

1 LPC55(S)1x 简介

LPC55(S)1x 是一款基于 Arm Cortex®-M33 内核的 MCU。该 MCU 集成有 Casper 安全加速器，最大 96kBytes 片上 RAM，最大 256kBytes 片上 Flash，PRINCE 模块支持加密固件边解密边执行，片上带有一路 CAN-FD 控制器，5 个通用定时器 CTIMER，1 个状态可配置定时器，1 个看门狗定时器，8 个 Flexcomm 串行接口（可以任意配置为 UART，SPI，I2C 或者 I2S），1 路 50MHz 高速 SPI，1 路 16 位 2.0MSPS 采样率的 ADC，片上集成温度传感器。

LPC55(S)1x 片上 ROM 启动非安全的部分支持：

- 支持片上 Flash 中固件的启动。
- 支持 CRC32 校验使能的固件检查以及启动。
- 支持片上 Flash 在系统中编程(ISP, In System Programming)的命令并支持以下接口：USB1 接口支持 HID 类设备，串口(Flexcomm0)支持自动波特率，SPI 从机接口（Flexcomm3 或者 9）使用 MODE3（CPOL=1,CPHA=1），支持 I2C 从机接口（Flexcomm1）。
- 支持 ROM API：Flash 编程 API，功耗模式配置，安全固件升级 API 支持 NXP Secure Boot 文件格式，版本 2.0。
- 支持从带有 PRINCE 加密的 Flash 区域的固件启动。
- 支持 1.0 版本的 NXP 调试身份认证协议（RSA-2048）以及 1.1 的版本（RSA-4096）。
- 支持在安全调试过程中的故障分析。

本应用笔记，针对非安全的状态下的 LPC55(S)1x 的固件升级，接口使用高速 USB 接口 USB Port1。可以配合 NXP 开源上位机 blhost 实现固件的升级。

2 非安全状态下 ROM 启动流程

2.1 非安全状态下 ROM 启动流程

本文主要针对的是非安全状态下 ROM 的启动流程，一是不是所有的客户都需要安全启动，二是本文重心在 USB 固件升级而不是安全，我们也有相应的应用笔记 AN 介绍安全启动以及固件的安全升级。

图 1 为 ROM 启动流程图，因为本文内容并没有使能 TrustZone(TZM)以及没有使能安全启动，所以在正常情况下整个启动流程会按照橙色线路进行。

绿色标出的程序执行路径为，片上 Flash 的固件启用了 CRC 校验的功能且固件有损坏的情况。

目录

1	LPC55(S)1x 简介.....	1
2	非安全状态下 ROM 启动流程.....	1
2.1	非安全状态下 ROM 启动流程.....	1
2.2	进入 ROM USB HID 固件升级的三种方式	2
3	软硬件工具：LPC55S16-EVK，BLHOST 和 ELFTOSB-GUI.....	2
3.1	LPC55S16-EVK 评估板.....	2
3.2	BLHOST 固件升级软件.....	3
3.3	ELFTOSB 安全固件生成软件.....	3
4	如何通过 USB1 接口更新固件.....	4
4.1	blhost 更新固件的命令.....	4
4.2	LPC55S16-EVK 如何进入 ISP 模式配合 blhost 进行固件升级	5
4.3	升级例程后的现象.....	5
5	如何通过 ELFToSB 工具生成使能 CRC 校验的固件	5
5.1	LPC55(S)1x ROM 如何支持固件的 CRC 校验	5
5.2	如何用 ELFToSB-GUI 工具生成带有 CRC 校验功能的固件	6
5.3	如何验证带有 CRC 的固件损毁不执行且重新使能 USB ISP 升级的功能	7
6	KEIL，IAR 和 MCUXpresso 生成 bin 文件	8
6.1	KEIL MDK 环境下生成 bin 文件... ..	8
6.2	IAR 环境下生成 bin 文件.....	8
6.3	MCUXpresso 环境下生成 bin 文件	9
7	结论.....	10
8	参考文档.....	10



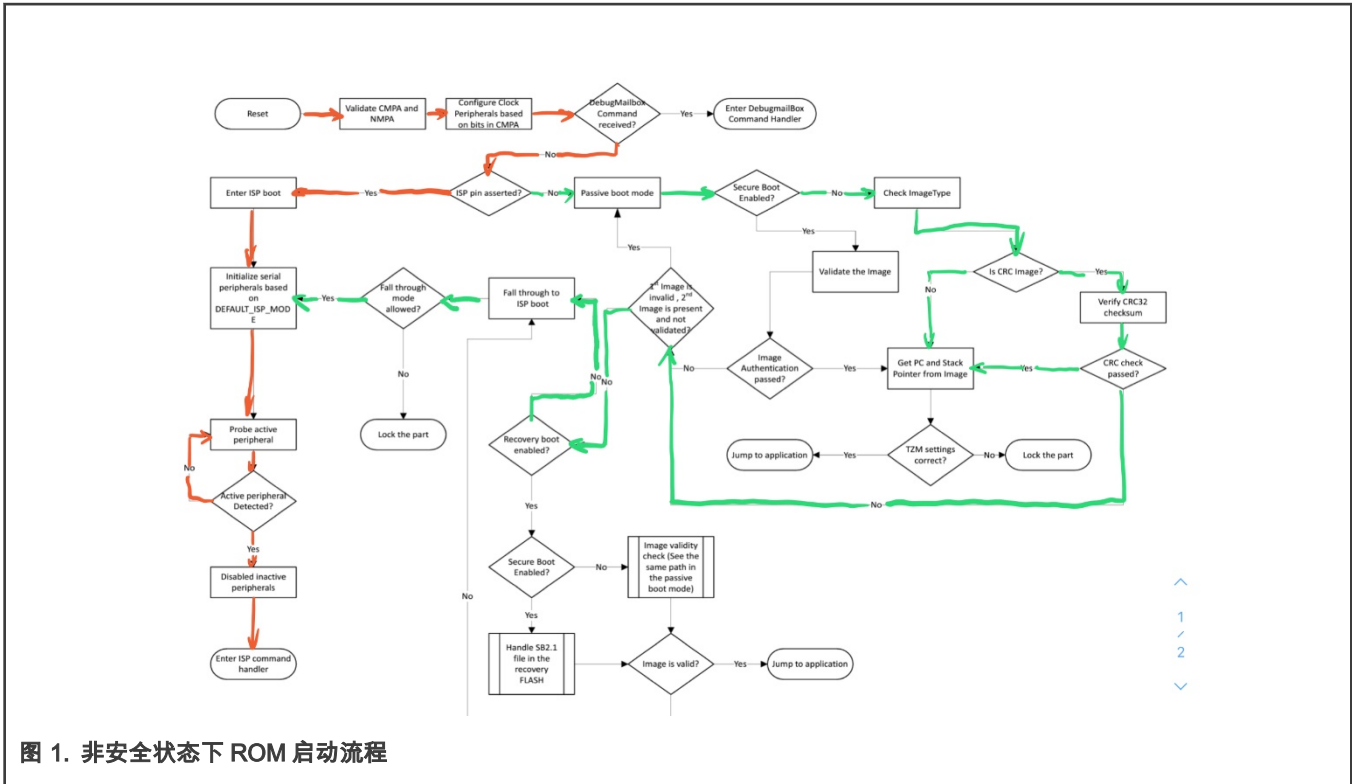


图 1. 非安全状态下 ROM 启动流程

2.2 进入 ROM USB HID 固件升级的三种方式

LPC55(S)1x 片上的 ROM 启动支持从 USB1 口以 HID 设备类的方式更新固件。通常有两种办法启动 ROM 固件升级的功能，一种是通过将 ISP 引脚（对 LPC55(S)1x 来说就是 PIO0_5）；另外一种就是在用户应用程序中调用 runBootloader() 这个 ROM 的 API 即可在应用程序中进入 ROM 的 ISP 固件升级模式。除了这两种方式外，还有一种通过启动流程中固件 CRC 校验和的检查成功与否来进入 USB HID ISP 升级的方式。

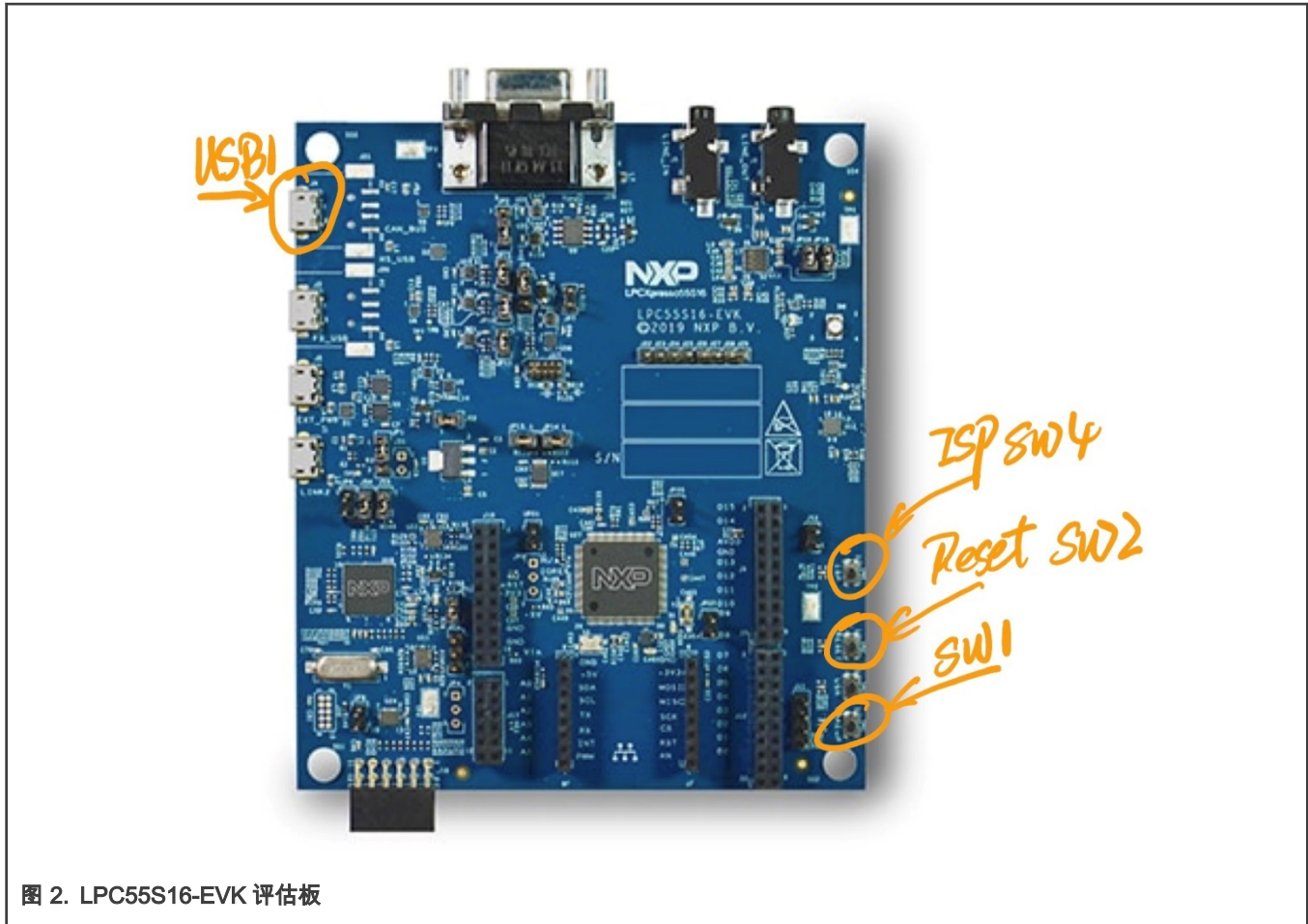
由启动流程用户可以了解到，非安全状态下 ROM 启动过程中可以选择固件是否有 CRC 校验和的检查。

- 如果固件没有使能 CRC 校验，则按照正常的启动流程启动。
- 如果固件使能了 CRC 校验，则 ROM 会在复位后检查 Flash 上固件的 CRC 值是否正确，如果不正确（意味着片上固件损坏了）则进入 ISP 固件升级的模式。

3 软硬件工具：LPC55S16-EVK，BLHOST 和 ELFTOSB-GUI

3.1 LPC55S16-EVK 评估板

图 2 是官方针对 LPC55(S)1x 系列的评估板 LPC55S16-EVK。该评估板可以通过‘SW4-ISP’按键配合‘SW2-RESET’按键进入 ISP 模式，USB HID ISP 则需要将 USB 接口 J4 (USB 1) 与 PC 机相连接。



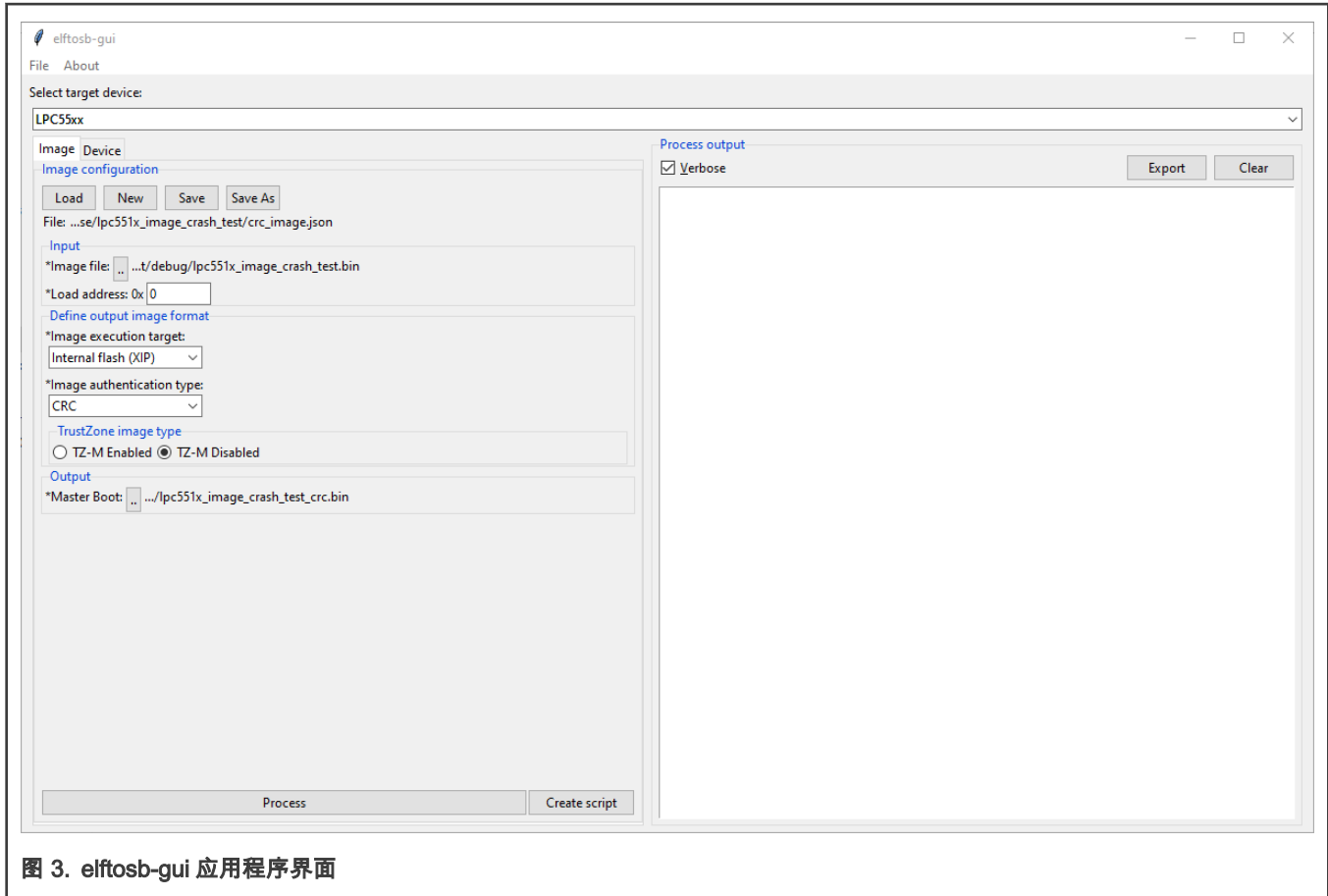
3.2 BLHOST 固件升级软件

BLHOST 软件是 NXP 官方开源的固件升级的上位机程序，用于支持片上 ROM 的 ISP 固件升级功能。BLHOST 是以命令行的方式来实现用户应用程序的更新，支持三个平台 Windows/Linux/MACOS。

其使用手册见 *blhost User's Guide* (document [MCUBLHOSTUG](#)).

3.3 ELFTOSB 安全固件生成软件

图 3 是 elftosb-gui 应用程序的界面，ELFTOSB 是 NXP 官方生成安全固件的工具，可以帮助客户在普通的应用程序的 binary 基础上，可选择的加入 CRC 校验和或者带有签名的固件。如果用户想自己了解 NXP 的 BOOT ROM 校验 CRC 的细节，本文在[如何通过 ELFTOSB 工具生成使能 CRC 校验的固件](#)会做详细介绍。



关于 blhost 以及 elftosb 的工具，用户可以从 [MCUBOOT: MCU Bootloader for NXP microcontrollers](#) 下载到最新的软件。

4 如何通过 USB1 接口更新固件


4.1 blhost 更新固件的命令

由于 elftosb 工具需要 bin 格式的固件才能加入 CRC 校验和。所以本文所有的固件升级都是基于 bin 格式的。固件更新并不会查看固件是否有 CRC 校验。

各种 IDE 下生成 bin 文件的方法见 [KEIL](#)，[IAR](#) 和 [MCUXpresso 生成 bin 文件](#)。

blhost 升级固件需要用到如下命令，如 [图 4](#) 所示。

```
blhost.exe -u 0x1FC9,0x0022 -- flash-erase-all
blhost.exe -u 0x1FC9,0x0022 -- write-memory 0x0 binary.bin
```



```

C:\MagicoeSync\Product_NXP\LPC55S1x\6. TestCase\lpc551x_image_crash_test>blhost.exe -u 0x1FC9,0x0022 -- flash-erase-all
Inject command 'flash-erase-all'
Successful generic response to command 'flash-erase-all'
Response status = 0 (0x0) Success.

C:\MagicoeSync\Product_NXP\LPC55S1x\6. TestCase\lpc551x_image_crash_test>blhost.exe -u 0x1FC9,0x0022 -- write-memory 0x0
binary.bin
Inject command 'write-memory'
Preparing to send 196612 (0x30004) bytes to the target.
Successful generic response to command 'write-memory'
(1/1)100% Completed!
Successful generic response to command 'write-memory'
Response status = 0 (0x0) Success.
Wrote 196612 of 196612 bytes.

C:\MagicoeSync\Product_NXP\LPC55S1x\6. TestCase\lpc551x_image_crash_test>

```

图 4. blhost 固件更新命令

4.2 LPC55S16-EVK 如何进入 ISP 模式配合 blhost 进行固件升级

LPC55S16-EVK 在配合 blhost 命令更新固件前，要进入 ISP 模式。具体有两种方法如下：

1. 开发板在有外部供电的情况下，按住 LPC55S16-EVK 板上的 ISP 按键（SW4），然后按下 RESET 按键（SW2）后释放 SW2 按键。通过 Micro USB 数据线连接 EVK 的 J4 接口（USB1/HS_USB）与 PC。
2. 如果开发板没有上电，则按住 ISP 按键（SW4），并对开发板上电，然后通过 Micro USB 数据线连接 EVK 的 J4 接口。

确保执行以上步骤后，在 PC 端打开命令界面（Command Prompt）通过 CD 命令进入工程文件夹，然后输入 [blhost 更新固件的命令](#)介绍的 blhost 命令即可。

4.3 升级例程后的现象

如果开发板升级程序成功后，可以按下复位按键（SW2），此时开发板上的绿色 LED 就会闪烁。

也可以通过以下命令直接复位芯片。

```
blhost.exe -u 0x1FC9,0x0022-- reset
```

5 如何通过 ELFtoSB 工具生成使能 CRC 校验的固件

5.1 LPC55(S)1x ROM 如何支持固件的 CRC 校验

ROM 工作原理的详细细节，用户可以参考 *LPC55S1x/LPC551x User Manual*（手册 [UM11295](#)）中的 **Boot ROM** 章节。这里只做简单的介绍。

如果固件是带有 CRC 校验功能的，则需要填充合理的数值到 imageLength 字段，见 [表 1](#)。CRC 值是基于片上 Flash 固件整体而言的，即 CRC 的计算是从 Flash 固件的起始 0x0 开始到有 imageLength 指定长度的位置结束。该长度不包括组成 CRC 值字段的 offsetToSpecificHeader 字段，即固件 CRC 值的计算不包括 CRC 值本身。芯片启动后 ROM 程序会重新针对 Flash 上的固件做 CRC 计算然后和固件带有的 CRC 的值做比较，如果不匹配则固件不会被执行。如果用户不使能 CRC 校验的功能，则固件无需加入 CRC 相关的数据如 imageLength 和 offsetToSpecificHeader 字段。

表 1. LPC55S1x/LPC551x 固件头信息说明

Offset	Size in bytes	Symbol	Description
0x00	4	Initial SP	Stack pointer

Table continues on the next page...

表 1. LPC55S1x/LPC551x 固件头信息说明 (continued)

Offset	Size in bytes	Symbol	Description
0x04	4	Initial PC	The application first execution instruction.
0x08	24	Vector table	Cortex-M33 Vector table entries.
0x20	4	imageLength	The length of the current image. Set to 0 if the image type is 0 as well. Set to actual image length if the image type is other value.
0x24	4	imageType	Image type <ul style="list-style-type: none"> 0x0000: Normal image for unsecure boot 0x0001: Plain signed Image 0x0002: Plain CRC Image 0x0004: Plain signed XIP Image 0x0005: Plain CRC XIP Image 0x8001: Signed plain Image with KeyStore Included.
0x28	4	offsetToSpecificHeader	Offset to specific header It means offset to certificate block header if the image type is 0x01, 0x04, or 0x8001. It means the <code>crcChecksum</code> if the image type is 0x02 or 0x05.
0x2c	8	Vector table	Cortex-M33 Vector table entries.
0x34	4	imageExecutionAddress	The execution address of the image. Set to 0 if image type is 0. Set to actual image execution address if the image type is other value.
0x38	8	Vector table	Cortex-M33 Vector table entries.

5.2 如何用 ELFtoSB-GUI 工具生成带有 CRC 校验功能的固件

ELFtoSB-GUI 工具在本应用笔记附带的软件包中，路径是 `mcu-boot/bin/Tools`。打开 `elftosb-gui(win)` 可执行文件后，在 `Select target device` 中选择 `LPC55xx`。

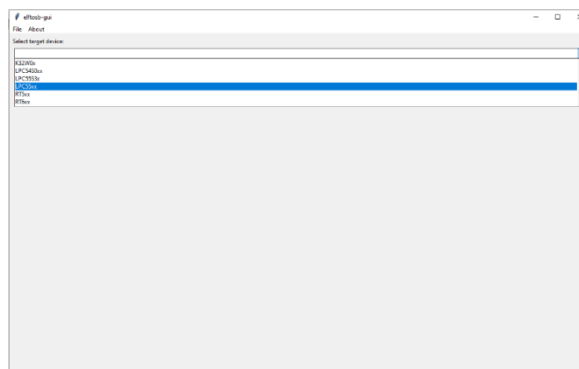


图 5. ELFtoSB-GUI 选择 LPC55xx

如 图 6 所示，

- 在 Image Configuration 中点击 New 按键。
- 在 Input 中：
 - Image file：选择原生的 bin 文件
 - Load address 0x 地址：用默认的 0
- 在 Define output image format 中：
 - Image execution target：选择 Internal flash (XIP)
 - Image authentication type：选择 CRC
- TrustZone image type 中，选择不启用 TZ-M Disabled。
- 在 Output 中：
 - Master Boot：修改输出 bin 文件的路径及名字

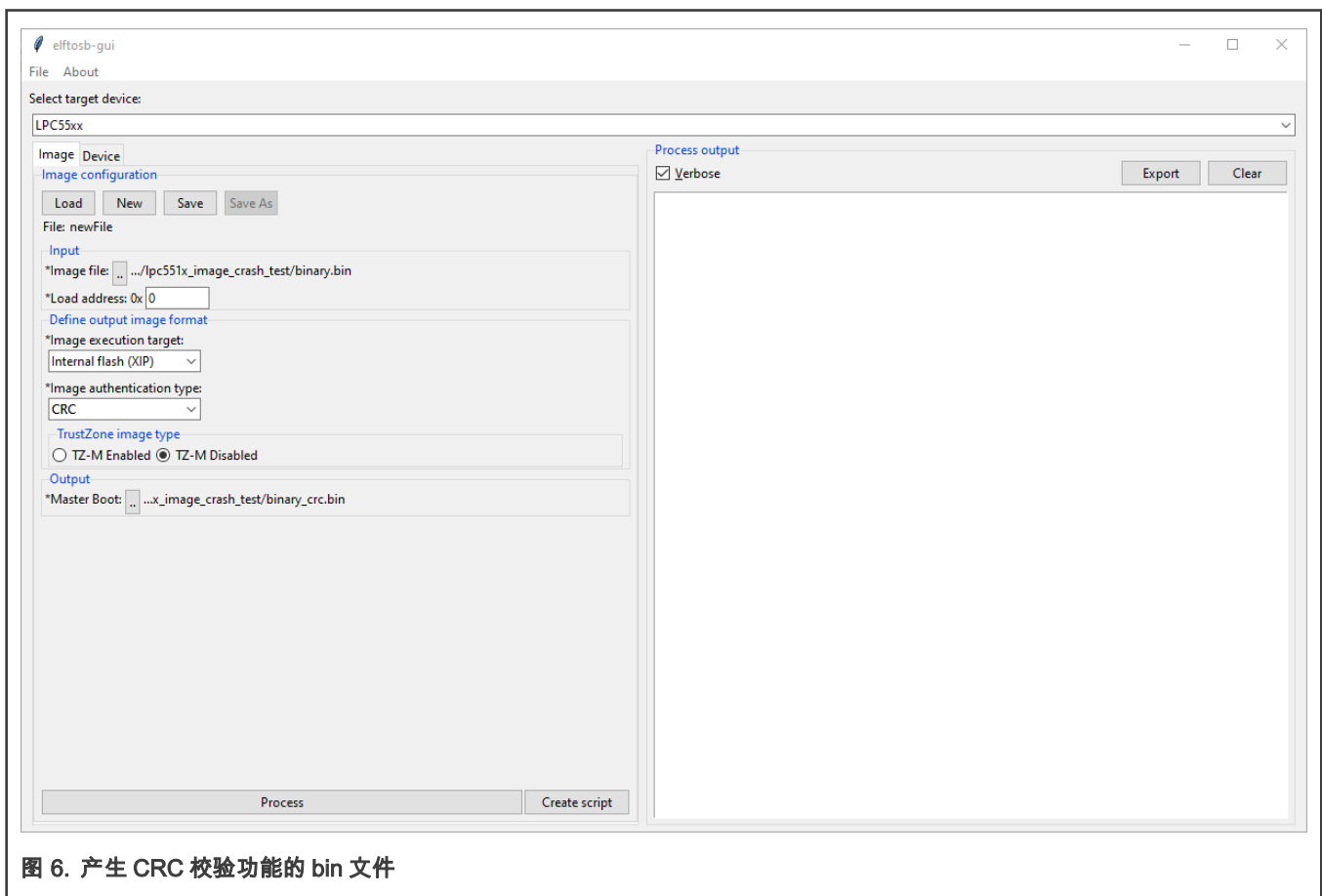


图 6. 产生 CRC 校验功能的 bin 文件

设置完成后点击 Process 按钮，即可生成带有 CRC 签名的固件。

5.3 如何验证带有 CRC 的固件损毁不执行且重新使能 USB ISP 升级的功能

将带有 CRC 的固件按照[如何通过 USB1 接口更新固件](#)的方式更新到 LPC55S16-EVK 后，正常情况下绿色的 LED 会闪烁，此时按下按键 SW1 后，片上固件会擦除 0x30000 开始的 512 字节的内容造成片上 Flash 中的固件丢失的假象。在此之后看用户需求是通过外部 Reset 按键复位，还是通过重新对开发板上电复位或者改变固件内容后通过 NVIC_SystemReset()复位 均可再次进 ROM ISP 的功能，如果开发板 USB1 的接口连接了 PC，则进入 USB HID ISP 升级的状态。

6 KEIL, IAR 和 MCUXpresso 生成 bin 文件

6.1 KEIL MDK 环境下生成 bin 文件

可以在 KEIL 工程的配置选项中选择“User”选项卡，在“After Build/Rebuild”的“Run #1”中填入“xxx\ARM\ARMCLANG\bin\fromelf.exe --bin -o ./binary.bin./output/@L.axf”。其中 xxx 是 KEIL 的安装路径。这样在每次编译后 IDE 就会自动产生 bin 文件

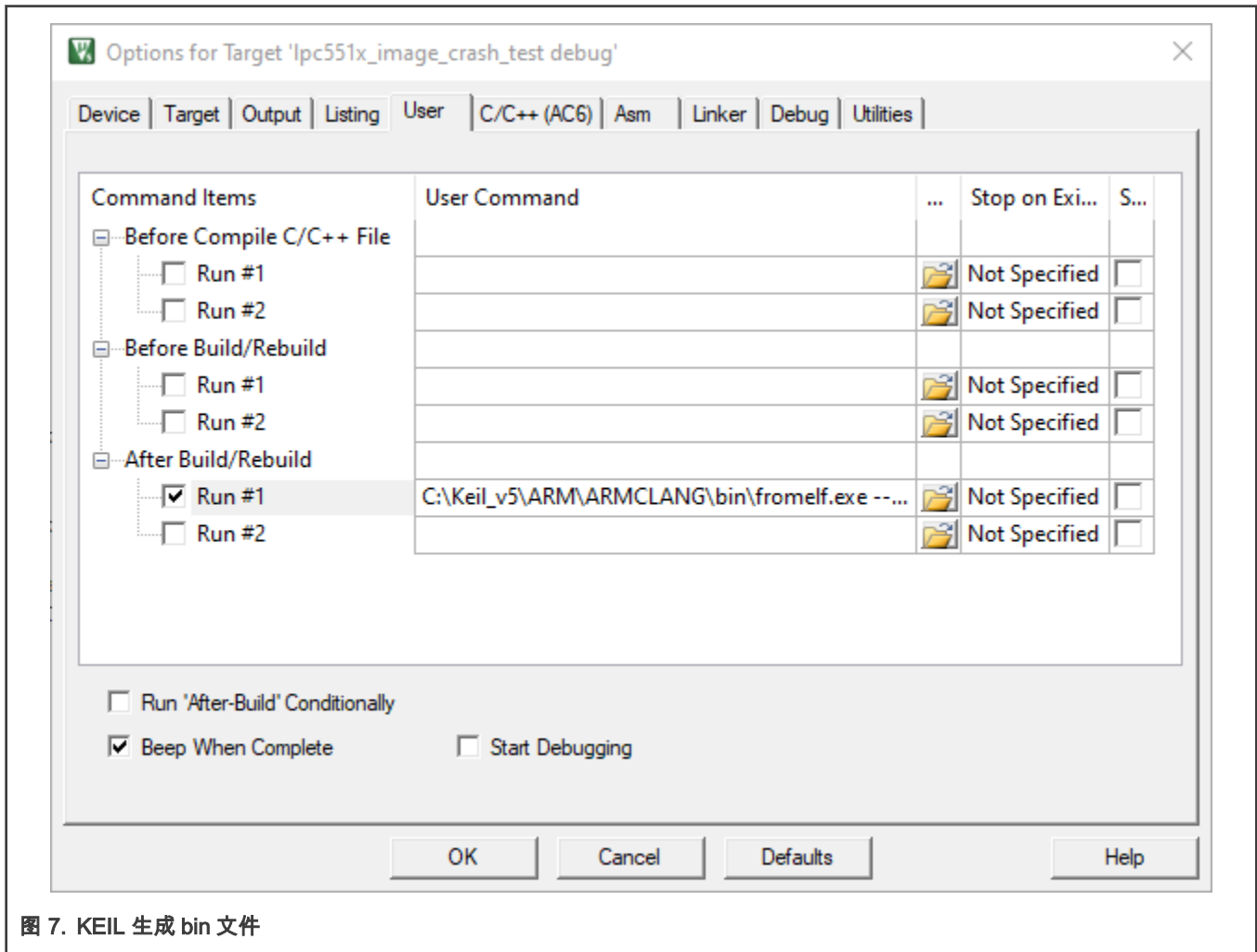


图 7. KEIL 生成 bin 文件

6.2 IAR 环境下生成 bin 文件

用户可以在工程配置选项中选择“Output Converter”，在选项卡中选中“Generate additional output”输出格式“Output format”中选择 Raw binary 即可。

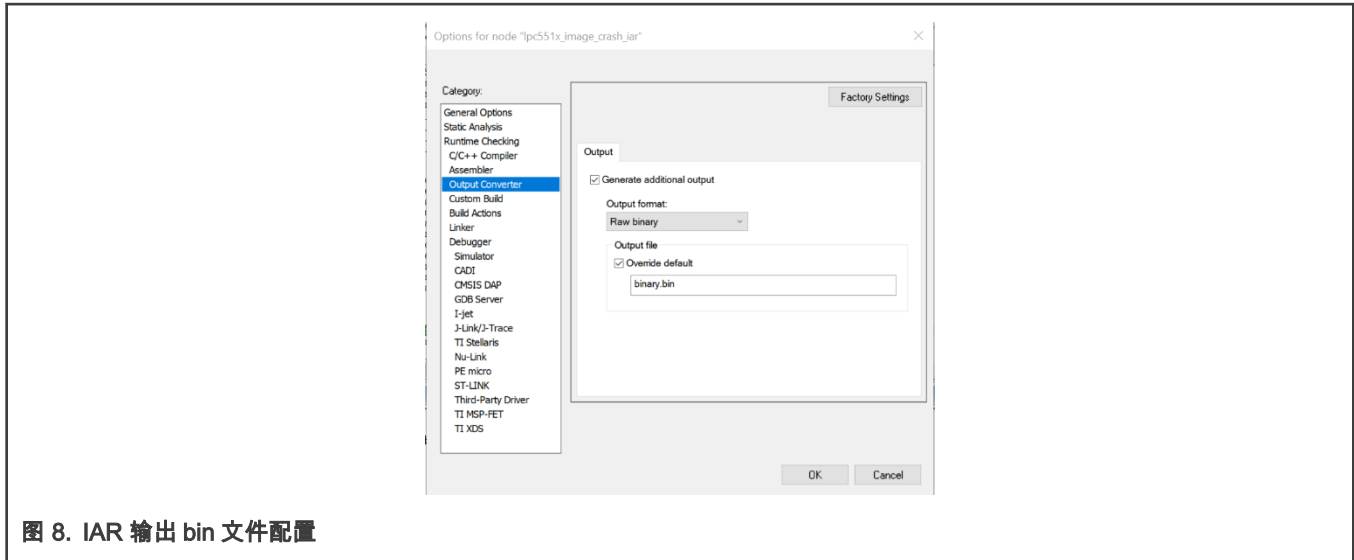


图 8. IAR 输出 bin 文件配置

6.3 MCUXpresso 环境下生成 bin 文件

在 MCUXpresso 编译后的 output 文件夹中，找到对应的 axf 文件然后鼠标右键。选择“Binary Utilities”->“Create binary”即可。

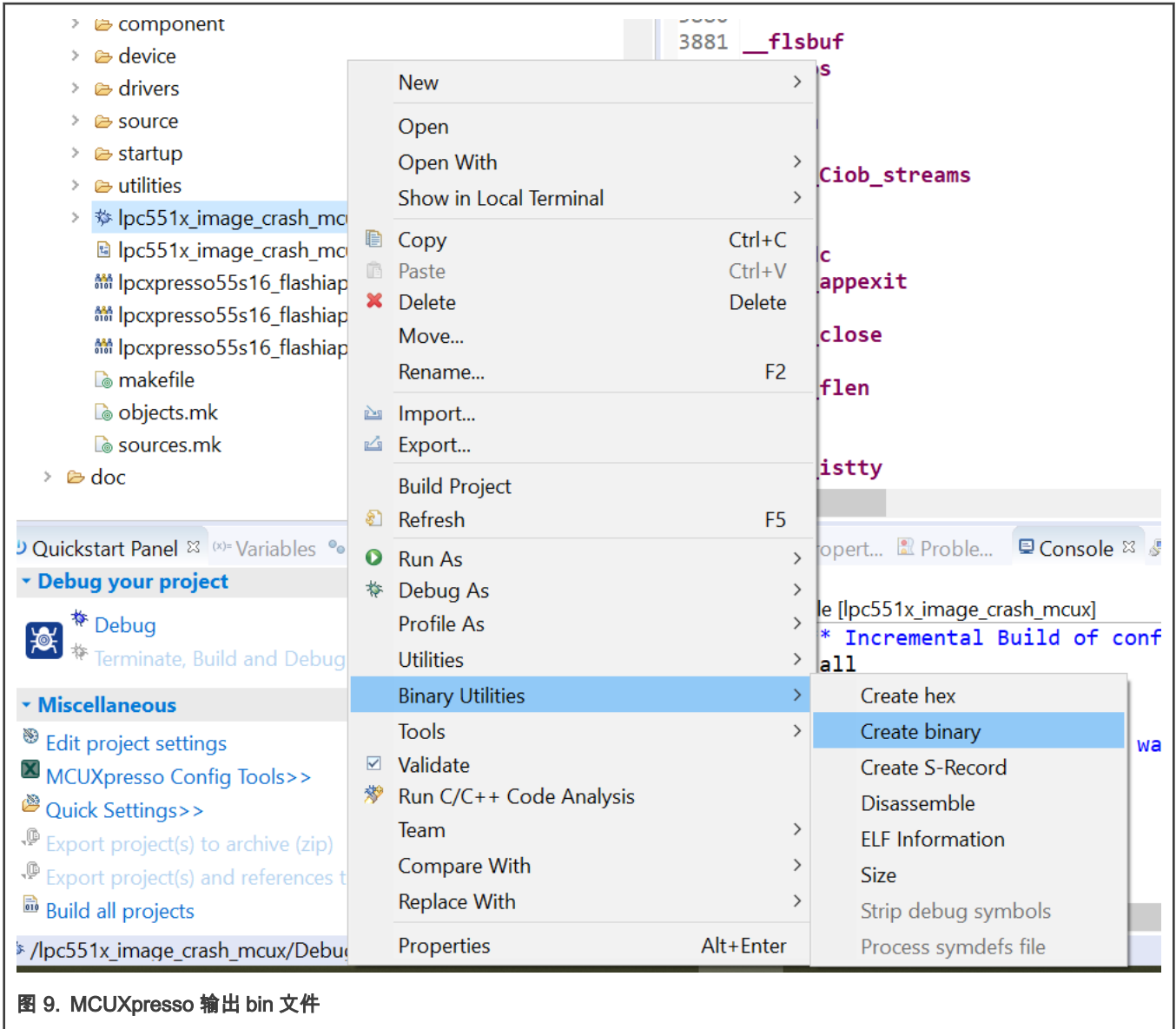


图 9. MCUXpresso 输出 bin 文件

7 结论

对于非安全类的 LPC551x 片上的 BOOT ROM 程序可以满足用户基本的固件升级功能，支持针对固件的 CRC 校验，以及通过 CRC 校验检查片上固件的完整性。如果片上带有 CRC 功能的固件发生了变化，则重新启动芯片后 MCU 会自动进入 ROM boot 升级程序的功能。

8 参考文档

- *LPC55S1x/LPC551x User Manual* (文档 [UM11295](#))

How To Reach Us

Home Page:

nxp.com

Web Support:

nxp.com/support

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including "typicals," must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

Right to make changes - NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, COOLFLUX, EMBRACE, GREENCHIP, HITAG, ICODE, JCOP, LIFE, VIBES, MIFARE, MIFARE CLASSIC, MIFARE DESFire, MIFARE PLUS, MIFARE FLEX, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TRENCHMOS, UCODE, Freescale, the Freescale logo, Altivec, CodeWarrior, ColdFire, ColdFire+, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, QorIQ Qonverge, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, Tower, TurboLink, EdgeScale, EdgeLock, eIQ, and Immersive3D are trademarks of NXP B.V. All other product or service names are the property of their respective owners. AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, μ Vision, Versatile are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

© NXP B.V. 2021.

All rights reserved.

For more information, please visit: <http://www.nxp.com>

For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: March 15, 2021

Document identifier: AN13183

