



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Sicurezza industriale 2026

Minacce, casi reali e quadro normativo europeo

ENISA e Clusit 2026, l'attacco alla rete energetica polacca, NIS2, CRA e Regolamento Macchine

Webinar · ottobre 2026



YCyber

HWG Sababa Group



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Contenuti

01	Il contesto cyber europeo	3
02	Il contesto italiano	9
03	Caso studio: la rete polacca	17
04	NIS2, CRA e IEC 62443	26
05	Macchine e prEN 50742	35
06	Sfide e conclusioni	43



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

SEZIONE 01

Il contesto cyber europeo

ENISA Threat Landscape 2026

8.257 incidenti analizzati nell'UE: tanto rumore, ma i danni veri vengono da accessi e ransomware

51,3%

DDoS: la tipologia più frequente, quasi sempre hacktivista

39,5%

accessi non autorizzati, per il 63,9% a scopo economico

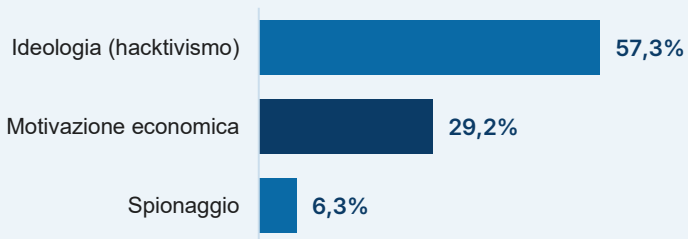
60,4%

delle intrusioni con vettore noto sfrutta una vulnerabilità

73%

degli incidenti colpisce soggetti essenziali o importanti NIS2

Perché attaccano: obiettivi stimati



Le tendenze del 2025

- ✔ Cybercrime, hacktivisti e attori statali usano gli stessi vettori e strumenti
- ✔ Supply chain e fornitori terzi come leva per colpire più vittime
- ✔ Social engineering evoluto: ClickFix, device-code phishing, app di messaggistica
- ✔ AI sempre più integrata nelle operazioni malevole

Fonte: ENISA Threat Landscape 2026 (settembre 2026), periodo di riferimento 1 gennaio – 31 dicembre 2025



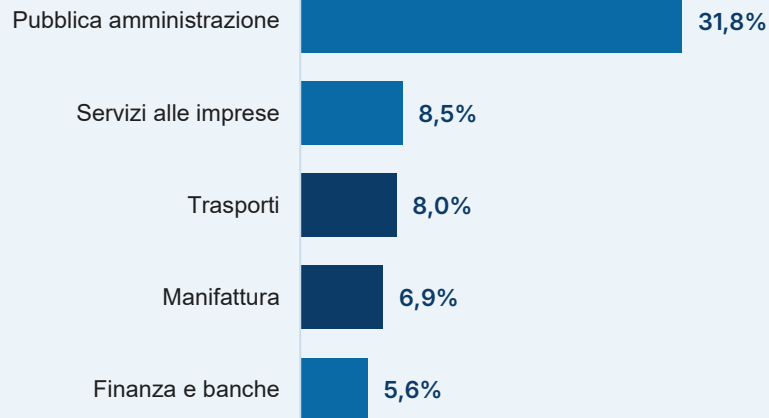
CONFINDUSTRIA
VENETO EST

START4.0

Settori più colpiti nell'UE

La manifattura è il primo bersaglio del cybercrime e il secondo degli attori statali

Top 5 settori per incidenti registrati



14,4%

Manifattura: primo settore per incidenti di cybercrime nell'UE

9,8%

Manifattura: secondo settore per attività di attori statali, dopo la PA (29,4%)

13,6%

Italia: terzo Stato membro per rivendicazioni ransomware (DE 26,5%, FR 14,7%)

Fonte: ENISA Threat Landscape 2026 (settembre 2026), periodo di riferimento 1 gennaio – 31 dicembre 2025

Focus manifatturiero

L'80,4% degli incidenti nel settore sono accessi non autorizzati, in gran parte ransomware



Chi viene colpito

- ✦ Macchinari e attrezzature: 23,3%
- ✦ Costruzioni: 21,8%
- ✦ Automotive, elettronica, apparecchiature elettriche



Come

- ✦ 61,1% degli incidenti con movente economico
- ✦ Ransomware: 82,8% di questi
- ✦ Qilin 17,4% · Akira 11,5% · SafePay 8%



Con quale impatto

- ✦ Fermo dei sistemi IT core e degrado dei servizi
- ✦ Effetti su più siti: un produttore tedesco di scambiatori di calore blocca filiali in Polonia e Cina
- ✦ Okuma: colpita anche la filiale europea

Non solo cybercrime. Hacktivismo (24,2% degli incidenti nel settore): DDoS e rivendicazioni crescenti di intrusioni in ambienti OT. Attori statali (8,4%): interesse per la difesa e la proprietà intellettuale.

Fonte: ENISA Threat Landscape 2026 (settembre 2026), periodo di riferimento 1 gennaio – 31 dicembre 2025



CONFINDUSTRIA
VENETO EST

START4.0

Energia, acqua e OT: l'interesse cresce

Nel 2025 le rivendicazioni di intrusioni in ambienti industriali si sono moltiplicate

Rivendicazioni OT degli
hacktivisti

37

nel 3° trimestre 2025

124

nel 4° trimestre 2025



Hacktivismo filorusso

- ▼ Z-Pentest Alliance e Infrastructure Destruction Squad rivendicano accessi a impianti energetici e idrici
- ▼ NoName057(16) entra nell'OT con il progetto DDoSia
- ▼ Energia: 4,8% delle attività hacktiviste nell'UE



Attori statali

- ▼ Russia-nexus: spionaggio su PA, difesa ed energia sfruttando vulnerabilità note
- ▼ Dicembre 2025: attacco coordinato al settore energetico polacco con un wiper
- ▼ Cina-nexus: trasporti marittimi, semiconduttori, manifattura

ENISA: *l'impatto OT verificato resta limitato, ma cresce l'interesse degli attaccanti per lo sfruttamento di configurazioni, interfacce e credenziali.*

Fonte: ENISA Threat Landscape 2026 (settembre 2026), periodo di riferimento 1 gennaio – 31 dicembre 2025



CONFINDUSTRIA
VENETO EST

START4.0

Vulnerabilità: più numerose, sfruttate prima

Oltre 48.000 nuove CVE nel 2025 (+22%): edge device e IoT non aggiornati restano il bersaglio preferito

48.000+

nuove CVE pubblicate
nel 2025, +22% sul 2024

39%

critiche (9%) o alte
(30%) secondo CVSS

71%

sfruttabili via rete: rischio
per i sistemi esposti

245

vulnerabilità aggiunte al
catalogo CISA KEV

Come entrano: vettori delle intrusioni

Vulnerabilità (N-day e 0-day)

60,4%

Misconfigurazione ed
esposizione

20,7%

Debolezze più sfruttate (KEV)

- ▼ CWE-78 OS command injection
- ▼ CWE-22 path traversal
- ▼ CWE-502 deserializzazione di dati non fidati
- ▼ Tempo di weaponizzazione in costante riduzione

Fonte: ENISA Threat Landscape 2026 (settembre 2026), periodo di riferimento 1 gennaio – 31 dicembre 2025



CONFINDUSTRIA
VENETO EST

START4.0



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

SEZIONE 02

Il contesto italiano

Clusit 2026: Italia e mondo

Nel 2025 gli incidenti gravi noti crescono del 48,7%: l'aumento più alto mai registrato

5.265

incidenti gravi noti nel mondo nel 2025 (3.541 nel 2024)

9,6%

avviene in Italia: circa uno su dieci, +42% in un anno

84%

degli incidenti con severity critica o alta (79% nel 2024)

+79%

incidenti al Manufacturing nel mondo, di nuovo 4° settore



AI moltiplicatore di forza

Phishing e social engineering +75%: l'AI rende più efficaci gli attacchi di ingegneria sociale.



Vulnerabilità al secondo posto

Lo sfruttamento di vulnerabilità cresce del 65% e resta la seconda tecnica d'attacco.



Italia: crimine e attivismo

Cybercrime 60,9%, hacktivism 38,7%: in Italia l'hacktivism cresce del 145%.

Fonte: Rapporto Clusit 2026 sulla Cybersecurity in Italia e nel mondo



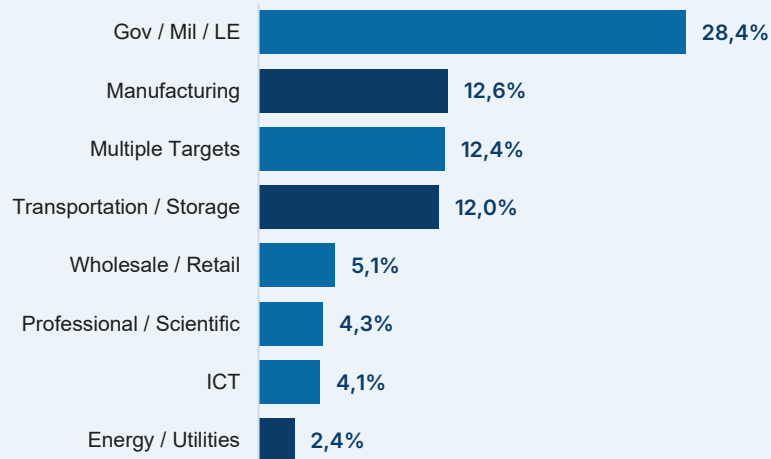
CONFINDUSTRIA
VENETO EST

START4.0

Vittime in Italia: manifattura e trasporti in testa

Il 16% degli incidenti al settore manifatturiero censiti nel mondo riguarda aziende italiane

Distribuzione delle vittime in Italia, 2025



La specificità italiana

- ▼ **64 su 400:** incidenti al Manufacturing nel mondo avvenuti in Italia
- ▼ **12,6%** delle vittime italiane è manifatturiero, contro il 7,6% globale
- ▼ **+134,6%** trasporti e logistica: da 26 a 61 incidenti
- ▼ **2,4%** energy e utilities, in peggioramento rispetto al 2024
- ▼ Aziende medio-piccole, spesso poco mature: difficile separare aumento degli attacchi e debolezza della postura

Fonte: Rapporto Clusit 2026 sulla Cybersecurity in Italia e nel mondo



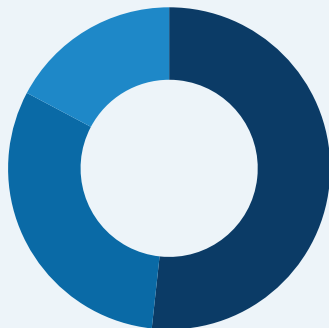
CONFINDUSTRIA
VENETO EST

START4.0

Focus IACS: il perimetro dell'analisi

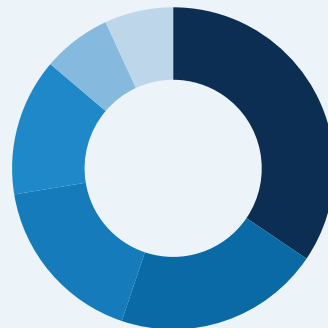
Gap analysis e risk assessment su Asset Owner, Integration Service Provider e Product Supplier

Attività per profilo



- Asset Owner
- Integration Service Provider
- Product Supplier

Attività per settore



- Energetico
- Logistica e trasporti
- Manifatturiero
- Alimentare e bevande
- Metallurgico
- Costruzioni

Asset Owner

IEC 62443-2-1:2024 · spinta dalla NIS2 (D.Lgs. 138/2024)

Integration Service Provider

IEC 62443-3-2 e 3-3 · spinta dal Regolamento Macchine e dal Data Act

Product Supplier

IEC 62443-4-1 e 4-2 · spinta dal Cyber Resilience Act

Fonte: Rapporto Clusit 2026, Focus On "Cybersecurity IACS e Compliance Normativa" (pp. 280-303), dati Q4 2024 – Q4 2025

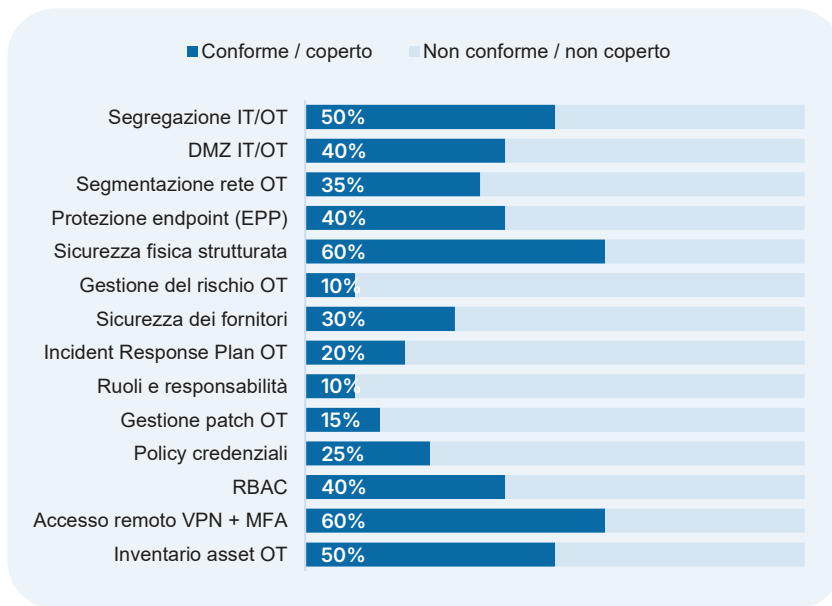


CONFINDUSTRIA
VENETO EST

START4.0

Asset Owner: misure presenti, ma non governate

Quota di Asset Owner conformi ai requisiti di IEC 62443-2-1:2024 (valori arrotondati)



90%

dei firewall IT/OT con
regole mai riviste

15%

degli inventari è
davvero completo

65%

usa credenziali deboli
anche su ruoli
privilegiati

5%

testa periodicamente il
piano di risposta

Fonte: Rapporto Clusit 2026, Focus On "Cybersecurity IACS e Compliance Normativa" (pp. 280-303), dati Q4 2024 – Q4 2025

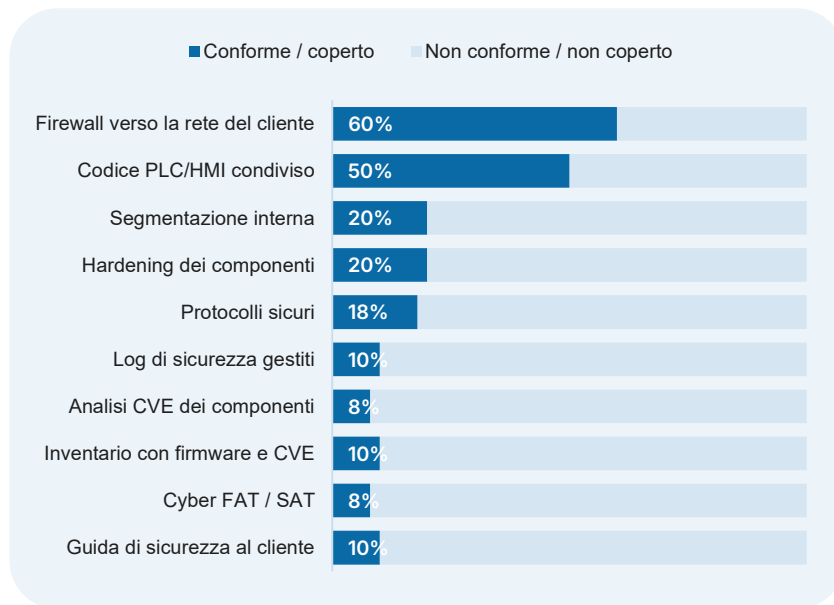


CONFINDUSTRIA
VENETO EST

START4.0

Integratori: il macchinario come porta d'ingresso

Quota di sistemi forniti che coprono i requisiti di IEC 62443-3-2 e 3-3 (valori arrotondati)



60%

usa gateway
GSM/4G/5G per
l'accesso remoto,
spesso non protetti

90%

dei firewall installati
lavora solo a livello 3

50%

sviluppa codice
compilato: diventa
product supplier per il
CRA

CVSS>7

firmware vulnerabili su
macchine nuove

Fonte: Rapporto Clusit 2026, Focus On "Cybersecurity IACS e Compliance Normativa" (pp. 280-303), dati Q4 2024 – Q4 2025

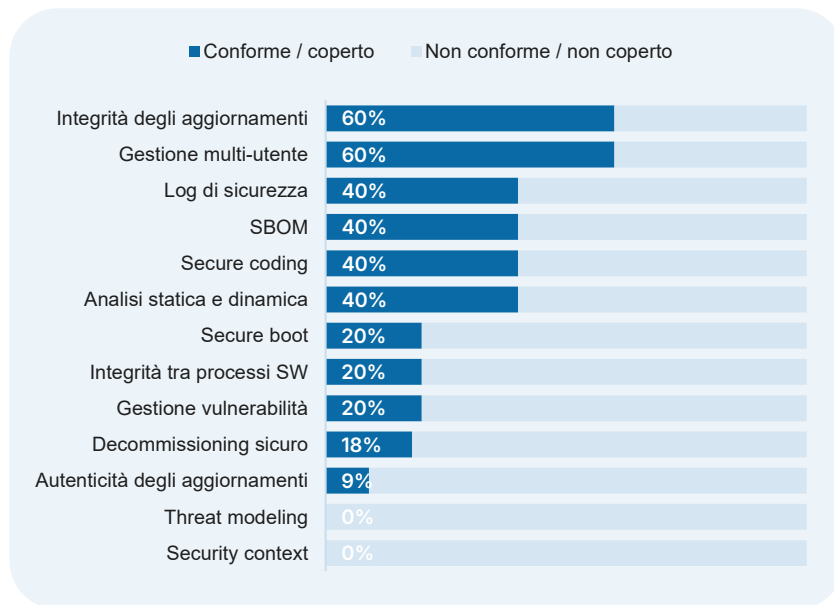


CONFINDUSTRIA
VENETO EST

START4.0

Product Supplier: security by design ancora lontana

Quota di componenti e processi che coprono i requisiti di IEC 62443-4-1 e 4-2 (valori arrotondati)



0

product supplier con
threat model o
security context

15%

verifica anche
l'autenticità del
firmware

5%

integra la gestione
utenti con sistemi
centralizzati

40%

genera log, ma solo in
locale

Fonte: Rapporto Clusit 2026, Focus On "Cybersecurity IACS e Compliance Normativa" (pp. 280-303), dati Q4 2024 – Q4 2025

Cosa ci dicono i dati italiani

Il rischio non è l'assenza di misure, ma frammentazione, scarsa visibilità e nessuna verifica di efficacia



Asset Owner

Postura reattiva, guidata dagli obblighi: reti piatte, credenziali deboli, piani mai testati.



Integratori

Focus su funzione e costo: niente hardening, accessi GSM diretti, niente log e quasi mai Cyber FAT/SAT.



Product Supplier

Security by design assente: niente threat model, vulnerabilità gestite poco, SBOM incomplete.

Dall'adempimento formale

→ alla gestione sostanziale del rischio

Dalla sicurezza aggiunta

→ alla sicurezza integrata nel ciclo di vita

Dalla responsabilità del singolo

→ alla responsabilità condivisa nella supply chain

Fonte: Rapporto Clusit 2026, Focus On "Cybersecurity IACS e Compliance Normativa" (pp. 280-303), dati Q4 2024 – Q4 2025



CONFINDUSTRIA
VENETO EST

START4.0



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

SEZIONE 03

Caso studio: l'attacco alla rete energetica polacca

29 dicembre 2025: il contesto e i target

Il primo grande attacco coordinato alle risorse energetiche distribuite (DER)

 **30+**

impianti eolici e fotovoltaici, attaccati nei punti di connessione alla rete (GCP)

 **~500.000**

utenti serviti dal grande impianto di cogenerazione (CHP) colpito

 **~50.000**

residenti serviti da un secondo CHP, emerso dall'analisi di follow-up

 **1**

azienda manifatturiera privata colpita con un wiper dedicato

Perché conta

- ✦ Attacco in pieno inverno, contro calore ed elettricità per i civili
- ✦ La Polonia produce oltre il 50% dell'energia da carbone; eolico e solare valgono circa il 25% della capacità
- ✦ DER: centinaia di piccoli siti, margini ridotti, molta connettività remota e pochi investimenti cyber
- ✦ Siti tutti sotto le soglie che fanno scattare gli obblighi cyber più stringenti

Fonti: CERT Polska, Incident Report (30/01/2026) e Follow-up Analysis (2026); Dragos, ELECTRUM intelligence brief (gen. 2026)

Chi c'è dietro: un'attribuzione contesa

Le analisi divergono sul nome del gruppo, ma convergono su attori statali legati alla Russia



CERT Polska

- ✔ Static Tundra, alias Berserk Bear, Dragonfly, Ghost Blizzard, Energetic Bear
- ✔ Cluster ritenuto legato al Centro 16 dell'FSB
- ✔ Prima attività distruttiva attribuita pubblicamente al gruppo
- ✔ Anche ENISA TL 2026 cita DragonFly



Dragos

- ✔ ELECTRUM, in parte sovrapposto a Sandworm (confidenza moderata)
- ✔ Autore degli attacchi in Ucraina del 2015 e 2016 (CRASHOVERRIDE)
- ✔ Industroyer2, CaddyWiper e attacco a KA-SAT nel 2022



ESET

- ✔ Sandworm, con confidenza moderata
- ✔ Sovrapposizioni tattiche con operazioni precedenti
- ✔ Storico nel settore energetico: BlackEnergy, GreyEnergy

Per chi difende conta il metodo: gli stessi punti deboli sono sfruttabili da qualsiasi attore, statale o criminale.

Fonti: CERT Polska, Incident Report (30/01/2026) e Follow-up Analysis (2026); Dragos, ELECTRUM intelligence brief (gen. 2026); ESET; ENISA TL 2026

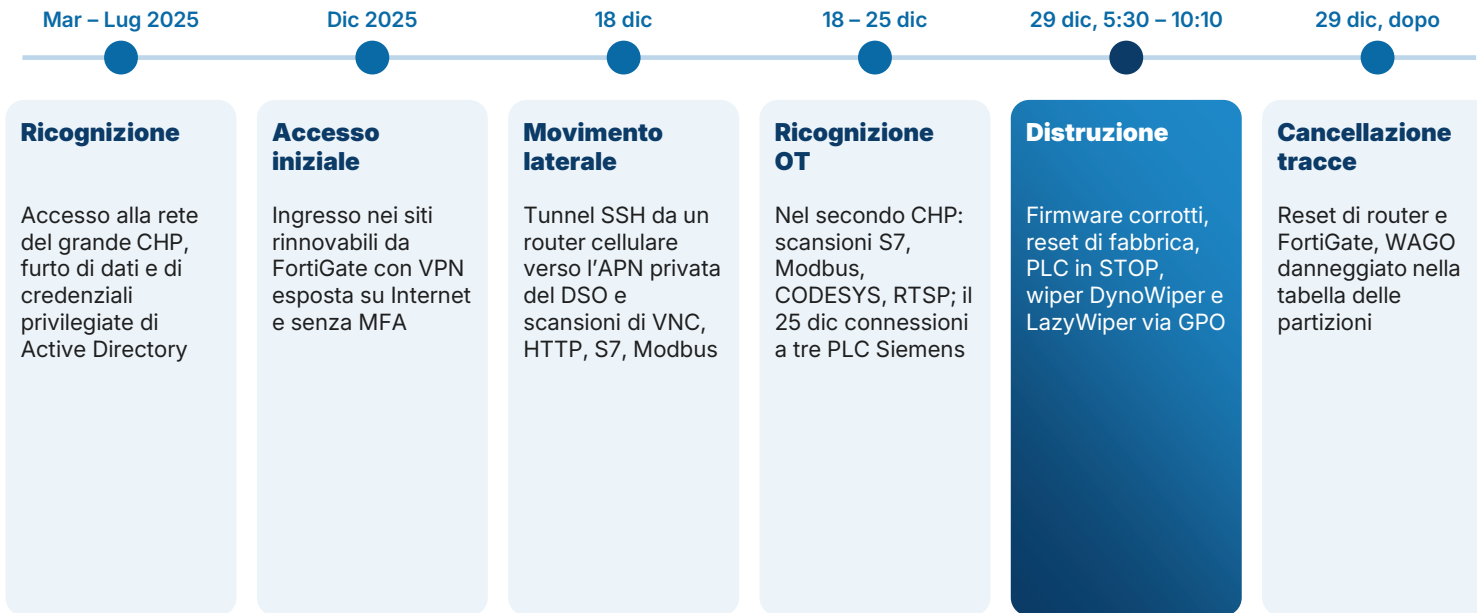


CONFINDUSTRIA
VENETO EST

START4.0

Le fasi dell'attacco

Mesi di preparazione, una settimana di ricognizione OT, cinque ore di azioni distruttive



Fonti: CERT Polska, Incident Report (30/01/2026) e Follow-up Analysis (2026); Dragos, ELECTRUM intelligence brief (gen. 2026)

Il vettore inedito: dalla wind farm alla centrale

CERT Polska: primo caso osservato di accesso a una rete OT attraverso una APN privata



Il punto cieco: il DSO imponeva solo DNP3 seriale verso la RTU, ma nessun requisito sull'interfaccia di amministrazione del router, collegata alla VLAN gestita dal firewall già compromesso.

Fonti: CERT Polska, Incident Report (30/01/2026) e Follow-up Analysis (2026); Dragos, ELECTRUM intelligence brief (gen. 2026)

Le vulnerabilità sfruttate

Quasi tutte configurazioni lasciate come in fabbrica: un solo CVE citato in tutta l'operazione

Dispositivo	Debolezza	Effetto ottenuto
FortiGate (VPN e firewall)	VPN esposta, account locali senza MFA; in un caso configurazione già trafugata online	Accesso iniziale con privilegi amministrativi
Router Teltonika RUTX50	Web e SSH di gestione raggiungibili dalla rete interna	Tunnel SSH verso l'APN privata
APN privata del DSO	Nessun isolamento tra i dispositivi collegati	Movimento laterale tra siti diversi
WAGO PFC200	Web su WAN con credenziali di default "admin"	SSH abilitato e accesso alla rete OT del CHP
RTU Hitachi RTU560	Account "Default"; CVE-2024-2617 (bypass del secure update)	Firmware corrotto: dispositivo in reboot loop
Mikronika, Moxa NPort, relè Hitachi Relion	Credenziali di default; SSH root, web e FTP attivi	File cancellati, reset di fabbrica, IP 127.0.0.1
PLC Siemens S7	Nessuna protezione di accesso o modifica della logica	PLC in STOP e bloccati con password
Active Directory	Credenziali privilegiate rubate mesi prima	Wiper distribuiti via Group Policy

Fonti: CERT Polska, Incident Report (30/01/2026) e Follow-up Analysis (2026); Dragos, ELECTRUM intelligence brief (gen. 2026)



Il risultato dell'attacco

Nessun blackout, ma accesso a sistemi OT critici e apparati distrutti in modo irreversibile

0

interruzioni di elettricità o calore per i clienti finali

30+

siti rinnovabili senza comunicazione con il DSO; la produzione prosegue

~5 h

di presenza nella rete OT del secondo CHP: turbina a vapore e trattamento acque fermi

1,2 GW

generazione potenzialmente coinvolta, circa il 5% del picco di 30 GW (stima Dragos)



Cosa ha limitato i danni

- ✓ L'EDR ha bloccato il wiper nel grande CHP
- ✓ Risposta rapida degli operatori del secondo CHP
- ✓ Inerzia del sistema (carbone) e interconnessioni con i paesi vicini



Cosa ha complicato la risposta

- ✓ RTU e controllori resi inutilizzabili, non ripristinabili sul posto
- ✓ Reset di fabbrica che hanno cancellato i log
- ✓ Evento scambiato all'inizio per un errore del manutentore

Fonti: CERT Polska, Incident Report (30/01/2026) e Follow-up Analysis (2026); Dragos, ELECTRUM intelligence brief (gen. 2026)



CONFINDUSTRIA
VENETO EST

START4.0

Riassunto: misconfigurazione e commissioning

Nessuno zero-day decisivo: l'attacco ha sfruttato ciò che nessuno aveva verificato alla messa in servizio

Ancora oggi le principali vulnerabilità sono la misconfigurazione e una fase di commissioning non controllata

Ciò che è successo in Polonia trova riscontro diretto nei dati raccolti negli impianti italiani.

In Polonia	In Italia (Clusit 2026, Focus IACS)
Credenziali di default su RTU, controllori, serial server e relè	75% degli Asset Owner senza policy sulle credenziali; 65% con credenziali deboli su ruoli privilegiati
Interfacce di gestione non necessarie attive: web, SSH, FTP	Hardening applicato da circa il 20% degli integratori
VPN senza MFA e accessi attraverso la rete cellulare	60% degli integratori usa gateway GSM, spesso senza protezioni aggiuntive
Requisiti di messa in servizio solo funzionali, nessuna verifica di sicurezza	Meno del 10% esegue Cyber FAT e Cyber SAT
Log assenti o persi durante il ripristino	Solo il 10% dei macchinari gestisce log di sicurezza

Fonti: CERT Polska, Incident Report (30/01/2026) e Follow-up Analysis (2026); Dragos, ELECTRUM intelligence brief (gen. 2026); Clusit 2026 Focus IACS



Cosa avrebbe fatto la differenza

Controlli di base, verificabili al collaudo e mappati sulla IEC 62443-3-3



Credenziali

Cambio obbligatorio al commissioning, account nominativi

SR 1.1, SR 1.5



Hardening

Disabilitare servizi e interfacce non necessari (web, SSH, FTP)

SR 7.7



Zone e condotti

APN e reti dei fornitori trattate come non fidate, traffico in allowlist

IEC 62443-3-2 · SR 5.1



Accesso remoto

MFA, sessioni a tempo, inventario di chi accede a quali siti

SR 1.13



Visibilità

Log centralizzati e monitoraggio dei protocolli OT (S7, Modbus, DNP3)

SR 2.8 · SR 6.2



Cyber FAT / SAT

Verifica documentata della configurazione prima della consegna

IEC 62443-2-4

Fonti: CERT Polska, Incident Report (30/01/2026) e Follow-up Analysis (2026); Dragos, ELECTRUM intelligence brief (gen. 2026); IEC 62443-3-3; SANS ICS Five Critical Controls



CONFINDUSTRIA
VENETO EST

START4.0



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

SEZIONE 04

Il quadro normativo europeo

Tre atti, tre ruoli, un linguaggio comune

Ogni atto si rivolge a un anello diverso della filiera; la IEC 62443 è il riferimento tecnico che li collega



NIS2

Dir. (UE) 2022/2555 · D.Lgs.
138/2024

Asset Owner: soggetti essenziali e importanti

Gestione del rischio
dell'organizzazione, supply chain e
notifica degli incidenti

IEC 62443-2-1 · 2-4 · 3-2 · 3-3



Regolamento Macchine

Reg. (UE) 2023/1230

Costruttori e integratori di macchine

Protezione contro la corruzione delle
funzioni di sicurezza

prEN 50742 → IEC 62443



Cyber Resilience Act

Reg. (UE) 2024/2847

**Product Supplier: fabbricanti,
importatori, distributori**

Prodotti con elementi digitali sicuri per
tutto il ciclo di vita

prEN 40000 · EN IEC 62443-4-1 · 4-2

IEC 62443-2-x

Politiche e procedure dell'Asset Owner e
dei service provider

IEC 62443-3-x

Sistema: rischio, zone e condotti, requisiti
di sistema e SL

IEC 62443-4-x

Componente: ciclo di sviluppo sicuro e
requisiti tecnici

Fonti: Dir. (UE) 2022/2555; D.Lgs. 138/2024; Reg. (UE) 2024/2847; Reg. (UE) 2023/1230; serie IEC 62443

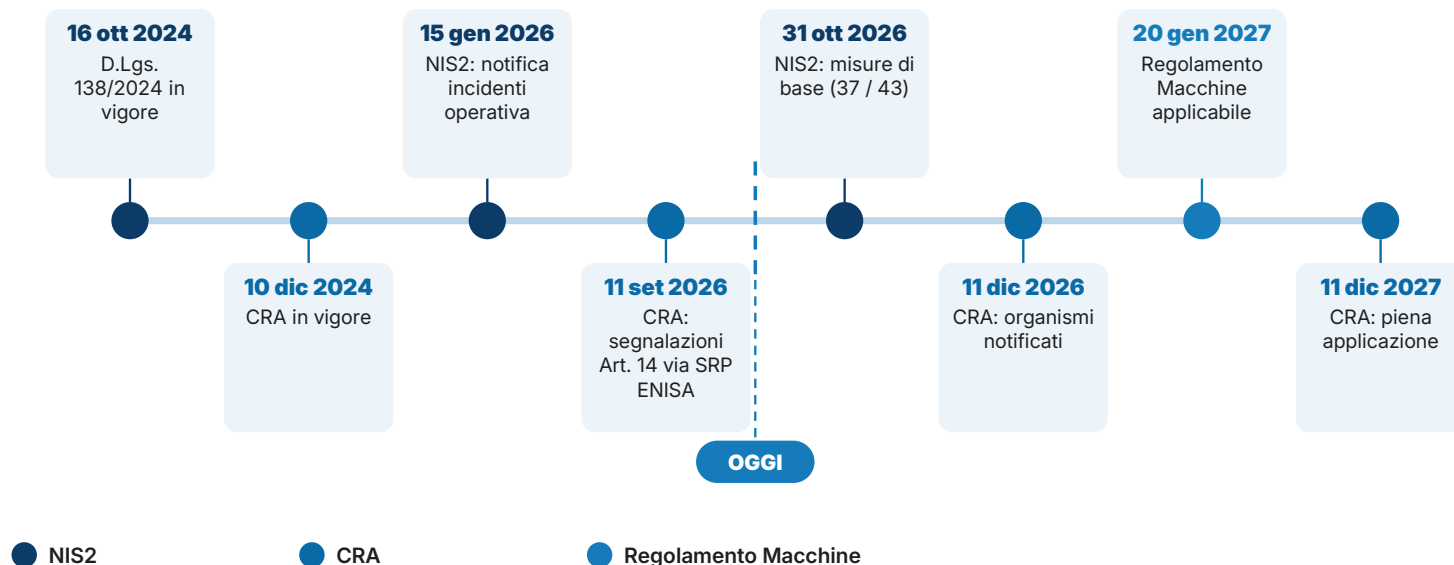


CONFINDUSTRIA
VENETO EST

START4.0

Le scadenze

Notifiche già operative, misure di base NIS2 a fine mese, Regolamento Macchine tra tre mesi



Fonti: Determinazione ACN 379907/2025; Reg. (UE) 2024/2847, art. 71; Reg. (UE) 2023/1230, art. 54; Commissione europea

NIS2: chi è coinvolto

Con la NIS2 l'industria manifatturiera entra nel perimetro accanto a energia, acqua e trasporti



Settori ad alta criticità

- ✦ Energia: elettricità, teleriscaldamento, petrolio, gas, idrogeno
- ✦ Trasporti aerei, ferroviari, marittimi, stradali
- ✦ Acqua potabile e acque reflue
- ✦ Sanità, infrastrutture digitali, PA



Altri settori critici

- ✦ Fabbricazione: macchinari, apparecchiature elettriche, elettronica, autoveicoli, mezzi di trasporto, dispositivi medici
- ✦ Fabbricazione e distribuzione di sostanze chimiche
- ✦ Produzione e distribuzione di alimenti
- ✦ Gestione dei rifiuti

Gli attori

- ✦ **Soggetti essenziali e importanti:** medie e grandi imprese dei settori, più alcuni casi a prescindere dalla dimensione
- ✦ **ACN:** autorità nazionale competente NIS e punto di contatto unico
- ✦ **CSIRT Italia:** riceve le notifiche di incidente
- ✦ **Organi di amministrazione:** approvano le misure e ne rispondono
- ✦ **Fornitori:** coinvolti tramite la sicurezza della supply chain

Fonti: Dir. (UE) 2022/2555, Allegati I e II; D.Lgs. 138/2024



CONFINDUSTRIA
VENETO EST

START4.0

NIS2: obblighi e scadenze

Governance, gestione del rischio e notifica: dal 31 ottobre 2026 le misure di base devono essere adottate



Governance

Gli organi di amministrazione approvano le misure, ne sovrintendono l'attuazione, seguono formazione e rispondono delle violazioni.



Gestione del rischio

Misure tecniche e organizzative: analisi dei rischi, incidenti, continuità, supply chain, sviluppo sicuro, efficacia, formazione, crittografia, accessi, MFA.



Notifica al CSIRT Italia

Preallarme entro 24 ore, notifica entro 72 ore, relazione finale entro un mese.

Scadenze in Italia

15 gennaio 2026 – notifica degli incidenti operativa

31 ottobre 2026 – misure di base adottate: 37 per i soggetti importanti, 43 per gli essenziali

Ogni anno, 1 gen – 28 feb – aggiornamento della registrazione sul portale ACN

Sanzioni

Essenziali: fino a 10 M€ o 2% del fatturato mondiale
Importanti: fino a 7 M€ o 1,4% del fatturato mondiale

Fonti: Dir. (UE) 2022/2555, artt. 20, 21, 23, 34; D.Lgs. 138/2024, artt. 23-25; Determinazione ACN 379907/2025 (24/12/2025)



CONFINDUSTRIA
VENETO EST

START4.0

NIS2 e IEC 62443: dalla misura al controllo OT

La NIS2 non prevede norme armonizzate: per l'OT la IEC 62443 traduce le misure in requisiti verificabili

Misura NIS2 (art. 21 Dir.)	IEC 62443	Esempio in impianto
Analisi dei rischi e politiche di sicurezza	2-1 · 3-2	Risk assessment, zone e condotti, SL target
Gestione degli incidenti	2-1 · 3-3 FR6	Piano di risposta OT testato, log e monitoraggio
Continuità operativa e backup	2-1 · 3-3 FR7	Backup della logica PLC e procedure di ripristino
Sicurezza della supply chain	2-4 · 4-1	Requisiti a integratori e fornitori, Cyber FAT/SAT
Acquisizione, sviluppo e manutenzione sicuri	TR 2-3 · 2-1	Gestione di patch e vulnerabilità OT
Controllo accessi, gestione asset, MFA	3-3 FR1 · FR2	RBAC, MFA per l'accesso remoto, inventario completo
Crittografia e comunicazioni sicure	3-3 FR3 · FR4	Protocolli sicuri: OPC UA, TLS
Valutazione dell'efficacia delle misure	2-1 · 3-3	Audit, test periodici, indicatori

Riferimenti: Reg. es. (UE) 2024/2690; ENISA Technical implementation guidance; Det. ACN 379907/2025. Mappatura: elaborazione Y Cyber



CRA: attori e classificazione dei prodotti

Ogni anello della filiera ha obblighi propri; la classe decide il percorso di valutazione

Fabbricante

Requisiti Allegato I, valutazione, marcatura CE, vulnerabilità, segnalazioni

Importatore

Immette prodotti extra-UE: verifica conformità e documenti

Distributore

Verifica marcatura CE, blocca e segnala i non conformi

Diventa fabbricante

chi vende col proprio marchio o fa una modifica sostanziale

Default

~90% dei prodotti

PLC, HMI, sensori, software applicativo, macchinari

Valutazione

Autovalutazione (Modulo A)

Classe I

Importanti, All. III

Router, switch, modem, VPN, SIEM, sistemi operativi

Valutazione

Modulo A con norma armonizzata, altrimenti terza parte

Classe II

Importanti, All. III

Firewall, IDS/IPS, hypervisor, microcontrollori tamper-resistant

Valutazione

Terza parte (Moduli B+C o H)

Critici

All. IV

Smart meter gateway, smartcard, secure element

Valutazione

EUCC se richiesta da atto delegato

Fonti: Reg. (UE) 2024/2847, artt. 13-22, 32, Allegati III-IV; Reg. di esecuzione (UE) 2025/2392



CONFINDUSTRIA
VENETO EST

START4.0

CRA: obblighi e scadenze

Sicurezza by design e gestione delle vulnerabilità per tutto il periodo di supporto



Allegato I, Parte I

- ✔ Nessuna vulnerabilità sfruttabile nota
- ✔ Configurazione sicura di default
- ✔ Superficie d'attacco limitata
- ✔ Controllo accessi, integrità, riservatezza
- ✔ Log e aggiornamenti di sicurezza



Allegato I, Parte II

- ✔ SBOM almeno delle dipendenze di primo livello
- ✔ Politica di divulgazione coordinata (CVD)
- ✔ Correzioni rapide e aggiornamenti gratuiti
- ✔ Advisory pubblici
- ✔ Supporto per almeno 5 anni

Art. 14: segnalazione

Vulnerabilità attivamente sfruttate e incidenti gravi, via Single Reporting Platform ENISA

24 h preallarme · **72 h** notifica

14 gg / 1 mese rapporto finale

Date chiave

11 set 2026 segnalazioni attive

11 dic 2027 piena applicazione

Sanzioni fino a 15 M€ o 2,5% del fatturato

Fonti: Reg. (UE) 2024/2847, artt. 13, 14, 64, 71, Allegato I; Guida CE C(2026) 5252



CONFINDUSTRIA
VENETO EST

START4.0

CRA: norme armonizzate e IEC 62443

Richiesta di normazione M/606: norme orizzontali, verticali e la serie IEC 62443 per i componenti OT

Il pacchetto normativo

- ▼ **prEN 40000-1-1/-2/-3:** vocabolario, principi di cyber resilienza, gestione vulnerabilità
- ▼ **~38 norme verticali** per le categorie degli Allegati III e IV
- ▼ **EN IEC 62443-4-1 e 4-2 prAA:** adattamento per i componenti industriali
- ▼ **prEN 50770:** profili per firewall, router, VPN, SIEM
- ▼ **Punto aperto:** presunzione via 62443 per i prodotti Default da confermare

Requisito CRA	IEC 62443
Valutazione del rischio e requisiti (Parte I)	4-1 Practice 1 SM, Practice 2 SR
Sicuro by design, superficie d'attacco ridotta	4-1 Practice 3 SD · 4-2 CR 7.7
Configurazione sicura di default	4-1 Practice 8 SG (linee guida)
Controllo accessi e autenticazione	4-2 FR1 · FR2
Integrità e riservatezza di dati e comandi	4-2 FR3 · FR4
Log e monitoraggio degli eventi	4-2 CR 2.8 · FR6
Disponibilità e resilienza a DoS	4-2 FR7
Vulnerabilità, CVD, SBOM (Parte II)	4-1 Practice 6 DM
Aggiornamenti sicuri	4-1 Practice 7 SUM · 4-2 CR 3.10
Test di sicurezza	4-1 Practice 5 SVV

Fonti: Commissione europea, CRA Standardisation; VDMA, CRA Status Update (mar. 2026); CENELEC TC 65X. Mappatura: elaborazione Y Cyber





CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

SEZIONE 05

Regolamento Macchine e prEN 50742

Regolamento Machine e cybersecurity

Dal 20 gennaio 2027 la protezione contro la corruzione è condizione per la marcatura CE

RES 1.1.9

Protezione contro la corruzione

Un dispositivo collegato o remoto non deve portare a situazioni pericolose. Hardware, software e dati critici per la sicurezza vanno protetti dalla corruzione accidentale o intenzionale e gli interventi devono lasciare evidenze.

RES 1.2.1

Sicurezza dei sistemi di comando

a) Resistere a tentativi dolosi ragionevolmente prevedibili di terzi. f) Tracciare gli interventi e le versioni del software di sicurezza caricate, conservando i dati per cinque anni.

Attori e date

- ✦ Fabbricante, mandatario, importatore, distributore
- ✦ Chi apporta una modifica sostanziale diventa fabbricante
- ✦ Allegato I, Parte A: componenti di sicurezza e macchine con comportamento autoevolutivo (machine learning) richiedono un organismo notificato
- ✦ **20 gen 2027:** applicazione e abrogazione della 2006/42/CE

Fonti: Reg. (UE) 2023/1230, artt. 3, 18, 25, 54, Allegato I e Allegato III



CONFINDUSTRIA
VENETO EST

START4.0

prEN 50742: protezione contro la corruzione

FprEN 50742:2026 al voto formale CENELEC fino al 9 ottobre 2026: il testo può ancora cambiare



Aspetto	Approccio A	Approccio B
Per chi	Macchine sviluppate senza riferimento alla IEC 62443	Macchine sviluppate nel contesto della IEC 62443
Processo	Cl. 5: security risk assessment innestato sulla ISO 12100	Cl. 6: security risk assessment e IEC 62443-4-1
Requisiti tecnici	Cl. 7: livelli SRSLO–SRSL3 per interfaccia	Cl. 8: sottoinsieme di SR (62443-3-3) e CR (62443-4-2)
Tracciabilità	Evidenze e tracing log conservato 5 anni (7.3)	Audit record persistenti per 5 anni (8.5)

Sempre valide: Clausola 4 (requisiti generali) e Clausola 9 (informazioni per l'uso). I due approcci si possono combinare a livello di componente nella stessa macchina.

Fonti: FprEN 50742:2026, Tabella 1, Annex ZZ; materiale corso EN 50742 Approccio A; IBF Solutions, prEN 50742 (2026)

Safety e security: due logiche, un obiettivo

Le vulnerabilità non creano nuovi pericoli, ma possono compromettere le misure di protezione

	Safety	Security
Origine	Guasti casuali e sistematici, uso scorretto	Minacce intenzionali e corruzione accidentale
Norme	ISO 12100, ISO 13849, IEC 62061	prEN 50742, IEC 62443
Metrica	PLr o SIL della funzione	SRSL per interfaccia, SL per zona
Natura	Definita in progetto, stabile	Dinamica: l'attack complexity cambia nel tempo
Confini	Uso previsto	Security context
Ciclo di vita	Validazione prima della consegna	Monitoraggio delle nuove minacce

Fonti: FprEN 50742:2026, Introduzione, Cl. 5.1, 7.4.1, Annex B; EN ISO 12100; IEC 62443

Tre principi per tutto il processo

1. La security non deve peggiorare la safety.

Una funzione crittografica può allungare il tempo di risposta della funzione di sicurezza.

2. L'attacco malevolo non si può escludere. La possibilità che qualcuno sfrutti una vulnerabilità va sempre considerata.

3. La valutazione va tenuta aggiornata finché la macchina è in produzione: nuove minacce, nuova analisi.



Il processo dell'Approccio A

La security risk assessment si innesta sulla valutazione dei rischi ISO 12100, non corre in parallelo



🔄 Ogni contromisura riporta al passo 0: può modificare il comportamento della funzione di sicurezza.

Fonte: FprEN 50742:2026, Clausola 5 e Figura 1; Annex B e C



CONFINDUSTRIA
VENETO EST

START4.0

Dall'interfaccia all'SRSL

L'Annex B rende quantitativa la probabilità: attack potential e severità determinano il livello

$$AP = (EL \times WoO) + AC$$

Exposure Level	Punti
EL0 interno (chiave o attrezzi)	0
EL1 porte fisiche: USB, RJ45, display	2
EL2 rete locale, fieldbus	6
EL3 rete di stabilimento	11
EL4 rete IT aziendale	18
EL5 Internet, radio remota, rete mobile	33

WoO finestra di opportunità: da 0,6 a 1 per tutta la macchina

AC attack complexity: da 1 (esperti) a 4 (abilità di base)

Severità / AP	AP0	AP1	AP2	AP3	AP4
Bassa (reversibile)	SRSL0	SRSL1	SRSL1	SRSL2	SRSL3
Alta (irreversibile)	SRSL0	SRSL1	SRSL2	SRSL3	SRSL3

SRSL1

- ✓ Entità autenticate
- ✓ Interventi autorizzati
- ✓ Integrità all'avvio (checksum)
- ✓ Validazione input

SRSL2

- ✓ Come SRSL1
- ✓ Integrità anche periodica
- ✓ Autenticità del software di sicurezza

SRSL3

- ✓ Autenticazione univoca, RBAC
- ✓ HMAC o CMAC
- ✓ Secure boot
- ✓ Canali crittografici anti-replay

Fonte: FprEN 50742:2026, Annex B (Tabelle B.1-B.6) e Clausola 7.4.3 (sintesi)



CONFINDUSTRIA
VENETO EST

START4.0

prEN 50742 e IEC 62443: la mappatura

I requisiti dell'Approccio A trovano corrispondenza nei requisiti di componente della IEC 62443-4-2

Requisito prEN 50742 (Approccio A)	SRSL1 – SRSL2	SRSL3	IEC 62443-4-2 / 3-3
Autenticazione (7.4.3.2)	Entità autenticate	Autenticazione univoca	CR 1.1 · CR 1.2 / SR 1.1, 1.2
Autorizzazione (7.4.3.3)	Interventi autorizzati	Privilegi per ruolo (RBAC)	CR 2.1 / SR 2.1
Integrità di software e dati (7.4.3.4.1)	Checksum all'avvio (e periodico)	HMAC o CMAC	CR 3.4
Integrità del boot (7.4.3.4.2)	Checksum all'avvio	Secure boot, radici di fiducia	EDR / HDR 3.14
Integrità degli scambi (7.4.3.4.3)	Checksum	Crittografica, anti-replay	CR 3.1 / SR 3.1
Validazione degli input (7.4.3.4.4)	Sì	Sì	CR 3.5 / SR 3.5
Autenticità del software di sicurezza (7.4.3.5.1)	Solo SRSL2: verificata	Firme crittografiche	CR 3.4 RE(1)
Evidenze e tracing log 5 anni (7.3)	Sempre richiesti	Sempre richiesti	CR 2.8 · CR 2.9 / SR 2.8

Approccio B: processo secondo IEC 62443-4-1 e un sottoinsieme di SR della 3-3 e di CR della 4-2, con audit record per 5 anni.

Fonti: FprEN 50742:2026, Cl. 7.3-7.4 e Cl. 8; IEC 62443-4-2:2019; IEC 62443-3-3:2013. Mappatura indicativa: elaborazione Y Cyber



Esercizio: la prEN 50742 applicata al caso polacco

Che SRSL avrebbe avuto l'interfaccia web del controllore WAGO raggiungibile dall'APN privata?

Exposure Level

Rete mobile e radio remota → EL5

33

Window of Opportunity

Accesso possibile sempre → illimitata

× 1

Attack Complexity

Credenziali di default, strumenti standard

+ 4

Attack Potential

$(33 \times 1) + 4 = 37 \rightarrow$ oltre 20

AP4

Tabella B.6: AP4 → SRSL3 con qualsiasi severità

Cosa avrebbe richiesto SRSL3

- ✓ **Autenticazione univoca:** nessun account "admin" con password di fabbrica
- ✓ **Autorizzazione per ruoli:** mettere in STOP o cambiare la password di un PLC solo per ruoli dedicati
- ✓ **Integrità crittografica e secure boot:** firmware corrotto rifiutato invece del reboot loop
- ✓ **Tracing log per 5 anni:** evidenze non perse con il reset di fabbrica
- ✓ **Informazioni per l'uso:** security context dichiarato, APN trattata come rete non fidata

Esercizio didattico su dati CERT Polska; metodo FprEN 50742:2026, Annex B



CONFINDUSTRIA
VENETO EST

START4.0



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

SEZIONE 06

Sfide e conclusioni

AI: più capacità, meno competenze

ENISA: l'AI abbasserà le barriere d'ingresso e aumenterà scala, automazione e velocità degli attacchi

"Nel 2026 un numero crescente di fasi della kill chain sarà probabilmente abilitato direttamente dall'AI, con possibili sperimentazioni di proof of concept senza l'uomo nel ciclo."

ENISA Threat Landscape 2026, Outlook

80–90%

delle operazioni tattiche eseguite in autonomia da un agente AI in una campagna di spionaggio statale (Anthropic, 2025)

8 min

per ottenere privilegi amministrativi in un'intrusione cloud assistita dall'AI (ENISA)

LLM

ha probabilmente scritto la funzione di sovrascrittura del wiper LazyWiper usato in Polonia (CERT Polska)

63 → 5

giorni: tempo medio di sfruttamento di una vulnerabilità, dal 2018-19 al 2023 (Mandiant)

Fonti: ENISA TL 2026; Anthropic, AI-orchestrated cyber espionage campaign (nov. 2025); CERT Polska (2026); Mandiant, Time-to-Exploit 2023



CONFINDUSTRIA
VENETO EST

START4.0

La sfida

Tre fattori che si sommano: per questo dobbiamo accelerare



Più capacità di calcolo

Modelli frontier e risorse a basso costo accelerano ricognizione, scoperta e sfruttamento delle vulnerabilità.



Meno competenze necessarie

L'AI supporta anche attaccanti poco esperti e abbassa la barriera d'ingresso.



Gestione insufficiente

Come in Polonia: credenziali di default, interfacce esposte, commissioning non verificato.

Le sfide nel mondo attuale sono l'aumento delle capacità di calcolo (risorse) e la riduzione delle skill necessarie, dovuta alla crescita degli algoritmi di AI che possono supportare gli attaccanti nello sfruttare le vulnerabilità. Se a questo si aggiunge, come nella rete polacca, una scarsa gestione, diventa sempre più fondamentale accelerare nel proteggere in maniera adeguata le nostre infrastrutture critiche.

Fonti: ENISA TL 2026; CERT Polska (2026); Rapporto Clusit 2026



CONFINDUSTRIA
VENETO EST

START4.0

Piano d'azione per ruolo

Cosa fare adesso, partendo da ciò che è già obbligatorio



Asset Owner

NIS2 · 31/10/2026

- ▼ Inventario con firmware, patch e CVE
- ▼ Segmentazione in zone e condotti
- ▼ Policy credenziali e MFA ovunque
- ▼ Piano di risposta OT testato
- ▼ Cyber FAT/SAT a contratto



Costruttori e OEM

Reg. Macchine · 20/01/2027

- ▼ Risk assessment prEN 50742 e SRSL
- ▼ Hardening, niente credenziali di default
- ▼ Accesso remoto sicuro, no gateway diretti
- ▼ Log degli interventi per 5 anni
- ▼ Security context nel manuale



Product Supplier

CRA · 11/12/2027

- ▼ Ciclo di sviluppo IEC 62443-4-1
- ▼ Threat model e security context
- ▼ SBOM e divulgazione coordinata
- ▼ Secure boot e firmware firmati
- ▼ PSIRT e segnalazioni via SRP

Fonti: D.Lgs. 138/2024; Reg. (UE) 2023/1230; Reg. (UE) 2024/2847; FprEN 50742:2026; IEC 62443. Elaborazione Y Cyber



CONFINDUSTRIA
VENETO EST

START4.0

Messaggi chiave

- ✚ La manifattura italiana è tra le più colpite al mondo: il 16% degli incidenti del settore riguarda l'Italia
- ✚ In Polonia nessuno zero-day decisivo: credenziali di default, interfacce esposte e commissioning non verificato
- ✚ NIS2, Regolamento Macchine e CRA coprono tutta la filiera; la IEC 62443 è il linguaggio comune
- ✚ La prEN 50742 lega safety e security: la security protegge le funzioni di sicurezza
- ✚ L'AI accelera gli attaccanti: la gestione di base non è più rinviabile

Come può aiutare Y Cyber

- ✚ Gap analysis NIS2 e IEC 62443-2-1
- ✚ Risk assessment IEC 62443-3-2 e prEN 50742
- ✚ Hardening, Cyber FAT e Cyber SAT
- ✚ Ciclo di sviluppo IEC 62443-4-1 e percorso CRA
- ✚ Monitoraggio OT e risposta agli incidenti





CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0



Y Cyber

HWG Sababa Group

Grazie!

www.y-cyber.com