

"Secure Manufacturing/Utility in the Cloud"

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



Enzo M Tieghi

ServiTecno – GE Digital Alliance Partner

CSA Italia – Coordinatore Area di Ricerca IoT/IIoT

Socio e Docente CLUSIT

etieghi@servitecno.it

www.servitecno.it

ServiTecno

OT/ICS Cyber Security

Ovvero come **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



Quali Sistemi di telecontrollo, controllo ed automazione nell'Industria e nelle Utility?

- ▶ **DCS (Distributed Control Systems)**
- ▶ **PLC** e reti di campo (Controllori programmabili)
- ▶ **SCADA/HMI** e reti di fabbrica
- ▶ Storicizzatori (**Historians, Database**, ecc.)
- ▶ **DNC/CNC, Robot, AGV**
- ▶ **MES, EBRS** e sistemi di gestione produzione, tracciabilità lotti, analisi efficienza, OEE, ecc.
- ▶ **LIMS**, QA/QC, sistemi di taratura, analisi e misura
- ▶ Sistemi di comunicazione da e verso l'esterno (portali, sistemi di **manutenzione remota, IoT, IIOT**, ...)
- ▶ Reti di impianto, Sistemi Facility/Building **BMS**
- ▶ ...

La gerarchia dei sistemi in Fabbrica e Utility

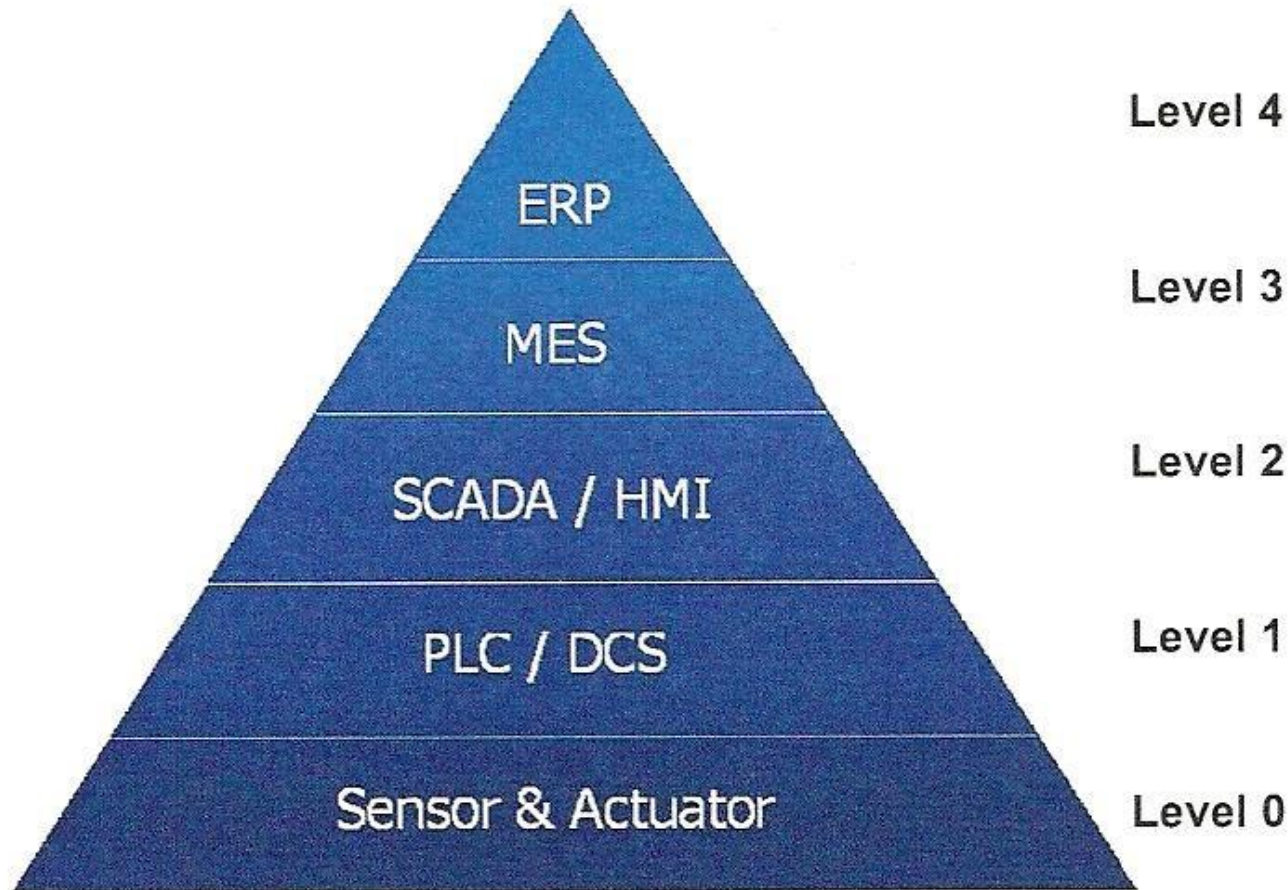
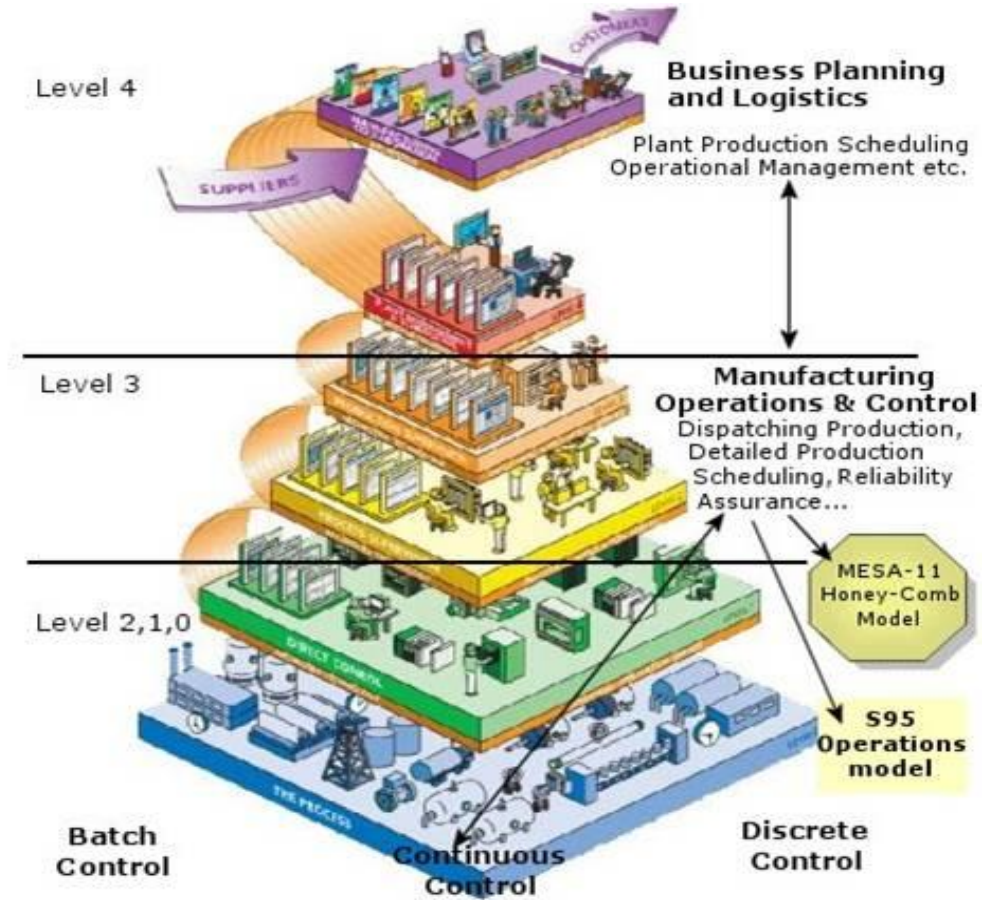
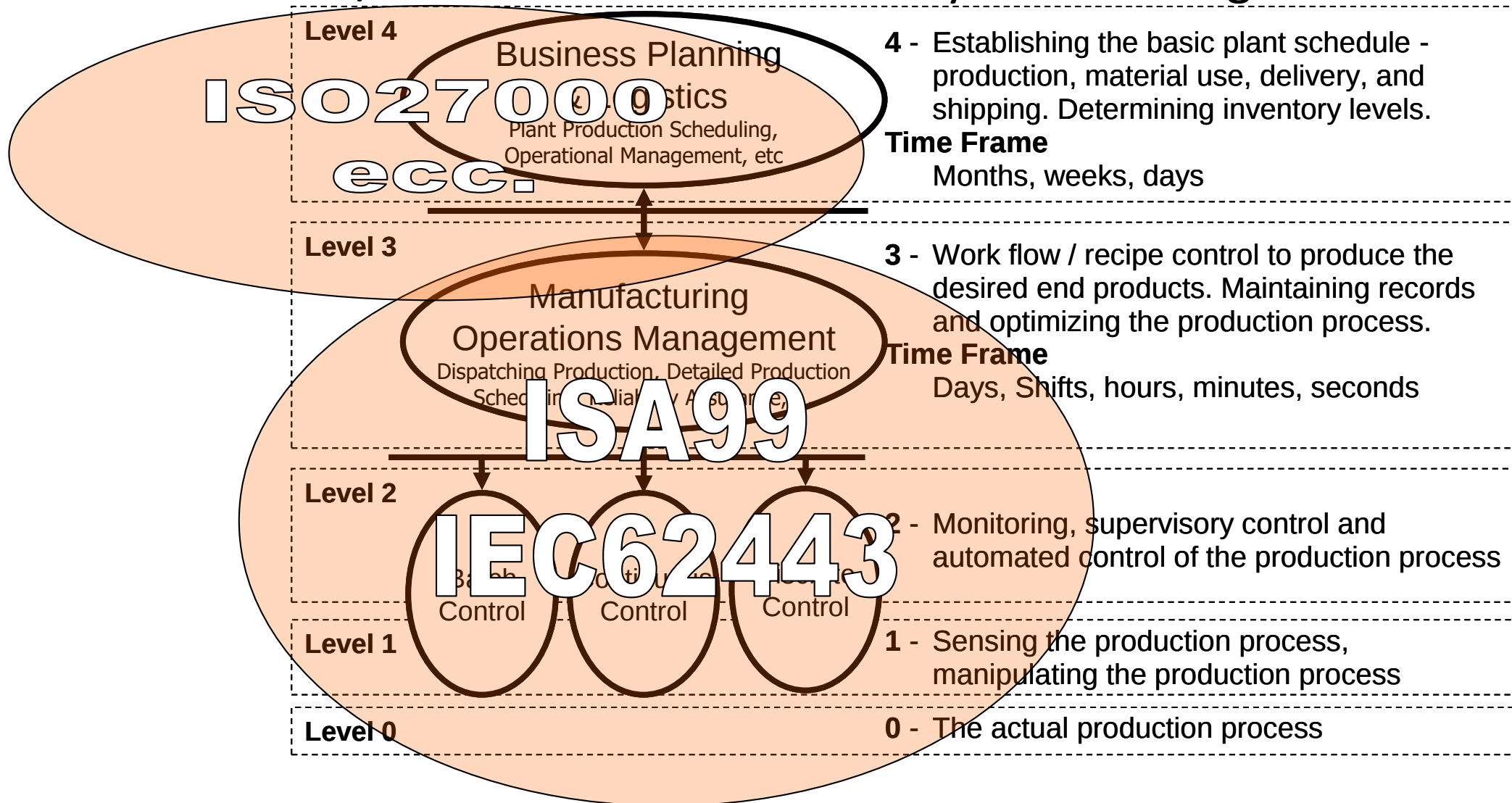


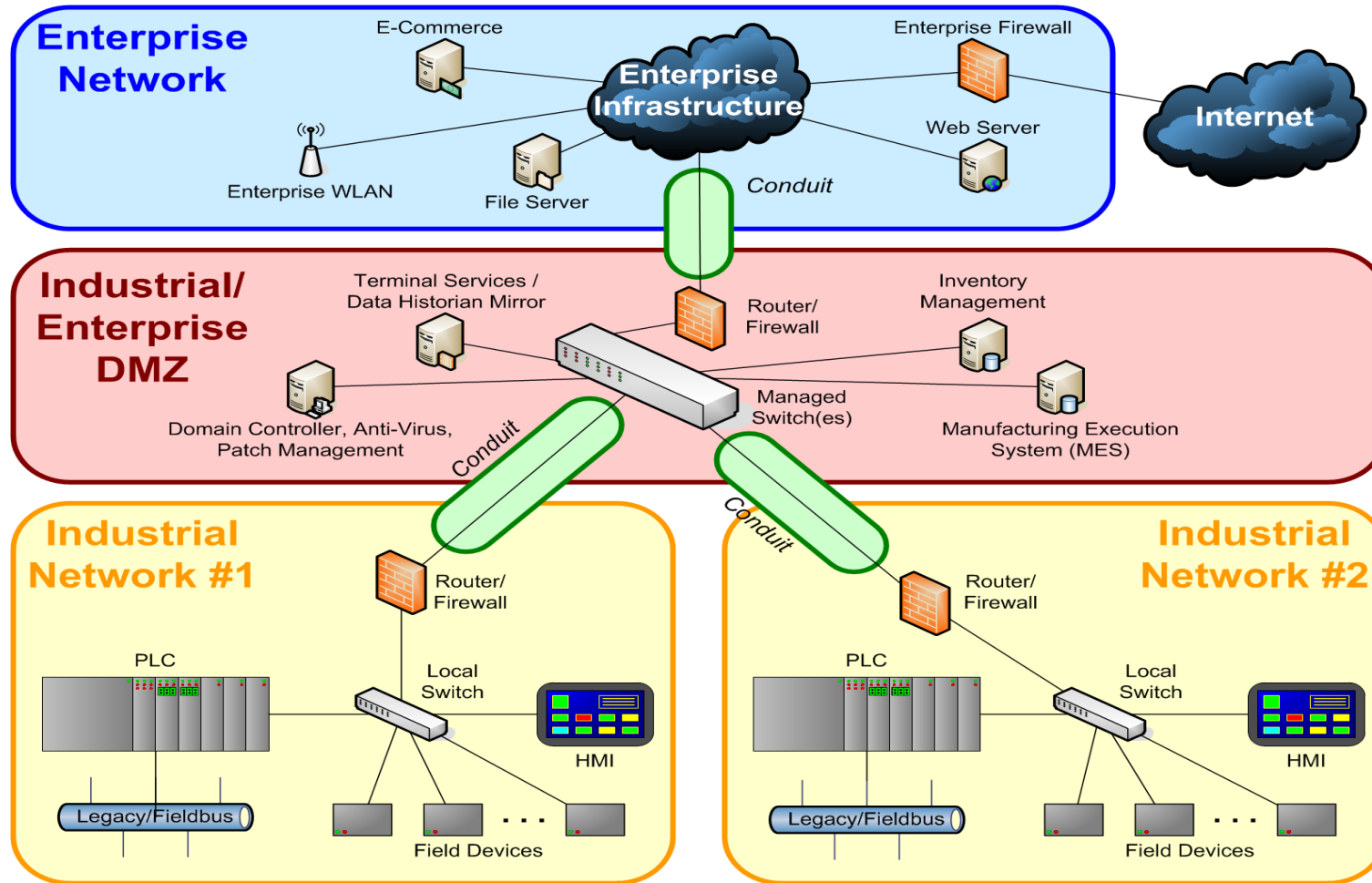
Figure 1 ISA95-1 model for production modelling.



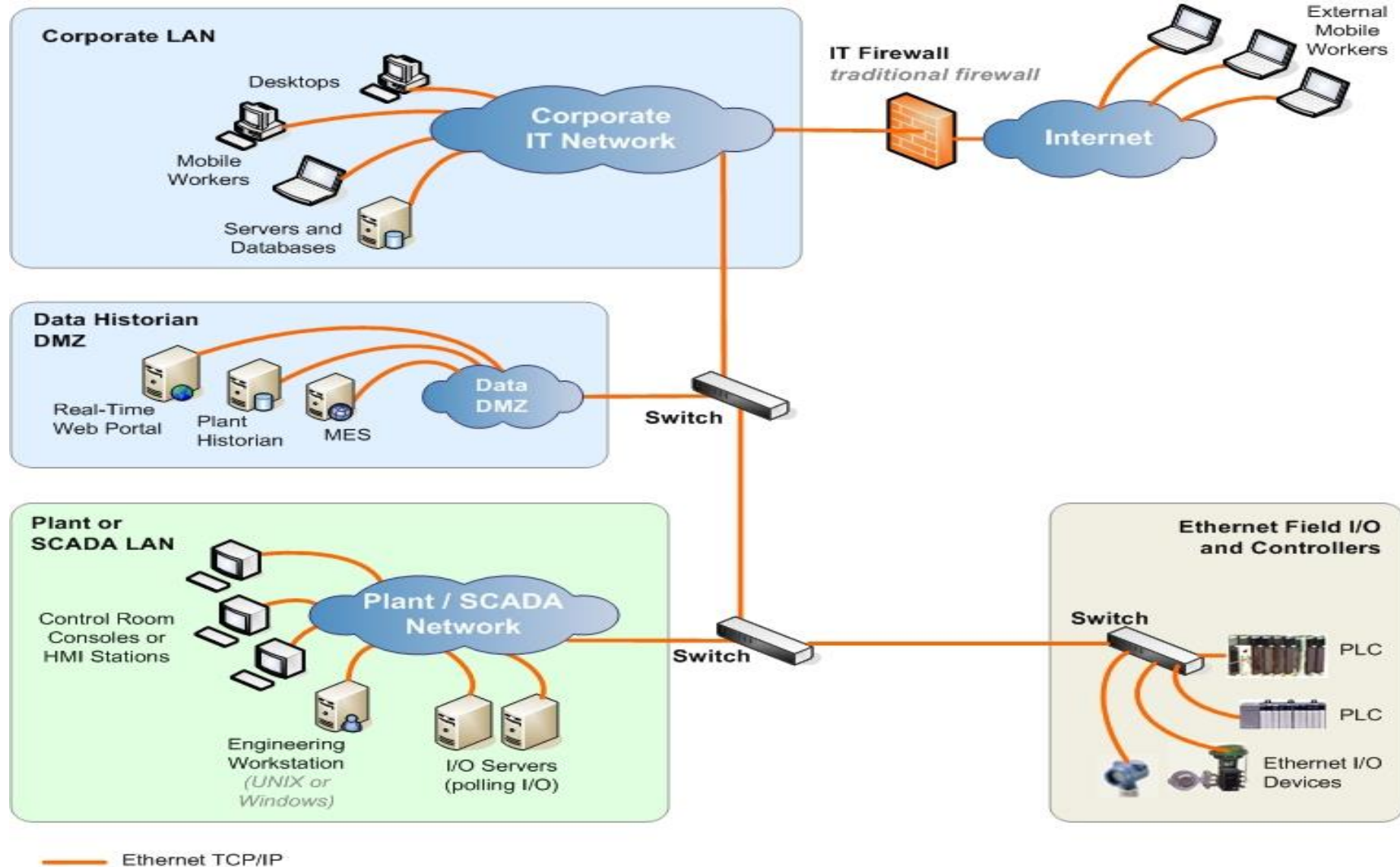
ANSI/ISA95 Functional Hierarchy www.isa.org



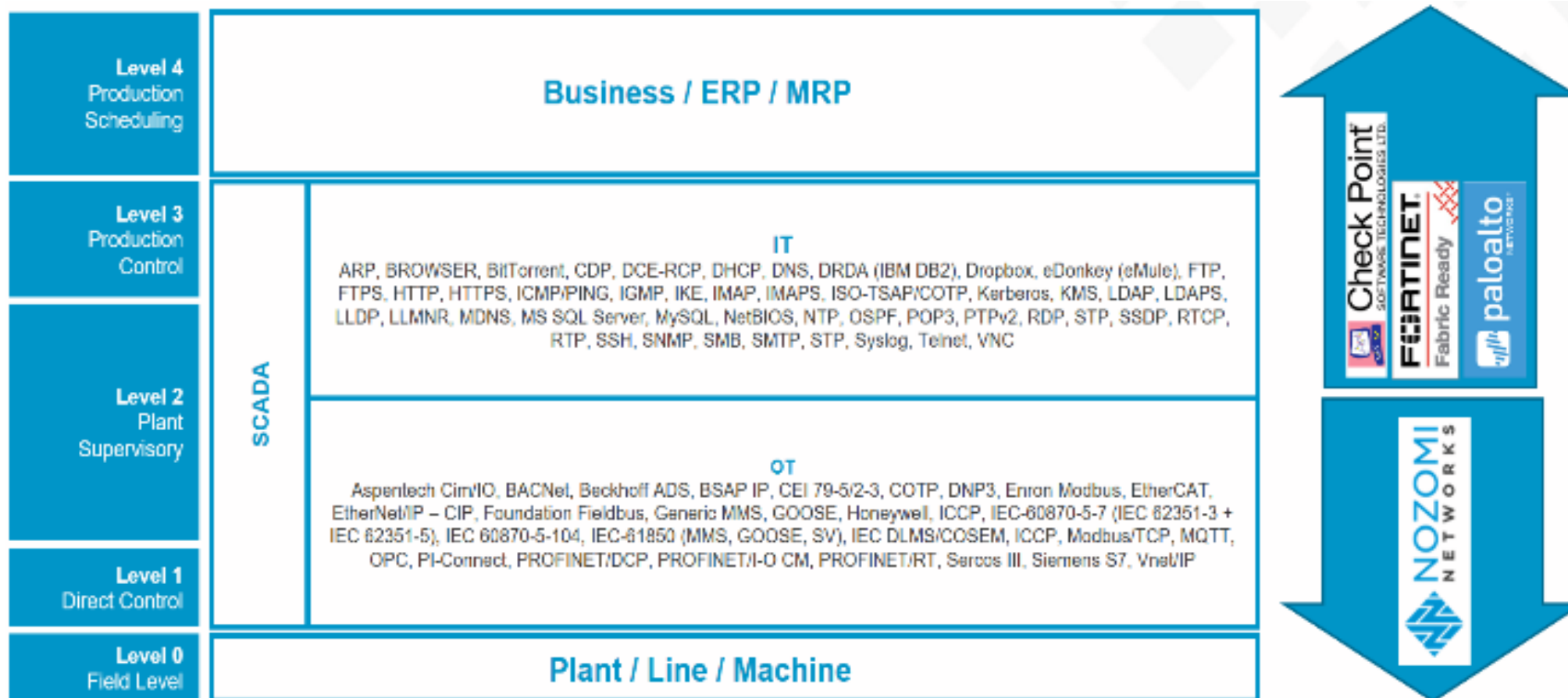
ISA99/IEC62443 Network/System Segmentation



Reti di Impianto & IT



Le frontiere dell'OT e le diverse tecnologie



Da Industria3.0 a Industria4.0

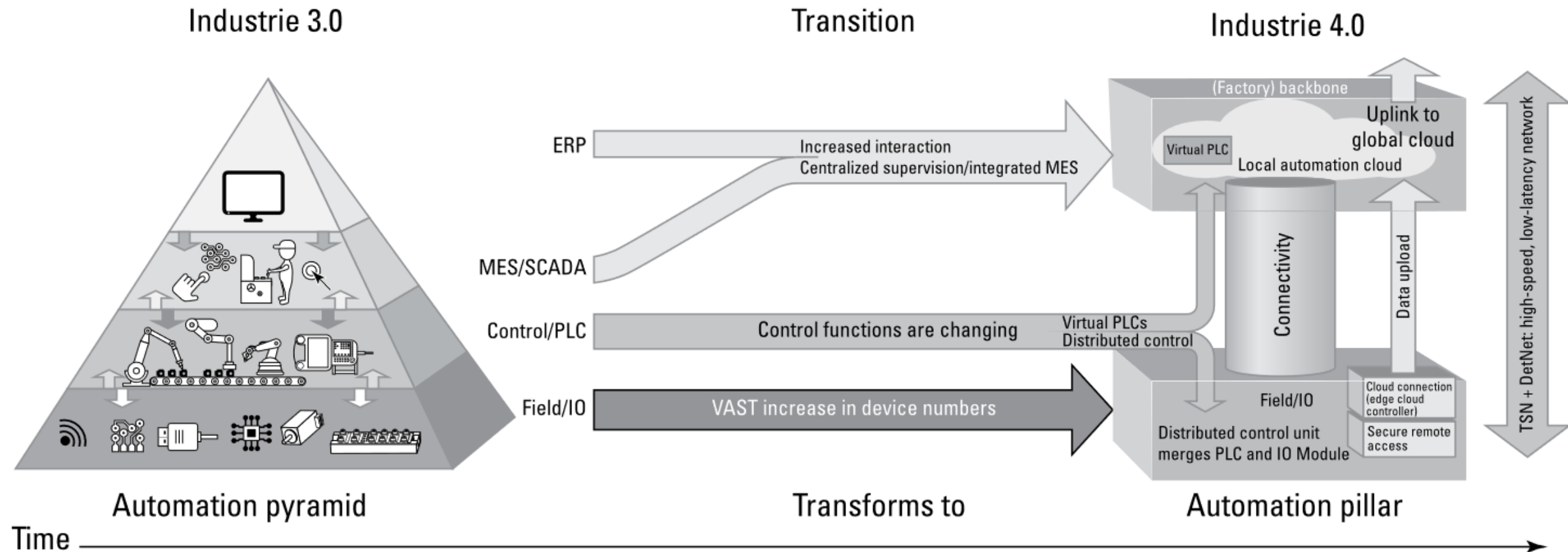
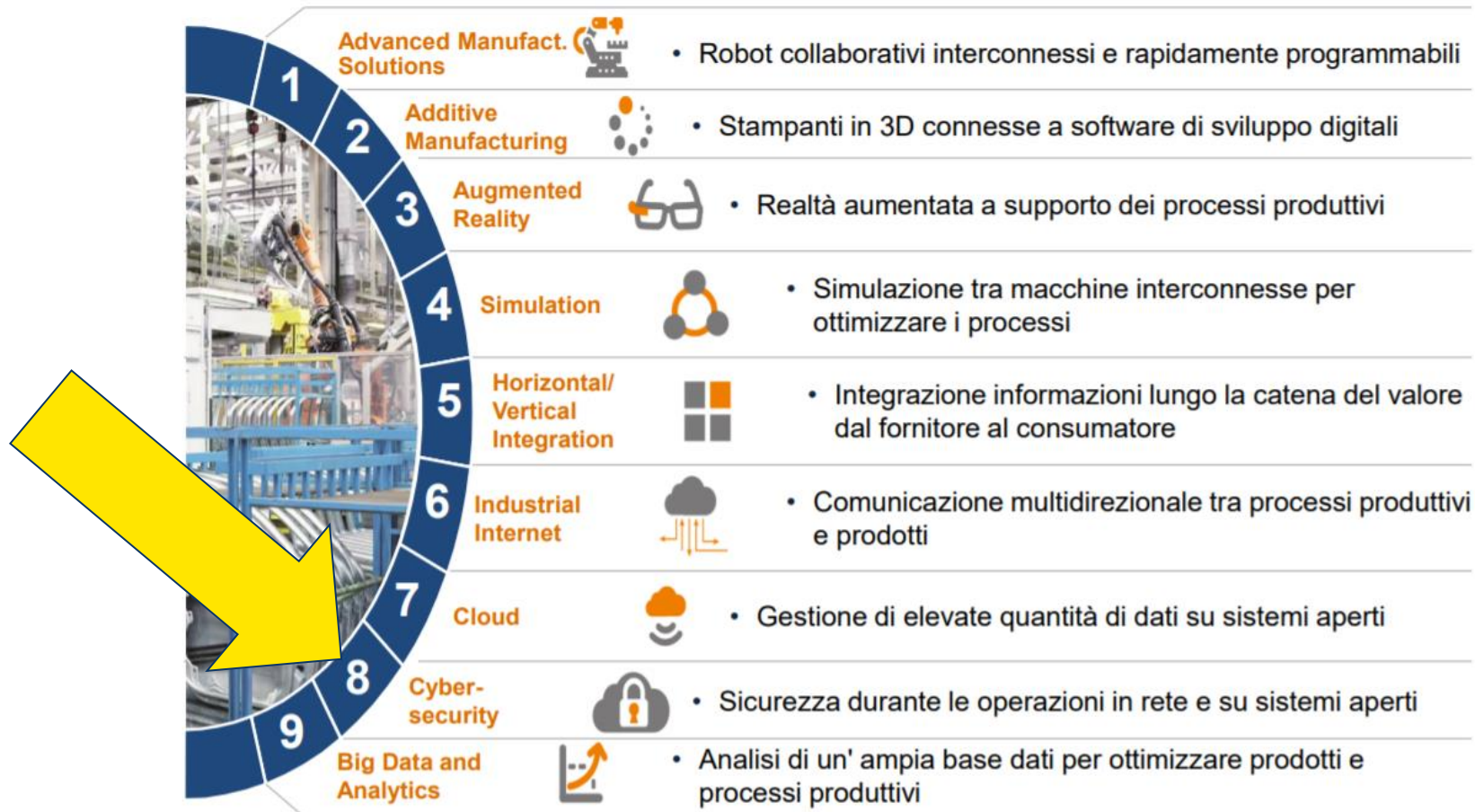


FIGURE 1-1: Moving from the automation pyramid to the automation pillar.

Industria4.0 e Cyber Security



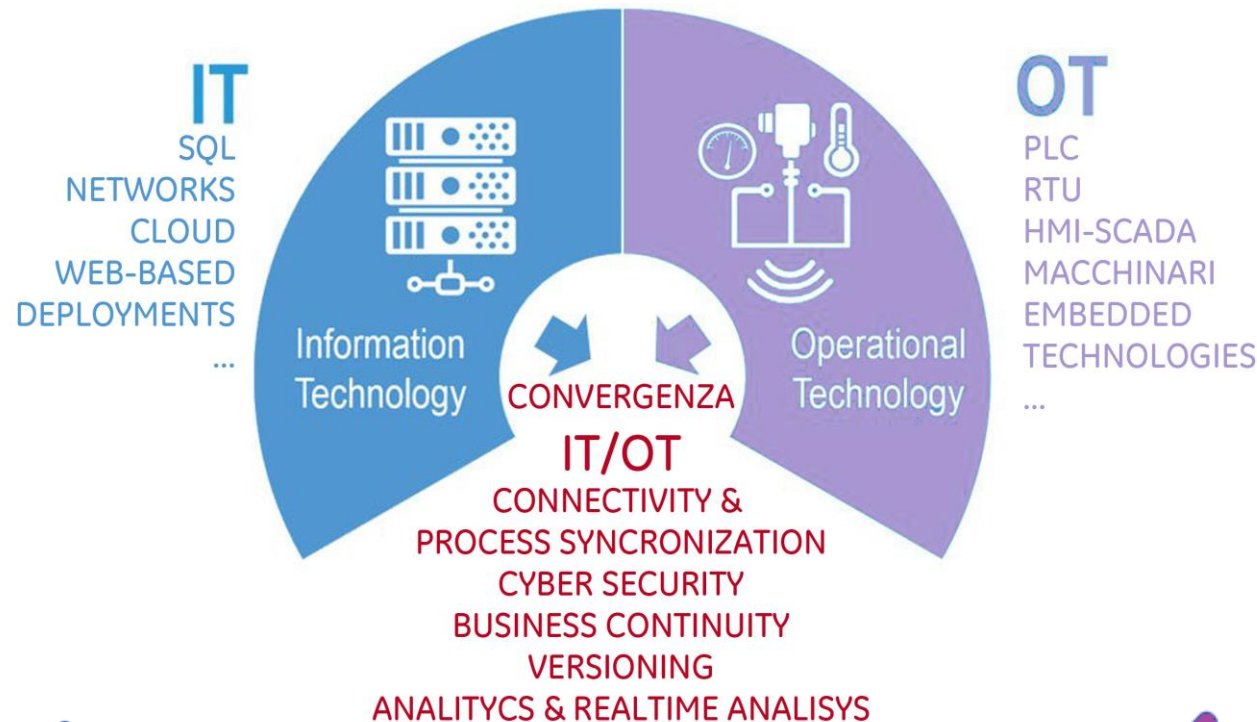
Industria 4.0: Le tecnologie abilitanti



Industria4.0, Convergenza IT – OT & il Cloud

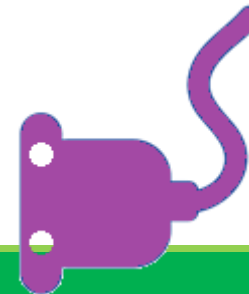
Tutti gli standard informatici aziendali, network, gestionale, cloud, analytics.

- Sistemi non-deterministici
- Sistemi non-realtime
- o al più near-realtime
- Data Integrity
- Data security
- Patent Infringement
- Business Continuity



Le interfacce informatiche primarie con macchine e impianti, attuatori e trasduttori fisici delle logiche programmabili.

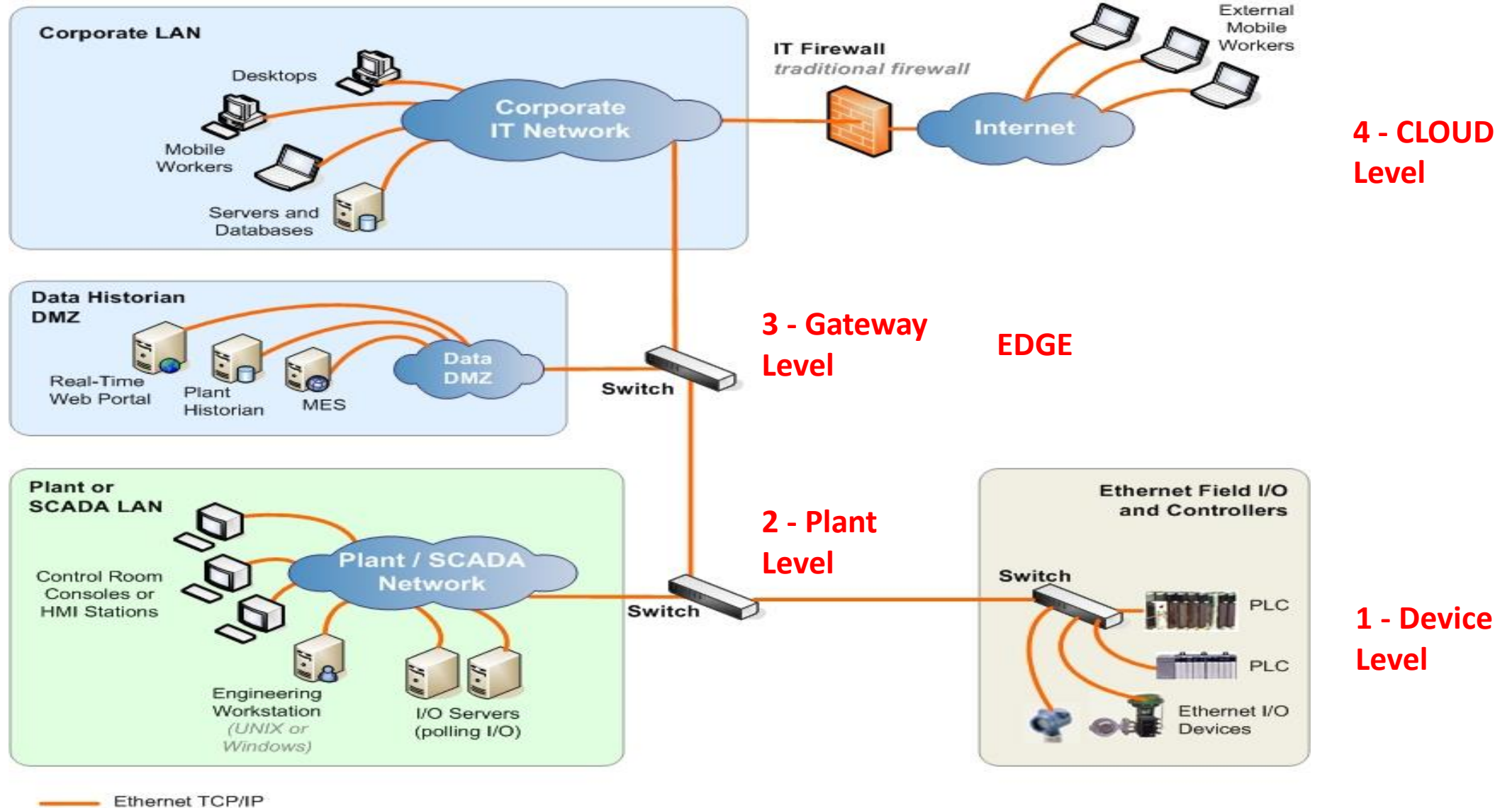
- Sistemi deterministici
- Sistemi strettamente realtime
- Brand specifici
- People Safety
- Business and Service Continuity



Quali i Sistemi nell'Industria e nelle Utility che potrebbero utilizzare Cloud ?

- ▶ **DCS (Distributed Control Systems)**
- ▶ **PLC** e reti di campo (Controllori programmabili)
- ▶ **SCADA/HMI** e reti di fabbrica
- ▶ Storicizzatori (**Historians, Database**, ecc.)
- ▶ **DNC/CNC, Robot, AGV**
- ▶ **MES, EBRS** e sistemi di gestione produzione, tracciabilità lotti, analisi efficienza, OEE, ecc.
- ▶ **LIMS**, QA/QC, sistemi di taratura, analisi e misura
- ▶ Sistemi di comunicazione da e verso l'esterno (portali, sistemi di **manutenzione remota, IoT, IIOT**, ...)
- ▶ Reti di impianto, Sistemi Facility/Building **BMS**
- ▶ ...

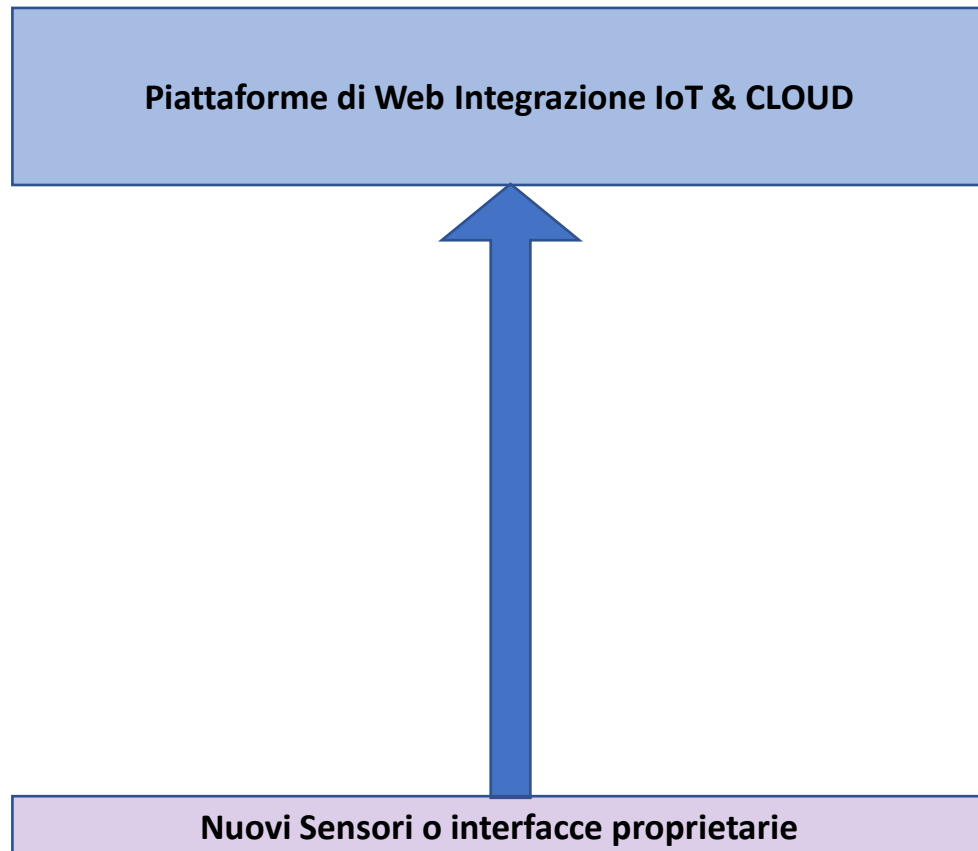
Reti di Impianto & IT con CLOUD



Dualismo IoT vs. IIoT industriale/automazione

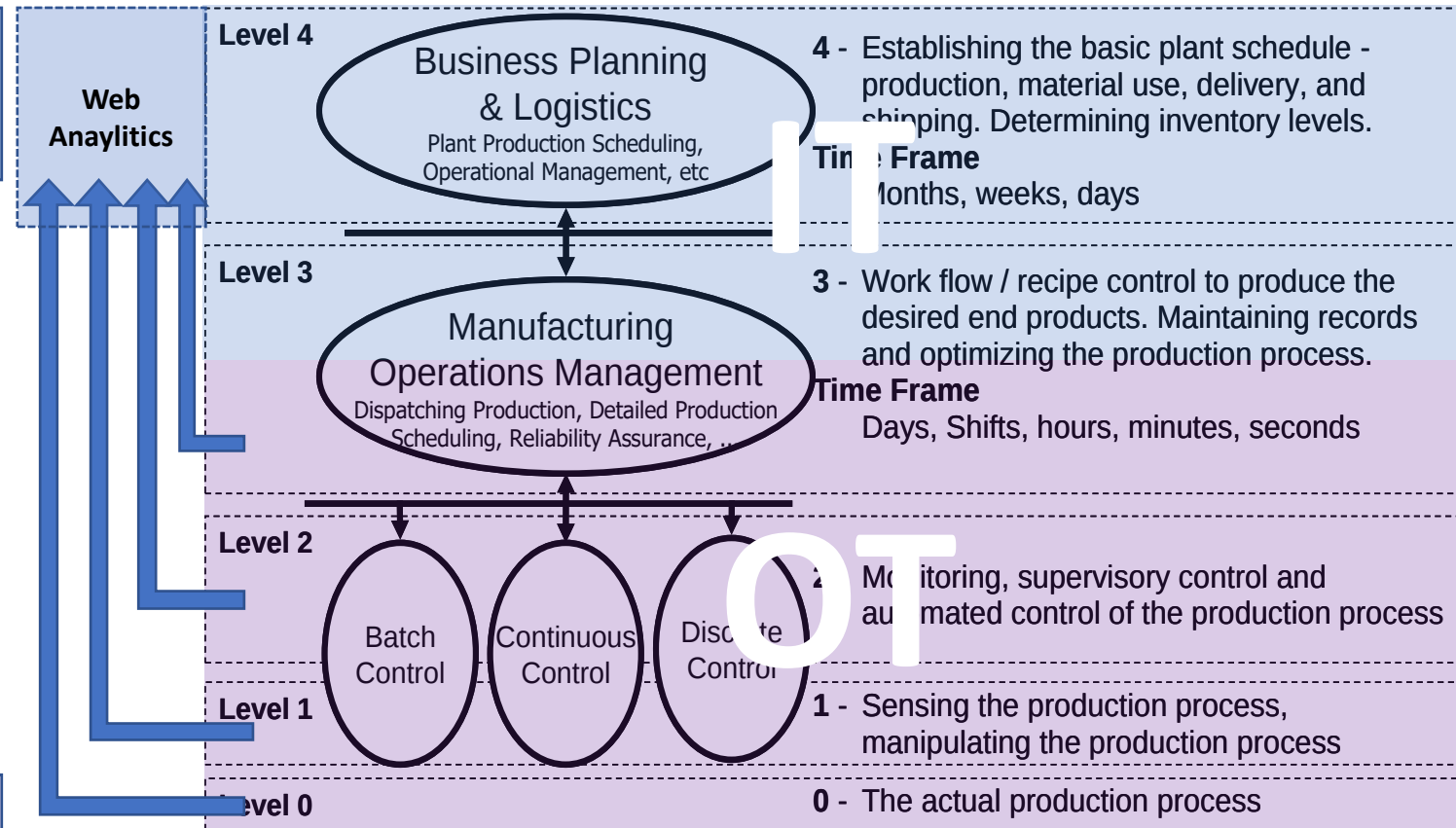
IOT Shortcut

Dati duplicati, non supervisionati

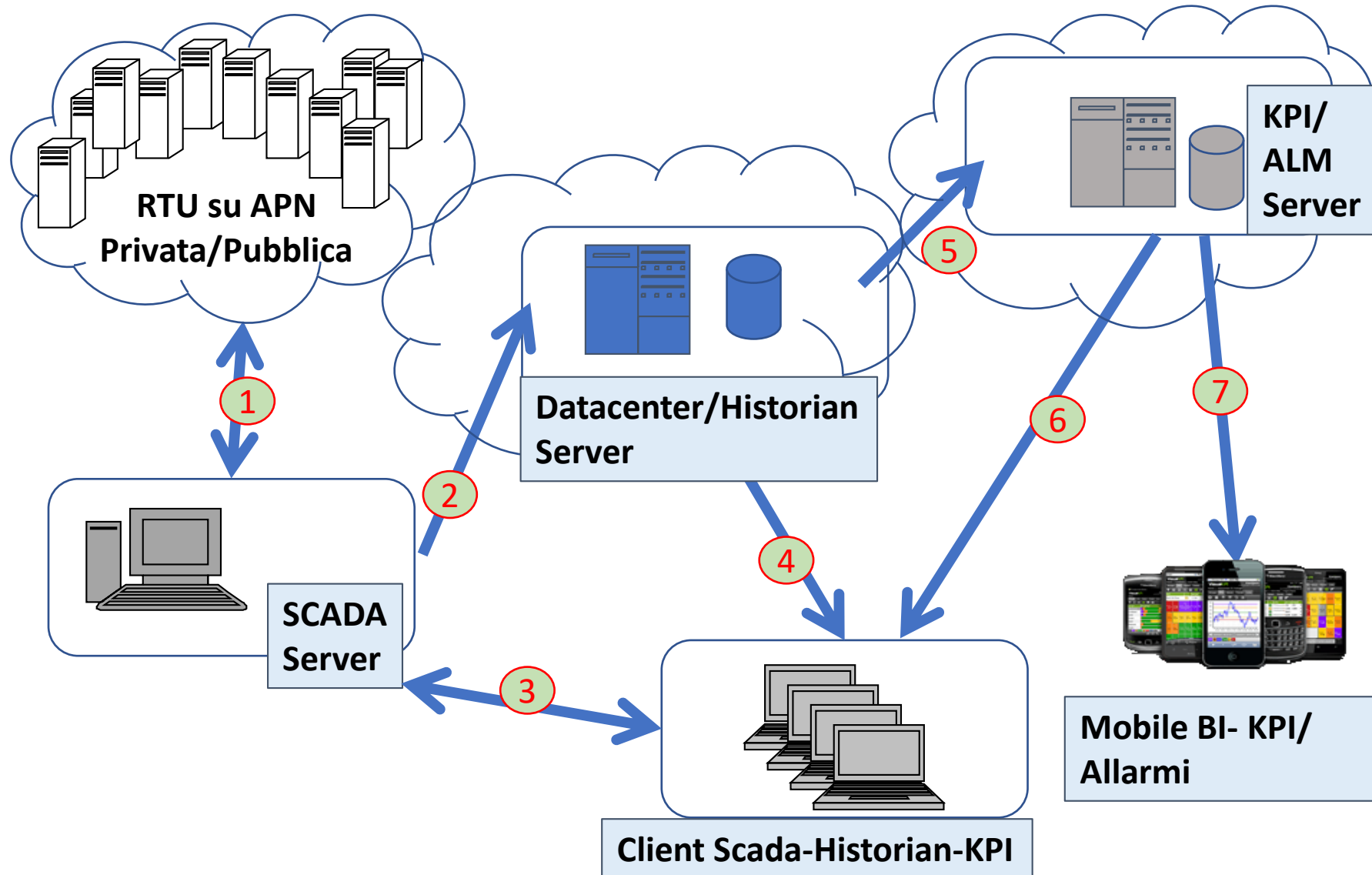


Gerarchia funzionale ANSI/ISA95

Dati sincronizzati, contestualizzati e supervisionati



Sistemi ICS/OT & Cloud e Multi-Cloud



IT vs OT: I rischi sono diversi!

- **Sistemi IT:**

- **perdita** di dati e informazioni, file e documenti, provocano ritardi di transazioni e incidono sul business (impatti su **risorse, tempo, soldi**), ...

- **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 cose*** (risorse, tempo, soldi, macchinari, ...)



NIST: SP800-53, SP800-82, SP800-144, SP800-183

NIST Special Publication 800-53A
Revision 1

NIST

**National Institute of
Standards and Technology**
U.S. Department of Commerce

Guide for Assessing the Security Controls in Federal Information Systems and Organizations

Building Effective Security Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Consistent with NIST SP 800-53, Revision 3

NIST Special Publication 800-183

Networks of 'Things'

Jeffrey Voas

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-183>

NIST Special Publication 800-82
Revision 1

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS),
(PLC)

uffer
Falco
rfone

NIST

**National Institute of
Standards and Technology**
U.S. Department of Commerce

Special Publication 800-144

Guidelines on Security and Privacy in Public Cloud Computing

Wayne Jansen
Timothy Grance

Proteggere IoT e IIoT: con quali standard?

22

Draft NISTIR 8200

23

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

Prepared by the Interagency International Cybersecurity Standardization Working Group.

NIST Editors:

Mike Hogan

Ben Piccarreta

Information Technology Laboratory



February 2018



43

44

45

46

47

48

49

50

U.S. Department of Commerce

Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology

Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

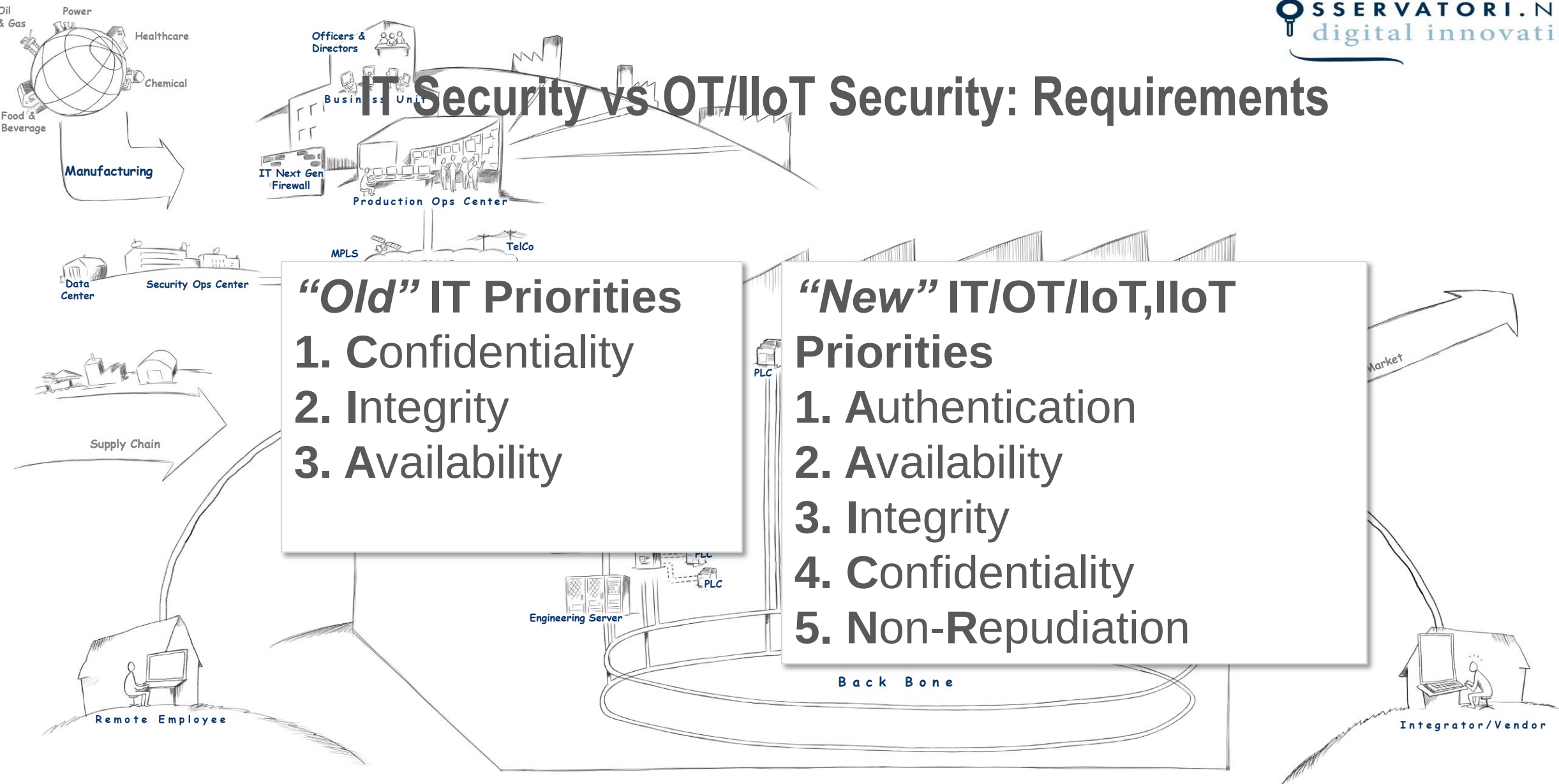
IT Security vs OT/IloT Security: Requirements

“Old” IT Priorities

1. Confidentiality
2. Integrity
3. Availability

“New” IT/OT/IloT,IIoT Priorities

1. Authentication
2. Availability
3. Integrity
4. Confidentiality
5. Non-Repudiation



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

→ Server Fault Tolerant

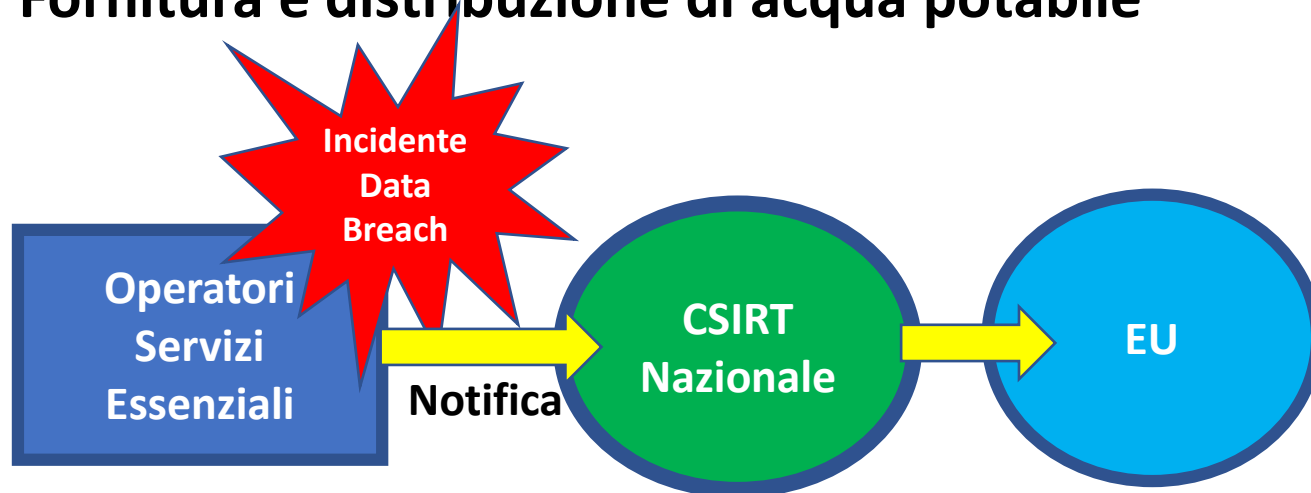
Requisiti sempre più stringenti!



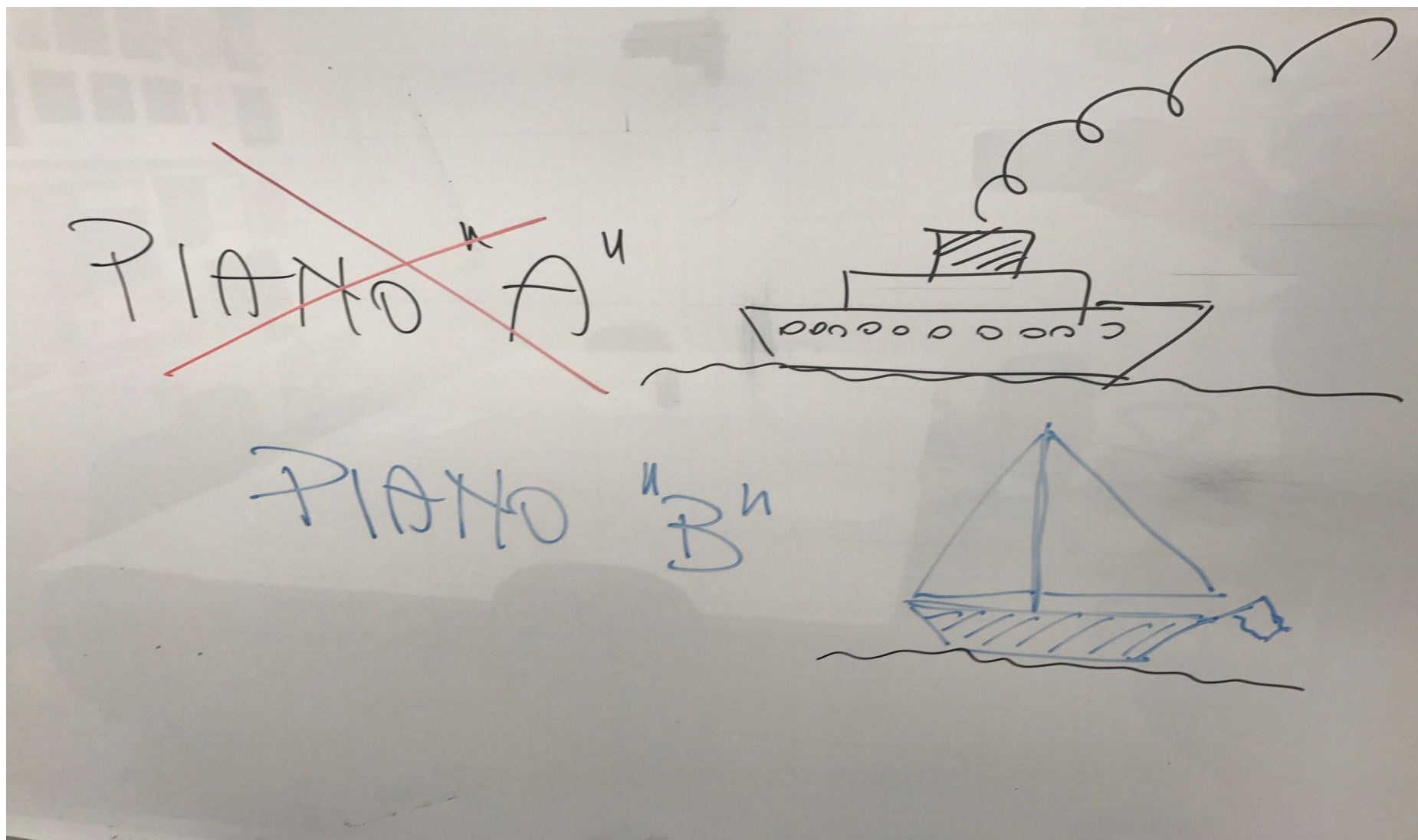
OT e Normativa NIS

Garantire la **continuità operativa** ed impatto **sulla salute pubblica** degli Operatori di Servizi Essenziali

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



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



Conosciamo «veramente» le minacce?



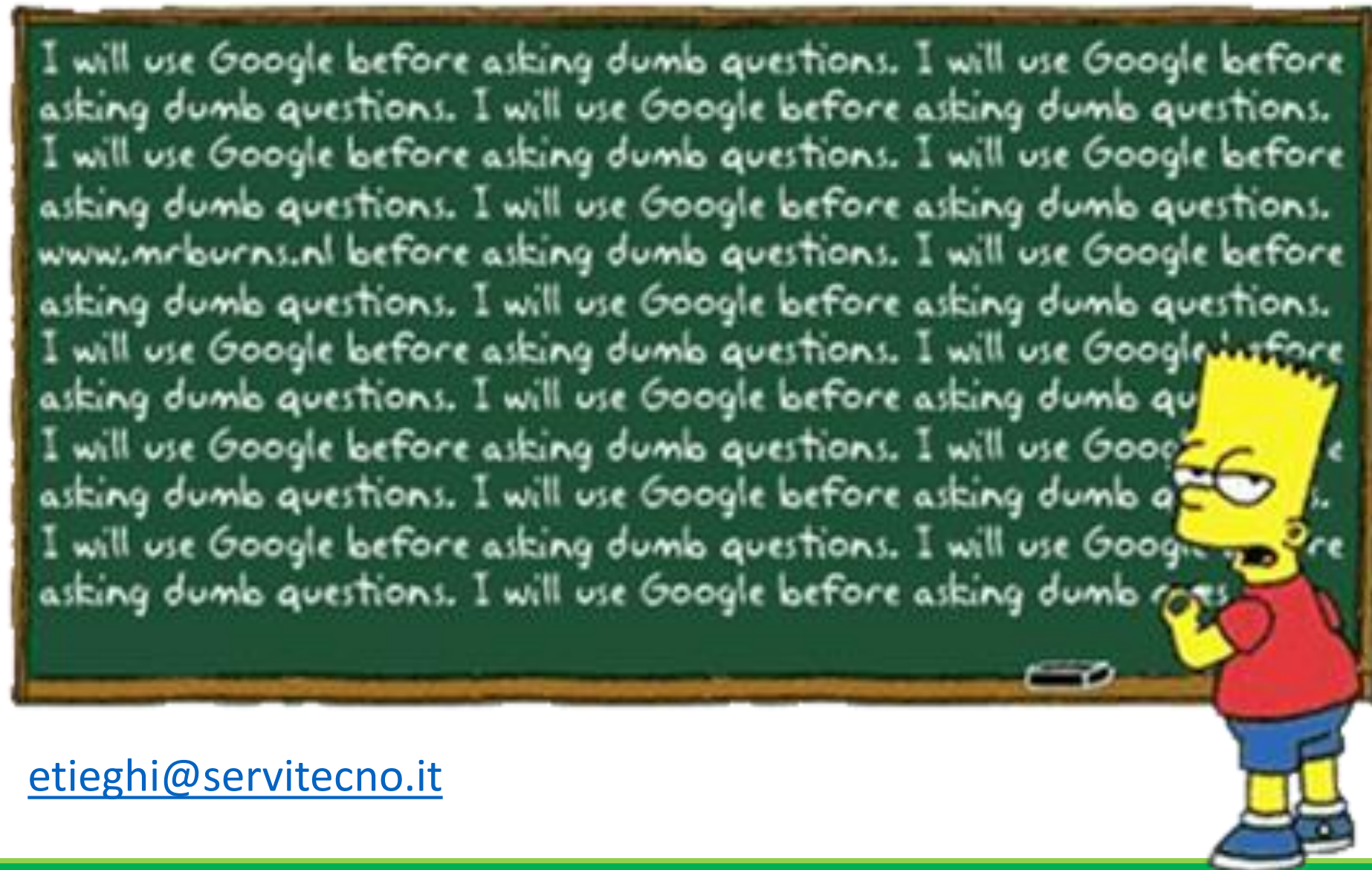
Petya
Ransomware

Oltre al «buonsenso», la tecnologia ci può aiutare?



...siamo sicuri che non ci sfugga qualcosa?

Dubbi? Domande?



etieghi@servitecno.it

"Secure Manufacturing/Utility in the Cloud"

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

Enzo M Tieghi

ServiTecno – GE Digital Alliance Partner

CSA Italia – Coordinatore Area di Ricerca IoT/IIoT

Socio e Docente CLUSIT

etieghi@servitecno.it

www.servitecno.it



ServiTecno