文章编号:1671-4598(2016)06-0298-04 DOI:10.16526/j.cnki.11—4762/tp.2016.06.081 中图分类号:TP181 文献标识码:A

一种高可靠宇航控制器设计及可靠性评估

王 豪,程利甫,刘 博,刘 攀
(上海航天电子技术研究所,上海 201109)

摘要:将8051、存储器等IP核集成在FPGA内部,可实现宇航控制器高可靠、小型化的应用需求。但FPGA在空间环境中容易发生单粒子翻转事件(SEU),影响系统正常功能,常采用在FPGA内部进行三模冗余(TMR)设计;针对三模冗余系统无法纠正存储区中发生的SEU故障,提出了一种采用三模冗余架构并对FPGA配置区域进行刷新重载的解决方案,同时采用马尔可夫模型对该设计方案进行了可靠性评估和仿真;结果表明,采用该设计架构的宇航控制器具有较高的可靠性与安全性,可实现飞行器的长期稳定运行。

关键词:8051核;宇航FPGA;单粒子翻转;三模冗余;回读刷新;可靠性

Design and Reliability Evaluation of Controller with High Reliability Used for Aerospace

Wang Hao, Cheng Lifu, Liu Bo, Liu Pan
(Shanghai Aerospace Electronic Technology Institute, Shanghai 201109, China)

Abstract: In order to meet the high-dependability requirement of electronic equipment for aerospace, a new method which integrating 8051 IP core and storage IP core into FPGA is proposed. After analyzing the shortcoming of traditional Triple Module Redundancy (TMR) design aiming to migrate the SEU effect on FPGA, a fault tolerance method based on TMR and readback-scrubing the configuration-data of FPGA is used. Then the reliability of this architecture is achieved in detail by Matlab tool with Markov model. Simulation results show that this FPGA architecture has higher reliability, which can meet the requirement of Aerospace electronic controller.

Keywords: 8051 IP core; Aerospace FPGA; SEU; triple module redundancy; readback and scrub; reliability

0 引言

长期以来,8051单片机以其性价比高、体积小、功能灵活等方面的独特优点被广泛应用于宇航产品中。但受其内部资源的限制,8051单片机需要在片外扩展众多硬件资源以满足不同应用的需求[1],其功能如图1所示。

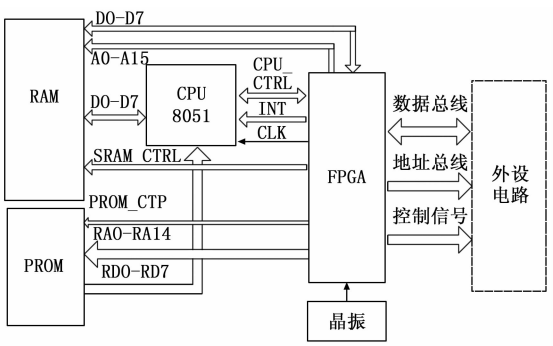

图1 典型8051宇航控制器功能框图

随着EDA(Electronic Design Automation,电子设计自动化)技术的发展,可重构的嵌入式CPU核—DW8051核、功能复杂的IP(Intellectual Property,知识产权)核及各种功能强大的EDA工具的出现,使得将CPU(Central Processing Unit,中央处理器)、存储器和一些外围电路集成到一个芯片——FPGA(Field Programmable Gate Array,现场可编程门阵列)中成为可能[2-3]。图2所示为集成后的原理框图,集成后的系统较之前体积大幅减小。

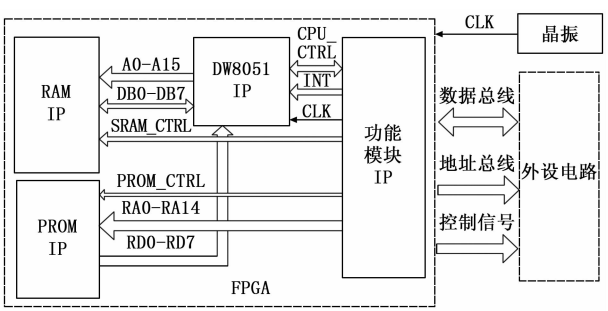

图2 FPGA内部嵌入IP核的控制器设计

采用FPGA进行系统集成可大幅缩减系统体积,但FPGA特别是可重构型静态存储器(static random access memory,SRAM)型FPGA应用于空间环境中存在抗空间辐射能力差,容易发生SEU(Single Event Upset,单粒子翻转)[4-5]故障,对卫星功能造成了不同程度的故障,因此必须采取一定的抗辐加固措施以提高其可靠性。

下文提出一种内嵌8051IP核并采取抗辐加固措施的宇航控制器设计方案并对其可靠性进行评估。

1 采用8051IP核的高可靠控制器设计

SRAM型FPGA内部的配置区——配置存储器,功能区——块存储器、触发器等都是单粒子反转的敏感区。当一个高能带电粒子穿过灵敏区时,将会使FPGA器件内部导通管截止、截止管导通,引起器件逻辑状态的翻转——即单粒子翻转[6]。

收稿日期:2015-11-30; **修回日期**:2016-01-04。

作者简介:王 豪(1989-),男,河南新安人,硕士,工程师,主要从事高可靠星载计算机方向的研究。

设计中常采用三模冗余（triple module redundancy，TMR）[7]技术对要在 FPGA 内实现的硬件设计进行保护。

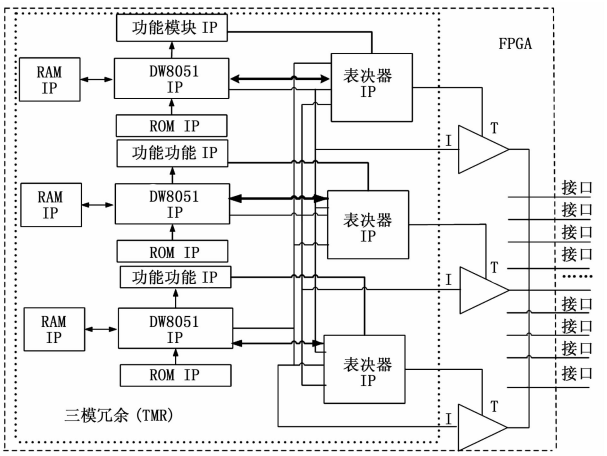

图 3　三模冗余系统原理框图

图 3 所示为采用三模冗余架构的 FPGA 系统原理框图，可以看出这种方法通过嵌入冗余处理机制到用户应用来屏蔽故障，从而获得正确的输出，本质上是一种利用硬件冗余或信息冗余进行故障屏蔽的容错方法。

然而，冗余容错方法无法改变 FPGA 的配置内容，对于发生在配置存储器中的 SEU 并无纠正能力[8]，若 SEU 积累最终将使得 TMR 失效，导致故障发作。

针对三模冗余（TMR）系统无法纠正存储区中发生的 SEU 故障，本文提出一种三模冗余加回读刷新的解决方案，应对空间 FPGA 单粒子翻转。

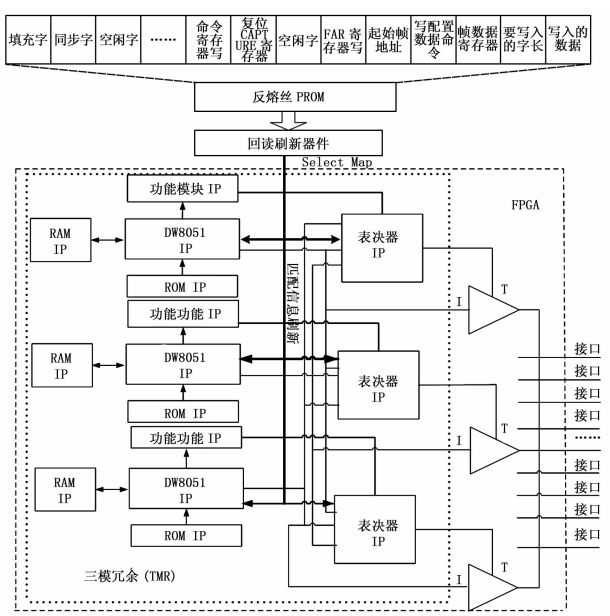

图 4　采用三模冗余与回读刷新架构 FPGA 功能框图

由于 SRAM 型 FPGA 配置信息存储于 SRAM 单元中，可对存储单元进行回读刷新操作纠正发生翻转的存储单元。回读刷新是通过回读刷新器件来实现的，有两种工作模式：回读和刷新。回读模式[9]下该器件读取 FPGA 内配置存储区的数据，并与存储在 PROM 中的原始配置数据进行比较，当发现数据不一致的情况时，就意味着配置存储器单元发生了 SEU，进而将 PROM 中存储的原始配置文件重新写入 FPGA。刷新模式[10]下不管 FPGA 有没有发生 SEU 均周期对配置存储区进行刷新。采用回读刷新加三模冗余架构的 FPGA 系统原理如图 4 所示。其中，PROM 芯片内部存储 FPGA 的配置信息，该器件采用反熔丝工艺不会受空间 SEU 干扰；回读刷新器件亦采用反熔丝工艺对空间 SEU 免疫；FPGA 内部电路采用 TMR 设计。

2　可靠性分析

系统可靠性是指系统在规定条件下和规定时间内完成规定功能的能力。由于系统是冗余系统，系统发生故障是余度性能降级的动态过程，利用马尔可夫过程理论能够对余度系统进行精确的可靠性建模分析，较为真实地描述系统的实际工作过程[11-12]。为方便讨论及建模，将图 4 所示的回读刷新加 TMR 的 FPGA 系统可简化为如图 5 所示的逻辑框图；回读刷新器件作为 SEU 故障修复模块，周期地对 FPGA 内部配置存储区进行刷新。

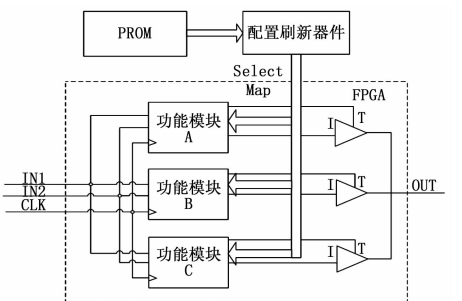

图 5　简化后三冗余及回读刷新 FPGA 系统框图

采用 TMR 的系统具有 $2^3=8$ 种状态，当一个模块发生故障时，不会影响系统的正常工作，而当失效模块数≥2 时，系统失效。这个状态可以视为马尔可夫吸收态。假设每个模块的失效率都相同均为 λ，修复率为 μ。

则根据可靠性分析理论[13]，若某模块在时刻 t 正常工作，则在 $t+\Delta t$ 时刻发生常规故障的概率为 $p=1-e^{-\lambda\Delta t}$，当 $\Delta t\to 0$ 该故障概率可简化为 $\lambda\Delta t$。

基于以上假设，在周期对 FPGA 配置区进行定时刷新且考虑共模故障影响下的三模冗余系统的马尔可夫模型状态转移如图 4 所示，其马尔可夫状态可描述如下：

1）状态 S1—“111”表示 A、B、C3 个模块均未受到 SEU 影响、功能均正常；

2）状态 S2—“110”表示某时刻 C 模块受到 SEU 影响，功能异常且翻转单元暂未得到刷新纠错。A、B 模块正常，经三取二表决后系统仍能正常工作。

3）状态 S3—“101”表示某时刻 B 模块受到 SEU 影响，功能异常且翻转单元暂未得到刷新纠错。A、C 模块正常，经三取二表决后系统仍能正常工作。

4）状态 S4—“011”表示某时刻 A 模块受到 SEU 影响，功能异常且翻转单元暂未得到刷新纠错。B、C 模块正常，经三取二表决后系统仍能正常工作。

5）状态 S5—“100”表示某时刻 B、C 模块受到 SEU 影响，功能异常而且翻转单元暂未得到刷新纠错，经三取二表决后系统功能失效。

6）状态 S6—“001”表示某时刻 A、B 模块受到 SEU 影

响，功能异常而且翻转单元暂未得

到刷新纠错，经三取二表决后系统功能失效。

7）状态 S7—“010”表示某时刻 A、C 模块受到 SEU 影响，功能异常而且翻转单元暂未得到刷新纠错，经三取二表决后系统功能失效。

8）状态 S8—“000”表示某时刻 A、B、C 模块均受到 SEU 影响，功能异常且翻转单元暂未得到刷新纠错，系统功能失效。

记 $P_i(t)=P(X(t)=i)$，表示 t 时刻系统处于状态 i 的概率，$i\in\{1,2,3,\ldots,8\}$，令 $P(t)=[P_1(t),P_2(t),\ldots,P_8(t)]$，则 $P(t)$ 满足状态方程：$P'(t)=AP(t)$，其中，A 为状态转移密度矩阵，有状态转移图可知：

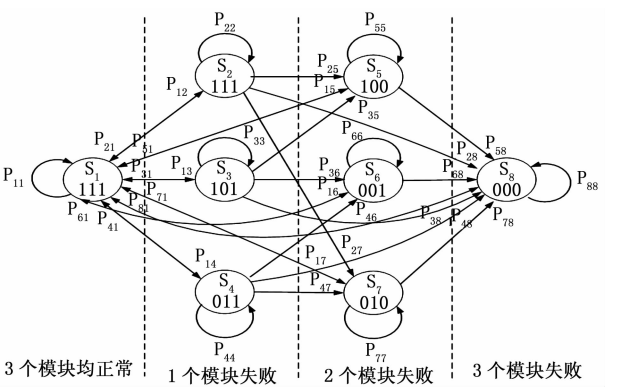

图 6 采用 TMR 和回读刷新的 FPGA 系统的马尔可夫状态转移图

$$A=\begin{bmatrix}
-(3\lambda+3\lambda^2+\lambda^3) & \lambda & \lambda & \lambda & \lambda^2 & \lambda^2 & \lambda^2 & \lambda^3\\
\mu & -(\mu+2\lambda+\lambda^2) & 0 & 0 & \lambda & 0 & \lambda & \lambda^2\\
\mu & 0 & -(\mu+2\lambda+\lambda^2) & 0 & \lambda & \lambda & 0 & \lambda^2\\
\mu & 0 & 0 & -(\mu+2\lambda+\lambda^2) & 0 & \lambda & \lambda & \lambda^2\\
\mu^2 & 0 & 0 & 0 & -(\mu^2+\lambda) & 0 & 0 & \lambda\\
\mu^2 & 0 & 0 & 0 & 0 & -(\mu^2+\lambda) & 0 & \lambda\\
\mu^2 & 0 & 0 & 0 & 0 & 0 & -(\mu^2+\lambda) & \lambda\\
\mu^3 & 0 & 0 & 0 & 0 & 0 & 0 & -\mu^3
\end{bmatrix} \tag{1}$$

并由此可得微分方程如下：

$$\begin{cases}
P'_1(t)=-(3\lambda+3\lambda^2+\lambda^3)P_1(t)+\mu P_2(t)+\mu P_3(t)+\mu P_4(t)+\mu^2 P_5(t)++\mu^2 P_6(t)+\mu^2 P_7(t)+\mu^3 P_8(t)\\
P'_2(t)=\lambda P_1(t)-(\mu+2\lambda+\lambda^2)P_2(t)\\
P_3(t)=\lambda P_1(t)-(\mu+2\lambda+\lambda^2)P_3(t)\\
P'_4(t)=\lambda P_1(t)-(\mu+2\lambda+\lambda^2)P_4(t)\\
P'_5(t)=\lambda^2 P_1(t)+\lambda P_2(t)+\lambda P_3(t)-(\mu^2+\lambda)P_5(t)\\
P'_6(t)=\lambda^2 P_1(t)+\lambda P_3(t)+\lambda P_4(t)-(\mu^2+\lambda)P_6(t)\\
P'_7(t)=\lambda^2 P_1(t)+\lambda P_2(t)+\lambda P_4(t)-(\mu^2+\lambda)P_7(t)\\
P'_8(t)=\lambda^3 P_1(t)+\lambda^2 P_2(t)+\lambda^2 P_3(t)+\lambda^2 P_4(t)+\lambda P_5(t)+\lambda P_6(t)+\lambda P_7(t)-\mu^3 P_8(t)
\end{cases} \tag{2}$$

A 和 $P(t)$ 代入方程 $P'(t)=AP(t)$ 中，并代入初始条件 $P(0)=[1,0,0,\ldots,0]$，可得到 t 时刻各个状态的概率，从而求得该系统的可靠度 $R(t)$ 和安全度 $S(t)$[14]：

$$R(t)=p_1(t)+p_2(t)+p_3(t)+p_4(t) \tag{3}$$

$$S(t)=R(t)=p_1(t)+p_2(t)+p_3(t)+p_4(t) \tag{4}$$

3 仿真结果分析

对于 $P(t)$ 的状态方程 $P'(t)=AP(t)$，可以通过 Laplace 变换的方法求得其解析解，进而求得系统的可靠度和安全度，但其计算工作量相当庞大[15]，为此，采用 Matlab 中的求解微分方程的 Ode45 指令进行仿真计算[8]。其中单粒子翻转故障率 λ 可参照表 1 所示 Xilinx 公司 FPGA 单粒子翻转率[16]。

表 1 Xilinx 公司 FPGA 单粒子翻转率

芯片	容量/bits	重离子翻转率/(bit-1 day^{-1})	太阳质子翻转率/(day^{-1})	总翻转率/(day^{-1})
XQVR300	1.6×106	4.39E−08	4.16E−01	0.49
XQVR1000	5.8×106	4.39E−08	4.16E−01	0.67
XQR2V3000	10×10^6	8.24E−08	2.42E−01	1.07
XQR2V6000	21×10^6	8.24E−08	2.42E−01	1.97

由表 1 可以看出随着 FPGA 容量的增加，单粒子翻转率也随之增加。系统修复率 μ 与回读刷新的频率有关，以 5 s、10 s、15 s、1 min、3 min 的刷新周期为例对采用 Virtex2 系列 XQR2V3000 型 FPGA 系统的可靠度、安全度进行分析。

表 2 λ=1.07 day−1 时 参数 μ 对系统可靠性安全性影响

μ	R/S	时间/h						
		0	4 320	8 640	17 280	25 920	43 200	86 400
1.2e−4	R	1	1.000 0	0.999 9	0.999 9	0.999 8	0.999 8	0.999 6
	S	1	1.000 0	0.999 9	0.999 9	0.999 8	0.999 8	0.999 6
6e−5	R	1	0.999 9	0.999 8	0.999 7	0.999 5	0.999 3	0.998 7
	S	1	0.999 9	0.999 8	0.999 7	0.999 5	0.999 3	0.998 7
4e−5	R	1	0.999 9	0.999 7	0.999 5	0.999 3	0.998 8	0.997 7
	S	1	0.999 9	0.999 7	0.999 5	0.999 3	0.998 8	0.997 7
1e−5	R	1	0.999 5	0.999 0	0.998 0	0.996 9	0.994 9	0.989 9
	S	1	0.999 5	0.999 0	0.998 0	0.996 9	0.994 9	0.989 9
3.3e−6	R	1	0.998 5	0.997 0	0.993 9	0.990 9	0.984 9	0.969 9
	S	1	0.998 5	0.997 0	0.993 9	0.990 9	0.984 9	0.969 9

注：假设刷新周期为 1 min、且存储容量为 10×10^6 时的修复率 μ 为 1e−5。

从表 2 可以看出，随着参数 μ 的增加，三模冗余系统的可靠度和安全度均有所提高，初始时刻系统完好可靠度和安全度

皆为 1.000，随着运行时间的增加，系统可靠度和安全度均有所下降。图 7 所示的仿真波形为 $t=0-3.5\times10^8$ s、$\lambda=1.07$ day^{-1}时，三模冗余与回读刷新系统的可靠度和安全度随修复率 μ 的变化曲线。

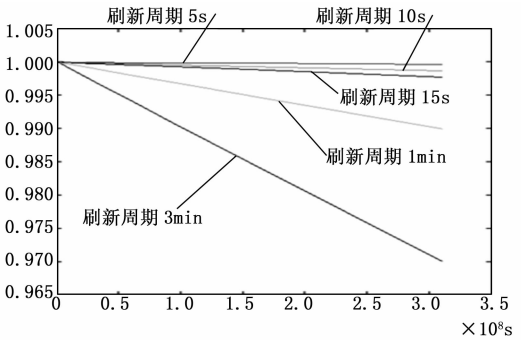

图 7　不同刷新周期系统可靠度 r 随时间 t 变化曲线

图 8 所示为 $t=0-3.5\times10^8$ s、$\lambda=1.07$ day^{-1}时，采用三模冗余有回读刷新设计的 FPGA 系统与三模冗余无刷新 FPGA 系统的可靠度比对。由图中可以看出，随时间的增加，两者的可靠度均有所下降，但采用三模冗余有回读刷新的 FPGA 系统可靠度明显优于无刷新系统。

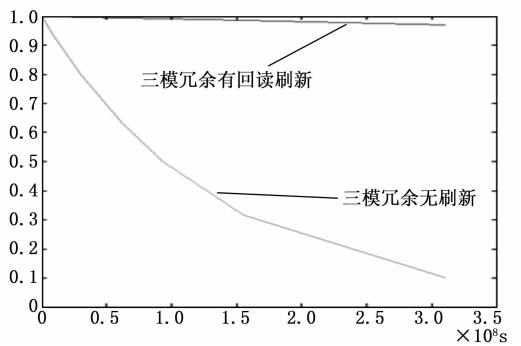

图 8　三模冗余有刷新系统与三模冗余无刷新系统的可靠度比对

4　结束语

为了提高宇航控制器的集成度、可靠性，本文提出一种在 FPGA 内部嵌入 CPU（8051）、存储器等 IP 核的设计方案，但 FPGA 应用于空间环境中易受空间高能粒子干扰，产生单粒子翻转（SEU）风险，对飞行器功能造成影响。文章分析了常规三模冗余抗辐加固设计的不足后，提出了一种采用三模冗余架构（TMR）并对 FPGA 配置区域进行刷新重载的解决方案，并对其可靠性进行了仿真分析，仿真数据证明该设计架构具有较高的可靠性，对小型化、高可靠宇航控制器设计具有较好的参考意义。

参考文献：

[1] 陈金恩，周赢武．基于 FPGA 与 MC8051 IP 核的可调窄脉冲激光泵浦源的研制［J］．闽江学院学报，2011，32（5）：23－27.

[2] 王　瑞，游志宇，杜　杨，等．MC8051 单片机 IP 核的 FPGA 实现与应用［J］．电子设计工程，2009，17（1）：57－63.

[3] 丁　昊，庄贵敏，宋　杰，等．基于 MC8051 内核的便携幅频特性测试仪设计［J］．嵌入式技术，2011，37（4）：29－32.

[4] 邢克飞，杨　俊，王跃科，等．Xilinx SRAM 型 FPGA 抗辐射设计技术研究［J］．宇航学报，2007，28（1）：123－129.

[5] 周秀娟，叶荣润．Virtex-II 系列 FPGA 的回读与部分重配置［J］．现代电子技术，2012，35（13）：159－161.

[6] 邱金娟，徐宏杰，潘　雄，等．SRAM 型 FPGA 单粒子翻转测试及加固技术研究［J］．电光与控制，2011，18（8）：84－85.

[7] 黄　伟，刘　涛，王　华，等．SRAM 型 FPGA 的单粒子效应及 TMR 设计加固［J］．航天返回与遥感，2012，33（2）：49－53.

[8] 顾义坤，倪风雷，刘　宏．Xilinx FPGA 自主配置管理容错设计研究［J］．宇航学报，2012，33（10）：1520－1521.

[9] 刘斐文，姚　睿．基于 FPGA 动态部分重构的 D/TMR 系统设计［J］．计算机工程与应用．2010，46（35）：55－57.

[10] Graham P，Caffrey M，Johnson D E，et al．SEU mitigation for half-latch in Xilinx Virtex FPGA［J］．IEEE Transactions on Nuclear Science，2003，50（6）：2139－2146.

[11] 邹见效，徐红兵，张正迁．基于三重冗余的 ETS 控制系统设计及可靠性评估［J］．电子科技大学学报，2010，39（5）：793－799.

[12] 王丽华，徐志根，王长林．可维修三模冗余结构系统的可靠度与安全度分析［J］．西南交通大学学报，2002，37（1）：103－107.

[13] 曾声奎．系统可靠性设计分析教程［M］．北京航空航天大学出版社，2004.

[14] 沈　洁，单　冬．三模冗余计算机联锁系统可靠性安全性分析［J］．北方交通大学学报，1998，22（5）：111－114.

[15] 靳红涛，焦宗夏，王少萍，等．高可靠三余度数字式作动器控制器设计与实现［J］．北京航空航天大学学报，2006，32（5）：548－552.

[16] Swift G M，et al．Dynamic testing of Xilinx Virtex-II field programmable gate array（FPGA）input/output blocks（IOBs）［J］．IEEE Tran．on Nuclear Science，2004，51（6）：3469－3474.

（上接第 297 页）

[3] 黄深喜，樊晓萍，刘少强，等．高速 ADC 频域特性测试系统的设计［J］．计算机工程，2009，35（9）：277－279.

[4] 董振龙，董　惠，武　锦．基于 FPGA 的高速高精度 ADC 测试平台的设计［J］．计算机测量与控制，2012，20（9）：2372－2374.

[5] 成　章，王　健，刘　敏，等．关于 ADC 测试平台的探讨［J］．电子信息对抗技术，2012，27（4）：77－80.

[6] 何　芹，黄　朴，虞致国，等．基于平均频谱测试高速 ADC 动态参数的方法［J］．电子测量与仪器学报，2014，28（7）：755－762.

[7] 裴颂伟，李兆麟，李圣龙，等．基于 V93000 的 SoC 中端口非测试复用的 ADC 和 DAC IP 核性能测试方案［J］．电子学报，2013，41（7）：1358－1364.

[8] 贺志容，石　坚，韩红星．93k 集成电路测试系统校准原理及实现方法研究［J］．宇航计测技术，2009（3）：66－69.

[9] NI．高性能测试测量与控制平台－PXI 产品［EB/OL］．http：//sine．ni．com/nips/cds/view/p/lang/zhs/nid/ 1527.

[10] Grace C R，Denes P，Gnani D，et al．Radiation－tolerant code-density calibration of nyquist-rate analog-to-digital converters［J］．IEEE Transactions on Nuclear Science，2013，60（2）：1303－1310.

[11] 周　娟，蒋登峰．基于 Matlab 的 ADC 自动测试系统开发［J］．中国计量学院学报，2008，19（3）：219－224.

[12] ADI．AD9254 14-Bit，150 MSPS，1．8 V，Analog-to-Digital Converter［M］．ADI INC．2006.

[13] He Q，Huang P，Zhao L，et al．A five-item MSLD windowed triple-spectrum-line interpolated FFT algorithm for measuring SFDR［A］．2014 12th IEEE International Conference on Solid-State and Integrated Circuit Technology（ICSICT）［C］．IEEE，2014：1－3.