AN5827

应用笔记

STM32MP1 系列 MPU 进入 RMA 状态的指南

简介

STM32MP1 系列微处理器包括 STM32MP15xx 和 STM32MP13xx 器件。
本应用笔记提供信息以支持退货分析状态进入过程（在本文档中称为 RMA）。

1 概述

本文档适用于基于 Arm® Cortex®核心的 STM32MP1 系列微处理器

注意 *Arm 是 Arm Limited（或其子公司）在美国和/或其他地区的注册商标。*

arm

参考文档

表 1. 参考文档

参考	文件标题
STM32MP13xx	
AN5474	STM32MP13x 系列硬件开发入门
DS13878	Arm® Cortex®-A7 频率可达 1 GHz、1×ETH、1×ADC、24 个定时器、音频
DS13877	Arm® Cortex®-A7 频率可达 1 GHz、1×ETH、1×ADC、24 个定时器、音频、密码和广播安全性
DS13876	Arm® Cortex®-A7 频率可达 1 GHz、2×ETH、2×CAN FD、2×ADC、24 个定时器、音频
DS13875	Arm® Cortex®-A7 频率可达 1 GHz、2×ETH、2×CAN FD、2×ADC、24 个定时器、音频、密码和广播安全性
DS13874	Arm® Cortex®-A7 频率可达 1 GHz、LCD-TFT、相机接口、2×ETH、2×CAN FD、2×ADC、24 个定时器、音频
DS13483	Arm® Cortex®-A7 频率可达 1 GHz、LCD-TFT、相机接口、2×ETH、2×CAN FD、2×ADC、24 个定时器、音频、密码和广播安全性
RM0475	基于 Arm®的 STM32MP13xx 高级 32 位 MPU
STM32MP15xx	
AN5031	STM32MP151、STM32MP153，以及 STM32MP157 系列硬件开发入门
DS12500	Arm® Cortex®-A7 800 MHz + Cortex®-M4 MPU、 TFT、35 个通信接口、25 个定时器、广播模拟
DS12501	Arm® Cortex®-A7 800 MHz + Cortex®-M4 MPU、 TFT、35 个通信接口、25 个定时器、广播模拟，密码
DS12502	Arm® dual Cortex®-A7 800 MHz + Cortex®-M4 MPU、TFT、37 个通信接口、29 个定时器、广播模拟
DS12503	Arm® dual Cortex®-A7 800 MHz + Cortex®-M4 MPU、TFT、37 个通信接口、29 个定时器、广播模拟，密码
DS12504	Arm® dual Cortex®-A7 800 MHz + Cortex®-M4 MPU、3D GPU、TFT/DSI、37 个通信接口、29 个定时器、广播模拟
DS12505	Arm® dual Cortex®-A7 800 MHz + Cortex®-M4 MPU、3D GPU、TFT/DSI、37 个通信接口、29 个定时器、广播模拟，密码
RM0441	基于 Arm®的 STM32MP151 高级 32 位 MPU
RM0442	基于 Arm®的 STM32MP153 高级 32 位 MPU
RM0436	基于 Arm®的 STM32MP157 高级 32 位 MPU

术语和缩略语

表 2. 缩略语定义

术语	定义
FAR	故障分析请求：用于将可疑器件返回意法半导体进行分析的流程。为了在这种分析过程中增强器件的全面可测试性，器件必须处于 RMA 状态。
JTAG	联合测试行动小组（调试接口）
PMIC	通过信号和串行接口提供具有很大可控性的各种平台电源的外部电源管理电路。
RMA[1]	返货分析：器件在生命周期中的特定状态，允许意法半导体根据需要激活全面测试模式，以便进行故障分析。

1. *在本文档中，首字母缩略词 RMA 在任何地方都没有提到“退货验收”，这是用于退回未使用部件（例如客户库存）的流程。*

2 FAR 流程中的 RMA 状态

FAR 流程在于将器件返回意法半导体进行更深入的故障分析，以防出现可疑的质量问题。部件必须以可测试状态返回意法半导体，以便可以执行分析。

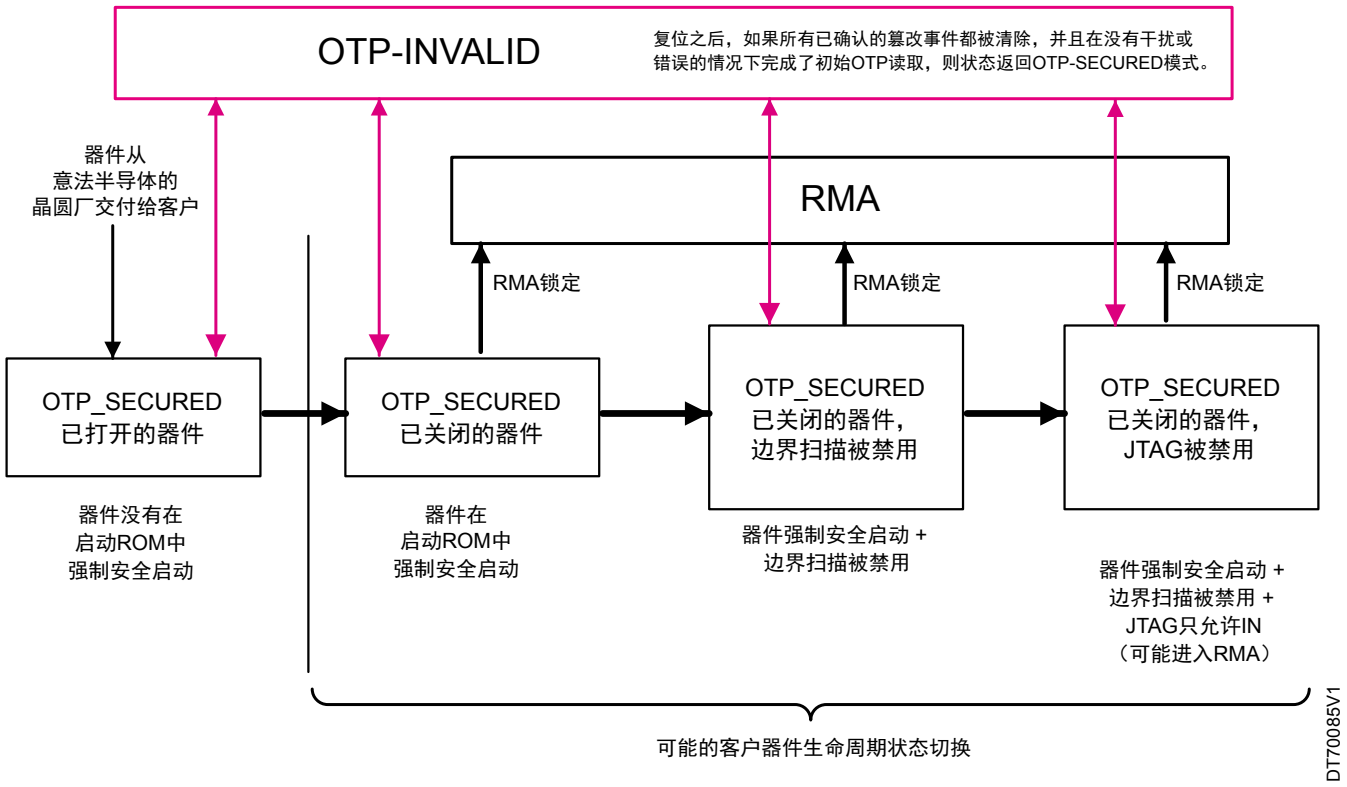
- 部件必须处于 RMA 状态
- 部件必须在物理上兼容原始器件（焊球尺寸、间距等）

2.1 STM32MP13xx 产品生命周期

对于 STM32MP13xx 器件，在将器件返回意法半导体之前，客户必须在器件上进入 RMA 状态，方法是通过 JTAG 输入客户预定义的 32 位密码（参见第 3 节）。一旦进入 RMA 状态，器件就不能再用于生产目的（参见图 1），并且激活全面测试模式以供意法半导体进行调查，而所有客户机密（参考手册中描述的 OTP 上层）都不会被硬件访问。

下图显示了 STM32MP13xx 器件的产品生命周期。该图表明：一旦进入 RMA 状态，器件就不能再回到其他模式。

图 1. STM32MP13xx 器件的产品生命周期

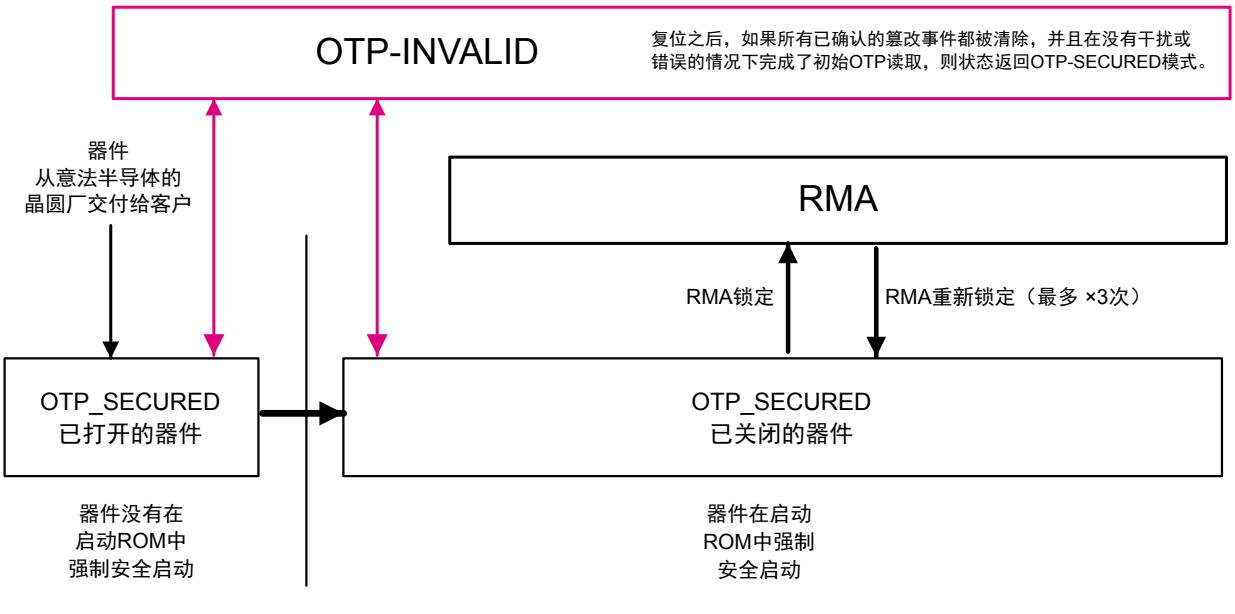


2.2 STM32MP15xx 产品生命周期

对于 STM32MP15xx 器件，在将器件返回意法半导体之前，客户必须在器件上进入 RMA 状态，方法是通过 JTAG 输入客户预定义的 15 位密码（参见第 3 节）。一旦进入 RMA 状态，器件可以通过输入客户预定义的 “RMA_RELOCK”密码，返回到 SECURE_CLOSED 状态。RMA 到 RMA_RELOCKED 的转换状态测试（参见图 2）至多只能进行 3 次。在 RMA 状态下，激活全面测试模式以供意法半导体进行调查，而所有客户机密（参考手册中描述的 OTP 上层）都不会被硬件访问。

下图显示了 STM32MP15xx 器件的产品生命周期。

图 2. **STM32MP15xx 器件的产品生命周期**



3 RMA 状态板件约束

要激活 RMA 状态，需要以下约束。

JTAG 访问应该可用

信号 NJTRST 和 JTDI、JTCK、JTMS、JTDO（STM32MP13xx 器件上的 PH4、PH5、PF14、PF15 引脚）必须可访问。在一些工具（例如，Trace32）上，JTDO 是不必要的；在其他工具（如 OpenOCD）上，工具在执行 JTAG 序列之前通过 JTDO 检查器件的 JTAG ID。

当 NRST 引脚激活后，不应关闭 V_{DDCORE} 和 V_{DD} 电源

在意法半导体的参考设计中，NRST 激活 STPMIC1x 或外部分立元件稳压器的断电重启。应用笔记 *STM32MP13x 系列产品硬件开发入门*（AN5474）中提供的参考设计示例中显示了可能的实现。 图 3 和图 4 是简化版本，只显示与 RMA 状态相关的组件。同样适用于 STM32MP15xx 器件。

图 3. 基于 STPMIC 的设计上与 RMA 状态有关的附加组件

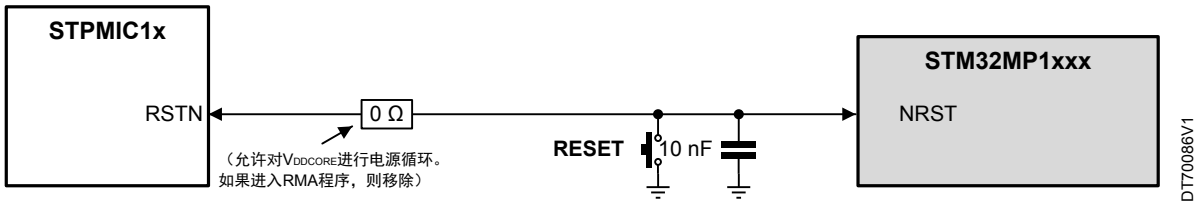
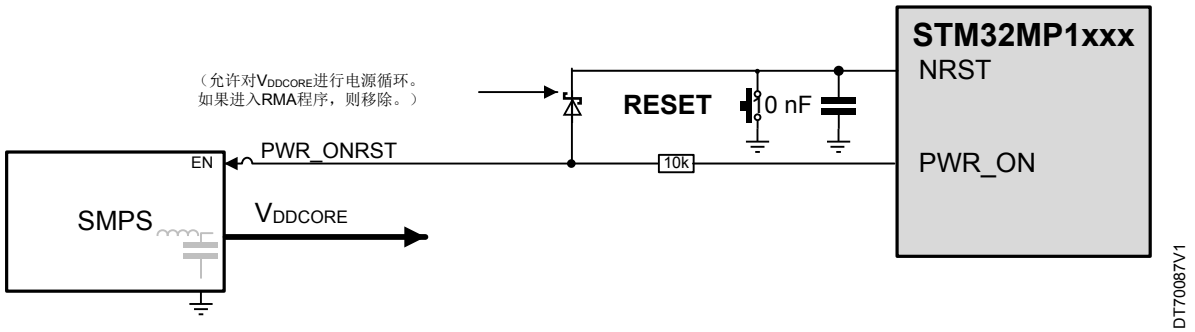


图 4. 基于分立元件供电的设计上与 RMA 状态有关的附加组件



仅配备 JTAG 引脚和适当插座的简单板件可以仅用于与 RMA 密码有关的用途（以防不能访问生产板件上的 JTAG）。在这种情况下，客户必须首先将器件从生产板件上拆焊，并重新填充封装焊球。

板件必须将表 3 中列出的 STM32MP1xxx 引脚按指示进行连接。其他引脚可以浮空。

表 3. （用于 RMA 密码输入的）简单板件的引脚连接

引脚名称（信号）		连接到	备注
STM32MP13xx	STM32MP15xx		
JTAG 和复位			
NJTRST	NJRST	JTAG 连接器	-
PH4 (JTDI)	JTDI		-
PH5 (JTDO)	JTDO		在某些调试工具（如 Trace32）上不需要
PF14 (JTCK)	JTCK/		-
PF15 (JTMS)	JTMS/		-
NRST	NRST	复位按钮	通过 10 nF 电容器连接到 V_{SS}
电源			
VDDCORE, VDDCPU	VDDCORE	外部电源	请参考产品数据手册以获取典型值
VDD, VDDSD1, VDDSD2, VDD_PLL, VDD_PLL2, VBAT, VDD_ANA, PDR_ON	VDD, VDD_PLL, VDD_PLL2, VBAT, VDD_ANA, PDR_ON, PDR_ON_CORE	3.3 V 外部电源	应先准备好再移除（可与其他电源一起）
VDDA, VREF+, VDD3V3_USBHS, VDDQ_DDR	VDDA, VREF+, VDD3V3_USBHS, VDDQ_DDR, VDD_DSI, VDD1V2_DSI_REG, VDD3V3_USBFS	0	AD、CVREFBUF、USB、DDR 未使用
VSS, VSS_PLL, VSS_PLL2, VSSA, VSS_ANA, VREF-, VSS_USBHS	VSS, VSS_PLL, VSS_PLL2, VSSA, VSS_ANA, VREF-, VSS_USBHS, VSS_DSI	0	-
VDDA1V8_REG, VDDA1V1_REG	VDDA1V8_REG, VDDA1V1_REG	浮空	-
其他			
BYPASS_REG1V8	BYPASS_REG1V8	0	1V8 调节器默认启用（REG18E = 1）
PC15- OSC32_OUT	PC15- OSC32_OUT	浮空	外部振荡器未使用（启动 ROM 使用 HSI 内部振荡器）
PC14- OSC32_IN	PC14- OSC32_IN		
PH0-OSC_IN	PH0-OSC_IN		
PH1-OSC_OUT	PH1-OSC_OUT		
USB_RREF	USB_RREF	浮空	USB 未使用
PI6 (BOOT2)	BOOT2	X	无论 boot[2:0]的值是多少，都可以进入 RMA 状态
PI5 (BOOT1)	BOOT1	X	
PI4 (BOOT0)	BOOT0	X	
-	NRST_CORE	10 nF 到 VSS	NRST_CORE 上的内部上拉
PA13 (BOOTFAILN)	PA13 (BOOTFAILN)	LED	可选

4 允许未来进入 RMA 状态的先决条件

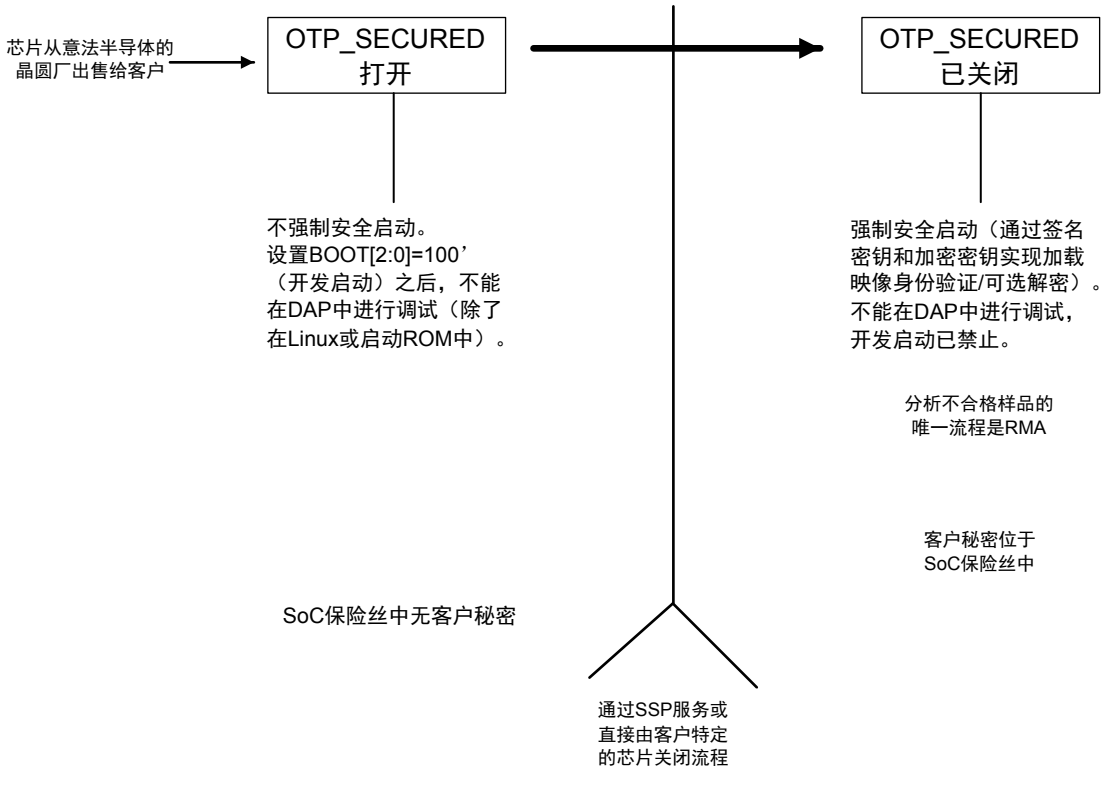
进入 RMA 状态的可能性必须由客户设置，在客户生产过程中先进行秘密配置，然后输入密码即可

- 意法半导体发货时，器件处于 OTP_SECURED 已打开状态。
- 器件包含由启动 ROM 保护的 ST 秘密，并没有客户秘密。
- 在复位或启动 ROM 执行后，可以通过 Linux 或启动 ROM“开发启动”模式重新打开 DAP 访问（OTP_SECURED 已打开 + 启动引脚 BOOT[2:0]=1b100 + 复位）。
- 在 OTP_SECURED 打开的情况下，客户必须在 OTP 中配置其秘密：
  - 直接由客户实施，自己承担风险，或者
  - 使用启动 ROM 的“SSP 功能”和 STM32 工具通过加密通道安全地实施。
- 在秘密配置结束时，客户可以：
  - 在 STM32MP13xx 上的 OTP_CFG56 中融入一个 32 位 RMA 密码（密码必须 ≠ 0）。
  - 在 STM32MP15xx 上的 OTP_CFG56[14:0]中融入一个 15 位 RMA 密码，在 OTP_CFG56[29:15]中融入一个 RMA_RELOCK 密码。

  密码不能是 0。
- 将 OTP_CFG56 设为“永久编程锁定”，避免以后在 0xFFFFFF 处编程，并允许在不知道初始密码的情况下进入 RMA 状态。
- 检查 BSEC_OTP_STATUS 寄存器，以验证 OTP_CFG56 的编程是否正确。
- 最终，器件切换到 OTP_SECURED 已关闭状态：
  - 在 STM32MP13xx 上，使 OTP_CFG0[3] = 1 且 OTP_CFG0[5] = 1。
  - 在 STM32MP15xx 上，使 OTP_CFG0[6] = 1。

  该器件可以在 RMA 状态下重新打开，以便意法半导体进行调查
- 当器件处于“OTP_SECURED 已关闭”状态时，“开发启动”不可用。

图 5. 切换到“OTP_SECURED 已关闭”状态



5 RMA 状态进入详情

如前所述，RMA 状态用于安全地重新打开全面测试模式，而不会暴露任何客户提供的秘密。这要归功于实用的 JTAG 输入，而所有的客户秘密对于硬件来说都是不可访问的。

如果需要对失败的样本进行分析，则需要进入 RMA 状态（参见图 5. 切换到“OTP_SECURED 已关闭”状态），这样可以保全客户秘密，并在 DAP 中重新打开安全和非安全的调试。

1. 客户使用 JTAG 在 BSEC_JTAGIN 寄存器中移入 RMA 密码（只接受除 0 之外的值）。
2. 客户复位器件（NRST 引脚）。

注意 在此步骤中，BSEC_JTAGIN 寄存器中的密码不能被擦除。因此，NRST 不能关闭 V_{DD} 或 V_{DDCORE} 电源。它也不应该连接到 NJTRST 引脚。如果使用 STPMIC1x，在复位期间可能强制屏蔽电源。这是通过对 STPMIC1x 屏蔽选项寄存器（BUCKS_MRST_CR）进行编程或移除为了 RMA 用途而在 STPMICx RSTn 和 STM32MP1xxx NRST 之间的板件上添加的电阻来完成的（参见图 3）。

3. 启动 ROM 被调用并通过 OTP_CFG56.RMA_PASSWORD 检查在 BSEC_JTAGIN 中输入的 RMA 密码：
   - 如果密码匹配，样品变为 RMA_LOCK 样品（永久留在 STM32MP13xx 上）。
   - 如果密码不匹配，则示例在 OTP_SECURED 中保持关闭状态，并且 OTP 中的 RMA“重新打开尝试”计数器递增。

注意 仅允许三次 RMA 重新打开尝试。三次尝试失败之后，不能再次尝试。器件保持其实际生命周期状态。

4. 客户通过 NRST 引脚第二次复位样品：
   - PA13 上的 LED 灯亮起（如果已连接）
   - DAP 调试访问重新打开。
5. 器件可以发给意法半导体。
6. 复位（NRST 引脚或任意系统复位）之后，启动 ROM 被调用：
   - 它检测 OTP8.RMA_LOCK = 1（RMA 已锁定的样本）。
   - 它确保意法半导体和客户的所有秘密安全。
   - 它在安全和非安全状态下重新打开 DAP 调试访问。

在 RMA 状态下，该部件忽略 Boot 引脚，无法从外部 Flash 或 USB/UART 启动。

6 “RMA 解锁”详述

可以将 STM32MP15xx 器件从 RMA 解锁并返回 SECURE_CLOSED 状态。

客户使用 JTAG 在 BSEC_JTAGIN 寄存器中移入 RMA 解锁密码（只接受除 0 之外的值）

- 客户复位器件（NRST 引脚）。

注意 仅允许三次 RMA 解锁尝试。三次尝试失败之后，不能再次尝试 RMA 解锁。器件保持其 RMA 生命周期状态。

- 客户通过 NRST 引脚第二次复位样品：
  - PA13 上的 LED 灯亮起（如果已连接），
  - 器件进入 SECURE_CLOSED 状态（DAP 调试访问已关闭）。

7 在进入 OTP_SECURED 已关闭状态之前禁用 RMA

在生产阶段，可以在器件被设为“OTP_SECURED 已关闭”状态之前完全禁用 RMA。

为此，“RMA 尝试”(OTP8 位[1:3]）应该熔合成 1。

- OTP8[1] rma_req1 第一次尝试 RMA 锁定
- OTP8[2] rma_req2 第二次尝试 RMA 锁定
- OTP8[3] rma_req3 第三次尝试 RMA 锁定

在 STM32MP13xx 器件上，用户还可以将 tamp_itamp6 (JTAG/SWD 访问)设置为已确认篡改，防止在 JTAG 访问尝试时对存储在 SRAM3 和备份 RAM 存储器中的秘密进行任何访问。

8 “通过 JTAG 脚本进入 RMA 状态”示例

输入密码并进入 RMA 状态的 STM32MP13xx 脚本示例以单独的 zip 文件形式提供。它们可以与 Trace32、OpenOCD（使用 STLINK 探针、OpenOCD（使用兼容 CMSIS-DAP 的探针，例如 ULink2）组合运用。更多信息请访问公司网站 www.st.com。参考 STM32MP13xx 产品“板件制造规范”一节中的“CAD 资源”。

也可以为 STM32MP15xx 器件生成类似的示例。通过 Trace32 进入 RMA 状态和退出 RMA 状态的示例以单独的 zip 文件形式提供。更多信息请访问公司网站 www.st.com。参考 STM32MP15x 产品“板件制造规范”一节中的“CAD 资源”。

修订历史

表 4. 文档修订历史

日期	版本	变更
2023 年 2 月 13 日	1	初始版本。
2023 年 7 月 10 日	2	增加了第 7 节: 在进入 OTP_SECURED 已关闭状态之前禁用 RMA。

目录

表一览

图一览