SEC10 - Cyber Resilience Act et systèmes embarqués

Objectives

- Comprendre la portée et les objectifs du Cyber Resilience Act (CRA) de l'Union européenne.
- Apprendre les exigences essentielles de cybersécurité pour les produits comportant des éléments numériques.
- Identifier les voies de conformité, y compris le marquage CE et les évaluations de conformité.
- Répondre aux exigences de cybersécurité pour les appareils embarqués tout au long de leur cycle de vie.
- Explorer des solutions et outils prêts à l'emploi pour satisfaire aux exigences du CRA.

Target Audience

- Développeurs de systèmes embarqués
- Chefs de produit

Prerequisites

- Connaissances de base en systèmes embarqués

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 au Cyber Resilience Act

- Vue d'ensemble et objectifs du CRA
- Principaux défis de cybersécurité pour les produits comportant des éléments numériques (PDE)
- Champ d'application et applicabilité : produits et entités concernés par l'Acte
- Lien avec les réglementations européennes existantes telles que NIS2

Exigences essentielles en matière de cybersécurité

- Exigences pour la conception et le développement sécurisés des produits

- Obligations de gestion des vulnérabilités, y compris les mises à jour et les divulgations
- Mesures de transparence : information des utilisateurs sur les vulnérabilités et les périodes de support
- Gestion des modifications substantielles dans les produits numériques

Conformité et évaluation

- Marquage CE et procédures de conformité pour les produits numériques
- Classification des produits (importants vs. critiques)
- Étude de cas : application des évaluations de conformité aux systèmes embarqués

Gestion de la sécurité tout au long du cycle de vie :

- Obligations des fabricants : du développement jusqu'à la fin du support
- Sécurisation des chaînes d'approvisionnement et des composants tiers
- Bonnes pratiques pour les analyses de risques et la diligence raisonnable

Mises en œuvre pour la conformité au Cyber Resilience Act

- Solutions de sécurité
  - Fonctionnalités de sécurité intégrées (Yocto Project, Zephyr RTOS)
  - Modules de sécurité matériels (ex. : TPM, Secure Elements)
  - Mécanismes de démarrage sécurisé (secure boot)
- Outils et cadres de conformité
  - Outils d'analyse de vulnérabilités (ex. : vérificateurs de CVE)
  - Outils automatisés pour la documentation de conformité et le marquage CE

Protocoles de communication et systèmes réseau

- Exigences de cybersécurité
  - Garantir l'intégrité des communications et le chiffrement des données conformément au Cyber Resilience Act
  - Traiter les risques liés aux systèmes embarqués connectés
- Protocoles de communication sécurisés
  - Importance des protocoles sécurisés (ex. : TLS, DTLS, SSH) dans les systèmes embarqués
  - Overview des protocoles industriels et spécifiques à l'IoT
  - Vulnérabilités des protocoles et stratégies d'atténuation
- Sécurité des systèmes réseau:
  - Mise en œuvre de configurations sécurisées pour les dispositifs réseau embarqués
  - Sécurisation des communications sans fil

Renseignements pratiques

Inquiry : 1 day