LPC55S6x 器件上的 TrustZone

由 soledad 于 2019-5-21 创建的文档 版本 1

原文：https://community.nxp.com/docs/DOC-343506

本文档介绍了 LPC55S6x 器件上的 TrustZone。

LPC55S6x MCU 平台和通用模块

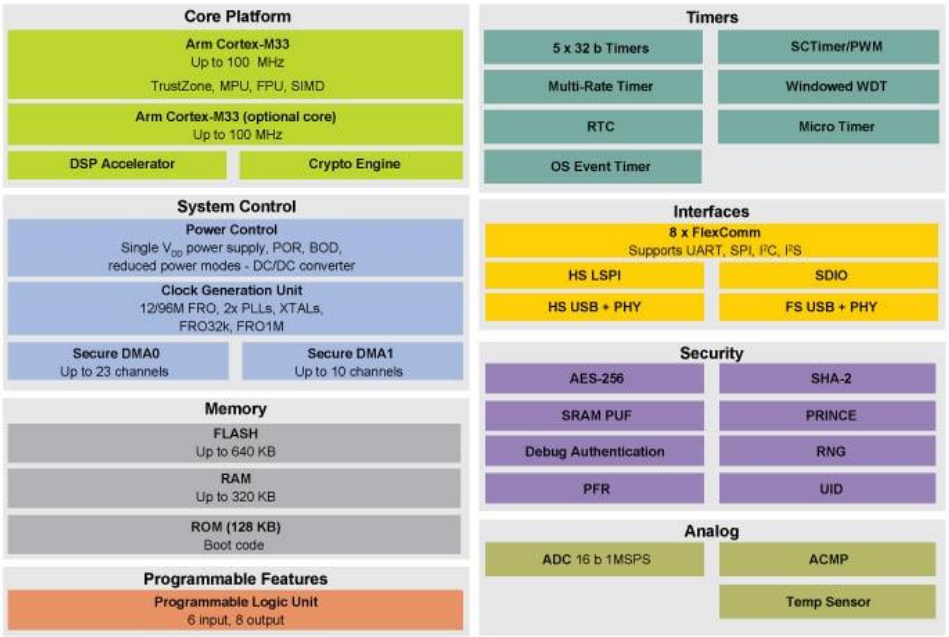
LPC55S69 含一个带有 TrustZone，MPU（存储器保护单元），FPU（浮点运算单元）和 SIMD 的 100-MHz Cortex-M33 内核以及另一个没有安全功能的 100-MHz Cortex-M33 内核。请注意 LPC55Sxx 系列中 LPC55S66 只能应用一个 100-MHz 内核。核心 0 上有两个协处理器，分别是一个叫做 PowerQuad 的 DSP 加速器和一个叫做 CASPER 的加密引擎。核心平台具有多层总线矩阵，允许两个内核同时执行指令以及进行其他主机与外设和存储器的并行访问。芯片的存储器包括高达 640 KB 的闪存，高达 320 KB 的 RAM 和 128 KB 的 ROM。

定时器包括 5 路——32 位标准定时器，一个可产生 PWM 的状态可配置定时器，一个多速率定时器，一个窗口看门狗定时器，一个实时时钟（RTC）和微定时器。每个内核都有自己的 systick 定时器。

通信接口包括一个集成了高速 PHY 的高速 USB，一个可无晶振工作的全速 USB，两个同时支持 WIFI 和 SD 卡的 SDIO 接口，1 个高达 50MHz 的高速 SPI 和 8 个 Flexcomms，可让客户灵活配置得到最多支持 8 个 SPI，I2C，UART 或 4 个 I2S。

模拟系统包括一个采样率为 1 MSPS 的 16 通道 16 位 ADC，一个模拟比较器，一个 16 通道电容式触摸控制器和一个温度传感器。

其他模块包括可编程逻辑单元，降压 DC-DC 转换器，及在-40 至 105°C 的温度范围内工作电压为 1.71 至 3.6 V。



什么是 TrustZone?

近年来，物联网（IoT）已成为嵌入式系统开发人员的热门话题。物联网系统产品变得更加复杂，需要更好的解决方案来确保系统安全。
ARM®TrustZone®技术是一种确保芯片级系统（SoC）和 CPU 系统范围安全的方法。ARMv8-M 上的 TrustZone®安全扩展针对超低功耗嵌入式应用进行了优化。它允许多个软件安全域只能受限制地访问受信任软件的安全内存和 I/O。

ARMv8-M 上的 TrustZone®：

- 保持安全域和非安全域的低中断延迟
- 不会产生代码开销，周期开销或基于虚拟化的解决方案的复杂性
- 以最小的开销引入高效的安全域调用指令

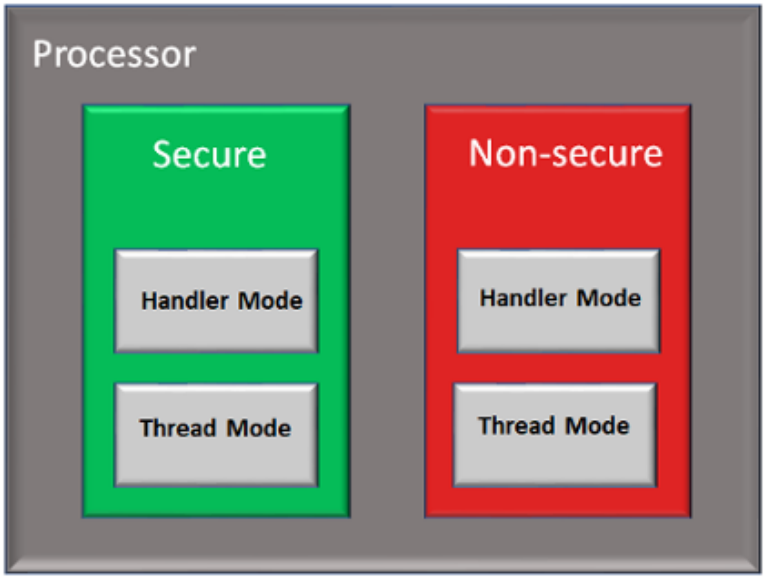
TrustZone®技术被引用在了 Cortex M23 和 Cortex M33 中。
TrustZone®提供了实施分离和访问控制的方法，以隔离可信软件和资源，从而减少关键器件的攻击面。创建的可信固件可以保护可信操作，是存储和运行关键安全服务的理想方法。该代码还可以保护可信硬件以增强和强化可信软件。这包括用于加密加速器，随机数生成器和安全存储的硬件辅助模块。如想获得最佳效果，此代码应是能提供安全服务的小型的且经过仔细审核的代码。
LPC55S66 和 LPC55S69 在内核 0 的 Cortex-M33 上启用了完整的 TEE 并支持 TrustZone®。LPC55S69 还有第二个 Cortex-M33（内核 1），它不使用 TrustZone（TZ）实现安全环境。分区隔离只是基础。安全性在于保护层的数量，添加更多硬件和软件以创建更多层。

TrustZone®技术的特性：

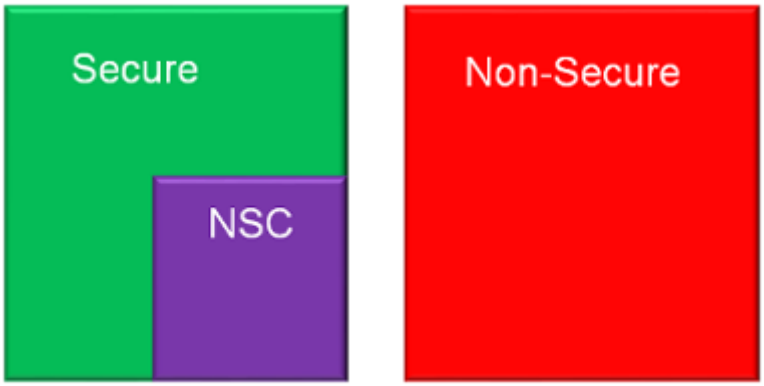
- 允许用户将内存划分为安全区域和非安全区域
- 允许在未经过身份验证时阻止调试安全代码/数据
- CPU 包括 SAU 以及 NVIC，MPU，SYSTICK，内核控制寄存器等的备份，使得安全/非安全代码可以独立访问自己分配到的资源。
- 堆栈管理从原来 Cortex-M 的两个堆栈指针（主堆栈指针（MSP）和进程堆栈指针（PSP））扩展到四个，将上述两对分别提供给安全和非安全区域。
- 提出了安全网关（Secure Gateway）操作码的概念，以允许安全代码从非安全代码中定义一组严格的入口点。

安全和非安全状的内存

TrustZone®技术将系统划分为两种状态：安全（S）和非安全（NS），并且可以通过相应的命令在两种状态之间切换。 CPU 状态可以是安全特权，安全非特权，特权（Handler）或非特权（Thread）。



安全内存空间进一步分为两种类型：安全（Secure）和非安全可调用（NSC）。

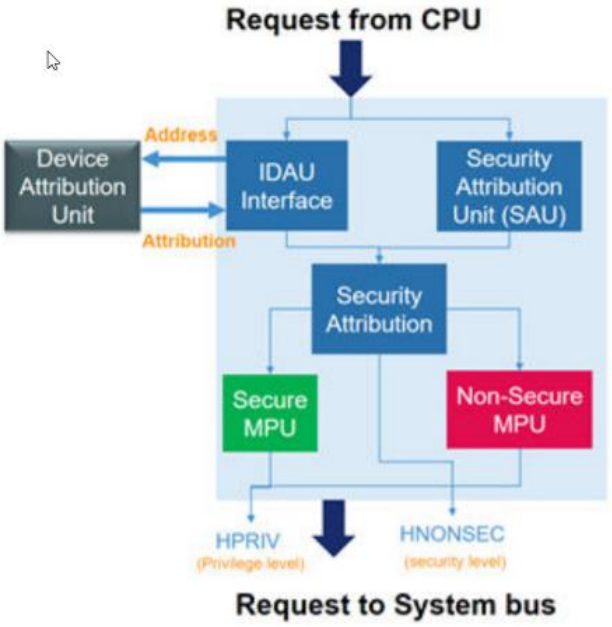


以下是 Trustzone 内存区域（S，NS，NSC）的功能/属性：

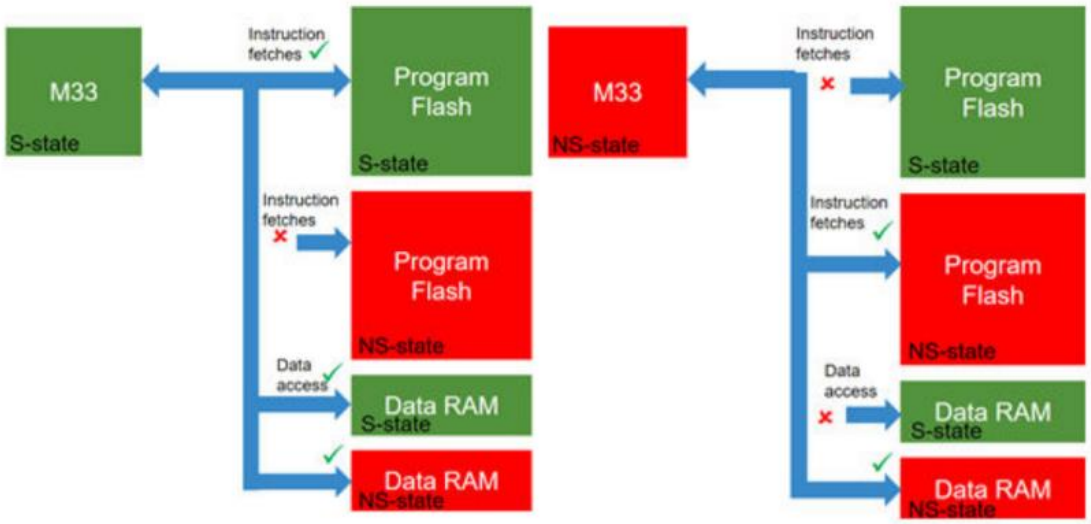
- 安全（S）
- 用于安全代码/数据
- 安全数据只能通过安全代码读取
- 安全代码只有 CPU 在安全模式才可被执行
- 非安全（NS）
- 用于非安全代码/数据
- 安全状态和非安全状态都可以访问非安全（NS）数据
- 非安全代码只能在 CPU 处于非安全状态时被执行，无法通过安全代码执行
- 非安全可调用（NSC）
- NSC 区域作为非安全代码防问安全代码的跳板，非安全代码可以通过安全网关（Secure Gateway）访问特定的安全代码。

属性单元（Attribution Units）

安全 SAU 和 IDAU 共同决定一块内存的安全属性（S, NS 或 NSC）。DAU 通过 IDAU 接口连接到 CPU0，如下图所示。 然后，来自 CPU0 的访问（取决于其安全状态及由 IDAU 和 SAU 共同确定的安全属性）由 AHB 控制器与特定检查器进行比较，该检查器标记存储器和外围设备的各种访问策略。所有地址只能是安全的或不安全的。ARMv8-M 内部的 SAU 与 MPU（存储器保护单元）配合使用。 其中 LPC55S69 支持 8 个 SAU 区域。



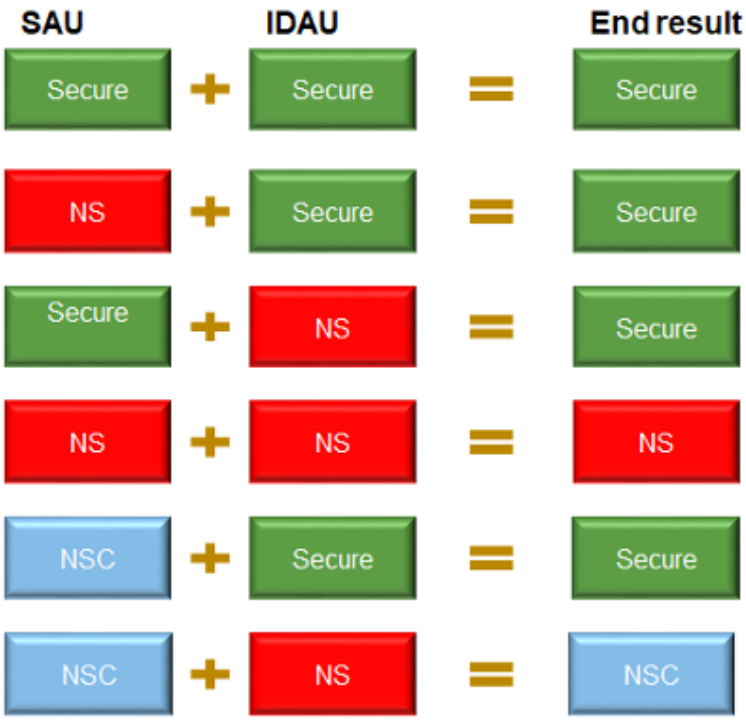
安全和非安全代码在单个 CPU 上运行，以实现高效的嵌入式实现。 处于非安全状态的 CPU 只能从非安全程序存储器执行。处于非安全状态的 CPU 只能访问两个 NS 存储器中的数据。对于安全可信代码，有一个新的安全堆栈指针和堆栈限制检查功能。 S 和 NS 区域有单独的存储器保护单元（MPUs），每个状态有私有 SysTick 定时器。 安全端可以配置中断的目标域。



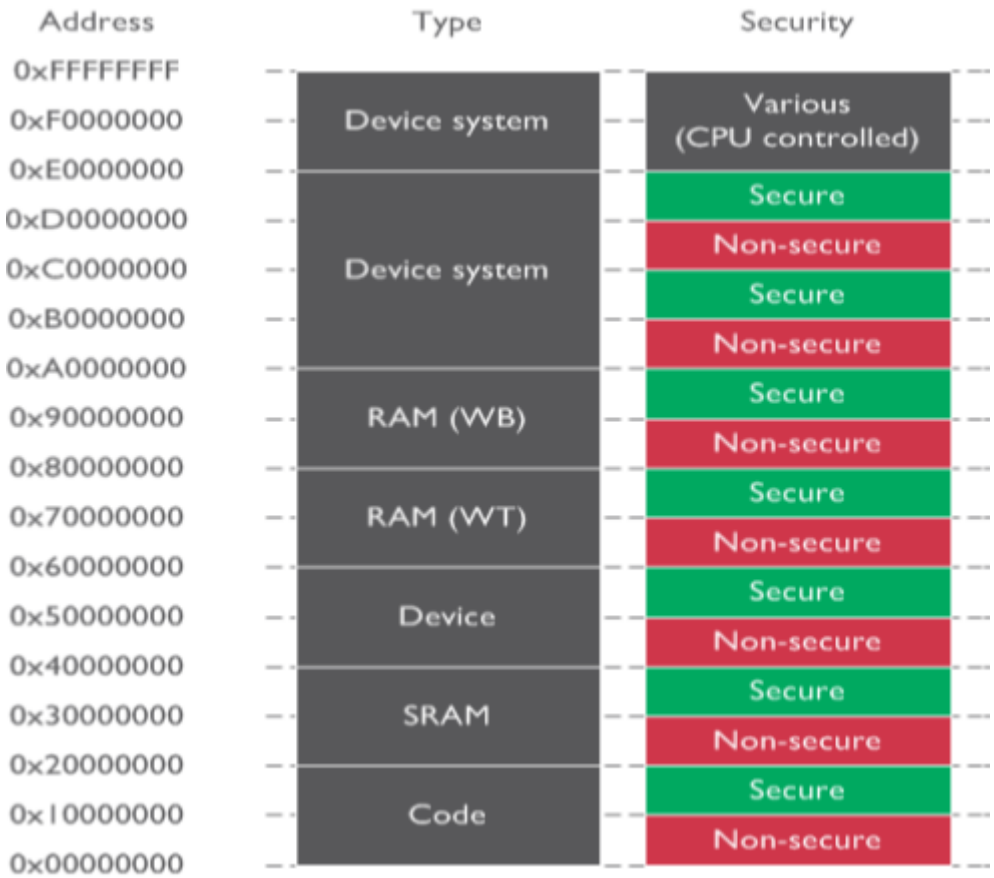
用于 core0 的 ARM TrustZone 的恩智浦 IDAU 是根据存储器地址的第 28 位(Address bit 28)将地址空间划分为潜在的安全和非安全区域。

地址位【28】未在存储器访问硬件中解码，因此每个物理位置可以出现在它们所在的任何总线上的两个位置。其他硬件决定允许对任何地址进行哪些类型的访问（包括 NSC）。IDAU 是一个简单的设计，使用地址位【28】允许在两个位置对内存进行映射。如果 Bit_28=0，则存储器不安全。如果 Bit_28=1，则存储器是安全的。

SAU 允许有 8 个内存区域，并允许用户覆盖 IDAU 的固定映射，以定义不安全的区域。默认情况下，所有内存都设置为安全。应使用至少一个 ASU 描述符使 IDAU 有效。如果 IDAU 或 SAU 标记了一个区域，则该区域是安全的。 NSC 区域可以在 IDAU 的 NS 区域中被定义。

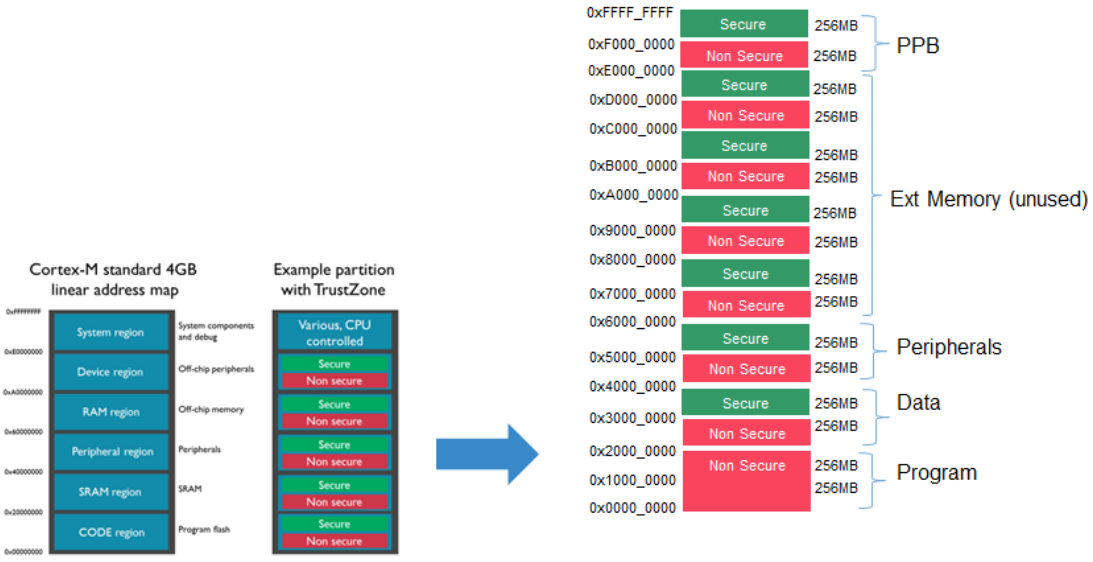


例如，设计者可以使用地址位【28】来定义存储器是安全还是非安全，从而产生以下示例的存储器映射。



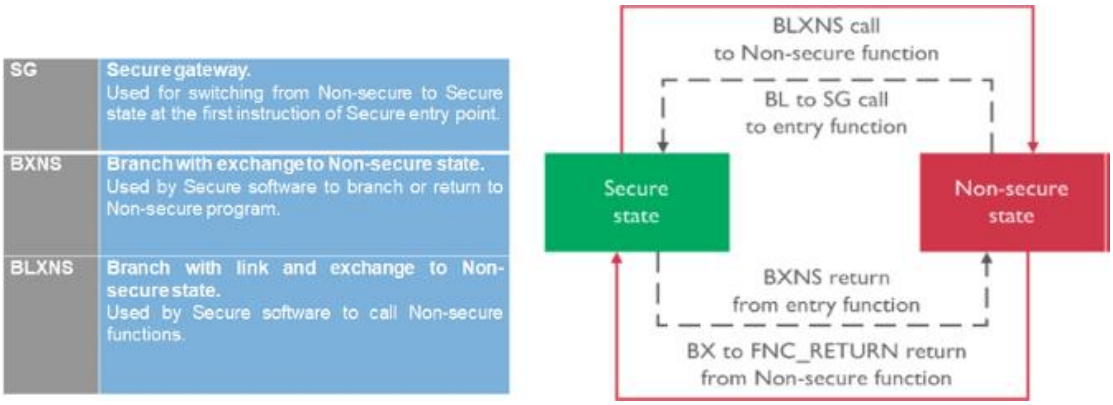
简单的 IDAU，无需创建关键时序路径。 （CM33 确实很少允许使用 IDAU 功能）
地址 0x0000_0000 到 0x1FFF_FFFF 是 NS 区域，在地址 0x2000_0000 到 0xFFFF_FFFF 范围内

如果地址 Bit_28 = 0 非安全
如果地址 Bit_28 = 1 安全
所有外围设备和存储器在两个位置都有映射。



SAU 为每个内存区域定义区域号。区域号为 8 位，由 TT 指令来决定目标内存的访问权限和安全属性。
SAU 中包含的区域数可以配置为 0,4 或 8。
注意：配置 SAU 非安全区域时，必须确保安全数据和代码不会暴露给非安全应用程序。

安全状态的转换
系统以安全状态启动，可以使用指令切换安全状态，如下图所示。



从安全到非安全状态的转换可以由软件通过使用 LSB 的 BXNS 和 BLXNS 指令来启动。
注意：Cortex-M 架构不支持 A32 指令集。这允许地址的最低有效位（LSB）表示安全状态。
从非安全状态到安全状态的转换可以通过两种方式由软件启动：

- 跳转到安全网关区域。
- 跳转到保留值 FNC_RETURN。

安全网关是在 NSC 区域中出现的安全网关指令（SG）。当从非安全状态跳转到安全网关时，SG 指令切换到安全状态并清除 lr 中返回地址的最低有效位（LSB）。在任何其他情况下，SG 指令不会更改安全状态或修改返回地址。保留值 FNC_RETURN 的跳转使硬件切换到安全状态，从安全堆栈的顶部读取地址，并跳转到该地址。在执行 BLXNS 指令时，保留值

FNC_RETURN 被写入 lr。安全状态转换可以由硬件通过处理中断实现。这些转换对软件是透明的，在本文档的其余部分中将被忽略。

TT 指令

ARMV8-M 体系结构引入了指令 TT。TT 指令获取一个内存地址，并返回该地址的 MPU 的配置。一个可选的 T 标志控制是否返回特权执行模式的权限或非特权执行模式的权限。当在安全状态下执行时，该指令的结果被扩展为返回特定地址处的 SAU 和 IDAU 配置。内存保护单元（MPU）在两个安全状态之间。当从安全状态执行 TT 指令时，可选的 A 标志使 TT 指令读取非安全状态的 MPU。 TT 指令用于检查不同安全状态和权限级别对指定地址的内存的访问权限。

您可以在以下链接中找到有关 ARM®TrustZone®的更多有用信息：

https://developer.arm.com/ip-products/security-ip/trustzone
https://www.nxp.com/docs/en/application-note/AN12278.pdf
http://www.keil.com/appnotes/files/apnt_291.pdf
http://infocenter.arm.com/help/topic/com.arm.doc.ecm0359818/ECM0359818_armv8m_security_extensions_reqs_on_dev_tools_1_0.pdf