

Secure Manufacturing/Utility in the Cloud

(ovvero, come proteggere OT e Industrial IoT in Cloud da incidenti Cyber per la Continuità Operativa in Fabbrica e Utility/Erogazione di Servizi Essenziali)

ServiTecno - GE Digital Alliance Partner

www.servitecno.it

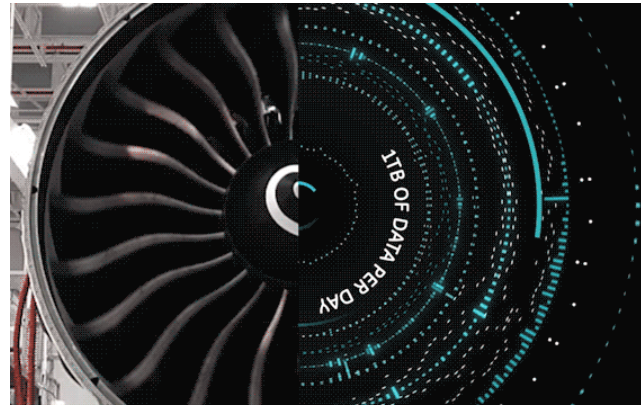
Proteggere dal rischio informatico i sistemi che gestiscono impianti, macchinari ed oggetti (IoT, IIoT) nell' Industria, Utility e nelle Infrastrutture.

OT: Operation Technology
ICS: Industrial Control Systems



Dove sono i sistemi da proteggere per proteggere gli impianti?

**Ovunque:
Industrial, Processes,
Buildings,
Manufacturing &
Infrastructures**



La gerarchia dei sistemi in Fabbrica e Utility

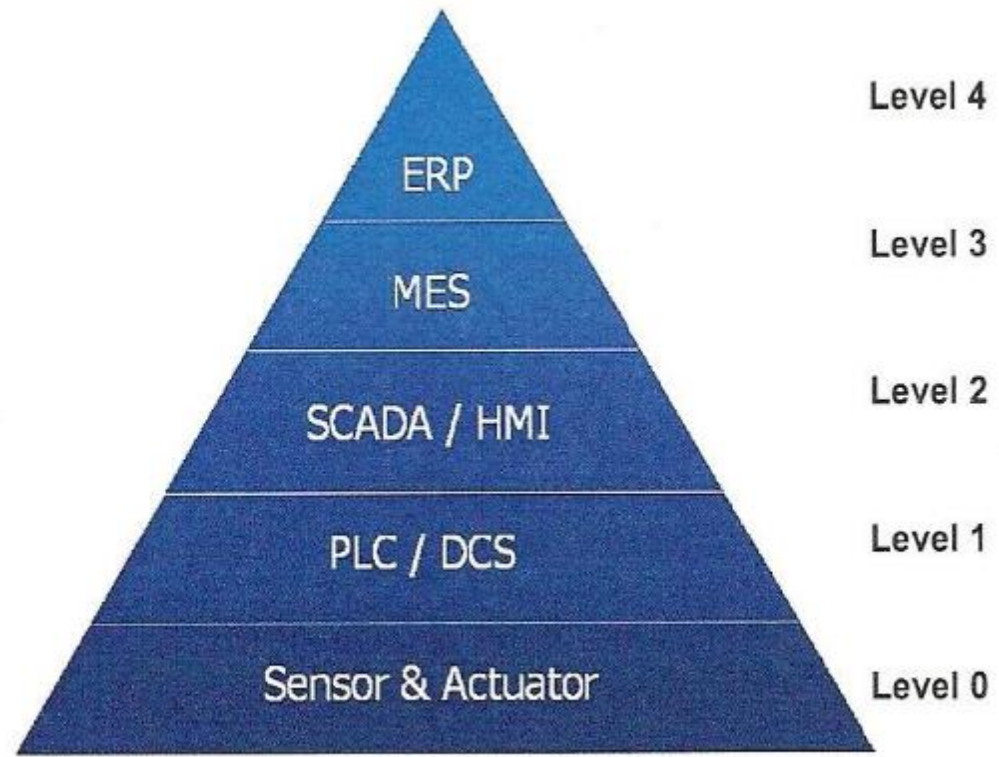
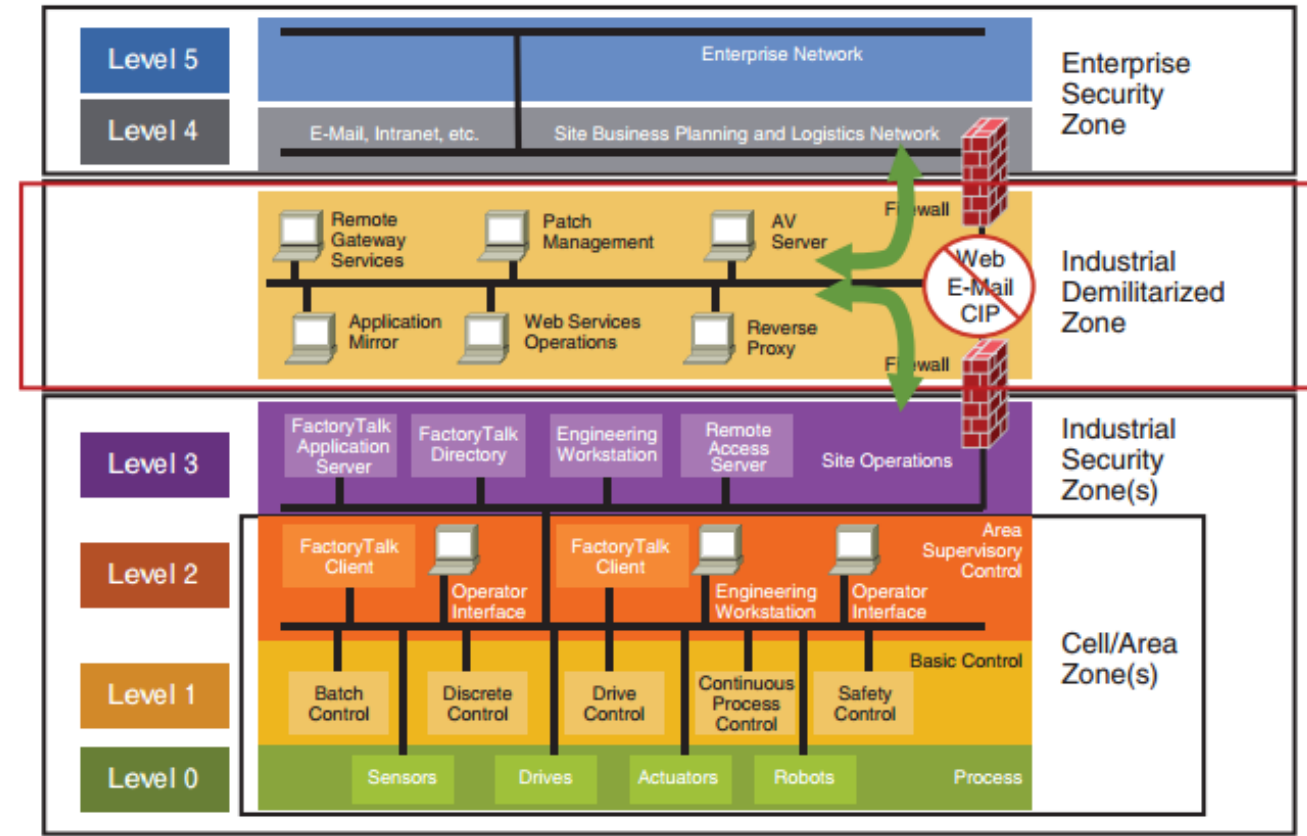
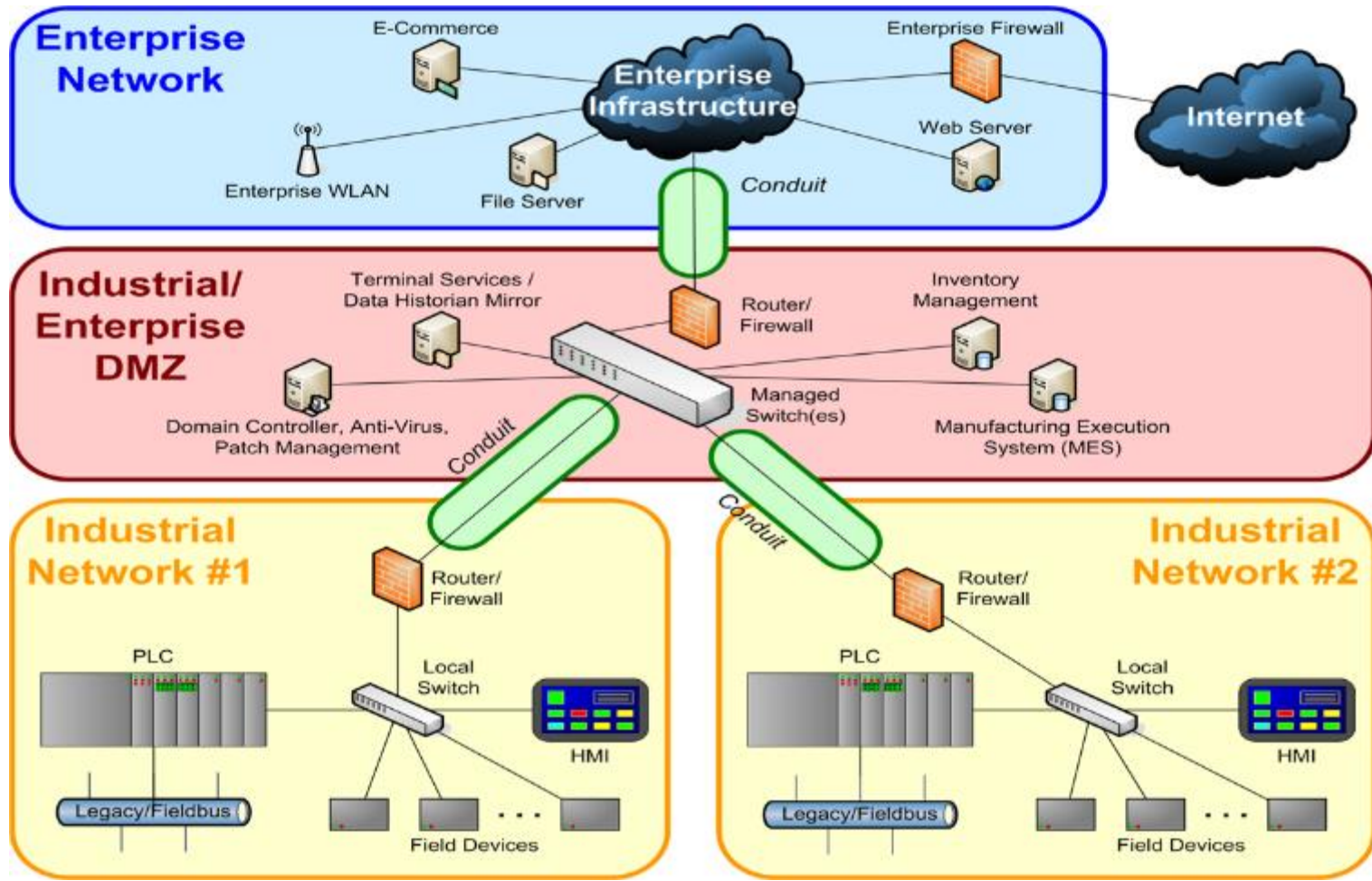


Figure 1 ISA95-1 model for production modelling.



Purdue Enterprise Reference Architecture (PERA)

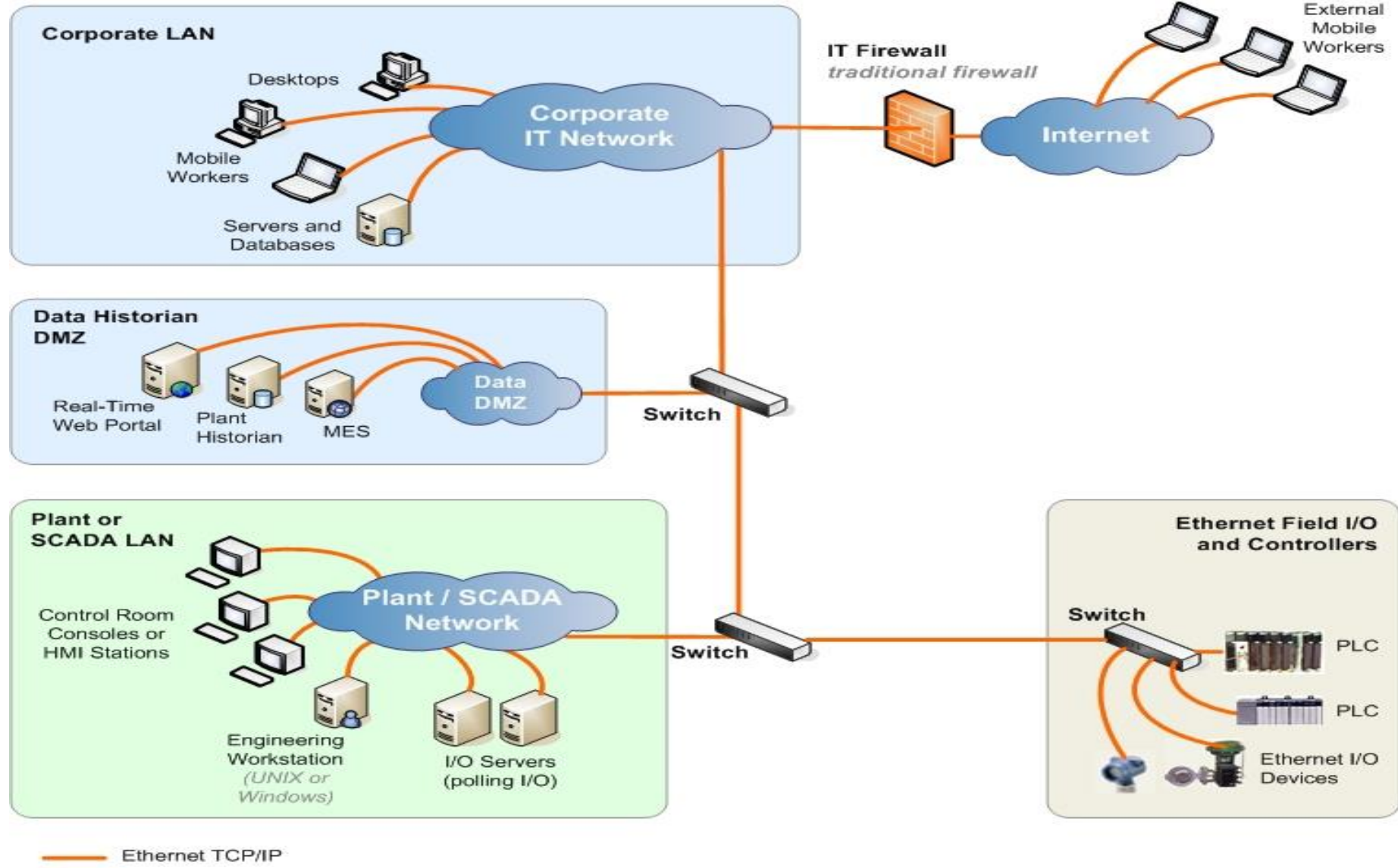
ISA99/IEC62443 Network/System Segmentation



**SEGMENTAZIONE E
SEGREGAZIONE
IN ZONE**

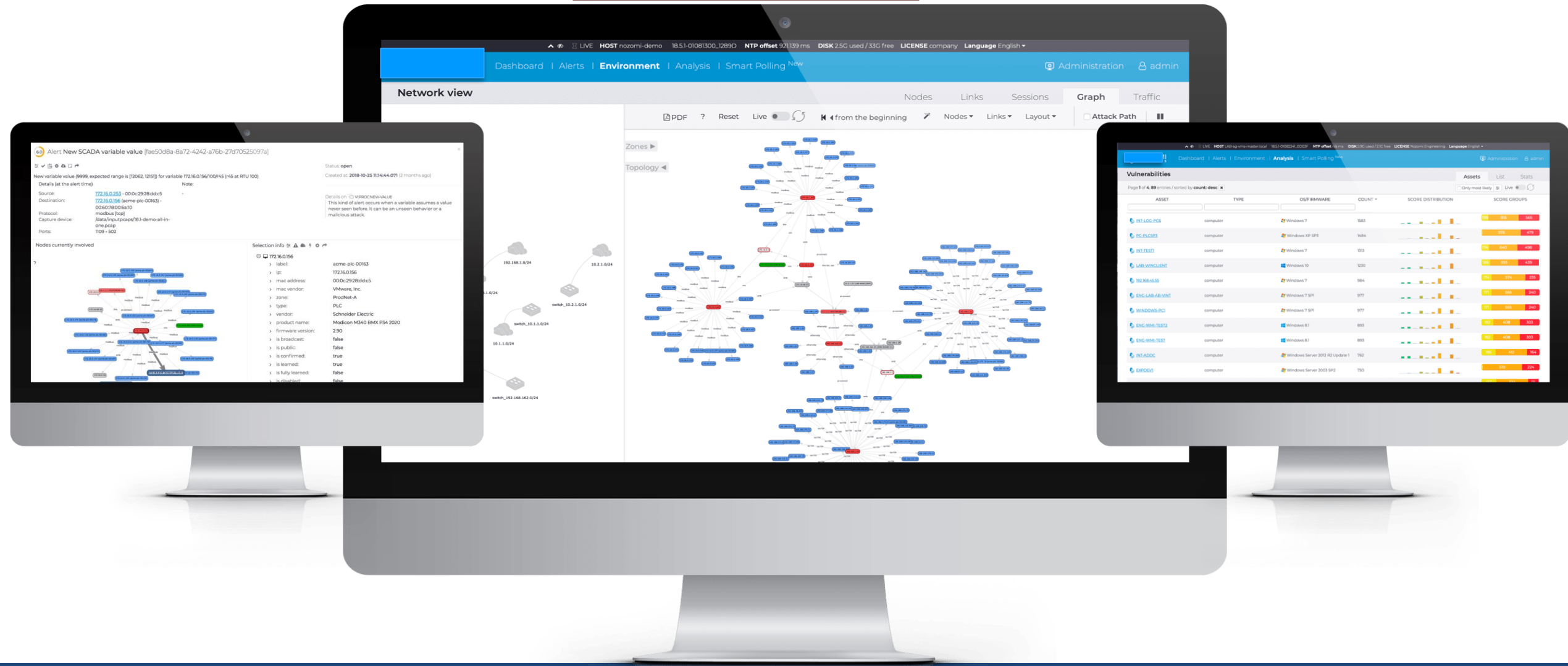
+

CONDUIT



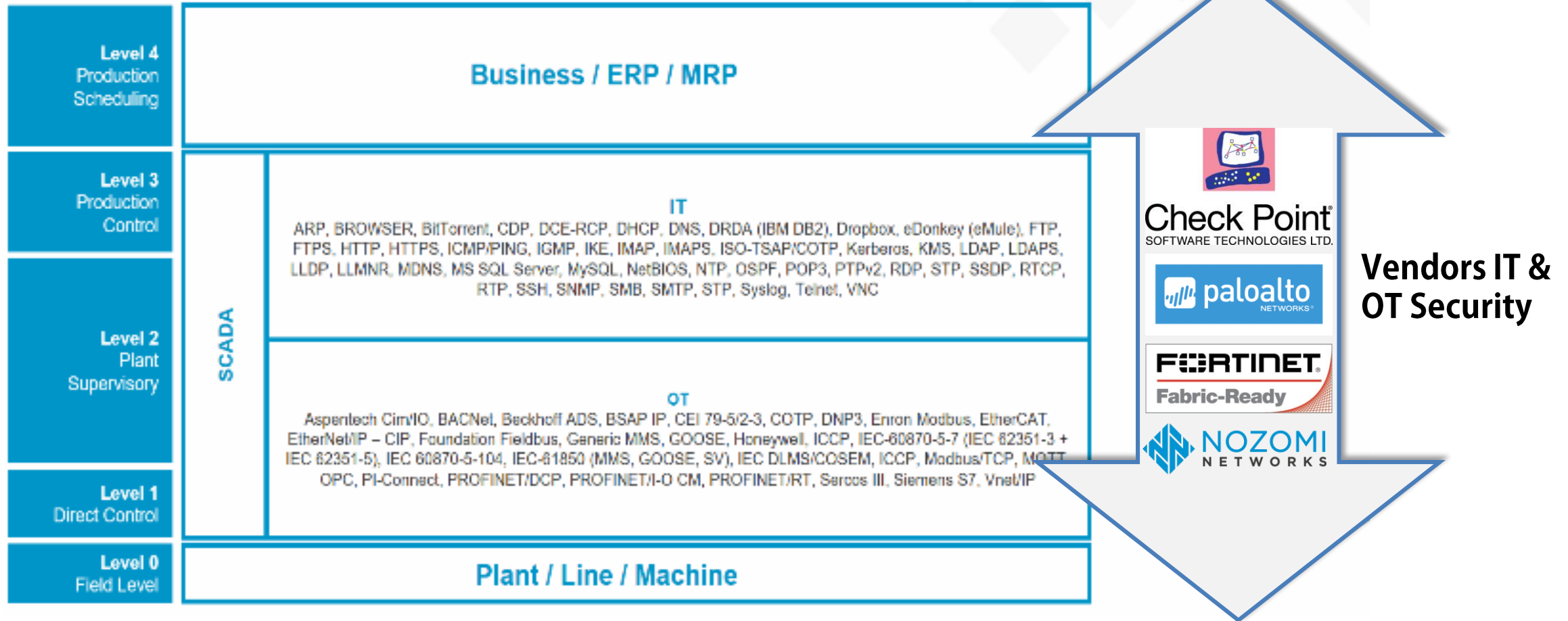
Reti di Impianto & IT

(nella realtà)



Le frontiere dell'OT e le diverse tecnologie

Tecnologie, Architetture, Dispositivi, Protocolli IT & OT



Da Industria3.0 a Industria4.0

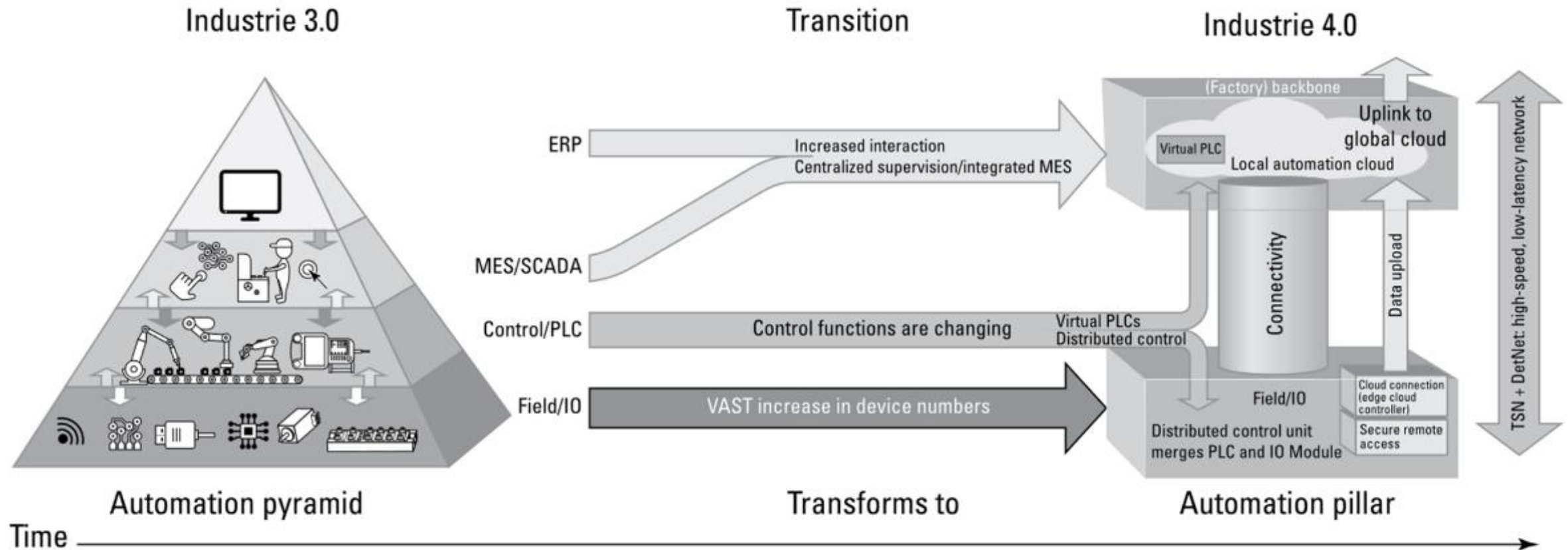
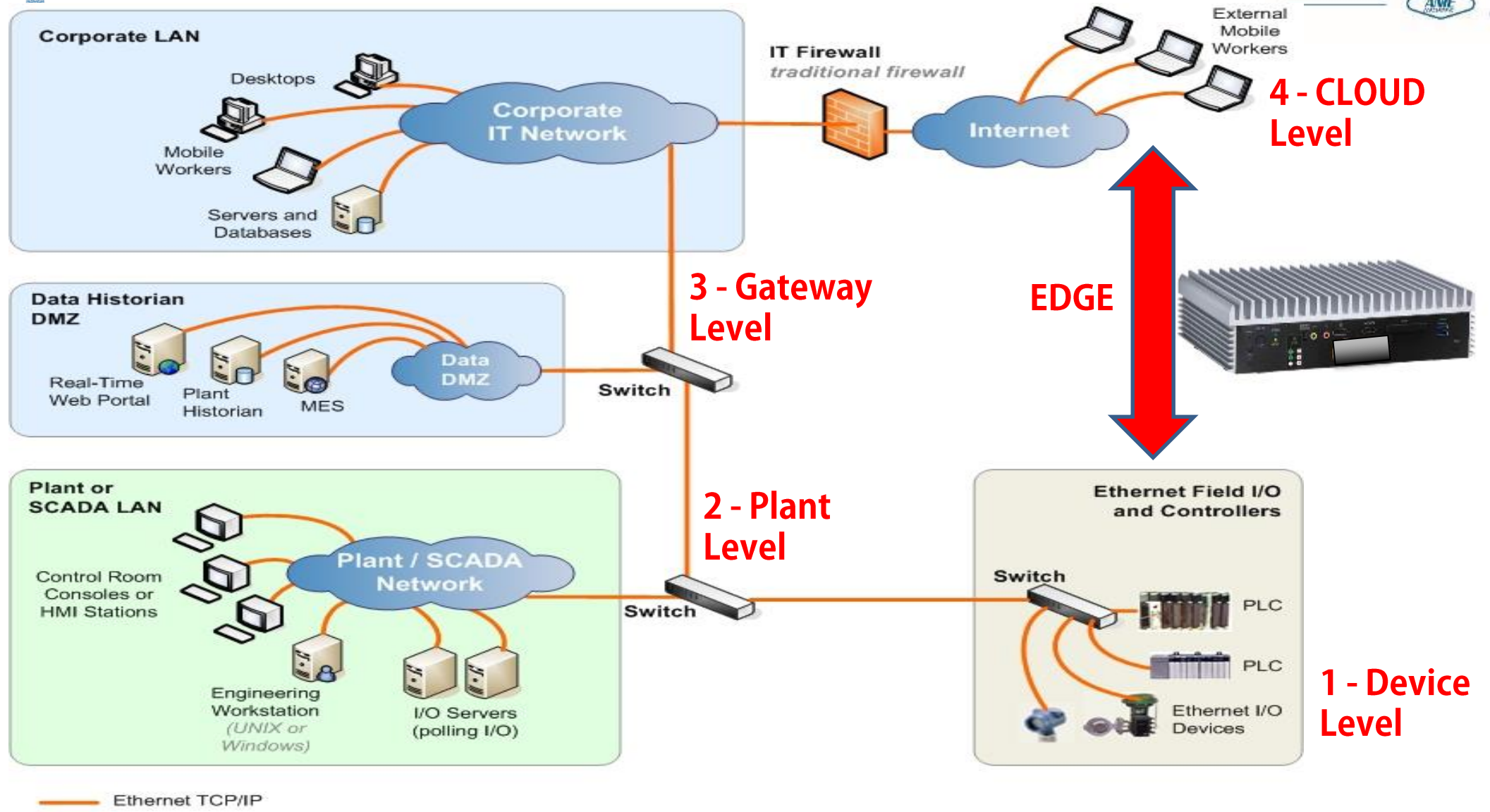


FIGURE 1-1: Moving from the automation pyramid to the automation pillar.

(fonte Belden/Hirschmann)

Reti di Impianto & IT con CLOUD

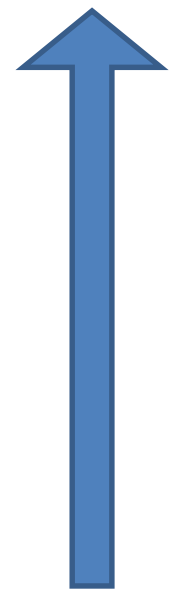


Dualismo IoT vs. IIoT industriale/automazione

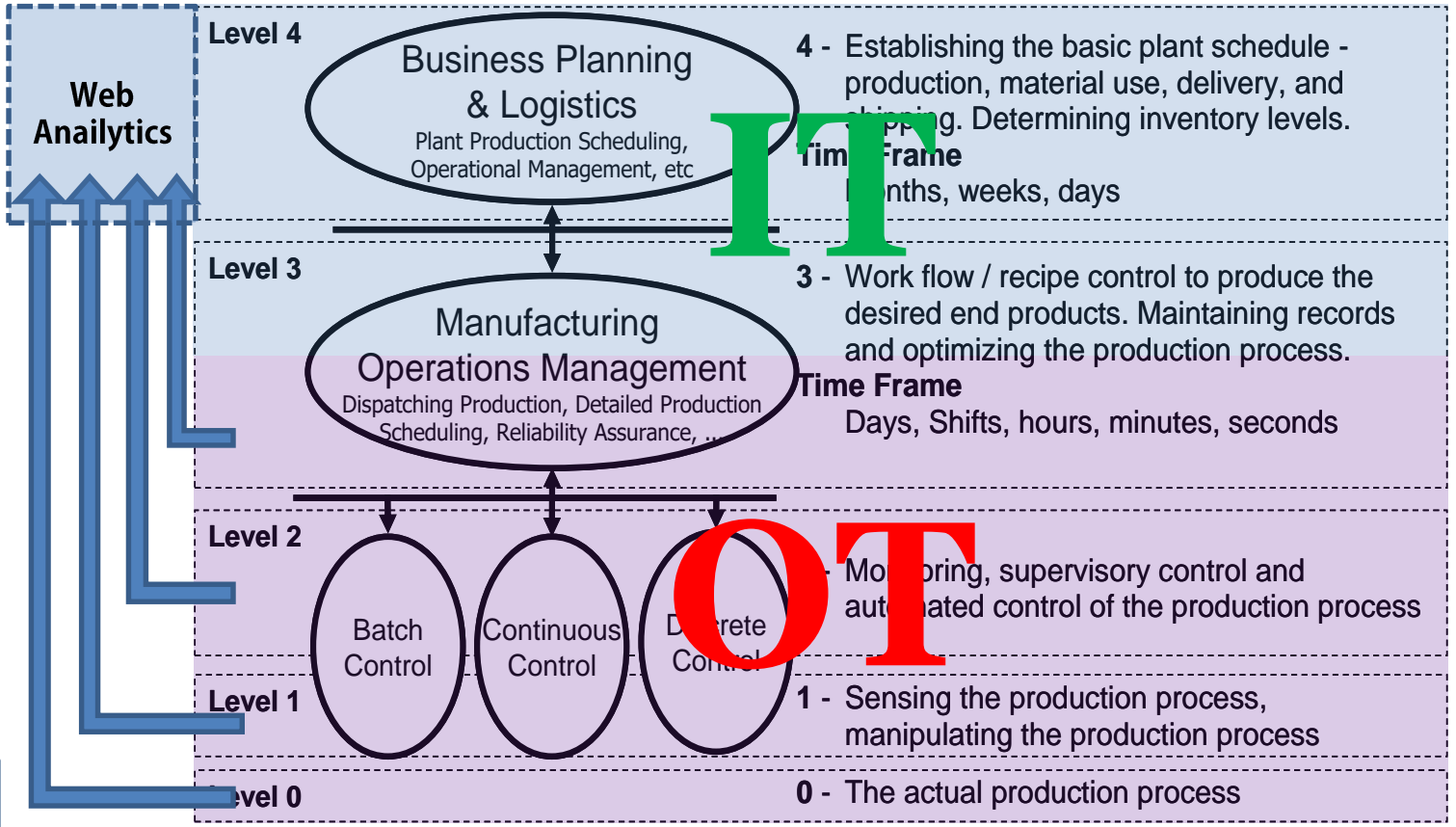
IOT/IIoT Shortcut
 Dati duplicati, non supervisionati

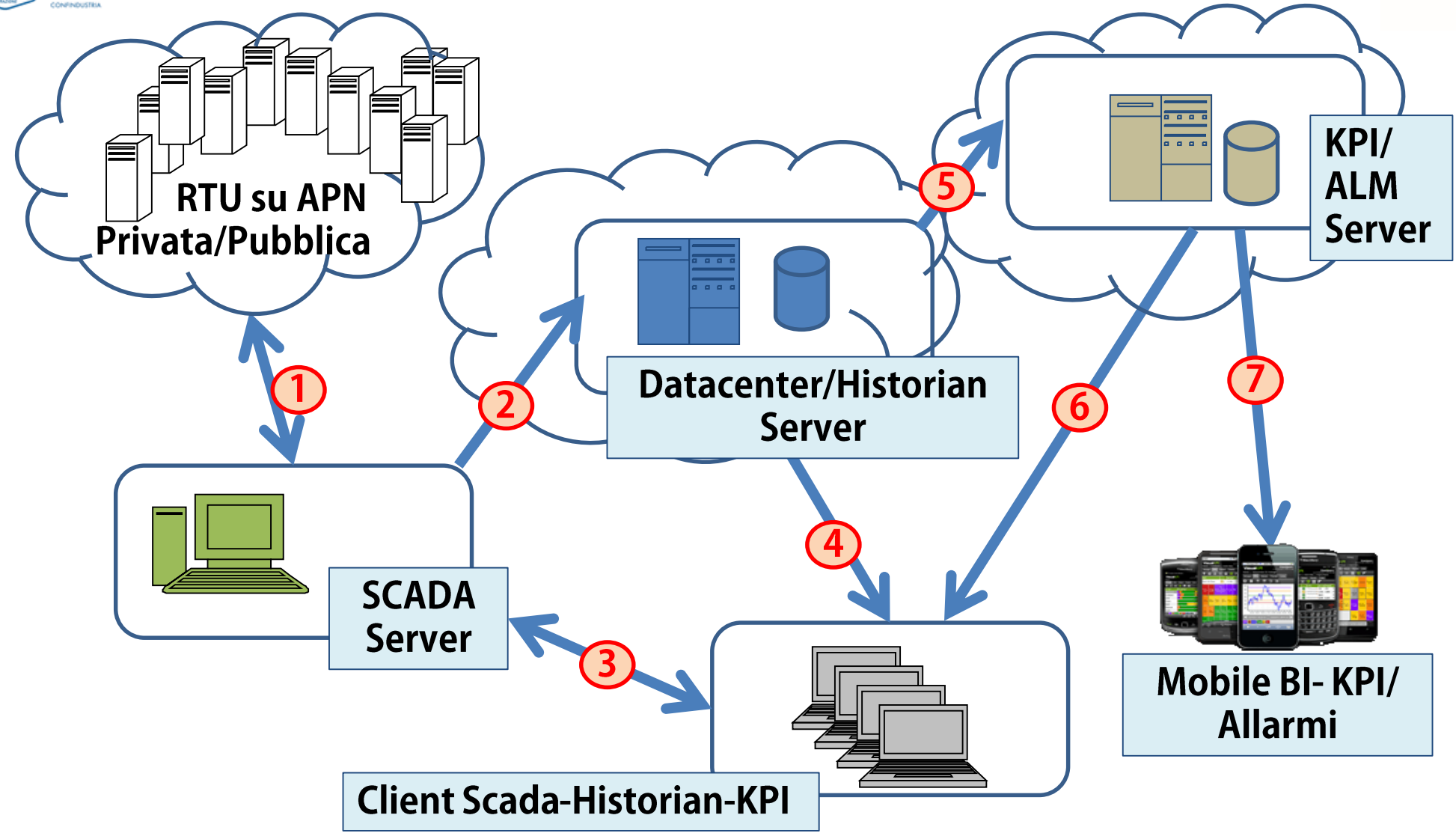
Gerarchia funzionale ANSI/ISA95
 Dati sincronizzati, contestualizzati e supervisionati

Piattaforme di Web Integrazione IoT/IIoT & CLOUD



Nuovi Sensori o interfacce proprietarie (IoT/IIoT)





La Control Room di Ieri/Oggi ...



Dati raccolti ovunque ...

…oggi/domani …



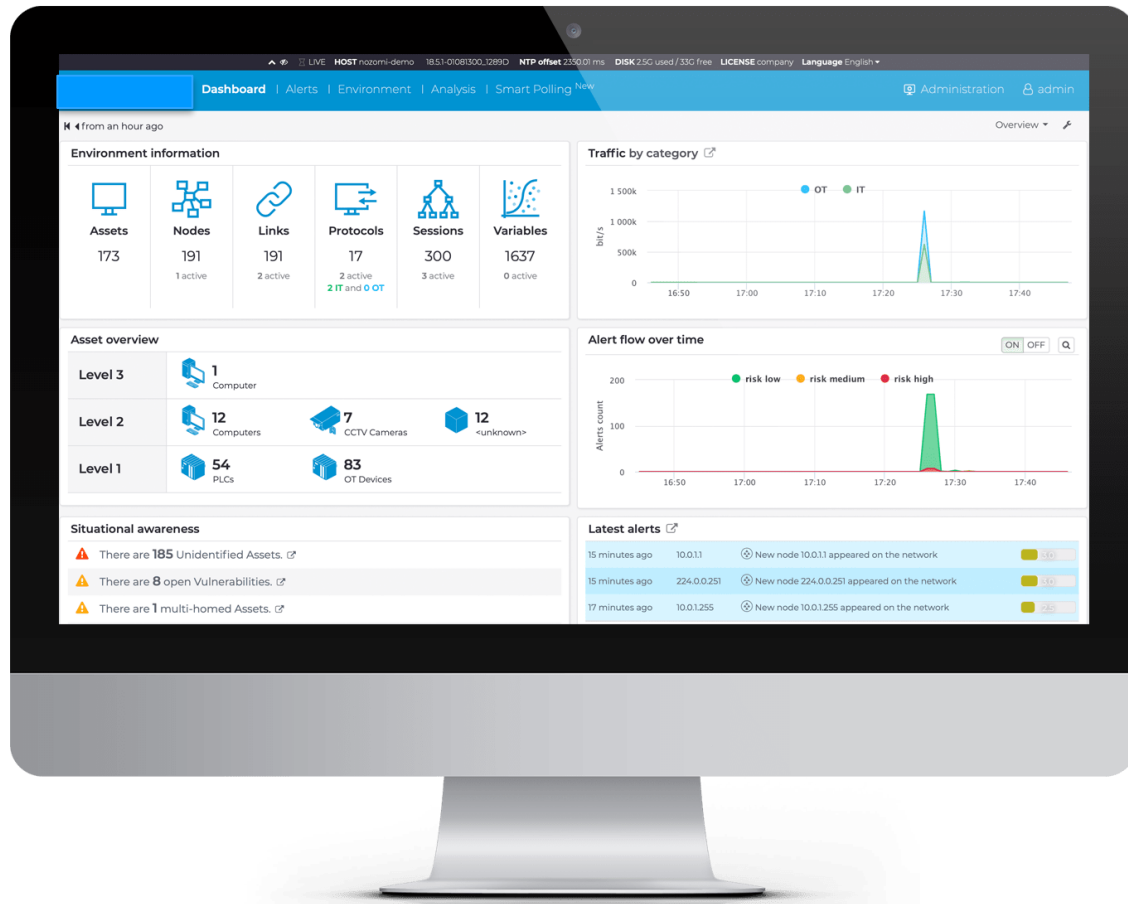
Contesto
Ruolo
Localizzazione
Notifiche intelligenti
Mobilità

…visibilità sempre e ovunque
di conoscenze operative

Cambiano le architetture: VISIBILITY è sicurezza



Cambiano le architetture: VISIBILITY è sicurezza



Domande da farsi:

- Cosa possiamo e cosa vogliamo vedere e proteggere?
- Monitoraggio attivo o passivo?
- Hardware di rete e infrastruttura è adeguato (switch, firewall, span/mirror port, TAP, ecc.)?
- Partire con POC/POV?

Ma ricordiamo sempre: IT vs OT, i rischi sono diversi!

- **Rischio Sistemi IT:**
 - perdita di dati e informazioni, file e documenti, I.P, provocano ritardi di transazioni e incidono sul business (impatti su risorse, tempo, soldi), ...
- **Rischio Sistemi di controllo / OT:**
 - oltre a quanto previsto per i Sistemi IT, la non sicurezza dei sistemi può incidere su
 - **integrità fisica di Persone e Ambiente** (salute, incidenti sul lavoro, rischio ambientale e territoriale)
 - **conservazione di Impianti di Produzione e materiali** (risorse, tempo, soldi, macchinari, ...)



Continuità Operativa di Servizio (SLA)

Livello SLA Uptime [%]	Tempo annuo di Downtime (Fermo)
99	3 giorni 15h 39m 29.5s
99.9	8h 45m 57.0s
99.99	52m 35.7s
99.999	5m 15.6s
99.9999	31.6s

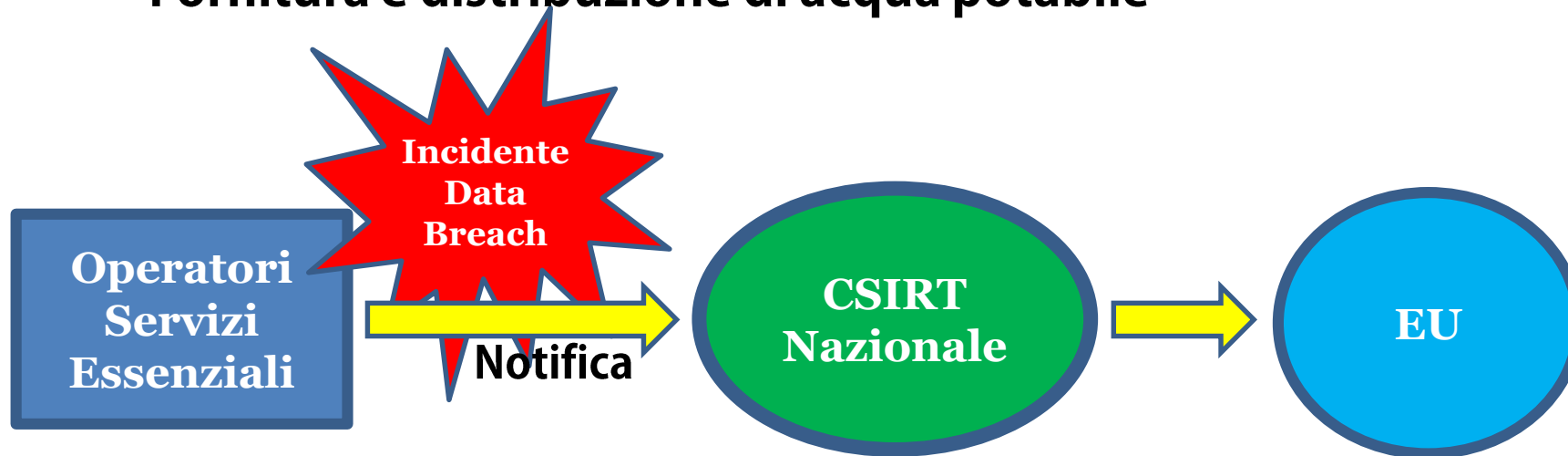
- i.e. Sistemi All Purpose, ecc
- i.e. Applicazioni Office
- **99,987% (1 h/anno)**
- **Server Fault Tolerant**

Requisiti sempre più stringenti!



Garantire la continuità operativa ed impatto sulla salute pubblica degli Operatori di Servizi Essenziali (OSE: **il MISE ne ha identificati 465!**) nei Settori:

- Energia
- Trasporti
- Settore Bancario
- Infrastrutture dei mercati finanziari
- Settore Sanitario
- Fornitura e distribuzione di acqua potabile



... importante è ripartire! (e, in fretta!)



← PLAN A
PLAN B →

NOT YOUR LANGUAGE? USE <https://translate.google.com>

What happened to your files?

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
 Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
 Sure. We guarantee that you can recover all your files safely and easily. But you do not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>.

Payment will be raised on 5/15/2017 15:58:08
 Time Left

Petya Ransomware

 PRESS ANY KEY!

infosecurity MAGAZINE

https://www.infosecurity-magazine.com/news/phishing-used-to-launch-greyenergy-ics-attacks

info security

Facebook Privacy Documents Seized by Parliament

News Topics Features Webinars White Papers Events & Conferences Directory

PHISHING ALERT

Phishing Used to Launch GreyEnergy's ICS Attacks

Racy Zurkus News Writer
 Email Racy Connect on LinkedIn

The advanced persistent threat (APT) group GreyEnergy has been targeting industrial networks across Ukraine and Eastern Europe for years, and according to analysis of the group's activities, the attacks begin with a malicious document sent in a phishing email.

Why Not Watch?

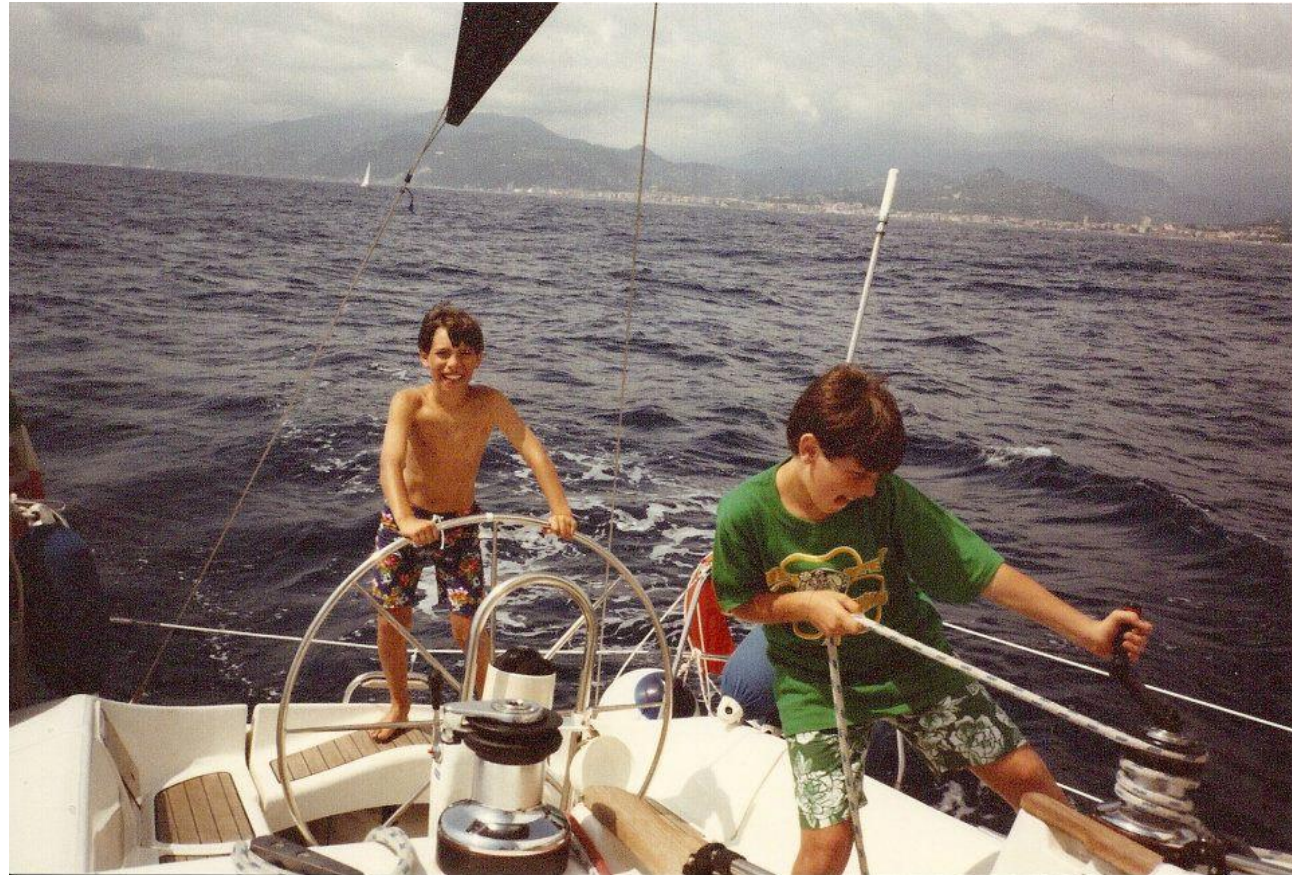
KEY WORD: VISIBILITY



•••siamo sicuri che non ci sfugga qualcosa?

OK, la Security è «buonsenso», ma la tecnologia ci può aiutare?

[Francesco Tieghi](#)
ftieghi@servitecno.it
www.servitecno.it



ANOMALY DETECTION

Disegno della rete, monitoraggio del traffico e delle anomalie



ANOMALY DETECTION

<https://www.servitecno.it/prodotti/anomaly-detection/>

BUSINESS CONTINUITY

Alta Disponibilità e Fault Tolerance



BUSINESS CONTINUITY

<https://www.servitecno.it/prodotti/ztcedge/>

OT VERSIONING

Change management e Versioning in ambiente produttivo



OT VERSIONING

<https://www.servitecno.it/prodotti/mdt-autosave/>

NETWORKING DESIGN

Consulenza e Training



NETWORKING DESIGN

<https://www.servitecno.it/soluzione/cyber-security/>