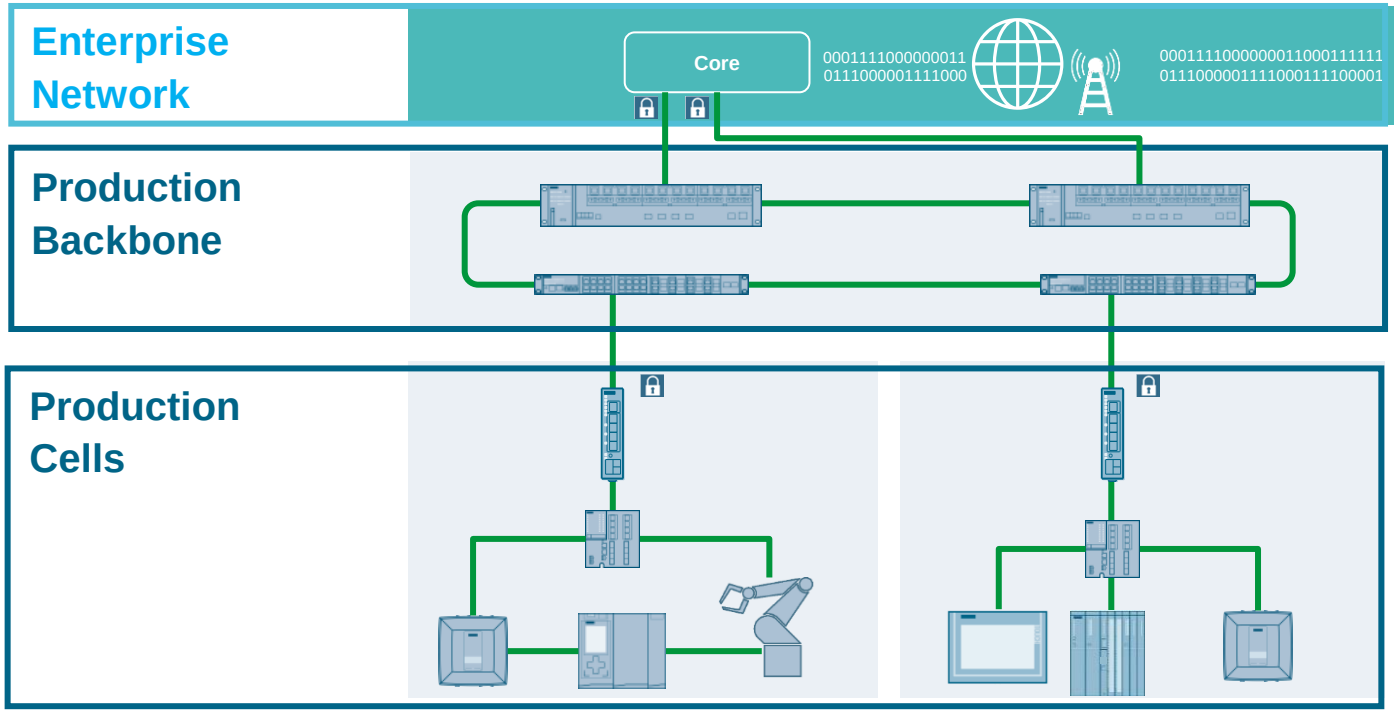
Permessa da un approccio olistico e un **concept** con portfolio "**security-integrated**". Abilitando una **comunicazione sicura ad impianti** e macchine

Reti di comunicazione interconnesse tramite una Backbone Aggregation industriale

Segmentazione delle strutture di rete

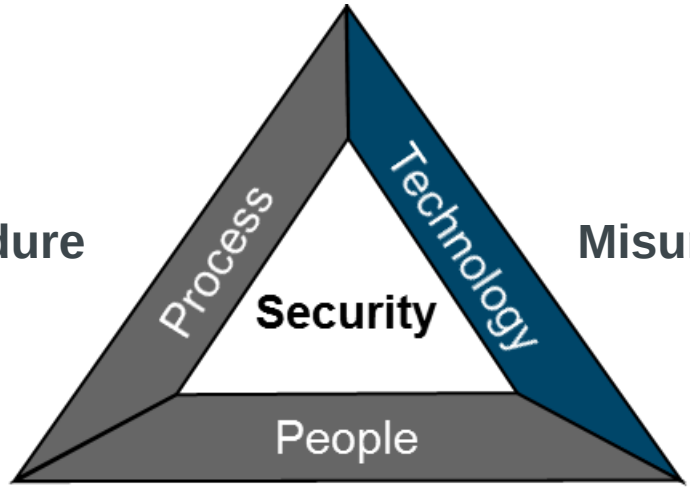
Cosa significa?

- ✓ **Celle di produzione protette**
- ✓ **Meccanismi di ridondanza di rete**
- ✓ **Separazione IT e OT**
- ✓ **Topologie di reti flessibili**



In primis, l' Industrial Security è legata a…

Policy e procedure



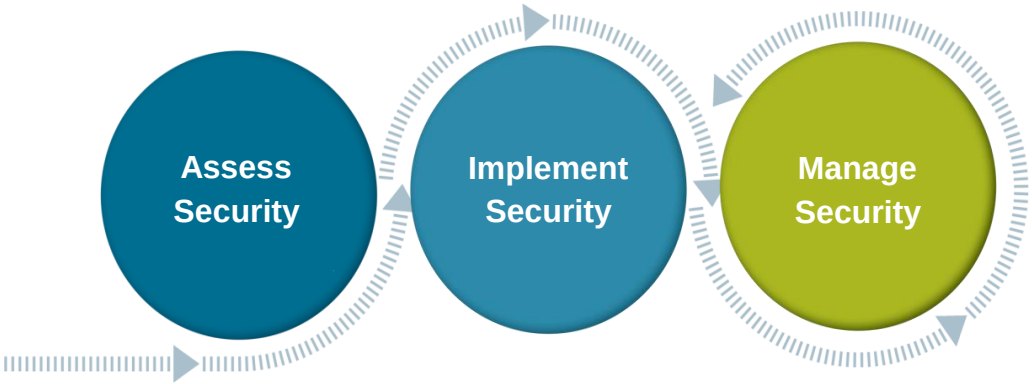
Misure di security

Competenza

Un approccio olistico per la security è un concetto che include: tecnologie, processi e persone

Garantire la disponibilità dell'impianto con un processo continuo di metodologia del rischio

Assess Security
Valutazione del sistema di security attualmente installato



Implement Security
Mitigazione del rischio attraverso l'implementazione di misure di security per una protezione reattiva

Manage Security
Gestione della sicurezza tramite monitoring e protezione proattiva

IEC 62443
Security per OT (Operation Technology)

IEC 62443: standard security in ambito IACS – Industrial Automation and Control System - **basato sul principo "Defense in depth"** → protezione su più livelli

Procedure, Linee guida, Training, …

Controllo accessi, Telecamere..

Firewall, DMZ, VPN, …

Sistemi di rilevamento intrusione …

Hardening di applicazione e sistema…

Gestione utenti, crittografia, certificati digitali …

Industrial Security

Concetto “Defense in Depth” – ISA 99 / IEC 62443

Defense in Depth

Plant security

- Meccanismi di protezione fisica per accesso ad aree critiche
- Implementazione processo di security management

Industrial Security Services
Assessment

Industrial Security Check

Assessment IEC 62443

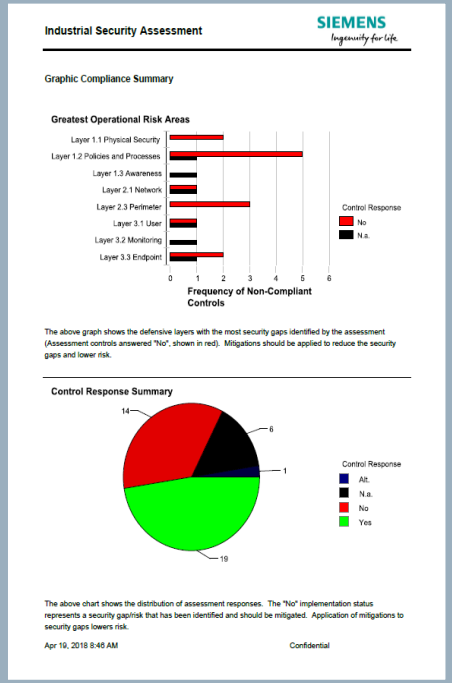
(e ISO 27001) per la sicurezza della fabbrica in funzione degli standard

Risk & Vulnerability

Assessment per l'identificazione, classificazione e valutazione per un programma basato sulla metodologia del rischio

Servizi di Scanning

per ottenere la trasparenza sugli asset e software usati nell'ambiente di automazione


Industrial Security Assessment

SIEMENS
Ingenuity for life

Graphic Compliance Summary

Greatest Operational Risk Areas

Layer 1.1 Physical Security
Layer 1.2 Policies and Processes
Layer 1.3 Awareness
Layer 2.1 Network
Layer 2.3 Perimeter
Layer 3.1 User
Layer 3.2 Monitoring
Layer 3.3 Endpoint

0 1 2 3 4 5 6

Frequency of Non-Compliant Controls

Control Response
No
N.a.

The above graph shows the defensive layers with the most security gaps identified by the assessment (Assessment controls answered "No", shown in red). Mitigations should be applied to reduce the security gaps and lower risk.

Control Response Summary

14
6
1
19

Control Response
Alt.
N.a.
No
Yes

The above chart shows the distribution of assessment responses. The "No" implementation status represents a security gap/risk that has been identified and should be mitigated. Application of mitigations to security gaps lowers risk.

Apr 19, 2018 8:46 AM Confidential

Vulnerability	Risk score
Flat network architecture/ No DMZ available	x.x
Flat network architecture/ No network segmentation	x.x
Unsecure/ Not controlled remote activities	x.x
No system hardening/Unneeded applications and services installed	x.x
Unpatched operating system	x.x
Obsolete Antivirus database	x.x
Windows firewall not active	x.x
Uncontrolled USB interfaces	x.x

Red (7.5 – 10) = Unaccaptable risk; Urgent action is necessary
Orange (5 – 7.5) = Unaccaptable risk; Acrtion is required
Yellow (2.5 – 5) = Accaptable risk; Subject to management approval
Green (0 – 2.5) = Accaptable risk; No action required

Industrial Anomaly Detection (IAD)
Cos'è e cosa fa?

Monitora la security in modo totalmente passivo e automatico!!!

1. Rileva i dispositivi (PLC, PC, drives…) **e le loro caratteristiche** (versione software, …)

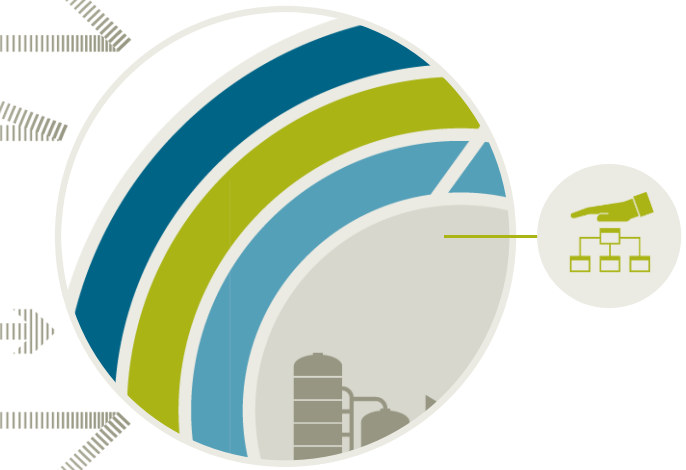
2. Avvisa in caso di attività ritenute anomale (es. PLC che inizia mandare comandi "strani")

16

Industrial Security

Concetto “Defense in Depth” – ISA 99 / IEC 62443

Defense in Depth



Network security

- Protezione di cella, DMZ assitenza remota
- Firewall e VPN

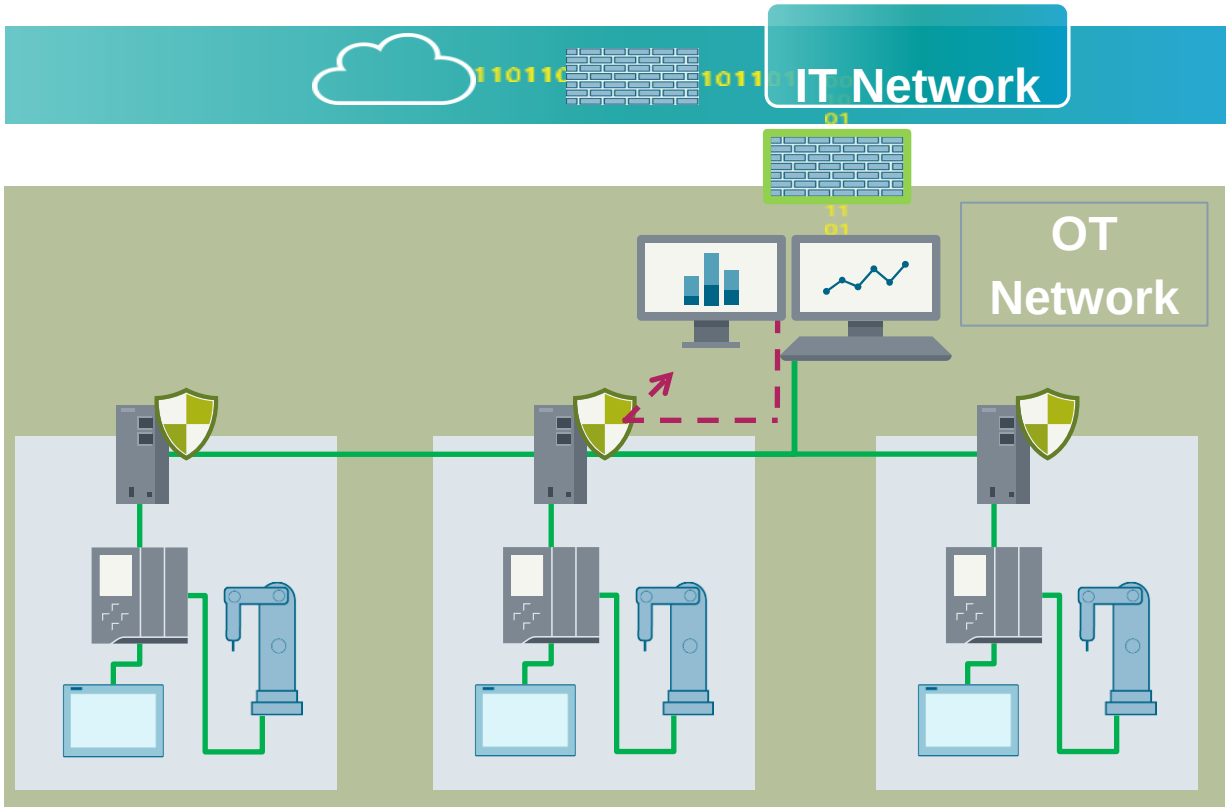
Network Security
Firewall e Segmentazione

Automation Firewall NG

- **Conessioni VPN** di **dispositivi** e **utenti** tramite gestione centralizzata

Protection Cell Firewall

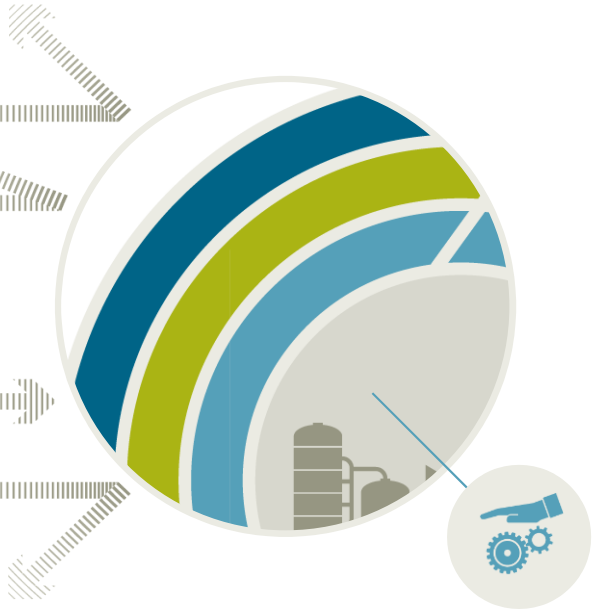
- **OpenVPN** con attivazione VPN tramite **Digital input**



Industrial Security

Concetto “Defense in Depth” – ISA 99 / IEC 62443

Defense in Depth



System integrity

- Hardening del sistema, OPC UA
- Piano di aggiormanto software permessi e antivirus
- Autenticazione riservata a gruppi di operatori

Caso applicativo Food production

Esigenze del cliente

Realizzare il raddoppio della linea di produzione

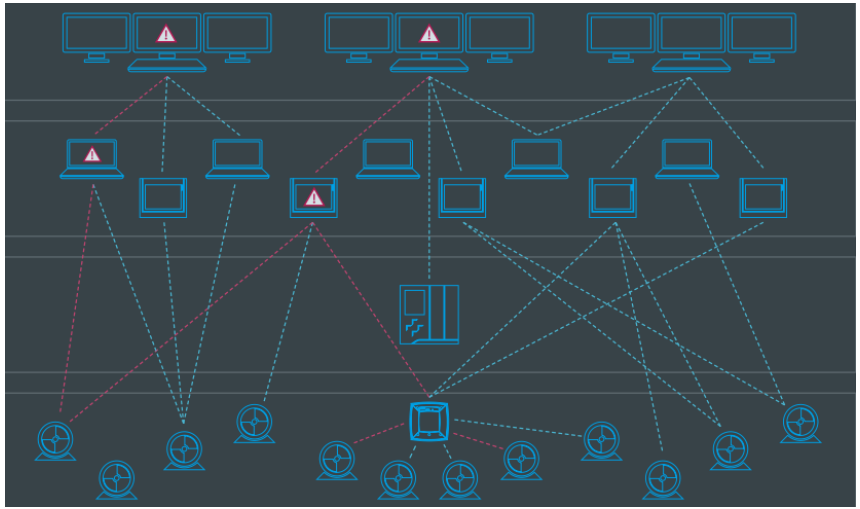
Raccolta dati da portare nella rete corporate in «sicurezza»

Segmentazione della rete industriale

Assistenza remota alle macchine degli OEM: come realizzarla in maniera «sicura»?

Caso applicativo Food production

Situazione iniziale



Assessment dell'impianto:

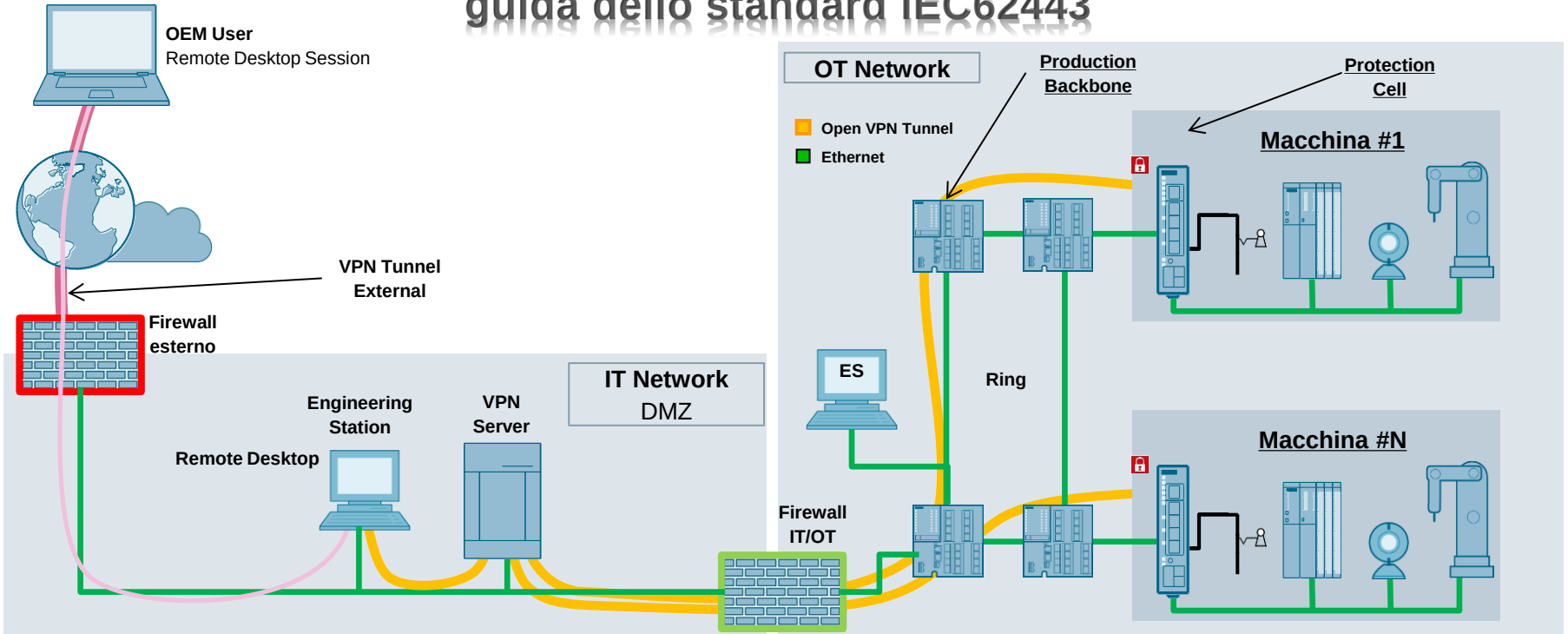
Rete di stabilimento «flat», gestione non strutturata dei dati, assenza di sicurezza

Teleassistenza gestita da IT ma senza controllo accessi degli OEM

Caso applicativo Food production

Project design & implementation con coinvolgimento IT e OT

Sviluppo del design di rete in accordo alle linee guida dello standard IEC62443



Caso applicativo Beverage production

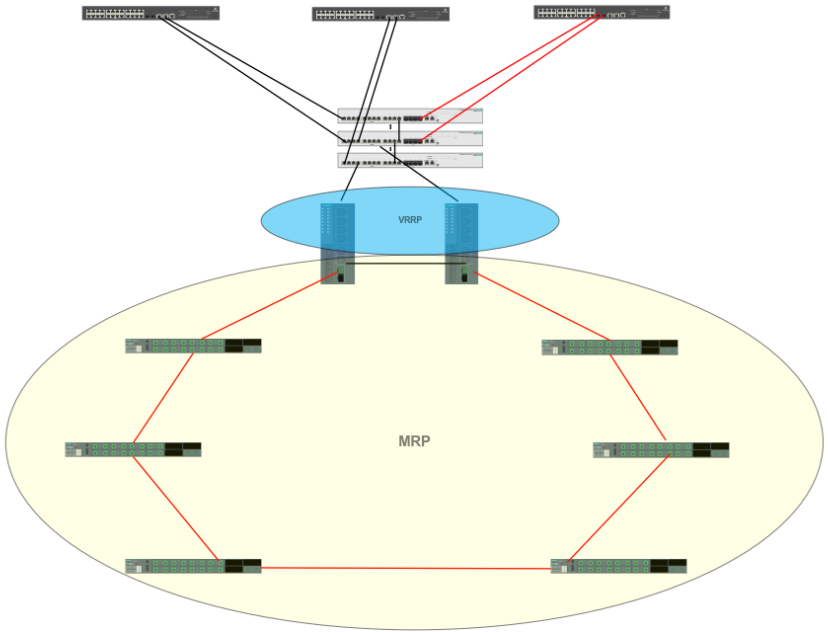
1. Come è nata la richiesta

- Vecchia linea industriale (>10 anni)
- Ammodernamento della linea per aumentare le performance, adesione al piano Impresa 4.0

2. Esigenze del cliente

- Autonomia di gestione della linea di produzione (controllo da parte dell'OT)
- Integrazione con i sistemi gestionali
- Assistenza remota sicura

3. Come è stata sviluppata la soluzione



- Assessment dell'impianto
- Project design &implementation
- Industrial Anomaly Detection