oSEC10 - Cyber Resilience Act and Embedded Systems

Objectives

- Understand the scope and purpose of the EU Cyber Resilience Act.
- Learn the essential cybersecurity requirements for products with digital elements.
- Identify compliance pathways, including CE marking and conformity assessments.
- Address cybersecurity requirements for embedded devices throughout their lifecycle.
- Explore market-ready solutions and tools to meet the Act's requirements.

Target Audience

- Embedded system developers
- Product managers

Prerequisites

- Basic Knowledge of Embedded Systems

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

Evaluation modalities

- The prerequisites indicated above are assessed before the training by the technical supervision of the traineein his company, or by the trainee himself in the exceptional case of an individual trainee.
- Trainee progress is assessed by quizzes offered at the end of various sections to verify that the trainees have assimilated the points presented
- At the end of the training, each trainee receives a certificate attesting that they have successfully completed the course.
  - In the event of a problem, discovered during the course, due to a lack of prerequisites by the trainee a different or additional training is offered to them, generally to reinforce their prerequisites,in agreement with their company manager if applicable.

Plan

Introduction to the Cyber Resilience Act

- Overview and objectives of the Regulation.
- Key challenges in cybersecurity for products with digital elements
- Scope and applicability: Products and entities impacted by the Act
- Relation to existing EU laws like NIS2, GDPR, and Cybersecurity Act

Essential Cybersecurity Requirements

- Requirements for secure design and development of products

- Vulnerability management obligations, including updates and disclosures
- Transparency measures: Informing users about vulnerabilities and support periods
- Handling substantial modifications in digital products

Compliance and Conformity Assessment

- CE marking and conformity procedures for digital products
- Classification of products (important vs. critical)
- Case study: Applying conformity assessments to embedded systems

Lifecycle Security Management

- Obligations for manufacturers: From development to end-of-support
- Securing supply chains and third-party components
- Best practices for risk assessments and due diligence

Implementations for Cyber Resilience Compliance

- Security Solutions
  - Built-in security features Yocto Project, Zephyr RTOS
  - Hardware-based security modules (e.g., TPMs, Secure Elements).
  - Secure boot mechanisms and encrypted storage solutions.
- Compliance Tools and Frameworks
  - Vulnerability scanning tools (e.g., CVE checkers)
  - Automated tools for compliance documentation and CE marking

Communication Protocols and Network Systems

- Cyber Resilience Requirements
  - Ensuring communication integrity and data encryption as per the Act
  - Addressing risks in networked embedded systems
- Secure Communication Protocols
  - Importance of secure protocols (e.g., TLS, DTLS, SSH) in embedded systems.
  - Overview of industrial and IoT-specific protocols
  - Protocol vulnerabilities and mitigation strategies
- Network System Security:
  - Implementing secure configurations for embedded network devices
  - Techniques for securing wireless communications

Renseignements pratiques

Inquiry : 1 day