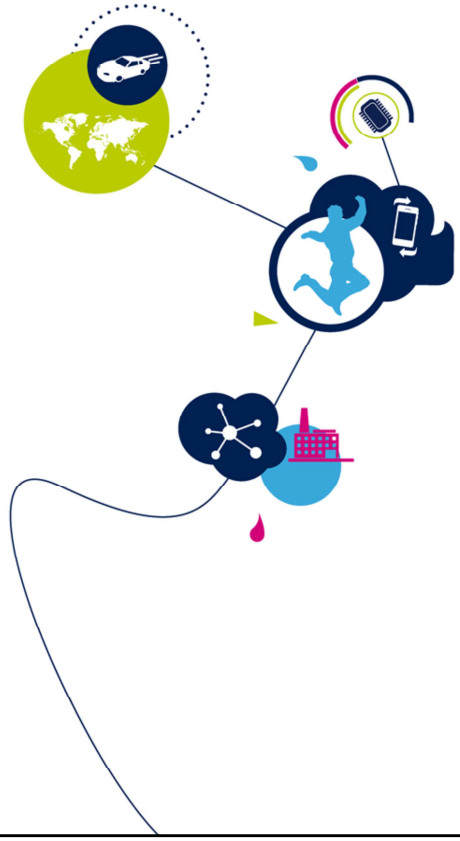
STM32L5- Arm® Core

Arm Cortex®-M33 Core

Revision 1.0

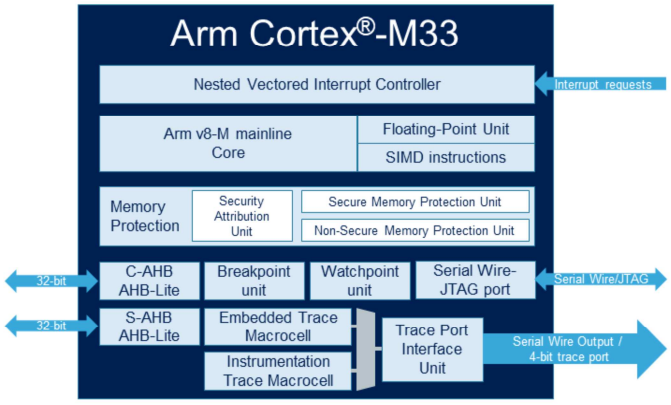


life.augmented

Hello, and welcome to this presentation of the Arm® Cortex®-M33 core which is embedded in all products of the STM32L5 microcontroller family.

Cortex®-M33 processor overview

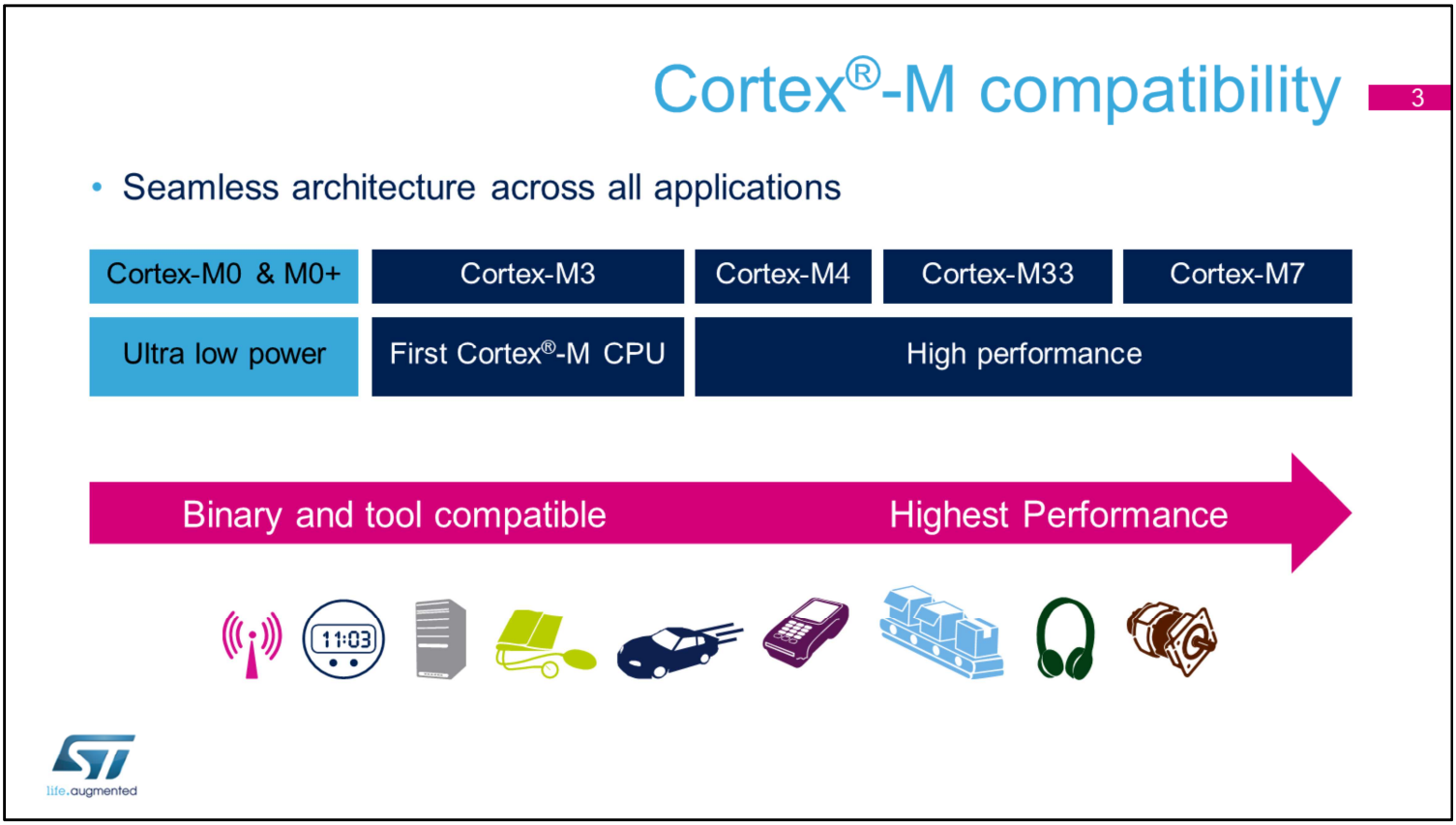
- Armv8-M architecture
- Harvard architecture, 3-stage pipeline
  - Floating-Point Unit
  - Single Instruction Multiple Data Instructions
- Memory Protection
  - Security Attribution Unit (SAU)
  - 2x Memory Protection Units (MPUs)
- Integrated Nested Vectored Interrupt Controller (NVIC)
- Invasive and non-invasive debug



Energy efficient	Software productivity	System security
Most energy efficient 32-bit embedded processor for MCU+DSP requirements	SIMD instructions accelerate data signal processing	TrustZone® for Armv8-M

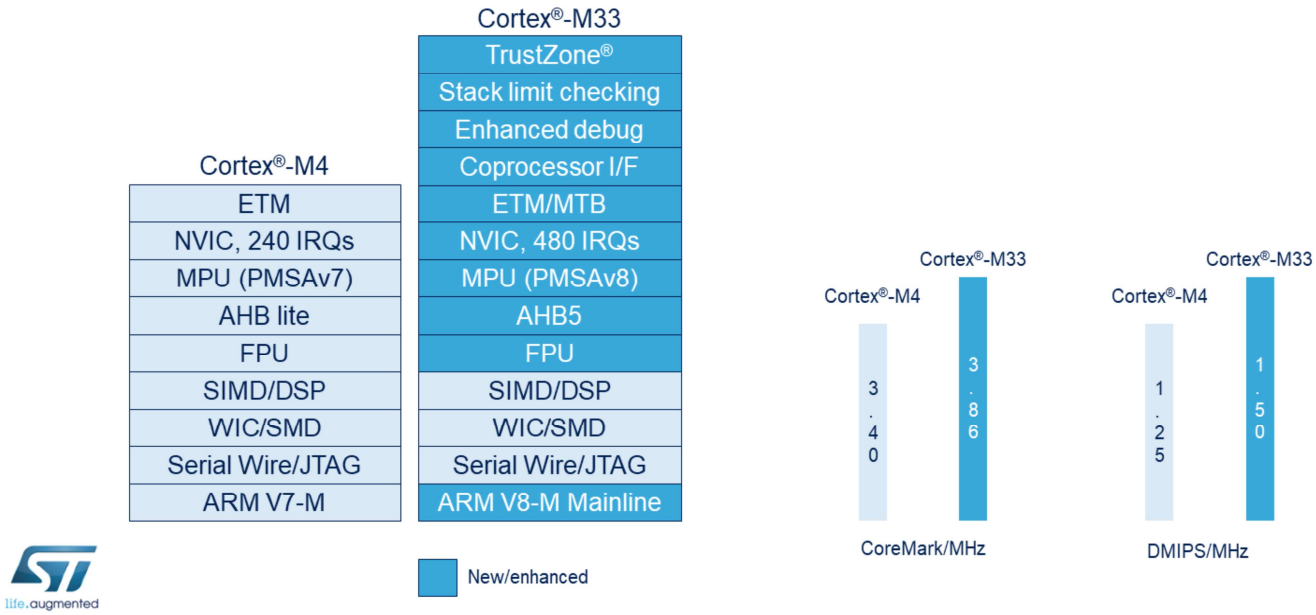
The Cortex®-M33 core is part of the Arm Cortex®-M group of 32-bit RISC cores. It implements the Armv8-M mainline architecture and features a 3-stage pipeline. In addition to scalar integer instructions, it also supports a single precision floating-point unit and SIMD integer instructions, used to improve the performance of DSP algorithms.
The processor implements ARM TrustZone® technology, using the ARMv8-M Security Extension supporting Secure and Nonsecure states.
The Cortex®-M33 has two AHB5 master ports, enabling concurrent instruction and data transactions.
Interrupts received from STM32L5 peripherals are handled by the Nested Vectored Interrupt Controller (or NVIC).
The Memory Protection is in charge of assigning security and privilege attributes as well as access permissions to instruction and data requests initiated by the core.
It is based on a Security Attribution Unit and two Memory Protection Units, one per security level.

Several debug units are implemented.
Two protocols can be used to communicate between the Serial Wire or the debug port (SWJ-DP) and the external debug probe: either serial wire or JTAG.
Invasive debug is performed by means of the breakpoint and watchpoint units.
For non-invasive debug, the Cortex®-M33 supports two real time trace capabilities: the Embedded Trace Macrocell (or ETM) and the Instrumentation Trace Macrocell (or ITM).
Trace packets are output to the external Trace Port Analyzer through the Trace Port Interface Unit (or TPIU).



STM32L5 microcontrollers integrate an Arm® Cortex®-M33 core in order to benefit from the powerful performance of its 32-bit processor architecture and particularly high level of deterministic processing.
All Cortex®-M CPUs have a 32-bit architecture.
The Cortex®-M3 was the first Cortex®-M CPU released by Arm.
Then Arm decided to distinguish two product lines: high performance and low power, while maintaining the compatibility between them.
The Cortex®-M33 belongs to the high performance product line.
The Cortex®-M33 processor is a low gate count, highly energy efficient processor that is intended for microcontroller and deeply embedded applications.
The processor is based on the ARMv8-M architecture and is primarily for use in environments where security is an important consideration.

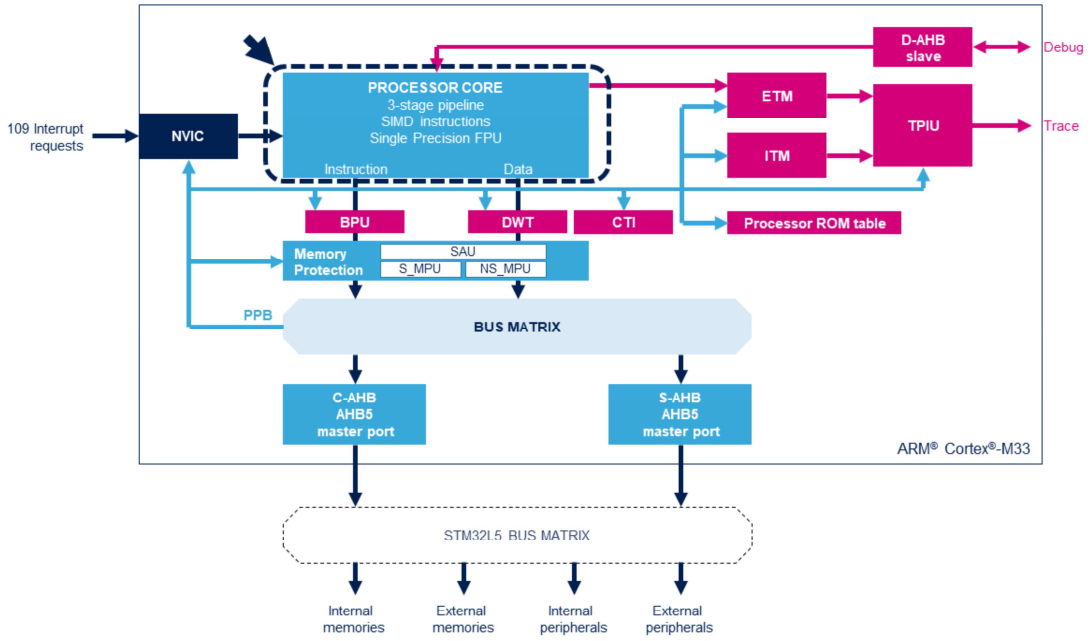
Cortex®-M33 enhancements vs Cortex®-M4



This slide highlights the differences between ARM Cortex-M4 and Cortex-M33.
The V8-M mainline is a superset of the V7-M architecture.
TrustZone is a new feature enabling the core to switch between two security states: secure and non-secure.
The AHB buses used to communicate with the STM32L5 bus matrix are compatible with the AHB5 specification, which supports the secure attribute.
TrustZone is by default disabled in the STM32L5 and in this case, the Cortex-M33 offers the same kind of features as the Cortex-M4, some of them being enhanced.
An interesting new capability is runtime stack overflow checking, which is achieved by programming stack limit registers.
Note that the PMSAv8 MPU present in the Cortex-M33 is not compatible with the PMSAv7 MPU present in the Cortex-M4.
In terms of performance, the Cortex-M33 is better than the Cortex-M4 as indicated by the results of CoreMark and

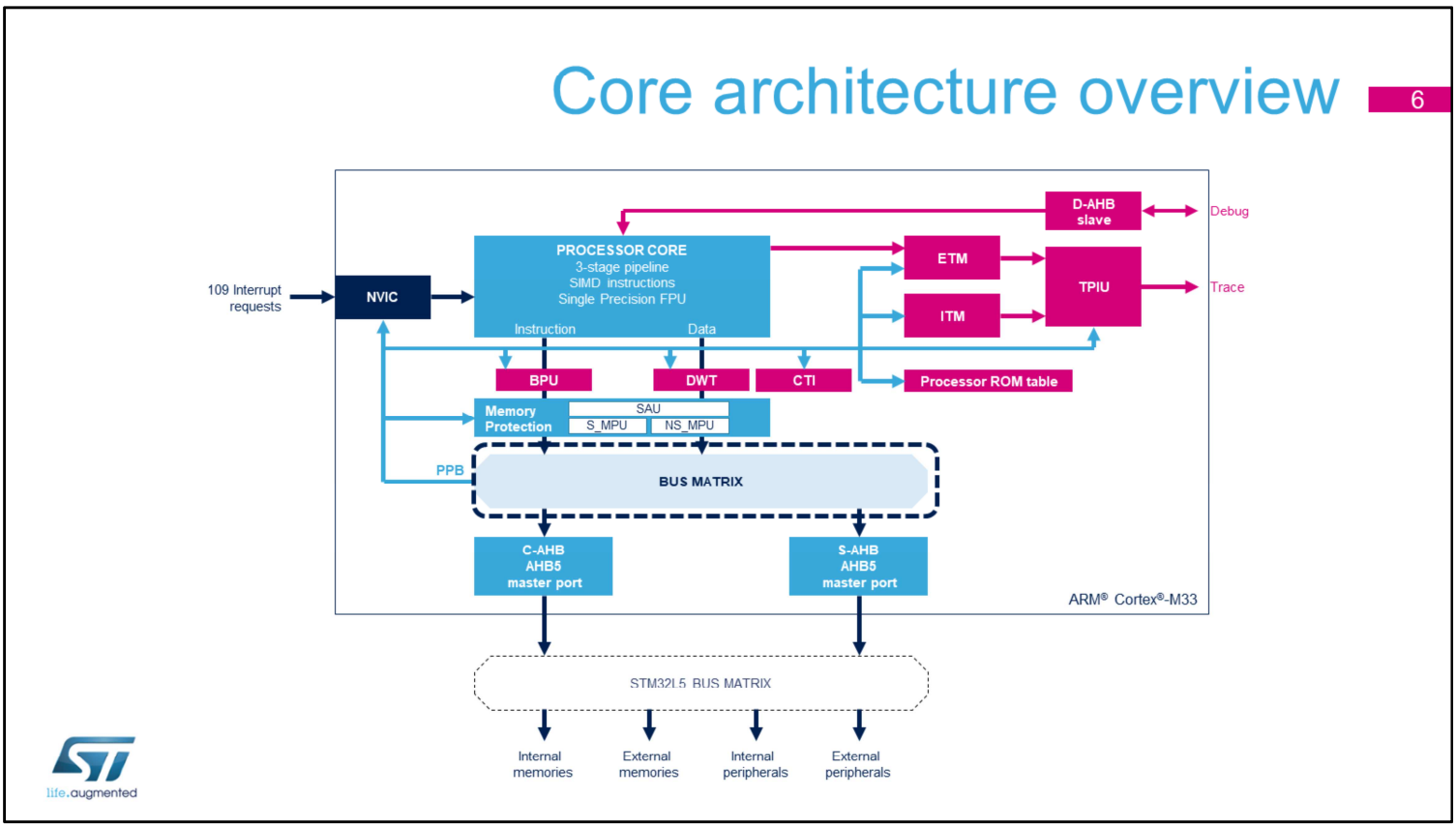
DMIPS benchmarks.

Core architecture overview



life.augmented

The processor core implements a Harvard architecture, supporting concurrent instruction fetch and data load/store transactions.
The instruction pipeline features three stages: a fetch stage, a decode and simple execute stage, and a complex execute stage.
Most arithmetic operations only take two clock cycles to execute.



The Cortex®-M33 has neither a cache nor internal RAM. Consequently any instruction fetch transaction and data access is steered to the internal bus matrix. This bus matrix selects the output AHB5 master port according to the address. Two AHB transactions can be in progress at the same time, for instance:

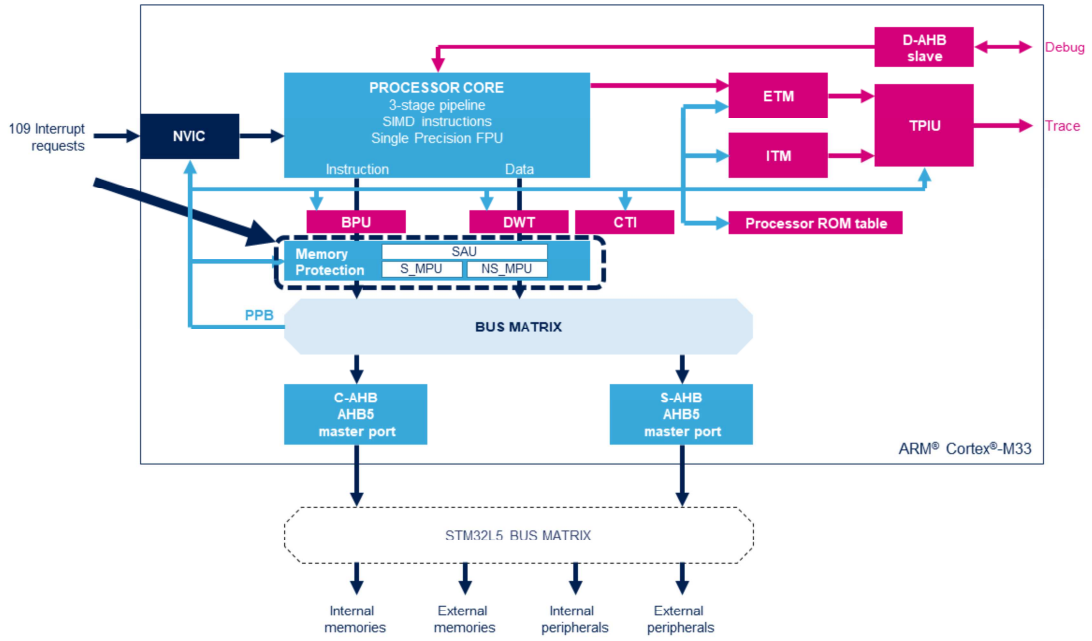
- An instruction access from flash memory using the C-AHB master port
- An SRAM access using the S-AHB master port.

The Cortex®-M33's bus matrix is connected to the STM32L5 MCU's AHB5 multi-layer bus matrix, enabling the CPU to access memories and peripherals. Since transactions are pipelined on AHB-Lite, the best throughput is 32 bits of data or instructions per clock cycle, with a minimum 2-clock cycle latency.

One of the outputs of the Cortex®-M33's bus matrix is the Private Peripheral Bus (or PPB), which is internal to the CPU. It is used to access memory-mapped registers present

in the NVIC, SAU, MPU and debug units.

Core architecture overview



life.augmented

Security attribution and memory protection in the processor is provided by the Security Attribution Unit (SAU) and the optional Memory Protection Units (MPUs).
The SAU is a programmable unit that determines the security of an address.
The MPU is banked between Secure and Non-secure states.

Memory Protection Unit/ Security Attribution Unit

- MPU attribute settings define access permissions
  - 8 secure MPU regions
  - 8 non-secure MPU regions
- 8 independent SAU regions
  - At reset, the SAU is disabled and all the memory is Secure
  - It is possible to define up to 8 non-secure memory regions, 1 SAU region per memory region
  - Any access outside the regions programmed in the SAU is marked as Secure.

life.augmented

In the STM32L5, the SAU supports eight regions.
Each region is defined by an address range and secure attribute: either non-secure or secure non-secure callable.
Any access that falls outside the programmed regions is marked as secure.
For instructions, the attribute determines the allowable Security state of the processor when the instruction is executed.
It can also identify whether code at a Secure address can be called from Nonsecure state.
For data, the attribute determines whether a memory address can be accessed from Non-secure state, and also whether the external memory request is marked as Secure or Non-secure.
If a data access is made from Non-secure state to an address marked as Secure, then a Security Fault exception is taken by the processor.
If a data access is made from Secure state to an address

marked as Non-secure, then the associated memory access is marked as Non-secure.

References

- For more details, please refer to the following documentation:
  - STM32L5 Series Cortex®-M33 processor programming manual
  - Arm website at the following link:
    - http://www.arm.com/products/processors/cortex-m/cortex-M33-processor.php

life.augmented

The NVIC and debug units are described in separate presentations.
For more details, please refer to these application notes and the Cortex®-M33 programming manual available on the www.st.com website.
Also visit the Arm website where you will find more information about the Cortex®-M33 core.