

数字太敏 SoC 的抗 SEU 加固设计

赵昌兵,付方发,肖立伊

(哈尔滨工业大学 微电子中心,黑龙江 哈尔滨 150001)

摘 要: 针对航天应用中数字式太阳敏感器高可靠性的要求,对基于 Leon3 处理器平台的数字式太阳敏感器 SoC 在 RTL 级进行抗 SEU 加固设计. 出于加固后整个系统速度和面积的考虑,本文针对 SoC 中不同部分采取不同的加固方法,综合使用了三模冗余、EDAC(Error Detection And Correction)电路、CPU 流水线重启和 Cache 强制不命中容错方法. 使用故障注入的方法测试寄存器文件加固后系统的软错误敏感性,对寄存器加固效果进行评估. 并在 FPGA 上进行原型实现,对比加固前后的速度及开销情况.

关键词: 数字太敏; SoC; SEU; 故障注入; FPGA

中图分类号: TN386

文献标识码: A

文章编号: 1000-7180(2017)01-0001-05

SEU-Tolerant Design for Digital Sun Sensor SoC

ZHAO Chang-bing, FU Fang-fa, XIAO Li-yi

(Microelectronics Center, Harbin Institute of Technology, Harbin 150001, China)

Abstract: For the high reliability of digital sun sensor in aerospace applications, the SEU-tolerant design for Leon3-based digital sun sensor SoC in RTL level was fulfilled. In considerations of the speed and size of the entire system, we adopt various strengthening methods for different parts of SoC, including triple modular redundancy, EDAC (Error Detection And Correction) circuit, pipeline restart of CPU, forcing cache to miss, etc. in order to evaluate the strengthening effect of registers, we need the soft error sensitivity getting from the fault injection test on the system with register file strengthened. Then, the prototype was implemented in FPGA and compared the speed and overhead with non-strengthened design.

Key words: digital sun sensor; SoC; SEU; fault injection; FPGA

1 引言

随着微小卫星事业的日益发展,数字式太阳敏感器 SoC(以下简称数字太敏 SoC)因为其体积小、重量轻、功耗低等一系列优点^[1],被广泛应用于人造卫星等航天领域,它可以实时提供太阳输出角,帮助卫星系统进行精确的姿态控制和轨道调整^[2]. 在太空辐射环境中,数字电路系统很容易受到单粒子翻转(SEU)的影响,使电路中的时序单元存储的值发生翻转,导致电路行为异常或者计算结果错误. 数字太敏 SoC 计算结果错误,将导致姿态控制系统控制错误,发生严重后果,对数字太敏 SoC 进行抗 SEU 加固设计尤为重要.

SoC 通常在片内集成了处理器、存储器以及诸多外设 IP,内部采用总线互联. 对不同部分的加固需要考虑不同的容错方法. 目前常用在 RTL 级的加固方法主要有三模冗余、EDAC 编码等. 对处理器的容错还可以使用流水线重启、Cache 强制不命中等方法.

国内外对于面向空间应用的高可靠 SoC 设计都有研究,如文献[3]使用三模冗余、片上 EDAC、流水线重启和强制 Cache 不命中等措施实现了容错的 Leon3 处理器;文献[4]提出使用具有自主知识产权的容错 IP 核进行高可靠的 SoC 设计,并使用加固型标准单元库实现了一款 32 位的 RISC 处理器 SoC 芯片. 本文将首先分析各种容错方法的优缺点

及适用性,权衡加固后的面积和速度,综合使用各种容错方法,对数字太敏 SoC 进行容错设计,使用仿真软件故障注入的方法对加固效果进行评估,最后在 FPGA 上实现,分析加固后的速度和资源占用等情况.

2 SoC 加固方法

对 SoC 的抗 SEU 加固设计可以从很多层面上进行,比如可以采用在芯片外加物理屏蔽的方式,还可以在电路的 RTL 级设计时加入容错的冗余结构,也可以在实现时使用容错的底层逻辑单元^[5]. 在 RTL 级的容错主要使用加入冗余结构的方法,常用的有三模冗余和编码冗余.

三模冗余是最常用的一种容错方法,它把寄存器复制三份,通过一个多数表决器输出,当三个寄存器有两个以上发生翻转时,结果错误,引起电路速度的损失为一个多数表决器的延时.

编码冗余通过把寄存器当做数据位进行编码,加入冗余的校验位. 常用的 EDAC 编码为扩展汉明码,它可以“纠一检二”. 相比三模冗余,其在寄存器数量较大时有明显的面积上的优势,但是对分布式的寄存器进行编解码会大大增加布线难度,故而汉明码只适用于排列整齐的寄存器堆.

另外,对 SoC 来说,可以在功能上设计容错策略. 比如针对处理器的流水线重启和 Cache 强制不命中及发生不可纠正错误时的系统复位,对于外设 IP 的发生不可纠正错误时产生中断,进入异常处理程序等. 功能上的容错方案针对具体设计,设计实现的功能不同,容错方案随之变化.

3 数字太敏 SoC 加固设计

3.1 数字太敏 SoC 结构

数字太敏 SoC 的结构如图 1 所示,其设计基于 Leon3 处理器平台.

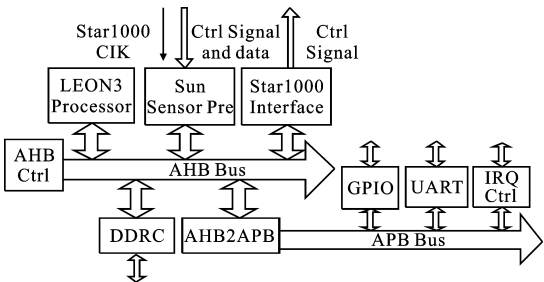


图 1 数字太敏 SoC 结构图

Leon3 处理器是基于 SparcV8 体系架构的 32

位 RISC 处理器,整型单元有七级流水,并采用指令 Cache 和数据 Cache 分离的哈佛结构. 整个 SoC 平台内部的互联遵循 AMBA2. 0 总线规范^[5],总线上的设备使用“即插即用”机制,方便 SoC 的设计. 数字太敏 SoC 中各 IP 核说明如表 1 所示.

表 1 数字太敏 SoC 各 IP 核说明

IP 核名称	说明
LEON3 Processor	Leon3 处理器
DDRC	DDR 控制器,DDR 存储 SoC 软件实现部分的程序(针对 XILINX ML510 开发板,若使用其他原型平台实现,可去掉)
Star1000 Interface	Star1000 图像传感器的 AHB 接口
Sun Sensor Pre	太阳敏感器数据预处理模块
AHB Ctrl	AHB 控制器,实现总线仲裁和“即插即用”
AHB2APB	AHB 总线到 APB 总线的总线桥
UART	串口,实现与外部的交互
IRQ Ctrl	中断控制器,实现中断的处理和仲裁
GPIO	通用输入输出端口,实现与外部交互

数字太敏 SoC 提供 Star1000 图像传感器的控制接,接收 Star1000 图像传感器的控制信号及图像像素数据. 数字太敏 SoC 中太阳敏感器像素预处理模块对像素数据进行预处理并通过中断将计算好的中间数据传递给软件处理部分,最后计算出太阳输出角.

3.2 数字太敏 SoC 加固

对数字太敏 SoC 进行加固设计首先需要分析各 IP 模块对 SEU 敏感的部分,有针对的选择合适的容错策略.

数字太敏 SoC 中对 SEU 敏感的部分有 LOEN3 处理器内部寄存器堆、cache 存储体和寄存器及其他模块中的 SRAM 和寄存器.

3.2.1 寄存器文件加固

数字太敏 SoC 的 Leon3 处理器寄存器窗口数量配置为 8 个,加上全局寄存器,一共包括 136 个 32 bits 的寄存器. 对这样数量巨大的寄存器组采取三模冗余的加固方式会增加大量的冗余寄存器,进而大大增加芯片面积,考虑到寄存器组排列规整,采用汉明码对寄存器文件进行加固,考虑缩减译码逻辑延时,将 32 位分为两组,每组 16 位采用(16, 22)汉明码进行编码.

寄存器文件为两个读端口和一个写端口的三端口寄存器文件,该三端口寄存器内部由两个双端口 RAM 组成,如图 2 所示.

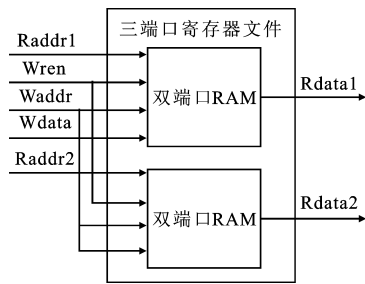


图 2 三端口寄存器文件

在 Leon3 的七级流水中,寄存器文件中的数据在 RA 段被读出,如果操作数来自寄存器文件,则经过一个多路选择器,该值被寄存在操作数寄存器中. 如果从寄存器文件读出的数据经过解码后再作为操作数进行运算,解码的过程会拖慢整个流水线的速度. 针对此问题,采用前瞻译码机制,即在 EX 段运算的同时进行译码,没有错误则不影响流水线执行;若发生可纠正错误,将纠正后的数据写回寄存器文件,防止错误积累,并重启流水线,从出错指令重新执行;发生不可纠正错误,复位整个系统. 实现该功能会在流水线上引入新的寄存器,数量为 225 位.

发生可纠正错误时,简单的把出错指令的 PC 值回推到 FE 段并不能实现流水线重启. SparcV8 体系结构定义在发出跳转指令后,下条指令并不会马上跳转到目的地址执行,而是有一个跳转延时,如果跳转延时的指令为有效指令,该条指令出现可纠正错误,简单的流水线重启会使程序顺序执行下去. 为解决该问题,需要记录下一个有效的 PC 值. 发生可纠正的寄存器文件 SEU 错误时,流水线重启分为两个周期:

- 第一周期:
- (1)废除流水线指令;

(2)把纠正的寄存器文件数据写入寄存器文件,记录下一个有效的 PC 值;

(3)把当前 PC 回推到 FE 段.
- 第二周期:
- (1)将下一个有效 PC 回推到 FE 段.

发生一位 SEU 时,流水线的时空表如表 2 所示.

借鉴异常的处理方法,直接利用发生异常时 XC 段的的全局指令取消信号 annul_all,达到清空流水线指令的目的.

3.2.2 cache 存储体加固

Cache 子系统由 Icache 控制器、

表 2 发生一位 SEU 时流水线时空表

IF	I1	I2	I3	I4		I2	I3	I4
ID		I1	I2	I3	I4	Flush	I2	I3
RA			I1	I2	I3	I4	Flush	I2
EX				I1	I2	I3	I4	Flush
MEM					I1	I2	I3	Flush
XC						I1	I2	Flush
WR							I1	Update

Dcache 控制器、cache 子系统与 AHB 总线的主设备接口 Acache 以及 cache 存储体组成.

LEON3 有一个高度可配置的 cache 系统,数字太敏 SoC 的 cache 系统配置如表 3 所示.

表 3 数字太敏 SoC 中 cache 配置情况

	sets	set size/kbytes	line size/bytes
Icache	4	8	32
Dcache	4	4	16

Cache 存储体包含两类存储单元,一种是数据存储器,另一种是 TAG 存储器. 对 cache 存储器的加固,考虑采用加循环冗余校验码,在数据存储体和 TAG 存储体都加 3 位的循环冗余校验码,修改 cache 命中机制,在循环冗余校验发生错误时,采取强制不命中的策略,使其从主存中取得数据或者向主存中写入数据并更新 cache.

修改后的 cache 命中机制如图 3 所示,圆圈标示的部分为在原来基础上增加的部分.

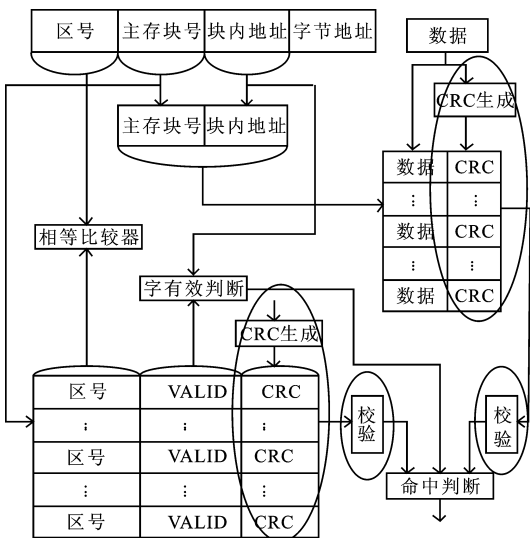


图 3 加固后的 cache 命中机制

可见,存储体增加了 CRC 编码,命中判断增加了两个不命中条件,数据存储体和 TAG 存储体的任何一个 CRC 校验出错,即不命中.

3.2.3 寄存器加固

一个 SoC 系统中并不是任何一个寄存器发生

SEU 错误都会引起系统故障,软错误敏感性(soft error sensitivity, SES)定义为系统发生故障数占故障注入总数的比例^[6],对系统中的寄存器进行遍历式的故障注入,便可以使用 SES 来表示一个系统中发生 SEU 会引起系统故障的寄存器占所有寄存器的比例.

对寄存器最简单实用的方法就是三模冗余,本文将采取此方法对寄存器进行加固,但该方法对速度及面积都有不利影响.为进行有效的加固,节省不必要的面积开销,有必要得到各 IP 核对于一位 SEU 的 SES 值,抓住主要矛盾,重点对 SES 较大的模块进行加固.

本文使用文献[7]的故障注入工具对各 IP 核的所有寄存器进行了 20 次遍历式一位 SEU 故障注入,其中,因为流水线重启会在增加新的流水线寄存器,在进行 SES 评估时这些新引入的寄存器也必须包括在内,所以,LEON3 处理器 IP 核为寄存器文件加固完成的版本.实验发现 AHB2APB 桥及 APB 总线上的从设备包括 UART、GPIO、IRQ Ctrl 对一位 SEU 的 SES 极其接近 0.这与系统的实际情况相符,系统的动作大部分在 AHB 总线上进行,APB 总线的上执行的动作极少.所以不对这些 IP 核进行加固.

实验得到各 IP 核中寄存器对于一位 SEU 的 SES 如表 4 所示.

表 4 各 IP 核寄存器对一位 SEU 的 SES 值

IP 核名称	SES/%
LEON3 Pro- 流水线寄存器(加固)	16.763
cessor Cache 子系统寄存器	18.362
Star1000 Interface	89.153
Sun Sensor Pre	52.264
AHB Ctrl	15.789

表 4 中的 IP 核在数字太敏 SoC 工作时一直都

会处于工作状态,SES 较高,所以加固的重点放在这些 IP 核上.对表 4 中所有 IP 核的寄存器进行加固.

4 验证方法和结果分析

4.1 验证方法

对加固后系统的验证主要分四个部分:

(1)寄存器文件流水线重启的功能验证.验证方法为:在操作数来源于寄存器文件的指令处,对寄存器文件输出数据使用 Modelsim 仿真软件的 force 命令注入一位 SEU 错误,观察波形;

(2)Cache 强制不命中机制功能验证.验证方法为:持续命中状态下,在 cache 存储体的输出数据上使用 Modelsim 仿真软件的 force 命令注入一位 SEU 错误,原本命中状态变为不命中状态即为加固成功;

(3)三模冗余加固效果分析.计算加固前后寄存器 SEU 引起的系统故障率,进行对比;

(4)加固前后资源占用及速度对比.验证方法为选择 Xilinx ML510 为实现的原型目标板,对加固前后的设计分别使用 ISE 进行综合及布局布线后静态时序分析,分析加固前后资源占用情况及速度.

4.2 结果分析

4.2.1 寄存器文件流水线重启的功能验证

在操作数来源于寄存器文件中时,使用 Modelsim 在寄存器文件的输出数据上注入一位的 SEU 翻转故障,选择跳转指令的下一条有效指令进行故障注入,观察流水线重启后,是否仍然能跳转到目的地址执行指令,进而验证流水线重启不会影响原来程序的执行流程,可以看到波形如图 4 所示.

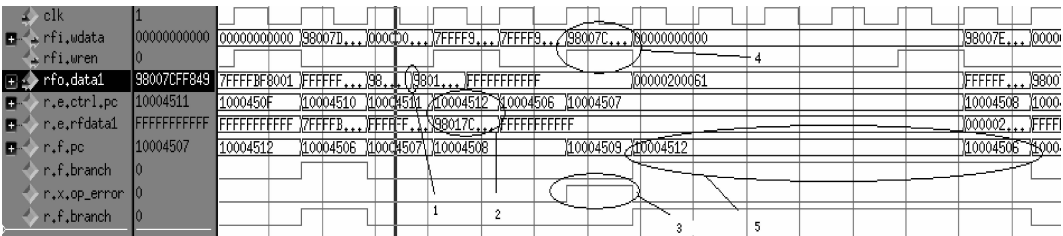


图 4 寄存器文件一位 SEU 故障注入波形图

从波形可以看出,在 1 处即寄存器文件输出数据注入一位 SEU 故障,引起 2 处即 PC 值为 0x10004512 的指令的 EX 段寄存器输出数据错误,进而引起 3 处即该指令 XC 级的 op_error 置 1,引起流水线重启,可见从 PC 值为 0x10004512 的出错指令处重新开始执行,并且下一个 PC 值为

0x10004506,为跳转目的地址的 PC 值,另外,4 处可见在出错指令的 XC 段实现了将纠正的数据写回寄存器文件,说明功能正确.

4.2.2 Cache 强制不命中机制功能验证

选择对 Icache 的数据存储体输出数据进行故障注入,波形图如图 5 所示.

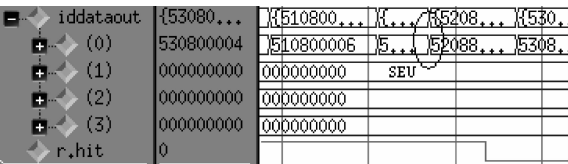


图 5 Icache 数据存储体故障注入验证结果

可见,注入故障后,cache 在下一时钟上升沿处变为不命中状态,说明功能正确.

4.2.3 三模冗余加固效果验证

根据文献[9],常规 SRAM 型存储器在空间发生 SEU 的频率为 $0.5\text{E-}4(\text{次}/\text{Mb} \times \text{天})$,在太阳活动剧烈时发生概率可能会提高一个数量级,所以选取发生 SEU 的概率 P 为 $0.5\text{E-}6(\text{次}/\text{位} \times \text{天})$ 进行计算.

系统中发生 SEU 会引起故障的寄存器位数为 N ,则 N 中的任何一位都不发生 SEU,系统便不会发生错误. N 可以由式(1) 计算出.

$$N = \sum_{i=1}^{N_i} R_i \times S_i$$

(1)

式中, N_i 为 IP 核数量, R_i 为第 i 个 IP 核寄存器总位数, S_i 为第 i 个 IP 核的 SES.

各 IP 核寄存器数量如表 5 所示.

表 5 各 IP 核寄存器数量

IP 核名称		SES
LEON3 Pro-processor	流水线寄存器(加固)	1 246+225
	Cache 子系统寄存器	4 063
Star1000 Interface		63
Sun Sensor Pre		3 753
AHB Ctrl		64

其中,流水线寄存器包括未加固流水线寄存器加上加固引入的寄存器. 由表 5 及表 4 中数据,根据式(1)可以计算出 N 为 3 021. 进而可以由式(2) 计算出未加固时寄存器发生 SEU 引起系统故障的概率 P_1 为 $1.51\text{E-}3$.

$$P_1 = 1 - (1 - P)^N$$

(2)

每个三模冗余后的寄存器在发生两个以上 SEU 时输出结果错误,所以可由式(3) 计算出该出错概率 P_{TMR} 为 $7.499\text{E-}13$.

$$P_{\text{TMR}} = C_3^1 \times P^2 \times (1 - P) + P^3$$

(3)

使用 P_{TMR} 替换式(2) 中的 P 即可计算出三模冗余加固后系统的故障率 P_{fi} 为 $2.27\text{E-}9$. 可见, P_{fi} 相对 P_1 减小了 6 个数量级,说明加固效果十分显著.

4.2.4 加固前后资源占用及速度对比

使用 Xilinx ML510 开发板作为数字太敏 SoC 的原型验证平台,搭建了验证系统. 得到加固前后整体的资源占用及速度如表 6 所示.

表 6 加固前后资源速度对比

	Registers	LUTs	BRAM/FIFO	速度/MHz
加固前	15 796	24 766	37	80. 212
加固后	34 849	47 371	38	80. 160

可见,加固后资源变大,速度变化不大. 但是表 6 所示的资源占用中包含了功能验证部分,该部分并未进行加固.

加固前后寄存器数量差 19 053 即为整体加固引入的寄存器数量,它等于寄存器文件加固前的整个系统寄存器数量 9 189 乘以 2,再加上寄存器文件加固引入的寄存器数量 225 乘以 3. 综合结果与系统实际情况相符.

5 结束语

本文针对数字太敏 SoC 中特定的结构采取了针对性的加固措施. 采用三模冗余对寄存器进行加固,使用 EDAC 电路对 SRAM 加固,处理器寄存器文件采用 EDAC 编码与流水线重启结合的方式实现了发生可纠正 SEU 错误时的流水线重启和发生不可纠正错误时的系统复位,cache 存储体增加 CRC 校验码,CRC 校验错误时,强制不命中. 整个系统加固后可以完全屏蔽一位的 SEU 错误,同时将由寄存器发生 SEU 引起的系统故障率降低了 6 个数量级. 增加的资源为冗余寄存器和表决器及实现流水线重启和 cache 强制不命中增加的逻辑资源. 性能基本没有损失.

参考文献:

[1] 傅永杰. 数字太敏 SoC 设计[D]. 哈尔滨:哈尔滨工业大学, 2013.

[2] Ning Xie, Albert J P Theuwissen, Bernard Büttgen. Micro-digital sun sensor: an imaging sensor for space applications [C] // ISIE 2010. Italy, Bari, 2010: 3362-3365.

[3] Gaisler J. A portable and fault-tolerant microprocessor based on the SPARC v8 architecture[C]//Dependable Systems and Networks, DSN 2002, Proceedings International Conference on. USA, Washinton, IEEE, 2002: 409-415.

国科学院计算技术研究所, 2014.

[6] Patil H, Pereira C, Stallcup M, et al. PinPlay: a framework for deterministic replay and reproducible analysis of parallel programs[C]//CGO 2010. Canada, Toronto, 2010:2-11.

[7] Bhansali S, Chen W K, de Jong S, et al. Framework for instruction-level tracing and analysis of program executions[C]//VEE 2006. Canada, Ottawa, 2006: 154-163.

[8] 应欢, 王东辉, 武成岗, 等. 适用于商用系统环境的低开销确定性重放技术[J]. 吉林大学学报(工学版), 2017, 49(1):1782-1790.

[9] Courtois P J, Heymans F, Parnas D L. Concurrent Control with ‘eaders’ and ‘writers’ [J]. Commun. ACM, 1971, 14(10):667-668.

[10] Bienia C, Kumar S, Singh J P, et al. The PARSEC benchmark suite: characterization and architectural implications [C]//PACT 2008. Canada, Toronto, 2008:72-81.

作者简介:

应欢 女, (1988-), 博士研究生. 研究方向为并行程序调试. E-mail:yinghuan1022@126.com.

王东辉 男, (1973-), 博士生导师. 研究方向为 VLSI 信号处理.

王喆 男, (1990-), 博士研究生. 研究方向为动态编译与软件安全.

(上接第 5 页)

[4] 辛明瑞, 时晨, 高德远, 等. 面向空间应用的片上系统集成技术研究[J]. 微电子学与计算机, 2006, 23(6): 194-197.

[5] GRLIB IP Core User’s Manual (Version 1. 2. 0 - B4121)[M]. New York: Aeroflex Gaisler Inc. 2012.

[6] Niu G, Krithivasan R, Cressler J D, et al. A comparison of SEU tolerance in high-speed SiGe HBT digital logic designed with multiple circuit architectures[J]. Nuclear Science, IEEE Transactions on, 2002, 49(6): 3107-3114.

[7] 武振平, 付方发, 肖立伊. 基于 VHDL 故障注入的处理器敏感性分析[J]. 微电子学与计算机, 2012, 29(10): 51-54.

[8] 黄海林, 唐志敏, 许彤. 龙芯 1 号处理器的故障注入方法与软错误敏感性分析[J]. 计算机研究与发展, 2006, 43(10): 1820-1827.

[9] 马兴瑞, 张永维, 白照广. 实践五号卫星及其飞行成果[J]. 中国航天, 1999, 21(11):3-8.

作者简介:

赵昌兵 女, (1992-), 硕士. 研究方向为先进集成系统与 SoC. E-mail:hitzcb@163.com.

付方发 男, (1984-), 博士, 讲师. 研究方向为片上网络体系结构研究.

肖立伊 女, (1961-), 博士, 教授, 博士生导师. 研究方向高可靠集成电路设计、SoC/IP 核设计与标准化.