



A TACH Systems Company

Cybersecurity for connected mobile devices

Practical implications of the Cyber Resilience Act
and ALMEC's 'security-by-design' architecture

Hardware | Software | IoT | Remote Support

www.almec.net

The Importance of Cybersecurity in Automotive Electronics

New EU rules: what's changing for connected machines.

European Regulations and Safety:

Cyber Resilience Act

CRA, the European regulation on the cybersecurity of products containing digital components, i.e. hardware and software. It requires that products be designed, developed, updated and maintained securely throughout their entire life cycle, thereby reducing vulnerabilities and cyber risks for users and businesses.

NIS2

European Directive on the security of network and information systems. It establishes a common cybersecurity framework for critical and important sectors, requiring organisations to implement measures relating to risk management, incident prevention, business continuity and cooperation at European level.

RED / EN 18031

The **Radio Equipment Directive** is the European directive governing radio equipment, setting out essential requirements regarding safety, electromagnetic compatibility and the efficient use of the radio spectrum. The EN 18031 standards support the cybersecurity requirements for connected radio devices, such as gateways, wireless modules, Wi-Fi, Bluetooth, LTE and radio controls.

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.

Regulatory framework: what's really changing

10.12.2024
CRA in force
EU Regulation 2024/2847
on products with digital
components

2025–2027
RED / EN 18031
Cybersecurity for
connected radio
equipment

11.12.2027
Key CRA obligations
Security by design,
support and
documentation

18.10.2024
NIS2 replaces NIS
It extends organisational and
supply chain obligations

11.09.2026
CRA Reporting
Exploited
vulnerabilities and
serious incidents

The connected device must be able to demonstrate security, updatability, vulnerability management and communication protection throughout its lifecycle.

Practical implications for the machine manufacturer

It's not just the software that's changing: the way in which the connected machine is designed, documented and maintained is changing too.

01 **Controlled access**
Anyone who is authorised to configure, diagnose or modify machine parameters must be identified.

02 **Secure firmware**
Signed updates and verifiable OTA processes prevent unauthorised software.

03 **Secure communications**
Gateways, HMIs and the cloud must protect data as it moves from machine to platform.

04 **Vulnerability Management**
A process is required to receive, assess, rectify and track vulnerabilities.

05 **Technical documentation**
The product dossier must include the design choices and cyber security measures adopted.

06 **Long-term support**
The customer needs to know for how long and how they will receive fixes, updates and support.

ALMEC can handle this complexity within the electronic design, allowing the client to integrate it gradually and in a manageable way.

ALMEC architecture: from the machine to the cloud

A clear roadmap for making an already connected machine cyber-resilient.

Levels of protection

- Device identity and authentication
- Device-to-cloud encryption
- Firmware and OTA
- Controlled diagnostic access
- Logging and event traceability
- Managed support and updates

ECU / I-O

HMI

Gateway IoT

Cloud IoT

You start with the existing CAN network, integrate the appropriate gateway or service, and ensure compliance throughout the product lifecycle.



Security by design: what does it mean



Secure boot

Controlled boot-up of the device, with a firmware integrity check.

Signed firmware

Installation of authorised and traceable versions only.

Secure OTA

Remote updates managed without taking the machine out of service in the field.

Encryption

Data protection along the gateway-portal path.

Authentication

Device recognised before sending or receiving commands.

Access control

Diagnostics and parameters restricted to authorised users and roles.

Result: protection from device to cloud, with simpler management for OEMs, service providers and end customers.

ALMEC products

Gateway IoT CAN Bus



Diaboard IoT Platform



ECU CAN I/O rugged



HMI rugged



Radio controls and wired controls



DC Motor Control



ALMEC guides you on your journey toward cybersecurity

Cybersecurity becomes a gradual process, not a roadblock to the project.

1

Let's map the existing architecture

CAN network, ECU, HMI, radio, gateway, cloud, users, and access points.

2

Let's set the security level

Gateway, authentication, encryption, OTA, access, and logs—right where they're needed.

3

We document for compliance

Technical decisions, support periods, vulnerability management, and updates.

4

We manage the lifecycle

Guided updates, remote support, ticketing, and continuous improvement.

With ALMEC, cybersecurity doesn't become a design burden for machine builders: it's integrated directly into the electronic architecture—from the ECU to the IoT gateway, from the HMI to remote updates.

THANK YOU

