Arm Cortex-M55 Processor Datasheet

February, 2020

Datasheet

Overview

The Arm Cortex-M55 processor is a fully synthesizable, mid-range, microcontroller-class processor that implements the Armv8.1-M mainline architecture and includes support for the M-profile Vector Extension (MVE), also known as Arm Helium technology. It's Arm's most AI-capable Cortex-M processor, delivering enhanced, energy-efficient digital signal processing (DSP) and machine learning (ML) performance. The Cortex-M55 processor achieves high compute performance across scalar and vector operations, while maintaining low energy consumption.

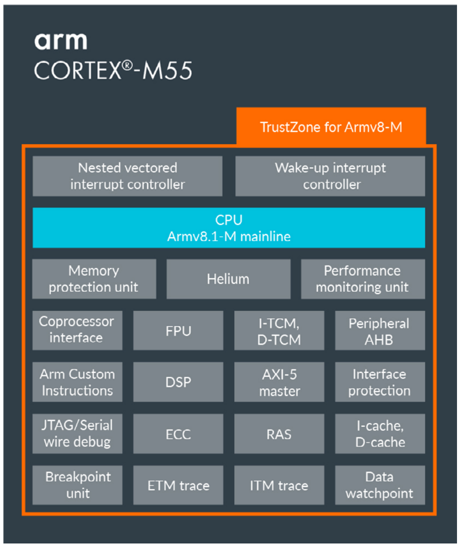

Figure 1:
Block diagram of the Cortex-M55 processor

Features

Feature	Description
Architecture	Armv8.1-M
Bus interface	AMBA 5 AXI5 64-bit master (compatible to AXI4 IPs)
Pipeline	4-stages (for main integer pipeline)
Security	Arm TrustZone technology (optional)
DSP Extension	32-bit DSP/SIMD Extension
MVE	Helium (optional)
Floating-point Unit	FPU (optional)
Coprcessor Interface	64-bit (optional)
Instruction cache	Up to 64KB with error correction code (ECC) (optional)
Data cache	Up to 64KB with ECC (optional)
Instruction TCM (ITCM)	Up to 16MB with ECC (optional)
Data TCM (DTCM)	Up to 16MB with ECC (optional)
Interrupts	Up to 480 interrupts + Non-maskable interrupt (NMI)
Wake-up Interrupt Controller (WIC)	Internal and/or external (optional)
Multiply-accumulate (MAC) / cycle	Up to: 2 x 32-bit MACs/cycle 4 x 16-bit MACs/cycle 8 x 8-bit MACs/cycle
Sleep modes	Multiple power domains, sleep modes (sleep and deep sleep), sleep-on-exit, optional retention support for memories and logic
Debug	Hardware and software breakpoints, Performance Monitoring Unit (PMU)

Trace	Optional Instruction trace with Embedded Trace Macrocell (ETM) Data Trace (DWT) (selective data trace, profiling and event trace) Instrumentation Trace (ITM) (software trace)
Arm Custom Instructions	Optional (available in 2021)

About the Processor

The Cortex-M55 processor is a fully synthesizable, mid-range processor that is designed for the microcontroller and deeply embedded systems market. The processor offers high compute performance across both scalar and vector operations with low energy consumption, fast interrupt handling, and enhanced system debug that includes extensive breakpoint and trace capabilities.

Interfaces supported by the processor include:

- Master AXI (M-AXI)
- Slave AHB (S-AHB) for TCM
- Peripheral AHB (P-AHB)
- External PPB (EPPB) APB
- Debug AHB (D-AHB)
- External Implementation Defined Attribution Unit (IDAU)
- ITM and ETM trace bus
- Coprocessor
- Cross Trigger Interface (CTI)
- Power control
- ITCM and DTCM

The processor has optional:

- Arm Helium technology
- Floating-point arithmetic functionality with support for scalar half, single, and double-precision floating-point operation
- Arm TrustZone technology, using the Armv8-M security extension supporting Secure and Non-secure states
- L1 instruction and data caches
- Memory Protection Units that you can configure to protect regions of memory
- Breakpoint Unit
- Data Watchpoint and Trace unit
- Instrumentation Trace Macrocell
- Performance Monitoring Unit
- Support for ETM trace
- Arm Custom Instructions (available in 2021)

Block Diagram

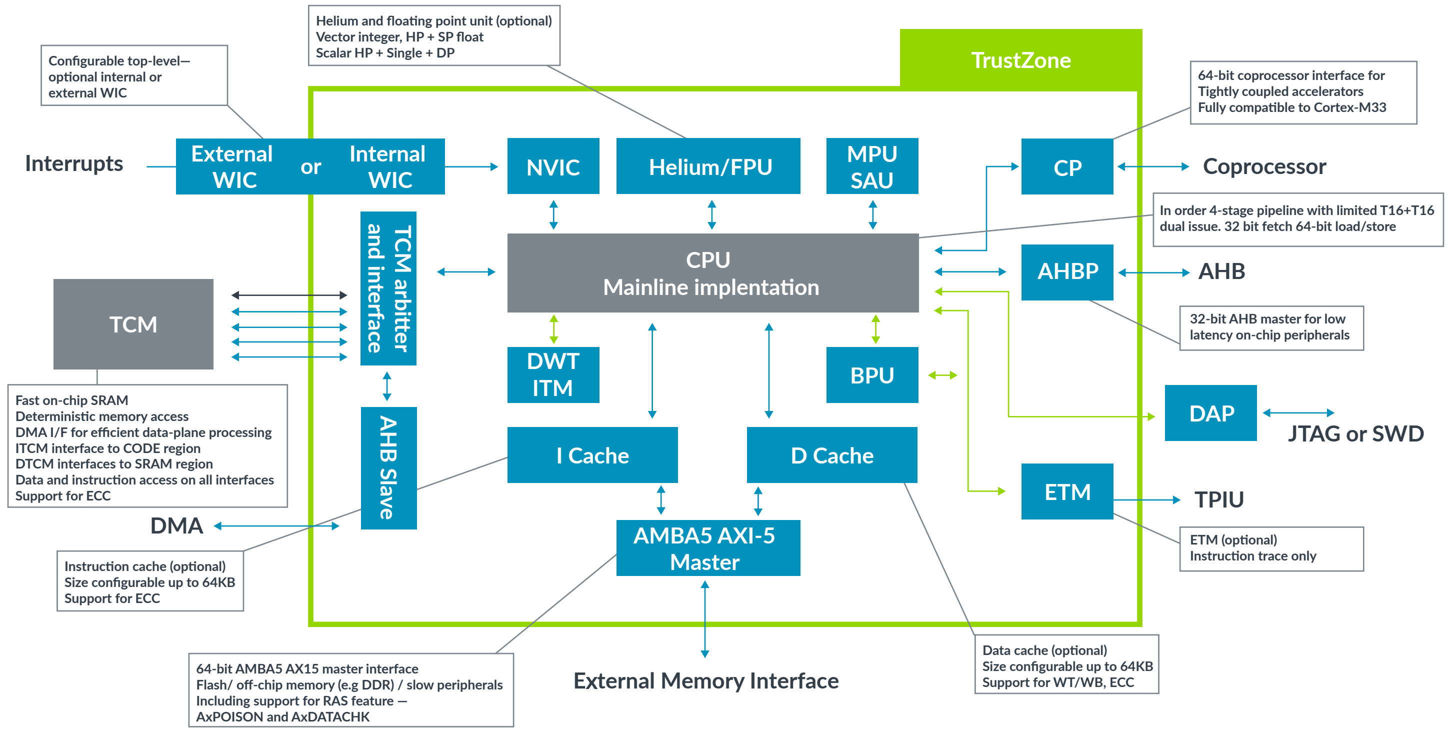

Figure 2: Cortex-M55 processor components

Cortex-M55 Components

Processor Overview

The Cortex-M55 processor is based on a 4-stage integer pipeline design, and when Helium vector extension is included, the vector engine increases the total pipeline stages to five. The pipeline is fully in-order (i.e. no out-of-order execution) and supports a small amount of dual-issue capability.

The instruction set supported in the Cortex-M55 processor is Armv8.1-M (with Mainline extension) and is available with optional Helium and floating-point instruction support. If Helium is not included, Armv8.1-M provides a number of new instructions not available in Armv8.0-M. For example, some of the low-overhead-branch instructions features are available across all configurations.

The Cortex-M55 processor supports the Arm TrustZone security extension. This makes the Cortex-M55 processor suitable for a range of IoT applications where security is essential to protect secret crypto keys, high-value algorithms and other trade secrets.

Helium

Helium, the vector processing extension adds over 150 new scalar and vector instructions, enabling the efficient compute of 8-bit, 16-bit and 32-bit fixed-point data. From instruction-set support, there are five combinations:

Config	FPU Data type: scalar float (fp16, fp32, fp64)	Helium Data type: vectored fixed-point (8-bit, 16-bit, 32-bit)	Helium Data type: vectored float-ing-point (fp16, fp32)
1	-	-	-
2	Included	-	-
3	-	Included	-
4	Included	Included	-
5	Included	Included	Included

These options allow SoC designers to customize the Cortex-M55 processor design to fit their specific application needs.

Floating-point

The Cortex-M55 FPU support is based on Arm FPv5 architecture which is fully IEEE-754 compliant. When the FPU is included, the Cortex-M55 processor supports scalar float-point instructions for data format of half-precision (16-bit, fp16), single-precision (32-bit, fp32), and double-precision (64-bit, fp64).

Memory Security Management

The Cortex-M55 processor contains several units that control access to the memory.

Memory Protection Unit

The MPU supports the Arm Protected Memory System Architecture (PMSA), which allows privileged software to define memory attributes (e.g. cache-ability) of different address ranges, and to define memory access permissions of unprivileged software components. For example, an RTOS can control the accessible memory ranges for each unprivileged threads at context switching, If an unprivileged thread accesses a memory location containing privileged data, or a memory location private to another unprivileged thread, an access violation fault exception is triggered so the RTOS can manage the situation. The architecture includes fault status registers to allow an exception handler to determine the source of the fault and to apply corrective action or notify the system. If TrustZone is implemented, the entire MPU logic can be split into Secure and Non-secure MPU regions.

Security Attribution Unit

When TrustZone is included, the Security Attribution Unit (SAU) defines and authenticates accesses to memory based on the security state of the core or the debugger.

This allows the memory space to be partitioned into Secure and Non-secure regions. The SAU in the Cortex-M55 processor supports up to eight regions, and also supports the addition of custom-defined attribution mapping using the Implementation Defined Attribution Unit (IDAU) interface to extend the number of security regions.

TCM Gate Unit

When the TrustZone security extension is included, the TCM Gate Unit (TGU) controls software and Slave AHB (S-AHB) accesses the TCMs based on the security attribute of the access. This allows the TCMs to be partitioned into Secure and Non-secure portions and to be compliant with requirements outlined in the Trusted Based System Architecture for M-profile (TBSA-M), which is a part of Platform Security Architecture (PSA).

Interface to Custom Defined Attribution Mapping (the IDAU interface)

DAUs are custom defined hardware unit that allows additional security regions to be defined in a TrustZone system and are present outside the processor. This unit defines memory regions as being either Secure, Non-secure, Non-secure Callable, or exempt from security checking. The final security mapping of memory regions is a combination of the response from the SAU and IDAU.

Memory System

The Cortex-M55 processor memory system provides the interface between the processor and the RAMs, external memory interfaces, and internal memory-mapped registers.

The memory system includes:

- A single interface to an ITCM and four interfaces to DTCMs, D0TCM, D1TCM, D2TCM, and D3TCM
- Master AXI (M-AXI) interface for high latency on-chip or off-chip memory and slow devices
- P-AHB for access to external peripherals
- S-AHB for system access to the TCMs
- L1 instruction cache
- L1 data cache
- EPPB APB interface for CoreSight debug and trace components
- A Store Buffer (STB) to hold store operations when they have left the load/store pipeline and the DPU has committed them. From the STB, a store can do either of the following:
    - Request access to the cache RAM through the Data Cache Unit (DCU)
    - Request the Bus Interface Unit (BIU) to initiate line fills
    - Request the BIU to write data on the AXI5 master interface

If several store transactions are associated with the same 64-bit aligned doubleword, the STB can merge these store transactions into a single transaction.

Nested Vectored Interrupt Controller

The Cortex-M55 processor NVIC is closely integrated with the processor to achieve low-latency interrupt processing.

The NVIC is responsible for:

- Maintaining the current execution priority of the Cortex-M55 processor
- Maintaining the pending and active status of all exceptions that are supported
- Invoking pre-emption when a pending exception has priority
- Providing wake up signals to wake up the Cortex-M55 processor from deep sleep mode
- Providing support to the Internal Wake-up Interrupt Controller (IWIC) and External Wake-up Interrupt Controller (EWIC)
- Providing priority and exception information to other processor components

The NVIC in the Cortex-M55 processor allows up 480 external interrupts, an NMI and several built-in system exceptions.

Wake-up Interrupt Controller

The Cortex-M55 processor supports a WIC unit that allows the Cortex-M55 processor to enter a low-power state.

Two WICs are supported:

- IWIC - synchronous with the processor and contained within the Cortex-M55 processor boundary,
- EWIC – a system-level component that can be asynchronous to the Cortex-M55 processor

The Cortex-M55 processor supports either no WIC, IWIC, EWIC, or both IWIC and EWIC

Coprocessor Interface

The Cortex-M55 processor supports an optional coprocessor interface which allows the integration of tightly coupled accelerator hardware with the processor. The programmer model allows the software to communicate with the hardware using architectural coprocessor instructions.

The external coprocessor interface supports up to eight separate coprocessors, CP0-CP7, depending on the implementation. The remaining coprocessor numbers, C8-C15, are reserved. CP10 and CP11 are always reserved for hardware floating-point. For more information, see the Armv8-M Architecture Reference Manual. Supports low-latency data transfer from the processor to and from the accelerator components.

Debug and trace components

The Cortex-M55 processor has optional and configurable debug and trace components.

Breakpoint Unit

A configurable BPU for implementing breakpoints.

Data Watchpoint and Trace

A configurable DWT unit for implementing watchpoints, data tracing and system profiling.

Instrumentation Trace Macrocell

An optional ITM that supports printf() style debugging using instrumentation trace.

Performance Monitoring Unit

A PMU which enables software to gather statistics on events taking place on the Cortex-M55 processor. These statistics can be used for performance analysis and system debug. The PMU is always present when the DWT is present.

ROM Tables

ROM tables allow debuggers to determine which CoreSight components are implemented in the Cortex-M55 processor.

Debug and Trace Interfaces

These interfaces are suitable for:

- Passing on-chip data through a Trace Port Interface Unit (TPIU) to a Trace Port Analyzer (TPA), including Serial Wire Output (SWO) mode
- Integrating a Debug Access Port (DAP), which is a debug port that is used to control debug functionality
- Integrating a CoreSight Embedded Trace Buffer (ETB), which is an optional licensable component for trace data to be written to an external SRAM

Cross Trigger Interface

The optional Cross Trigger Interface (CTI) enables the debug logic and ETM to interact with each other and with other CoreSight components.

PMC-100

PMC-100 is an optional on-line MBIST controller that is used to test RAMs, ECC logic, and any other associated logic.

SBIST Controller

The SBIST controller is an optional component that is used to facilitate the testing of functional logic (excluding memories).

Cortex-M55 Interfaces

Name	Protocol	Width	Details
Master AXI	AMBA 5 AXI master interface	64-bit	Provides efficient access to high-latency memory and peripheral components in the system.
Instruction Tightly Coupled Memory and Data Tightly Coupled Memory	-	32-bit	One ITCM interface and four DTCM interfaces to support efficient and high-bandwidth access from the Cortex-M55 processor and Slave AHB (S-AHB) interface to local low-latency memory. The ITCM is mapped to the code memory region and the DTCMs are mapped to the SRAM memory region. Access to ITCM is through the 32-bit wide ITCM interface. Access to DTCM is through the 32-bit wide D0TCM, D1TCM, D2TCM, and D3TCM interfaces. The size of both TCM instances is configurable, and in the range of 4KB-16MB in powers of 2. The Cortex-M55 processor also supports zero size TCMs.
AHB slave port	AMBA 5 AHB	64-bit	Provides system access to the TCMs. The DMA engine typically uses this interface.
Tightly coupled master Peripheral AHB interface	AMBA 5 AHB	32-bit	Provides efficient access to system peripherals.
External Private Peripheral Bus interface	AMBA 4 APB	32-bit	Used to connect to external CoreSight-compliant peripherals
External IDAU interface	-	-	Allows the system to define security attributes
ITM and ETM interfaces	AMBA 4 ATB	8-bit	Provides tracing capability
Coprocessor interface	-	64-bit	Used for closely coupled external accelerator hardware
Debug AHB slave interface	AMBA 5 AHB	32-bit	Provides debug access to registers, memory, and peripherals
Optional Cross Trigger Interface interface	-	Four channels	Used for debug and trace synchronization
Power control interface	Low-power P-Channel and Q-Channel	-	Optional support for internal power domains which can be enabled and disabled using the P-Channel and Q-Channel interfaces connected to a power controller in the system
External Wake-up Interrupt Controller interface	-	-	Provides access to an optional EWIC, which is peripheral to the system and is suitable for sleep states where the entire processor subsystem is powered down

Cortex-M55 Supporting IP

Arm Ethos-U55 microNPU

The Ethos-U55 is the industry's first microNPU designed for microcontroller-class devices. It is integrated with a single Cortex-M toolchain to provide exceptional performance uplift without additional software complexity. Combine the Cortex-M55 processor with the Ethos-U55 to deliver up to 480x uplift in ML performance over previous generation Cortex-M processors.

Arm Corstone-300 Reference Design

The Arm Corstone-300 is the ultimate starting point for integrating the Cortex-M55 and the Ethos-U55 (optional) processors into an SoC with the lowest risk and development cost. It includes various system IP components and a reference design integrating the processor, security and system IP, as well as a range of software and development tools.

The Corstone-300 simplifies security implementation with an optimized AXI5 system for Arm TrustZone technology, and easier porting to Trusted Firmware-M, accelerating the route to PSA Certified silicon and devices.

- Implementation of an Arm-defined system architecture
- Integration of the main components
- Extensively verified
- Broad software roadmap
- Build your SoC on top of it
- Configurable and modifiable
- Tailor it to specific needs
- Accelerates PSA Certified
- Silicon-proven

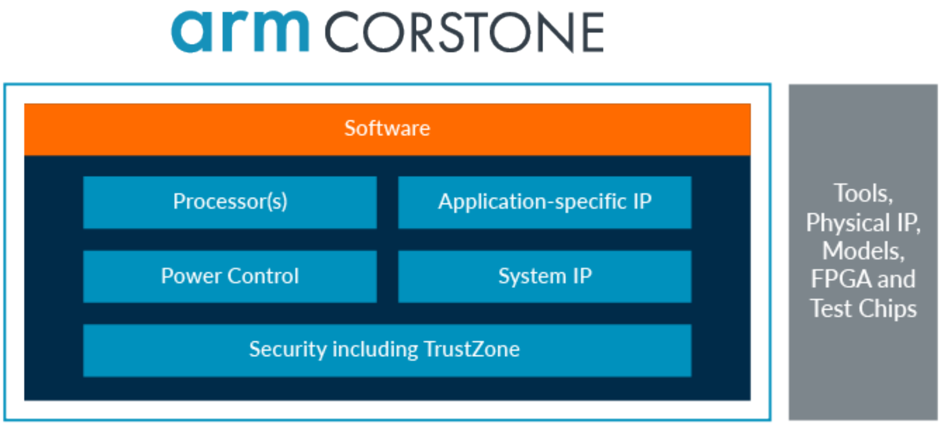

Figure 3: Corstone reference design diagram

Processor Configuration Options

The Cortex-M55 processor has configurable options that can be set during the implementation and integration stages to match functional requirements

Feature	Options
Floating-point	Floating-point
	Floating-point included
MVE when floating-point is not included	Helium included
	Integer subset of Helium included
MVE when floating-point is included	Helium not included
	Integer subset of Helium included
	Integer, half-precision and single-precision Helium included

TrustZone	No TrustZone for Armv8-M security extension
	TrustZone for Armv8-M security extension
Coprocessor	No support for coprocessor hardware
	Support for coprocessor hardware
Secure MPU	0 region, 4 regions, 8 regions, 12 regions, or 16 regions when TrustZone is included
SAU	0 region, 4 regions, or 8 regions when TrustZone is included
Instruction cache	No ICU
	ICU included and size can be 4KB, 8KB, 16KB, 32KB, or 64KB
Data cache	Area optimized M-AXI interface, no DCU
	DCU included and size can be 4KB, 8KB, 16KB, 32KB, or 64KB
Error correcting code	No ECC on cache or TCMs
	ECC on all implemented caches and TCMs
Interrupts	1-480 interrupts + NMI
Exception priority bits	3-8 priority bits
Lowest interrupt latency interrupt numbers	Lowest latency One additional latency cycle
Debug resources	Minimal debug
	Reduced set
	Full set
Instrumentation Trace Macrocell and Data Watchpoint Trace	No ITM and DWT trace
	Complete ITM and DWT trace
Embedded Trace Macrocell	No ETM support
	ETM support
Cross Trigger Interface	No CTI
	CTI included
Internal Wake-up Interrupt Controller	No IWIC
	IWIC included
Interface protection	No interface protection
	Interface protection included
ICTM security gating	No ICTM security gate
	ICTM security gate included
PMC100	No Programmable MBIST Controller
	(PMC-100)
	PMC-100 included
Number of PMC-100 program registers	2-32
Reset all registers functionality	Only reset states that architecture requires
	Reset all synchronous states

Supporting technical documents coming soon. Learn more about the Cortex-M55 processor here.

Glossary of Terms

BIU	Bus Interface Unit
BPU	Breakpoint Unit
CTI	Cross Trigger Interface
D-AHB	Debug AHB
DAP	Debug Access Port
DCU	Data Cache Unit
DMA	Direct Memory Access
DP	Double-precision
DPU	Data Processing Unit
DSP	Digital Signal Processing
DTCM	Data Tightly Coupled Memory
DWT	Data Watchpoint and Trace
ECC	Error Correcting Code
EPPB	External Private Peripheral Bus
ETB	Embedded Trace Buffer
ETM	Embedded Trace Macrocell
EWIC	External Wakeup Interrupt Controller
FPU	Floating Point Unit
HP	Half-precision
ICU	Instruction Cache Unit
IDAU	Implementation Defined Attribution Unit
IEEE	Institute of Electrical and Electronics Engineers
IT	Instruction Trace
ITCM	Instruction Tightly Coupled Memory
ITM	Instrumentation Trace Macrocell
IWIC	Internal Wakeup Interrupt Controller
JTAG	Joint Test Action Group
M-AXI	Master AXI
MAC	Multiply-accumulate Cycle
MBIST	Memory Built-in Self-Test
ML	Machine Learning
MPU	Memory Protection Unit
MVE	M-Profile Vector Extension
NMI	Non-maskable Interrupt
NPU	Neural Processing Unit
NVIC	Nested Vectored Interrupt Controller
P-AHB	Peripheral AHB
PMSA	Protected Memory System Architecture
PMU	Performance Monitoring Unit
PSA	Platform Security Architecture
RAS	Reliability, Availability and Serviceability
ROM	Read-only Memory
S-AHB	Slave AHB
SAU	Security Attribution Unit
SBIST	Software Built-In Self-Test

SIMD	Single Instruction, Multiple Data
SP	Single-precision
SRAM	Static Random Access Memory
STB	Store Buffer
SWO	Serial Wire Output
TBSA-M	Trusted Based System Architecture for M-Profile
TCM	Tightly Coupled Memory
TGU	TCM Gate Unit
TPA	Trace Port Analyzer
TPIU	Trace Port Interface Unit
WB/WT	Write-back and Write-through
WIC	Wake-up Interrupt Controller

Contact details

UK
Salesinfo-eu@Arm.com

USA
Salesinfo-us@Arm.com

Europe
Salesinfo-eu@Arm.com

Asia Pacific
Salesinfo-us@Arm.com

Japan
Salesinfo-eu@Arm.com

Korea
Salesinfo-us@Arm.com

Taiwan
Salesinfo-eu@Arm.com

Israel
Salesinfo-us@Arm.com

China
Salesinfo-eu@Arm.com

India
Salesinfo-us@Arm.com