life.augmented

STM32 生态系统 第十五期

信息安全 . Information Security

06. STM32的存储与执行保护

2020.03

本期内容概览

1 STM32安全特性概览

2 STM32的存储与执行保护模块

life.augmented

SFI服务：安全固件安装

HSM

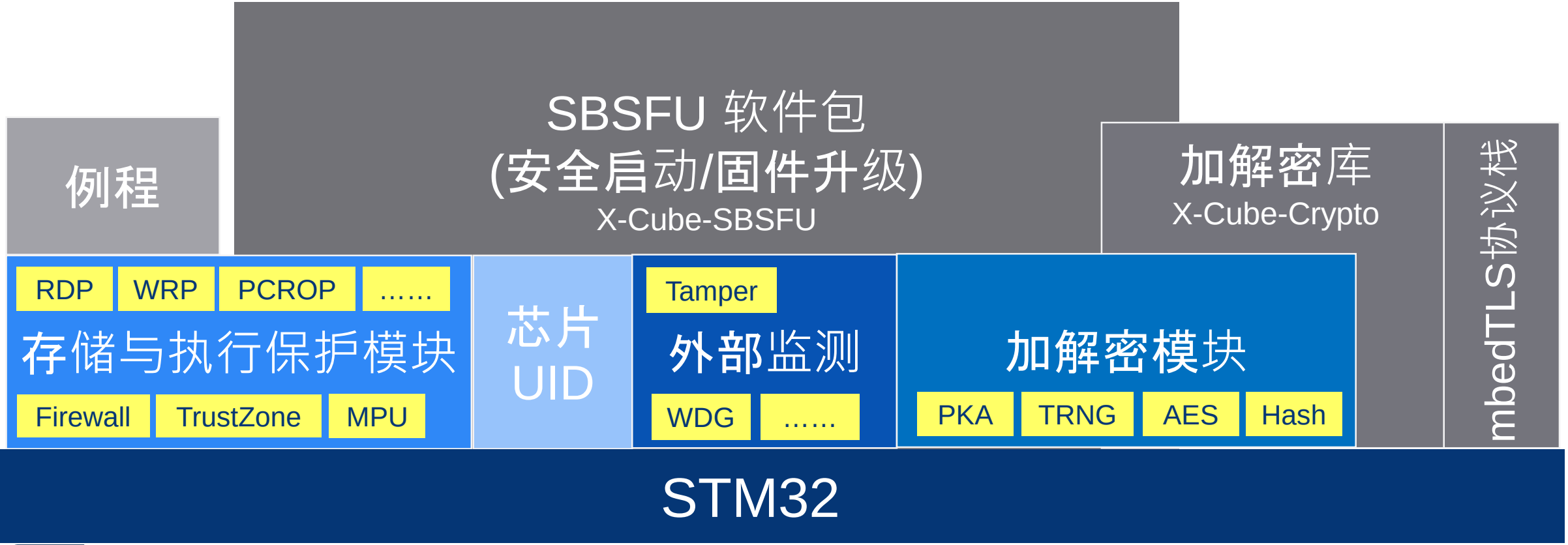
STM32CubeProgrammer

TrustPackageCreator

STM32安全特性概览

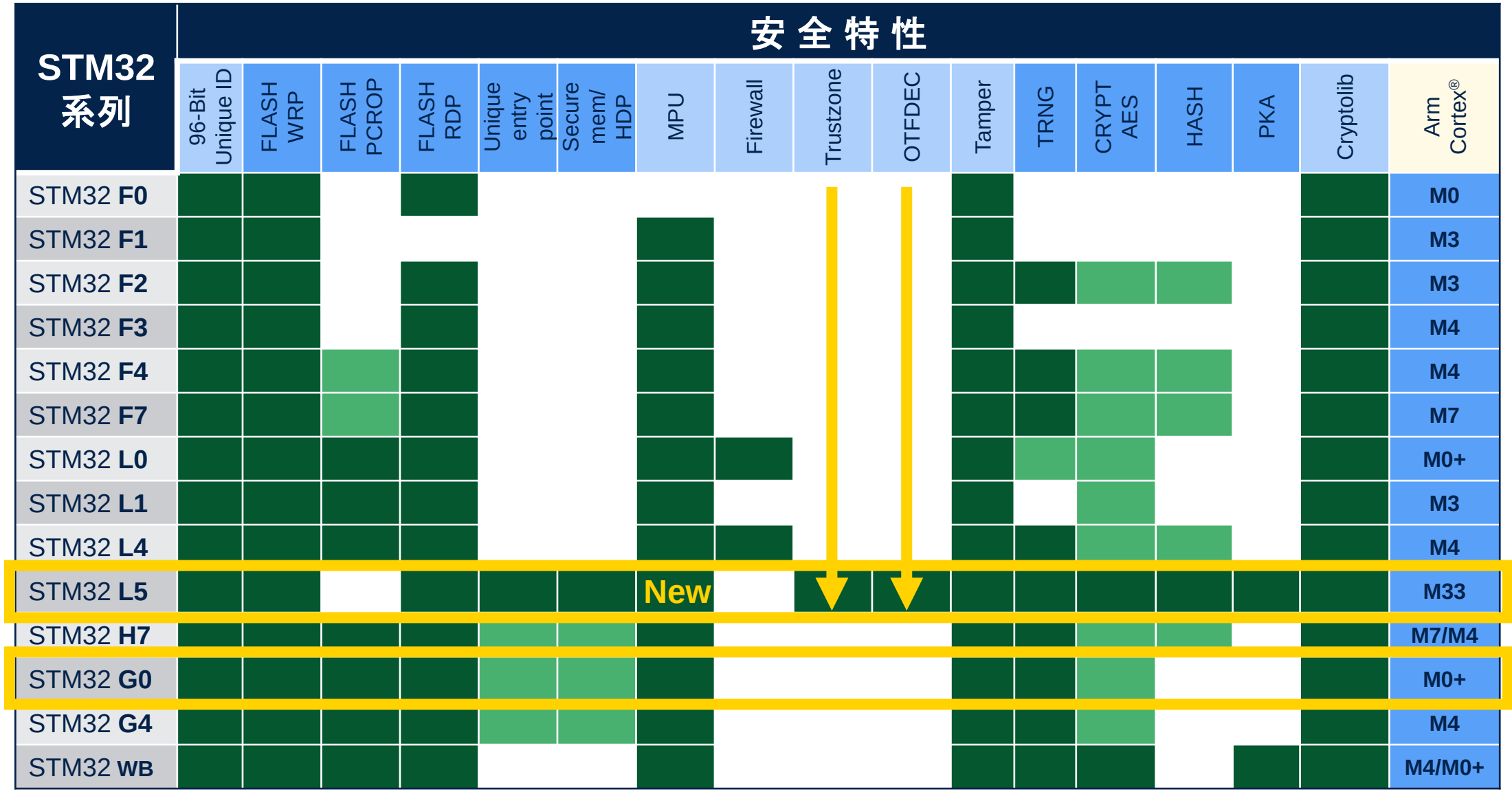
www.st.com/stm32trust

www.stmcu.com.cn中国官网



所有系列都有　　取决于产品型号

从产品系列来看...



life.augmented

STM32 UID

- 出厂前由STM32烧写在芯片的系统Flash部分，提供STM32芯片的唯一标志号
  - Wafer位置，X坐标值BCD编码 @ 2字节
  - Wafer位置，Y坐标值BCD编码 @ 2字节
  - Lot编号低地址，ASCII编码 @ 3字节
  - Wafer编号 @ 1字节
  - Lot编号高地址，ASCII编码 @ 4字节

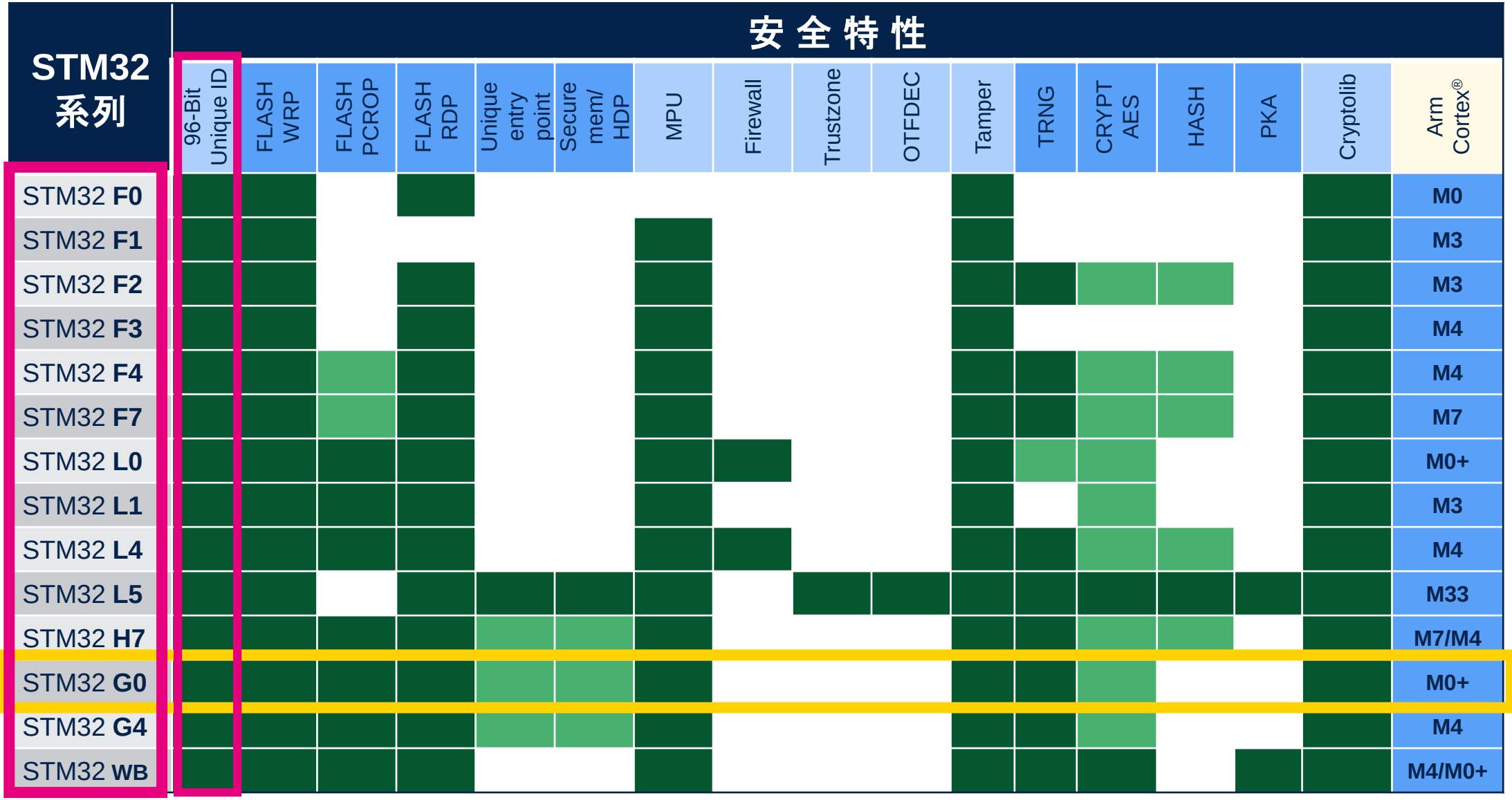
以STM32G0为例 @ 0x1FFF 7590

Address	0	4	8	C	ASCII
0x1FFF7590	003C0075	3136500A	20393546	FFFFFFFF	u.<..P61F59 ÿÿÿÿ

- 常见用途
  - 通过某种算法生成该芯片所在产品的序列号
  - 密钥派生
- 芯片的参考手册有专门章节描述 @ Device electronic signature

所有系列都有　　取决于产品型号

从产品系列来看 UID



life.augmented

STM32 Flash写保护

- 保护片上Flash指定区域的内容不被意外地修改，也不能被擦除
- 常见用途：WRP + RDP2，锁定一段片上Flash区域成为ROM
- 通过选项字节使能保护和撤除保护 → 静态保护（一上电即生效）
  - L4、G0、G4、WB、L5：设置起始page和末尾page，连续地址

FLASH_WRP1AR	Res.	Res.	Res.	Res.	Res.	Res.	Res.	Res.	Res.	WRP1A_END[5:0]						Res.	Res.	Res.	Res.	Res.	Res.	Res.	Res.	Res.	WRP1A_STRT[5:0]					
Reset value										X	X	X	X	X	X										X	X	X	X	X	X
FLASH_WRP1BR	Res.	Res.	Res.	Res.	Res.	Res.	Res.	Res.	Res.	WRP1B_END[5:0]						Res.	Res.	Res.	Res.	Res.	Res.	Res.	Res.	Res.	WRP1B_STRT[5:0]					
Reset value										X	X	X	X	X	X										X	X	X	X	X	X

以STM32G0为例

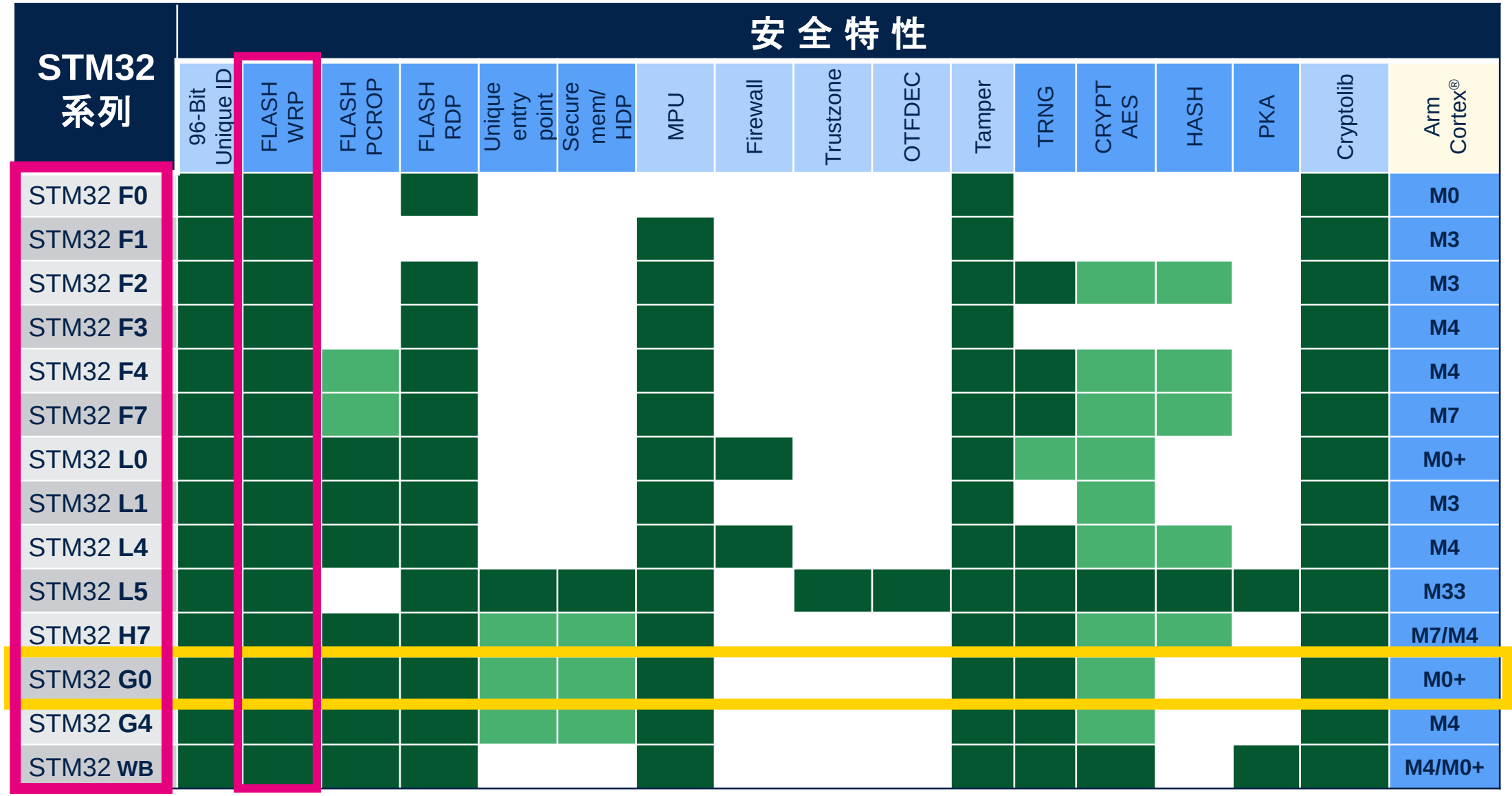
  - 其他系列：每个page/sector可独立设置

FLASH_OPTCR	SPRMOD	nWRP14_15	nWRP[13:0]													RDP[7:0]								nRST_STDBY	nRST_STOP	WDG_SW	Res.	BOR_LEV		OPTSTRT	OPTLOCK
Reset value	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	0	1	0	1	1	1		1	1	0	1

以STM32F4为例

所有系列都有　　取决于产品型号

从产品系列来看 WRP



life.augmented

STM32私有代码保护 PCROP

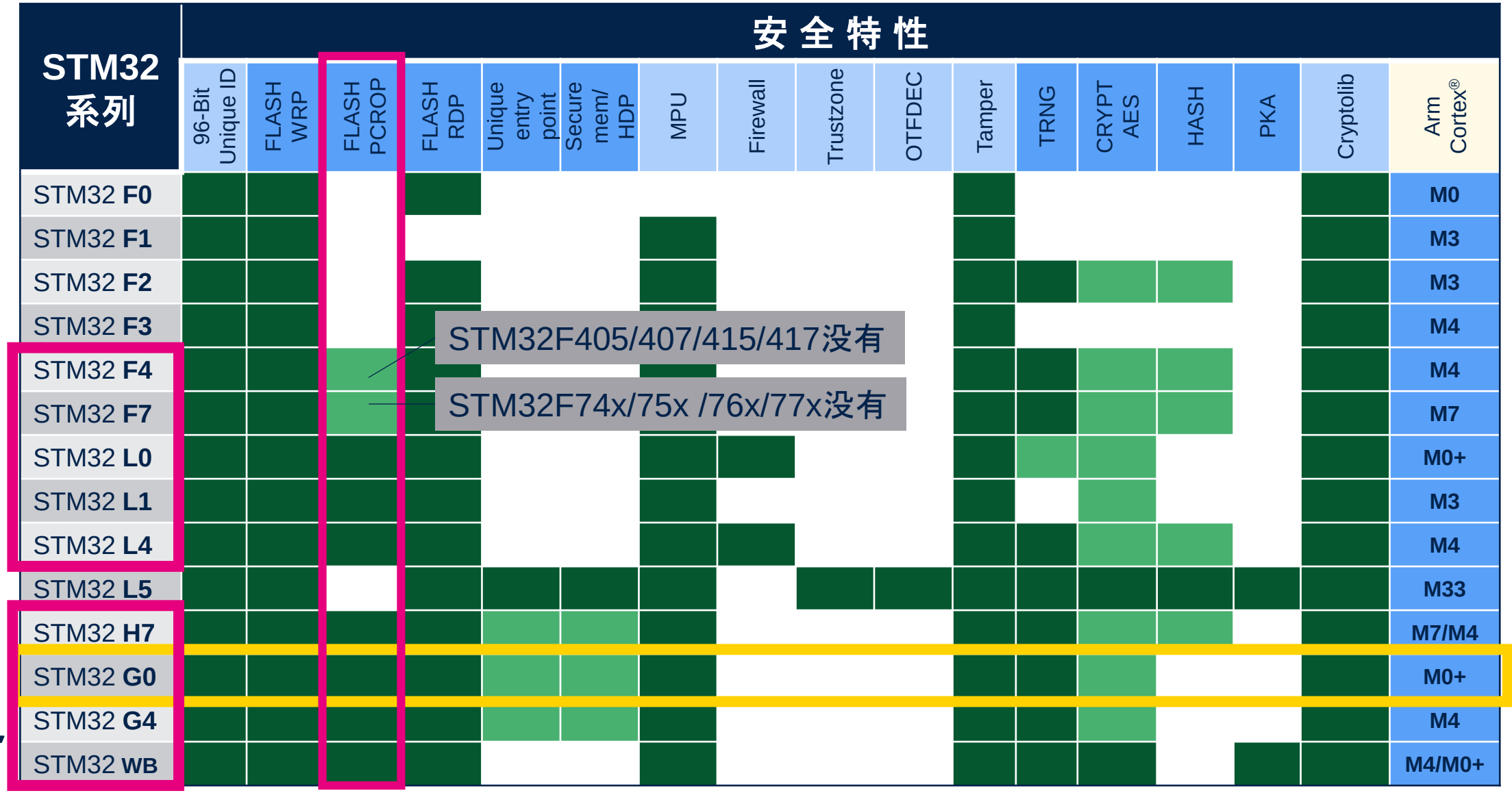
- 保护片上Flash指定区域不能被数据总线访问，只能执行
  - 不能被读、修改、擦除
  - 调试接口也无法读出区域里的内容
  - 这段代码可以被调试：观察寄存器、堆栈等上下文
- 常见用途：联合开发时，对IP代码进行保护，不被终端用户读出或修改
- 通过选项字节使能保护 → 静态保护
  - L4、H7、G0、G4、WB：设置起始page和末尾page，连续地址
  - 其他系列：每个page/sector可独立设置（独立的PCROP控制位，或和WRP控制位共享）
- 通过选项字节撤除保护：RDP降级 + 同时取消保护区域的范围设置
  - PCROP_RDP = 1，RDP降级：片上Flash所有内容被擦除，包括PCROP保护的区域
  - PCROP_RDP = 0，RDP降级：只擦除PCROP区域以外

PCROP 使用技巧

- 使用技巧1，关于敏感代码涉及的常数
  - 在IDE中设置特别的编译选项
  - 代码用到的常量放到保护区域之外
- 使用技巧2，存储敏感数据
  - 也要结合其他保护机制，把敏感数据恢复到安全的寄存器/SRAM
- 使用技巧3，可以增大PCROP保护区域
- 其它相关设计资源
  - X-Cube-PCROP（F4、L4、F7）
  - AN4758（ L4， L4+，G4 ）、AN4246（L1）、AN4968（F7）、 AN4701（F4）

所有系列都有　　取决于产品型号

从产品系列来看 PCROP



life.augmented

STM32读保护 RDP

- 在不同保护级别(level)下，可以实现对谁的，什么保护(什么条件下的什么行为)

保护对象		保护级别 RDP level	从用户Flash启动			调试模式或从SRAM启动或从系统FLASH启动		
			读	写	擦除	读	写	擦除
All	用户 FLASH	1	Yes	Yes	Yes	No	No	No
		2	Yes	Yes	Yes	不允许启动 或者 连接		
All	系统 FLASH	1						
		2						
All	选项字节	1						
		2						
	后备寄存器 /SRAM	1						
		2	Yes	Yes	N/A：SRAM自身没有擦除机制	不允许启动 或者 连接		
L4/L5/ WB	SRAM2	1	Yes	Yes		No	No	N.A
		2	Yes	Yes		不允许启动 或者 连接		
G4	CCM-SRAM	1	Yes	Yes		No	No	N.A
		2	Yes	Yes		不允许启动 或者 连接		

RDP级别：

- 大多数STM32系列具有三级读保护
- STM32F1，没有RDP 2
- STM32L5，新增RDP 0.5，和TrustZone搭配使用

STM32读保护 RDP

- 在不同保护级别(level)下，可以实现对谁的，什么保护(什么条件下的什么行为)

保护对象		保护级别 RDP level	从用户Flash启动			调试模式或从SRAM启动或从系统FLASH启动		
			读	写	擦除	读	写	擦除
All	用户 FLASH	1	Yes	Yes	Yes	No	No	No
		2	Yes	Yes	Yes	No	No	No
All	系统 FLASH	1	Yes	Yes	Yes	No	No	No
		2	Yes	Yes	Yes	No	No	No
All	选项字节	1	Yes	Yes	Yes	No	No	No
		2	Yes	Yes	Yes	No	No	No
	后备寄存器 /SRAM	1	Yes	Yes	Yes	No	No	No
		2	Yes	Yes	Yes	No	No	No
L4/L5/ WB	SRAM2	1	Yes	Yes	Yes	No	No	No
		2	Yes	Yes	Yes	No	No	No
G4	CCM-SRAM	1	Yes	Yes	Yes	No	No	No
		2	Yes	Yes		不允许启动 或者 连接		

保护对象：哪些片上存储区域？

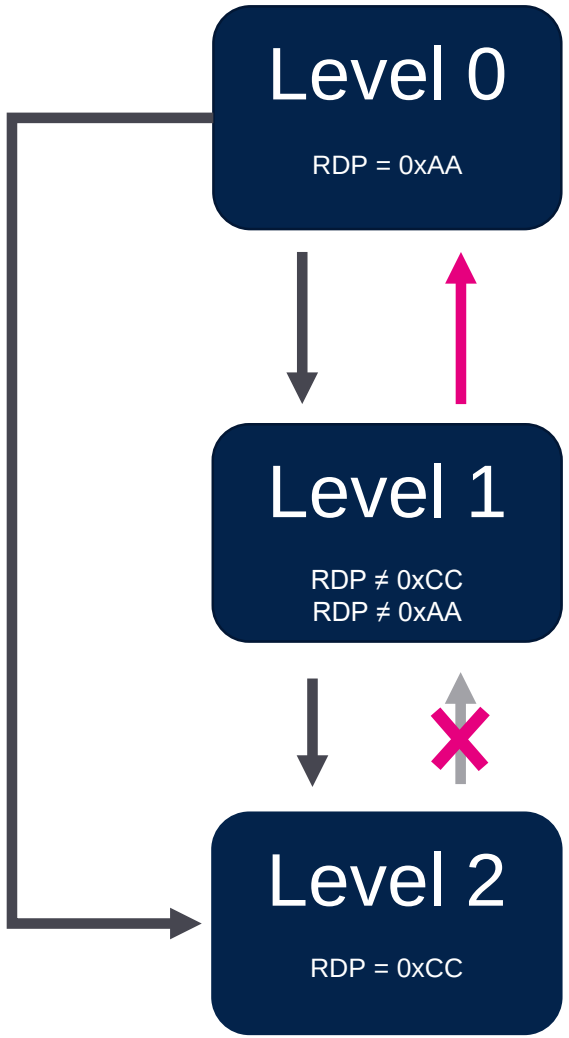
- 主要区域：用户Flash， 选项字节
- 电池备份域：
  - BKP寄存器：F0, F3, L4, L5, G0, G4, WB
  - BKP SRAM：F2, F4, F7, H7
- 其它区域，取决于具体系列
  - SRAM2：L4, L5, WB
  - CCM-SRAM：G4

STM32读保护 RDP

- 在不同保护级别(level)下，可以实现对谁的，什么保护(什么条件下的什么行为)

保护对象		保护级别 RDP level	从用户Flash启动			调试模式或从SRAM启动或从系统FLASH启动		
			读	写	擦除	读	写	擦除
All	用户 FLASH	1	Yes	Yes	Yes	No	No	No
		2	Yes	Yes	Yes	不允许启动 或者 连接		
All	系统 FLASH	1	Yes	No：系统flash只读		Yes	No：系统flash只读	
		2	Yes			不允许启动 或者 连接		
All	选项字节	1	Yes	Yes	Yes	Yes	Yes	Yes
		2	Yes	No	No	不允许启动 或者 连接		
	后备寄存器 /SRAM	1	Yes	Yes	N/A：SRAM自身没有擦除机制	No	No	N.A
		2	Yes	Yes		不允许启动 或者 连接		
L4/L5/ WB	SRAM2	1	Yes	Yes		No	No	N.A
		2	Yes	Yes		不允许启动 或者 连接		
G4	CCM-SRAM	1	Yes	Yes		No	No	N.A
		2	Yes	Yes		不允许启动 或者 连接		

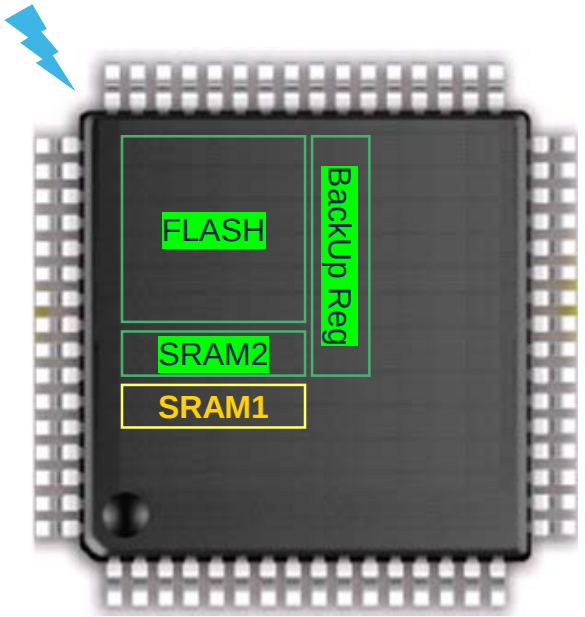
RDP 级别转化



@ 出厂状态

会引发用户Flash的全片擦除

- WRP设置的影响？
- PCROP设置的影响？

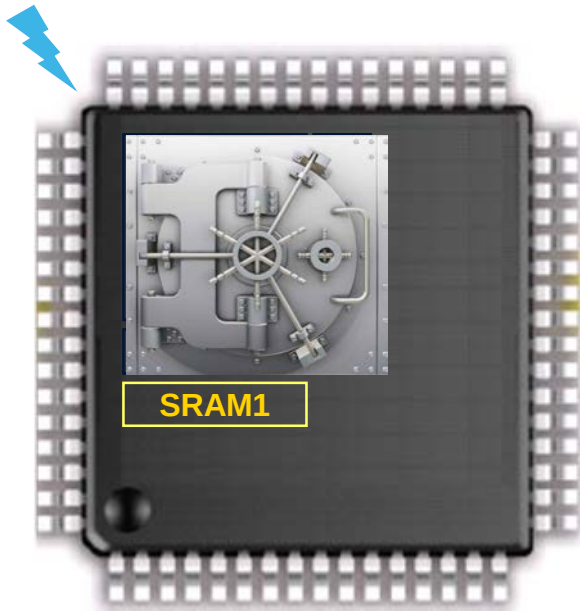


通过选项字节修改RDP级别，仅仅是**修改了都需要Flash中寄存器的**值；需**要在**”选项字节装载”**后才在系**统生效

- 软件置位OBL_Launch
- **上电复位：BOR复位，或从待机模式退出**

RDP级别1

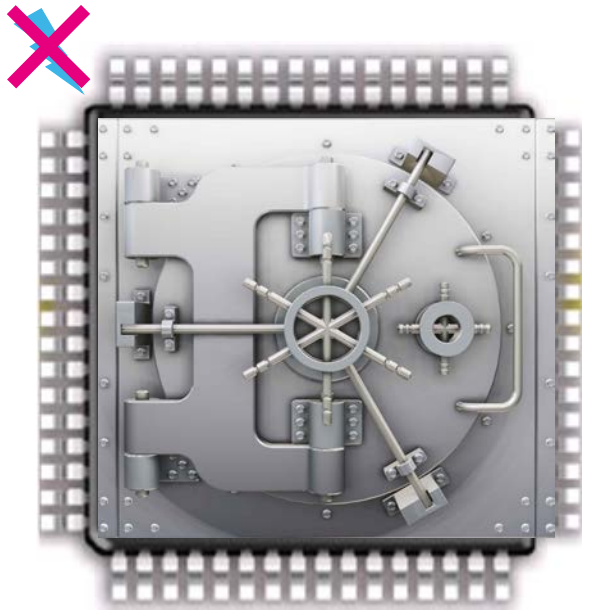
- **能做什么…**
  - **从用户Flash启动**，对所有保护对象的操作不受任何限制（除非介质本身的属性限制）
  - **允**许调试器连接，读、修改选项字节
  - **被**调试器连接，**但是内核复位**
  - **被**调试器hotplug连接，读取SRAM1**和外**设寄存器当前值
- **不能做什么…**
  - **被**调试器连接**/从**SRAM**启**动**/从系**统Flash**启**动，看不到用户Flash、备份域、受保护SRAM**的内容**
  - **从**SRAM**启**动的代码不能通过DMA读出用户Flash**的内容**



从SRAM启动，无法通过修改PC跳到用户Flash执行(**去做无限制操作**)

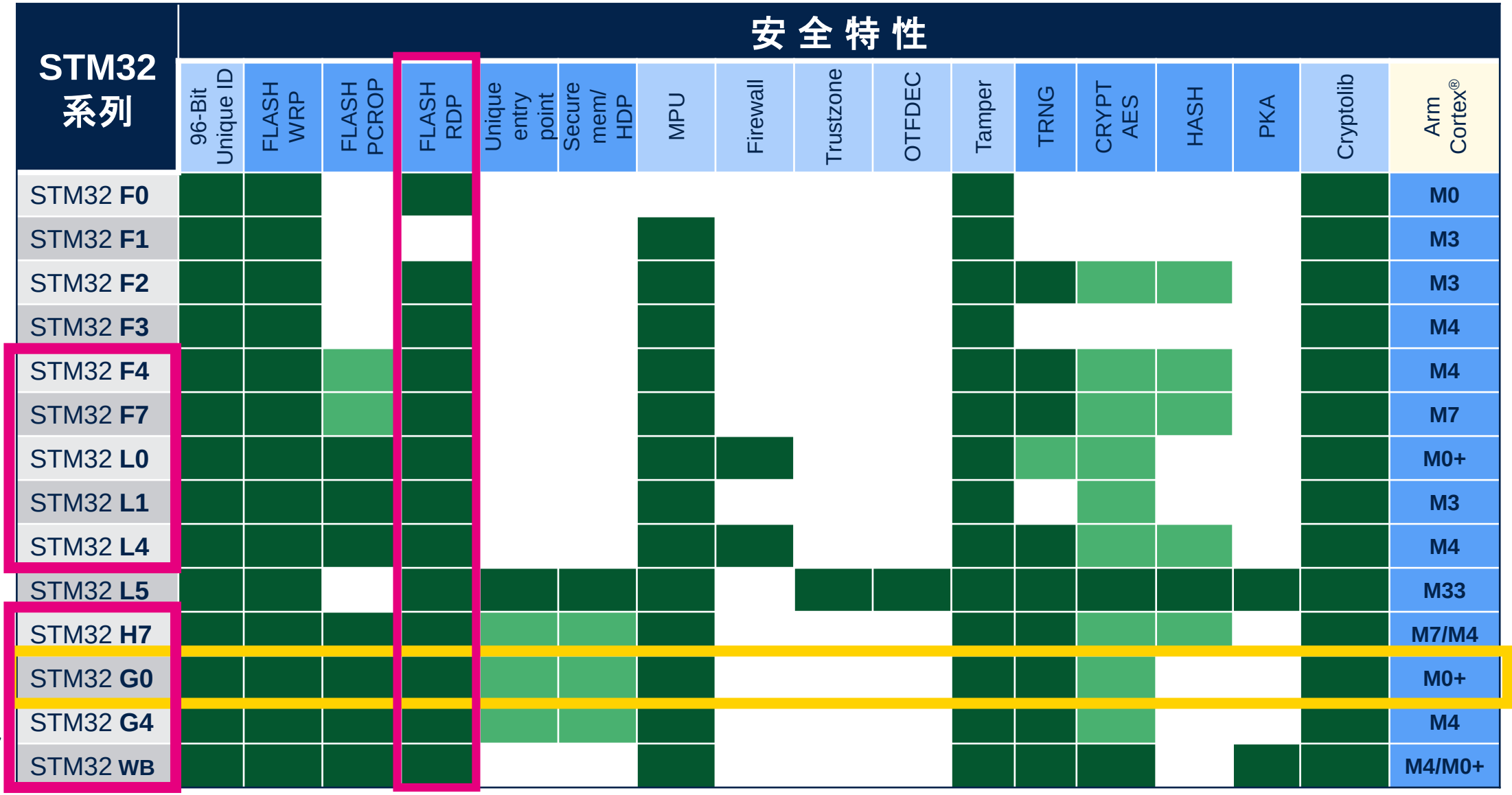
RDP级别2

- 选项字节被锁死，任何代码都无法再修改它
  - 选项字节的配置永久生效：读保护、启动地址、PCROP ……
  - **写保护 + RDP2 → ROM**
- 调试接口再也无法连接
  - **失效分析受影响**
- **只能从用户Flash启动，仍可做用户Flash的固件更新**



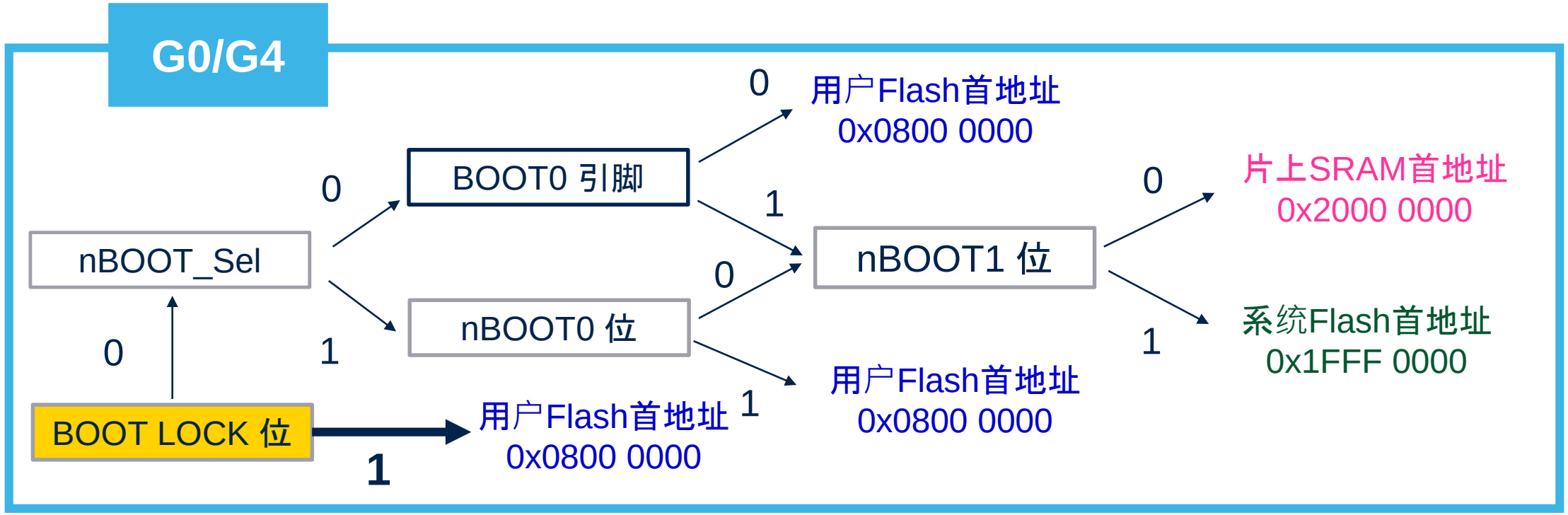
所有系列都有　　取决于产品型号

从产品系列来看 RDP



life.augmented

STM32唯一启动入口 UBE



G0/G4的UBE控制位

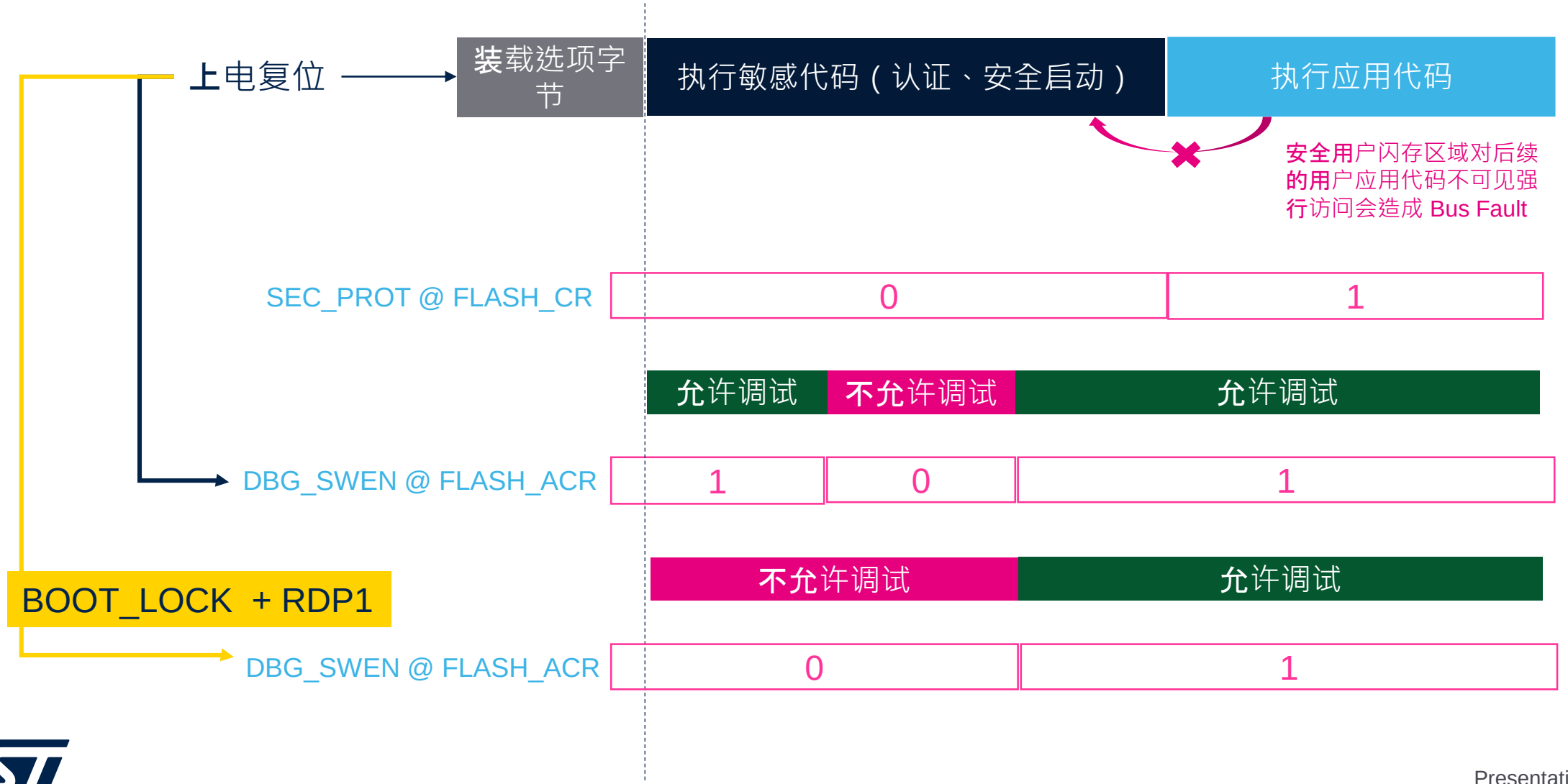
- RDP1 + BOOT LOCK → 调试端口连接不上 + **只能从**0x0800 0000**启**动
- **只能靠用户**Flash**里的代**码操作RDP降级，或者使能DBG_SWEN @ FLASH_AR，**若用户**Flash**代**码里没有该功能 → 调试端口永远连接不上了

life.augmented

STM32安全用户存储区 / G0,G4

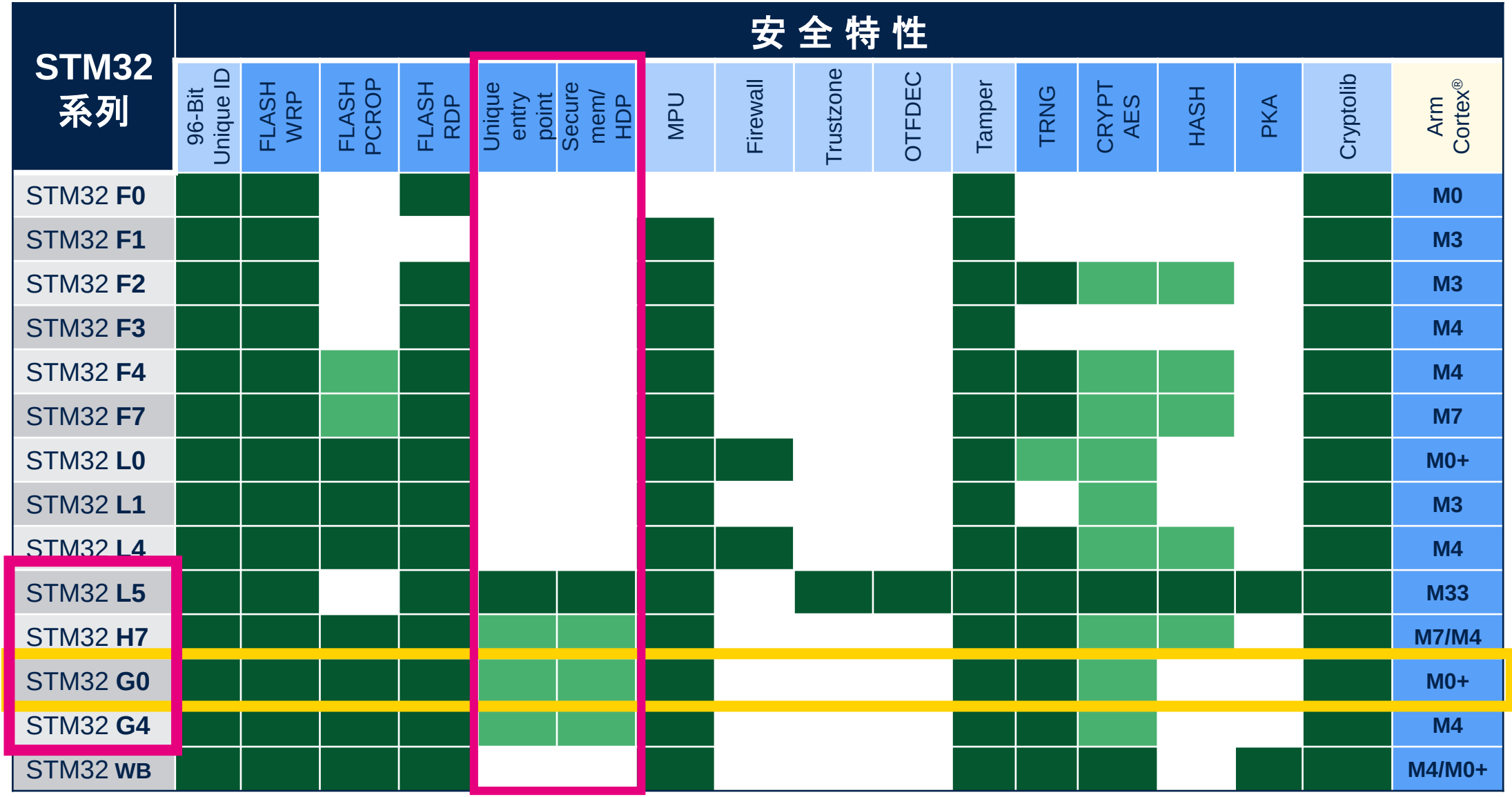
- 安全用户闪存(Secure User Memory)，用于配合UBE，做安全启动
  - 用于隔离用户代码和敏感代码：Secure开关打开后，这段区域不可见，直到下次复位
  - （Secure开关打开之前）执行敏感代码时，可关闭调试访问
- 安全用户闪存是用户Flash的一部分
  - 起始地址固定在0x0800 0000
  - 大小可配置，SEC_SIZE @ FLASH_SECR（和UBE的使能控制在同一寄存器）
    - 大小为0时，表示没有安全用户闪存
    - 只能在RDP0时修改该位域
    - 大小粒度，和Flash page相同：2KB/4KB
- Secure开关，用户软件置位后，只能由系统复位清零

STM32安全用户闪存 / G0,G4



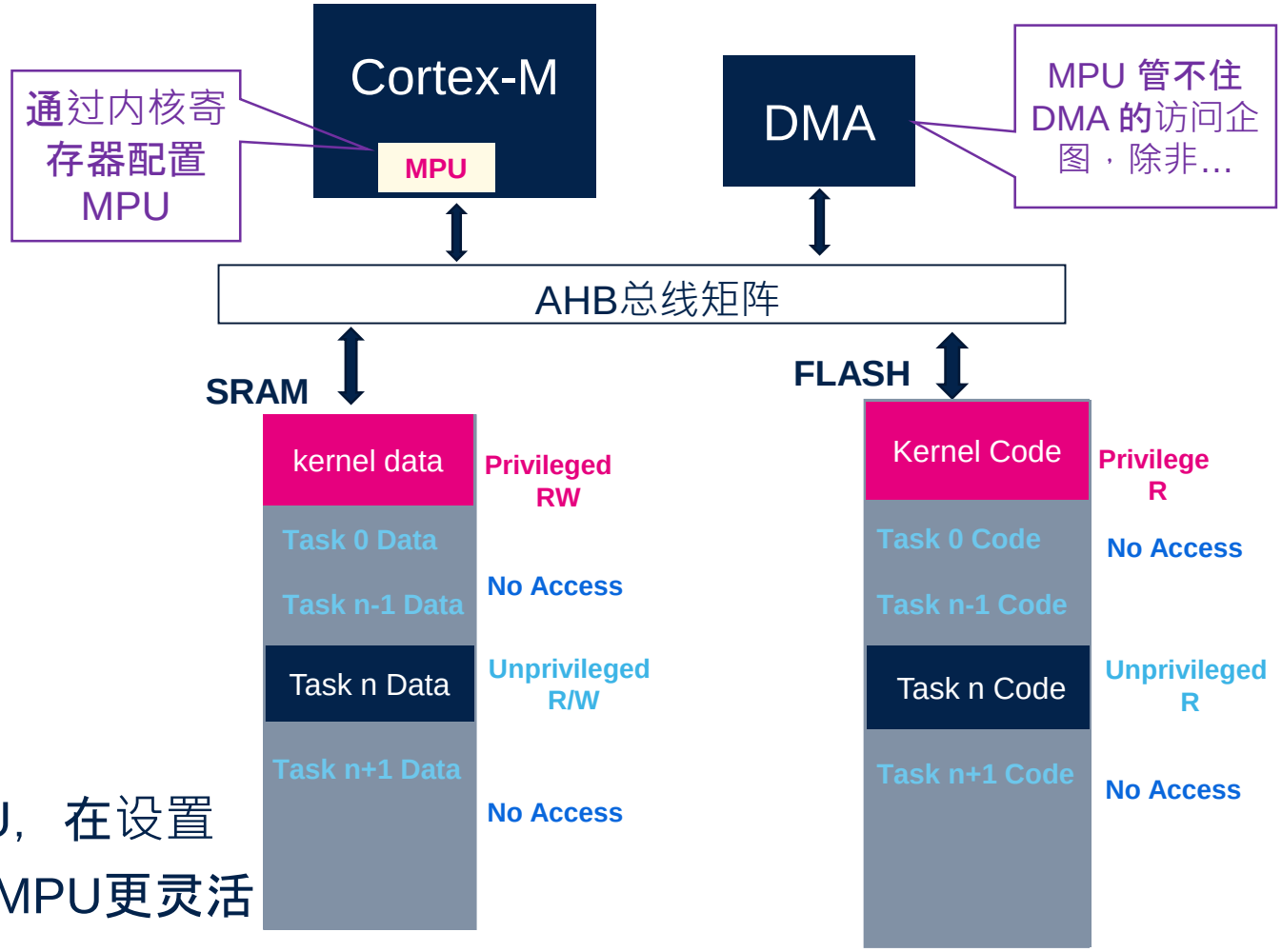
所有系列都有　　取决于产品型号

从产品系列来看 UBE+安全用户存储区



STM32集成的 MPU

- 原理
  - 动态保护：由内核寄存器配置
  - 保护对象是？
  - 防的是谁？
  - 限制了怎样的操作？
    - 什么样特权级别的内核访问
    - 可以对哪些存储区域(region)
    - 做怎样的访问：读、写、执行
    - 违反以上规则，就触发Fault
- 实现
  - STM32L5里采用的Armv8-m中的MPU，在设置区域大小的时候，比以往STM32系列的MPU更灵活

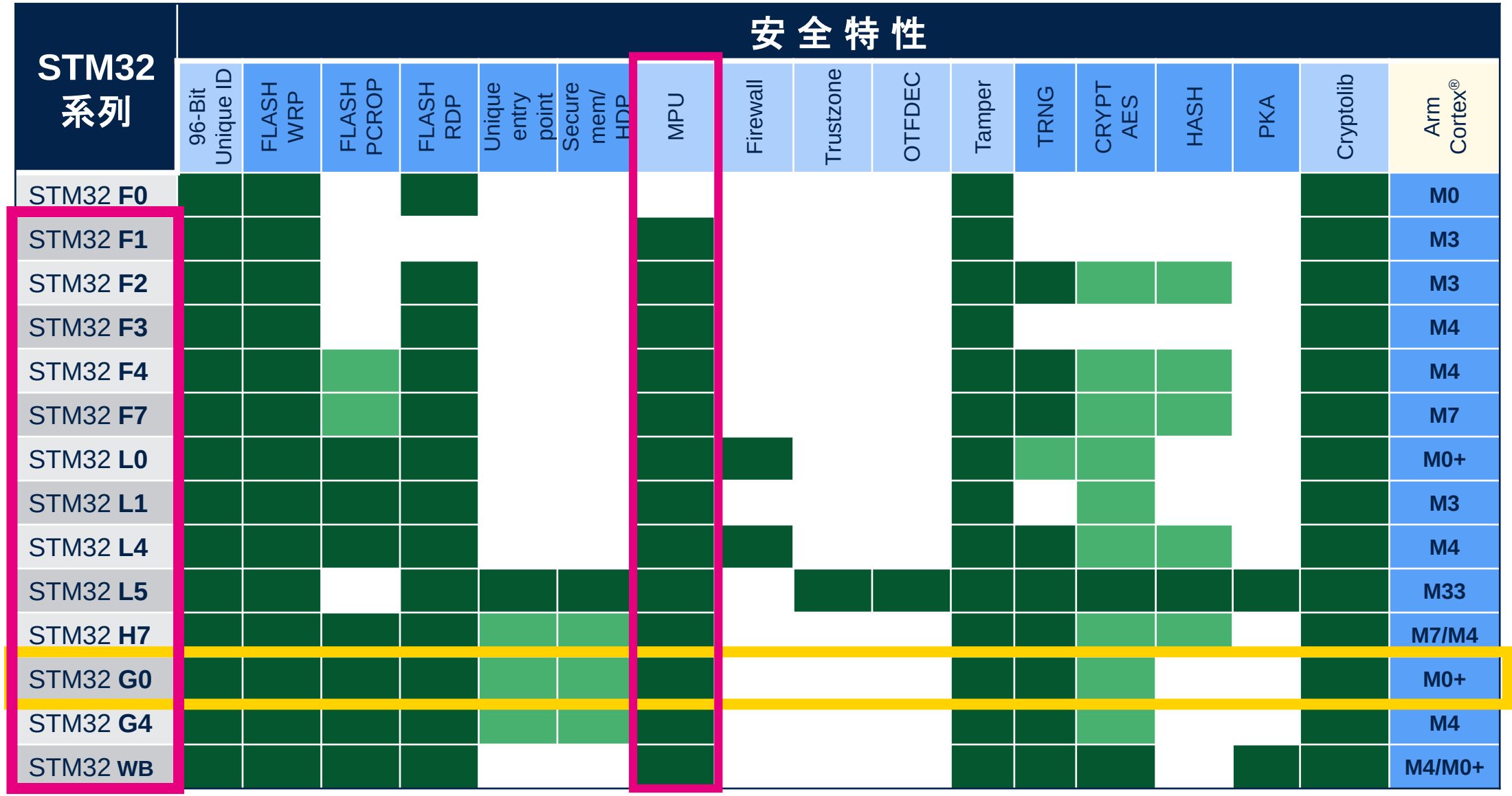


MPU常见用法 和 相关设计资源

- MPU常见用法
  - OS或者敏感代码设置成 特权级别的代码才能访问，防止不可靠的非特权级别用户代码因为软件漏洞，而污染了敏感代码
  - 把DMA控制寄存器所在区域设置成 只能特权级别代码访问，防止非特权级别的用户代码操作DMA来避开MPU的限制
  - 把RAM区域设置成XN， 以免缓冲区溢出造成的攻击
  - 任务切换之前，把其他任务的数据区设置成不能访问，以免造成相互污染
- 相关设计资源
  - AN4838 STM32上的MPU
  - PM0056, PM0223 , PM0214, PM0253 Cortex-M3/M0+/M4/M7 内核编程手册

所有系列都有　　取决于产品型号

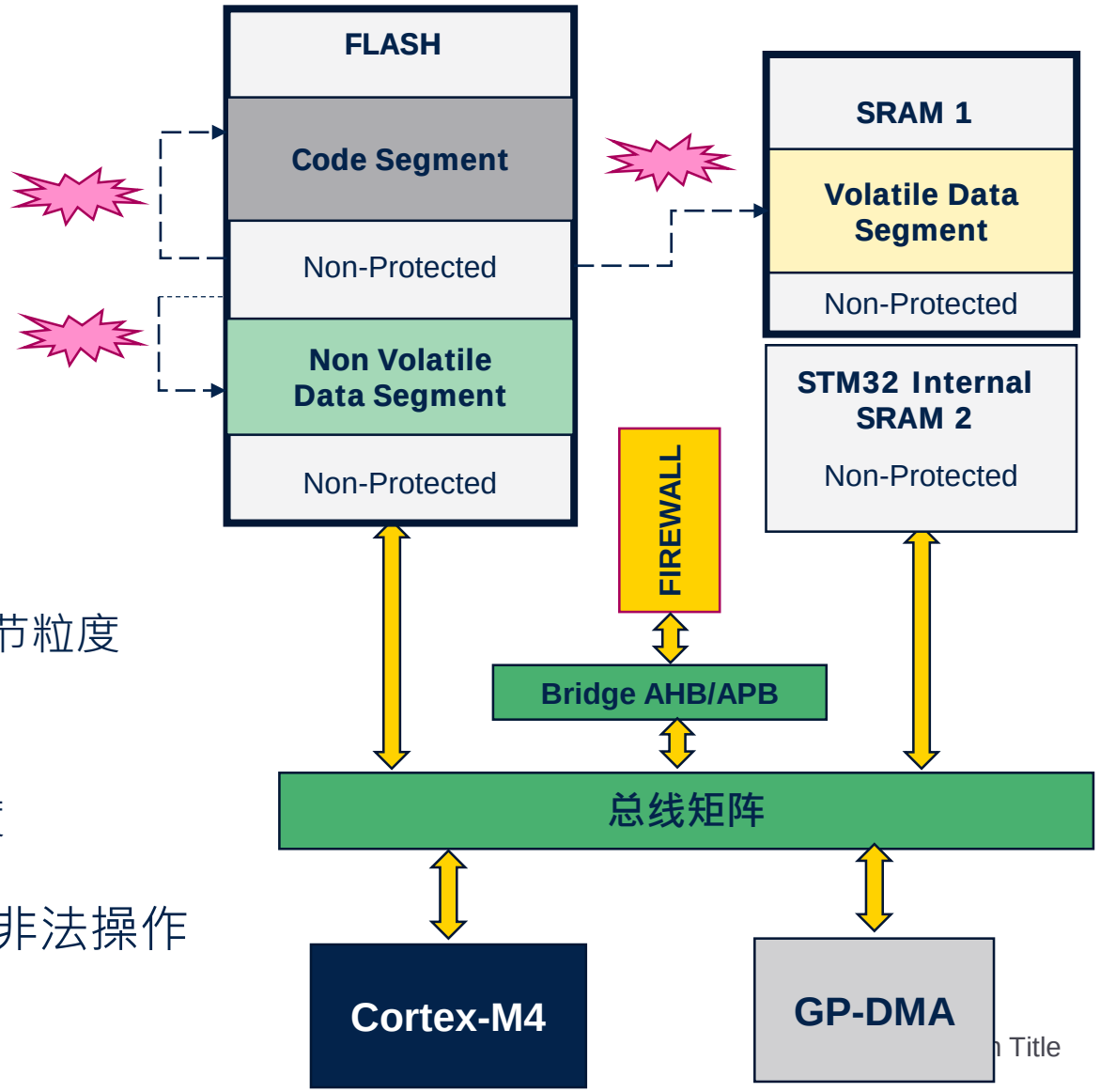
从产品系列来看 MPU



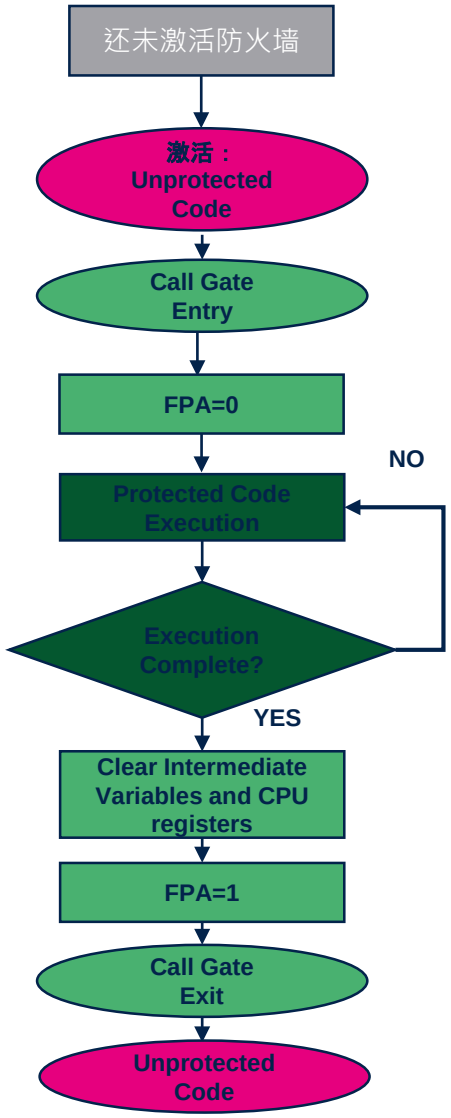
life.augmented

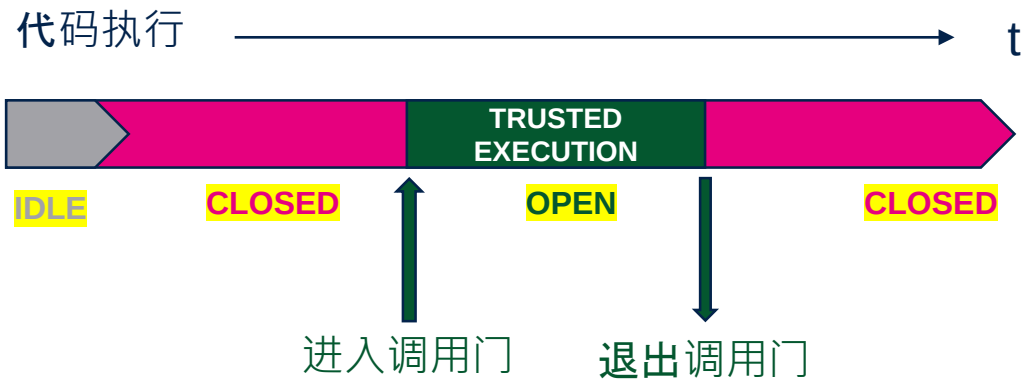
STM32防火墙 Firewall

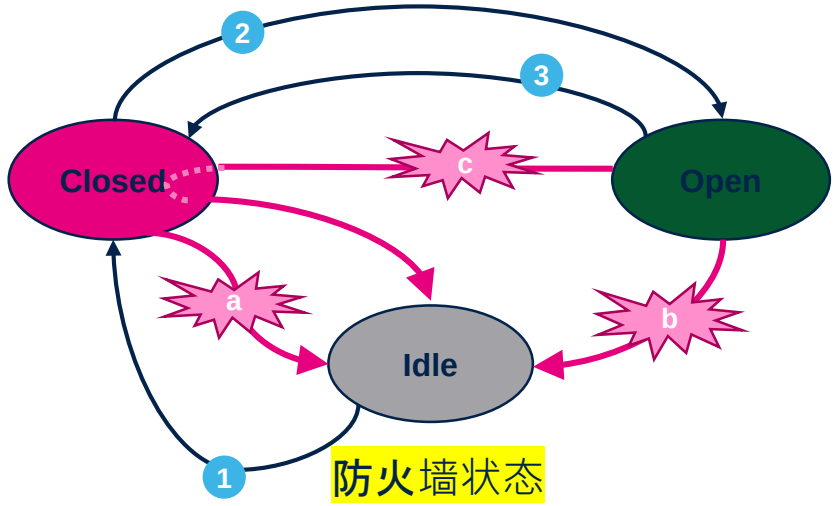
- 原理
  - 保护的对象是？防的是谁？
- 实现
  - Flash上的Code segment
    - 存放敏感操作；256字节粒度
  - Flash上的NV Data segment
    - 通常存放敏感常数，比如加解密密钥；256字节粒度
  - SRAM1上的V Data segment
    - 可以存放受保护代码相关的变量；64字节粒度
  - 所有违背segment属性和当前防火墙状态的非法操作都会触发复位



防火墙的运行时保护







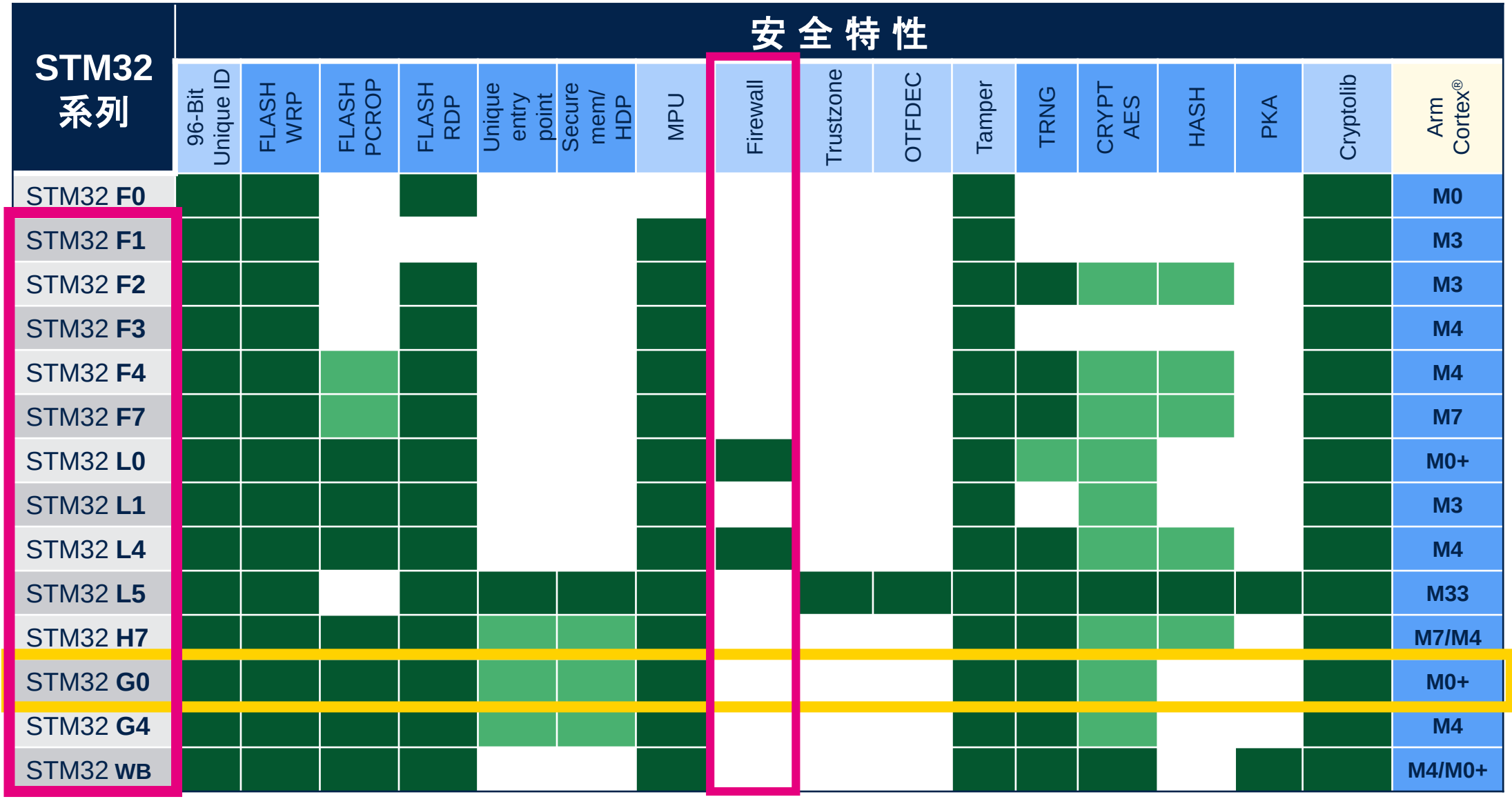
- **正确的跳转**
  1. **配置后并激活防火墙**
  2. 进入调用门 // **按照合适的序列**进入
  3. **离开保护区域 // 遵循合适的退出序列**
- **异常会导致复位**
  - a. **未**经调用门而非法访问保护区
  - b. **非法退出**
    - 马上复位
    - c. **防火墙关闭，执行完返回时触发复位**

防火墙常见用法

- 防火墙使用注意事项
  - 进入防火墙执行前，最好关闭中断（如果ISR在墙外）
    - 否则中断发送时会立刻产生复位，或者在ISR执行完返回时复位，取决于FPA
  - 通过寄存器操作激活防火墙功能（防火墙状态IDE → Close）， 直到下一次系统复位，防火墙状态才能再次回到IDLE
  - PC从固定的入口进入，才能Open防火墙；此状态下是可以调试的
- 相关设计资源
  - AN4730 使用L0和L4的防火墙来安全访问敏感代码和数据
  - STM32CubeL4 Nucleo-L496/L476 example/FIREWALL

所有系列都有　　取决于产品型号

从产品系列来看 Firewall



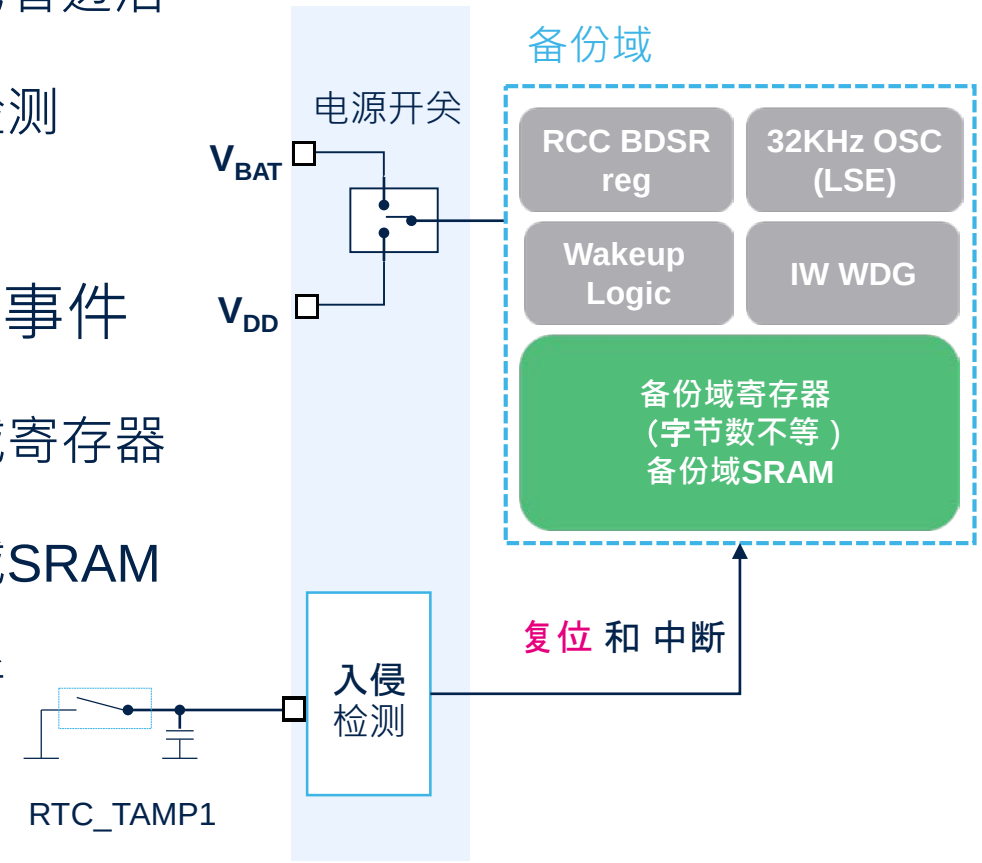
life.augmented

STM32L5 引入新的安全特性

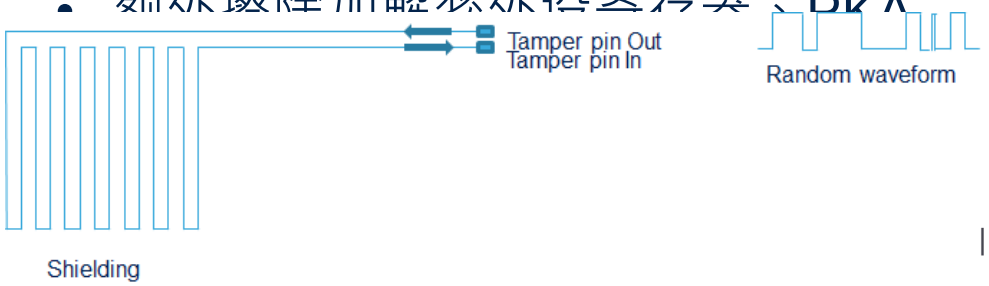
- TrustZone，从ARM Cortex-M33内核，扩展到STM32L5整个系统
  - 新的系统架构，启动模式
  - 新的编程模型
  - 新的安全规划思路
  - 新的生态系统
- OTFDEC
  - 对存储在外部OSPI Flash的数据和指令，取指和取数据，与实时解密同时进行
  - 该功能仅在TZ使能时可用

STM32的入侵检测 Tamper

- **静**态入侵检测，**L5之外的STM32系列**
  - 检测电平或者边沿
  - **容易**绕开检测
- 检测到入侵事件
  - **擦除**备份域寄存器
  - **擦除**备份域SRAM
  - **可**产生中断



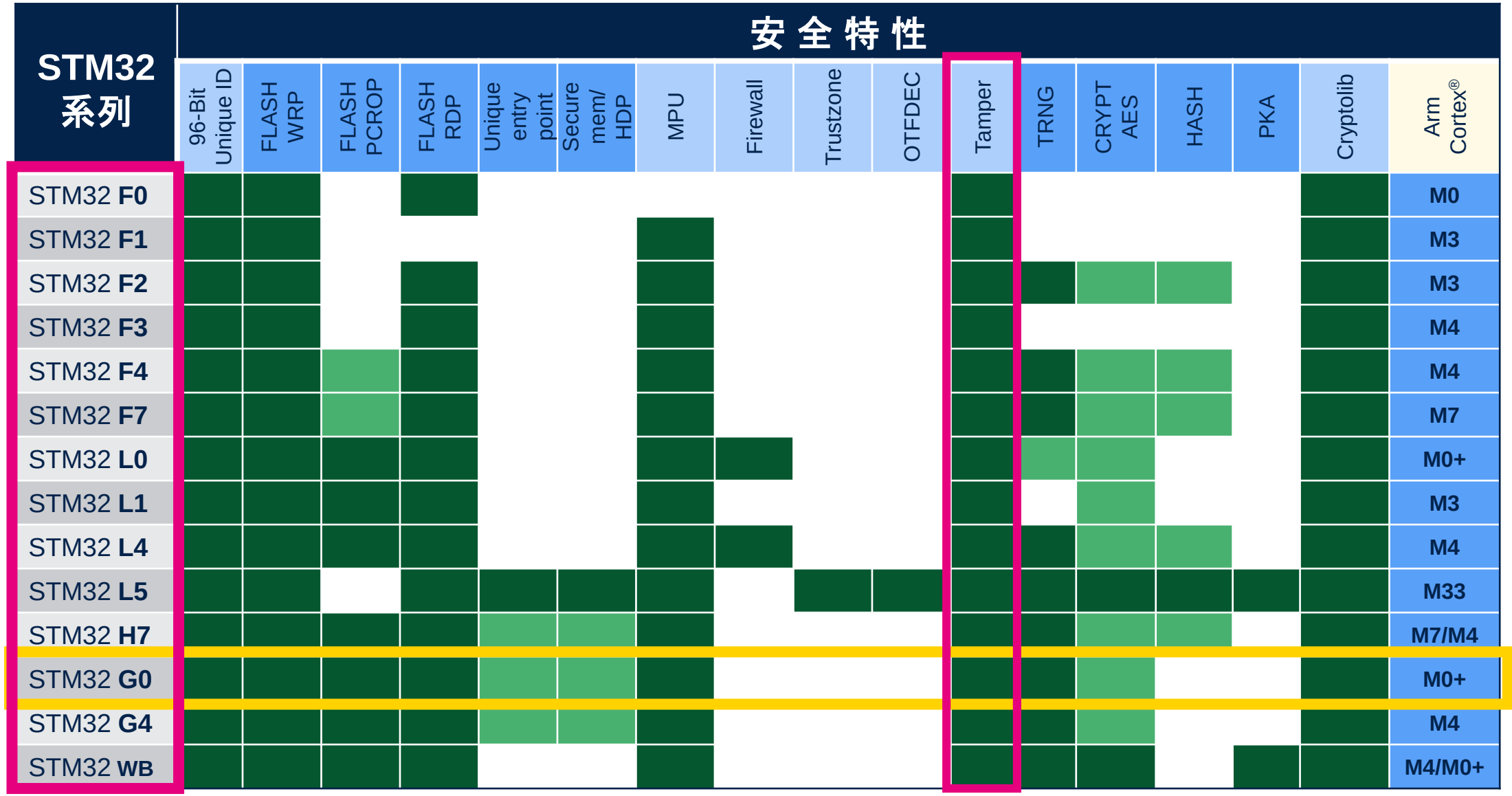
- 动态入侵检测， STM32L5
  - **高达**8对检测回路 Tamper_pin_INx/Tamper_pin_OUTx
  - **在回路上**发送随机数pattern
- 检测到入侵事件
  - 额外擦除ICACHE、4KB SRMA2
  - 额外擦除加解密外设寄存器、PKA



life.augmented

所有系列都有　　取决于产品型号

从产品系列来看 tamper



life.augmented

本期回顾

- **STM32安全特性概览**
  - 存储与执行保护模块
  - 密码学加速模块
  - 信息安全软件包
  - 信息安全的服务：SFI
- **STM32的存储与执行保护模块**
  - WRP、PCROP、RDP、UBE、TZEN
  - Firewall、Secure user memory
  - MPU、Tamper

谢　谢

life.augmented