TrustZone for ARMv8-M Overview

Summary:

This live WebEx delivered course provides software engineers, who already have development experience on ARMv6-M and/or ARMv7-M platforms, knowledge 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. As well as hearing first hand from the engineer, you will also have the opportunity to ask questions to gain further specific knowledge on the subject.

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

TrustZone:

- Secure Memory Configuration
- Communication Between Security States
- Security of Exceptions and Interrupts
- TrustZone Support in the Toolchain