SEC7 - ARM TrustZone sur les composants à base de Cortex-M

Objectifs

- Comprendre l'architecture ARM v8-M et ses mécanismes de sécurité
- Découvrir les évolutions du mécanisme de Memory Protection de l'ARMv8-M
- Configurer la Security Attribution Unit
- Gérer les Security access faults
- Construire et déboguer un logiciel secure et non-secure

Environnement du cours

- Les participants disposent d'un système de fichiers partagé pour enregistrer et échanger leur travail.
- Support de cours au format PDF
- Les travaux pratiques utilisent une carte à base d'ARM Cortex-M33

Prérequis

- Compétences en programmation : une première expérience de la programmation, en particulier en C
- Connaissance de base des implémentations ARM Cortex-M
- Notions d'algorithmes de sécurité et de secure coding

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

Plan du cours

Premier jour

Architecture ARM et sécurité

- Présentation de la technologie ARM TrustZone
- Architecture TrustZone
  - Présentation de l'architecture TrustZone
  - Processeurs compatibles TrustZone et leurs caractéristiques
  - Secure world et non-secure world
- Sécurité TrustZone
  - Présentation du modèle de sécurité TrustZone
  - Cortex-M compatible TrustZone
- Points de conception d'un logiciel secure

Memory Protection de l'ARMv8-M

- Types de mémoire
- Ordre des accès
- Memory barriers, code auto-modifiant
- Présentation de la memory protection, PMSA de l'ARM v8
- MPU du Cortex-M33 et bus faults
- Présentation des régions, type de mémoire et contrôle d'accès
- Mise en place de la MPU

TrustZone sur Cortex-M

- Processeurs Cortex-M compatibles TrustZone et leurs caractéristiques
- Security states
- Banking des registres entre security states
- Piles et security states
- Security Extension et exceptions
- Interactions entre états secure et non-secure
- Exceptions et Security Extension
  - Traitement des Secure Exceptions
  - Traitement des Non-Secure Exceptions depuis l'état secure
  - Retour d'une exception non-secure vers l'état secure
- La Security Attribution Unit (SAU)
- L'Implementation Defined Attribution Unit (IDAU)
- Débogage des processeurs Cortex-M compatibles TrustZone