TrustZone for Armv8-M

Summary:

This topic is the first of two topics designed to provide an overview of TrustZone for Armv8-M. The second topic, not covered here, describes how the exception model has changed to support the new Armv8-M security features.

At the end of the session, participants will:

- Gain knowledge on what new security features have been added to the Armv8-M architecture.
  - Programmer model improvements.
  - Memory model improvements.
- Understand how it is possible to configure the Security Attribution Unit (SAU) to set up Secure and Non-secure memory regions.
- Know how to switch security state via function calls using C/C++ language extensions.

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 TrustZone for Armv8-M Security Extension.

Delivery Method:

- Online

Length:

1 hour

Modules:

- TrustZone for Armv8-M Overview
- Programmers Model
- Memory Model
- Configuring the Secure Attribution Unit (SAU)
- Function Calls