文章编号:1671-4598(2025)10-0312-08 DOI:10.16526/j.cnki.11-4762/tp.2025.10.040 中图分类号:V446+.2 文献标识码:A

低轨道商业卫星的星务计算机备份仲裁系统设计

万 军[1],史碧莹[2],邓 祺[3]
(1.上海蓝箭鸿擎科技有限公司,上海 201100;2.北京航天测控技术有限公司,北京 100041;
3.中国航空无线电电子研究所,上海 200241)

摘要:低轨道低成本商业卫星的星务计算机常采用货架器件双备份设计,在卫星主计算机出现故障时切换到备份计算机,保障卫星的稳定运行;通过对可靠仲裁和数据恢复的需求进行研究,对比了现有的冷备/热备设计,实现了一种以三模冗余为基础的特别温备仲裁电路设计方案:采用3个低复杂度的单片机作为智能判断单元,可接收地面指令主动切机,也可通过实时监控星务计算机的运行参数,按照预设逻辑自动切机;同时按周期备份任务关键参数和数据,触发切机后,能恢复系统和任务的关键任务参数,实现了星载任务的延续性;验证结果表明在故障注入后,双机切换准确并能快速恢复星载任务,提高了系统的可靠性和容错能力,实现了预期目标。

关键词:商业卫星;三模冗余;仲裁电路;星务计算机;任务恢复

An Arbitration System for Backup OBCs of Low-Orbit Commercial Satellites

WAN Jun[1], SHI Biying[2], DENG Qi[3]
(1. Shanghai Lanjian Hongqing Technology Co., Ltd., Shanghai 201100, China;
2. Beijing Aerospace Measure & Control Corp. Ltd, Beijing 100041, China;
3. Aeronautical Radio-Electronic Research Institute of China, Shanghai 200241, China)

Abstract: On-board computers (OBCs) in low-orbit low-cost commercial satellites often adopt the dual-backup design of commercial-off-the-shelf (CTOS) devices. It will switch to the backup OBC if the main OBC fails, thus ensuring the stable operation of the satellite. Research is conducted on the requirements of reliable arbitration and task parameters recovery. A comparison of existing cold/hot standby solutions is made, which achieves a special warm-stand-by arbitration circuit scheme based on triple modular redundancy (TRM). Three simple microcontroller units (MCUs) are taken as the intelligent judgment unit, it can receive ground commands and switch the active OBC, monitor the OBC' operating parameters in real time and automatically switch according to preset logic commands, periodically back up the key parameters and task data of tasks, and restore the system and key parameters and task data of tasks after triggering the switch, achieving the continuity of on-board tasks. Verification results show that after the fault injection, the dual OBC arbitration system can quickly recover on-board missions, improving the reliability and fault tolerance of the system, and achieving an expected goal.

Keywords: commercial satellites; TRM; arbitration circuit; OBC; task recovery

0 引言

低轨道卫星作为商业航天技术的重要组成部分,在通信、遥感及导航等领域发挥着重要作用。然而,由于其轨道特性,常面临复杂的空间环境,如辐射、温度变化及微重力等,这些都对卫星上的电子系统提出了严苛的要求。星务计算机作为卫星的核心控制单元,其稳定性和可靠性直接影响到整个卫星的运行状态,故障将直接威胁到卫星的整体运行。星务计算机是卫星的核心部件,主要负责姿态控制、任务管理、数据处理、遥控管理和遥测管理等任务,当卫星在轨出现故障或冲突的时候,进行有效的故障检测、故障隔离及故障处理。在空间辐射环境中,遍布着各种高能量的辐射粒子,这些粒子会对元器件带来影响,星务计算机内部的电子器件将受到高能粒子的严重影响,出现工作异常或故障。另外,星务计算机的工作特点具有长期性和不可维护性。因此,要求星务计算机需具备极高的可靠性,这对其容错设计与可靠性分析都提出了较高的技术要求。

收稿日期:2024-10-28; **修回日期**:2025-06-03。

作者简介:万 军(1987-),男,硕士,高级工程师。

引用格式:万 军,史碧莹,邓 祺.低轨道商业卫星的星务计算机备份仲裁系统设计[J].计算机测量与控制,2025,33(10):312-319.

基于商业卫星成本可控的大目标，星务计算机模块一般也由 CTOS（Commercial-Off-The-Shelf）货架型器件设计而成。在无法提高使用 COTS 器件单机可靠度的条件下，设计一套高效、可靠的双备份星务计算机冗余控制仲裁机制，形成双核心协同工作系统，对于保障低轨道商业卫星的持续运行具有重要意义。

国内外相关科技人员对使用 COTS 器件实现星务计算机备份系统的可靠性设计进行了广泛深入的研究，并发射了相关实验卫星进行验证，如美国 CFESat 卫星、SpaceX 的 Dragon 宇宙飞船、我国哈工大 TS-1 卫星、上海卫星工程研究所“和德一号”海事卫星等[1]。采用看门狗软硬件设计和地面站干预等措施提高星务计算机系统的可靠性，微小卫星星务计算机系统的备份方式有[2]：热备份、冷备份、温备加三取二等冗余方式以提高可靠性。目前各种星务计算机模块冗余备份方式的优缺点如下[3]：

1）热备份方式实时性最好，但双节点同时工作，控制管理需要权限管理模块，故障诊断算法逻辑复杂，因样本量和数据有限模型准确度无法保证，数据备份和传递都有出错的风险，同时受空间环境影响寿命不可控。

2）典型温备方式：与热备份方式类似，一个节点为主机，运行星务管理系统，另一个节点作为从机充当系统的备份，它平时处于等待状态，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工作。实时性居中，但故障逻辑判断算法也同样复杂，双节点均需要上电工作，同时受空间环境影响寿命不可控[4]。

3）冷备份方式理论上具备两倍延长寿命，一般需要模拟监控电路（电压、电流、喂狗等）以实现安全模式，监测粒度较粗，切机后星务和任务需要重新初始化，实时性最差。

根据低轨道商业卫星星座任务要求（通信、遥感等）和星务计算机容错子系统的设计，本文提出了一种新型的温备份方式的仲裁系统，双节点星务计算机模块使用冷备方式最大延长寿命，增加 3 个低复杂度的单片机 MCU（Microcontroller Unit）作为状态监测和数据备份的温备辅助系统，在成本、可靠性、实时性和策略灵活性上达到了平衡。

1　总体设计

冗余控制备份计算机系统，应遵循以下原则[5]：

1）简洁性：仲裁电路应设计得尽可能简洁，减少不必要的元器件和复杂度，以降低故障率并提高系统的可靠性。

2）快速性：在主计算机故障时，仲裁电路必须能够迅速响应并启动切换过程，以最小化对卫星运行的影响。

3）准确性：仲裁电路应能准确判断主计算机的状态，避免误切换或漏切换的发生。

4）冗余性：通过引入冗余设计，提高系统的容错能力，确保在主计算机故障时备份计算机能够无缝接管工作。

依据上述设计原则，商业卫星星务计算机一般采用最小系统多机异构来实现冗余，每个计算机均具备完整的处理能力和接口资源。这种架构能够确保在主计算机出现故障时，备份计算机能够立即接管工作。

为了实现最长寿命，双星务计算机模块采用冷备当班机制，最大程度地减少空间环境影响[6]。

为了可靠切换，本文设计一个专门的仲裁辅助系统，如图 1 所示。图中，星务计算机冗余控制方案采用了计算机心跳机制，计算机心跳机制是一种用于监控和维护计算机系统稳定的机制[7]。它周期性地发送信号（即心跳信号）来确定计算机是否处于正常运行状态。当心跳信号未能在预定时间内到达时，系统讲自动触发一系列的故障处理程序，以确保计算机系统的可用性和可靠性。

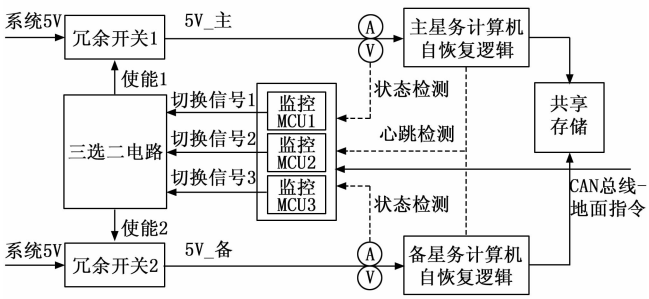

图 1　星务计算机冗余控制方案

星务计算机中的心跳信号包括 CPU 占用率、秒脉冲时间戳、卫星姿态更新状态、CPU 温度、ID 号等信息。

图 1 采用 3 个低复杂度的单片机 MCU，以三模冗余的方式检测主计算机的状态并控制切换过程。仲裁辅助系统能够接收来自主计算机的状态信号或心跳信号，根据这些信号判断主计算机是否正常运行。当检测到主计算机故障时，仲裁电路将启动切换机制，将控制权转移给备份计算机[8]。

同样，备份计算机工作时，仲裁辅助系统实时监控备份计算机状态，按需启动切换机制，将控制权转移回主计算机。

仲裁辅助系统同时可以接受从测控模块接收的地面直接切机指令、当班星务计算机重启指令和禁止/使能自动切机指令，指定当班星务计算机或禁止/使能自动切机功能。

1.1 星务计算机自恢复逻辑

当星务计算机 CPU 工作受到空间高能粒子辐射和系统的电磁等外界因素的干扰会造成各种寄存器和内存的数据混乱，导致程序跑飞，使软件陷入死循环，整个电子系统将陷入停滞状态，发生不可控制的状态。设计上首先通过看门狗自恢复逻辑处理故障，看门狗定期地查看芯片内部存储器的状态，一旦发生错误就向芯片发出重启信号的电路[9]。看门狗命令在程序的中断中拥有最高的优先级。常见的看门狗自恢复电路有两种：

1）软看门狗（见图 2）：使用程序实现看门狗喂狗和检测。缺点是 CPU 在完全死机的情况下（看门狗模块也死机）无法进行看门狗复位。

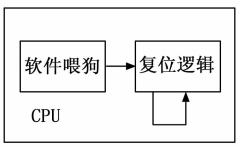

图 2 软件看门狗

2）改进型看门狗（见图 3）：在 CPU 看门狗与 CPU 复位管脚之间增加了复位芯片（类似 MAX706），复位芯片在指定时间内（一般为 1.6 s）没有收到 WDI 喂狗脉冲，就会产生一个低电平脉冲复位信号。

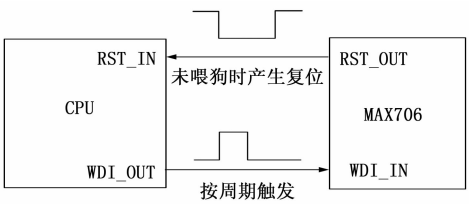

图 3 增加复位芯片的看门狗电路

当 CPU 完全死机时，CPU 的喂狗信号 WDI _ OUT 信号无输出，MAX706 的 WDI _ IN 信号接收不到喂狗信号后会通过 RST _ OUT 输出一个复位信号给 CPU 的复位管脚 RST _ IN，触发 CPU 的复位。

本设计采用第 2 种设计。在设备刚上电时，MAX706 要比 CPU 早启动，然后开始计时监控喂狗 WDI 信号的到来。故 CPU 在软件启动过程中需要给 MAX706 提供 WDI 喂狗信号，否则 MAX706 会频繁地复位 CPU，造成 CPU 无法正常启动。

CPU 通常采用 Linux 系统，在 Uboot 加载到 Kernel 的过程中，即启动提前喂狗进程。

1.2 监控 MCU 的选型

图 1 中的监控 MCU1、MCU2、MCU3 为相同软硬件设计的同一型号单片机，可以使用抗 SEU（单粒子翻转）和 SEL（单粒子锁定）的定制单片机，如国科安芯 AS32A401、Microchip SAMV71Q21RT、Microchip SAMD21RT 等。因为使用了三模冗余，本设计使用 CTOS 类型的意法半导体 STM32 类型的通用单片机来实现，通过增加异常过流等硬件保护的设计方法，在降低成本的同时，保证质量。

1.3 监控 MCU 的切换逻辑

监控 MCU 设计有两种切换方式。

1.3.1 自动切换方式

上述单片机同时接收来自主星务计算机的状态心跳信号和电源质量信号，根据这些信号判断主计算机是否正常运行。当检测到主计算机故障时，3 个单片机均输出各自的切换控制信号。3 个切换控制信号采用三模冗余的判决后，生成最终的切换信号，将控制权转移给备份计算机[10]。

星务计算机的状态心跳信号包含如下参数：

1）CPU 占用率：超过指定值（如 80%）为异常，部分进程未正确关闭；

2）秒脉冲时间戳：若连续 3 s（可配置）未收到秒脉冲时间戳，认为任务管理异常；

3）卫星姿态更新状态信息：若卫星姿态参数超过 60 s（可配置）未更新，可认定姿态运算逻辑异常；

4）主动温度检测：CPU 内置的温度传感器超范围（如超过 60 ℃）认为异常；

5）当前任务 ID 号和执行进度节点，对应任务数据在共享 emmc 中的地址。

同时每个单片机使用电压运放检测电路和霍尔电流检测电路，获得给星务计算机供电的电源电压和电流信号：

1）电源电压应在 5 V±0.3 V 的范围内，超差可认为供电异常；

2）启动后的正常工作电流应在 1.5±0.5 A 的范围内。

3 个监控 MCU 在收到上述信息后，按照既定的流程处理错误信息并输出错误标志，并对应 3 个切换信号。

错误标志的肯定及复位的步骤如下：

1）错误验证肯定：检测上述错误任一种，持续时间大于 5 s 后，即错误验证肯定；

2）设置错误标志：错误验证肯定后，10 ms 以内输出内部错误标志；

3）切换信号：错误验证肯定后，输出稳定状态切换信号；

4）复位错误标志：切换信号完成输出后或接收到指定当班指令，复位错误标志；

5）禁止错误标志：接收到自动切换禁止指令，错误标志位复位，且不再判断。

1.3.2 指令切换方式

卫星系统的测控收发机在收到地面指令后，通过

CAN 总线传递给星务计算机的同时也传递给 3 个监控 MCU。如图 1 所示，仲裁辅助系统同时可以接受从测控模块接收的地面直接切机指令、当班星务计算机重启指令和禁止/使能自动切机指令，指定当班星务计算机或禁止/使能自动切机功能。

图 4 展示两种切换模式，可由预设/地面后续上传的指令确定实施方案，逻辑如下：备份计算机当班工作后，仲裁辅助系统实时监控备份计算机状态，按上述逻辑启动切换机制，满足触发条件时将控制权转移回主计算机。

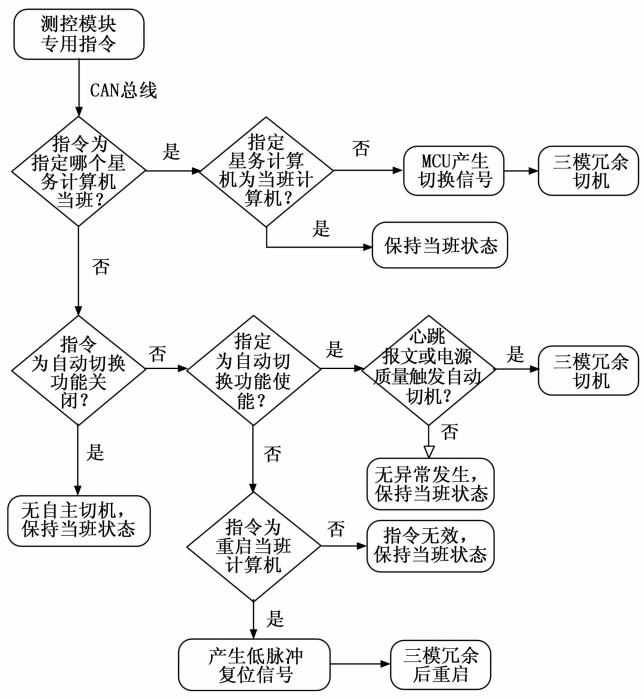

图 4　两种模式共存的判断逻辑

2　系统硬件设计

2.1　监控 MCU 设计

基于成本和采购周期等因素的考虑，星务计算机的监控 MCU 芯片采用 ARM（Advanced RISC Machine，高级精简指令集计算机）单核架构，支持控制器局部网（CAN，controller area network）总线，可以存储当班 OBC 按周期广播的关键信息。每个 MCU 自带 RTC（Real _ Time Clock，实时时钟）来存储时间戳，并通过 CAN 的 GNSS（Global Navigation Satellite System，全球卫星导航系统）广播帧按秒更新内部时钟源。每个 MCU 产生切机指令主要有两种情况[11]：

1）测控模块转发的地面指令，直接指定切换或者重启当班星务计算机。

2）测控模块转发地面指令使能了自动切机功能，监控 MCU 在综合判断了当班星务计算机的供电电压、供电电流是否正常、心跳报文是否正常、运行关键参数是否正常后，自动产生切机指令。

监控 MCU 功能见图 5，其供电 3.3 V，由 VBUS 母线双冗余 DCDC 供电。每个 MCU 自带看门狗控制自身故障断电重启。为了避免 MCU 写存储时突然断电，增加法拉电容，供电拓扑如图 6 所示。

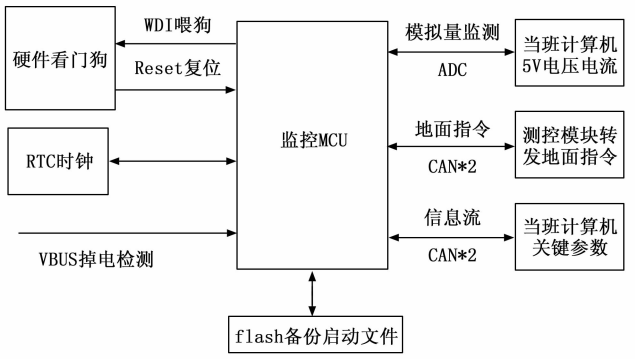

图 5　监控 MCU 主要功能

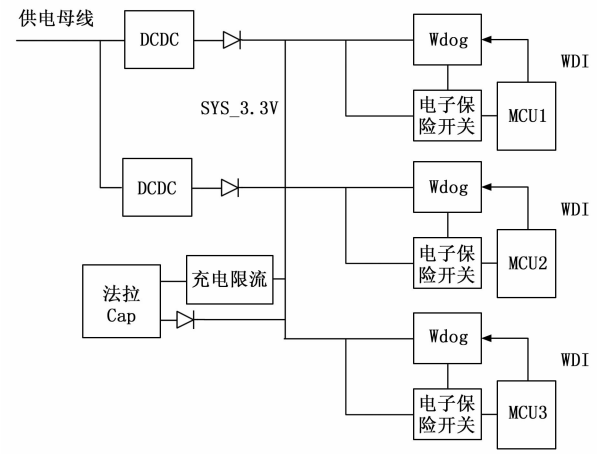

图 6　监控 MCU 供电拓扑

如图 7 所示，为了避免 SEU（单粒子翻转）、SEL（单粒子锁定）和其他异常因素，保证工业芯片级别的监控 MCU 正常工作，同样采用改进型看门狗设计，并增加过流保护的电子保险丝芯片，过流发生时断开供电 3.3 V 并经过可配置的掉电时间（如 200 ms）后自动恢复 3.3 V，经过完整的复位冷启动，彻底恢复自身的工作稳定[12]。

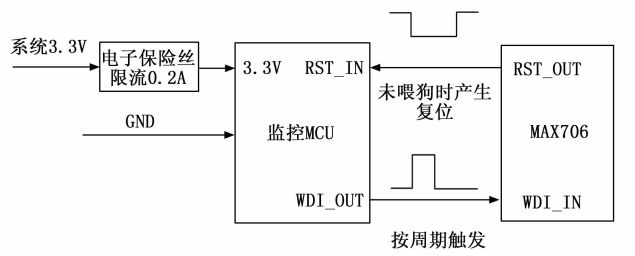

图 7　监控 MCU 自恢复逻辑

2.2 三选二控制设计

“三选二经典电路”指的是一种在电路设计中用于提高系统可靠性和准确性的电路设计结构，其中 3 个相同的模块或组件同时执行相同的操作，以多数（即两个或两个以上）的输出结果作为整个系统的最终输出。这种设计结构被称为三模冗余（TMR，triple modular redundancy）结构[13]，它在电路设计中被广泛应用以提高电路的容错能力和可靠性，三取二实现逻辑电路如图 8 所示。具有如下特性：

模块并行操作：3 个完全相同的模块电路同时接收三路输入的任意两路输入信号，并各自独立地进行处理。

多数表决系统：3 个模块电路的输出通过或逻辑集成为一个输出，只有输出高/输出低两种状态，对应到两路互斥的冗余开关的使能[14]。

实现上可通过二极管或三极管等可靠器件搭建的分立式与门和或门，在不增加复杂性的前提下实现判决的可靠。

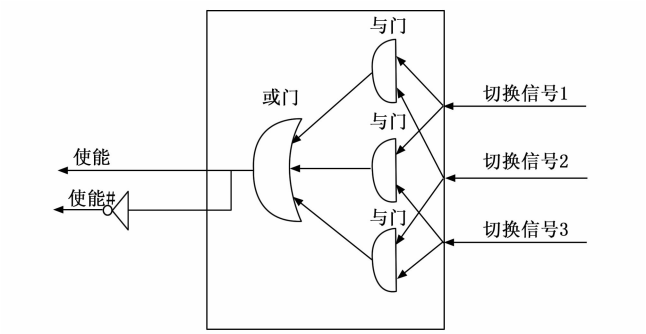

图 8 三选二实现逻辑

2.3 冗余开关设计

冗余开关指的是使用低压 mos 管或其他开关设备搭建冗余路径，提供备份路径。当主路径上的设备或组件出现故障时，冗余开关能够自动切换到备份路径，确保系统的连续运行。

1）提高可靠性：通过增加冗余组件，减少因单一故障点导致的系统停机时间。

2）增强容错性：确保系统在部分组件失效时仍能保持一定的功能或性能。

3）简化维护：在需要维护或更换故障组件时，能够方便地切换到备份路径，减少停机时间。

冗余开关实现方案上有如下特点：

1）并联冗余：将多个相同的开关并联连接，当某个开关出现故障时，冗余开关可以迅速切换到其他正常工作的开关，能够解决单个开关不能正常闭合的故障，但是不能解决不能正常断开的故障[15]；

2）串联冗余：采用串联冗余方式将相同的开关串联联连接。与并联冗余相反，能解决不能正常断开的故障但不能解决单个开关不能正常闭合的故障，可能导致整个路径失效[16]。

3）混合冗余：结合并联和串联冗余的优点，根据系统需求设计混合冗余方案。

依据子系统的设计要求，可靠开和可靠关均需要实现[17]，故采用混合冗余开关设计的方案，其逻辑电路如图 9 所示。

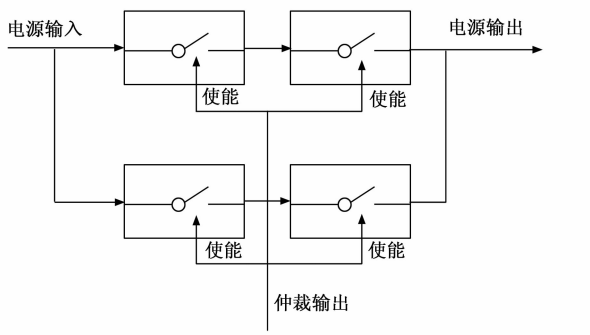

图 9 混合冗余开关设计

3 系统软件设计

主/备星务计算机内部采用软硬件看门狗设计，能应对偶发软件故障导致程序跑飞。其启动相关参数可以多份和校验的方式存储于内部 Flash，保证每次重启能读取到正确的启动参数[18]。

为了保证主/备星务计算机切机时星务任务不被中断过长时间，任务的节点信息将按照里程碑周期分别存储，以便切机后的星务计算机完成任务恢复，星务计算机自监控设计电路原理如图 10 所示。

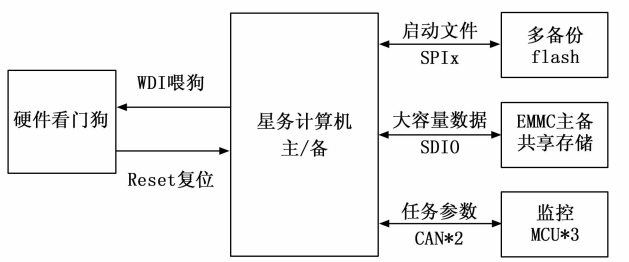

图 10 星务计算机自监控设计

其设计逻辑如下：

1）单板配置和启动相关参数：

以多份和校验的方式存储于内部双份 Flash（见图 11），默认从 Flash1 启动。如果从默认 Flash 启动校验不成功，则通过启动切换技术从备份 Flash 校验启动，并重写校验失败 Flash 的启动文件。

版本升级按照断点续传的方式，将增量升级包存储于两个 Flash 的升级版本地址段，当传输完成时，复制到当前版本地址段，并保留当前的配置参数，将启动次数配置成默认 10 次。按照图 12 的设计恢复出厂版本。

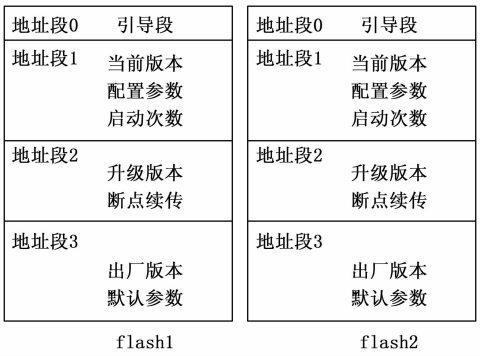

图 11　双 Flash 存储

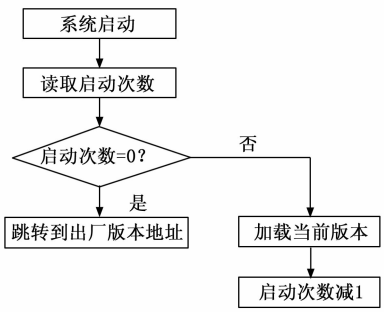

图 12　恢复出厂的跳转方式

2）任务参数和数据恢复：

为了保证主/备星务计算机切机时星务任务不被中断过长时间，任务的节点信息将按照里程碑周期分别存储于共享 EMMC 中，以便切机后的星务计算机读取并完成任务恢复。

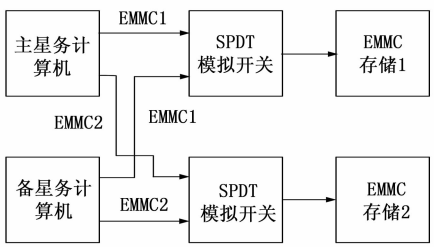

图 13　共享存储方案

如图 13 所示，共享存储逻辑如下：

1）正常工作时，当班星务计算机按周期将任务数据存储到共享 EMMC 存储 1 和中存储 2 中，以大于 20 MB/s的速度读写，并带 1 位纠错功能；

2）启动后，星务计算机通过 CAN 总线从 3 处监控 MCU 读取星务/关键任务的参数，并按照软件 3 选 2 的校验后，恢复任务节点信息。

3）如发现某一监控 MCU 数据错误，下发此 MCU 完全重启指令，并将恢复后的星务和任务参数重新下发；

4）任务节点信息恢复后，按照回读的数据地址，从共享 emmc 存储中回读任务数据，实现任务中继。

4　星务计算机冗余设计的关键技术

星务计算机的备份仲裁系统采用了如下关键技术。

4.1　一种通过添加冗余代码实现错误检测和恢复的技术

其基本思想是将软件模块分成若干个较小的恢复块，每个恢复块都有一个检验码用于检测错误，每个恢复块是独立的[19]。当出现错误时，对应的验收测试单元可以通过检测码快速识别出故障位置，并认为程序结果需要重新在另一个恢复块执行一次，当再次遇到故障时以此类推，直到结果判断可用时认为运行成功。

4.2　星务配置时间冗余技术

指通过耗费时间资源多次执行同一任务来检测和纠正可能存在的错误。具体来说，当计算机系统执行某个任务时，在不同的时间点上进行多次执行，然后将多次执行得到的结果进行比较，从而检测出潜在的错误，并采取相应的纠正措施，以确保系统的正确性和可靠性。

4.3　关键参数信息冗余技术

在数据发送和传输处理中使用的技术，可以在传输和存储数据时减少错误并提高可靠性。信息冗余通过将额外的数据添加到原始数据中，以便在出现错误时进行纠正，添加的数据位使原有的数据各位信息位的顺序产生关联性，以便于检测出是否某一位在传输过程中被更改。在两个传输设备之间加入错误检测与纠正（EDAC）电路是较为常见的方法[20]。

EDAC 编码通过在数据中添加冗余的比特位，以便在数据传输过程中检测和纠正出现的错误。它可以用于单个芯片上的内存，也可以用于分布式系统中的网络通信。EDAC 编码包括奇偶校验码、汉明码、循环冗余校验码、R-M 码、RS 码和 BCH 码等，本系统使用的是汉明码和循环冗余校验码。

4.4　星务计算机双 Flash 启动切换技术

如上所述，切换到主/备份计算机每次都不成功，考虑 Flash 启动文件问题。监控 MCU 通过选择 Flash 的片选信号，让星务计算机从备份 Flash 中读取运行程序。启动完成后，将备份 Flash 的内容复制到主 Flash，如图 14 所示。

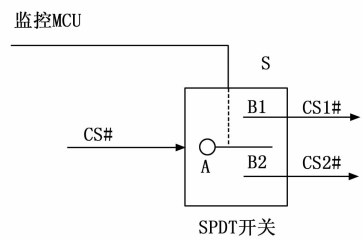

图 14　Flash 切换控制

4.5 断点续传技术

星务计算机增量升级包通过测控通道上传时，由于带宽限制，可能一轨升级不完，故采用断点续传的技术，将已传输的文件通过分段，传输给星务计算机内存，接收完成整包后，再写入双 Flash 的升级程序区。

同时，遥测报文打包下载，通过测控通道，也使用断点续传的技术，分轨接力下载，断点续传流程如图 15 所示。

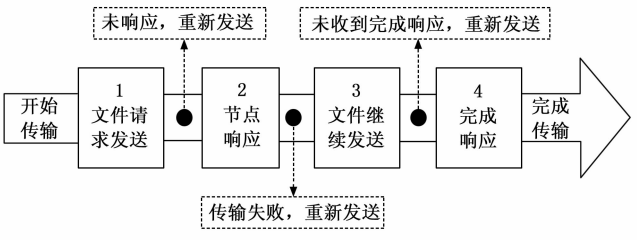

图 15 断点续传

4.6 任务数据包故障标识技术

对共享 emmc 存储中的任务数据包，按周期存储时，分成若干个较小的恢复块，每个恢复块都有一个检验码用于检测错误，每个恢复块是独立的。当任务恢复校验出现错误时，可以通过检测码快速识别出故障位置，并从备份的 emmc 存储中读取相同编号的恢复块。任务恢复后，重新按周期覆盖原来的过时数据包。

4.7 星务配置时间冗余技术

星务计算机从冗余的 GNSS 模块中可以读取两份时钟源信息，同时与通过内部高精度低温漂的时钟源守时值对比。

如果两份 GNSS 模块的时钟源同步，则更新内部的时钟源信息。

如果两份 GNSS 模块的时钟源不一致，则选取与内部守时时钟源更接近的 GNSS 的时钟源信息更新内部时钟源。

4.8 关键参数信息纠错技术

星务计算机与监控 MCU 之间的心跳数据传递、与内部 Flash 芯片之间的启动次数等关键参数的存储，使用错误检测与纠正（EDAC）技术，通过将额外的数据添加到原始数据中，以便在出现错误时进行纠正，添加的数据位使原有的数据各位信息位的顺序产生关联性，以便检测出是否某一位在传输过程中被更改。

EDAC 编码 EDAC 编码包括奇偶校验码、汉明码、循环冗余校验码、R-M 码、RS 码和 BCH 码等，本系统使用的是汉明码和循环冗余校验码。

5 实验结果与分析

按照前面的设计思路，投产实际电路的 PCBA 进行测试验证，搭建如下的测试环境如图 16 所示。

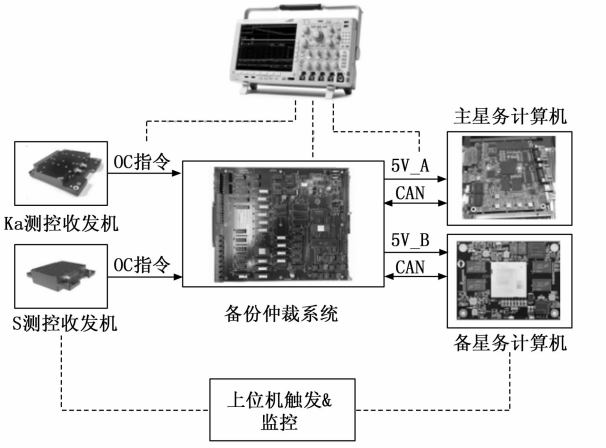

图 16 备份仲裁系统测试拓扑

地检上位机通过遥控指令总线，对测控收发机发送指定当班信号，或者使能自动切机信号，并检测主/备星务计算机的上电后的遥测信号，确认启动是否成功，并完成任务恢复。

示波器测试点包含：地面指定当班 OC（Open-Collector，开集电极）指令，监控 MCU1/2/3 的输出，5V_A/B 输出电压，CAN 心跳报文等，直接指令指定和自动切换上的时序波形见图 17，CAN 指令心跳报文错误帧解析波形见图 18。

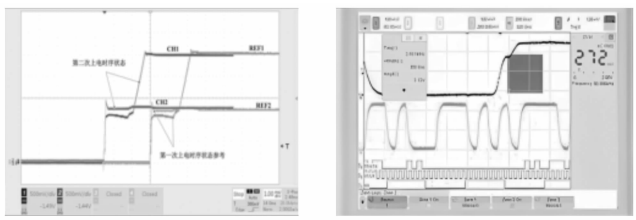

图 17 直接指令指定和自动切换上电时序

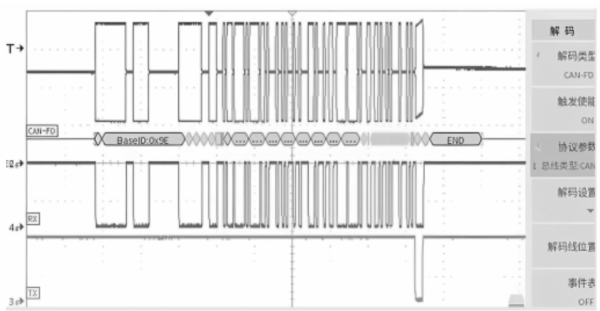

图 18 CAN 心跳报文错误帧解析

综合切换测试效果见表 1，当 3 个监控 MCU 有 2 个故障不工作时，默认是备机当班。

通过表 1 的测试结果显示，本电路实现了三取二的冗余备份仲裁电路的功能，验证了设计思路的正确，表明系统设计是成功有效的。

表 1　综合切换测试效果

触发动作	监控 MCU1	监控 MCU2	监控 MCU3	实际效果
地面指定主当班	主上电高，备上电低	主上电高，备上电低	主上电高，备上电低	冗余开关 1 使能，2 关闭。主当班，任务同步
地面指定主当班，监控 MCU1 断电	主上电低，备上电低	主上电高，备上电低	主上电高，备上电低	冗余开关 1 使能，2 关闭。主当班，任务同步
地面指定备当班	主上电低，备上电高	主上电低，备上电高	主上电低，备上电高	冗余开关 2 使能，1 关闭。备当班，任务同步
地面指定备当班，监控 MCU2 断电	主上电低，备上电高	主上电低，备上电低	主上电低，备上电高	冗余开关 1 使能，2 关闭。主当班，任务同步
地面指定主当班，监控 MCU1/2 断电	主上电高，备上电低	主上电低，备上电低	主上电低，备上电低	冗余开关 2 使能，1 关闭。备当班，任务同步
当班主机 5V_A 触发拉低电压或过流	主上电低，备上电高	主上电低，备上电高	主上电低，备上电高	冗余开关 2 使能，1 关闭。备当班，任务同步
当班备机 5V_B 触发拉低电压或过流	主上电高，备上电低	主上电高，备上电低	主上电高，备上电低	冗余开关 1 使能，2 关闭。主当班，任务同步
当班主机进入测试模式，不发心跳报文	主上电低，备上电高	主上电低，备上电高	主上电低，备上电高	冗余开关 2 使能，1 关闭。备当班，任务同步
当班备机进入测试模式，不发心跳报文	主上电高，备上电低	主上电高，备上电低	主上电高，备上电低	冗余开关 1 使能，2 关闭。主当班，任务同步

通过实验分析可以得到如下结论：

1）3 个监控 MCU 都是按照三模冗余的方式判定切换的，单个 MCU 异常不影响结果；

2）地面指令能打开和关闭自动切换功能，并能指定当班星务计算机；

3）当班主机出现电流、电压异常或者主机不发心跳报文/报文错误时，能自动切换到备计算机；

4）切换完成后，任务数据均能正常恢复。

6　结束语

本文提出的新型温备份方式的仲裁系统，通过合理的系统规划和可靠的软硬件设计，方案满足了整星对星务系统的可靠性需求。实际电路投产后的样件，通过测试后证明了设计思路的正确性，同时也实现了低成本的目标。未来随着批量部署，可以进一步优化仲裁电路的设计，如修正监测的参数和阈值，并借助大模型技术的发展，通过大量数据训练系统模型实现健康状态的预测，以提高系统的智能化水平和故障避免能力。

参考文献：

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

[2] 杨孟飞，化更新，冯彦君，等. 航天器控制计算机容错技术 [M]. 北京：国防工业出版社，2014.

[3] 徐　夏，夏德天，郑久寿，等. 高升力系统控制计算机容错技术研究 [J]. 微电子学与计算机，2015，32 (6)：36－40.

[4] 马秀娟，张秀珍，曹喜滨，等. 容错星务计算机系统结构设计 [J]. 微处理机，2003 (2)：47－49.

[5] 肖爱斌，胡明明，任宪朝. 四模冗余拜占庭容错计算机可靠性分析 [J]. 空间控制技术与应用，2014，40 (3)：42－46.

[6] 李淑侠，魏广平. 高可靠并行星务计算机软件容错技术研究 [J]. 物联网技术，2014 (5)：63－64.

[7] 孙秀娟. 基于双冗余容错技术的数据采集系统设计界 [J]. 电测与仪表，2008，45 (8)：49－52.

[8] 高丽娜，杨宝奎. 容错飞控计算机体系结构研究 [J]. 战术导弹技术，2013 (5)：107－110.

[9] 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)：96－98.

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

[11] 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.

[12] SAAB Space. Study of fault tolerant techniques for satellite data handling [R]. SAAB Space Final Report，1987：48－55.

[13] GREAMER G，DELAHUNT P，GATES S，et al. Attitude determination and control of clement in during lunar mapping [J]. Journal of Guidance，Control and Dynamics，1996，19：505－511.

[14] QU F，CUI G，YANG X Z. The design of house-keeping computer system for TS-1.1 [J]. Computer Engineering & Science，2002，24 (2)：96－104.

[15] 徐立颖，许松伟，冯　笑，等. 计算机运行全过程日志记录系统设计 [J]. 计算机测量与控制，2024，32 (1)：172－178.

[16] CENA G，VALENZANO A. Effcient implementation of semaphores in controller area networks [J]. IEEE Transactions on Industrial Electronics，1999：417－427.

[17] 陈玉坤，张生艳，刘　冬，双模冗余器载计算机设计与实现 [J]. 2016. 24 (12)：130－133.

[18] 朱明俊，周宇杰. 一种低成本纳卫星星务计算机容错方法 [J]. 航天器工程，2016，25 (2)：52－57.

[19] 吴兰蕙，刘凯俊，彭　攀. 基于 VP 技术的星载智能计算机虚拟原型机的构建 [J]. 计算机测量与控制，2020，28 (12)：222－226.

[20] 高月红，高　翔，张洪坤，等. 基于通用计算机和 USRP 的 LTE 通信系统开发与实现 [J]. 计算机测量与控制，2021，29 (10)：193－198.