life.augmented

STM32U5介绍

STM32中国团队

Agenda

1 STM32U5 VS STM32L5

2 系统架构

3 Flash

4 RAMCFG

5 系统时钟

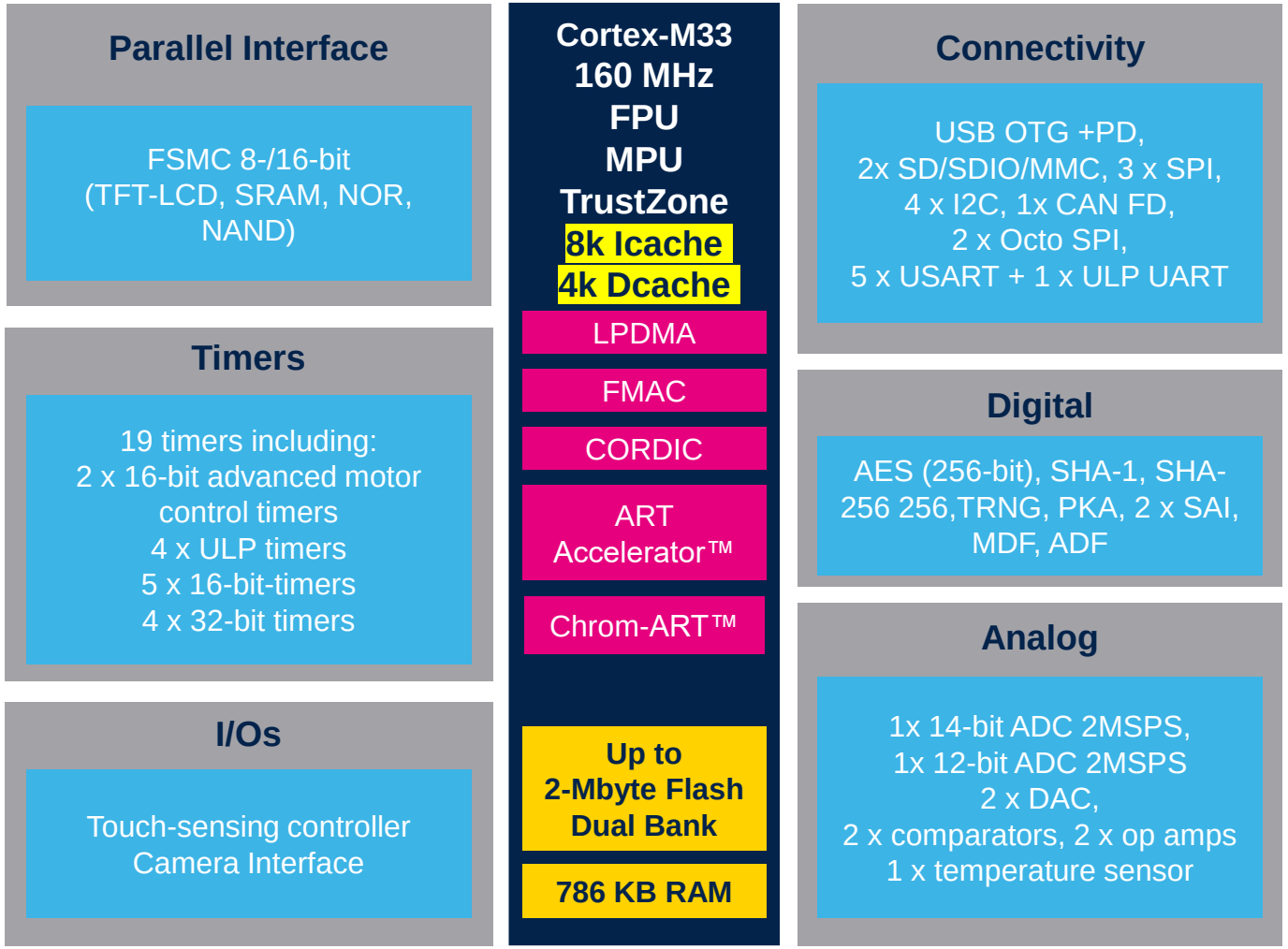
6 DMA

7 电源管理和低功耗

8 信息安全

life.augmented

丰富片上资源



集成丰富外设资源

先进的运算加速设计

充足的片上存储空间

STM32U5 VS STM32L5

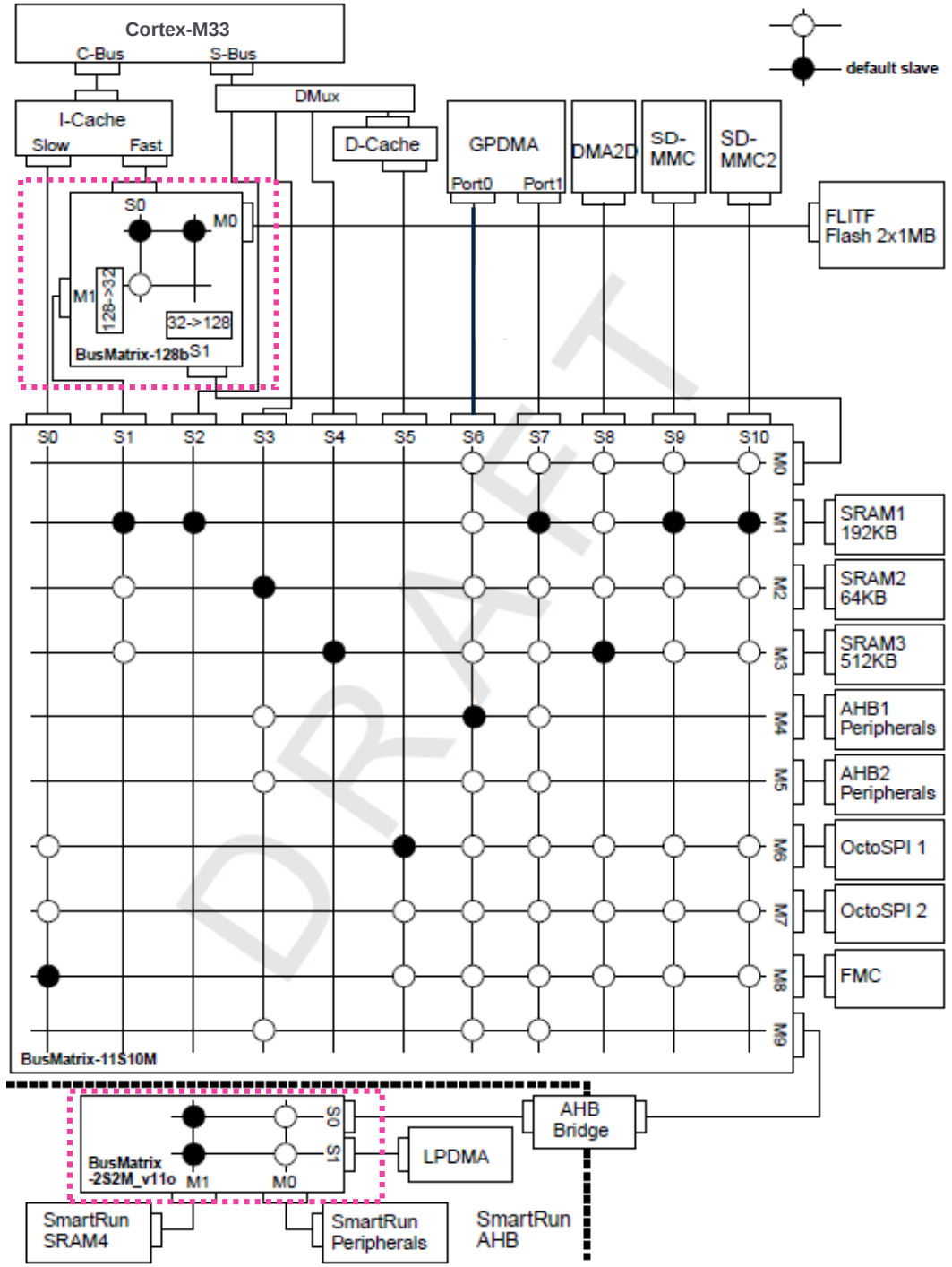
STM32U5 *VS* STM32L5

	STM32U5	STM32L5
存储	Flash: 2MB dual bank(4MB coming soon) SRAM: 786KB(2M+ coming soon)	Flash: up to 512KB, single or dual bank SRAM: 256KB
Caches	ICACHE: 8KB +DCACHE:4KB	ICACHE: 8KB
供电方案	LDO, SMPS(U5不再支持外置SMPS方案)	LDO, SMPS, ext. SMPS
ADC	1 x 14-bit 2 Msps + 1 x 12-bit 2.5 Msps	2 x 12-bit ADC 5Msps
USB	1 x USB OTG 全速 device/**host/OTG** +1 x UCPD	1 x USB 全速 device +1 x UCPD
信号处理	MDF+ADF	DFSDM
Octo-SPI	2 x Octo-SPI +OCTOSPIM(OCTOSPI I/O 管理器)	1 x Octo-SPI
DMA	Normal mode, Link mode	Normal mode
新外设	CORDIC, FMAC	NA
信息安全	TrustZone + 增强的安全密钥存储+SAES,PKA可防侧信道攻击, OTFDEC	TrustZone + AES,PKA,OTFDEC

life.augmented

总线架构

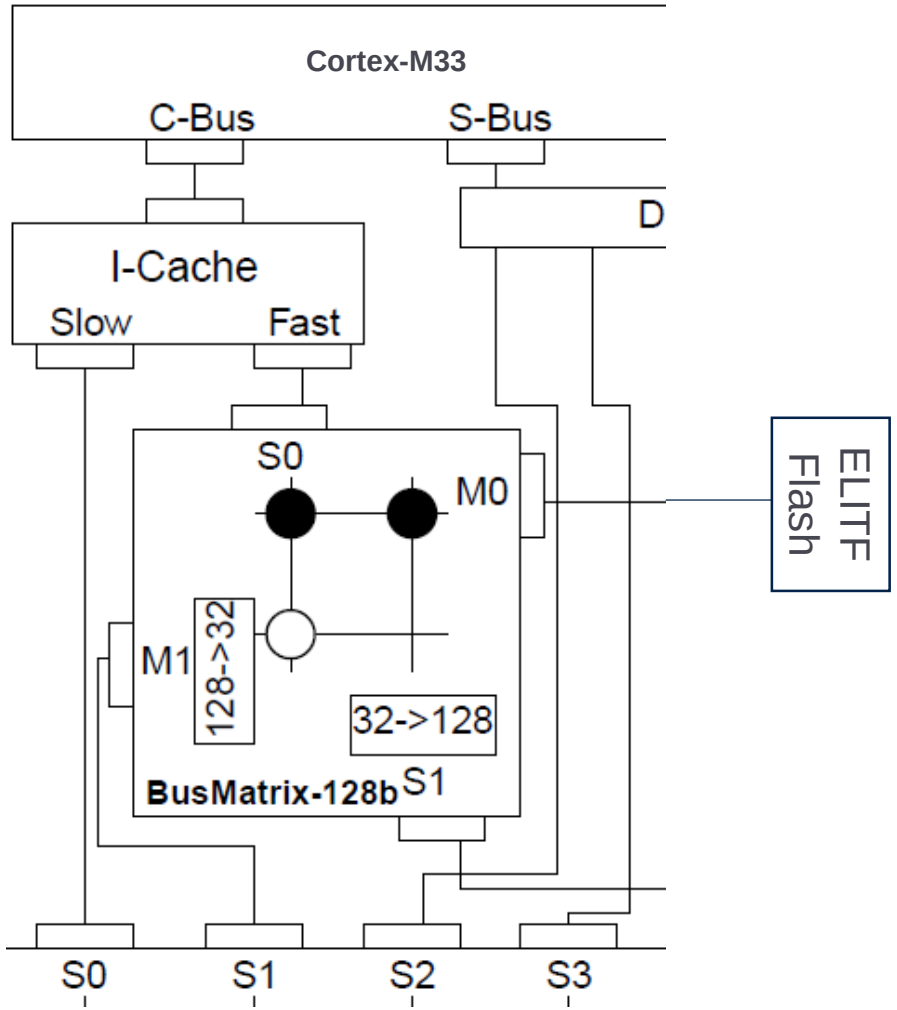
总线矩阵概览



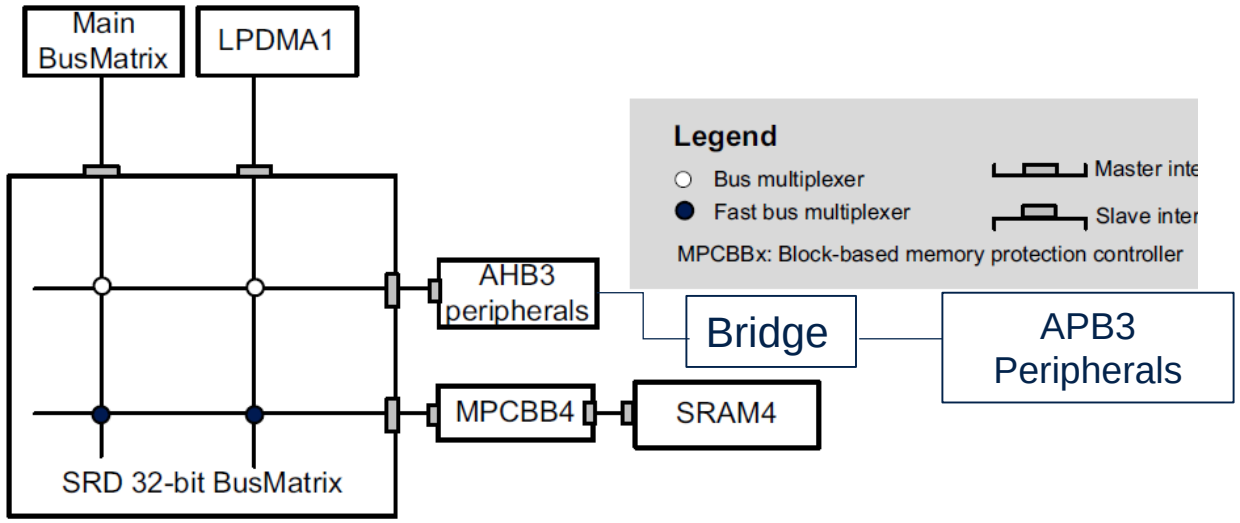
- 主总线矩阵:
  - 32位的多AHB总线矩阵
  - 11个AHB从接口 (S0~10) + 10个AHB主接口 (M0~9)
  - 挂着9个主设备+10个从设备
- Cache 可重填总线矩阵
  - 128位总线矩阵
  - 2个(M0+S0)128位的AHB接口和2个(M1+S1)32位的AHB接口
- SRD 总线矩阵:
  - 32位总线矩阵
  - 2个AHB从接口(S0~1) + 2个AHB主接口(M0~1)

128位总线矩阵

- 128位的 2x2 内联矩阵:
  - 1 个从接口 (S0) 和 1 个主接口 (M0) 是128位AHB总线
  - 1 个从接口 (S1) 和 1 个主接口 (M1) 是32位AHB总线
- **128位** S0 连接到128位的I-Cache快速总线上
- **128位** M0 连接到128位的Flash接口上
- **32位** M1 连接到主总线矩阵上:
  - 使I-Cache的快速总线可以访问内部SRAM(1~3)
- **32-bit** S1 连接到主总线矩阵上:
  - 使得GPDMA, SDMMC 和 DMA2D 可以访问Flash.
- 向下位宽转换器 (M1) 和 向上位宽转换器 (S1):
  - 使得128位到32位消息格式转换,或者反过来转换也可以.



智能运行域(SRD)总线矩阵



- GPDMA 仅在CPU域内可用(当系统时钟可用时).
- 当系统时钟存在时, GPDMA 可以访问所有SRD从设备
- LPDMA 仅可访问SRAM4和AHB3/APB3外设

- 依靠DMA在低功耗模式下的自主运行特性:
  - LPDMA最低可达到stop 2模式
- 一个32位的ABH总线矩阵连接了:
  - 2个主节点:
    - 主AHB总线矩阵
    - LPDMA1 (低功耗DMA, 拥有一个主端口)
  - 2 个从节点:
    - AHB3外设包含AHB-APB转换桥并连接APB3
    - 内部SRAM4 (16 Kbytes)

life.augmented

Flash

New versus STM32L5

FLASH 特性

- 最高2M Flash(U575/585), 带ECC校验, 双bank, 支持 RWW (Read-While-Write)
  - 每页8 K
  - 128位宽的数据读
  - 所有FLASH存储空间支持10K次的擦写周期, 512 K 的空间内支持100K次
- 512 bytes OTP
- 预取指
- 支持Bank交换功能(bank swapping)
- 改进的设备生命周期管理 (参考信息安全部分,主要是指RDP)

life.augmented

FLASH 耐久度

对于所有flash 10 K次 耐久度

每个bank上256K(32页)具有100K次的耐久度

可以选择任意页使其支持到100K次的耐久度

由软件负责每个bank上支持100K次的FLASH区域,不超过256K

life.augmented

FLASH 读访问等待延时

Wait states (latency)	HCLK max (MHz) (当LPM = 0时)			
	VCORE Range 1	VCORE Range 2	VCORE Range 3	VCORE Range 4
0 WS (1 CPU cycle)	32	25	12,5	8
1 WS (2 CPU cycles)	64	50	25	16
2 WS (3 CPU cycles)	96	75	37,5	24
3 WS (4 CPU cycles)	128	100	50	-
4 WS (5 CPU cycles)	160	-	-	-

当LPM=1时:

- Range 1/2/3 : WS ≥ HCLK (MHz) / 10 -1
- Range 4: 与LPM=0时相同

life.augmented

FLASH 预取指

- CM33 通过C-Bus和I-Cache来取指和取数据(常量/数据)
  - 使能I-Cache可以增加C-Bus访问效率,减少缓存重填的延时.
- 当访问连续代码时,预取指是非常有用的:
  - 当前指令正在填入指令缓存和正在被CPU执行时,允许下一条连续指令线被提前从FLASH中读取
- 由于额外的FLASH访问, 预取指可以增加代码执行效率.
- 但会影响功耗

FLASH 低功耗模式

- Bank power-down模式: 每个BANK可节约~40µA
  - 访问正处于power-down模式下的flash, 将自动唤醒对应的bank.
  - 唤醒bank时将至少花费5 µs的时间代价.
- Sleep模式下的Flash power-down: 节省 80µA, 但需要更长的唤醒时间
- Flash LPM模式(低功耗模式): 节省 45µA, 但更高的读访问延时

RAMCFG

RAM 配置概述

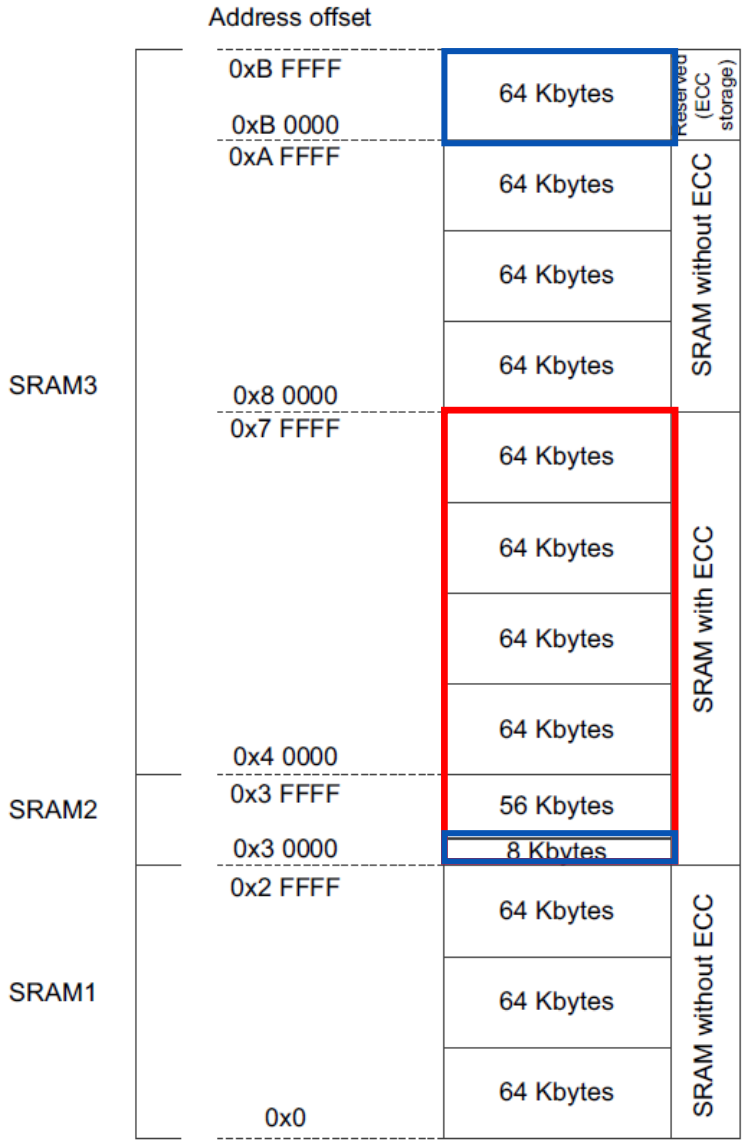
- 错误码纠正ECC(SRAM2/3 & BKPSRAM带ECC功能)
- SRAM-ECC功能软件通过key来关闭
- SRAM 软件擦除也需要key
- SRAM2写保护 (粒度为1K)
- 在VOS Range4时提供可编程的等待延时

SRAM 特性

X = 此特性支持	SRAM1 (192 Kb)	SRAM2 (64 Kb)	SRAM3 (512 Kb)	SRAM4 (16 Kb)	BKPSRAM (2 Kb)
Stop 0/1模式下的 LPBAM模式	X	X	X	X	X
Stop2下的LPBAM模式	-	-	-	X	-
Standby模式下可选的内容保留	-	X	-	-	X
VBAT模式下可选的内容保留	-	-	-	-	X
RDP回退时内容擦除	X	X	X	X	X
检测到入侵事件时内容擦除	-	X	-	-	X
系统复位时可选的内容擦除	X	X	X	X	-
软件擦除	X	X	X	X	X
ECC	-	X	X	-	X
写保护	-	X	-	-	-
等待延时	X	X	X	X	X

SRAM1/2/3 带ECC时的存储映射

- ECC 保存位置:
  - SRAM3: 64 K区域, 高地址区间
  - SRAM2: 8 K区域, 位于SRAM2最低地址区间
- SRAM3 ECC 的管理:
  - 当ECC使能时,只有前256K字节才带ECC功能.
  - 剩下的192K字节不带ECC功能
  - 最后一个block(64K)存储ECC, 因此不能给应用使用
- ECC
  - SEDC: 单个错误检测并纠正 (产生中断)
  - DED: 两个错误检测 (产生中断 或者 NMI)



通过软件打开/关闭ECC功能

- RAM ECC通过选项字节使能,在系统复位后寄存器位ECCE位会自动设置
- 软件可以通过执行一软件序列来关闭ECC:
  - 这有助于检查ECC对应用程序的影响
- 当ECC关闭时(ECCE = 0), SRAM3 ECC 保存区域用户可用来做ECC读写测试
- 当ECC打开时(ECCE = 1),此区域为预留区,用来保存ECC数据, 不可读写

写保护(SRAM2)

- SRAM2具有64个页,每页1K大小
- 每个1K的页可各自设置写保护
- 通过寄存器*RAMCFG_RAM2WPR1* 和 *RAMCFG_RAM2WPR2* 的 PxWP (x = 0 to 63) 位来打开写保护.

软件擦除

- 可通过执行一软件序列来请求SRAM 擦除
- 如果当前正在擦除, 此时若读/写相同地址的SRAM, 那么等待状态(AHB时钟周期)将会自动插入到AHB总线上, 直到擦除结束
- 总擦除耗时:

  N 个AHB 时钟周期, N=SRAM的大小(以word为单位)

- 注: 在擦除时是不可能访问RAM的:
  - 在擦除期间,SRAM的中断状态寄存器的SRAMBUSY标志位被置位
  - 访问被阻塞
  - 等待状态插入到AHB总线上,直到擦除结束

RAMCFG 中断

- 中断:
  - SEDC 带中断产生
  - DED 带中断或者NMI产生
  - SEDC 和 DED 状态
  - 错误地址锁存到寄存器中

	中断事件	可导致退出 Sleep mode	可导致退出 Stop mode	可导致退出 Standby modes
RAMCFG	ECC 检测到单个错误检测并纠正	Yes	Yes (Stop 0/1)	No
	ECC 检测到两个错误	Yes	Yes	No
NMI	ECC 检测到两个错误	Yes	Yes	No

life.augmented

系统时钟

主要特性

6个内部时钟源

HSI16

MSIS 和 MSIK

LSI

HSI48

专用于SAES的安全高速48MHz的SHSI

2个外部振荡器

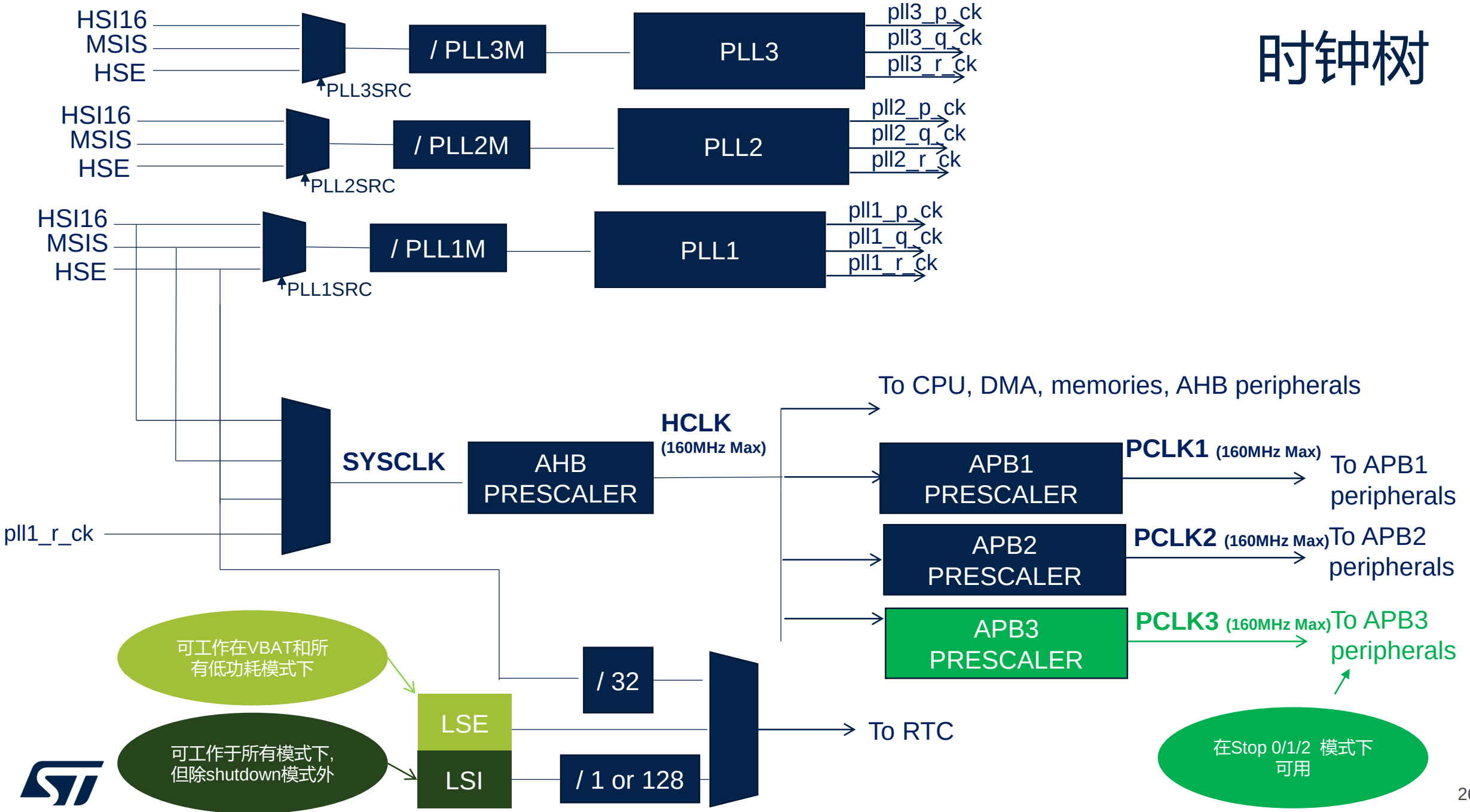
4~50MHz的HSE带CSS

32.768KHz的LSE,带 CSS

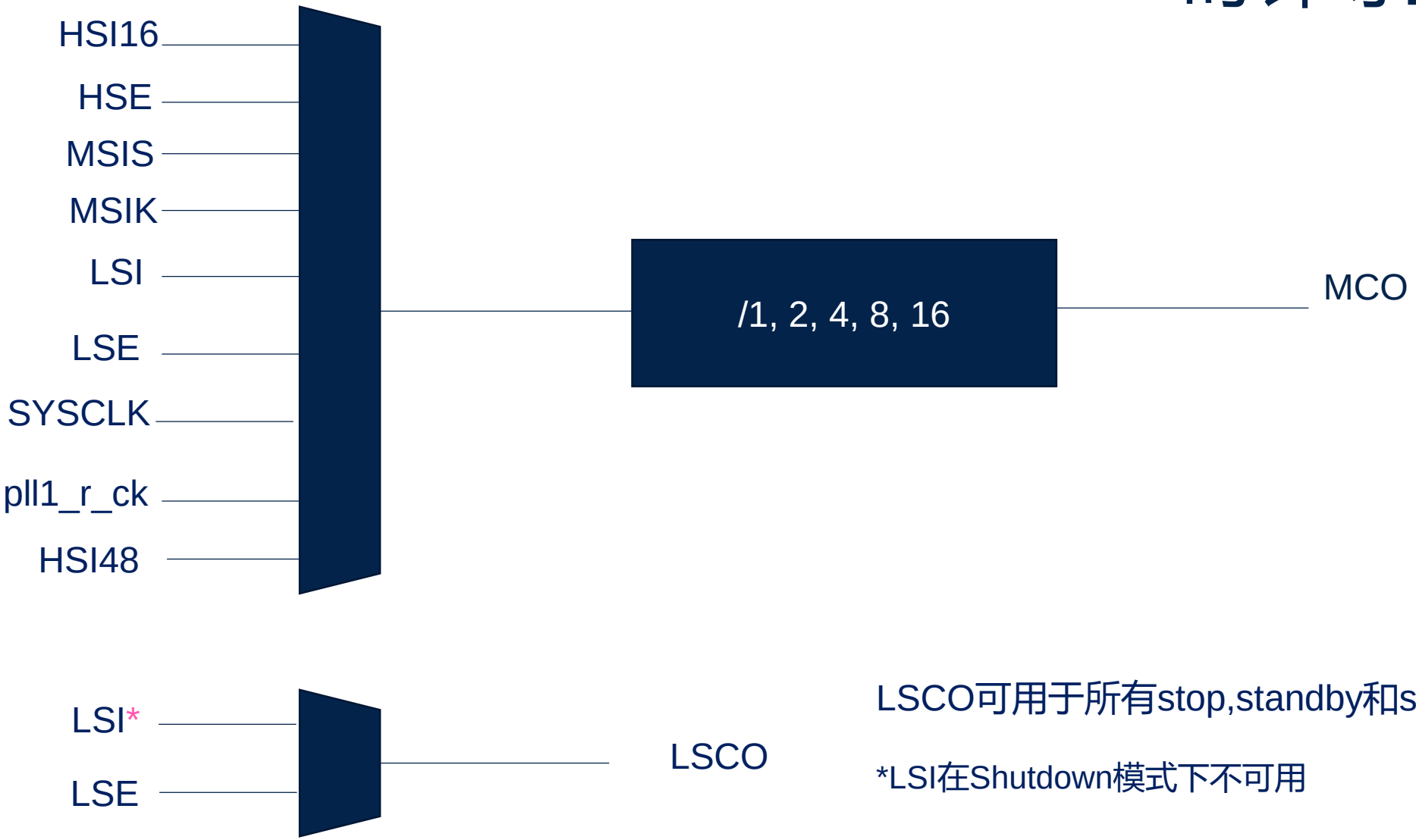
3个 PLL, 每个都带三路输出

life.augmented

时钟树


HSI16
MSIS
HSE
PLL3SRC
/ PLL3M
PLL3
pll3_p_ck
pll3_q_ck
pll3_r_ck
HSI16
MSIS
HSE
PLL2SRC
/ PLL2M
PLL2
pll2_p_ck
pll2_q_ck
pll2_r_ck
HSI16
MSIS
HSE
PLL1SRC
/ PLL1M
PLL1
pll1_p_ck
pll1_q_ck
pll1_r_ck
pll1_r_ck
SYSCLK
AHB PRESCALER
HCLK (160MHz Max)
To CPU, DMA, memories, AHB peripherals
APB1 PRESCALER
PCLK1 (160MHz Max)
To APB1 peripherals
APB2 PRESCALER
PCLK2 (160MHz Max)
To APB2 peripherals
APB3 PRESCALER
PCLK3 (160MHz Max)
To APB3 peripherals
可工作在VBAT和所有低功耗模式下
可工作于所有模式下，但除shutdown模式外
LSE
LSI
/ 32
/ 1 or 128
To RTC
在Stop 0/1/2 模式下可用

时钟导出能力



LSCO可用于所有stop,standby和shutdown*模式下

*LSI在Shutdown模式下不可用

LSI输出要么32KHz,要么250Hz, 最决于RCC_BDCR的LSIPREDIV配置

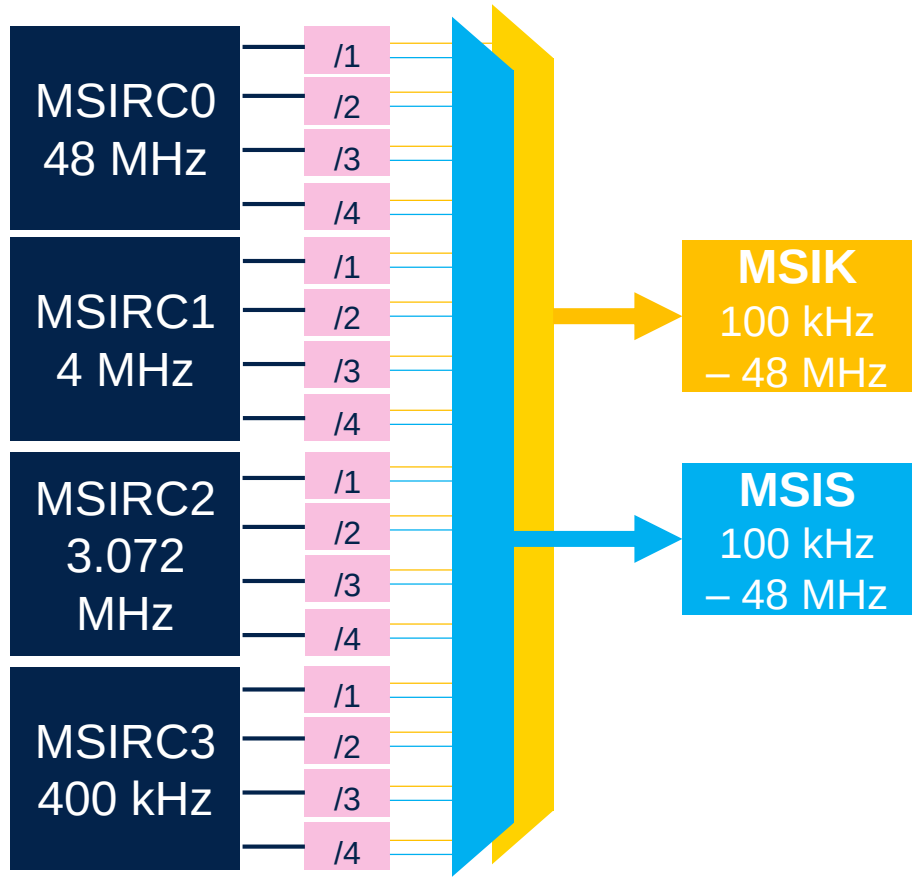
HSE, HSI16, HSI48, SHSI,LSI

- **HSE** 4 ~ 50 MHz. CSS 带自动切换到HSI功能.
- **HSI16**: 16 MHz 内部RC 带用户修正功能.
  可用于从stop模式下唤醒时作为时钟源,或在Stop 0,1,2 模式下作为时钟源 (RCC_CFGR1.STOPWUCK=1)
- **HSI48**: 48 MHz 振荡器用于USB (OTG_FS with CRS), SDMMC 和 RNG
  当Range 4时, 可选的2分频用于RNG
- **SHSI** 是SAES专用内核时钟, 48 MHz +/- 15% 误差
- **LSI**: 32kHz 或 250kHz, 通过RCC_BDCR. LSIPREDIV选择
  可用于除shutdown模式之外的所有模式, 和VBAT模式

life.augmented

MSI (MSIK 和 MSIS) – 概述

- 16 档频率从100 kHz ~ 48 MHz
  - MSI由4个 RC振荡器组成
  - 每一个MSIRCx带着一个分频器,其分频系数可为1, 2, 3 或 4.
  - 3.072MHz RC 用于音频方面
  - 每一个MSIRCx有用户修正码
- 2个时钟输出
  - **MSIS**, 可用于系统时钟
  - **MSIK**, 可用于一些外设的IP时钟.
  - MSIS 和 MSIK 相互独立, 通过RCC_ICSCR1. MSISRANGE/MSIKRANGE 来配置



MSI (MSIK 和 MSIS) vs. MCU 低功耗模式

- 复位后的系统时钟,从standby/shutdown模式下唤醒后的系统时钟.
  - 复位或从shutdown模式退出后, MSIS 和 MSIK = 4 MHz.
  - MSIS 和 MSIK在standby唤醒后的频率可通过软件配置,配置范围为1 ~ 4 MHz.
- MSI可用于从stop唤醒后的系统时钟,最高可配置到24 MHz, 也可用于stop 0,1,2模式下的时钟源 (RCC_CFGR1.STOPWUCK=0)
- MSI的工作模式:
  - 当RCC_ICSCR1.MSIBIAS=1 ,内核电压处于range 4 且工作于低功耗时, MSI工作为**采样模式** (sampled mode),此时功耗更低但精度也更低
  - MSI工作于**连续模式**(continuous mode):
    - Range 1,2,3时或
    - Range 4 且 低功耗模式时, 但RCC_ICSCR1.MSIBIAS=0

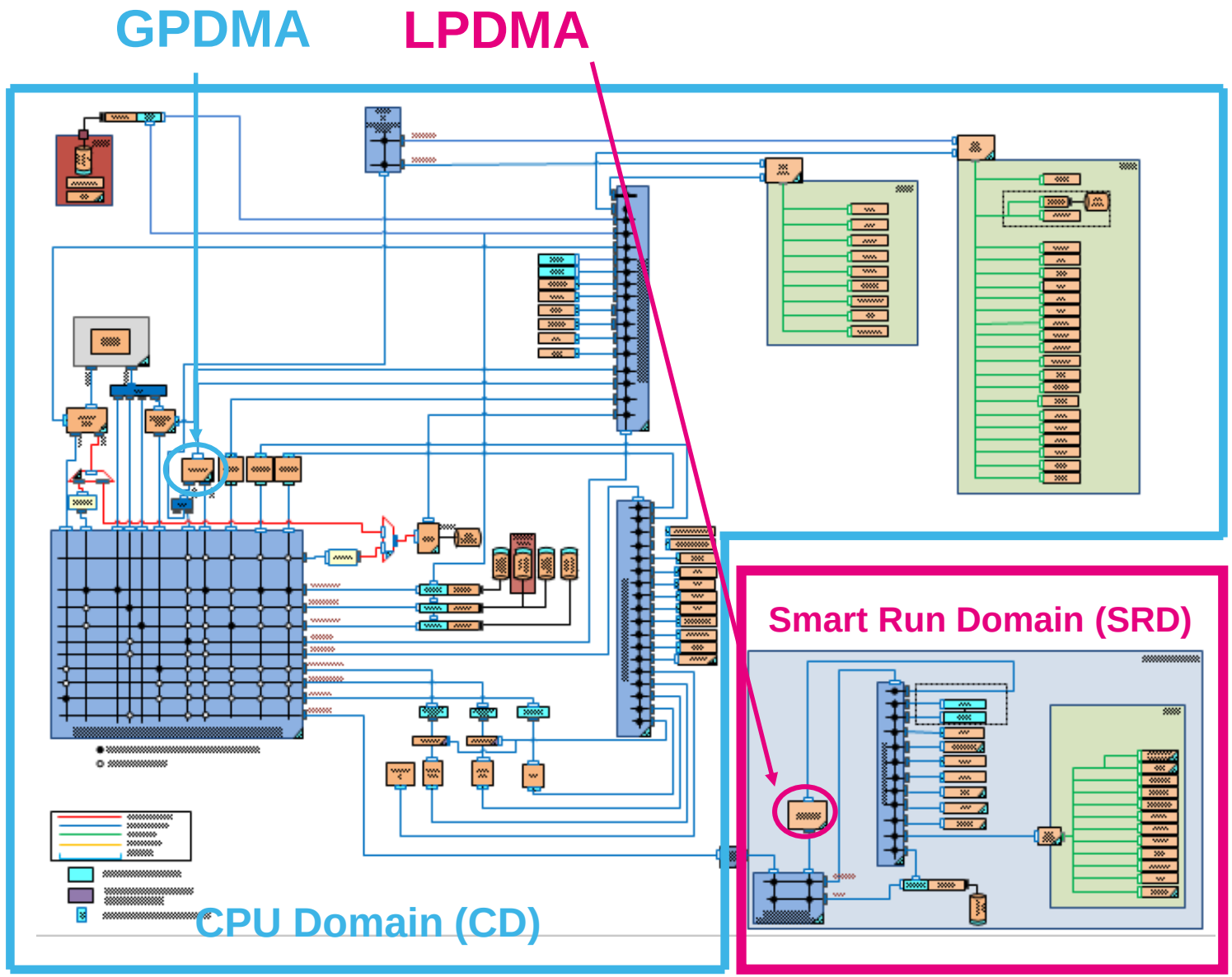
时钟频率

内核电压范围	SYSCLK	MSIK/MSIS	HSI16	HSI48	SHSI	HSE	PLL outputs (VCO max)
1	160 MHz	All ranges	Allowed	Allowed	Allowed	50 MHz	208 MHz* (128 to 544 MHz)
2	100 MHz	All ranges	Allowed	Allowed	Allowed	50 MHz	100 MHz (128 to 544 MHz)
3	50 MHz	All ranges	Allowed	Allowed	Allowed	50 MHz	50 MHz (128 to 330 MHz)
4	24 MHz	Up to 24 MHz	Allowed	Allowed (divided by 2)	Allowed (divided by 2)	24 MHz	Not allowed

* 200 MHz OCTOSPI kernel clock allowed

DMA

系统架构 & DMA 概述



给应用带来的好处

用于从存储源地址到目标地址的数据传输,无需CPU参与

- 新的DMA IP(*vs* L5)
  - 统一的DMA驱动程序
  - 2个硬件实体
    - GPDMA
    - LPDMA
  - 基于链表的编程
  - 集成了DMAMUX特性
  - 改进的自主性
    - 拥有时钟请求管理
    - 灵活的通道内和通道间输入/输出控制

DMA 主要特性

- 双向AHB主端口 (LPDMA: 1x, GPDMA: 2x)
- 从源到目标的基于内存映射的数据传输
  - 外设->内存
  - 内存->外设
  - 内存->内存
  - 外设->外设
- 在Sleep和Stop模式下自主数据传输
- 多个DMA通道可同时工作
- 传输仲裁基于4个优先等级的策略
  - 一个预留的最高优先级队列, 用于时间敏感的传输
  - 三个次优先级队列用于加权轮询分配

life.augmented

LPDMA *VS* GPDMA

特性	LPDMA	GPDMA
主端口(s)	1x (32-bit) AHB	2x (32-bit) AHB
DMA 传输	仅Single模式	Single 和 burst 模式
DMA 调度器	直接传输(读完后直接写)	基于FIFO的burst (dual issue)
通道数	4	16
通道FIFO的大小	NA	Ch0-11 (*): 8 字节 (2 个字) Ch12-15 (**): 32 字节 (8 个字)
通道寻址模式	线性 (固定地址或者以连续数据递增)	Ch0-11: 线性 Ch12-15: 2D 寻址
最大请求ID	16	123
最大触发ID	31	56

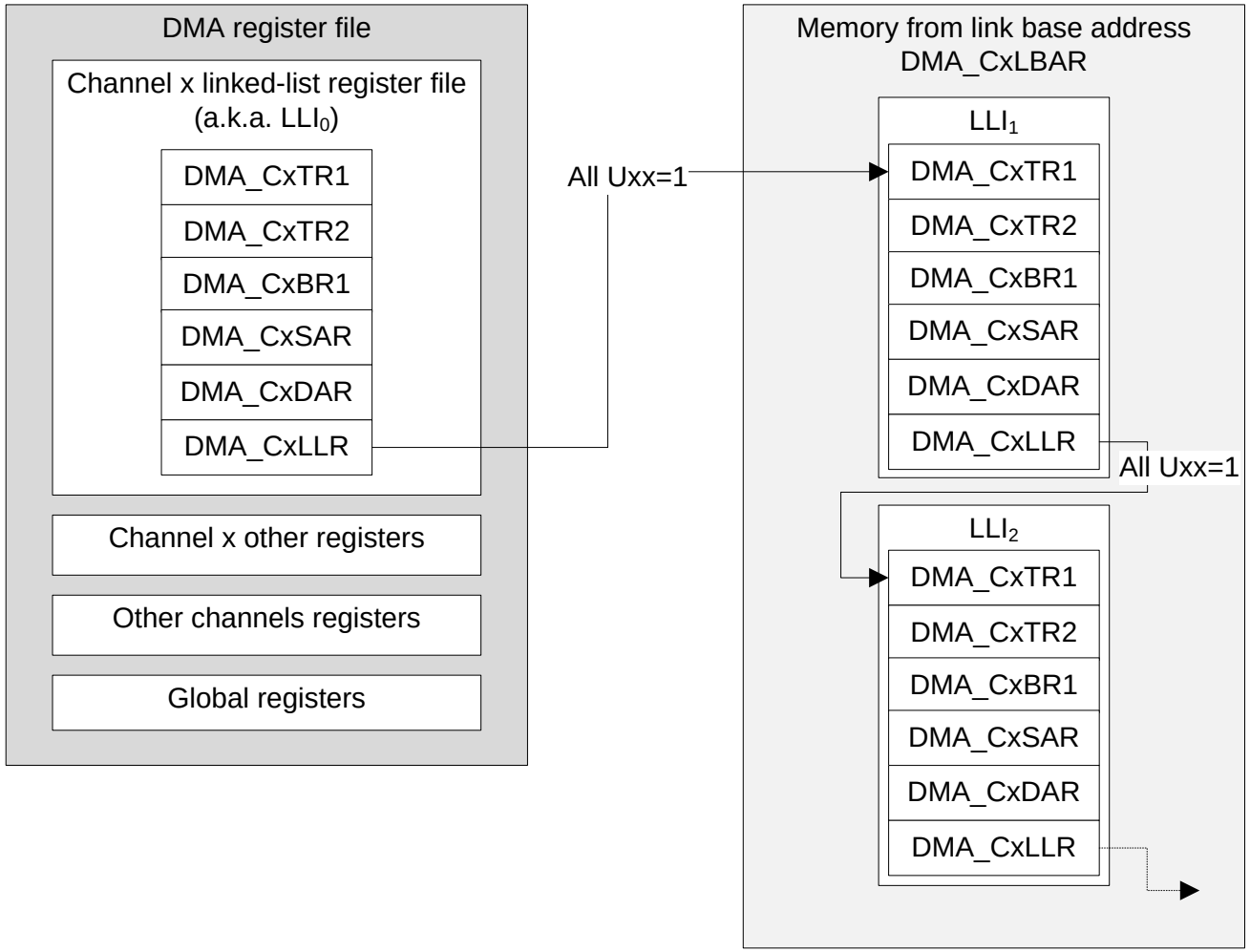
- (*) 这些通道通常用来在APB/AHB外设和SRAM间进行数据传输
- (**) 这些通道也可能用在对数据有要求的AHB外设和SRAM之间的数据传输, 或者与外部存储之间

life.augmented

链表模式

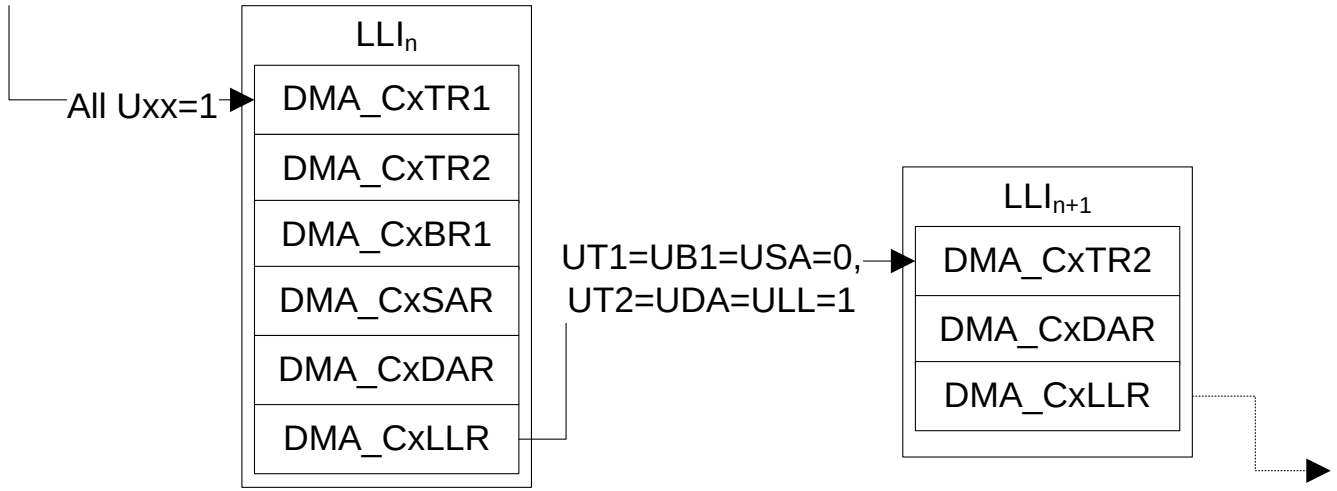
- 纵观直接编程模式, 可为一个通道配置一个传输列表
  - 每个链表节点(又叫 LLI)由它的数据结构来定义.
  - 下一个节点(LLI_{n+1})的数据结构在内存中的基地址是:
    - 64K对齐的静态基地址(i.e. DMA_CxLBAR)
    - 和距离上一节点($_{LLIn}$)的链接地址偏移量(DMA_CxLLR寄存器的LA[15:2]位域
- 下一节点的数据结构自动装载到链表寄存器
- 每个节点的数据结构可以是特定的，并最小化到两个连续节点之间的差异
  - 条件更新位(相对于上一节点有变动): UT1, UT2, UB1, USA, UDA(也可能是 ch12~15的UB2 和 UT3), 由当前DMA_CxLLR表示.

链表数据结构(LP/GP ch0-11)



条件更新 & 压缩的数据结构

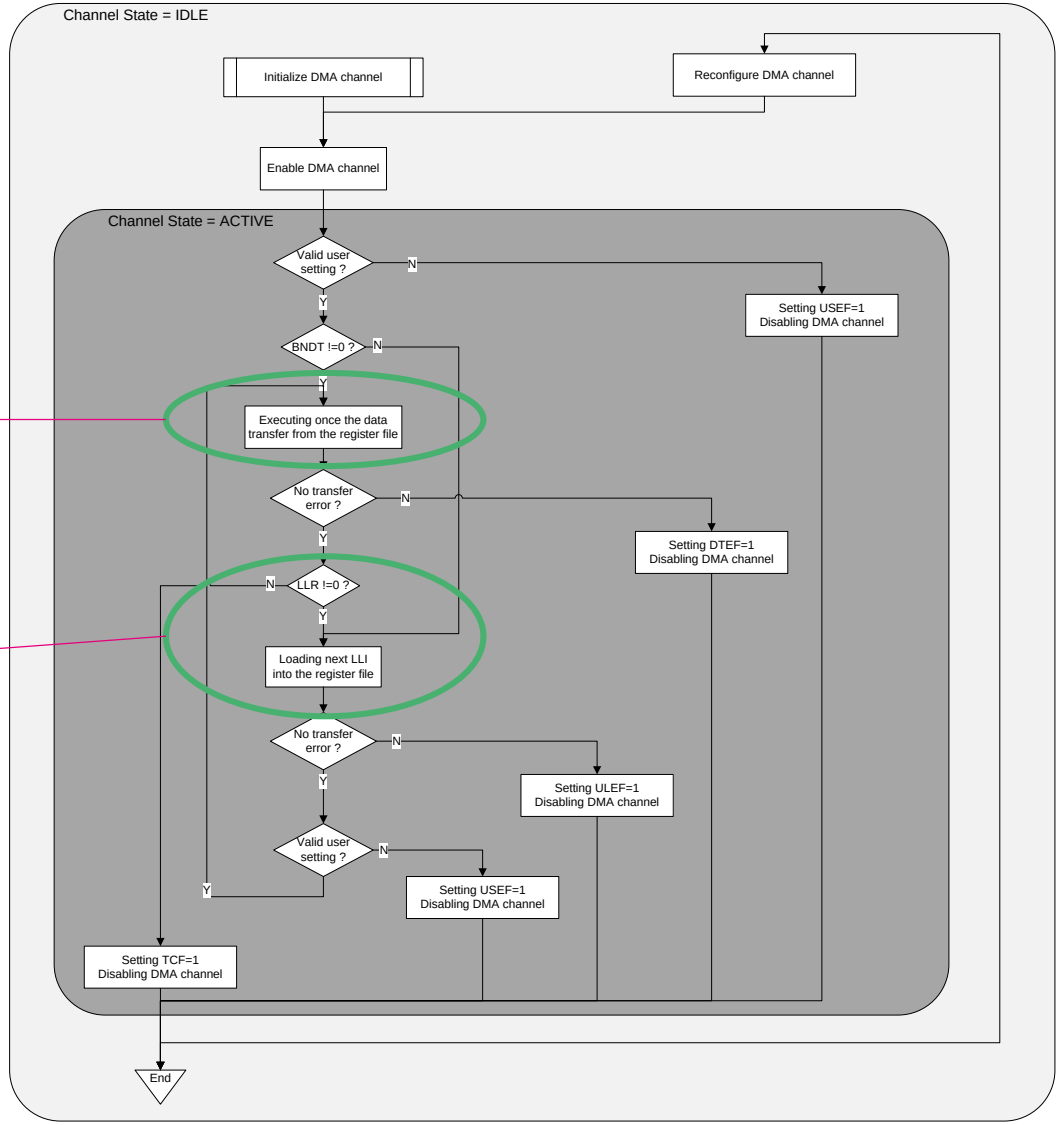
链表数据结构 (LP/GP ch0-11)



ULL表示是否还有下一个节点. 而UT2, UDA=1则表示下一节点的更新内容:TR2和DAR

通道链表模式编程

正常/运行到完成模式(LSM=0)

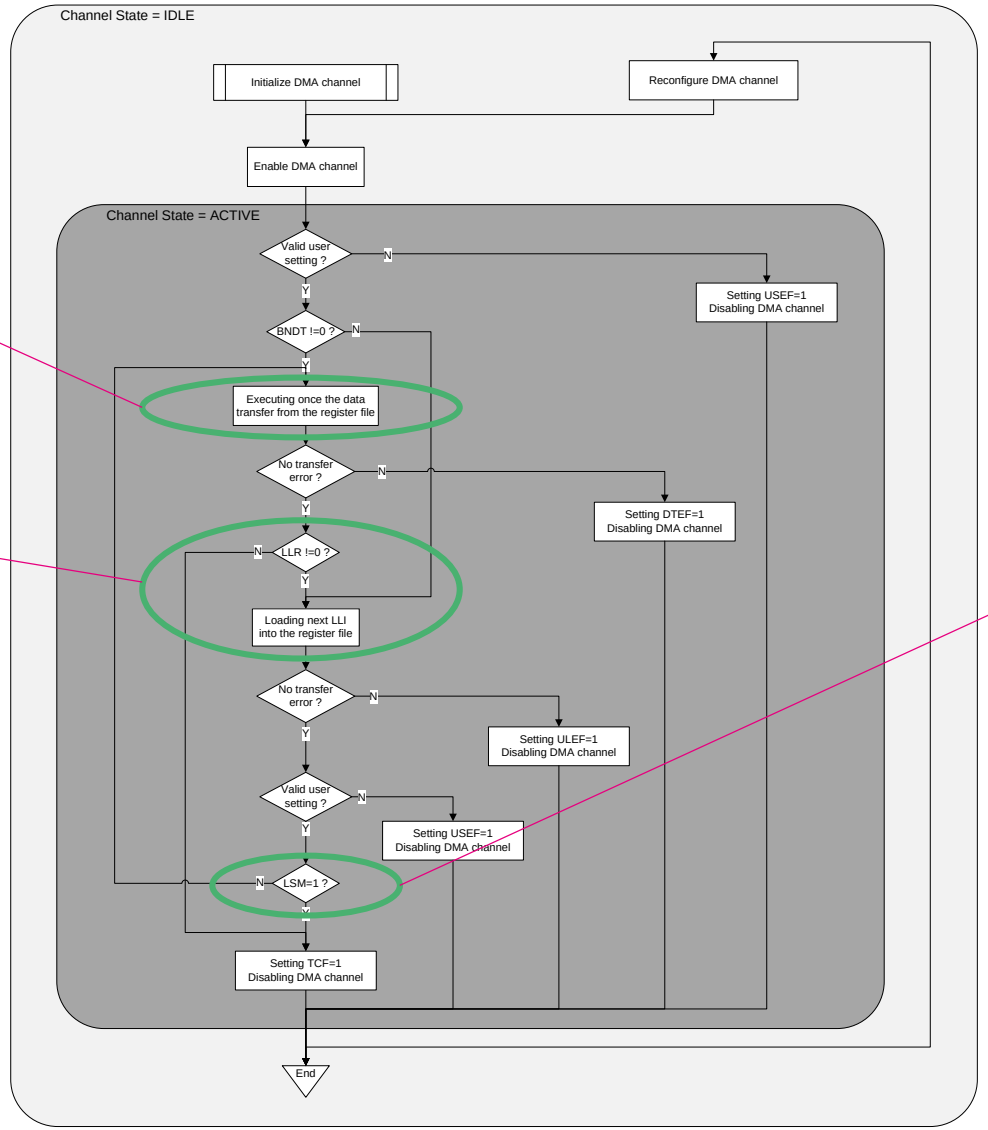


执行数据搬运

装载下一节点

如果没有出现错误, 则一直运行完所有节点.

通道链表模式编程
LSM !=0



执行数据搬运

装载下一节点

LSM表示是否结束标志,
=1时结束, =0时继续执行

由软件来控制

相比较于上一模式, 软件可控制随时中途停止.

自主LP/GPDMA

- DMA精细地管理它自己的时钟门控;在任何工作模式下，只有在立即需要时才向RCC请求其时钟
- 在低功耗模式下,DMA可被编程为:
  - CPU在DMA传输完成时被中断唤醒
  - 自动继续和操作下一个节点(LLI_{n+1})传输

低功耗模式	LPDMA/GPDMA
Sleep	无效果. DMA中断使MCU退出Sleep模式
Stop (*)	当进入到Stop模式时,DMA寄存器的内容保留, 且DMA寄存器的内容可以自动装载下一节点对应数据来更新, 以便实现自动数据传输.DMA中断会使MCU退出Stop模式.
Standby	DMA下电, 且必须在退出Standby模式后重新初始化

(*): GPDMA 可工作在Stop 0 和 Stop1 模式. GPDMA Stop 2模式下已掉电.
而LPDMA可工作在低至stop2模式下.

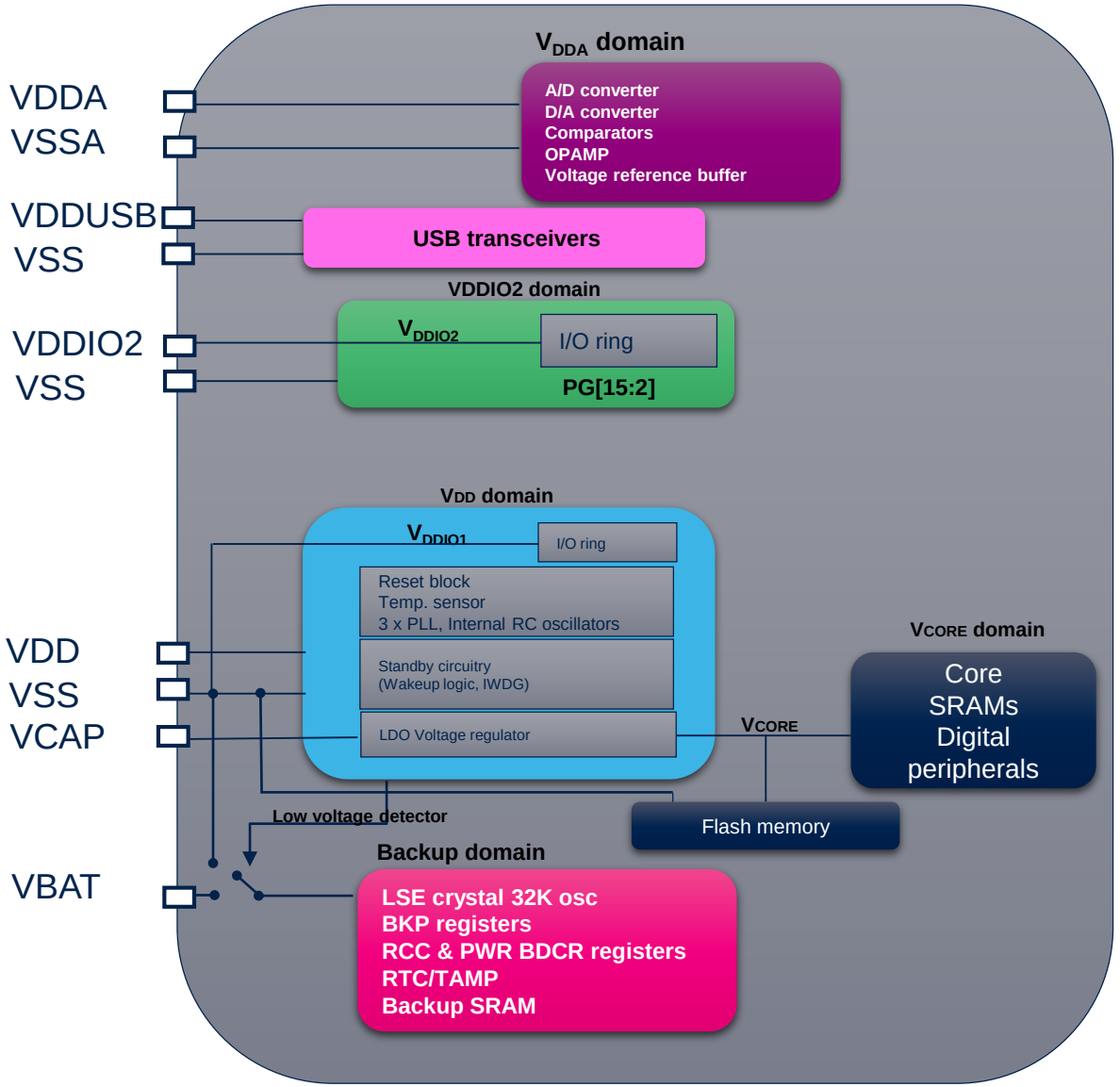
life.augmented

电源管理和低功耗

供电– 传统芯片

STM32U575xxxx 和 STM32U585xxxx

- 内部电压调节器: LDO, 需要外接4.7 µF退耦电容
- 独立供电:
  - VDD = 1,71V (at power-up) ~ 3,6 V, 最低 BOR0 可小到 1.58V
  - VDDA = 1,62 V (ADC, DAC, COMP, OPAMP)/ 1.8V (VREFBUF) ~ 3.6V
  - VDDUSB = 3 V ~ 3,6 V
  - VDDIO2 = 1,08 V ~ 3,6 V
  - VBAT = 1,58 V (BOR min) ~ 3,6 V

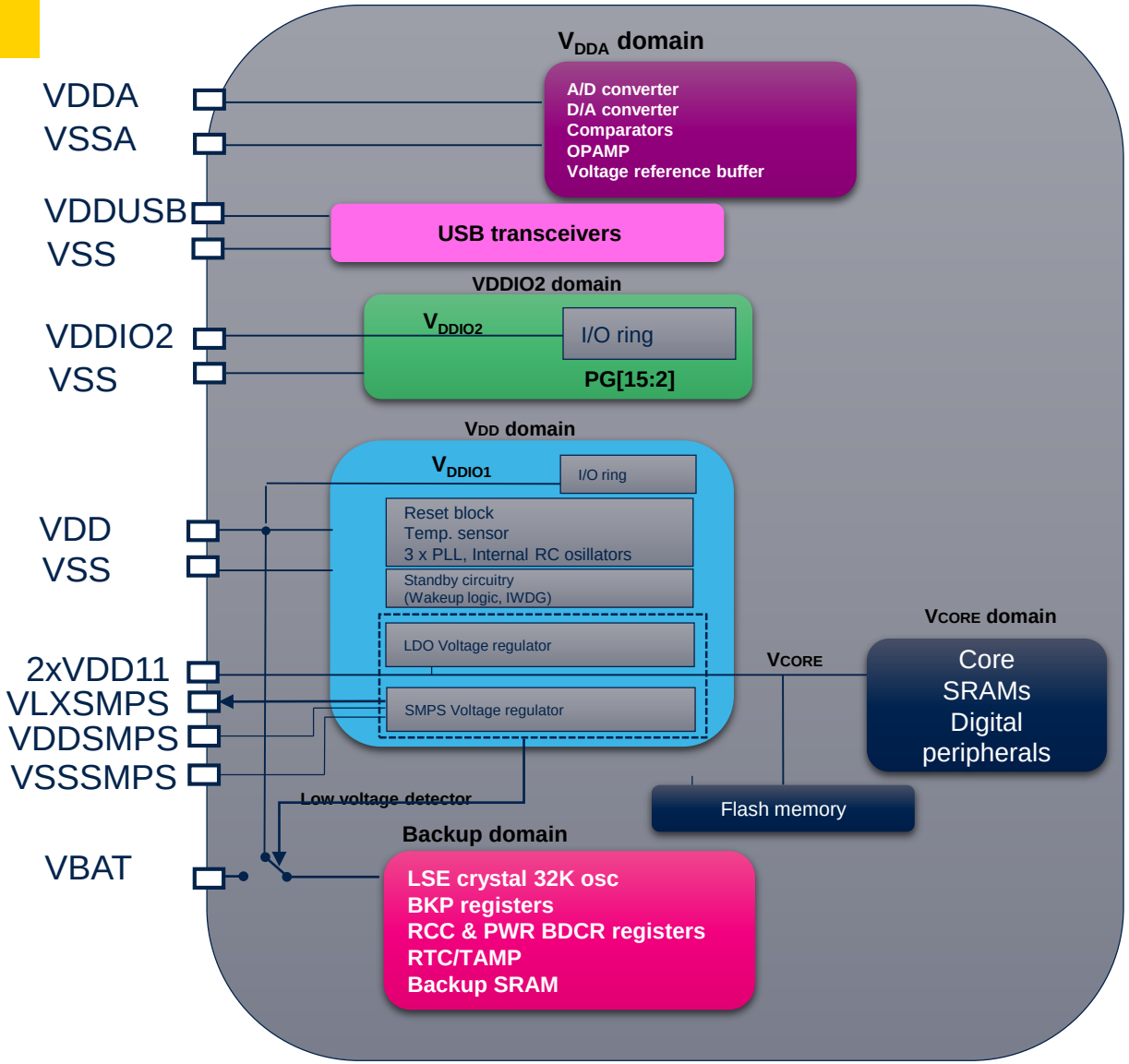


供电 – 带SMPS芯片

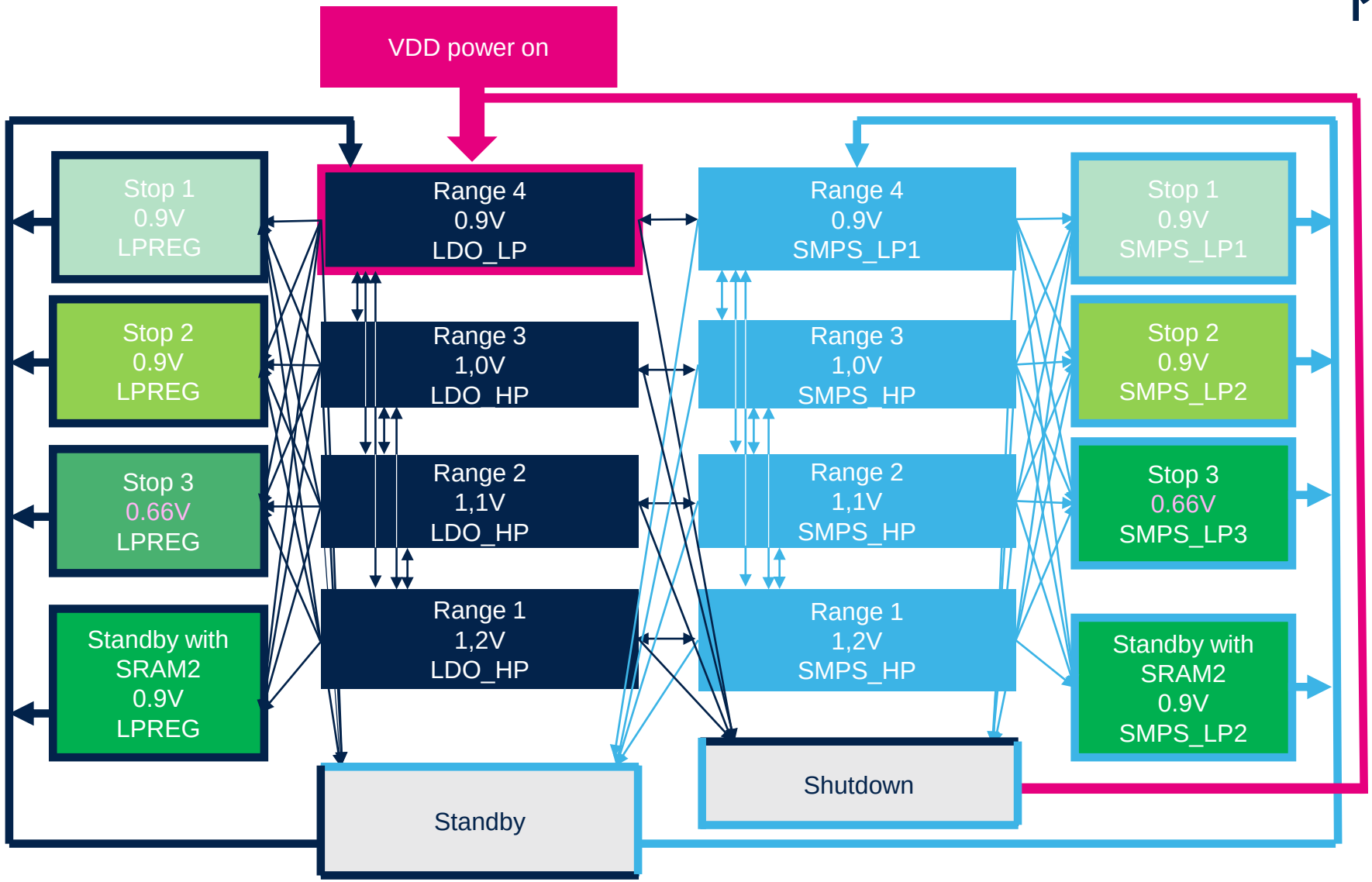
STM32U575xxxxQ and STM32U585xxxxQ

- 内部电压调节器: LDO 和 SMPS, 需外接4.7 µF电容和2.2 µH 电感
- VDDSMPS= 1,71 V ~ 3,6 V, 必须与VDD相连
  VLXSMPS: 开关电源SMPS降压转换输出

- **SMPS设计只用于芯片内部负载(切勿用于外部模块)**



内部电压调节器



所有电源模式都支持SMPS和LDO:

- 从stop和standby模式退出后,总能恢复到range 4(SMPS或者LDO)
- 从shutdown模式和上电启动后默认使用LDO

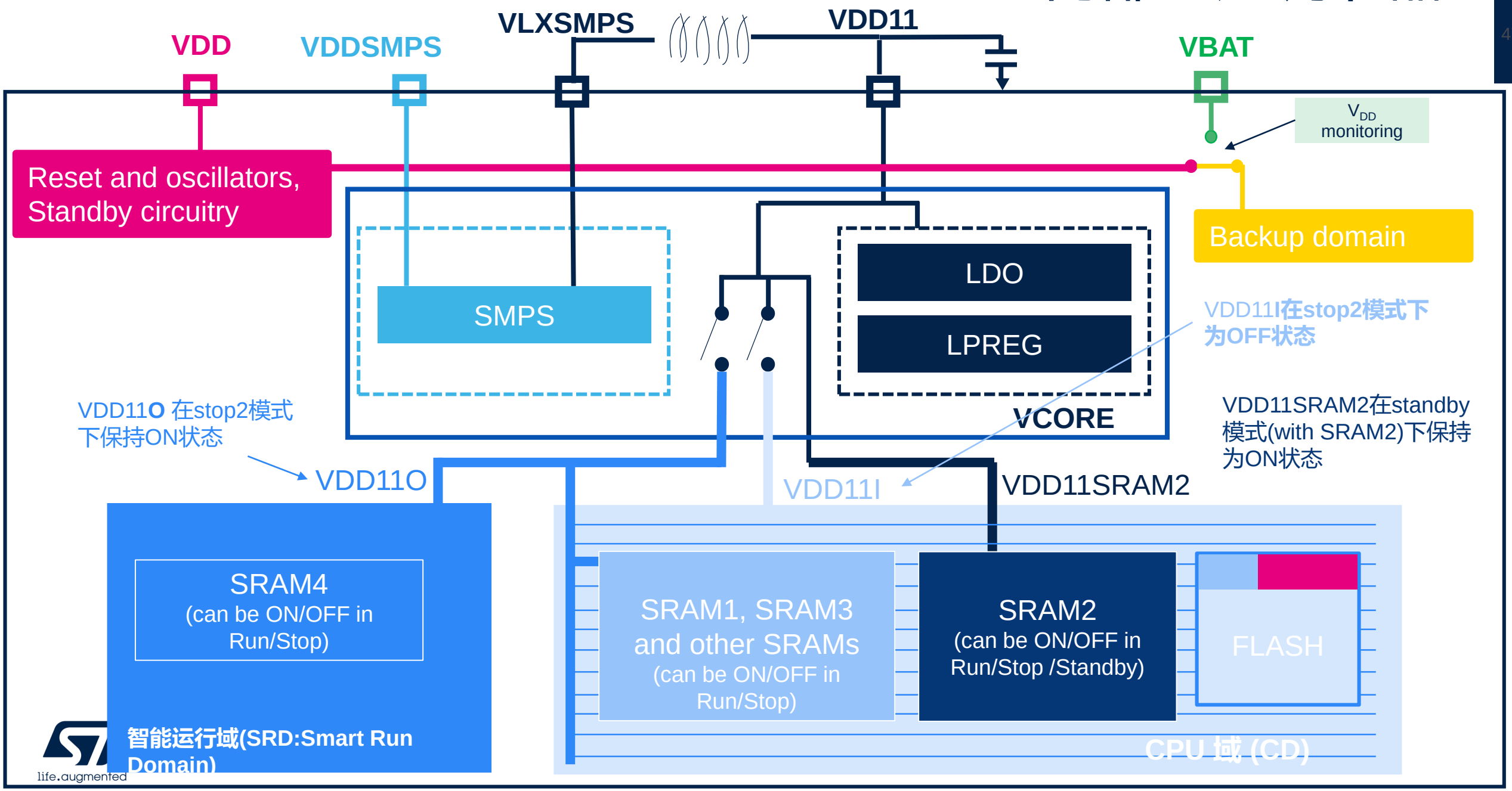
life.augmented

在Run和Sleep模式下降低功耗的技巧

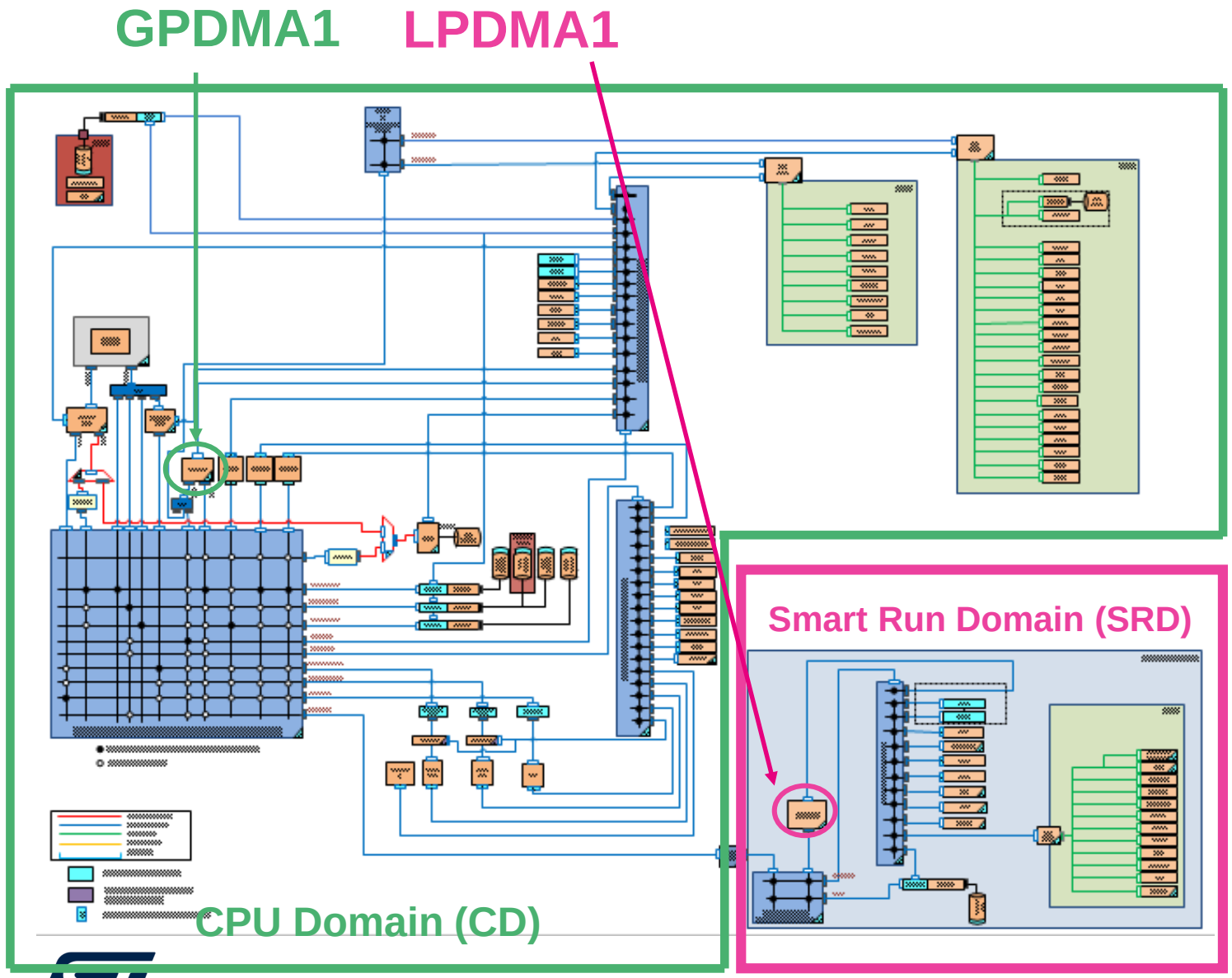
- 配置ICACHE工作在1-way模式, 打开FLASH的预取指功能
- 下电未使用的flash bank
  - 在运行模式下,每个bank的flash可配成下电
  - 当进入到sleep模式时,整个flash可配成下电
- 下电未使用的SRAM
  - SRAM1, SRAM2, SRAM3, SRAM4可各自独立配成下电
  - 时钟可关闭
- 如果某个总线上没有使用任何外设, 整个总线的时钟可关闭
  - 适用于无任何相关总线外设时, 但这些除外: IWDG, SRAM1, SRAM2, SRAM3, SRAM4, FLASH, BKPSRAM, ICACHE, DCACHE1,这些组件的时钟将依然保留
- 通常: 使用合适的内核电压(voltage scaling), 关闭无用的外设…

life.augmented

内部电压调节器


VDD
VDDSMPS
VLXSMPS
VDD11
VBAT
VDD monitoring
Reset and oscillators, Standby circuitry
Backup domain
SMPS
LDO
LPREG
VCORE
VDD11I在stop2模式下为OFF状态
VDD11O 在stop2模式下保持ON状态
VDD11O
VDD11I
VDD11SRAM2
VDD11SRAM2在standby模式(with SRAM2)下保持为ON状态
SRAM4 (can be ON/OFF in Run/Stop)
SRAM1, SRAM3 and other SRAMs (can be ON/OFF in Run/Stop)
SRAM2 (can be ON/OFF in Run/Stop /Standby)
FLASH
智能运行域(SRD:Smart Run Domain)
CPU 域 (CD)

CPU 域 (CD) 和智能运行域(SRD)



- Stop 0 & Stop 1:
  - CD & SRD 完全上电状态 =>得益于GPDMA1和LPDMA1,所有的自主外设的都能正常工作.
- Stop 2:
  - CPU域处于”保持”状态,少量漏电流 => 无任何动态活动
  - SRD域完全上电状态 => 得益于LPDMA1,SRD域的自主外设仍可正常工作.

life.augmented

低功耗模式: Stop 模式

SRAM内容保持且外设仍然可工作的最低功耗模式 (LPBAM)

- SRAM和外设寄存器内容全部保持, 且SRAM可**按页**单独在stop (stop0,1,2,3)模式下配置下电(power down):
  - SRAM1 : 3 x 64KB-pages(共3页)
  - SRAM2 : 8KB + 56KB pages(共2页)
  - SRAM3 : 8 x 64KB-pages(共8页)
  - SRAM4 : 1 x 16KB-Page(共1页)
  - ICACHE, DCACHE1, DMA2D SRAM, FMAC/FDRAM/USB SRAM, PKA SRAM(每 一项对应一个寄存器位)
- 唤醒时钟可以是HSI16 或 MSI(最大到24 MHz, 仅range 4)
  - FLASH low-power /fast wakeup modes in Stop 0/1
  - SRAM4 low-power /fast wakeup modes in Stop 0/1/2
- BOR的超低功耗模式 (采样模式) 用于 Stop 1, Stop 2, Stop 3, 和 Run/Sleep/Stop 0 Range 4 @PWR_CR1.ULPMEN=1
  - 注! 此模式并非默认

Stop 0 mode

Regulators
SMPS (LP1)
LDO (HP)
LPREG

CPU
Cortex®-M33

I/Os
Configuration kept

Clocking
HSI16
HSI48
HSE
MSI (up to 24 MHz)
LSI
LSE
PLL
CSS
CSS on LSE

Memories
Flash (2 MB)
SRAM1 (192 KB)
SRAM2 (64 KB)
SRAM3 (512 KB)
SRAM4 (16 KB)
BKPSRAM (2KB)
Backup registers
FSMC
OCTOSPI

Internal peripherals	
GPIOs	ADC1
LPGPIO	ADC4
GPDMA1	Temp. sensor
LPDMA1	DAC1-2
DMA2D	VREFBUF
CRC	OPAMP1-2
USART1-5	COMP1-2
LPUART1	CORDIC
I2C1,2,4	FMAC
I2C3	MDF1
SPI1-2	ADF1
SPI3	DCMI
FDCAN1	PSSI
SDMMC1-2	TSC
SAI1-2	TIM1-8,15-17
OTG_FS, UCPD1	LPTIM1,3,4
RNG	LPTIM2
AES, SAES	IWDG
HASH accelerator	WWDG
OTFDEC1-2	RTC
PKA	TAMP
SYSTICK	Supply & temperature monitoring for TAMP

Reset sources and Wakeup events	
NRST	GPIOs (EXTI
BOR	ADC4
PVD	GPDMA1
PVM	LPDMA1
RTC	USART1-5
TAMP	LPUART1
SRAM2-3 ECC error	I2C1,2,4
OTG_FS	I2C3
COMP	SPI1-2
LPTIM1,3,4	SPI3
LPTIM2	MDF1
IWDG	ADF1

Active Cell when enabled

Clocked-off cell, not functional

Cell in power-down

Enabled source of reset

Enabled source of wakeup

Cannot be used as source or reset or wakeup

life.augmented

Stop 1 mode

Regulators
SMPS (LP1)
LDO (HP)
LPREG

CPU
Cortex®-M33

I/Os
Configuration kept

Clocking
HSI16
HSI48
HSE
MSI (up to 24 MHz)
LSI
LSE
PLL
CSS
CSS on LSE

Memories
Flash (2 MB)
SRAM1 (192 KB)
SRAM2 (64 KB)
SRAM3 (512 KB)
SRAM4 (16 KB)
BKPSRAM (2KB)
Backup registers
FSMC
OCTOSPI

Internal peripherals	
GPIOs	ADC1
LPGPIO	ADC4
GPDMA1	Temp. sensor
LPDMA1	DAC1-2
DMA2D	VREFBUF
CRC	OPAMP1-2
USART1-5	COMP1-2
LPUART1	CORDIC
I2C1,2,4	FMAC
I2C3	MDF1
SPI1-2	ADF1
SPI3	DCMI
FDCAN1	PSSI
SDMMC1-2	TSC
SAI1-2	TIM1-8,15-17
OTG_FS, UCPD1	LPTIM1,3,4
RNG	LPTIM2
AES, SAES	IWDG
HASH accelerator	WWDG
OTFDEC1-2	RTC
PKA	TAMP
SYSTICK	Supply & temperature monitoring for TAMP

Reset sources and Wakeup events	
NRST	GPIOs (EXTI
BOR	ADC4
PVD	GPDMA1
PVM	LPDMA1
RTC	USART1-5
TAMP	LPUART1
SRAM2-3 ECC error	I2C1,2,4
OTG_FS	I2C3
COMP	SPI1-2
LPTIM1,3,4	SPI3
LPTIM2	MDF1
IWDG	ADF1

Active Cell when enabled

Clocked-off cell, not functional

Cell in power-down

Enabled source of reset

Enabled source of wakeup

Cannot be used as source or reset or wakeup

life.augmented

Stop 2 mode

Regulators
SMPS (LP2)
LDO (HP)
LPREG

CPU
Cortex®-M33

I/Os
Configuration kept

Clocking
HSI16
HSI48
HSE
MSI (up to 24 MHz)
LSI
LSE
PLL
CSS
CSS on LSE

Memories
Flash (2 MB)
SRAM1 (192 KB)
SRAM2 (64 KB)
SRAM3 (512 KB)
SRAM4 (16 KB)
BKPSRAM (2KB)
Backup registers
FSMC
OCTOSPI

Internal peripherals	
GPIOs	ADC1
LPGPIO	ADC4
GPDMA1	Temp. sensor
LPDMA1	DAC1-2
DMA2D	VREFBUF
CRC	OPAMP1-2
USART1-5	COMP1-2
LPUART1	CORDIC
I2C1-2	FMAC
I2C3	**MDF1**
SPI1-2	ADF1
SPI3	DCMI
FDCAN1	PSSI
SDMMC1-2	TSC
SAI1-2	TIM1-8,15-17
OTG_FS, UCPD1	LPTIM1,3,4
RNG	**LPTIM2**
AES, SAES	IWDG
HASH accelerator	WWDG
OTFDEC1-2	RTC
PKA	TAMP
SYSTICK	Supply & temperature monitoring for TAMP

Reset sources and Wakeup events	
NRST	GPIOs (EXTI)
BOR	ADC4
PVD	GPDMA1
PVM	LPDMA1
RTC	USART1-5
TAMP	LPUART1
SRAM2-3 ECC error	I2C1,2,4
OTG_FS	I2C3
COMP	SPI1-2
LPTIM1,3,4	SPI3
LPTIM2	MDF1
IWDG	ADF1

Active Cell when enabled

Clocked-off cell, not functional

Cell in power-down

Enabled source of reset

Enabled source of wakeup

Cannot be used as source or reset or wakeup

life.augmented

Stop 3 mode

Regulators
SMPS (LP3)
LDO (HP)
LPREG

CPU
Cortex®-M33

I/Os
Pull-up / Pull-down

Clocking
HSI16
HSI48
HSE
MSI (up to 24 MHz)
LSI
LSE
PLL
CSS
CSS on LSE

Memories
Flash (2 MB)
SRAM1 (192 KB)
SRAM2 (64 KB)
SRAM3 (512 KB)
SRAM4 (16 KB)
BKPSRAM (2KB)
Backup registers
FSMC
OCTOSPI

Internal peripherals	
GPIOs	ADC1
LPGPIO	ADC4
GPDMA1	Temp. sensor
LPDMA1	DAC1-2
DMA2D	VREFBUF
CRC	OPAMP1-2
USART1-5	COMP1-2
LPUART1	CORDIC
I2C1,2,4	FMAC
I2C3	MDF1
SPI1-2	ADF1
SPI3	DCMI
FDCAN1	PSSI
SDMMC1-2	TSC
SAI1-2	TIM1-8,15-17
OTG_FS, UCPD1	LPTIM1,3,4
RNG	LPTIM2
AES, SAES	IWDG
HASH accelerator	WWDG
OTFDEC1-2	RTC
PKA	TAMP
SYSTICK	Supply & temperature monitoring for TAMP

Reset sources and Wakeup events	
NRST	GPIOs **(24 pins)**
BOR	ADC4
PVD	GPDMA1
PVM	LPDMA1
RTC	USART1-5
TAMP	LPUART1
SRAM2-3 ECC error	I2C1,2,4
OTG_FS	I2C3
COMP	SPI1-2
LPTIM1,3,4	SPI3
LPTIM2	MDF1
IWDG	ADF1

Active Cell when enabled

Clocked-off cell, not functional

Cell in power-down

Enabled source of reset

Enabled source of wakeup

Cannot be used as source or reset or wakeup

life.augmented

低功耗后台自主模式 (LPBAM)

一种可实现复杂应用场景的低功耗模式的智能方式

- 无需CPU干预 – 所有活动基于DMA(LPDMA 和 GPDMA)
  - 得益于DMA的链表模式,外设的配置和活动可衔接起来, 最低可工作在stop2模式. DMA可用来”模拟”软件并重新配置外设.
  - 硬件可触发外设工作 (如. ADC 转换, 通信外设开始传输, DMA传输等…).

- 功耗受益:
  - 大部分外设在stop模式下都已经关闭
  - 在stop模式下只有必要的供外设的时钟才保留
  - 在stop模式下模拟外设和振荡器只有必要时才保持上电

自主外设特性

自主外设	
Stop 0/1下可工作的外设	**Stop 2下可工作的外设**
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

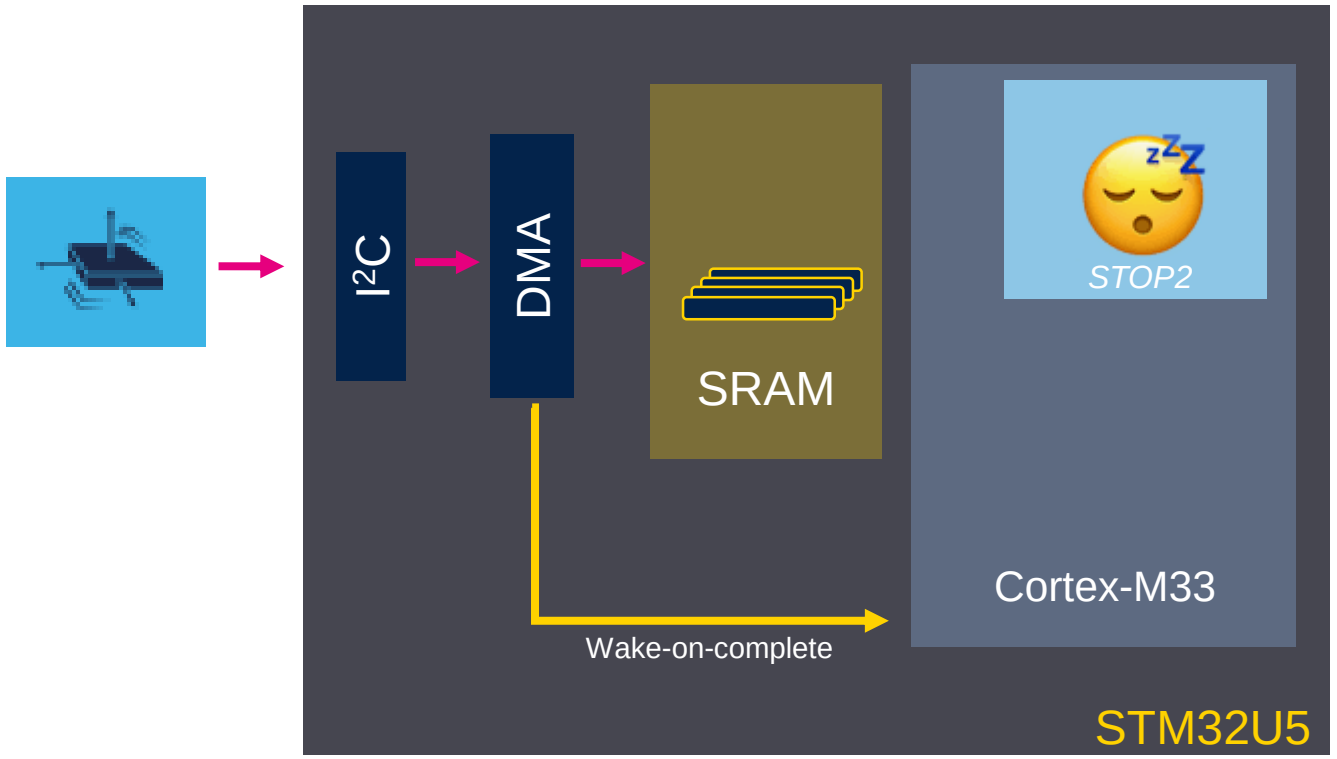
- 外设的活动独立于MCU的工作模式 (Run, Sleep, Stop)
- 在stop模式下依然支持DMA传输
  - 得益于IP内核和AHB/APB时钟请求
- 在stop模式下,外设的活动可由异步触发开启:
  - 通信外设开始传输
  - ADC/DAC开始转换
  - DMA开始传输

  ➢ 触发器可选择来自LPTIM的输出,比较器的输出,I/O…
- 自主外设的中断可将MCU从stop模式唤醒

life.augmented

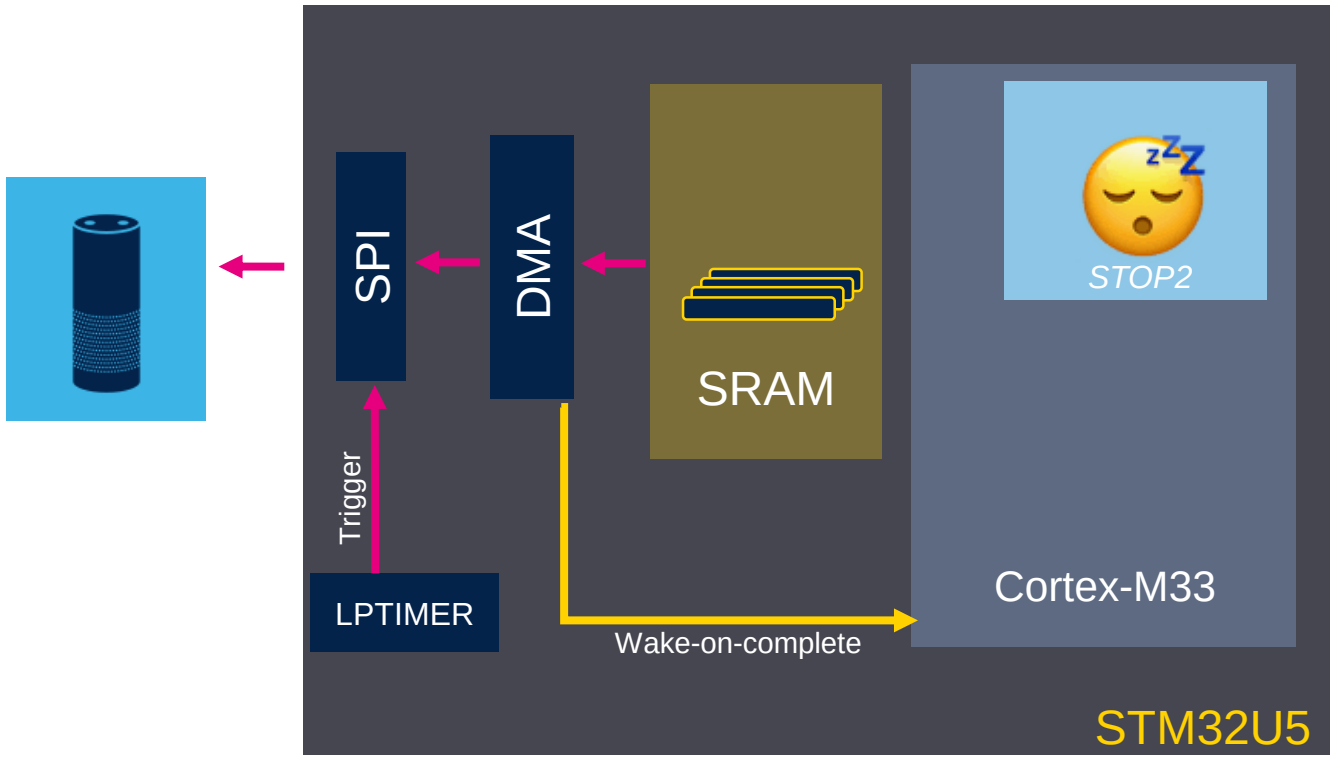
LPBAM 案例

- **I²C 从接收 ; SPI / UART 接收**
- I²C 主发送 ; SPI / UART 发送
- ADC 转换
- DAC 转换
- 语音检测
- LPTIM PWM 比值变化, 输入捕获, 脉冲计数…
- I/O 控制 (输入, 输出)
- 外设衔接
- ….



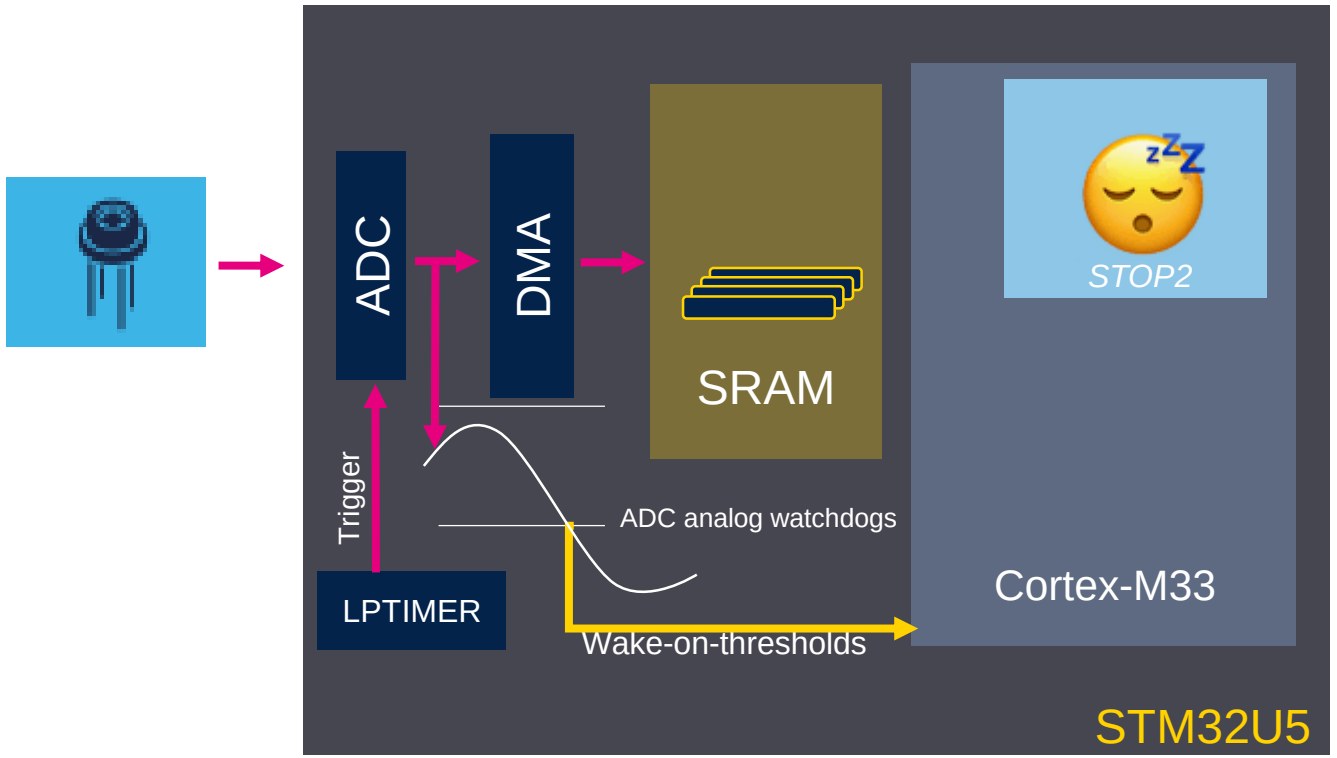
LPBAM 案例

- I2C 从接收 ; SPI / UART 接收
- **I2C 主发送 ; SPI / UART 发送**
- ADC 转换
- DAC 转换
- 语音检测
- LPTIM PWM 比值变化, 输入捕获, 脉冲计数…
- I/O 控制 (输入, 输出)
- 外设衔接
- ….



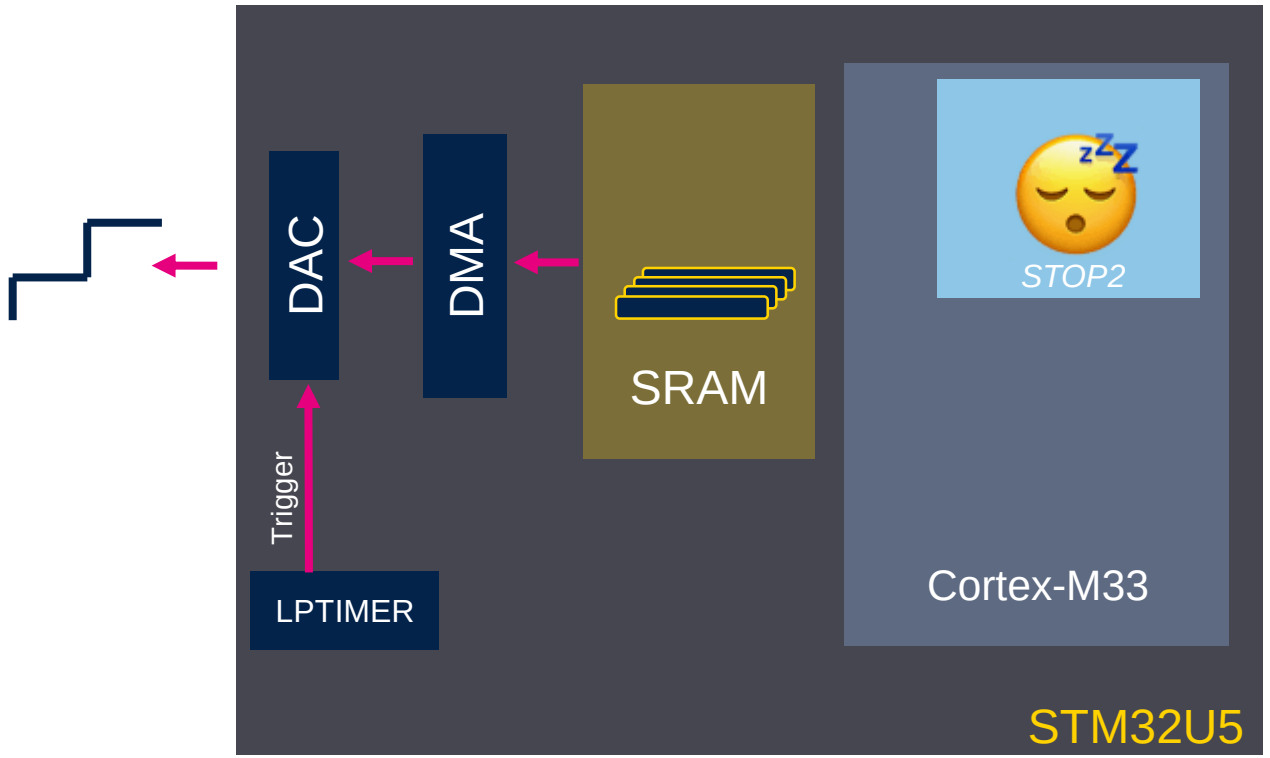
LPBAM 案例

- I2C 从接收 ; SPI / UART 接收
- I²C 主发送 ; SPI / UART 发送
- **ADC 转换**
- DAC 转换
- 语音检测
- LPTIM PWM 比值变化, 输入捕获, 脉冲计数…
- I/O 控制 (输入, 输出)
- 外设衔接
- ….



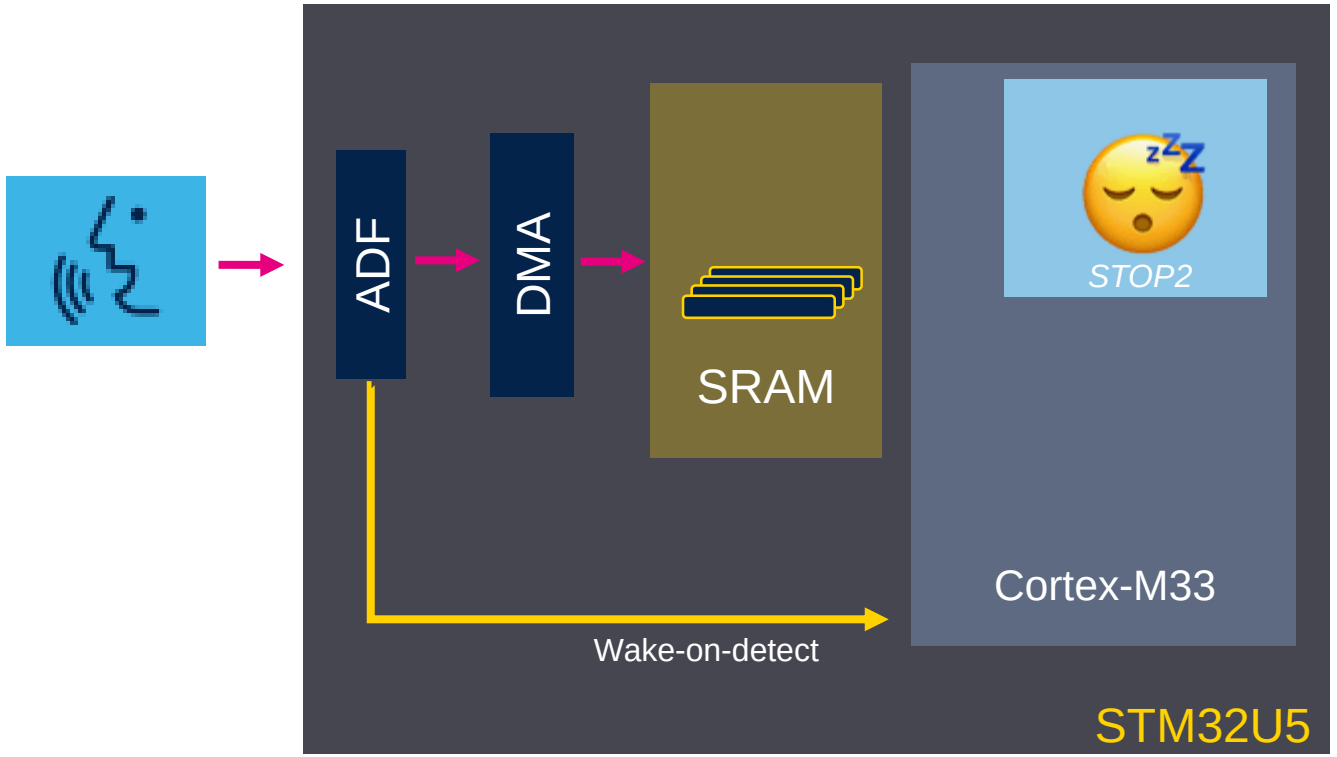
LPBAM 案例

- I2C 从接收 ; SPI / UART 接收
- I²C 主发送 ; SPI / UART 发送
- ADC 转换
- **DAC 转换**
- 语音检测
- LPTIM PWM 比值变化, 输入捕获, 脉冲计数…
- I/O 控制 (输入, 输出)
- 外设衔接
- ….



LPBAM 案例

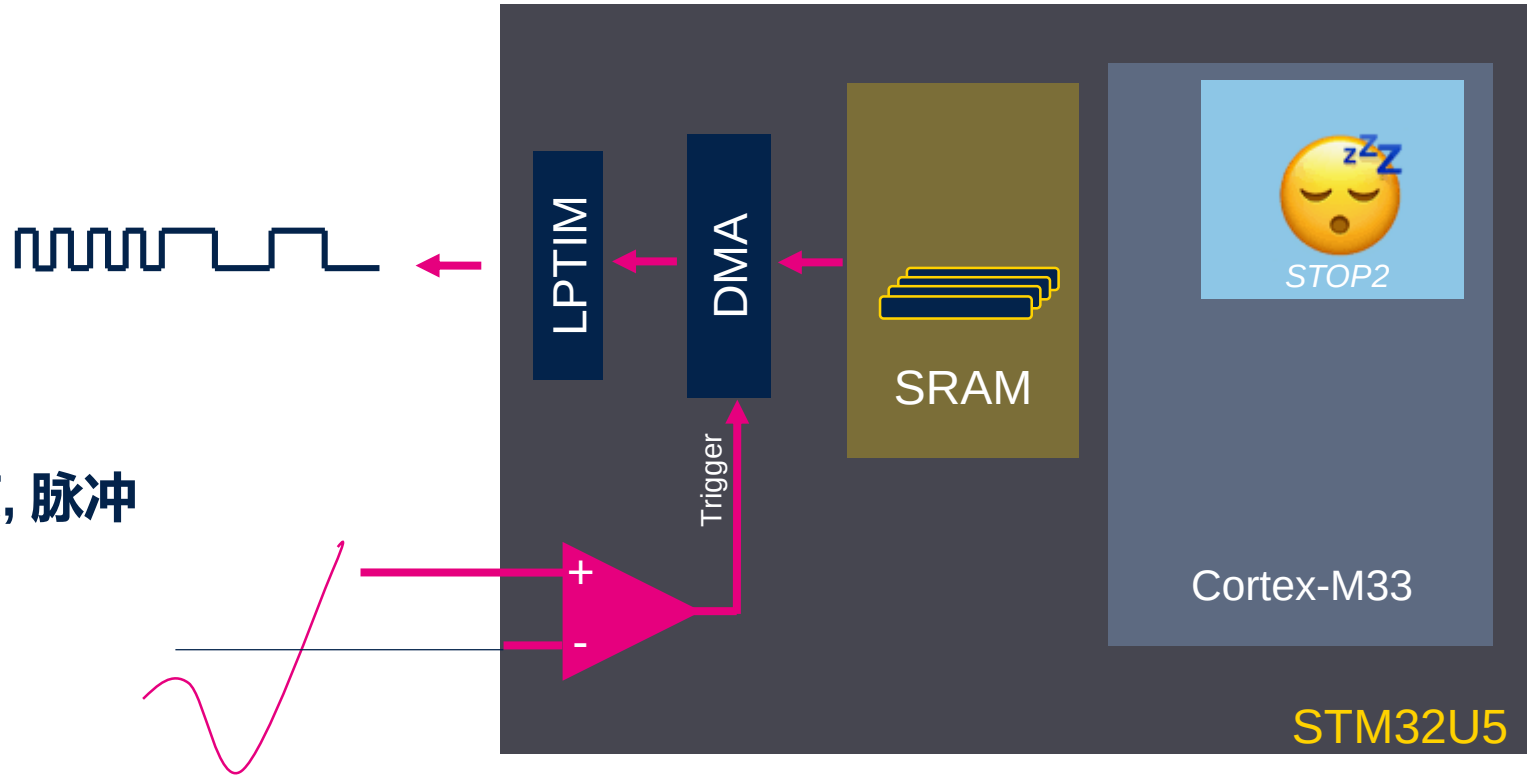
- I2C 从接收 ; SPI / UART 接收
- I²C 主发送 ; SPI / UART 发送
- ADC 转换
- DAC 转换
- **语音检测**
- LPTIM PWM 比值变化, 输入捕获, 脉冲计数…
- I/O 控制 (输入, 输出)
- 外设衔接
- ….



life.augmented

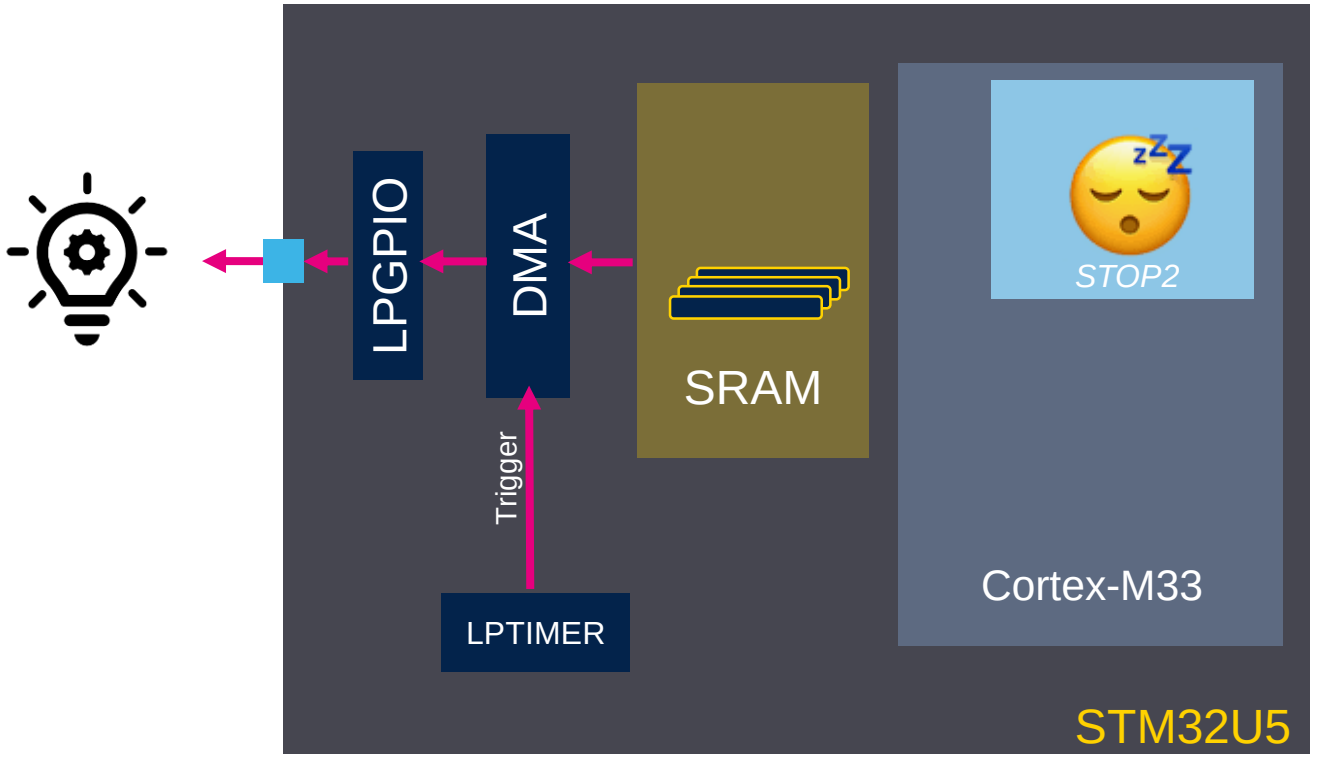
LPBAM 案例

- I2C 从接收 ; SPI / UART 接收
- I²C 主发送 ; SPI / UART 发送
- ADC 转换
- DAC 转换
- 语音检测
- **LPTIM PWM 比值变化, 输入捕获, 脉冲计数…**
- I/O 控制 (输入, 输出)
- 外设衔接
- ….



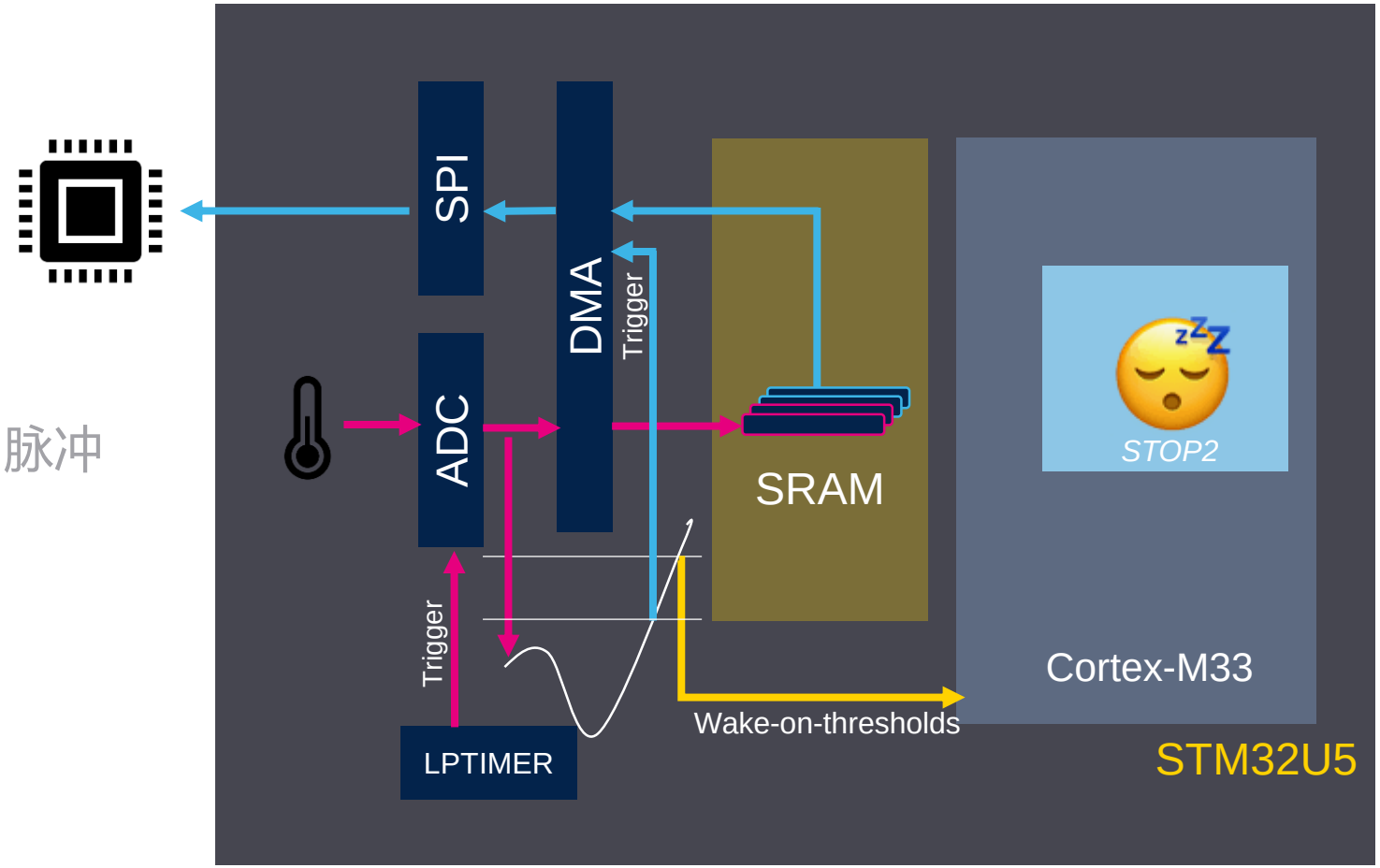
LPBAM 案例

- I2C 从接收 ; SPI / UART 接收
- I²C 主发送 ; SPI / UART 发送
- ADC 转换
- DAC 转换
- 语音检测
- LPTIM PWM 比值变化, 输入捕获, 脉冲计数…
- **I/O 控制 (输入, 输出)**
- 外设衔接
- ….



LPBAM 案例

- I2C 从接收 ; SPI / UART 接收
- I²C 主发送 ; SPI / UART 发送
- ADC 转换
- DAC 转换
- 语音检测
- LPTIM PWM 比值变化, 输入捕获, 脉冲计数…
- I/O 控制 (输入, 输出)
- **外设衔接**
- ….



Stop 模式总结

	Stop 0	Stop 1	Stop 2	Stop 3
电压调节器	与Run模式相同	Low-power	Low-power	Low-power
可工作的外设及唤醒源	CPU域和SRD域		SRD域	与Standby模式相同
时钟	LSE / LSI / HSI16 / MSI 最高可达 24MHz			LSE / LSI
I/O	状态保持 GPDMA1可动态控制I/O 所有I/O可唤醒		状态保持 LPDMA1可动态控制16个IO, 所有I/O可唤醒	上/下拉可保持 24 个唤醒引脚
使用SMPS且所有SRAM保持 (µA)	70		8,7	3,5
唤醒时间(µs)	12	18	23	36

life.augmented

Standby 模式

Regulators
SMPS (ULP) (if SRAM2)
LDO (HP)
LPREG (if SRAM2)

Clocking
HSI16
HSI48
HSE
MSI (up to 24 MHz)
LSI
LSE
PLL
CSS
CSS on LSE

CPU
Cortex®-M33

I/Os
Pull-up/ Pull-down

Memories
Flash (2 MB)
SRAM1 (192 KB)
SRAM2 (64 KB)
SRAM3 (512 KB)
SRAM4 (16 KB)
BKPSRAM (2KB)
Backup registers
FSMC
OCTOSPI

Internal peripherals	
GPIOs	ADC1
LPGPIO	ADC4
GPDMA1	Temp. sensor
LPDMA1	DAC1-2
DMA2D	VREFBUF
CRC	OPAMP1-2
USART1-5	COMP1-2
LPUART1	CORDIC
I2C1,2,4	FMAC
I2C3	MDF1
SPI1-2	ADF1
SPI3	DCMI
FDCAN1	PSSI
SDMMC1-2	TSC
SAI1-2	TIM1-8,15-17
OTG_FS, UCPD1	LPTIM1,3,4
RNG	LPTIM2
AES, SAES	IWDG
HASH accelerator	WWDG
OTFDEC1-2	RTC
PKA	TAMP
SYSTICK	Supply & temperature monitoring for TAMP

Reset sources and Wakeup events	
NRST	GPIOs (24 pins)
BOR	ADC4
PVD	GPDMA1
PVM	LPDMA1
RTC	USART1-5
TAMP	LPUART1
SRAM2-3 ECC error	I2C1,2,4
OTG_FS	I2C3
COMP	SPI1-2
LPTIM1,3,4	SPI3
LPTIM2	MDF1
IWDG	ADF1

Active Cell when enabled

Clocked-off cell, not functional

Cell in power-down

Enabled source of reset

Enabled source of wakeup

Cannot be used as source or reset or wakeup

life.augmented

Shutdown模式

Regulators
SMPS (ULP)
LDO (HP)
LPREG

CPU
Cortex®-M33

I/Os
-

Clocking
HSI16
HSI48
HSE
MSI (up to 24 MHz)
LSI
LSE
PLL
CSS
CSS on LSE

Memories
Flash (2 MB)
SRAM1 (192 KB)
SRAM2 (64 KB)
SRAM3 (512 KB)
SRAM4 (16 KB)
BKPSRAM (2KB)
Backup registers
FSMC
OCTOSPI

Internal peripherals	
GPIOs	ADC1
LPGPIO	ADC4
GPDMA1	Temp. sensor
LPDMA1	DAC1-2
DMA2D	VREFBUF
CRC	OPAMP1-2
USART1-5	COMP1-2
LPUART1	CORDIC
I2C1,2,4	FMAC
I2C3	MDF1
SPI1-2	ADF1
SPI3	DCMI
FDCAN1	PSSI
SDMMC1-2	TSC
SAI1-2	TIM1-8,15-17
OTG_FS, UCPD1	LPTIM1,3,4
RNG	LPTIM2
AES, SAES	IWDG
HASH accelerator	WWDG
OTFDEC1-2	RTC
PKA	TAMP
SYSTICK	Supply & temperature monitoring for TAMP

Reset sources and Wakeup events	
NRST	GPIOs **(24 pins)**
BOR	ADC4
PVD	GPDMA1
PVM	LPDMA1
RTC	USART1-5
TAMP	LPUART1
SRAM2-3 ECC error	I2C1,2,4
OTG_FS	I2C3
COMP	SPI1-2
LPTIM1,3,4	SPI3
LPTIM2	MDF1
IWDG	ADF1

Active Cell when enabled

Clocked-off cell, not functional

Cell in power-down

Enabled source of reset

Enabled source of wakeup

Cannot be used as source or reset or wakeup

life.augmented

低功耗模式: Standby 和 Shutdown 模式

- 从Standby模式唤醒后的时钟为
  MSI 1 ~ 4 MHz
- Standby:
  8 KB + 56 KB SRAM2 (总共64 KB) 可分别配置保留
  2 KB BKPSRAM 能够保留
- 24 个唤醒引脚多路复用到8个事件, 还有内部唤醒事件
  - 当使用RTC或TAMP唤醒时, WUSELx必须设为11
  - 当 WUSELx=11: 当所有内部唤醒源都被清除时, WUFx标志 硬件自动清除

Wakeup event	(WUSELx = 00)	(WUSELx = 01)	(WUSELx = 10)	(WUSELx = 11)
WKUP1	PA0	PB2	PE4	-
WKUP2	PA4	PC13	PE5	-
WKUP3	PE6	PA1	PB6	-
WKUP4	PA2	PB1	PB7	-
WKUP5	PC5	PA3	PB8	-
WKUP6	PB5	PA5	PE7	RTC_ALRA_S or RTC_ALRB_S or RTC_WUT_S or RTC_TS_S
WKUP7	PB15	PA6	PE8	RTC_ALRA or RTC_ALRB or RTC_WUT or RTC_TS
WKUP8	PF2	PA7	PB10	TAMP or TAMP_S

VBAT 模式

Regulators
SMPS (ULP) (if SRAM2)
LDO (HP)
LPREG (if SRAM2)

Clocking
HSI16
HSI48
HSE
MSI (up to 24 MHz)
LSI
LSE
PLL
CSS
CSS on LSE

CPU
Cortex®-M33

I/Os
Pull-up/ Pull-down

Memories
Flash (2 MB)
SRAM1 (192 KB)
SRAM2 (64 KB)
SRAM3 (512 KB)
SRAM4 (16 KB)
BKPSRAM (2KB)
Backup registers
FSMC
OCTOSPI

Internal peripherals	
GPIOs	ADC1
LPGPIO	ADC4
GPDMA1	Temp. sensor
LPDMA1	DAC1-2
DMA2D	VREFBUF
CRC	OPAMP1-2
USART1-5	COMP1-2
LPUART1	CORDIC
I2C1,2,4	FMAC
I2C3	MDF1
SPI1-2	ADF1
SPI3	DCMI
FDCAN1	PSSI
SDMMC1-2	TSC
SAI1-2	TIM1-8,15-17
OTG_FS, UCPD1	LPTIM1,3,4
RNG	LPTIM2
AES, SAES	IWDG
HASH accelerator	WWDG
OTFDEC1-2	RTC
PKA	TAMP
SYSTICK	Supply & temperature monitoring for TAMP

Reset sources and Wakeup events	
NRST	GPIOs
BOR	ADC4
PVD	GPDMA1
PVM	LPDMA1
RTC / TAMP	USART1-5
LSE detector ; Supply & temperature monitoring through TAMP	LPUART1
SRAM2-3 ECC error	I2C1,2,4
OTG_FS	I2C3
COMP	SPI1-2
LPTIM1,3,4	SPI3
LPTIM2	MDF1
IWDG	ADF1

Active Cell when enabled

Clocked-off cell, not functional

Cell in power-down

Enabled source of reset

Enabled source of wakeup

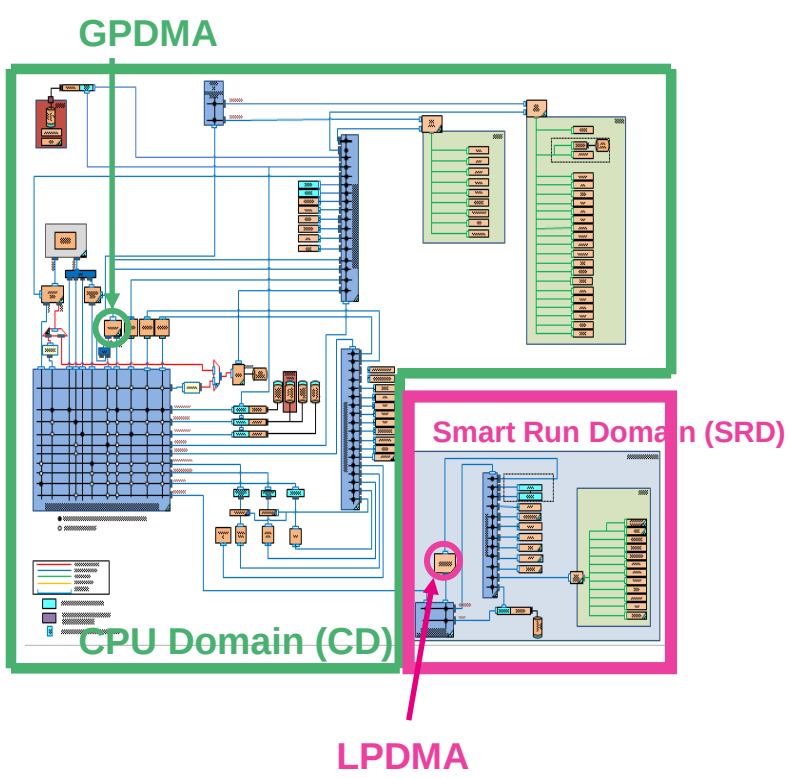
Cannot be used as source or reset or wakeup

life.augmented

VBAT 模式

- 当VDD存在时,VBAT电池充电
- VBAT BOR (1.58V)
- 2 KB BKPSRAM 可保持 (可选的,被tamper保护)
- RTC 和 TAMP 采用 LSE 或 LSI 时钟, 包含8个入侵检测引脚
- LSE CSS系统连接到tamper:
  - 时钟丢失检测 & 过频检测 (2MHz)
  - Glitch 过滤 (2MHz)
- 温度和备份域电压(VBAT)检测连接到tamper

PWR 模式输出引脚

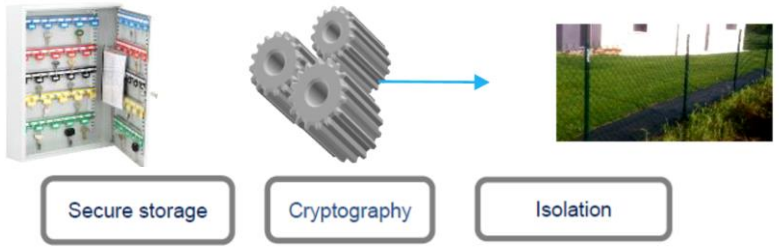


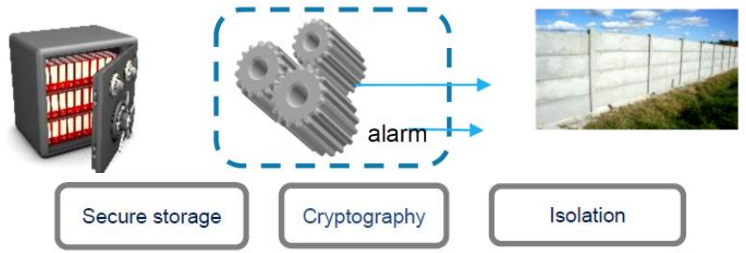
CSLEEP	CDSTOP	SRDSTOP	MCU 模式
0	0	0	Run 模式
1	0	0	Sleep 模式 或 Stop 0 或 Stop 1 模式, AHB/APB 时钟运行在CPU 域 (CD) 和 SRD域
1	1	0	Stop 0, Stop 1 or Stop 2 模式, AHB/APB 时钟运行在SRD域
1	1	1	Stop 0, Stop 1, Stop 2 或 Stop 3 模式

life.augmented

信息安全

信息安全改进概览





STM32L5

- 硬件隔离
  - Secure, non-secure (*)
  - ST可选服务 (HDP)
- 密码学算法加速器
  - 标准密码学算法加速器
  - 可以使用自定义的加密库
- 安全存储
  - 密钥管理(KMS)的示例代码, 运行在安全模式下.
    - *帮助客户加快实现最终的解决方案!*

STM32U5

- 硬件隔离
  - Secure, non-secure privileged & unprivileged
  - ST可选服务 (HDP)
  - 安全协处理硬件 (**)
- 密码学算法加速器
  - 防侧信道攻击 密码学算法加速器 (AES, PKA), 产生入侵报警
- 安全存储
  - 与L5相同, 但在硬件隔离上有所加强

(*) 使用MPU进行特权/非特权隔离 (Cortex-M)
(**) 安全硬件,隔离设备的资产,CPU无法访问(如密钥存储) [ARM PSA]

life.augmented

信息安全改进概览

- 增强的生命周期管理
  - RDP, 解锁机制
- 改进的任务隔离
- 写保护锁定
- 改进了资源隔离
- 增强了密钥存储
- 升级的密码学算法加速器
  - 安全AES(SAES) 外设
  - 传统 AES 外设
  - 公钥算法加速器 (PKA)
  - HASH 引擎(SHA-2)
  - 真随机数产生器 (RNG)
- 增强的防篡改检测

增强的生命周期管理

读保护 (RDP)

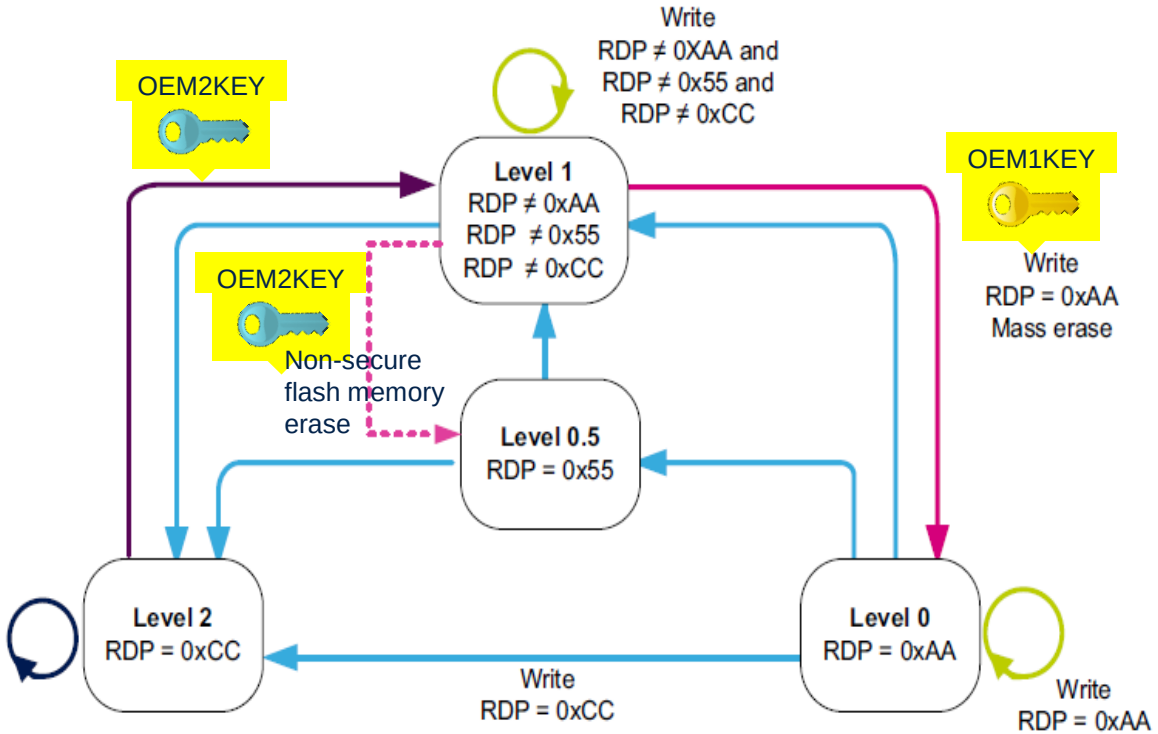
- RDP 传统模式
  - 与STM32L5完全相同
- RDP 密码模式
  - 基于密码的RDP等级回退
  - 支持两个不同的 OEMKEY 密码
  - 与L5相比,客户可以通过密码从RDP2降级.
    - 在这种情况下, JTAG/SWD在RDP2下仍然可以连接, 但仅限于注入密码操作

对应用的益处

- ✓ 支持不同的密码, 分别保护安全和非安全的代码
- ✓ 支持传统RDP2模式（无法降级）和基于密码的RDP回退模式. 用户可以根据需要进行选择.

增强的生命周期管理

基于密码的RDP回退



TZ enable

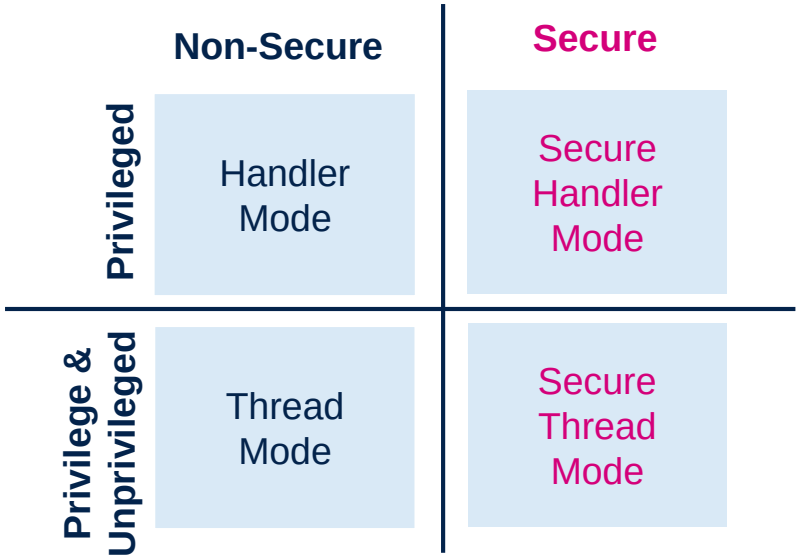
- 两个密钥 - **OEM1KEY**, **OEM2KEY**
  - 都是64位, 只可写, 不可读
  - 如果未配置则默认为传统模式
- OEM1KEY用在RDP1->RDP0时
- OEM2KEY用在RDP2->RDP1和RDP1->RDP0.5
- 解锁时,密钥在复位期间通过JTAG/SWD写入
- 新的32位设备ID(**Chip ID**)
  - 设备ID与密钥关联

life.augmented

资源隔离改进

改进 PSA Level 2 支持

- 系统外设和存储具有4个隔离状态 (new vs.SM32L5)
  - Secure/Privilege (S/P)
  - Secure/Non Privilege (S/NP)
  - Non Secure/Privilege (SN/P)
  - Non Secure/ Non Privilege (NS/NP)
- 新的安全配置寄存器:
  - FLASH
  - RCC
  - PWR



Secure 和 Non-Secure 寄存器具有独立的 Privilege 和 Non Privilege 属性

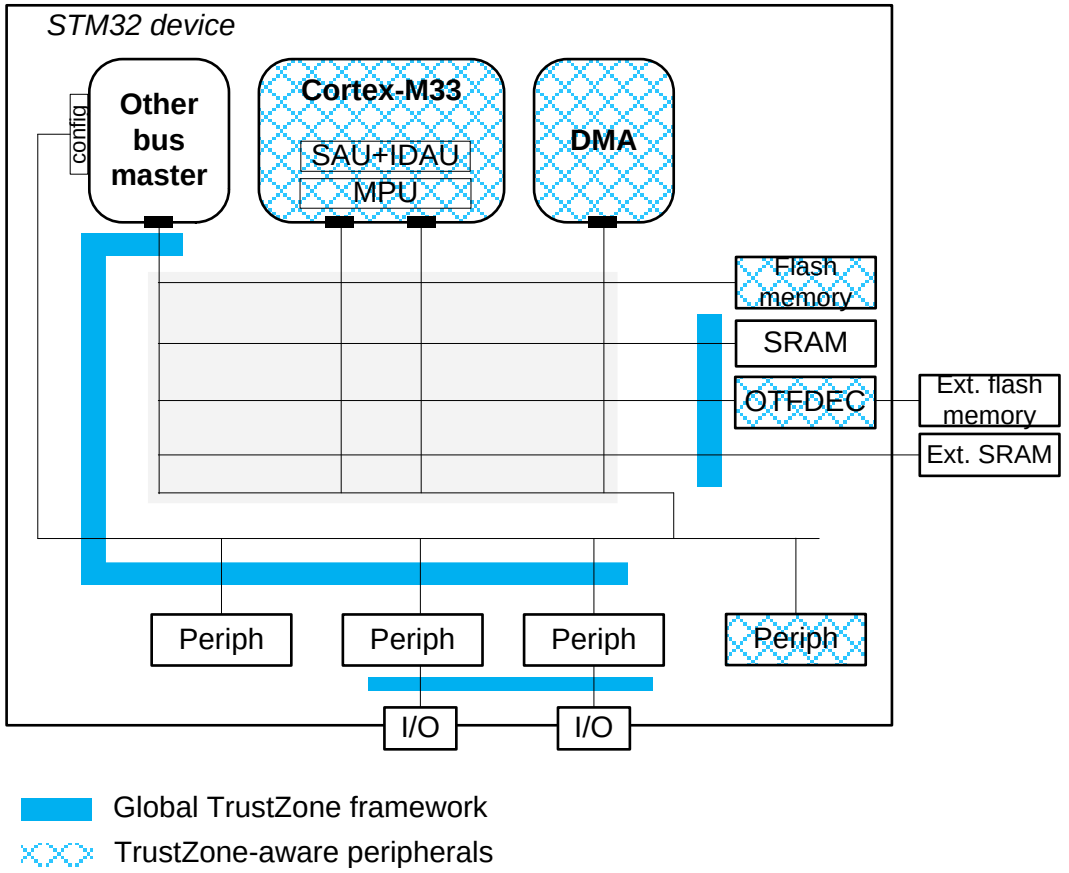
life.augmented

New versus STM32L5

资源隔离改进

改进 PSA Level 2 支持

- 全局 TrustZone 控制器 (GTZC)
  - Secure/Privilege (SP) 访问模式的 securable 和 TrustZone-aware 外设
  - Secure/Privilege (SP) 访问模式的 securable 传统主设备
  - 内部 SRAM 的基于块的 secure 和 privilege 配置
  - 外部存储 OCTOSPI / FSMC 和 备份 SRAM 子区且带水标的Secure 和 privilege 配置



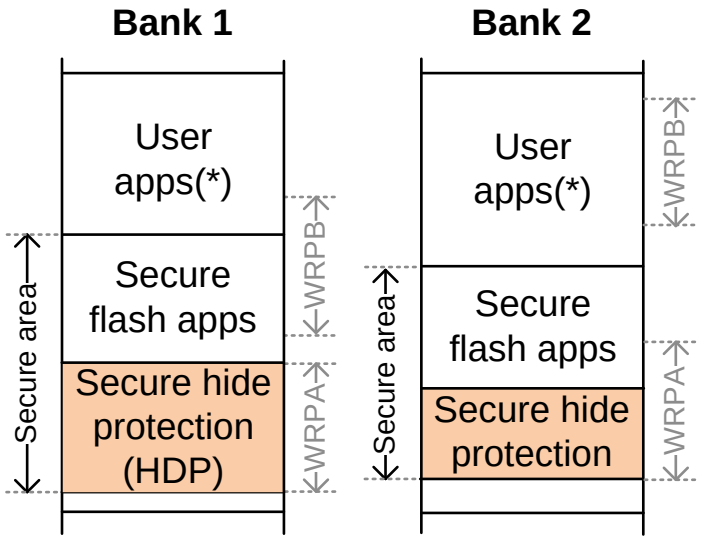
→ 这种特权隔离粒度是外设/内存资源端的，很好地补充了Cortex 内核 (8x MPU区域)中可用的比较粗糙的特权隔离

New versus STM32L5

资源隔离改进

内部FLASH更新

- FLASH为双BANK架构
- 类似于STM32L5,每个BANK有两个写保护区域(静态配置)
  - 有了写保护锁定功能,U5可以使FLASH区域ROM化, 而L5要实现这一功能则要依赖HDP区域.
  - 由于写保护锁定只能在RDP回退时解锁, 应用如果要保持写保护区域的锁定, 则应尽量避免此操作 (如写入随机OEM密钥)
- 每页(8KB) 可配置成 S/NS 和 / 或 P/NP (动态配置)



(*) Any page set as non-secure can be set as secure on-the-fly using the volatile, block-based configuration registers

→这种特权隔离粒度是外设/内存资源端的，很好地补充了Cortex 内核 (8x MPU区域)中可用的比较粗糙的特权隔离

life.augmented

增强的密钥存储

硬件密钥

- 用一机一密的方式为每个设备建立健壮的信任根是一种很好的安全做法，可以将密钥与特定芯片绑定
- 硬件密钥是不可知且不能由软件设置的密钥，它通过内部私有总线提供给AES引擎
- 应用可使用硬件密钥对存储在NVM和本地SRAM上的敏感数据进行加密
- U5拥有3个不的硬件密钥来源
  - **DHUK** – 基于设备根密钥RHUK,结合TZ状态和密钥使用状态KMOD派生而得
    - 因此有6种派生值
  - **BHK** – 来自安全备份寄存器
    - 由安全启动软件初始化，在锁定后，这些寄存器不可再被访问，当检测到入侵事件时，内容将会被清空.
  - **XORK** – BHK和DHUK的异或(XOR)结果

根硬件唯一密钥(RHUK)

- **Root Hardware Unique Key (RHUK)**
  - 密钥长度: 256 位
  - 密钥类型: 不可变更 – 常数
  - 随机值 (256位熵) 每块芯片唯一, STM32通过 HSM(*) 设置
    - 非易失性, 存储在NVM
  - 用来派生DHUK
    - 安全AES不可直接使用它
  - 应用或调试不可访问

给应用带来的益处

✓ 硬件保护的密钥, 对于应用是完全保密的

(*) HSM – 硬件安全模块, 一种高度安全和反侵入式的设备, 用在产线上实现安全功能

life.augmented

硬件派生密钥(DHUK)

- **Derived Hardware Unique Key (DHUK)**
  - 密钥长度: 256 位
  - 密钥类型: 可变更 – 派生产生 – 常数
  - 硬件保护的AES密钥, 每次使用后清除
  - 使用KDF(Key Deviation Function)派生, 输入参数有:RHUK, TrustZone状态,密钥使用状态(KMOD)

DHUK Value	TrustZone State	Key Usage (KMOD)
DHUK_N_S	Secure	Normal state
DHUK_N_NS	Non Secure	
DHUK_S_S	Secure	Share state
DHUK_S_NS	Non Secure	
DHUK_W_S	Secure	Wrap state
DHUK_W_NS	Non Secure	

  - 任何软件,调试或测试模式均不可访问

对应用带来的益处

- ✓ 密钥生成和派生, 防侧信道攻击
- ✓ 提高信任根的鲁棒性
- ✓ 可作为安全存储密钥解密(封装密钥模式)的主密钥
- ✓ 支持业界安全标准(PSA /SESIP/…)
- ✓ 使得一机一密的片上加密存储技术成为可能

life.augmented

启动硬件密钥(BHK)

- **Boot Hardware Key (BHK)**
  - 密钥长度: 256 位
  - 密钥类型: 可变更
  - 由安全启动软件产生
  - 值存储在安全备份寄存器(TAMP_BKP[7:0]R)
  - 锁定后软件不可再访问
  - 当检测到入侵事件后自动清除

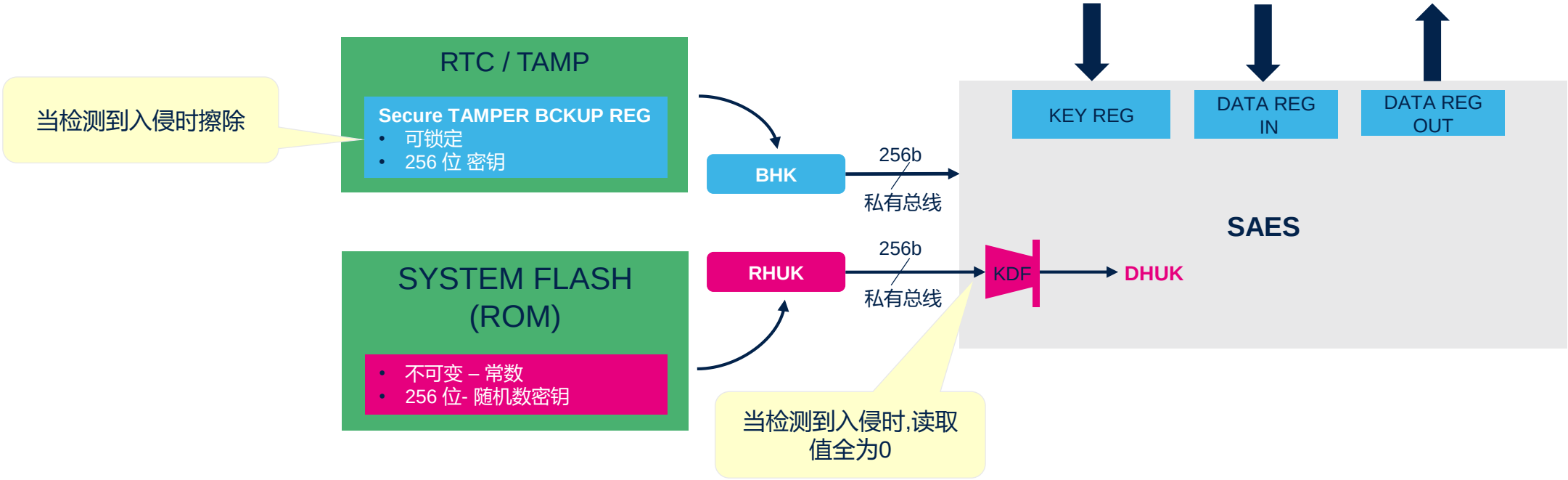
对应用的益处

- ✓ 密钥产生和派生, 防侧信道攻击
- ✓ 提高信任根的鲁棒性
- ✓ 与DHUK异或后的密钥变成与应用相关, 可用于安全存储密钥解密(封装密钥模式)
- ✓ 支持IoT安全标准(PSA /SESIP)
- ✓ 可用于外部FLASH映象解密的主密钥,或IoT点到点解密的共享密钥

安全 AES(SAES) 外设

硬件密钥的两个来源

- SAES通过私有总线接收硬件锁定的密钥, 对CPU和调试均不可见
- 当检测到入侵事件时, 硬件密钥的使用是受限制的



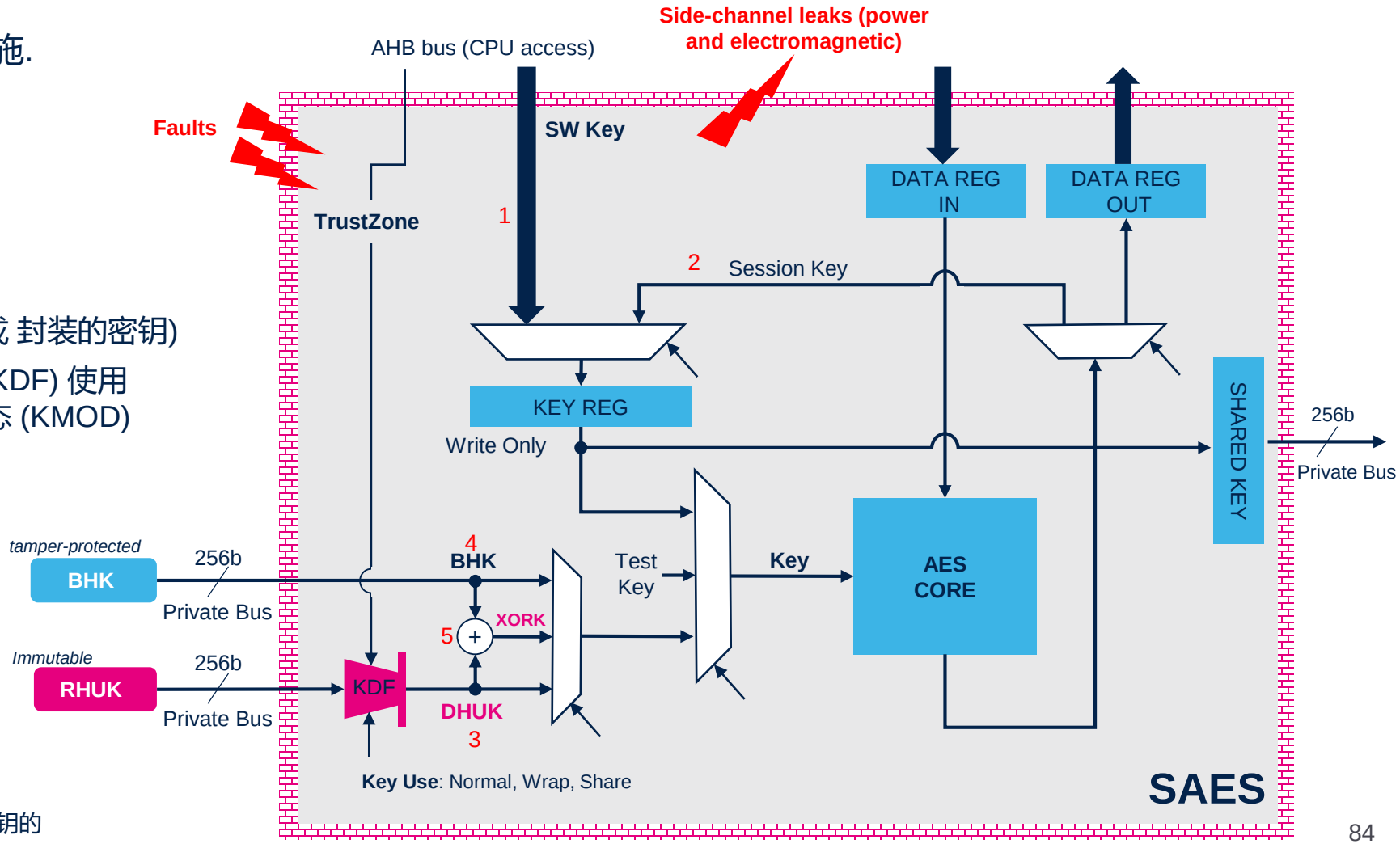
安全 AES(SAES) 外设

密钥管理特性细节

- 针对1阶功率和电磁侧通道攻击的反措施.
  - 缓解2阶侧信道攻击
  - 对抗故障分析的反措施(temporal redundancy)

- 5种密钥输入:
  1) 来自CPU的软件密钥
  2) 硬件保护的会话密钥(解密共享的密钥 或 封装的密钥)
  3) 硬件派生密钥 (DHUK). 密钥派生算法 (KDF) 使用 RHUK, TrustZone 状态 和 密钥使用状态 (KMOD)
  4) 入侵保护的启动硬件密钥(BHK)
  5) XORK – 来自BHK 和 DHUK的异或值

- 密钥共享方式更快, 非DPA AES 引擎

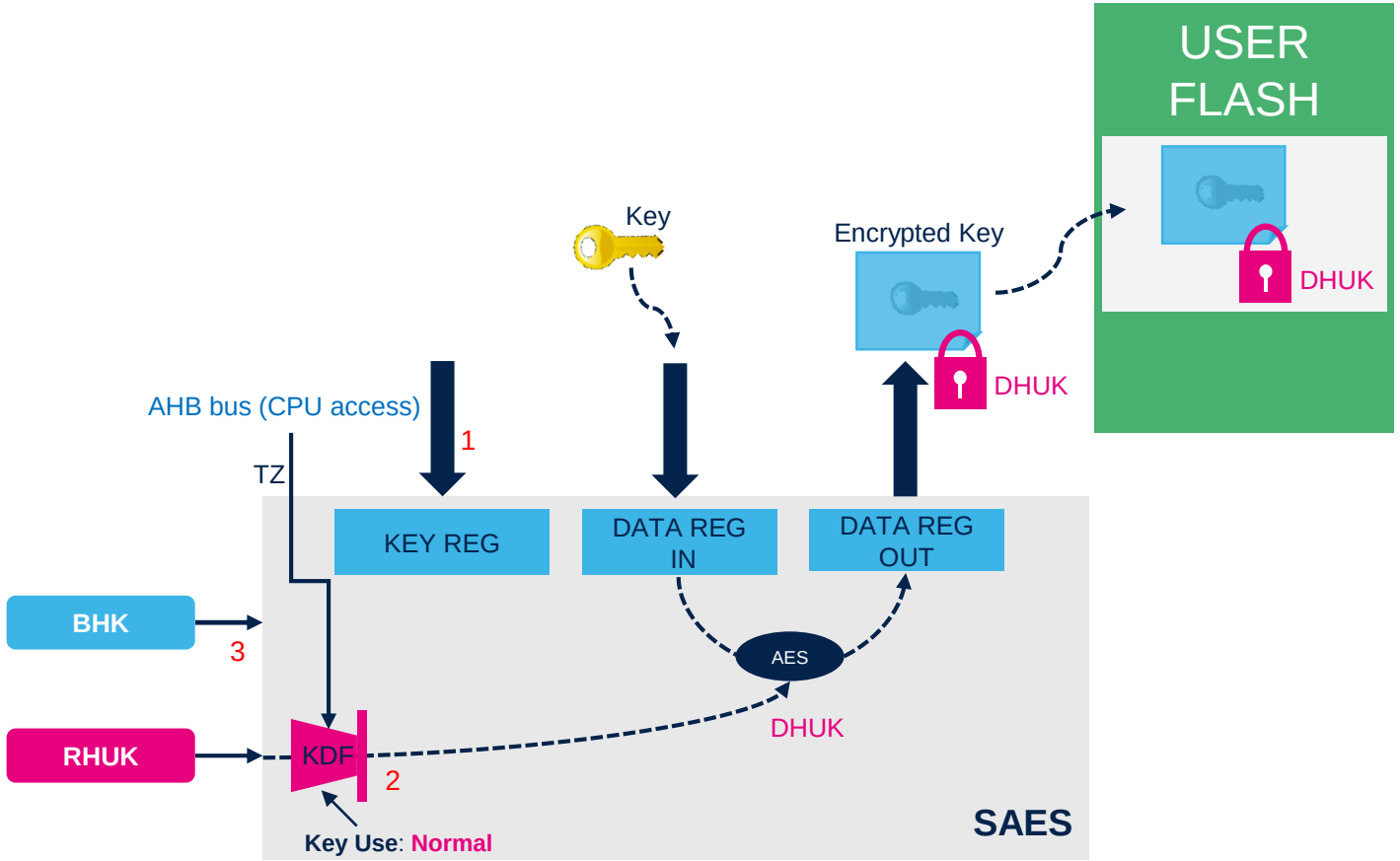


注: KMOD – 是 SAES 寄存器值用来选择密钥的使用方式

安全 AES(SAES) 外设

加密一个密钥或数据

- SAES 可对一个密钥进行加密并放在存储器上
- 5种加密密钥来源:
  1) 来自CPU的软件密钥
  2) 硬件派生密钥 (DHUK). 密钥派生算法 (KDF) 使用 RHUK, TrustZone 状态 和 密钥使用状态(KMOD = =**Normal**）产生
  3) 入侵保护的启动硬件密钥(BHK)
  4) XORK – 来自BHK 和 DHUK的异或值
  5) 会话密钥

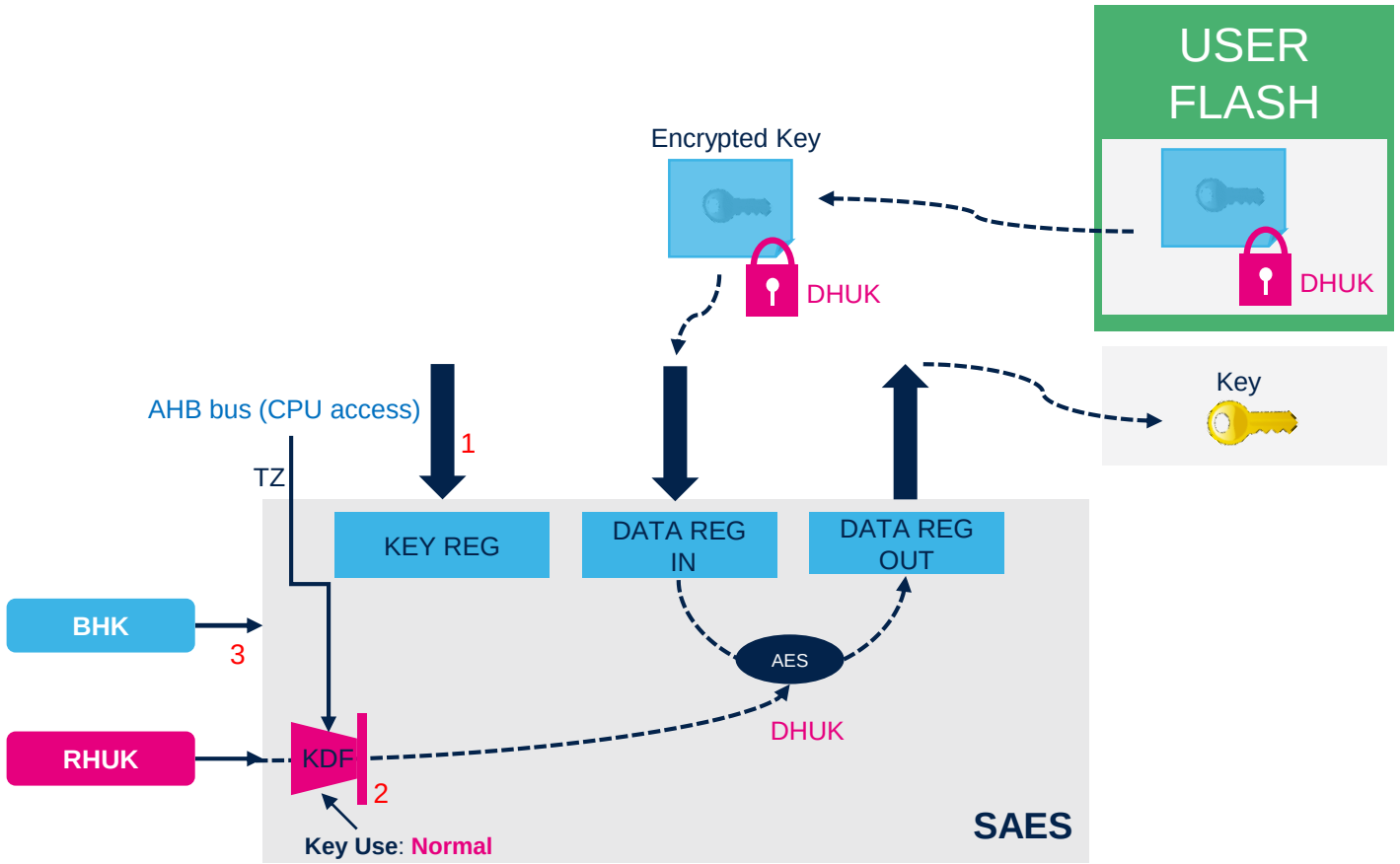


此示例使用DHUK, Normal模式

安全 AES 外设

解密一个密钥或数据

- SAES可解密一个密钥或数据并放在存储器中
- 5种加密密钥来源:
  1) 来自CPU的软件密钥
  2) 硬件派生密钥 (DHUK). 密钥派生算法 (KDF) 使用 RHUK, TrustZone 状态 和 密钥使用状态 (KMOD= =**Normal**）产生
  3) 入侵保护的启动硬件密钥(BHK)
  4) XORK – 来自BHK 和 DHUK的异或值
  5) 会话密钥



此示例使用DHUK, Normal模式

STM32U5 vs. L5: 密码学引擎特性

密码学引擎特性		STM32L5	STM32U5
对称算法	AES-128 或 256 ECB, CBC, CTR, GCM, CCM	AES 外设 (相同)	
	AES-128 或 256 模式 ECB, CBC 侧信道攻击保护 硬件密钥保护	不支持	SAES 外设 通过专门的私有总线将密钥分享给普通AES外设
非对称算法	基于GF(p)的RSA、DH和ECC公钥 primitives	PKA 外设 32位存储	PKA 外设 64位存储, 更快内核, 防DPA攻击
哈希算法 (+HMAC)	摘要值: MD5, SHA-1	HASH 外设 (相同)	
	密码学哈希: SHA-256, SHA-224		
随机数	FIPS 140-2 NDRNG (NIST SP800-90B certifiable)	RNG 外设	RNG 外设 专门的总线, 防侧信道攻击
存储器加密	OTFDEC	OTFDEC 外设 (相同)	

life.augmented

SBSFU和TFM 示例

SBSFU 示例
(U5 DK 板)

MCU boot

Secure application template
(“Basic” Secure GPIO toggle)

安全启动
安全固件更新

TFM 示例
(U5 DK 板)

MCU boot

TFM-core

*each crypto algorithm can be independently deactivated

Initial Attestation

Secure Storage

Internal Trusted Storage

Secure Crypto

运行时使用安全服务的安全应用

非常容易移植到NUCLEO板...

□: 模块化

life.augmented

Thank you

life.augmented