



A TACH Systems Company

Cybersecurity per macchine mobili connesse

Implicazioni pratiche del Cyber Resilience Act e architettura ALMEC security-by-design

Hardware | Software | IoT | Remote Support

www.almec.net



L'importanza della Cybersecurity nell'Elettronica sui Mezzi Mobili

Nuove regole UE: cosa cambia per le macchine connesse.

Normative Europee e Sicurezza:

Cyber Resilience Act

CRA, regolamento europeo sulla cybersecurity dei prodotti con elementi digitali, quindi hardware e software. Impone che i prodotti siano progettati, sviluppati, aggiornati e mantenuti in sicurezza lungo tutto il ciclo vita, riducendo vulnerabilità e rischi cyber per utenti e aziende.

NIS2

Direttiva europea sulla sicurezza delle reti e dei sistemi informativi. Definisce un quadro comune di cybersecurity per settori critici e importanti, imponendo alle organizzazioni misure di gestione del rischio, prevenzione degli incidenti, continuità operativa e cooperazione a livello europeo.

RED / EN 18031

Radio Equipment Directive, è la direttiva europea per le apparecchiature radio, con requisiti essenziali su sicurezza, compatibilità elettromagnetica e uso efficiente dello spettro radio. Gli standard EN 18031 supportano i requisiti di cybersecurity per dispositivi radio connessi, come gateway, moduli wireless, Wi-Fi, Bluetooth, LTE e radiocomandi.

GDPR

General Data Protection Regulation, regolamento europeo sulla protezione dei dati personali. Si applica quando vengono raccolti, trattati, conservati o trasmessi dati riconducibili a una persona fisica, come dati identificativi, posizione, accessi, log utente o informazioni operative associabili a un individuo.

Quadro normativo: cosa cambia davvero

10.12.2024
CRA in vigore
Reg. UE 2024/2847 sui
prodotti con elementi
digitali



18.10.2024
NIS2 sostituisce NIS
Estende obblighi
organizzativi e supply
chain



2025–2027
RED / EN 18031
Cybersecurity per
apparati radio
connessi



11.09.2026
Reporting CRA
Vulnerabilità sfruttate
e incidenti gravi



11.12.2027
Obblighi principali
CRA
Sicurezza by design,
supporto e
documentazione



La macchina connessa deve poter dimostrare sicurezza, aggiornabilità, gestione vulnerabilità e protezione delle comunicazioni lungo il ciclo vita.

Implicazioni pratiche per il costruttore macchina

Non cambia solo il software: cambia il modo in cui si progetta, documenta e mantiene la macchina connessa.

01 Accessi controllati

Chi può configurare, diagnosticare o modificare parametri macchina deve essere identificato.

02 Firmware protetto

Aggiornamenti firmati e processi OTA verificabili evitano software non autorizzato.

03 Comunicazioni sicure

Gateway, HMI e cloud devono proteggere i dati da macchina a piattaforma.

04 Gestione vulnerabilità

Serve un processo per ricevere, valutare, correggere e tracciare vulnerabilità.

05 Documentazione tecnica

Il fascicolo di prodotto deve includere scelte progettuali e misure cyber adottate.

06 Supporto nel tempo

Il cliente deve sapere per quanto e come riceverà fix, aggiornamenti e assistenza.

ALMEC può assorbire questa complessità nel progetto elettronico, lasciando al cliente un'integrazione progressiva e gestibile.

Architettura ALMEC: dalla macchina al cloud

Un percorso chiaro per rendere cyber-resiliente una macchina già connessa.

Livelli di protezione

- Identità dispositivo e autenticazione
- Cifratura macchina-cloud
- Firmware e OTA
- Accessi diagnostici controllati
- Log e tracciabilità eventi
- Supporto e aggiornamenti gestiti

ECU / I-O

HMI

Gateway IoT

Cloud IoT

Si parte dalla rete CAN esistente, si inserisce il gateway/servizio adeguato e si costruisce la conformità sul ciclo vita del prodotto.



Security by design: cosa significa



Secure boot

Avvio controllato del dispositivo, con verifica dell'integrità del firmware.

Firmware firmato

Installazione solo di versioni autorizzate e tracciabili.

OTA sicuro

Aggiornamenti remoti gestiti senza fermare la macchina sul campo.

Crittografia

Protezione del dato lungo la tratta gateway-portale.

Autenticazione

Dispositivo riconosciuto prima di trasmettere o ricevere comandi.

Access control

Diagnostica e parametri riservati a utenti e ruoli autorizzati.

Risultato: protezione dal dispositivo al cloud, con una gestione più semplice per OEM, service e cliente finale.

Prodotti ALMEC

Gateway IoT CAN Bus



Piattaforma IoT Diaboard



ECU CAN I/O rugged



HMI rugged



Radiocomandi e filocomandi



DC Motor Control



ALMEC ti accompagna nel percorso verso la Cybersecurity

La cybersecurity diventa un percorso graduale, non un blocco del progetto.

1

Mappiamo l'architettura esistente

Rete CAN, ECU, HMI, radio, gateway, cloud, utenti e punti di accesso.

2

Inseriamo il livello di sicurezza

Gateway, autenticazione, cifratura, OTA, accessi e log dove servono davvero.

3

Documentiamo per la conformità

Scelte tecniche, support period, gestione vulnerabilità e aggiornamenti.

4

Gestiamo il ciclo vita

Aggiornamenti guidati, supporto remoto, ticketing e miglioramento continuo.

Con ALMEC la cybersecurity non diventa un peso progettuale per il costruttore macchina: viene integrata direttamente nell'architettura elettronica, dalla ECU al gateway IoT, dall'HMI agli aggiornamenti remoti.

GRAZIE

