life.augmented

STM32L5，从通用到安全

STM32 全国研讨会

2020年9月

STM32

主要内容

1 STM32L5 DEMO SHOW

2 STM32L5，兼顾高性能和低功耗

3 STM32L5的安全，除了TrustZone还有更多

4 不仅芯片，生态系统同样出类拔萃

life.augmented

STM32CubeMonitor-Power - v1.1.1

STM32 CubeMonitor-Power

RELEASE CONTROL | CALIBRATE | RESET TARGET | GET TEMPERATURE (°C) 33.0

Board firmware version 1.0.4

ACQUISITION & REPLAY | ULP BENCH

CONFIGURATION

Sampling Frequency [Hz] 100

Acquisition Time [s] ∞

Current threshold [µA] 1000

Trigger source sw

Trigger delay [ms] 1

Input Voltage [mV] 3300

Functional Mode

START ACQUISITION

Show Report

155000 150000 145000 140000 135000 130000 125000 120000 115000 110000 105000 100000 95000

2 2.5 3 3.5 4 4.5 5 5.5 6 6.5 7 7.5 8 8.5 9 9.5 10

Time (s)

SAVE GRAPH | ADD DATA LOG

STM32L5： 兼顾高性能和低功耗

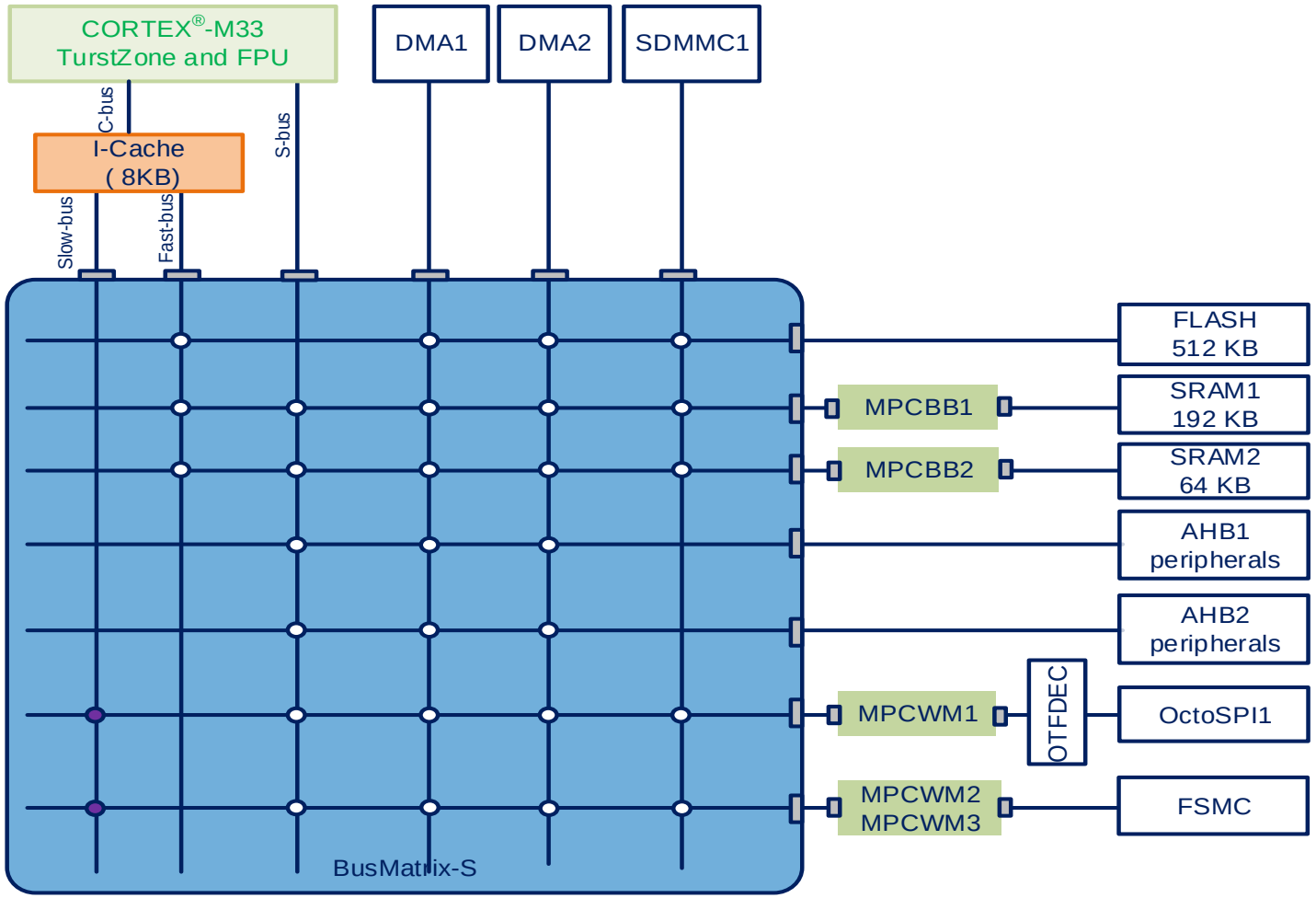
高性能，不仅仅是主频

低功耗，我有一颗绿色的心

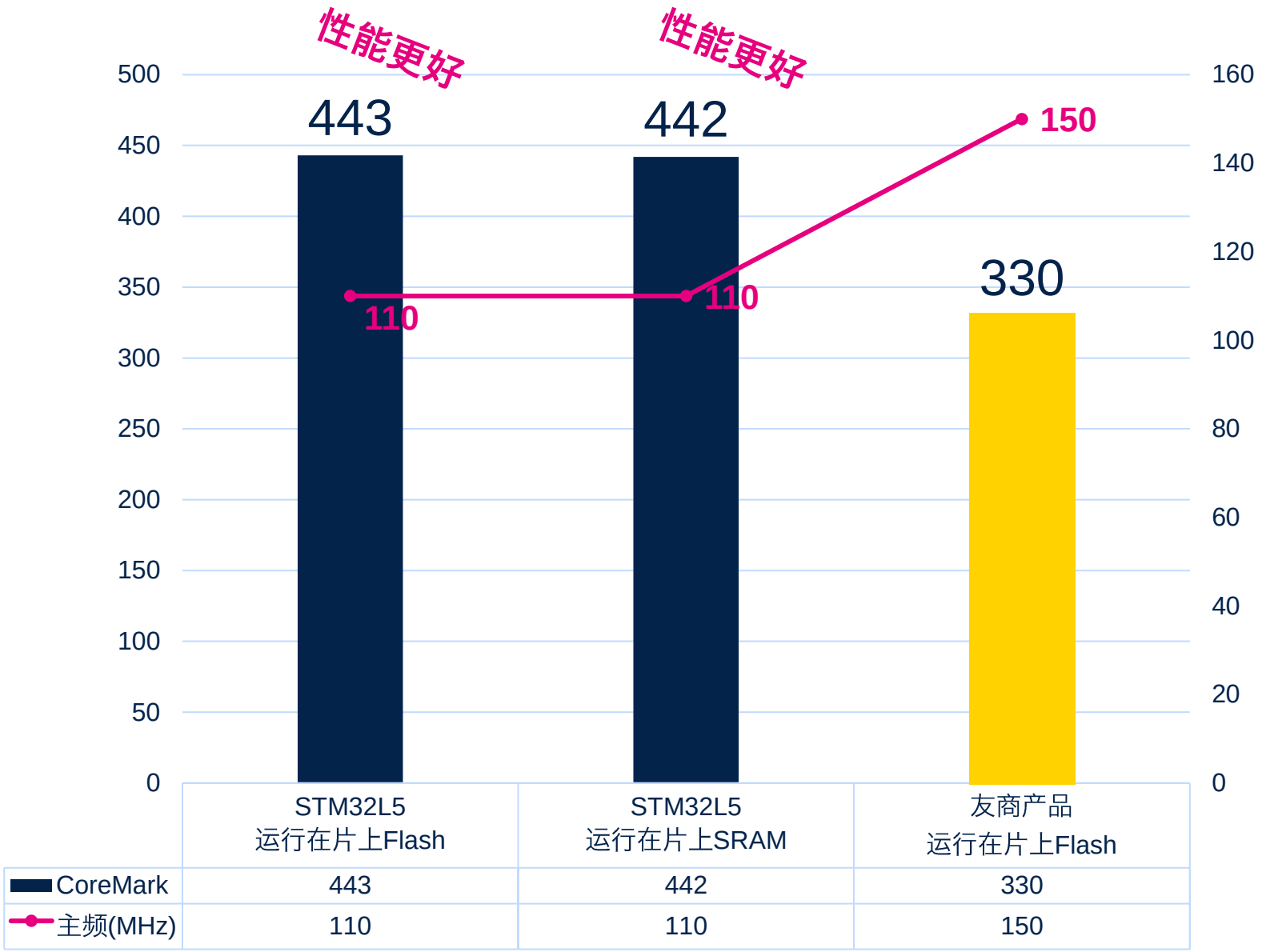
life.augmented

性能更好，响应更及时

- CM33内核
  - 内核性能比CM4 +20%
- 110MHz 主频
- 8KB ICACHE
  - 对片上、片外Flash都可加速
  - Cache miss时的优化策略，降低失效延时
- Flash 等待周期
- AHB总线矩阵提高并行性
- Crypto硬件引擎



CoreMark跑分

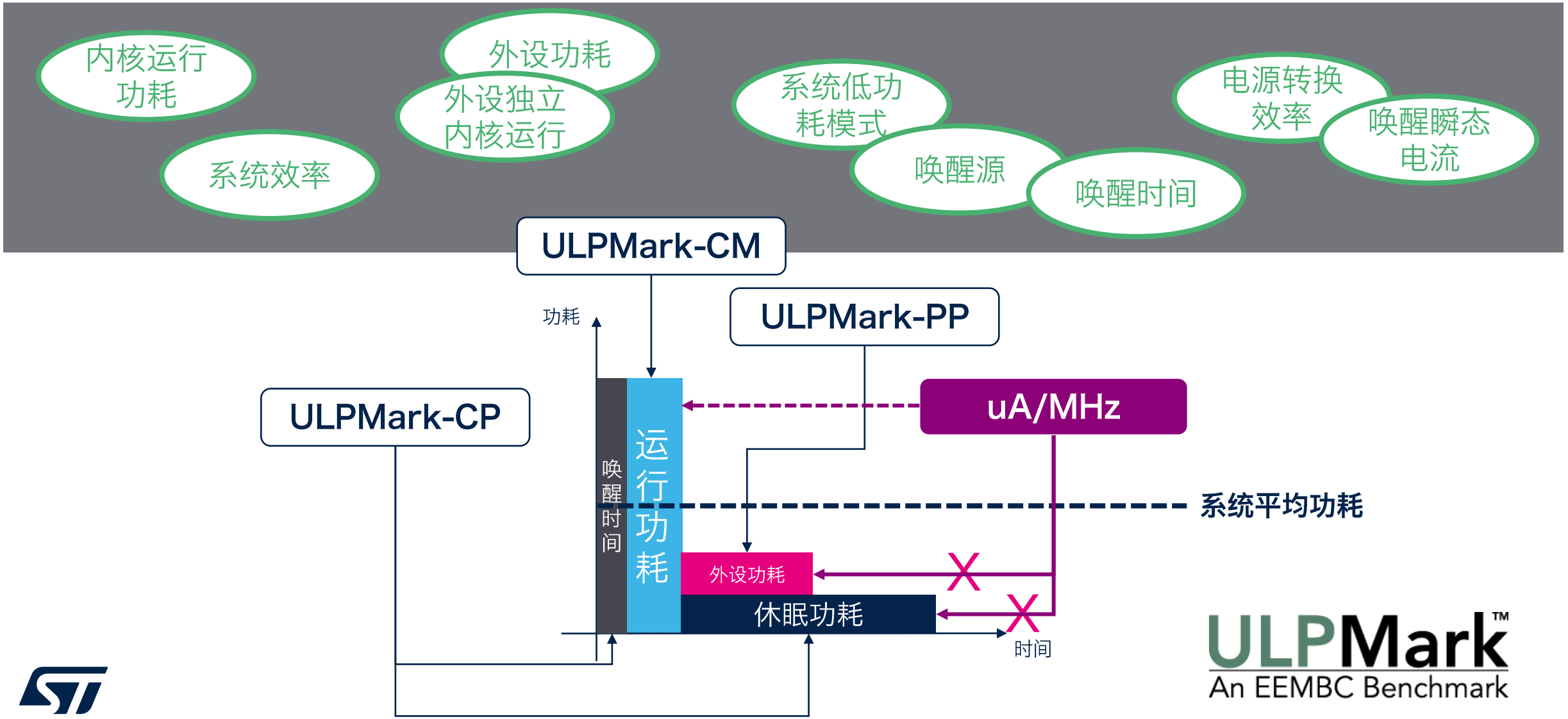


	STM32L5 运行在片上Flash	STM32L5 运行在片上SRAM	友商产品 运行在片上Flash
CoreMark	443	442	330
主频(MHz)	110	110	150

- 性能高低，不仅仅看主频
  - 443分 vs. 330分
  - 110MHz vs. 150MHz
- 8KB ICACHE，对片上、片外Flash都可加速
- Flash 等待周期更短
  - 6个时钟周期 vs. 12个时钟周期

life.augmented

MCU低功耗 ≠ uA/MHz



ULPMark™
An EEMBC Benchmark

life.augmented

STM32L5，为低功耗而优化

- 供电策略：新增对内置SMPS的集成
  - P/N：STM32L5x2xxxx**Q**
- 多种系统低功耗模式
  - LPRun, Sleep, LPSleep, Stop0/1/2, …
- 为低功耗应用助力的系统模块
  - ICACHE、MSI
- 专为低功耗应用优化的外设模块
  - LPUART、LPTIM、DAC
- 专为低功耗应用优化的工作模式：**BAM**

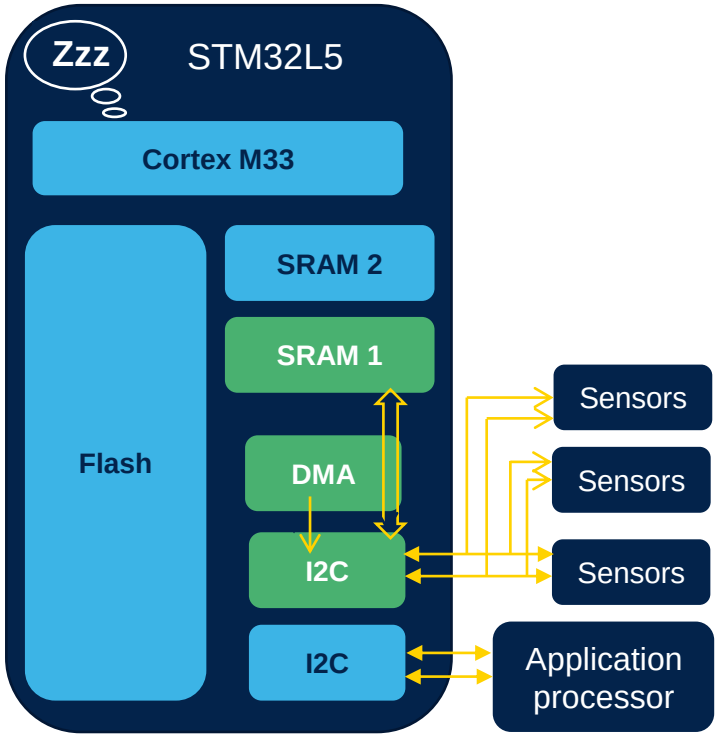
电源转换效率

系统低功耗模式

系统效率

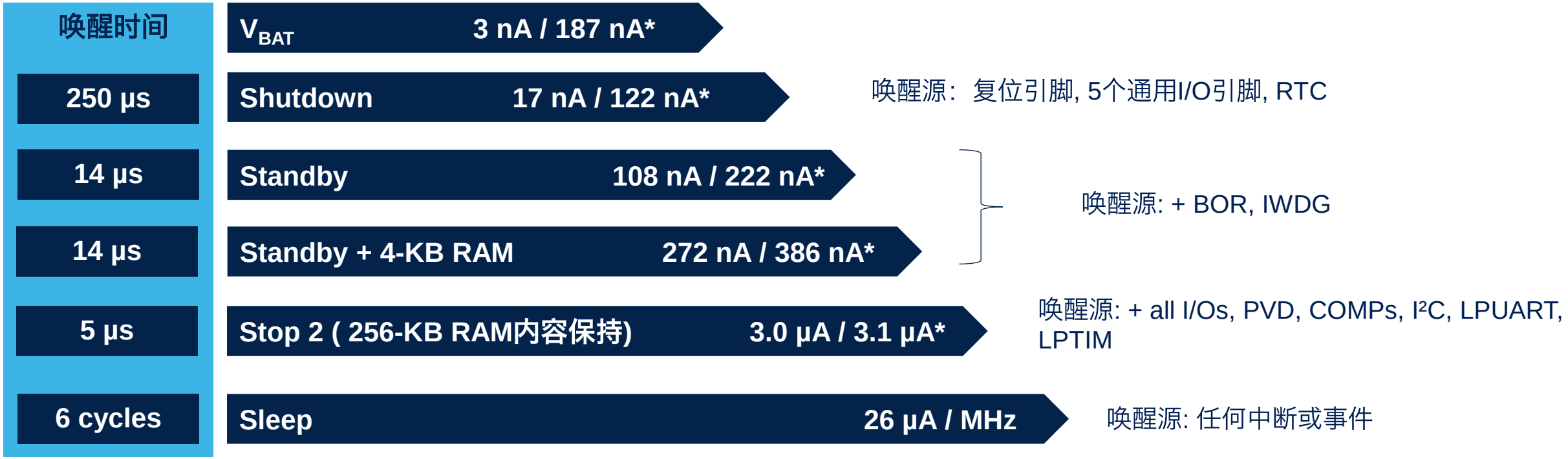
外设功耗

外设独立内核运行



life.augmented

STM32L5，多种系统低功耗模式



注意 : * RTC工作 / RTC不工作

life.augmented

STM32L5：保护您设备的信息安全

安全，

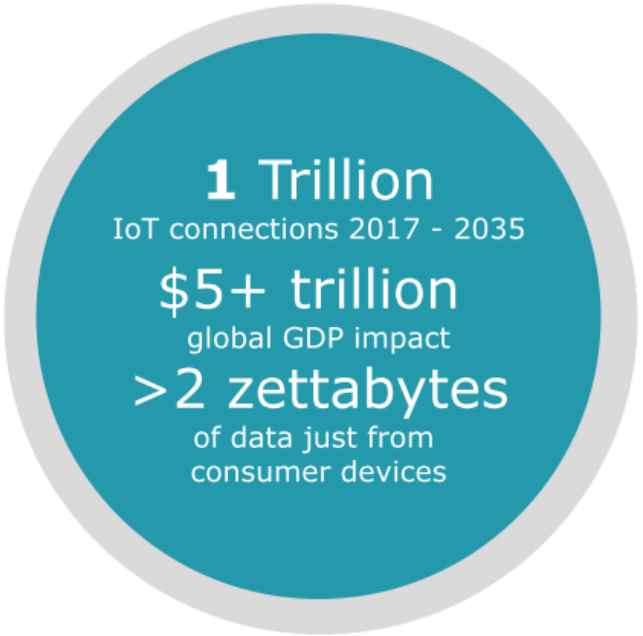
不仅仅是加解密；

在隔离方面，除了TrustZone还有更多

life.augmented

为什么需要信息安全?

- 全球网络威胁不断攀升，每个联网设备都可能面临威胁
- 设备复杂度引起的漏洞
- 供应链污染
  - 仿冒和克隆
  - 过量生产



- 安全法律法规，日益凸显重要性
  - 欧洲：GDPR隐私法、网络安全法 (EU Cybersecurity Act)
  - 北美：NIST不断发展网络安全法案
  - 亚洲：韩国、日本、新加坡
    中国，由政府赞助的工作组发布的官方标准
- 行业认证与标准
  - ARM PSA
  - Global Platform
  - IEC 62443

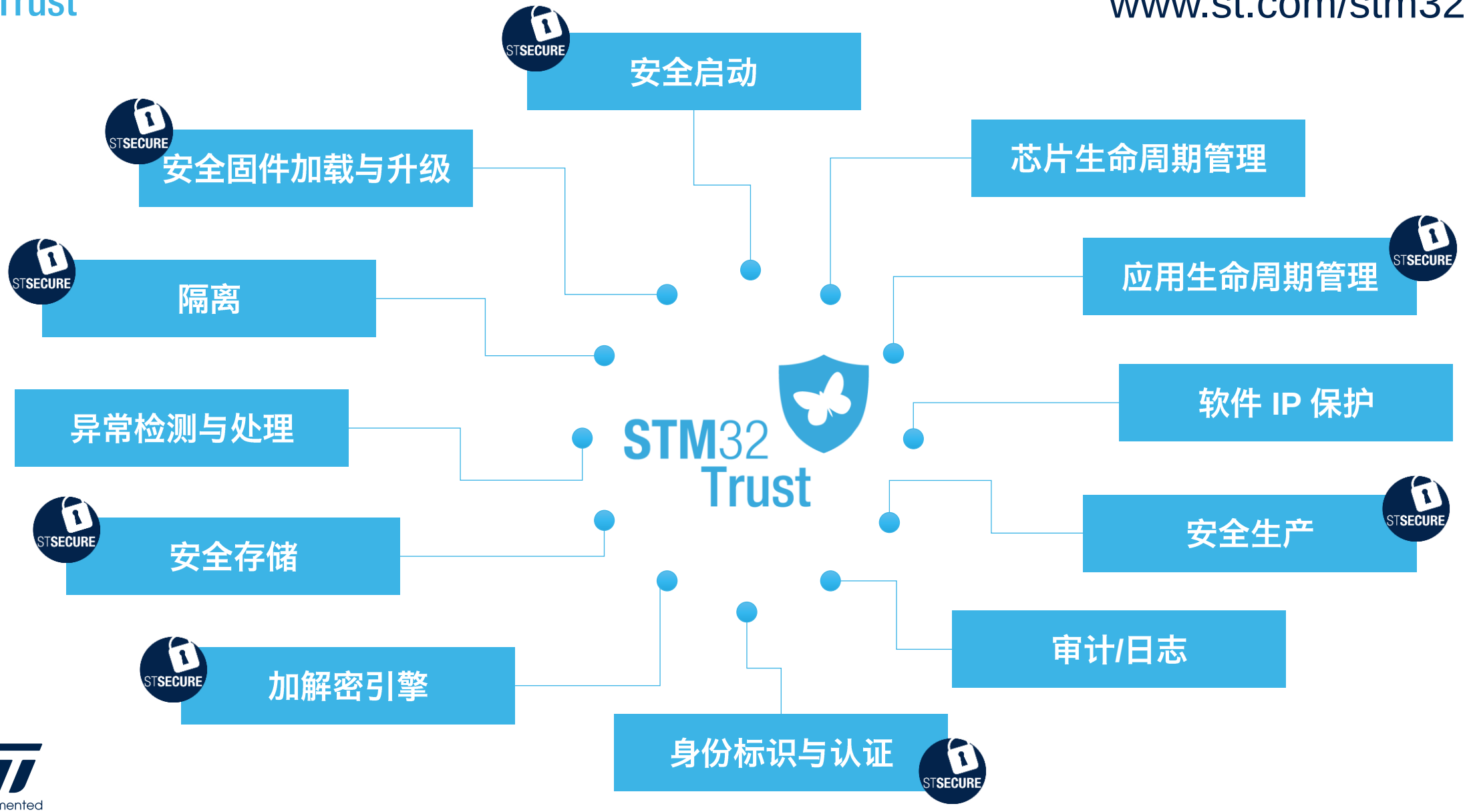
psacertified™

SESIP

life.augmented

您可能的安全需求...

www.st.com/stm32trust



STM32L5提供的安全支撑：软硬件、工具、服务

FREE

安全启动和升级
X-CUBE-SBSFU

安全固件
TFM

加解密软件库
X-CUBE-CRYPTO

硬件驱动
HAL

存储与执行
保护单元

加解密
硬件单元

支持TrustZone的Cortex-M33

安全分析器

可信执行环境

STM32CubeMX

STM32CubeIDE

STM32CubeProgrammer

STM32CubeMonitor

life.augmented

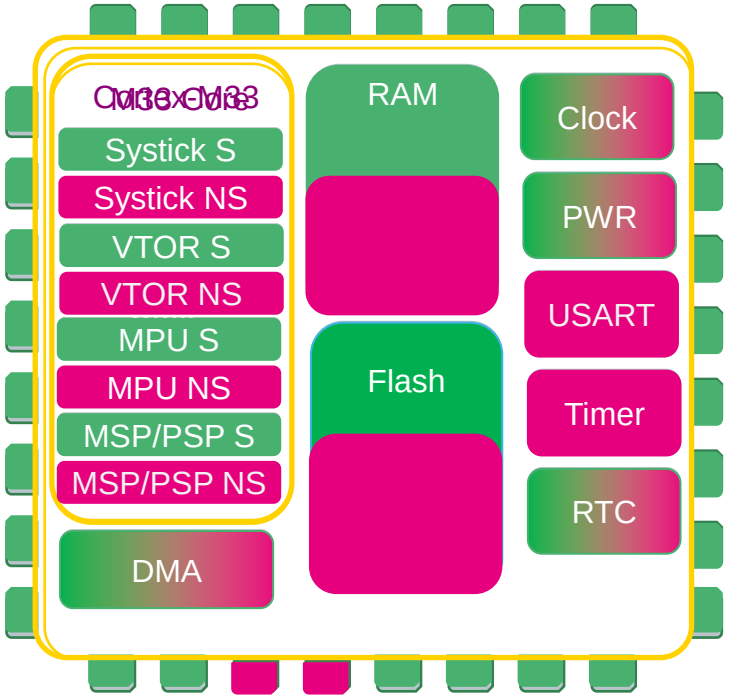
隔离，安全的基础

- TrustZone平台提供的隔离，增强系统安全性
  - 把软、硬件资源、存储区分成两类:
  - 带安全属性的，只能接受安全访问
  - 带非安全属性的，可接受 安全和非安全访问

- STM32L5安全架构
  - 基于带安全扩展(TrustZone)的 Cortex-M33内核
  - ST把TrustZone概念，从内核延伸到整个系统
    - 外设、存储区、DMA、时钟，都兼容TrustZone设计

- STM32L5还有其他隔离机制
  - Memory Protection Unit，区域范围设置更加灵活
  - 隐藏保护扇区(HDP)：在安全扇区里做进一步隔离

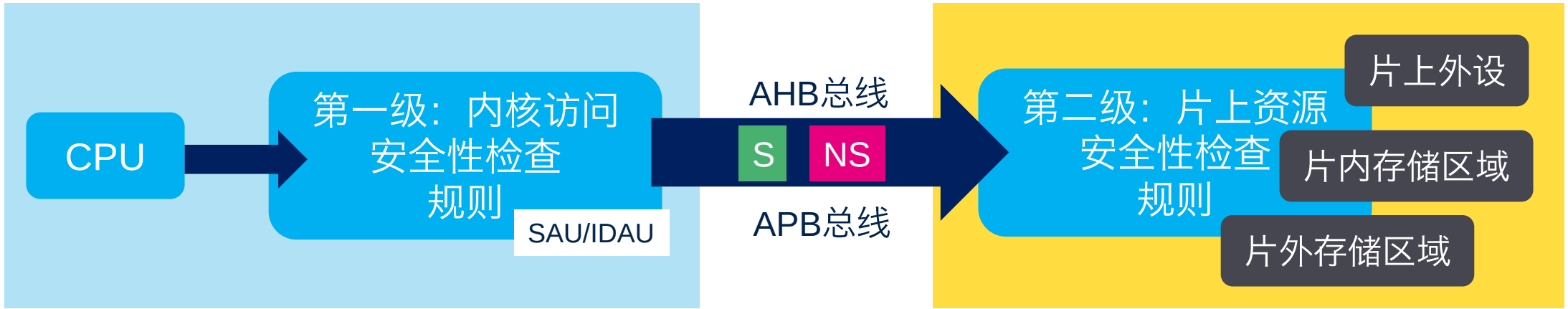
STM32L5 TrustZone未激活的状态



隔离

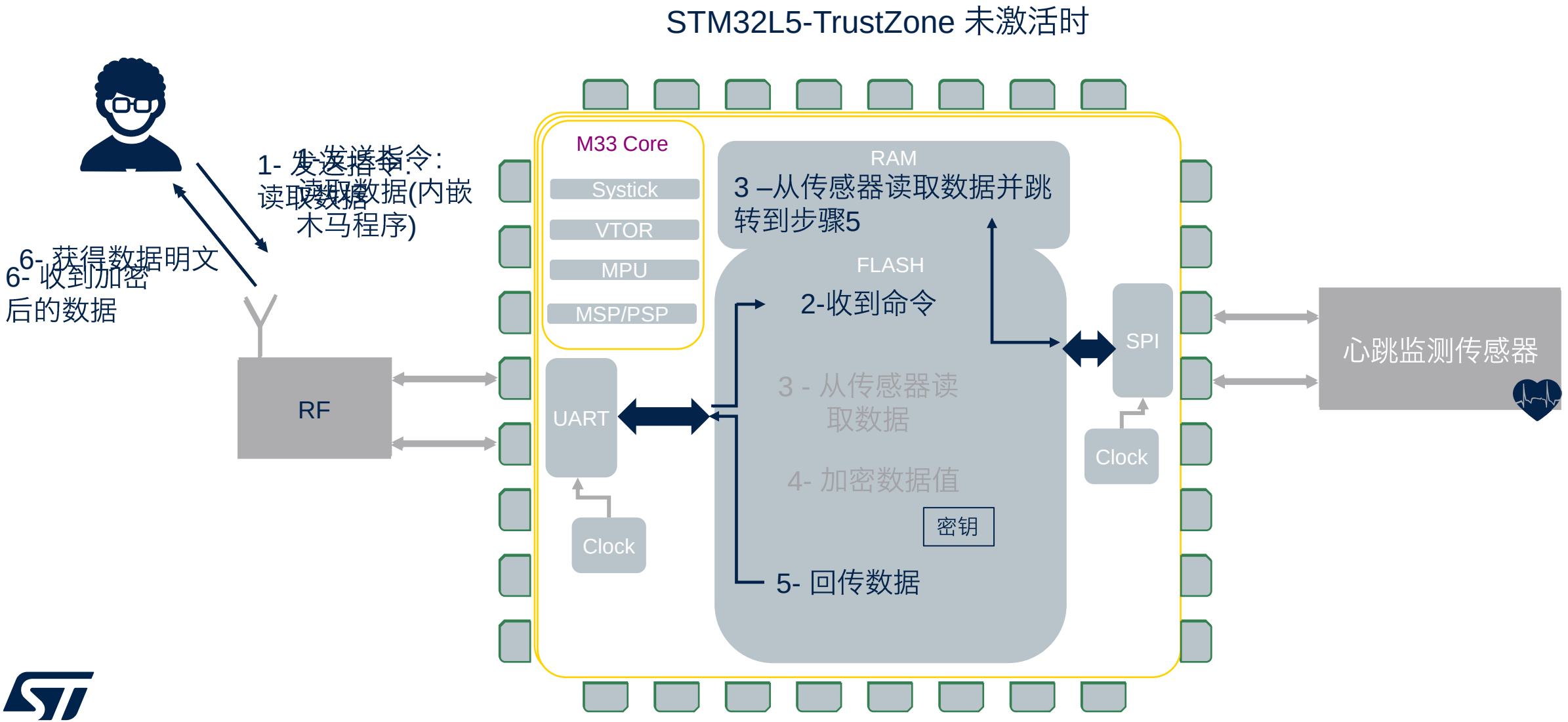
隔离，从内核到全片系统

- 内核视角
  - 产生携带不同安全属性的AHB访问
- 总线
  - 总线上传输的访问携带安全属性
- Trust-Zone aware外设
  - 可配置自身资源的安全属性
  - 例如：GPIO、DMA、EXTI、Flash、…
- Securable外设
  - 由GTZC负责配置其安全属性

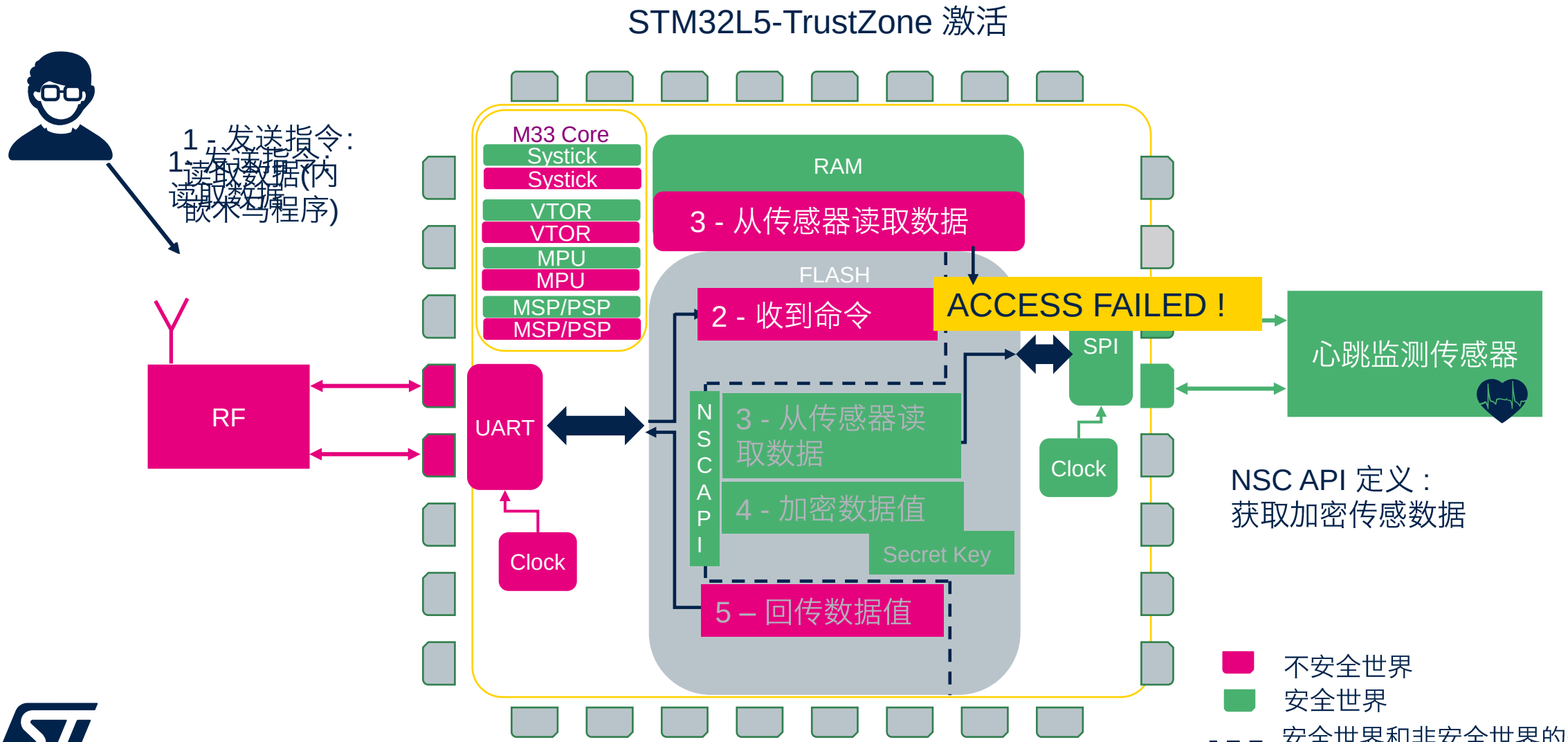


life.augmented

举例：没有隔离的漏洞


STM32L5-TrustZone 未激活时
1- 发送指令：读取数据(内嵌木马程序)
6- 获得数据明文
6- 收到加密后的数据
RF
M33 Core
Systick
VTOR
MPU
MSP/PSP
UART
Clock
RAM
3 –从传感器读取数据并跳转到步骤5
FLASH
2-收到命令
3 - 从传感器读取数据
4- 加密数据值
密钥
5- 回传数据
SPI
Clock
心跳监测传感器

举例：隔离带来的安全


STM32L5-TrustZone 激活
1 - 发送指令：
读取数据(内
嵌木马程序)
M33 Core
Systick
Systick
VTOR
VTOR
MPU
MPU
MSP/PSP
MSP/PSP
RAM
3 - 从传感器读取数据
FLASH
2 - 收到命令
ACCESS FAILED !
SPI
心跳监测传感器
RF
UART
Clock
NSCAPI
3 - 从传感器读取数据
4 - 加密数据值
Secret Key
5 – 回传数据值
Clock
NSC API 定义：
获取加密传感数据
不安全世界
安全世界
安全世界和非安全世界的边界

安全启动

安全启动，构建信任链

- 信任根/ Root of Trust
  - 唯一启动入口
  - Boot Lock：选项字节配置，只能从定义好的片上闪存基地址启动
  - 启动代码的执行不能被跳过
  - 扇区写保护：防止启动代码被篡改
  - 启动代码不能被修改

- 安全启动代码
  - 检查和设置当前安全环境
  - SBSFU参考软件包
  - 认证下一阶段要运行的代码
  - HDP (隐藏保护扇区)：选项字节配置，启动代码执行完毕后使能；保护启动代码安全性，和系统其他代码隔离开

life.augmented

安全固件更新

- 安全固件更新 /SFU
  - 固件保密（可选）
  - 固件完整未被篡改
  - 固件来源可靠
  - 部分、全片升级

STM32L5

- SBSFU & TFM-Boot
- mbedCrypto、ST密码学算法库
- 支持GCM、RSA、ECDSA
- 支持固件明文、密文升级

life.augmented

加解密引擎

加解密硬件引擎

AES

- 模式
  - ECB
  - CBC
  - CTR
  - GCM
  - GMAC
  - CCM
- 密钥长度
  - 128位
  - 256位

HASH

- 算法

PKA

- 模式
- 密钥长度
  - 3136位
  - 640位

TRNG

- 每次产生

UID

- 96位

加解密软件库，支持全系列STM32

X-CUBE-CRYPTO

life.augmented

软件IP保护

I. 开发阶段

- TZ：隔离，非安全代码无法随意访问安全代码
- RDP0.5：仅能对非安全区域的代码进行调试

II. 量产烧录阶段

- SFI：在不可信产线环境做安全烧录

III. 产品出厂后

- MPU：权限 + 隔离，防止恶意代码内部攻击
- TZ：隔离，防止恶意代码内部攻击
- RDP1、RDP2：阻断调试端口，防止外部攻击
- OTFDEC：实时访问存储在外部Flash的密文

STM32L5 AI demo使用了该功能

安全生产：SFI

- SFI解决的问题
  - 私有代码在不可信产线的安全烧录
- SFI是一套安全服务
  - 包含芯片端、软件工具、硬件工具

三大安全功能

1. 确定烧写的是STM32芯片
2. 确保OEM的代码不会在产线被窃取、篡改
3. 确保OEM的代码的烧录次数

- 在TrustZone使能时才可使用SFI服务

1. STM32芯片端支持

- 预置Secure BL
- 预置公私钥对、数字证书

2. 软件工具

免费下载

- PC端 – Trusted Package Creator @ OEM开发
- 烧录器上位机 – STM32CubeProgrammer @ 烧录产线

3. 硬件工具

付费服务

- HSM www.st.com/stm32hsm @ 烧录产线
- STLINK @ 烧录产线

异常监测 & 入侵检测

- 扩展的检测条件
  - 8个/4对外部入侵检测引脚，支持active模式
  - 5个内部监测信号
- 保护措施
  - 擦除敏感信息存储区域

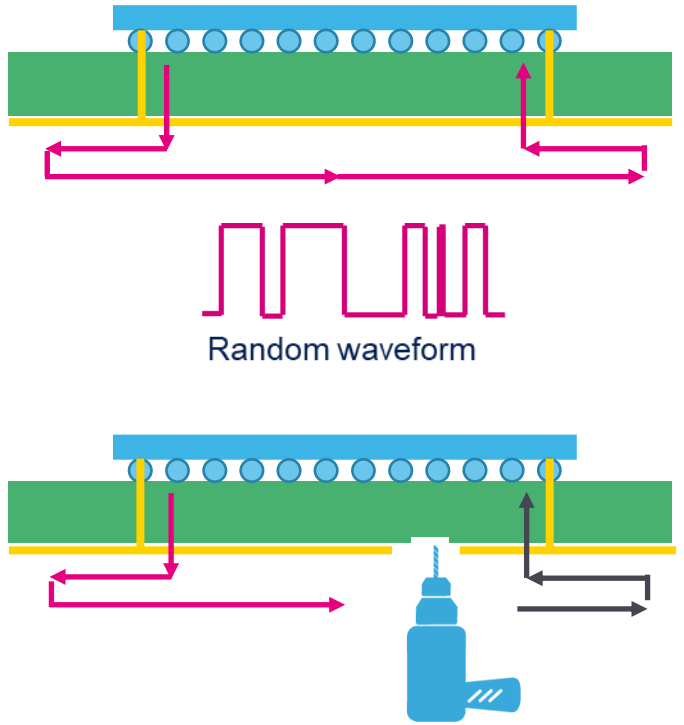
擦除 备份寄存器、4KB SRAM2
PKA RAM、ICACHE,
OTFDEC region key

TAMP 模块

外部信号 tamper引脚

内部信号 电压、温度、LSE (CSS)
RTC 日历溢出
单向计数器溢出

- Active 入侵检测，对抗开箱板级攻击
  - tamper输入、输出引脚之间布上mesh loop 电路
  - 输出端发出、输入端检测期盼的随机序列



STM32L5 安全认证

STM32L5最先获得PSA Level2认证的MCU

life.augmented

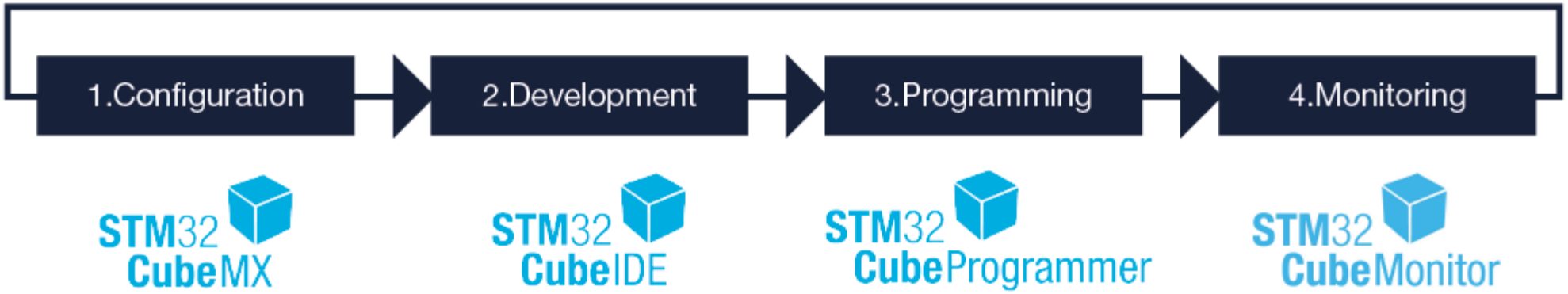
STM32L5： 生态系统

继承优秀基因，同样出类拔萃

life.augmented

STM32Cube工具家族

- 支持STM32L5的全链路开发过程



	配置 & 代码自动生成	项目开发 & 烧录 & 调试	选项字节配置 & 代码烧录	观察 & 测量
对L5的特别支持	支持TZ：对外设、存储区域的安全属性配置	支持TZ：自动生成S和NS初始工程框架	特殊选项字节设置 支持SFI	STM32L5-DK板上集成功耗测量电路

life.augmented

STM32L5 学习资料

https://www.stmcu.com.cn/ecosystem/chip/chipfamily-STM32L5-entry

STM32L5快速入门	
03. 认识ARM Cortex-M33内核	40 分钟
04. STM32L5系统新架构：支撑TZ	30 分钟
05. 新的用户编程模型：支撑TZ	60 分钟
06. STM32CubeMX：支撑TZ应用	40 分钟
07. STM32L5的低功耗特性	30 分钟

STM32L5进阶课程	
08. Flash和启动机制的安全机制	90分钟
09. Cache，为STM32L5提速助力	90分钟
10. DMA，兼顾传输灵活性和TZ架构下的安全性	60分钟
11. OTFDEC，无缝扩大代码的安全存储空间	60分钟
12. PKA，为IoT时代安全服务提供硬件加速	60分钟

技术文档

- 重要应用笔记 (及译文)、工程师笔记、在线课程 (理论+实践)

固件例程

- STM32CubeL5固件包 (包括SBSFU， TFM)、加解密软解库

PC工具

- STM32Cube 工具家族

方案

- SFI、第三方TEE

life.augmented

Take Away

高性能，不仅仅是主频

低功耗，我有一颗绿色的心

安全，不仅仅是加解密；系统上的隔离也很重要

https://www.stmcu.com.cn/ecosystem/chip/chipfamily-STM32L5-entry

www.st.com/stm32trust

life.augmented

Thank you

life.augmented