AN13204

i.MX RT1170 ECC 应用

第 1 版—2022 年 1 月 14 日 应用笔记

目录

1 介绍

i.MX RT1170 涵盖了汽车领域，因此，与以前的 i.MX RT 产品（如 i.MX RT1060）相比，ECC 功能得到了很大的增强。对于具有高安全级别要求较高的使用案例，我们需要在 ECC 错误发生时检测到它，并通知应用系统来决定如何处理这个错误。

本文将讨论 ECC 在存储器上的应用，包括 TCM、Cache、OCRAM 和外部存储器，并分享一些关键点和经验。本文不包括 ECC 在外设上的应用，诸如 FlexSPI、Fuse、OCOTP、CSI、MIPI CSI、MIPI DSI、ENET QOS 和 FLEX CAN。

对于 i.MX RT1170 上的存储器的 ECC 应用，我们需要考虑：

- 在哪些存储器上应用 ECC？

  i.MX RT 1170 包含以下存储器类型：

  — TCM
  — Cache
  — OCRAM
  — 外部存储器

- 如何注入/捕获 ECC 错误？

  与 ECC 有关的熔丝设置和软件配置。

- 与 ECC 有关的 ROM 功能。

2 i.MX RT1170 ECC 功能列表

表 1 列出了 i.MXRT1170 的 ECC 功能。

表 1. i.MX RT1170 ECC 功能列表

项目	ECC 功能
[CM7] CM7 FlexRAM 中的 TCM	ITCM：64 位数据 + 8 位 ECC DTCM：32 位数据 + 7 位 ECC
[CM7] Cache	I-Cache：64 位数据 + 8 位 ECC D-Cache：32 位数据 + 7 位 ECC
[CM4] TCM/LMEM	Hsiao 奇数权重列标准 ECC 码 32 位数据 + 7 位 ECC

表格在下一页继续...

表 1. i.MX RT1170 ECC 功能列表（续）

项目	ECC 功能
[CM4] Cache	奇偶检查
[CM7/CM4] OCRAM1/OCRAM2	Hsiao Hamming 算法 64 位数据 + 8 位 ECC
[CM7/CM4] 来自 CM7 FlexRAM 的 OCRAM	Hsiao Hamming 算法 64 位数据 + 8 位 ECC
[CM7/CM4] 来自 CM4 TCM/LMEM 的 OCRAM	Hsiao 奇数全重列标准 ECC 码 32 位数据 + 7 位 ECC
[CM7/CM4] XECC	Hsiao Hamming 算法 4 位数据 + 4 位 ECC 扩展为：32 位数据 + 32 位 ECC

3 与 ECC 功能相关的熔丝设置和软件配置

要启用 ECC 功能，请启用相关的熔丝设置和软件配置

表 2 列出了与 ECC 有关的熔丝设置。

表 2. 与 ECC 有关的熔丝设置

熔丝映射	功能
0x840[2]	MECC，针对 OCRAM1/OCRAM2
0x840[3]	XECC，用于外部存储器，如 SDRAM、SRAM、FlexSPI 设备。
0x840[15]	CM7 Flex RAM ECC（包括 CM7 Flex RAM TCM 和 CM7 Flex RAM OCRAM）
0x950[0]	ROM 预加载

表 3 列出了软件的配置。

表 3. 与 ECC 有关的软件配置

项目	软件配置要求	是否由 ROM 执行？
[CM7] 来自 CM7 FlexRAM 的 TCM	SCB->ITCMCR | = SCB_ITCMCR_RMW_Msk; SCB->DTCMCR | = SCB_DTCMCR_RMW_Msk; FLEXRAM_CTRL |= TCM_ECC_EN_Msk	如果 0x840[15]熔断，是。
[CM7] Cache	CACR &= ~ECCEN_Msk	否，默认启用。
[CM4] TCM/LMEM	LMDR0 |= 0xB; LMDR1 |= 0xB; （仅通过 CM4）	如果 0x840[2]熔断，是。

表格在下一页继续...

表 3. 与 ECC 有关的软件配置（续）

项目	软件配置要求	是否由 ROM 执行？
[CM4] Cache	LMDR2 |= 0xF0; LMDR3 |= 0xF0; （仅通过 CM4）	否
[CM7/CM4] OCRAM1/OCRAM2	MECC1_PIPE_ECC_EN |= ECC_EN_Msk MECC2_PIPE_ECC_EN |= ECC_EN_Msk	如果 0x840[2]熔断，是。
[CM7/CM4] 来自 CM7 FlexRAM 的 OCRAM	FLEXRAM_CTRL |= OCRAM_ECC_EN_Msk	否
[CM7/CM4] 来自 CM4 TCM/LMEM 的 OCRAM	LMDR0 |= 0xB; LMDR1 |= 0xB; （仅通过 CM4）	如果 0x840[2]熔断，是
[CM7/CM4] XECC	XECC_ECC_CTRL |= 7;	否

4 通过 MCU 启动工具实现熔丝设置

MCU 启动工具可用于熔丝设置。

1. 配置启动模式，配置电源跳线（不是必须的），并连接 USB1 端口，如图 1 所示。

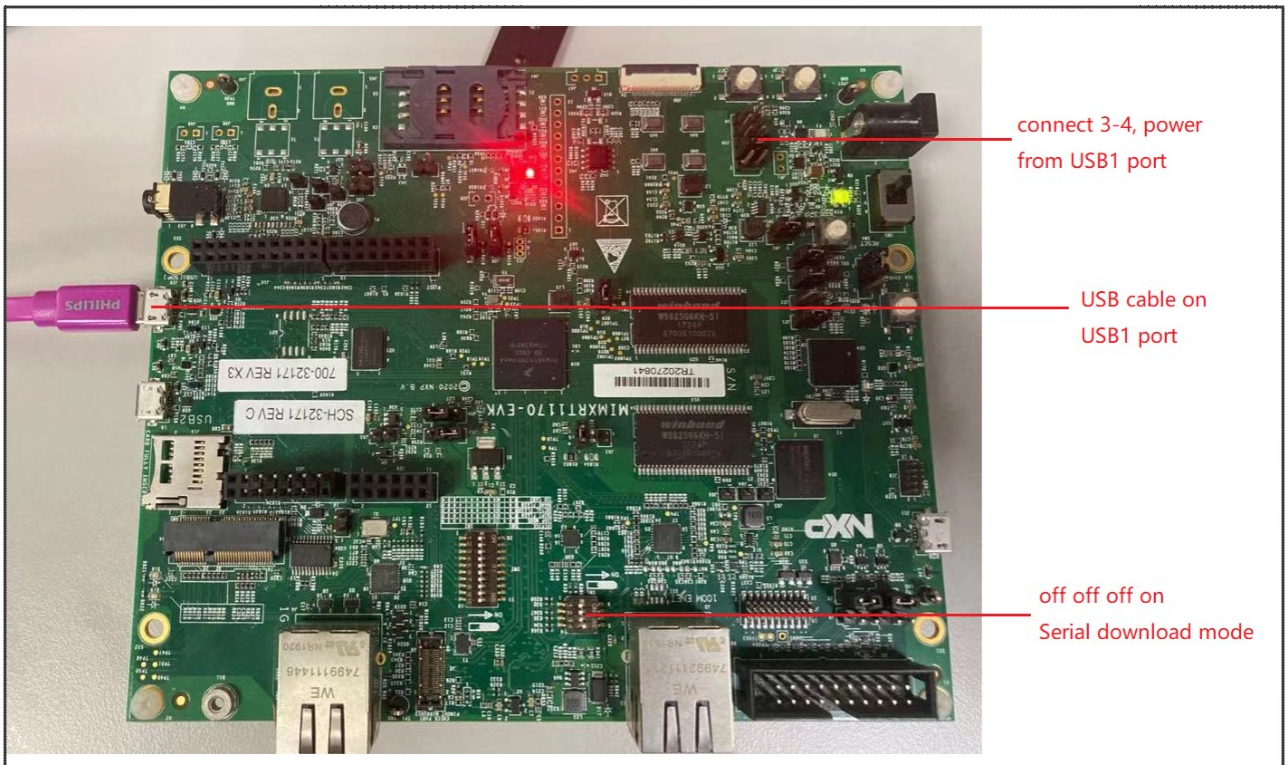

图 1. 硬件设置

2. 运行 MCU 启动工具，须正确识别 PID 和 VID。

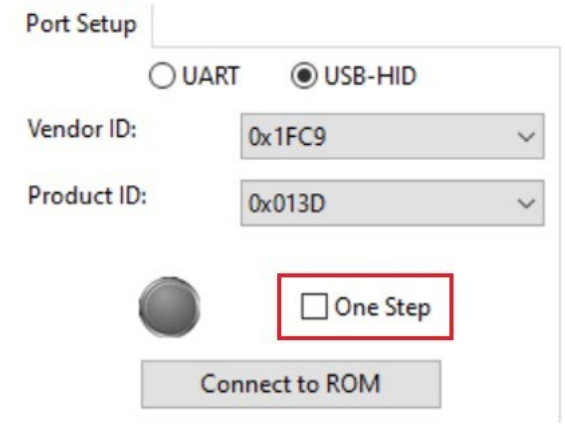

图 2. 识别到 PID 和 VID

3. 不要选图 2 中的 One Step 选项。
4. 在图 2 中，点击“连接到 ROM”，就会出现图 3。

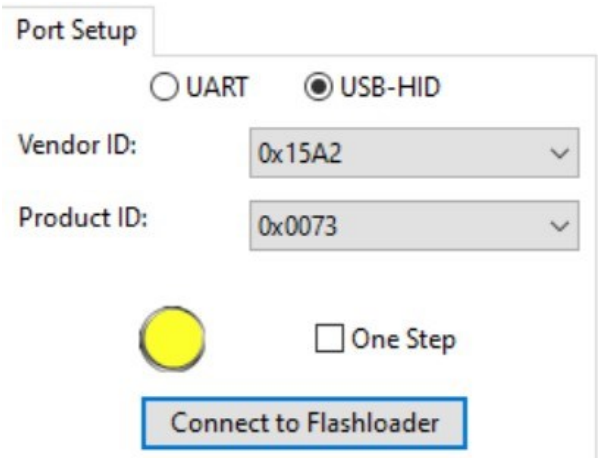

图 3. 连接到 Flashloader

5. 在图 3 中，点击“连接到 Flashloader”，然后进入“eFuse 操作工具面板”，如图 4 所示。

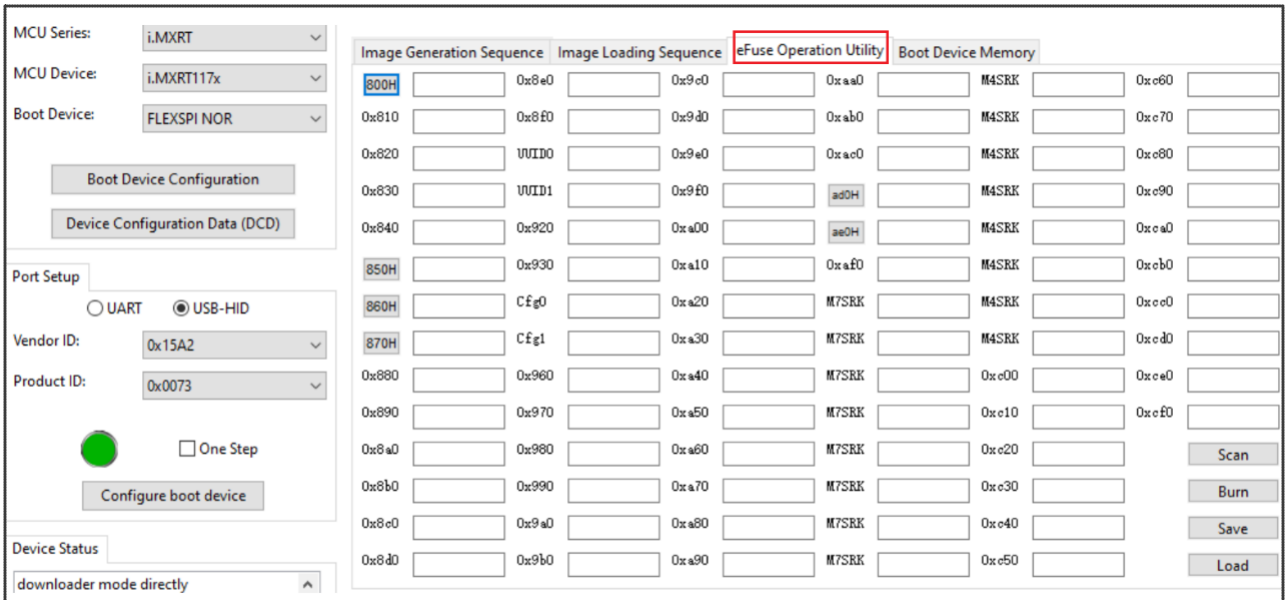

图 4. eFuse 操作工具面板

6. 在图 4 中，按下“扫描”按钮，熔丝值就会被加载，如图 5 所示。可以编辑熔丝值，并按下“烧录”按钮，将新的熔丝设置落实到芯片上。

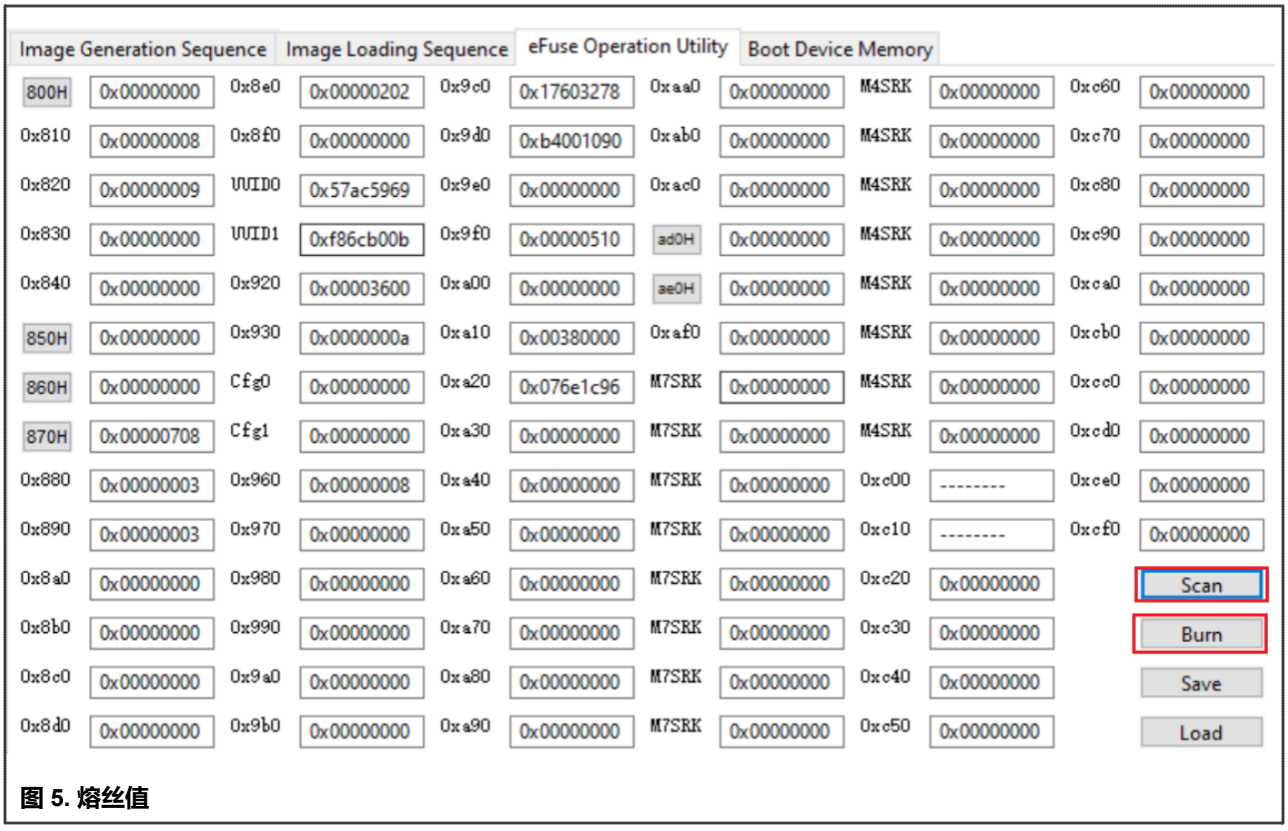

图 5. 熔丝值

5 预加载操作

对于 ECC 存储器区域，在读取之前，所有的存储器空间必须被写入正确的 ECC 值。否则在读取存储器时可能会发生 ECC 错误事件。第一次写操作也被称为预加载。

ROM 负责一些存储器区域的预加载，这取决于熔丝设置，如表 4 所示。

对于没有 ROM 预加载的存储区，在 ECC 存储器初始化中执行预加载。

表 4. ROM 预加载

项目	是否由 ROM 预加载
[CM7] 来自 CM7 FlexRAM 的 TCM	如果 0x840[15]和 950[0]熔断，是。
[CM7] Cache	—
[CM4] TCM/LMEM	如果 0x840[2]和 950[0] 熔断，是。
[CM4] Cache	—
[CM7/CM4] OCRAM1/OCRAM2	如果 0x840[2]和 950[0] 熔断，是。
[CM7/CM4] 来自 CM7 FlexRAM 的 OCRAM	—
[CM7/CM4] 来自 CM4 TCM/LMEM 的 OCRAM	如果 0x840[2]和 950[0] 熔断，是。
[CM7/CM4] XECC	—

6 ECC 错误注入

错误注入是为调试的目的提供的一种方法。通常，我们看不到应用中的 ECC 错误。为了验证 ECC 功能是否按预期工作，我们可以向存储器注入一些错误位。当访问带有错误位的存储器时，我们可以看到 ECC 失败。在 ECC 错误注入完成后，ECC 错误注入功能必须禁用，然后系统才能继续正常运行。

表 5 列出了支持 ECC 错误注入的存储器区域。

表 5. ECC 错误注入

项目	支持错误注入
[CM7] 来自 CM7 FlexRAM 的 TCM	√
[CM7] Cache	—
[CM4] TCM/LMEM	—
[CM4] Cache	—
[CM7/CM4] OCRAM1/OCRAM2	√
[CM7/CM4] 来自 CM7 FlexRAM 的 OCRAM	√
[CM7/CM4] 来自 CM4 TCM/LMEM 的 OCRAM	—
[CM7/CM4] XECC	√

7 与 ECC 功能相关的 SDK 示例

在 SDK 中，以下示例展示了如何通过 ECC 错误注入来触发 ECC 错误的细节：

- *boards\evkmimxrt1170\driver_examples\mecc*

- *boards\evkmimxrt1170\driver_examples\xecc*
- *boards\evkmimxrt1170\driver_examples\flexram\flexram_ecc*

要运行这些示例，首先要熔断表 2 中提到的位。

注意

熔断操作是不可逆的。

此外，随本文还提供了一个针对 MECC 和 FlexRAM 的演示代码 AN13204SW，以显示以下的完整的流程：

- 错误注入
- 禁用错误注入（在错误注入后，必须为应用禁用错误注入功能）
- ECC 错误触发和捕获

8 i.MX RT1170 ECC 应用的注意事项

- 对于启用了 ECC 的存储器区域，在读取之前要写入所有的存储器区域，否则可能会发生 ECC 失败。
- 有些存储器是按 64 位宽度组织的（详见表 1），所以即使是 32 位的写入，实际上也是按以下方式执行的：
  1. 读取 64 位
  2. 修改其中的 32 位
  3. 写回 64 位

  因此，在某些情况下，即使是一个 32 位的写操作，也可能由于伴随它的第一个 64 位的读操作而触发 ECC 错误事件。
- 表 4 中列出的预加载操作只有在检测到 POR 时才由 ROM 执行。在某些复位情况下，如果 SNVS 一直处于上电状态，ROM 将不做预加载。复位后，这可能导致存储器访问 ECC 失败。在 SDK 的代码中，有一个操作可以记录和清除 SRSR 寄存器。它在 SystemInit()函数中，由 ROM_ECC_ENABLED 宏控制，该宏默认为禁用。对于 ECC 应用，ROM_ECC_ENABLED 应由用户启用。对于不是基于恩智浦 SDK 的应用，开发者应该对 ECC 应用的这一点加以考虑。
- ECC 错误注入并不区分主机。不要进行动态的 ECC 错误注入，这将破坏来自外围的数据，如 DMA 或其他总线主机。建议在开始时向指定的存储器地址注入一些错误，然后在运行时禁用 ECC 错误注入功能。
- 对于映射自 CM4 TCM/LMEM 的 OCRAM：
  - 启用/禁用操作只能由 CM4 核完成。
  - 对于单核芯片，ECC 功能是默认启用的。
  - 它不能触发 CM7 核的 ECC 中断（ERR050634）。

9 参考资料

- *i.MX RT1170 处理器参考手册*（文档 IMXRT1170RM）

10 修订历史

版本号	日期	实质性变更
1	2022 年 1 月 14 日	• 更新了与 ECC 功能相关的 SDK 示例 • 在 AN13204SW 中添加了 FlexRAM ECC 示例

表格在下一页继续...

表格续上一页...

版本号	日期	实质性变更
0	2021 年 3 月	初版发布

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.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 14 January 2022
Document identifier: AN13204

arm