

基于BM3803的高可靠星载软件重注方法

罗仝仝, 王永成, 肖辉

(中国科学院长春光学精密机械与物理研究所, 长春 130033)

摘要:为了适应航天器高可靠、长寿命的需求,以某实际项目应用为背景提出一种基于BM3803处理器的高可靠星载软件在轨重注方法。该方法通过1553B总线接收中央处理系统发送的重注程序,采用两个EEPROM实现原程序和重注程序存储,针对软件重注中接收、存储、固化和切换四个重要过程进行详细设计。设计了重注程序接收过程的多重校验,提高文件上传过程的可靠性;提出了基于包序号的重注程序存储方法,解决传输过程中包不连续的问题;采用了通过地面测控系统发送指令和引导程序相结合的方式进行重注程序加载,实现原程序和重注程序可靠切换。实验结果表明,该方案能够实现软件重注,并具有较高的可靠性。

关键词:星载软件;BM3803;软件重注;可靠性设计

中图分类号: TP311.1

文献标志码:A

文章编号:1672-9870(2020)04-0008-06

A High Reliability Satellite Software Re-injection Method Based on BM3803

LUO Quan-quan, WANG Yong-cheng, XIAO Hui

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

Abstract: In order to meet the requirements of high reliability and long life of spacecraft, a high reliability on-orbit software re-injection method based on BM3803 processor was proposed. The method receives the program sent by the central processing system through 1553B bus, uses two EEPROM to realize the original program and re-injection program storage and carries out detailed design for the four important processes of receiving, storing, curing and switching in software re-injection. The multi-check of the receiving process of the program is designed to improve the reliability. A storage method of re-injection program based on package number solves the problem of package discontinuity during transmission. The re-injection program is loaded by the combination of bootloader and instruction from ground operation control system, and the original program and re-injection program are switched reliably. The effectiveness and high reliability of the method is verified by experiments.

Key words: satellite software; BM3803; software re-injection; reliability design

随着航天器向着高可靠、长寿命发展,对星载软件也提出了更高要求。由于空间环境恶劣,空间辐射和单粒子容易造成存储器故障,引起程序运行异常。同时,由于在轨时间长,存在

系统更新升级的需求,而软件升级的代价远远小于硬件升级。因此,软件重注功能成为当前发展趋势。

目前,重注技术已经得到了广泛的应用。郝

收稿日期: 2019-04-01

基金项目: 国家重大科研项目(902017000590)

作者简介: 罗仝仝(1993-),女,硕士,实习研究员, E-mail: quanquan-luo93@163.com

通讯作者: 王永成(1980-),男,博士,研究员, E-mail: wyc-dyy@sina.com

佳宁等人^[1]提出基于文件的软件在轨升级方法, 采用了配置数据与程序代码独立存储的方式实现星载信息流实时在轨重构。钱方亮等人^[2]基于SRAM+FLASH存储器配置, 设计模块地址表实现模块灵活调用, 提高在轨编程的可靠性和灵活性。刘德胜等人^[3]通过CPU和FPGA交互的方式, 将重注程序直接发送到CPU的SRAM中存储, 不需要重新断电重启即可实现重注程序切换。何双宗等人^[4]针对多核DSP系统设计了一种动态重构方案, 实现单个核上的系统重构。郭宗芝等人^[5]基于VxWorks操作系统, 提出基于模块的加载机制, 更加安全便捷。在空间相机^[6-7]、无线电系统^[8-9]、光电经纬仪^[10]等领域, 软件重注成为提高系统可靠性的重要手段。

提出一种基于BM3803处理器的星载软件重注方法, 该方法通过在接收过程中对数据的双重校验确保接收重注程序的有效性。在重注程序存储过程中, 采用了基于包序号的存储方式, 避免数据包不连续出现的存储错误。本方案结合EEPROM的特点进行固化, 并利用指令和引导程序的方式可以实现程序相互切换, 在重注程序出现错误时, 仍可以切换到原程序保证系统的正常运行。该在轨重注方案在全过程均采用了高可靠性设计。

1 重注系统组成及工作原理

重注系统功能框图如图1所示。重注功能由地面测控系统、中央处理单元(MCU)和载荷综合管理系统共同实现。

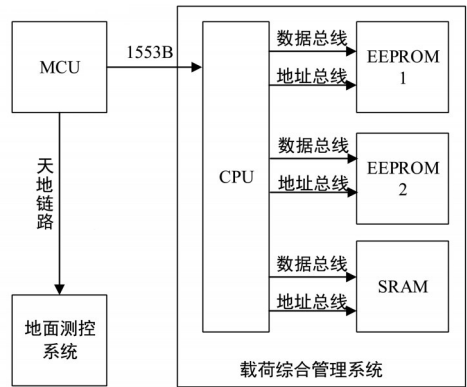


图1 软件重注功能框图

中央处理单元通过天地链路接收地面测控系统发送的数据包, 载荷综合管理系统经1553B接收转发的数据包并解析, 提供给其他的子系统。综合管理系统实现通讯数据管理作用, 并且需要具备软件重注功能。软件重注功能实现基于“CPU+EEPROM+SRAM”结构, CPU接收地面上传的重注程序数据包暂存于SRAM中, 经校验后再固化在EEPROM中, 完成程序重注。

SPARC体系处理器以其高可靠性广泛地应用于航天领域^[11-12]。本系统处理器选用SPARC体系的国产CPU芯片BM3803。BM3803是基于SPARC V8结构的抗辐射加固微处理器, 可以用于嵌入式实时操作系统, 能够满足航天任务需求。BM3803通过外部存储器控制器可以访问PROM、I/O设备、SRAM和SDRAM。表1为BM3803存储器地址分配。BM3803处理器外接PROM的起始地址为0x00000000, 大小为512 M; 外接I/O设备的起始地址为0x20000000, 大小为256 M; 外接SRAM/SDRAM的起始地址为0x40000000, 大小为1 G。

表1 3803存储器地址分配

地址范围	大小	映射
0x00000000-0x1FFFFFFF	512 M	PROM
0x20000000-0x3FFFFFFF	256 M	I/O
0x40000000-0x7FFFFFFF	1 G	SRAM/SDRAM

EEPROM用于存储综合管理系统的应用程序, 其中EEPROM1用于存储原程序(出厂程序), EEPROM2用于存储在轨重注程序。在轨进行软件重注时, EEPROM1保持不变, 能够保证系统在重注失败的最坏情况下仍能够运行应用程序。根据系统硬件设计, 两片EEPROM的地址范围如表2所示。EEPROM1的起始地址为0x00000000, EEPROM2的起始地址为0x10000000。CPU启动时从地址0x00000000处开始运行。

表2 EEPROM地址空间分配

起始地址	映射
0x00000000	EEPROM1
0x10000000	EEPROM2

SRAM 为程序提供运行环境。系统启动后,通过引导程序将存储在 EEPROM 中的应用程序搬移到 SRAM 中进行运行。此外,SRAM 还为重注程序存储提供暂存区。

软件重注包括接收、存储、固化和切换四个主要过程。

(1)接收过程是指地面测控系统通过天地链路向卫星数管平台发送重注程序,CPU 通过 1553B 总线接收重注程序的过程。

(2)存储过程是指将重注程序按照规定的顺序存储在 SRAM 中,并对重注程序完成校验的过程。

(3)固化过程是指将检验完的重注程序写入 EEPROM2 中的对应位置。

(4)切换过程是指软件重注完成后,从原程序切换到重注程序的过程,包括切换指令发送和重注程序引导。

2 在轨软件重注的关键算法

2.1 重注程序接收

地面测控系统按照一定的格式将数据进行封装后发送给综合管理单元,封装格式如图 2 所示。

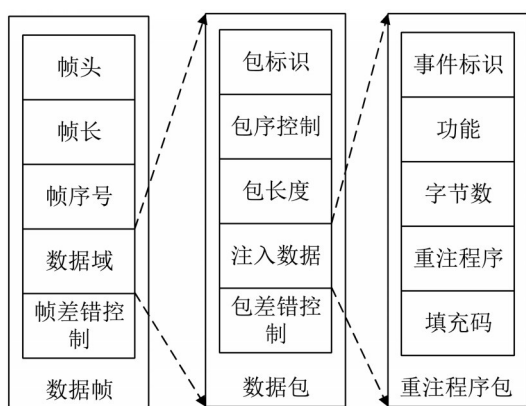


图2 重注数据格式

数据帧和数据包均包含头、长度、序号、数据域和差错控制等信息,用来识别数据的类型以及进行数据的校验。数据帧和数据包的长度均为固定值。重注程序包格式包括用来判断重注功能的事件标识和功能、对重注程序长度进行

校验的字节数。当重注程序字节数小于注入数据可容纳字节数时,需在重注程序有效数据后以填充码进行补充。一个数据帧中包含一个或多个数据包,一个数据包的注入数据中也包含一个或多个重注程序包。

根据功能不同,重注数据可分为三种类型:

(1)重注程序字节数和校验和。字节数和校验和用来判断重注程序的正确性,在重注程序处理过程中使用。

(2)重注程序开始/结束指令。重注程序开始指令表明开始接收重注程序,同时对 SRAM 中的程序暂存区进行清零,将与程序重注相关的遥测参数设置为初始状态。重注程序结束指令表明所有的重注程序传输存储完毕,此时计算存储区全部重注程序的校验码。

(3)重注程序。重注程序为应用程序代码。由于每帧/包对长度有限制,因此重注程序需要拆分成多帧/包的形式进行传输。

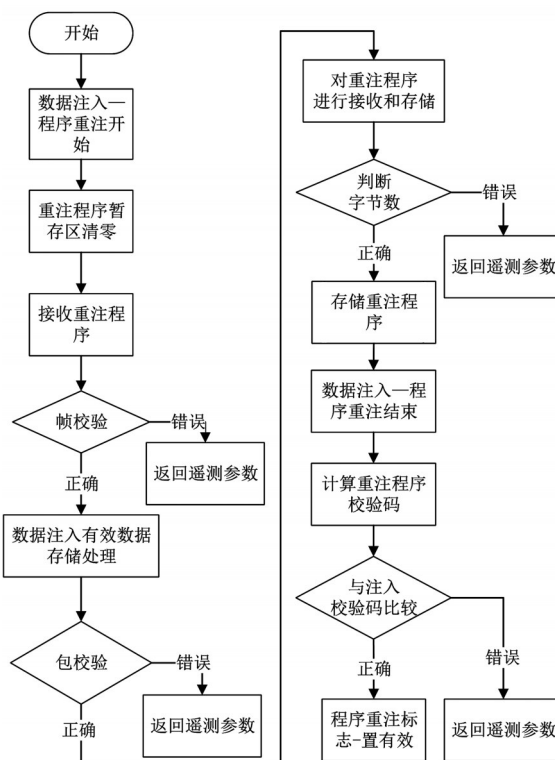


图3 数据接收流程

重注程序接收过程如图 3 所示,重注过程开始时,先注入“数据注入—程序重注开始”指令,然后将重注程序上传,接收过程中先进行帧校

验,若帧校验正确则接收数据帧。再对数据帧中的每包数据进行拆分,分别进行包校验,校验正确则接收相应数据包。最后对数据包中的参数字节数进行判断,若字节数正确则将重注程序存储在SRAM的暂存区中。帧校验和包检验及参数字节数校验错误,返回相应的遥测参数供地面测控系统分析处理。所有重注程序传输完后发送“数据注入—程序重注结束”指令,计算重注程序校验码,若校验码与地上传的校验码一致,则将重注状态标志位置有效。

2.2 重注程序存储

数据传输过程中可能出现错误,从而导致帧或包丢失,使得重注程序数据包不连续。提出一种基于包序号存储重注数据的方法对每包重注数据进行存储,能够有效地解决数据包不连续的问题,提高重注过程的可靠性。在SRAM中设计重注程序存储区,按每包重注程序字节数划分区域,不同包序号对应不同的存储区域。重注程序包解析后将重注程序存储在对应区域。

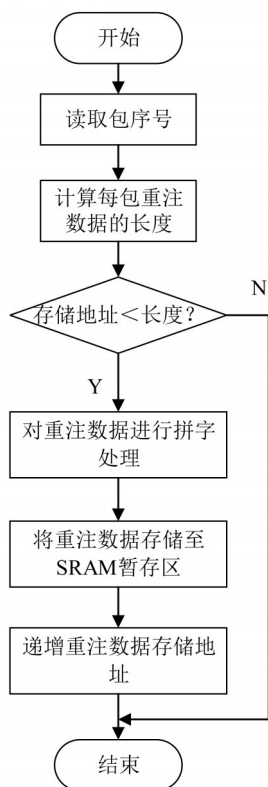


图4 重注程序存储流程

图4为重注程序存储流程。CPU接收到经校验有效的重注程序包后解析,将有效的重注程序存储在SRAM对应的重注程序存储区。首先读取数据包中的包序号,然后计算数据包中的重注程序的字节数,存储过程中通过判断存储地址是否小于字节数,对数据包中的重注程序进行存储。由于选用CPU BM3803的存储机制,因此在存储过程中需要将重注数据进行拼字处理后再存储到SRAM暂存区中。当前数据包所有重注程序存储完后进行下一数据包的存储。

2.3 重注固化

EEPROM在轨受单粒子影响可能发生位翻转现象,从而造成软件失效。根据芯片手册,在写模式下EEPROM抗单粒子能力大大降低。因此,在重注固化过程中,采用页写和字节写的方式提高固化的可靠性。

本方案选用3D-Plus公司的40位EEPROM,其中高8位为校验位,低32位为数据位。EEPROM具有SDP保护机制,能够防止对EEPROM误操作。因此在进行重注固化时,需要先分别对EEPROM的数据位和校验位解除SDP保护。页写过程中,通过对EEPROM的I/O6进行监控,判断页写是否完成。页写完成后,逐字节进行比较,错误时再将错误字节重写,防止页写过程中出现位翻转。EEPROM写完成后对其数据位进行SDP保护。BM3803具备EDAC功能,CPU向EEPROM写32位数据时,同时生成相应校验位存储在EEPROM的高8位。对数据位进行SDP保护时,生成相应的校验位覆盖之前的检验位,因此在数据位进行SDP保护后重写数据生成正确的校验位进行存储。重注固化结束后通过发送遥测参数至地面判断固化是否成功。

2.4 程序切换

完成软件重注后,可通过指令和引导程序相结合的方式程序切换。程序切换控制采用

指令控制继电器进行,继电器采用磁保持继电器,继电器一端连接CPU的一个I/O引脚,另一端为MCU程控指令,通过“加载原程序/加载重注程序”程控指令控制CPU I/O引脚电平高低,“加载重注程序”时为高电平。根据系统硬件设计,CPU引导程序存于EEPROM1中,从地址0x00000000开始,原程序存储于引导程序后。系统上电后从地址0x00000000开始运行,即先运行CPU引导程序。引导程序将EEPROM中存储的程序搬至SRAM中运行,提高程序运行速率。引导程序同时也完成程序切换,CPU通过判断I/O引脚电平高低选择加载原程序或重注程序。

引导软件加载流程如图5所示。地面运控系统发送“加载重注程序”指令后,上电复位后运行引导程序,判断I/O引脚电平,若为高电平则引导存储于EEPROM2中的重注程序,启动应用软件。

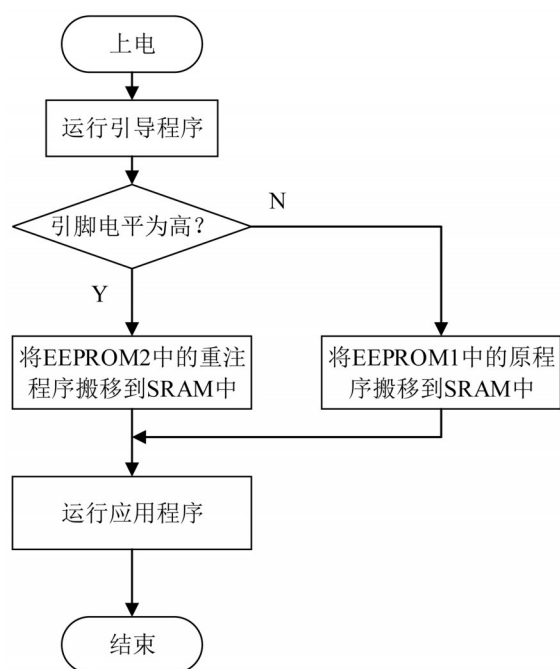


图5 引导软件加载流程

3 可靠性设计

由于空间环境恶劣,空间载荷需要经历低温以及严重的空间辐射,其中EEPROM和SRAM受空间单粒子效应,引起程序运行错误,因此软件重注过程采取了以下可靠性设计提高重注的

可靠性:

(1)为了防止程序重注过程中系统通讯控制异常,在重注程序固化过程中关闭所有中断,停止其他操作,此时系统只进行程序固化;

(2)为了防止天地链路间通信错误,对每帧数据和每包数据均进行校验位检验,如果检验结果错误,则丢弃该帧/包数据;

(3)为了防止程序存储SRAM过程中出现错误,在重注程序接收结束后对存储的完整程序进行校验,校验项包括重注程序的字节数和重注程序内容;

(4)为了防止EEPROM固化过程错误,采用了“页写+字节校验再写”的方式,提高固化过程的可靠性;

(5)在程序切换方式选择上,为了防止传输过程中数据注入指令出现错误引起程序切换错误,采用了“程控指令+继电器”的方式进行切换,其中程控指令相比于数据注入指令具有更高的可靠性。

4 实验验证

通过地检设备向CPU发送“重注程序字节数和校验和”并存储在RAM中,发送“程序重注开始”数据注入指令,判读相应遥测量正确后将重注程序按照帧格式发送给CPU,并存储在RAM的相应地址中。所有重注程序数据包发送完毕后再通过地检设备发送“程序重注结束”数据注入指令,通过相应遥测量判断软件重注成功。发送“加载重注程序”程控指令后,重启系统运行程序,根据相应遥测量的值判断重注程序是否运行,通过观察发现遥测量值已经更新为重注程序的标识号,重注程序已加载成功。

5 结论

以工程项目为背景,针对在轨软件故障或软件升级的需求,提出了一种基于BM3803的星载软件高可靠重注方法,该方法采用多重数据包校验保障接收数据的可靠性,设计基于包序号

的存储方式对不连续的数据包进行存储, 结合BM3803和EEPROM特点采用页写和字节写相结合的方式对重注程序进行固化, 另外设计程控指令和引导程序进行程序切换, 提高了星载软件在轨重注的可靠性。目前该方案已经在某项目综合控制软件前期实验中得到验证。实验证明, 提出的星载软件重注方法具有广泛的工程实际应用价值。

参考文献

- [1] 郝佳宁, 刘畅, 韩延东, 等. 小卫星可复用软件技术研究[J]. 计算机测量与控制, 2019, 27(6): 130–134.
- [2] 钱方亮, 林荣锋, 周宇, 等. 一种基于微小卫星系统软件在轨编程功能的设计方法[J]. 计算机应用与软件, 2018, 35(12): 16–20.
- [3] 刘德胜, 王淦泉. 易失性存储器的程序重注方案研究与应用[J]. 单片机与嵌入式系统应用, 2017, 17(10): 9–12.
- [4] 何双宗, 王巍, 田会娟, 等. 多核DSP的动态重构方案的设计与实现[J]. 机械设计, 2018, 35(S1): 29–32.
- [5] 郭宗芝, 刘彬, 邹玉龙, 等. 基于模块动态加载机制的航天器软件重构方案研究[J]. 计算机测量与控制, 2018, 26(6): 126–129+148.
- [6] 徐伟, 朴永杰. 航天相机控制器在轨软件重注[J]. 光电工程, 2013, 40(4): 65–71.
- [7] 张然峰, 郝贤鹏, 金龙旭, 等. 空间相机软件在轨重注方法研究与实现[J]. 光机电信息, 2011, 28(6): 30–34.
- [8] 丁磊, 刘海峰, 张小林. 一种星载软件无线电系统的高可靠智能重构方法[J]. 航天电子对抗, 2018, 34(4): 24–28+33.
- [9] 康国栋, 薛超, 李琳琳, 等. 一种基于软件无线电的卫星跟踪平台设计[J]. 电子技术应用, 2019, 45(2): 50–52+66.
- [10] 修大朋. 基于软件重构的光电经纬仪自修复系统[J]. 自动化与仪器仪表, 2019(10): 13–17.
- [11] 徐伟, 谭超, 王绍举, 等. 基于TSC695F的高可靠航天相机控制器设计[J]. 长春理工大学学报(自然科学版), 2011, 34(3): 28–32.
- [12] 张涛, 李瑞军, 范延芳. 基于SPARC V8的星载嵌入式软件全数字仿真平台设计与实现[J]. 计算机测量与控制, 2020, 28(1): 11–15.