life.augmented

New innovations in embedded peripherals

Sridhar Ethiraj
Technical Marketing & Applications , India.
STMicroelectronics.

Agenda

- # Introduction
- # Low power innovation
- # Communication peripherals
- # Graphics innovation
- # Security

Applications are more and more demanding!

more autonomy

more integration

more security

more power efficient

Application examples:

- Industrial Applications
- Metering
- Medical monitoring devices
- POS
- Wearables

life.augmented

STM32 MCU and MPU portfolio

MPU

STM32MP1
Up to 1 GHz Cortex-A7
209 MHz Cortex-M4

High Perf MCUs

STM32F7
1082 CoreMark
216 MHz Cortex-M7

STM32H7
Up to 3224 CoreMark
Up to 550 MHz Cortex -M7
240 MHz Cortex -M4

STM32F2
Up to 398 CoreMark
120 MHz Cortex-M3

STM32F4
Up to 608 CoreMark
180 MHz Cortex-M4

STM32H5
Up to 1023 CoreMark
250 MHz Cortex-M33

Mainstream MCUs

Mixed-signal MCUs

STM32F3
245 CoreMark
72 MHz Cortex-M4

STM32G4
569 CoreMark
170 MHz Cortex-M4

STM32C0
114 CoreMark
48MHz Cortex M0+

STM32F0
106 CoreMark
48 MHz Cortex-M0

STM32G0
142 CoreMark
64 MHz Cortex-M0+

STM32F1
177 CoreMark
72 MHz Cortex-M3

Ultra-low Power MCUs

STM32L0
75 CoreMark
32 MHz Cortex-M0+

STM32L4
273 CoreMark
80 MHz Cortex-M4

STM32L4+
409 CoreMark
120 MHz Cortex-M4

STM32L5
443 CoreMark
110 MHz Cortex-M33

STM32U5
651 CoreMark
160 MHz Cortex-M33

Wireless MCUs

STM32WL
162 CoreMark
48 MHz Cortex-M4
48 MHz Cortex-M0+

STM32WB
216 CoreMark
64 MHz Cortex-M4
32 MHz Cortex-M0+

STM32WBA
407 CoreMark
100 MHz Cortex-M33

Legend: Latest product generation Radio co-processor only

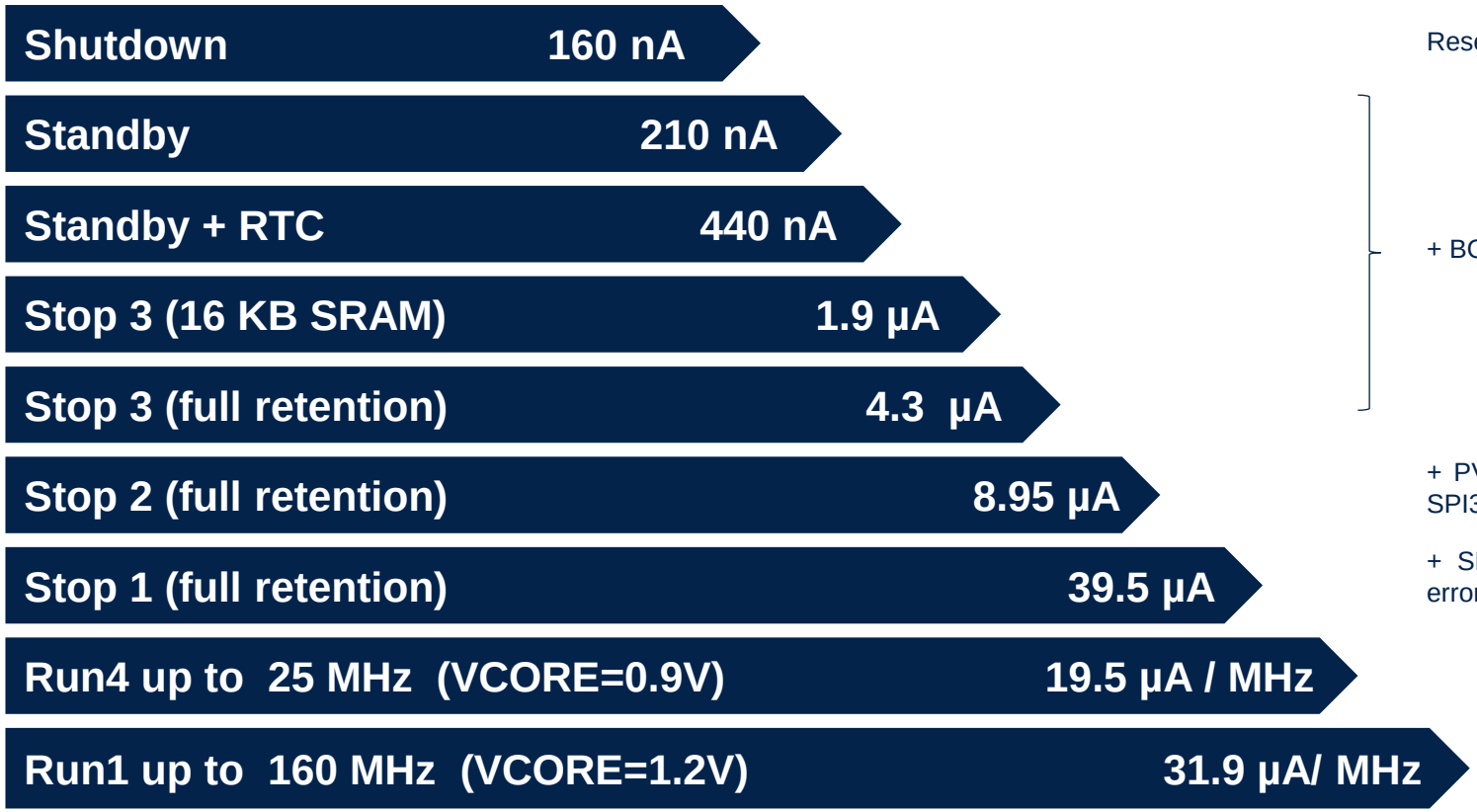
Innovation in peripherals

life.augmented

Low power modes

Ultra-low-power modes

Best power consumption numbers with full flexibility



Wake-up sources

Reset pin, 24 I/Os, RTC/TAMP, CSS

+ BOR, IWDG

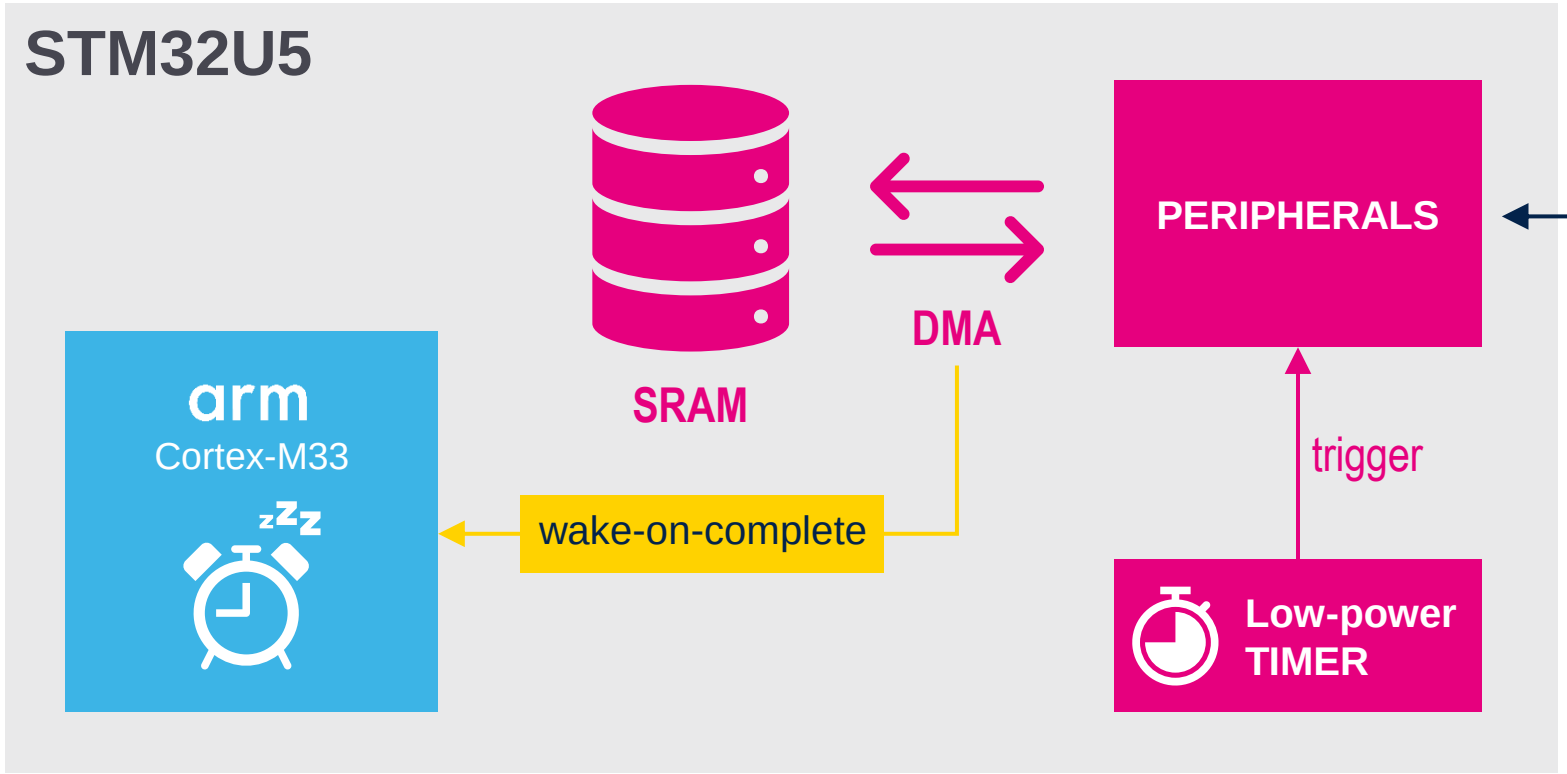
+ PVD, peripheral voltage monitor, LPDMA1, LPUART, I2C3, SPI3, ADC4, COMP1-2, LPTIM1-3-4, ADF1

+ SRAM2 ECC error, SRAM3 ECC error, BKPSRAM ECC error, GPDMA1, MDF1, I2C1-2, SPI1-2, UART1-5, LPTIM2

life.augmented

Cut MCU power consumption by 90%*

Low power background autonomous mode (LPBAM)



Peripherals:

- I2C master or slave
- SPI / UART reception or transmission
- ADC / DAC
- Voice Activity Detection
- LPTIM
- I/O

** Typical application where peripherals need to acquire data regularly*

Low power background autonomous mode (LPBAM)

Smart way to implement complex applicative scenario in low-Power mode

- No need for CPU – all is based on DMA (LPDMA & GPDMA)
  - Peripherals configuration & activity can be chained thanks to DMA linked-list, down to Stop 2 mode. DMA can be used to “emulate” software and reconfigure peripherals.
  - Hardware triggers can start peripheral activity (i.e. ADC conversion, communication peripheral transfer, DMA transfer…).

- Power gain:
  - Most of the product can be shut-down in Stop mode
  - Clock is provided to IP only when necessary in Stop mode
  - Analog peripherals / oscillators are powered-on only when necessary in Stop mode

Autonomous peripherals features

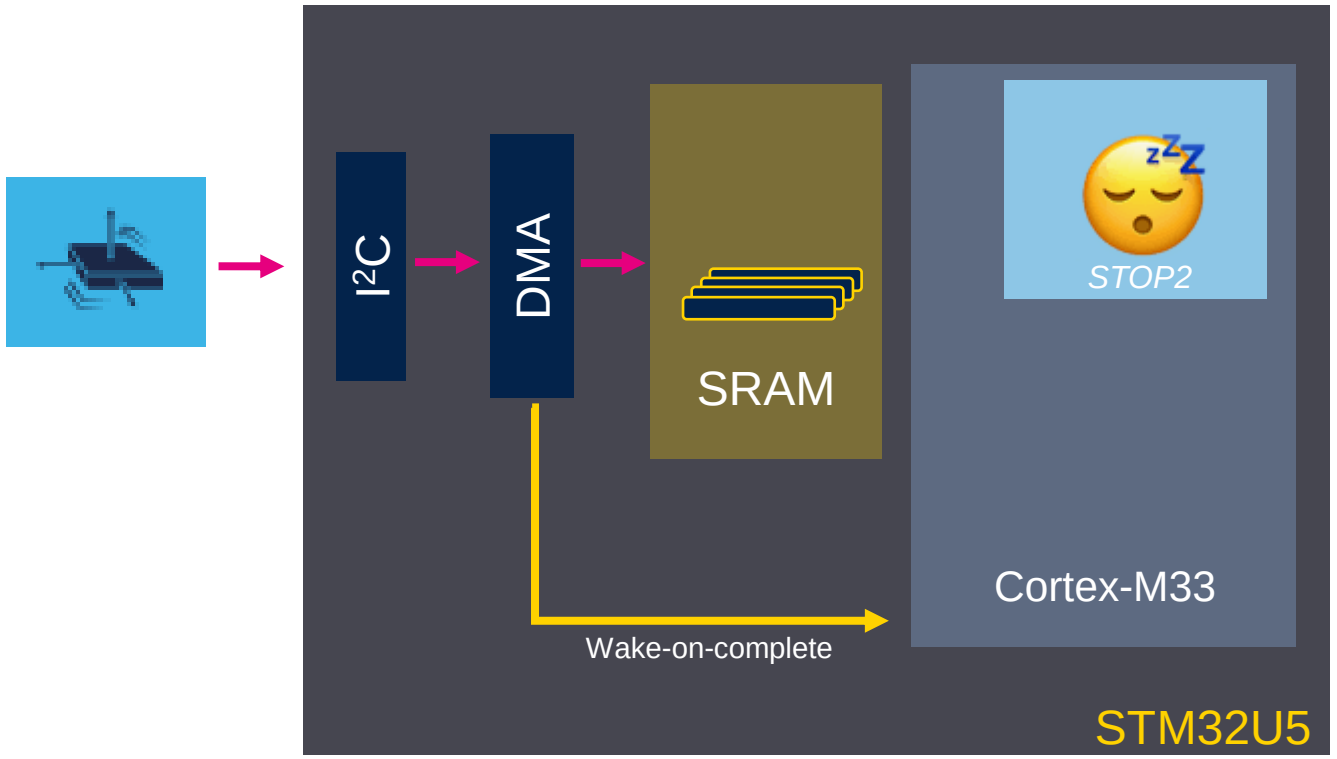
Autonomous peripheral	
Down to Stop 0/1	**Down to Stop 2**
GPDMA1	
LPDMA1	**LPDMA1**
USART(1,2,3,4,5)	
LPUART1	**LPUART1**
I2C(1,2,4)	
I2C3	**I2C3**
SPI(1,2)	
SPI3	**SPI3**
ADC4 (12-bit)	**ADC4 (12-bit)**
DAC	**DAC**
LPTIM(1,3,4)	**LPTIM(1,3,4)**
LPTIM2	
MDF1	
ADF1	**ADF1**

- Peripheral activity is independent from MCU power mode (Run, Sleep, Stop)
- DMA transfers supported in Stop mode
  - Thanks to kernel and AHB/APB clocks requests
- Peripheral activity can be started with an asynchronous trigger in Stop mode:
  - Communication peripherals start of transfer
  - ADC/DAC start of conversion
  - DMA start of transfer

  ➢ Triggers can be selected between LPTIM output, comparator output, I/O…
- Autonomous peripherals interrupts wake up from Stop

LPBAM use-cases

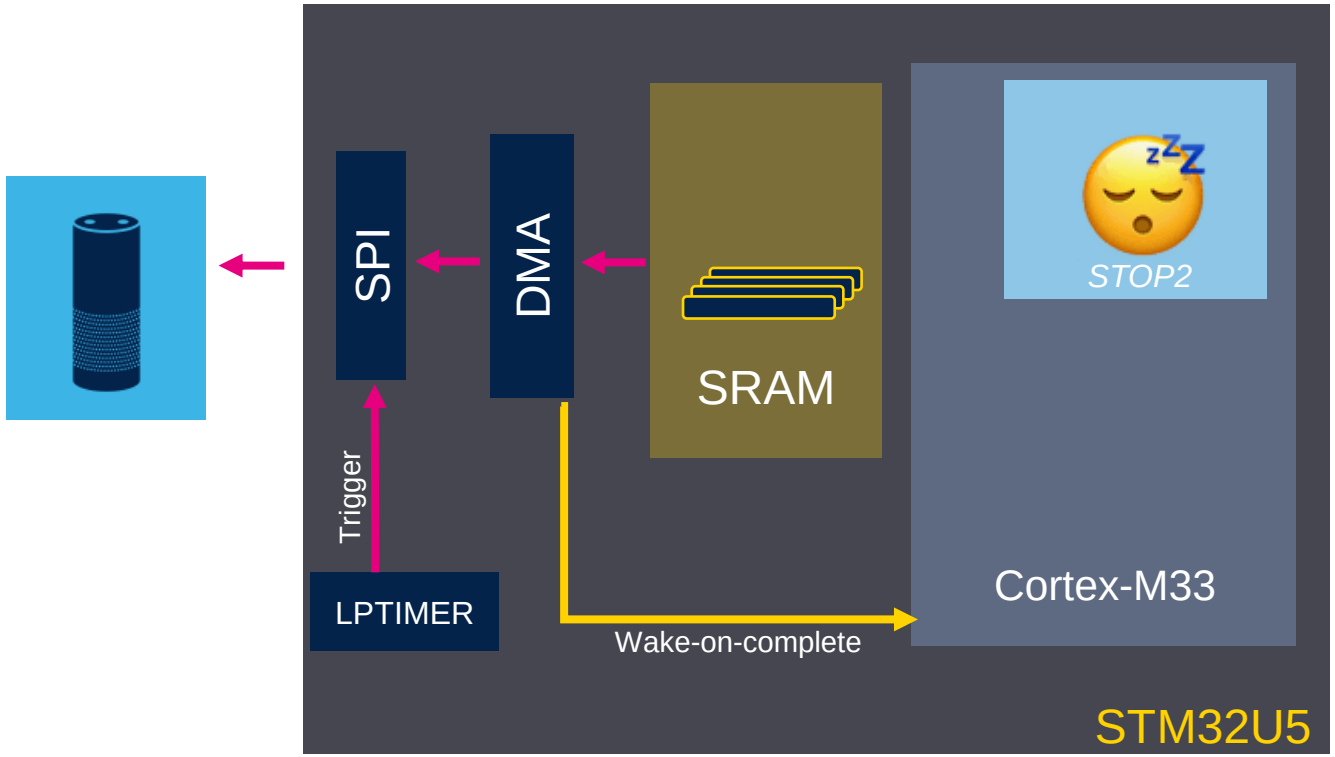
- **I²C slave transfer ; SPI / UART reception**
- I²C master transfer ; SPI / UART transmission
- ADC conversion
- DAC conversion
- Voice Activity Detection
- LPTIM PWM ratio change, input capture, pulse counter…
- I/O control (input, output)
- Peripherals chaining
- ….



life.augmented

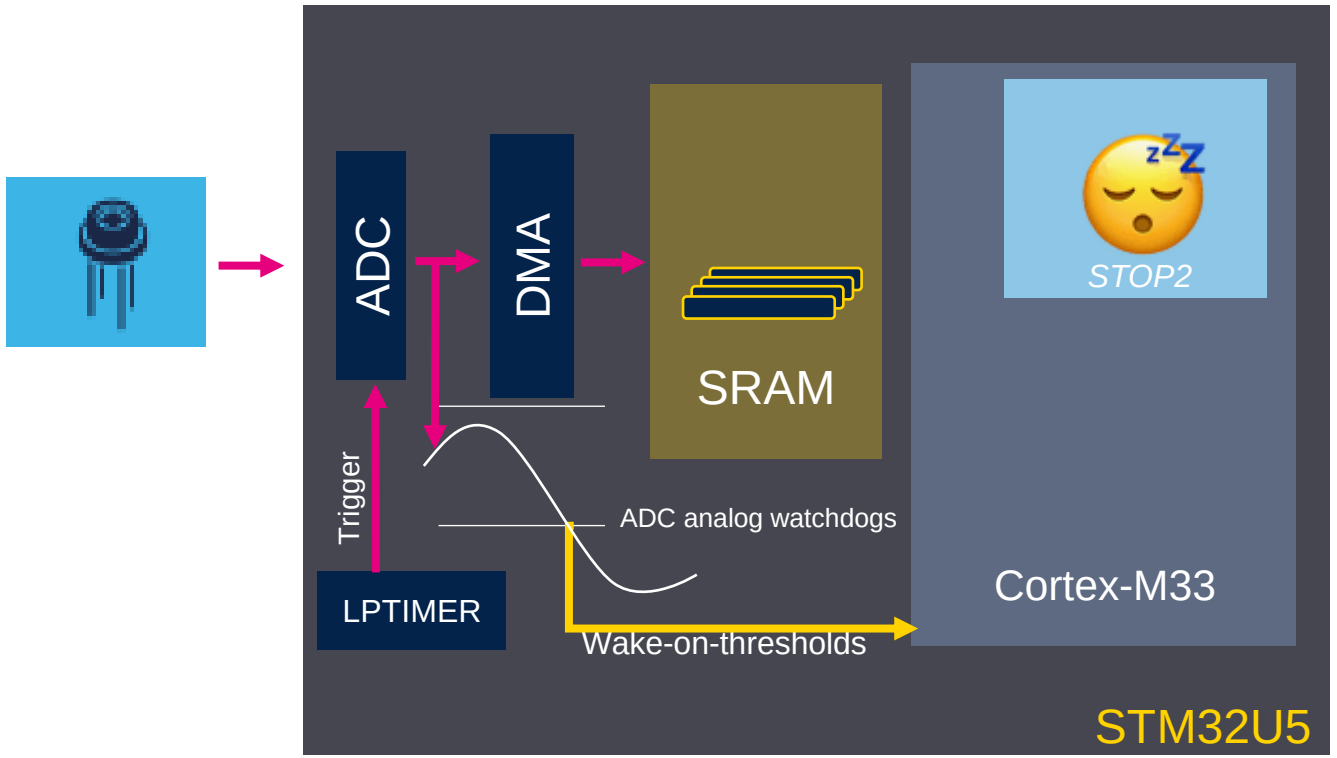
LPBAM use-cases

- I²C slave transfer ; SPI / UART reception
- **I²C master transfer ; SPI / UART transmission**
- ADC conversion
- DAC conversion
- Voice Activity Detection
- LPTIM PWM ratio change, input capture, pulse counter…
- I/O control (input, output)
- Peripherals chaining
- ….



LPBAM use-cases

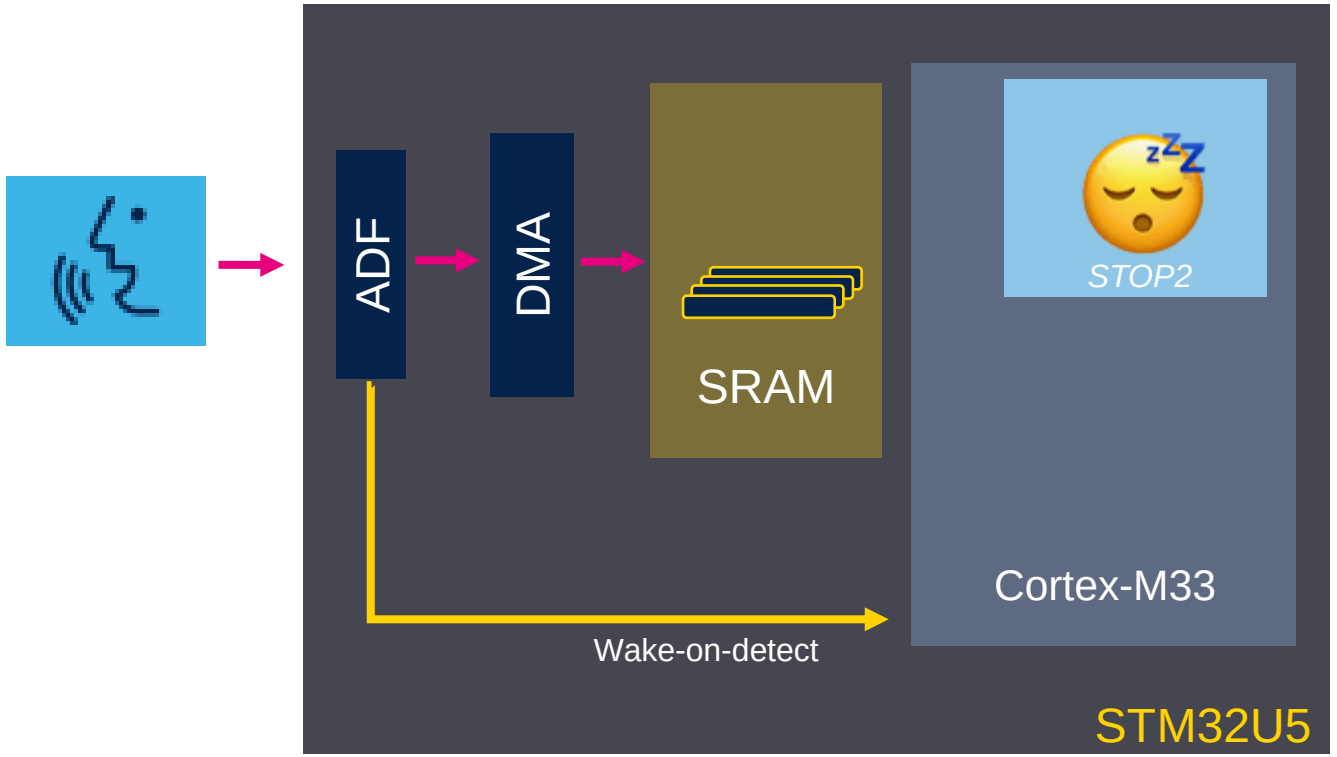
- I²C slave transfer ; SPI / UART reception
- I²C master transfer ; SPI / UART transmission
- **ADC conversion**
- DAC conversion
- Voice Activity Detection
- LPTIM PWM ratio change, input capture, pulse counter…
- I/O control (input, output)
- Peripherals chaining
- ….



life.augmented

LPBAM use-cases

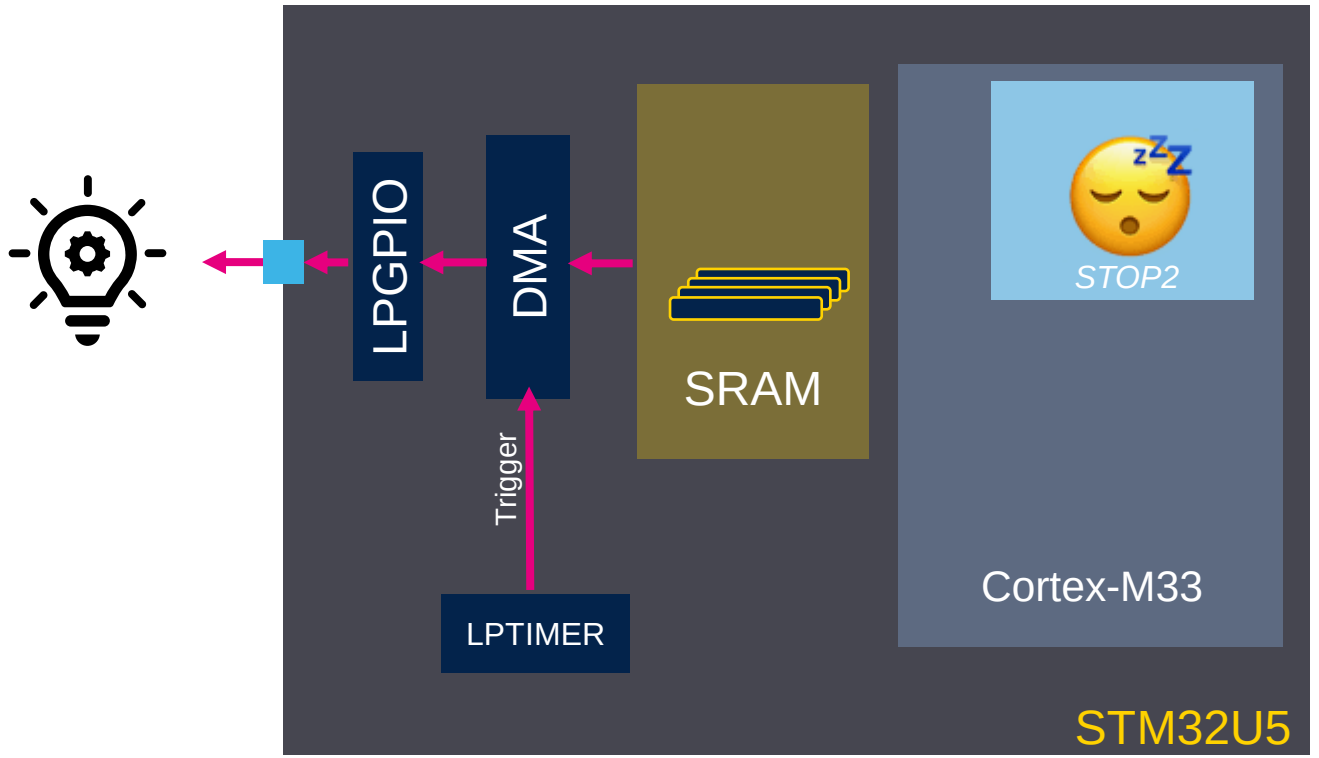
- I²C slave transfer ; SPI / UART reception
- I²C master transfer ; SPI / UART transmission
- ADC conversion
- DAC conversion
- **Voice Activity Detection**
- LPTIM PWM ratio change, input capture, pulse counter…
- I/O control (input, output)
- Peripherals chaining
- ….



life.augmented

LPBAM use-cases

- I²C slave transfer ; SPI / UART reception
- I²C master transfer ; SPI / UART transmission
- ADC conversion
- DAC conversion
- Voice Activity Detection
- LPTIM PWM ratio change, input capture, pulse counter…
- **I/O control (input, output)**
- Peripherals chaining
- ….

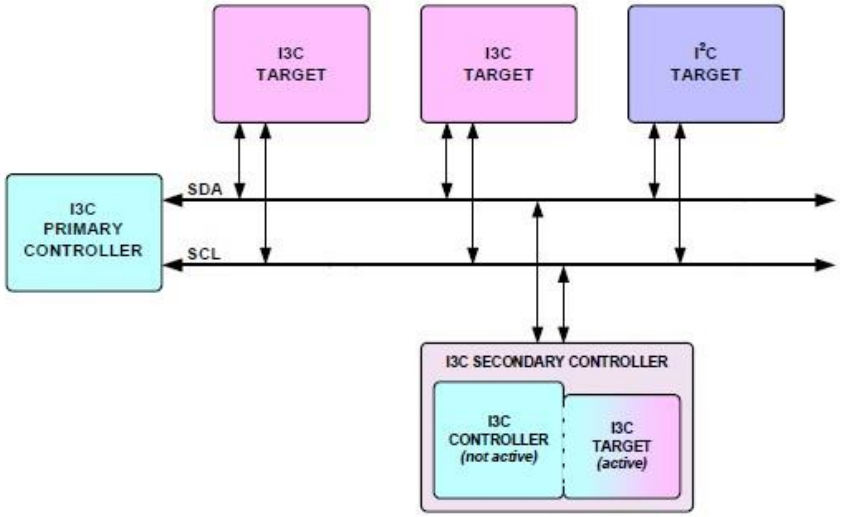


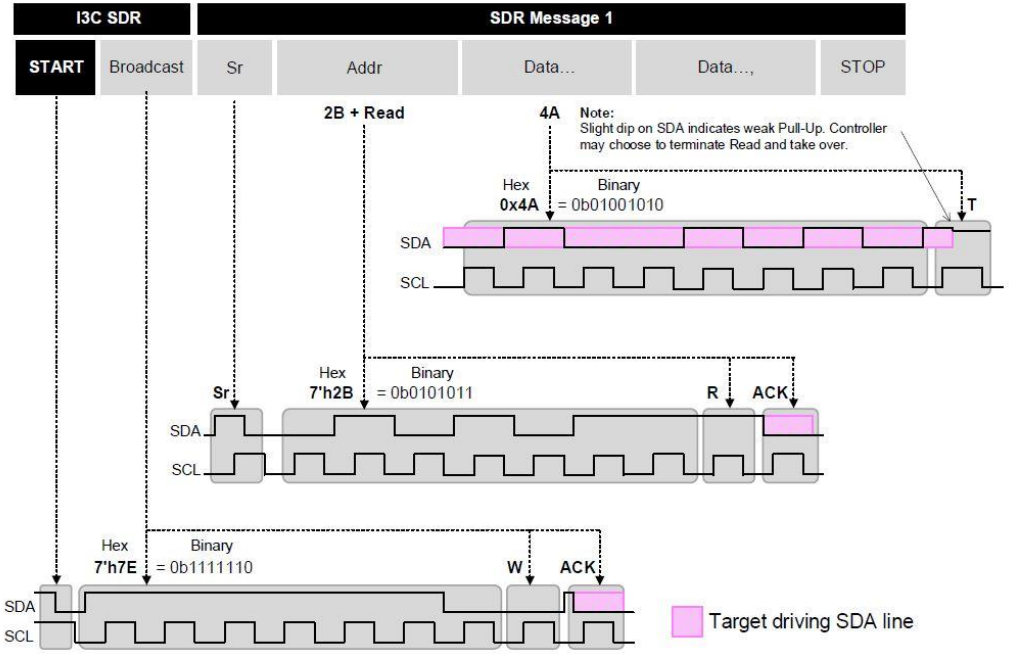
Communication peripherals

I3C, OCTOSPI & OTFDEC, HSPI

life.augmented

I3C overview





Application benefits: Improved I²C

- Low pin count
  - In-band prioritized interrupts
  - In-band target reset
  - In-band power modes control
- Low power
  - Push-pull (SCL and most of the time SDA)
  - Open-drain SDA mode with controller pull-up
- Legacy I²C mode (if no clock stretch, 50ns spike filter)
- Higher speed up to 12.5 MHz (mid-speed SPI)
- Low implementation cost (especially if target)
- Bus error detection & recovery
- Target read termination
- Hot-join
- Standard specification (MIPI v1.1)

I3C key features 1/2

- MIPI I3C specification v1.1
  - SDR-only primary controller
  - SDR-only secondary controller
  - SDR-only target
- Programmable I3C bus timing
  - When controller
    - SCL high and low time
    - SCL stall time
    - Bus free condition time
  - When target
    - SDA hold time
    - Bus available & idle condition time
- Queued data transfers
  - Transmit FIFO (TX-FIFO)
  - Receive FIFO (RX-FIFO)
- Queued control and status transfers, when controller
  - Control FIFO (C-FIFO)
  - Optional status FIFO (S-FIFO)
- For each FIFO, optional DMA mode with a dedicated DMA channel
- Target-initiated requests
  - In-band interrupts, with payload (up to 4 bytes)
  - Up to 4 simultaneous targets, when controller
  - Bus control & hot-join request

I3C Key features 2/2

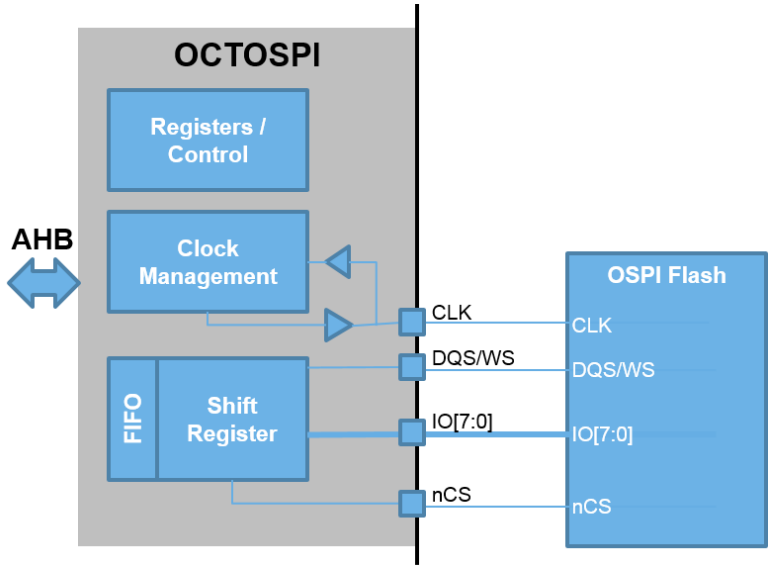
- Frame-level messages management
- Individual event-based management
- Bus error detection and recovery
- Multi-clock domain management
  - APB clock, I3C kernel clock and I3C bus clocks
- Automatic SDA push-pull & open-drain modes by I3C hardware
- Configured GPIOs for SCL & SDA
  - Alternate function
  - With no pull

- Wakeup from Stop (with SVOS3)
  - When controller, on an acknowledged and received target request
    - hot-join
    - IBI without MDB
    - controller-role
  - When target
    - On a reset pattern detection
    - On a missed start detection

OCTOSPI overview

Two OCTOSPI + IO manager

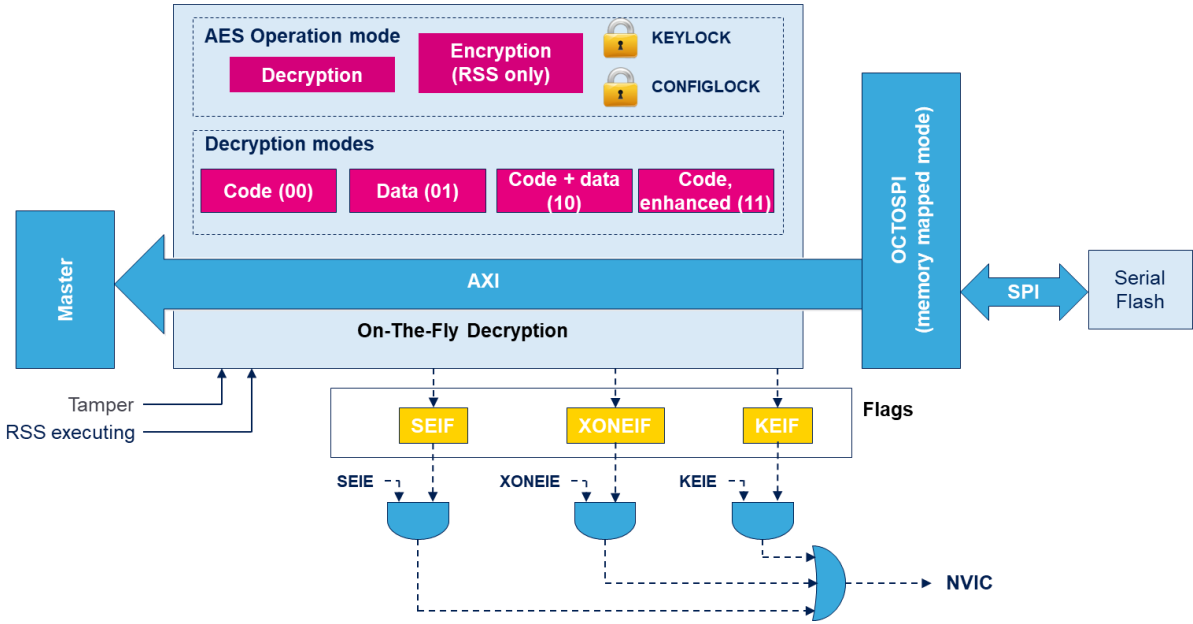
- Provides communication interface with external serial memories such as serial PSRAMs, serial NAND and serial NOR flash memories, HyperRAMs and HyperFlash
- Fully configurable from single, dual, quad to octal
- Supports memory mapped read & write
- Supports eXecute In Place (XIP)
- Support data qualifier & write strobe



life.augmented

On-the-fly decrpytion engine (OTFDEC)

- On-the-fly decryption during OCTOSPI Memory-mapped read operations
- Key feature
  - On-the-fly 128-bit decryption (AES CTR mode)
  - Up-to 4 independent encrypted area
  - Encryption key confidentiality & integrity protection
  - Encryption mode
- Benefit
  - Execution of encrypted application code from external serial flash



Only H5-2M

STM32H7, STM32U5 & STM32H5 features comparison

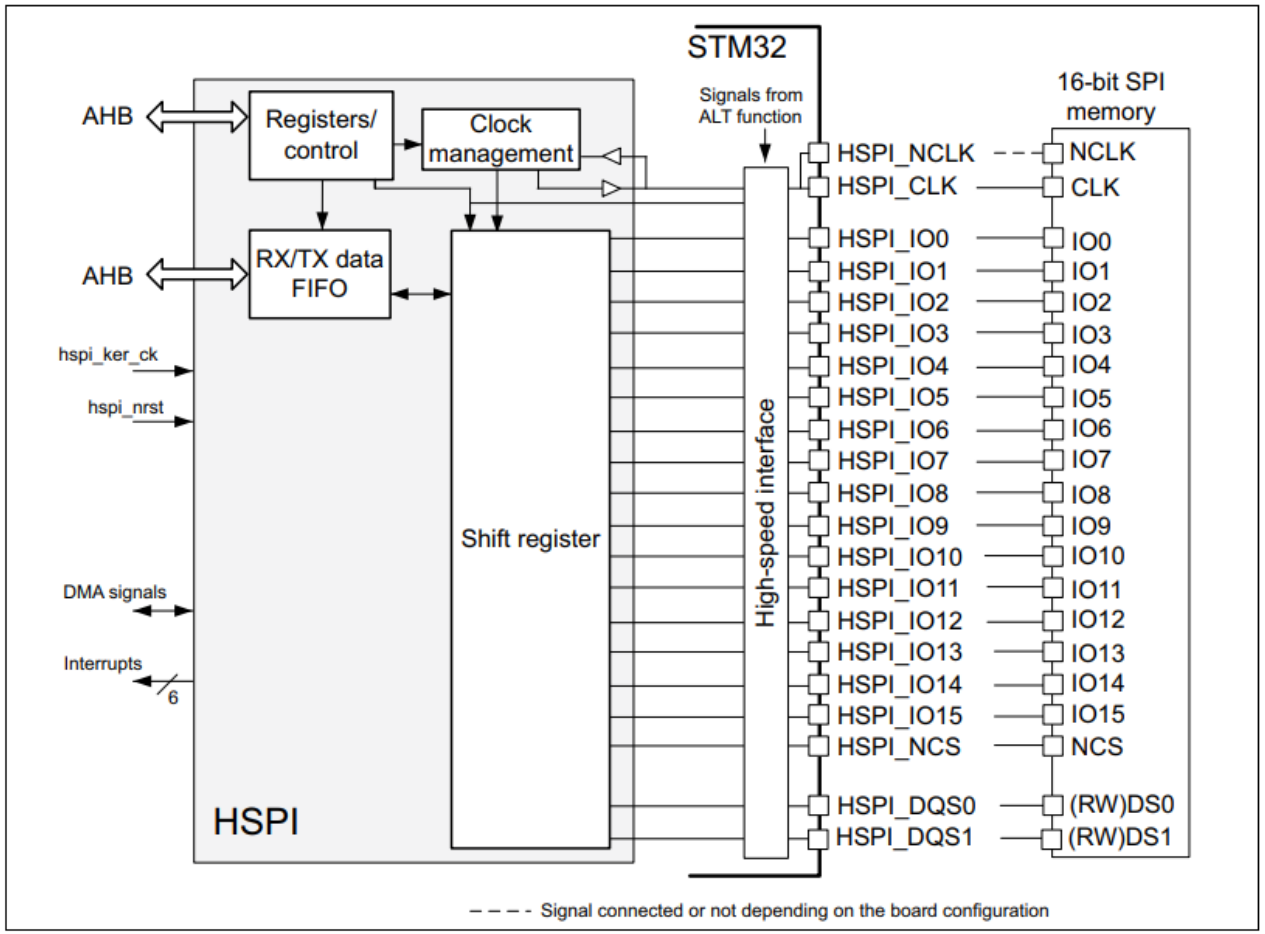
OCTOSPI features	STM32H7	STM32U5	STM32H5
Number of instances	2	2	1
OctoSPI IO Manager (OCTOSPIM) No Muxed mode !	Y	Y	N
Single ended clock for 3V0 HyperBus™ mode	Y	Y	Y
Differential clock for 1V8 HyperBus™ mode	Y	Y	Y
Zero wait states like performance execution thanks to I-Cache	Y	Y	Y
Support of QSPI and OSPI PSRAMs (from APMemory)	Y	Y	Y
CS boundary (to manage the RBX) and refresh (for self refresh)	Y	Y	Y
Full Support for HyperRAM™ memories	Y	Y	Y
On-the-fly decryption engine (OTFDEC) protecting flash code	Y	Y	Y
Maximum Frequency in DTR mode (Mhz)	120	100	120(1)

(1) Preliminary Data and are subject to change

life.augmented

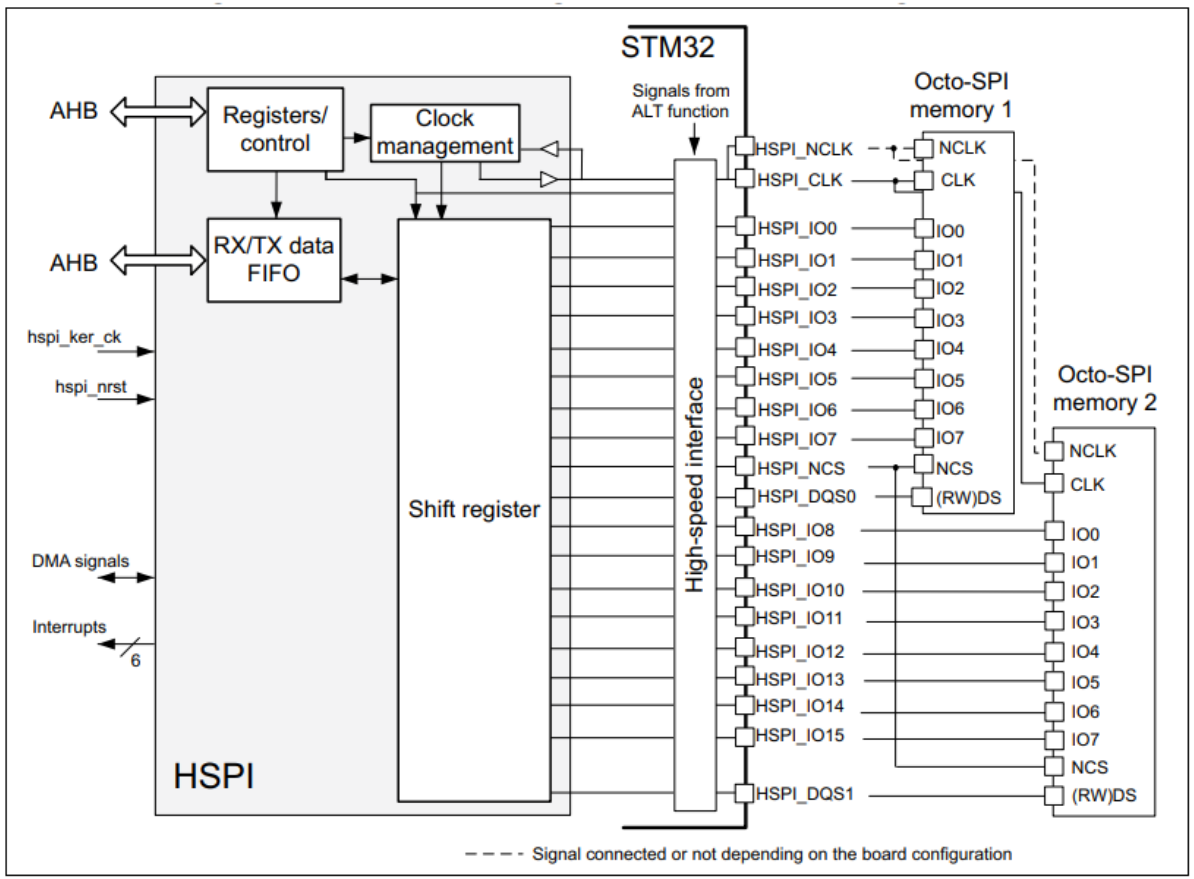
Hexadeca-SPI interface (HSPI) overview

- The HSPI supports most external serial memories such as serial PSRAMs, serial NAND and serial NOR flash memories, HyperRAM™ and HyperFlash™ memories
- Functional modes: indirect, automatic status-polling, and memory-mapped
- Fully configurable from single, dual, quad & octal communication mode
- HSPI mode accessing a single 16-bit memory
- Supports memory mapped read & write
- Supports eXecute In Place (XIP)



HSPI: dual Octal mode

- Dual-memory configuration, where 8 bits can be sent/received simultaneously by accessing two quad or two octal memories in parallel
- Fully programmable frame format
- Support wrapped-type access to memory in read direction
- SDR (single-data rate) and DTR (double-transfer rate) support
- Support data qualifier & write strobe
- Integrated FIFO for reception and transmission



life.augmented

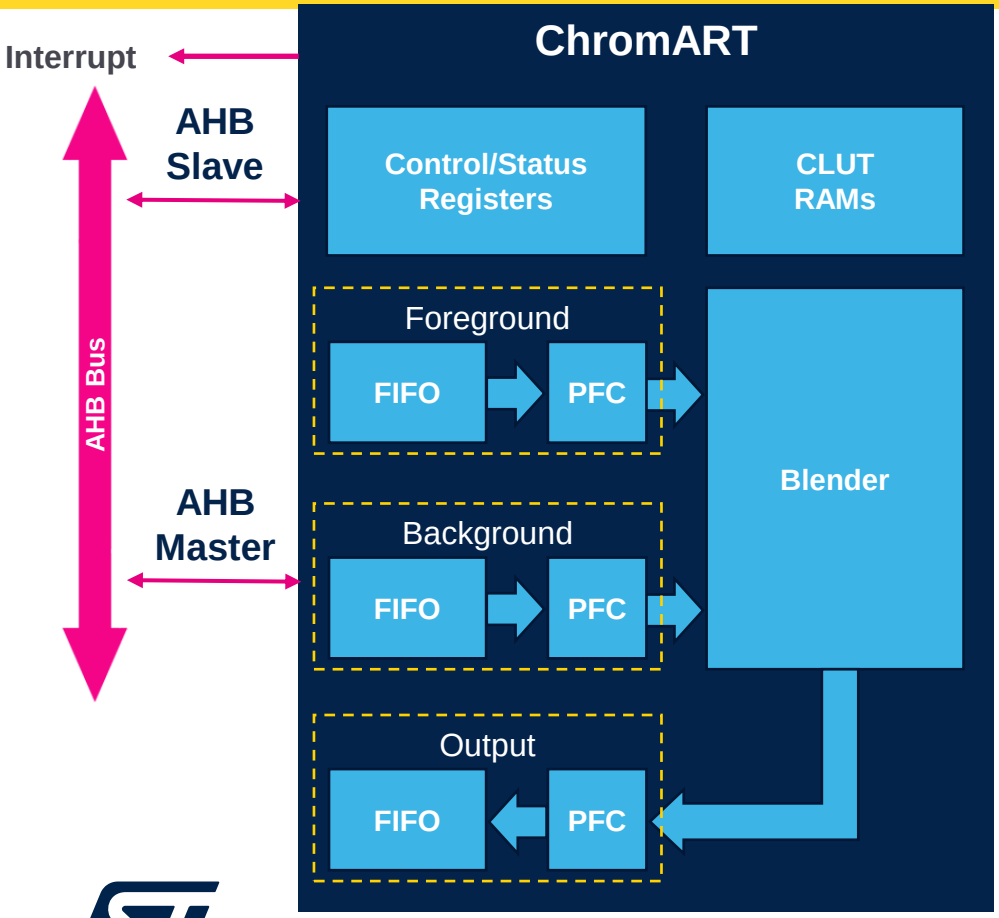
Graphics innovations

life.augmented

Chrom – ART, Chrom-GRC, NEO Chrom

Chrom-ART overview

2D graphic accelerator



- Provides hardware acceleration for graphical operations
  - Graphic oriented 2D DMA
  - Planes blending & pixel format conversion
  - Specific modes for anti aliased fonts

Application benefit

- Offload CPU for graphical operation
- One pixel per cycle calculation
- Integrated pixel format converter & blender
- Simple integration through graphical stack

life.augmented

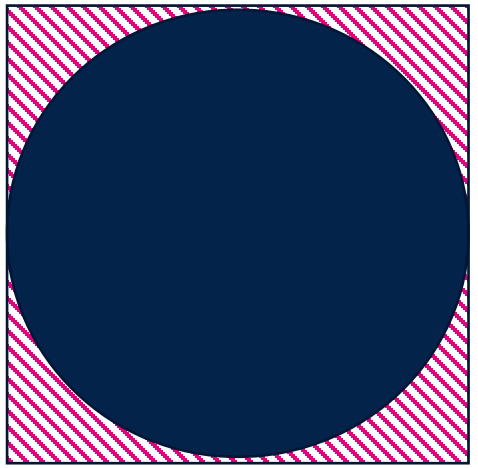
STM32 hardware embedded graphics memory optimization

Chrom-GRC™

Memory optimization for round displays
Saving up to 20% of the framebuffer's

➔ The technology behind

- Graphic Resource Cutter for non-square displays
- No modification nor special management at SW level
- RAM needs:
  - For 360x360 round display
    @16bpp ~205kBytes (vs.253kBytes)
    @24bpp ~307kBytes (vs.380kBytes)
  - For 400x400 round display
    @16bpp: 250kBytes (vs.312kBytes)
    @24bpp: 372kBytes (vs.469kBytes)



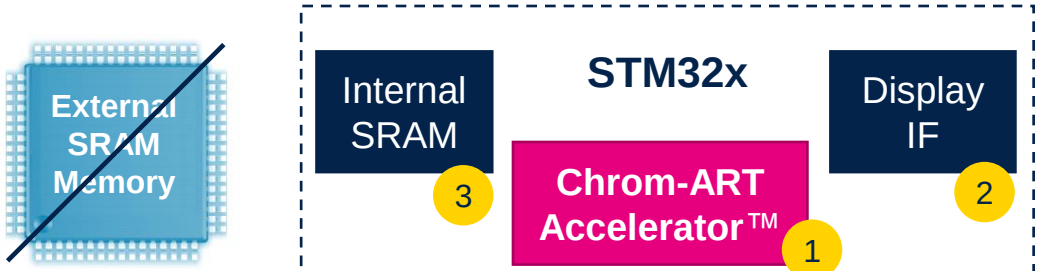
Saved memory
(up to 20%)

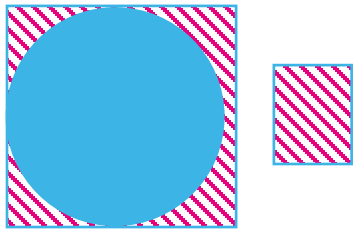
life.augmented

Chrom-GRC

1. Chrom-ART Accelerator™
2. Large choice of display interfaces

- Integration and resource optimization
  - Chrom-GRC™ memory optimization for round displays
  3. Large internal SRAM allowing
     - BOM cost and power consumption optimization
     - Support of up to 400x400 24 bpp MIPI-DSI round displays
     - Support of up to 4’, WQVGA 16 bpp TFT displays with no external memory





20% Memory saving

NeoChrom

STM32 hardware embedded graphics HW acceleration

NeoChrom GPU

Offloads the CPU from graphics tasks
Lower memory consumption
Higher GUI performance – smooth and richer graphics effects:

- Realizing 3D-like graphics on STM32 microcontroller

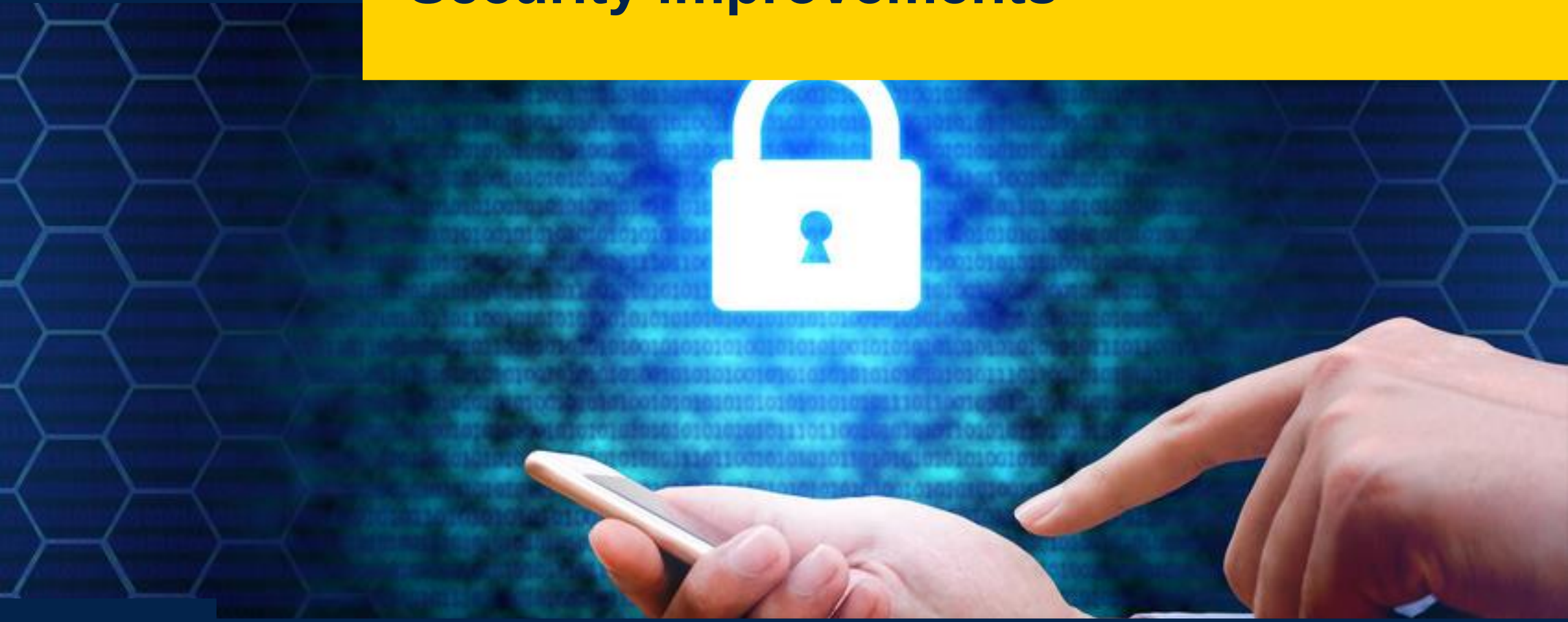
➔ **The technology behind**

- Simple Drawing
- 2D Copy
- Alpha blending
- Color format conversion

- **Advanced Drawing**
- **Scaling, Rotation**
- **Perspective correct texture mapping**
- Image format compression

NeoChrom GPU video!

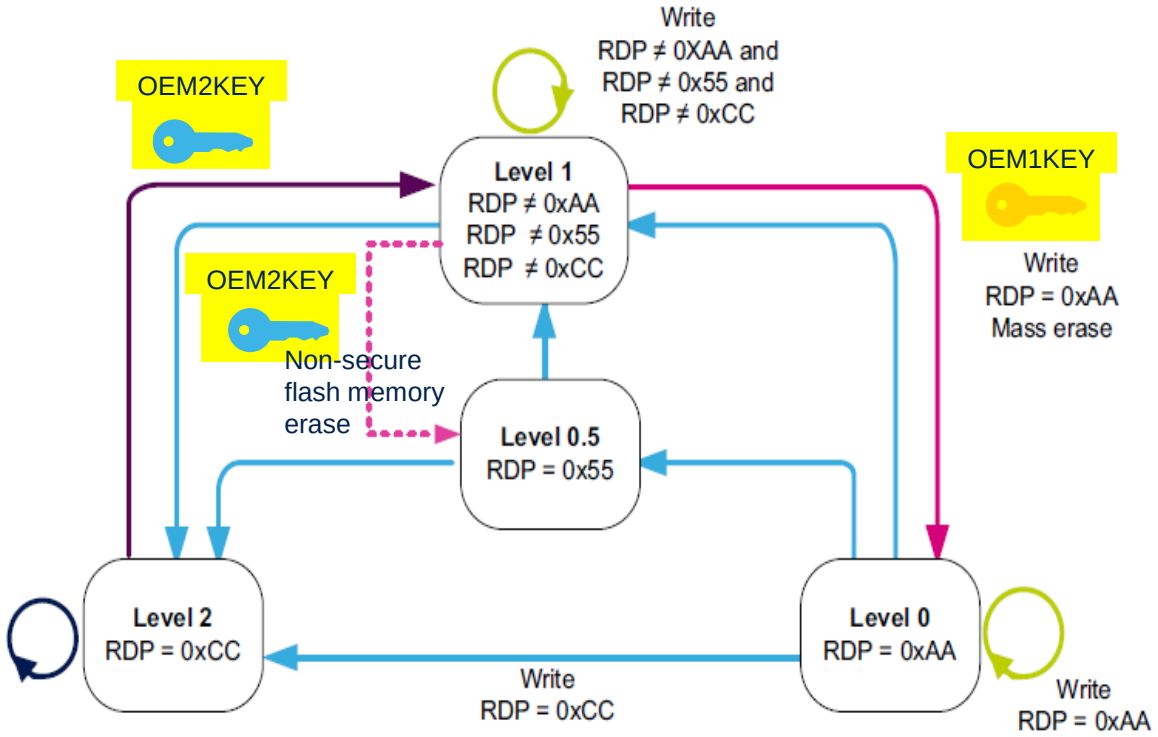
Security improvements



life.augmented

Enhanced life cycle management

Password key-based RDP regressions



Example of STM32U5 lifecycle when TrustZone is enabled

- Two password keys - **OEM1KEY**, **OEM2KEY**
  - Both 64-bit, write only, none readable
  - RPD **Legacy Mode** if left **un-programmed**
- OEM1KEY is used to manage the RDP level regression from **Level 1** to **Level 0**
- OEM2KEY is used to manage the RDP level regression from **Level 2** to **Level 1** and **Level 1** to **Level 0.5**
- To unlock, the password key is shifted through JTAG/ SWD pins **during reset**
- New 32-bit device specific ID (**Chip ID)**
  - Allowing password keys to be associated with a Chip ID

life.augmented

Symmetric Crypto

life.augmented

STM32U5 AES feature list

- NIST FIPS197 compliant AES implementation
- AES chaining modes
  - Electronic codebook (ECB)
  - Cipher block chaining (CBC)
  - Counter (CTR) mode
  - Galois counter mode (GCM)
  - Galois message authentication code (GMAC)
  - Counter with CBC-MAC (CCM) mode
- AES operation modes on 128-bit block of data, 128 or 256-bit of key
  - Encryption (mode 1)
  - Decryption (mode 3), with associated key derivation for decryption (mode 2)
- AHB slave with suspend/resume & DMA support (IN + OUT channels)
- 32-bit data words swapping support (bit, byte or half-word)
- Atomic key writing/loading enforcement

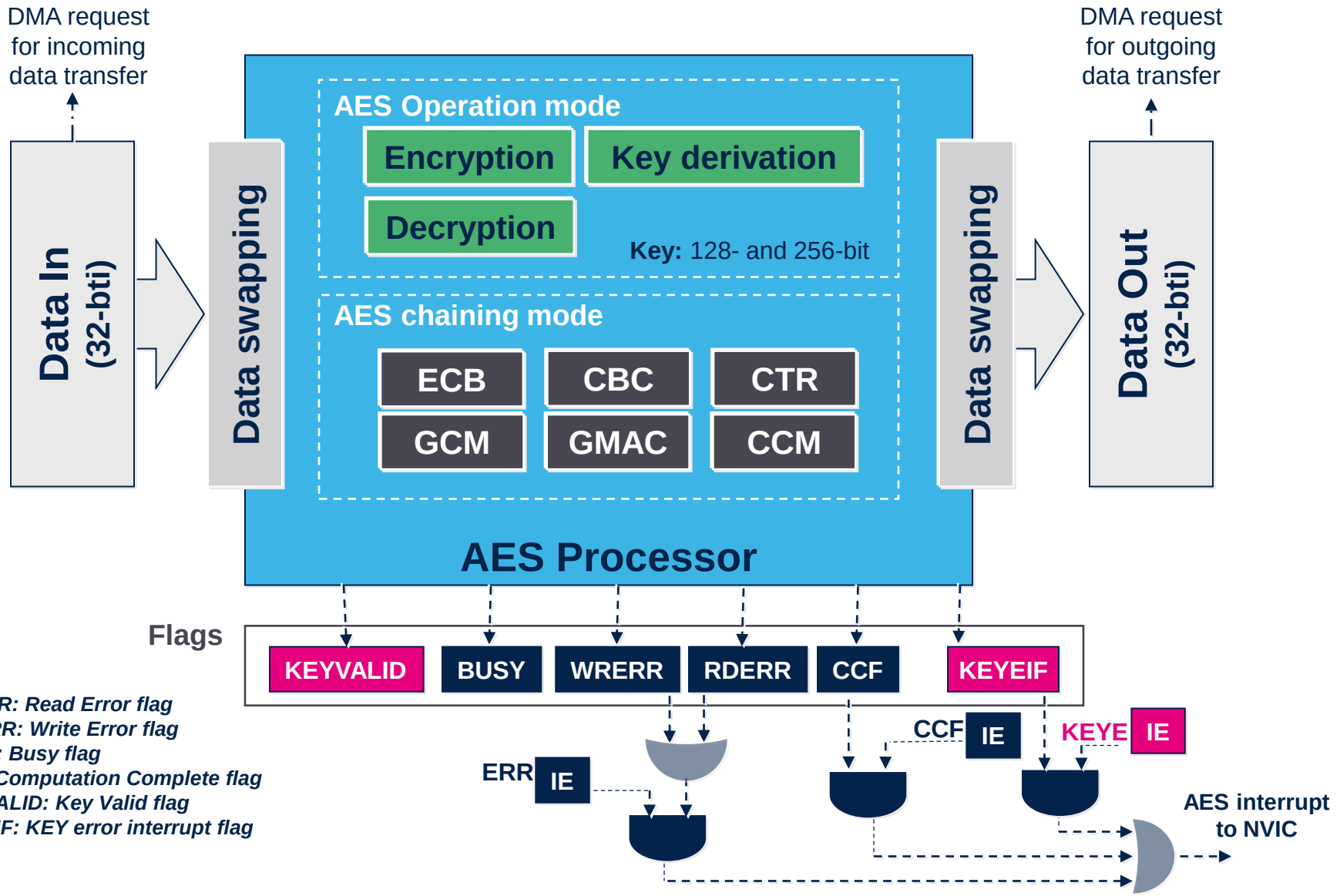
Key size	ECB	CBC	CTR	GCM				CCM			
				Init	Header	Payload	Tag	Init	Header	Payload	Tag
128b	51(*)		51	64	35	51	59	63	55	114	58
256b	75 (*)		75	88	35	75	75	87	79	162	82

(*) For decryption you must add key derivation time, once

Number of cycles required to process a 128-bit block
Clock frequency= AHB clock of peripheral

life.augmented

AES block diagram



RDERR: Read Error flag
WRERR: Write Error flag
BUSY: Busy flag
CCF: Computation Complete flag
KEYVALID: Key Valid flag
KEYEIF: KEY error interrupt flag

life.augmented

Specific to SAES peripheral

SAES feature list (STM32U5 only)

- NIST FIPS197 compliant AES implementation
- AES chaining modes
  - Electronic codebook (ECB)
  - Cipher block chaining (CBC)
- Enhanced secure key storage
  - Hardware keys (DHUK, BHK)
    - Device-dependent, with DHUK
    - Application dependent, with BHK
  - Hardware secret key decryption (key unwrap)
  - Key valid: atomic key writing / loading enforcement
- AES operation modes:
  - Encryption (mode 1)
  - Decryption (mode 3), with associated key derivation for decryption (mode 2)
- Key modes
  - Normal, wrapped and shared key
    - Sharing key to faster AES engine
- AHB5 slave
  - with suspend / resume & DMA support
- Resistant to side channel attacks

Key size	Encryption		Decryption	
	ECB	CBC	ECB	CBC
128b	528		528 [+200] (*)	
256b	743		743 [+324] (*)	

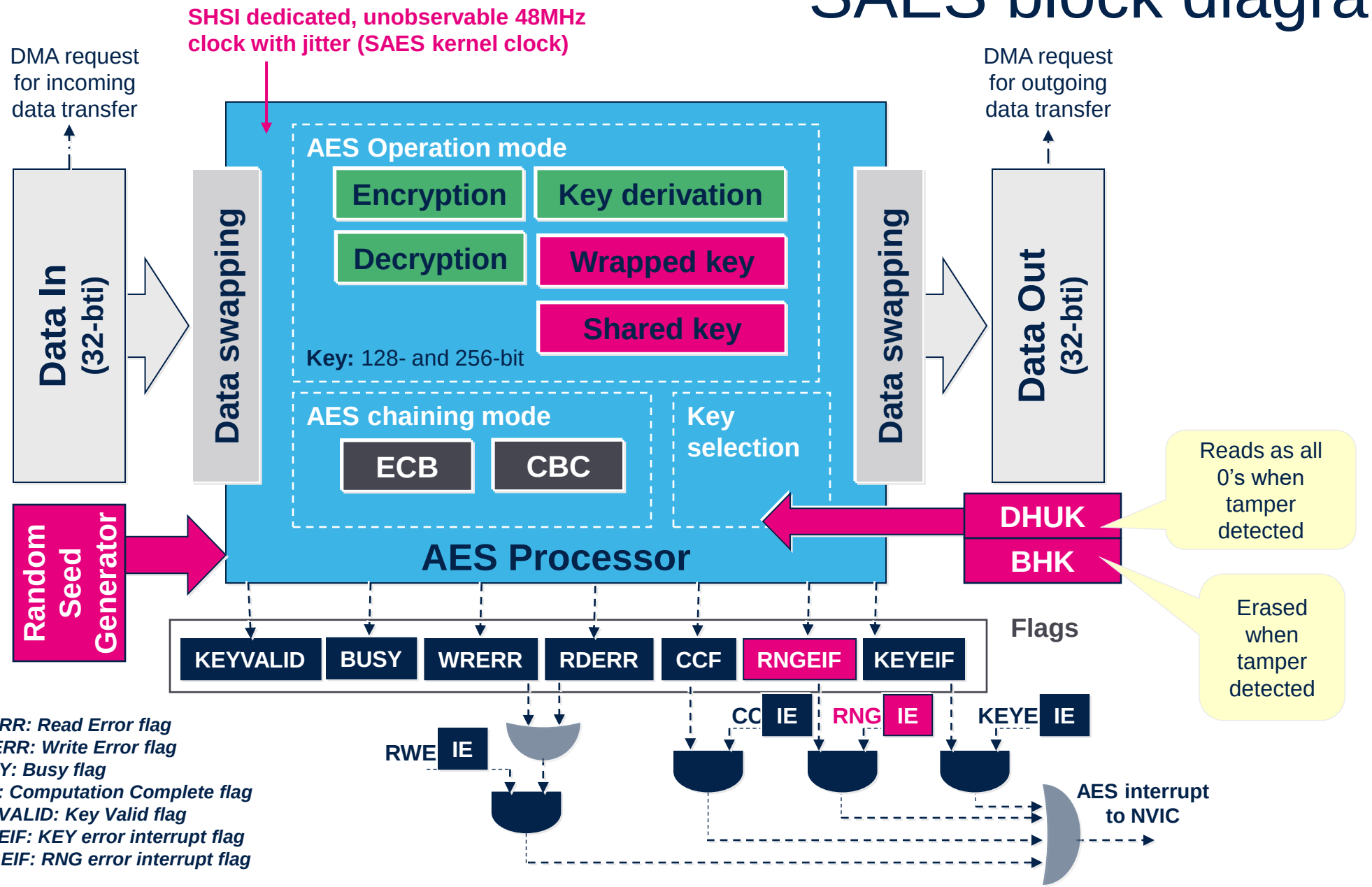
(*) For decryption you must add key derivation time, once

Number of cycles required to process a 128-bit block
Clock frequency = 48MHz unobservable clock (SHSI)

life.augmented

New versus AES

SAES block diagram



RDERR: Read Error flag
WRERR: Write Error flag
BUSY: Busy flag
CCF: Computation Complete flag
KEYVALID: Key Valid flag
KEYEIF: KEY error interrupt flag
RNGEIF: RNG error interrupt flag

(*) DPA resistant

life.augmented

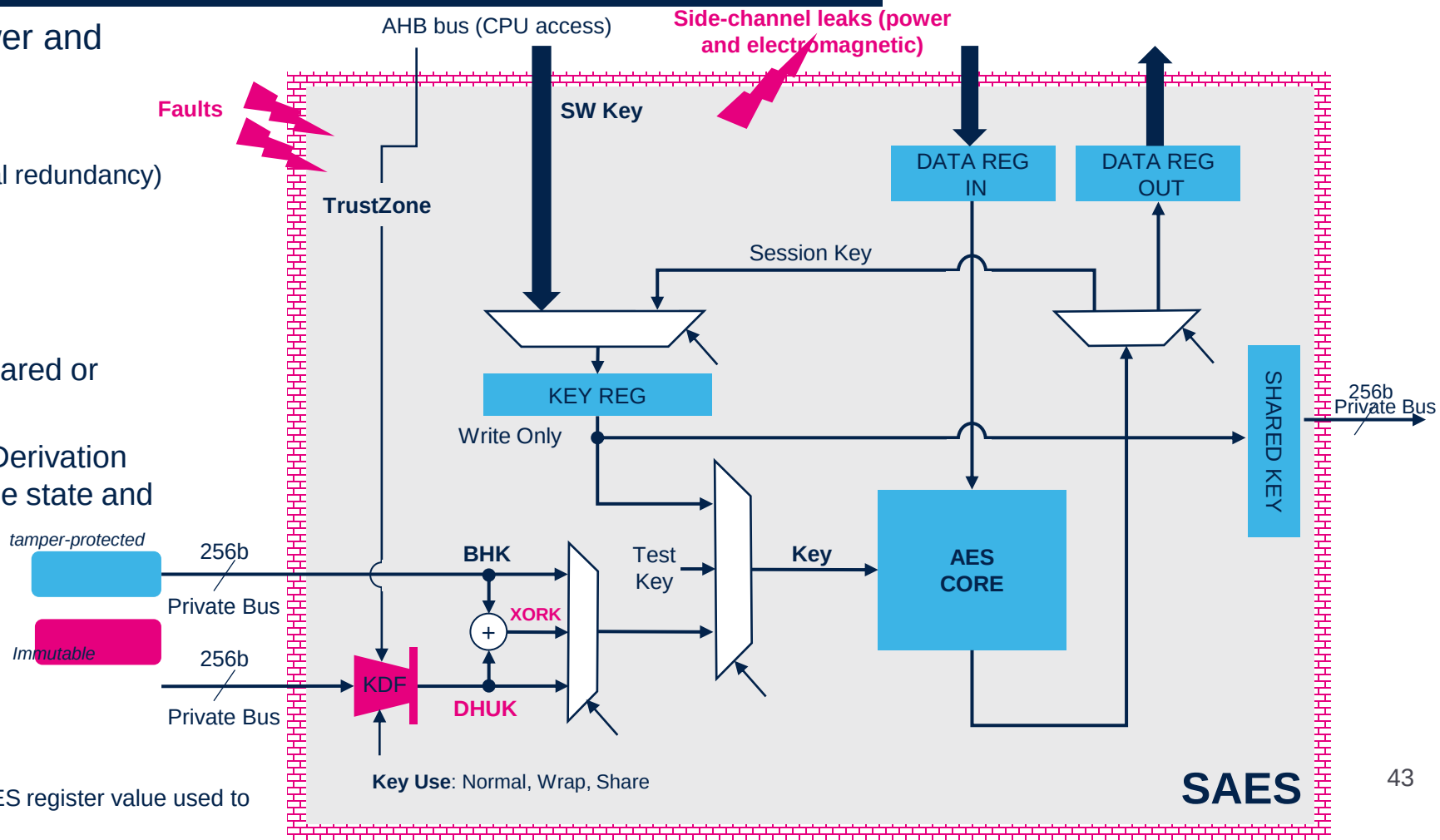
Secure AES peripheral

Detailed key management features

- Counter measures against 1st order power and electromagnetic side-channel attacks.
  - Mitigations against 2nd order side-channel attacks
  - Counter measures against fault analysis (temporal redundancy)

- Five key inputs:
  1) SW Key from CPU
  2) HW protected Session Key (decrypted Shared or Wrapped key)
  3) Derived hardware key (DHUK). The Key Derivation Function (KDF) uses RHUK, the TrustZone state and the Key Use state (KMOD)
  4) Tamper protected Boot HW Key (BHK)
  5) XORK - XOR of BHK and DHUK

- Key sharing with faster, non-DPA AES engine

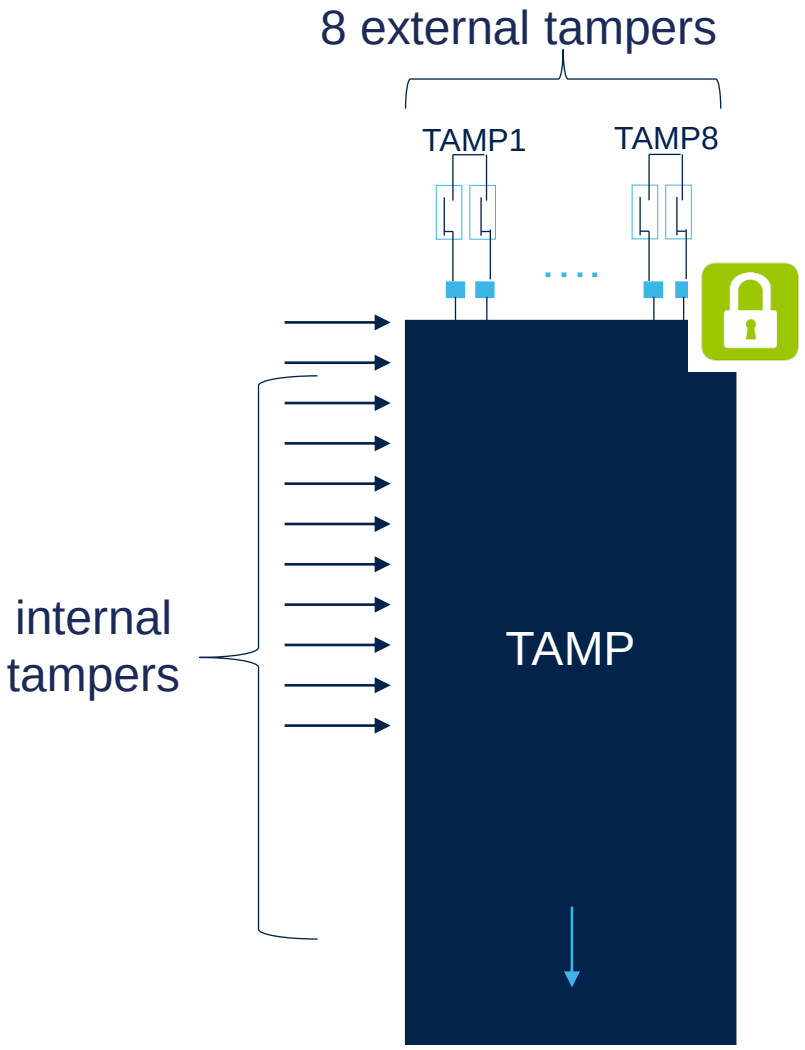


Note: KMOD – is SAES register value used to select the Key Usage

Enhanced anti-tamper

life.augmented

Tamper overview



Erase backup registers and other device secrets

- 128 bytes of backup registers, retained in all low-power modes and VBAT, erased on tamper detection
- 8 external tamper events, active or passive
- 11 internal monitoring tamper events
- Monotonic counter
- Fully securable with TrustZone and privilege access filtering, 3 protection zones in backup registers

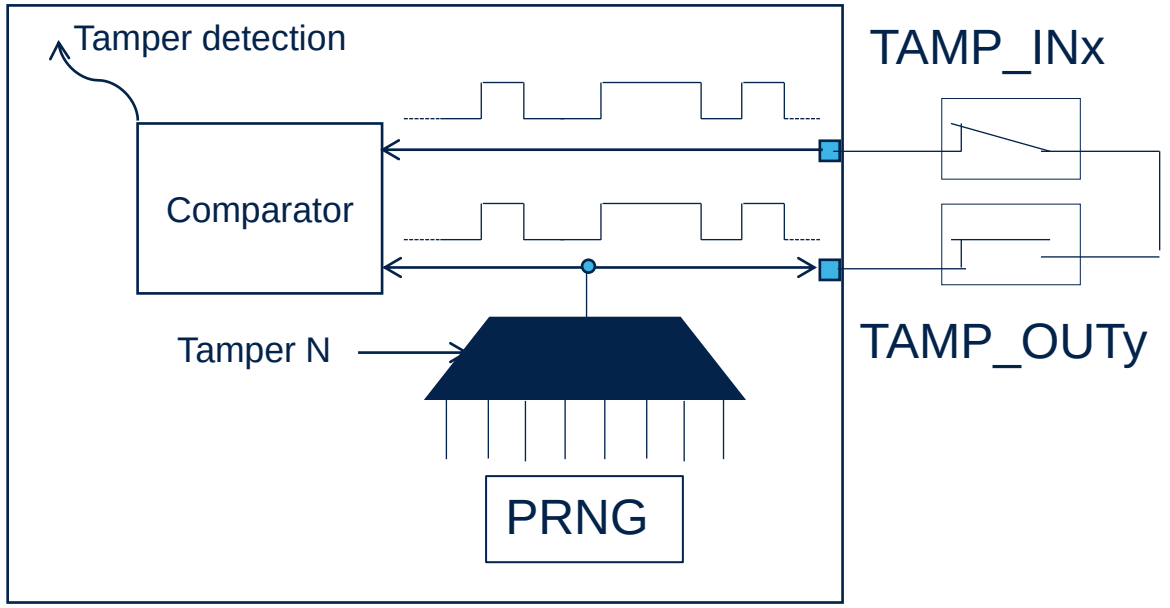
Application benefits

- Protection against physical attacks robustness with active tampers allowing short or open detection
- Protection against environmental perturbation attacks
- Anti-rollback protection with monotonic counter
- Configurable frequency for fast detection time/low-power compromise

Tampers list

Protection against physical attacks

- 8 tamper I/Os, available in all low power modes and in VBAT modes
  - 8 TAMP_IN, 8 TAMP_OUT
  - 4 independent meshes, up to 7 meshes if one output used for several inputs
  - Programmable detection time
  - Digital filtering:
    - 2 comparisons false, in 4 consecutive comparison samples



Our technology starts with You

Find out more at www.st.com

life.augmented