SEC10 - EU Cyber Resilience Act (CRA)

Objectifs

- Comprendre le champ d'application et la finalité du Cyber Resilience Act de l'UE.
- Connaître 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 des dispositifs embarqués tout au long de leur cycle de vie.
- Explorer des solutions et des outils prêts à l'emploi pour satisfaire aux exigences du règlement.

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 au Cyber Resilience Act

- Présentation et objectifs du règlement.
- Principaux enjeux de cybersécurité pour les produits comportant des éléments numériques.

- Champ d'application et applicabilité : produits et entités concernés.
- Articulation avec les textes européens existants (NIS2, RGPD, Cybersecurity Act).

Exigences essentielles de cybersécurité

- Exigences de conception et développement sécurisés des produits.
- Obligations de gestion des vulnérabilités, y compris mises à jour et divulgations.
- Mesures de transparence : informer les utilisateurs des vulnérabilités et des périodes de support.
- Gestion des modifications substantielles des produits numériques.

Conformité et évaluation de la conformité

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

Gestion de la sécurité sur le cycle de vie

- Obligations des fabricants : de la phase de développement jusqu'à la fin de support.
- Sécurisation de la chaîne d'approvisionnement et des composants tiers.
- Bonnes pratiques pour les évaluations de risque et la due diligence.

Mises en œuvre pour la conformité en cyberrésilience

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

Protocoles de communication et systèmes réseau

- Exigences du Cyber Resilience Act
  - Garantir l'intégrité des communications et le chiffrement des données conformément au règlement.
  - Traiter les risques propres aux systèmes embarqués connectés.
- Protocoles de communication sécurisés
  - Importance de l'usage de TLS, DTLS, SSH dans les systèmes embarqués.
  - Aperçu des protocoles industriels et IoT.
  - Vulnérabilités de protocoles courantes et stratégies de mitigation.
- Sécurité des systèmes réseau:
  - Mettre en place des configurations sécurisées pour les équipements réseau embarqués.
  - Techniques pour sécuriser les communications sans fil.

Renseignements pratiques

Renseignements : **1 jour**
Prochaines sessions : **le 16 janvier 2026 - Ac6 - Courbevoie / Paris (France)**
le 16 février 2026 - Ac6 - Courbevoie / Paris (France)
le 16 mars 2026 - Ac6 - Courbevoie / Paris (France)
le 20 avril 2026 - Ac6 - Courbevoie / Paris (France)
le 11 mai 2026 - Ac6 - Courbevoie / Paris (France)