Associazione Italiana Strumentisti

ISA Italy Section

«LE DIMENSIONI DELLA SICUREZZA INDUSTRIALE»
I percorsi della sicurezza industriale dagli standard ISA/IEC 62443 ai temi della cybersecurity

Milano, 30 Maggio 2018

Auditorio TECNIMONT

Nuove Soluzioni Intelligenti OT per la Protezione dei Network Industriali

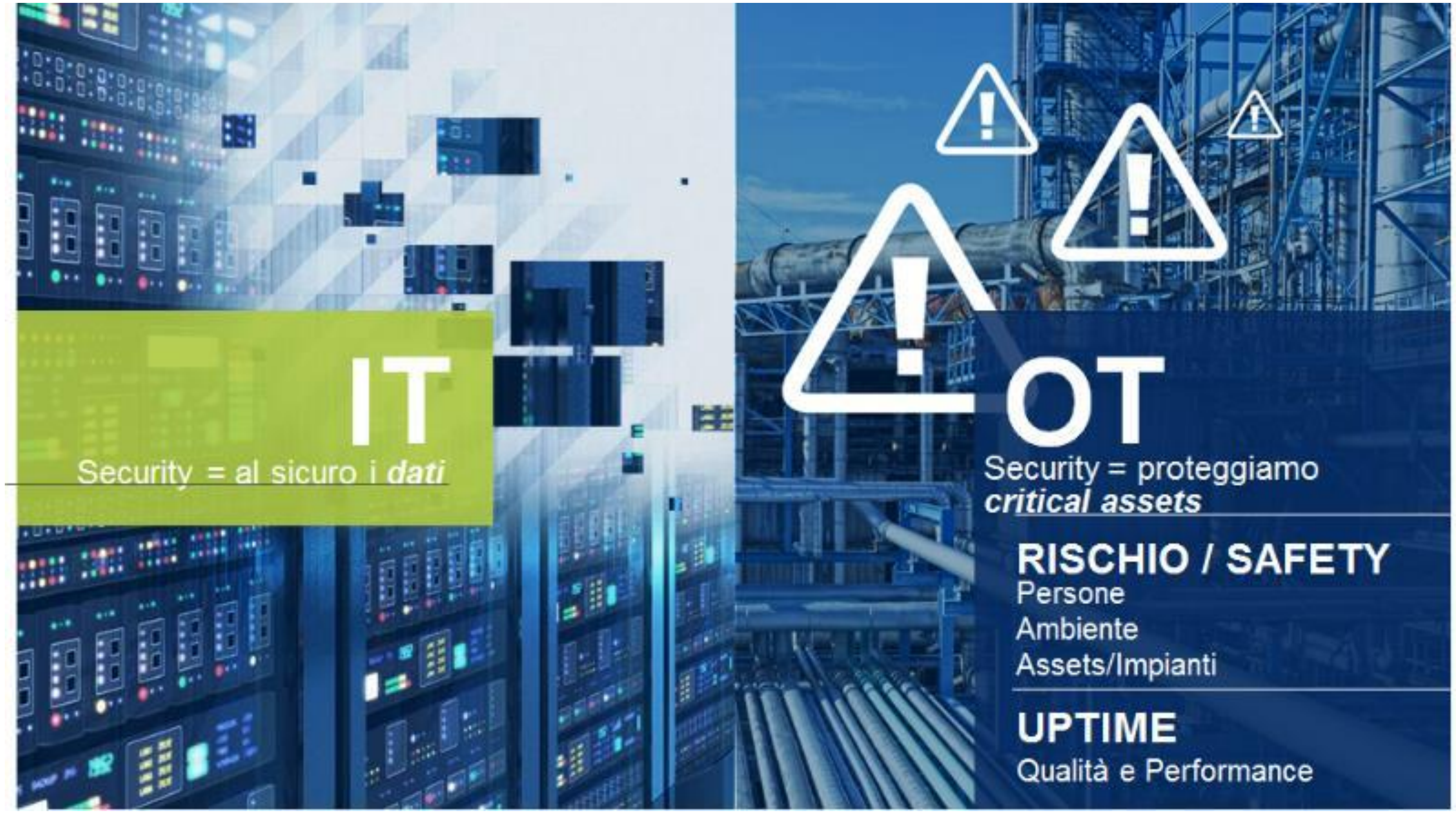
ServiTecno

NOZOMI NETWORKS

Authors / Speaker
Mario Testino

Differenze tra IT e OT

I **SISTEMI OT** controllano fisicamente linee, impianti, macchine *(anche)* all'interno di **INFRASTRUTTURE CRITICHE**



Security, Safety e Business continuity sono i parametri fondamentali.

Convergenza IT - OT

Quello che era isolato ora è connesso ed è facile da accedere

In the past, they were …

- Isolated from IT
- Run on proprietary control protocols
- Run on specialized hardware
- Run on proprietary embedded operating systems
- Connected by copper and twisted pair

Now they are …

- Bridged into corporate networks
- Riding on common internet protocols
- Running on general purpose hardware with IT origins
- Running mainstream IT operating systems
- Increasingly connected to wireless technologies

Minacce Cyber Security OT

La Cyber Security nell’era dell’industrial internet

Security Solutions

Standard IT Network Security Solutions Don’t Work – Protocol Barrier

The Perimeter

The Perimeter Is Breached: Software Updates, Technicians, Physical Presence

Connectivity

OT Networks Are More Connected Than Ever

Vendors’ Vulnerabilities

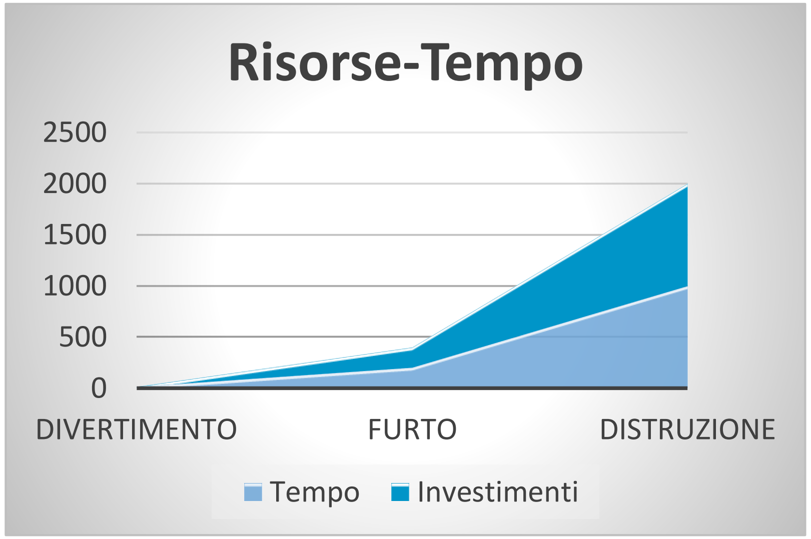
Vendors’ Vulnerabilities' Leave Your Network Exposed

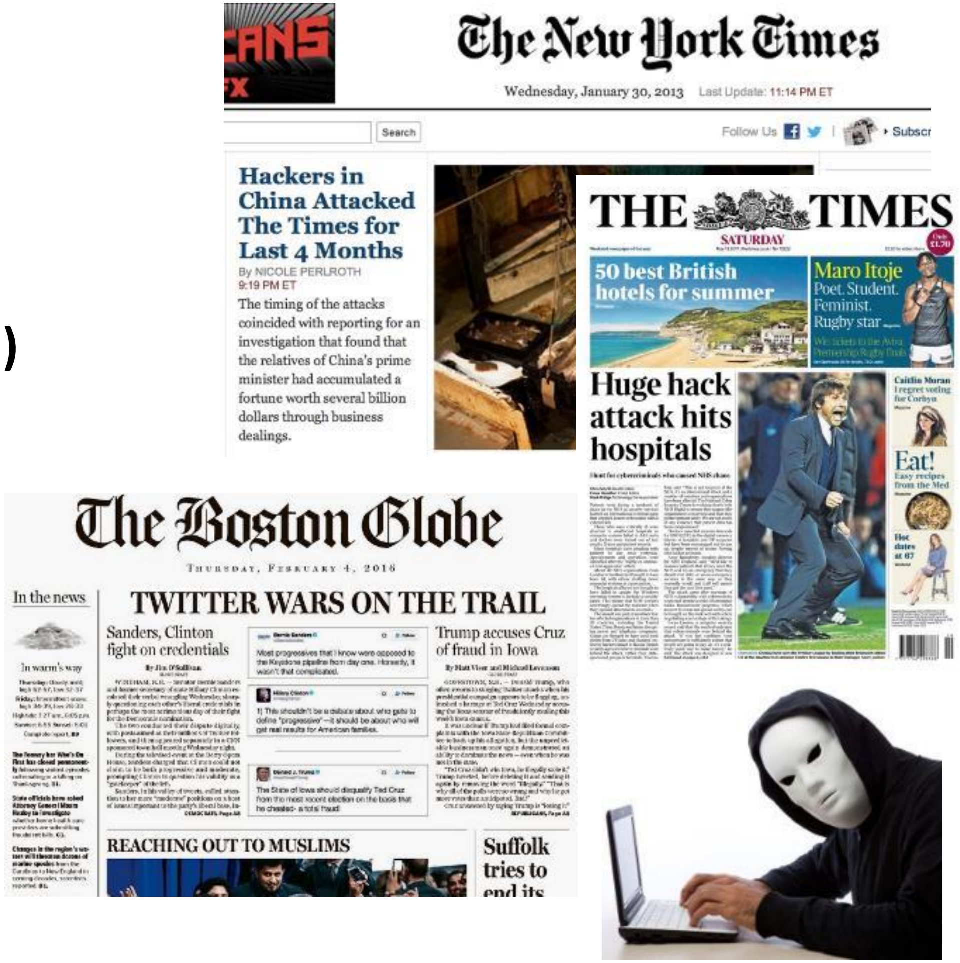
Le Ragioni dell’Hacking

~~Hacking for fun (Personal Gratification)~~

Hacking to steal (Information or Money)

Hacking to disrupt (Terrorism or Warfare)




The New York Times

Wednesday, January 30, 2013 Last Update: 11:14 PM ET

Search

Follow Us

Subscr

Hackers in China Attacked The Times for Last 4 Months

By NICOLE PERLROTH
9:19 PM ET

The timing of the attacks coincided with reporting for an investigation that found that the relatives of China's prime minister had accumulated a fortune worth several billion dollars through business dealings.

THE TIMES

SATURDAY

Only £1.70

50 best British hotels for summer

Maro Itoje
Poet. Student. Feminist. Rugby star

Huge hack attack hits hospitals

Caitlin Moran
I regret voting for Corbyn

Eat!
Easy recipes from the Med

Hot dates at 67

The Boston Globe

Thursday, February 4, 2016

In the news

In warm's way

TWITTER WARS ON THE TRAIL

Sanders, Clinton fight on credentials

Most progressives that I know were opposed to the Keystone pipeline from day one. Honestly, it wasn't that complicated.

1| This shouldn't be a debate about who gets to define "progressive"—it should be about who will get real results for American families.

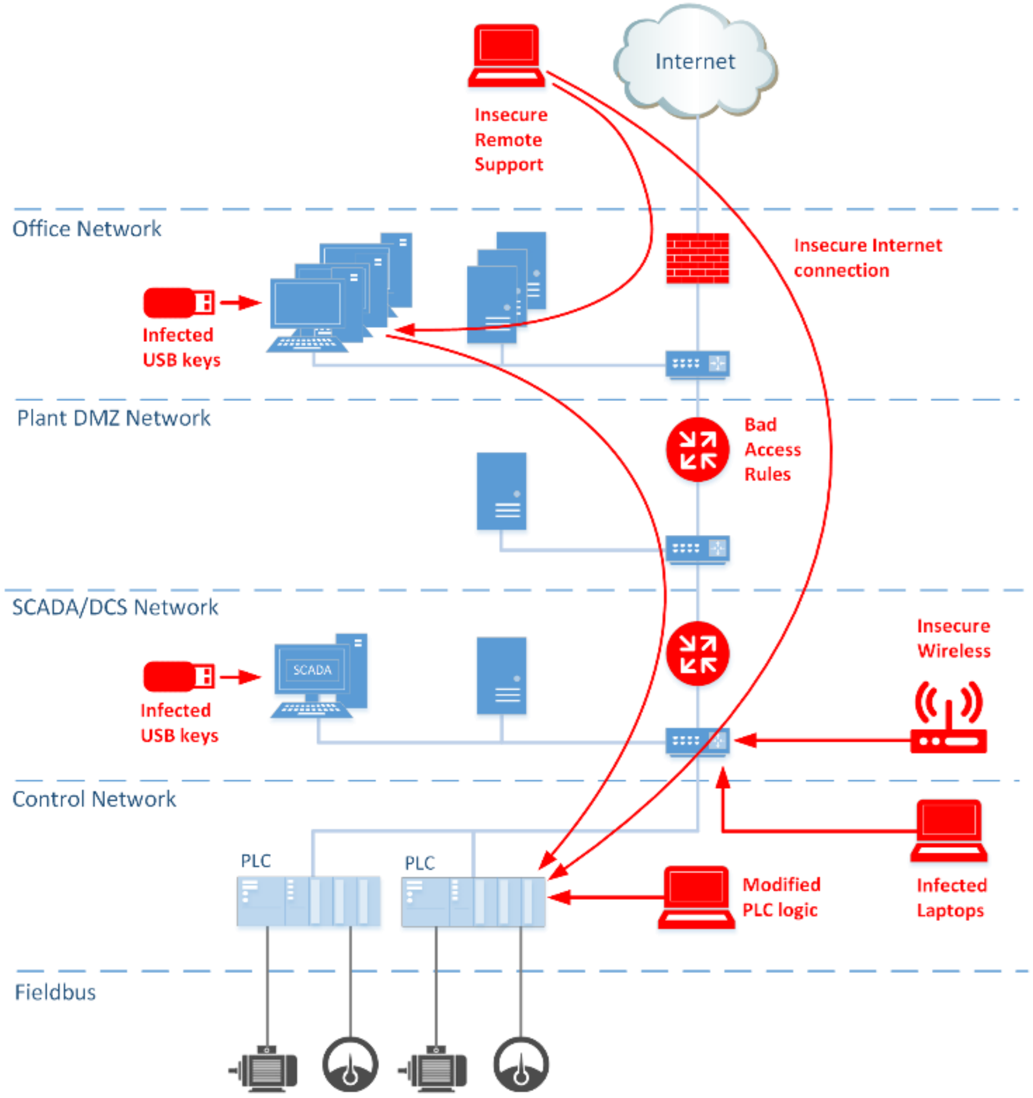
The State of Iowa should disqualify Ted Cruz from the most recent election on the basis that he cheated- a total fraud!

Trump accuses Cruz of fraud in Iowa

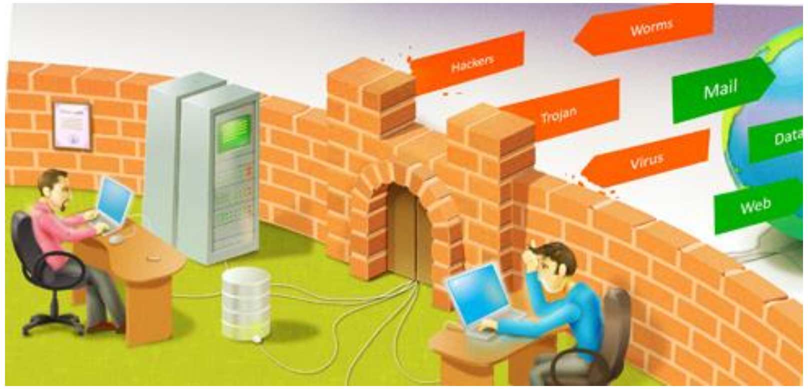
REACHING OUT TO MUSLIMS

Suffolk tries to end its

…e degli “Incidenti” informatici



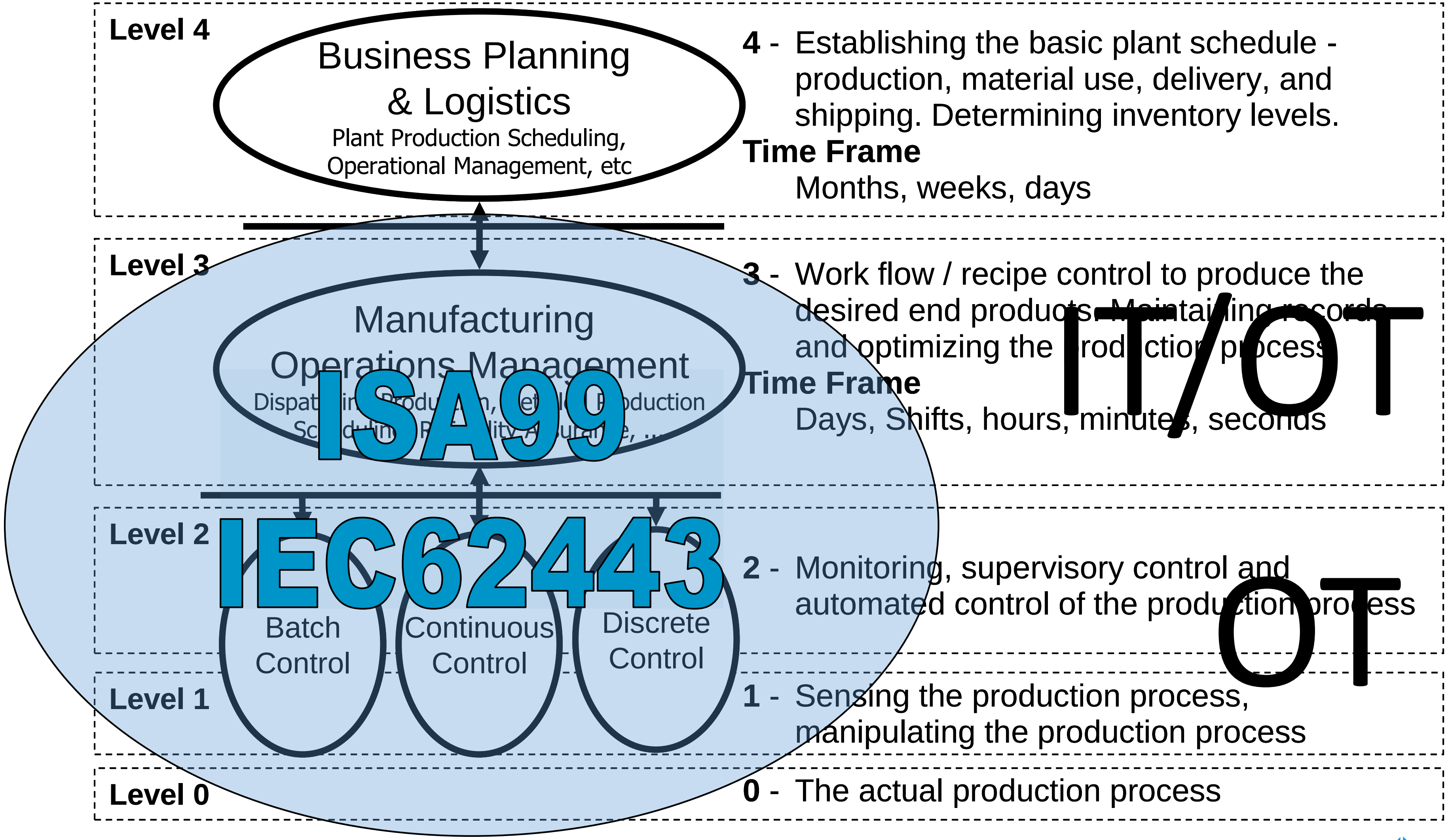
Non ho ancora ricevuto attacchi cyber quindi sono al sicuro…vero?



ServiTecno

NOZOMI NETWORKS

ANSI/ISA95 Functional Hierarchy



Level 4
Business Planning & Logistics
Plant Production Scheduling, Operational Management, etc
Level 3
Manufacturing Operations Management
Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...
ISA99
Level 2
IEC62443
Batch Control
Continuous Control
Discrete Control
Level 1
Level 0
IT/OT
OT

4 - Establishing the basic plant schedule - production, material use, delivery, and shipping. Determining inventory levels.

Time Frame

Months, weeks, days

3 - Work flow / recipe control to produce the desired end products. Maintaining records and optimizing the production process

Time Frame

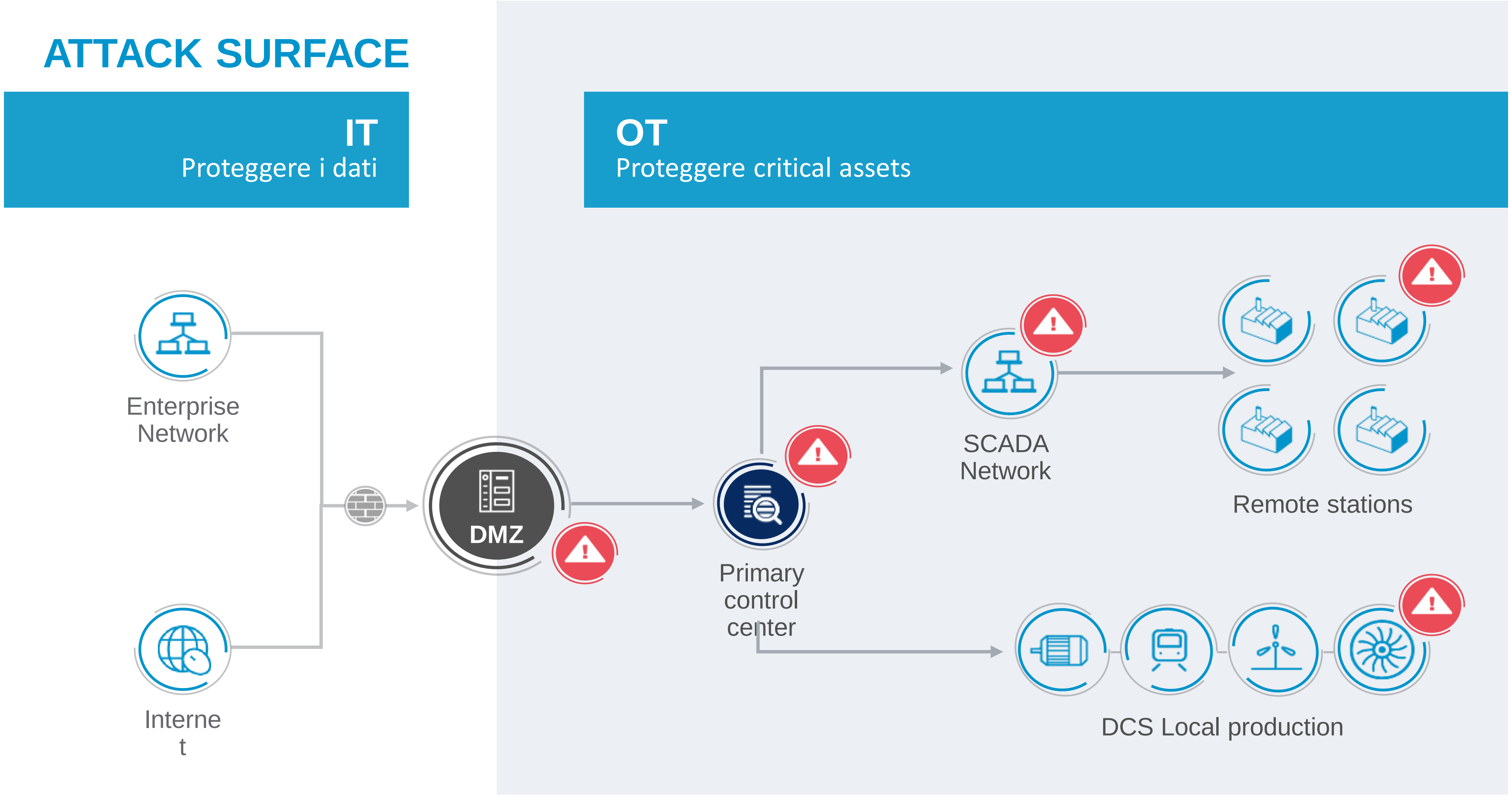
Days, Shifts, hours, minutes, seconds

2 - Monitoring, supervisory control and automated control of the production process

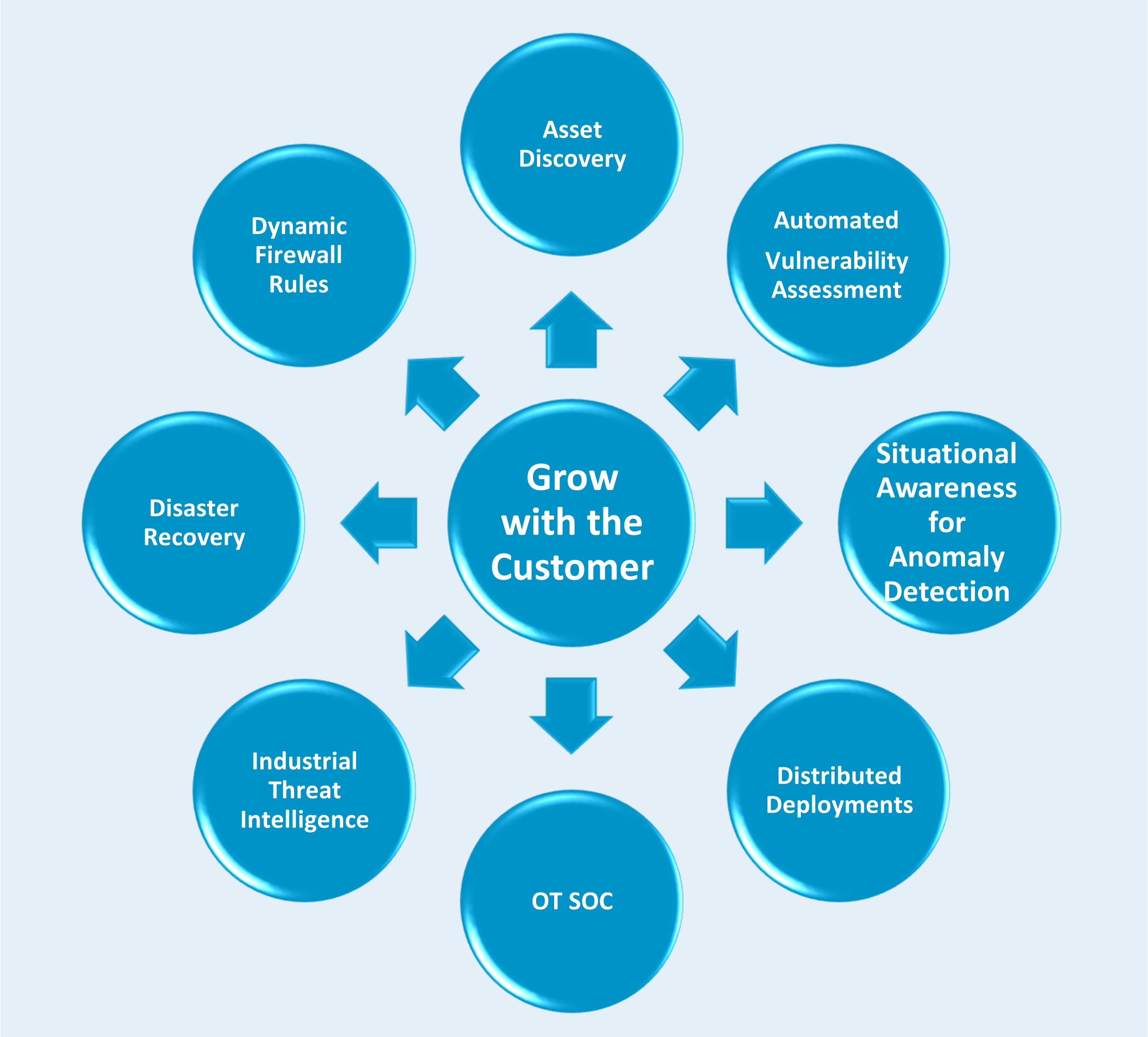
1 - Sensing the production process, manipulating the production process

0 - The actual production process

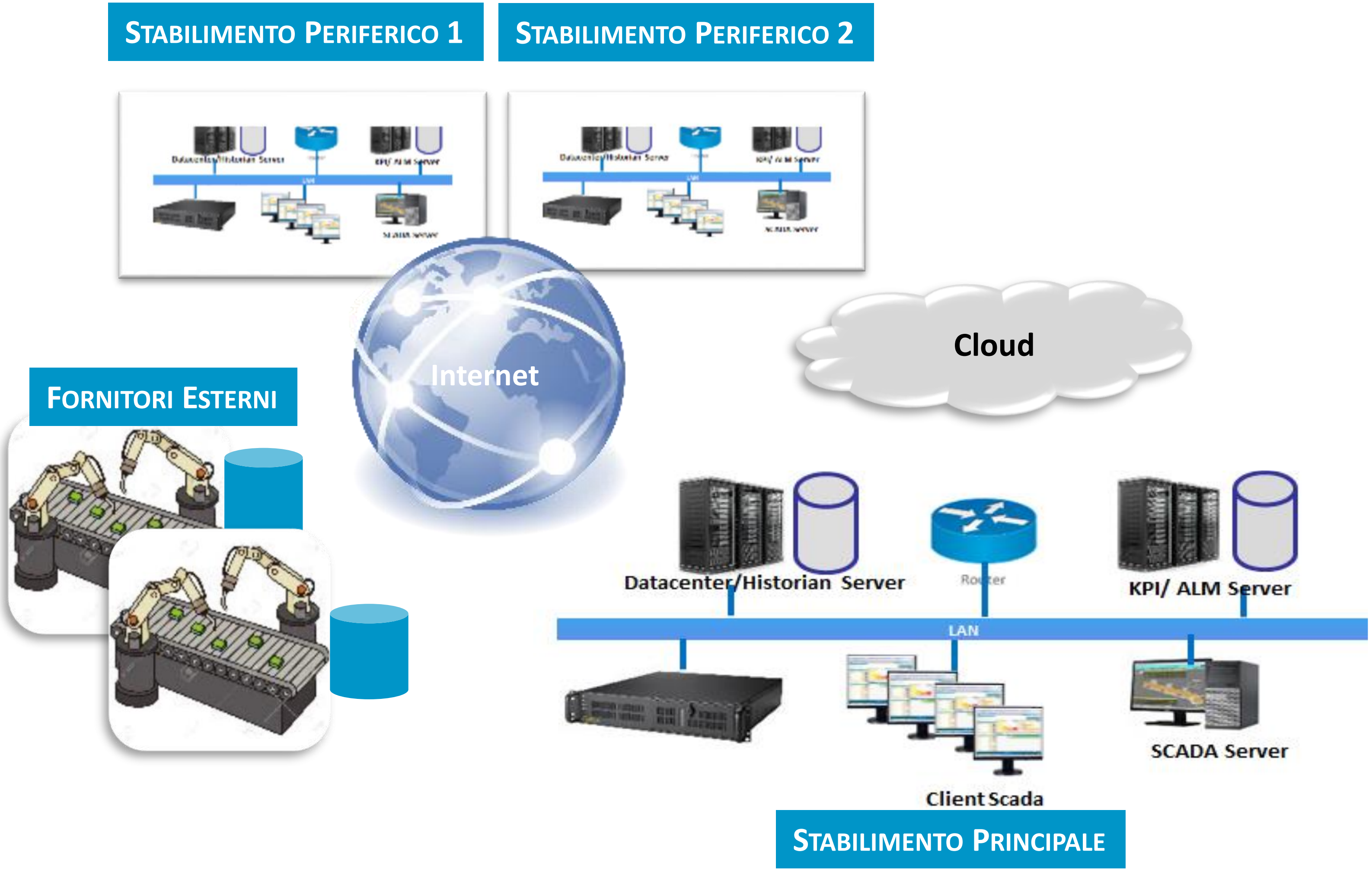
IT e OT: perimetro e superficie d’attacco



Difesa Modulare per l’OT


Grow with the Customer
Asset Discovery
Automated Vulnerability Assessment
Situational Awareness for Anomaly Detection
Distributed Deployments
OT SOC
Industrial Threat Intelligence
Disaster Recovery
Dynamic Firewall Rules

Un perimetro dinamico nella supply chain



STABILIMENTO PERIFERICO 1

STABILIMENTO PERIFERICO 2

FORNITORI ESTERNI

Internet

Cloud

Datacenter/Historian Server

Router

KPI/ ALM Server

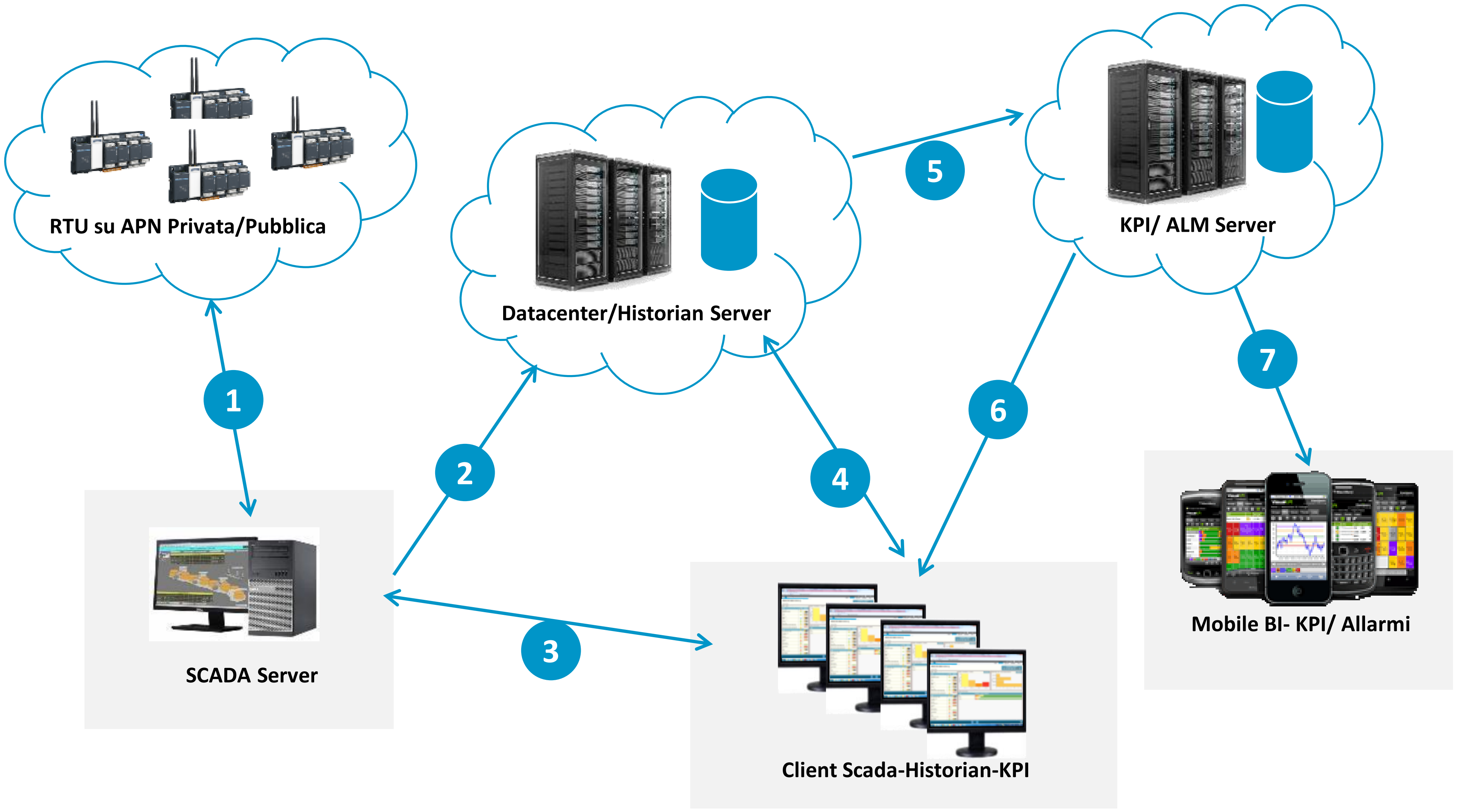
LAN

Client Scada

SCADA Server

STABILIMENTO PRINCIPALE

L’affermarsi di Architetture Cloud

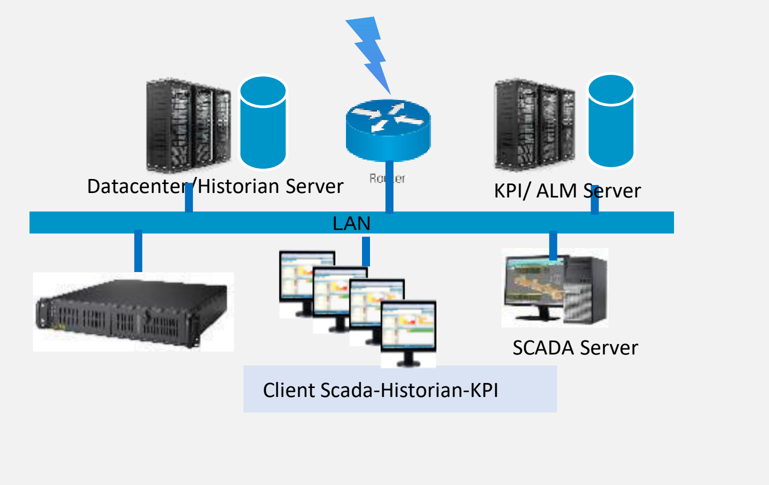

RTU su APN Privata/Pubblica
Datacenter/Historian Server
KPI/ ALM Server
1
2
3
4
5
6
7
SCADA Server
Client Scada-Historian-KPI
Mobile BI- KPI/ Allarmi

ServiTecno

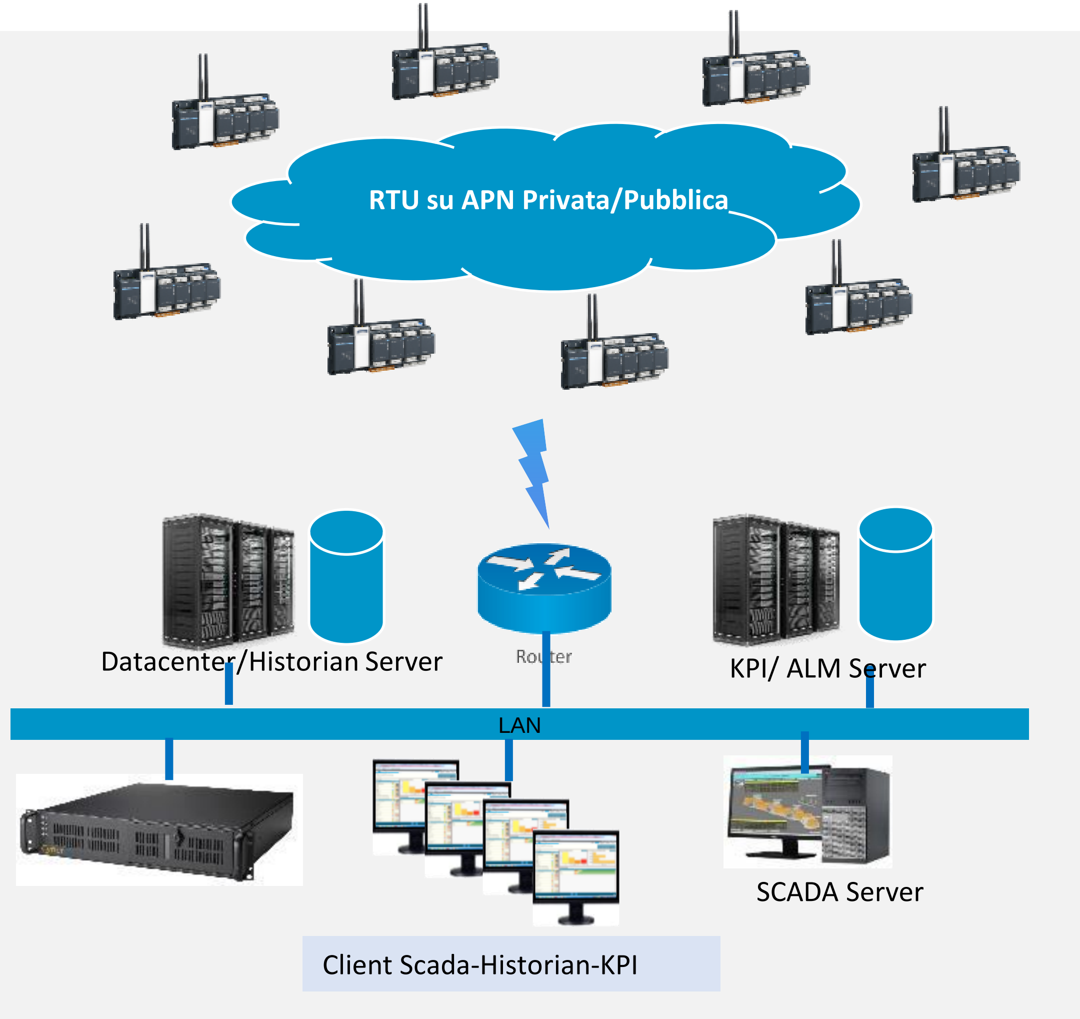
NOZOMI NETWORKS

APN Telefonici Pubblici

Impianti secondari completi

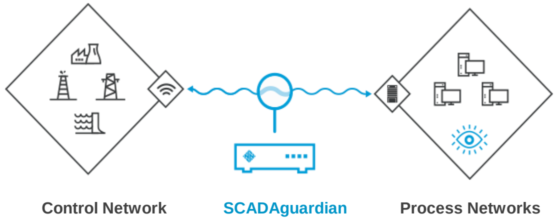


Sede principale e relative RTU


RTU su APN Privata/Pubblica
Datacenter/Historian Server
Router
KPI/ ALM Server
LAN
SCADA Server
Client Scada-Historian-KPI

Una Tecnologia Innovativa: Nozomi Networks SCADAGuardian

SCADAguardian implements an innovative technology for monitoring and assessing Industrial Control Systems.

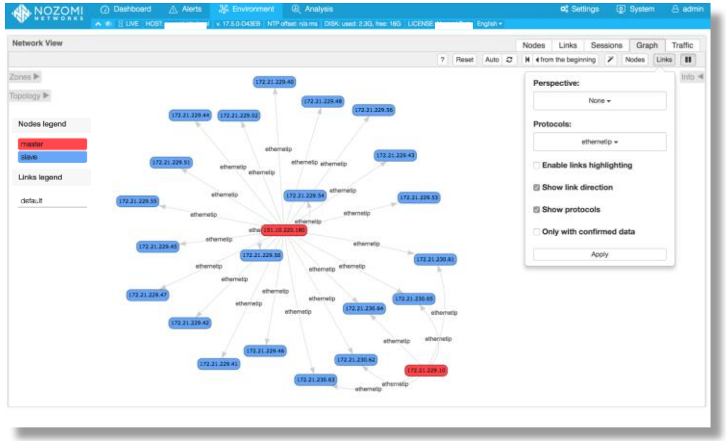


Is an appliance (physical or virtual) that passively connects to the industrial network non-intrusively

Listens to all traffic within the control and process networks, analyzing it at all levels of the OSI stack, passively (L1 to L7)

Uses Artificial Intelligence and Machine Learning techniques to create detailed behavior profiles for every device according to the process state to quickly detect critical state conditions

Provides best-in-class network visualization, asset management, ICS anomaly intrusion, vulnerability assessment, as well as dashboards and reporting



LIVE HOST: [redacted] v. 17.5.0-D43EB NTP offset: n/a ms DISK: used: 2.3G, free: 16G LICENSE: [redacted] English

Perspective: None

Protocols: ethernetip

□ Enable links highlighting

☑ Show link direction

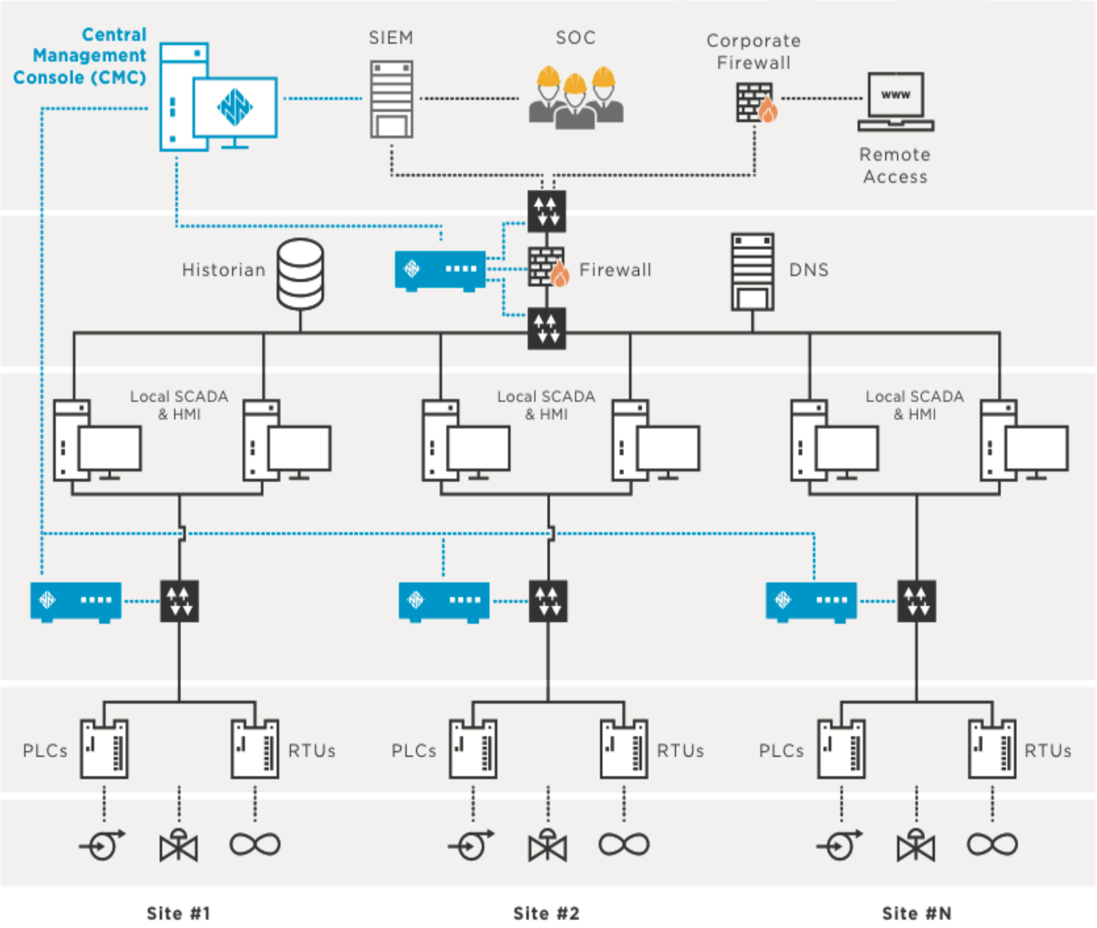
☑ Show protocols

□ Only with confirmed data

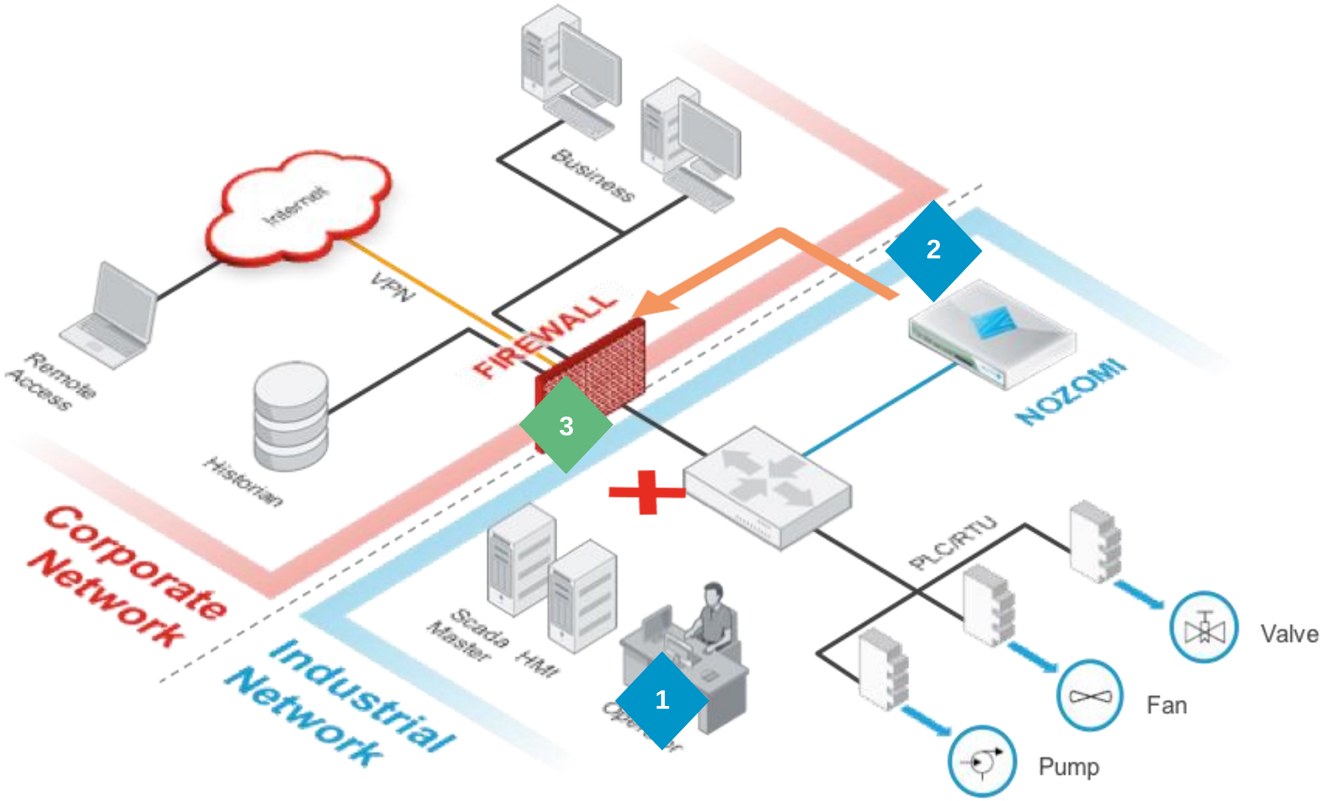
Apply

Sample Deployment Architecture

	Detected threats
Level 4 Production Scheduling	• Monitoring of remote access connection to networks • Connection to Internet\corporate network DMZ • MITM & Scanning Attacks (Port, Network) • Unauthorized cross level communication • IP conflicts
Level 3 Production Control	• Weak passwords (FTP / TFPTP / RDP / DCERPC) • Traffic activity summaries Bad configurations (NTP / DNS / DHCP/ etc.) • Network topologies • Used ports of assets • Unencrypted communications (Telnet) • Insecure Internet connections
Level 2 Plant Supervisory	• Anomalous protocol behavior • Online edits to PLC projects • Communication changes • Configuration downloads • New assets in the network • Non-responsive assets • Corrupted OT packets • Firmware downloads • Logic changes
Level 1 Direct Control	• Authentication to PLCs • PLC actions (Start, Stop, Monitor, Run, Reboot, Program, Test)
Level 0 Field Level	• Fieldbus I/O monitoring



Integrazione



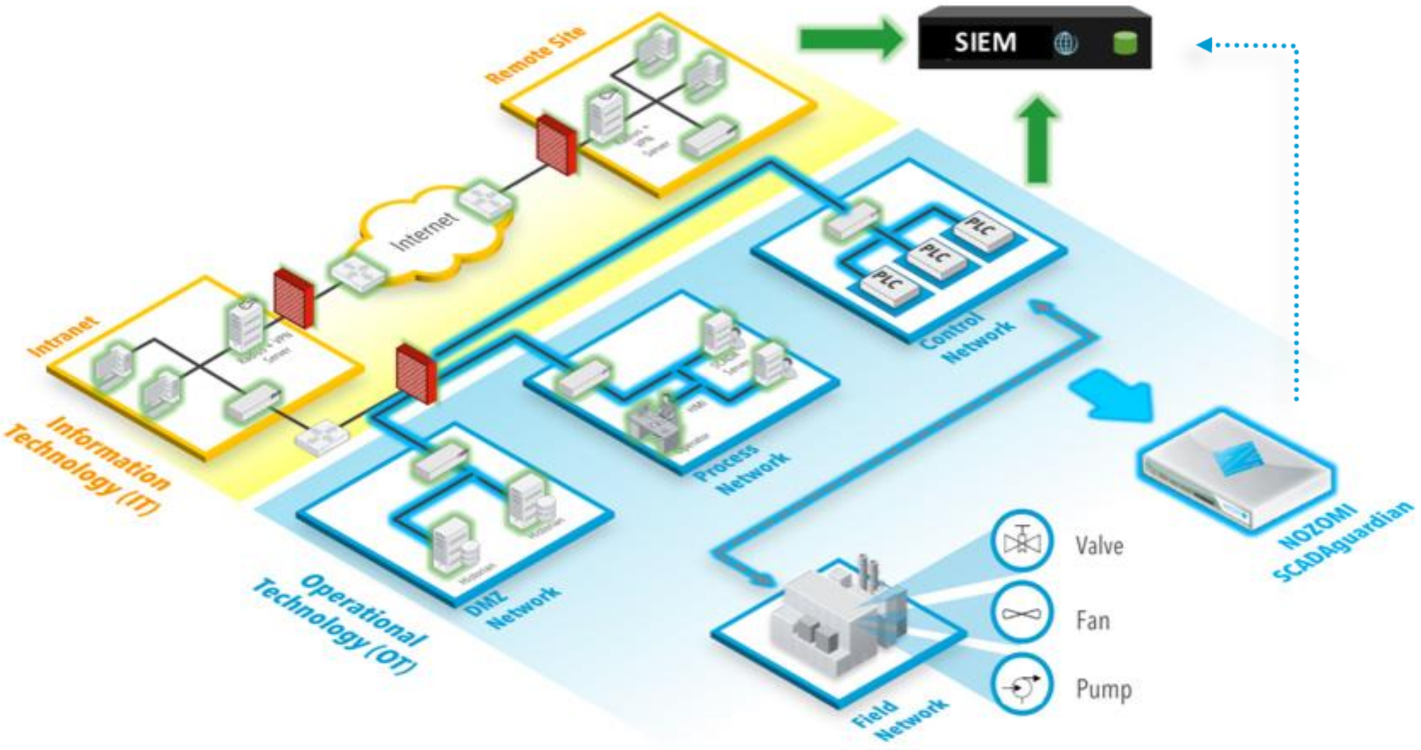
1 **Monitor**
A threat is detected by SCADAguardian and an alert is generated.

2 **Detect**
User-defined policies are rapidly examined and the appropriate corresponding action is triggered.

3 **Protect**
Firewall responds according to the user-configured action (Node Blocking, Link Blocking, or Kill Session) and mitigates the issue.

Integrazione

Security and Monitoring for ICS environments – SIEM integration



1 A SIEM collects standard logs end security events from different systems. This requires the deployment of parser and correlation rules to give the data meaning.

2 SCADAguardian deeply understands ICS protocols, variables and function codes. It generates security events that are relevant and specific to the OT environment.

3 SCADAguardian can send native logs to SIEMs, extending its scope and enriching the data collected.

ServiTecno

NOZOMI NETWORKS

Clienti e Uses Cases

Multi National Power Company (Fortune 500)

Security monitoring of operational network plus distributed deployment in all Regional Control Centers and TSO Interconnection Centers.

Super Major Oil & Gas Company (Fortune 500)

ICS security assessment to analyze the security levels of process networks at onshore and offshore sites in several countries.

Large Refinery Company

ICS security assessment and real-time monitoring of the main company plant in a distributed multi-vendor environment.

Metropolitan City Water Treatment Company

Security monitoring of the network communications and process variables of the water distribution system.

Multi-Utility Gas & Water Distribution

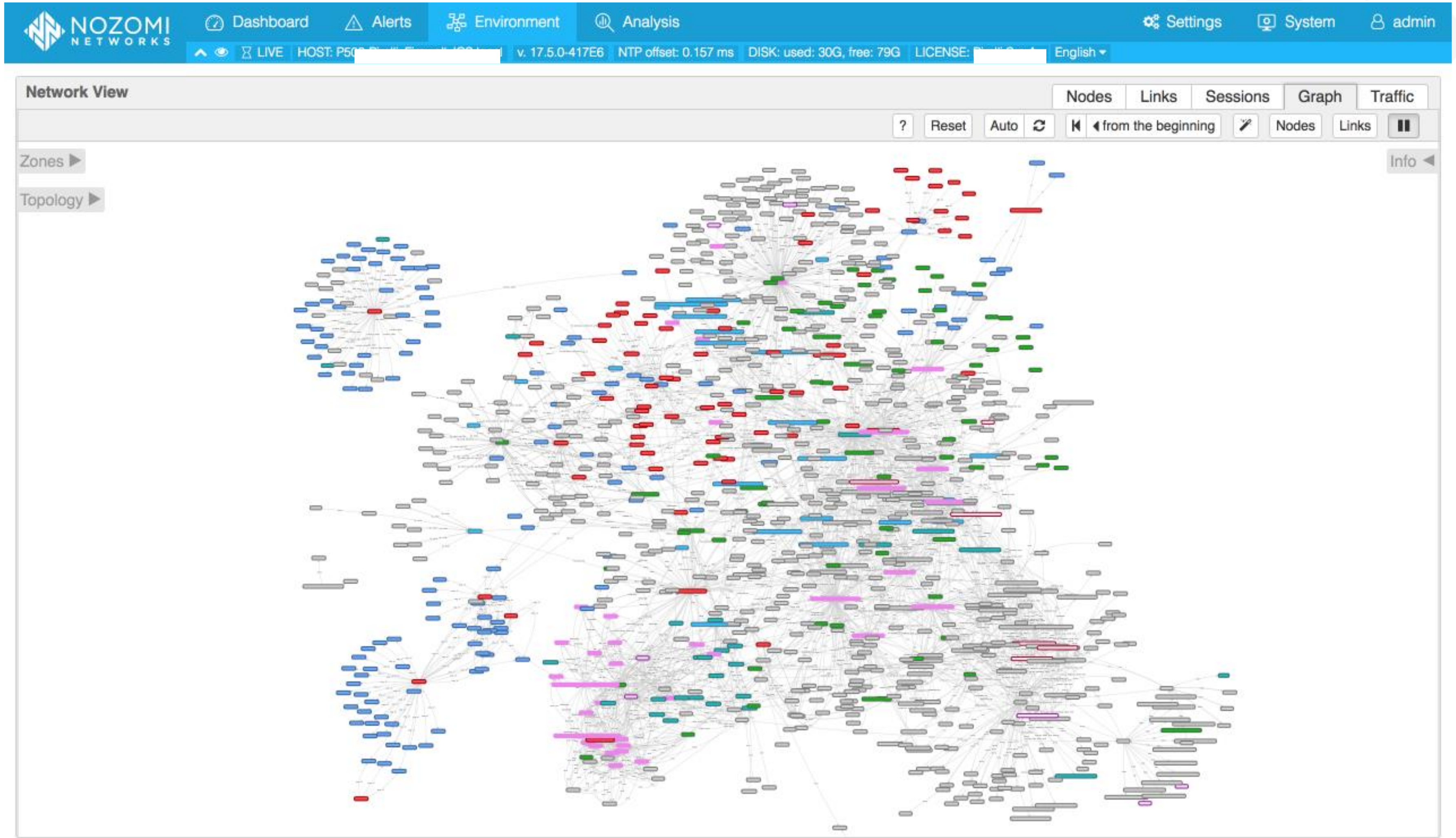
ICS and IT monitoring of a hydro plant production environment.

Pharmaceutical Company

ICS monitoring of the pharma production network communications and process variables.

Use Case 1: Network Visualization and Monitoring

From a ”tangled” situation (situazione caotica) …



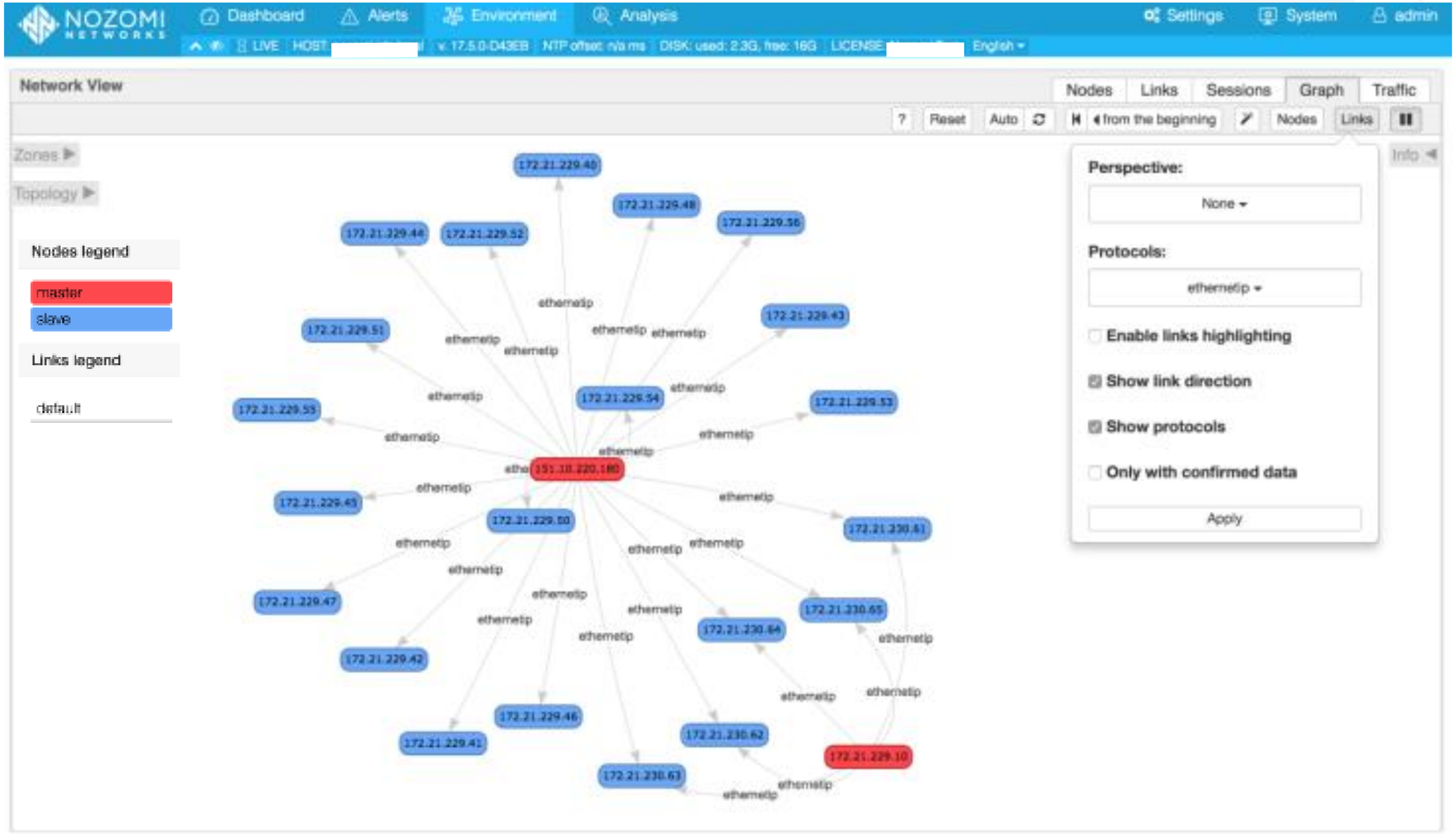
LIVE HOST: P50[redacted] v. 17.5.0-417E6 NTP offset: 0.157 ms DISK: used: 30G, free: 79G LICENSE: [redacted] English

ServiTecno

NOZOMI NETWORKS

Use Case 1: Network Visualization and Monitoring

...with two clicks the operator can filter the communications of interest …



Perspective:

None

Protocols:

ethernetip

□ Enable links highlighting

☑ Show link direction

☑ Show protocols

□ Only with confirmed data

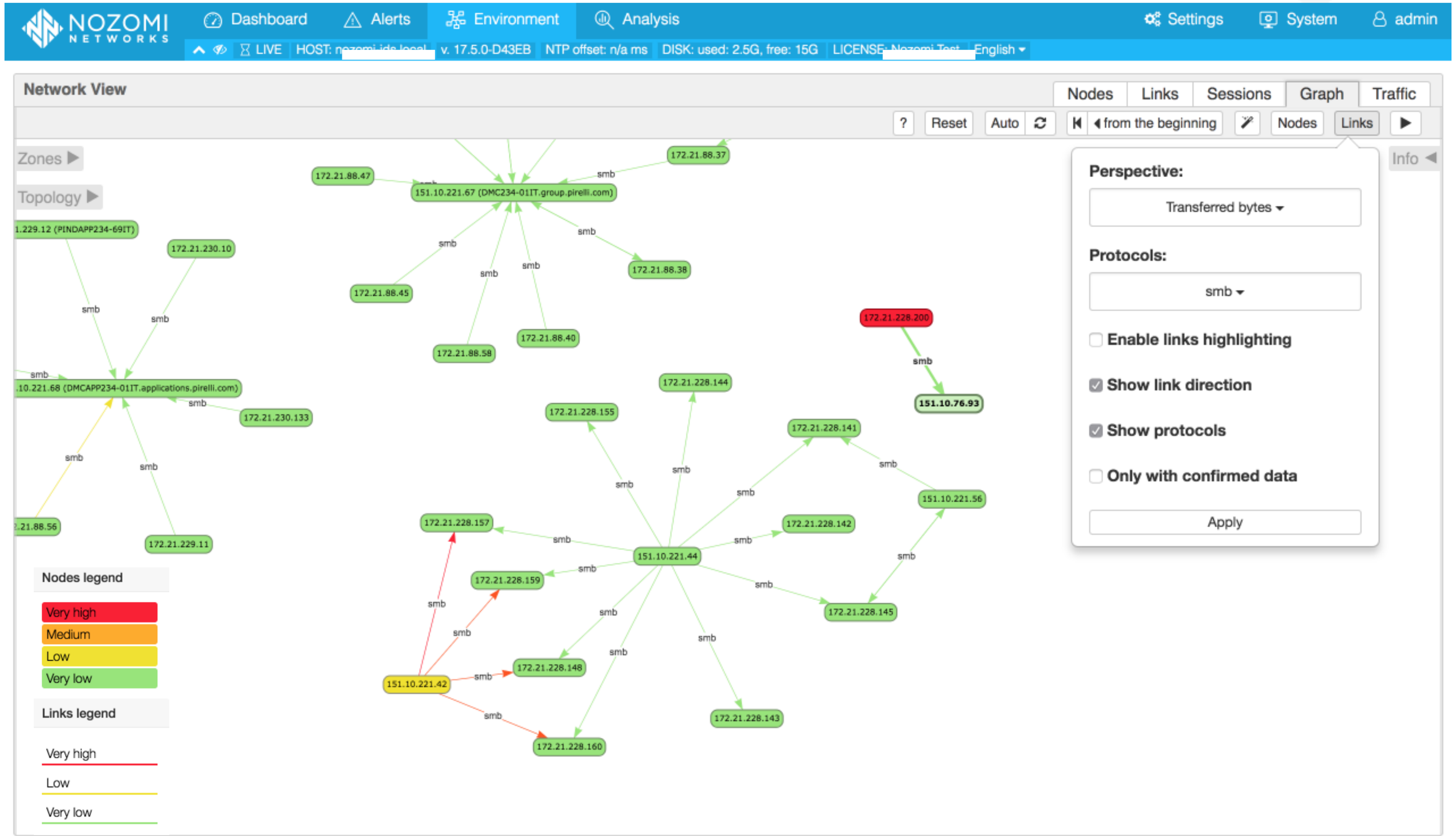
Apply

ServiTecno

NOZOMI NETWORKS

Use Case 2: ICS Anomaly Intrusion and Risk Detection

A lot of traditional IT communications, common vectors for malwares and attacks, are commonly present also in the OT environment (i.e. smb)



LIVE HOST: [redacted] v. 17.5.0-D43EB NTP offset: n/a ms DISK: used: 2.5G, free: 15G LICENSE: [redacted] English

Perspective: Transferred bytes

Protocols: smb

☐ Enable links highlighting

☑ Show link direction

☑ Show protocols

☐ Only with confirmed data

Apply

Nodes legend

🟥	Very high
🟧	Medium
🟨	Low
🟩	Very low

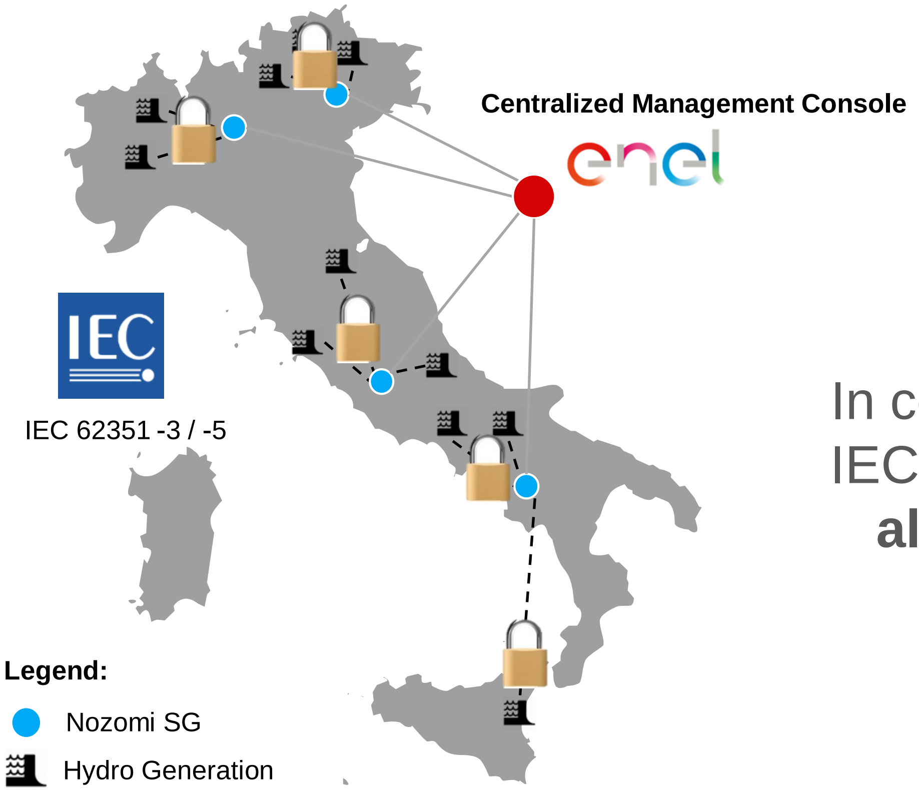
Links legend

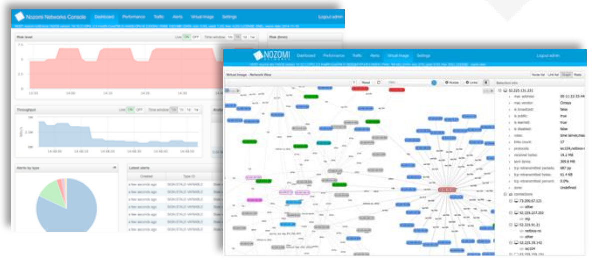
- Very high
- Low
- Very low

ServiTecno

NOZOMI NETWORKS

Case Study: ENEL – Hydropower Generation Plants





In cooperation with ENEL and following IEC/TR 62351-90-2 **we are working to allow SCADAguardian** to securely inspect encrypted traffic too.