

Corso - 16/04/2026

Industrial Cybersecurity per Macchine e Impianti OT

Regolamento Macchine (UE) 2023/1230, CRA, NIS2 e NIST - Requisiti globali e applicazioni pratiche

Obiettivi

Il corso fornisce una visione completa, aggiornata e operativa dell'evoluzione normativa e tecnica che porta dalla Safety tradizionale al nuovo concetto integrato di Safety & Security (Cybersecurity industriale).

L'attenzione è focalizzata su:

- macchine industriali
- sistemi robotizzati
- impianti connessi e contesti Industry 4.0 / 5.0

Programma

Evoluzione normativa della sicurezza: dalla Safety tradizionale al mondo OT e la Cybersecurity industriale

- Limiti dell'approccio safety "classico"
- Nuovi scenari di rischio: connessione, accessi remoti, aggiornamenti software
- Impatto degli attacchi cyber sulla sicurezza delle persone

Nord America

- National Electrical Code (NEC 2026)
 - o Introduzione dei requisiti legati alla sicurezza dei sistemi connessi
 - o Impatti su quadri elettrici, macchine e impianti industriali

Europa

- Regolamento Macchine (UE) 2023/1230
 - o Nuovi Requisiti Essenziali di Sicurezza e Salute (RESS) 1.1.9 e 1.2.1
- Cyber Resilience Act (CRA)
 - o Ambito di applicazione
 - o Sovrapposizioni e punti di contatto con il Regolamento Macchine
 - o Differenze tra sicurezza del prodotto e sicurezza funzionale

Confronto tra approcci Europei e Nord Americani

- Approccio prescrittivo vs risk-based
- Responsabilità del costruttore e dell'integratore
- Requisiti essenziali per la connessione sicura di macchine e impianti
- Impatti su:
 - o OEM
 - o system integrator
 - o end user

Norme armonizzate e standard tecnici E

N di Tipo C e macchine speciali

- Impatti della cybersecurity su:

robot industriali
macchine per il packaging
linee automatiche

Nuova ISO/DIS 12100 – Edizione 2025

- Evoluzione dell'analisi dei rischi
- Capitolo 6 ed il paragrafo Cybersecurity and protection against corruption
- Integrazione tra:
 - o rischi safety
 - o rischi cyber
 - o misuse ragionevolmente prevedibile
- prEN 50742 – Safety of machinery – Protection against corruption
 - o Concetto di “corruzione” (software, dati, segnali)
 - o Requisiti di progetto e verifica
- Integrazione con:
 - o IEC 62443-3-2
 - o IEC 62443-3-3

La famiglia delle norme IEC 62443

- Struttura della serie IEC 62443
- Ruoli e responsabilità:
 - o costruttori di macchine
 - o fornitori di componenti
 - o integratori
- Concetti chiave:
 - o zone & conduits
 - o Security Level (SL)
 - o defense in depth

Connessione sicura di macchinari e impianti

Best practice e soluzioni tecniche

- Architetture sicure OT / IT
- Gestione accessi e autenticazione
- Segmentazione di rete
- Aggiornamenti e patch management
- Logging, monitoring e incident response

Casi pratici e applicazioni sul campo

- Analisi di una macchina esistente (IEC 62443-3-2)
- Integrazione safety + cybersecurity
- Errori comuni e non conformità frequenti

Esempi reali di applicazione su robot collaborativi, macchine automatiche, impianti complessi.

Ulteriori informazioni

- La quota di partecipazione include il materiale didattico digitale, l'attestato di partecipazione e il pranzo durante le giornate di formazione in presenza.
- Sono previste sconti per l'acquisto di più partecipazioni.
- Si intendono aziende associate quelle aderenti alle associazioni: ACIMAC, ACIMALL, AMAPLAST, FEDERTEC E UCIMA.

Destinatari

- Costruttori di macchine (OEM)
- System integrator
- Responsabili tecnici e R&D
- Safety manager
- Responsabili Cybersecurity / IT e OT
- Responsabili di conformità normativa e progettazione di impianti

Durata

20 ore

Quota di adesione:

880,00 € + IVA a persona per le aziende associate

1.100,00 € + IVA a persona per le aziende non associate

Date e Sedi di svolgimento

16/04/2026 09.00-18.00 - Modena

17/04/2026 09.00-13.00 - ONLINE

29/04/2026 09.00-18.00 - Modena



è un marchio di S.A.L.A. Srl a Socio Unico - Via Fossa Buracchione 84 - 41126 Modena(MO) - Tel: 059 512 108