Corso - 11/01/2027

Sicurezza delle macchine e protezione contro la corruzione: applicare la EN 50742

Come proteggere hardware, software e dati della macchina dalla corruzione secondo il Regolamento Macchine (UE) 2023/1230

Obiettivi

- **Comprendere l'applicabilità della EN 50742:2026** alle proprie macchine e individuare il percorso più appropriato tra **Approccio A e Approccio B**, anche in relazione alla serie **EN IEC 62443**.
- **Definire il Security Context della macchina** e valutare l'**Attack Potential** delle interfacce rilevanti per la sicurezza.
- **Determinare il Safety-Related Security Level (SRSL), da SRSL0 a SRSL3**, e individuare le misure tecniche di protezione richieste.
- **Impostare il logging e la tracciabilità degli interventi critici**, gestendo la conservazione delle evidenze prevista dalla norma.
- **Integrare nella documentazione tecnica e nelle istruzioni per l'uso** le informazioni richieste dalla EN 50742:2026.
- **Applicare il Threat Modelling alla macchina**, utilizzando **Data Flow Diagram (DFD), Trust Boundaries e metodo STRIDE** per identificare minacce e possibili contromisure.

Programma

Scopo della norma e principi generali

- Allineamento legale: presunzione di conformità al Regolamento Macchine (UE) 2023/1230 una volta armonizzata
- Campo di applicazione: hardware, software, dati e interfacce locali e remote
- Doppio binario: Approccio A (macchine sviluppate senza IEC 62443) e Approccio B (macchine che già adottano la IEC 62443)

Approccio A: valutazione e livelli di sicurezza

- Definizione del security context: limiti operativi, accessi fisici e logici, ambiente previsto
- Attack potential: exposure level, window of opportunity, complessità dell'attacco
- Safety-Related Security Levels (SRSL) da 0 a 3 per ogni interfaccia
- Requisiti tecnici crescenti: autenticazione, controllo accessi, integrità del software al boot, crittografia dei dati

Approccio B: integrazione con la serie EN IEC 62443

- EN IEC 62443-4-1: ciclo di vita di sviluppo sicuro del prodotto
- EN IEC 62443-3-3: requisiti di sistema per la macchina (segmentazione di rete, controllo accessi)
- EN IEC 62443-4-2: requisiti tecnici per i componenti

Tracciabilità, informazioni per l'uso e workshop pratico

- Logging degli interventi critici (modifiche ai parametri di sicurezza, aggiornamenti software)
- Tracing log attivo dalla messa in servizio e conservazione dei dati per almeno 5 anni
- Informazioni per l'uso: contesto di sicurezza, accesso ai log, divieti di modifica, identificazione delle versioni software
- Workshop di threat modelling: diagrammi di flusso dei dati (DFD), trust boundaries e metodo STRIDE

Ulteriori informazioni

- Sono previste scontistiche per l'acquisto di più partecipazioni.
- La quota di partecipazione è comprensiva di materiale didattico in formato digitale e attestato di partecipazione e pranzo di lavoro per le giornate svolte in presenza.
- Si intendono aziende associate quelle aderenti alle associazioni: ACIMAC, ACIMALL, AMAPLAST, FEDERTEC E UCIMA.
- Possibilità di finanziare il corso tramite Fondimpresa e Fondirigenti.

Destinatari

Target:

- Responsabili R&D
- System Integrator
- Responsabili Fascicolo Tecnico
- Responsabili Certificazione CE
- Progettisti Software e Automazione
- Responsabili Cybersecurity OT

Durata

8 ore

Quota di adesione:

400,00 € + IVA a persona per le aziende associate

500,00 € + IVA a persona per le aziende non associate

Date e Sedi di svolgimento

11/01/2027 14.00-18.00 - ONLINE

14/01/2027 09.00-13.00 - ONLINE