文章编号:1671-4598(2018)11-0213-05 DOI:10.16526/j.cnki.11—4762/tp.2018.11.047 中图分类号:V19 TP368.2 文献标识码:A

基于 COTS 器件的高费效比商业卫星计算机研究

刘凯俊[1,2]，彭 攀[2]，王新元[2]
（1. 上海交通大学 电子与通信工程学院，上海 200240；
2. 上海卫星工程研究所，上海 200240）

摘要：对国内外基于 COTS（commercial off—the—shelf）器件的商业卫星计算机进行了研究；针对商业卫星公司对卫星可靠性、运算性能、成本控制、研发周期等要求和实际空间运行环境，分析了目前国内外商用卫星的设计模式和特点，提出一种基于汽车级 COTS 器件的商业卫星单板计算机系统；在可靠性设计上采用了 EDAC、双核 Lock—Step 等技术，选用单粒子免疫的器件的 MRAM 和反熔丝 FPGA，在保证计算机系统安全性、可靠性、成本控制和运算性能的同时，避免了多核或多处理器冗余加固方案导致的额外软件开发成本，缩短产品研发周期；研究对基于 COTS 器件的商业卫星计算机的可靠性设计有一定参考价值。

关键词：商业卫星；单粒子；EDAC；Lock—Step；COTS

Research on Cost—Effective Commercial Satellite Computer Based on COTS Devices

Liu Kaijun[1,2], Peng Pan[2], Wang Xinyuan[2]
(1. School of Electronics and Communication Engineering, Shanghai Jiao Tong University, Shanghai 200240, China;
2. Shanghai Institute of Satellite Engineering, Shanghai 200240, China)

Abstract: This paper research on commercial satellite computers based on COTS (Commercial Off—The—Shelf) devices at home and abroad. Focusing on the requirements of commercial satellite companies on satellite reliability, computational performance, cost control, and research and development cycle, and the actual space operation environment, the current domestic and foreign commercial satellite design patterns and characteristics are analyzed, and a commercial satellite single board computer system based on COTS devices is proposed. In the reliability design, EDAC, dual—core Lock—Step and other technologies are adopted. The MRAM and anti—fuse FPGA of the single—particle immunity device are used to ensure the security, reliability, cost control, and computing performance of the computer system. It avoids the extra software development cost caused by the multi—core or multi—processor redundancy reinforcement scheme and shortens the product development cycle. Research has certain reference value to the reliability design of commercial satellite computer based on COTS device.

Keywords: commercial Satellite; single event effect; EDAC; Lock—Step; COTS

0 引言

随着近年来航天产业的不断发展，商业卫星发射的爆发式的增长，按照传统 3～5 年的大卫星的研发周期不能满足商业航天的业务需求。宇航级的器件受到禁运、供货周期长，并且价格昂贵等特点限制，是影响商业航天公司对卫星成本和风险控制的主要因素，因此采用商业现货（COTS）器件替代宇航级器件成为了商业航天公司发展的一个主要方向。但是 COTS 器件通常不能直接在空间应用上直接使用，需要利用三模冗余（TMR）技术或者其他冗余措施来避免空间效应引起的故障，而通常该类冗余措施使系统设计复杂化，增加了额外的开发成本，引入了新的技术风险。

本文综合对比了国内外一般 COTS 器件的星载计算机设计模式。考虑到商业卫星在空间实际工作环境，如大部分商业卫星为低轨观测或通讯卫星，设计寿命较短，以及星载业务处理能力的需求不断提高，提出了一种基于 COTS 器件的高费效比商业卫星计算机。该计算机平台根据商业卫星运行环境的特点，合理的选用冗余加固措施，在保证星载计算机平台运行安全可靠的同时，不复杂化系统设计，提高了卫星的星载业务处理能力，满足商业卫星空间工作安全性、可靠性和星载业务扩展的需求。

1 国内外商业卫星计算机分析

目前商业卫星公司对卫星产品的设计模式还是在摸索阶段，发射的卫星大多为工作在 100～1 000 km 的低轨地球观察卫星或者商业通讯卫星。一般空间辐射环境中会引发器件产生故障的主要有辐射累积的总剂量效应（TID）和单

收稿日期:2018-04-19； 修回日期:2018-05-23。

作者简介:刘凯俊(1989-)，男，上海人，硕士研究生，主要从事星载计算机方向的研究。

粒子事件（SEE）。在这个轨道上辐射总剂量引起的故障不严重，约为 1～2 rad（Si）/天，一般器件耐辐射剂量在 5 krad（Si）以上[4]，考虑到贴铅皮和卫星结构等屏蔽措施，总剂量指标满足大部分商业卫星的寿命要求，所以对于低轨卫星来说引发故障的主要原因是由高能带电粒子造成的单粒子翻转。受单粒子翻转影响最大的是大规模逻辑处理芯片和存储器件，有针对性的对 COTS 器件实行板级和系统级的冗余加固措施可以有效的避免单粒子引起的功能中断。

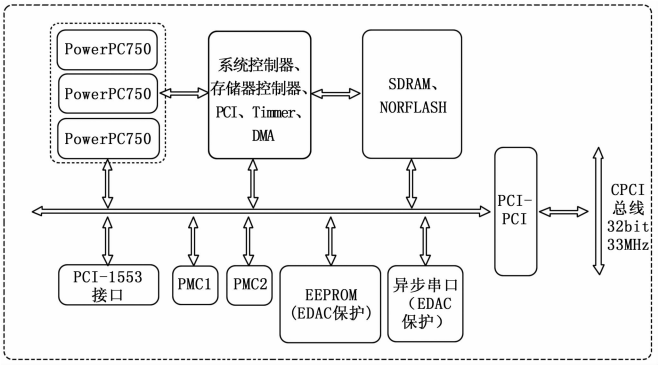

图 1 SCS750 板计算机体系框图

图 1 是美国 MAXWELL 公司的 SCS750 单板计算机的系统结构框图，该设计综合了芯片 TMR 的三模冗余技术、指令同步技术和 EDAC 技术，选用 3 个 IBM 的 PowerPC750Fx，通过表决机制输出计算结果，并且使用 EDAC 技术保护存储系统，在检测到 3 个处理器输出结果不一致的时候，通过程序 s 的回卷，再重新同步，继续执行，SC750 在保证处理器在轨运行可靠性的同时，处理能力达到了 1 800 MIPS[1]。

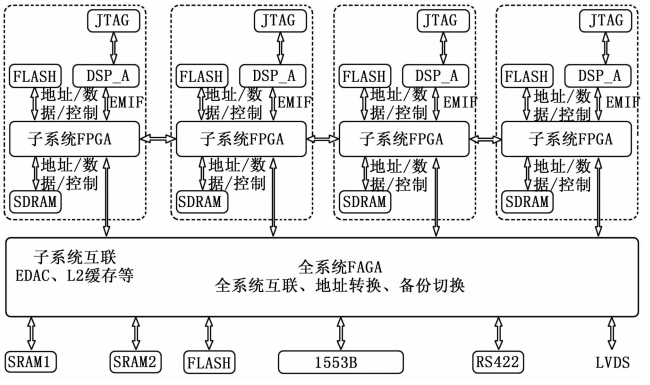

图 2 “4DSP＋FPGA”体系框图

图 2 是以高可靠的并行星载计算机任务为需求，构建了“4DSP＋FPGA”的多处理器并行星载计算机体系结构，提出了运行一种“3＋1”（3 并行 1 备份）的工作模式，可以将出错的处理器进行替换提升了系统的可靠性，同时利用了 DSP 快速、丰富的对外接口实现多处理器的数据信息交互，以保证计算机的高性能需求[2,10]。

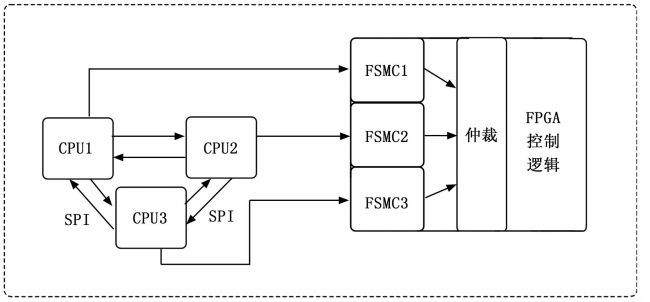

图 3 基于三模冗余通用计算机体系框图

图 3 同样为针对低成本高可靠商用小卫星方案给出的基于三模冗余的微纳卫星通用计算机平台，FPGA 根据每次收到的 CPU 的最新状态后进行更新，仲裁模块根据 3 个 SPI 数据冗余交换区的数据进行三取二判断，将判决结果告知各 CPU，各 CPU 依据判决结果，判断自己是否为当班计算机[3]。片外存储芯片为了减少面积和 FPGA 的设计复杂度，选用了自带 EDAC 的 SRAM 器件。

由于受到 COTS 器件等级的限制，大多数 COTS 没有芯片级的抗辐射设计和辐射指标，采用系统级的多核或多处理器冗余设计，可以有效的弥补 COTS 器件在宇航应用中可靠性上的缺陷。但是多核或多处理器的冗余加固设计需要在同步点比对处理器的输出结果[1-2]，多点的分布式同步设计增加了系统调试和故障分析的复杂性，引入了额外的技术风险。

2 基于 COTS 器件的高费效商业卫星计算机

2.1 系统架构设计

一般将产生的故障分为两类：一类是可检测故障，在产生故障后进入故障处理现场，进行故障处理和隔离，避免故障进一步传播；第二类是产生不可检测故障，程序继续执行，故障传播直至卫星平台崩溃。第二类故障几乎是灾难性的，在选用 COTS 器件或组件进行计算机系统设计的时候，需要尽可能的避免第二类故障的发生。

对计算机系统内各个功能模块进行分类，大致可分为：处理器模块、存储器模块、接口通讯模块、运行保障模块。

1）处理器模块可以通过关键器件三模冗余的策略，检测关键器输出的结果，当检测结果不一致，进入到故障处理模式，或采用单粒子免疫的反熔丝器件。

2）存储器模块的单粒子翻转故障可以通过软硬件的 EDAC 技术降低发生功能中断故障的概率，或者选用单粒子免疫的磁性随机存储器（MRAM）。

3）接口通讯模块的故障依赖通讯协议来保障，当通讯中发生校验错误或超时响应，通过重新请求数据或者编码还原原始数据。

4）运行保障模块故障，一般不能被本板计算机检测，只能通过切机操作，切换到备用计算机运行，断电复位故障机器。

综合考虑计算机系统的运算性能、可扩展性、可靠性和可测试性，选用了汽车级的双核锁步处理器作为核心处理芯片。片外存储器为了简化 FPGA 和 PCB 板的设计，选用单粒子免疫的磁性随机存储器（MRAM）。MRAM 掉电不易失，可以作为掉电复位后的重要数据备份区，并且有和 SRAM 一样的访问速度。使用单粒子免疫的反熔丝器件 FPGA 作功能接口和 CPCI 总线的扩展，在 FPGA 内对关键寄存器和内部 RAM 做 TMR 和 EDAC，计算机系统框图如图 4 所示。

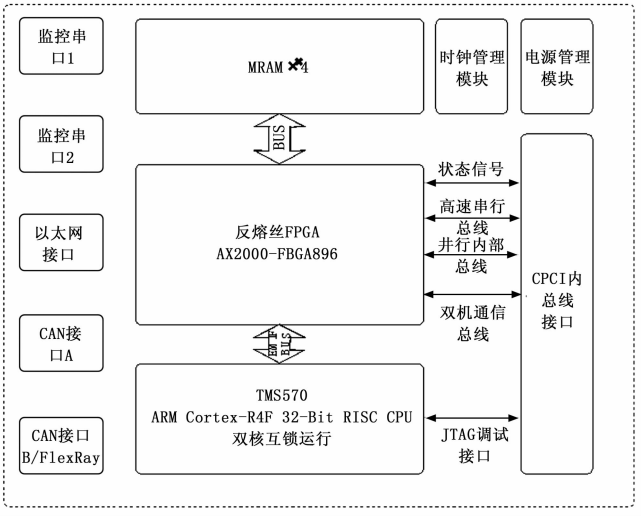

图 4　基于 COTS 器件商业卫星计算机系统框图

2.2　核心器件的可靠性分析

主处理器选用 TMS570LS3137 为内嵌 Cortex－R4F 带有浮点运算的微处理器，该芯片运行再 180 Mhz 主频下，处理性能高达 298 MIPS。TMS570LS3137 器件是一款用于安全系统的高性能汽车级系列微控制器。此安全架构包括：以 Lock－Step（锁步模式）运行的双核 CPU 和 3 MB 带 EDAC 的内置 FLASH 和 256KB 带 EDAC 内嵌 SRAM。针对商业低轨卫星，高能带电粒子引起的单粒子效应是引起卫星故障的主要因素，内嵌 EDAC 技术的 FLASH 和 SRAM 有效降低了单粒子效应引起的功能中断和不可检测故障的概率。

图 5 为 TMS570 的双核锁步运行模式框图。检测芯片和主芯片分别前后延迟两个时钟周期以后，在比较模块中进行输出比对，若发生比对错误进入到故障处理模式中，避免故障继续传播。双核锁步的这种方式不仅可以减少板级系统设计的额外开销，编程模型和单核的一致，简化了开发模型，但是这种检测方式只存在 CPU 与外部总线之间，外部资源无法检检测[5]。因此片外存储器选用单粒子免疫掉电不易失的 MRAM 器件，并且 TMS570 片内的存储器件采用 EDAC 进行数据冗余，确保卫星系统的正常运行。

2.3　软件可靠性分析

eCos 是一款面向深度嵌入式应用的开源实时操作系统

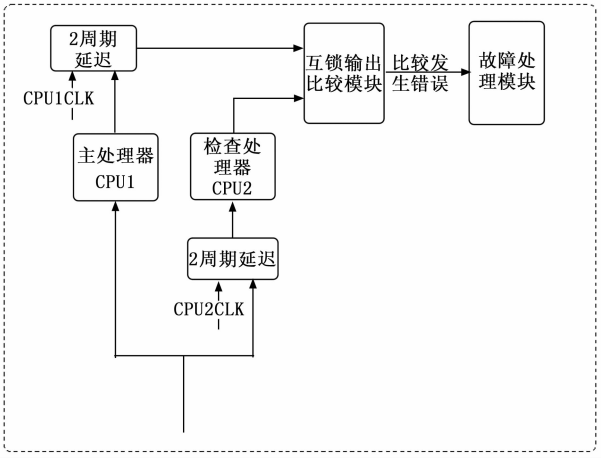

图 5　TMS570 双核锁步模式框图

（RTOS）。它已被部署在各种各样的市场和设备上，在空间应用和地面终端上有较多的应用案例。2011 年 5 月，“奋进号”航天飞机于 2011 年 5 月 16 日成功发射，并将 Alpha 磁谱仪（AMS）宇宙线探测器运送到国际空间站中，其中作为主数据采集的四冗余计算机采用了 eCos 做为操作系统[6]。Thrane 公司的 Sailor mini－C 海事卫星终端采用了 eCos 操作系统负责舰载安全，导航和星地网络一体化通信系统。功能包括遇险警报和消息，电子邮件，传真，GPS 位置调查报告和记录[7]。

图 6 是 TMS570 的地址映射表。在软件开发中，eCos 将任务主要分为两部分：星上业务任务，包含了数管业务和姿轨控业务；运行可靠保障任务，运行可靠保障任务为低优先级的背景任务，主要负责遍历读取存储器的各地址段和对重要数据进行自主的冗余备份。运行可靠保障任务遍历读取片内 FLASH 地址段 0x20000000～0x202FFFFF，片内 SRAM 地址段 0x08000000～0x083FFFFF，如果发生单比特为位的单粒子错误，则产生单比特中断，由软件回写正确数据。若发生多比特中断，复位当前机，若功能仍异常，则将控制权交给备份机器，以免故障影响范围扩大。运行可靠保障任务还对重要关键数据自主的备份到 0x6400000 地址段，该地址段为 MRAM 映射地址段。

2.4　系统可靠性分析

TMS570 无法配置成从片外 PROM 启动，并且程序空间位于片内 FLASH，若片内 FLASH 发生单粒子翻转则会产生不可恢复故障。因此针对片内用于存储程序段的 FLASH 进行分析。FLASH 的翻转以 FLASH K9XXG08UXA 系列为参考，单粒子效应试验在线性能量传递值小于时，没有发现单粒子锁定现象，空间辐射环境采用 ADAMS 90％最坏情况模型，太阳同步轨道高度 965 Km，单粒子翻转错误发生概率大约为[8]。K9XXG08UXA1 以 8 Gbit 为例，可知单比特翻转概率为，TMS570 片内 FLASH 为 3MByte，同时在一个编码区里面发生两位比特位的翻转才会发生不可恢复的单粒子功能中断，因此发生

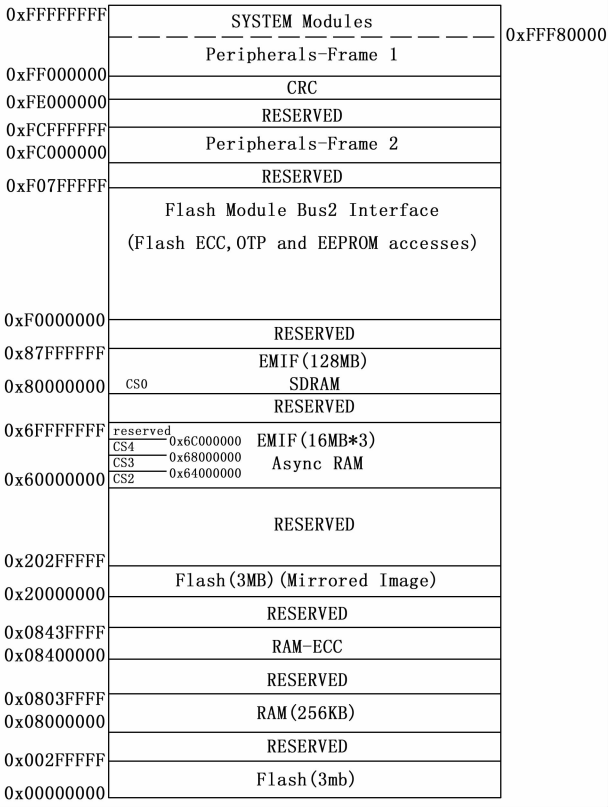

图 6 TMS570 地址映射表

两位或两位以上的不可恢复故障概率为。

$$f(x) = P^2 \times Q \tag{1}$$

式中，P 是器件单比特翻转概率，Q 是 EDAC 编码后的逻辑字节大小（即 8 bit+编码区比特）。同样的，在这个轨道上 SRAM 约为，DRAM 约为[4]，TMS570 片内 SRAM 为 256 KB，则发生两位或两位以上不可恢复的概率为。TMS570 在双核互锁模式只有两个 CPU 输出相同才会输出，在发生单粒子翻转并且双核输出一致的概率很小，认为不会发生，因此满足低轨商业卫星的实际生产要求。

2.5 系统优缺点分析

由 2.4 的论证可知，存储器采用 EDAC 技术或采用单粒子免疫的 MRAM 器件进行加固，安全性和可靠性均能满足低轨卫星的运行环境的要求，而直接对处理器进行三模冗余加固受到工艺的限制，比较困难，因此影响商业计算机系统安全的主要是由单粒子翻转引起的处理器内部寄存器的跳变导致的 PC 指针错误跳转、错误地址操作等。通常处理器的加固方案是通过多核或多处理器冗余备份和自检，进行故障隔离和快速恢复。

2.5.1 指令同步三模冗余（TMR）星载计算机

以 SCS750 单板计算机是指令同步的三模冗余星载计算机，其故障现场处理流程如图，当检测到单粒子翻转以后，三态隔离故障处理器，通过 TMR 技术保存正确数据到有 EDAC 加固的存储器中，回写正确数据到故障处理器中，重新同步 3 个微处理器。SCS750 片外存储区同样采用 EDAC 技术加固措施。运行在 LEO 和 GEO 轨道，单板发生不可检测的单粒子故障概率约为，故障恢复时间为 1 ms[9]。该设计方案为三核指令同步运行，对于软件设计来说屏蔽了底层多核的故障隔离和备份操作（由 FPGA 完成），可以基本继承单核的开发模式，操作系统移植也较为简单，但是 FPGA 基于 60x 的三核锁步运行实现比较困难。PowerPC 的性能高但是功耗大，以国微 SM750 为例，单核处理器运行在 150 Mhz 情况下，功耗约为 5 W，则推算三核冗余方案为 15 W。

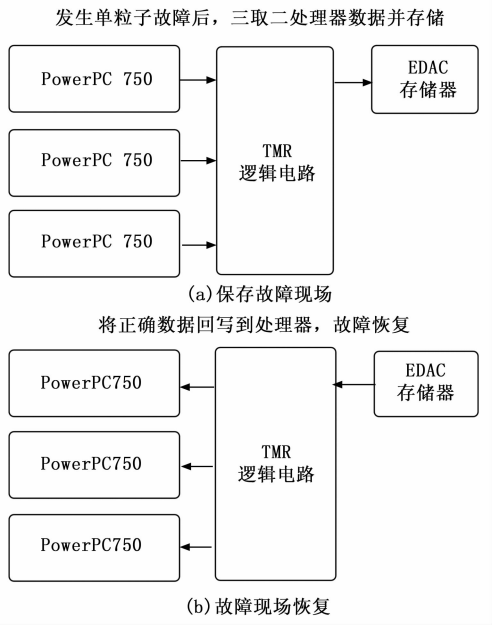

图 7 SCS750 单板计算机故障处理示意图

2.5.2 任务同步多处理器星载计算机

多处理器星载计算机通过约定同步点来达到功能模块或者任务的同步，载同步点进行输出结果比对和恢复点。以多处理器大规模星载计算机为例，工作在“3+1”模式下，备份 DSP 根据各个 DSP 历史运行数据进行判断，然后对某个运行 DSP 进行备份，DSP 运行的时候通过设置“比较点”和“比较队列”，并且对处理的任务进行“处理进度备份”和快速“恢复站”技术，通过比较“比较队列”的输出结果，最优情况可以在出现问题以后，在比较点无缝衔接，但是最差情况需要等待故障处理器重启，恢复到比较点继续运行[10]。该计算机系统的故障恢复性能对插入“比较点”的位置选择和如何选择任务模块的划分依赖很大，软件设计模式和计算机系统设计的耦合度较高，增加了额外的设计成本和风险。

2.5.3 指令同步双核互锁星载计算机

双核 Lock－Step 处理器同样屏蔽了底层多核故障隔离的操作，同样继承了单核软件的开发模式。但是双核 Lock－Step 处理器为指令同步自检输出，没有故障恢复功能，因此在出现问题后直接进入到故障处理入口，进行复位操

作或者其他故障隔离措施，图 8 是双核 Lock－Step 处理器的故障处理流程。

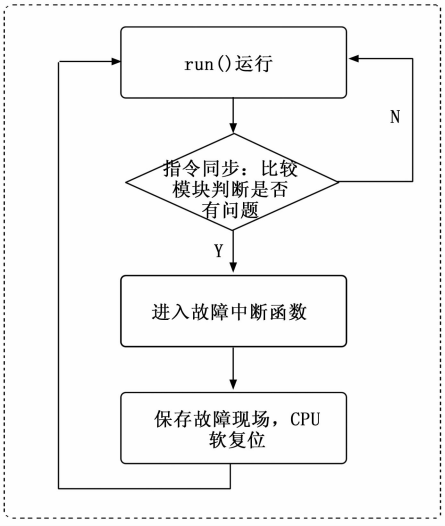

图 8　双核互锁处理器故障处理流程

2.6　小结

由表 1 可以看到，双核 Lock－Step 处理器星载计算机优点是可以继承单核的开发模式，相比任务同步的多处理器开发模型简单，并且没有额外的软件故障处理开销，298 MIPS 的处理性能和的不可测故障发生概率，已经可以满足大部分商业卫卫星处理平台的要求。缺点是相比指令同步的三模冗余计算机在处理器发生故障以后，只能进行故障隔离重启恢复计算机，因此在设计系统软件的时候需要控制处理器的启动时间。

表 1　3 种星载计算机设计模式比较

名称	指令同步三模冗余计算机	任务同步多处理器星载计算机	双核互锁处理器星载计算机
编程模型	单核	多核	单核
功耗	27W	7.5W	4.35W
运算性能	1800MIPS	/	298MIPS
故障恢复时间	1ms	重启时间	重启时间
发生不可检测故障概率	2.7×10^{-5}次/天	/	6.4×10^{-8}次/天
软件故障处理开销	60x 总线指令同步，故障处理隔离和恢复	比较点选择，任务备份，任务恢复	无

3　商业应用前景

基于 COTS 器件的高费效比商业卫星计算机有着高可靠、高性能、低成本快速研发等优势，适合空间科学实验和新技术的空间应用演示，分布式空间任务的部署和快速侦查等应用。图 9 为基于 COTS 器件的高费效比商业卫星计算机，其中硬件设计方案已经应用在“和德一号”商用 AIS（船舶自动识别）海事卫星上，该卫星于 2017 年 11 月 15 日在中国太原卫星发射中心由长征四号丙运载火箭成功发射并顺利进入预定轨道，目前卫星各项技术指标正常，任务顺利展开。

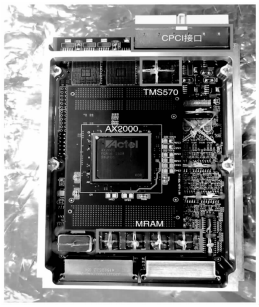

图 9　基于 COTS 器件商业卫星计算机平台

4　结论

本文针对商业卫星计算机的发展，提出了一种基于 COTS 器件的高费效比的商业卫星计算机，通过采用 EDAC 技术、选用单粒子免疫的器件和基于双核 Lock－Step 处理器，通过推论分析满足一般商业低轨卫星的工作环境要求。该系统基于 COTS 器件开发，利用双核互锁处理器单核开发模型的优势，在保证系统可靠性前提下，不增加系统的复杂度，并提升了星载数据的处理能力，降低了卫星研发成本。计算机系统已经在“和德一号”上验证，系统安全可靠，并且在空间科学实验、分布式空间任务部署和快速侦查等领域中具有良好的应用前景。

参考文献：

[1] Larry Iongden，Chad Thibodeau，Robert using Hillman，Designing A Single Board Computer For Space Using the Most Advanced Processor and Mitigation Technologies［EB/OL］. Http：//maxwell. com.

[2] 彭小燕，鹏　飞，刘凯俊，等. 一种基于多处理器的星载计算机抗辐射加固设计方案［J］. 航天标准化，2016，(2)：1－7.

[3] 何　建，张旭光，刘凯俊，等. 基于三模冗余设计的低成本高可信微纳通用计算机［J］. 计算机测量与控制，2015，23(7)：2556－2558.

[4] 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，(11)：3－8.

[5] 周　啸，李　鹏，韩　强. 基于 60x 总线的 Lockstep 处理器架构［J］. 航空计算技术，2016，45 (1)：127－130

[6] eCOS　RTOS based control system used for Alpha Magnetic Spectrometer［EB/OL］. Http：// www. ecoscentric. com.

[7] eCos and RedBoot based products showcase［EB/OL］. Http：// www. ecoscentric. com.

[8] 张洪伟，于庆奎，张大宇，等. 大容量 Flash 存储器空间辐射效应试验研究［J］. 航天器工程，2011，20 (6)：130－134.

[9] maxwell－technologies－scs750［EB/OL］. Http：//maxwell. com.

[10] 申　奥. 高可靠并行星载计算机软件容错技术研究［D］. 上海：上海交通大学，2013.