ARM

White Paper

Introducing ARM Cortex-M23 and Cortex-M33 Processors with TrustZone for ARMv8-M

Tim Menasveta, Diya Soubra, Joseph Yiu

Cortex-M Product Marketing

October 2016

Useful terms:

• MPU- Memory Protection Unit • DSP- Digital Signal processing • FPU- Floating Point Unit • ETM- Embedded Trace Macrocell • MTB- Micro Trace Buffer • BPU- Break Point Unit	• DWT- Data Watch and Trace unit • ITM- Instrumentation Trace Macrocell • NVIC- Nested Vectored Interrupt Controller • AHB- Advanced High-performance Bus • AMBA- Advanced Microcontroller Bus Architecture

Useful documents:

Cortex-M for Beginners - An overview of the ARM Cortex-M processor family and comparison

Whitepaper - ARMv8-M Architecture Technical Overview

Security Extensions and Privilege Levels

Introduction

Every day objects are becoming smart and connected. Not only will these smart objects change the way that we live and work, they will also change the embedded market, where security will become a key requirement. Connectivity has become a key feature that requires security and device management, which increases the complexity of embedded firmware. Many companies offer solutions for these requirements today, but none has yet been able to offer a common standard on which an ecosystem of solution can flurish. The result is a fragmented solution space which hinders mass market adoption, due to concerns about lock-in from the developers.

Over the past ten years, ARM® has worked with all its partners to create a vibrant ecosystem around the Cortex®-M family of 32-bit embedded processors. As a result, over 22 billion Cortex-M based devices have been shipped by ARM partners. Given the rising demand for IoT, it is only natural to respond by addressing these new requirements by releasing next generation Cortex-M processors that have been designed with the technology required to become the security foundation for all embedded systems.

The Cortex-M23 and Cortex-M33 processors are the newest members of the highly popular Cortex-M product family. As such, the two processors maintain the expected characteristics of the embbeded profile such as real-time deterministic interrupt response, low power, low area, ease of development, and 32-bit performance. The security foundation is introduced via the addition of TrustZone® technology. **The two processors, with such a vibrant ecosystem, will open the door for opportunities across many diverse market segments.**

TrustZone for ARMv8-M

TrustZone is the cornerstone of the new ARMv8-M processors. It offers hardware access control to code, memory and I/O while retaining the requirements of embedded applications: real-time response, minimal switching overhead, constrained on-chip resources, and ease of software development.

ARMv8-M adds an extra state to the operation of the processor so that there are both secure and non-secure execution states. These security states are orthogonal to the existing Thread and Handler modes, thereby having both modes in both secure and non-secure states.

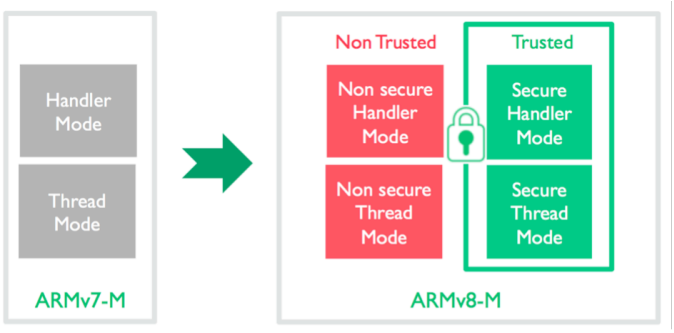

Figure 1 Additional states with ARMv8-M

The processor design includes features such as:

- Four stacks and four stack pointer registers
- Hardware stack-limit checking

- The memory space is partitioned into secure and non-secure spaces using programmable MPU-like Security Attribution Unit (SAU), or fixed/external security configuration
- Exception handling hardware automatically saves and then clears the secure register states when switching to the non-secure exception state.
- Non-secure entry to secure code restricted to secure code locations containing a Secure Gateway (SG) instruction and tagged as a non-secure callable (NSC) region.

The presence of two full states opens the door to many new opportunities and applications. High value firmware may be delivered in the secure state to be used in the system by non-secure applications, while being completely protected. Supervisor code placed in the secure state can be used to recover a system after a software attack or unreliable operation, while the non-secure side remains available to millions of developers currently programming software for Cortex-M.

TrustZone is designed in such a way that all existing users can continue to develop in the non-secure zone, just as before. Debug and trace are enhanced to make development of complex applications easier. All programming may be done entirely in C language, as is the case for all Cortex-M processors, including all exception handlers. Existing code can be easily reused on Cortex-M23 and Cortex-M33 with only minor configuration changes (if any), e.g. MPU setup code. **Combined together, these items increase developer productivity enabling them to deliver more complex solutions to market in a shorter period.**

Programmers' model

Developers are the most precious resource when it comes to embedded solutions, so maintaining the familiar development environment is a key consideration for any new processor design. With Cortex-M23 and Cortex-M33 the complexity of creating secure solutions is removed by using TrustZone to restore the traditional programmers' model that all developers are accustomed to.

One way to describe the setup is with Figure 2 on the next page. Developers are used to the classic model of having two levels, privileged and un-privileged. Secure solutions that are shipping today need to reserve the privileged level for the trusted resource manager, which then pushes all the remaining software into the other level. With Cortex-M33 and Cortex-M23, two additional states are inserted. The user side is restored to the classic model and the secure side is now dedicated for trusted software, which is split across two states. Such a setup opens up the door for innovation in secure solutions, while safe guarding the programmer's model that users are accustomed to.

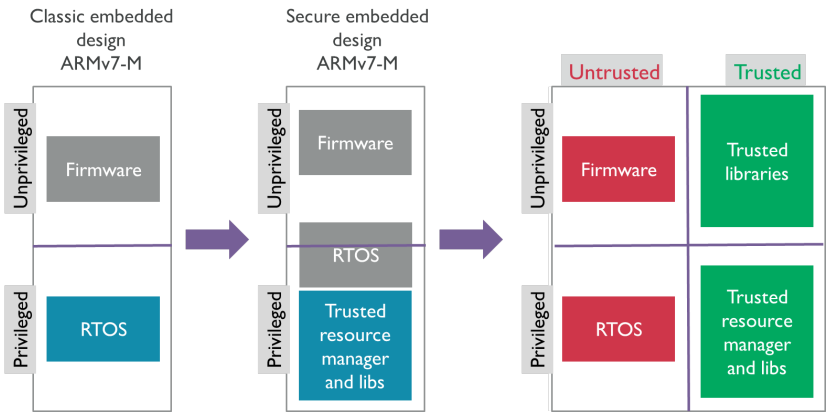

Figure 2: Restoring the traditional programmer's model

Secure debug

The security capabilities of the new architecture cover multiple aspects of the whole system, including debug and trace features. Debug authentication interfaces are provided on the Cortex-M23 and Cortex-M33 processors to allow chip designers to integrate debug authentication solutions, such as ARM TrustZone CryptoCell. With the debug authentication feature, chips can be configured to allow all debug and trace, only allow non-secure debug and trace, or disable all debug and trace features. The permission level for debug features (e.g. breakpoint, single stepping and core register accesses) and trace features (e.g. instruction trace, data trace, event trace) can also be configured separately.

If only non-secure debug and trace are enabled, secure memories cannot be accessed by the debugger and software developers will only have visibility of non-secure software operations. The hardware prevents the processor from being halted (e.g. by means of single stepping) during execution of secure code, and trace feature also prevents any leakage of execution information of secure code. Therefore, the secure software is fully protected.

Ecosystem expansion

The Cortex-M family is at the heart of the world's #1 embedded ecosystem. Such a vibrant ecosystem is essential for all developers looking to create secure embedded solutions.

ARM is already working with many of its existing partners to provide them with the technical information to migrate their offering to include Cortex-M23 and Cortex-M33. Many of these partners will be releasing products alongside the release of the next generation processor family.

Since the two processors use the ARMv8-M instruction set, which is a superset of ARMv6-M and ARMv7-M, the migration of the whole ecosystem presents relatively few obstacles. Software and tools are being modified to support the changes in some register definitions, and drivers are being updated to use the new memory management unit, but these are small tasks compared to the world of new opportunities that arise from this next generation of processors with TrustZone technology.

The exciting part is that now partners who used to develop tools and software to support TrustZone for ARMv8-A will now want to expand their coverage to include support for TrustZone for ARMv8-M. This easy migration further expands the Cortex-M ecosystem, for the benefit of all developers.

Cortex-M23 Overview

Cortex-M23 is the smallest and most energy efficient ARM processor with TrustZone technology. Based on the ARMv8-M baseline architecture, Cortex-M23 is the ideal processor for constrained embedded applications with efficient security requirements.

TrustZone for ARMv8-M brings hardware-enforced separation between the trusted and un-trusted resources on each Cortex-M23 device. As such, TrustZone provides a foundation for building embedded applications that in the past might have required two separate physical processors, to ensure a physical separation between trusted and un-trusted resources. Cortex-M23 provides a robust security foundation for requirements such as device identification management, high-value firmware protection, software certification, and secure booting, to name a few.

The Cortex-M23 is a two-stage pipelined processor that is compact, yet supports the full ARMv8-M baseline instruction set. The instruction set comprises around 80 Thumb instructions, most of which are 16-bits wide to maximize code compactness, but also include a few 32-bit instructions where efficiency gains can be made. All ARMv6-M instructions are supported to ensure the ease of code migration from Cortex-M0 and Cortex-M0+. Several new instructions have also been included in the ARMv8-M baseline instruction set to improve performance efficiency for conditional operations, mutually exclusive accesses, divide operations, and immediate moves.

Being the most compact and energy-efficent ARM processor with TrustZone technology, Cortex-M23 will make large-scale deployments of secured connected sensor nodes a reality. Low-power microcontrollers based on Cortex-M23 will also bring more trust to everyday electonics of tomorrow, such as home security cameras or biometric authentication devices. Its tiny silicon footprint will make it ideal for high-volume ubiquitous self-authenticating device wire connections. Finally, another fitting example for the use of Cortex-M23 would be in energy-sipping biomedical implants, which are typically implemented with larger, more mature technology nodes and with special low-leakage libraries. Compactness is essential in large technology node implementations and TrustZone enhances safety though isolation.

Finally, **the integrated debug capabilities of the Cortex-M23 processor allow for faster software development.** The system can be viewed through either a JTAG port or a 2-pin Serial Wire Debug port. The optional ETM and MTB provide excellent instruction trace capabilities while the BPU and DWT provide the capability to use breakpoints and hardware watchpoints for debug.

Cortex-M33 Overview

The Cortex-M33 delivers an optimal balance between performance, energy efficiency, security and productivity. It is the first full feature processor based on the ARMv8-M architecture, with TrustZone security technology and digital signal processing capability.

The processor supports a large number of flexible configuration options to facilitate deployment in a wide-range of applications and offers a dedicated co-processor interface for accelerating tightly coupled, frequent, compute intensive operations.

Cortex-M33 features and functionality include:

- Mainline Extension of the ARMv8-M architecture including the 16-bit and 32-bit Thumb instruction set
- ARMv8-M exception model
- Optional Memory Protection Unit (MPU), based on ARM Protected Memory System Architecture (PMSAv8), with up to 16 regions for each of the security states.
- Optional support for the ARMv8-M Security Extensions (TrustZone)
- Optional Configurable Security Attribution Unit, supporting up to 8 memory regions
- Optional single precision FPU based on ARM FPv5 architecture
- Optional ARM DSP extension
- Optional execution trace using MTB or ETM
- Integrated interrupt controller supporting 1 to 480 external interrupts with up to 256 priority levels
- Optional co-processor interface supporting up to 8 co-processor units

The Cortex-M33 core has been designed with an in-order three stage pipeline. Most instructions complete in two stages while complex instructions require three. Some 16-bit instructions are dual-issued. The core has two AMBA® 5 AHB5 interfaces. The AHB5 specification expands security across the whole system.

The Cortex-M33 processor includes a dedicated co-processor bus interface designed for the integration of tightly coupled accelerator hardware. This interface includes both the control and data channels for up to eight co-processors. The co-processors are provided with information about the privilege and security state of the processor along with the instruction type and associated register and operation fields.

The co-processor operation is expected to either complete in a reasonable number of cycles or to interrupt on completion. The operation can be started when the data and/or operands are transferred, or when the processor reads back the result. Wait states can be inserted if the result is not ready. **For frequently used compute intensive operations, this interface gives a mechanism to add custom processing to the system with minimal design and validation effort, whilst importantly retaining all of the benefits to developers of the widest choice of tools, software and operating systems that the Cortex-M ecosystem provides.**

The optional integer DSP extension adds 85 saturating arithmetic and Single Instruction Multiple Data (SIMD) operations. **In most cases the DSP instructions are expected to increase performance by an average of three times over a software libarry giving a boost to all applications that are centred around signal processing.**

The optional single precision floating point extension based on FPv5 includes an additional 16-entry 64-bit register file and associated interrupt handling mechanics. The option adds 45 IEEE754-2008 compatible single-precision floating-point instructions. Using floating-point instructions usually yields on average a ten times increase in performance over the equivalent software libraries. The FPU is contained in a separate power domain allowing the unit to be powered-down when not enabled or in use.

The increasingly time-consuming validation of applications can make on-chip debug and trace invaluable to on-time delivery of products. **The integrated debug capabilities of the Cortex-M33 processor allow for faster software development.** The system can be viewed through either a JTAG port or a 2-pin Serial Wire Debug port. The optional ETM and MTB provide excellent instruction trace capabilities while the BPU and DWT provide the capability to use breakpoints and hardware watchpoints for debug.

Given all of these optional features, the Cortex-M33 processor is highly configurable and easily adaptable to diverse system requirements. Designers can quickly create complex systems by including the most suitable combination of these optional MPU, DSP, FPU, TrustZone, ETM, MTB, ITM, BPU, DWT and co-processor interface features. In simple control systems, the NVIC can be configured to one interrupt, while in interrupt intensive systems applications, the NVIC can be configured to support up to 480 physical interrupts with up to 256 levels of priorities. In systems demanding safer operation of many different processes, the MPU can be included to enforce process separation and use of privileged access modes. For the next level of code, data and resource protection, TrustZone is a better choice.

Summary

The Cortex-M33 and the Cortex-M23 were designed to fill the market need for smart and connected devices built on a common security foundation. The traditional programmers' model is maintained to simplify the migration path for ecosystem partners and developers. TrustZone, the cornerstone of both processors, was implemented for the embedded profile, with a focus on real-time deterministic interrupt response, low power and small area. ARM, along with the world's #1 ecosystem, is expanding the current software and tools product offering to encompass ARMv8-M, for the benefit of all developers. Cortex-M33 and the Cortex-M23, are the latest industry processors of choice for the next 20 billion devices.

Trademarks