

航天应用 FPGA 配置可靠性研究^{*}

王文华 韩双丽 张宇 李国宁 李新娥 任建岳

(中国科学院长春光学精密机械与物理研究所 长春 130033)

摘要 航天应用系统必须保证每一单元的安全性及可靠性。现场可编程门阵列 (Field Programmable Gate Array, FPGA), 以其 I/O 管脚丰富、设计灵活等优势, 逐渐被广泛应用于航天领域。其设计与工艺不断完善, 以适应太空中电子辐射等复杂的工作环境。由于基于 SRAM 的 FPGA 芯片断电后程序丢失, 因此每次上电后都需要先从 PROM 等外部存储器中加载程序才能正常工作。然而, 并不是每一个芯片的每一次加载配置都能成功完成, FPGA 的上电配置结果将直接关系到卫星任务的成败。研究发现, 诸如环境温度、信号完整性、供电电压、配置时钟速率等因素会影响 FPGA 的配置过程, 致使出现偶尔的配置失败, 这在航天应用中是绝对不允许的。针对实际应用的 Xilinx 公司 FPGA 芯片, 为提高上电配置可靠性, 提出了一系列设计保障措施, 在 FPGA 航天应用领域具有一定的参考价值。

关键词 FPGA, 配置监控, 重配置, 反熔丝, 看门狗

中图分类号 V44

Research on the Reliability of FPGA Configuration in Space-based Systems

WANG Wenhua HAN Shuangli ZHANG Yu

LI Guoning LI Xine REN Jianyue

(Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033)

Abstract Designers of space-based systems face unique challenges to insure each unit against failure. FPGA are used gradually in the aerospace field since it is invented with abundant I/O pins and flexible design margin. Many manufactures have been improving those space-qualified FPGA devices to adapt the aerospace high-radiation environments. FPGA devices based on SRAMs have to load configuration data from external PROMs on power-up before the logic is activated. However, not each batch or each device can be configured successfully with zero-failure. This paper explores every possible factor such as environment temperature, signal integrality, configuration rate and so on. Aiming at Xilinx FPGA devices, this paper provides a series of safeguard solutions for higher reliability of configuration. It has significant reference value in aerospace application fields for its feasibility and reliability.

Key words FPGA, Configuration monitor, Reconfiguration, Anti-fuse, Watchdog

* 国家高技术研究发展计划项目基金资助 (863-2-5-1-13B).

2009-11-27 收到原稿, 2010-11-03 收到修定稿

E-mail: wangwh900@yahoo.com.cn

1 引言

现场可编程门阵列 (Field Programmable Gate Array, FPGA) 以其高度的灵活性以及丰富的 I/O 资源与内嵌模块等优势, 在航天领域应用越来越广泛. FPGA 的生产工艺主要有 SRAM 结构、反熔丝结构以及 Flash 结构, 目前最大的两个 FPGA 厂家 Xilinx 和 Altera 的所有 FPGA 产品都是基于 SRAM 工艺来实现的, 由于掉电后 SRAM 会失去所有配置, 因此基于 SRAM 的 FPGA 必须配备一个 PROM 芯片, 用以存放 FPGA 的编程数据, 每次上电都需要重新加载^[1]. 这种方式不仅增加了整个系统的成本, 而且引入了不稳定的因素, 加载的过程容易受到外界干扰而导致程序配置失败.

在航天应用领域, 对可靠性的要求非常苛刻, 尤其是常常作为主处理器的 FPGA 器件^[1], 绝对不能容许上电加载配置失败. 本文就目前航空航天领域应用最广泛的 Xilinx-FPGA 芯片上电配置问题展开讨论, 研究出增强其配置可靠性的可行性方案.

2 Xilinx-FPGA 上电配置原理

以 Xilinx 公司的 XC1800 系列 PROM 在主串模式下的配置原理为例说明 FPGA 的上电配置过程^[2]. 电路原理如图 1 所示, 首先在加电状态下, PC 机通过 JTAG 口向配置链上的 PROM 注入程序数据, 以待再次加电时, FPGA 能够主动发起配置过程, 读取 PROM 中的程序数据并完成上电配置.

这里重点关注的是 FPGA 上电后的主动配置过程, 如图 2 所示, 可分为三个步骤^[2].

步骤 1 FPGA 监测到 VCC 电压达到一定数值后, PROG_B 信号自动进行配置初始化, 由 INIT 信号 (低电平有效) 清空 FPGA 配置内存.

步骤 2 FPGA 通过 CCLK 引脚发送时钟给 PROM, 该配置时钟驱动 PROM 的地址计数器并读出数据, 送到 FPGA 的 DIN 引脚.

步骤 3 FPGA 在读取数据的同时, 对接收到的数据进行 CRC 校验. 数据加载完成后, 若校验正确, 则由 FPGA 启动进程加载逻辑; 若校验错误, 则将 INIT 信号拉低报错.

以上步骤 1 和步骤 3 是由 FPGA 厂商固化在芯片中的程序决定的, 用户无法分析或干预该过程, 只

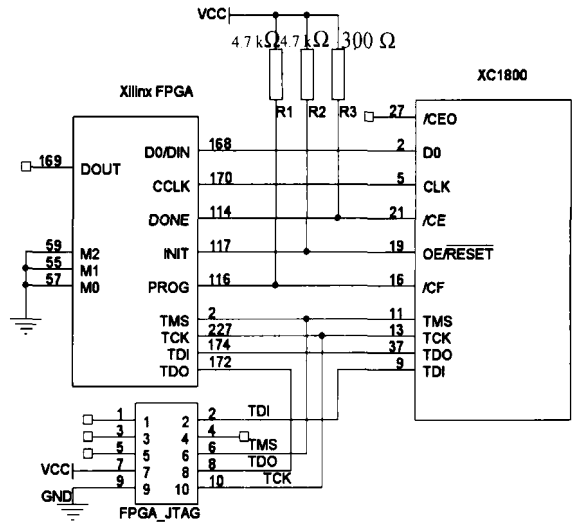


图 1 Xilinx-FPGA 主串配置模式原理

Fig.1 Schematic of Xilinx-FPGA configuration

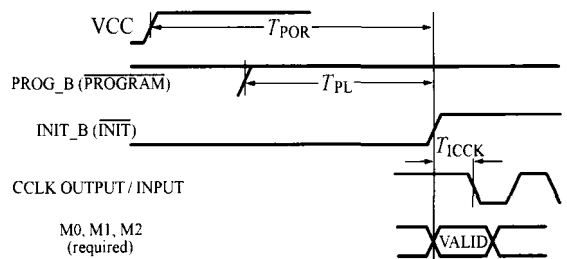


图 2 上电配置信号时序

Fig.2 Power-up timing of configuration signals

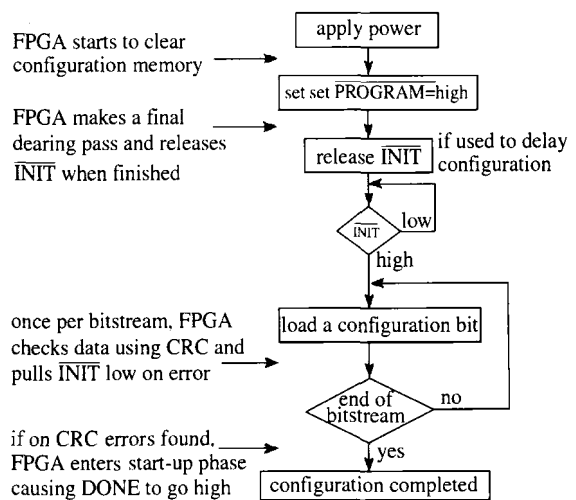


图 3 串行模式配置流程

Fig.3 Serial configuration flowchart

能测试步骤 2 中配置时钟与读取数据的情况. 由图 3 所示的配置流程可知, 在配置失败的情况下 (例如 CRC 校验错误), 没有任何复位信号来重新发起配

置过程, INIT 信号报错只会一直为低电平, 即 FPGA 不具备自行重配置功能, 只能依靠外部重新加电。

航空航天领域对可靠性要求极高, 且不允许在加电配置失败的情况下任意重复加电, 否则时间上的延误对单次航拍任务影响极大^[3]。若 FPGA 不能保证零失败上电加载, 则必须增加上电过程监控功能, 一旦上电加载失败, 立即自动重新加载配置, 在无人干预的情况下将潜在的风险消除。因此, 本文从所有可能影响上电配置过程的因素入手, 探讨如何增强航天应用 FPGA 的配置可靠性。

3 影响 FPGA 上电配置的因素

FPGA 配置失败的标志是 Done 信号一直为低电平, CCLK 信号一直有效, D0 串行数据位后半段出现异常的拉高现象, 持续约 800 ms 后拉低; Program 信号一直为高。在这种状态下, 芯片不能自检并发起重新配置过程。各引脚信号状态的示波器波形如图 4 所示, 由于测试板在高低温箱体内, 测试点长线引出, 测试设备距离比较远, 因此波形不够清晰。下面从不同方面讨论影响上电配置的因素。

3.1 PCB 信号完整性

数字电路在具有逻辑功能的同时, 也具有丰富的模拟特性。数字电路本身具有一定的抗干扰能力, 目前仍然需要估计或精确测定各种噪声的幅度及其时域变化, 来控制总噪声不超过电路的抗干扰能力, 以最小的综合成本达到最高的整体性能。

信号完整性 (Signal Integrity, SI) 是指信号在信号线上的质量^[4]。信号具有良好的信号完整性是指, 当在需要的时候具有所必须达到的电压电平数值。

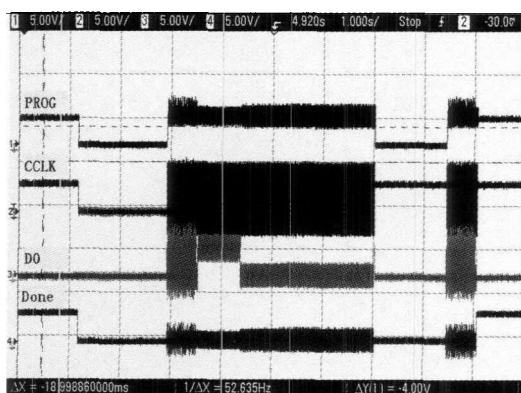


图 4 FPGA 配置失败时序显示

Fig. 4 Timing of configuration failure

信号完整性是保证系统稳定的基础, 分析讨论系统信号完整性是非常必要的。由于寄生阻抗、传输线效应等因素, 信号在传输过程中容易出现反射、串扰、过冲、延时、转换噪声、边沿畸变等现象, 严重时会造成时序数据的读写错误, 最终导致任务失败。

在电子学领域, 信号完整性影响着每一个设计环节, 尤其在数字通信方面, 可能会造成严重后果。同样, FPGA 上电配置过程是一个读 ROM 数据的过程, 如果读时钟 CCLK、读数据 D0 等关键信号的完整性不够好, 就会造成配置失败。作者在实验室利用 8 块电路板进行试验 (板图完全相同, 但在不同时期加工), FPGA 为相同批次的 XQVR300 芯片, 采用相同配置速率反复测试上电配置结果, 发现 8 块板出现配置失败的次数存在较大差异, 测试结果如表 1 所示 (-20°C 条件)。试验说明不同的电路板对不同的配置速率具有不同的电子学响应特性。

3.2 FPGA 加电瞬间供电性能

假定在信号完整性良好的前提下, 探讨 FPGA 供电部分对上电配置的影响。Xilinx 公司在用户手册中声明^[2,5]: FPGA 上电时需要一定量的供电电流来确保器件正常工作。实际消耗的电流取决于上电时间, 即电压由 0 上升到 2.7V 所用的时间, 时间越短, 瞬间供电电流越大, Xilinx 推荐上电时间在 2 ~ 50 ms 之间, 如图 5 所示。对于工业级 Virtex 系列芯片, 要求最小供电电流为 2 A, 要保证芯片正常上电初始化, 必须给芯片提供至少 2 A 的供电电流。若供电电流不足, 可能会造成芯片配置失败。

表 1 电路板配置试验每千次失败次数
Table 1 Statistics of configuration experiment per thousand times with different boards

电路板 编号	配置速率/MHz					
	5	7	8	9	13	15
1	3	4	0	4	0	9
2	0	5	3	4	4	4
3	0	2	3	2	8	13
4	0	5	11	2	3	4
5	2	4	2	0	4	5
6	1	3	4	0	2	5
7	4	3	0	4	5	5
8	3	1	0	9	1	2

另外, 电压模块的输入/输出电压差的大小也会对供电性能造成影响, 电压差越小, 上电瞬间产生的纹波也越小, 在短时间内需要尽可能保证输出电压的性能. 试验证实, 当供电电压差小于 0.5V 时, 上电配置失败现象发生的概率明显减少 (电源芯片为 MSK5230 系列).

3.3 配置时钟速率

FPGA 的配置时钟是配置过程的基准源, 时钟速率最高能达到 60 MHz, 将直接影响到上电配置的结果. Xilinx 集成开发工具 ISE 中专门提供了一项针对配置时钟速率的选项配置速率^[6], 即允许设计人员根据需求设置配置速率, 最小速率为 4 MHz, 最大速率为 60 MHz. 需要指出的是, 这里的速率只是形式上的配置速率, 虽然 Xilinx 标称单位是 MHz, 并不代表实际的 CCLK 时钟速率, 但前者约为后者的 0.7 倍. 配置时钟速率越快, FPGA 从 PROM 中加载程序数据的时间越短, 这种可供用户自定义的设计虽然方便了灵活调节上电配置时间, 但也给配置安全带来了一定风险.

在 PCB 印制定型后, 基板材料、生产工艺等差异也会对信号完整性造成一定影响^[7], 因此对单板而言, 并不是所有的配置速率都绝对可靠. 当然, 从信号的建立保持时间角度来说, 配置速率越低越可靠, 具体到实践中仍需要经过高低温试验才能确定.

3.4 FPGA 上电顺序

试验证实, FPGA 的配置过程与双电压的上电顺序无关^[6], 不论内核电压先上电还是外围 I/O 电压先上电, 都不影响配置结果, 只有两者都上电后, 配置过程才会开始. 两种上电顺序下配置时序示波器波形如图 6 所示, 其中由于 Done 引脚接有上拉电

阻, 因此 3.3V 先上电会使 Done 信号先拉高, 待 2.5V 上电后, Done 信号先拉低表示配置过程开始, 配置结束后 Done 信号拉高标志着配置成功.

3.5 环境温度

综合对以上影响因素的探讨, 按照航天研制要求, 对实际应用电路进行高低温环境试验^[8]. 对装配有 FPGA 的电路板进行适当保护处理后, 将其放入高低温试验箱中进行环境试验, 观察 FPGA 的上电配置加载情况. 在不同的配置速率情况下, 抽取若干个温度点进行频繁上电试验, 以一千次加电断电测试为参照标准, 记录上电配置加载情况. 表 2 为其中一块电路板的试验结果.

由表 1 分析可知, 除了配置速率对配置可靠性有影响外, 环境温度也是不可忽视的因素. 尽管目前影响机理还在研究中, 但以试验结果来看, 环境温度越低, 配置加载可靠性越差, 越容易造成上电配置失败, 而结果只能是先断电然后再次加电尝试. 另外,

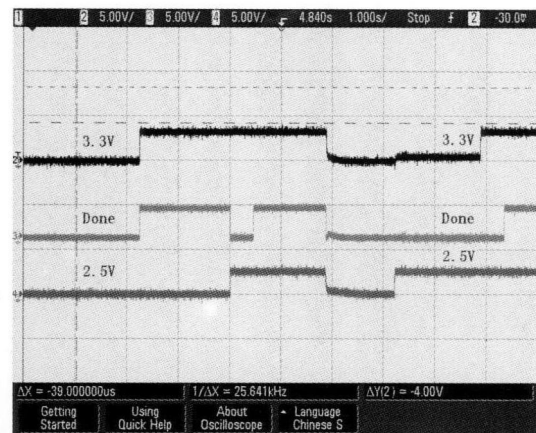


图 6 加电顺序对 FPGA 配置结果影响
Fig. 6 Influence of power-on sequence to configuration

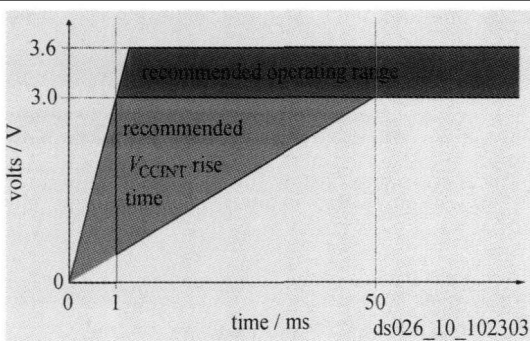


图 5 FPGA 加电瞬间供电要求
Fig. 5 Power supply power-on requirements

表 2 高低温试验配置每千次失败次数
Table 2 Statistics of configuration experiment per thousand times in high-low temperature environment

环境 温度/(°C)	配置速率/MHz			
	4	10	30	55
-40	2	9	11	97
-20	0	4	7	36
25	0	0	0	2
40	0	0	2	1

FPGA 本身的上电配置失败次数是一个概率统计问题,表中记录的配置失败次数仅代表当次试验的结果.

4 提高上电配置可靠性的措施

针对影响配置过程的几个因素,结合航天产品的要求与实际应用,可将提高上电配置可靠性的措施分为主动和被动两个方面.

4.1 主动措施

针对以上分析的客观影响因素,可采取以下主动预防性措施.

(1) 尽可能使环境温度在 0°C 以上,至少不能低于 -20° .

(2) 精心设计 PCB 布线,与配置有关的时钟、数据走线应加地线保护,必要时增加匹配电阻,降低过冲与反射.

(3) 选用供电电流大的电源模块,并在设计时尽可能降低输入/输出电压差.

(4) 选用较低的默认配置速率,不要选择太高,尽量使配置速率 $\leq 20\text{MHz}$.

4.2 被动措施

在设计已经成型的情况下,FPGA 及其所在的电路板系统如果依然存在上电配置失败的可能性,则需要有这样一个设备来代替人工,对 FPGA 在不断电状态下进行重新配置.假定原来系统某次上电配置失败的概率为 10^{-4} ,则连续两次配置失败的概率会降到 10^{-8} .所谓被动措施,是指对配置完成标志状态(Done 信号或 FPGA 工作信号)进行监控,第一次 FPGA 加电配置失败时,对 FPGA 进行反复重新配置.

在此提出以下两种监控方案.

一种方案是可以利用其他加电启动可靠性高的可编程逻辑器件,例如 CPLD 的配置无需外部存储器,能够自动进行内部配置启动^[9],反熔丝 FPGA 上电后不经配置过程也可直接工作.本文利用 Actel 公司生产的的宇航级 A1280 芯片,监控 XQVR300 芯片的 Done 引脚,一片 Actel 可监控多片 FPGA 的上电配置,只要 Actel 芯片与被监控的 FPGA 同时加电即可,原理如图 7 所示.

另一种方案是,FPGA 加电配置成功后便开始运行程序,若能从 I/O 口引出一个周期信号,则可以利

用外部看门狗来实现 FPGA 的配置监控.以看门狗芯片 MAX706 为例,将 MR 引脚与 WDO 相连,使其工作在自动监控复位状态,如图 8 所示.FPGA 加电配置成功后,该 I/O 引脚输出一定频率的周期信号,作为 MAX706 芯片的触发信号提供给 WDI 引脚,RESET 端将保持高电平,不影响 FPGA 工作;当 FPGA 配置失败时,由于程序没有运行,看门狗芯片没有及时获得触发信号,使 RESET 引脚每隔 1.6s 发出重配置信号提供给 FPGA,直到 FPGA 配置成功.这里应该注意的是,看门狗芯片一定要选用具有 WDI 边沿触发清零功能的,不能使用电平清零的,因为当 FPGA 故障时,FPGA 的输出端口有可能保持高电平或低电平.

一般而言,FPGA 从 PROM 加载程序的时间小于 1s,同时加电后,Actel 芯片等待一段时间(图 9 所示间隔为 3.2s)后检测 Done 引脚状态.若为时间低电平则发出一段低电平重配置信号,然后拉高等待此次配置结果;若为高电平则不动作.需要注意的是,监控配置功能是辅助性的,不能影响 FPGA 自身上电配置过程,即只有当 FPGA 配置失败时,监控重配置才会起作用.

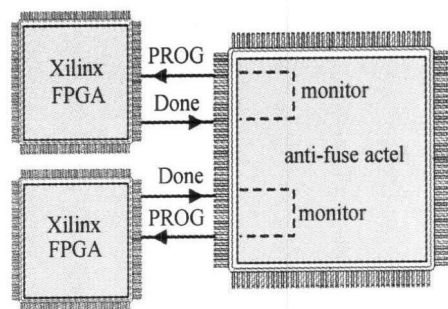


图 7 Actel 监控 FPGA 配置原理

Fig. 7 Configuration monitor by anti-fuse device

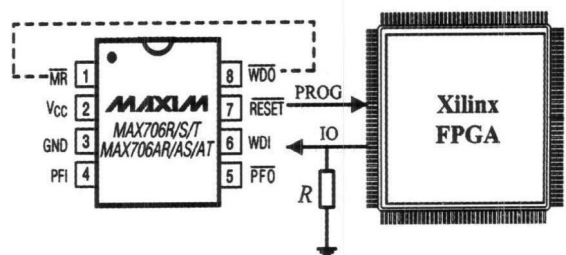


图 8 看门狗监控原理

Fig. 8 Configuration monitor by Watch-dog devices

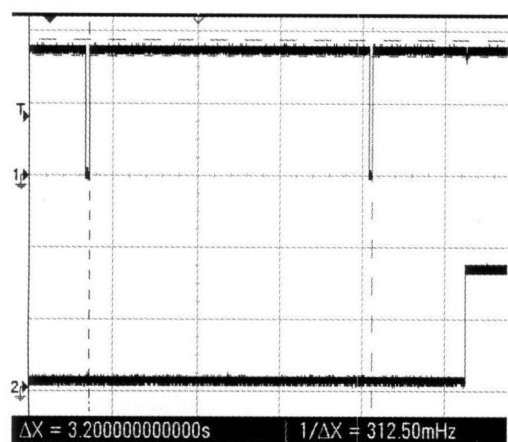


图9 FPGA 重配置过程时序显示

Fig.9 Timing of reconfiguration signals

5 结语

随着航天技术的不断发展, FPGA 被越来越广泛地应用. 本文针对 FPGA 可能遇到的加载配置可靠性问题进行了一系列探讨与试验, 并提出了切实可行的解决方案. 为了满足航天绝对可靠性的要求, 建议对所有 FPGA 上电配置采取被动监控措施, 基于反熔丝可编程逻辑芯片及看门狗芯片的设计方法, 进一步提高了 FPGA 的应用可靠性. 本文仅就 FPGA 的一种配置模式进行了探讨, 但对其他配置模式下的可靠性研究具有参考价值.

参考文献

[1] Yan Lei, Wang Qiang, Fang Liang, Gu Hongjing, Li Nan.

- Application of FPGA in space electronics device [J]. *Chin. J. Space Sci.*, 2009, **29**(1):54-58. In Chinese (闫蕾, 王强, 房亮, 顾红静, 李楠. 可编程逻辑器件在空间电子学设备中的应用 [J]. *空间科学学报*, 2009, **29**(1):54-58)
- [2] Xilinx Inc. XC18V00 Series in System Programmable Configuration PROMs datasheet [S]. 2006, DS026 (V5.1.0)
- [3] Yu Shaoan. Research on the reliability of power-supply subsystem of satellites [J]. *Elect. Prod.*, 2009, **2**:90-92. In Chinese (俞绍安. 卫星电源分系统可靠性设计与研究 [J]. *今日电子*, 2009, **2**:90-92)
- [4] Zhou Ping. Signal integrity designs of high-speed PCB [J]. *Reliab. Ana.*, 2009, **32**(1):32-36. In Chinese (周萍. 高速 PCB 板的信号完整性设计 [J]. *可靠性分析*, 2009, **32**(1):32-36)
- [5] Xilinx Inc. Powering Xilinx FPGAs datasheet [S]. 2001, XAPP158(V1.4)
- [6] Xilinx Inc. Virtex™ 2.5V Field Programmable Gate Arrays datasheet [S]. 2001. 4, DS003 (V2.5)
- [7] Su Donglin, Wang Xiaoxiao. Relationship between PCB material and power/ground impedance [J]. *J. Beijing Univ. Aeron. Astron.*, 2007, **33**(5):568-571. In Chinese (苏东林, 王晓晓. PCB 材料与电源/地层谐振阻抗关系 [J]. *北京航空航天大学学报*, 2007, **33**(5):568-571)
- [8] Jin Xunshu. The development status and application of spacecraft verification and test standards [J]. *Chin. Space Sci. Tech.*, 2004, **6**(12):25-31. In Chinese (金恂叔. 航天器环境试验和航天产品的质量与可靠性保证 [J]. *中国空间科学技术*, 2004, **6**(12):25-31)
- [9] Xilinx Inc. A CPLD-Based configuration and revision manager for Xilinx platform Flash PROMs and FPGAs datasheet [S]. 2005.1, XAPP693 (V1.1)