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

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

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

Renseignements : 1 jour