



SEC10 - Cyber Resilience Act (CRA) 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.

Course Environment

- Theoretical course
 - PDF course material (in English) supplemented by a printed version for face-to-face courses.
 - Online courses are dispensed using the Teams video-conferencing system.
 - The trainer answers trainees' questions during the training and provide technical and pedagogical assistance.
- At the start of each session the trainer will interact with the trainees to ensure the course fits their expectations and correct if needed

Course Outline

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