DOI:10.19651/j.cnki.emt.2209074

基于故障注入的 NOR Flash 单粒子效应模拟方法研究*

黄姣英[1] 何明瑞[1] 袁 伟[2] 高 成[1] 王乐群[1]
(1.北京航空航天大学可靠性与系统工程学院 北京 100191;2.陆军装备部驻北京地区第四军事代表室 北京 100072)

摘 要: 针对目前大容量 NOR Flash 存储器单粒子效应模拟缺乏具体操作方法的问题,本文提出 NOR Flash 单粒子翻转、单粒子功能中断、单粒子闭锁 3 种单粒子效应对应软件故障注入方法,设计适用于大容量器件的板级测试系统并进行功能验证,通过故障注入方法开展单粒子效应模拟实验。NOR Flash 存储器单粒子效应测试系统包括 FPGA 控制逻辑、Flash 检测板和上位机软件三部分。结果表明,单粒子翻转、单粒子闭锁和单粒子功能中断 3 种单粒子效应的软件故障注入方法均通过 NOR Flash 存储器单粒子效应测试系统得到验证。本文的研究可以为相关单粒子效应模拟提供参考,为分析存储器单粒子效应对电子系统的可靠性影响打下基础。

关键词: NOR Flash;单粒子效应;故障注入;测试系统;模拟方法
中图分类号: TN43 **文献标识码:** A **国家标准学科分类代码:** 510.10

Research on single particle effect simulation of NOR Flash based on fault injection

Huang Jiaoying[1] He Mingrui[1] Yuan Wei[2] Gao Cheng[1] Wang Lequn[1]
(1. School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China;
2. The Fourth Military Representative Office of the Army Armament Department in Beijing, Beijing 100072, China)

Abstract: In view of the lack of specific operation methods of single particle effect simulation in large capacity NOR Flash memory, this paper proposes three methods of single particle effect software fault injection in NOR Flash memory: single particle flip, single particle function interrupt and single particle latching. The board level test system is designed for large capacity devices and its function is verified. The single particle effect simulation experiment is carried out by fault injection method. The single particle effect test system of NOR Flash memory consists of FPGA control logic, flash detection board and host computer software. Results indicate that single particle flip, single particle latching and single particle function interruption software fault injection methods are verified by single particle effect test system of NOR Flash memory. This paper can provide a reference for related single particle simulation and the electrical system reliability analysis for single particle effect.

Keywords: NOR Flash; single particle effect; fault injection; test system; simulation method

0 引 言

空间环境中存在的各种带电粒子会对航空航天系统中半导体器件造成辐射损伤,伴随着半导体器件尺寸的不断缩小,单粒子效应随之出现,并已经成为影响宇航电子系统正常工作的主要因素[1]。单粒子效应即射入到半导体器件中的高能粒子与器件灵敏区域相互作用产生电子-空穴进而引发的器件功能异常或损坏。常见的单粒子效应包括单粒子翻转、单粒子闭锁、单粒子功能中断等[2]。

Flash 存储器的基本单元是基于浮栅工艺的 MOS 管,它存在两个栅:控制栅以及位于沟道和控制栅之间的浮栅。按照 Flash 内部结构以及技术实现特点,可以将其分为 NOR 型和 NAND 型。NOR Flash 存储器各单元间是并联的,它的传输效率高,读取速度快,每一位信息均可被寻址,并具有片上执行功能[3]。单粒子效应会对 NOR Flash 存储器的存储内容和存储功能造成影响,如存储单元中的数

收稿日期:2022-02-24
* 基金项目:国家国防科技工业局技术基础科研项目(JSZL2016601B007)资助

据可能发生从 1 到 0 或从 0 到 1 的翻转，进而影响整个电子系统的可靠性。NOR Flash 存储器作为重要的程序及指令存储器，大量应用于各型号航天系统，故对 NOR Flash 存储器单粒子效应的评价至关重要。

针对于存储器单粒子效应的评价方法主要有实际故障注入法、软件故障注入法两种。实际故障注入即通过试验方法让器件产生故障，如将粒子加速器加速过的粒子流作用在器件的功能区，使存储器产生数据翻转等失效模式[4]。实际故障注入可以较真实地模拟空间辐射环境，但测试周期长且费用高昂。软件故障注入是通过修改存储单元内容或检测控制程序等手段来模拟实际试验中产生的故障[5]，它的优点是成本较低操作简便，无需进行实际试验。王梦茹等[6]提出了一种 SRAM 型 FPGA 单粒子软件故障注入实验集的筛选方法；刘博铭等[7]设计了一种针对 FPGA 和 STM32 的多类型软件故障注入系统。目前，针对于大容量 NOR Flash 存储器单粒子效应的软件故障注入方法还缺乏相关总结与研究。

针对以上问题，本文对 NOR Flash 存储器单粒子效应的检测方法进行总结，提出单粒子翻转、单粒子闭锁、单粒子功能中断 3 种典型单粒子效应的软件故障注入方法，搭建单粒子效应测试系统并进行功能验证，通过软件故障注入方法对单粒子效应进行模拟实验，最后通过测试系统对单粒子效应的模拟结果进行验证。

1　NOR Flash 单粒子效应检测方法研究

Flash 存储器在重离子辐照后的主要故障模式有单粒子翻转、单粒子功能中断、单粒子闭锁。单粒子翻转按出现错误的数据规模可分为随机位翻转与集群翻转，单粒子功能中断按故障持续时间可分为瞬态功能中断与持续功能中断，本文主要针对单粒子随机位反转、持续功能中断与单粒子闭锁开展研究。NOR Flash 存储器常见单粒子效应的分类和故障模式如图 1 所示。

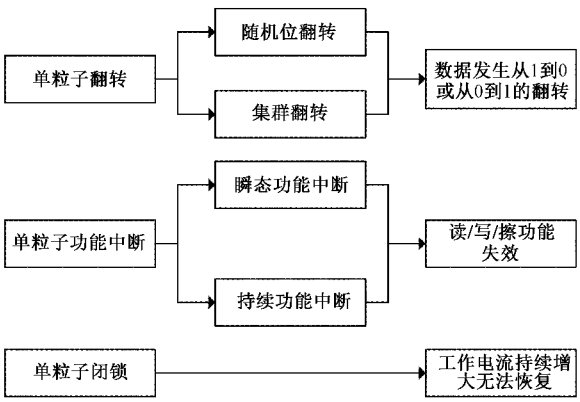


图 1　NOR Flash 单粒子效应分类及故障模式

Flash 存储器单粒子效应的检测途径主要为进行写读擦操作，并根据数据输出结果的具体表征进行判断。若在测试过程中检测到存储单元数据发生从 1 到 0 或从 0 到 1 的翻转，则可初步判断器件发生单粒子翻转；若存储器出现读/写/擦功能失效或大面积有规律的翻转，则可判断器件发生单粒子功能中断；若器件工作电流增大且无法自动回复则可判断器件发生了单粒子闭锁。

2　NOR Flash 单粒子效应测试系统研究

2.1　测试系统控制逻辑研究

本文从具体效应的检测方法中总结功能需求，开展 NOR Flash 存储器单粒子效应测试系统研究和设计[8-9]。测试系统由 FPGA 作为控制器，控制逻辑分为 6 部分，分别是 Flash 控制、电流检测器控制、继电器控制、UART 通信、数据输入控制和数据输出控制。系统总控制逻辑如图 2 所示。

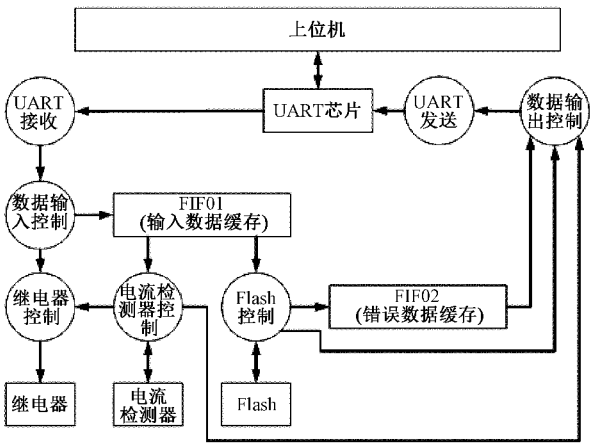


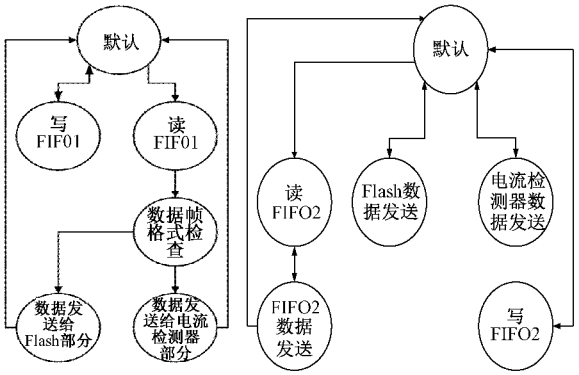
图 2　测试系统控制逻辑

检测端和上位机采用 UART 通信协议，测试系统设置了对 Flash 存储器的 4 种检测操作模式，即全片写 ΛΛΛΛh、全片写 5555h、全片读和全片擦。系统检测工作流程如下：指令由上位机输入后由数据输入控制逻辑进行读取并发送同时写入 FIFO1 存储器缓存，之后通过 Flash 控制、电流检测器控制、继电器控制 3 部分逻辑完成故障注入与检测，检测完成后将 Flash 错误数据写入 FIFO2 存储器缓存，错误数据可在上位机软件端读取。数据输入控制具体逻辑状态设计如图 3(a)所示，数据输出控制具体逻辑状态设计如图 3(b)所示。

2.2　测试系统软硬件设计

为完成单粒子翻转、单粒子闭锁和单粒子功能中断的模拟与检测，测试系统硬件部分要实现 3 部分主要功能：提供测试平台对 Flash 器件进行控制、进行电流监测以及发生单粒子闭锁时保护电路。本文选用 Xilinx 公司的 Artix-7 系 FPGA 作为主控制板，具体型号为 XC7A35T-1FTG256，主要参数如表 1 所示。

NOR Flash 存储器选用上海复旦微电子集团生产的航天用 JFM29GL256 型存储器，容量大小为 256 Mbit，配



(a) 数据输入逻辑　　(b) 数据输出逻辑

图 3　数据输入/输出控制逻辑状态设计

表 1　FPGA 主要参数

参数	数值
逻辑单元 Logic Cells	33 280
乘法器 DSP48	90
可配置逻辑块 CLBs	41 600
内嵌式块 RAM/KB	1 800
时钟单元 CMTs	2
可用 IO 数量	200
内核电压/V	1
分布式 RAM/KB	400

置有一个 64 Byte 的写入缓冲区,在一次操作中可以编程 32 个地址。JFM29GL256 管脚定义如表 2 所示。

表 2　JFM29GL256 管脚定义

管脚名	输入/输出	说明
A23-A0	输入	24 位地址输入
DQ14-DQ0	输入/输出	15 位数据输入/输出
CE#	输入	片选使能
OE#	输入	输出使能
WE#	输入	写使能
RY/BY#	OD 输出	准备/忙状态输出

为了实现电流监测功能,需配置电流检测器件,本文采用 INA226 型电流/功率检测器,具有 I^2C 接口,可实现电流值和功率值的直接读取。发生单粒子闭锁时,电路工作电流会不断增大,若不及时处理会导致器件永久性损伤,本文采用继电器实现电路保护。继电器的控制信号由 FPGA 施加,当工作电流小于设定的阈值时,FPGA 控制信号为高电平,继电器吸合;当电流大于设置的阈值时,FPAG 拉低控制信号,继电器断开。

Flash 检测板主要完成 Flash 器件检测座和 FPGA 核心板的连接,使 Flash 正常工作。测试系统硬件部分如图 4 所示。

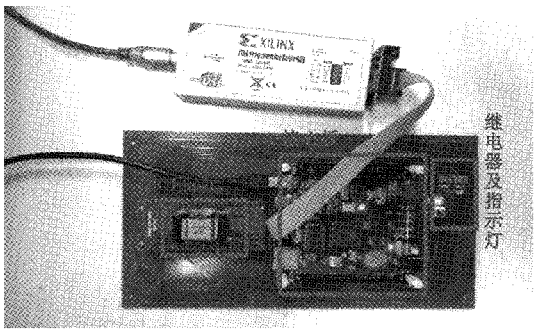


图 4　测试系统硬件实物

本文基于 LabVIEW 的上位机软件具有和检测端进行串口通信、显示 Flash 存储器工作电流波形和显示单粒子翻转数据 3 种功能,界面如图 5 所示。软件发送指令后,检测端发送的数据会在发送区显示,按下显示波形按键,软件可以把电流检测器发送的 16 位数据转化为电流值并以波形显示在右侧波形区。在发送读取错误数据的指令后,单粒子翻转的错误数、错误数据和错误地址会出现在下方错误数据区。

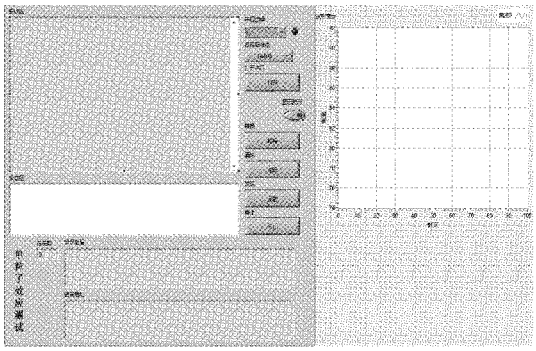


图 5　测试系统软件界面

2.3　测试系统功能验证

测试系统的功能验证分为 Flash 控制逻辑验证与电流监测功能验证两方面。通过测试系统的功能验证,证明 UART 通信协议配置正确,且测试系统能够成功实现对 Flash 存储器进行控制以及电流监测[10-12]。

1)Flash 控制逻辑验证

Flash 控制逻辑验证通过 ModelSim 软件分别进行写入缓冲区编程、读取操作两部分验证。逻辑验证部分的工作流程如图 6 所示。

(1)Flash 写入缓冲区编程功能验证

通过 UART 通信逻辑发送字节数据并写入 FIFO1 存储器中,Flash 控制逻辑中的信号收发部分在收到 FIFO1 指令后开始读取数据,验证格式正确后,发送指令到 Flash 控制逻辑的 Flash 通信部分。根据器件手册的指令要求,写入缓冲区编程需要 4 个解锁周期、1 个字写入缓冲区周期以及 1 个嵌入式算法编程的确认周期。Flash 写入缓冲区编程信号波形如图 7(a)所示,CE 信号先拉低,然后 WE

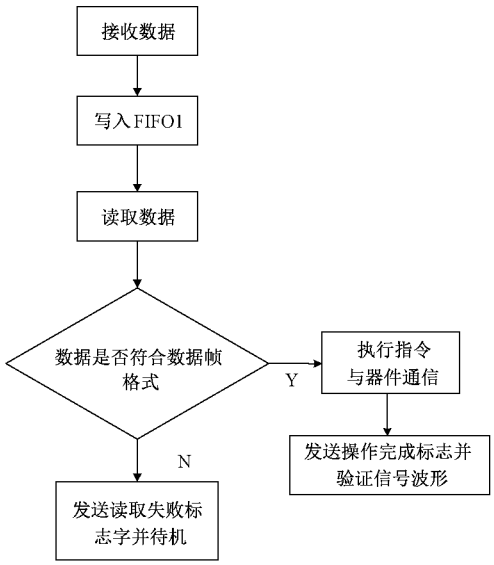
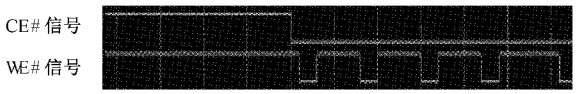
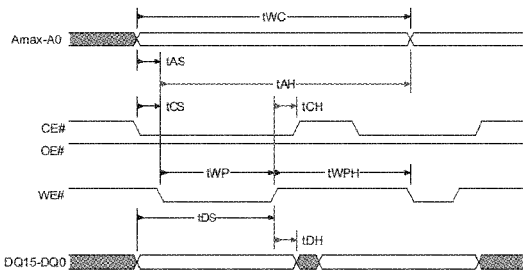


图 6　控制逻辑验证工作流程

信号拉低接着拉高，完成一个指令周期。地址在 WE 下降沿捕捉，数据在 WE 上升沿捕捉，在每个 WE 信号下降沿到来前，数据和地址提前发生变化，符合图 7(b)中时序要求和指令要求。



(a) Flash写入缓冲区编程信号波形



(b) Flash写操作时序图

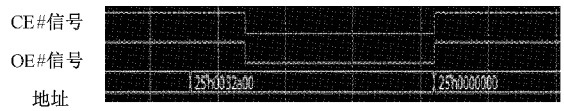
图 7　Flash 写入缓冲区编程验证

(2)Flash 读取操作验证

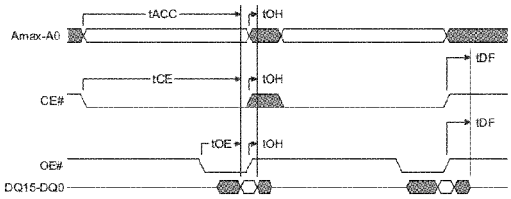
读操作的信号收发部分波形和写入缓冲区编程相似，当 CE 信号为低、OE 信号为低、地址保持稳定、且满足异步访问时间时，数据会出现在 DQ15-DQ0 端口上。通信部分的 CE、OE 和地址波形如图 8(a)所示，符合图 8(b)中时序和时间参数要求。

2)电流监测功能验证

调用 Vivado 中的 ILA IP 核对电流检测器控制逻辑进行监测，写 INA226 寄存器波形图如图 9(a)所示，在 link_sda 信号为低时，I2C 数据线 SDA(图中 cnt)由电流检测器 INA226 控制，可见每次写入后都收到了器件应答信号。读 INA226 寄存器波形图如图 9(b)所示，在 link_sda 信号



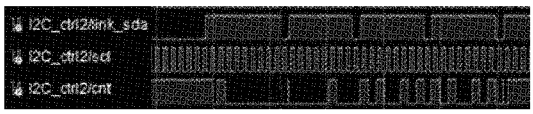
(a) Flash读操作验证信号波形



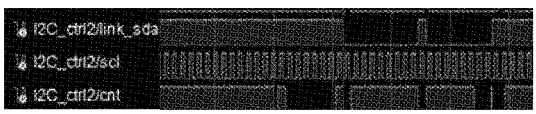
(b) Flash读操作时序图

图 8　Flash 读取操作验证

为低时，上位机可接收到 8 位数据帧格式验证成功标志 FFh 和 16 位寄存器输出数据。



(a) 写INA226寄存器ILA波形图



(b) 读INA226寄存器ILA波形图

图 9　INA226 寄存器 ILA 波形图

上位机发送检测开始指令后程序开始进行电流监测，每 540 ms 输出一次，实时输出电流值如图 10 所示，电流监测功能验证成功。

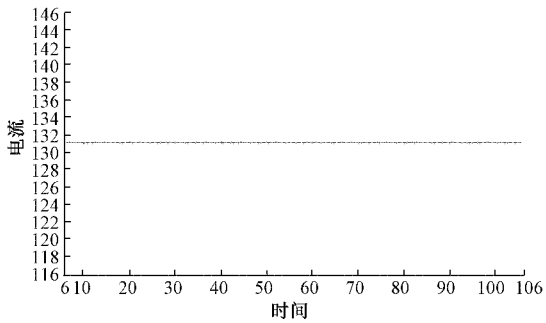


图 10　检测开始后实时电流值输出

3　单粒子效应故障注入模拟实验

3.1　单粒子翻转故障注入

单粒子翻转的故障注入实现方法为：首先进行数据写入，之后进行全片擦除操作。在全片擦操作后，向部分存储单元中写入与上次操作不同的数据来模拟单粒子翻转。实现方法的逻辑如下：因为单字写入不是全片操作，此时控制逻辑仍然认为存储单元内容是上次全片操作后的数据。检测控制逻辑在读取存储单元数据时会把它和擦除后的数据在 FPGA 内部进行比较，将单字写入的内容视为错误。若

读取某一地址的数据与上次全片操作的数据不相同,控制逻辑会把错误数据和地址写入 FIFO2 存储器中,以此判断发生单粒子翻转[13-15]。

单粒子翻转故障注入的具体操作方法为:发送向 NOR Flash 写入 5555h 的指令,成功写入 5555h 后,对器件进行全片擦除,擦除成功后向存储器地址 EEEEEEh 写入 AAAAh,向存储器地址 EEEEEFh 写入 5555h,完成单粒子翻转的故障注入。

3.2 单粒子功能中断故障注入

对单粒子功能中断的故障注入实现方法为:首先对存储器进行全片擦除操作,之后向某一地址写入数据,最后进行全片写入操作。实现方法的逻辑如下:由于 Flash 存储器只能先通过擦除操作将 0 变为 1,再通过写入操作将其变为 0,而不能直接向已有存储数据的地址继续写入数据,故先向部分存储位为 1 的单元写入 0 再进行全片写入操作来模拟单粒子功能中断[16]。

单粒子功能中断故障注入的具体操作方法为:首先进行全片擦除操作,向存储器地址 AAAAAAh 写入数据 5555h,最后执行全片写入 ΛΛΛΛh 操作。

3.3 单粒子闭锁故障注入

单粒子闭锁故障注入实现方法为:将单粒子闭锁电流阈值设置在正常工作电流以下,通过测试系统检测器件的工作电流,若继电器断开则判断发生了单粒子闭锁。实现方法的逻辑如下:单粒子闭锁的现象是工作电流持续增大,且不能自动恢复。在本文的测试系统中,当电流大于设置的阈值即 150 mA 时,FPGA 会拉低控制信号,继电器切断电源,避免单粒子闭锁破坏电路。

单粒子闭锁故障注入具体操作方法为:上电后对电流检测器进行配置,将测试开始指令设置为 AA5580A5h,停止测试指令设置为 AA5500A5h。测试系统输出的实时电流值若大于 150 mA 则判断发生单粒子闭锁,FPGA 会拉低继电器控制引脚,继电器开关释放,将电路断开。

4 模拟结果验证

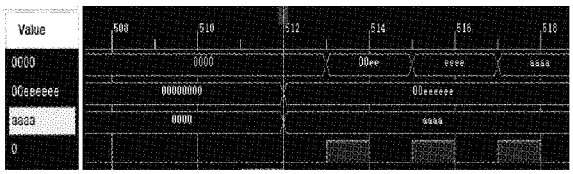
4.1 单粒子翻转模拟结果验证

完成故障注入后发送全片读操作,如图 11 所示,可以从在线逻辑分析仪中看到 FPGA 向 FIFO1 中写入了发生“翻转”的地址 EEEEEEh 和数据 AAAAh,地址 EEEEEFh 和数据 5555h。

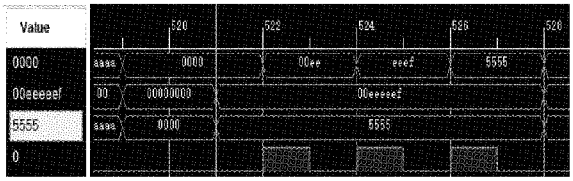
全片读操作完成后发送指令读取 FIFO2 存储器中内容,此时上位机接收到 2 处发生翻转的地址和错误数据,如图 12 所示,即地址 EEEEEEh 和数据 AAAAh,地址 EEEEEFh 和数据 5555h,单粒子翻转模拟成功。

4.2 单粒子功能中断模拟结果验证

单粒子功能中断验证方法是监测 Flash 存储器的 RY/BY#引脚电平并在 RY/BY# 信号为低时读取 Flash 存储器的状态寄存器。RY/BY# 信号为器件忙碌标志,在



(a) 故障地址及故障数据1



(b) 故障地址及故障数据2

图 11　FIFO1 中写入的故障地址及数据波形

图 12　发生翻转的地址、数据及数量

Flash 的内嵌算法执行期间为低电平。在 RY/BY# 信号为低时,状态寄存器连接 Flash 的数据引脚标志操作是否成功执行。部分状态寄存位和 RY/BY# 的信号功能如表 3 所示。

表 3　信号含义

位名称	功能
DQ6	翻转位,内嵌算法执行期间连续翻转。
DQ5	超时限制位,指示编程或擦除操作时间是否已经超过了内部脉冲计时限制,超过时为 1,表明操作没有成功。
RY/BY#	器件忙碌标志,内嵌算法执行期间为 0。

在故障注入后,因全片写入操作不能向已写入数据的地址再次写入数据,器件进入保护状态,无法再进行写入和擦除操作。器件进入保护状态后,RY/BY# 信号会拉低,如图 13 所示,此时只能对器件进行读操作。

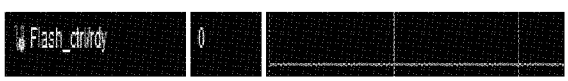


图 13　故障注入后 RY/BY 信号波形

状态寄存器输出如图 14 所示,DQ6 位连续翻转,表示器件没有完成写入操作;同时 DQ5 为 1,可见操作超过内部计时限制,没有成功执行。因此判断器件发生写入功能中断,需要复位命令来返回读模式,单粒子功能中断模拟成功。

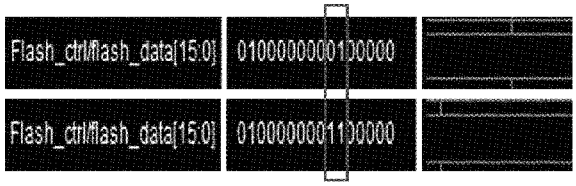


图 14　故障注入后状态寄存器翻转情况

4.3　单粒子闭锁模拟结果验证

由于将单粒子闭锁电流阈值设置在正常工作电流以下，故在发送测试开始指令后系统检测到电流超过阈值，继电器开关释放，Flash 工作电路断开。发送停止测试指令后按下系统复位按键，工作电路恢复正常，LED 指示灯功能如表 4 所示。

表 4　LED 功能说明

指示项	功能
LED0	操作完成标志，每次对 Flash 的操作完成后 LED0 亮起，当上位机开始传输数据时 LED0 熄灭，按下复位按键后 LED 为灭状态。
LED1	指令作用于控制逻辑标志，当指令在数据输入控制逻辑中判断为作用于 Flash 控制逻辑时 LED1 亮。

可见电路正常工作时继电器工作电路的指示灯 LED0 和 LED1 均亮，系统检测到电流超过阈值且继电器释放后继电器保护部分指示灯 LED1 熄灭，如图 15 所示，单粒子闭锁模拟验证成功。

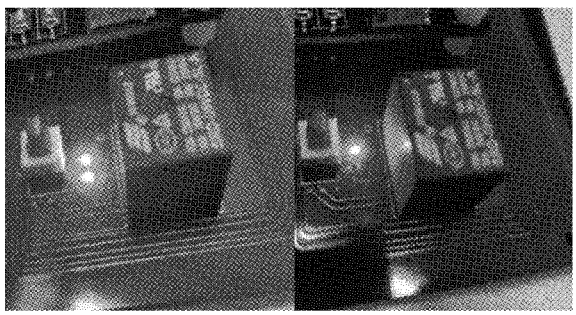


图 15　继电器吸合和释放状态指示灯情况

5　结　　论

本文依据具体单粒子效应的检测方法提出了单粒子翻转、单粒子功能中断、单粒子闭锁 3 种单粒子效应的软件故障注入方法并搭建了 NOR Flash 单粒子效应测试系统，通过该系统对故障注入的单粒子效应模拟进行了验证。本文的研究可以为相关单粒子效应模拟提供参考，支撑 NOR Flash 存储器的抗辐照鉴定检验，同时为器件的单粒子加固技术的研究打下基础。

参考文献

[1]　赵兴，栗伟珉，程向丽，等. 航天空间环境单粒子效应研究[J]. 电子制作，2021(13)：87-89.

[2]　黄姣英，王乐群，高成. Flash 存储器单粒子效应测试研究综述[J]. 电子技术应用，2020，46(7)：44-48，52.

[3]　陆游游，舒继武. 闪存存储系统综述[J]. 计算机研究与发展，2013，50(1)：49-59.

[4]　陈鑫，施聿哲，白雨鑫，等. 单粒子翻转效应的 FPGA 模拟技术[J]. 电子与封装，2021，21(9)：70-76.

[5]　刘强，唐鸿辉. 电磁故障注入攻击对动态随机存取存储器安全性的影响研究[J]. 电子与信息学报，2021，43(9)：2449-2457.

[6]　王梦茹，周珊，张弛，等. 一种 SRAM 型 FPGA 单粒子故障注入实验集的筛选方法[J]. 微电子学与计算机，2021，38(1)：38-44.

[7]　刘博铭，王志超，林岩. FPGA 和 STM32 的多类型故障注入系统设计[J]. 单片机与嵌入式系统应用，2020，20(11)：43-46.

[8]　郑晓云，陶淑苹，冯汝鹏，等. SRAM 型 FPGA 抗单粒子翻转技术研究[J]. 电子测量技术，2015，38(1)：59-63.

[9]　陈晨，徐微，张善从. Flash 型 FPGA 单粒子效应测试系统设计[J]. 电子测量技术，2014，37(9)：70-78.

[10]　王红敏，董涛，宁生科. 超大规模集成电路内部单粒子翻转效应仿真[J]. 计算机仿真，2021，38(8)：277-281.

[11]　王颖，李郑梅，李毅强，等. 单粒子效应在线检测系统设计与实现[J]. 电子技术与软件工程，2018(13)：53-54.

[12]　余永涛，陈煜海，余俊杰，等. SRAM 型 FPGA 单粒子效应测试方法及试验验证[J]. 航天器环境工程，2021，38(5)：534-540.

[13]　黄东巍，吕贤亮. DC/DC 单粒子效应的多通道高速测控系统实现[J]. 国外电子测量技术，2017，36(8)：42-45.

[14]　薛旭成，吕恒毅，韩诚山. 空间电子系统 FPGA 抗单粒子闩锁设计[J]. 电子测量与仪器学报，2014，28(8)：865-869.

[15]　张鑫宇，韩跃平，张鹏，等. 基于 FPGA 的片上多通道采集模块设计[J]. 国外电子测量技术，2021，40(4)：144-149.

[16]　ZHU B，LI J L，CHEN H X，et al. Research on single event effects of ethernet MAC controller on manned spacecraft[J]. Journal of Physics：Conference Series，2021，1754：012100.

作者简介

黄姣英，博士，高级工程师，主要研究方向为电子元器件可靠性分析与评价。

E-mail：huangjy@buaa.edu.cn

何明瑞，硕士研究生，主要研究方向为电子元器件可靠性分析。

E-mail：hemingrui@buaa.edu.cn