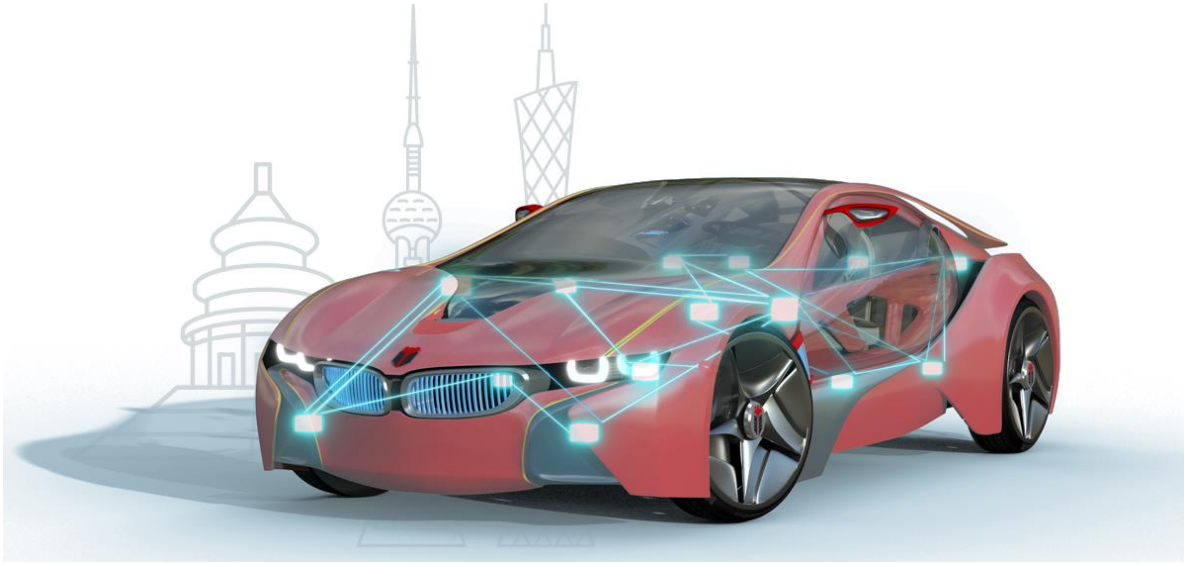
知从木牛瑞萨 RH850 ICUM 信息安全应用介绍

CyberSecurity Application of ZC.MuNiu on Renesas RH850 ICUM

知从木牛基础软件平台信息安全库

ZC.MuNiu Basic Software Platform CryptoLibrary



知从木牛瑞萨 RH850 ICUM 信息安全应用介绍

CYBERSECURITY APPLICATION OF ZC.MUNIU ON RENESAS RH850 ICUM

知从木牛基础软件平台信息安全库

ZC.MuNiu Basic Software Platform CryptoLibrary

1 RH850 ICUM 介绍及信息安全应用 INTRODUCTION OF CYT4BB AND CYBERSECURITY APPLICATIONS

RH850/U2X 系列 32 位汽车微控制器（MCU）专为高性能车身控制单元及多种汽车电子系统设计。该系列芯片采用多核架构，集成多达 4 个主频高达 400 MHz 的 RH850 内核（作为主处理单元）以及一个用于安全处理的附加 ICPM 核。其安全子系统内置丰富的硬件加密加速模块，支持 AES、CHACHA、CMAC、CRC、DES/TDES、SHA1/SHA2/SHA3、HMAC、TRNG/PRNG、RSA 等多种密码算法，可高效实现安全启动、安全刷写、安全通信与安全诊断等关键功能，满足 ASIL-D 等级功能安全及信息安全要求，适用于对实时性与可靠性严苛的汽车应用场景。

CYT4BB TRAVEO™ T2G 32-bit automotive MCU is targeted at automotive systems such as high-end body control units.The CYT4BB features two Arm® Cortex®-M7 CPUs (for main processing) and one Arm Cortex-M0+ CPU (for peripheral and security processing). Among them, the CM0 core integrates a variety of hardware algorithm functions, including: AES, CHACHA, CMAC, CRC, DES/TDES, SHA1/SHA2/SHA3, HMAC, TRNG/PRNG, RSA, and many other algorithms, based on which it can be implemented to extend a variety of information security applications, such as: SecureBoot, SecurUpdate, SecureDiagnostics other functions.

知从木牛信息安全库在原有的硬件算法功能基础上，集成了多种软件算法及扩展应用，如：SM2/3/4、ED25519、RSASSA-PKCS-v1_5(3072、4096bits Key)、RSASSA-PSS-(3072、4096bits Key)、KeyGen(SM2)、KeyGen(ED25519)等算法功能。

In addition, ZC Muniu CryptoLibrary integrates a variety of software algorithms and extended applications based on the original hardware algorithm function, such as: SM2/SM3/SM4, ECDSA 256R1, RSASSA-PKCS-v1_5(4096bits Key), RSASSA-PSS-(4096bits Key), SHE/ USERKEY Load, GetUid, KDF, DebugHandling, etc., to achieve secure storage.

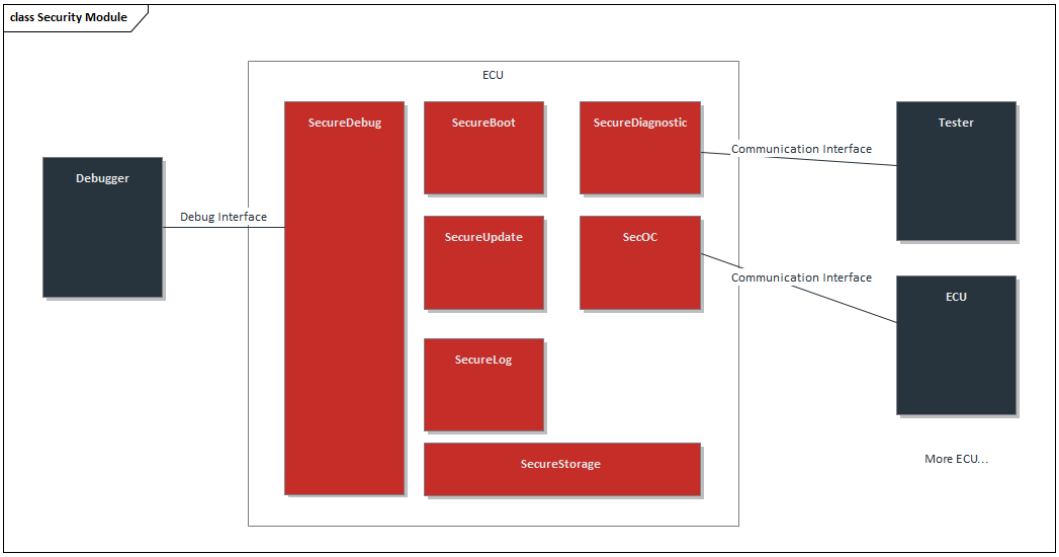


FIGURE 1 CRYPTOLIBRARY ARCHITECTURE

方案对比 Scheme Comparison	硬件加速算法（以具体芯片型号为准） Hardware-Accelerated Algorithm (chip-specific)	软件算法 Software Algorithm
随机数 Random Number	● TRNG ● PRNG	● /
对称算法	● AES128 ECB/CBC/CTR/OCF/CFB ● AES256 ECB/CBC/CTR/OCF/CFB	● SM4
哈希算法 Hash Algorithm	● SH1 ● SHA2 224/256/384/512 ● SHA3	● SM3
消息认证码	● AES128-CMAC ● SHA2-256-HMAC	● AES256-CMAC
签名算法 Digital Signature Algorithm	● ECDSA SECP256r1 ● RSASSA-2048withPSS/PKCS1V15	● RSASSA-3072/4096withPSS/PKCS1V15 ● ECDSA SECP256r1/SECP384r1/SECP521r1 ● ED25519 ● SM2
密钥生成 Key Generation	● ECC SECP256r1	● ED25519
密钥交换 Key Exchange	● ECDH	● X25519
证书支持 Certificate		● X.509

Support		

TABLE1-知从基于 RH850 U2X ICUM 核算法功能实现

TABLE 1 – ZC RH850 U2X ICUM-CORE CRYPTOGRAPHIC FUNCTION IMPLEMENTATION

2 安全启动 SECURE BOOT

安全启动（SecureBoot）是 MCU 的基本功能，通过硬件加密模块来实现，该机制必须独立于用户程序运行，不能被破坏。作为整个安全启动信任链的基础，安全启动主要用于在 MCU 启动之后，用户程序执行之前，对用户定义的 Flash 中关键程序的数据完整性和真实性进行验证，确定是否被篡改。如果验证失败，说明 MCU 处于不可信的状态，部分功能甚至整个程序不能运行。

Secure Boot is a fundamental function of the MCU, implemented through hardware encryption modules. This mechanism must operate independently of user programs and cannot be compromised. As the foundation of the entire secure boot trust chain, Secure Boot is mainly used to verify the integrity and authenticity of key programs defined by users in Flash memory after the MCU starts and before user programs execute, to determine if they have been tampered with. If the verification fails, it indicates that the MCU is in an untrusted state, and some functions or even the entire program cannot run.

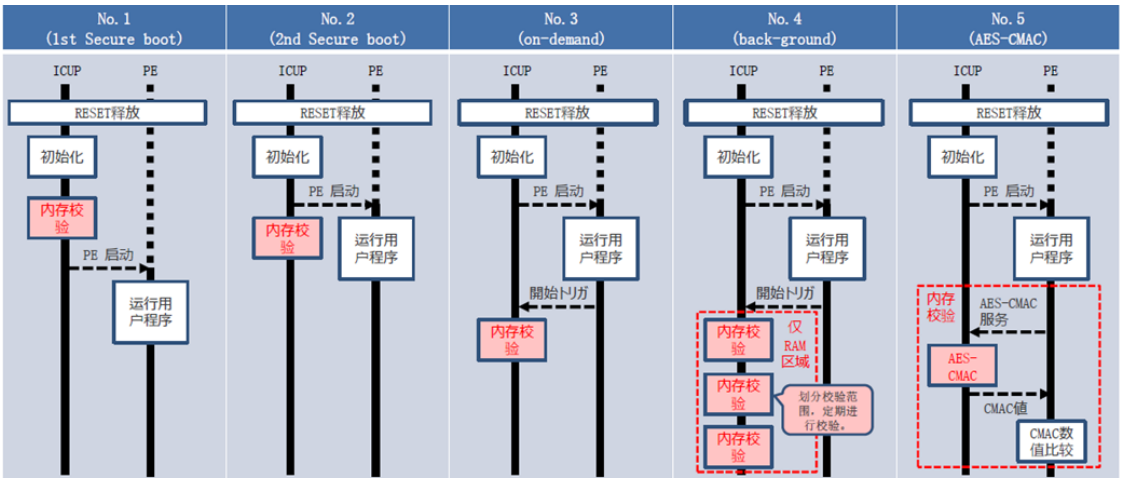


FIGURE 2 SECURE BOOT

SecureBoot 包含 5 个子功能：1st Secure boot, 2nd Secure boot, on-demand，back-ground, AES-CMAC。其中 1st Secure boot 和 2nd Secure boot 为 ICUM 启动后自动执行的 SecureBoot 功能，on-demand、back-ground 和 AES-CMAC 为需要 Host 手动调用的校验功能。

SecureBoot consists of five functions: 1st Secure boot, 2nd Secure boot, on-demand, background, and AES-CMAC. Among them, 1st Secure boot and 2nd Secure boot are SecureBoot functions that are automatically executed after the ICUM is started, while on-demand, background, and AES-CMAC are verification functions that need to be manually invoked by the Host.

用户可以通过 SERVICE_05_MEMCLSTR_VERIFY 和 SERVICE_05_MEMCLSTR_VERIFY_AUTO 功能执行 on-demand、back-ground 和 AES-CMAC 的校验功能。其中 on-demand 为手动定义校验区域内容，通过相关接口直接执行并获取相应校验结果。back-ground 为后台周期性校验所定义的区域，并通过相关接口获取校验结果。

The user can perform on-demand, back-ground, and AES-CMAC checksum functions with the SERVICE_05_MEMCLSTR_VERIFY and SERVICE_05_MEMCLSTR_VERIFY_AUTO functions. On-demand refers to manually defined validation areas where content is directly processed via relevant interfaces to obtain corresponding validation results. Background denotes areas defined for periodic background validation, with results retrieved through relevant interfaces.

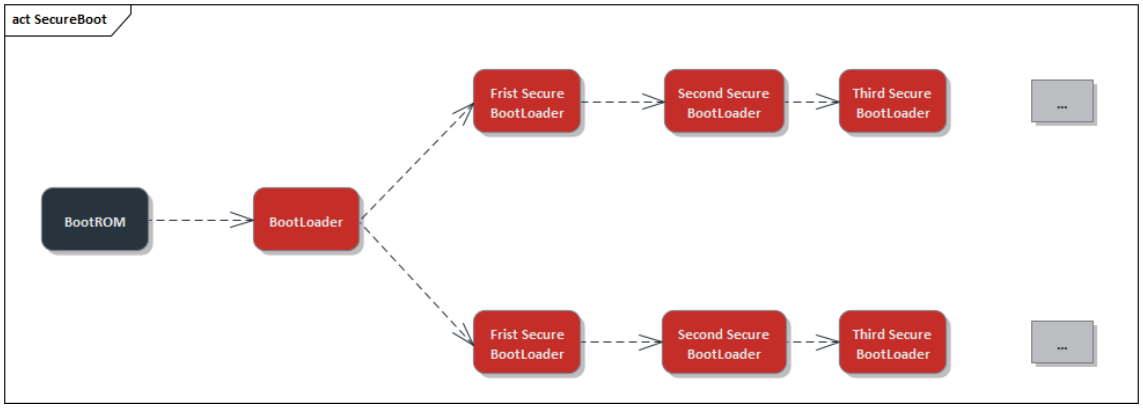


FIGURE 3 SECURE BOOT ROUTINE

SecureBoot 启动自检流程通过 ICUM 实现，ECU 上电启动后 PE 不会被唤醒，优先执行 ICUM 功能，ICUM 检测 1st Secure boot 和 2nd Secure boot 功能是否开启。

The SecureBoot startup self - check process is implemented through ICUP and ICUM. After the ECU is powered on and starts up, PE1 will not be awakened, and the ICUM function will be executed first. The ICUM checks whether the 1st Secure boot and 2nd Secure boot functions are enabled.

若 1st Secure boot 功能开启，则 ICUM 按照预设的校验算法、校验数据范围等配置执行 SecureBoot 校验功能，若校验通过则 ICUM 唤醒 PE1，否则 ECU 停留在 ICUM 中。

If the 1st Secure boot function is enabled, the ICUM will execute the SecureBoot verification function according to the preset configuration such as the verification algorithm and the verification data range. If the verification passes, the ICUM will wake up PE1; otherwise, the ECU will remain in the ICUM state.

若 2nd Secure boot 功能开启，则 ICUM 唤醒 PE1，再按照预设的校验算法、校验数据范围等配置执行 SecureBoot 校验功能，若校验通过则 ICUM 继续执行剩余功能，否则 ICUM 将记录故障并使 ECU 复位，并在启动时按照 1st Secure boot 功能配置对数据进行校验。

If the 2nd Secure boot function is enabled, the ICUM will wake up PE1 first, and then execute the SecureBoot verification function according to the preset configuration such as the verification algorithm and the verification data range. If the verification passes, the ICUM will continue to execute the remaining functions; otherwise, the ICUM will record the fault, reset the ECU, and verify the data according to the 1st Secure boot function configuration during startup.

3 安全诊断 SECURE DIAGNOSTICS

安全诊断（Secure Diagnostic）是保护 ECU 内部数据安全的重要手段，主要用于将程序或数据下载 / 上传到服务器以及从服务器读取特定内存位置的诊断服务需要进行身份验证。异常的程序上传或下载到服务器的数据可能会潜在地破坏电子设备或其他车辆部件，或可能违背车辆的排放或安全等标准。另一方面，当从服务器检索数据时，可能会违反数据安全性。因此需在这些服务执行前，要求上位机证明其身份，在合法身份确认之后，才允许其访问数据和诊断服务。

Secure Diagnostic is an important means of protecting the internal data security of ECUs (Electronic Control Units). It is primarily used for diagnostic services that require identity verification when programs or data are downloaded/upload to a server and when specific memory locations are read from the server. Unusual program uploads or downloads to the server could potentially damage electronic devices or other vehicle components, or may violate vehicle emission or safety standards. On the other hand, when retrieving data from the server, data security could be compromised. Therefore, it is necessary to require the upper computer to prove its identity before executing these services, and only after legal identity confirmation is allowed to access data and diagnostic services.

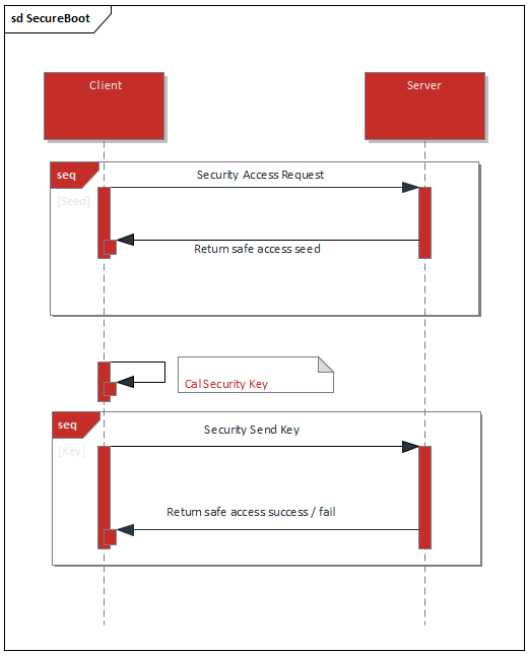


FIGURE 4 SECURE DIAGNOSTIC

基于 RH850 ICUM 核采用可使用 TRNG\PRNG、AES128\256、AES-CMAC、HMAC 等多种硬件加密算法机制，来确认客户端的身份，并决定客户端是否被允许访问。其中，对 AES、CMAC、HMAC 等算法所使用的密钥，皆可使用 LoadKey 接口进行预先存储，通过 KeyID 调用的方式在 ICUM 侧进行处理，保证了身份验证信息的可靠性。

Base on RH850 ICUM core we can uses various hardware encryption algorithms such as TRNG/PRNG, AES128/256, AES-CMAC, HMAC, etc. to confirm the identity of the client and decide whether the client is allowed to access. The keys used for AES, CMAC, HMAC and other algorithms can be stored in advance using the LoadKey interface, and processed on the ICUM side by means of KeyID call, which ensures the reliability of the authentication information.

4 安全升级 SECURE UPDATE

RH850 U2X 一方面可采用其 ICUM 核内部自带的 RSASSA- PSS /PKCS-v1_5 (2048bits Key)、ECDSA SECP256r1 算法，也可采用知从木牛所集成 CryptoLibrary 中的 Ed25519、RSASSA-PKCS-v1_5(3072/4096bits Key)、RSASSA-PSS-(3072/4096bits Key)等，可满足用户的多种算法使用需求。并且，对于其中非对称算法所使用的 PublicKey、PrivateKey，同样可以使用 LoadKey 接口,输入不同类型的 KeyType，将其预先存储于 ICUM 核指定位置，并通过 KeyID 进行调用，保证了安全升级过程的真实性和完整性。

On the one hand, RH850 U2X can adopt the RSASSA-PSS/PKCS-v1_5(2048bits Key) 、ECDSA SECP256r1 algorithm that comes with its ICUM core, and on the other hand, it can also adopt Ed25519, RSASSA-PKCS-v1_5(3072/4096bits Key), RSASSA-PSS-(3072/4096bits Key), and so on, which can satisfy the user's needs for multiple algorithms. Key. Moreover, for the PublicKey and PrivateKey used by the asymmetric algorithms, Inputing different types of KeyType and the same LoadrKey interface can be used to pre-store them in the specified location of ICUM DATAFLASH and invoke them through the KeyID, which ensures the authenticity and integrity of the security upgrade process.

此外，RH850 U2X 也支持证书解析，通过 X.509 证书解析调用接口并配置对于算法，实现基于证书的安全升级机制。

Additionally, the RH850 U2X supports certificate resolution, enabling secure upgrade mechanisms based on certificates by invoking interfaces through X.509 certificate resolution and configuring algorithms.

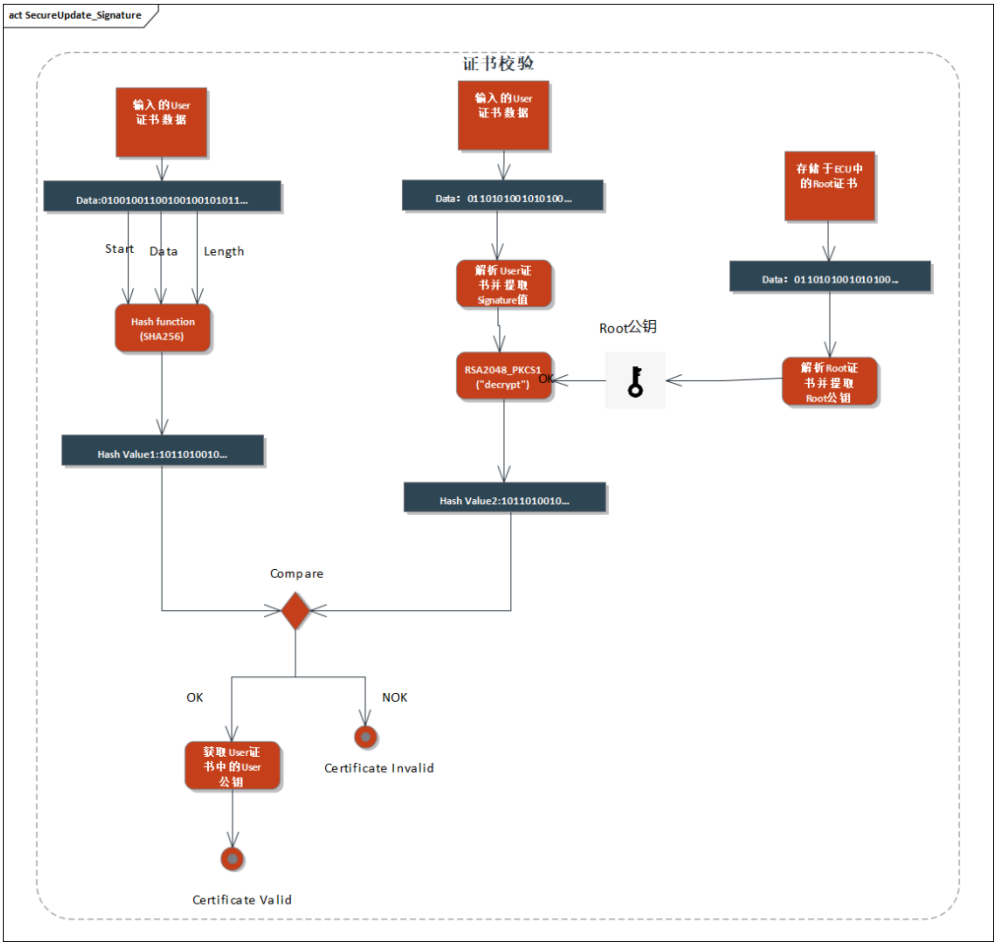


FIGURE 5 SECURE UPDATE WITH CERTIFICATE

5 安全存储 SECURE STORAGE

RH850 ICUM 核通过烧录 OPBT 配置字，在内部专门划定一块用于密钥信息存储的 DFLASH 区域，实现了安全存储的基础。在此基础上，ICUM 核内部配置多把不同类型的密钥槽，包括 AES、RSA、ECDSA 等，每种类型的密钥槽配置多把 KeySlot，可供用户进行不同需求的选择与适配。

The RH850 ICUM core achieves secure storage by programming the OPBT configuration word to dedicate a specific DFLASH region for key information storage. Building upon this foundation, the ICUM core internally configures multiple key slots of different types, including AES, RSA, and ECDSA. Each key slot type supports multiple KeySlots, enabling users to select and adapt to diverse requirements.

RH850/U2X 通过 Option Byte(配置字）修改芯片的 Secure Code Flash 或者 Secure Data Flash。Option byte 位于 Flash 中的特定区域 Configuration Area 中。因此，修改这些 option byte 的方式包括（以 RH850 U2A8/16 举例）：

RH850/U2X modifies the chip's Secure Code Flash or Secure Data Flash via Option Bytes (configuration bytes). Option bytes reside within a specific region of the Flash called the Configuration Area. Therefore, methods for modifying these option bytes include (using the RH850 U2A8/16 as an example):

■ 通过串行编程，使用 RFP/PG-FP6 等上位机程序修改
Modify using host computer programs such as RFP/PG-FP6 via serial programming.
■ 通过芯片自编程修改
Modified through chip self-programming
■ 通过 Debug 指令修改
Modify using the Debug command

生命周期相关的 Option Byte 包括:

Option bytes related to the lifecycle include:

Option byte	Description
ICUMRAC	Secure Code Flash 0/1 Start Address
ICUMRAD	Secure Data Flash Start Address
ICUMRESV	ICUP Reset Address
ICUMON	ICU-M switch (on/off)

ICUMUPGP1	Upgrade Switch 1: Flash Update Lock
ICUMUPGP2	Upgrade Switch 2: Option Bytes Update Lock

上述配置项分布在 ICUM_OPBT0~4 中，位于 Flash 的 Security Configuration Area, 地址为 <SSAk_base>+0x0700~0x0710，U2A16 SSAk_base = 0xFF322700.

ICUMON 位于 ICUM_OPBT0[31:28],默认为 0xF，当设为除 0xF 外其它值时代表 ICUMHB On；

ICUMRESV 位于 ICUM_OPBT1[31:0]，默认值为 0xFFFFFFFF；

ICUMRAC 分别位于 ICUM_OPBT2[31:0]，默认值为 0xFFFFFFFF；

ICUMRAD 位于 ICUM_OPBT3[31:0]，默认值为 0xFFFFFFFF；设置上述 Option Byte 后，安全区域的非安全区域的分配如图所示：

The above configuration items are distributed across ICUM_OPBT0~4, located in the Security Configuration Area of Flash memory at addresses <SSAk_base>+0x0700~0x0710, where U2A16 SSAk_base = 0xFF322700.

ICUMON resides at ICUM_OPBT0[31:28], defaulting to 0xF. Setting it to any value other than 0xF indicates ICUMHB On;

ICUMRESV resides at ICUM_OPBT1[31:0], defaulting to 0xFFFFFFFF;

ICUMRAC is located at ICUM_OPBT2[31:0], with a default value of 0xFFFFFFFF;

ICUMRAD is located at ICUM_OPBT3[31:0], with a default value of 0xFFFFFFFF; After setting the above Option Bytes, the allocation of the secure and non-secure regions is as shown in the figure：