TrustZone for ARMv8-M

Summary:

This course is designed for Software Engineers who already have development experience on ARMv6-M and/or ARMv7-M platforms and wish to gain experience of the TrustZone Security Extension introduced in ARMv8-M. It begins by covering the basic architectural features of ARMv8-M and continues to cover features provided by the new Security Extension.

Prerequisites:

Thorough knowledge of ARMv6-M and/or ARMv7-M
Familiarity embedded programming in C and assembler
Experience of embedded system development

Audience:

Software engineers needing to gain knowledge of the new feature of ARMv8-M including the TrustZone for ARMv8-M security extension.

Length:

4 hours

Agenda:

Architectural Overview:

- Sub-profiles and ISA changes from ARMv6-M/ARMv7-M
- ARMv8-M Memory Architecture
- Exception and Privilege Model
- Memory Protection
- Debug Features and Authentication

Break

TrustZone Basics:

- Secure Memory Configuration
- Communication Between Security States

Break

TrustZone Continued:

- Security of Exceptions and Interrupts
- TrustZone Support in the Toolchain