

一种嵌入式实时操作系统高可靠文件系统

李书根, 潘海燕, 王 培

(西安微电子技术研究所, 陕西 西安 710054)

摘 要: 提出了一种管理层数据热备份的高可靠文件系统. 与传统的高可靠文件系统不同, 提出的高可靠文件系统对管理层数据进行了热备份, 能够避免因管理层数据损坏导致的文件系统崩溃, 该文件系统能够动态检测管理层数据的完整性, 当发生因单粒子翻转或物理器件损坏引起的管理层数据损坏时, 实时切换到备份的管理层数据, 能够保证高可靠文件系统的无缝切换和运行.

关键词: 嵌入式文件系统; 管理层数据热备份; 管理层数据再恢复、再备份

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2014)03-0014-03

A High-reliable File System Based on Embedded RTOS

LI Shu-gen, PAN Hai-yan, WANG Pei

(Xi'an Microelectronics Technology Institute, Xi'an 710054, China)

Abstract: In this paper, we propose a high-reliable file system, which hot backups its own management data. With the difference from traditional works, the file system proposed here can avoid the crash by the damage of management data. It detects the damage of management data dynamically, and switches to the backup one when the damage of management data happens, leading to continuum of the file system.

Key words: embedded file system; management data hot backup; management data recovery; backup again

1 引言

随着嵌入式实时操作系统在卫星等领域的广泛应用, 嵌入式高可靠文件系统在空间数据存储和管理方面显得越来越重要. 受到接收区域的影响, 卫星采集到的大量数据必须先存储到 FLASH 等存储器中, 待卫星飞越到国境上空时再进行下传. 因此, 必须通过高可靠文件系统对卫星采集到的大量数据进行存储和管理.

当前国内外嵌入式文件系统方面已做了相关工作^[1-7], 其中应用较为广泛的嵌入式文件系统主要有 FAT^[1]、JFFS^[2]、YAFFS^[3]、TrueFFS^[4]等. FAT 结构简单, 占用资源少, 兼容性好, 但读写性能低, 空间开销大, 不能满足大容量、高速访问的用户需求^[6]. JFFS 等是基于 Flash 存储器的日志文件系统, 虽有改进, 但仍有提升的空间.

针对管理层数据损坏导致的文件系统崩溃问

题, 本文提出了一种管理层数据热备份的高可靠文件系统. 该文件系统通过对管理层数据的热备份, 能够实现管理层数据损坏后的管理层实时切换, 从而保证文件系统的正常运行. 该高可靠文件系统还实现了对故障管理层数据的再恢复功能, 能够对因单粒子翻转导致的管理层数据损坏进行数据恢复. 对于因存储器物理损坏导致的管理层数据损坏, 我们设计了管理层数据再备份机制, 能够分配新的数据空间, 对当前正常运行的管理层数据进行再备份.

本文提出的管理层数据热备份, 采取了将管理层数据进行热备份的方法, 能够避免因管理层数据损坏而导致的文件系统失效, 提高了嵌入式文件系统的可靠性.

2 管理层数据热备份的高可靠文件系统

提出的管理层数据热备份的高可靠文件系统分为四层: 应用层、管理层、驱动层和物理层, 如图 1

所示。



图1 文件系统层次划分

应用层提供高可靠文件系统与操作系统用户的交互接口,包括文件的创建、删除、打开、关闭、读写等基本操作。

管理层主要完成存储管理、坏块管理、均衡擦写、备份块管理等功能。

驱动层主要完成存储介质读写、检查状态、执行特定命令等功能。

物理层根据不同的存储器型号有相应的硬件操作函数。

管理层数据热备份机制包括五个部分:文件系统初始化、动态故障检测、热备份数据切换、故障管理层数据恢复和管理层数据再备份。

2.1 文件系统初始化

文件系统初始化实现对 Flash 存储器的坏块检测和管理层数据的热备份初始化。如图2所示。

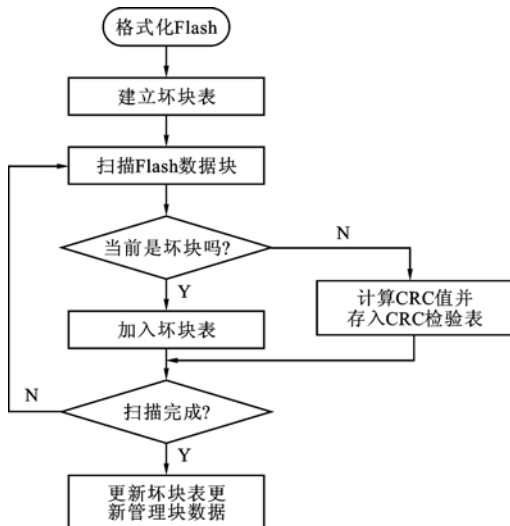


图2 首次初始化坏块管理

2.1.1 坏块检测

文件系统对 Flash 存储器的坏块检测有两种情况:一是文件系统首次初始化时的坏块检测,二是文件系统再次初始化时的坏块检测。

文件系统首次初始化时,以扇区(Sector)为单位对 Flash 存储器进行自检,对自检中发现的坏块

进行坏块管理。文件系统对坏块的管理通过坏块表完成,如表1所示。坏块表为 Flash 存储器的每个扇区都分配了一个标识,用于表明扇区是否是坏块。文件系统完成对 Flash 存储器的自检后,建立 Flash 存储器的 CRC 校验表,如表2所示。CRC 校验表中存储了 Flash 存储器每个扇区的 CRC 校验值,用于文件系统的动态故障检测。

表1 坏块表

Sector(扇区号)	Flag(标记是否坏块)
...	...

文件系统再次初始化时,为了不破坏存储的文件系统数据,不能再对 Flash 存储器进行自检。因此,需要通过 CRC 校验表对 Flash 存储器数据的完整性进行自检。此时如果某个 Flash 扇区计算的 CRC 校验值与 CRC 校验表中的存储值不一致,则判定该 Flash 扇区为坏块,如图3所示。

表2 CRC 校验表

Sector(扇区号)	CRC 校验值
...	...

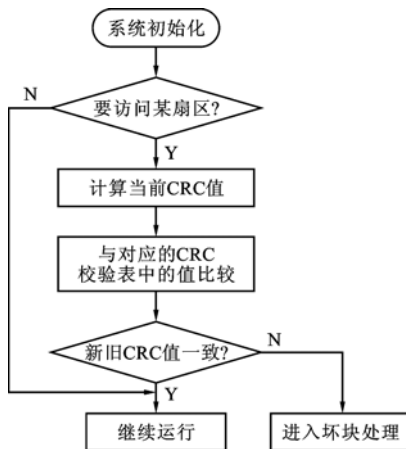


图3 再次初始化坏块管理

2.1.2 管理层数据热备份初始化

与坏块检测相同,管理层数据热备份初始化也包括两种情况:一是文件系统首次初始化,二是文件系统再次初始化。

文件系统首次初始化时,文件系统分配独立的存储区域用于存放热备份的管理层数据。

文件系统再次初始化时,文件系统需要对热备份的管理层数据存储区域进行一致性检查,如果当前管理层数据的 CRC 校验值与 CRC 校验表中存储的校验值不一致,则判定当前管理层数据损坏,需要切换到热备份的管理层数据上,并对损坏的管理层

数据进行故障管理层数据恢复.

2.2 动态故障检测

对文件系统的动态故障检测是通过 CRC 校验值完成的.

动态故障检测在每次文件系统写 Flash 存储器的操作完成后进行,通过对扇区进行回读,将读出的数据和写操作的写入数据进行一致性比较,如果二者一致则认为写操作正常完成,否则判定数据块是坏块.

对于判定的坏块,如果是普通数据块,则将此坏块加入坏块表进行管理,同时按照均衡擦写的原则重新分配一个空闲数据块,完成写操作;如果判定的坏块是管理块,则进入热备份数据切换操作.

2.3 热备份数据切换

当动态故障检测发现管理层发生数据损坏时,进行管理层热备份数据的切换,使用热备份数据完成文件系统的正常运行,同时更新当前备份块数据,确保热备份数据保持一致,过程如图 4 所示.

如果在系统运行中出现故障,应该将数据回滚,切换回上一次正确操作的位置,继续运行.

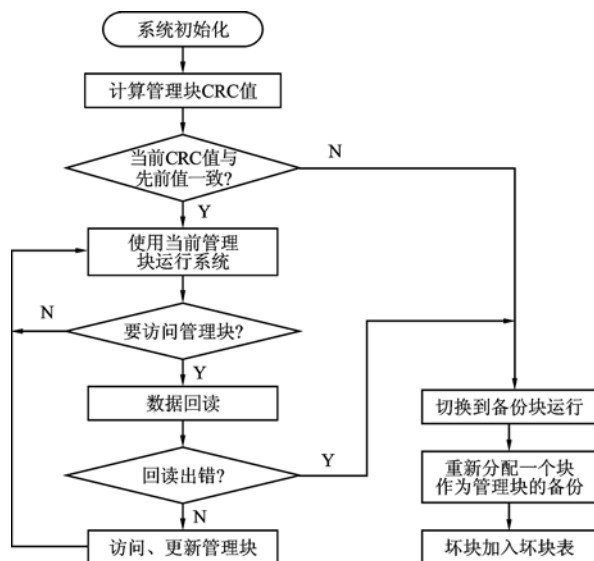


图4 管理层热备份

2.4 故障管理层数据恢复

我们提出了故障管理层数据恢复机制,试图对单粒子翻转导致的管理层数据损坏进行数据恢复,以防止对坏块的误判.

完成管理层数据热备份切换后,首先对损坏的管理层数据存储区进行 Flash 存储器检测. 如果未发生故障,则将热备份的管理层数据复制到该存储区中,实现新的管理层数据热备份;如果发生故障,则判定该存储器为坏块,进行坏块管理,并启动管理

层数据再备份机制.

2.5 管理层数据再备份

由于故障管理层数据恢复机制不能对因 Flash 存储器物理损坏导致的管理层数据损坏进行恢复,为了保证管理层数据热备份机制的持续运行,需要启动管理层数据再备份机制. 管理层数据再备份机制,为正常运行的管理层数据分配新的存储空间,对当前正常运行的管理层数据进行再备份.

在分配新的存储区给再备份管理层数据块之前,需要对分配的存储区进行坏块动态检查,仅当分配的存储区为正常数据块时才分配给管理层数据进行再备份,否则,加入坏块表管理,如图 5 所示.

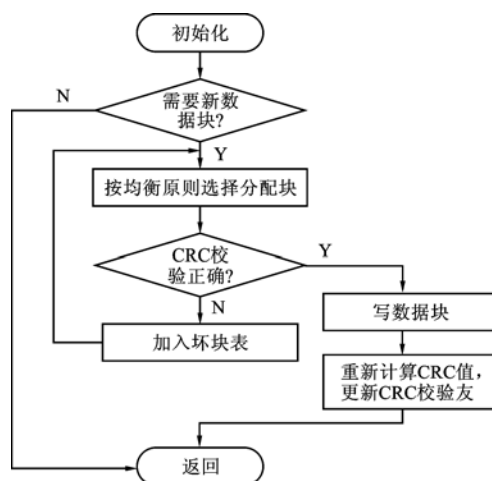


图5 动态块分配

3 结束语

本文针对高可靠文件系统管理层数据导致的文件系统崩溃问题,提出一种管理层数据热备份的高可靠文件系统. 该文件系统通过对文件系统管理层进行热备份,能够避免因管理层数据损坏导致的文件系统崩溃问题. 该文件系统提出的故障管理层数据恢复机制,能够恢复因单粒子翻转导致的管理层数据损坏,提高了管理层热备份高可靠文件系统的运行寿命. 该文件系统提出的管理层再备份机制,能够解决因存储器物理损坏导致的管理层数据损坏,实现对正常运行的管理层数据的再备份,延长了管理层热备份高可靠文件系统的运行寿命.

参考文献:

- [1] Microsoft Corp. Description of the FAT file system [EB/OL]. [2007-01-19]. <http://support.microsoft.com/kb/154997>.

(下转第 22 页)

- markov usage models[J]. Performance Evaluation, 2000, 40(4): 199-222.
- [7] Shi H L, Ma J, Zou F Y. Software dependability evaluation model based on fuzzy theory[C]//International Conference on Computer Science and Information Technology. France, Paris, 2008: 102-106.
- [8] Ma Y F, Zhang M. A computation model of trustworthy degree[C]//International Symposium on Intelligent Information Technology Application Workshops. Shanghai, 2008: 523-526.
- [9] Mei L, Xu Y S. An adaptive dependability model of component-based software[J]. ACM SIGSOFT Software Engineering Notes, 2003, 28(2): 10-14.
- [10] Zhang Y, Fang B, Xu C Y. Trustworthy metrics models for internetwork[J]. Wuhan University Journal of Natural Sciences, 2008, 13(5): 547-552.
- [11] Zhu M X, Luo X X, Chen X H, et al. A non-functional requirements tradeoff model in Trustworthy Software[J]. Information Sciences, 2012(191): 61-75.
- [12] 王怀民. 软件可信分级规范[EB/OL]. [2009-06-01]. <http://www.trustie.com>.
- [13] 邱苑华. 群组决策特征根法[J]. 应用数学和力学, 1997, 18(11): 1027-1033.
- [14] 邱苑华. 管理决策与应用熵学[M]. 北京: 机械工业出版社, 2002.
- [15] 周剑, 张明新. 软件可信评估综述[J]. 计算机应用研

究, 2012, 29(10): 3609-3613.

作者简介:



赵玉洁 女, (1986—), 博士研究生. 研究方向为管理信息系统和软件可信性评估.



罗新星 男, (1956—), 教授, 博士生导师. 研究方向为管理信息系统和软件可信性评估.



刘福军 男, (1989—), 硕士研究生. 研究方向为软件可信性评估.

(上接第 16 页)

- [2] Woodhouse D. JFFS: The Journaling flash file system [C]//Linux Symposium, 2001. Ottawa, 2001.
- [3] Manning C. YAFFS, the first NAND-specific flash file system[R]. Linux Devices, HK Trade Development Council, 2002.
- [4] Schmidt D. TrueFFS wear-leveling mechanism[J]. Technical Note(TN-DOC-017), M-Systems Flash Disk Pioneers, 2002(20): 1-4.
- [5] 黄珊. 军用嵌入式系统中的 Flash 文件系统设计[J]. 现代电子技术, 2003(16): 45-47.
- [6] 陈文华, 郭培源, 陈岩. S3C44BOX 嵌入式系统中 Flash 文件系统的设计与实现[J]. 北京工商大学学报:

自然科学版, 2006, 24(3): 40-43.

- [7] 张明磊, 尚利宏. 几种源码开放的嵌入式文件系统分析与比较[J]. 单片机与嵌入式系统应用, 2007(11): 15-18.

作者简介:

李书根 男, (1985—), 硕士研究生. 研究方向为计算机应用技术.

潘海燕 男, (1964—), 研究员. 研究方向为实时嵌入式软件等.

王培 男, (1983—) 博士, 工程师. 研究方向为嵌入式计算机.