

引用格式:王梦茹,周珊,薛盼盼,等. 基于 SEM IP 和部分重配置的 SRAM 型 FPGA 单粒子故障注入[J]. 微电子学与计算机, 2021,38(8):8-12. [WANG M R, ZHOU S,XUE P P,et al. SRAM FPGA single event fault injection based on SEM IP and partial reconfiguration[J]. Microelectronics & Computer,2021,38(8):8-12.

基于 SEM IP 和部分重配置的 SRAM 型 FPGA 单粒子故障注入

王梦茹^{1,2},周 珊^{1,2},薛盼盼²,孔 璐²,王金波²

(1 中国科学院大学,北京 100049;

2 中国科学院 空间应用工程与技术中心,北京 100094)

摘 要: SEM IP(Soft Error Mitigation 软错误缓解核)是对 SRAM FPGA 设计进行单粒子故障注入的一种有效方法.然而由于目标设计与 SEM IP 部分随机布局布线在一块芯片上,导致进行故障注入时很有可能会打翻 SEM IP 所使用的配置寄存器而导致故障注入停止工作,同时对于目标设计失效率统计不准确.为解决这一问题,基于 SEM IP 和部分重配置技术开发了一套单粒子故障注入原型系统用于单粒子故障注入实验.该方法将 SEM IP 和目标设计布局布线到芯片的不同区域,能够只对目标设计所在区域进行故障注入并且不中断目标设计运行,并且在发生不可纠正错误后对目标设计所在区域进行部分重新配置,配置数据更少,用时更短,系统故障的注入效率大大提高,提高对于目标设计软错误失效率估计的准确性.

关键词: SEM IP;部分重配置;单粒子故障注入;SRAM 型 FPGA

中图分类号: 510.1035

文献标识码: A

文章编号: 1000-7180(2021)08-0008-05

SRAM FPGA single event fault injection based on SEM IP and partial reconfiguration

WANG Mengru^{1,2},ZHOU Shan^{1,2},XUE Panpan²,KONG Lu²,WANG Jinbo²

(1 University of Chinese Academy of Sciences, Beijing 100049, China;

2 Technology and Engineering Center for Space Utilization, Chinese Academy of Sciences, Beijing 100094, China)

Abstract: SEM(Soft Error Mitigation) IP is an effective method of single event fault injection for SRAM FPGA design. However, the target design and the SEM IP part are randomly placed and routed on the same chip, when fault injection is performed, the configuration register used by the SEM IP is likely to be overturned, causing the fault injection system to stop working and the failure rate of the target design is not accurate. To solve this problem, a single event fault injection prototype system based on SEM IP and partial reconfiguration technology is developed for single particle injection. The method places and routes the SEM IP and the target design to different areas of the chip, can only perform fault injection into the area where the target design is located without interrupting SEM IP operation itself. Besides, the area of the target design can be reconfigured when an uncorrectable error occurs. The method needs less configuration data and shorter time, which greatly improves the efficiency of fault injection experiment and the accuracy of the target design soft failure rate estimation.

Key words: SEM IP;partial reconfiguration;single particle fault injection;SRAM FPGA

1 引言

对 SRAM 型 FPGA 的抗单粒子效应进行安全性设计、评估的方法之一是故障注入,基于 SEM IP (Soft Error Mitigation 软错误缓解核)的单粒子故障注入方法由于其可移植性、能够不中计,与目标设计实际运行时遭受的高能粒子攻击效果更接近,成为一种应用最广泛的一种故障注入方法. 由于 SEM IP 和目标设计共同组成整个工程设计,在正常布局布线的过程中会将目标设计和 SEM IP 随机布局布线到任意位置. 该状态下,若对目标设计执行故障注入,会打翻 SEM IP 使用的配置寄存器,这种情况下一方面需要重新下载配置文件使得 SEM IP 能够正常工作,另一方面对目标设计的失效率统计就不准确. 因此,为了有针对性的对目标设计进行故障注入而不涉及其他无关的部分,需要找到一种将 SEM IP 和目标设计分开布局布线的方法. 这样一来能够只对设计者关心的部分进行故障注入,从而依据故障注入结果对目标设计的失效率进行统计,提高失效率统计的准确性;同时,当目标设计发生不可修复的故障时,可通过部分重配置的方法对目标设计进行配置文件下载而不中断设计运行.

本文将 SEM IP 在线故障注入技术和部分重配置技术结合起来开展单粒子故障注入实验;SEM IP 提供了向 FPGA 配置存储器进行故障注入的能力,部分重配置提供了在单个 FPGA 上动态地对硬件进行时间复用的能力,提高灵活性的同时,可以对目标设计进行在线故障注入,同时不会因为将故障注入到 SEM IP 而影响故障注入系统的正常工作.

2 SEM IP 简介

2.1 SEM IP 接口

SEM IP 的结构如图 1,主要包括外部设置模块 (EXT Shim)、HID 设置模块 (HID Shim)、MON 模块 (MON Shim)以及控制器 (Controller).

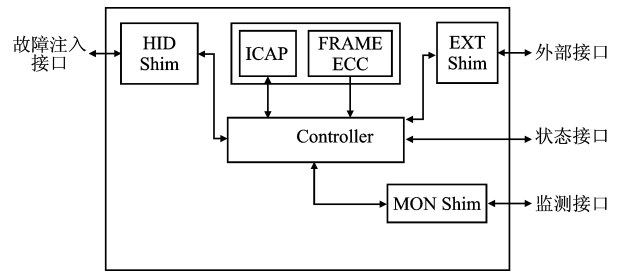


图 1 SEM IP 核结构图

控制器 (Controller) 的对外呈现的接口包含 ICAP 接口、FRAME 接口、外部接口 (External Interface)、状态监视接口 (Monitor Interface)、故障注入接口 (Error Injection Interface) 分别对应着外部设置模块 (EXT Shim)、MON 模块 (MON Shim)、HID 设置模块 (HID Shim). 另外还有与控制器直接相连的状态接口 (Status Interface), 为 SEM IP 提供时钟信号的时钟接口. 这些接口并不是在所有的设计中都会用到,依据在产生 SEM IP 的时候的选项不同,控制器对外呈现的接口种类为 4 到 6 个.

1)故障注入接口

该接口是可选的,在对 SEM IP 进行配置时若使能 Error Injection 选项和相应的 I/O 管脚,控制器就会呈现出故障注入接口. 故障注入接口提供了命令控制器往配置存储器注入故障的命令集合.

故障注入接口接受五种类型的命令:

- (1)进入空闲状态的命令
- (2)进入观察状态的命令
- (3)执行软件重置的命令
- (4)在物理帧地址处注入错误
- (5)在线性帧地址处注入错误

2)状态接口

通过状态接口我们可以获知控制器正在进行的操作. 通过状态接口信号我们可以获知的信息有三类:

- (1)State:表示控制器正在执行的操作
- (2)Flags:标识检测到的错误类型
- (3)Heartbeat:表示扫描处于活动状态

3)监控接口

该接口为串行接口,主要作用为交换命令、状态,采用 RS232 协议,由信号 monitor_tx 和 monitor_rx 实现.

4)ICAP 接口

ICAP 接口是 SEM 控制器和 ICAP 原语之间的点对点连接. 通过 ICAP 原语,可以对 FPGA 配置系统内部的寄存器进行读写访问.

5)FRAME_ECC 接口

FRAME_ECC 接口是 SEM 控制器和 FRAME_ECC 原语之间的点对点连接. FRAME_ECC 原语均为输出接口,它提供了进入 FPGA 配置系统中的软错误检测功能的途径.

2.2 SEM IP 状态

SEM IP 的工作状态有 5 种:初始化 (Initialization)、观察态 (Observation)、纠正态 (Correc-

tion)、分类态(Classification)、空闲态(Idle)、注入态(Injection)、致命错态(Fatal Error)。

故障注入过程是一个读 - 修改 - 写操作,用于故障注入命令中指定的地址处进行配置存储器状态翻转. 对单 bit 位进行故障注入时,SEM IP 的工作状态从注入态(Correction)跳转到空闲态(Idle). 如果要进行多位故障注入,可以通过重复的故障注入命令实现,每个故障注入命令结束后 SEM IP 控制器都会进入空闲态继续接收故障注入指令. 故障注入完成时,SEM IP 的工作状态会从空闲态跳转到观察态.

2.3 SEM IP 指令

在本文的故障注入实验中,我们通过状态监控接口进行故障注入并观察 SEM IP 当前的状态,本节将介绍监控接口上的几类消息. 监控接口消息可分为给 SEM IP 发送的消息和从 SEM IP 接收的消息.

- 发送消息
- 1)错误注入
- “N”命令用于执行错误注入. 控制器仅在处于空闲状态时接受此命令.
- 该命令的格式为:
- N {10-digit hex value}
- 发出此命令类似于在错误注入接口上执行错误注入命令.
- 2)软件重置
- “R”命令用于进行软件重置. 控制器仅在处于空闲状态时接受此命令.
- 该命令的格式为:
- R {2-digit hex value}
- 接收消息
- 3)初始化报告
- 当 SEM IP 控制器执行初始化序列时,它会生成初始化报告. 此报告包含一些诊断信息. SEM IP 控制器首次启动时以及软件重置时会生成此报告. 以 Xilinx 7 系列芯片为例,初始化报告如下:

X7_SEM_V4_1	Name and Version
SC 01	State Change, Initialization
FS {2-digit hex value}	Core Configuration Information
ICAP OK	Status; ICAP Available
RDBK OK	Status; Readback Active
INIT OK	Status; Completed Setup
SC 02	State Change, Observation

- 4)状态改变报告
- 当 SEM IP 控制器的状态发生改变时会发出状态变化报告.
- 报告格式如下:
- SC {2-digit hex value}
- 状态接口输出表现为 2 位十六进制值.

Report String	State Name
SC 00	Idle
SC 01	Initialization
SC 02	Observation
SC 04	Correction
SC 08	Classification
SC 10	Injection
SC 1F	Fatal Error

3 部分重配置技术

可重配置系统通过将配置流文件下载到可重配置逻辑器件的配置存储器中来实现系统的不同的功能. 根据重配置的发生时间,可将重配置技术划分为动态和静态两种,其中动态重配置技术又可分为动态全局重配置技术和动态部分重配置技术^[1].

3.1 静态重配置

静态重配置技术是指在系统开始运行前,将配置文件加载到可重构逻辑设备中,一旦系统开始运行起来,将不再加载新的配置文件;如果任务变化需要重新进行配置文件加载,则需要终止系统运行才能够进行重新配置.

3.2 动态重配置

动态重配置,又称运行时重配置(Run Time Reconfiguration, RTR)^[2],相比于静态重配置技术,动态重配置更加灵活高效,它能够在系统运行时对其进行实时配置. 依据配置的对象范围不同,动态重配置又可分为动态全局重配置和部分重配置.

3.2.1 动态全局重配置

动态全局重配置中多采用配置缓存和配置文件两种方式,这两种方式都是利用片内或者片外的存储介质存储配置文件,当需要对系统进行重新配置时切换配置文件重新配置器件. 动态全局重配置前后的电路一般差别较大,而且每次重新配置时需要将所有资源的重新分配.

3.2.2 部分重配置

部分重配置,支持在 FPGA 某一区域,进行部分功能的重新编译,而且在部分重配置的过程中,能

持续运行当前功能,不中途断开.即,在芯片其它不需配置的区域中持续运行之前配置.部分重配置需要的配置数据少,执行时间短,大大提高了 FPGA 芯片的灵活性.部分重配置技术基于对任务的空间划分,将不同的模块布局布线至器件的不同区域.图 2 所示为部分重配置示意图^[3].图中该设计将可重配置的 R 功能单独放在 FPGA 芯片的某个区域 A,依据任务需要可能涉及 4 种不同的功能,分别对应配置文件 R1~R4,在整个设计的运行过程中,可以随时将这 4 份配置文件下载到区域 A,实现重配置功能.

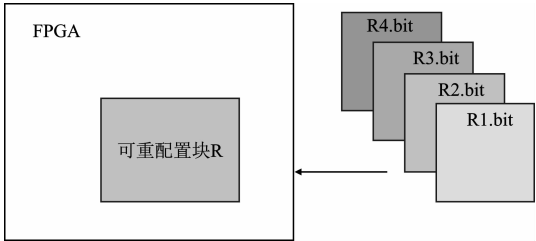


图 2 部分可重配置结构

不同开发工具实现分区布局布线的方式不同,本文基于 Vivado 实现分区布局布线和部分重配置.具体操作如下:

- (1)首先,从 Vivado IP 目录生成 SEM IP 内核后生成输出设计;
- (2)设计生成完成后,右键单击 sem_ultra_0 (sem_ultra_0.xci)并选择“打开示例设计”,选择示例项目目录 sem_ultra_0_example 存放到指定位置;
- (3)运行综合(Flow> Run Synthesis)生成参考设计的所有必需文件;
- (4)定义 RP Pblock.不需要运行实现,但必须打开综合设计以定义 RP 的 Pblock 约束;
- (5)打开工具中的设备视图,通过 Pblock 方式将除 SEM IP 之外的其他放置到指定的位置,保存 PR Pblock 约束.
- (6)在输出设计的 sem_ultra_0_example_design.v 基础上添加用户的目标设计(布局布线到可配置区)形成包含目标设计的设计文件;
- (7)将对于目标设计的区域约束、管脚约束等添加到原有的 XDC 文件;
- (8)编写 tcl 运行脚本文件,脚本文件中包含目录结构定义、分别对静态和可重配置模块进行综合、布局布线、生成配置文件等,生成的配置文件有完整设计的配置文件以及只包含目标涉及的配置文件.

可以依据需要选择完整下载或者部分下载.

4 故障注入原型系统设计

本文设计的基于 SEM IP 的单粒子故障注入原型系统架构如图 3,整个原型系统包含软件和硬件两部分.其中,硬件平台实现在 FPGA Board 上,采用的为 Xilinx 7 系列芯片 ARTIX-735TCSG324,主要功能包括故障注入、自动纠错、部分重置等;软件平台运行在上位机中,主要功能包括故障注入信号生成模块、SEM 控制模块、DUT 控制模块、FPGA 配置模块等.

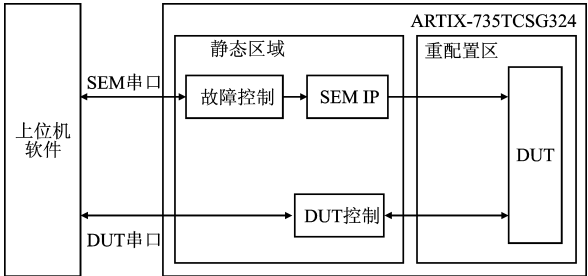


图 3 基于 SEM IP 的故障注入原型系统框架

故障注入实验分为两种模式:自动故障注入和手动故障注入.自动故障注入的实现过程为:先对 FPGA 进行配置,选好 SEM 串口或者 DUT 串口后,根据设置的测试次数与起始测试地址,开始进行测试.上位机软件将自动比对 DUT 返回的结果与期望结果是否一致,并统计 DUT 发生故障的次数和正常工作的次数.手动故障注入在对 FPGA 和串口的配置与自动故障注入相同,但是此种模式下设置测试次数为 0,起始地址可以进行设定,此时在 SEM 串口发送帧地址命令,然后在 DUT 串口中进行测试,随后在 SEM 串口中进行纠错,DUT 串口再发送复位命令.

5 实验结果及分析

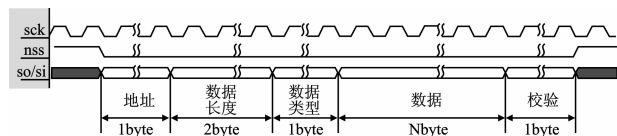
故障注入实验的对象是 PDHU 总线接口逻辑,其采用 SPI 接口进行命令接收和结果返回.本实验平台采用串口进行通信,因此对其接口进行了协议转换.

其中 SPI 命令发送模块用来向 PDHU 总线接口逻辑发送遥测参数采集指令如下:



地址: 0x56; 指令长度: 0x0000; 指令类型:

0x38;校验码:0x6E;



SPI 结果串口结果转发模块接收故障注入对象的 SPI 接口输出结果,并转为串口协议上传到 PC 机。期望被测软件返回的指令为:0x56+0x001E+0xF4+29 字节的 0x00+0x80+0x3C。上位机软件收到 DUT 返回的内容后与期望结果对比,从而判断结果是否正确。

1) 自动故障注入测试

• 故障注入地址未发生故障

设置起始测试地址为 0000D1F7A4,测试次数为 1,点击开始测试:

从上位机中的 DUT 串口输出来看,DUT 输出与期望一致,未发生故障。

• 故障注入地址发生故障

从上位机中的 DUT 串口输出来看,返回结果与正确结果不一致,故障注入导致实验电路发生故障。

2) 手动故障注入测试

• 故障注入地址未发生故障

SEM 串口先输入 O 命令纠正已注入的故障,再输入 I 命令进入故障注入态,然后输入 N 0000D1F7A4 对该地址进行故障注入。DUT 串口输入先选择 0x55AA55AA 对设计进行复位,然后再选择 0x55BB55BB 让 DUT 开始工作。

从上位机中的 DUT 串口输出来看,DUT 输出与期望一致,未发生故障。

• 故障注入地址未发生故障

SEM 串口先输入 O 命令纠正已注入的故障,再输入 I 命令进入故障注入态,然后输入 N 0000D1F7AF 对该地址进行故障注入。DUT 串口输入先选择 0x55AA55AA 对设计进行复位,然后再选择 0x55BB55BB 让 DUT 开始工作。

从上位机中的 DUT 串口输出来看,在该地址上进行故障注入使得实验电路功能异常。

6 结束语

FPGA 器件的单粒子效应,多发生在在轨运行

期间的空间环境中,为了模拟单粒子效应对其进行研究,本文针对 SRAM 型 FPGA,提出了一种基于 SEM IP 和部分重配置的故障注入方法;该方法将目标设计实现在可重配区,只向目标设计注入错误,避免了向其他模块注入错误,实现高效、可靠的单粒子故障注入;基于该方法,本文还搭建出一套完整的故障注入原型系统开展故障注入实验,实验结果证明该原型系统正确、有效,能够为空间环境中的单粒子翻转效应,构建类似的测试环境,对设计的安全性进行尽可能有效的评估,为电路设计的测试提供高效、可靠的地面验证平台。

参考文献:

- [1] EL-ARABY E, GONZALEZ I, EL-HAZAWI T. Exploiting partial run-time reconfiguration for high-performance reconfigurable computing[J]. ACM Transactions on Reconfigurable Technology and Systems, 2009, 1(4): Article No.: 21. DOI: 10.1145/1462586.1462590.
- [2] SCALERA S M, VAZQUEZ J R. The design and implementation of a context switching FPGA[C]//IEEE Symposium on FPGAs for Custom Computing Machines. Napa Valley, CA, USA: IEEE, 1998: 78-85. DOI: 10.1109/FPGA.1998.707884.
- [3] 何宾. Xilinx FPGA 权威设计指南[M]. 北京: 电子工业出版社, 2018.
HE B. Xilinx FPGA Definitive Design Guide[M]. Beijing: Electronic Industry Press, 2018.

作者简介:

王梦茹 女,(1991-),博士研究生,工程师。研究方向为 SRAM 型 FPGA 单粒子故障注入与安全性设计。

E-mail:wmmomo@163.com.

周珊 女,(1983-),博士研究生,高级工程师。研究方向为 FPGA/SOPC 验证方法。

薛盼盼 女,(1986-),硕士,工程师。研究方向为 FPGA 验证。

孔璐 女,(1986-),硕士,工程师。研究方向为 FPGA 验证。

王金波 男,(1978-),博士,研究员。研究方向为高可靠软件测试验证技术。