ARM 最新的 Cortex-M23 與 M33 處理器有哪五大特色？

2017-01-11 *由 集微網 發表於 3C*

原標題：作為 ARM Cortex-M 家族的繼承者 Cortex-M23 與 M33 有哪五大特色？

集微網消息，ARM 處理器在嵌入式設備領域的應用非常廣泛。基於 ARM Cortex 處理器的片上系統（SoC）解決方案適用於多種嵌入式設計細分市場，如物聯網、電機控制、醫療、汽車、家電自動化等。Cortex 系列處理器主要基於 3 大產品類型量身開發，A 系列：運行複雜系統的精細高端應用；R 系列：高性能硬實時系統；M 系列：低功耗、確定性、成本敏感的微控制器，專門優化以滿足其需求。

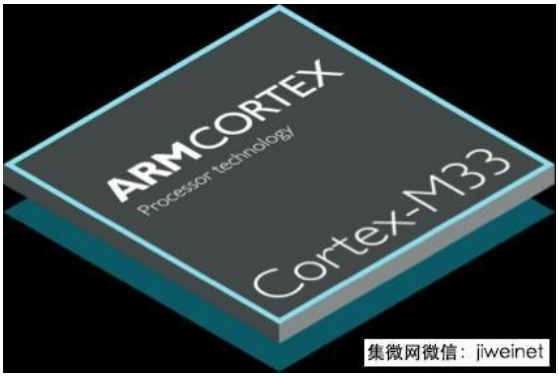
其中，Cortex-M 家族 32 位微控制器（MCU）在業內最廣為人知。該家族包括超低功耗的 Cortex-M0/0+、主流的 Cortex-M3、帶 DSP 浮點運算的 Cortex-M4 和最高性能的 Cortex-M7 系列。

去年 11 月，ARM 公司又推出了 Cortex-M 家族的繼承者，分別是 Cortex-M23 和 Cortex-M33 MCU。其中，Cortex-M23 是 Cortex-M0+的繼任者，主打超低功耗，而 Cortex-M33 是 Cortex-M3 和 Cortex-M4 的繼任者，性能更強，具有 DSP 浮點運算功能。

據悉，ARM Cortex-M23 與 Cortex-M33 是首款基於 ARM 公司最新的 ARMv8-M 架構的嵌入式處理器，而 Cortex-M0/0+、Cortex-M3、Cortex-M4 和 Cortex-M7 則是基於上一代的 ARMv7-M 架構。

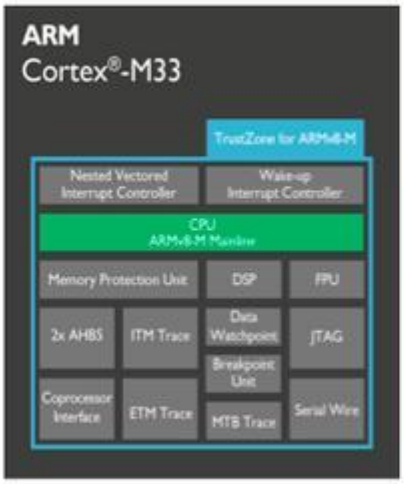
那麼，Cortex-M23 與 Cortex-M33 到底擁有著怎樣的特色呢？

Cortex-M33 是一款能在性能、功耗和安全之間實現最佳平衡的處理器



Cortex-M33 是首款採用 TrustZone 安全技術和數位訊號處理技術的 ARMv8-M 全功能實現處理器。該處理器可以支持大量靈活的配置選項，並在廣泛應用中進行部署，此外還提供專用的協同處理器界面以支持經常需要加速和大量運算的運作。Cortex-M33 是一款在性能、功耗、安全與生產力之間達到最佳平衡的處理器。

為了顯著降低系統功耗，Cortex-M33 處理器採用有序三階管線技術。大部分指令在頭兩個階段就能完成，而複雜的指令則需要 3 個階段。此外，某些 16 位指令將採用雙發射機制，以增強性能。處理器內核有兩個 AMBA 5 AHB5 界面：C-AHB 和 S-AHB，完全對稱，指令和數據提取性能不分伯仲。



- MPU 存储保护单元
- DSP 数字信号处理
- FPU 浮点单元
- SP 单精度

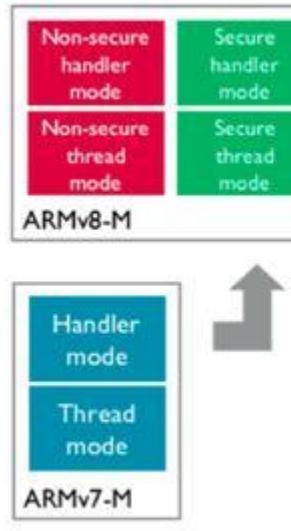
- ETM 嵌入式跟踪宏单元
- MTB 微追踪缓冲器
- BPU 断点单元
- DWT 数据观测与追踪单元
- ITM 仪器追踪宏单元

- NVIC 嵌套向量中断控制器
- WIC 唤醒中断控制器
- AHB 先进高性能总线
- AMBA 先进微控制器总线架构

接下來，讓我們瞭解一下 Cortex-M33 的五大特色：

1 、為 ARMv8-M 量身優化的 TrustZone 技術為整個系統的安全保駕護航

採用 TrustZone 技術的 Cortex-M33 處理器擁有兩個安全狀態及多種相關特色：



- 安全状态
- 非安全状态
- 4 个堆栈和 4 个堆栈指示寄存器
- 硬件堆栈极限检查
- 支持安全属性单元（SAU）的可编程 MPU

- 用于发出系统安全指示的界面
- 被预先设定的接入点限制的非安全（NS）领域中可以看见安全代码
- 其它硬件转向非安全领域时可以自动保存并清除安全寄存器的状态

- 大量堆积中断或异常控制，SysTick
- 安全和非安全侧都配备存储保护单元

两种全新的正交状态

安全狀態和非安全狀態的全面利用，必將開啟眾多新機遇和新應用的大門。該系統使用的高價值專利固件可以在安全狀態下運行。在安全狀態下設置的監管員代碼則可以在系統受到攻擊或

不可靠運行後將其恢復初始;而非安全側則像以前一樣向正在用 Cortex-M 開發軟體的數百萬開發者開放。

2 、協同處理器界面，實現高擴展性

對某些應用而言，專用運算起到的作用可謂非同小可；但為了實現專用運算，這個全球最強大設計生態系統的所有優點必須完美保留，即允許設計師在開發工具、編譯器、調試器、作業系統和中間件之間最大限度的進行選擇。ARM 生態系統可以幫助開發商節約時間和成本，進一步提高生產力。

Cortex-M33 處理器包含一個可以選配、類似總線的專用界面，主要用於集成緊耦合加速器硬體。對需要頻繁運算的操作而言，該界面可以幫助設計師用自定義的處理硬體提升通用運算能力。須著重指出的是，這樣做並不會使整個生態系統分裂。該界面包含最多可用於 8 個協同處理器的控制和數據通路，發出的信號可顯示處理器的特權狀態和安全狀態、指令類型、相關寄存器和操作欄位。協同處理器通常會合理的在幾個少數循環內完成，或在後台運行並在完成時自動停止。操作的細節和數據可以通過該界面與單指令同時傳輸，如有需要，還可插入等待狀態。

3 、用於任務隔離的存儲保護單元（MPU）

設計師可以自行對選配的 MPU 編程，為每個安全狀態和非安全狀態提供多達 16 個區域。在多任務環境中，作業系統可以在任務情境切換時重新編程 MPU，為每個任務定義存儲訪問許可。比如說，某個應用的某個任務只被允許訪問某些應用數據和特定的周邊設備，這種情況下，MPU 將保護所有其他的存儲和周邊設備,將訛誤或未授權訪問阻擋在外,有效提升系統可靠性。

存储区设置更简易

Cortex-M33 存儲保護架構的開發基於受保護的存儲系統架構 PMSAv8。最新版本搭載了針對各區域的基線與限值比較器，而非此前的二次方尺寸對齊模型。每個區域都有一個基線的初始地址、終止地址，以及訪問許可和存儲性質的設定值，因此在這一架構中，設計師設計 MPU 區域時再也無需顧慮將多個區域整合在一起的麻煩了。功能強化後，軟體開發變得更加簡單，客戶的使用意願提升，編程步驟也得以減少，並將進而降低情境轉換次數。

4 、DSP 拓展

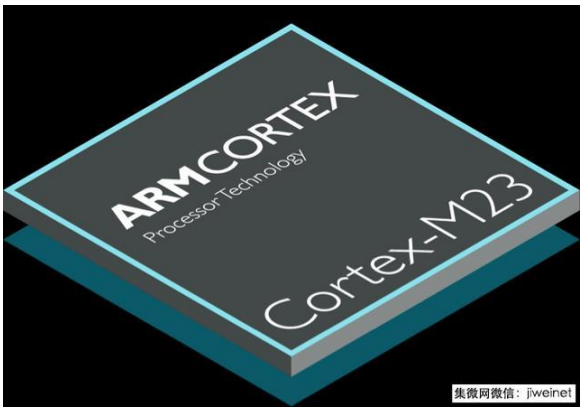
選配的整數 DSP 拓展可以為系統增加 85 個新指令。大多數情況下，DSP 指令可將性能平均提升 3 倍，讓所有以數位訊號控制為中心的應用性能突飛猛進。

為幫助設計師加速軟體開發，ARM 將在 CMSIS 項目中提供免費的 DSP 庫，包含整套過濾、轉換和數學功能（如矩陣），並支持多種數據類型。CMSIS 項目是開源的，其開發詳情發佈在 github 上。

5 、單精度浮點單元

基於 FPv5 的選配單精度浮點拓展單元包括一份額外的 16-入口 64 位寄存器文件。該拓展新增 45 個與 IEEE754-2008 兼容的單精度浮點指令。使用浮點指令通常可將軟體庫平均性能提升 10 倍。FPU 位於單獨的電源域，負責在整個單元不使用的時候切斷電源。

Cortex-M23 是一款尺寸最小、能效最高的處理器



ARM Cortex-M23 採用 TrustZone 技術，是尺寸最小、能效最高的處理器。小型嵌入式應用對晶片的安全性能有嚴格要求，基於 ARMv8-M 基線架構的 Cortex-M23 處理器則是最佳解決方案。

同樣地，讓我們也來瞭解一下 Cortex-M23 的五大特色：

1、為 ARMv8-M 量身打造的 TrustZone 技術：安全實現的基礎

TrustZone 技術為 ARMv8-M 度身優化，可以在每一台搭載 Cortex-M23 處理器的設備上以硬體形式實現可信軟體和非可信軟體強制隔離。因此，採用 TrustZone，設計師只需一個處理器就可以設計嵌入式應用，此前則必須使用多個處理器才能在可信區域和非可信區域之間實現物理隔離。僅需 Cortex-M23 處理器，既可出色實現多項安全需求，如設備識別管理、高價值固件保護、軟體認證、安全根等等。

採用 TrustZone 技術的 Cortex-M23 處理器具備以下兩種安全狀態：

•安全狀態 – 可以訪問安全和非安全資源（存儲、周邊設備等）

•非安全狀態 – 只可訪問非安全資源

兩種安全狀態下的代碼執行轉換和代碼訪問均由硬體監管，最大限度地降低轉換管理成本並保證確定性—這也是所有 Cortex-M 處理器的標誌性功能。

2、緊湊二階布線處理器

Cortex-M23 是一款簡單的二階布線馮諾依曼處理器（Von Neumann processor），但卻足以支持全套 ARMv8-M 基線指令集。熟悉 Cortex-M0+的用戶一定可以迅速指出 Cortex-M23 使能效最大化的眾多相似特色：WFI（等待中斷）／WFE（等待事件）和睡眠／深度睡眠模式、退出時睡眠、SysTick 定時器和選配的單循環 IO 等。

指令集共包含 80 條左右的拇指指令，其中大多數都是 16 位指令（為了儘可能提高代碼的緊湊度），但仍有一些為了提升效率而設置的 32 位指令。Cortex-M23 支持所有的 ARMv6-M 指令，以幫助設計師輕而易舉地將代碼從 Cortex-M0 和 Cortex-M0+處理器轉移至 Cortex-M23。此外 ARMv8-M 基線指令集中還加入了多條新指令以提升條件運算、互斥訪問、硬體劃分運算和即時移動的效率。

3、強化的調試糾錯與追溯能力

僅憑一台高效安全的 32 位處理器，尚無法成功實現欄位部署，軟體開發的成本通常超過生產和硬體 IP 的總和。Cortex-M23 引入更多可配置的硬體斷點和數據觀測點，對比其他 ARMv6-M 處理器，可以助設計師更輕鬆地實現軟體開發與調試。除了 Cortex-M0+ 處理器中也配置的微型跟蹤緩衝器（MTB），Cortex-M23 還包括選配的嵌入式跟蹤宏單元（ETM）。有了這些選配功能，設計師可以自行判斷，究竟選擇更加豐富全面的指令追溯能力；還是性價比更高、更加精簡的指令追溯能力。

4、 用於任務隔離的存儲保護單元

Cortex-M23 還包括選配存儲保護單元（MPU），基於全新 PMSAv8 架構打造，設計師使用起來非常方便。它可以在安全和非安全狀態的任何一個狀態下最多「保護」16 個區域。每個區域都有一個基礎地址、結束地址、訪問許可和存儲屬性設置。在多任務環境下，作業系統可以在任務情境切換的過程中重新編程 MPU，定義每個任務的存儲許可，比如允許應用任務訪問全部或部分應用數據和特定的周邊設備。通過保護許可之外的數據免遭污染，並阻止未授權來源訪問許可之外的周邊設備，該 MPU 可以顯著提升系統可靠性。

更易設置的存儲區域

Cortex-M23 的存儲保護架構採用基線和限值比較器，用以定義存儲區域，而此前使用的是二次方尺寸對齊比較器。這項改進簡化了軟體研發的複雜程度，而且在某些情況下，當區域尺寸不是完美的二次方尺寸時，還能減少存儲浪費。

5、 全新 ARMv8-M 基線指令

對比 ARMv6-M，Cortex-M23 加入了許多全新指令，但絲毫沒有折損 Cortex-M 系列處理器的超高能效。大多數新指令（除用於安全拓展外）都繼承自 ARMv7-M 的架構指令集，進一步拓展 Cortex-M23 的功能，並與 Cortex-M0+ 處理器形成鮮明區分。

5.1 安全拓展

ARMv8-M 採用的 TrustZone 安全技術為基線指令集補充了全新指令，包括安全網關（SG）、非安全支路（BXNS、BLXNS）以及測試目標（TT）指令。欲知詳情，請參閱 Yiu 撰寫的《ARMv8-M 架構介紹》。

5.2 僅執行代碼生成

對僅執行（Execute-Only）代碼存儲區的支持也獲得改善，新增加的即時移動指令（從 ARMv7-M 繼承的 MOV/MOVT）可以在僅執行代碼中生成即時數據，讓設計師僅憑 2 條指令便能生成 32 位值，且無需運行實際負載。

5.3 代碼優化

條件比較和支路指令（從 ARMv7-M 繼承的 CBNZ/CBZ）可以提高多項條件控制代碼序列的性能。長偏移即時支路（從 ARMv7-M 繼承的）可以將支路指向遙遠的目標地址；硬體整數劃分指令（從 ARMv7-M 繼承的 SDIV/UDIV）則可以減少除法運算的處理循環。

5.4 排斥存取

Cortex-M23 還從 ARMv7-M 繼承了負載和儲存的專用指令，提升 Cortex-M23 在多核系統中的一貫性，確保多個處理器以同樣的機制處理信號。此外，為了對 C11/C++11 提供穩定支持，Cortex-M23 還新增 ARMv8-A（Thumb 32 版本）的負載獲取與儲存釋放指令，并包括這些指令的排斥存取變種。

原文網址：https://kknews.cc/digital/6kgpaxv.html