文章编号:1671-4598(2022)06-0253-06 DOI:10.16526/j.cnki.11-4762/tp.2022.06.039 中图分类号:V19 文献标识码:A

一种高可靠的工业级星载计算机及其引导设计

姜同全，薛淑娟，张 腾，刘中伟，王 磊，崔战国，姜连祥
（山东航天电子技术研究所，山东 烟台 264670）

摘要：传统星载计算机通常采用价格昂贵的高质量等级CPU和存储器芯片，用于保证系统的可靠性；因制造成本和研制周期等方面的限制，商业卫星计算机更倾向于采用商业现货器件（COTS），但其可靠性和安全性会随之降低；采用工业级SmartFusion2处理器芯片，提出一种低成本的星载计算机最小系统架构，并通过工业级存储器异构备份的方式，显著提高系统可靠性；在星载计算机软件设计中，应用软件会采用三模冗余的方式提高可靠性，但引导软件往往只有单份；为了避免引导软件的单节点故障效应，针对SmartFusio2星载计算机架构，提出一种基于多TMR副本的片外启动方法，此启动方法可进一步提高工业级星载计算机的可靠性和安全性，并成功用于多个型号商业卫星。

关键词：工业级；星载计算机；SmartFusion2；多TMR副本；片外启动

A High-Reliable On-Board Computer Base on Industry and Design for Boot Loading System

JIANG Tongquan, XUE Shujuan, ZHANG Teng, LIU Zhongwei, WANG Lei,
CUI Zhanguo, JIANG Lianxiang
(Shandong Institute of Space Electronic Technology, Yantai 264670, China)

Abstract: CPU and memory chips with expensive high quality grade is usually used for traditional on-board computer, so the higher reliability of the system is obtained. Due to the limitations of manufacturing cost and production cycle, the on-board computers of commercial satellites are prone to apply more and more commercial-off-the-shelf (COTS) components. Of course, the COTS components decrease the system reliability and security. By making use of the industrial-grade processor chip named SmartFusion2, a minimum system structure of low-cost on-board computer is proposed, which can extremely improve system reliability by the heterogeneous redundancy for the industrial-grade memory chips. For the software design of the on-board computer, although the triple module redundancy is applied by the application software to obtain higher reliability and better security, the boot-loading software is single. In order to avoid the single point of failure in the boot-loading software, a off-chip boot-loading method is based on multi-TMR copies for the on-board computer using SmartFusion2 processor, which improves the reliability and security for the on-board computer with industrial-grade. In addition, the boot-loading method has been successfully applied in the multiple commercial satellites.

Keywords: industrial-grade; on-board computer; SmartFusion2; multi-TMR copies; off-chip boot-loading method

0 引言

为了保证产品的可靠性需求，传统的星载计算机通常选用高质量等级的元器件：中央处理器（CPU，central processing unit）则选用抗辐照性能高的器件，程序存储器则选用具有防单粒子的反熔丝器件，数据存储器则选用具有EDAC功能的器件[1]。但是，高等级元器件的选用不但增加了产品的研制成本还会影响产品的研制周期。近年来，商业航天市场领域取得了飞速的发展，而低成本和短周期的微纳卫星平台则备受众多商业卫星公司的青睐。

凭借采购周期短、成本低和集成度高等优点，商用现货（COTS，commercial-off-the-shelf）器件越来越多地被应用在商业微纳卫星的平台上[2-3]。但由于抗空间环境的能力较弱，COTS器件在轨经常会出现单粒子翻转和单粒子锁定等问题，从而一定程度上降低了产品的可靠性。为了解决低成本和高可靠之间的需求矛盾，文献[4]采用双机冗余、代码备份的方法提出了一种基于工业器件的星载计算机系统，并通过建立马尔可夫链数学模型，从数学理论的角度证明了，具有冷备资源的冗余方案可获得相对高的系统可靠性。文献[5]采用基于PowerPC体系结构的SM750处理器作为控制核心，提出了一种“SM750+FPGA”架构的高性能星载计算机方案，并搭载嵌入式操作系统AIC-OS，为星载计算机设计提供一种新思路。文献[6]针对系统级芯片（SOC，system on a chip）具有集成性高、可编程性强的特点，提出了一种片内热备份、片外冷备份和混合冗余策略的星载计算机处理系统设计方案，并通过建模的方式进行了系统可靠度验证。

在星载计算机软件设计中，对应用软件通常采用三模

收稿日期:2022-03-09； 修回日期:2022-04-02。
作者简介:姜同全(1990-),男,山东烟台人,硕士研究生,工程师,主要从事星载计算机和FPGA软件设计方向的研究。
引用格式:姜同全,薛淑娟,张 腾,等.一种高可靠的工业级星载计算机及其引导设计[J].计算机测量与控制,2022,30(6):253-258.

冗余的加载方式，并具备在轨软件重构的功能，以提高计算机应用程序对空间环境的可靠性。为了支持软件三模冗余加载和在轨软件重构等功能，星载计算机的软件架构通常采用“引导＋应用”的方式[7]：具体而言，在星载计算机加电，并完成硬件系统复位之后，由引导软件将应用软件的三模冗余副本进行三取二比对，并在完成相关配置后由引导软件对应用软件进行加载启动[8]。通常地，由于星载计算机所用的处理器在固化启动方式上的限制，引导程序只能在可编程只读存储器（PROM，programmable read-only memory）里存储单份，因此具有单点故障的风险。针对 SPARC V8 架构处理器（AT697），文献［9］将错误检测与纠正（EDAC，error detection and correction）和三模冗余两种方法结合起来，并将引导（BOOT）区域和主程序区域进行三模冗余处理，提出一种容错启动系统设计方法；在启动阶段，此方法利用 AT697 的 EDAC 功能对 BOOT 区域进行检查和纠错；但此方法仅限于特定类型的处理器，而且其并未考虑 BOOT 三模冗余失效的情况。

采用工业级的处理器芯片 SmartFusion2，本文提出了一种低成本的星载计算机最小系统架构，通过挂载异构形式的存储器芯片，既降低了星载计算机的研制成本，又进一步地提高了系统可靠性和安全性。通过结合基于 SmartFusion2 的计算机系统架构，本文提出一种星载计算机的多 TMR 副本的片外启动方法，不但实现了 Cortex M3 处理器内核的片外启动的方式，还通过将引导软件的多个副本存储在分散的不同区域，且每个软件副本均进行三模冗余，以进一步地提高整个星载计算机系统的可靠性。

1 基于 SmartFusion2 的星载计算机最小系统

伴随着对综合电子技术集成度要求的提高，越来越多的星载计算机采用具有片上 SOC 资源的控制处理器，既可以节省单独的 CPU 芯片及其外围电路，而且还可依靠芯片上丰富的场可编程门阵列（FPGA，field programmable gate array）逻辑资源对外提供更灵活的接口功能扩展[10]。如图 1 所示，本文提出了一种基于工业级 COTS 器件的低成本星载计算机最小系统设计架构，其选用的 SmartFusion2 系列 M2S090T 型 FPGA 芯片，其内部集成了一个 166 MHz 的 Cortex M3 硬处理器内核，逻辑资源丰富，功耗低而且体积小。具体地，在片内存储资源方面，M2S090T 型 FPGA 芯片具有 512 K 的内部 ENVM 程序存储器（embedded NVM），支持错误检查与纠正（ECC，error correcting code），可用于存放固化程序，64 K 的内部 ESRAM 数据存储器[11-12]（embedded SRAM），支持 EDAC，可用于存储程序变量。在片内接口控制器方面，M2S090T 型 FPGA 芯片内部集成了 1 路 CAN 控制器，2 路多模式异步串口控制器（MMUART，multi-mode universal asynchronous/synchronous receiver/transmitter），以及 2 路串行外设接口（SPI，serial peripheral interface）控制器和 2 路集成电路总线（I2C，inter-integrated circuit）控制器等。更重要的是，此款工业级的 FPGA 芯片目前已经具有大量飞行验证经历。

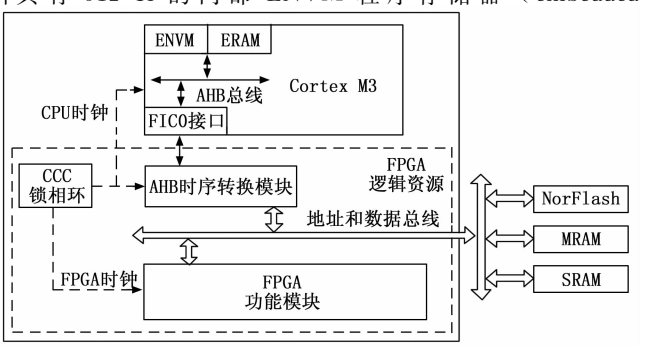

图 1 基于 SmartFusion2 的星载计算机框架图

除了 ENVM 和 ESRAM 等片上存储资源外，本文提出的星载计算机最小系统还在片外并行地挂载两片非易失闪存（NorFlash）芯片 S29GL512P、并行地挂接两片 MRAM 芯片 MR25H512 均作为程序存储器，并行地挂载两片具有支持 EDAC 功能的静态随机存取存储器（SRAM，static random-access memory）芯片 IS61WV51216EDBLL 作为数据存储器。其中，NorFlash 芯片 S29GL512P（支持 16 位数据和 32 位读写操作）共 128 M 可用于存储引导程序和应用程序，并分别按照三模冗余方式进行存储；磁性随机存储器（MRAM，magnetoresistive random access memory）芯片 MR25H512（支持 8 位、16 位和 32 位读写操作）共 1 M，在物理特性上具有抗单粒子的特点，可对引导程序和应用程序的副本按照单份方式进行存储，以节省 MRAM 的使用空间；片上 ENVM 芯片（支持 8 位、16 位和 32 位读写操作）具备 ECC 错误检查与纠正功能，也可对引导程序和应用程序的副本分别按照单份的方式进行存储；片外 SRAM 芯片 IS61WV51216EDBLL 具有硬件 EDAC 功能，可对存储数据的单比特翻转进行自动纠正，一方面可以作为数据存储器，用于全局变量和局部变量的分配，另一方面还可作为应用程序的运行空间（应用程序可由引导程序从程序存储器搬移到 SRAM）；片上 ESRAM 支持 EDAC 功能，可作为数据存储器，用于全局变量和局部变量的分配。

M2S090T 型 FPGA 芯片上的 Cortex M3 内核是通过内部集成的 AHB 总线[13-14]，实现对片上 ENVM、ESRAM、CAN 控制器等模块的读写访问；其中，Fabric interface controller（FIC0）是片上 SOC 系统内部的一个扩展模块，挂接在 AHB（advanced high performance bus）总线上，实现 Cortex M3 内核与 FPGA 逻辑之间的 AHB 总线时序转换，作为 Cortex M3 内核对外进行读写访问的唯一接口。基于 SmartFusion2 的星载计算机最小系统框架如图 1 所示，Cortex M3 内核和 FPGA 逻辑分别作为两大相对独立的功能模块，在 FPGA 资源内实现了一个“AHB 时序转换模块”，作为 AHB 总线时序协议和 Local 总线时序协议之间的转换桥梁，实现 Cortex M3 内核与 FPGA 内部寄存器和片外存储器之间的数据访问。另外，采用 FPGA 自带的 CCC 锁相环模块实现由 FPGA 板上晶振到 CPU 时钟和 FPGA 工作时钟频率变换，Cortex M3 内核和 FPGA 逻辑分别属于两个时钟域，在进行 FPGA 逻辑设计使需充分考虑跨时钟域时序处理，并在综合布局布线中添

加对应的时钟约束。在片上 Cortex M3 处理器内有一个 CPU 锁相环模块（MCCC，MSS clock conditioning circuitry），通过对 CPU 时钟进行分频产生挂接在 AHB 总线上的各类控制器的工作时钟。

2　多 TMR 副本的片外启动方法

2.1　SmartFusion2 的片外启动方法

2.1.1　Cortex M3 复位启动序列

在传统的 ARM 架构中，0x0000，0000 地址是一条跳转指令，并由 0x0000，0000 地址开始执行第一条指令。但在 Cortex M3 架构中，0x0000，0000 地址用于存储主堆栈指针（MSP，main _ stack _ pointer）初始值，中断向量表[15]紧接其后，其中中断向量表的第一个条目指向复位完成后第一条进行执行的指令[16]。Cortex M3 复位序列示意如图 2 所示，在复位信号撤销之后，Cortex M3 处理器所执行的第一个操作就是：首先从 0x0000，0000 地址获取 MSP 的初始值，然后再从 0x0000，0004 地址获取 PC 的初始值（其数据最低位必须是 1）。其中，程序计数器（PC，program counter）初始值就是复位向量的地址，并从此地址进行取指。

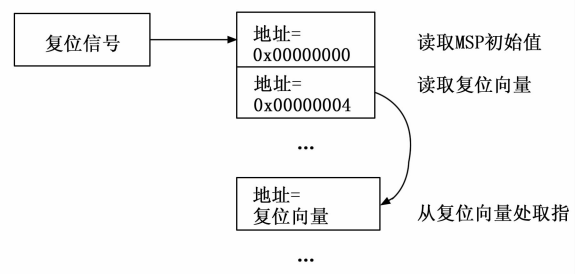

图 2　Cortex M3 复位序列示意图

2.1.2　Cortex M3 中断向量表

Cortex M3 中断向量表的分布如表 1 所示，在应用程序执行过程发生某类异常或者中断后，Cortex M3 根据中断向量表确定其服务例程或者中断服务程序的入口地址。其中，Cortex M3 中断表默认起始地址是 0x0000，0000，但为了支持动态重分发中断，Cortex M3 允许从其它地址进行异常和中断向量的定位，即中断向量表重定位。具体地，通过修改 Cortex M3 的“中断向量表偏移量寄存器”（0xE000，ED08 地址），可实现中断向量表的重定位，其中，中断向量表偏移量寄存器（VTOR，vector table offset register）的具体定义如表 2 所示。在支持软件重构的“引导程序＋应用程序”的实现方式下，中断向量表重定位最常用的实现方式是：在数据存储区（SRAM 或者 ESRAM）分配部分连续空间用于存储中断向量表。在程序引导期间完成各中断向量入口地址的赋值，并在引导完成后，通过修改 VTOR 寄存器，启用内存空间中的新向量表，实现中断向量表的重定位和动态调整。

2.1.3　SmartFusion2 启动地址重映射

在 M2S090T 型 FPGA 中，SmartFusion2 默认是将片上 ENVM（起始地址 0x6000，0000）重映射为 0x0000，0000 地址，因此在片上系统完成复位操作后，Cortex M3 内核默认从片上 ENVM 启动，即从 ENVM 上加载程序并启动运行。除此之外，SmartFusion2 还支持将片上 ESRAM（起始地址 0x2000，0000）和闪存（MDDR，Mobile DDR SDRM）（起始地址 0xA000，0000）重映射为 0x0000，0000 地址，并可指定一定大小的偏移地址。SmartFusion2 启动地址重映射配置如图 3 所示，在 Microsemi 厂商自带的 FPGA 集成开发环境 Libero SOC 中，通过修改 Cortex M3 内核的“AHB Bus Matrix 模块”中的“Remapped Region to location 0x0000000 of Cortex-M3 ID Code space”即可实现 SmartFusion2 默认启动地址的重映射。另外，“eNVM Remap Base Address（Cortex-M3）”用于指定中断向量表的偏移地址，最大支持 256K 的偏移地址大小。

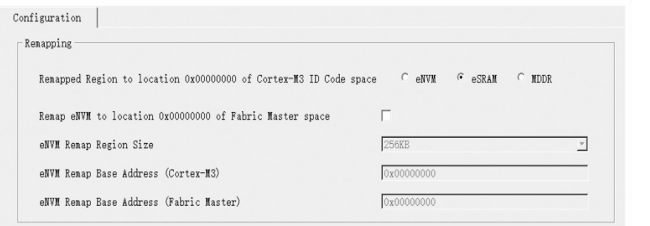

图 3　SmartFusion2 启动地址重映射配置图

表 1　Cortex M3 中断向量表分布

地址	异常编号	向量值(32 位整数)	startup_m2sxxx.s 启动文件的异常/中断入口地址
0x0000,0000	—	MSP 初始值	__initial_sp
0x0000,0004	1	复位向量(PC 初始值)	Reset_Handler
0x0000,0008	2	NMI 服务例程的入口地址	NMI_Handler
0x0000,000C	3	硬件异常服务例程的入口地址	HardFault_Handler
…	…	其它异常服务例程的入口地址	其它异常和外部中断

表 2　中断向量表偏移量寄存器含义

位段	名称	类型	复位值	描述
B7-B28	TBLOFF	RW	0	向量表的起始地址
B29	TBLBASE	R	—	向量表是在 Code 区(0)，还是在 RAM 区(1)

2.1.4　SmartFusion2 的片外启动方法

充分利用 Cortex M3 内核的复位启动序列、中断向量表可重定位和 SmartFusion2 支持启动地址重映射的特性，本文设计了一种可灵活扩展的片外启动方法（片外存储器的程序进行加载和启动），具体的设计要点如下：

1）在 FPGA 逻辑开发过程中，按照图 3 所示，在 Libero SOC 集成开发环境中通过更改 FPGA 的“Remapped Region to location 0x00000000 of Cortex-M3 ID Code space”

配置，将 ESRAM 重映射为 0x0000，0000 地址。

2）系统加电运行后，由 FPGA 逻辑对 Cortex M3 内核提供足够时间的持续复位，在 Cortex M3 内核复位信号撤销之前，由 FPGA 逻辑实现的“FPGA 引导启动模块”将片外存储器上引导程序的中断向量表搬移到片上 ESRAM 的 0x2000，0000 为首地址的一段地址空间内。

3）在本文的设计中，由于 ESRAM 被重映射为启动地址，在 FPGA 逻辑的复位信号撤销之后，Cortex M3 内核会从 ESRAM 首地址（即 0x2000，0000 地址）获取 MSP 初始值，并从 0x2000，0004 地址获取 PC 指针的初始值，由于 ESRAM 上的中断向量表指向的是片外存储器上的引导程序，因此 Cortex M3 内核将从指向片外的复位向量地址取指。这样，依靠其自身特有的复位启动序列，Cortex M3 内核便自动地跳转到片外程序存储器的空间运行。

4）在本文的设计中，由于 ESRAM 被映射到 0x0000，0000 地址，而且中断向量表已经被 FPGA 逻辑的“FPGA 引导启动模块”搬移到 ESRAM 空间，在 Cortex M3 内核成功启动程序运行并发生异常或者中断后，Cortex M3 内核会从 ESRAM 的中断向量表获取指向片外程序存储器的中断服务程序入口地址，因此本文的设计方法无需再额外进行中断向量表重定向设置。

2.2 多 TMR 副本的启动方法

考虑到空间环境的单粒子效应影响，本文设计对引导程序进行三模冗余处理，以提高系统引导的可靠性：三份程序分别存储在不同存储区域，每次复位时由 FPGA 进行三取二比对，并将其搬移到片外 SRAM 运行。另外，为了防止程序存储器局部故障，本文设计在分散的地址空间上分别放置多个引导程序的副本，而且每个副本都进行三模冗余处理。进一步地，为了防止程序存储器整体故障，本文设计还在不同存储介质上分别放置多 TMR 副本。

具体地，在本文提出的基于 SmartFusion2 的星载计算机最小处理系统中，引导程序的副本存储分布如图 4 所示：1）外部 NorFlash 芯片存储 3 个引导的程序副本，而且每个副本都进行三模冗余（TMR，triple modular redundancy）处理[17-18]；2）考虑到其自身固有的防单粒子物理特性和存储空间大小的限制，外部 MRAM 芯片只存储单份引导程序副本，且不做三模冗余（TMR）处理；3）考虑到其具备 ECC 错误检查与纠正功能和存储空间大小限制，片上 ENVM 只存储单份引导程序副本，且不做三模冗余（TMR）处理。

综合 2.1 节内容，针对基于 SmartFusion2 的星载计算机最小处理器系统，本文提出的一种多 TMR 副本的片外启动方法基本流程如下所示：

1）系统加电并完成复位之后，由 FPGA 逻辑暂时控制喂狗输出，并尝试从片外 NorFlash 芯片的首组 TMR 副本进行三取二比对和引导程序加载启动。如果引导程序加载启动成功，则由 Cortex M3 内核进行喂狗控制，并继续完成应用程序的加载和启动，否则 FPGA 逻辑继续尝试从片外 NorFlash 芯片的下一组 TMR 副本进行加载启动。

2）如果从片外 NorFlash 芯片的三组 TMR 副本均加载启动失败，则 FPGA 逻辑切换到片外 MARAM 芯片的单份副本启动引导程序，如果加载启动成功，则由 Cortex M3 内核进行喂狗控制，并继续完成对应用程序的加载和启动。

3）如果从片外 MRAM 芯片的单份副本加载启动失败，则 FPGA 逻辑再次切换到片上 ENVM 的单份副本启动引导程序，如果加载启动成功，则由 Cortex M3 内核进行喂狗控制，并继续完成对应用程序的加载和启动。

4）如果从片外 NorFlash 芯片、片外 MRAM 芯片和片上 ENVM 均加载启动失败，则由 FPGA 逻辑将系统热复位计数加一，并返回到步骤 1）对下一份应用程序进行重新加载启动。进一步地，如果系统热复位计数过多，则由硬件仲裁电路执行星载计算机自断电重启或者主备份切机的措施。

3 功能仿真和试验验证

3.1 基于 SmartFusion2 的星载计算机

按照商业微纳卫星对综合电子的工业化、模块化和标准化要求，按照本文的架构设计方案，实现了两种通用型的星载计算机。第一种星载计算机为 3U 结构大小，底部焊接两个工业级 CPCI 连接器[19]，通过底板与综合电子内的其它模块进行电气连接，外部焊接 J30J 类型连接器，与卫

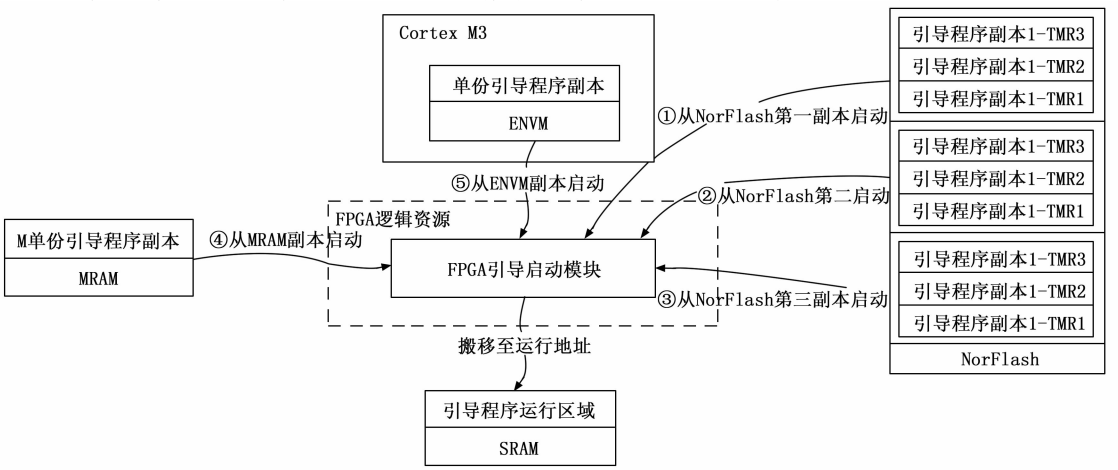

图 4 多 TMR 副本的启动方法示意图

星上其它设备进行电气连接。3U 类型星载计算机结构紧凑，接口资源丰富，适合于一百公斤内的微纳卫星。第二种星载计算机为 1U 结构大小，底部焊机两个工业级 PC104 连接器[20]，与堆栈体内其它模块通过底部 PC104 接插件进行电气连接，外部焊接 Molex 类型连接器，与卫星上其它设备进行电气连接。1U 类型星载计算机结构更紧凑，但资源相对有限，更适合于十公斤左右的立方星。目前，3U 类型和 1U 类型的星载计算机均用于多个商业卫星型号上，而且在轨运行稳定。

3.2　FPGA 引导启动模块的功能仿真

在 FPGA 逻辑中实现“引导启动模块”，用于负责将异构程序存储器中的引导程序副本进行三取二比对，并将处理结果搬移至 SRAM 芯片的运行区，同时依据引导和加载运行的结果，对引导程序副本进行管理和选择。在 Libero SOC 集成开发环境中，利用 Modelsim 仿真工具 V10.5c，对 FPGA 逻辑的“引导启动模块”的功能和时序进行仿真。仿真结果如图 5 所示，fpga _ boot 信号组反映引导程序副本的切换，code _ flash _ mram 信号组反映片外 NorFlash、片外 MRAM 和片外 sram 的读写控制时序，code _ envm 反映片上 ENVM 的读写控制时序，仿真结果波形与 FPGA 引导启动模块的功能设计完全相符。

在 fpga _ boot 信号组中，fpga _ rst _ boot 表示 FPGA 逻辑的复位信号，信号 mss _ rst _ boot 和 m3 _ rst _ boot 信号表示 FPGA 逻辑在“引导启动模块”进行程序加载过程中，对 Cortex M3 内核的复位信号。boot _ ok _ i 表示 FPGA 逻辑对引导程序是否加载成功的判别，在本次测试的仿真激励中，此信号被强制设置为加载无效，以便充分模拟“引导启动模块”对所有异构存储区域的程序副本加载启动过程。bootcopy _ selec _ o 信号则反映出“引导启动模块”的副本选择过程：其值为 0 表示从 NorFlash 引导副本 1 进行加载运行；其值为 1 表示从 NorFlash 引导副本 2 进行加载运行；其值为 2 表示从 NorFlash 引导副本 3 进行加载运行；其值为 3 表示从 MRAM 引导副本进行加载运行；其值为 4 表示从 ENVM 引导副本进行加载运行。

在 code _ flash _ mram 信号组中，flash _ cs _ o 表示片外 NorFlash 的片选信号，mram _ cs _ o 表示片外 MRAM 的片选信号，sram _ cs _ o 表示片外 SRAM 的片选信号，sram _ rd _ o 表示读使能信号，sram _ we _ o 表示写使能信号，sram _ addr _ o 表示地址总线信号，sram _ data 表示数据总线信号，sram _ byte _ o 表示高低字节使能信号。其中，sram _ rd _ o、sram _ we _ o、sram _ addr _ o、sram _ data、sram _ byte _ o 是片外 NorFlash、片外 MRAM 和片外 SRAM 的复用信号。对于片外 NorFlash 和片外 MRAM 主要是读取操作，用于对引导程序副本进行三取二比对处理，对片外 SRAM 主要是写入操作，用于引导程序的加载。

在 code _ envm 信号组中，组内所有信号表示由 FPGA 逻辑“引导启动模块”从片上 ENVM 的读取引导程序副本的操作，仿真波形完成满足 AHB 总线控制时序要求。

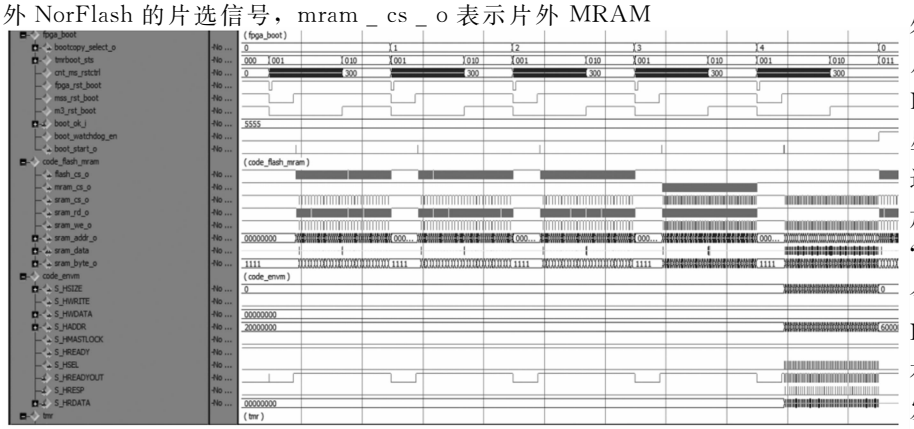

图 5　FPGA 引导启动模块的功能仿真图

3.3　SmartFusion2 计算机的多 TMR 副本的启动验证

按照第 1 节中的设计方案，本文采用工业级 SmartFusion2 系统的 FPGA 芯片 M2S090T 设计和实现了星载计算机单板。按照第 2.2 节的内容对片外 NorFlash、片外 MRAM 和片上 ENVM 的引导程序副本进行分配。为了便于测试，除必需的应用程序搬移和跳转功能外，本文测试用的引导程序还具备测试指令，用于破坏指定存储区域的程序副本。测试过程的具体测试用例如表 3，通过地测串口打印的引导程序加载启动测试结果如图 6 所示，测试结果表明：在引导副本启动失败后，本文系统能够自动切换到下一个引导副本进行启动。

表 3　测试用例说明表

次序	测试项目	测试用例
1	NorFlash 引导程序副本 1 启动	计算机正常加电
2	NorFlash 引导程序副本 2 启动	①发送测试指令 1：破坏 NorFlash 引导程序副本 1 ②计算机板重新上电
3	NorFlash 引导程序副本 3 启动	①发送测试指令 2：破坏 NorFlash 引导程序副本 2 ②计算机板重新上电
4	MRAM 单份引导程序副本启动	①发送测试指令 3：破坏 NorFlash 引导程序副本 3 ②计算机板重新上电
5	ENVM 单份引导程序副本启动	①发送测试指令 4：破坏 MRAM 引导程序副本 ②计算机板重新上电

具体的测试过程为：1）首先通过地面测试系统，将片外 NorFlash 芯片的 3 个引导程序副本 1、片外 MRAM 芯片引导程序副本和片上 ENVM 引导程序副本进行固化；2）对星载计算机进行正常加电，测试 FPGA 逻辑对片外 NorFlash 引导程序副本 1 的加载运行情况；3）通过地测通道发送“破坏 NorFlash 引导程序副本 1”测试指令，并对星载计算机重新加电，测试 FPGA 逻辑对片外 NorFlash 引导程序副本 2 的加载运行情况；4）通过地测通道发送“破坏 NorFlash 引导程序副本 2”测试指令，并对星载计算机重新加电，

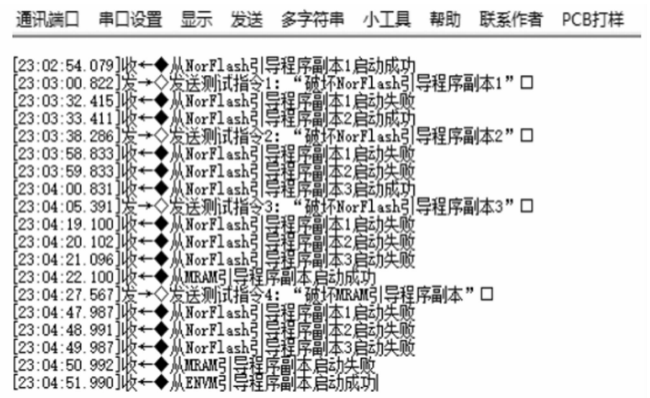

图 6 多 TMR 副本的启动方法验证结果图

测试 FPGA 逻辑对片外 NorFlash 引导程序副本 3 的加载运行情况；5）通过地测通道发送“破坏 NorFlash 引导程序副本 3”测试指令，并对星载计算机重新加电，测试 FPGA 逻辑对片外 MRAM 引导程序副本的加载运行情况；6）通过地测通道发送“破坏 MRAM 引导程序副本”测试指令，并对星载计算机重新加电，测试 FPGA 逻辑对片上 ENVM 引导程序副本的加载运行情况。

4 结束语

为了满足低成本微纳卫星对高可靠性的要求，本文采用工业级处理器 SmartFusion2 设计了一种低成本高可靠的星载计算机最小处理系统。针对 SmartFusion2 星载计算机架构，本文提出了一种多 TMR 副本的片外启动方法，既实现了 Cortex M3 内核的片外启动，还将引导软件的副本进行三模冗余处理，并分别存储在异构存储芯片，进一步提高了系统引导可靠性。

参考文献：

[1] 徐 楠，李朝阳，王兆琦，等. 高轨卫星星载计算机优化设计与实现 [J]. 中国空间科学技术，2020，40 (1)：94－100.
[2] 刘伟鑫，汪 波，马林东，等. 低成本和商业卫星元器件抗辐射保证流程研究 [J]. 微电子学，2020，285 (1)：80－85.
[3] 刘凯俊，彭 攀，王新元. 基于 COTS 器件的高费效比商业卫星计算机研究 [J]. 计算机测量与控制，2018，26 (11)：213－217.
[4] 李 杰，沈 锐. 空间计算机冗余架构可靠性分析比 [J]. 深空探测学报，2018，5 (6)：575－581.
[5] 高宗彦，王志国，苏嘉玮，等. 基于 SM750 的嵌入式星载计算机设计 [J]. 航天标准化，2020，180 (2)：36－39.
[6] 赵 波，姜大力. SOC 技术在星载计算机系统中的设计与应用 [J]. 仪器仪表学报，2011，32 (6)：36－39.
[7] XU W，PIAO Y. Bootstrap loader design of aerospace payload controller based on TSC-695F [C] //Second International Conference on Computational Intelligence and NaturalComputi-ng. 2010：60－64.
[8] 熊浩伦，闫国瑞，李国军，等. 基于最小系统的小卫星在轨软件重构系统设计 [J]. 遥测遥控，2020，41 (3)：48－55.
[9] 王 钊，李 勇，崔维鑫，等. 一种星载嵌入式软件容错启动系统设计 [J]. 电子设计工程，2019，27 (8)：1－5.
[10] 李光学，孙宇伟，何雨昂，等. 基于 SOPC 技术的综合电子系统应用 [J]. 电子技术与软件工程，2019 (14)：101－102.
[11] 谭竹慧，李华旺，常 亮，等. 基于可编程 SOC 的多节点星上温度采集系统设计 [J]. 电子设计工程，2016，24 (16)：54－57.
[12] Microsemi. SmartFusion2 system-on-chip FPGAs datasheet [EB/OL]. [2012-02-15]. http：//www.microsemi.com/products/fpga-soc/soc-fpga/smartfusion2.
[13] 一种 AHB 总线矩阵 IP 核的设计与实现 [J]. 计算机应用，2018 (6)：64－68.
[14] 罗惠文，吴 斌，尉志伟，等. AHB Matrix 互连总线 IP 的设计与实现 [J]. 微电子与计算机，2015，32 (10)：54－57.
[15] 朱亚杰，王劲强，石志成，等. 一种基于向量表的在轨程序上注方法的研究 [J]. 电子设计工程，2013，21 (11)：140－143.
[16] JOSEPH Y，姚文详，宋 岩. ARM Cortex-M3 权威指南 [M]. 北京：北京航空航天大学出版社，2009.
[17] AO R，CHEN Q Q，LI Z W，et al. Multi-objective evolutionary design of selective triple modular redundancy systems against SEUs [J]. Chinese Journal of Aeronautics，2015，28 (3)：804－813.
[18] 张 超，赵 伟，刘 峥. 基于 FPGA 的三模冗余容错技术研究 [J]. 现代电子技术，2011，34 (5)：167－171.
[19] International Electrotechnical Commission. American National Standards Institute. Euro-card Specification：IEC 60297-3 and-4 [S/OL]. (2004-08-22) [2021-03-16]. http：//www.iec.ch.
[20] 陈寅昕，葛逸民，单悌磊，等. 一种新型 PC104 板卡用堆栈组合体结构 [P]. 中国：CN109041501A，2018－12－18.

(上接第 228 页)

[75] 张 驰. 风电场短期风速预测若干问题研究 [D]. 南京：东南大学，2017.
[76] 周亚同，赵翔宇，何 峰，等. 基于高斯过程混合模型的大气温湿度预测 [J]. 农业工程学报，2018，34 (5)：219－226.
[77] POPESCU S G，SHARP D J，COLE J H，et al. Distributional Gaussian process layers for outlier detection in image segmentation [C] //International Conference on Information Processing in Medical Imaging，Springer，2021：415－427.
[78] 范文超，李晓宇，魏 凯，等. 基于改进的高斯混合模型的运动目标检测 [J]. 计算机科学，2015，42 (5)：286－288，319.
[79] BLUM M，RIEDMILLER M. Electricity demand forecasting using Gaussian processes [C] //Proceedings of the 15th AAAI Conference on Trading Agent Design and Analysis，AAAI Press，2013：10－13.
[80] 尹金良，朱永利，俞国勤，等. 基于高斯过程分类器的变压器故障诊断 [J]. 电工技术学报，2013，28 (1)：158－164.