

Application Note

# Jacinto™ 7 和 Sitara™ 处理器 DDR 内联 ECC 错误注入与验证指南



Linjun Meng

Central FAE

摘要

DDR 内联 ECC 是在 Jacinto™ 7 和 Sitara™ 处理器上实现的一种关键可靠性和安全机制。虽然 ECC 功能在硬件中实现，但仅启用 ECC 无法证明能够正确检测、报告和处理存储器故障。错误注入测试提供了一种受控的方法，用于验证 ECC 检测、纠错、错误日志记录和诊断报告功能。

本应用手册介绍了建议的离线和在线 DDR 内联 ECC 错误注入方法。本文档说明了单比特、双比特和多相位 ECC 事件的验证程序，并演示了如何使用 ECC 错误日志和 ESM 通知来验证整个诊断链是否正常运行。这些信息适用于基于 Jacinto 7 和 Sitara 处理器开发汽车和工业系统的软件开发人员、系统架构师和功能安全工程师。

内容

|                           |    |
|---------------------------|----|
| 商标.....                   | 1  |
| 1 简介.....                 | 3  |
| 2 详细说明.....               | 4  |
| 2.1 为什么需要 ECC 错误注入测试..... | 4  |
| 2.2 DDR 内联 ECC 保护机制.....  | 4  |
| 2.3 离线错误注入.....           | 5  |
| 2.4 在线错误注入.....           | 6  |
| 2.5 单比特错误验证.....          | 7  |
| 2.6 双比特错误验证.....          | 8  |
| 2.7 多相位 ECC 验证.....       | 9  |
| 2.8 使用 ECC 错误日志进行验证.....  | 9  |
| 2.9 使用 ESM 进行验证.....      | 10 |
| 2.10 建议的验证策略.....         | 10 |
| 3 总结.....                 | 11 |
| 4 参考资料.....               | 12 |

插图清单

|                               |    |
|-------------------------------|----|
| 图 2-1. 验证流程.....              | 4  |
| 图 2-2. 单比特损坏事件.....           | 5  |
| 图 2-3. 双比特损坏事件.....           | 5  |
| 图 2-4. 离线错误注入流程.....          | 6  |
| 图 2-5. 专用 ECC 验证区域在线错误注入..... | 7  |
| 图 2-6. 单比特注入方法.....           | 7  |
| 图 2-7. 单比特注入预期行为.....         | 8  |
| 图 2-8. 双比特注入方法.....           | 8  |
| 图 2-9. 双比特预期行为.....           | 8  |
| 图 2-10. 汽车离线验证典型序列.....       | 10 |

表格清单

商标

Jacinto™ 和 Sitara™ 是德州仪器 (TI) 的商标。

所有商标均为其各自所有者所有。

## 1 简介

DDR 内联 ECC 通过生成和检查与 DDR 数据相关的纠错码 (ECC)，提供基于硬件的存储器损坏保护。

ECC 机制旨在：

- 纠正单比特错误
- 检测双比特错误
- 提高针对 DDR 故障的稳健性
- 提高安全相关系统的诊断覆盖率

尽管 ECC 功能在硬件中已实现，但仅启用 ECC 不足以验证系统是否正常运行。

为证明其正常运行，通常使用受控的 ECC 故障注入进行验证：

- ECC 检测
- ECC 纠错
- ECC 事件分类
- 错误日志生成
- ESM 中断生成
- 软件故障处理

本应用手册介绍了启动和运行时环境的实用 ECC 错误注入方法和验证程序。

## 2 详细说明

### 2.1 为什么需要 ECC 错误注入测试

从诊断角度来看，启用 ECC 只是配置了保护机制。启用 ECC 无法证明诊断链正常运行。

完整验证必须核实以下各项：

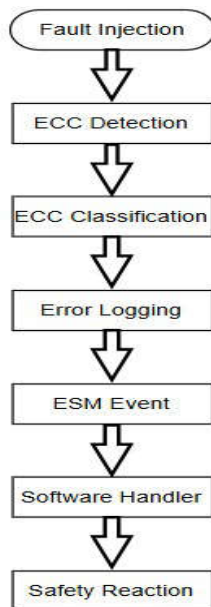


图 2-1. 验证流程

错误注入提供了一种可重复的机制，用于遍历整个诊断路径。

典型的验证目标包括：

- 可纠正错误检测
- 不可纠正错误检测
- ECC 错误日志记录
- ESM 事件生成
- 软件故障处理
- 地址日志报告

### 2.2 DDR 内联 ECC 保护机制

DDR 内联 ECC 将 ECC 校验特征码与 DDR 数据存储在一起，并在存储器读取期间执行自动检查。

#### • SECDED 保护

ECC 引擎提供：

- 单比特纠错 (SEC)
- 双比特检错 (DED)

对于单比特损坏事件：

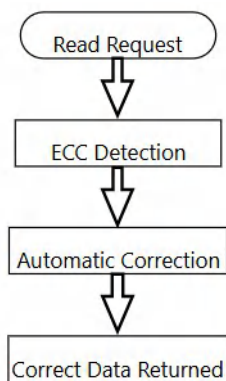


图 2-2. 单比特损坏事件

对于双比特损坏事件：

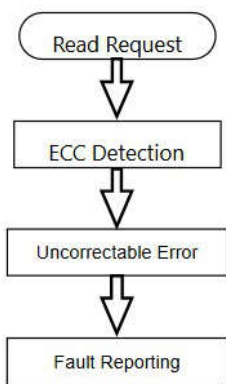


图 2-3. 双比特损坏事件

### 2.2.1 多相位 ECC 保护

DDR 访问以包含多个相位的突发事务形式进行。

传统的 SECDED 实现仅保护单独的数据字。DDR 内联 ECC 实现多相位 ECC 保护，可将覆盖率扩展到超出单独的相位。

这种机制可针对以下故障提供额外保护：

- 地址故障
- 命令故障
- 地址别名使用
- 突发损坏
- 大规模存储器损坏

因此，与传统的仅 SECDED 实现相比，DDR 内联 ECC 提高了诊断覆盖率。

## 2.3 离线错误注入

离线错误注入通常用于汽车验证流程。

常见的序列如下：

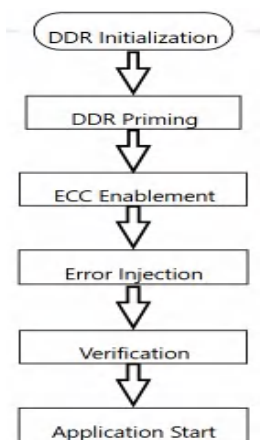


图 2-4. 离线错误注入流程

由于该应用程序尚未运行，因此可以安全地修改任意 DDR 位置，而不会影响软件执行。

典型程序

1. 完成 DDR 初始化。
2. 完成 DDR 预填充。
3. 启用 ECC 生成。
4. 禁用 ECC 检查。
5. 从目标位置读取数据。
6. 修改一个或多个比特。
7. 写回修改后的数据。
8. 重新启用 ECC 检查。
9. 读取修改后的位置。

此时，ECC 引擎会检测到注入的损坏。

## 2.4 在线错误注入

工业系统通常持续运行，无法轻易停止以进行启动式验证。

示例包括：

- PLC
- 机器人控制器
- 工业网关
- 边缘 AI 系统

在这些系统中，通常使用在线诊断。

### 2.4.1 方法 1：ESM 故障注入

ESM 模块可以提供故障注入功能。

此方法可验证：

- ESM 基础架构
- 中断路由
- 软件故障处理

不过，ESM 模块不会验证实际的 DDR ECC 功能。

### 2.4.2 方法 2：预留 DDR 验证区域

可以在 DDR 内预留专用的 ECC 验证区域。

要求：

- 无可执行代码
- 无栈分配
- 无堆分配
- 无应用程序数据

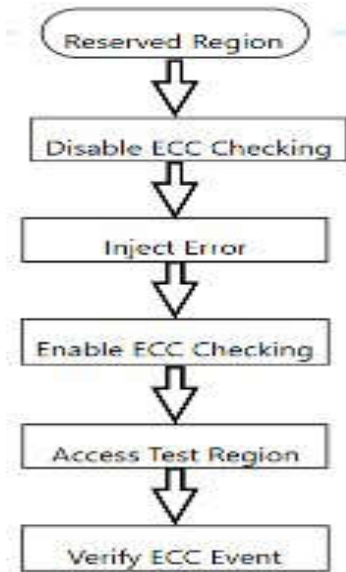


图 2-5. 专用 ECC 验证区域在线错误注入

此方法可在允许正常应用程序执行的同时验证完整的 ECC 数据路径。

## 2.5 单比特错误验证

注入方法

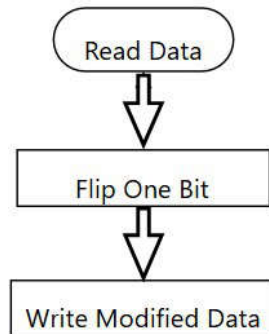


图 2-6. 单比特注入方法

预期行为

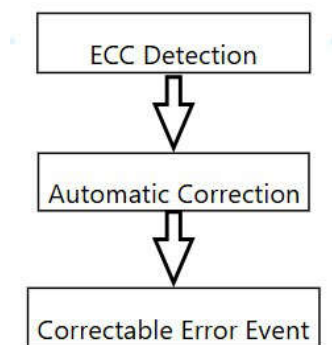


图 2-7. 单比特注入预期行为

预期结果：

- 数据正确返回
- 可纠正错误计数器递增
- 记录 ECC 地址
- 生成 ESM 通知

## 2.6 双比特错误验证

注入方法

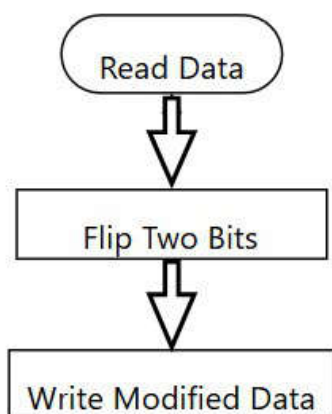


图 2-8. 双比特注入方法

预期行为

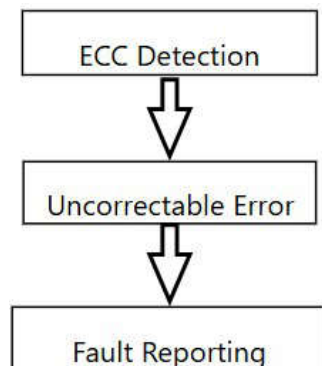


图 2-9. 双比特预期行为

预期结果：

- 生成 UECC 事件
- 记录错误
- 生成 ESM 通知
- 执行软件异常处理

## 2.7 多相位 ECC 验证

对于安全相关系统，验证还必须包括多相位 ECC 覆盖率。

这是一种代表性的验证方法，它将故障注入同一 DDR 突发的多个相位中。

示例：

相位 1 → 单比特错误

相位 5 → 单比特错误

预期行为：

多相位 ECC 检测

↓

不可纠正的错误

该测试用于验证对以下故障的检测能力：

- 地址故障
- 命令故障
- 突发损坏
- 大规模存储器损坏

## 2.8 使用 ECC 错误日志进行验证

发生 ECC 事件后，软件必须验证：

### ECC 错误计数器

示例：

- ECC\_1B\_ERR\_CNT
- ECC\_2B\_ERR\_CNT

### ECC 错误日志

示例：

ECC\_1B\_ERR\_ADR\_LOG

ECC\_1B\_ERR\_MSK\_LOG

ECC\_2B\_ERR\_ADR\_LOG

ECC\_2B\_ERR\_MSK\_LOG

记录的信息必须与注入的故障位置相对应。

### 地址验证

注入的地址 == 解码的错误地址

匹配成功表明：

- ECC 检测功能正常

- 错误日志记录功能正常
- 地址报告功能正常

## 2.9 使用 ESM 进行验证

除了 ECC 日志外，系统还必须验证 ESM 行为。

确认：

- 触发正确的 ESM 通道
- 生成正确的中断
- 正确的事件分类
- 执行预期的软件响应

这可确认故障通过诊断链正确传播。

## 2.10 建议的验证策略

### 2.10.1 汽车系统

建议的方法：

离线验证

典型序列：

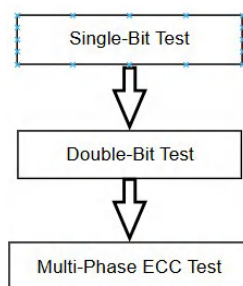


图 2-10. 汽车离线验证典型序列

优势：

- 超高覆盖率
- 确定性执行
- 对安全验证实用

### 2.10.2 工业系统

建议的方法：

- 定期 ESM 测试
- 预留 DDR 区域 ECC 测试

### 3 总结

DDR 内联 ECC 错误注入提供了一种实用方法，用于在 Jacinto™ 7 和 Sitara™ 处理器上验证 DDR 存储器保护机制。

通过将受控的故障注入与 ECC 错误日志验证和 ESM 监控相结合，系统开发人员可以验证 ECC 检测、纠错、多相位 ECC 保护、错误日志记录、中断路由和以及软件故障处理是否正常运行。离线验证通常是汽车系统启动验证的首选，而在线验证方法对持续运行的工业系统而言更为实用

## 4 参考资料

1. 德州仪器 (TI) , [TDA4VE TDA4AL TDA4VL 功能安全手册版本 0.99](#) , 功能安全手册。
2. 德州仪器 (TI) , [J721S2、TDA4AL、TDA4VL、TDA4VE 和 AM68A 技术参考手册 \(TRM\)](#) , 技术参考手册。

## 重要通知和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做任何明示或暗示的担保，包括但不限于对适销性、与某特定用途的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他安全、安保法规或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 [TI 销售条款](#)、[TI 通用质量指南](#) 或 [ti.com](#) 上其他适用条款或 TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

版权所有 © 2026，德州仪器 (TI) 公司

最后更新日期：2025 年 10 月