Linea Pilota

Use case dell'area IoT

Le tecnologie

Additive Manufacturing

Selective laser melting (SLM)

Deposizione Diretta - DED

Materiali Plastici

Rifinitura e metrologia

Stazioni di Misura

Centro di lavoro - CNC

5G

Robotica

Robotica Mobile

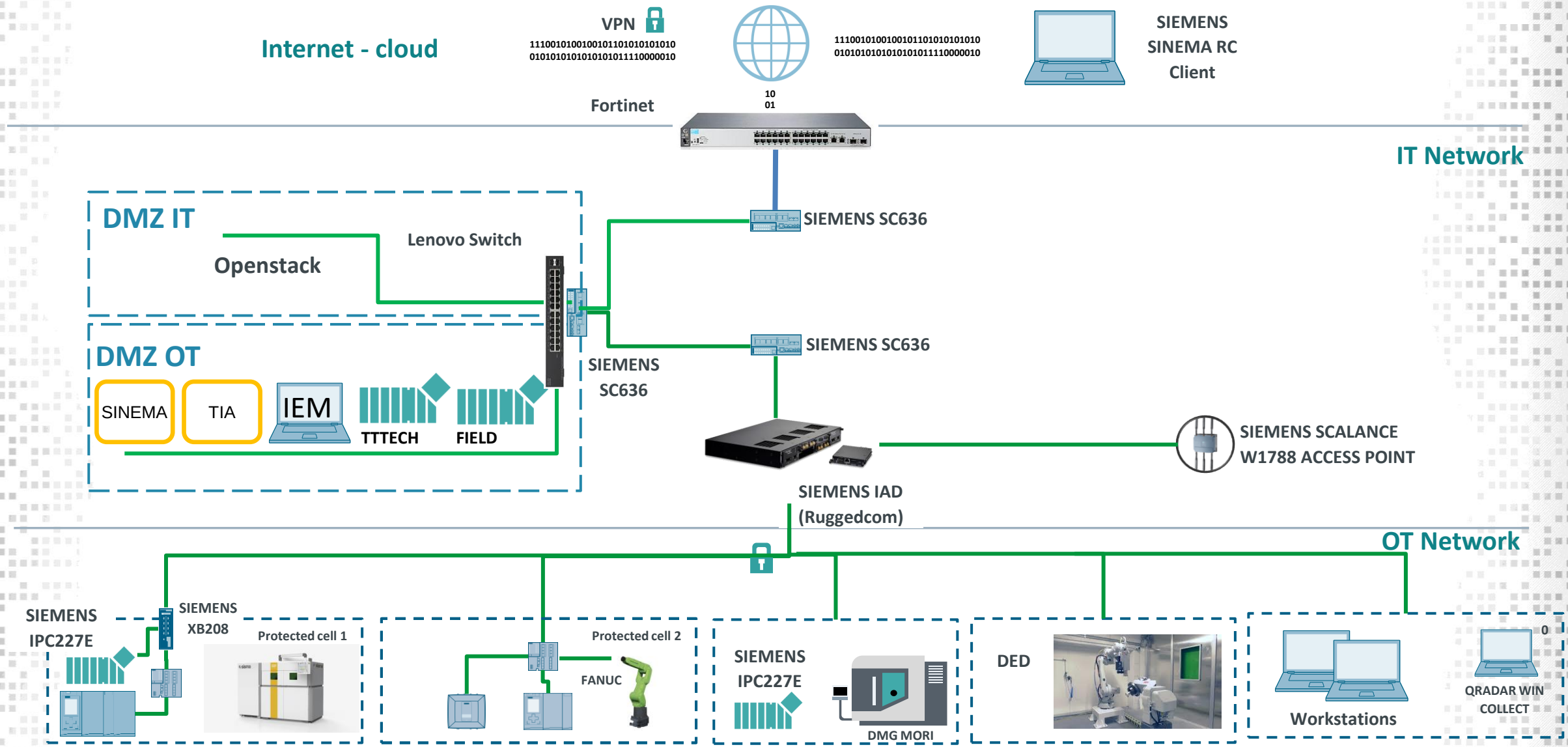
Robotica Collaborativa

IoT e Big Data

Edge computing

Cloud e analytics

Architettura di rete - HW



Cybersecurity compliance

Standard ISA 62443

- Separazione tra IT e OT
- Segregazione e Segmentazione
- Introduzione DMZ IT/OT con accesso in VPN
- Ispezione traffico OT e Intrusion-Anomaly Detenction (Nozomi)

Perché?

- Impedire flusso di dati diretto tra le macchine e l'esterno (in ambo le direzioni)
- Monitoraggio della rete
- Identificazione e prevenzione di attacchi
- Notifica verso il management e automazione di azioni di reazione agli attacchi (QRadar)

Architettura di rete – SW monitoring

QRadar

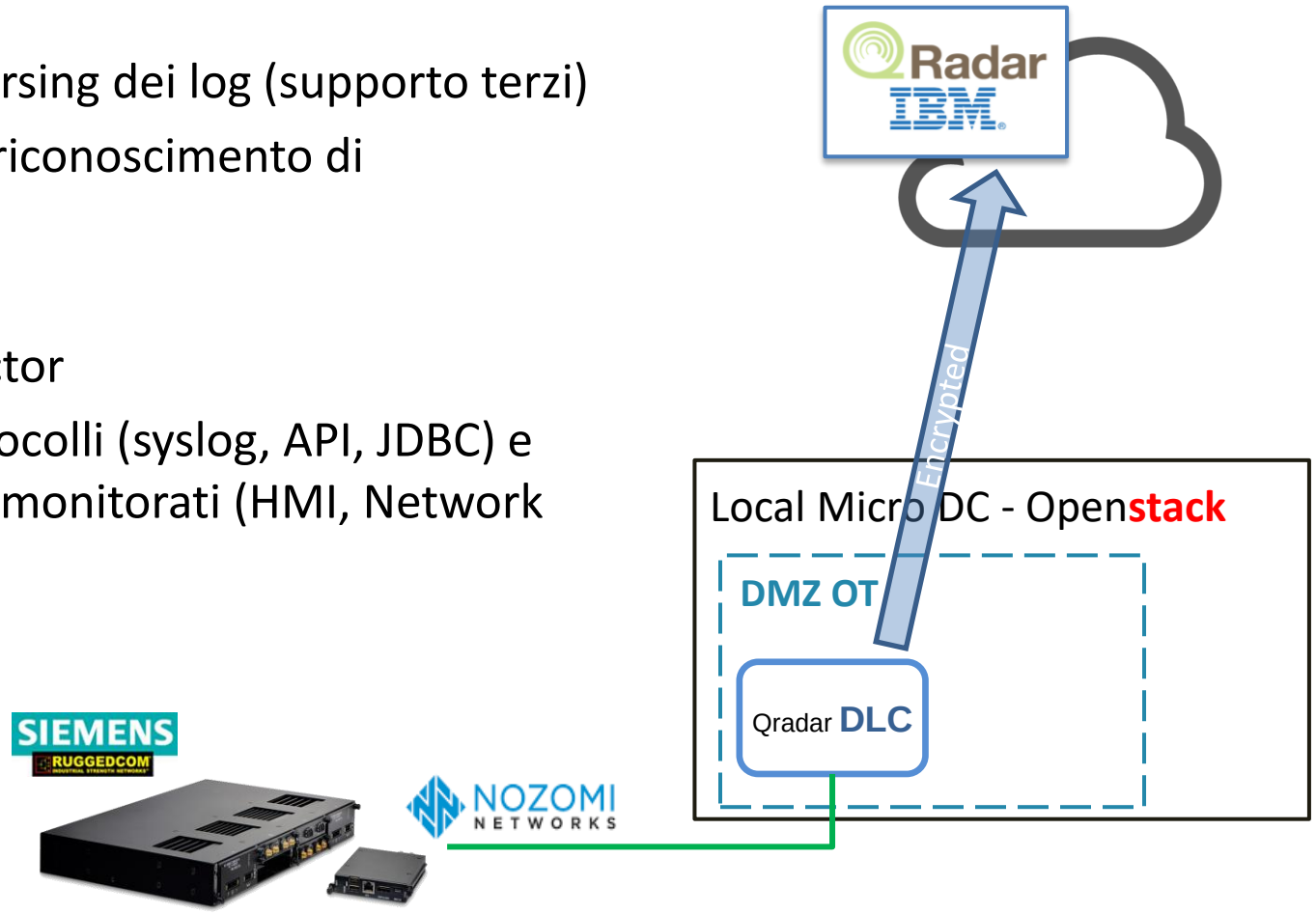
- Moduli Add-On per il parsing dei log (supporto terzi)
- Trigger per azioni dopo riconoscimento di determinati pattern

DLC

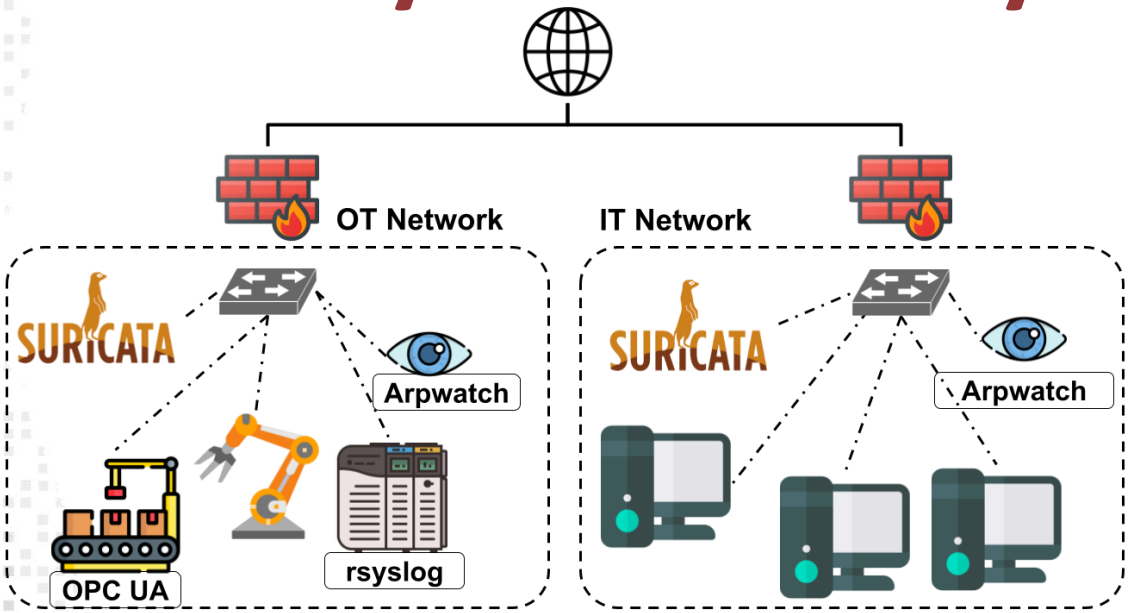
- Disconnected Log Collector
- Supporta differenti protocolli (syslog, API, JDBC) e eterogeneità dei device monitorati (HMI, Network device, Nozomi)

Nozomi

- Anomaly detection
- Log report



SS4SP:
Safety and Security for Smart Production



Metodologie e tecniche per la cyber security
basate su approccio integrato IT/OT

Obiettivi

- Migliorare sicurezza informatica, continuità operativa e safety di impianti dell'Industria 4.0

Output e Benefici

- Riduzione dell'esposizione al rischio cyber
- Prevenzione e mitigazione delle conseguenze su safety e continuità
- Adeguamento delle modalità operative

SACMI IMA SPA imola informatica SIEMENS SAMP Alascom

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Università degli Studi di Ferrara

UNIMORE UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA