STM32L5 MCU series excellence in ultra-low-power with more security
Main concerns for embedded design

- **Security**
  - Increase the robustness against attacks

- **Low power consumption**
  - Long life time, small battery size

- **Integration, performance, ecosystem**
  - Best fit versus the application requirements
First STM32 based on Cortex-M33

STM32L5 is the answer

- More security with TrustZone and ST security implementation
  - HW to increase resistance to logical and board level attack
- Lower Power consumption
  - STM32 ultra-low-power technology
- Integration, performance, ecosystem
  - More performance, choice of packages and wide ecosystem
Security: TrustZone for isolation

ST implementation provides a high granularity of isolation

- Each GPIO or peripheral, DMA channel, clock configuration register, ART or small part of Flash memory or SRAM can be configured as **Trusted** or **un-Trusted**

- **Full isolation** of trusted and non-trusted worlds
Security: TrustZone for isolation

TrustZone provides full isolation

Example of IoT application implementation

STM32L5

Un-Trusted

Un-Trusted Application

Trusted

Trusted Application

RF

Sensors
Security: TrustZone and privileged zones

- More partitioning
- Possibility to separate the trusted and un-trusted area with **privileged and un-privileged** zone
- Strong **granularity** to define each part of memory or each peripheral, DMA channel as privileged or un-privileged

<table>
<thead>
<tr>
<th>Privileged &amp; Privileged</th>
<th>Trusted &amp; Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Un-Privileged &amp; Un-Privileged</td>
<td>Trusted &amp; Un-Privileged</td>
</tr>
</tbody>
</table>
TrustZone: example

STM32L5

Un-Trusted & Un-Privileged

Un-Trusted

RTC

Trusted

& Privileged

Secured Keys

Secured Boot

Trusted & Privileged

RF Stack

Secured data

Sensor IP

RF

Sensors
A full set of security

Encryption
- AES-128/256 Encryption
- SHA-256 Authentication
- Public Key Acceleration (PKA): for RSA, Diffie-Hellmann or ECC (Elliptic Curve Cryptography)
- Certified Crypto library
- True Random Number Generator
- Unique ID
- OTP Zone

Decryption

Authentication

STM32L5

Memory & IP Protection
- Active and static Anti-tamper detection
- Memory Protection Unit (MPU)
- Secure Boot
- Read and Write Protection
- HDP (Hide Protect)
- Unique Boot Entry
- OTFDEC (On-the-fly decryption) on Octo SPI to protect external memory
- JTAG fuse
- TrustZone
- SFI (Secure Firmware Installation)
• STM32L5 reuses the STM32L4/L4+ technology achieving **best-in-class** power consumption

• STM32L5 integrates an optional **SMPS** (DC/DC buck voltage regulator) which can be enabled/disabled on the fly to avoid external noise for external RF or data acquisition.

• Proven by EEMBC test results:
  - **ULPBENCH** 370 ULPMark-CP
  - **ULPBENCH** 54 ULPMark-PP
## Ultra-low-power modes

### Best power consumption numbers with full flexibility

<table>
<thead>
<tr>
<th>Wake-up time</th>
<th>$V_{BAT}$</th>
<th>Tamper detection: 3 I/Os, RTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>250 µs</td>
<td>3 nA / 187 nA*</td>
<td></td>
</tr>
<tr>
<td>14 µs</td>
<td>17 nA / 122 nA*</td>
<td></td>
</tr>
<tr>
<td>14 µs</td>
<td>108 nA / 222 nA*</td>
<td></td>
</tr>
<tr>
<td>14 µs</td>
<td>272 nA / 386 nA*</td>
<td></td>
</tr>
<tr>
<td>5 µs</td>
<td>3.0 µA / 3.1 µA*</td>
<td></td>
</tr>
<tr>
<td>6 cycles</td>
<td>26 µA / MHz</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Down to 62 µA / MHz</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** * without RTC / with RTC

- **Shutdown:** Wake-up sources: reset pin, 5 I/Os, RTC
- **Standby:** Wake-up sources: + BOR, IWDG
- **Standby + 4-Kbyte RAM:** Wake-up sources: + all I/Os, PVD, COMPs, I^2^C, LPUART, LPTIM
- **Stop 2 (full retention: 256-Kbyte RAM):** Wake-up sources: any interrupt or event

**V_{BAT}** represents the voltage at which the device operates.
More performance

Better responsiveness of the application

• **New** Arm® Cortex®-M33 performance: +20% versus Cortex-M4
  - 1.5 DMIPS/MHz
  - 4.02 CoreMark/MHz
  - 165 DMIPS
  - 442 CoreMark

• **New** ST ART Accelerator™: working both on internal and external Flash
  - 8 Kbytes of instruction cache
**High integration and innovation**

**Large memory, USB Type-C™ w/ power delivery controller, CAN FD**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parallel interface</td>
<td>FSMC 8-/16-bit (TFT-LCD, SRAM, NOR, NAND)</td>
</tr>
<tr>
<td>Digital</td>
<td>2x SAI, DFSDM (4 channels)</td>
</tr>
<tr>
<td>Timers</td>
<td>14 timers including: 2x 16-bit advanced motor control timers</td>
</tr>
<tr>
<td></td>
<td>2x LPUART timers</td>
</tr>
<tr>
<td></td>
<td>3x 16-bit-timers</td>
</tr>
<tr>
<td></td>
<td>2x 32-bit timers</td>
</tr>
<tr>
<td>I/Os</td>
<td>Up to 115 I/Os</td>
</tr>
<tr>
<td></td>
<td>Touch-sensing controller</td>
</tr>
<tr>
<td>Arm® Cortex®-M33 CPU</td>
<td>110 MHz</td>
</tr>
<tr>
<td></td>
<td>TrustZone®</td>
</tr>
<tr>
<td></td>
<td>FPU</td>
</tr>
<tr>
<td></td>
<td>MPU</td>
</tr>
<tr>
<td></td>
<td>ETM</td>
</tr>
<tr>
<td>DMA</td>
<td></td>
</tr>
<tr>
<td>ART Accelerator™</td>
<td></td>
</tr>
<tr>
<td>Connectivty</td>
<td>USB Device Crystal-less, USB Type-C and PD,</td>
</tr>
<tr>
<td></td>
<td>1x SD/SDIO/MMC, 3x SPI,</td>
</tr>
<tr>
<td></td>
<td>4x PC, 1x CAN FD,</td>
</tr>
<tr>
<td></td>
<td>1x Octo-SPI,</td>
</tr>
<tr>
<td></td>
<td>5x USART + 1x LPUART</td>
</tr>
<tr>
<td>Encryption</td>
<td>AES (256-bit), PKA, SHA-1, SHA-256,TRNG, CRC, OTFDEC</td>
</tr>
<tr>
<td>Analog</td>
<td>2x 12-bit ADC 12/16 bits</td>
</tr>
<tr>
<td></td>
<td>5 MSPS, 2x DAC,</td>
</tr>
<tr>
<td></td>
<td>2x comparators,</td>
</tr>
<tr>
<td></td>
<td>2x op amps</td>
</tr>
<tr>
<td></td>
<td>1x temperature sensor</td>
</tr>
</tbody>
</table>
Large portfolio

7 packages, several options

Flash memory size / RAM size (bytes)

512 K / 256 K
- STM32L562CE
- STM32L562RE
- STM32L562ME
- STM32L562VE
- STM32L562QE
- STM32L562ZE

256 K / 256 K
- STM32L552CC
- STM32L552RC
- STM32L552VC
- STM32L552QC
- STM32L552ZE

Legend:
- without HW crypto
- with HW crypto

Pin count
- 48-pin LQFP/QFN
- 64-pin LQFP
- 81-pin WLCSP
- 100-pin LQFP
- 132-pin UFBGA (0.5 mm pitch)
- 144-pin LQFP
STM32L ULP portfolio

STM32L5 completes the ultra-low-power subclass

**Cost-smart ULP champion**

STM32L0

Cortex-M0+ at 32 MHz
1.65 to 3.6V
8-/16-bit applications
Wide range of pin-counts

3 product lines,
Cost-effective,
Smaller packages,
USB, LCD, Analog
8 to 192 Kbytes of Flash,
Up to 20 Kbytes of SRAM

**Broad-range foundation**

STM32L1

Cortex-M3 at 32 MHz
1.65 to 3.6V
Wide choice of memory sizes

3 product lines,
USB, LCD, AES,
Rich Analog
True EEPROM,
Dual-bank Flash memory (RWW),
32 to 512 Kbytes of Flash,
Up to 80 Kbytes of SRAM

**ULP With performance**

STM32L4

Cortex-M4 w/ FPU at 80 MHz
1.71 to 3.6V
High-performance, advanced analog circuits

5 product lines,
5-MSPS ADC,
PGA, Compar.,
DAC, Op Amp, USB
OTG, LCD, AES
64 Kbytes to 1 Mbyte
Up to 320 Kbytes of SRAM

**ULP with more performance**

STM32L4+

Cortex-M4 w/ FPU at 120 MHz
1.71 to 3.6V
Wide choice of memory sizes

3 product lines,
5-MSPS ADC,
PGA, Compar.,
DAC, Op Amp, USB
OTG, LCD, AES
1 to 2 Mbytes of Flash,
Up to 640 Kbytes of SRAM

**Advanced security**

STM32L5

Cortex-M33 w/ FPU at 110 MHz
1.71 to 3.6V
Wide choice of memory sizes

1 product line,
5-MSPS ADC,
PGA, Compar.,
DAC, Op Amp,
USB Type C, AES
256 to 512 Kbytes of Flash,
Up to 256 Kbytes of SRAM
A Complete Ecosystem
### STM32CubeL5

**One-stop-shop software package**

#### STM32Cube MCUs Packages

<table>
<thead>
<tr>
<th>STM32Cube MCU Packages</th>
<th>STM32Cube MCU Middleware</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>freeRTOS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>USB</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FatFS file system</strong></td>
<td></td>
</tr>
<tr>
<td><strong>mbedTLS and mbedCrypto</strong></td>
<td></td>
</tr>
<tr>
<td><strong>USB Device stacks</strong></td>
<td></td>
</tr>
</tbody>
</table>

#### STM32Cube HAL & LL drivers

#### STM32Cube Middleware

<table>
<thead>
<tr>
<th>Generic Middleware</th>
<th>Dedicated Middleware</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FreeRTOS</strong></td>
<td><strong>Secure Boot and Secure Firmware Update</strong></td>
</tr>
<tr>
<td><strong>FatFS file system</strong></td>
<td><strong>TF-M for trusted execution environment</strong></td>
</tr>
<tr>
<td><strong>mbedTLS and mbedCrypto</strong></td>
<td><strong>USB-PD device driver</strong></td>
</tr>
<tr>
<td><strong>USB Device stacks</strong></td>
<td><strong>STM32 Touch Sensing library</strong></td>
</tr>
</tbody>
</table>

#### Peripheral drivers

- **HAL API**
  - Hardware Abstraction Layer, highly portable and easy to use
- **LL APIs**
  - Low-Layer APIs, light weight and highly optimized for runtime efficiency

#### Project Examples

- **STM32CubeMX ready**
  - More than 300 project examples for KEIL, IAR and STM32CubeIDE toolchains, with a STM32CubeMX configuration file

**www.st.com/stm32cubel5**
SBSFU and TF-M in STM32CubeL5

Reference code framework for a trusted Execution Environment

**STM32L5**
- Un-Trusted Un-Privileged
- Un-Trusted Privileged
- TF-M (Application Root of Trust)
- TF-M (PSA Root of Trust)
- SBSFU TF-M (PSA immutable Root of Trust)

**TF-M Framework**
- Isolation and Secure execution
- Secure services (crypto, initial attestation, secure storage)
- Easy addition of user secure services
- Leveraging STM32L5 security features

**SBSFU TF-M**
- Secure Boot
- Secure Firmware Update
STM32L5 is one of the first MCU PSA Level 2 certified

psa_certified™
level two

PSA Level 2 certified
STM32CubeIDE

All-in-1 STM32 development tool

Configure and generate code

STM32CubeMX integrated

Develop code, Compile and Link

TrustZone support

- TrueSTUDIO / SW4STM32 importer
- Advanced editor
- GNU C/C++ for Arm® toolchain

Program and Debug

TrustZone support

- GDB and OpenOCD debugger
- Support of ST-Link and J-Link debug probes
Partners IDEs development flow

Arm V8-M TrustZone architecture support

STM32CubeMX
- STM32CubeMX enhanced for TrustZone
  - Peripherals/middleware configuration
  - Resources allocation to security domains

IDEs Compile and Debug
- TrustZone Support
  - Partners IDE
  - STM32CubeIDE based on Eclipse
  - TrustZone debugging

STM32 Programming Tool
- STM32CubeProgrammer
  - Device and memory configuration
  - Program the application
  - Secure Firmware Install

Optional step
Configuration tool

- Power Consumption Calculator
- MCU or board Selector
- Load an Example .ioc file
- Pinout Configuration
- Clock Tree Initialization
- Peripherals Configuration
- TrustZone configuration and GPIOs, memories, DMA, peripherals allocation to security domains

- Code Generation
- TrustZone support
- Middleware Parameters
- FreeRTOS
- FatFS
- USB device
All-in-one programming software tool

- Intuitive GUI
- Command Line Interface for scripting
- API DLL for Custom Integration
- STLink (JTAG, SWD)
- STM32 Bootloader Interface (USB, UART, SPI, I2C, CAN)
- Secure Firmware install (SFI)

- MCU Internal Flash and external Flash services
- MCU configuration (Option bytes)
STM32L5 hardware solutions

Speed-up evaluation prototyping and design

**Evaluation Boards**
- Full feature STM32L5 evaluation
  - STM32L552E-EV

**Discovery Kit**
- Flexible prototyping & demo
  - STM32L562E-DK

**Nucleo Boards**
- Affordable and quick prototyping
  - NUCLEO-L552ZE-Q

$275
$76
$20
Discovery kit

Prototype your wearable or sensor application with STM32L562E-DK

Fan-out expansion board included

Key Features

- STM32L562 MCU with AES and PKA
- 240 x 240 pixel-TFT color Display
- state-of-the-art Energy Meter
- 3D accelerometer and 3D gyroscope
- Bluetooth® V4.1 low energy module
- Audio Codec and Headphone amplifier
- Digital microphone
- USB Type-C™ Sink device FS
- 512Mbit Octal Flash memory extension
- ST-Link V3
- STMod+ connector with fan-out expansion board for Wi-Fi®, Grove and mikroBUS™ compatible connectors
STM32CubeMonitor-power

State-of-the-art on-board power consumption measurement

STM32L562E-DK
On-board Energy Meter
300 nA to 150 mA measurement range
Secure your production flow with Secure Firmware Install (SFI)

Protect your code and control the number of products manufactured

Customer premises

- FW
- Encrypted FW
- Store encryption key and production counter into HSM
- ST Hardware Secure Module (HSM)

Untrusted environment

- STM32L5 SFI
- Authenticate target STM32
- Generate installation license
- HSM physical transfer
- Encrypted FW transfer

Number of products controlled

Secure Module (HSM)
Conclusion

STM32L5 helps designers to answer IoT challenges

• More security
• Lower power consumption
• Integration, performance, ecosystem
Releasing your creativity

/STM32
@ST_World
community.st.com
www.st.com/STM32L5
Thank you