微小卫星星务计算机系统的容错控制策略研究

向 琳, 吴翔虎, 廖明宏, 崔 刚, 杨孝宗
(哈尔滨工业大学 计算机科学与技术学院, 哈尔滨 150001)

摘 要: 微小卫星系统是一个可靠性要求很高的系统, 需要由具有容错能力的星载计算机来控制。针对微小卫星重量、体积、功耗的限制, 提出了一种微小卫星的星务计算机系统的可靠性设计方案, 设计中采用双模冗余方案搭建系统的容错结构, 并根据卫星的运行要求提出了适用于微小卫星的温备份方式容错控制策略, 介绍了一些用于支持温备份方式容错控制策略的关键技术。通过分析在微小卫星设计中的适用情况, 温备份策略从硬件开销和时间开销两个方面都有利于卫星的设计。在立体测绘微小卫星"试验卫星一号"的星务计算机系统中的应用表明, 提出的可靠性设计方案能够提高小卫星的可靠性、安全性以及实时性。

关键词: 可靠性; 容错; 双模冗余; 温备份
中图分类号: TP302 文献标识码: A 文章编号: 1000-1328(2005)04-0400-05

0 引言

卫星系统是一个可靠性要求很高的系统, 需要具有容错能力的星载计算机的控制[1]。当前在卫星系统中常采用的容错控制策略有热备份、冷备份、互备援等方式。低轨返回式微小卫星采用了三模热备份方式, 海洋微小卫星采用的是双模冷/热备份方式。

三模备份方式电路最复杂, 虽然实时性最好, 但在小卫星中基本不用。

热备份方式虽然实时性最好, 但具有仲裁模块, 电路复杂, 当双机热备份比对不一致时, 仍无法判断故障机。

冷备份方式具有监控模块, 小卫星还需要模拟电路以实现安全模式, 发生故障时不具备自主的实时恢复能力, 需要地面人工干预才能恢复, 实时性最差。

"试验卫星一号"是哈尔滨工业大学自行研制的立体测绘微小卫星, 2004 年 4 月 18 日于西昌卫星发射中心成功发射, 并在轨一直稳定工作。它工作于 600km 左右的太阳同步圆轨道, 属于太阳同步轨道(SSO)卫星, 工作寿命不小于两年。

由于试验卫星一号是一个重量仅仅 204kg 的微小卫星, 其计算机系统的设计既要满足可靠性的需求, 同时又受到重量和功耗的严格限制。

根据试验卫星一号星务计算机容错子系统的设计, 本文提出了适用于微小卫星的容错控制策略, 即温备份方式。

温备份方式没有仲裁电路, 虽双机切换时间比热备份方式稍长, 但对于飞轮控制的姿态变化较慢的小卫星, 这种容错控制策略足够适用, 而且发生故障时可自动切换, 提高了小卫星的可靠性和安全性, 实时性也较好。

1 星务计算机系统的容错功能和结构

由于微小卫星重量、体积、功耗的要求, 试验卫星一号采用集中控制的设计思想, 星务计算机系统集中了卫星的定姿、遥测遥控和数据处理等星务管理功能, 因此也称作星务管理子系统[2]。由于星务管理系统是微小卫星集中控制的核心, 所以星务管理系统的可靠性就成为整星正常运行的关键。为了提高系统的可靠性, 作为核心的星务计算机节点采用冗余设计, 并配以合适的容错控制策略, 以保证星务管理和定姿控制的正确进行[3]。

容错方案的选择同样受到体积、功耗的限制, 既不能过于复杂, 又必须保证一定的可靠性。因此, 在中央处理单元的容错方案中, 比较了系统级的三模表决和双模冗余方案。由于三模表决策略在短寿命

收稿日期: 2004-09-29; 修回日期: 2005-02-27
基金项目: 国家高技术研究发展计划资助项目(863-2-8-1-1)

的应用系统中的可靠度较高, 而在较长寿命的系统中, 其可靠度小于双模冗余系统。所以在试验卫星一号中选择双模冗余作为最终的系统设计方案, 采用两个星务计算机节点互为备份, 每个节点的核心使用一个 Intel386EX 处理器。星务计算机节点通过系统通信总线与下位机相连, 执行命令的传输和状态的获取。下位机包括电源系统、通信系统和有效载荷系统等, 其中电源子系统负责整星的电源管理, 通信子系统负责星上与地面的通信。这些子系统之间通过系统通信总线构成星上计算机网络系统, 如图 1 所示。

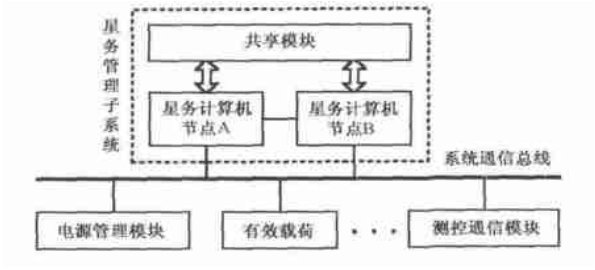

图 1　星上系统的基本结构

Fig. 1　The architecture of the computer on the satellite

利用双模设计方案对试验卫星一号的星务管理系统建立可靠性模型[4], 可以得出该子系统工作两年的可靠度为 0. 9739, 高于设计要求中规定的 0. 95。因此, 星务管理子系统的可靠性能满足系统的设计要求, 卫星的实际飞行也验证了理论推算的结果。

从功能上看, 星务管理子系统由星务计算机节点、系统通信总线、A/D 模块、D/A 模块、D/D 模块、存储单元等组成。每个星务计算机节点包含私有的处理器和存储器模块, 并可以与共享模块进行交互。共享模块包括 A/D 模块、D/A 模块、D/D 模块等, 与两个星务计算机节点相连。在正常状态下, 只有主机具有共享模块的访问权; 在故障状态下, 共享模块将从故障机向另一计算机节点进行切换, 保证星务管理功能的连续可用。

每个星务计算机节点构成系统的一模, 包含自己的存储器系统。每个节点的存储器系统包括引导区、系统区和主存区三个部分。其中引导区存放引导程序, 引导程序负责系统的基本功能检测和操作系统的引导; 系统区存放固化的嵌入式操作系统程序, 操作系统程序需要提取到主存区来运行, 它负责星上所有事务的管理和进程的调度; 主存区存放可执行的操作系统程序和必要的数据信息, 是星上系统执行的重要媒质。

2　基于温备份的容错控制策略

系统工作期间, 采用温备份的控制策略, 选取一个节点为主机, 运行星务管理系统, 管理星上的各类大小事务; 另一个节点作为从机, 即充当系统的备份, 它平时处于待命状态, 仅当主机故障后开始运行星务管理系统, 接替星上事务的管理。

在微小卫星中, 常用来配合双模冗余硬件结构采用容错控制策略有热备份、冷备份、互备援三种。表 1 给出了这三种容错策略与温备份策略的比较, 并分析了在微小卫星设计中的适用情况。

表 1　容错控制策略的比较

Table 1 The comparison of fault-tolerant mechanisms

	检测与诊断开销	恢复时间	通信开销	失效率	并行性	适用性
热备份	较大	较短	较大	较大	无	较好
冷备份	较大	较长	无	最小	无	一般
互备援	最大	最短	最大	最大	最强	较差
温备份	极少	一般	极少	较小	无	好

从表 1 可以看出, 温备份策略在微小卫星中的适用性最好, 从硬件开销和时间开销两个方面都有利于卫星的设计。

热备份方式虽然实时性最好, 但具有仲裁模块, 电路复杂, 当双机热备份比对不一致时, 仍无法判断故障机。热备份方式虽然可以很快执行故障恢复, 但也由于双机的同时运行增加了失效率, 而且需要增加部分故障检测和诊断的开销。

冷备份方式具有监控模块, 小卫星还需要模拟电路以实现安全模式, 不利于系统的小型化。发生故障时需要地面人工干预才能恢复, 会增加系统的恢复时间, 对于维持系统的姿态控制是不利的, 实时性最差。

互备援方式并行性较好, 适合系统较复杂时任务的分担, 但由于双机都将处于运行状态, 关键任务失效的机会多, 而且也需要在故障检测和诊断方面带来很大的开销。

温备份方式没有仲裁电路, 虽双机切换时间比热备份方式稍长, 对于飞轮控制的姿态变化较慢的小卫星, 这种容错控制策略足够适用, 而且发生故障

时可自动切换, 提高了小卫星的可靠性和安全性, 实时性也较好。

试验卫星一号的星务管理子系统同时掌控多种任务, 在星务控制周期的 500ms 内, 既要获取所有的星上信息, 又要负责任务的调度和姿态的掌控, 所需时间较为紧张。基于减少开销的原则和卫星的实时控制要求, 设计中选择了温备份的容错控制策略。

温备份方式是主从备份方式的一种, 主机执行全部的关键任务, 从机处于监控状态, 主机故障时由从机接管全部关键任务。在这种模式下, 主机不与从机进行任何形式的通信, 减少了主机的通信开销; 监控的任务完全由从机来执行, 减少了额外的硬件开销和主机的故障检测开销; 从机作为备份机时仅运行监控任务, 监控任务涉及到的部件极少, 降低了监控机的失效率, 同时也保证了主机故障时系统的正确重构。

星务计算机运行包含两个阶段, 引导阶段和星务管理阶段。在引导阶段, 程序在引导区中运行, 完成操作系统的提取后, 转到星务管理阶段, 开始整星的控制。在温备份策略中, 主机运行于星务管理阶段, 它的代码在主存区中; 从机运行于引导阶段, 它的代码在引导区中。由于引导区容量较小, 且设计中采用只读存储器, 所以引导区每个数据位出错的概率远低于主存区, 从而降低了从机在监控时的失效率。再加上采用被动监听方式工作, 涉及到的系统部件少, 进一步保证了从机的稳定运行。

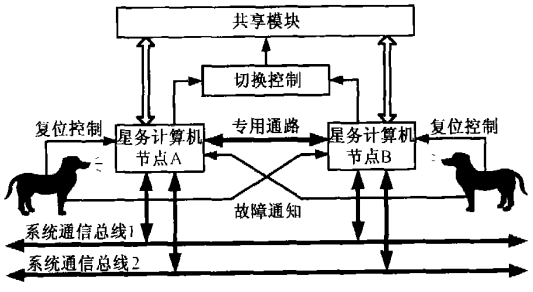

图 2 星务管理子系统的容错结构框图

Fig. 2 The framework of house-keeping system

图 2 描述了基于温备份思想的系统容错控制结构。假设初始状态下 A 机为主机, 则 B 机在引导区运行监控程序, 充当备份。当 A 机出现故障时, 如果可以利用容错设计将其屏蔽, 则不做其他的处理。如果故障引发的失效不是致命的, 可由 A 机自行软复位, 同时通知 B 机接替星务管理工作; 如果故障引发了致命的失效, A 机出现死锁或没有响应, B 机将通过系统通信总线的侦测或 A 机看门狗电路的故障通知, 证实 A 机的故障状态, 然后 B 机接管星务管理工作, 完成系统的重构。由于采用温备份策略, B 机失效率极低, 而且重构时间也很短。系统的重构以切换控制模块为支持, 在星务管理容错软件的调度下进行。A 机故障修复后, 将重新加入系统, 执行温备份的监控功能。

3 可靠性关键技术

星务管理子系统的可靠性设计中, 采用了一些关键技术来支持温备份的容错控制策略, 本节将作以简单介绍。

3.1 存储器系统编码策略

在卫星飞行的过程中, 星务计算机内的存储器系统会受到空间辐射的影响, 容易出现故障, 所以在容错设计中采用编码技术对存储器系统提供保护[5]。

主存区采用检错和纠错编码(EDAC 编码)来克服 SEU 的危害。选择的 EDAC 编码芯片是 74LS630。该芯片采用汉明编码, 把 16 位数据字和 6 位校验字对应起来, 支持编码的生成或检查。编码机制要求主存区每两个字节的数据信息要有 6 位校验字与之对应, 所以需要增加一个存储器芯片以存放校验信息。加入编码机制后的主存区数据访问由四个阶段组成:

(1) 数据准备: 从主存中将所需数据读出, 准备进行编码检查。

(2) 锁存校验: 锁存读出数据, 并进行校验, 判断编码的正确性。

(3) 纠错处理: 如果编码有误, 纠正错误的编码。如果进行写操作, 则重新生成新编码。

(4) 更新恢复: 将纠正后的数据信息传送到 CPU, 并同时更正主存区中的内容。

存储器系统的引导区和系统区存放的是固定的信息, 采用只读存储器来实现。为了保证系统信息的完整性, 针对引导区和系统采用了分段编码的技术, 以 256 字节为单位进行编码处理。在使用相应信息时, 可先行检验编码是否正确, 然后再提取到主存区执行。

3.2 冗余通信总线

随着各种智能芯片纷纷嵌入到航天计算机的各个子系统中替代传统电路, 微小卫星系统通信总线上的数据量越来越大, 系统通信总线的通信能力和

容错能力显得越来越重要[6] 。我们提出了双冗余系统通信总线的设计方案, 方案的核心思想就是总线备份、出错切换。为此, 系统通信总线需要提供总线的故障检测、故障隔离和故障恢复的功能。

系统启动之后对两条总线都进行初始化, 使得他们都具有通信能力。系统开始正常的通信之后各功能模块之间的数据在某一总线上进行数据通信, 发送的报文和接收报文分别采用 CRC 编码和 CRC 校验, 可用于检测系统通信总线是否出现故障。通过两个错误计数器——接收错误计数器和发送错误计数器——来记录故障信息。当故障计数器超出报警极限, 说明错误条件已过分积累, 将切换到另一总线上以保证正常通信, 同时隔离出错的总线。隔离后对故障总线进行故障恢复, 如果是偶然性错误, 该总线就能重新恢复工作作为备份总线。

3.3　切换部件的三模表决设计

切换器在容错系统中是非常关键的部件, 它的工作正常与否直接影响到系统的可靠性等性能, 只有高可靠性的切换器才能胜任容错系统中故障的隔离及模块的切换。星务计算机的切换器采用三模表决的方法进行设计, 保证在切换器局部受到干扰或遭遇故障时, 仍能正确执行切换操作。切换器支持主动切换和被动切换两种方式, 当某个星务计算机节点发现对方故障时, 可执行主动切换, 取得全部共享设备的控制权; 反之, 当某个星务计算机节点发现自身故障时, 可执行被动切换, 出让全部共享设备的控制权。

3.4　看门狗检测

为了避免因瞬时干扰造成系统死锁, 采用硬件看门狗对系统进行监控。每个星务计算机节点中都提供了一个硬件看门狗, 在系统引导时启动其工作, 并在每个星务控制周期中对其重新初始化。如果系统死锁, 看门狗将溢出, 并对故障机复位, 同时通知备份机进行系统重构。

4　结论

本文结合哈工大立体测绘微小卫星(试验卫星一号) 星务计算机系统的研制, 讨论了应用在微小卫星星务计算机系统的可靠性设计技术。考虑到微小卫星体积和功耗的要求和应用的特点, 设计中采用基于温备份的双模冗余结构来提高系统的可靠性。

温备份方式没有仲裁电路, 对于飞轮控制的姿态变化较慢的小卫星, 这种容错控制策略足够适用, 而且发生故障时可自动切换, 提高了小卫星的可靠性和安全性, 实时性也较好。

温备份的容错控制策略在以往的微小卫星设计中是不多见的, 试验卫星一号在运行期间的故障记录信息表明, 该策略是切实有效的, 既保证了可靠性, 也满足星上系统的实时性要求。温备份的容错控制策略由于具有诸多优点, 可以在未来的微小卫星容错设计中推广应用。

参考文献:

[1] Hihara H. A novel architecture for data management for small satellite [J]. Journal of Information Processing Society of Japan. 1995, 35(6): 497- 503

[2] SAAB Space. Study of Fault Tolerant Techniques for Satellite Data Handling[R]. SAAB Space Final Report. 1987: 48- 55

[3] Glenn Greamer, Paul DeLaHunt, Steve Gates and Marv Levenson. Attitude determination and control of clementine during lunar mapping [J]. Journal of Guidance, Control and Dynamics, 1996, 19: 505- 511

[4] 曲峰, 崔刚, 杨孝宗. TS-1.1 小卫星星务计算机系统设计[J]. 计算机工程与科学, 2002, 24(2): 96- 104[Qu Feng, Cui Gang, Yang Xiaozong. The design of house-keeping computer system for TS-1.1[J]. Computer Engineering & Science, 2002, 24(2): 96- 104]

[5] 曲峰, 崔刚, 杨孝宗, 唐心悦. TS-1.1 小卫星星务计算机 RAM 纠检错电路的设计与实现[J]. 计算机工程与科学, 2002, 24(2): 70- 76[Qu Feng, Cui Gang, Yang Xiaozong, Tang Xinyue. The design and implementation of EDAC module in the House-keeping computer system of TS-1.1[J]. Computer Engineering & Science, 2002, 24(2): 70- 76(in Chinese)]

[6] Gianluca Cena, Adriano Valenzano. Effcient implementation of semaphores in controller area networks[J]. IEEE Transactions on Industrial Electronics. 1999: 417- 427

作者简介: 向琳(1975-), 女, 博士研究生, 专业为计算机系统结构, 研究方向为容错计算技术和移动计算技术。

通信地址: 哈尔滨工业大学 320 信箱 (150001)

电话: (0451) 86413754- 603

Fault-Tolerant Mechanisms of House-keeping Computer System for The Small Satellite

XIANG Lin, WU Xiang-hu, LIAO Ming-hong, CUI Gang, YANG Xiao-zong
(School of Computer Science & Technology, Harbin Institute of Technology, Harbin 150001, China)

Abstract: Small satellites need computer systems with fault tolerance for the reason of requiring high reliability. This paper presented a reliability design for housekeeping computer systems used in small satellites. Based on the dual redundancy, the reliability design uses warm backup fault-tolerant mechanism which has the advantage of reliability and real-time control and is supported by some key technologies mentioned in the paper. An application of the reliability design to a housekeeping computer system used in Solid Measurement Micro Satellite of HIT, named TS-1 satellite, proved that the design can improve the reliability of the small satellite.

Key words: Reliability; Fault-tolerance; Dual redundancy; Warm backup fault-tolerant

(上接第 399 页)

参考文献:

[1] David G Gilmore. Spacecraft Thermal Control Handbook, Volume I: Fundamental Technologies[M]. Second Edition, El. Segundo California, USA, The Aerospace Corporation, 2002, 95-137

[2] 张加迅. 热管在航天器舷窗热控设计中的应用[J]. 南京工业大学学报(自然科学版), 2003, 25(增刊): 17-21[Zhang Jiaxun. The application of the heat pipes in the thermal design of the spacecraft porthole[J]. Journal of Nanjing University of Technology (Natural Science Edition), 2003, 25(Supplement): 17-21]

[3] 闵桂荣, 郭舜. 航天器热控制[M]. 第二版, 北京, 科学出版社, 1998, 282-296[Min Guirong, Guoshun. Spacecraft Thermal Control[M]. Second Edition, Beijing, China, Science Publishing Corporation, 1998, 282-296]

[4] 闵桂荣. 航天器热控制技术[M]. 北京, 宇航出版社, 1991, 19-22, 174-197[Min Guirong. Spacecraft Thermal Control[M]. Beijing, China, Astronautics Publishing Corporation, 1991, 19-22, 174-197]

作者简介: 张加迅(1971-), 男, 军用型号主任设计师, 高工, 专业为飞行器设计, 主要研究方向为航天器热控制、相变传热。
通信地址: 北京 5142 信箱 86 分箱(100094)
电话: 010-68746696

The Application and Simplified Thermal Analysis of the Porthole Thermal Cover Technique for Earth Observation Spacecraft

ZHANG Jia-xun, LIU Qing-zhi
(Chinese Academy of Spacecraft Technology, P. O. Box 5142 Exit 86, Beijing 100094, China)

Abstract: The application background of the porthole thermal cover was summarized firstly in this paper, and then the porthole thermal cover, which was the first time to be used in the satellite of our country, was taken as an example to introduce the typical structural and thermal design of a thermal cover for earth observation spacecraft. According to different operational states of the thermal cover, the differential equation sets of the thermal cover and the porthole glass were established and solved numerically, and the comparison was made between the numerical solution and the experimental data. By the analysis, it can be known that, the application of the thermal cover can reduce the negative thermal effects of the deep space on the temperature field of the porthole.

Key words: Thermal control; Spacecraft; Porthole