TrustZone for Armv8-M Secure System Design

Summary
TrustZone for Armv8-M technology adds security partitioning to Arm Cortex-M processors. It can be used to design a secure IoT device using different Arm technologies including an Armv8-M processor, TrustZone CryptoCell IP and industry standard techniques for developing software. Correctly combined these technologies can be used to design a system that can achieve Platform Security Architecture (PSA) certification.

This course covers the architectural features that underpin the security partitioning at a software level and how security can be implemented in the wider system using AMBA AHB5. Workbooks are used to give trainees some practical experience on how to create secure and non-secure applications mapped appropriately to secure and non-secure memories, using secure APIs and TrustZone-aware compiler toolchain.

Prerequisites:
- Knowledge of existing M-profile devices
- Knowledge of programming in C
- Experience of assembler programming is not required but would be beneficial
- Knowledge of embedded systems
- Introduction to Arm (included)
- Armv8-M Overview (included)
- TrustZone for Armv8-M (included)

Audience:
- Hardware and software system architects
- System security architects
- Embedded software developers

Delivery method
Face to face

Length:
2 days

Modules

Pre-course Online Training
- Introduction to Arm
- Armv8-M Overview
- TrustZone for Armv8-M

Days 1-2
- Introduction to Security
- Armv8-M Overview
- Introduction to the Armv8-M Security Extension
- TrustZone for Armv8-M System IP Overview

- Toolchain Support for the Armv8-M Security Extension
- Armv8-M Security Extension Workbook (Sessions 1-3)
- Exception Handling for the Armv8-M Security Extension
- Security Attribution
- Armv8-M Security Extension Workbook (Session 4)
- TrustZone for Armv8-M Secure System Design
- TrustZone for Armv8-M Secure System Design Workbook