OAD Osservatorio Attacchi Digitali in Italia

malabo ICT Advisory

Attacchi e difese per l'ambiente OT, Operational Technology

Marco R. A. Bozzetti
Presidente Onorario AIPSI
Ideatore e coordinatore OAD
Founder e CEO Malabo srl

Massimo Chirivì
Presidente AIPSI
Founder e CEO Innovamind srls

AIPSI e OAD

AIPSI, capitolo italiano della mondiale ISSA

- Associazione no-profit di **sole persone fisiche**
- Obiettivo principale: **l'indirizzamento e la crescita professionale dei suoi Soci**
- **Tre tipologie di Socio**
  - **AIPSI-ISSA (US$ 160,00 /anno)**
  - **SOLO AIPSI (€ 50,00/anno)**
  - **AIPSI GIOVANE (fino a 26 anni: primo anno gratuito, poi € 25,00/anno)**
  - Si veda: https://www.aipsi.org/associazione/come-associarsi.html
- AIPSI è Socio **FIDAInform**

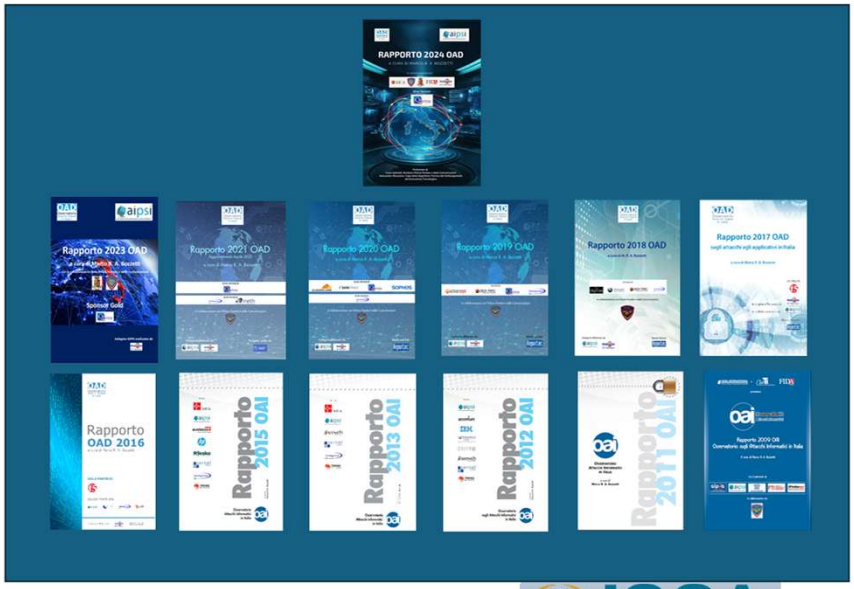
2025
20 anni AIPSI e 40 anni ISSA

- **Servizi riservati a tutti i Soci AIPSI**
  - **supporto alle certificazioni**, in particolare per **eCF Plus** (EN 16234-1:2016) e per **CIAD DigCom 2.2** di AICA con **forti sconti**
  - **Mentorship gratuita sull'indirizzamento e sulla crescita professionale**
  - **SIG di approfondimento e discussione**
  - ***Network Soci a livello nazionale***
- **Servizi riservati ai Soci AIPSI-ISSA**
  - **ISSA Journal**
  - **ESG ISSA Survey "The Life and Times of Cyber Security Professionals"**
  - Convegni, workshop, webinar in inglese
  - Corsi online in inglese
  - **SIG, Special Interest Group**
    - Privacy
    - Women in Security
  - **Accordi con sconti per certificazioni individuali**
  - ***Network Soci a livello mondiale***

L'iniziativa OAD

- **OAD** è l'unica indagine online in Italia (**completamente indipendente e "terza" rispetto ai vari attori in gioco**) sugli **attacchi digitali intenzionali** ai sistemi informativi delle aziende e degli enti pubblici operanti in Italia, e **sulle misure tecniche ed organizzative** che questi hanno in esercizio.
- **OAD** non predefinisce uno specifico bacino di rispondenti, il medesimo negli anni, ma consente a chiunque, interessato e coinvolto nella gestione di un sistema informativo di una azienda/ente, un **pieno e libero accesso al questionario online**, in maniera totalmente anonima.

- **Con OAD 2025, 18 anni consecutivi di indagini**
  - basate su questionari online anonimi
  - libero accesso al questionario per tutti i referenti di un sistema informativo operante in Italia
- **Per tutti i settori merceologici + Pubbliche Amministrazioni Centrali e Locali**
- **13 Rapporti pubblicati**
- Uno **specifico sito web** che costituisce il **repository** di tutti i Rapporti OAD/OAI pubblicati e della documentazione sui vari eventi e sugli articoli pubblicati nei quali AIPSI ha presentato dati emersi dalle indagini: www.oadweb.it



OAD 2025: l'indagine diviene maggiorenne

- Il piano di lavoro, con allegate le proposte di sponsorizzazione (in italiano e in inglese) e di patrocinio gratuito, è in https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2025.html

- **Il questionario OAD 2025, rigorosamente anonimo, è online e compilabile**: https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2025/questionario-oad-2025.html

COMPILATELO (o fatelo compilare dai vostri tecnici) e PASSATE PAROLA ad aziende/enti che conoscete

La struttura del Questionario OAD 2025

S1 - **Brevi informazioni sulla Azienda/Ente della/del rispondente**

S2 - Attacchi digitali di ogni tipo al Sistema Informativo rilevati nell'intero 2024

S3 - Approfondimento **attacchi ai *siti e alle applicazioni web*** del Sistema Informativo, con riferimento alle top ten vulnerabilità individuate da OWSAP per questi ambienti

S3B - Approfondimento sugli attacchi ad ***applicativi basati su Intelligenza Artificiale***, con riferimento alle top ten vulnerabilità 2025 individuate da OWSAP per questi ambienti

S3C - Approfondimento sugli **attacchi a sistemi ed apparati *OT, Operation Technology***

S4 - **Attacchi più temuti nel prossimo futuro**

S5 - Macro caratteristiche del Sistema Informativo cui la/il rispondente fa riferimento

S6 - **Misure tecniche** in atto per la sicurezza digitale dell'intero Sistema Informativo

S7 - **Misure organizzative** di sicurezza digitale nell'Azienda/Ente della/del rispondente

S8 - **Ruolo della/del rispondente**

S10 – Calcoli (non visibili) e presentazione finale in tempo reale della macro valutazione del livello di sicurezza del SI

Gli elementi caratterizzanti il questionario OAD 2025

- Due sole domande sugli attacchi rilevati nel 2024 in riferimento alle tipologie di attacco ed alle famiglie di tecniche di attacco così da poter avere dati di trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 al 2024;
  - **Tra le tipologie di attacco la supply chain informatica**
- le **domande di approfondimento** (se nel 2024 si sono subiti attacchi in queste aree):
  - ai **siti e agli ambienti web**,
  - **alle applicazioni basate su Intelligenza Artificiale**
  - agli **ambienti OT, Operational Technology**, che includono anche apparati informatici medico-sanitari chirurgici;
- **Sono opzionali** le domande sulle **misure di sicurezza digitale** presenti nei sistemi informativi oggetto delle risposte,
  - ma solo se si risponde a queste **domande si potrà avere, alla fine della compilazione, la macro-valutazione del livello di sicurezza digitale in essere un funzione delle risposte selezionate**
- **L'Intelligenza Artificiale è inserita anche nelle tipologie di attacco (che cosa attacco) e nelle tecniche di attacco (come attacco)**

Le (famiglie di) tipologie di attacco in OAD 2025: che cosa si attacca

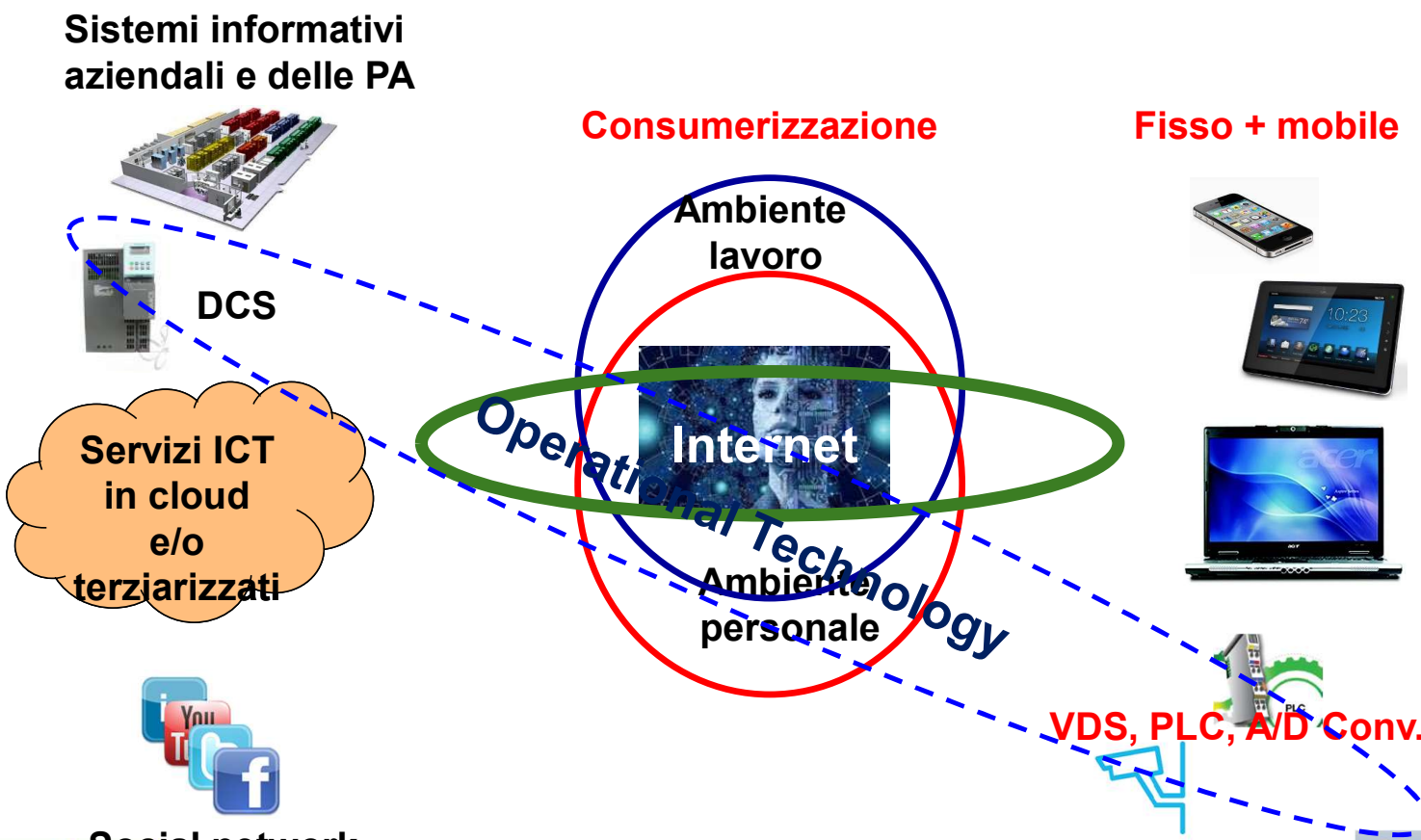
- Distruzione e/o compromissione FISICA di dispositivi ICT FISSI o di loro parti
- FURTO dispositivi FISSI ICT o di loro parti
- FURTO di dispositivi ICT MOBILI di proprietà dell'azienda/ente e in uso presso i suoi dipendenti/collaboratori
- FURTO INFORMAZIONI da singoli specifici sistemi FISSI ICT (PC, server, storage system, etc.) del Sistema Informativo, anche terziarizzati/in cloud
- FURTO INFORMAZIONI relative all'azienda/ente da sistemi MOBILI (palmari, smartphone, tablet, ecc.) sia di proprietà dell'azienda/ente sia dell'utente finale che li usa in logica BYOD
- Attacchi ALL'IDENTIFICAZIONE, AUTENTICAZIONE E CONTROLLO ACCESSI degli utenti finali e privilegiati
- Attacchi alle RETI locali e geografiche, fisse e wireless, inclusi i collegamenti ad Internet, e ai DNS nel corso del 2024
- Attacco e/o uso non autorizzato di SISTEMI IT NEL LORO COMPLESSO (dal PC agli host fisici e virtuali). anche terziarizzati o in cloud
- MODIFICHE malevoli e/o non autorizzate ai PROGRAMMI APPLICATIVI e alle loro configurazioni, del Sistema Informativo anche terziarizzate e in cloud
- MODIFICHE malevoli e/o non autorizzate alle INFORMAZIONI trattate dalle applicazioni del Sistema Informativo, anche quelle terziarizzate/in cloud
- SATURAZIONE (DoS, DDoS) risorse digitali del Sistema Informativo, anche quelle terziarizzate/in cloud
- Attacchi ai propri sistemi/servizi digitali in CLOUD o comunque TERZIARIZZATI presso Fornitori terzi
- Attacchi a dispositivi dei sistemi OT, OPERATIONAL TECHNOLOGY, ivi inclusi i sistemi IoT/IIoT, i sistemi per l'automazione industriale ((SCADA, DCS, PLC, ..) e la robotica
- Attacchi alla "SUPPLY CHAIN" causati da vulnerabilità di fornitori e/o clienti interconnessi
- Attacchi a sistemi/servizi/applicativi basati su Intelligenza Artificiale.

Le (famiglie di) tecniche di attacco in OAD 2025: come si attacca

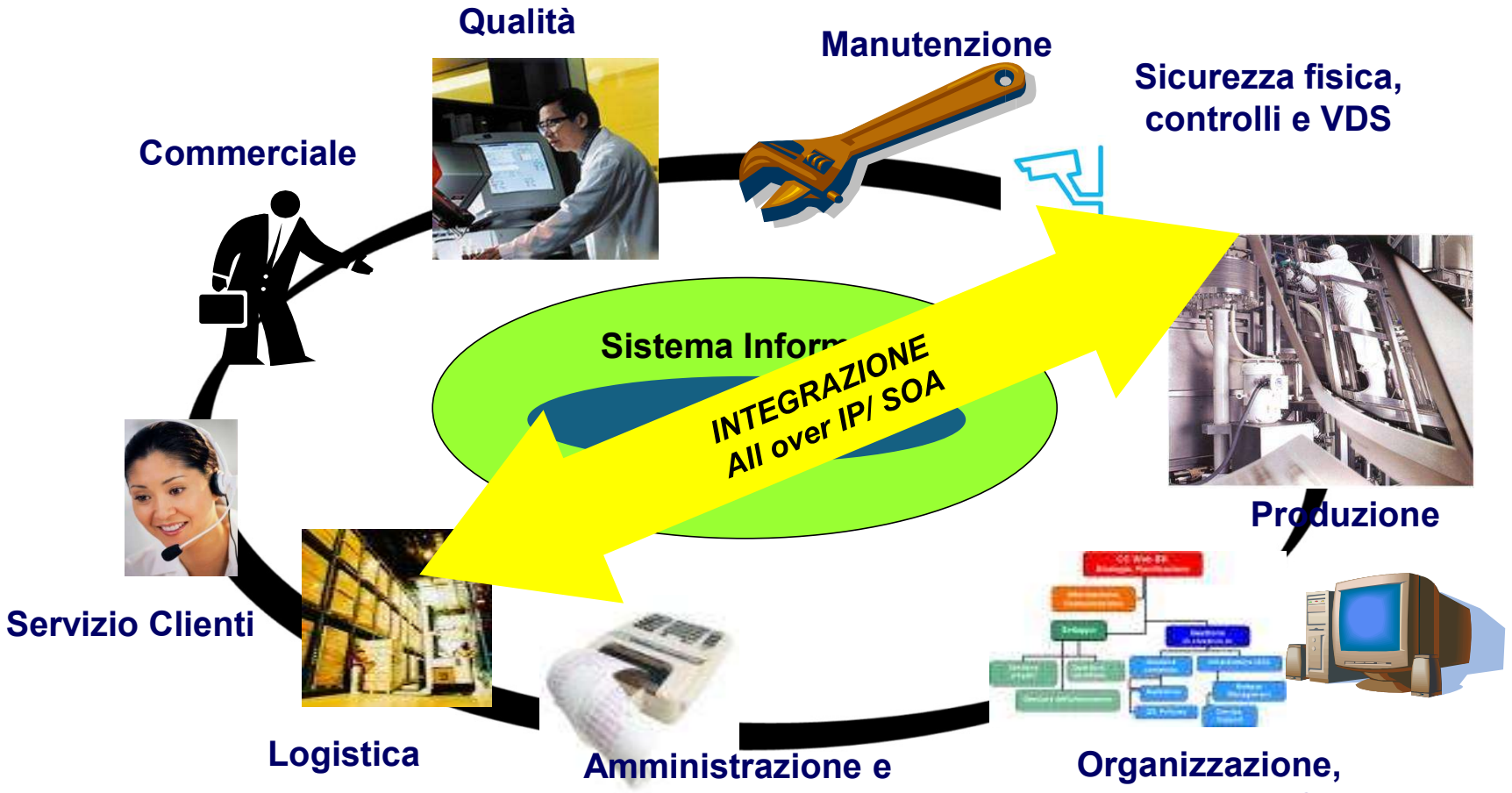
- Attacco fisico
- Raccolta malevola e non autorizzata di informazioni
- Script e programmi maligni
- Agenti autonomi
- Toolkit
- Botnet e simili
- Utilizzo di strumenti e tecniche di Intelligenza Artificiale
- Utilizzo di due o più tecniche di attacco, inclusi gli APT, Advanced Persistent Threat

OT, Operational Technology

Il mondo digitale nel quale viviamo e lavoriamo …



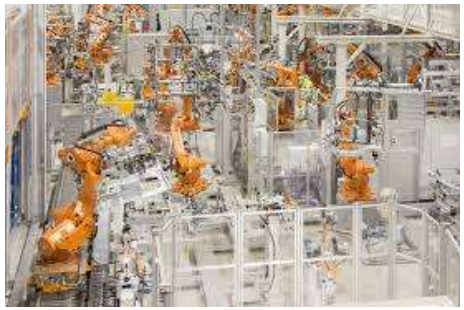
Processi aziendali e ICT come tecnologia abilitante



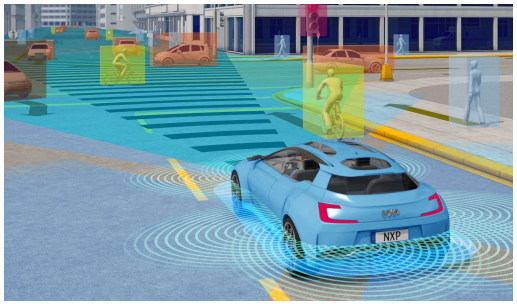
OT, Operational Technology

- **Insieme dei vari sistemi di controllo ed automazione sia dei processi industriali sia di altre tipologie, sia di tipo continuo (processi chimici) sia di tipo discreto (processi manifatturieri).**
- Esempi di sistemi OT includono i sistemi a controllo numerico (CNC), i sistemi SCADA, i Distributed Control System (DCS), gli Industrial Control System (ICS), i Programmable Logic Controlle (PLC), i Programmable Automation Controller (PAC), i sistemi robotizzati per la produzione manifatturiera e la logistica, gli IoT e gli IIoT, i sistemi di controllo del territorio e le smart city, , le smart grid per la distribuzione dell'energia, i sistemi di analisi e controllo sanitario, i robot per le operazioni chirurgiche (controllabili/effettuabili anche da remoto), le simulazioni e le emulazioni nell'R&D, la domotica.
- Tipici settori meceologici che usano sistemi OT includono: settore chimico, settore sanitario e della sanità pubblica, settore alimentare e agricolo, settore ICT e delle comunicazioni, strutture commerciali (in particolare della grande distribuzione), manifattura di prodotti critici, costruzioni dighe, ponti, grattacieli ed altre grandi strutture critiche, sistemi e manufatti per la difesa (militari), servizi di emergenza, settore energia, servizi finanziari, strutture governative, reattori nucleari, materiali e rifiuti, sistemi di trasporto, sistemi idrici e acque reflue, domotica.

I tipici ambienti OT



INTERNET & 4/5 G



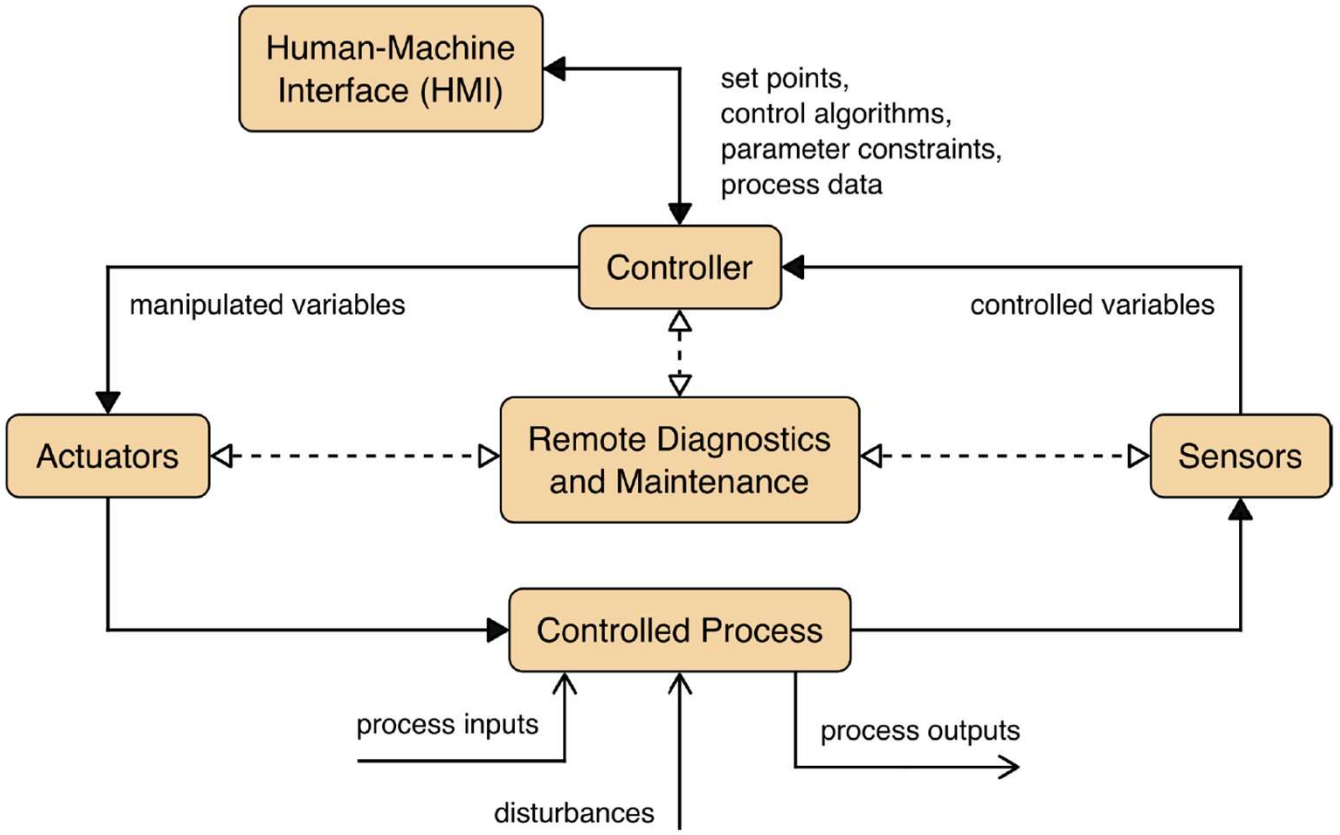
OT, ICS, IIoT-IoT, SCADA, DCS, PLC, PAC, ….

- **Termini generali**
  - **OT**, Operational Technology
  - **ICS**, Industrial Control System
  - **IoT,** Internet of Things
  - **IIoT**, Industrial IoT

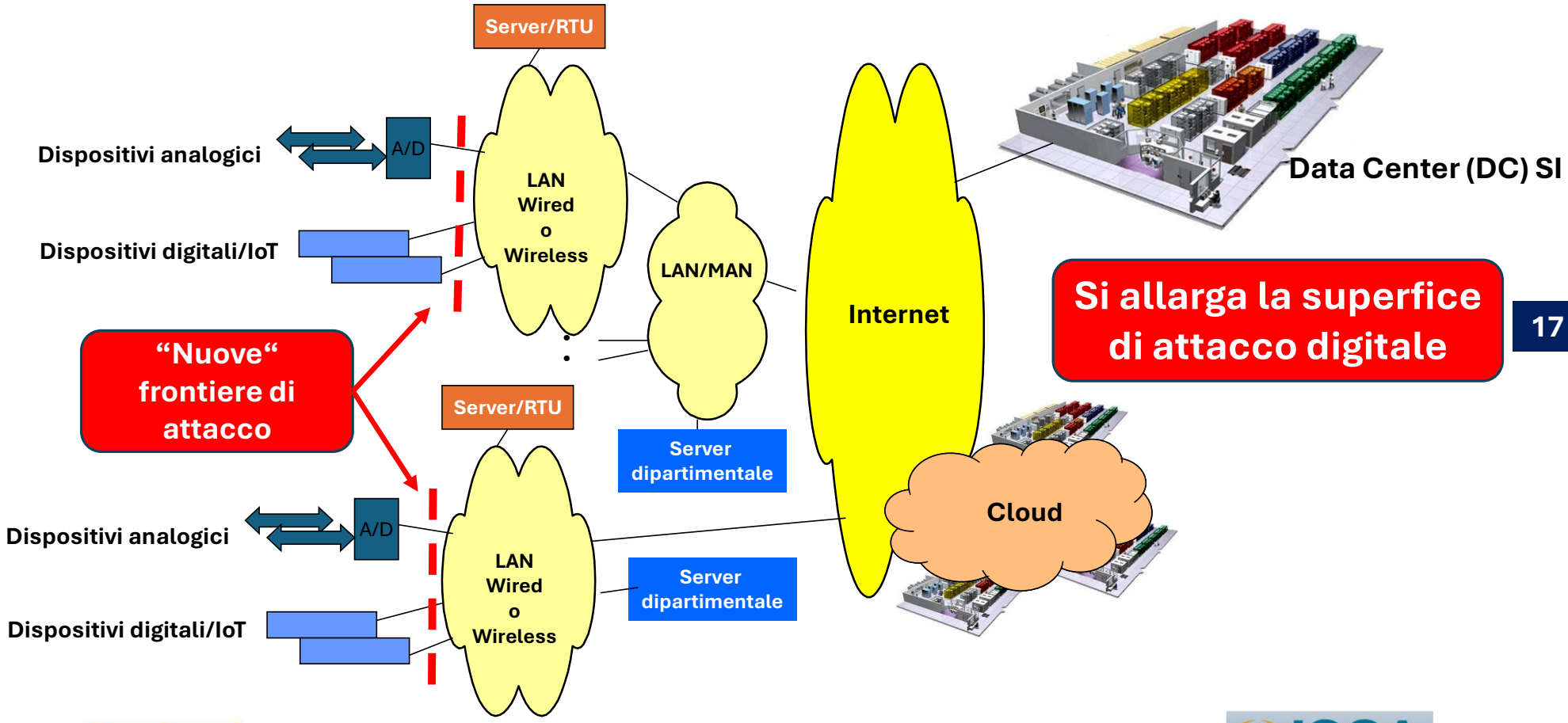
- **a livello architetturale**:
  - **SCADA**, Supervisory Control And Data Acquisition
  - **DCS**, Distributed Control System

- **a livello di attuatori-controllori** (dispositivi distribuiti che attuano e controllano localmente il funzionamento di un dispositivo ed inviano dati ad un sistema centrale di raccolta e di elaborazione)
  - **PLC**, Programmable Logic Controller, si indicano dispositivi, ad esempio una valvola, una saracinesca, un motore, ecc., tramite una rete di comunicazione.
  - **PAC**, Programmable Automation Controller

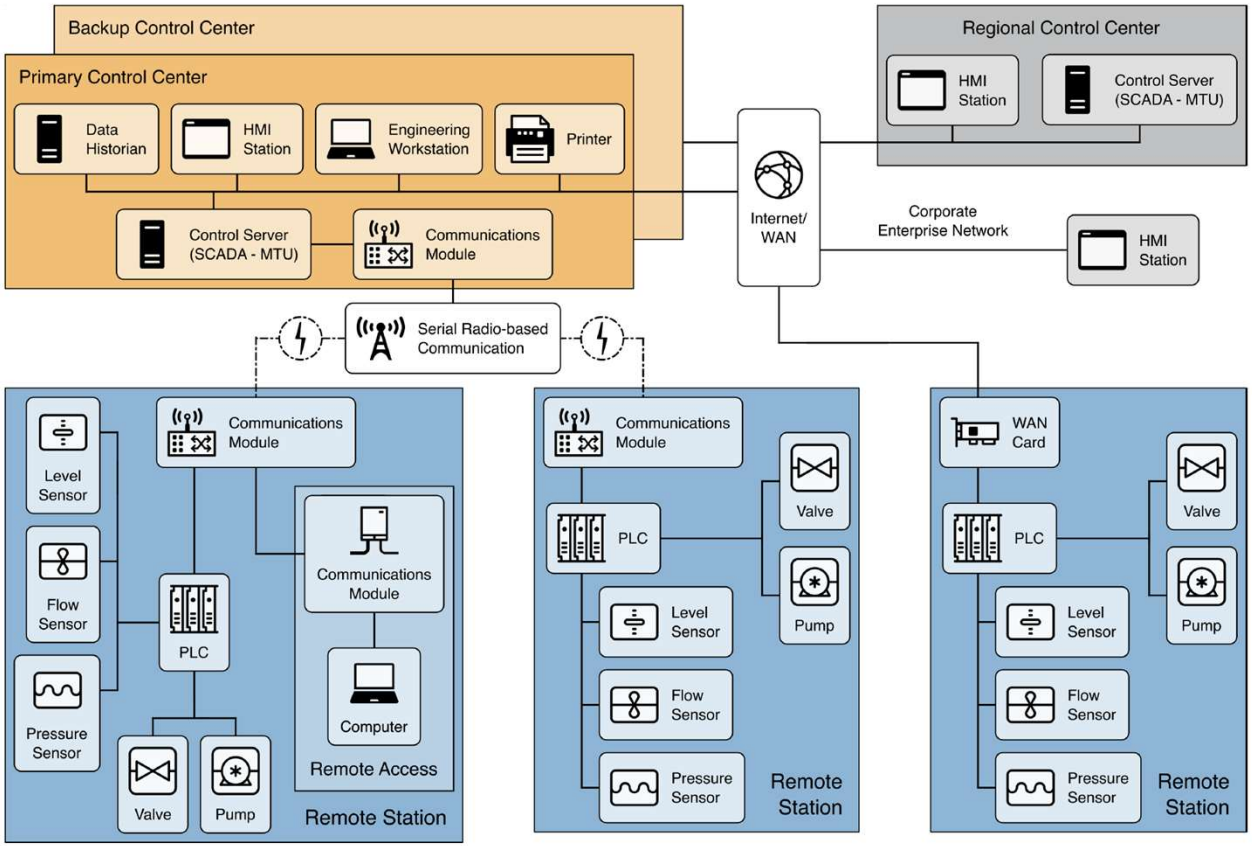
Schema di un tipico sistema OT (da NIST)



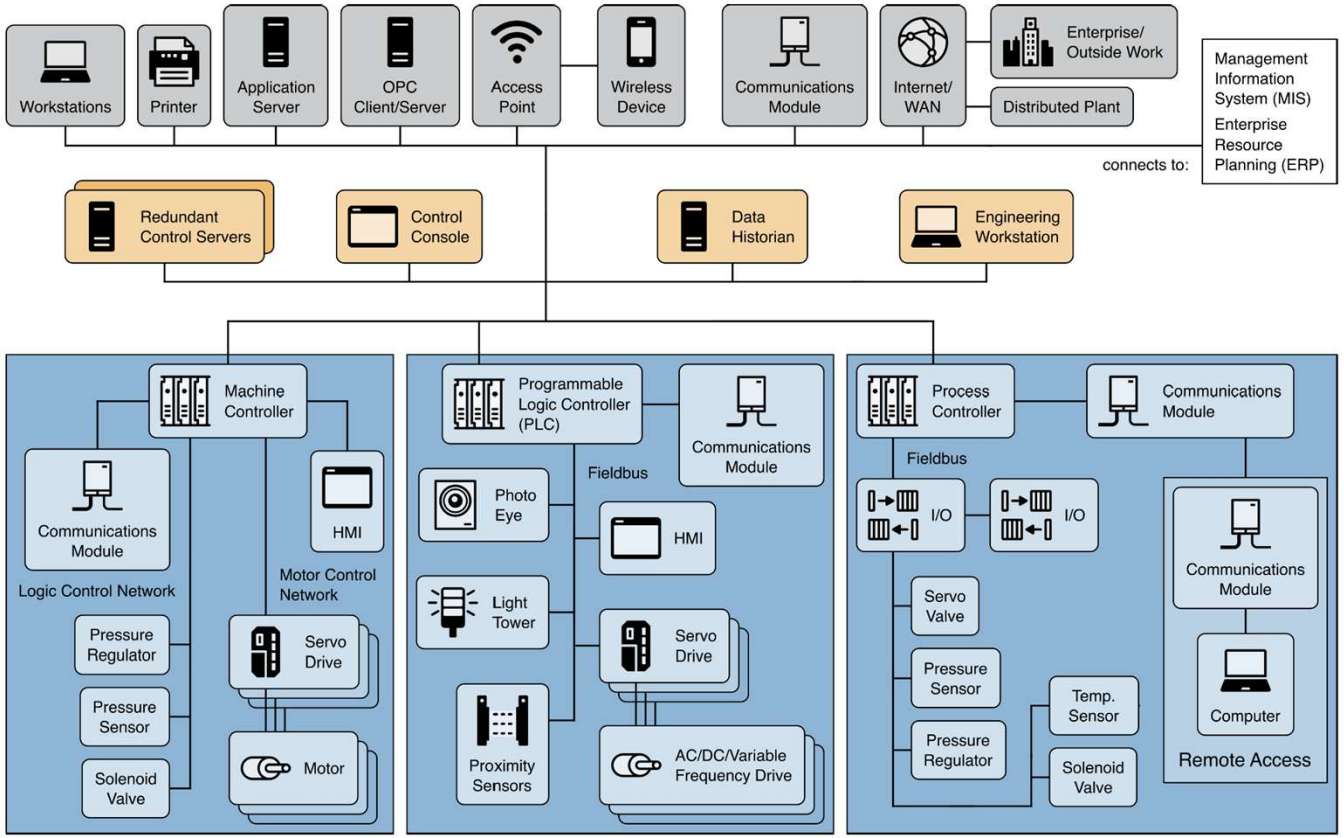
Esempio integrazione OT con il Sistema Informtivo



Esempio implementativo di un sistema SCADA (da NIST)



Esempio implementativo di un sistema DCS (da NIST)



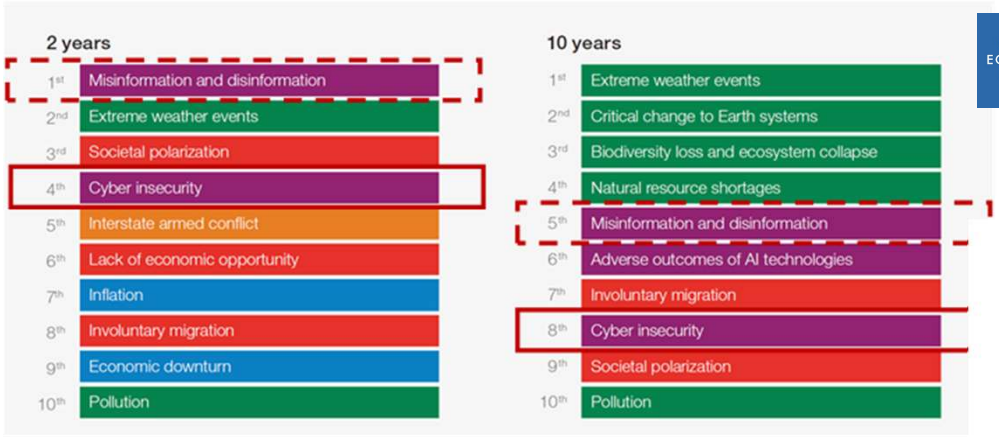
OT e Sicurezza Digitale

Convergenza ICT-OT: si usano le stesse tecnologie

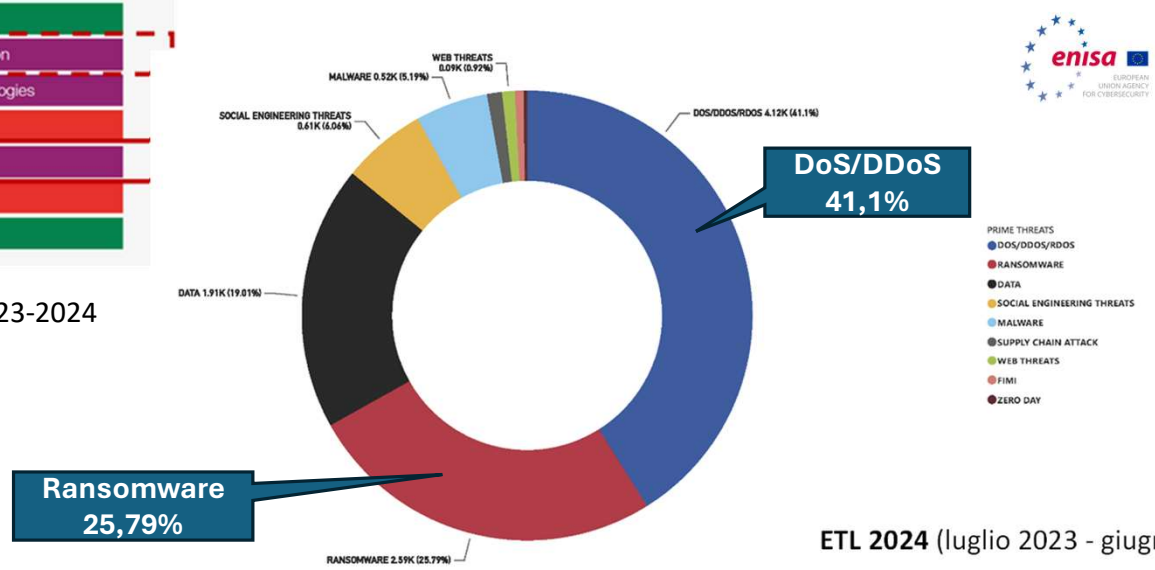
- La maggior parte dei sistemi OT sono oggi **basati sulle più diffuse soluzioni ICT** in termini di **CPU**, di **sistemi operativi**, di **linguaggi di programmazione** e tendono in maniera crescente **ad interoperare,** via Internet e/o reti dedicate, con gli altri ambienti ed applicativi del Sistema Informativo,

- **Questa tendenza ha ampliato e continua ad ampliare la superficie di possibile attacco digitale, attaccabile in pratica con le stesse logiche e strumenti per il mondo ICT**

Il quadro degli attacchi/rischi digitali a livello mondiale ed europeo (Rapporto OAD 2024)



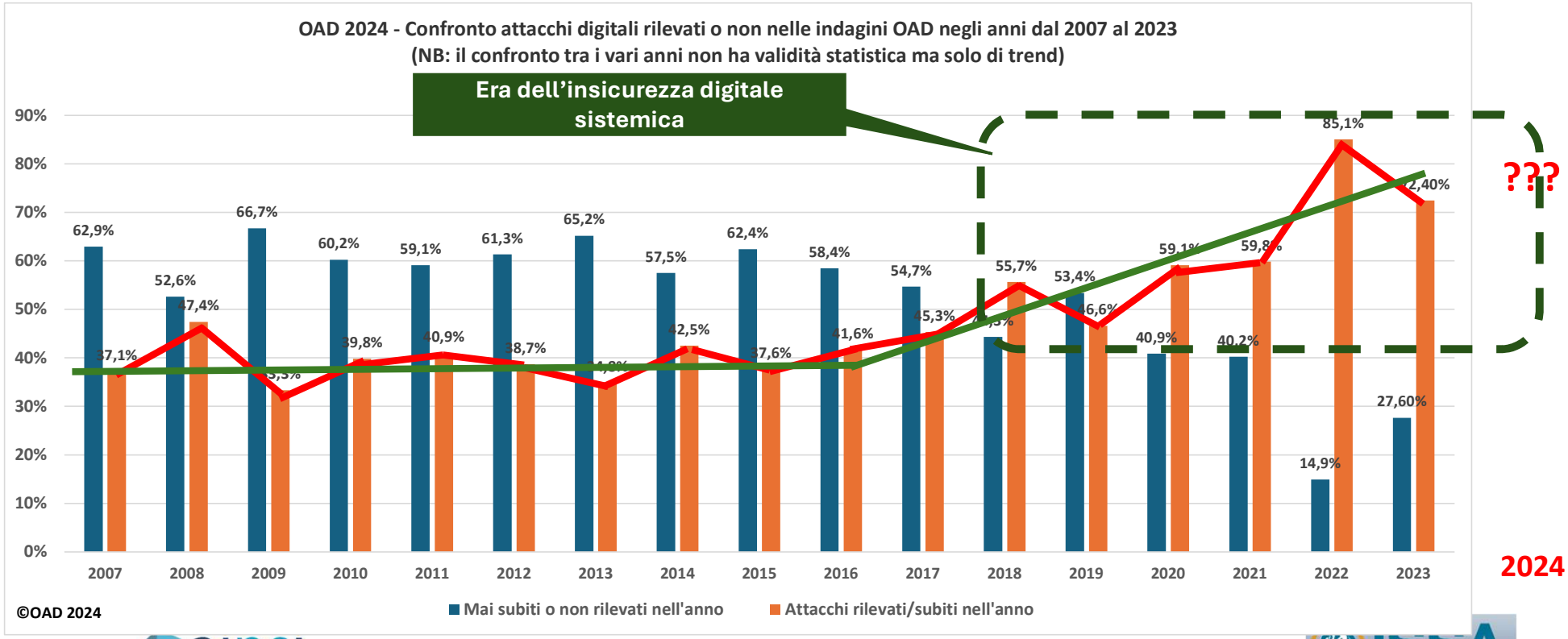
World Economic Forum Global Risks Perception Survey 2023-2024



ETL 2024 (luglio 2023 - giugno 2024)

Il trend degli attacchi digitali dalle indagini OAD

L' **INSICUREZZA** digitale diviene **quasi incontenibile** e **SISTEMICA**

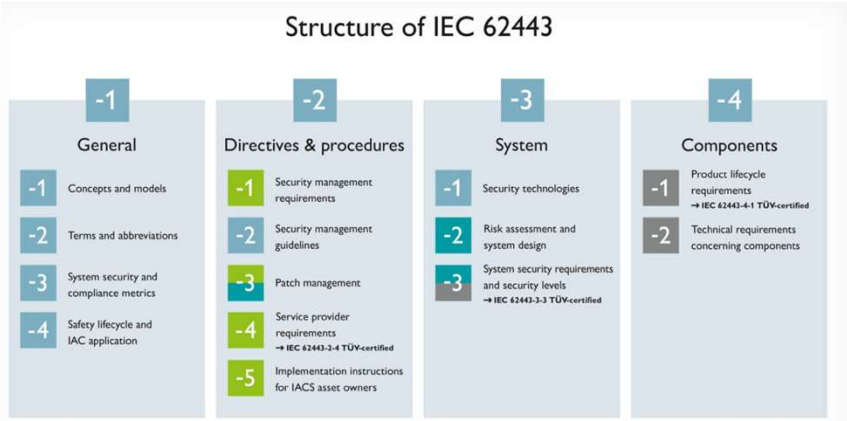


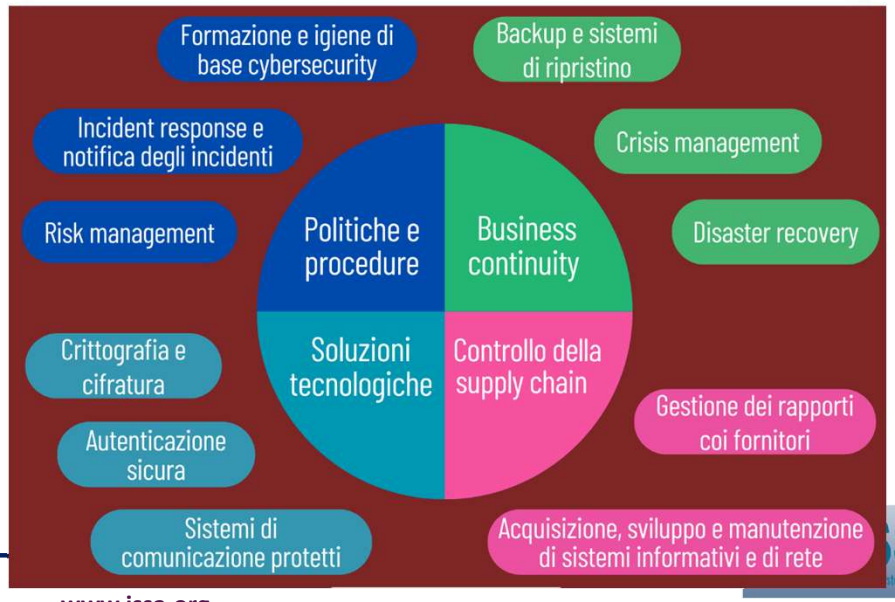
Standard di riferimento per la sicurezza digitale nel mondo OT

- La famiglia di standard **IEC 62443**

- **NIST SP 800-82r3** - Guide to Operational Technology (OT) Security

- I sistemi OT possono essere **infrastrutture critiche (essenziale** o **importante)** e quindi devono seguire la normativa **NIS 2**

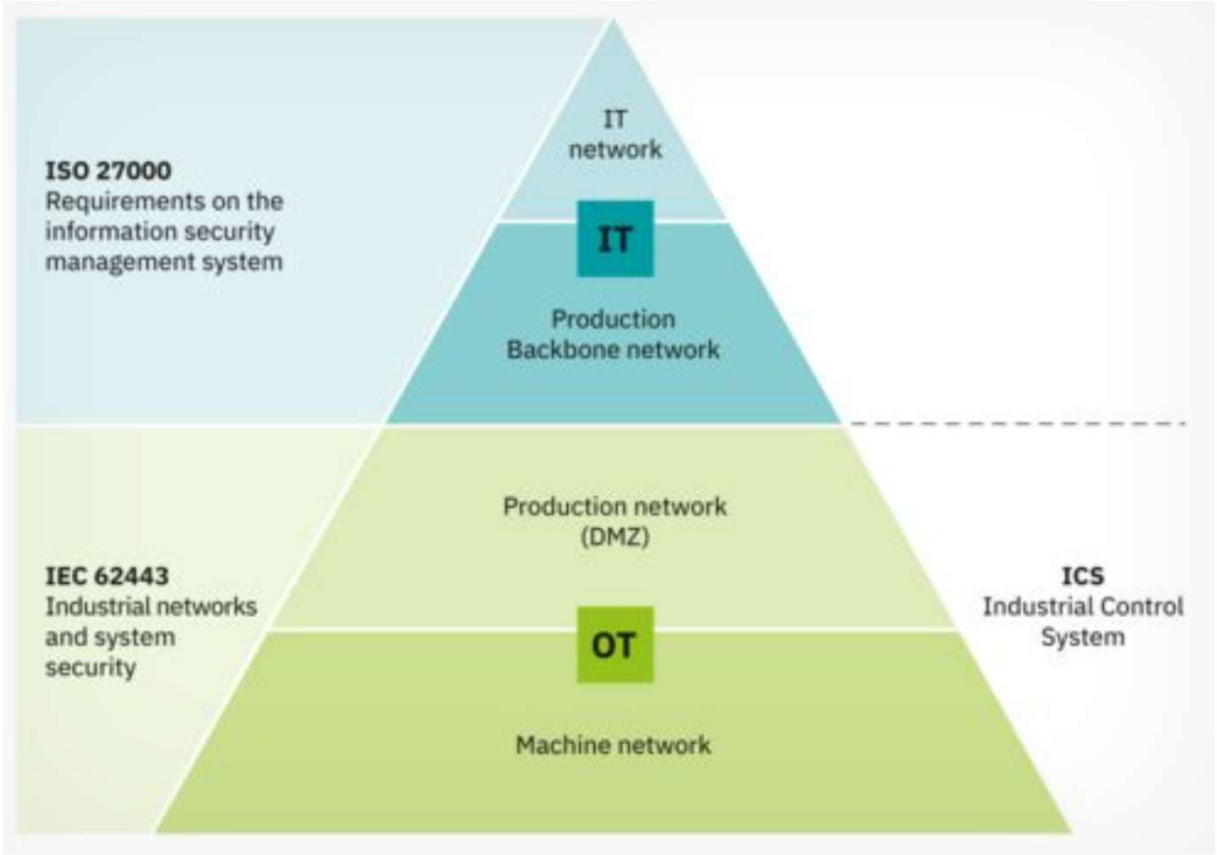




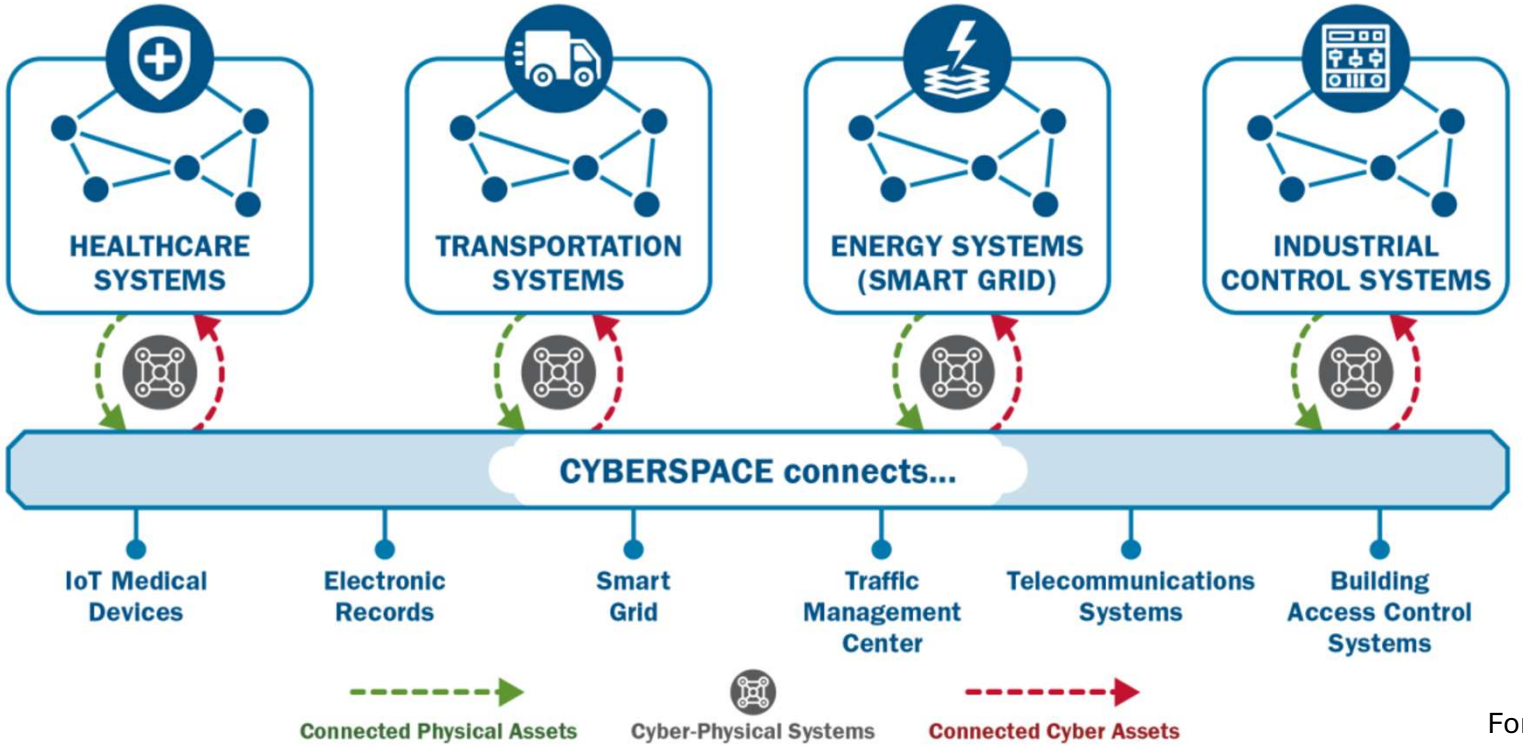
Fonte: Studio Legale Delli Ponti

www.issa.org

Integrazione ISO 27000 con IEC 62443



Integrazione safety e security nel mondo OT



Fonte: Cisa

Focalizziamo l'attenzione su:

BLACK HAT & BUSINESS

LE ORGANIZZAZIONI CRIMINALI SUL WEB

RECRUITING CONTINUO E MARKETPLACE DI SOFTWARE ILLEGALE

IL RISCATTO COME FONTE DI BUSINESS ILLEGALE

TRASFORMAZIONE DEL FENOMENO

TENSIONI GEOPOLITICHE

GUERRE DIGITALI

Insieme di cambiamenti

- Tecnologici
- Culturali
- Organizzativi
- Sociali
- Geopolitici
- Creativi
- Manageriali

associati alla Cyber Security


Why Does Social Engineering Work
Insufficient Security Policies
Lack of a Technological Fix
Difficult Detection
Lack of Training
There is no patch for human stupidity

Deep Web & Dark web

www.aipsi.org
www.issa.org

Una strategia di difesa profonda per sistemi OT (NIST) - 1

- Developing **security policies, procedures, training, and educational material** that apply specifically to the OT system
- Considering OT security policies and procedures based on the National Terrorism Advisory System and deploying increasingly heightened security postures as the Threat Level increases
- Addressing security **throughout the life cycle of the OT system**, including architecture design, procurement, installation, operations, maintenance, and decommissioning
- Implementing a **network topology** for the OT system that has **multiple layers,** with the most critical communications occurring in the most secure and reliable layer
- Providing **logical separation between the corporate and OT networks** (e.g., stateful inspection firewalls between the networks, unidirectional gateways)
- Considering where **physical separation** may be required as opposed to logical separation

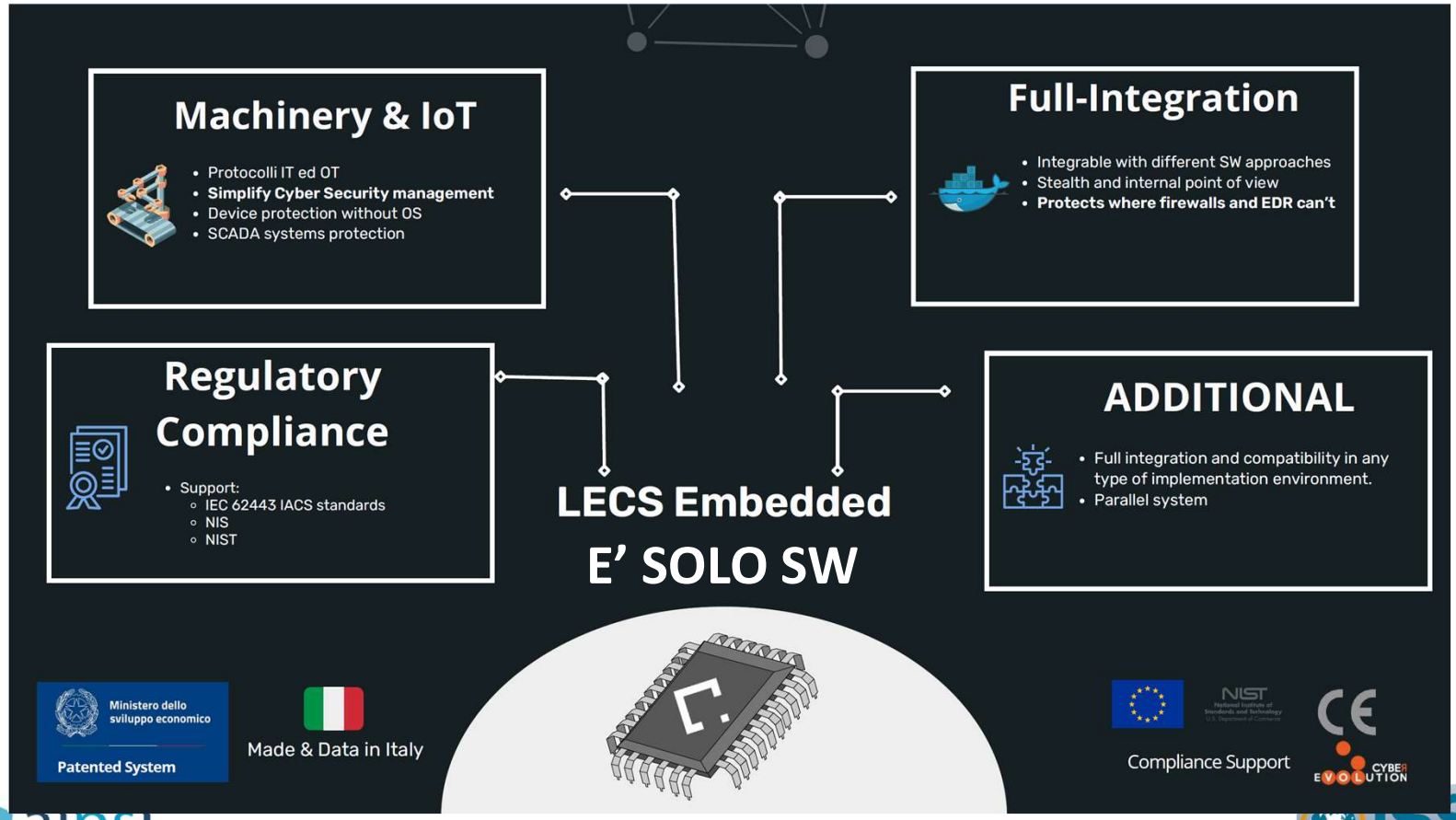
Una strategia di difesa profonda per sistemi OT (NIST) - 2

- Employing a **DMZ network architecture** (e.g., prevent direct traffic between the corporate and OT networks)
- Using **multi-factor authentication for remote access** to the OT system
- Ensuring that **critical components are redundant and are on redundant networks**
- Designing critical systems for graceful degradation (**fault tolerant**) to prevent catastrophic cascading events
- **Disabling unused ports and services on OT devices** after testing to ensure that this will not impact OT operation
- **Restricting physical access** to the OT network and devices
- **Restricting OT user privileges** to only those that are required to perform each user's function (e.g., establishing role-based access control, configuring each role based on the principle of least privilege)

Una strategia di difesa profonda per sistemi OT (NIST) - 3

- Using **separate authentication mechanisms and credentials for users** of the OT network and the corporate network (i.e., OT network accounts do not use corporate network user accounts)
- Using modern technology, such as smart cards for user authentication
- Implementing security controls (e.g., intrusion detection software, antivirus software, file integrity checking software) where technically feasible to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the OT system
- Applying security techniques, such as encryption and/or cryptographic hashes, to OT data storage and communications where appropriate
- Expeditiously deploying security patches after testing all patches under field conditions on a test system, if possible, before installation on the OT system
- Tracking and monitoring audit trails on critical areas of the OT system
- Employing reliable and secure network protocols and services where feasible

LECS Embedded-Custum per OT – Un esempio di prodotto italiano di NDR-IPS con 3 motori AI cooperanti



Esempi di domande su OT nel Questionario OAD 2025

Questionario OAD 2025 su attacchi a sistemi OT

Gli attacchi più gravi rilevati nel 2024 agli ambineti OT hanno riguardato i seguenti sistemi ed apparati:

Nello spazio per commenti a fianco delle risposte selezionate si possono inserire precisazioni e commenti che potranno fornire ulteriori indicazioni, sempre anonime, per l'elaborazione del rapporto finale OAD 2025.

Il commento è permesso solo quando l'opzione relativa è stata scelta.

☐ Sistemi ICS, Industrial Control Systems	
☐ Sistemi DCS, Distributed Control Systems	
☐ Sistemi PLC, Programmable Logic Controllers	
☐ Sistemi SCADA, Supervisory Control And Data Acquisition	
☐ Sistemi IIoT/IoT (Industrial Internet of Think)	
☐ Sistemi di diagnosi e controlli sanitari	
☐ Sistemi robotizzati (Robot) utilizzati in vari campi-settori, dall'automazione industriale agli interventi chirurgici.	
☐ Altri sistemi/dispositivi OT (indicare il tipo)	
☐ Non lo so	

Questionario OAD 2025: impatti tecnici attacchi ai sistemi OT

Impatti tecnici dell'attacco più grave rilevato in ambito OT nel corso del 2024 per l'operatività dei sistemi OT (e dei macchinari da questi supportati/controllati) e dell'intero Sistema Informativo (SI)

Un attacco intenzionale ad un sistema OT può causare non solo problemi sullo specifico sistema OT e sui dispositivi che controlla e/o manipola, ma anche all'intero Sistema Informativo o a sue parti.
NB: Nello spazio per commenti a fianco delle risposte selezionate si possono inserire precisazioni e commenti che potranno fornire ulteriori indicazioni, sempre anonime, nell'elaborazione del Rapporto finale OAD 2025.

Il commento è permesso solo quando l'opzione relativa è stata scelta.

☐ Disservizio in locale sui sistemi controllati poco/per nulla avvertito	
☐ Interruzione del servizio in locale di breve durata (poche ore)	
☐ Interruzione del servizio in locale di media durata (2-3 giorni)	
☐ Interruzione del servizio in locale di lunga durata (> 3 giorni)	
☐ Estensione del disservizio ad altre parti del Sistema Informativo di breve durata (poche ore)	
☐ Estensione del disservizio ad altre parti del Sistema Informativo di media durata (2-3 giorni)	
☐ Estensione del disservizio ad altre parti del Sistemi Informativo di lunga durata (> 3 giorni))	
☐ Non è stato possibile misurare l'impatto dell'attacco più grave OT in termini di durata del disservizio	
☐ Non lo so	

Questionario OAD 2025: impatti economici attacchi ai sistemi OT

Impatto sui costi (e quindi sul budget del Sisteama Informativo e/o dell'intera azienda/ente) dell'attacco più grave rilevato ai sistemi OT nel corso del 2024.

Nello spazio per commenti a fianco della risposta selezionata si possono inserire precisazioni e commenti che potranno fornire ulteriori indicazioni, sempre anonime, nell'elaborazione del Rapporto finale OAD 2025

Il commento è permesso solo quando l'opzione relativa è stata scelta.

☐ Impatto irrilevante o nullo sui costi e/o sul budget del Sistema Informativo	
☐ Impatto ridotto sui costi e sul budget del Sistema Informativo	
☐ Impatto significativo sui costi e sul budget del Sistema Informativo	
☐ Impatto non trascurabile anche sul bilancio complessivo dell'azienda/ente (costi per perdita di immagine, perdita di clienti, etc.)	
☐ Non si è potuto/riuscito a valutare la perdita economica	
☐ Non lo so	

Questionario OAD 2025: misure di sicurezza per sistemi OT – reti separate

I sistemi OT in uso operano localmente su proprie specifiche reti locali, separate da quelle locali del SI (ambiente IT), anche se i sistemi OT possono essere collegati ed interoperanti col SI ?

Scegliere solo una delle seguenti voci

- ○ NO, i sistemi OT operano TUTTI sulle stesse reti locali degli apparati IT
- ○ Non lo so
- ○ SI, tutti i sistemi OT operano su specifiche reti locali a loro dedicate
- ◉ SOLO alcuni sistemi OT operano su specifiche reti locali a loro dedicate

Questionario OAD 2025: misure di sicurezza per sistemi OT – controllo centrale o locale

I sistemi OT in uso sono controllati anche dal Centro, o sono controllati e monitorati solo localmente?

*NB: **Controllo e monitoraggio dal Centro** significa che esiste ed opera un sistema centralizzato a livello italiano per il controllo ed il monitoraggio dei singoli sistemi OT operanti (in produzione). Tale sistema centrale può essere nella stessa sede "centrale" dell'azienda/ente, all'interno di un Data Center, etc. Volutamente non si pongono domande di dettaglio per non appesantire il questionario.*

Scegliere solo una delle seguenti voci

- ◯ Controllo sia in locale che dal Centro di tutti i sistemi OT
- ◯ Controllo sia in locale che dal Centro SOLO di alcuni sistemi OT
- ◯ Controllo solo in locale
- ◯ Non lo so

Questionario OAD 2025: misure di sicurezza per sistemi OT – fault tolerant

I sistemi OT sono in replica per un significativo aumento della loro disponibilità ed affidabilità?

Scegliere solo una delle seguenti voci

- ◯ Operano tutti almeno in duale e con replica dei dati tra loro in tempo quasi reale
- ◯ Solo quelli più critici operano (almeno) in duale replicandosi tra loro
- ◯ In locale sono presenti sistemi OT di scorta che possono essere installati e resi operativi in breve tempo
- ◯ NO, non esistono nè scorte nè sistemi OT in replica tra loro
- ◯ Non lo so

Questionario OAD 2025: misure di sicurezza per sistemi OT – Incident Management

Sono definite, conosciute ed applicate procedure organizzative da seguire in caso di malfunzionamenti e/o incidenti sui sistemi OT?

Scegliere solo una delle seguenti voci

- ○ Vengono applicate le procedure di "Incident Management" previste per l'intero Sistema Informativo
- ○ NO, non esistono specifiche procedure organizzative per la gestione di malfunzionamenti e/o incidenti sui sistemi OT
- ○ Non lo so
- ○ SI, esistono, sono conosciute ed applicate procedere organizzative di "Incident Management" SPECIFICHE per i sistemi OT

GRAZIE PER L'ATTENZIONE e …

Questa presentazione sarà scaricabile in pdf dal sito web di AIPSI

COMPILATE o FATE COMPILARE il QUESTIONARIO OAD 2025 e PASSATE PAROLA ai vostri interlocutori:

https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2025/questionario-oad-2025.html

https://www.aipsi.org/

Se volete essere sistematicamente aggiornati e **crescere professionalmente** nel campo della sicurezza digitale:

- **Diventate Soci di AIPSI**
  - **https://www.aipsi.org/associazione/come-associarsi.html**

https://www.issa.org/