FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

ANIE AUTOMAZIONE

Dal prodotto connesso al sistema resiliente: cosa cambia per l'automazione industriale con CRA, NRM e IEC 62443



Mauro Cerea

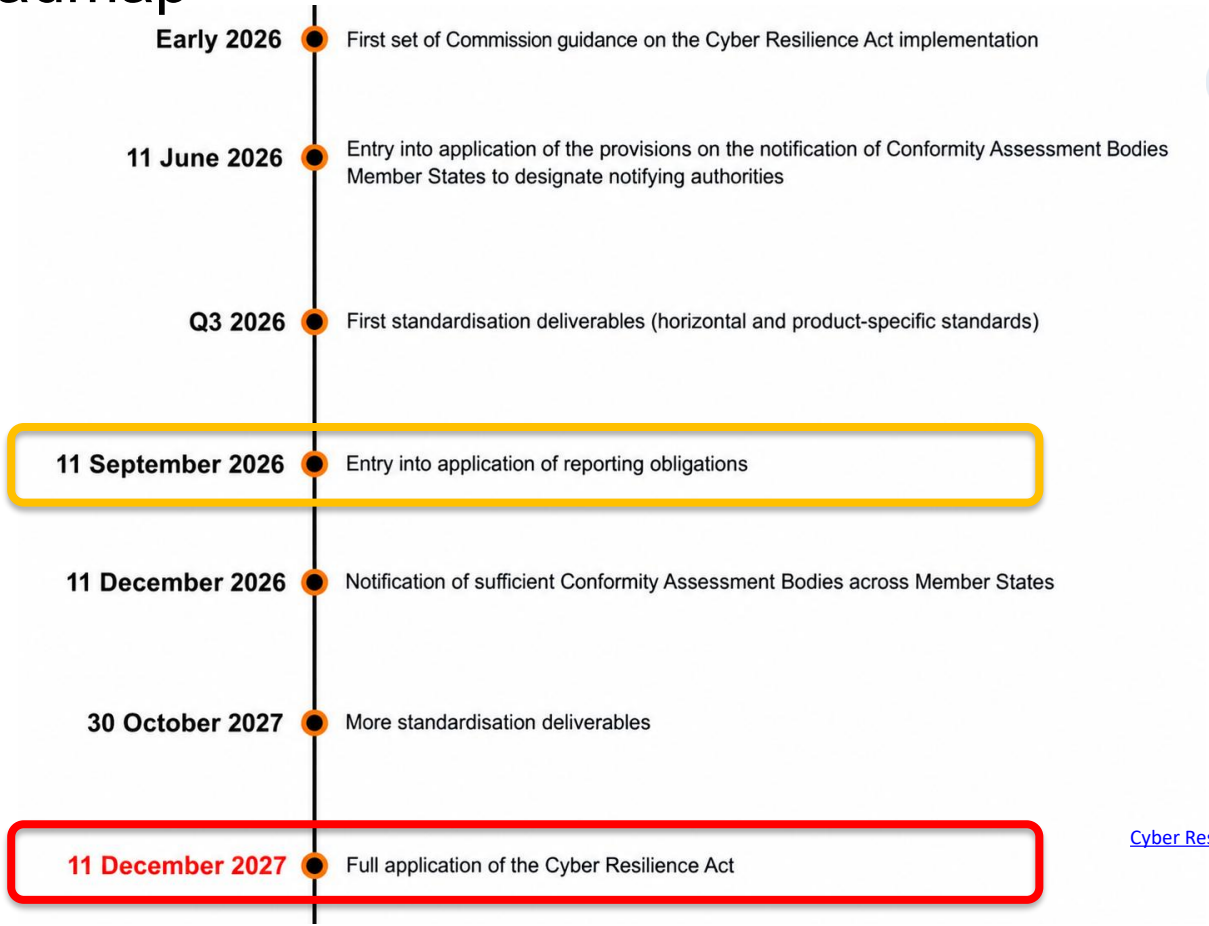
CRA: Cyber Resilience Act_Reg. (UE) 2024/2847

Cosa significa per imprese, produttori e mercato



- Il CRA è un regolamento dell'Unione Europea pensato per rafforzare la sicurezza informatica dei prodotti con elementi digitali (hardware, software, ecc.). E' direttamente applicabile, senza recepimento da parte dei suoi singoli Stati membri.
- Si inserisce nel più ampio quadro della strategia europea per la cybersecurity, insieme ad altre normative come NIS2 o Digital Operational Resilience Act (DORA), contribuendo a un approccio integrato.
- Stabilisce obblighi non solo per i produttori, ma anche per importatori, distributori e altri operatori nella filiera del prodotto; i prodotti conformi al CRA dovranno recare la marcatura CE per attestazione.
- Introduce l'obbligo di progettare prodotti che siano nativamente sicuri, seguendo la filosofia di security-by-design e security-by-default.
- Impone la gestione delle vulnerabilità durante l'intero ciclo di vita del prodotto: patch, aggiornamenti, monitoraggio, comunicazione vulnerabilità se critiche.
- Richiede notifica e trasparenza: se viene individuata una vulnerabilità sfruttabile o un incidente, i produttori **devono** comunicarlo secondo le modalità e tempistiche previste.

CRA: roadmap



Cyber Resilience Act - Implementation

CRA: standard di armonizzazione

Horizontal & Vertical: definiscono principi, termini o condizioni di riferimento.

30 agosto 2026

Pubblicazione dei primi due deliverable horizontal:

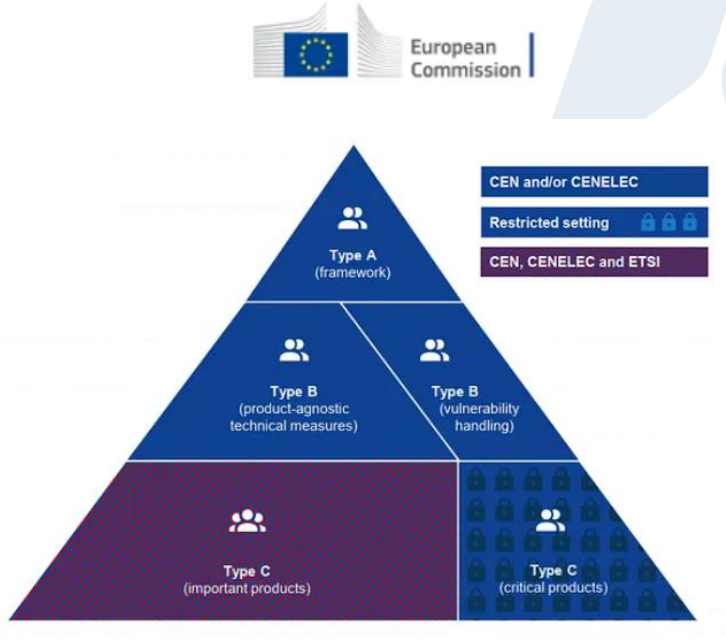
- framework/principi di cyber resilience;
- vulnerability handling.

30 ottobre 2026

Pubblicazione vertical standard/product-specific per i prodotti importanti e critici di Annex III e IV.

30 ottobre 2027

Pubblicazione di gran parte degli altri **Horizontal Standards**, cioè quelli destinati a tradurre i requisiti essenziali di **Annex I Part I** in requisiti tecnici generici.



Il termine di adozione da parte degli ESO non coincide automaticamente con la pubblicazione della citazione nell'OJEU.
È quest'ultima che rende lo standard effettivamente “harmonised standard” ai fini della **presumption of conformity** del CRA.

ESO: European Standardisation Organisation
OJEU: Official Journal of the European Union

Nuovo Regolamento Macchine

Reg. (UE) 2023/1230)

Direttiva Macchine 2006/42/CE

Requisiti

- Safety

Nuovo Regolamento Macchine

Requisiti

- Safety + Cybersecurity

Obiettivo

- Introdurre sul mercato e mettere in servizio le macchine garantendo un livello elevato di tutela della salute e di sicurezza delle persone
- Stabilire norme concernenti la libera circolazione dei prodotti rientranti nell'ambito di applicazione del presente regolamento nell'Unione.

Focus

- Requisiti di sicurezza e di tutela della salute per la progettazione e la costruzione di macchine, prodotti correlati e quasi-macchine

Destinatari

Tutti i 27 paesi EU_Applicazione 20 Gennaio 2027

Nuovo Regolamento Macchine

Standard di armonizzazione EN 50742

È una norma europea armonizzata che introduce requisiti vincolanti di cybersecurity per le macchine e si concentra sulla protezione contro attacchi informatici che possono comprometterne il funzionamento sicuro.

- Nel 2024 un comitato tecnico del CENELEC ha iniziato i lavori su una norma armonizzata prEN 50742 (Safety of machinery - Protection against corruption), per coprire le sezioni 1.1.9 e 1.2.1 del Regolamento Macchine. Questo standard è una bozza, con pubblicazione stesura finale attesa per Ottobre 2026 (*)



- Traduce i requisiti di cybersecurity del Regolamento Macchine in misure pratiche e implementabili per i costruttori di macchine.
- Non è uno standard generale di sicurezza OT, ma specifico per le macchine e orientato alla sicurezza: si applica quando le minacce informatiche possono mettere a repentaglio la sicurezza delle macchine.

La EN 50742 fornisce due approcci di implementazione:

- Un metodo autonomo incentrato sulla EN 50742 stessa.
- Uno in linea con la IEC 62443 per le organizzazioni che già hanno adottato questo standard.

(*) Come da 10° meeting "Commission Expert Group on Machinery", Bruxelles, 27 Aprile 2026

EN 50742: New draft standard for cybersecurity of machines

IEC 62443: lo standard internazionale OT

ISA

International Society of Automation. Organo riconosciuto a livello internazionale.

All'interno di ISA il comitato ISA99 è formato da più di 500 volontari di tutto il mondo. ISA99 ha creato e mantiene lo standard 62443. Collabora continuamente con altri organi quali IEC ed ISO.

ISA / IEC 62443

Standards to secure your Control Systems. E' uno standard riconosciuto a livello internazionale, adottato da diversi paesi e da diversi produttori di automazione. Descrive tutto il processo di gestione della cybersecurity degli impianti industriali, dal prodotto all'impianto completo.

ISA/IEC 62443 Series of Standards - ISA

IEC 62443 e le sue 4 aree di applicazione

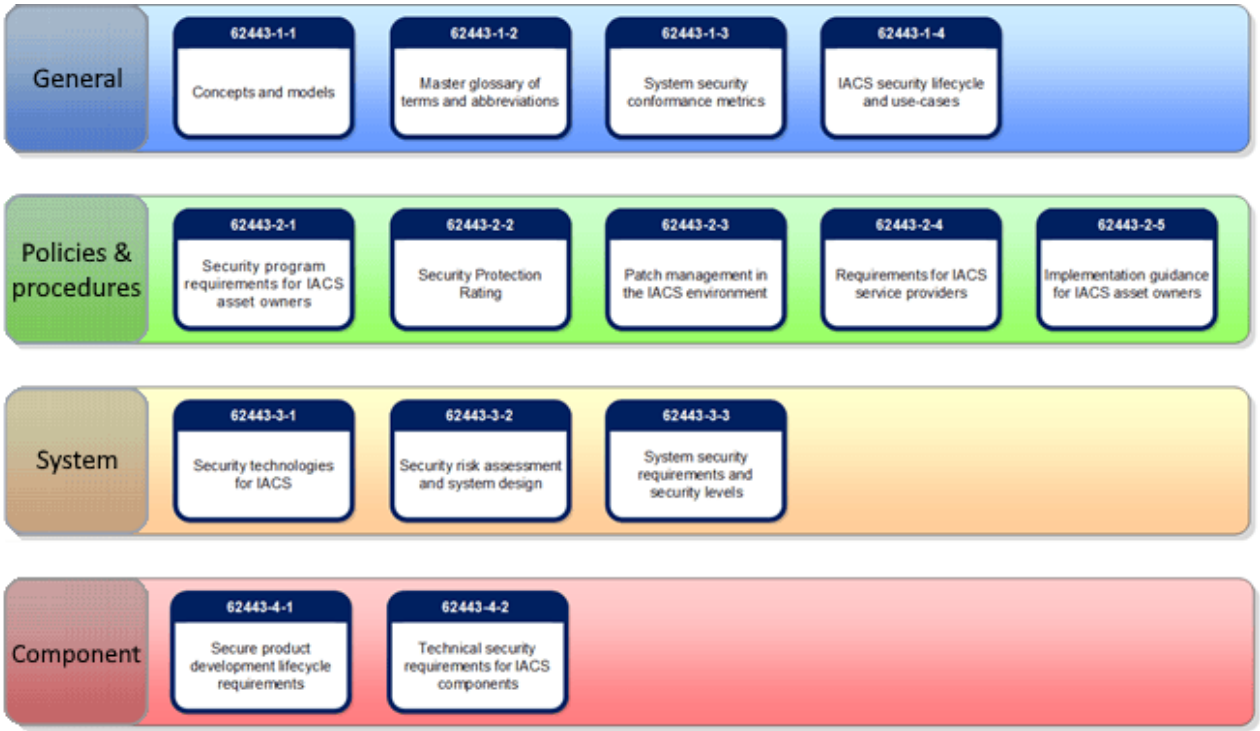
- L'IEC 62443 è lo standard per la Cybersecurity dei sistemi di controllo industriale, (IACS) che definisce requisiti e processi per renderli sicuri. Si rivolge a operatori, fornitori di componenti e integratori per garantire che i sistemi siano protetti da minacce informatiche in tutte le fasi del ciclo di vita.
- Aiuta a proteggere gli impianti industriali da attacchi informatici che potrebbero causare guasti, blocchi di produzione e costi imprevisti.
- Essere conformi alla IEC 62443 dimostra che un'organizzazione adotta un approccio metodico e coerente alla sicurezza, aumentando la fiducia dei clienti e rafforzando la sua competitività.



- La IEC 62443 definisce requisiti per la cybersecurity dei sistemi di controllo industriale (ICS/OT), organizzati in quattro aree:

1. **General** – Principi e concetti (IEC 62443-**1**-*)
2. **Policies & Procedures** – Gestione della sicurezza (IEC 62443-**2**-*)
3. **System Requirements** – Sicurezza del sistema (IEC 62443-**3**-*)
4. **Component Requirements** – Prodotti e dispositivi (IEC 62443-**4**-*)

IEC 62443: struttura dello standard e ruoli



Tutti (generale)

Asset Owners

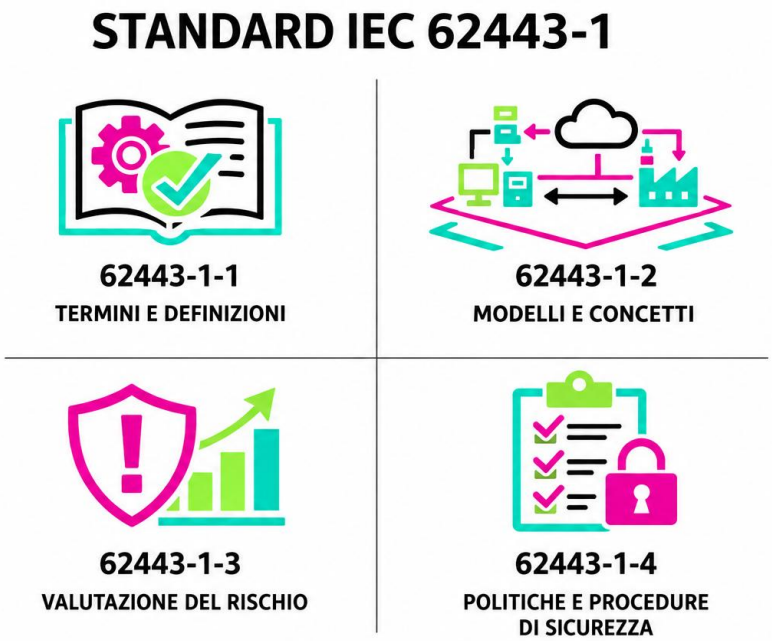
System Integrators

Product Owners

ISA/IEC 62443 Series of Standards | ISAGCA

IEC 62443-1: General

La IEC 62443-1 (General) impatta principalmente gli organismi aziendali che definiscono governance, terminologia, concetti, gestione del rischio e organizzazione della cybersecurity industriale (OT/ICS).



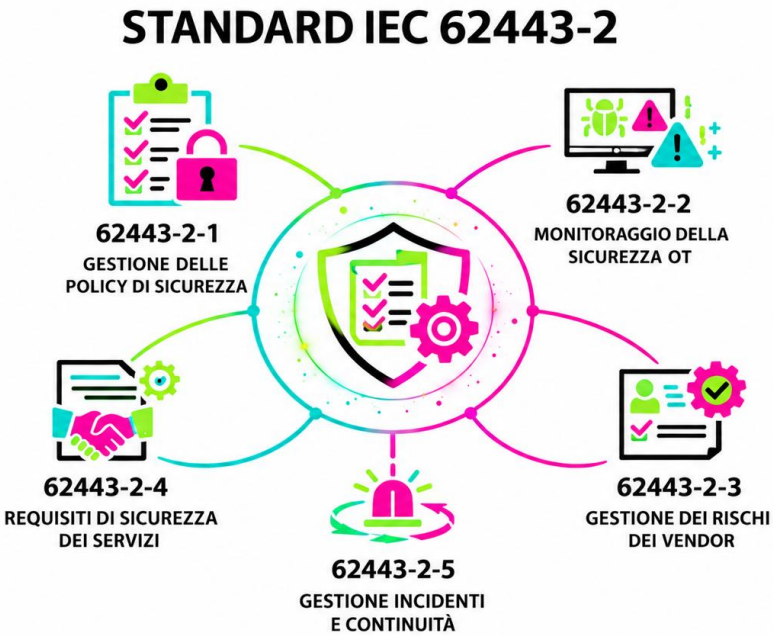
Cybersecurity / OT Security Governance
(es. CISO, OT Security Manager, Cybersecurity Office)
- definizione del framework di sicurezza OT
- coordinamento tra IT e OT
- impostazione dei requisiti di alto livello

Risk Management
- gestione e valutazione del rischio cyber su sistemi industriali
- definizione delle metodologie di risk assessment

Incident Response / Business Continuity
- definizione processi di gestione incidenti OT
- gestione crisi e recovery

IEC 62443-2: Policies & Procedures

La IEC 62443-2 (Policies & Procedures) insiste in modo diretto tutti gli organismi aziendali che definiscono, applicano e controllano i processi organizzativi di cybersecurity industriale (OT/ICS).



Engineering / Automation / Operations

- applicazione procedure di sicurezza nei progetti
- gestione configurazioni e modifiche
- definizione standard tecnici di impianto coerenti con le policy
- gestione accessi di tecnici e fornitori
- gestione operativa di incidenti, guasti e ripristini

HR / Formazione

- gestione consapevolezza e training cybersecurity
- definizione competenze minime richieste per ruoli OT
- gestione onboarding / offboarding del personale

Legal / Contract Management

- clausole contrattuali su sicurezza, responsabilità e incidenti
- gestione aspetti di responsabilità e compliance

IEC 62443-3: System

La IEC 62443-3 (System) ha focus sugli organismi aziendali che progettano, implementano, gestiscono e mantengono un sistema OT/ICS sicuro. È la parte più “tecnica” della serie.



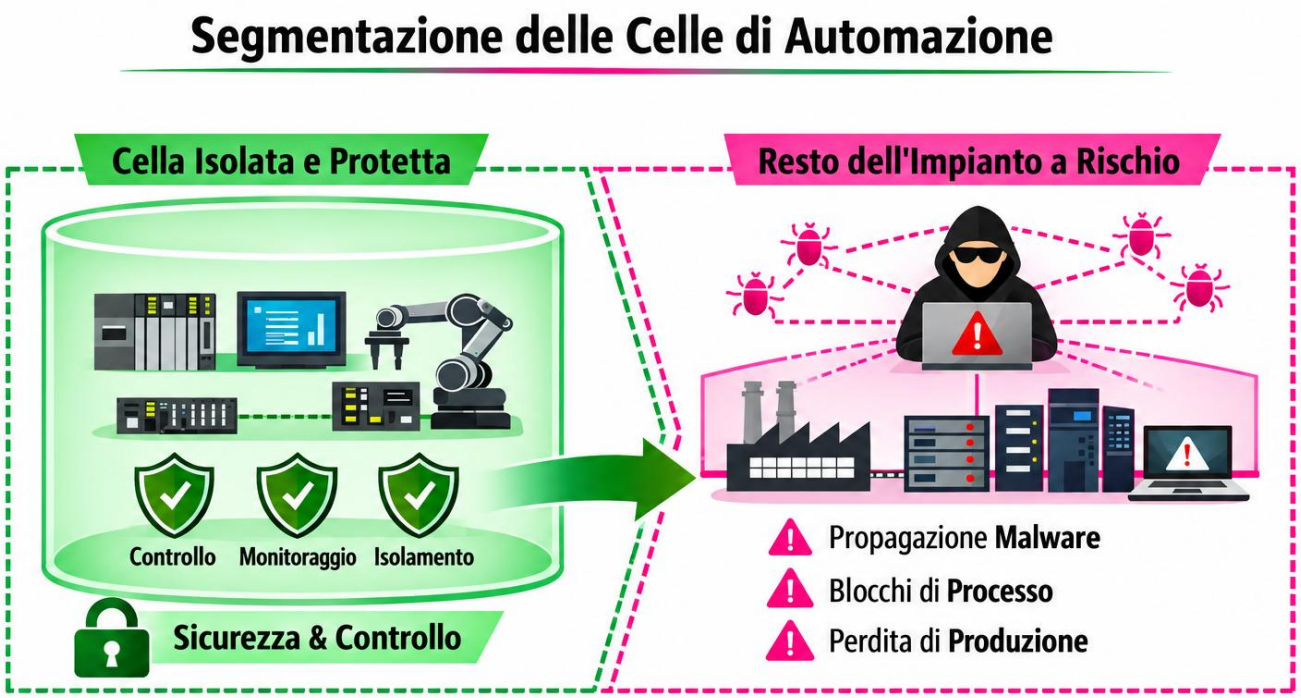
System Integrator / Project Management
- gestione del progetto di implementazione sicurezza
- coordinamento fornitori e stakeholder
- gestione requisiti e documentazione

Engineering / Automation / Progettazione
- definizione architettura OT (zone & conduits)
- progettazione reti industriali e segmentazione
- definizione requisiti di sicurezza di sistema

IT Department / Network & Cybersecurity
- protezione perimetrale (firewall, VPN, DMZ)
- gestione identità e accessi, monitoraggio e logging
- hardening e patching infrastrutture OT

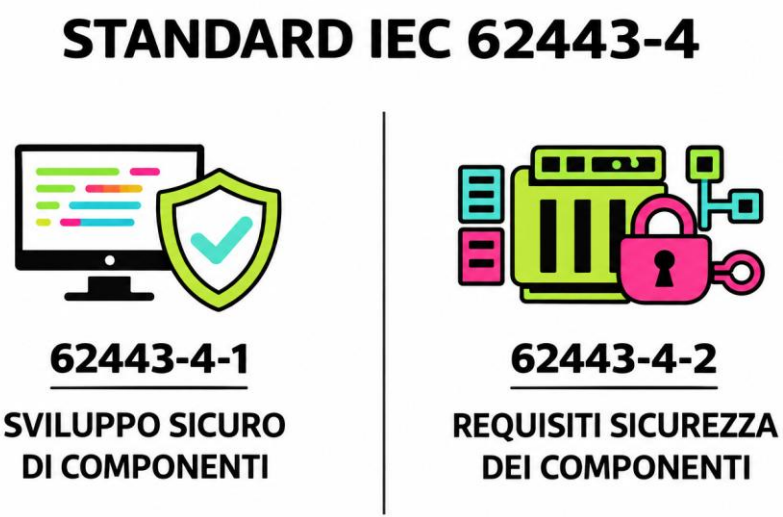
Manutenzione (Maintenance & Field Service)
- gestione aggiornamenti e modifiche della configurazione
- **gestione accessi remoti** per manutentori
- interventi controllati su PLC, HMI e SCADA

IEC 62443-3: System (System Integrators)



IEC 62443-4: Component

La IEC 62443-4 (Component) impatta principalmente su chi sviluppa, seleziona, valida e mantiene componenti OT/ICS, come PLC, HMI, SCADA, gateway, switch industriali, sensori intelligenti e software di automazione.



Product Management / Technical Marketing
- definizione requisiti prodotto legati alla cybersecurity
- comunicazione delle caratteristiche di sicurezza ai clienti
- gestione roadmap di miglioramento

R&D / Sviluppo Software e Firmware
- sviluppo sicuro (Secure Development Lifecycle)
- gestione vulnerabilità e patch
- coding guidelines, secure design, secure update

Engineering / Automation / Progettazione Soluzioni
- scelta dei componenti in funzione dei requisiti di sicurezza
- definizione architettura e integrazione sicura

Testing / Validation / Laboratory
- penetration test e vulnerability assessment
- test di hardening e configurazione sicura
- verifica di robustezza e gestione aggiornamenti

Service / Field Support / Maintenance
- gestione patch e firmware upgrade
- gestione accessi remoti e account sui dispositivi
- interventi di sostituzione componenti mantenendo la postura di sicurezza

IEC 62443-4: Component (Product Owners)

Prodotti di automazione “Secure by Design”

I prodotti industriali devono essere progettati per la sicurezza fin dall’inizio del ciclo di sviluppo, secondo IEC 62443-4-1: **Secure Development Lifecycle.**

- Migliori pratiche di coding sicuro
- Continui test su software e hardware
- Processo di patching tempestivo



IEC 62443: i security levels



NIS2 - Art. 32

IEC 62443: la matrice di valutazione del rischio

Impact	Likelihood				
	Remote	Unlikely	Possible	Likely	Certain
1 Trivial	1	2	3	4	5
2 Minor	2	4	6	8	10
3 Moderate	3	6	9	12	15
4 Major	4	8	12	12	20
5 Critical	5	10	15	20	25

La valutazione del rischio cyber in ambito OT deve tenere conto di aspetti differenti rispetto all'ambiente IT:

- Danni fisici alle persone e/o all'ambiente
- Danni economici e/o di immagine
- Interruzione del business
- Perdita di dati confidenziali e proprietà intellettuale
- Violazioni dei regolamenti pubblici
- Impatto sulla sicurezza nazionale

La IEC 62443 attribuisce ai diversi attori dell'ecosistema OT responsabilità diverse a seconda del ruolo:

SL-T	Target Security Level	Deriva dal risk assessment del sistema/impianto
SL-C	Capability Security Level	Capacità intrinseca di sicurezza di un sistema/componente
SL-A	Achieved Security Level	Livello effettivamente raggiunto nella soluzione installata

IEC 62443: i security levels in pratica

La IEC 62443-3-3 classifica il conseguimento del livello di sicurezza a seconda dei criteri soddisfatti che suddivide in SR (System Requirement) e RE (Requirement Enhancement: requisiti di rafforzamento) propri di ogni FR (Functional Requirement) della IEC 62443 stessa.

SRs and REs

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	
RE (3) Multifactor authentication for all networks				✓
SR 1.2 – Software process and device identification and authentication				
RE (1) Unique identification and authentication	✓	✓	✓	✓
SR 1.3 – Account management				
RE (1) Unified account management	✓	✓	✓	✓

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

ANIE AUTOMAZIONE

Dal prodotto connesso al sistema resiliente: cosa cambia per l'automazione industriale con CRA, NRM e IEC 62443

Grazie per l'attenzione



Mauro Cerea