GigaDevice Semiconductor Inc.

GD32H73x_75x 系列安全体系介绍

应用笔记

AN121

1.2 版本

（2026 年 02 月）

目录

图索引

表索引

1. 前言

GD32H73x_75x 系列微控制器（MCU）拥有强大的安全架构，同时提供高性能。

整个生命周期管理包括硬件、芯片中的固件资源以及由 Gigadevice 开发的相关工作软件工具。

本文档帮助用户全面了解 GD32H73x_75x 系列微控制器的安全架构，包括安全特性、安全安装和更新解决方案、安全启动和安全模式。

表 1-1. 适用产品

产品系列	型号
GD32H73x	GD32H737 系列
GD32H75x	GD32H757、GD32H759、GD32H75E 系列

注意：本应用手册仅作参考，若与用户手册或数据手册内容有冲突，以用户手册或数据手册为准。

2. 安全特性

GD32H73x_75x 系列微控制器提供多种安全特性，其中一些是安全外设，如 CRC、TRNG、HAU、CAU，它们是通用加密算法的硬件加速器。还有一些是安全机制，如安全模式、RDP、PCROP、WRP。其他的则是安全固件，如基本安全服务（BSS）、不可变的安全启动代码。

内部闪存通过 FMC AES 加密算法、RDP、PCROP、WRP 以及外部 OSPI 存储器的 RTDEC 进行保护。

这些特性共同促成了一个非常安全的系统。

2.1. 存储器保护单元（MPU）

MPU 是 ARM Cortex-M 提供的一个特性，它允许对所有内存资源设定特定的访问权限，这种保护由 CPU 在运行时动态管理。MPU 将内存地址空间分割成几个区域，每个区域的访问权限可以独立设置，例如：可执行、不可执行（XN）、读写（RW）、只读（RO）或无访问权限。特权和非特权模式。

2.2. 安全保护（SPC）

SPC 对于保护软件或固件免受非法用户侵害非常有用。安全保护是全局性的，不仅可以保护闪存，还可以保护其他安全区域。其他安全区域包括备份 SRAM（BKPSRAM）、RTC 备份寄存器和受实时解密（RTDEC）保护的加密区域。安全保护等级划分三等。

无保护状态：未执行保护。

保护级别低：主存储闪存块仅能被用户代码访问。主闪存只能被用户代码访问。在低安全保护等级下，对于选项字节的所有操作都被允许。

保护级别高：调试模式，从 SRAM 中启动，或者从 boot loader 启动都被禁止。选项字节块可以读取但不能修改。SPC 字节不能重新编程。它不能退回到低保护级别或无保护级别。

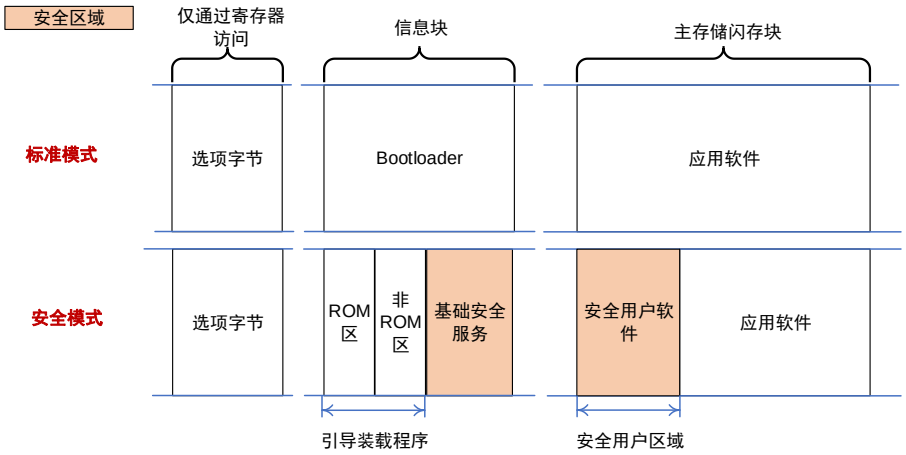
2.3. 内部 Flash 存储器的安全保护

为了保护各种数据和代码，GD32H73x_75x 系列 MCU 提供了标准模式和安全模式。

在标准模式下，内部闪存的主要闪存块可以分割为用户区域和 DCRP 区域，DCRP 区域仅允许来自系统的指令，但不允许数据访问。

在安全模式下，可以在内部闪存的主存储闪存块，定义一个安全用户区域。

图 2-1. 标准模式和安全模式内部存储架构



2.3.1. 扇区擦除/编程保护

扇区擦除/编程保护功能可以防止对闪存的意外操作。在受保护的扇区上，FMC 将不能被被擦除或编程。配置选项字节的 WP[21:0]某位为 0 可以单独使能某几扇区的保护功能。

表 2-1. 扇区保护的 WP 位

WP位	扇区保护
WP[0]	扇区 0~扇区 15
WP[1]	扇区 16~扇区 31
. . .	. . .
WP[14]	扇区 224~扇区 239
WP[15]	扇区 240~扇区 255
WP[16]	扇区 256~扇区 383
WP[17]	扇区 384~扇区 511
. . .	. . .
WP[20]	扇区 768~扇区 895
WP[21]	扇区 896~扇区 959

注意：对于 WP[x] (x=0…15)，1 位对应 16 个扇区，范围为扇区(x*16)~扇区(x*16+15)；

对于 WP[x] (x=16…20)，1 位对应 128 个扇区，范围为扇区(x*128 - 1792)~扇区(x*128 - 1665)；

对于 WP[21]，1 位对应 64 个扇区，范围为扇区 896~扇区 959；

修改内部闪存或选项字节只能通过 FMC_CTL 或 FMC_OBCTL 寄存器完成。

2.3.2. 专用代码读取保护（DCRP）

在主存储闪存块，FMC 可以定义仅执行区域，仅允许来自系统的指令，但不允许数据访问。

可以通过设置粒度为 4KB 字节的 DCRP_AREA_END[10:0]和 DCRP_AREA_START[10:0]选项字节来定义一个 DCRP 区域。DCRP 区域也可以通过修改熔丝中的 MCU 保留参数来配置，粒度为 32KB 字节。

在该区域执行代码时，将忽略调试事件。只有 CPU 可以访问它，且只使用指令获取任务。在其他所有情况下，访问 DCRP 区域都是非法的。有效的 DCRP 区域受擦除保护。

2.3.3. 安全用户区域

在主存储闪存块，可以定义安全用户区域。只有在 CPU 执行安全应用程序时，才能访问此区域。

安全用户区域可以将安全用户代码与应用程序非安全代码隔离。安全用户区域可用于保护自定义安全引导库、固件更新代码或第三方安全库。

可以通过设置粒度为 4KB 字节的 SCR_AREA_END[10:0]和 SCR_AREA_START[10:0]选项字节来定义一个安全用户区域。除了选项字节，安全用户区域还可以通过修改熔丝中的用户控制参数来配置，粒度为 32KB。

在该区域执行代码时，将忽略调试事件。只有通过 CPU 执行 GD 安全库或用户安全应用程序来访问它。在其他所有情况下，访问安全用户区域是非法的。

有效的安全用户区域受擦除保护，不能擦除位于该区域的扇区。

有关安全存储管理的更多信息，请参考 ***AN113 GD32H73x_75x 系列安全存储管理***。

2.4. 外部 Flash 存储器的安全保护

GD32H73x_75x 系列微控制器仅对外设 SPI 存储器提供安全保护。

2.4.1. OSPI 存储器的实时解密（RTDEC）

GD32H73x_75x 系列微控制器提供多达两个 RTDEC。每个 RTDEC 可以配置四个独立且不同的加密区域。每个 RTDEC 块被分配给两个 OSPI 端口之一，且 OSPI 应配置为内存映射模式。当从 OSPI 闪存读取加密数据时，RTDEC 以 AES-128 CTR 模式执行实时解密。

有关从 OSPI 闪存启动的更多信息，请参考 GD32H7 微控制器用户指南中的 ***AN122 GD32H7 系列 MCU OSPI flash 执行环境用户指南***。

2.5. 唯一设备标识符

每个设备都有一个 96 位的唯一标识符，该标识符无法修改。这些位可以被用户读取，并且在

所有 GD32H73x_75x 产品中不会重复。它可以用作序列号，或作为安全密钥的一部分等。这个唯一的设备 ID 不能由用户指定或更改。

2.6. 硬件唯一密钥（HUK）

每个设备都有一个硬件唯一密钥，这是一个 128 位的私钥。硬件唯一密钥为保密性提供信任根（RoT）。硬件唯一密钥不能被用户直接访问，只能通过 ROM 代码访问。

2.7. 设备证书

每个设备都有一个用于交换加密消息的证书。该证书由 Gigadevice 使用我们的私钥签名。它包含公钥、签名和其他信息。

2.8. 电子熔丝

GD32H73x_75x 系列微控制器支持 32×32 位的一次性可编程 EFUSE，用于用户数据个性化或配置。作为非易失性存储单元，EFUSE 宏单元的位一旦被编程为 1，就不能恢复为 0。EFUSE 数据结构如下：

表 2-2. EFUSE 数据结构

名称	位宽/字节	起始地址	描述
用户控制段	4B	10'd0	用户控制参数. 详细内容请参考用户手册中的用户控制寄存器(EFUSE_USER_CTL)
MCU 保留段	4B	10'd32	MCU 保留参数 详细内容请参考用户手册中的 MCU 保留寄存器(EFUSE_MCU_RSV)
调试秘钥	8B	10’d64	调试秘钥 详细内容请参考用户手册中的调试秘钥寄存器 x (EFUSE_DPx) (x = 0,1)
AES 密钥	16B	10'd128	加密固件所需的 AES 秘钥 详细内容请参考用户手册中的固件 AES 密钥寄存器 x (EFUSE_AES_KEYx) (x = 0…3)
用户数据	16B	10'd256	用户自定义数据 详细内容请参考用户手册中的用户数据寄存器 x (EFUSE_USER_DATAx) (x = 0…3)

2.9. 循环冗余校验管理单元（CRC）

循环冗余校验（CRC）是一种错误检测码，通常用于数字网络和存储设备中，以检测原始数据

的意外变化。CRC 计算单元可以用来计算用户可配置多项式内的 7/8/16/32 位 CRC 码。

2.10. 真随机数生成器（TRNG）

真随机数生成器（TRNG）模块可以通过使用连续模拟噪声生成一个 32 位随机值，并且已经预先通过了 NIST SP800-90B 认证。128 位随机值种子是从模拟噪声中生成的。

2.11. 密码加速单元（CAU）

加密加速单元（CAU）用于使用 DES、Triple-DES 或 AES（128、192 或 256）算法对数据进行加密和解密。支持具有不同密钥长度的 DES/TDES/AES 算法，在 CAU 中以多种模式执行数据加密和解密。CAU 是一个 32 位外设，支持 DMA 传输，并且数据可以在输入和输出 FIFO 中被访问。

2.12. 哈希加速单元（HAU）

哈希加速单元（HAU）用于信息安全。支持安全哈希算法（SHA-1、SHA-224、SHA-256）、消息摘要算法（MD5）和基于密钥的哈希消息认证码（HMAC）算法，以满足各种应用需求。对于长度为（264 - 1）位的消息，SHA-1、SHA-224、SHA-256 和 MD5 算法分别计算出的摘要长度为 160/224/256/128 位。在 HMAC 算法中，SHA-1、SHA-224、SHA-256 或 MD5 将被调用两次作为哈希函数，以产生认证消息。

2.13. 安全 JTAG

安全 JTAG 功能仅适用于 JTAG 接口，而不适用于 SWD 接口。当通过编程相关 EFUSE 从 0 变为 1 时，调试接口将不可逆地从 SWD 接口切换到 JTAG 接口。

有关 Secure JTAG 的更多信息，请参考 ***AN111 GD32H73x_75x 系列软件开发指南***。

2.14. 系统监控

系统监控功能可用于检测错误操作，并有助于防止某些类型的攻击。

2.14.1. 防篡改保护

防篡改检测是专门针对安全的功能，它可以通过微控制器引脚检测系统级别的物理篡改尝试，例如打开产品的外壳。此功能可以由 RTC 备用电池供电，这意味着即使 VDD 关闭，也能始终检测并触发保护。当检测到篡改尝试时，相关寄存器可能会被重置，内存可以被用户擦除。

2.14.2. 时钟监控

HXTAL 时钟监控（CKM）和 LXTAL 时钟监控（LCKM）用于保护免受外部振荡器故障的影响。一旦检测到外部振荡器故障，相应的时钟将自动切换到内部时钟。并且将生成一个时钟故障事件或中断。此故障中断连接到不可屏蔽中断。

如果时钟故障注入、冻结或毛刺被用作攻击的一部分，它将被检测并阻止。

2.14.3. 电源监控

将检测异常低的电压水平，以确保微控制器在特定的电压范围内工作。为了保证微控制器的行为，防止故障注入攻击。

2.14.4. 温度传感器

内部温度传感器可以实时测量设备温度。改变环境温度可能是故障注入攻击或在线拆卸的一部分。用户可以持续监控设备温度并采取适当行动。

2.15. 安全固件

在 GD32H73x_75x 系列中存在固件，该固件只能在安全模式下使用，即使在安全模式下也无法读取。

2.15.1. 基础安全服务（BSS）

基础安全服务（BSS）是 Gigadevice 提供的用于安全服务配置的软件，它位于内存映射中信息块的安全区域。

有关 BSS 的更多信息，请参考 ***AN115 GD32H73x_75x 系列基础安全服务用户指南***。

BSS 在启动时和运行时提供安全服务。

BSS 函数如下所列，通过 bss.h 调用相关的安全服务。

表 2-3. BSS 函数

函数	描述
BSS_get_version	获取BSS版本
BSS_get_status	获取BSS状态
BSS_get_certificate	获取BSS证书
BSS_get_certificate_size	获取BSS证书大小
exitSecureArea	退出安全用户区并跳转到用户应用程序
resetAndInitializeSecureAreas	根据SCR_AREA_START和SCR_AREA_END选项字节设置安全用户区的范围

2.15.2. 不可变的安全启动代码

安全启动代码有助于实现系统的安全启动，它将在从 ROM 启动后执行，负责在执行前对应用程序进行认证和完整性检查。

这些代码在启动后被隐藏，用户无法读取。

3. 安全安装和更新

固件安装和更新是设备生命周期管理中非常重要的一部分。固件使用非对称密钥签名，并将在安装到 GD32H7 系列微控制器之前进行验证。

3.1. 授权固件安装（LFI）

LFI 是在 GD32 微控制器中实现的一种安全机制，它允许在不受信任的生产环境中（例如 OEM 合同制造商）安全且有计数地安装 OEM 固件。SFI 是在安全引导程序中实现的。授权固件安装（LFI）用于帮助安全地将 OEM 固件安装到内部闪存中。LFI 仅在安全模式下可访问。

LFI 允许原始设备制造商固件代码和配置数据以加密文件的形式交付和编程，然后解密并安装在微控制器内部，以降低固件泄露的风险。

LFI 必须使用 Gigadevice 提供的 HSM（硬件安全模块）来实现认证和完整性检查，OEM 必须使用 GD32 LFI Creator 工具来使用自己的 AES 密钥对安全固件进行编程。

有关 LFI 的更多信息，请参考 ***AN118 GD32H73x_75x 系列微控制器授权固件安装（LFI）概览***。

3.2. 授权固件安装 X (LFIx)

LFIx（Licensed Firmware Install X）用于帮助安全地将 OEM 固件安装到 OSPI 闪存中。LFIx 可以在标准模式或安全模式下使用，以加密图像的形式对外部 OSPI 闪存进行编程。这确保了产品整个生命周期中外部固件和数据的安全。

用户的程序和数据在生命周期中始终被加密。

有关 LFIx 的更多信息，请参考 ***AN122 GD32H73x_75x 系列微控制器 OSPI 闪存执行环境用户指南***。

有关软件操作的更多信息，请参考 ***GD Licensed Data Creator User Manual***。

3.3. 授权固件更新（LFU）

产品交付给最终用户后，OEM 通常需要更新固件。更新环境可能是不可信的。

授权固件更新（Licensed Firmware Update, LFU）有助于支持安全更新，并且可以使用各种通信接口，例如 USB 磁盘、SD 卡、串行端口 DFU 和以太网。

LFU 是由 Gigadevice 提供的一系列演示程序。用户可以根据自己需要重新开发，并自由组合。

有关安全存储的更多信息，请参考 ***AN119 GD32H73x_75x 系列微控制器授权固件更新（LFU）概览***。

4. 安全启动

GD32H73x_75x 系列微控制器提供了一个启动起始 ROM，根据相关的安全标准，例如 ARM 的 PSA，这允许系统实现安全启动到内部安全的闪存区域。

有关安全存储的更多信息，请参考 ***AN130 GD32H73x_75x 系列安全启动概述***。

安全启动的安全目标是验证下一阶段固件的完整性和认证。安全启动代码，也称为不可变引导程序（IBL），在芯片制造时烧录在 ROM 或类似 ROM 的存储器中。使用的数字签名验证算法是 ECDSA-secp256r1-SHA256。公钥哈希值的高 16 字节由用户存储在 EFUSE 中作为信任根。如果验证成功，则执行下一阶段的固件。如果验证失败，代码将处于循环中等待复位。

4.1. 启动 ROM

在安全模式下，系统复位后，微控制器（MCU）首先启动进入到安全状态，并始终先执行 ROM 代码。ROM 中的代码验证下一个阶段的启动代码是否被允许执行。

4.2. 不可变的安全启动代码

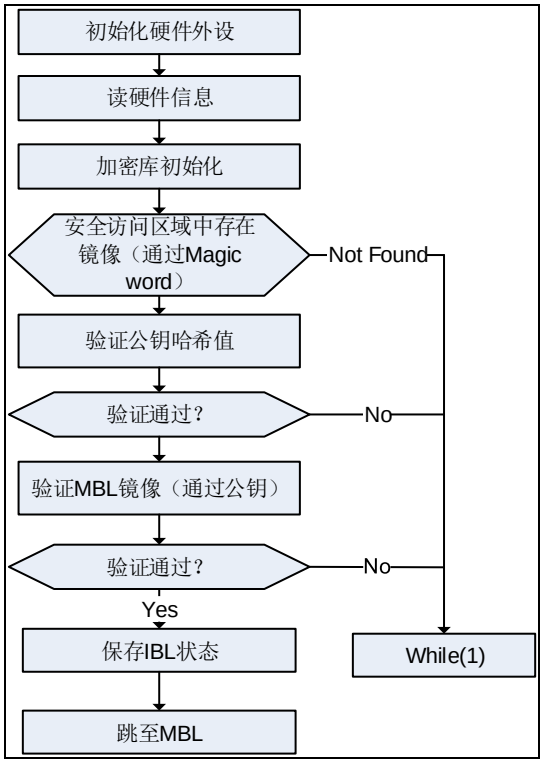
安全启动代码（IBL）被设置为仅执行一次，且无法从外部 ROM 访问。下***表 4-1. 安全启动相关硬件特性***列出了微控制器的安全启动硬件特性。IBL 支持通过 ECDSA 算法进行签名验证。因此，用户可以定制自己的安全引导程序代码，称为主引导程序（MBL）。

表 4-1. 安全启动相关硬件特性

项	硬件特性
熔丝	1. EFUSE User data 密钥仅可写一次。 2. EFUSE 中的位可开启安全启动。
ROM	1. 在将跳转到 MBL 之前，通过写入特定位来关闭 ROM。此后安全引导代码只能在系统复位后才能再次执行。 2. 当代码在安全引导代码区域时，安全引导代码可以访问 SRAM 和安全访问区域，此时调试被关闭。
SRAM	1. 系统复位后，安全引导代码使用的 SRAM 区域会自动清除。
外设	1. TRNG、CAU、HASH 引擎的数据寄存器在系统复位后自动清除。

图 4-1. 安全启动代码流程展示了安全启动过程。系统复位后，IBL（初始引导加载程序）配置外设以进行后续的签名认证过程。如果验证通过，MCU（微控制器单元）跳转到 MBL（主引导加载程序），否则，它进入无限循环并等待下一次复位。

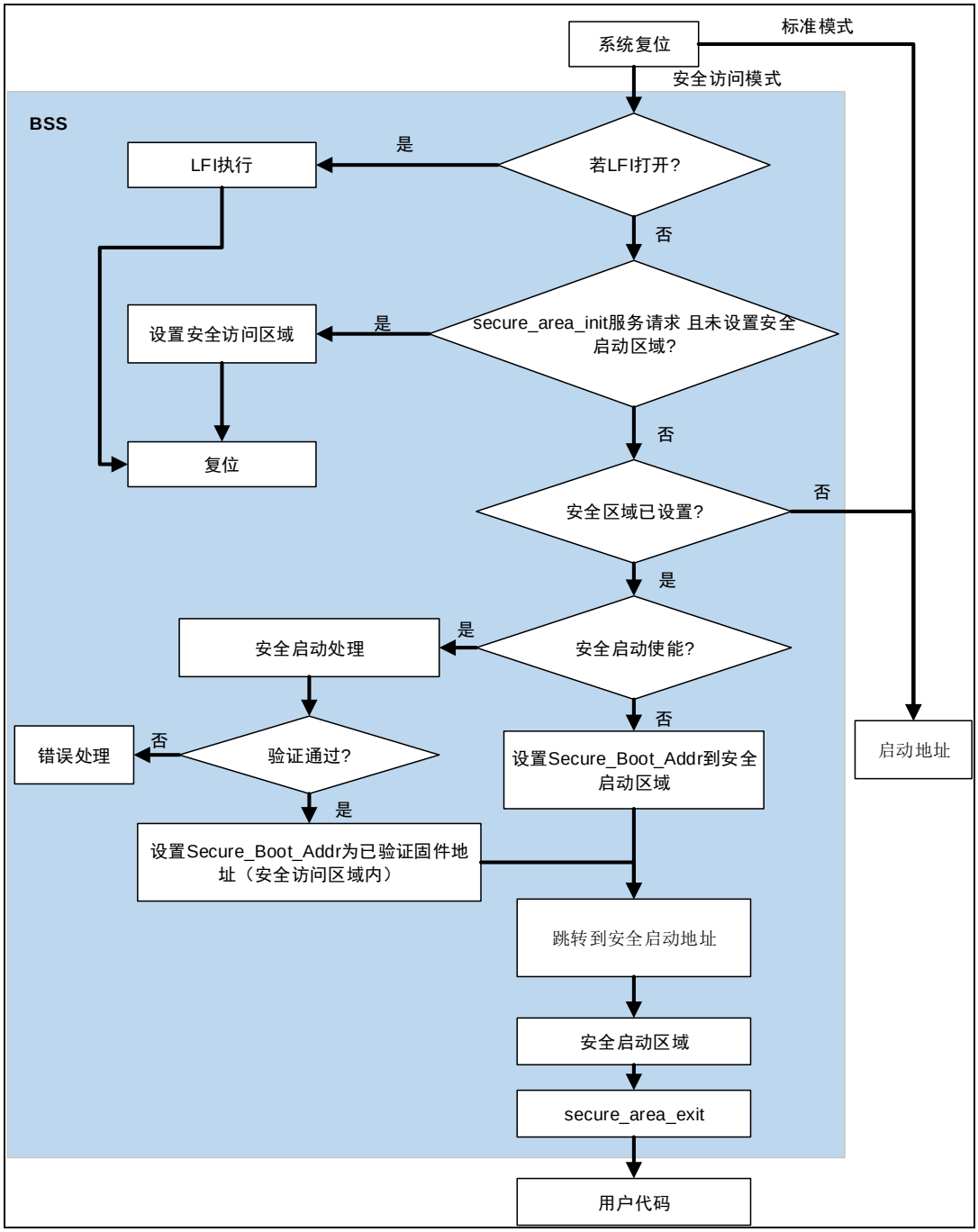
图 4-1. 安全启动代码流程



4.3. 从内部 Flash 存储器安全启动。

当用户应用程序在内部闪存中运行时，安全启动会检查代码，并在代码正确时跳转到代码。具体的启动过程如*图 4-2. 从内部闪存的 Secure Boot 流程*所示。从内部闪存的安全启动流程。

图 4-2. 从内部闪存的 Secure Boot 流程



用户需要修改代码的起始地址和中断向量表，以确保代码的正确跳转和中断响应。LFI Creator 和 ALL IN ONE 用于代码封装，并且激活了 MCU 的安全启动功能。GD32 All-In-One Programmer 和 GD LFI Creator 的使用可以参考 ***GD32AllInOneProgrammer*** 和 ***GD LFI Creator*** 章节。

5. 从 OSPI 存储器启动

GD32H73x_75x 系列微控制器在标准模式下提供了从外部 OSPI 存储器启动的能力，其中安全启动必须在安全模式下工作。

类似于安全启动，当从 OSPI 存储器启动时，不可变的 Secure Boot 代码会在执行 OSPI 存储器中的程序之前配置 RTDEC 和 OSPI 主机。OSPI 存储器中的代码和数据在下载前通过工具加密，因此可以有效保护设备制造商的固件知识产权，甚至是设备中的最终用户私有数据（例如，定制的初始登录密码）。

有关从 OSPI 闪存启动的更多信息，请参考 GD32H73x_75x 微控制器用户指南中的 ***AN122 GD32H7 系列 MCU OSPI flash 执行环境用户指南***。

6. 安全模式

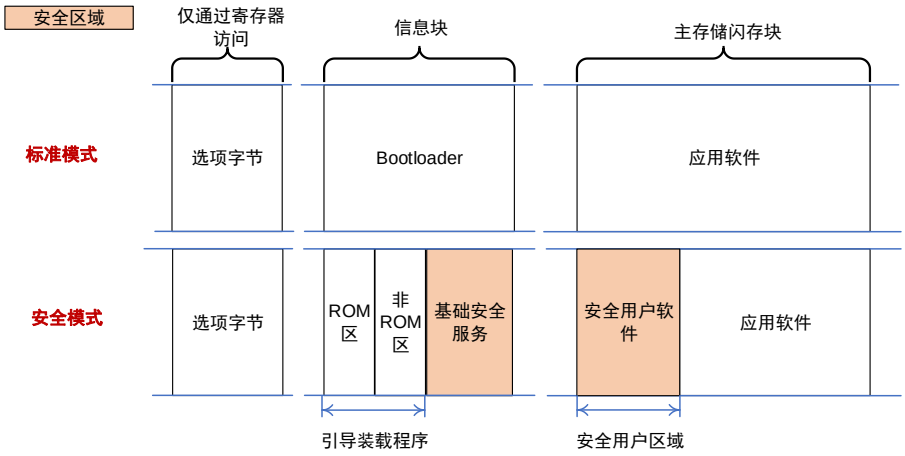
安全模式是实现安全启动、安全存储和安全访问的专用模式。

6.1. 内部 Flash 存储器中的独立安全区域

用户可以将安全区域独立开，与普通区域隔离，安全区域只能在安全模式下访问。

*图 6-1. 闪存保护区域*显示了受保护区域之间的关系。

图 6-1. 闪存保护区域



有关安全存储的更多信息，请参考 ***AN113 GD32H73x_75x 系列安全存储管理***。

6.2. 安全模式规则

安全模式遵循以下规则：

- 无论启动配置（BOOT引脚和启动地址）如何，MCU都将被强制从安全ROM区域启动。

- 从安全区域跳转到应用软件后，无法跳回安全区域。
- 基础安全服务（BSS）只能在安全模式下调用。
- 要返回标准模式，需要移除安全区域和DCRP区域。
- 在安全用户软件执行后，如果代码跳转到用户的主应用程序（非安全），则无法访问安全用户区域的内容。在退出安全区域之前，用户必须调用exitSecureAreas安全函数以实现跳转。

有关安全存储的更多信息，请参考 ***AN113 GD32H73x_75x 安全存储管理***。

7. 安全生态系统

7.1. 硬件安全模块（HSM）

HSM 是一种安全设备，用于与微控制器协商 KEK 并生成许可证。HSM 负责：

1. 安全存储 OEM 密钥。
2. 验证用于认证 GD 微控制器的证书。
3. 协商密钥封装密钥并提供许可。
4. 计算生产的 GD 设备数量。

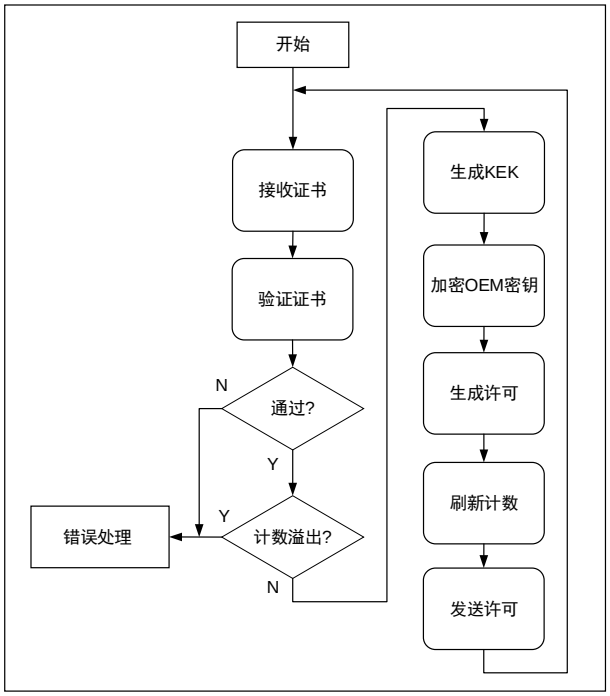
有关 HSM 的更多信息，请参考 AN116 GD32 MCU 硬件安全模块概述。

HSM 与 PC 之间的交互遵循 USB-HID 协议。

Gigadevice 不负责开发 HSM。然而为了演示，开发了一个 HSM 示例。

下面描述了一个示例性的硬件安全模块（HSM）工作流程图。

图 7-1. HSM 工作流示例



7.2. GD32AllInOneProgrammer

GD32 All-In-One Programmer 支持基于 EFUSE 密钥的加密编程功能。

有关此工具的更多信息，请参考 ***GigaDevice All-In-One Programmer User Manual***。

7.3. GDLicensedDataCreator/Programmer

GDLicensedDataCreator 支持固件加密功能， 有关此工具的更多信息，请参考 ***GD Licensed Data Creator User Manual***。

GDLicensedDataProgrammer 支持加密固件安装功能，有关此工具的更多信息，请参考 ***GD Licensed Data Programmer User Manual***。

8. 修订历史

表 8-1. 修订历史

版本号.	说明	日期
1.0	初始版本	2025年04月10日
1.1/1.2	芯片系列修改为 GD32H73x75x	2026年02月10日

Important Notice

This document is the property of GigaDevice Semiconductor Inc. and its subsidiaries (the "Company"). This document, including any product of the Company described in this document (the “Product”), is owned by the Company according to the laws of the People’s Republic of China and other applicable laws. The Company reserves all rights under such laws and no Intellectual Property Rights are transferred (either wholly or partially) or licensed by the Company (either expressly or impliedly) herein. The names and brands of third party referred thereto (if any) are the property of their respective owner and referred to for identification purposes only.

To the maximum extent permitted by applicable law, the Company makes no representations or warranties of any kind, express or implied, with regard to the merchantability and the fitness for a particular purpose of the Product, nor does the Company assume any liability arising out of the application or use of any Product. Any information provided in this document is provided only for reference purposes. It is the sole responsibility of the user of this document to determine whether the Product is suitable and fit for its applications and products planned, and properly design, program, and test the functionality and safety of its applications and products planned using the Product. The Product is designed, developed, and/or manufactured for ordinary business, industrial, personal, and/or household applications only, and the Product is not designed or intended for use in (i) safety critical applications such as weapons systems, nuclear facilities, atomic energy controller, combustion controller, aeronautic or aerospace applications, traffic signal instruments, pollution control or hazardous substance management; (ii) life-support systems, other medical equipment or systems (including life support equipment and surgical implants); (iii) automotive applications or environments, including but not limited to applications for active and passive safety of automobiles (regardless of front market or aftermarket), for example, EPS, braking, ADAS (camera/fusion), EMS, TCU, BMS, BSG, TPMS, Airbag, Suspension, DMS, ICMS, Domain, ESC, DCDC, e-clutch, advanced-lighting, etc.. Automobile herein means a vehicle propelled by a self-contained motor, engine or the like, such as, without limitation, cars, trucks, motorcycles, electric cars, and other transportation devices; and/or (iv) other uses where the failure of the device or the Product can reasonably be expected to result in personal injury, death, or severe property or environmental damage (collectively "Unintended Uses"). Customers shall take any and all actions to ensure the Product meets the applicable laws and regulations. The Company is not liable for, in whole or in part, and customers shall hereby release the Company as well as its suppliers and/or distributors from, any claim, damage, or other liability arising from or related to all Unintended Uses of the Product. Customers shall indemnify and hold the Company, and its officers, employees, subsidiaries, affiliates as well as its suppliers and/or distributors harmless from and against all claims, costs, damages, and other liabilities, including claims for personal injury or death, arising from or related to any Unintended Uses of the Product.

Information in this document is provided solely in connection with the Product. The Company reserves the right to make changes, corrections, modifications or improvements to this document and the Product described herein at any time without notice. The Company shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. Information in this document supersedes and replaces information previously supplied in any prior versions of this document.