Tavola Rotonda
Manufacturing Security Summit 2021

Modera:

***Enzo M. Tieghi**, CS Clusit*

7 ottobre 2021 orario 10.00-12.30 - Security Summit Vertical

#securitysummitvertical

Tavola Rotonda

Manufacturing Security Summit 2021

Intervengono:

***Andrea Provini**, Presidente AUSED*

***Fabio Massimo Marchetti**, Vice Presidente ANIE Automazione con delega alla digitalizzazione*

***Andrea Boraschi**, Presidente ANIPLA*

***Mirco Marchetti**, Prof. CRIS Università degli Studi di Modena e Reggio Emilia*

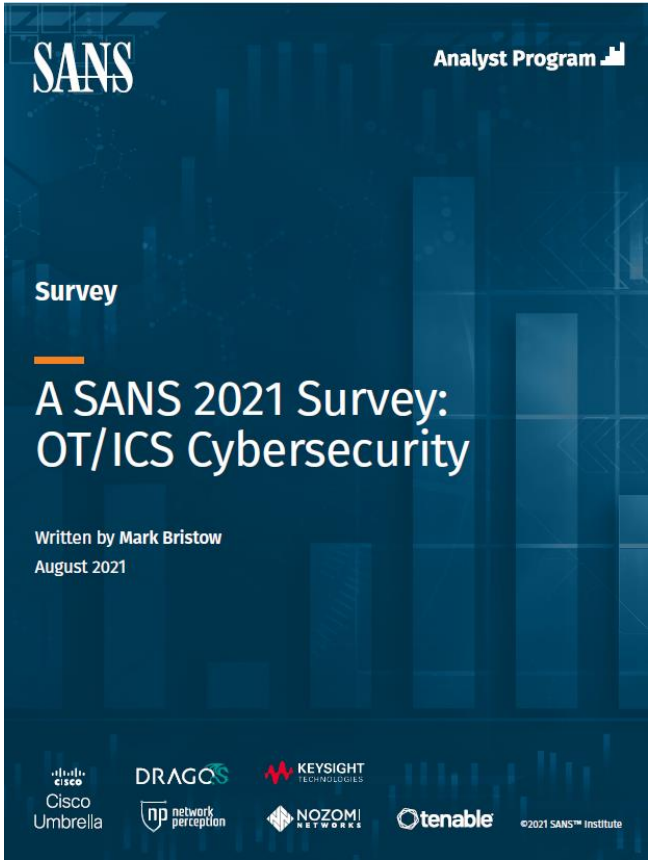
7 ottobre 2021 orario 10.00-12.30 - Security Summit Vertical

#securitysummitvertical

Enzo M. Tieghi

COMITATO SCIENTIFICO CLUSIT,
CONTROLLO ED AUTOMAZIONE IN AMBITO INDUSTRIALE, INDUSTRIAL IOT

HTTPS://IT.LINKEDIN.COM/IN/ETIEGHI



Survey Annuale di SANS su OT/ICS Cybersecurity:
nel 2021 quasi 500 intervistati e quasi 1300 Plants
(30% in Europa)

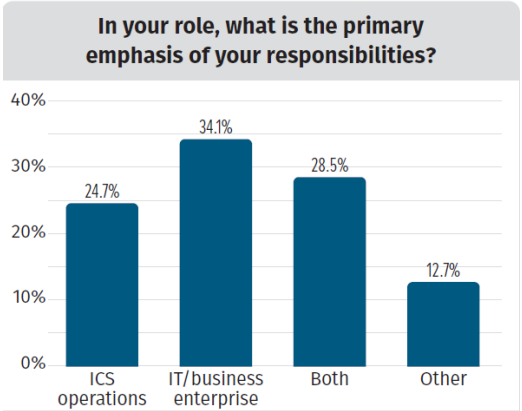


Figure 1. IT/OT Role Focus

https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

1) Attenzione / Visibilità :
Ha subito incidenti sui sistemi di controllo OT negli ultimi 12 mesi?

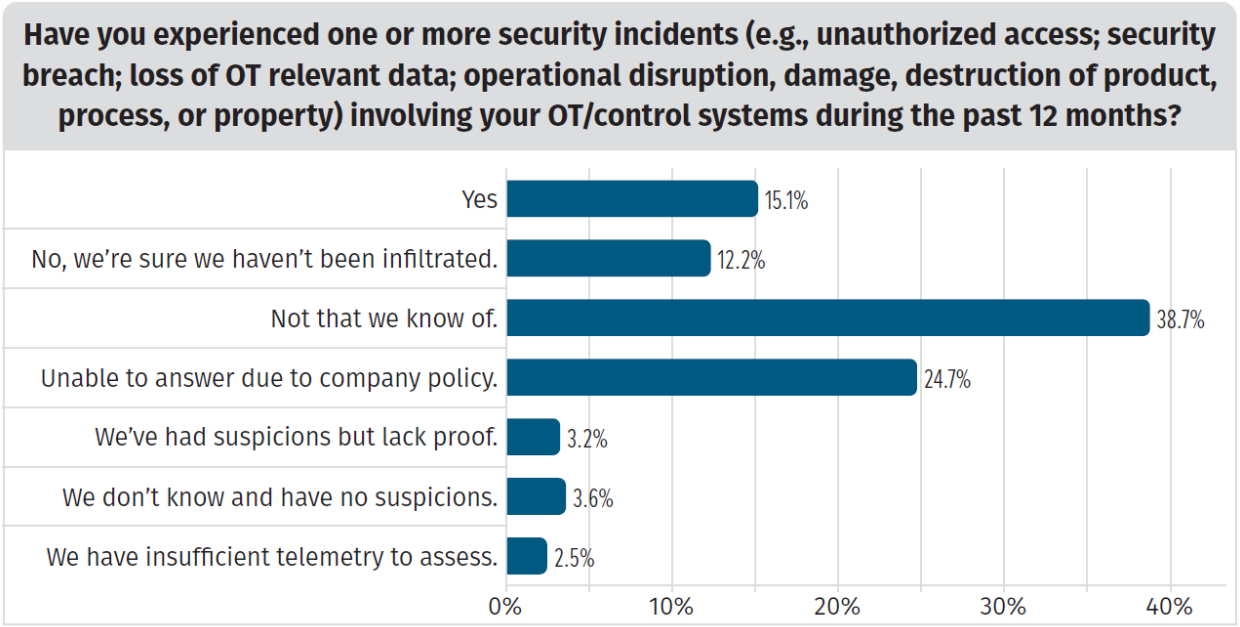


Figure 8. Incidents in the Past 12 Months

37,8 + 3,2 + 3,6 + 2,5 =

48% Non sa / non si è accorto se ha avuto incidenti

2) OK incidenti, ma quanti?
… e con quale impatto ?

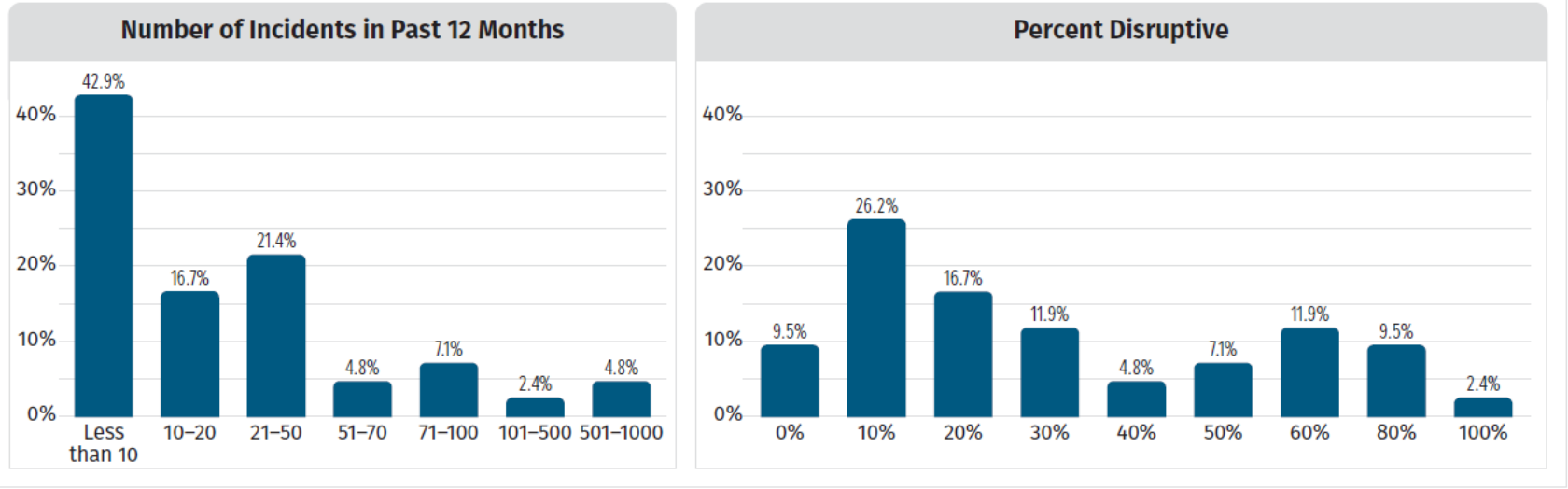


Figure 9. Incident Frequency and Process Disruption

Quasi il 60% ha subito più di 10 incidenti in un anno
Quasi il 90% ha avuto ripercussioni in Produzione

3) Quali le minacce più presenti ?
Ransomware al 54,2%,
e sono sempre alte quelle «interne», sia accidentali che intenzionali

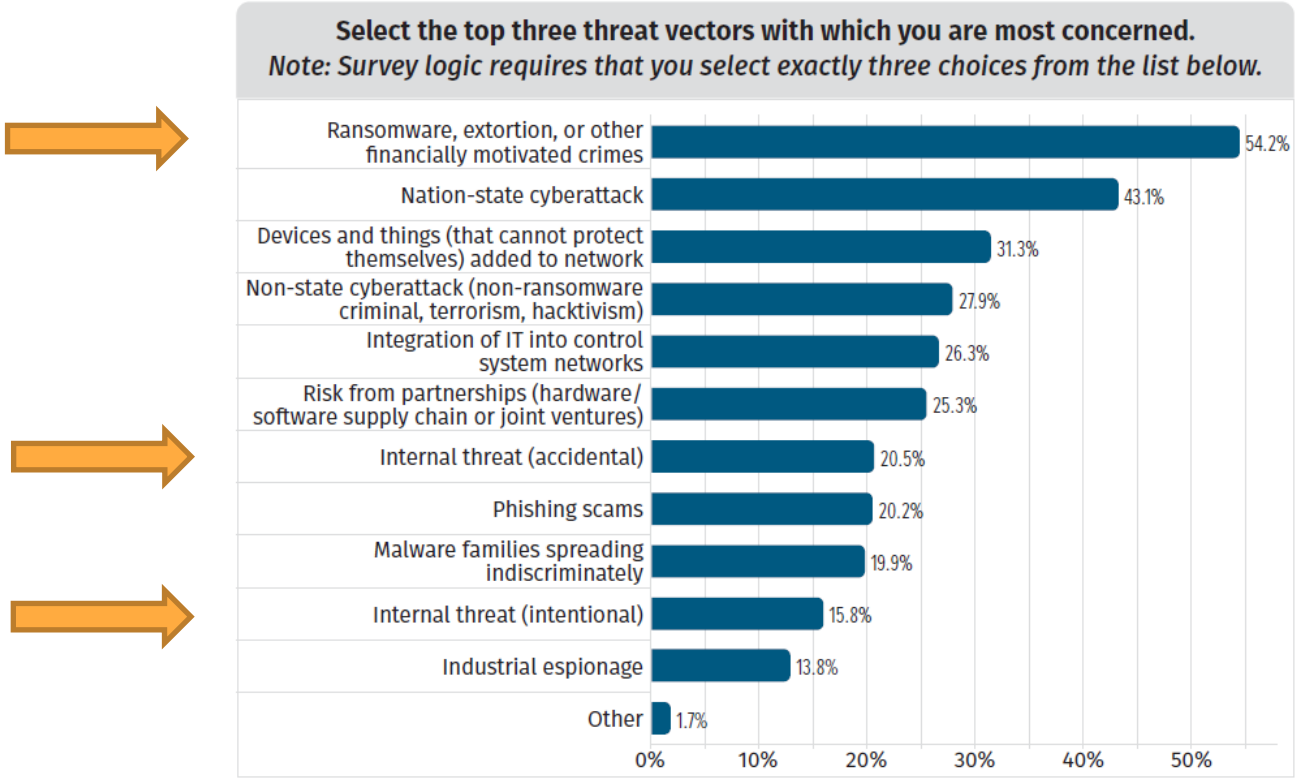


Figure 5. Top Threat Vectors

4) Cloud in Fabbrica: ormai lo usa il 40%,
…. e il 49,2% di questo con anche «funzioni operative»

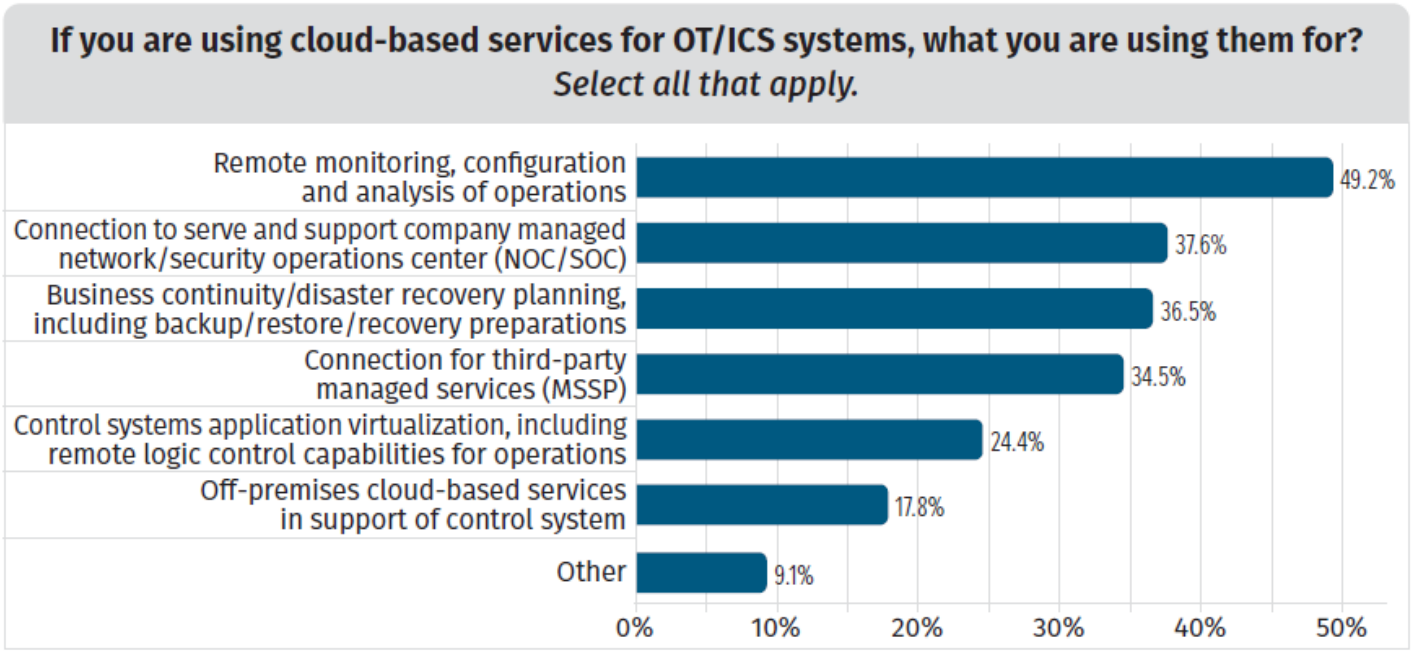


Figure 15. Functional Use of Cloud Technologies

Draft NISTIR 8374

Cybersecurity Framework Profile for Ransomware Risk Management

William C. Barker
Dakota Consulting
Silver Spring, MD

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374-draft

September 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

NIST su Gestione del Rischio Ransomware:

Public comment period *September 8, 2021* through *October 8, 2021*

5) Ma in Azienda, chi si occupa della OT/ICS Cyber Security?

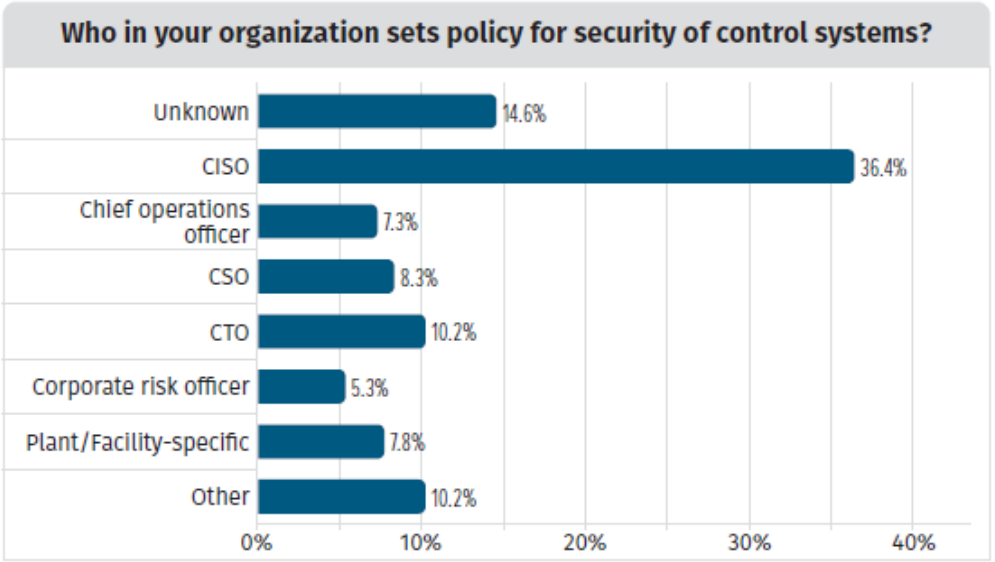


Figure 28. Security Policy Responsibility

Figure 29. Security Control Implementation

Rapporto CLUSIT 2020
La gestione dell'OT Security- La Survey dell'Osservatorio Information Security & Privacy:

- **Quasi 700 CIO/CISO intervistati**
- **180 Grandi Aziende**
- **501 PMI**

Alcuni dati:

- **68% fa Audit di OT Security**
- **60% ha contromisure OT Sec**
- **15% senza alcun presidio OT Sec**
- **52% non ha skill specifiche OT**

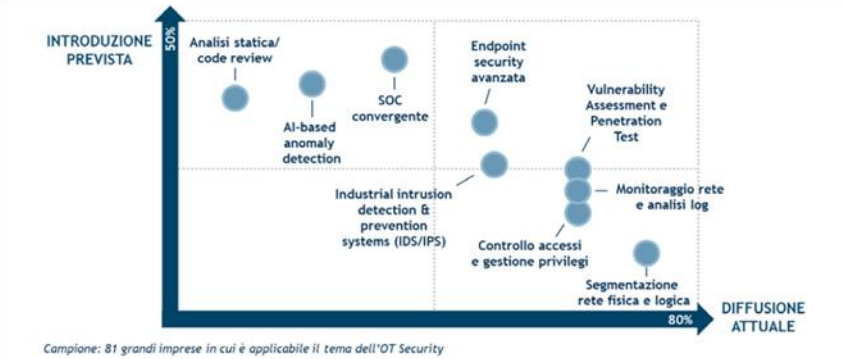


Figura 1: *Gli strumenti e le tecnologie adottate – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

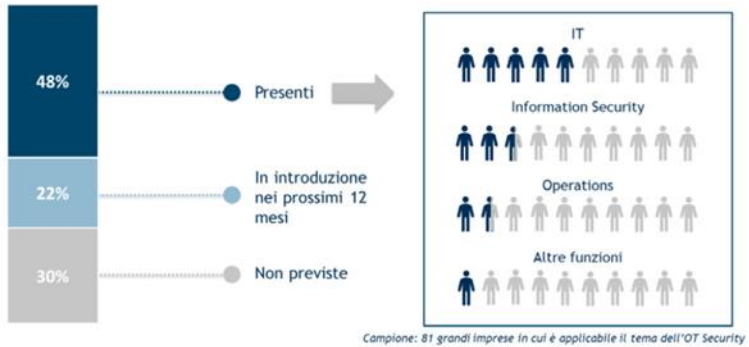
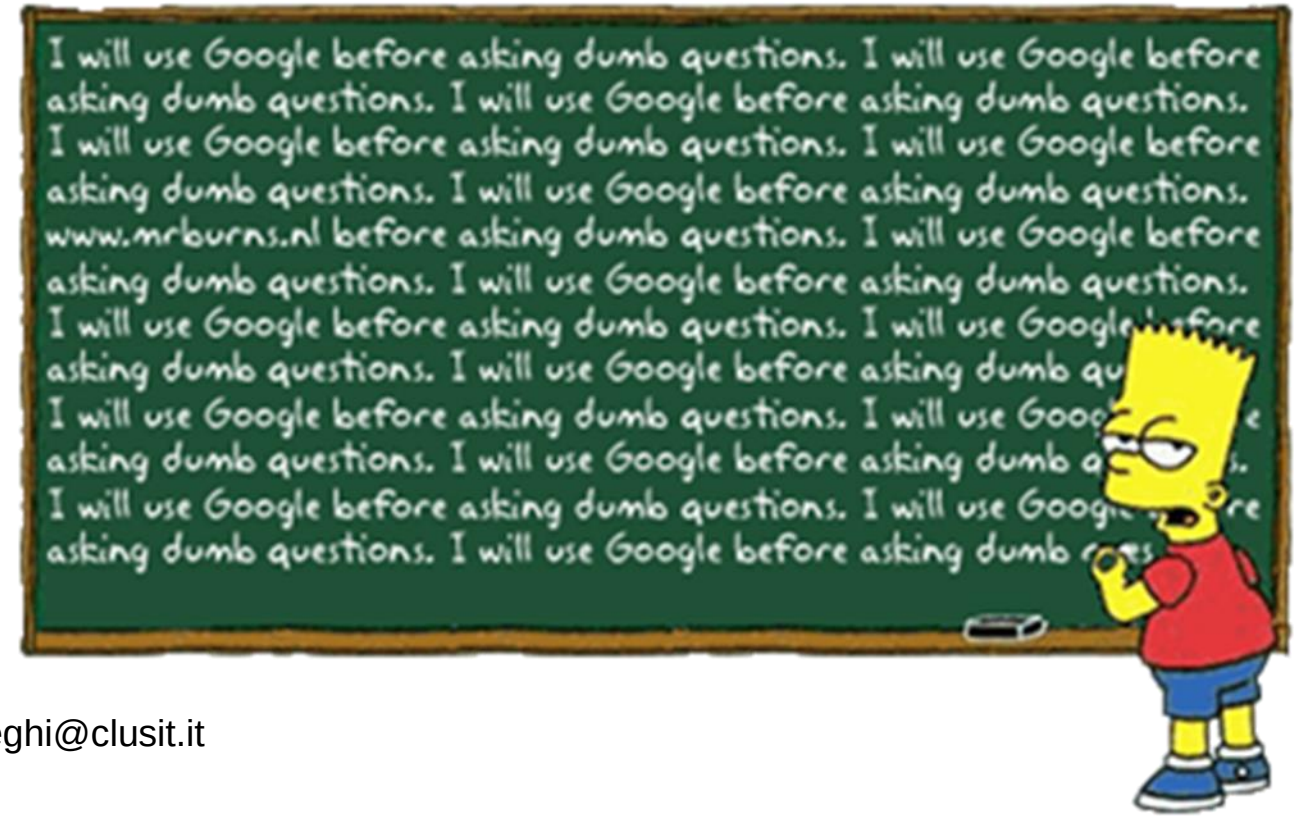


Figura 2: *Le figure specializzate in OT Security – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Domande? Dubbi?



Enzo M Tieghi – etieghi@clusit.it

“Industrial cybersecurity. Criticità ed evidenze”

Fabio Massimo Marchetti
Vice Presidente ANIE Automazione con delega alla digitalizzazione

Federazione ANIE

Federazione Nazionale Imprese Elettrotecniche ed Elettroniche

- **13** Associazioni
- **1.500** imprese
- **84** Mld € di fatturato aggregato
- **500.000** addetti
- **4%** del fatturato investito in R&S

ANIE Automazione

- L'Associazione rappresenta i **fornitori di componenti e sistemi per l'automazione industriale** manifatturiera, di processo e delle reti
- **Oltre 100** imprese
- **4,5** Mld € di fatturato aggregato
- I Gruppi operanti in ANIE Automazione lavorano su due aree principali: **Prodotto** e **Sistema**

PRODOTTO
AUTOMAZIONE DI PROCESSO
AZIONAMENTI ELETTRICI
COMPONENTI E TECNOLOGIE PER LA MISURA E IL CONTROLLO *(WG WIRELESS, NETWORKING, RFID, ECONDER, SAFETY, VISIONE)*
HMI-IPC-SCADA
PLC-I/O

SISTEMA
MECCATRONICA *(QUADRI BORDO MACCHINA, RIDUTTORI)*
SOFTWARE INDUSTRIALE
TELECONTROLLO DIGITALIZZAZIONE RETI E APPLICAZIONI DISTRIBUITE
OPC UA
5G
TELEMATICA APPLICATA A TRAFFICO E TRASPORTI

Gruppo Software Industriale

Il Gruppo è composto da una trentina tra le più importanti imprese del settore e si pone i seguenti obiettivi:

Redigere linee guida
per l'implementazione di tecnologie abilitanti 4.0 e benefici derivanti dall'utilizzo di soluzioni software avanzate, anche attraverso la pubblicazione di **«libri bianchi»**

Definire modelli di calcolo del ROI
con riferimento ad aree applicative specifiche

Aiutare a comprendere
e utilizzare gli **acceleratori di ROI** disponibili (incentivi di legge)

Organizzare eventi di divulgazione
sui temi relativi al software industriale e in particolare organizzare un **forum** di riferimento per questa tecnologia abilitante

forum Software Industriale

Industria 4.0: un mondo in transizione

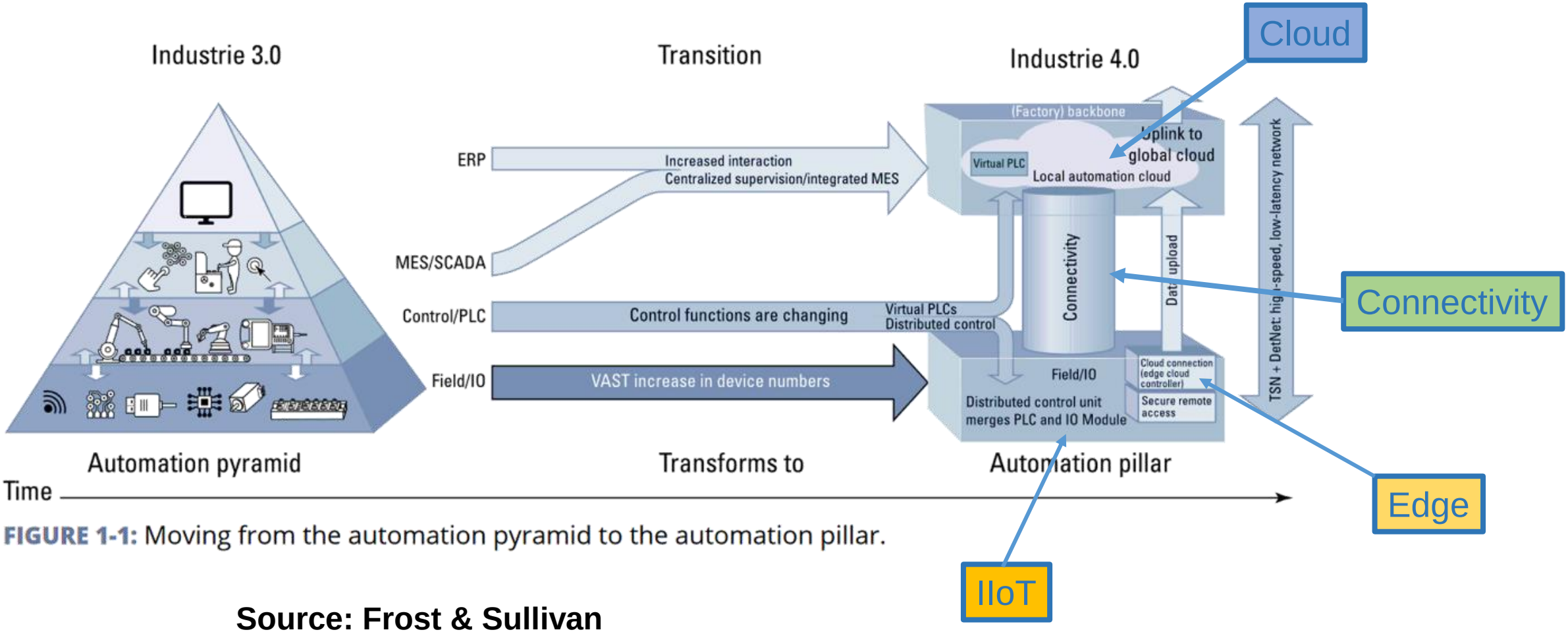
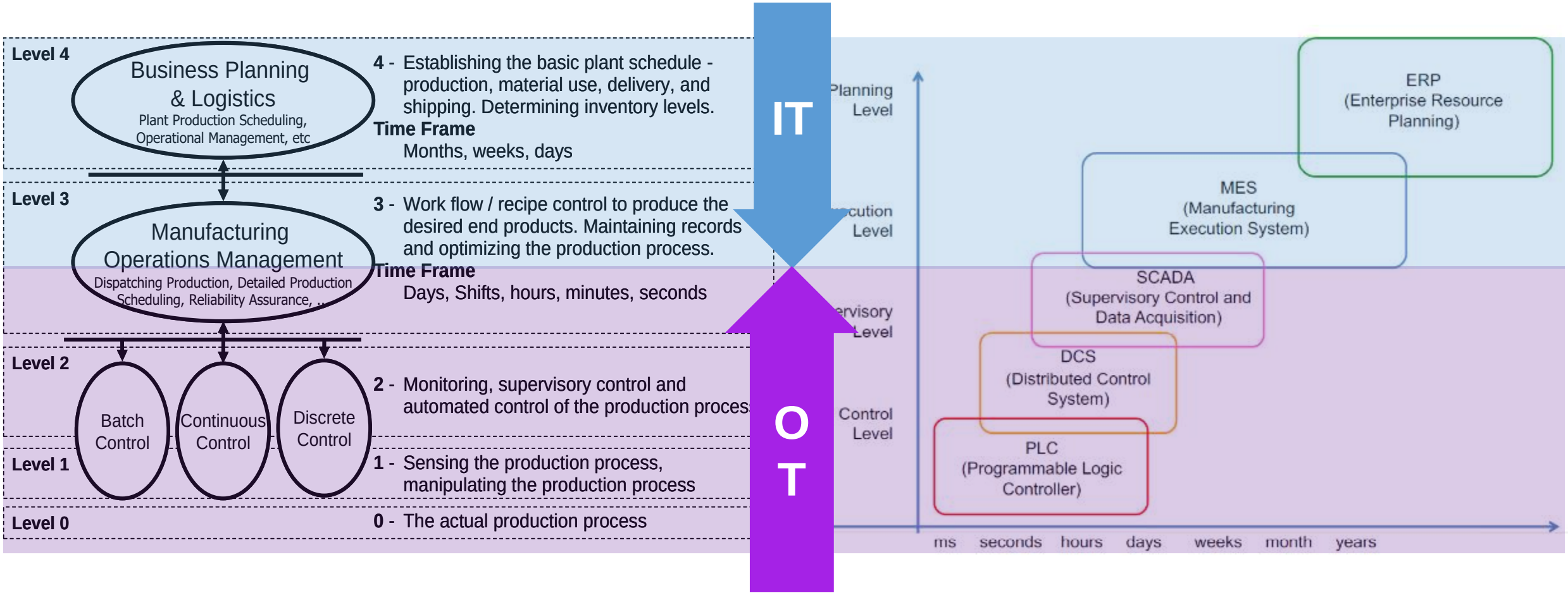


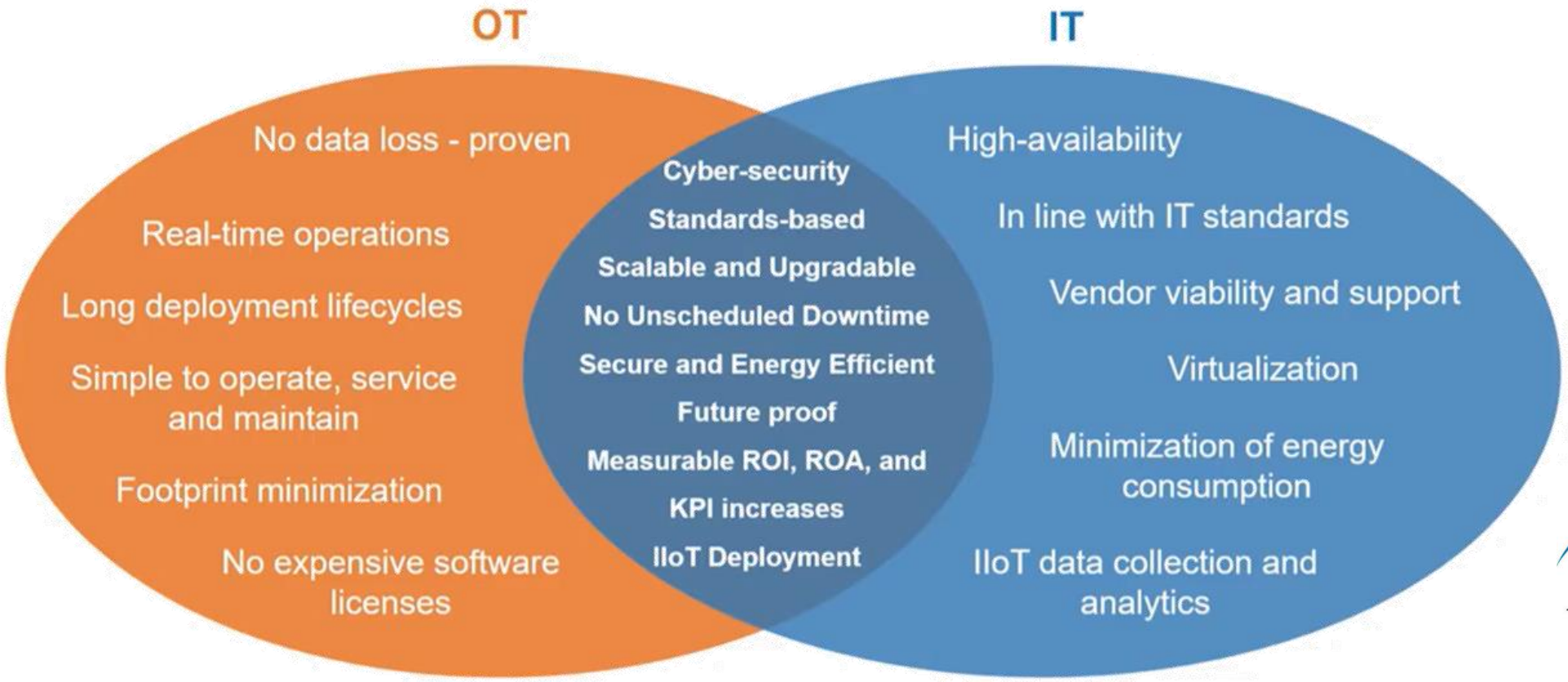
FIGURE 1-1: Moving from the automation pyramid to the automation pillar.

Source: Frost & Sullivan

Gestione processi e gestione produzione due mondi convergenti



IT e OT un rapporto complesso (cultura, risorse, organizzazione e processi)



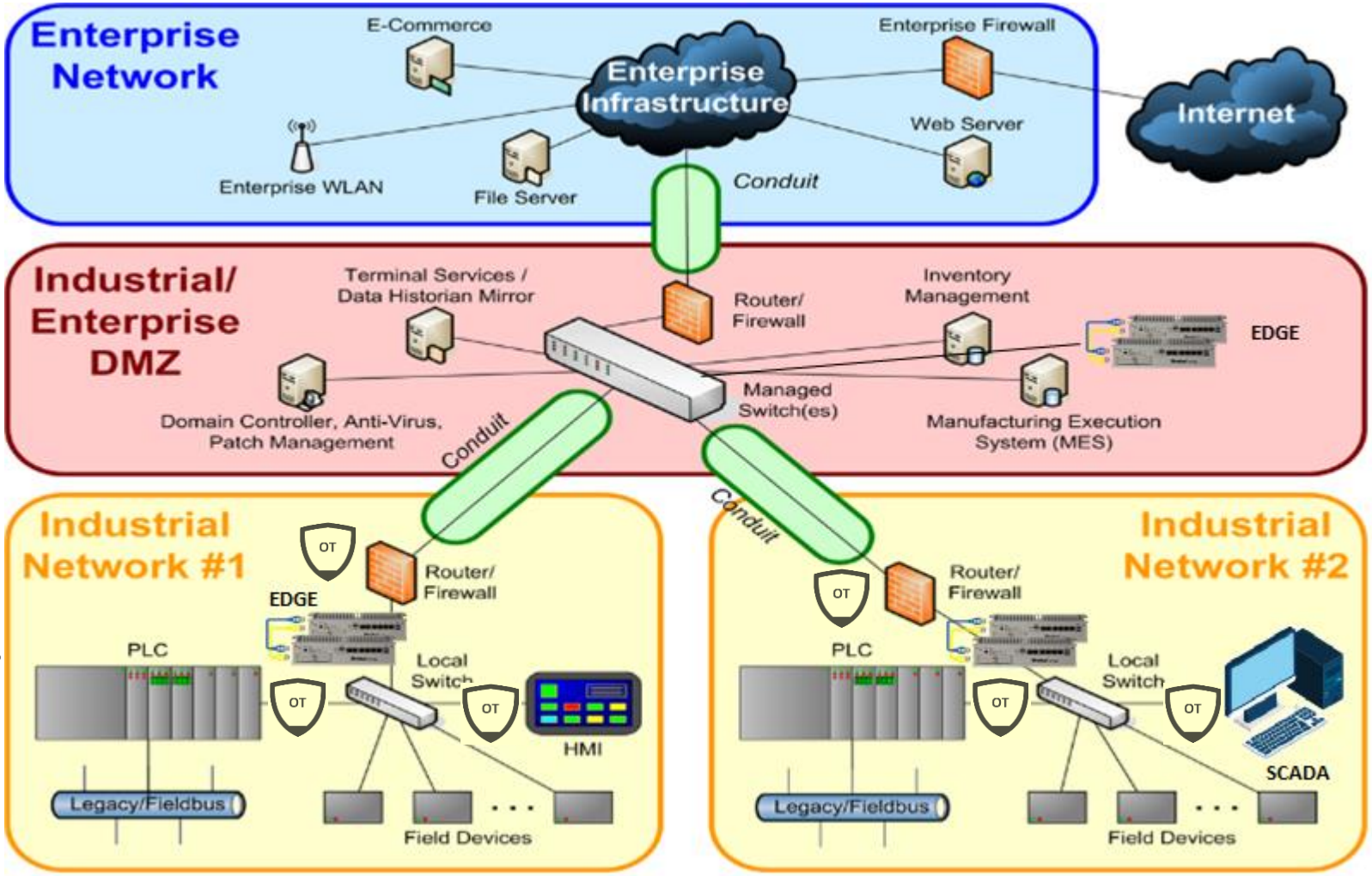
ARC Advisory Group

ANIE AUTOMAZIONE

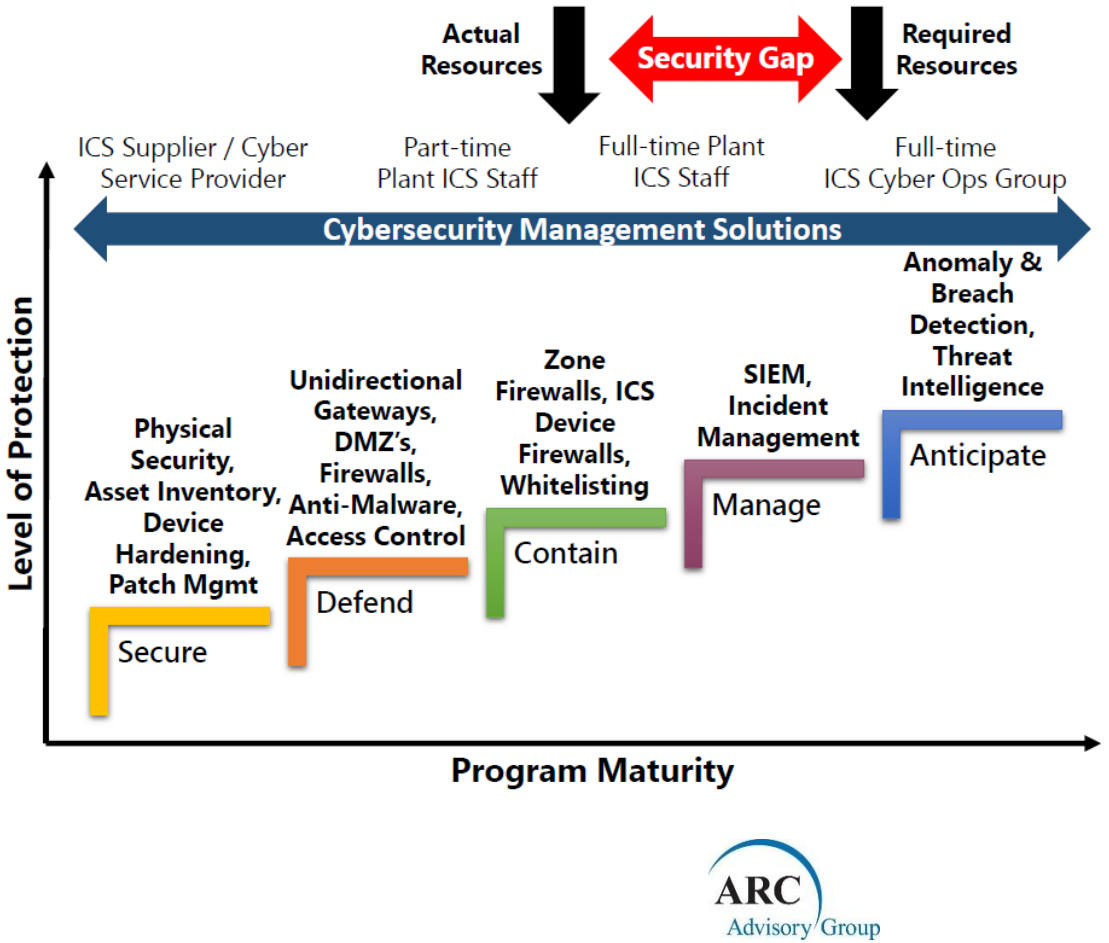
Alcuni «cyber-ingredienti» per l'integrazione IT/OT

- Cybersecurity Posture Assessment
- Cybersecurity Target Definition
- Segmentazione e segregazione
- Vulnerability Detection
- Anomaly Detection
- Continuous Improvement

- **IEC 62443**
- **NIST Cyber Security Framework 1.1**
- **NIST Special Publication 800-82**
- **ISO/TR22100-4:2018**



Gestione delle risorse in funzione degli Obiettivi



ARC Advisory Group

Security Level	Description	Target	Skills	Motivation	Means
SL1	Capability to protect against casual or coincidental violation	Misconfiguration	No awareness	Confusion	No ojective
SL2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation	No security measures implemented, hacker	Basic	Low	Straight forward
SL3	Capability to protect against intentional violations using sophisticated means with moderate resources, IACS specific skills and moderate motivation	Only moderate security measures implemented, high level hacker	Industrial specific	Average	Intentional
SL4	Capability to protect against intentional violations using sophisticated means with extended resources, IACS specific skills and high motivation	Economical Damage	Industrial specific	High	Aggressive

IEC 62443

Table 2: Security Levels Categorization

Maturity Level	Category	Description
ML 1	Initial	Capability of performing a service without a documented process that is poorly controlled
ML 2	Managed	Capability of performing a service in a formal documented characterized process with evidence of expertise and trained personnel
ML 3	Defined	Capability of performing ML2 level including evidence of practicing the process e.g. Documented process plus list of participants in the training of personnel
ML 4	Improved	Capability of performing ML3 level including demonstration of continuous improvement e.g. internal audit report

IEC 62443

Table 3: Maturity Levels Categorization and description

ANIE AUTOMAZIONE

ANIPLA

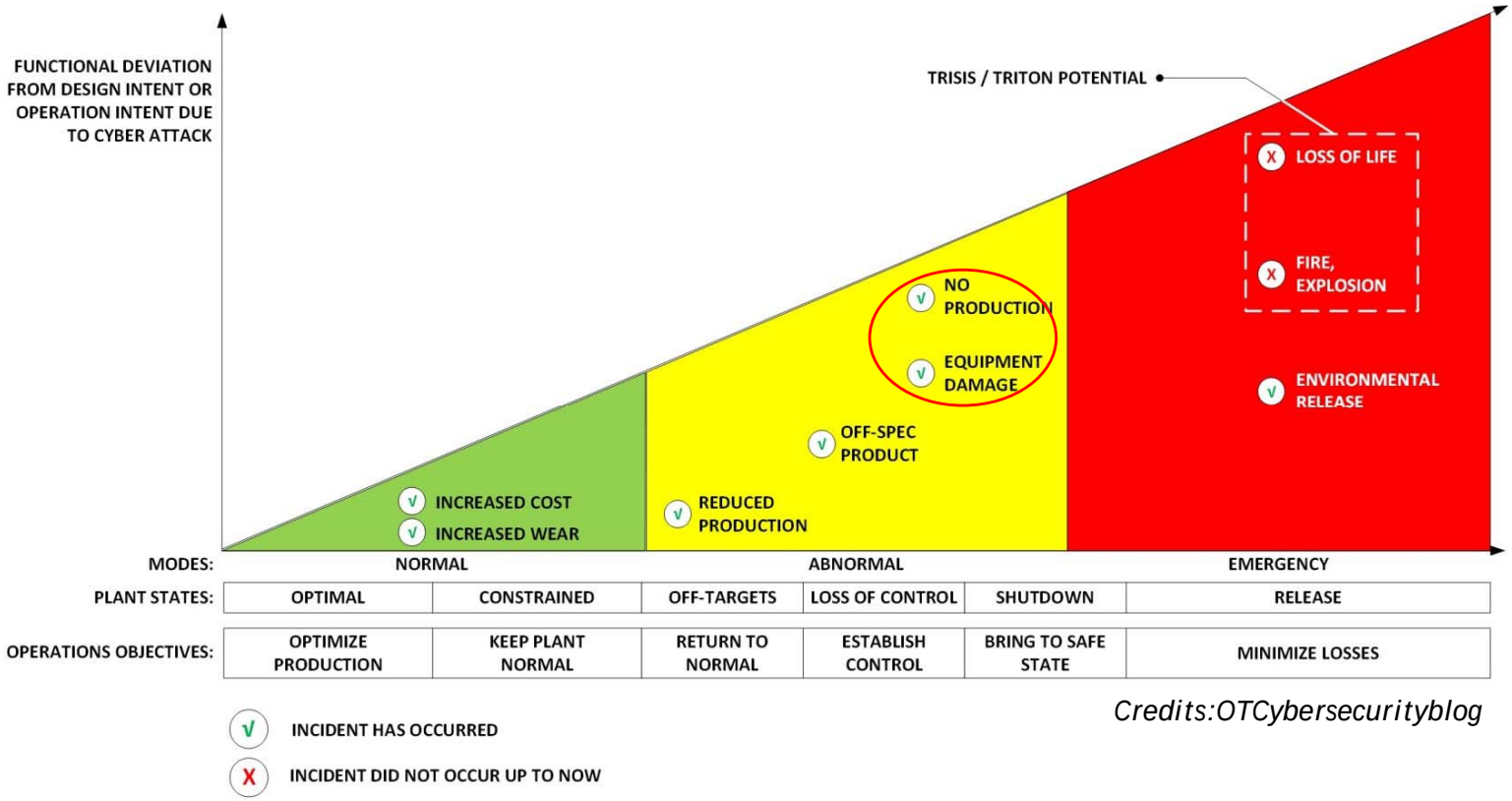
Associazione **N**azionale **I**taliana **P**er **L**'**A**utomazione

Functional Security in Project Engineering Design

Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

To Start

Why Functional Security or Cybersecurity



Credits:OTCybersecurityblog

- Cyber Kill Chain
- Time lag between infection and attack
- Detection strategies and means shall be different with respect to infection "maturity"
- Experience and use cases instruct on how the risk shall be managed and technically addressed

OT Systems in Plants are weak links which must be hardeded

=>Procedures & Standards
=>Devices and tech. solutions
=>People

Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

To Start

Cybersecurity Risk

- Cybersecurity represents the set of security controls and strategies able to mitigate the risk which is a function of a given threat source exercising a potential vulnerability and the resulting impact of the event on the organisation

Cyber Security Risk
=
(Threat likelihood x Vulnerability) x Consequence

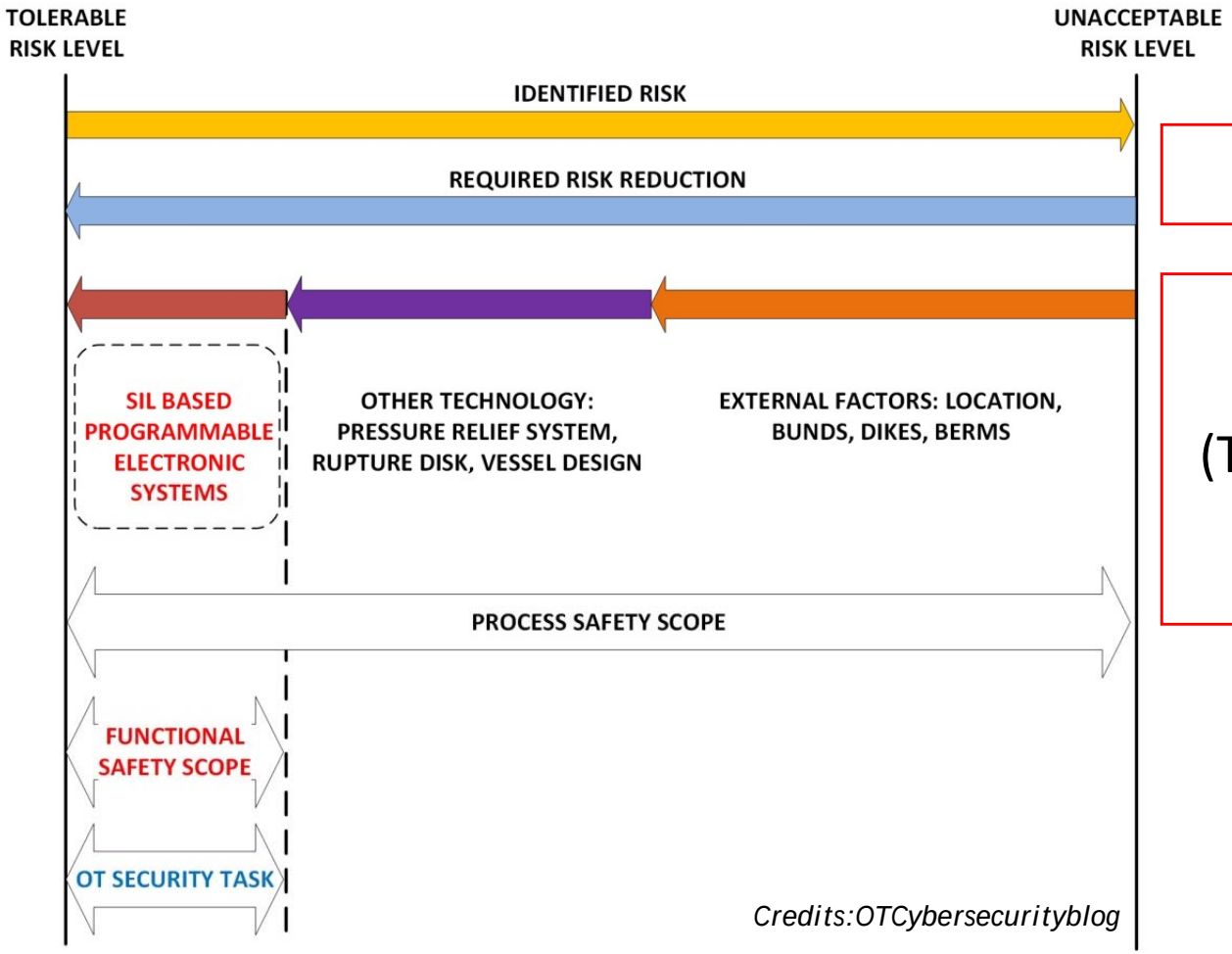
NIST SP800-30

- It provides means of prevention of illegal (wilfull) or unwanted penetration, intentional or unintentional interference with the intended operation, inappropriate access to confidential information in networked systems of Operational Technology system (OT)

ANIPLA
Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

Cybersecurity (or Functional Security)

Functional Security and Safety



Risk= Likelihood x Consequence

Security Risk
=
(Threat likelihood x Vulnerability)
x Consequence

NIST SP800-30

OT Cybersecurity risk assessment and coverage COMPLIMENTS Functional Safety

Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

Cybersecurity (or Functional Security)

Risk assessment, addressment and management

1. Security control based (IEC61443-3-3 & ISA TR84.00.09)
2. Zone/Conduit Security based (ANNSI,IEC61443-3-2/IEC61443-3-3 & ISA TR84.00.09)
3. asset based risk assessment
4. threat modelling based risk assessment (e.g. ISF, MITRE)

- Defence in depth approach
- Documenting the security requirements
- Maintaining the security requirements in time
- Continuously updating the CSSRS

Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

Cybersecurity (or Functional Security)

A guideline- Project Flow

- CS SRS draft - classify the plant under consideration (type, criticality)
- Collection of applicable standards, norms and local laws (e.g. RF laws)
- Assign the overall SL-T of the ICS based on classification
- Definition of the equipment under control (EUC)➔ Initial System Block diagram
- Definitions of zone and conduits / dataflow directions
- Assign a SL-T to them: the higher the network layer, the higher the SL-T
- Market investigation / PO assignment
- threat modelling workshop: with Owner and Vendor/Consultant
- Threat Gap analysis and risk assessment
- Update to detailed system architecture
- Update the CS SRS
- Fabrication
- Tests

ANIPLA
Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

Cybersecurity (or Functional Security)

A Guideline

- ensure that personnel shall have assigned roles, rights and privileges
- Building Walkflow study
- at least 2 MFA concept is implemented when accessing rooms: Room access is granted based on roles and privileges (ACS in place)
- No external mass storage devices are allowed and blocked
- System Panels are closed by keys managed by supervisors, not “passe part tout”
- Hardware Access to CPU configuration is granted by hot work permits and key switches

ANIPLA
Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

Cybersecurity (or Functional Security)

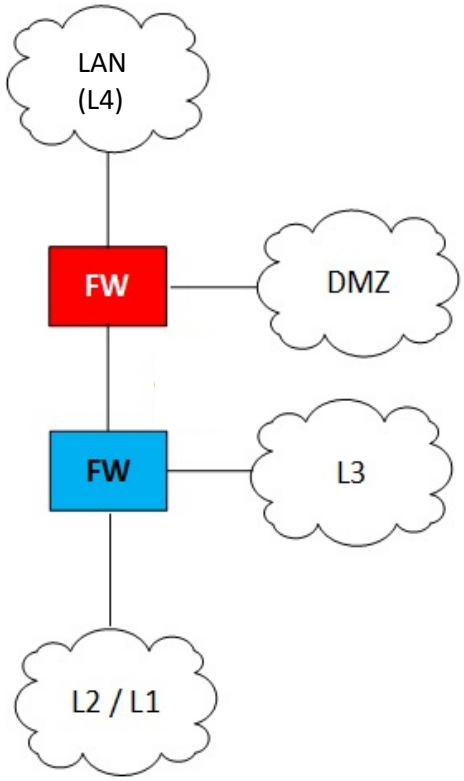
General Security Controls

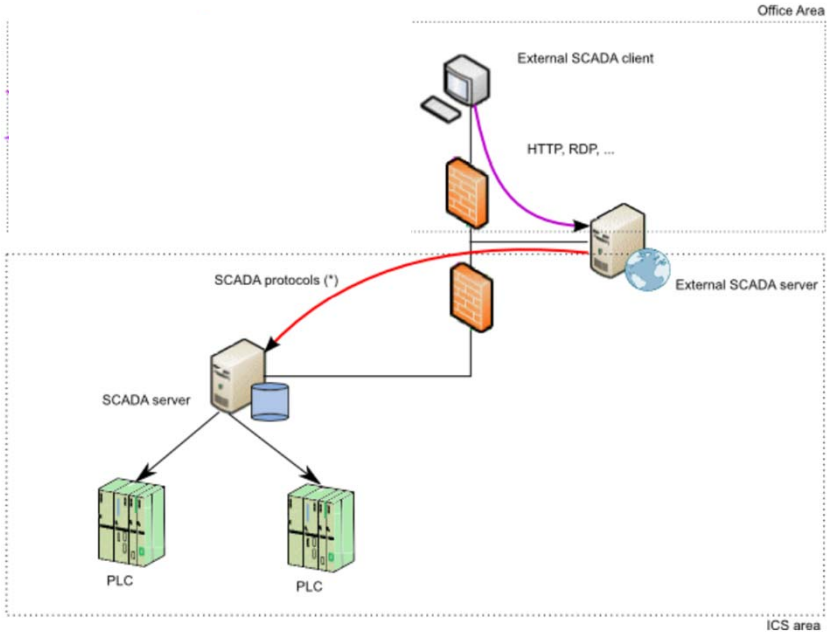
- Authentication/Authorisation security controls (2MFA)
- segmentation to Purdue model layers (or ISA95/API554)
- Use of DMZ
- separation of networks from the most remote location: Serials, IoT,
- one unique interface to DCS from UCPs
- stateful FW towards critical machines PLCs or direct connection to DCS via Modbus RTU
- Modbus FW towards other UCPs
- segregation & FW of SIS/GDS and FDS from DCS
- In Russia the fire detection/suppression systems are a critical infrastructures so they must be “parallelly cyber-secured” from top L3.5/DMZ
- Network inventory scanning
- Mixup of network protection measures and endpoint protection measures (e.g. FW)

Cybersecurity (or Functional Security)

General Security Controls @ L3.5 / DMZ

- Protocols disjunction from untrusted to trusted zones
- Remote access / File server
- Manual Vulnerability scanner
- Av server
- Patch management srv
- Zta (pep /pdp) or VPN
- NGFW
  - unidirectional
  - SSL inspection,
  - App control and intrusion Prevention





- Limit access to ports dedicated to remote access protocols

Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

Cybersecurity (or Functional Security)

General Security Controls @ L3 and L2

L3/L2.5

- Backup & Restore
- SIEM
- Passive traffic monitoring via SW SPAN port / TAP devices
- Domain controller
- NAC

L2

- AV nodes agent
- Device control agent
- Application control Agents (white/blacklisting)
- B&R agent on System backups
- Domain controller(s), if the case

L1

- Modbus Firewalls
- Avoid networking of UCP EWS

Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

Thank you

Palazzo UCIMU - Viale Fulvio Testi 128 – 20092 Cinisello B.mo (MI)
Tel 02 39 28 93 41 mail anipla@anipla.it

POR FESR EMILIA-ROMAGNA 2014/2020

UNIONE EUROPEA
Fondo europeo di sviluppo regionale

RegioneEmilia-Romagna

Industria 4.0 Sicura – Obiettivi e partnership

Obiettivi: mitigare i rischi informatici causati dall'adozione dei paradigmi dell'Industria 4.0

Partner di ricerca

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CENTRO INTERDIPARTIMENTALE DI RICERCA INDUSTRIALE ICT

t3lab
TECHNOLOGY TRANSFER TEAM

MechLav
Laboratorio per la Meccanica Avanzata

romagnatech
INNOVATION VALUE

Partner industriali

Bonfiglioli
Forever Forward

VEM sistemi

SACMI

Sfide

1

Valutazione del rischio informatico industriale

2

Minimizzare la vulnerabilità industriale

3

Customizzazione delle soluzioni i4s

Principali risultati

1

Nuovi strumenti di analisi del rischio

Sviluppo e consolidamento di nuovi strumenti informatici per valutare in modo oggettivo l'esposizione al rischio

Linee guida per la progettazione di impianti

Attraverso linee guida per progettare impianti industriali connessi basati sulle esigenze dell'industria regionale

2

3

Miglior resilienza ad attacchi informatici

Sviluppo delle tecnologie esistenti e miglioramento della loro capacità di resilienza delle aziende in caso di cyber attacchi

Elaborazione di un "digital twin" dell'impianto

Sviluppo di un dimostratore per sperimentare e valutare le soluzioni individuate prima di implementarle in ambito operativo

4

Analisi del rischio cyber per smart manufacturing

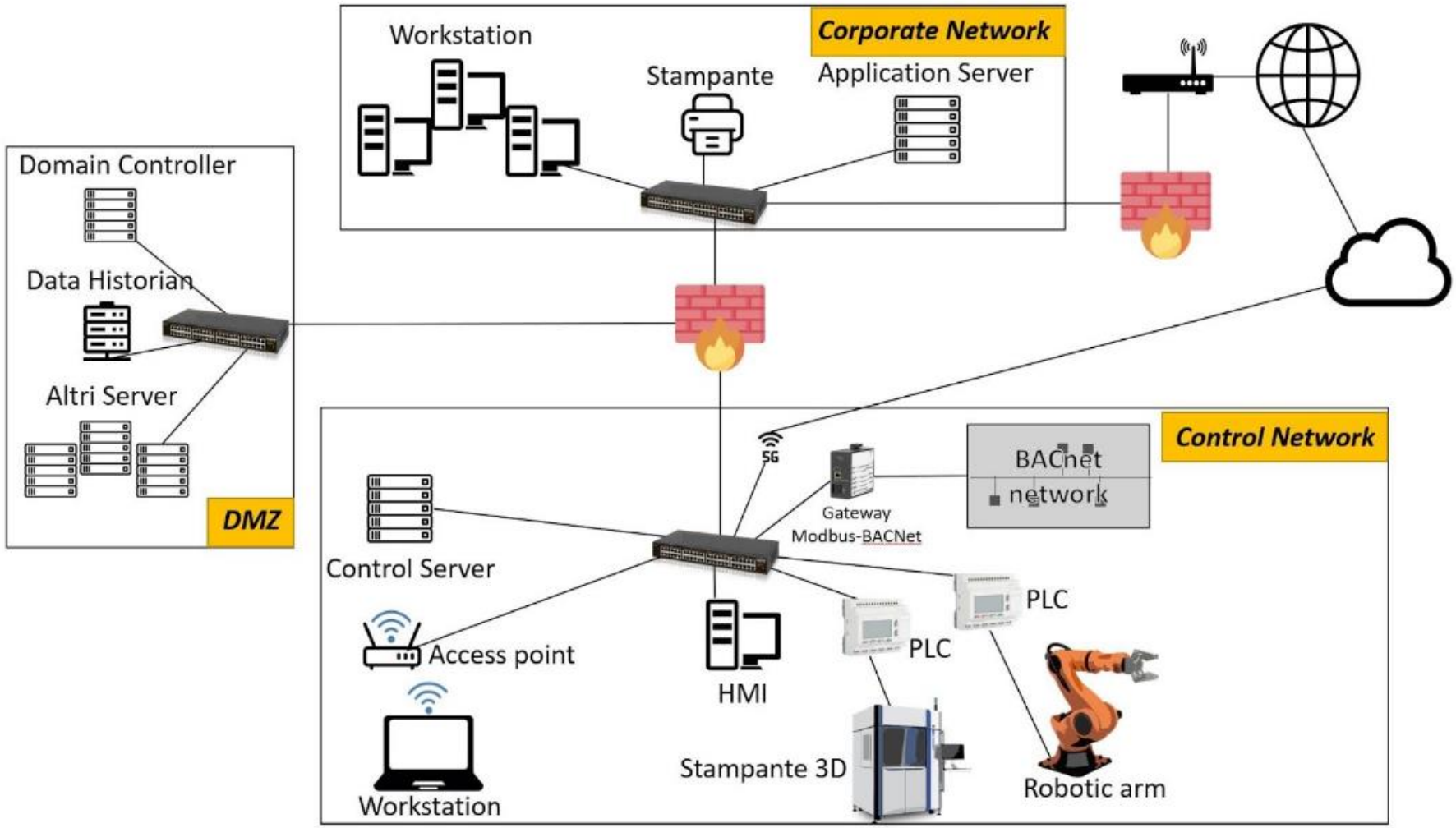
- Vulnerabilità specifiche di protocolli e dispositivi industriali
  - … anche wireless!
- Analisi di attacchi informatici specifici
- Strumenti di supporto per l’analisi del rischio cyber di impianti produttivi connessi

Linee guida per la progettazione di impianti

- Esistono varie normative relative alla sicurezza fisica (safety)
  - Tra tutte: IEC 62443
- Non esistono normative relative alla sicurezza cyber
- Numerose linee guida e «best practice» (NIST, Purdue Model, …)
  - Non tutte applicabili → dimensione aziendale!
  - Non sempre concordi

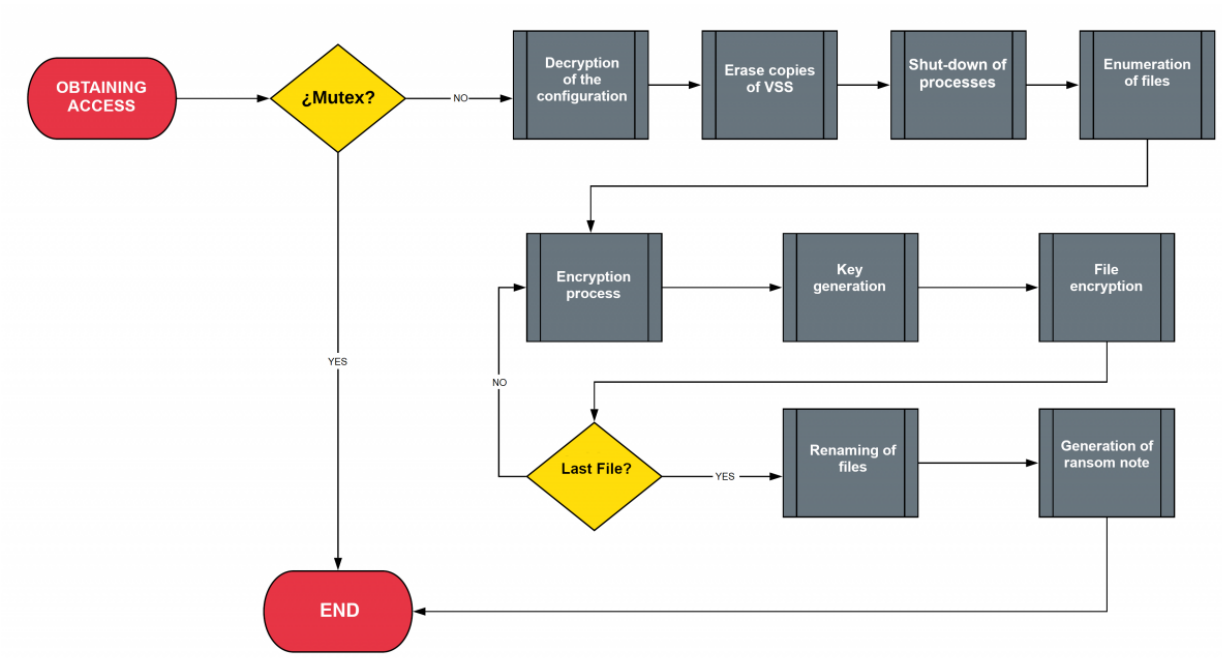
Obiettivo → proporre linee guida progettate per le specificità delle aziende manifatturiere del territorio

Linee guida per la progettazione di impianti



Migliore resilienza agli attacchi informatici

- Sviluppo di soluzioni tecnologiche innovative per bloccare attacchi a sistemi industriali
- Esempio: malware Ekans e Megacortex



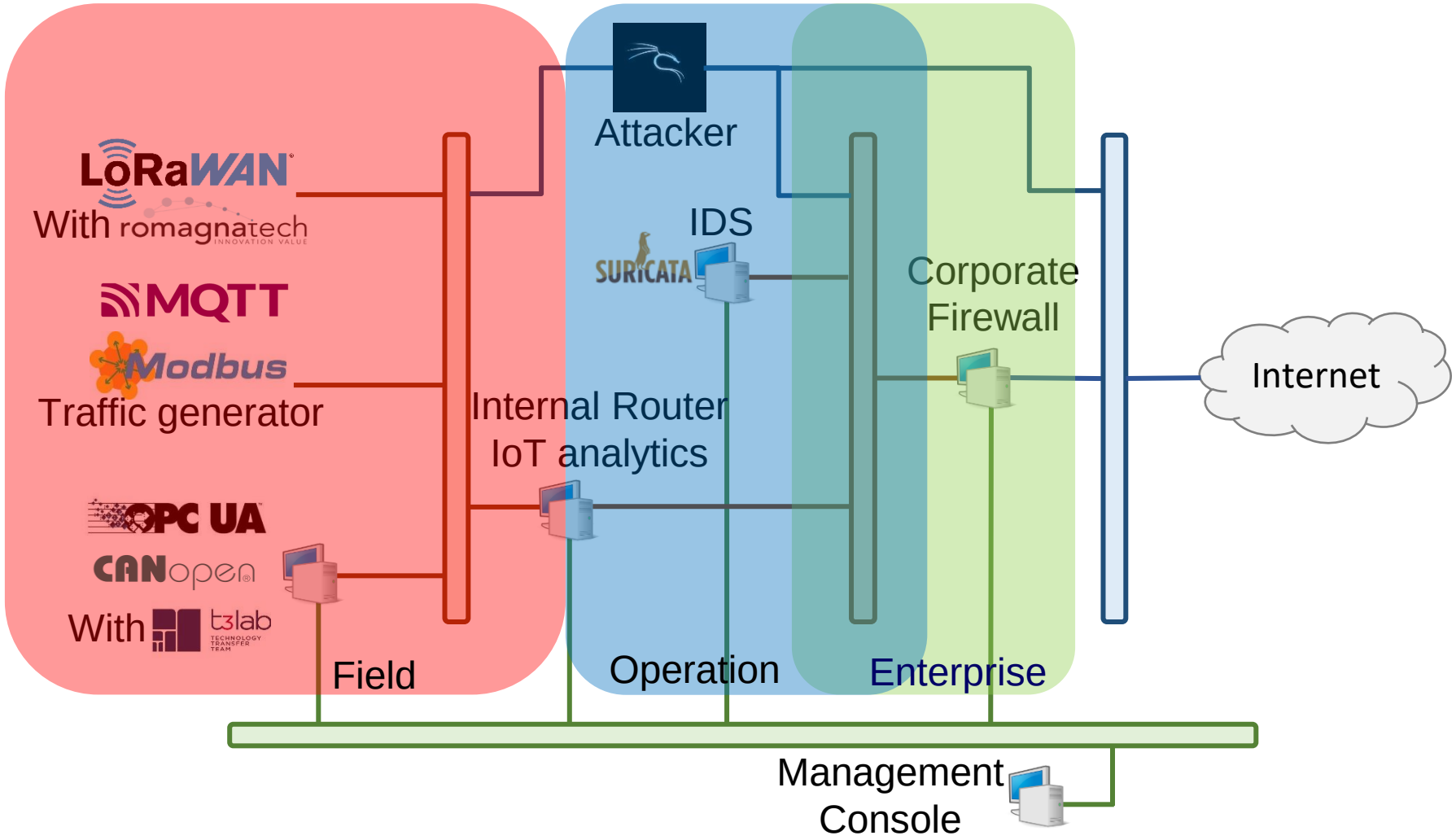
Migliore resilienza agli attacchi informatici

- Risultato: sistema di *intrusion detection* e *intrusion prevention* in grado di rilevare e bloccare infezioni

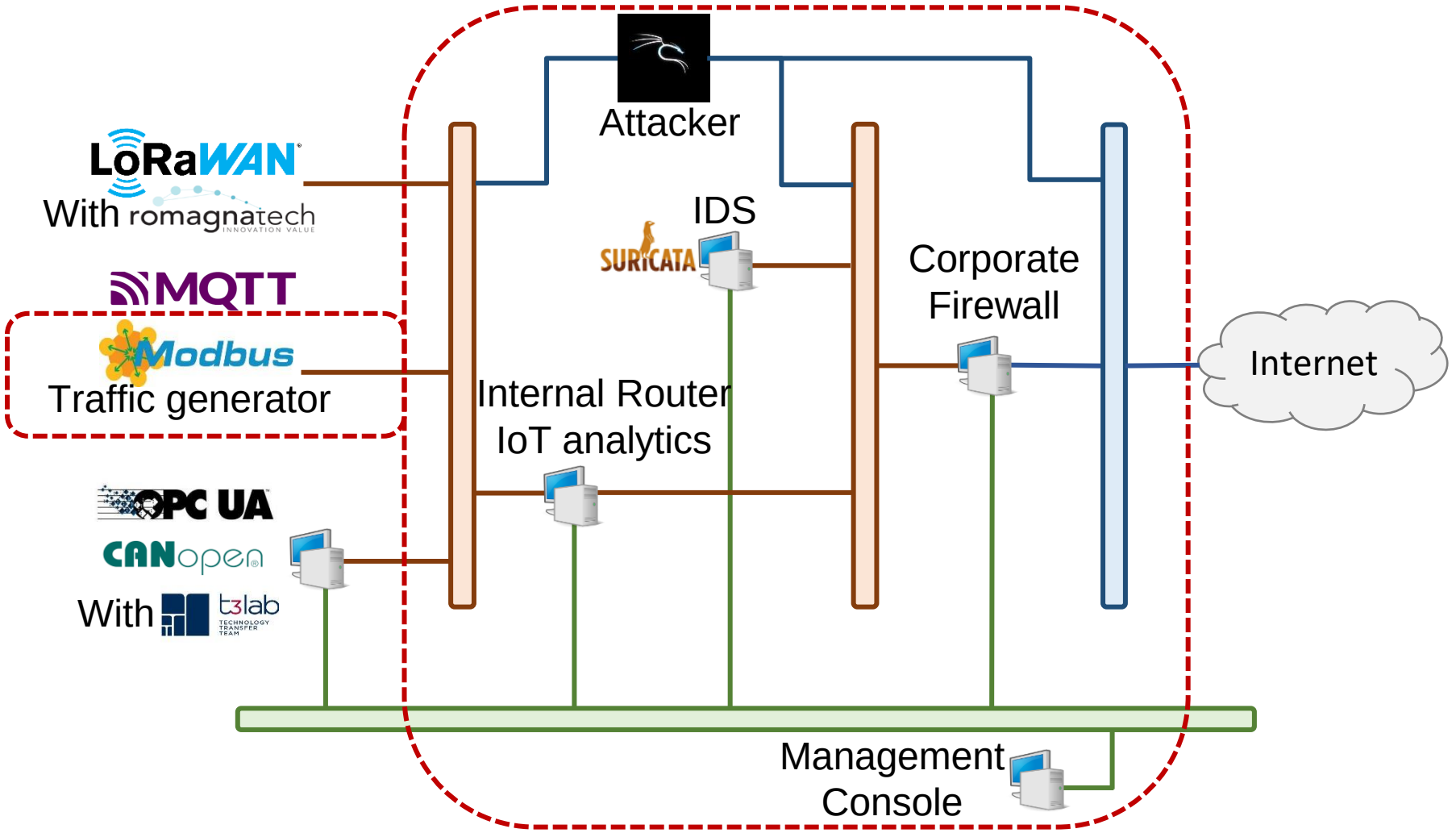
- Testato in ambienti simulati con esemplari reali del malware

Digital twin

- Modello IEC 62443



Digital twin



Contatti

Prof. Mirco Marchetti

Centro di Ricerca interdipartimentale sulla Sicurezza e la Prevenzione dei rischi (CRIS)
Università di Modena e Reggio Emilia

mirco.marchetti@unimore.it - info@i4s-project.it

Q&A