

Learn practical EU Cyber Resilience Act compliance for Embedded Systems

Objectives

- Understand the scope and purpose of the EU Cyber Resilience Act and how it applies to your embedded products
- Master the essential cybersecurity requirements for secure design and development
- Learn to conduct compliance gap assessments and create a compliance roadmap
- Identify compliance pathways, including CE marking and conformity assessment procedures
- Plan manufacturer obligations from development through end-of-support
- Evaluate and implement market-ready security solutions for compliance

Target Audience

- Embedded Systems Engineers building products with digital elements
- Firmware Architects designing systems for compliance
- Product Managers overseeing compliance and communicating
- Manufacturing & Supply Chain teams responsible for product security at all stages

Prerequisites

- Basic Knowledge of Embedded Systems

Training delivery methods

- LIVE ONLINE
 - Interactive virtual classroom with remote lab access, digital materials, same expertise as classroom format, available for distributed teams
- ON-SITE/PRIVATE (Your Facility)
 - Customized to your products, your schedule, your team. Can be tailored to your specific industry or product type.

Environnement du cours

- Cours théorique
 - Support de cours au format PDF (en anglais) et une version imprimée lors des sessions en présentiel
 - Cours dispensé via le système de visioconférence Teams (si à distance)
 - Le formateur répond aux questions des stagiaires en direct pendant la formation et fournit une assistance technique et pédagogique
- Au début de chaque demi-journée une période est réservée à une interaction avec les stagiaires pour s'assurer que le cours répond à leurs attentes et l'adapter si nécessaire

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

Modalités d'évaluation

- Les prérequis indiqués ci-dessus sont évalués avant la formation par l'encadrement technique du stagiaire dans son entreprise, ou par le stagiaire lui-même dans le cas exceptionnel d'un stagiaire individuel.
- Les progrès des stagiaires sont évalués par des quizz proposés en fin des sections pour vérifier que les stagiaires ont assimilé les points présentés
- En fin de formation, une attestation et un certificat attestant que le stagiaire a suivi le cours avec succès.
 - En cas de problème dû à un manque de prérequis de la part du stagiaire, constaté lors de la formation, une formation différente ou complémentaire lui est proposée, en général pour conforter ses prérequis, en accord avec son responsable en entreprise le cas échéant.

Plan

EU Regulatory Landscape & CRA Fundamentals

- Why CRA Matters Now
- CRA Scope & Applicability - Product classification
- CRA vs. Related EU Regulations
- CRA Timeline & Entry Into Force

Essential Cybersecurity Requirements

- Secure Design & Development
 - Threat modeling
 - Design principles
- Vulnerability Management
 - Lifecycle approach (discover -> assess -> remediate -> deploy)
- Transparency & User Information
 - Required disclosures
 - Communication channels
- Handling Substantial Modifications
 - Decision matrix approach

Compliance and Conformity Assessment

- CRA Classification: Important vs. Critical
- CE Marking & Conformity Assessment
 - self-cert vs. notified body
 - Technical Docs.
- Case study: Applying conformity assessments to embedded systems
 - Industrial IoT gateway example
 - Step-by-step walkthrough
- Assessment Pathway Selection Activity

Lifecycle Security Management

- Manufacturer Obligations
 - Pre-market, post-market, end-of-life phases
 - Support period expectations
 - clear responsibility mapping
- Supply Chain Security
 - Due diligence requirements
 - Open source considerations
 - Risk assessment matrix
- Risk assessment & Due diligence
 - 6-step framework
 - CVSS scoring explained

Implementation & Compliance solutions

- Security Solutions

- Secure boot architecture
- Hardware security options (TPMs, Secure Elements)
- RTOS & OS Security Features
 - Comparison table (Zephyr, Linux, FreeRTOS)
 - CRA readiness scores
- Compliance Tools and Frameworks
 - Vulnerability scanning tools (e.g., CVE checkers)
 - Compliance management platforms
 - Security testing frameworks

Renseignements pratiques

Renseignements : 1 jour

Prochaines sessions : le 16 mars 2026 - Online EurAsia (9h-16h CET)
le 20 avril 2026 - Online EurAsia (9h-16h CET)
le 11 mai 2026 - Online EurAsia (9h-16h CET)