forum Software Industriale

Ma bisogna proprio proteggere anche le reti di fabbrica e IIoT?

Chiariamoci qualche dubbio su OT/ICS/IIoT Cyber Security

Enzo M. Tieghi, *Clusit*, Comitato Scientifico,
Controllo ed automazione in ambito Industriale & *Industrial IoT*

etieghi@clusit.it – http://www.clusit.it

Clusit

Clusit Education

Bisogna proprio proteggere anche le reti di fabbrica e IIoT?

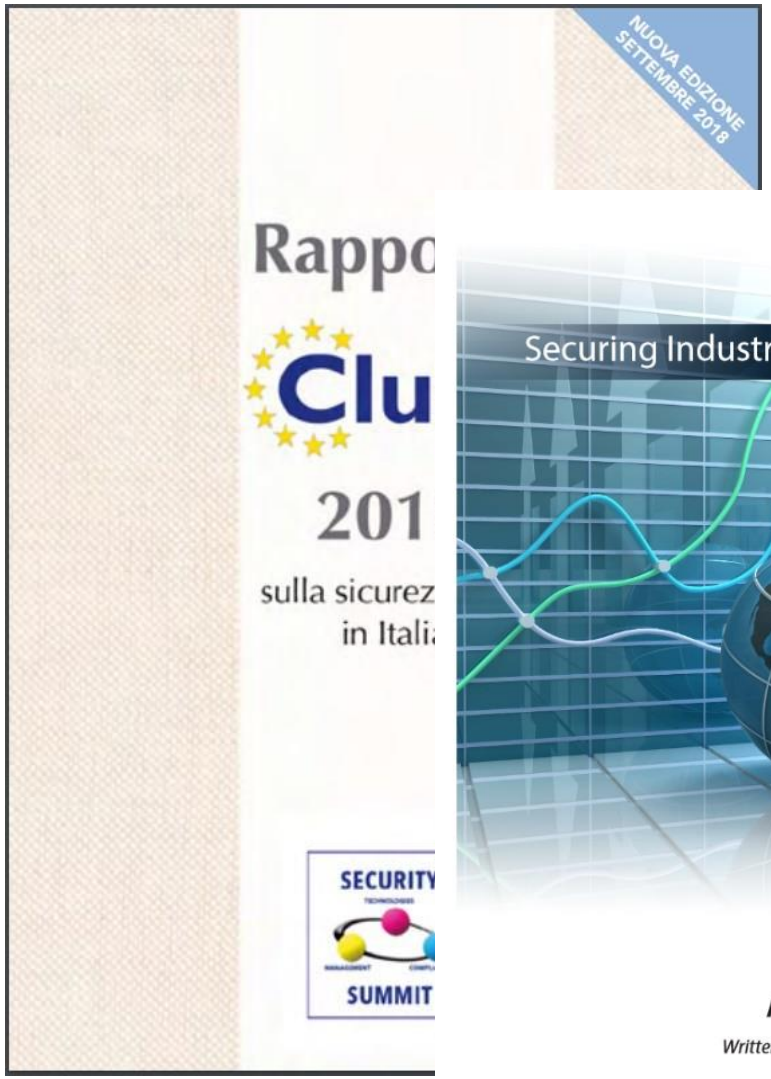
A) ***Perché dovrei*** *proteggere anche reti e sistemi in fabbrica che* ***NON sono collegati a internet****!*

B) ***Certo che si****. L'anno scorso qualcuno in Sede ha aperto un allegato e-mail e abbiamo avuto la* ***fabbrica ferma*** *due settimane* ***per colpa del ransomware «Wannacry»****!*

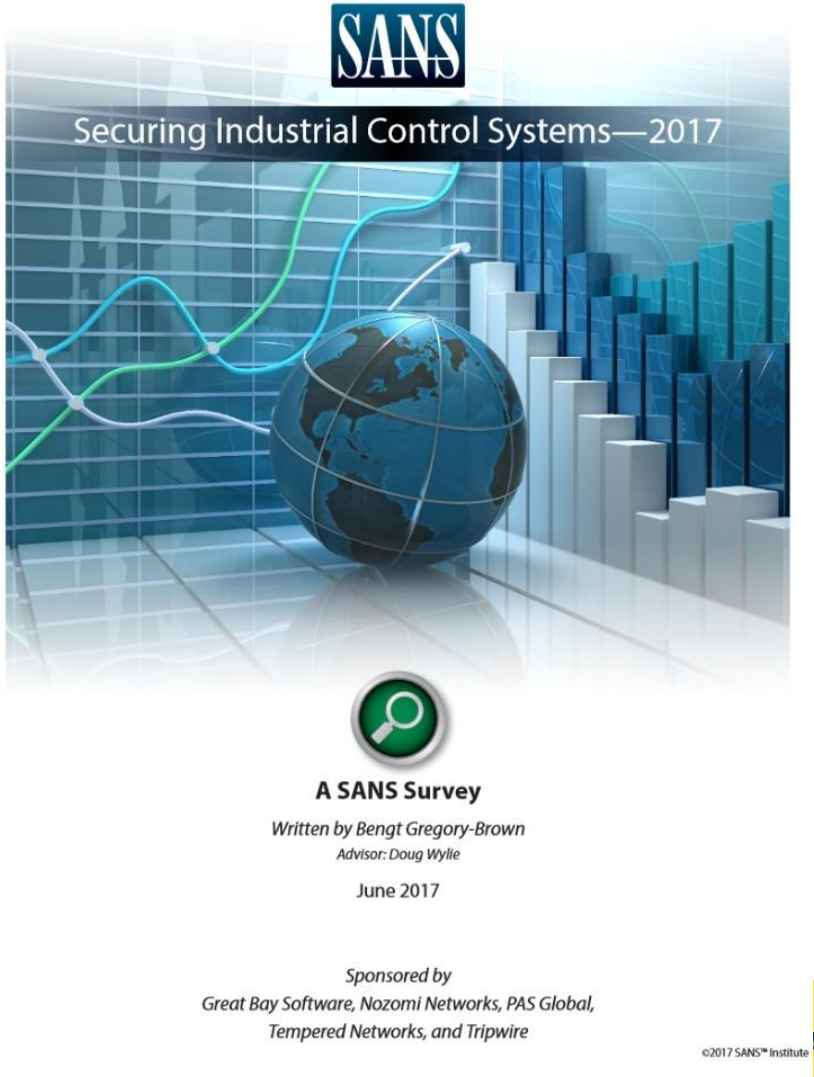
C) ***Perché dovrei?*** *Abbiamo già speso un* ***sacco di soldi per il GDPR*** *ed il* ***nostro IT*** *ha già messo in campo* ***tutte le sicurezze****!*

D) ***Dipende*** *dal disegno della rete di fabbrica: facciamo* ***analisi del rischio ed assessment*** *e poi decidiamo*

Scegli la risposta giusta: ***(A)*** ***(B)*** ***(C)*** ***(D)***



INDUSTRY 4.0:
La nuova frontiera dei c
criminali nell'anno del



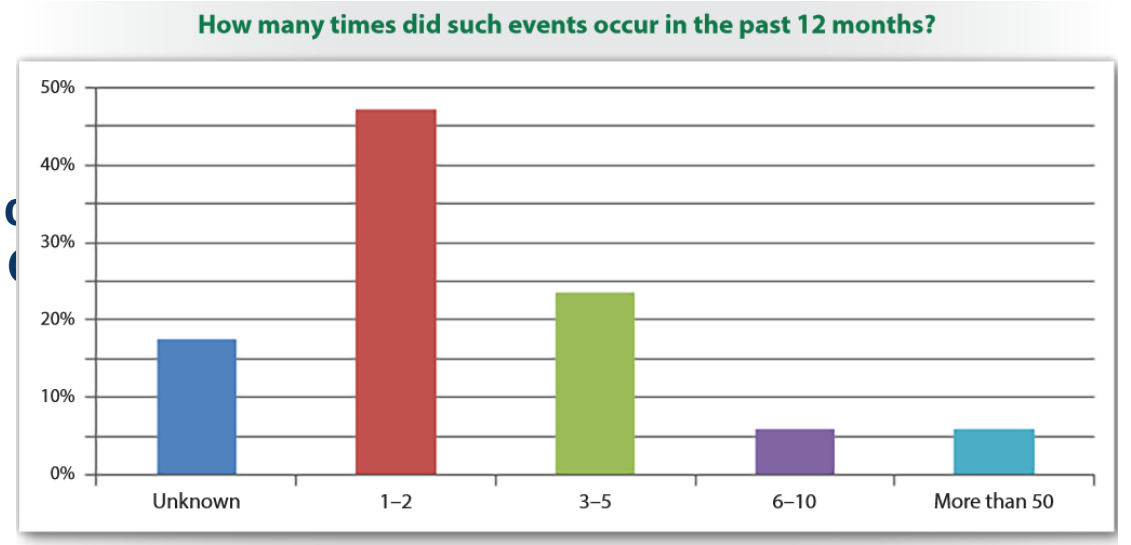


Figure 8. Infiltrations/Infections in the Past 12 Months

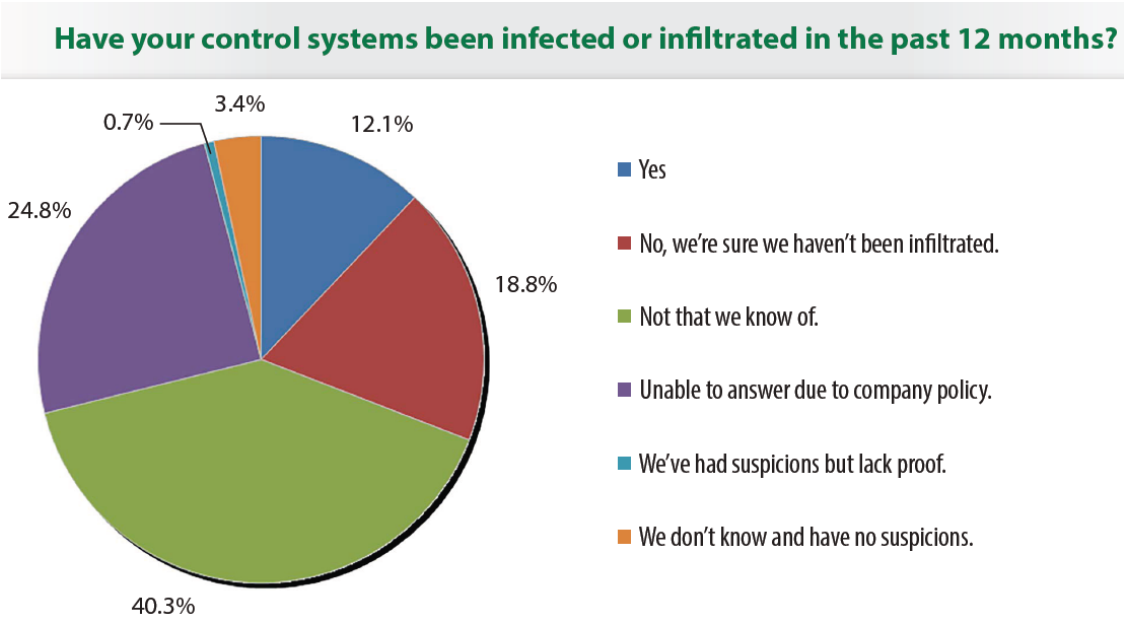
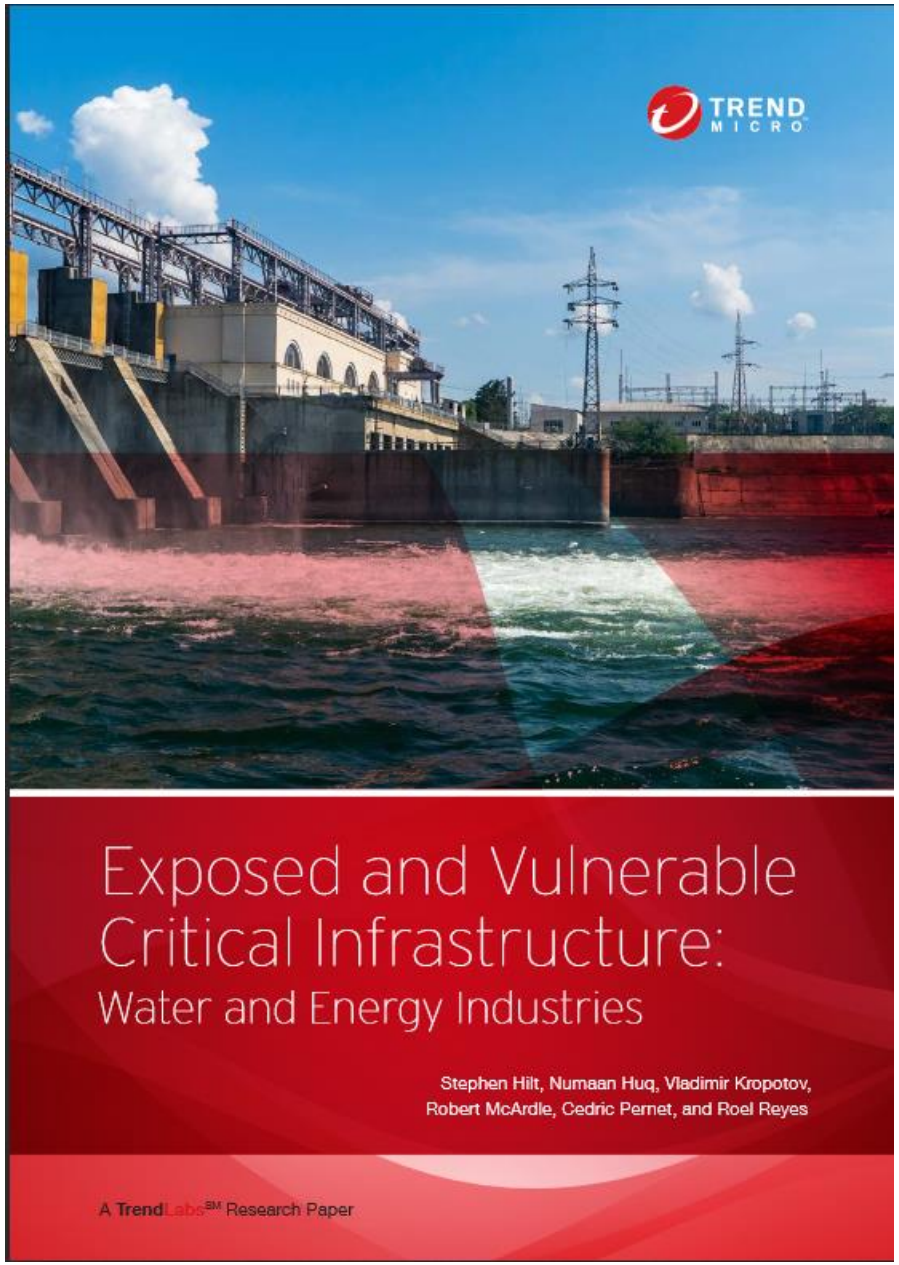


Figure 7. Infections/Infiltrations in the Past 12 Months

Alcuni sistemi «esposti» (in Italia)

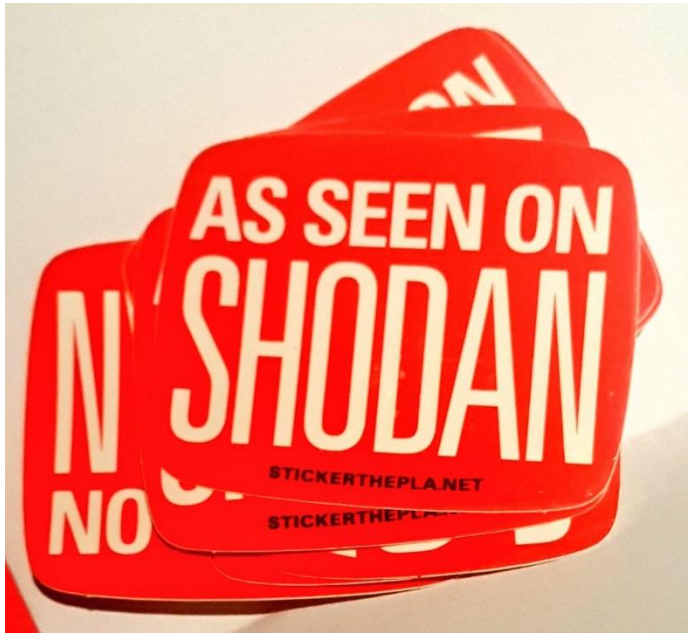
Dal report TrendMicro «Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries» (2018)

by
Stephen Hilt, Numaan Huq, Vladimir Kropotov, Robert McArdle, Cedric Pernet, and Roel Reyes



Exposed Biogas HMIs

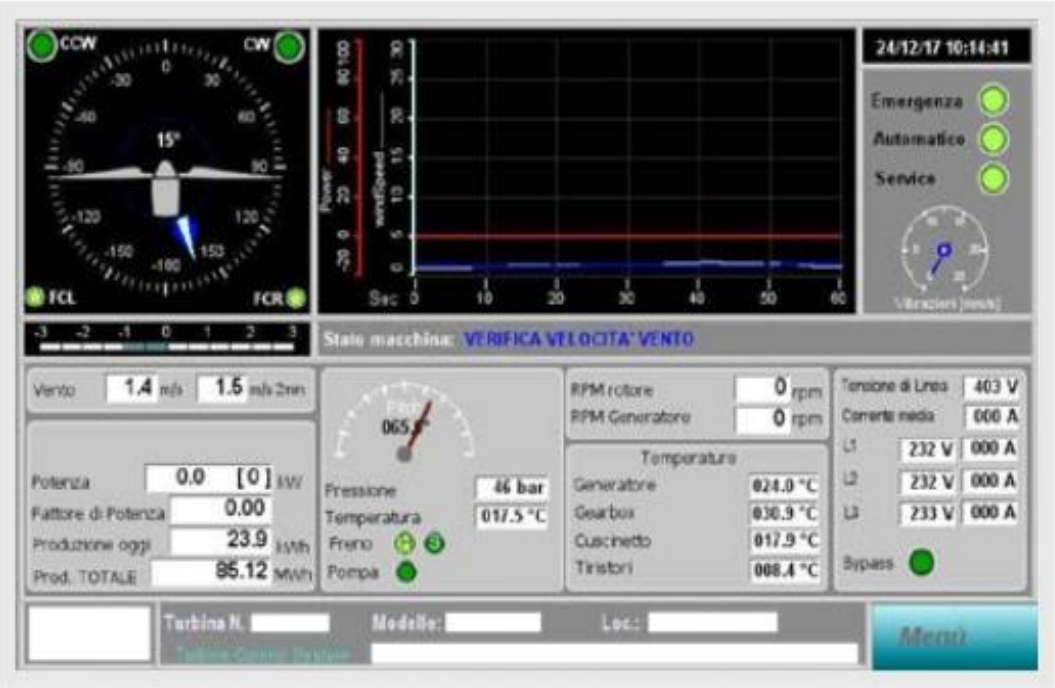
Exposed biogas HMIs were discovered in Germany, France, Italy, and Greece, where this form of energy extraction is prevalent.



Top-level menu for a biogas facility in Italy. Submenus, system reset, and alarm are all accessible from this page.

Exposed Power System HMIs

Exposed power system HMIs were discovered in Germany, Spain, Sweden, the Czech Republic, Italy, France, Austria and South Korea, and include systems from solar, wind, and hydroelectric plants. Surprisingly, no North American instances were found using our methods.



The controls for this wind turbine are located in Italy. According to additional screenshots found on the turbine manufacturer's website (name deleted for privacy), all aspects of the turbine, i.e., start, stop, reset, and system parameters, can be controlled using this software.

Looking at the exposed cameras on the device, we surmised that it is related to a hydro facility. Based on the information that we collected, we can say that the power plant is located in Italy.

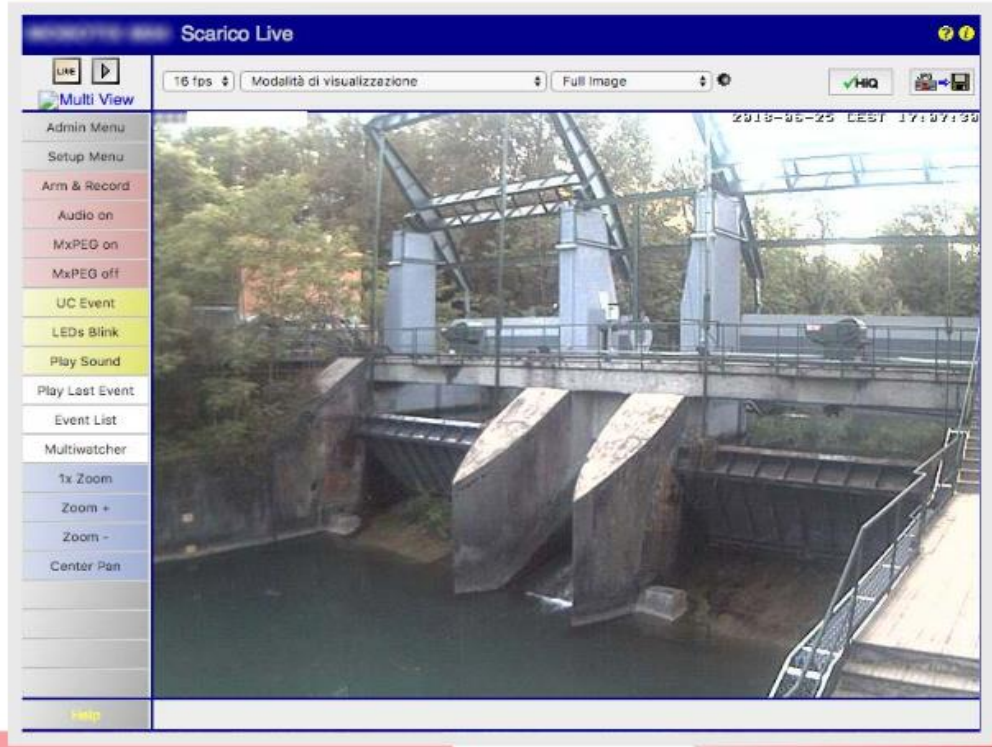


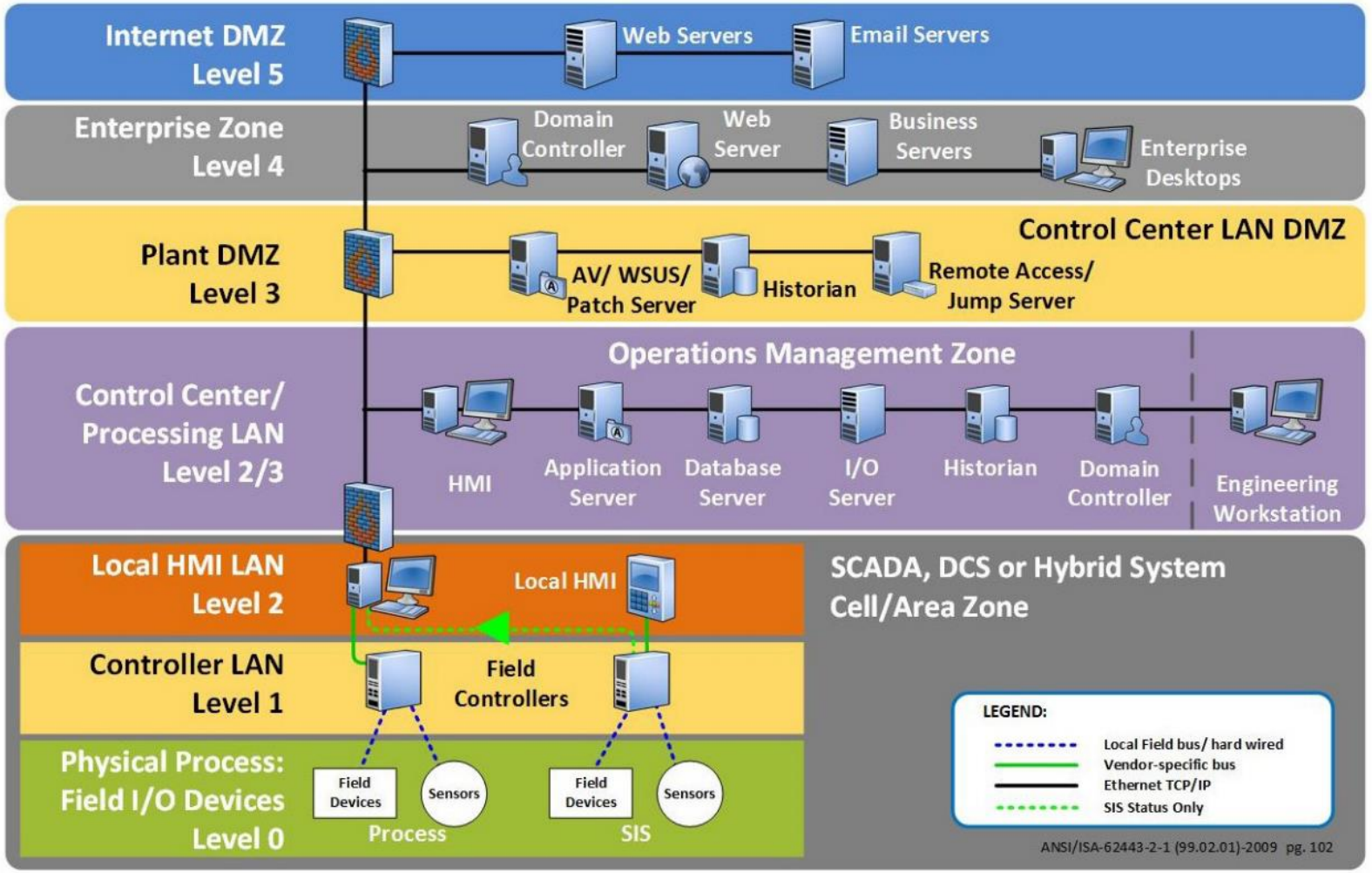
Figure 27. View of the spill gates of the hydro facility

Industria4.0 e Cyber Security

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

- **DCS (D**istributed **C**ontrol **S**ystems**)**
- **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**
- **…**

OT/ICS: dove si trovano e come sono collegati secondo il “The Purdue Model”



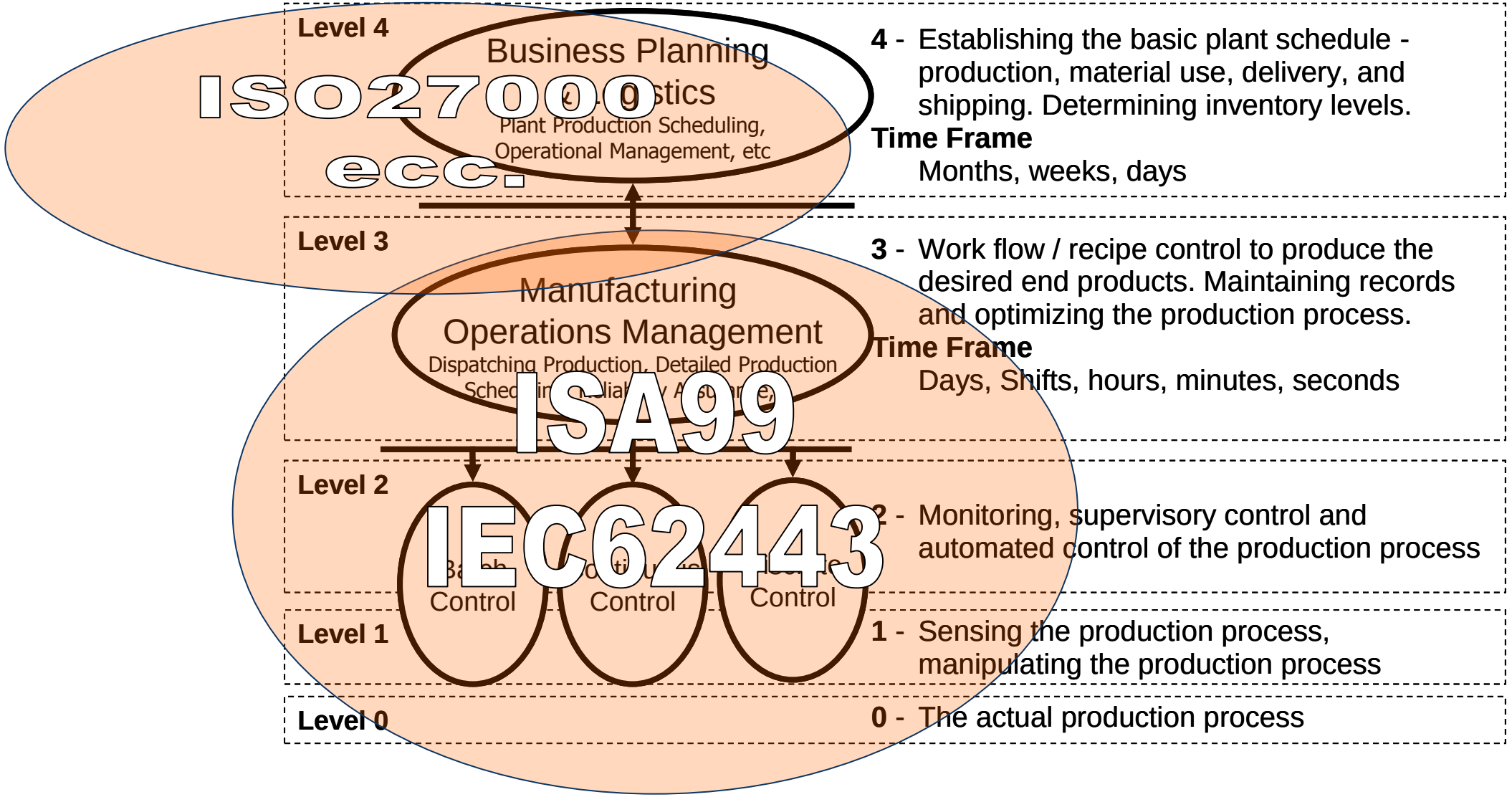
Visto che ora abbiamo tutti questi preziosi dati nell’Historian, vogliamo vederli!. Quindi creiamo un'interconnessione con la rete aziendale «corporate».

Vogliamo dei Client sulla rete aziendale in grado di visualizzare i dati in tempo reale dall'impianto

Gli ingegneri devono fare modifiche sulla workstation di ingegneria e cambiare altre impostazioni direttamente dal proprio desktop aziendale

Dobbiamo permettere a chi ci fa la manutenzione su PLC e SCADA di potersi collegare da remoto

ANSI/ISA95 Functional Hierarchy www.isa.org



Industria4.0, Convergenza IT – OT & il Cloud

Reshaping Industrial Controls

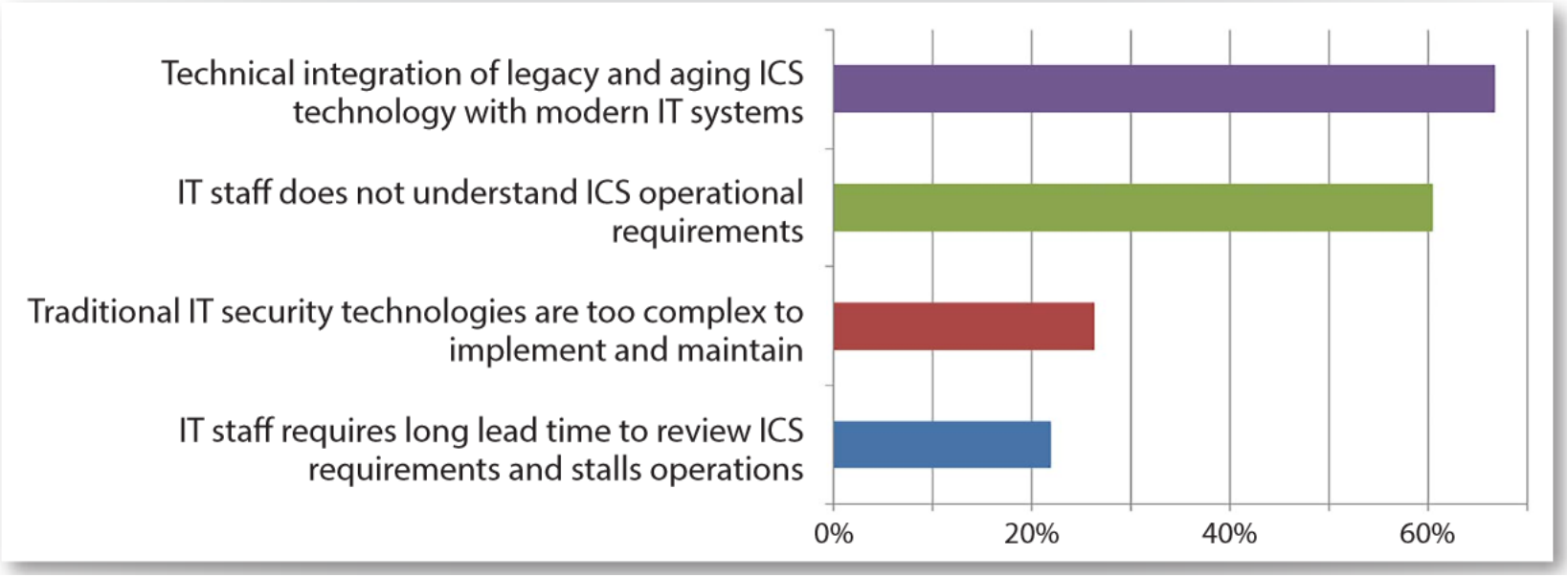
32%

of IIoT devices connect directly to Internet, bypassing traditional IT security layers.

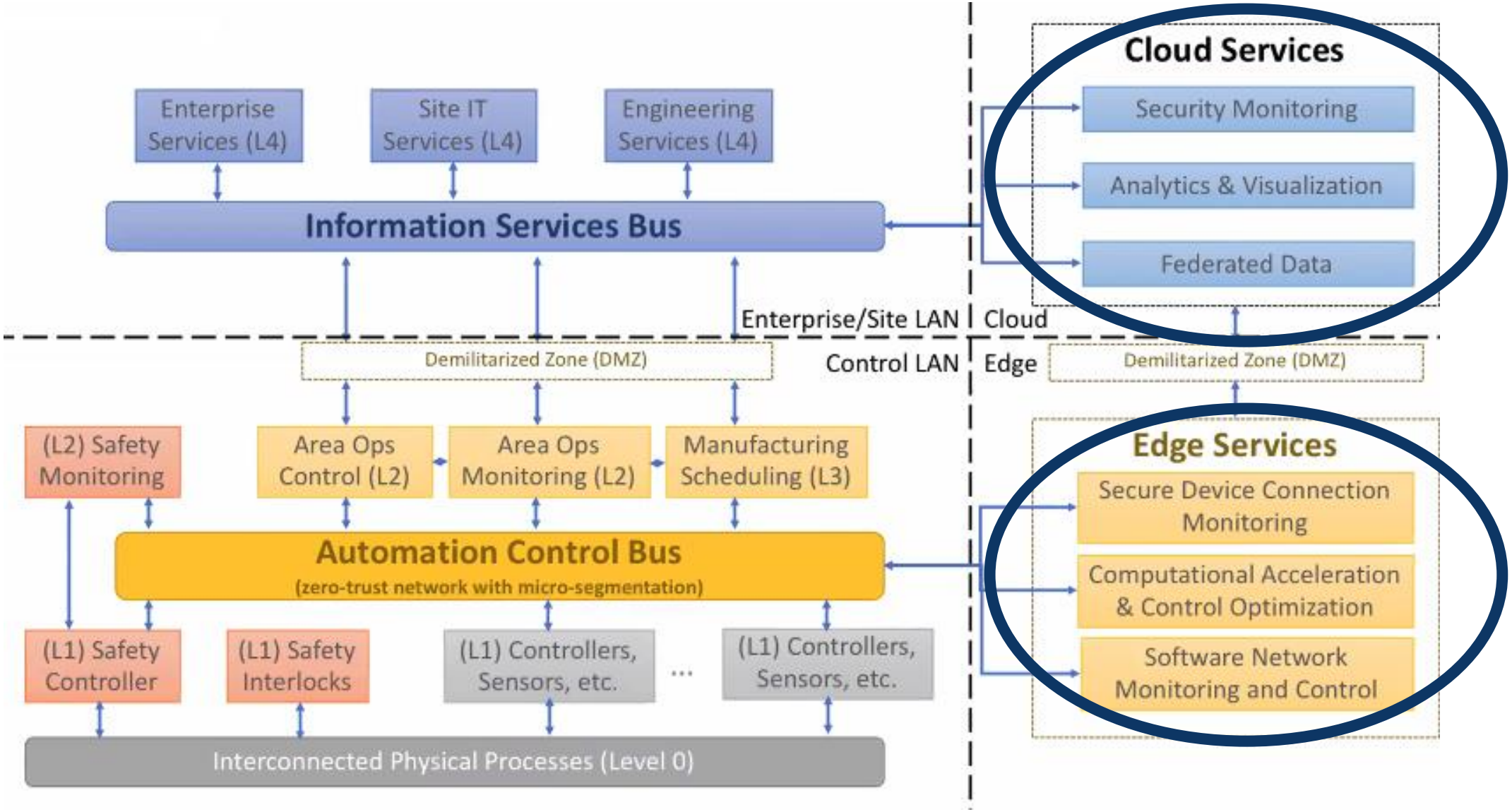
Le interfacce informatiche primarie con grandezze fisiche e elettriche, sensori, macchine e impianti, attuatori e trasduttori fisici delle logiche programmabili.

- **Sistemi deterministici**

What are the biggest challenges your organization faces in integrating IT and ICS technologies?



Sistemi OT/ICS, la rete di fabbrica, la rete Enterprise, Edge e il Cloud

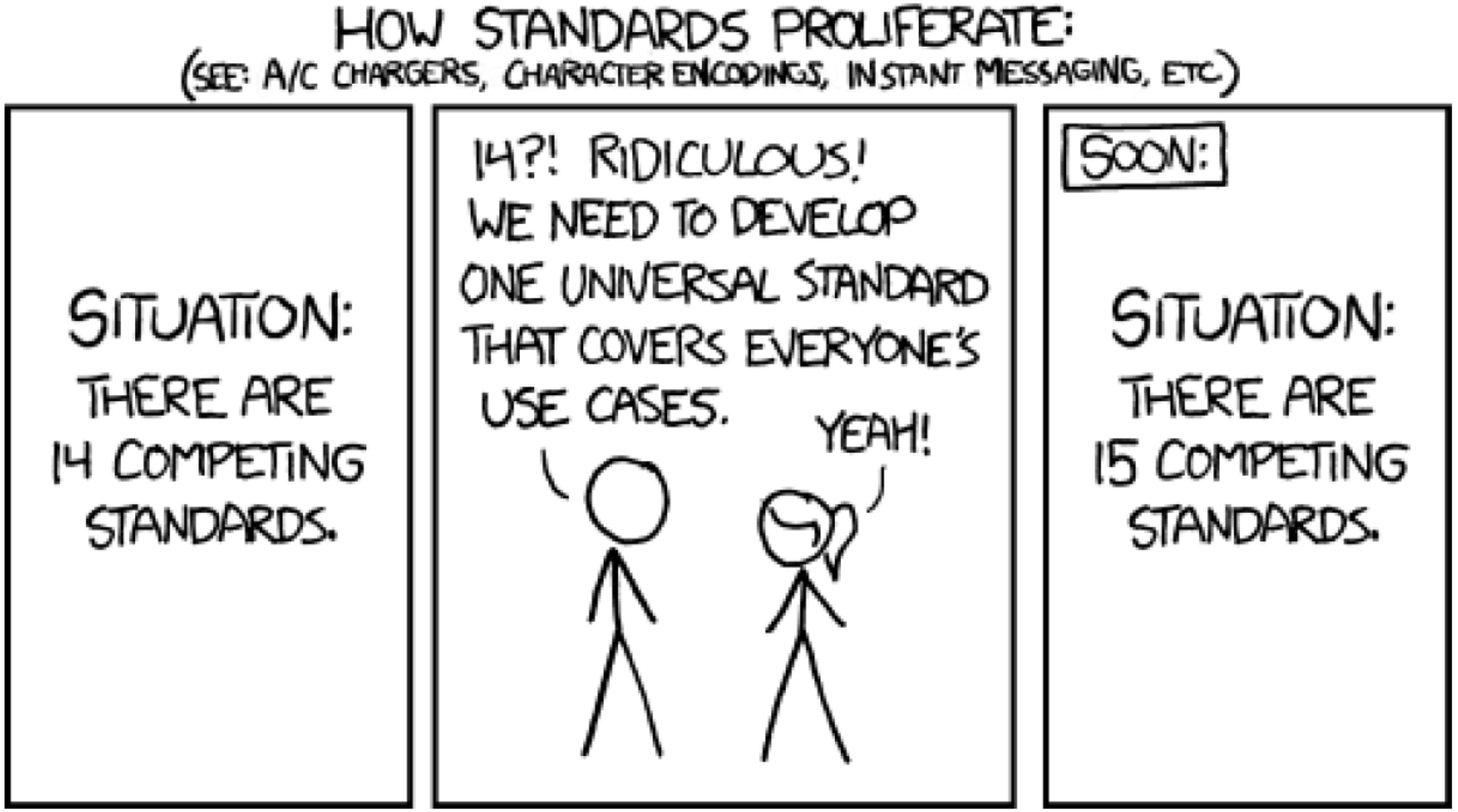


Fonte: Dragos/GE

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

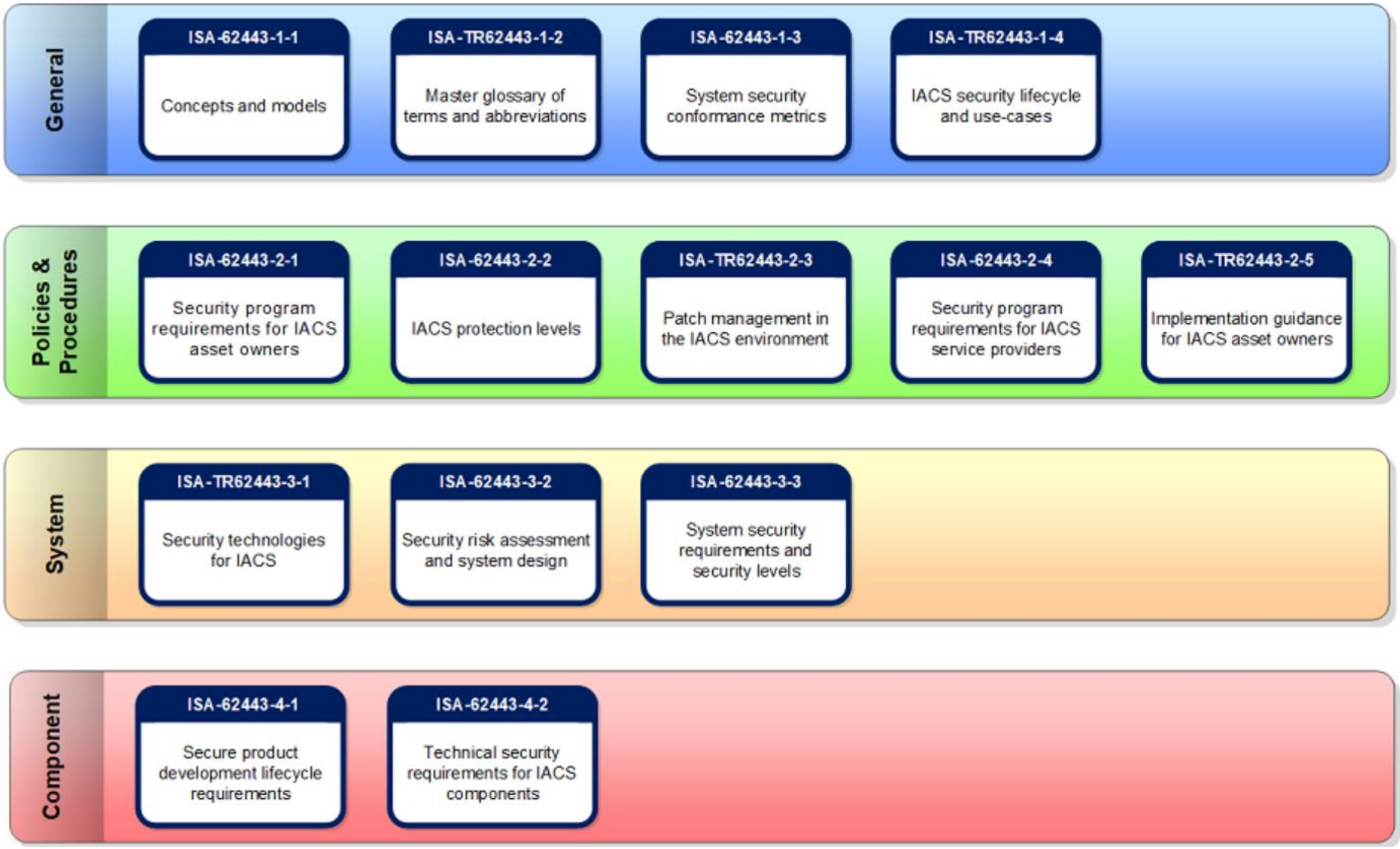
- DCS (Distributed Control Systems)
- PLC e reti di campo (Controllori programmabili)
- SCADA/HMI e reti di fabbrica
- Storicizzatori (**Historians**, **Database**, ecc.)
- **DNC/CNC, Robot, AGV**
- **MES, EBRS** e sistemi di gestione produzione, tracciabilità lotti, analisi efficienza, OEE, ecc.
- **LIMS,** 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**
- **…**

Quali sono gli standard per ICS/OT Cyber Security?

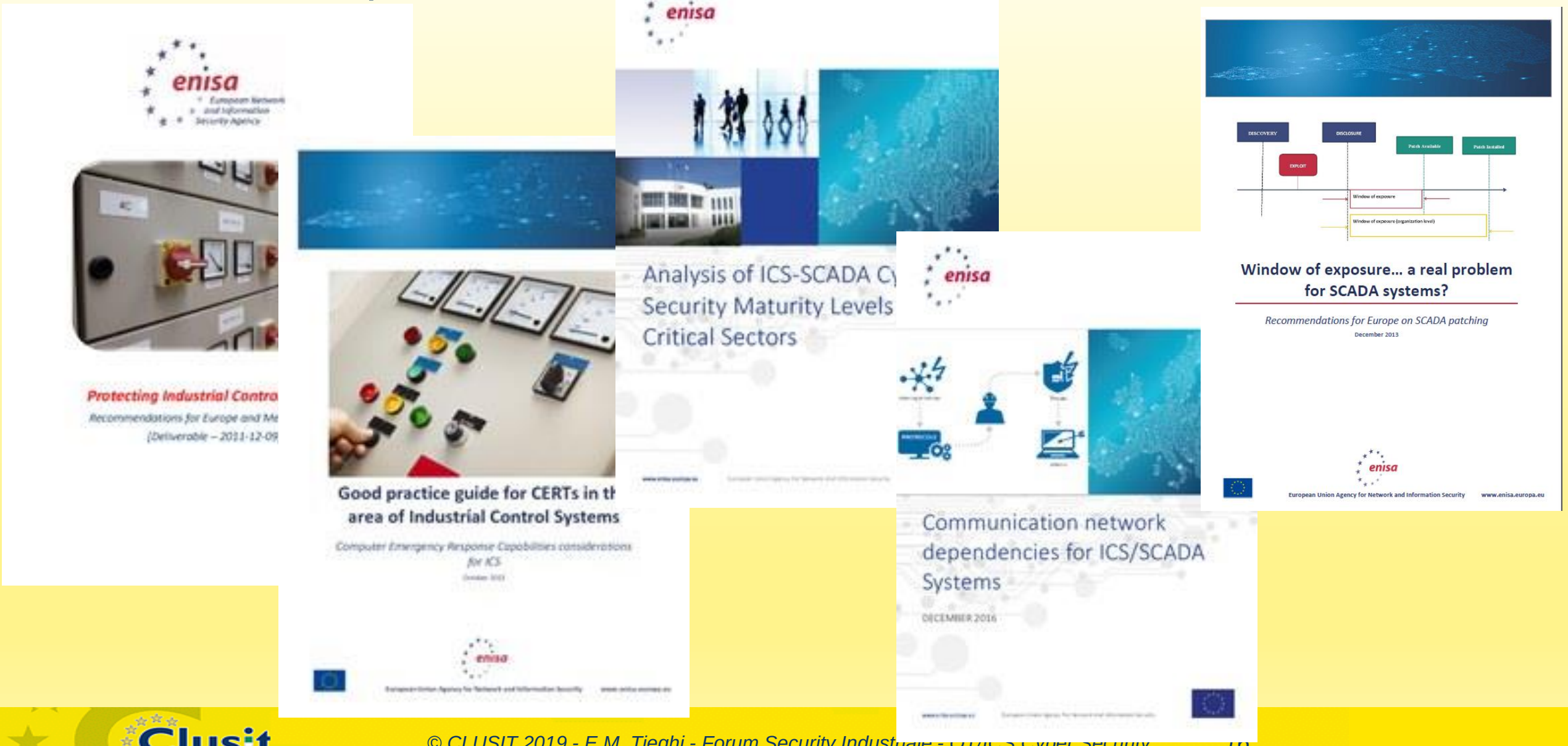


ng courtesy of XKCD[10]

ISA99-IEC62443 (www.isa.org/ISA99)



ENISA, Protecting ICS, ICS CERT, ICS Maturity Levels, Network Communication, Patch



NIST CSF (Cyber Security Framework) + SP800-82

SANS Institute: Reading Room | iec62443 - Cerca con Google | Cybersecurity Framework | NIST

https://www.nist.gov/cyberframework

Cerca

NIST

CYBERSECURITY FRAMEWORK [*Helping organizations to better u*

- **Framework** +
- **New to Framework** +
- **Perspectives** +
- **Success Stories** +
- **Online Learning** +
- **Evolution** +
- **Frequently Asked Ouestions** +

Credit: N. Hanacek/NIST

NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

ST MENU

isk

uidelines,
d risk.
e, and
ection and
rs

Proteggere IoT e IIoT: con quali standard?

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

COMPUTER SECURITY

enisa

Draft NISTIR 8200

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

repared by the Interagency International Cybersecurity Standardization Working Group.

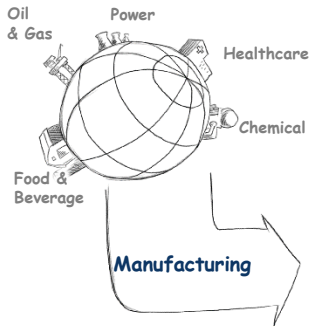
NIST Editors:
Mike Hogan
Ben Piccarreta
Information Technology Laboratory

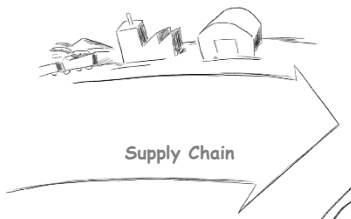
February 2018

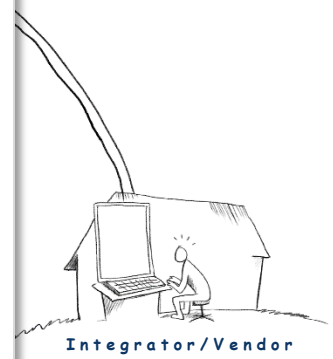
U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

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

IT Security vs OT/IIoT Security: Requirements







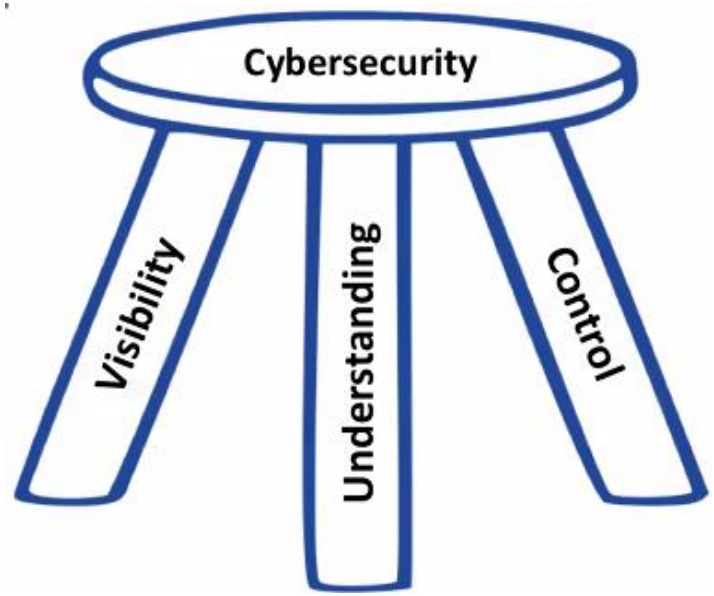
"Old" IT vs OT Priorities

1. **C**onfidentiality
2. **I**ntegrity
3. **A**vailability
4. Safety
5. Reliability
6. Product/Service Impacted

"New" IT/OT/IoT, IIoT Priorities

1. **A**uthentication
2. **A**vailability
3. **I**ntegrity
4. **C**onfidentiality
5. **N**on-**R**epudiation
6. Safety
7. Reliability
8. Product/Service Impacted

OT/ICS Cybersecurity vs. Cyber Hygiene



3 cose essenziali:

- Visibilità
- Capire cosa c'è e cosa succede
- Controlli

OT/ICS Cyber Hygiene: esempio 1

Visibilità per capire cosa c'è e succede

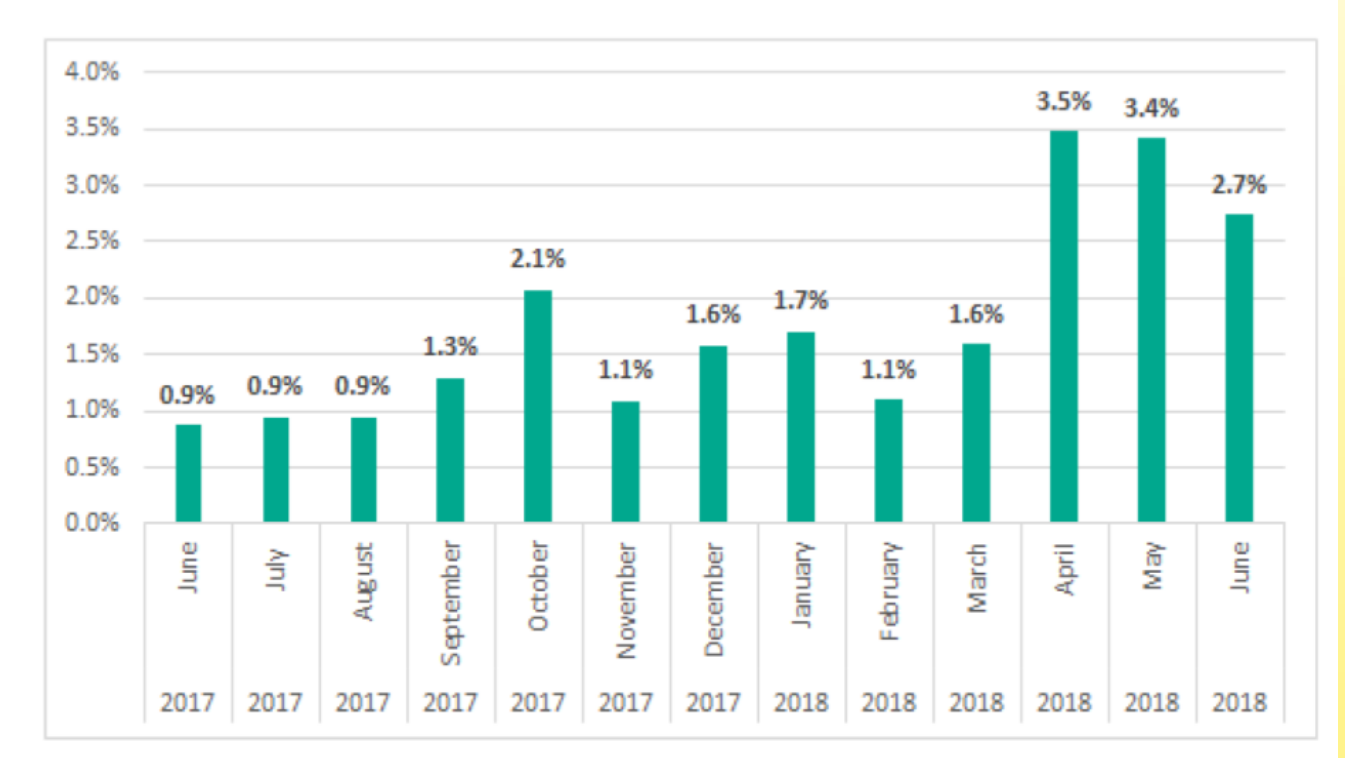
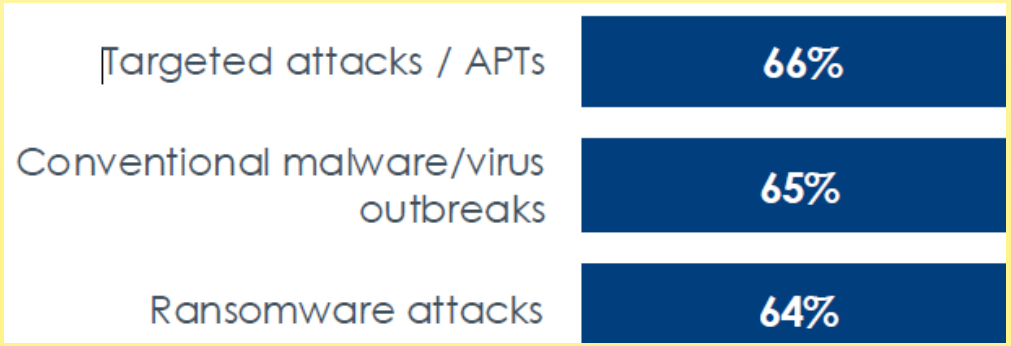


Figure 35: Share of ICS computers attacked by cryptomining malware

OT/ICS Cyber Hygiene: esempio 2

Controlli: Segmentazione e Segregazione

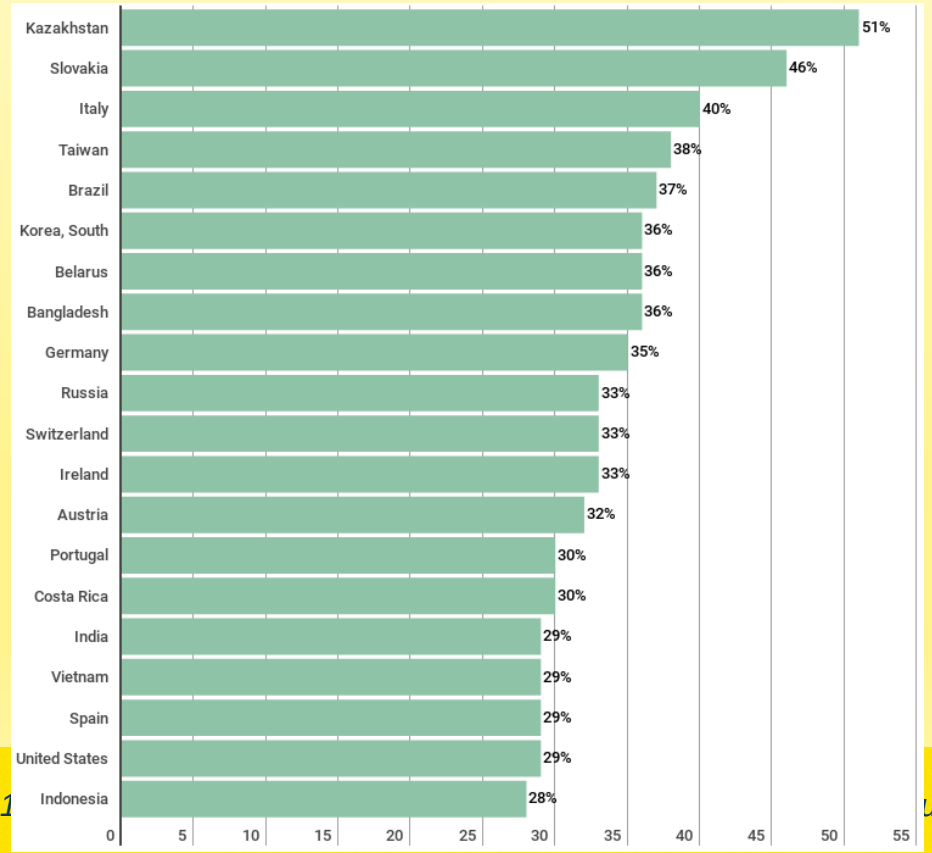
64% of the major incidents targeting industrial control systems or networks were ransomware.

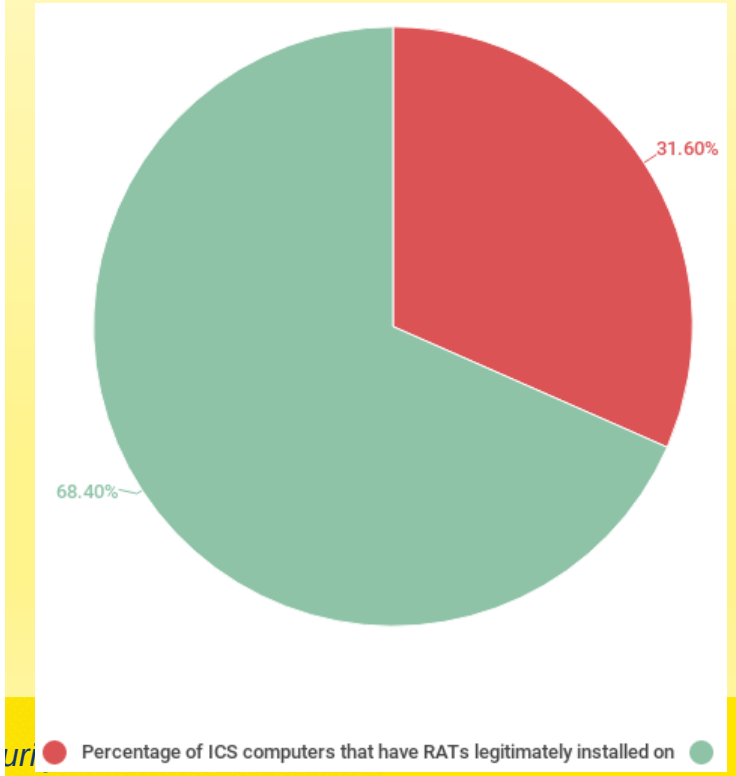


OT/ICS Cyber Hygiene: esempio 3

Remote Access Tools installati

Operational technology (OT) networks of industrial enterprises is a field of glory for espionage threat actors. These actors use remote administrator tools (RATs) which are already installed in the industrial control systems (ICS). (40% in Italia, solo 1 su 3 è legittimo e saputo)





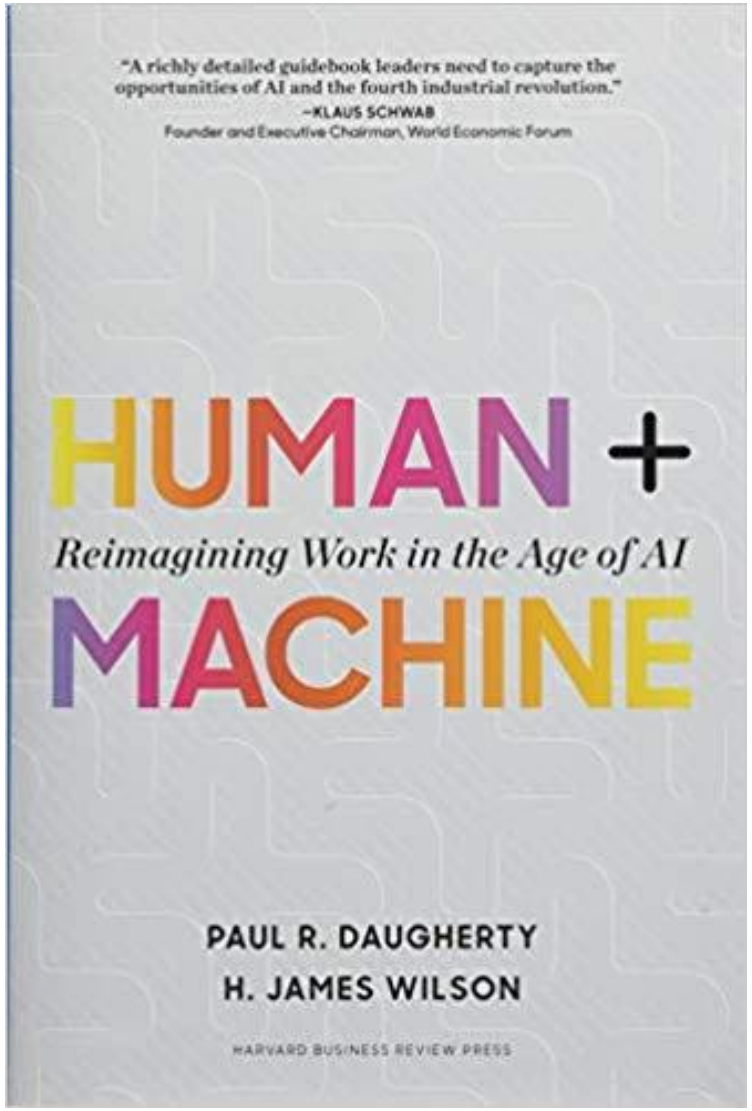
Servono tool e skill OT per proteggere ICS/OT o bastano quelli IT?

Table 5. Critical Drivers for IIoT Security and Rankings by Responsible Party

Driver		Overall Response	IT Team Rankings	OT Team Rankings
1	Protection of data (company, customer, vendor, other)	47.2%	1	6
2T	Protection of equipment and systems	40.5%	4T	3
2T	Protection against financial loss (assets, brand, company value)	40.5%	2	4T
4T	Compliance with industry regulations	36.0%	3	4T
4T	Increases in reliability, availability, efficiency, productivity	36.0%	4T	1
4T	Safety inside the operation	33.7%	6	2
7	Integration and synergistic alignment of IT and OT practices, policies and procedures	23.6%	7T	7T
8	Reduce corporate liability/improve enterprise risk management	16.9%	7T	9T
9	Safety outside of the operation	15.7%	9T	7T
10	Mitigate supply chain risks, both upstream and downstream	9.0%	9T	9T

Quelli IT sono sempre necessari, spesso non sono sufficienti.

Cybersecurity e tool: A.I. & Machime Learning



Sperimentazione di Intelligenza Artificiale in Diagnostica Medica:

- **A.I. da sola raggiunge il 92% delle diagnosi**
- **Il Medico fa meglio: è al 96%**
- **A.I.+Medico congiuntamente: si supera il 99,5% di diagnosi corrette**

Ma bisogna proprio proteggere anche le reti di fabbrica e IIoT?

Chiariamoci qualche dubbio su OT/ICS/IIoT Cyber Security

Enzo M. Tieghi, *Clusit*, Comitato Scientifico,
Controllo ed automazione in ambito Industriale & *Industrial IoT*

etieghi@clusit.it – http://www.clusit.it

Il Clusit, Associazione Italiana per la Sicurezza Informatica

Il Clusit, (www.clusit.it) nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Il Ruolo Istituzionale

- In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, CERT Nazionale e CERT PA , Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA .

I Rapporti Internazionali

- In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Network and Information Security), ITU (International Telecommunication Union), UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), European DIGITAL SME Alliance, le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC2, ISSA, SANS) e le associazioni dei consumatori.

I numeri del Clusit

- 500 Organizzazioni rappresentate
- 8.000 partecipanti alle attività del Clusit nel 2018

EVENTI - FORMAZIONE

- Eventi divulgativi organizzati nel 2018: circa 50
- Webinar e seminari tenuti nel 2018: più di 80
- Speaker e docenti coinvolti: più di 350
- Nel 2018 hanno partecipato agli eventi Clusit oltre 5.000 persone

PUBBLICAZIONI

- Documenti prodotti (rapporti, quaderni, pillole di sicurezza, White Papers): oltre 150
- Contributori/autori delle pubblicazioni Clusit: oltre 120
- Lettori delle pubblicazioni Clusit (rapporti, quaderni, pillole di sicurezza): oltre 80.000

.

- Copertura mediatica nel 2018: più di 300 articoli e servizi su web, cartaceo, Radio e TV.

Le Attività e i Progetti in Corso

- **CLUSIT Security Summit**: Milano (13-15 Marzo 2019), Treviso, Roma, Verona, la maggiore manifestaziuone italiana dedicata alla sicurezza delle informazioni, delle reti e dei sistemi informatici
- **Formazione specialistica**: i Webinar, 28 in programma per il 2019, di cui 14 dedicati ai DPO (Data Protection Officer)
- **Ricerca e studio**: Premio “Innovare la Sicurezza delle Informazioni” per la migliore tesi universitaria, arrivato alla 14a edizione.
- **Le Conference specialistiche**: Security Summit (Milano, Treviso , Roma e Verona).
- **Produzione di documenti tecnico-scientifici**: i Quaderni CLUSIT e le Pillole di Sicurezza.
- **Gruppi di Lavoro su**: ROSI - Ritorno dell’investimento in sicurezza informatica; FSE - Fascicolo Sanitario Elettronico; CCE - Cartella Clinica Elettronica; Sicurezza nei Social Networks; Frodi; Mobile; Privacy; Cloud Security; Industria 4.0 e Protezione di reti e sistemi di controllo in ambito industriale.
- **Focus per il 2019**: **Intelligenza Artificiale, Blockchain, IoT.**
- **Progetto Scuole**: la Formazione sul territorio.
- **Rapporti Clusit**: Rapporto annuale sugli eventi dannosi (Cybercrime e incidenti informatici) in Italia; analisi del mercato italiano dell’ICT Security; analisi sul mercato del lavoro.
- **Il Mese Europeo della Sicurezza Informatica (ECSM)** , iniziativa di sensibilizzazione promossa e coordinata ogni anno nel mese di ottobre in Italia da Clusit, in accordo con l’ENISA e con Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Milano 12-13-14 Marzo 2019

https://securitysummit.it/

Tre giornate con focus su:

- 12 marzo, Cyber Crime,
- 13 marzo, Sicurezza del e nel Cloud,
- 14 marzo, A.I. e a Blockchain.