

**Corso - 14/06/2023**

## **Cybersecurity applicata alle macchine e impianti**

**Come connettersi in sicurezza, i protocolli esistenti, le normative internazionali di riferimento per una corretta analisi dei rischi.**

### **Obiettivi**

L'avvento di Industry 4.0 sta sempre più determinando l'esigenza di connettere in rete tutte le macchine ed impianti, il più delle volte però senza una precisa direttiva e protocolli tecnici e spesso in modo "non protetto".

I rischi in questo caso sono enormi: difendere le macchine da attacchi hacker non riguarda solo l'evitare l'accesso e l'acquisizione impropria dei dati di produzione, ma anche evitare interferenze sulla parte safety dei macchinari, risvolti sulla qualità dei prodotti, fino ad arrivare ad accessi all'intera rete informativa aziendale.

**Il corso ha lo scopo di definire i nuovi requisiti per la Cyber Security e come impattano su macchine ed impianti nuovi ed esistenti, identificando le principali Cyber minacce, validando anche una procedura di corretta analisi dei rischi, definendo gli opportuni livelli e configurazioni di Protection Level, Security Level Target e Maturity Level, alla luce dei più recenti standard internazionali.**

### **Programma**

#### **Parte 1**

- La Cyber Security nel NEC2023 e nel Nuovo Regolamento macchine, che cosa è richiesto, gli standard.
- Concetto di Safety and Security ? Sinonimi o Complementari ?
- Alcuni casi di Cyber Attack, ransomware e furto di dati
- Cyber Security e GDPR

#### **Parte 2**

- Introduzione alla sicurezza informatica (CIA)
  - o Obiettivi sicurezza informatica, vulnerabilità ed attacco ad un sistema, concetto di rischio
- Distinzione IT/OT e requisiti di sicurezza associati
  - o Definizione IT/OT, differenze e peculiarità, defence in depth
- Struttura dello standard IEC 62443
  - o Concetti generali: organizzazione, ruoli (service provider, asset owner, manufacturer)
- Maturity e Security Level
  - o Definizione e descrizione dei relativi livelli
- IEC 62443-2 (Policies e procedure)
  - o IEC 62443-2-1 Establishing an Industrial Automation and Control System Security Program

#### **Parte 3**

L'analisi dei rischi e definizione di Protection Level, Security Level Target e Maturity Level

- IEC 62443-3 (Sistema)
  - o IEC 62443-3-2 Security Risk Assessment and System Design
- IEC 62443-3-3 System Security Requirements and Security Levels
- L'analisi della struttura di rete, connessioni, i requisiti del software e Hardware per i SL 1, 2, 3 e 4
- Esempi pratici ed esercizi di analisi delle singole parti con la matrice di analisi dei SL.
- I componenti e sistemi, requisiti Hardware e configurazione
- IEC 62443-4 (Componenti)
  - o IEC 62443-4-2 Technical Security Requirements for IACS Components

## Docenti

AC&E Srl – Verona. Società di consulenza nel settore della sicurezza dei macchinari e degli impianti, al servizio delle aziende italiane costruttrici di macchine che esportano in Europa e in tutto il mondo.

## Destinatari

Il corso è diretto a Responsabili IT, responsabili OT, programmatori di PLC, Uffici Tecnici aziendali e post vendita.

## Durata

14 ore

## Quota di adesione:

**650,00 € + IVA a persona per le aziende associate**

750,00 € + IVA a persona per le aziende non associate

## Date e Sedi di svolgimento

14/06/2023 09.00-17.00 - Modena

15/06/2023 09.00-17.00 - Modena

---

## Allegati

» [BROCHURE](#)



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