基于三层防护的CAN寄存器翻转恢复方法

宋 智 李志刚 史 简 李军予 李琳琳
(航天东方红卫星公司 北京 100094)

摘 要:当星上CAN总线寄存器发生翻转效应时,往往导致星上的电子设备之间通信受阻,甚至导致整条总线的工作异常。目前缺乏有效的手段检测和定位星上的哪个设备CAN总线寄存器发生了翻转,导致在恢复卫星总线时需要对星上设备进行尝试性的断电/加电,为了及时准确恢复CAN总线通信异常,设计了"三层防护"方法,并将寄存器翻转对CAN总线通信造成的影响按时间长短分成了3类,分别是:只影响当前值、短暂影响总线通信和长时间影响总线通信。"三层防护"方法有效解决了在轨CAN总线寄存器发生翻转的问题。通过实验验证该方法为排除卫星CAN寄存器翻转故障提供了创新的技术支持。

关键词:卫星;CAN;寄存器;翻转;影响;恢复
中图分类号: TN61/65 V474 **文献标识码**:A **国家标准学科分类代码**: 510.1050

Recovery method of SEL happened to registers of satellite's CAN based on three safeguard

Song Zhi Li Zhigang Shi Jian Li Junyu Li Linlin
(DFH Satellite Co. Ltd, Beijing 100094, China)

Abstract: When reversal occurs on a register of CAN bus in a satellite, the communication between digital devices is often hindered, and even the whole bus will work abnormally. Currently, there is not an effective method to detect and locate which register in CAN bus generates reversal, that the only thing we could do was closing firstly then opening all the nodes of the satellite one by one, so designed a novel method called three safeguard and classified the influence of reversal on register of CAN according to continuance. The first is only changing numerical value. The second is affecting communication for a whole. The last is affecting communication long-term. The method three safeguard can save those satellites which taken reversal on register of CAN. Through simulation verification, this method can offer an innovative technology to solving the trouble caused by reversal on register of CAN.

Keywords: satellite; CAN; register; reversal; effect; rehabilitate

1 引 言

CAN(controller area network)即控制器局域网[1],是一种多主方式的串行通信总线,可实现全分布式多级系统,可以用点对点、一点对多点以及全局广播几种方式传送和接收数据。最初是德国的Bosch公司为了汽车控制可控制系统而设计的,现在广泛应用于汽车、航天、工业控制等领域[2-4]。在1993年CAN已成为国际标准ISO11898和ISO11519。

目前,国内小卫星主要采用CAN总线作为星上网络[5]数据传输总线,CAN总线是星务主机与各下位机进行通信的链路,采用主从方式进行通信,同时也支持多主方式通信。国内小卫星CAN控制器SJA1000主要工作模式是BasicCAN模式,采用符合CAN2.0规范的标准协议。星上CAN总线采用双冗余的总线型网络结构,包括A、B两条CAN总线。

带电粒子在地磁场作用下被捕集在地球周围形成辐射带。因此在日地空间范围内存在大量的高能粒子,主要是银河宇宙线、太阳宇宙线和地球辐射带粒子,这些共同构成航天器轨道高能带电粒子环境。在恶劣的空间环境影响下,星上CAN总线由于单粒子翻转[6-8]或单粒子瞬态脉冲[9-10]会导致星上通信异常,严重时甚至会拉垮整条CAN总线。当星上发生CAN总线异常时,会影响到数据轮询应答,甚至会影响到整星安全。目前,在轨卫星CAN总线异常时,往往不能准确定位到发生异常的设备,导致在恢复卫星总线时需要对星上的每个设备进行尝试性的

收稿日期:2016-07

断电/加电。这个过程耗费大量的时间和精力,总线问题恢复之后,还要对各设备进行状态恢复设置,过程非常繁琐。本文对CAN寄存器翻转造成的影响按时间长短分成3类,分别是:只影响当前值、短暂影响总线通信和长时间影响总线通信。只影响当前值的情况和短暂影响总线通信的情况不会对卫星后续通信造成持续的影响。当星上CAN总线异常时文章提供的方法能快速准确定位发生异常的设备,并恢复CAN总线异常。文章设计了"三层防护"方法,分别从单机层面、整星层面和系统层面来解决星上CAN寄存器翻转异常。第一层防护从单机层面有效的解决单粒子翻转造成的软错误;第二层防护从整星层面启动智能防护模式;第三层防护是从系统层面分析星上状态进行防护。"三层防护"方法适用于使用CAN总线的多个平台。"三层防护"方法的第一层防护方法很好的解决了在轨不具备按照传统的切机复位重新初始化CAN总线寄存器的航天器发生CAN寄存器翻转的问题。

2 星上CAN总线

2.1 CAN总线网络结构

小卫星星上CAN总线网络采用双冗余的总线型网络结构,包括A、B两条CAN总线,由星务主机和其他下位机组成通信节点,结构如图1所示。

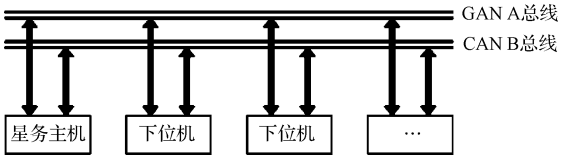

图1 星上CAN总线网络结构

2.2 通信节点工作模式

星务主机作为主节点通过轮询向各下位机发出轮询命令,各下位机设置接收滤波参数只接收有关的数据,平时处于空闲等待状态,可接收总线数据。卫星可根据实际需要,设置某节点在必要时以主节点方式发送数据,其他时间该节点处于数据接收状态。

3 卫星CAN总线异常的影响

3.1 卫星CAN总线异常

造成卫星总线通信异常的原因包括:硬件故障、软件设计缺陷和单粒子效应,其中单粒子效应又包括单粒子硬错误和单粒子软错误,如图2所示。

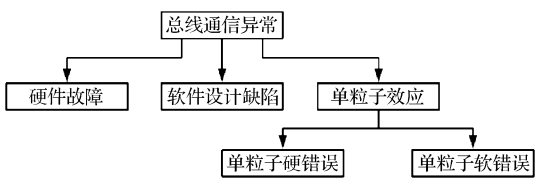

图2 CAN总线异常原因

3.1.1 硬件故障

通信设备硬件故障会引起卫星总线通信异常。包括:

1)低等级器件并不保证其整个生产、采购过程受控,会出现不一致的可能性;

2)将进口SJA1000芯片换成了国产芯片,而未识别出两者的不一致性;

3)CAN总线接插件接口插接不良等。

本文建议在卫星设计、生产、试验过程中要严格按照规定的要求及标准保证硬件设备的安全性、可靠性。

3.1.2 软件设计缺陷

卫星星上软件异常也会导致星上总线通信异常,例如:

1)软件设计不符合通信协议要求;

2)软件时序设计不合理;

3)软件受到异常干扰跑飞等。

为了减少卫星在轨软件异常的概率,文章建议在工作中做到以下几点:

1)严格按照软件工程化的要求进行开发和质量控制;

2)软件设计中存在的引起通信异常的固有缺陷要在测试及试验过程中发现,并及时更改正确并且通过验证;

3)对于星上软件设计软件复位策略。

在卫星设备的设计生产过程中,要从硬件设计和软件设计两方面保证卫星的正常工作。

3.1.3 单粒子故障

单粒子效应(single event effect,SEE)是指电子器件处在高强度辐射环境中,高能粒子穿透电路芯片,在穿透的路径上发生电离,从而产生多种辐射效应。空间高能粒子轰击微电子器件的敏感节点,导致微电子器件逻辑功能翻转或器件损坏。空间高能粒子辐射主要来源于地球辐射带、银河宇宙线和太阳宇宙线。单粒子效应根据产生机理及影响结果又分为硬错误和软错误。

硬错误会使受到辐射的电路损伤,严重时即使通过断开电源或重新写入都无法使受到损伤的器件恢复正常。目前国内对硬错误的研究主要集中在工艺器件级,并且取得了突出的成果。可恢复的硬错误通过断开电源或重新写入排除故障;不可恢复的硬错误通过切机,使用备份设备工作。

软错误效应使器件逻辑状态翻转,原来存储的"0"变为"1",或者"1"变为"0"这种效应不会损坏电子器件,只是改变了器件逻辑状态,可以被重新写入状态进行状态恢复。导致卫星CAN寄存器位翻转软错误的原因主要是单粒子翻转和单粒子瞬态脉冲。

在空间复杂环境下,高能粒子能量很大,穿透力极强,所以不可能完全用硬件来屏蔽空间高能辐射。当CAN总线寄存器发生翻转时会导致CAN总线通信异常,严重影响卫星总线正常工作,常常给卫星的使用带来不便,并且给卫星维护人员带来很大的额外工作量。

3.2 CAN寄存器翻转影响分类

CAN寄存器发生翻转时，按影响时间的长短将其分为3类，如图3所示。

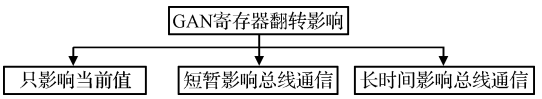

图3 影响的类别

1）只影响当前值：状态寄存器的翻转只影响当前值，不影响通信，会在下次置位时写回正常值；

2）短暂影响总线通信：命令寄存器、中断寄存器翻转，影响本次通信，会在下次置位时写回正常值；

3）长时间影响总线通信：控制寄存器、验收滤波器、总线时序0、总线时序1、输出控制和时钟分频器。

对于“只影响当前值”的翻转，不需要卫星做工作进行恢复。“短暂影响总线通信”的翻转只需卫星对其作出标志即可，不需要卫星做工作进行恢复。“长时间影响总线通信”的翻转则需要采取措施对其进行状态恢复。

4 星上总线异常的定位及恢复方法

针对目前缺乏有效的手段检测、定位并快速恢复星上发生CAN总线寄存器翻转造成总线通信异常的情况，提出了“三层防护”方法，分别从单机层面、整星层面和系统层面解决上述问题。首先让星上自主智能恢复，星上不能自主恢复时，再地面采取人工干预。

4.1 单机层面

单机层面即第一层防护：星上每个设备单独保存CAN寄存器的正确值，包括控制寄存器、验收滤波器、总线时序0、总线时序1、输出控制和时钟分频器等翻转会长时间影响总线通信的寄存器。软件周期性读取各寄存器的当前值且存储在遥测数据中，将寄存器当前值与寄存器的正确值进行比较，通过对寄存器值的比较定位设备的寄存器是否发生了异常。如果寄存器的值发生了翻转，重新设置CAN寄存器值，恢复CAN总线的正常工作。在遥测中对星上CAN寄存器的自动恢复进行记录。第一层防护可以有效的解决单粒子翻转造成的软错误。遥测数据中的恢复记录反映星上哪个设备发生了异常，并且标志发生异常的寄存器。第一层防护执行流程如图4所示。

4.2 整星层面

整星层面即第二层防护：星上软件设计中增加总线异常恢复方法，星务主机将每次轮询到的各下位机CAN寄存器的值与存储的各下位机CAN寄存器正确值进行比较，软件自主分析判断各设备CAN寄存器值的正确性，当某下位机的CAN总线寄存器的值异常时，如果发生异常的下位机没有通过“第一层防护”在规定的时间内自动恢复正常，那么星务主机启动该下位机CAN总线的恢复模式，通过CAN寄存器初始化指令，初始化异常下位机CAN

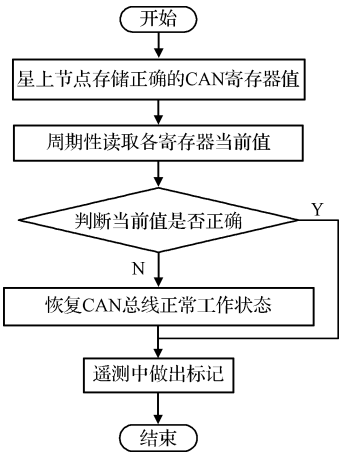

图4 第一层防护执行流程

寄存器的值。如果CAN寄存器的值正常而该下位机通信异常，可能是下位机软件故障引起的通信异常，星务主机在恢复模式中对该下位机软件发出重启指令。在遥测数据中增加对该处理的标记，并标记哪个设备启动了恢复模式。第二层防护执行流程如图5所示。

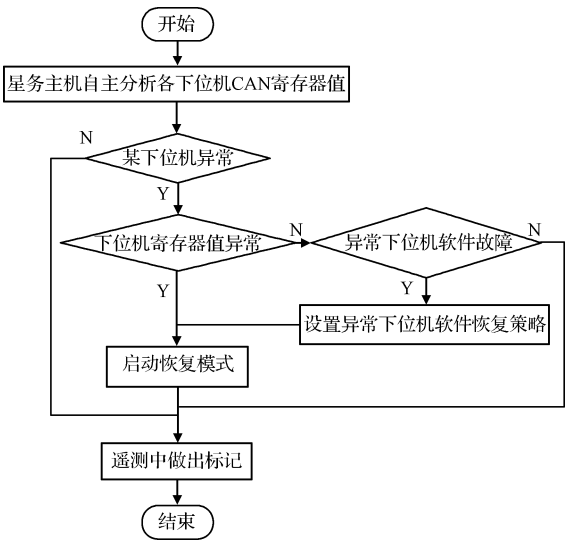

图5 第二层防护执行流程

4.3 系统层面

系统层面即第三层防护：如果总线通信异常仍然没有恢复正常，那么卫星方和运控中心需要对星上遥测数据及星上设备工作情况进行分析。首先，分析各设备寄存器的遥测值及星上对各设备自主操作的记录情况，判断星上设备CAN寄存器是否发生了单粒子硬错误，定位发生错误的设备，及时采取恢复措施；其次，组织设计人员分析星上软件是否有缺陷，如果星上软件有缺陷，那么修改软件并对星上的软件进行上注更改。最后，判断是否是星上设备硬件故障，如果该故障不可修复，则将故障设备切换到备份设备。第三层防护执行流程如图6所示。

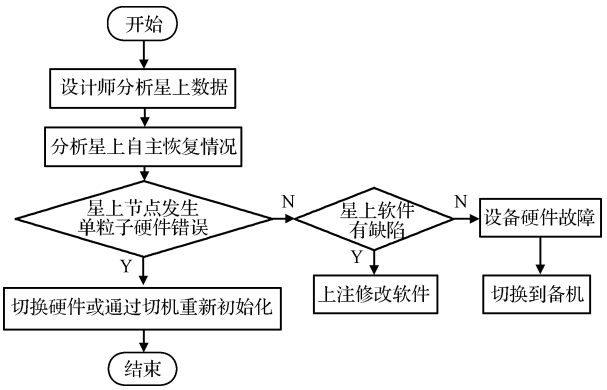

图 6　第三层防护执行流程

对于发生单粒子翻转后不具备通过常规切机复位方法恢复工作状态的在轨飞行器，可以采用“三层防护”方法的第一层防护方法避免灾难性后果的发生，恢复正常状态后飞行器可以继续在轨工作，完成既定的任务。

5　“三层防护”方法验证及应用

CAN 总线 BasicCAN 模式寄存器主要包括：控制寄存器、命令寄存器、状态寄存器、中断寄存器、验收代码、验收屏蔽、总线时序 0、总线时序 1、输出控制、发送缓冲器、接收缓冲器和时钟分频器。当卫星设备不同的寄存器发生单粒子翻转时，会对卫星的正常工作造成不同的影响。

状态寄存器的翻转只影响当前值，不影响通信，会在下次置位时写回正常值；命令寄存器、中断寄存器翻转，影响本次通信，会在下次置位时写回正常值。

控制寄存器、验收滤波器、总线时序 0、总线时序 1、输出控制和时钟分频器如果发生了寄存器翻转，则长时间影响总线通信。

“三层防护”方法验证在星务测试床进行，主要包括遥控单元、星务主机、热控下位机及地面设备。实验环境如图 7 所示。

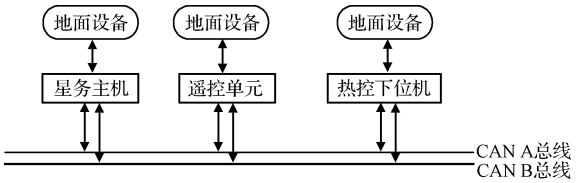

图 7　实验环境

实验一：在实验过程中模拟卫星在轨热控下位机 CAN 寄存器发生单粒子翻转，热控下位机软件利用“三层防护”方法的第一层防护方法在软件一个时间周期内可以快速定位并恢复发生单粒子翻转的寄存器，并恢复星上正常的 CAN 总线通信。

实验二：在实验过程中模拟卫星在轨热控下位机 CAN 寄存器发生单粒子翻转，且热控下位机软件没有自主恢复发生单粒子翻转的寄存器，星务主机判断热控下位机总线异常后，判断其 CAN 寄存器发生了单粒子翻转。星务主机向热控下位机发送指令，重新初始化热控下位机 CAN 寄存器的值，恢复星上总线正常通信。

通过实验验证，“三层防护”方法可以及时、准确恢复星上设备 CAN 寄存器单粒子翻转异常。目前，某些预研型号已经采用“三层防护”方法进行设计。“三层防护”方法适用于使用 CAN 总线的多种平台。“三层防护”方法将减少以往型号在轨总线异常时需要地面人员投入的时间和精力，在恢复 CAN 总线通信异常的过程中能够发挥出“快、准、灵”的作用。

6　结　论

本文研究分析了卫星在轨 CAN 总线寄存器发生翻转对卫星的影响，根据影响时间的长短分为 3 类，分别是：只影响当前值、短暂影响总线通信、长时间影响总线通信。设计的“三层防护”方法分别从单机层面、整星层面和系统层面快速、准确、智能的定位，解决卫星在轨 CAN 总线异常。“三层防护”方法在恢复 CAN 总线通信异常的过程中实现了“快、准、灵”的作用。“三层防护”方法的第一层防护方法即可很大程度的修复和避免在轨单粒子引起的 CAN 寄存器翻转造成的不良影响。“三层防护”方法可以应用于使用 CAN 总线的多种平台。如果在不具备切机复位功能的飞行器（如某些飞卫星或皮卫星等）使用“三层防护”方法的第一层防护方法，可以解决由于 CAN 寄存器翻转软错误导致的不可恢复的问题，有效的降低了这些飞行器变成太空垃圾的概率。

“三层防护”方法有效的提高了卫星在轨 CAN 总线异常的恢复效率，达到了提高卫星智能化和减轻地面运控中心在轨维护耗时、费力、压力大的作用，为卫星在轨良好的工作及减少地面运维成本提供强有力的技术支持。

参 考 文 献

[1] 邹继军，饶运涛. 现场总线 CAN 原理与应用技术[M]. 北京：北京航天航空大学出版社，2007.

[2] 刘鑫，林兆华，杜璧秀. CAN 总线分布式自动调整控制系统设计[J]. 国外电子测量技术，2014，33(8)：44-48.

[3] 杨华伟，万正权. CAN 总线在船舶结构安全监测系统中的应用[J]. 电子测量与仪器学报，2014，28(5)：553-559.

[4] 刘铁根，王双，江俊峰，等. 航空航天光纤传感技术研究进展[J]. 仪器仪表学报，2014，35(8)：1681-1692.

[5] ZHAN Y J，MA SH CH，ZHUANG T，et al. Research on network integration technology of observation sttions[J]. Instrumentation，2015，2(3)：35-42.

[6] 陈晨，徐微，张善从. Flash 型 FPGA 单粒子效应测试系统设计[J]. 电子测量技术，2014，37(9)：70-78.

（下转第 49 页）