PRESS RELEASE
Pessac, 10 November 2026

Cyber Resilience Act: SERMA helps embedded systems manufacturers prepare for compliance

As the Cyber Resilience Act (CRA) approaches full application in December 2027, embedded systems manufacturers must incorporate new cybersecurity requirements into their products. SERMA Safety and Security supports them in securing their architectures, assessing vulnerabilities and preparing for compliance with the European regulation.

The CRA: a new challenge for embedded systems manufacturers

Connected electronic boards, control units, industrial equipment and smart devices: embedded systems combine hardware and software components whose security must be maintained over time. The CRA requires manufacturers within its scope to address cybersecurity risks from the design stage, document their protective measures and establish vulnerability management processes.

Since 11 September 2026, certain reporting obligations for actively exploited vulnerabilities and severe incidents have already applied. The main product-related requirements will apply from 11 December 2027. Manufacturers must therefore prepare well in advance, taking into account development cycles, hardware constraints and the often-long service lives of their equipment.

Beyond security testing, compliance requires collaboration between electronics and software design teams, quality managers and cybersecurity specialists. The objective is to establish an approach tailored to each product's risks and constraints, from architecture through to maintenance.

Technical support at every stage of compliance

- **Scoping and risk assessment** to identify products in scope, applicable requirements and gaps in existing practices.
- **Embedded systems security** to integrate cybersecurity requirements into hardware and software architectures, interfaces and development processes.
- **Cybersecurity audits and testing** to assess equipment, firmware and protocols, and support the preparation of compliance evidence and vulnerability management.

This approach enables manufacturers to build on their existing standards and processes, particularly those based on IEC 62443, while taking into account standards being developed to support the CRA. The applicable conformity assessment procedure depends on each product's category and characteristics.

Cybersecurity expertise aligned with industrial constraints

SERMA Safety and Security provides cybersecurity expertise for embedded systems and electronic products in demanding sectors. Combined with the Group's capabilities in electronics, microelectronics and engineering, this expertise enables an integrated approach to architecture, technical assessment, reliability and compliance throughout the product lifecycle.

Meet SERMA experts at electronica in Munich

At electronica, from 10 to 13 November 2026, journalists and industry professionals can meet the SERMA teams to discuss the implications of the CRA for embedded systems. Visit us at Messe München, Hall C3, Stand 448.

About SERMA Group

Founded in 1991, SERMA Group is a leading French specialist in the design, security and reliability of products and data. As an independent, expert-led group, SERMA supports customers in sectors with stringent safety, reliability and environmental requirements, including aerospace, space, defence, automotive, rail, medical and banking.

With a strong culture of technical excellence and a network of specialists, SERMA operates throughout the product lifecycle, from R&D and design to operational maintenance.

The Group offers a comprehensive range of services:

- Energy
- Electronics and materials technologies
- Cybersecurity and functional safety
- Engineering
- Microelectronics
- Telecommunications

With 1,500 employees across 30 sites in Europe, Tunisia and the United States, SERMA generated revenue of €201 million in 2025.

For more information, visit www.serma.com

MEDIA CONTACT
Florie Bousquié | SERMA Group Communications Manager | f.bousquie@serma.com