life.augmented

STM32L5 入门课程系列

04. STM32L5的系统新架构

Lilian YAO

课程内容一览

STM32L5快速入门		
课程章节名称	章节介绍	时长
03. 认识ARM Cortex-M33内核	从内核角度认识TrustZone，包括为了支持TZ功能而在内核里新增的外设，以及原有内核外设为了支持该功能的更新	40 分钟
04. STM32L5的系统新架构	光有内核的TrustZone是不够的，STM32L5把“隔离”的概念和措施从内核延伸出来，部署到了全片系统	20 分钟
05. TrustZone环境下新的用户编程模型	通过GPIO toggle例程，体会新的用户编程模型，深入理解Cortex-M33内核和STM32L5外设对TZ的支持和使用	30 分钟
06. STM32CubeMX对TrustZone环境的支持	使用STM32CubeMX在STM32L5上生成TZ应用初始代码及其框架，添加用户应用逻辑，实现前三节课里讲的知识点	20 分钟
07. STM32L5的低功耗特性	理解L5的供电策略、各种低功耗模式，内置DC/DC SMPS的使用，以及外设对于低功耗方面的设计考虑，BAM模式介绍	

STM32L5的安全特性，不仅仅是TZ

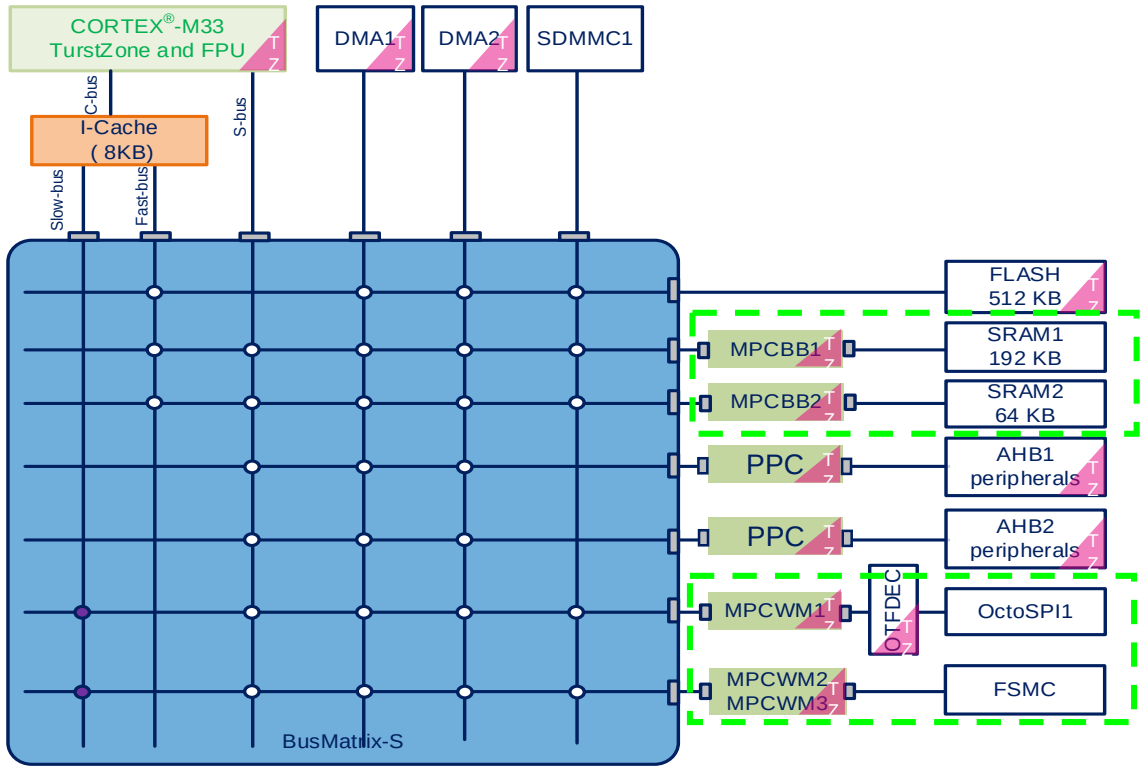
- 支持安全启动，信任链锚点
  - Boot Lock，可保证唯一启动入口
  - HDP，可隐藏的安全用户闪存区域
- TZ赋予STM32L5对隔离的硬件支持
  - 从内核扩展到全片系统
  - AHB总线主设备：DMA
  - 存储模块
    - Flash, SRAM, 外部存储区，…
  - 系统模块（TZ aware）
    - Clock、PWR、EXTI、SysConfig、…
  - 外设
    - securable外设
    - TZ aware 外设
- 对软件IP和敏感数据的保护
  - 安全调试
  - 存储在外部闪存区域的密文，可实时解密执行和读取
- 对密码学操作的硬件支持
  - 真随机数产生器（TRNG）
  - 对称加解密、非对称加解密
- 外部监测
  - 防篡改检测从static到active的升级
  - 时钟、供电电压、环境温度的实时监测
- 可信执行环境(TFM)、安全生产(SFI)

life.augmented

TZ从内核向外扩展...

- **内核**传递出来的transaction，**具有S和NS属性**
- **在AHB5总线上，使用信号“HNONSEC”来表示**
- **芯片上其他外**设模块如何识别？
  - **非TZ aware的外**设，需要通过TZSC**来定义**
  - TZ aware**的外**设，自己有对应寄存器来控制

TZ aware的外设			
总线	外设	总线	外设
AHB1	GTZC – MPCBB/TZIC/TZSC(MPCWM)	AHB2	GPIOA, …. GPIOH
	EXTI	AHB2	OTFDEC
	Flash memory	APB1	PWR
	RCC		RTC
	DMA1/DMA2/DMAMUX1	APB2	SYSCFG



GTZC：全局TZ控制器
由三个子模块组成

MPCBB – block based

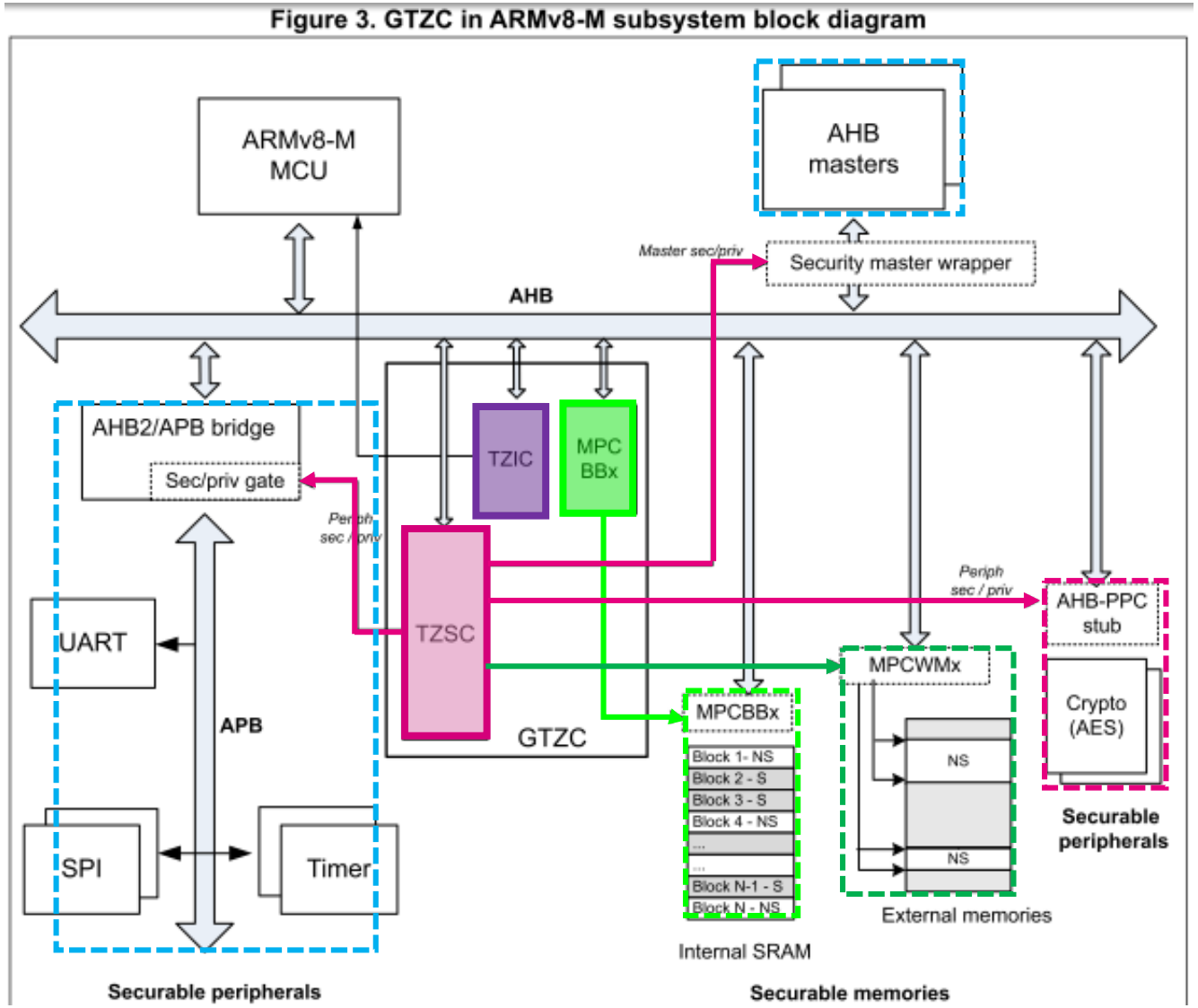
- 设置片上SRAM1、SRAM2的安全属性
- 以block（256字节）为单位

TZSC – TZ security control

- 设置片外存储区FSMC、O-SPI的安全属性
  - water mark的方式设置NS范围
- 设置master/slave外设的安全性和特权性
  - AHB slave外设、master外设
  - APB slave外设

TZIC – TZ illegal access concentrator

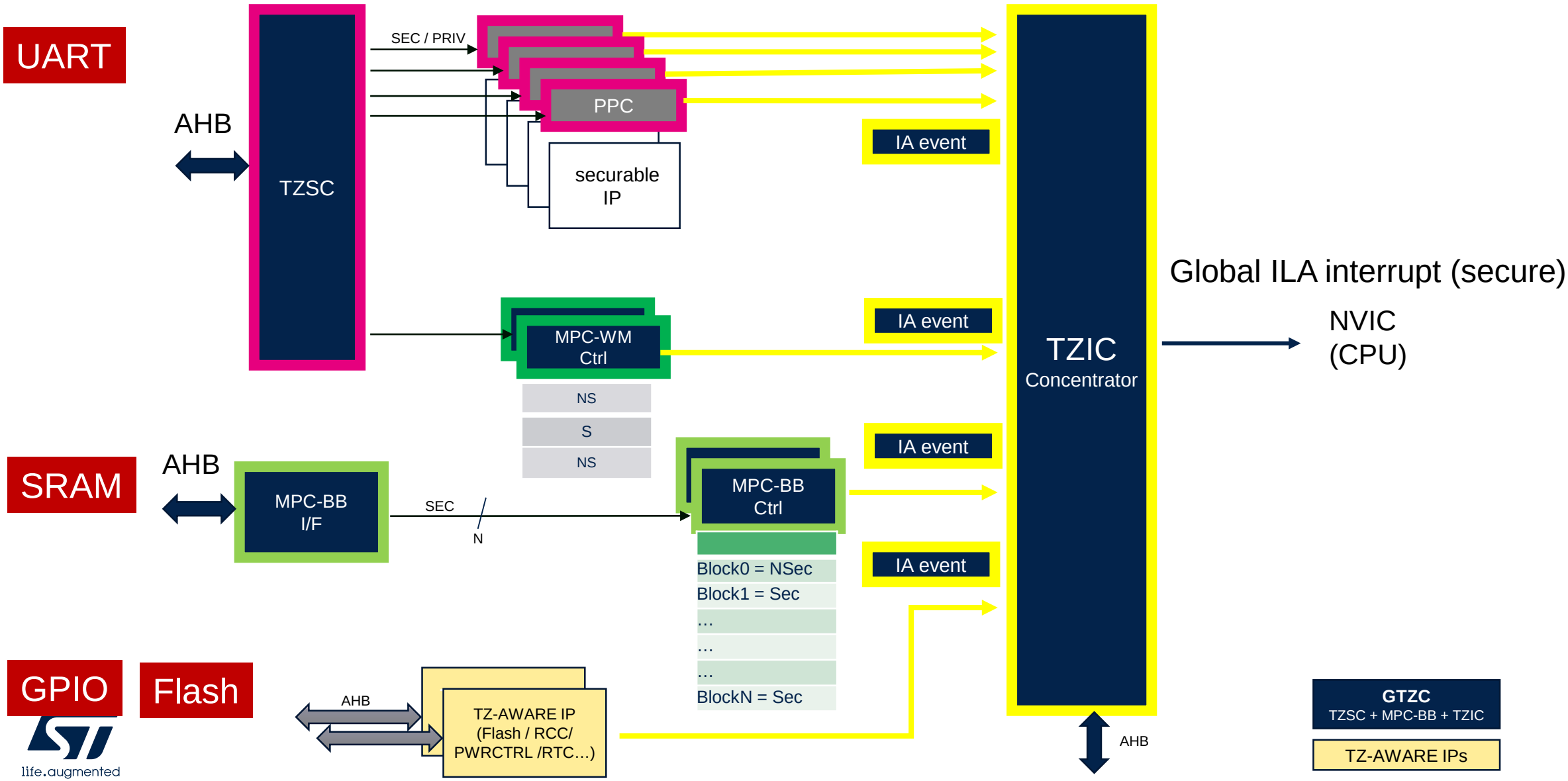
- 监测所有安全相关的非法访问并触发中断



life.augmented

GTZC = MPCBB + TZSC + TZIC

举个例子



life.augmented

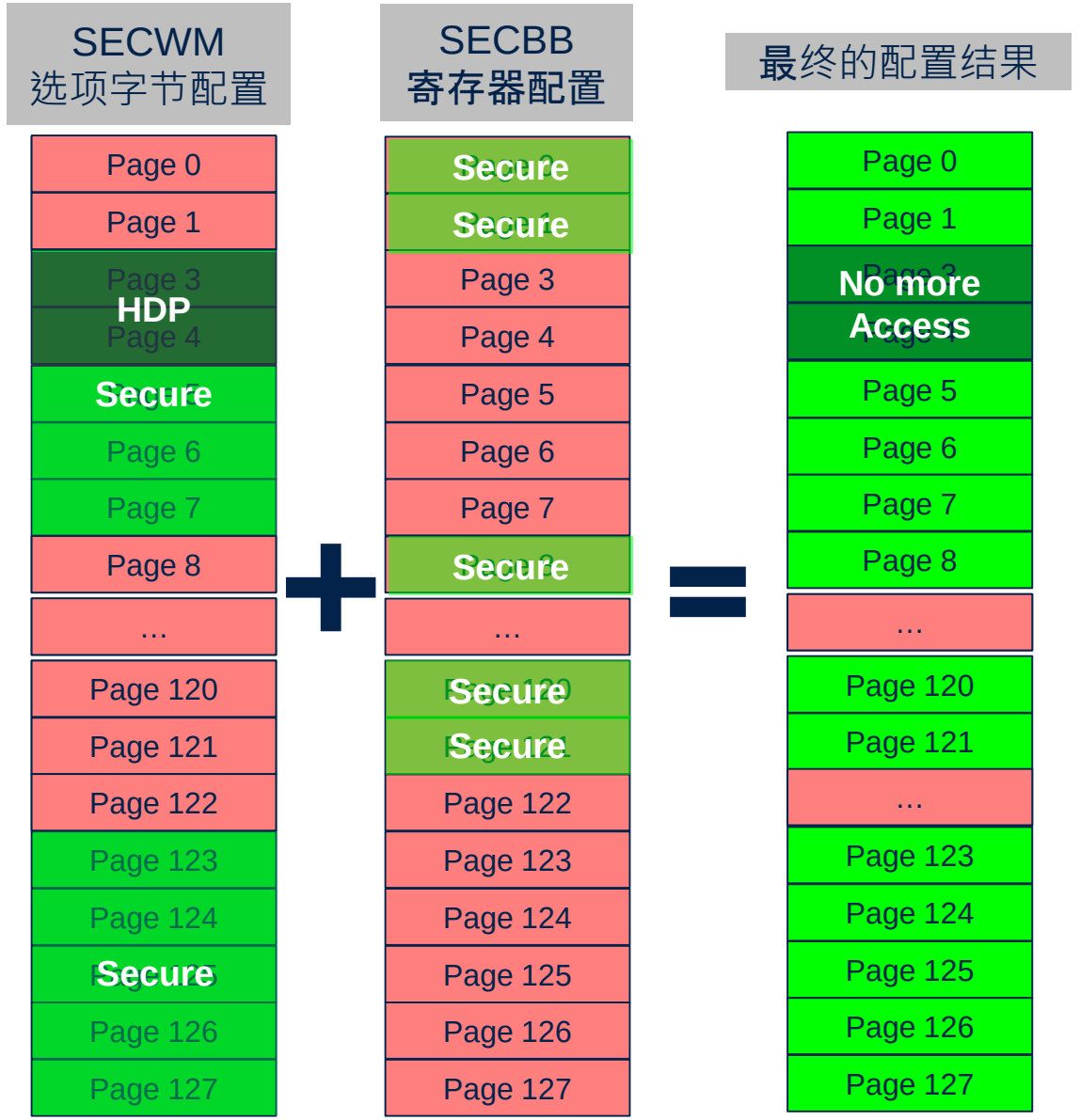
片上Flash的TZ 安全性

TZ-aware IP

- 通过选项字节，以watermark的方式，定义“S” 区域和HDP区域 @ 静态配置
  - HDP区域是“S”区域的一部分，起始地址相同，尺寸自定义
  - 首次使能TZ后，选项字节的初始状态是全部都是S，没有HDP区域
- 通过寄存器，以page为粒度，定义“S”区域和“NS”区域 @ 动态配置
  - 复位值，全部page都是NS
- 区域从S属性改成NS配置后，内容不会被自动擦除，需要用户自己操作
- “S”和“NS”区域的擦除、写操作，使用对应模式下的控制和状态位来完成，中断分别映射到Flash_S和Flash_NS
  - NVIC的两根中断线

编号	名称	地址
6	FLASH	0x0000 0058
7	FLASH_S	0x0000 005C

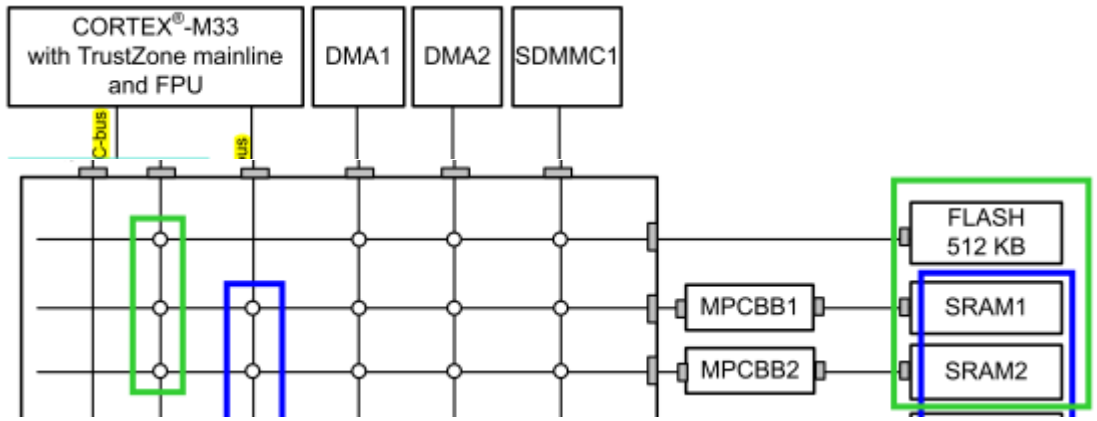
- 其他安全特性
  - RDP0.5，安全调试



Securable IP

片上SRAM的TZ 安全性

- TZ使能的情况下，复位后，所有SRAM都是“S”的
  - 可通过GTZC的MPCBB子模块，把SRAM部分区域设置成“NS” → 动态配置
  - 以256字节为单位设置不同的安全属性



SRAM1：192KB 768个page	Page 0 ~ 31	GTZC_MPCBB1_VCTR0 [0:31]	复位值： 1 → S 0 → NS
	Page 32 ~ 63	GTZC_MPCBB1_VCTR1 [0:31]	
	…	。。。。。。	
	Page 767	GTZC_MPCBB1_VCTR23 [0:31]	
SRAM2：64KB 256个page	Page 0/768	GTZC_MPCBB2_VCTR1 [0:31]	同上
	…	。。。。。。	
	Page 255/1023	GTZC_MPCBB2_VCTR7 [0:31]	

- SRAM2的其他安全特性
  - 受RDP保护；可以设置SRAM2的写保护，粒度以1K字节单位
  - 可配置对其ECC保护 → SIL和ClassB应用

life.augmented

TZ-aware IP

GPIO的TZ 安全性

- TZ使能的情况下，复位后，所有引脚都是“S”的
  - 可通过寄存器(GPIOx_SECCFGR)，把引脚单独配置成“NS” → 动态配置
  - 每个引脚可以独立配置
- 当引脚处于“S”，它相关的AF、模式选择、IO数据等寄存器位，也都是“S”
  - 对这些“S”状态下的寄存器的NS访问，效果都是：RAZ/WI (Read as Zero / Write ignore)
  - 但是并不产生非法访问事件/中断
- 某个引脚的安全状态，要和它所连的外设的安全状态匹配
  - IO vs. AF IP
  - IO vs. 模拟外设

引脚属性	AF选择的外设		模拟外设	
	安全外设	非安全外设	安全外设	非安全外设
安全 - S	OK	nOK	OK	nOK – 模拟开关断开
非安全 – NS	nOK - 无论引脚上电平，外设看到都是0；无论外设怎么驱动，引脚输出0	OK	nOK	OK

life.augmented

TZSC – TZ security control

Securable IP

- 设置master/slave外设的安全性和特权性
  - AHB master外设 - SDMMC
  - AHB salve外设、**APB slave外设**

GTZC_TZSC secure configuration register 1 (GTZC_TZSC_SECCFGR1)

Bit 21 **LPUART1SEC**: secure access mode for LPUART1
- 0: non-secure
- 1: secure

Bit 13 **UART5SEC**: secure access mode for UART5
- 0: non-secure
- 1: secure

Bit 12 **UART4SEC**: secure access mode for UART4
- 0: non-secure
- 1: secure

Bit 11 **USART3SEC**: secure access mode for USART3
- 0: non-secure
- 1: secure

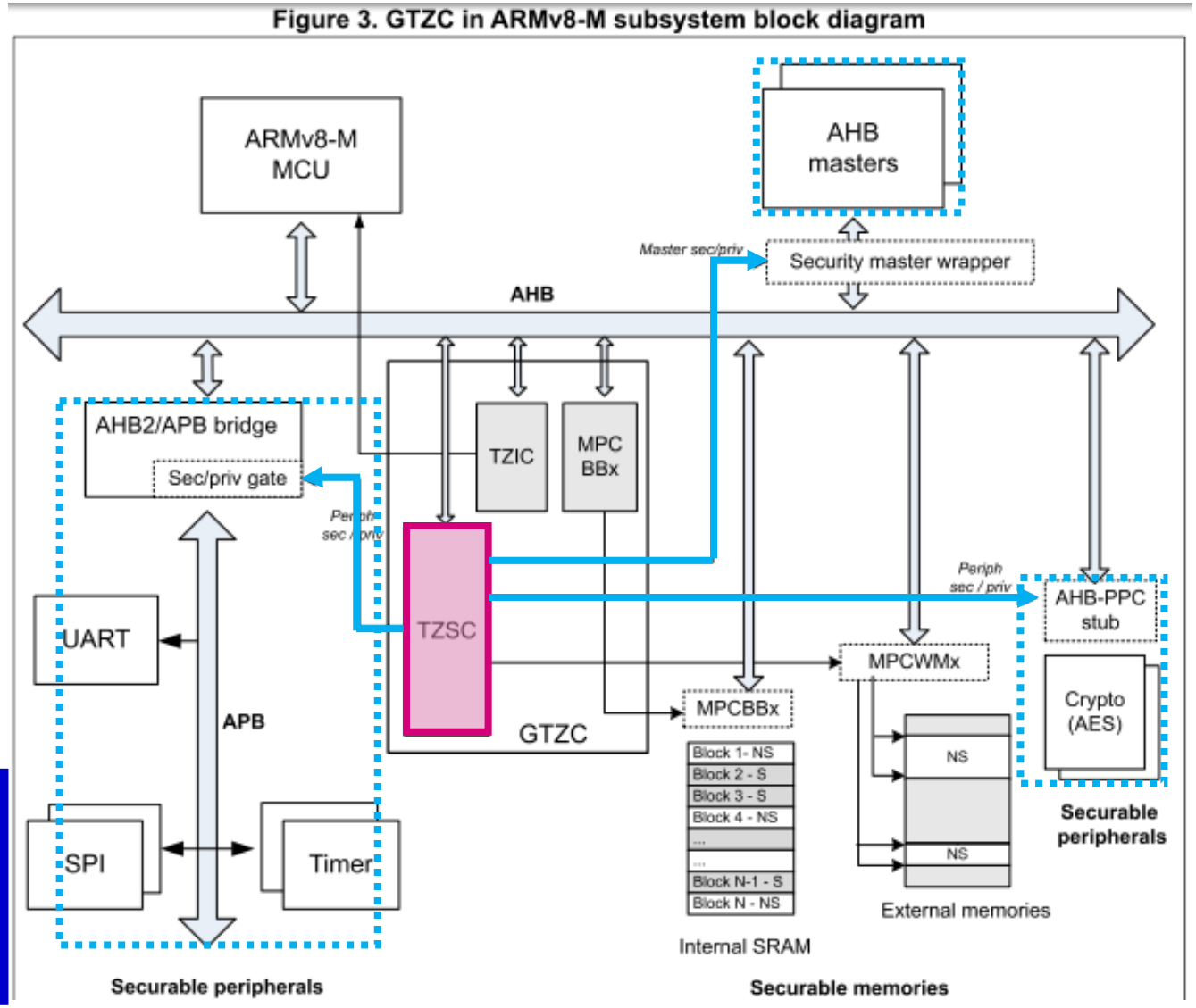
Bit 10 **USART2SEC**: secure access mode for USART2
- 0: non-secure
- 1: secure

GTZC_TZSC secure configuration register 2 (GTZC_TZSC_SECCFGR2)

Bit 1 **USART1SEC**: secure access mode for USART1
- 0: non-secure
- 1: secure

UART的TZ 安全性

Figure 3. GTZC in ARMv8-M subsystem block diagram



life.augmented

各种模块的复位默认安全状态

- 内核
  - 处于安全状态，启动地址必须在安全区域里
- 内核从SAU/IDAU 看出来
  - 所有的地址空间都是安全的

- 片上Flash
  - 选项字节初始watermark设置：全部安全
  - 寄存器block base设置：全部非安全
  - 综合结果：全部安全
- 片上SRAM
  - 寄存器block base设置：全部安全

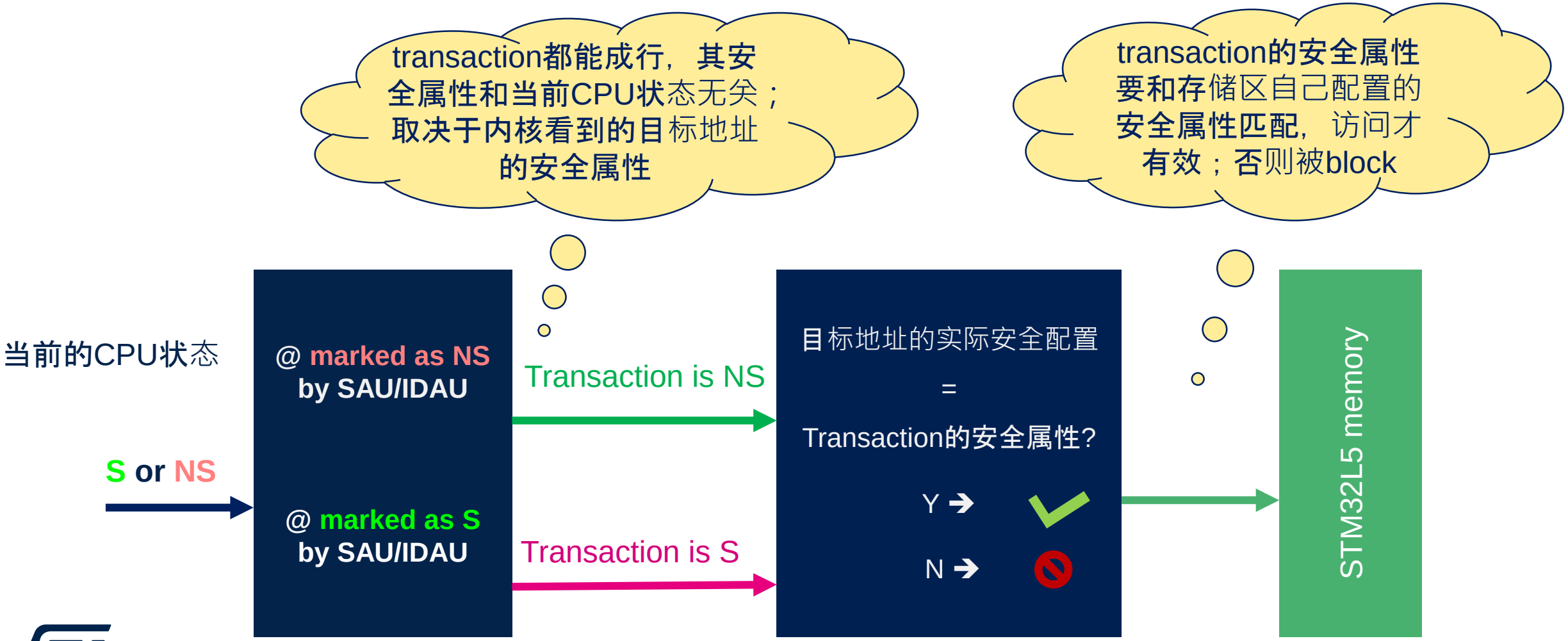
- 片外存储区
  - 寄存器watermark设置：全部安全
- GPIO端口
  - 引脚全部安全
- 其他外设
  - Securable外设：全部非安全 (例如：LPUART1)
  - TZ-aware外设：全部非安全 (例如：OTFDEC)
- 中断
  - 全部中断都target到安全状态
  - 有独立的NVIC_S和NVIC_NS

life.augmented

资源访问规则

- CPU对片上资源的访问，遵循的主要原则
  - 第一级检查：从内核看出去
    - SAU、IDAU，从安全/非安全的角度检查 transaction是否valid
    - MPU_S、MPU_NS，从特权级别/非特权级别的角度检查 transaction是否valid
  - 第二级检查：目标资源自身的安全配置，是否可以接受这样的访问
    - Flash控制器，知道目标片上Flash地址的安全性
    - GTZC.MPCBB，知道目标片上SRAM地址的安全性
    - GTZC.TZSC.MPCWM，知道目标片外存储地址的安全性
    - GTZC.TZSC.PPC，知道目标外设的安全性 @ Securable 外设
    - TZ-aware 外设，自身知道自己的安全性

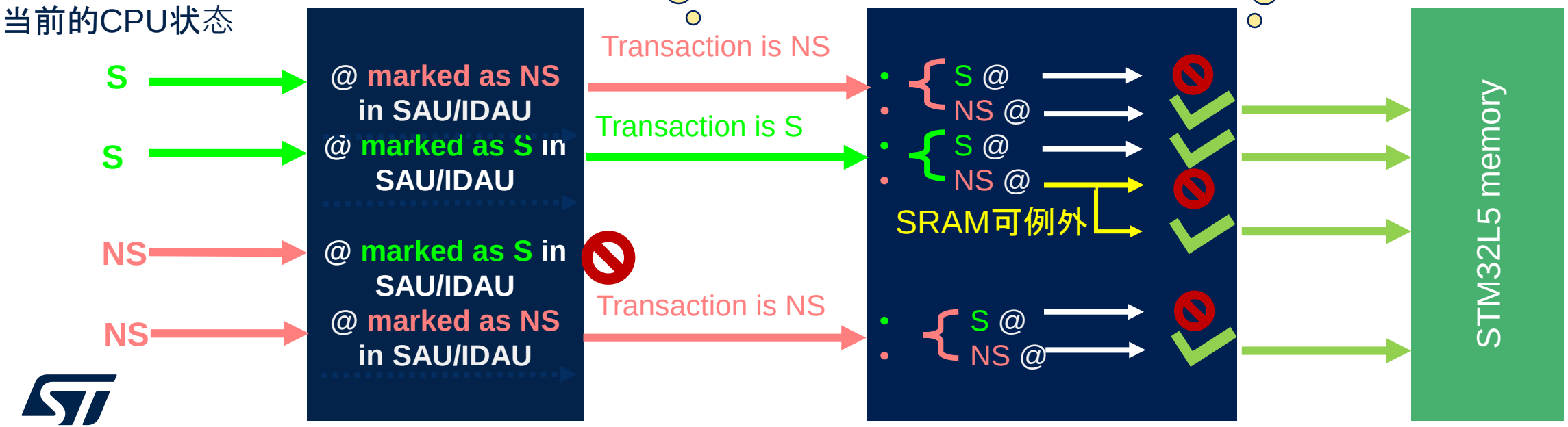
资源访问规则 . (存储区上的)取指



资源访问规则．存储区上的数据访问

NS状态的CPU访问它看来的S区域，**会被block**；S状态的CPU访问它看来的S区域，transaction **具有S属性；其他都是NS属性**

transaction**的安全属性要和存**储区自己配置的安全**属性匹配**，访问才有效；否则被block

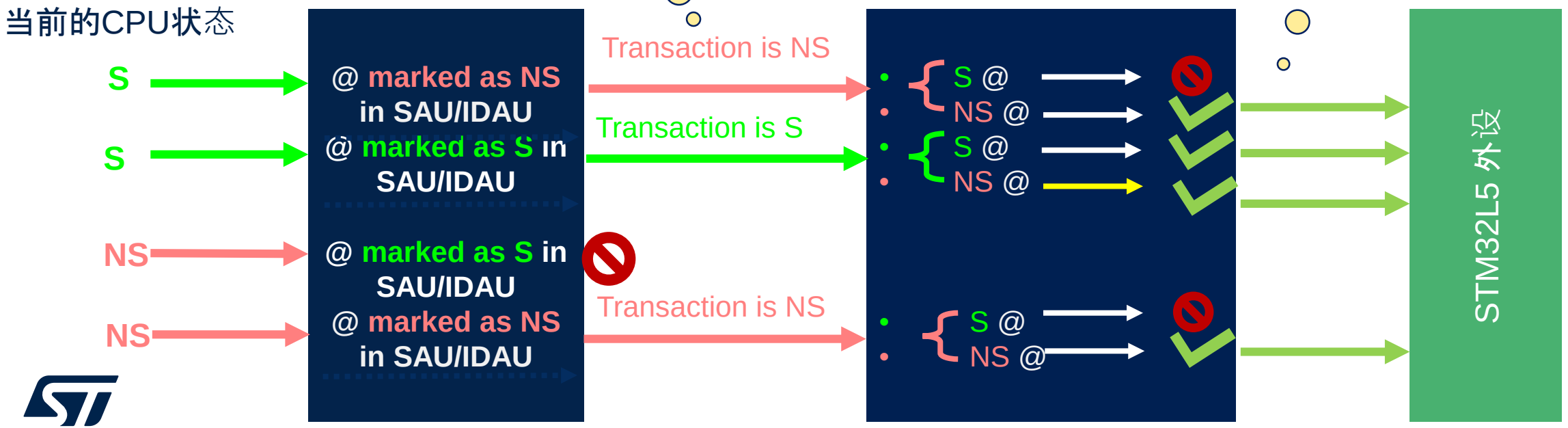


life.augmented

资源访问规则．外设访问

NS状态的CPU访问它看来的S区域，会被block；S状态的CPU访问它看来的S区域，transaction具有S属性；其他都是NS属性

只有NS属性的transaction访问S属性的外设，才会被block

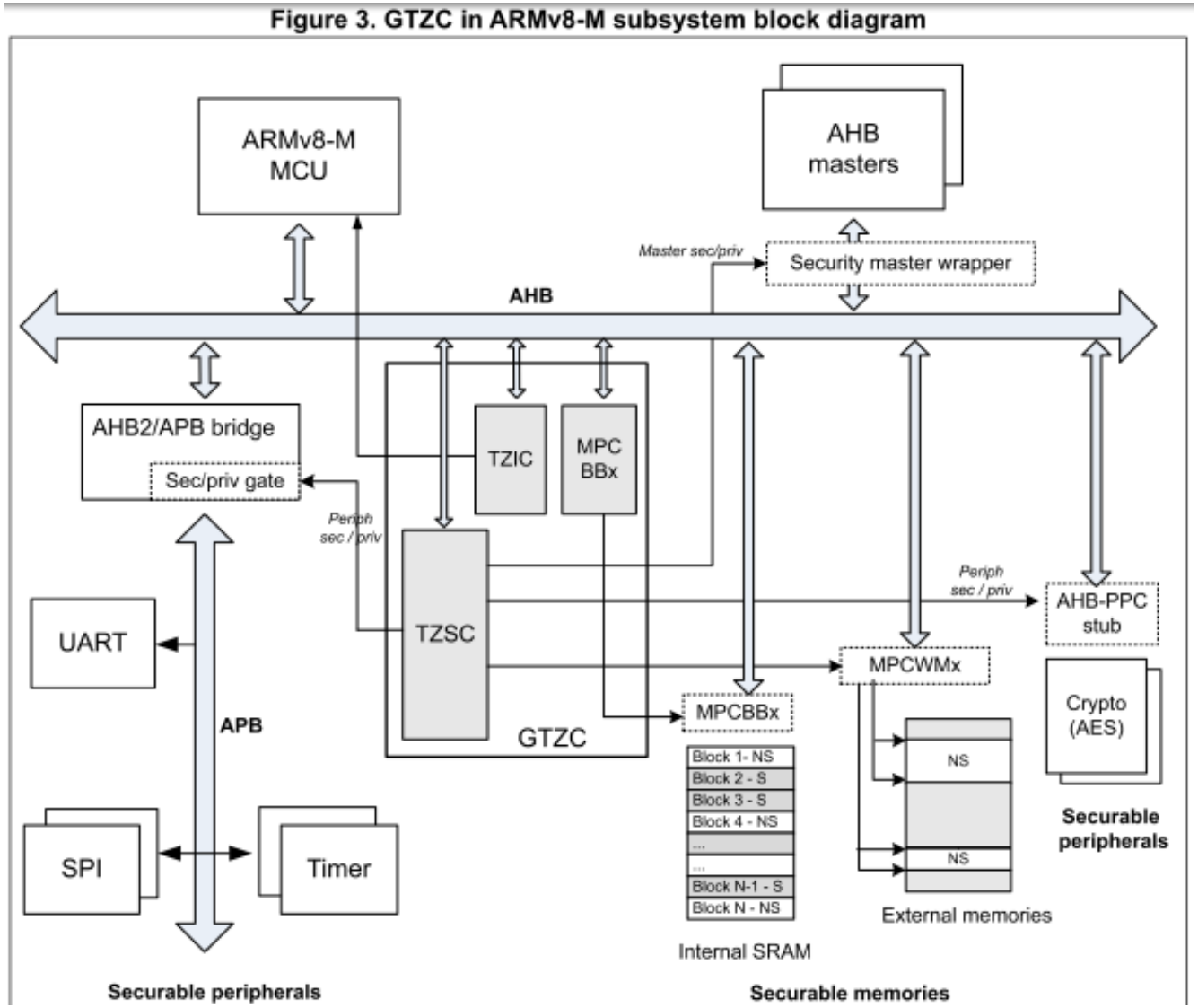


life.augmented

小结

- TZ aware的设备，可以配置自身的安全属性
- 非TZ aware，又Securable的设备，通过GTZC配置自身的安全属性
- CPU对片上资源的访问，经过两级检查
  - SAU/IDAU检查是否可以发出该访问
  - 物理设备检查是否可以接受该访问

Figure 3. GTZC in ARMv8-M subsystem block diagram

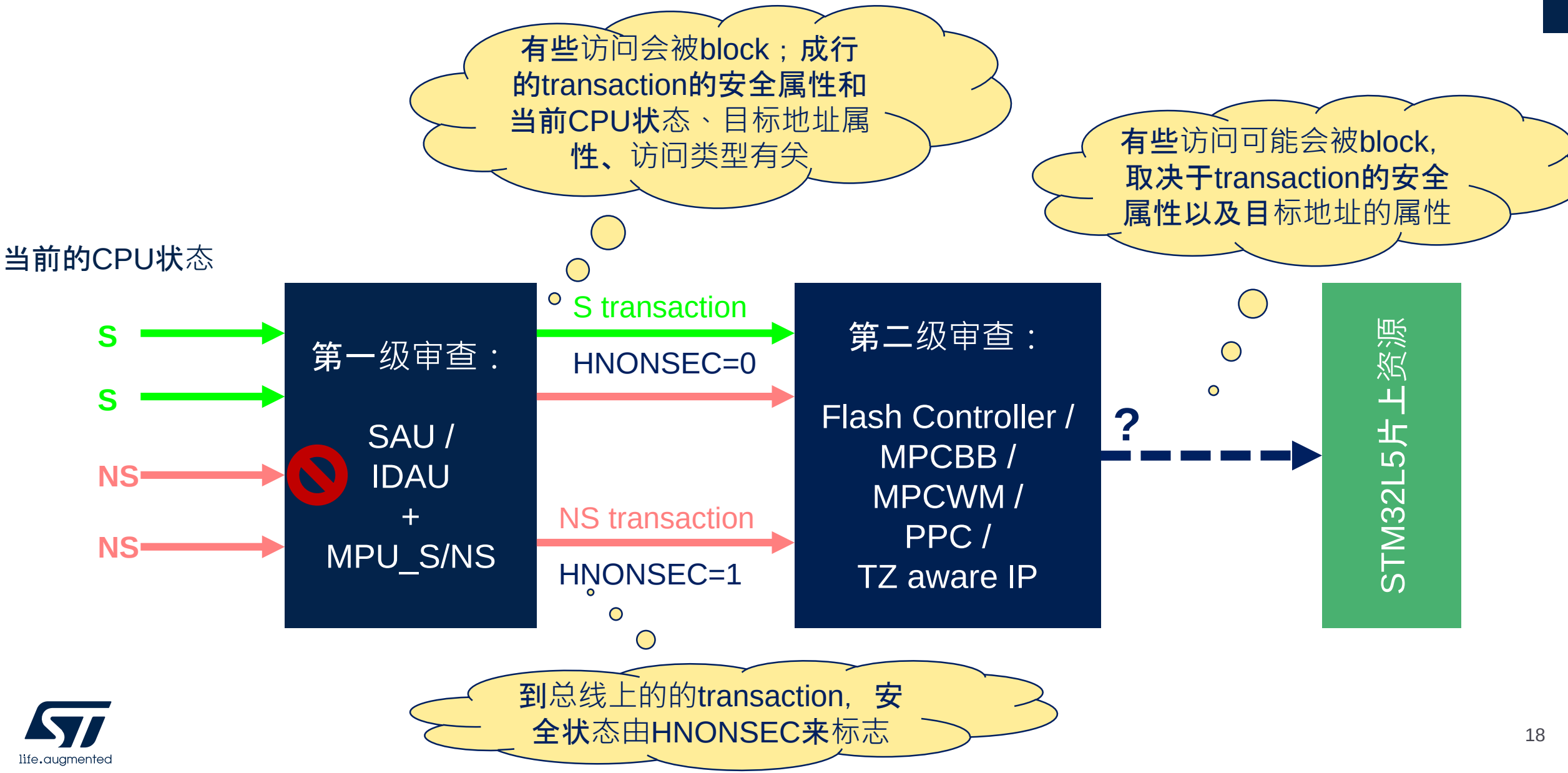


life.augmented

Thank you

life.augmented

资源访问总体规则 . 图解


有些访问会被block；成行的transaction的安全属性和当前CPU状态、目标地址属性、访问类型有关
有些访问可能会被block，取决于transaction的安全属性以及目标地址的属性
当前的CPU状态
S
S
NS
NS
第一级审查：
SAU / IDAU + MPU_S/NS
S transaction
HNONSEC=0
NS transaction
HNONSEC=1
第二级审查：
Flash Controller / MPCBB / MPCWM / PPC / TZ aware IP
?
STM32L5片上资源
到总线上的的transaction，安全状态由HNONSEC来标志