An Introduction to the Arm Cortex-M35P Processor

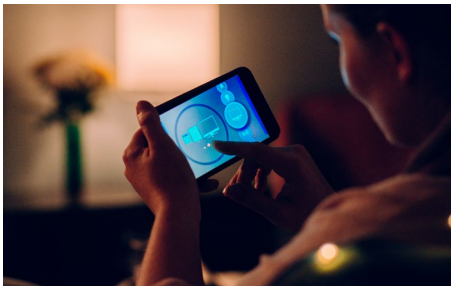
Kobus Marneweck, Senior Product Manager, Embedded, Arm

2018

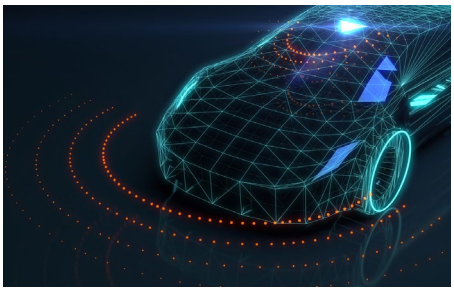
White Paper

Table of Contents

1. Introduction



Cortex-A: Highest performance
Designed for high-level operating systems



Cortex-R: Faster responsiveness
Designed for high performance, hard real-time applications

Cortex-M: Smallest/lowest power
Designed for discrete processing and microcontrollers

SecurCore: Tamper resistant
Designed for physical security

Arm processor families: Diverse applications need diverse compute

System-on-chip (SoC) solutions based on Arm processors address many different embedded market segments including IoT, motor control, healthcare, automotive, home automation, wearables, robotics, retail, industrial, networking and wireless connectivity. The Arm Cortex family of processors provides a standard architecture to address the broad performance spectrum and cost range required by these diverse product markets. The Arm Cortex family includes processors based on three distinct profiles:

- The Cortex-A processor family for sophisticated, high-end applications running mainly complex operating systems
- The Cortex-R processor family for high performance hard real-time systems
- The Cortex-M processor family optimized for low power, deterministic, cost-sensitive microcontroller applications
- The SecurCore processor family is designed with physical security in mind, featuring built-in anti-tampering capabilities

This whitepaper will focus on the Cortex-M35P processor. Cortex-M35P is part of the Cortex-M product family, which is selected by developers who wish to scale their product across the Cortex-M range, as they can reuse their existing software base. It is the first Armv8-M processor with tamper-resistance designed in, making it easier and faster to get IoT, payment or telecom-certified security at the core. It is a fortress of a processor with multiple layers of security, combining software protection with Arm TrustZone technology and physical protection featured in our SecurCore family of processors. The Cortex-M35P is an extension of Arm's comprehensive security portfolio, following the principles of Arm's Platform Security Architecture (PSA).

Cortex-M35P with security against physical attacks

Communication Attacks
- Man-In-The-Middle
- Weak RNG
- Code vulnerabilities

Physical Attacks
- Fault injection: clock or power glitch, alpha ray
- Side-channel analysis
- Probing, FIB

Lifecycle Attacks
- Code downgrade
- Excess manufacturing
- Integrity vulnerabilities

Software Attacks
- Buffer overflows
- Interrupts
- Malware

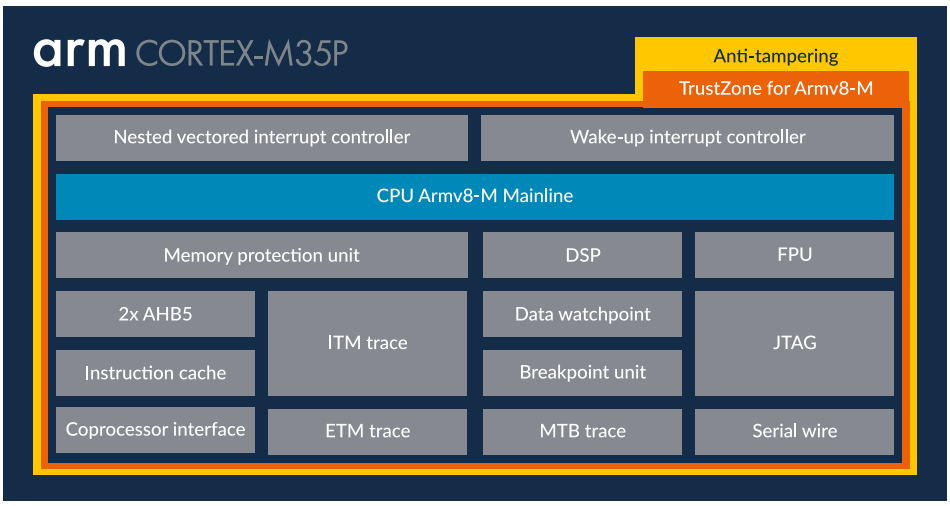
The Cortex-M35P is part of a family of physical security technology. This suite of IP provides protection from both invasive and non-invasive silicon attacks, accessible for all chip designers. The related IP are marked with a "P" tag for "physical security":

- **Arm CryptoCell-312P:** Provides a rich set of functions enabling robust cryptography, code and data protection, keys and lifecycle management and more
- **CryptoIsland-300P:** A security enclave, handling all hardware and software aspects of a security subsystem by providing a fully-isolated execution environment to handle workloads requiring smartcard-like security

Here is a quick summary of the benefits of using the Cortex-M35P:

Design with confidence Based on proven, widely-supported security technology	Security and safety Physical security with advanced safety features	Accelerate success Broad IP portfolio and ecosystem support to reduce development cost
Builds on proven physical resilience technology deployed in billions of SecurCore processors	Adds physical resilience to the familiar Cortex-M family, without compromising performance	Optimized fit within our comprehensive Arm security solution portfolio
Incorporates TrustZone technology, supported in billions of Cortex-A based devices	Flexible, with optional features for advanced functionality, including signal processing	Easy upgrade path from the Cortex-M33 processor
Reuses existing knowledge with the same programmers' model deployed by millions of Cortex-M developers	Extra safety (lockstep, configurable parity, observability) for faster and lower cost deployment of system safety functions	Reuses existing software built on Cortex-M based devices
		Supported by the world's #1 embedded ecosystem with the largest open knowledge base

The Cortex-M35P is a fully synthesizable, mid-range microcontroller class processor based on the Armv8-M architecture. The design focuses on energy efficiency by maintaining high compute performance with low-power consumption. It also supports a large number of configurable options to facilitate deployment in a wide-range of applications. As mentioned above, it features anti-tampering capabilities that are proven in the SecurCore processor series, as well as TrustZone for Armv8-M technology – together offering silicon and software security. With these design criteria, Cortex-M35P delivers a high degree of energy efficiency, software productivity and the basis for system security for embedded applications.



Here's a snapshot of the technical features of the Cortex-M35P:

- Mainline Extension of the Armv8-M including the 16-bit and 32-bit Thumb instruction set
- Armv8-M exception model
- Arm PMSAv8 memory system architecture
- Optional configurable memory protection unit supporting up to 16 regions for each of the Secure and Non-secure states
- Optional support for the Armv8-M Security Extensions
- Optional Configurable Security Attribution Unit supporting up to 8 memory regions
- Optional Arm FPv5 hardware single precision floating point unit
- Optional Arm DSP Extension instruction set
- Optional execution trace using MTB or instruction trace using ETM
- Integrated interrupt controller supporting up to 480 external interrupts with up to 256 priority levels

Useful terms:

MPU	Memory Protection Unit
DSP	Digital Signal processing
SIMD	Single Instruction Multiple Data
FPU	Floating Point Unit
FP	Floating Point
SP	Single Precision
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
WIC	Wake-up Interrupt Controller
CTI	Cross Trigger Interface
AHB	Advanced High-Performance Bus
AMBA	Advanced Microcontroller Bus Architecture

1.1. Energy Efficiency

The first pillar of the Cortex-M family is very high, system-wide energy efficiency. Reducing power consumption over time, of the whole system, is nearly always a key design goal. A standard approach to reduce system power is to apply the known design rule of: wake-up, execute as fast as possible, then go back to sleep. When the processor is active then all the I/O, memory, and other system components are usually active. The shorter the amount of time that a processor remains active, the better the overall system energy efficiency.

In order to achieve higher performance or execution speed, processors can either work hard or work smart. Pushing higher clock frequencies may increase performance but is also accompanied by higher system power consumption and design complexity. On the other hand, the Cortex-M 32-bit higher compute efficiency at slower clock speeds results in simpler and lower power system designs that deliver the same computational tasks and desired response time.

The Cortex-M35P processor supports extensive clock gating, power islands and software controlled integrated sleep modes. With these features, the processor delivers a power consumption of just 20.8uW/MHz when implemented at a target frequency of 100MHz on the TSMC 40LP process node.

1.2. Ease of Use

The second pillar of the Cortex-M family is ease of use. Reducing time-to-market and lowering development costs are critical criteria in the choice of microcontrollers, and the ability to quickly and easily develop software is the key factor for these requirements. The Cortex-M35P processor continues along with the Cortex-M simplified stack-based programmer's model where it is fast and easy to program. Users are not required to write any assembler code or have deep knowledge of the architecture to create applications. Additionally, a hardware-based interrupt scheme means that writing interrupt service routines is like writing any other routine, and that start-up code is significantly simplified, as no assembler code register manipulation is required.

The Cortex-M processor family has the widest ecosystem of operating systems, tools, and middleware of any processor on the market today. Such a vibrant ecosystem opens up the choice for users and ensures a steady supply of innovative products created to help design hardware and software for Cortex-M systems. Arm also maintains and drives the Cortex Microcontroller Software Interface Standard (CMSIS), a vendor-independent hardware abstraction layer. CMSIS enables consistent and simple software interfaces to the processor for interface peripherals, real-time operating systems, and middleware thus further reducing the learning curve and time to project completion. The CMSIS core layer simplifies migration between the various processors in the family. More details are to be found here https://github.com/Arm-software/CMSIS_5.

1.3. 32-bit Performance

The Cortex-M35P processor is based on a 32-bit RISC architecture like the other processors in the Cortex-M family. At the heart of the Cortex-M35P processor is an in-order 2/3-stage pipeline core, based on a Harvard architecture, which delivers an exceptional Dhrystone benchmark performance of 1.50 DMIPS/MHz. Some instructions take two stages to complete; others require three, while some 16-bit instructions are dual issued.

The Integrated Nested Vectored Interrupt Controller (NVIC) is the unit behind the low latency interrupt response time and the various other features for increasing the performance for interrupt handlers such as tail chaining, pre-empting and the like. In addition, the Cortex-M35P processor has an optional integrated cache that improves performance when running from embedded flash or external serial Flash. Flash access time does not scale as well as RAM, and is a common performance bottleneck. This problem is solved by activating the optional internal cache. The information stored in the cache is also protected against physical attacks.

The Cortex-M35P processor has many configuration options including DSP, Floating point, TrustZone and a co-processor interface. Specific configurations will meet requirements for different products. The DSP and floating-point instructions are essential for signal processing applications.

1.4. Reduced System Cost

All processors in the Cortex-M family have an integrated interrupt controller and various debug and trace blocks. Be it the instrumentation trace, watchpoints, breakpoints, Micro Trace Buffer (MTB) or the Embedded Trace Macro cell (ETM), all increase productivity by simplifying the process of software development and debug.

The Cortex-M35P processor is very small in area; 0.06mm2 at 40nm at 100MHz. Given the analog components, memory and peripherals found in devices these days, the size of the processor represents only a very small fraction of the whole die.

1.5. Silicon and Software Security

The hallmark security features in the Cortex-M35P relate to anti-tampering (silicon security) and TrustZone for Armv8-M (software security).

When the value of the protected asset is high enough then hackers will resort to physical attacks on the device. The processor is built with multiple elements to protect it from and detect such attacks.

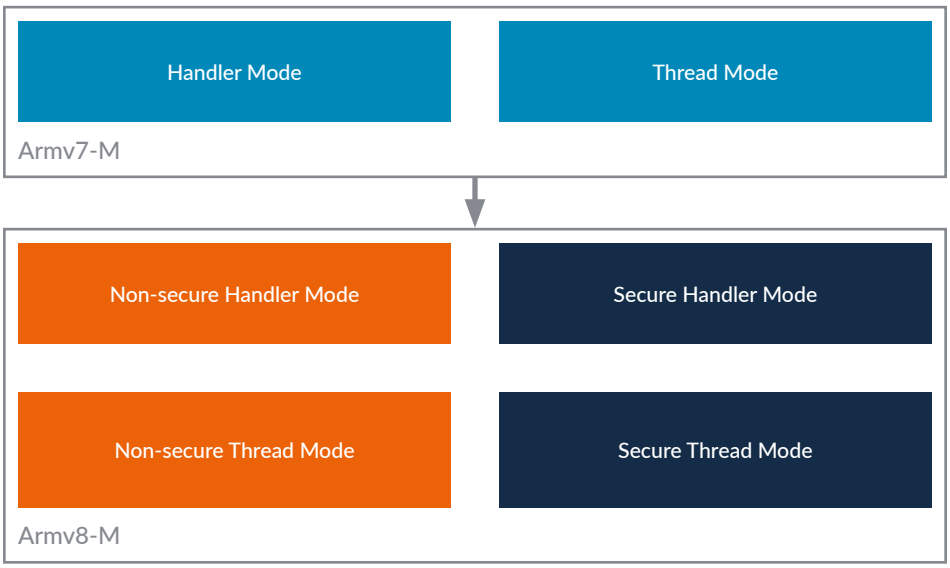
For example, uniform-timing allows certain instructions to execute in a constant number of cycles whatever the operands, preventing information leaks. The activation of this feature is optional.

Another example is 100% parity coverage. Every flop in the processor is protected with a configurable parity. This allows random errors or intentionally-injected faults to be detected. There are of course many more features that give the Cortex-M35P the anti-tampering protection. These features are covered under NDA so please contact your account manager for details.

For software security, the hardware-enforced isolation mechanism in our Armv8-M processors is referred to as TrustZone: a foundation for embedded devices. It offers hardware access control to code, memory and I/O, while retaining the requirements of embedded applications: real-time response, minimal switching overhead, and ease of software development.

The Armv8-M architecture adds an extra state to the operation of the Cortex-M35P processor so that there are both a Secure and Non-secure execution states. These security states are orthogonal to the existing Thread and Handler modes, thereby having both a Thread and Handler mode in both Secure and Non-secure modes.

Armv8-M additional security states



1.6. Faster Time-to-Market

Every embedded system designer faces the challenge of fast turnaround, the problem being compounded in many cases by design complexities and the unavailability of quality software tools. Most recently, the rise of connectivity has imposed a burden of security on system designers. Productivity and security now go together. A bias towards one or the other puts the viability of the product at risk.

The reuse of design and software from earlier systems is a standard technique applied to meet the challenge of time to market. The Cortex-M35P processor inherits and builds upon the existing large ecosystem of Cortex-M. The ecosystem partners have also realized the need for security and are actively expanding their product offerings to meet the demand. Supported by integrated system components and that broad ecosystem of software tools, the Cortex-M35P processor offers a complete solution that facilitates faster time-to-market for both new systems and those migrating to the Armv8-M architecture.

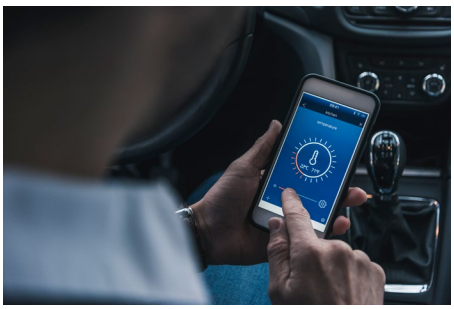
2. Cortex-M35P Processor Features and Benefits

2.1. The Cortex-M35P Processor

The core has been redesigned from the ground up with an in-order 2/3-stage pipeline. Most instructions complete in two stages while some instructions require three. The combined decode/execute stage evaluates and branches in the same cycle hence there is no need for branch predictor. Some 16-bit instructions are dual issued. The overall result is a dramatic increase in system energy efficiency.

The core has two AMBA 5 AHB5 interfaces. The previous I-CODE and D-CODE interfaces are merged into a single interface (C-AHB) to improve energy efficiency with no loss in performance. The System bus (S-AHB) is the same as before. The advantages of separate buses for instructions and data are low compared to the gain in energy efficiency using a combined bus. The C-AHB and S-AHB are symmetric. The performance of instruction and data fetches on the two interfaces is identical, only the mapped address is different. One could run code from system memory without an extra cycle penalty.

The Cortex-M35P processor is highly configurable and is easily adapted to system requirements. Designers can create complex systems faster by including the optional MPU, DSP, FPU, TrustZone, ETM, MTB, ITM, BPU, DWT and co-processor interface in the system or not. In simple control systems the NVIC can be configured to one interrupt, while in interrupt intensive systems like automotive 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 would be used.



The increasingly time-consuming validation of applications can make on-chip debug and trace extremely valuable to on-time delivery of products. The integrated debug capabilities of the Cortex-M35P processor allow for faster verification. The system can be viewed through either a JTAG port or a 2-pin Serial Wire Debug port. The optional ETM provides excellent instruction trace capabilities while the DWT provide the capability to use breakpoints and hardware watchpoints for debug.

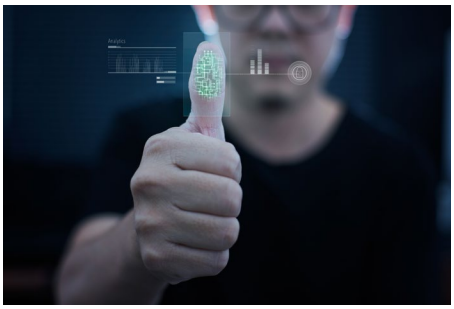
Given all these features and options, one design can be used as the base to a whole set of devices thus reducing overall development cost. TrustZone protects valuable firmware and reduces the support load, and the enhanced debug features reduce the development cost for the end user.

2.2. Cortex-M35P Instruction Set

Cortex-M35P is an implementation of the Armv8-M architecture, including baseline with the Mainline, DSP/SIMD, security and the single precision floating-point extensions. The baseline Armv8-M architecture is derived from the Armv6-M architecture and has the following extensions:

- Mainline extension:
  The mainline extension is derived from the Armv7-M architecture. It enhances the baseline Armv8-M architecture by adding more instructions and dedicated fault handlers. Here are a few highlights:
  - Supports all instructions from Armv7-M, full Thumb®-2 Technology set
  - Extended immediate ranges, more addressing modes, “IT” for conditional instructions
  - C11 Atomics
- DSP extension:
  This optional extension adds the Arm DSP instructions to the Armv8-M Thumb instruction set. These instructions include saturating and unsigned SIMD instructions.
- Floating-point extension:
  This optional extension adds floating-point instructions to the Armv8-M instruction set to provide support for single-precision and, optionally, double-precision implementations.
- Security extension:
  The security extension provides two private states of execution. Areas of memory and other critical resources, which are marked as private, can only be accessed when in one of the private states.

The Armv8-M architecture only supports execution of T32 instructions. The Floating-point (FP) extension adds floating-point instructions to the T32 instruction set. The complete instruction set of Cortex-M35P makes it very well positioned to become the next industry standard for general-purpose embedded 32-bit compute. The implementation of floating-point in Cortex-M35P does not include double precision.



2.3. Anti-tampering (or physical security)

The anti-tampering features of the Cortex-M35P are covered by an NDA so please contact your account manager for full details.

2.4. DSP/SIMD Extension

To accelerate software development, Arm also delivers a free DSP library in the CMSIS project. The library contains a range of filter, transformation and math functions (e.g. matrix), and supports a range of data types. The CMSIS project is now open source and the development is published in GitHub.

The optional integer DSP extension adds 85 instructions. In most cases, the DSP instructions would increase performance by an average of three times, giving a boost to all applications that are centered around digital signal control.

2.5. Single Precision FPU

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 approximately 45 IEEE754-2008 compatible single-precision floating-point instructions. Using floating-point instructions usually yields a ten times increase in performance over the equivalent software libraries.

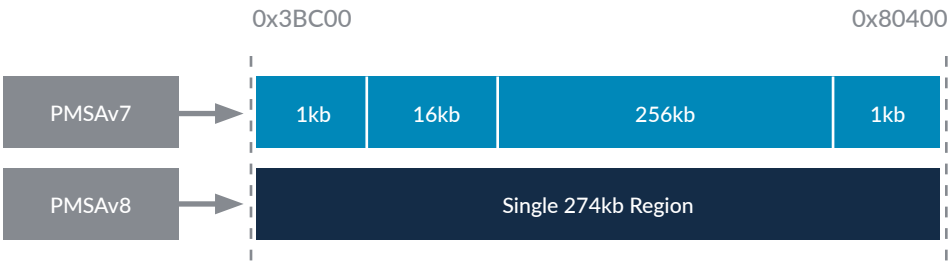
The FPU is contained in a separate power domain allowing the unit to be powered-down when not enabled or in use to further reduce power.

2.6. Memory Protection Unit (MPU)

Software reliability and system security improves when each module is allowed access only to specific areas of memory required for it to operate. This protection, complementary to TrustZone, prevents unexpected access that may overwrite critical data. Each of the security zones can have a dedicated MPU that may be configured with a different number of regions. Programming the regions is easier, removing the constraint to align regions on power-of-two size.

The MPU is programmable and provides up to 16 regions for each of the Secure and Non-secure states. Each region has a base address, size, access permission and memory attribute settings. In multi-tasking environments, the OS can reprogram the MPU during task context switching to define the memory permissions for each task. For example, tasks of an application may be granted access to all or some application data and specific peripherals. The MPU protects all other data from corruption and other peripherals from unauthorized access to dramatically improve system reliability.

Easier to setup memory regions



Cortex-M35P's memory protection architecture is based on the protected memory system architecture PMSAv8-M, which uses elements of both PMSAv8-R and PMSAv7-M. PMSAv8-M adopts base and limit style comparators for regions as opposed to the previous power-of-two size, sized aligned scheme. The result is that one can produce MPU regions without having to consider joining a number of regions together. This enhancement simplifies software development, encourages usage and reduces programming steps, which reduces context switch times.

2.7. Security Extensions (TrustZone)

The Cortex-M35P processor with the Security Extension has two Security states:

- Secure state
- Non-secure state

A few highlights of the security extension feature set:

- Four stacks and four stack pointer registers
- Stack-limit checking
- Each memory address tagged as either being Secure or Non-Secure
- Support for programmable MPU-like Security Attribution Unit (SAU), or fixed/ external configuration
- Visibility of Secure code from Non-Secure (NS) domain restricted to function calls
- Exception hardware automatically stashes Secure register state when switching to Non-Secure. Registers cleared after stashing
- Non-Secure entry to Secure restricted to Secure locations containing Secure Gateway (SG) instruction
- Extensive banking of interrupt / exception control, SysTick and entire MPU (if present)

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

2.8. Nested Vectored Interrupt Controller (NVIC)

All Cortex-M processors, including Cortex-M35P, are designed for deterministic and fast interrupt response. The built in NVIC is a key element of that design. The NVIC supports late arrival and pre-emption based on priority groups and Tail-chaining for interrupts that occur back-to-back, In case of the late arrival of a higher priority interrupt during the execution of the stack Push for a previous interrupt, the NVIC immediately fetches a new vector address to service the pending interrupt, Similarly, the NVIC abandons a stack Pop if an exception arrives and services the new interrupt immediately. By pre-empting and switching to the second interrupt without completing the state restore and save, the NVIC achieves lower latency in a deterministic manner. The Non-Maskable Interrupt (NMI) further enhances determinism by allowing the critical interrupt source to be made non-maskable; a particularly important feature in systems with a watchdog timer that needs to be reliably serviced at particular time intervals.

The NVIC fully supports the security extension with further controls for setting the target state of each interrupt and for setting the relative priority between Secure and Non-secure interrupts. The NVIC will automatically save and clear registers of the Secure state if preempted by a Non-secure interrupt.

Fast and predictable response to interrupts is critical for safe operations. The Cortex-M35P processor maintains that response despite the addition of the two security states.

2.9. Wake up Interrupt Controller (WIC)

The Cortex-M35P processor includes an optional WIC which, when activated is responsible for latching pending exceptions and detecting wake-up conditions. The NVIC can therefore be inactive and the clocks to the remainder of the processor can be clock gated or potentially powered down in a software transparent manner if the logic is implemented with retention.

When the WIC is active the processor will handshake with the WIC to offload all prioritization information about exceptions before entering sleep mode. For WIC based operation, the system is required to establish the WICDSREQn/WICDSACKn handshake with the processor before it enters sleep mode. While in sleep mode, indicated by either the SLEEPING signal or the Q-Channel COREQACTIVE signal, the events which will wake up the processor can be read on the WICSENSE bus.

When an appropriate event is detected by the WIC in the processor it will raise the WAKEUP signal to indicate to the system that the processor will be woken-up by the WIC and if powered-down needs to be powered-up. The WAKEUP signal is also taken into account in the Q-Channel COREQACTIVE signal.

An integrated WIC is essential to reduce the power of the system by totally shutting down the processor and the majority of the peripherals during sleep periods.

2.10. Code and System Bus Interfaces

The Cortex-M35P processor has two AMBA 5 AHB5 interfaces. The C-AHB interface is used for any instruction fetch and data access to the Code region of the Armv8-M memory map. In a microcontroller system the interface is usually connected to flash memory. The S-AHB interface is used for any instruction fetch and data access to the SRAM, Peripheral, External RAM and External device regions of the memory map.

The internal Bus matrix will arbitrate access to the C-AHB and S-AHB interfaces, with higher priority given to data read and write requests. An AHB to APB Bridge, inside the processor bus matrix, is used to access the internal debug and trace peripherals and to drive the external APB peripherals.

Cortex-M35P also includes a number of other interfaces that are designed to service debug and trace operations.

Most AHB5 signals have the same behavior as in AHB-Lite, the interface used by previous Cortex-M processors. So in many instances, AHB bus masters and bus slaves can be reused as they are. The key enhancements to AHB5 over AHB-Lite are:

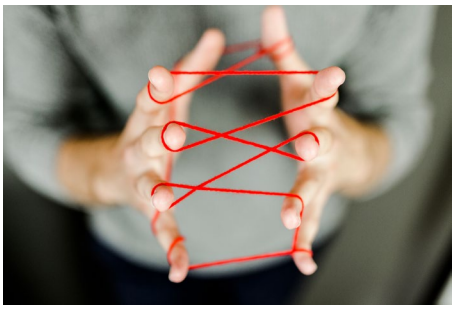
- Addition of a new sideband signal to support TrustZone
- Extension of HPROT signal for additional memory attributes
- Addition of several new sideband signals to support exclusive accesses, including HMASTER signals
- Addition of user defined signals (HxUSER)

The two AHB5 interfaces yield the optimal balance between throughput and power while maintaining compatibility with the large variety of existing peripherals that are available today for AHB-Lite.

2.11. The Co-processor Interface for Extensibility

For certain applications, special-purpose compute can make a difference. It is essential that this is done in a way that maintains all of the benefits of the world's #1 ecosystem – the widest choice of development tools, compilers, debuggers, operating systems, and middleware.

The Cortex-M35P processor includes an optional, dedicated 64-bit bus interface designed for the integration of tightly coupled accelerator hardware. The 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-processors are expected to either complete in a reasonable number of cycles or to interrupt on completion. The operation is started when the operands are transferred and then the application may either poll for a result or the co-processor could generate an interrupt when the result is available.

This interface gives the mechanism to add custom processing to the system with minimal design effort.

For extensibility, certain hardware operations need to be tightly coupled with the processor. The co-processor interface offers this dedicated interface direct to the processor in order to move the hardware block from the system bus to reduce the traffic on the system bus and most of all to achieve the tight operation with the processor.

2.12. Integrated Debug and Trace

Cortex-M35P includes a wide range of optional Armv8-M and CoreSight features designed to support debug and trace of software running on the processor including:

- A Breakpoint Unit (BPU) with configurable support for 4 or 8 hardware breakpoints
- A data Watchpoint and Trace unit (DWT) with configurable support for 2 or 4 hardware comparators which can match both address and data values
- Full access to the memory map and registers via a 32-bit D-AHB interface
- Instrumentation Trace Macrocell (ITM) for software driven ‘printf’ debugging which can be linked to the DWT
- Embedded Trace Macrocell (ETM) supporting full instruction trace using the ETMv4.2 architecture. Data trace is not supported
- Micro Trace Buffer (MTB), a low area cost execution trace solution
- Access control preventing unauthorized debug or trace of Secure state or memory.

The debug features of Cortex-M35P are generally a super-set of those available on previous Cortex-M processors. The comprehensive debug and trace features are necessary to boost the productivity of software developers. The higher the quality of the debug and trace information the faster the application code can be written.

2.13. Low Power Operation

The objective of most designers of embedded solutions is to reach the lowest possible system power at the best possible performance. The Cortex-M35P processor is designed with that objective in mind with various low power enabling features.

2.13.1. Clock Gating

The Cortex-M35P processor uses a single clock source for all internal logic. To minimize the dynamic power used by the processor this clock is gated throughout the design according to the structural hierarchy of the design and the operating mode, for example the hardware floating-point unit is only clocked when a floating-point instruction is present in the pipeline. Clock gating is also applied to power domains that have been disabled.

2.13.2. Integrated sleep modes

Armv8-M defines an architectural low power state called sleep mode. A transition to sleep mode can be initiated by the features described in the table below. All these features are included in the Cortex-M35P processor together with interfaces to allow them to be efficiently implemented in a system.

Feature	Description
WFI (wait for Interrupt)	On execution of this instruction, the processor enters sleep mode until an interrupt is raised
WFE (wait for event)	On execution of this instruction, the processor enters sleep mode until the internal architectural event register is set (for example, if an external event is raised on the external RXEV signal)
SLEEPONEXIT	When this bit is set in the control register, the processor enters sleep mode when executing an exception return to Thread mode. It can subsequently tail-chain when an interrupt is raised. This allows reduction in the energy spent on stacking and un-stacking in a purely interrupt-driven system

There are two levels of sleep controlled using the System Control Register, regular sleep and deep sleep. The sleep modes are used to implement more invasive power reduction; with deep sleep generally indicting that wake-up will take longer. The Cortex-M35P processor does not internally distinguish between these two sleep modes, but indicates which mode is active using the SLEEPING and SLEEPDEEP output signals. In addition to these architectural features Cortex-M35P also supports functionality to optimize the power used by the processor including:

- Optional Wake-up Interrupt controller (WIC) to allow the wake-up requirements to be managed by a single block, while the majority of the processor logic is clock-gated in sleep mode.
- Block level dynamic clock gating, reducing dynamic power when the associated functionality is not in use
- Multiple power domains to allow blocks to be turned off when not used, reducing leakage.

2.13.3. Q Channel

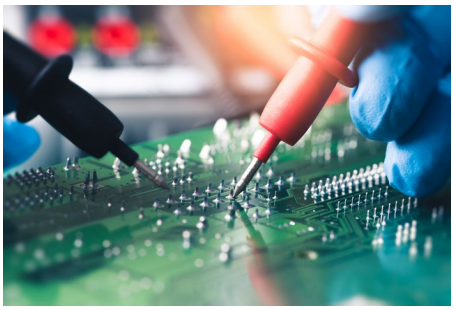
The Q-Channel architecture allows a device including power domains to define a contract with a power management unit (PMU) to support a set of defined power states, and logical transitions between these states. It also allows the device to indicate to the PMU that a particular domain must be powered-up, or that a domain could be powered-down. Power state changes can be initiated by System level conditions, for example when the device is put in to stand-by mode, or by the Cortex-M35P processor when either entering sleep, or when functionality is enabled or disabled during run-time. An example of the latter case is when the FPU domain must be powered-on when hardware floating point is used in software.

The Cortex-M35P processor has the following power domains:

- Always-on Domain: Includes the WIC, top-level clock gating and reset control and Q-channel logic
- Core Domain: Includes the majority of the processor logic
- FPU Domain: The floating point arithmetic data-path and control logic
- Debug Domain: The BPU, DWT and ITM state and comparator logic and the ETM/MTB

Each domain is controlled using a separate Q-Channel interface on the Cortex-M35P processor.

The implementation of the above low-power states and techniques are specific and different to each system. The important item is that with such a collection of low power technologies, embedded systems will easily push further in reducing system power while boosting performance.



3. Migration from Cortex-M4

For people familiar with the Cortex-M4, here is a list of the differences between Cortex-M35P and the Cortex-M4.

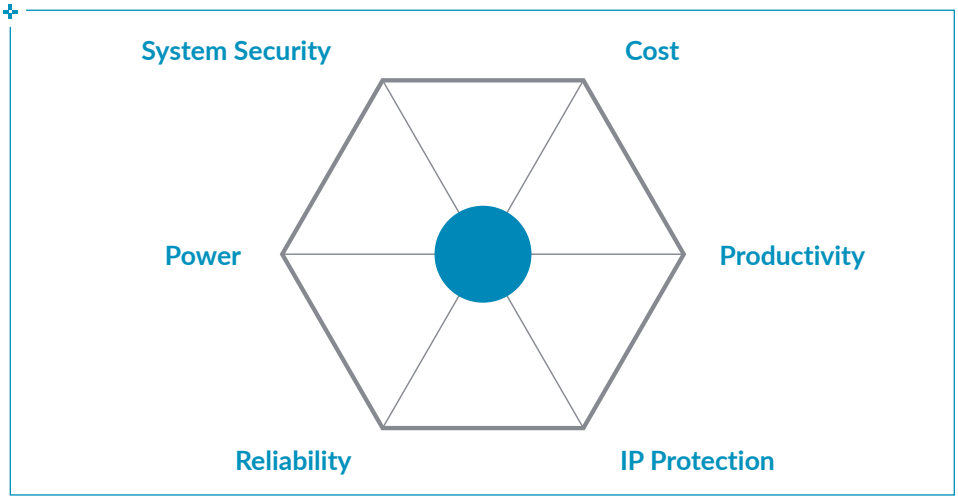
- The PMSAv8 Memory Protection Unit now uses TrustZone programmer's model
- The Data Watchpoint and Trace Unit with improved comparator programming and configuration
- The Breakpoint Unit has a different programmer's model and no flash patch capability
- The Embedded Trace Macro Cell upgraded from ETMv3.5 to ETMv4.2
- The Floating Point Unit upgraded from FPv4 to FPv5
- Additional processor's debug registers
- TPIU added ATB flush feature
- No bit-banding feature
- Extension to the EXC_RETURN codes
- VECTRESET in AIRCR (Application Interrupt Reset Control Reg) is removed
- Some ID registers have different values
- The stack-pointer can only be double word aligned
- A few additional instructions for Semaphores and atomics (load acquire, store release)
- The UNDEF and UNPREDICTABLE space is different
- By default exclusive access instructions utilize exclusive sideband signals only when the memory address is shareable
- Execution timing is different
- Addition of stack limit registers
- VTOR initial values are configurable for both Secure and Non-secure
- Auxiliary Fault Status Register removed
- VECTCLRACTIVE become RAZ/WI from software (debug access remains unchanged).
- Non-Base Thread Enable always enabled

When the TrustZone option is enabled in Cortex-M35P:

- New instructions such as TT and SG added to support TrustZone
- Each interrupt can be assigned to the Secure or Non-secure side
- A Security Attribution Unit is added for TrustZone configuration
- By default HardFault, BusFault and NMI will target Secure state
- System Reset Request can be configured to be inaccessible from Non-secure side
- Deep sleep can be configured to be inaccessible from Non-secure side

4. Summary

Benefits of the Cortex-M35P Processor



The complexity of embedded solutions is rising dramatically, but so is their value. Designers are faced with the task of finding the right balance between the opposing factors present in any system design. The amount of software included in an SoC is also rising dramatically, while project schedules are shrinking. In order to deliver the right product, at the right time, with the right performance and cost, we need to start with the proper foundation.

The Cortex-M35P processor was created to be the foundation of such designs. It builds upon previous processors and the existing Cortex-M ecosystem, reducing development cost. System power is also reduced due to a new design with multiple low-power technologies. TrustZone and the anti-tampering capabilities set the foundation to protect user applications and valuable IP for building secure solutions. The enhanced MPU and TrustZone combine to form the base for reliable and safe systems.

Finally, we get to the endless pursuit of better productivity. TrustZone is designed in a way that all existing users may continue to develop in the Non-secure zone just as before. Debug and trace are enhanced in Cortex-M35P to simplify working with complex code. All programming can be done in C language, as is the case for all Cortex-M processors, including all exception handlers. Existing code can be easily recompiled for Cortex-M35P after some configuration changes for control and MPU setup registers. Taken together, all these items add up to increase developer productivity in order to deliver more complex solutions to market in a shorter time period.

For more information on the Cortex-M35P or our physical security IP suite:

Explore the full range of security solutions from Arm
Get in touch with one of our technical experts
Learn more about our side-channel attack IP