引用格式:郝玉锴,吴姣,李向东,等. 一种机载高安全高可靠数据存储模块的设计[J]. 电光与控制,2019,26(1):109-113. HAO Y K, WU J, LI X D, et al. Design of an airborne data storage module with high security and high reliability[J]. Electronics Optics & Control, 2019, 26(1):109-113.

一种机载高安全高可靠数据存储模块的设计

郝玉锴, 吴 姣, 李向东, 徐 宁
(航空工业西安航空计算技术研究所,西安 710065)

摘 要: 针对综合化、模块化航空电子系统架构中现场可更换模块的设计特点,讨论了一种机载高安全、高可靠的大容量Nand-Flash数据存储模块在符合ARINC653标准的分区操作系统中的设计方法,具有Flash驱动层、Flash管理层、文件系统层架构。通过采用应急关键数据销毁的方式保障系统的高安全性,通过采用坏块管理、损耗均衡以及可信恢复性文件系统的方式保障系统的高可靠性。对数据存储模块进行了不同层级、不同文件大小的读写测试,应急毁钥测试和可靠性测试,测试结果表明模块满足设计要求,可以应用于需要高可靠性和高安全性的航空电子领域。

关键词: 综合模块化航空电子; 现场可更换模块; 坏块管理; 应急毁钥; 分区操作系统
中图分类号: TP311 **文献标志码**: A **doi**:10.3969/j.issn.1671-637X.2019.01.023

Design of An Airborne Data Storage Module with High Security and High Reliability

HAO Yu-kai, WU Jiao, LI Xiang-dong, XU Ning
(AVIC Xi'an Aeronautic Computing Technique Research Institue, Xi'an 710065, China)

Abstract: Aiming at the design features of the Line Replaceable Module (LRM) in the Integrated Modular Avionics, a method is proposed for the design of a Nand-Flash data storage module with high security, high reliability, and large capacity with ARINC653 compliant partitioning operating system. It has a three-layer structure including flash driver layer, flash management layer and file system layer. The method of emergency key data destruction is used to ensure the high security of the system, and the reliability of the system is guaranteed by adopting bad block management, wear leveling and trusted restoring file system. Read/write test, emergency key data destruction test and reliability test were made to the data storage module at different levels and with different file sizes, and the test results show that the module meets the design requirements and can be applied to the field of avionics requiring high reliability and high security.

Key words: Integrated Modular Avionics (IMA); LRM; bad block management; emergency key data destruction; partition operating system

0 引言

航空电子系统自诞生以来经历了从分立式、联合式、综合化到高度综合化的发展过程,从各分系统相互独立到采用模块化高度综合的层次型架构[1]。综合化、模块化航空电子(Integrated Modular Avionics,IMA)系统架构是当今航空电子系统的主流架构模型[2-3],采用可重配的通用模块构建复杂的航空电子系统,有助于提升系统的可用性,增加系统的健壮性,大幅度减少系统的体积、功耗及全寿命周期成本。

现场可更换模块(Line Replaceable Module,LRM)是IMA系统的基本硬件单元,在航电系统中提供一个或多个结构功能,具有高度集成、通用化、故障隔离、带有自检测和维护接口等特点。通过采用标准化模块设计和现代封装技术,提高了LRM在运输、存储、工作以及维护时的可靠性。相比于传统的现场可更换单元(LRU),模块化结构散热能力的提高、模块外壳及安装箱外壳的双重保护,提高了系统的安全性。但是标准化模块的设计理念对软硬件设计提出了新的要求,即在软件设计方面,需要符合ARINC653标准[4];在硬件设计方面,除了相关行业标准,还需要考虑体积和功耗

收稿日期:2017-12-05 修回日期:2018-12-05
基金项目:国家科技重大专项基金(2012ZX01041-006);航空科学基金(2013ZC31005)
作者简介:郝玉锴(1986—),男,山东莱州人,硕士,高工,研究方向为机载嵌入式软件技术。

的要求。1个典型的IMA核心系统可以包括3~4个通用处理模块、1个数据存储模块、2个机载网络交换模块和2个电源模块等[5]。

本文根据IMA架构航电系统LRM模块的特点，讨论一种机载高可靠的数据存储模块设计，具有坏块管理、损耗均衡、分区管理和应急销毁关键数据等特点，应用于符合ARINC653标准的分区操作系统，可以满足航空电子领域高可靠性和高安全性的要求。

1 系统架构

数据存储模块是IMA系统中的典型模型，用来实现机载海量数据的处理、存储、备份等功能。目前阶段，在大容量数据存储领域有着广泛应用的是Nand-Flash，具有存储密度高、改写速度快的优点，在大容量数据存储领域有着广泛的应用。由于自身原因，Nand-Flash在出厂和使用的过程中都有可能产生坏块，但是坏块的存在并不影响有效块的性能，实现坏块管理和损耗均衡是基于Nand-Flash芯片的数据存储设备必备的功能[6-7]。Nand-Flash以“页”(Page)为单位读写数据，而以“块”(Block)为单位擦除数据[8-9]，地址和命令在I/O[7:0]上串行传输，数据宽度是8位。

本文模块设计采用美国美光(Micron)公司的Nand-Flash芯片，每片提供的有效存储空间为2 GiB，每片包含16384个块，每块有64页，每页有2112字节，其中，2048字节用于存储数据，64字节用于存放包括ECC校验和以及好坏块标记等其他信息。硬件采用4片并行的方式提供8 GiB的实际存储空间。结合ARINC653标准的要求和Nand-Flash硬件特点，本文所述系统架构如图1所示。

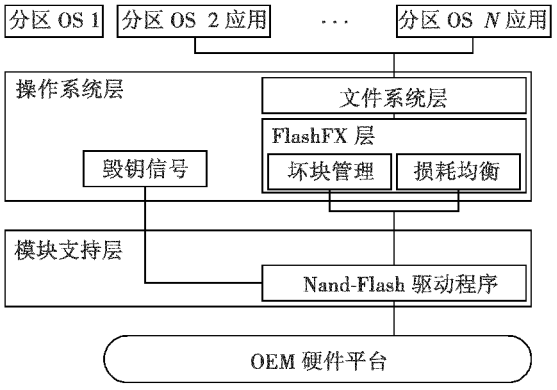

图1 系统架构图

Fig. 1 System structure

通过采用销毁应急关键数据的方式保障系统的高安全性，通过采用坏块管理、损耗均衡以及可信恢复性文件系统的方式保障系统的高可靠性。相比于文献[10]机载数据加卸载卡的设计方案和文献[11]高可靠固态存储模块的设计方案，本文所述系统架构更符合ARINC653标准，文件系统更专用，毁钥实现更彻底，并且能够在机载LRM模块上实现全部功能。

2 数据存储模块的设计

数据存储模块采用1片PowerPC 7447A处理器，配备有4片并行的2 GiB容量Nand-Flash芯片，运行符合ARINC653标准的WindRiver VxWorks653操作系统。

2.1 Flash驱动层设计

Flash驱动层是直接操作OEM硬件芯片的最底层驱动程序，主要涉及Nand-Flash的初始化(包括PCI空间和数据拷贝的初始化、DMA的初始化、获取设备ID、建立坏块信息映像、使能硬件ECC等)、Nand-Flash的块擦除操作、Nand-Flash的扇区写入操作、Nand-Flash的扇区读取操作、Nand-Flash的状态获取操作(包括硬件ECC状态、Flash操作状态、坏块状态等)。

2.2 Flash管理层设计

在Nand-Flash出厂和使用的过程中产生的坏块分别称为固有坏块和使用坏块，Flash管理层通过坏块管理使之不影响Flash的正常使用，通过损耗均衡来降低坏块产生的概率[12]。

2.2.1 坏块管理

本文模块设计的坏块管理采用地址重映射的方法，将Nand-Flash的固有坏块和使用坏块映射到坏块替换区来保证被存储数据的可靠性，坏块管理的基础是通过坏块映射表构建坏块索引。在Nand-Flash芯片第一次使用时，通过驱动层的状态获取函数检测坏块状态，识别出固有坏块并且存储到坏块映射表中。在Nand-Flash芯片的正常读写过程中，通过驱动层的状态获取函数检测Flash操作状态，当操作出现特定错误时，被操作块就会被认定为坏块，更新存储到坏块映射表中。实际使用时，在对一个地址进行读写操作前，通过坏块映射表构建的坏块索引，对地址进行重新映射。本文的坏块映射区为128 MiB，可以替换256×4个坏块，Nand-Flash芯片的物理空间分配如图2所示。

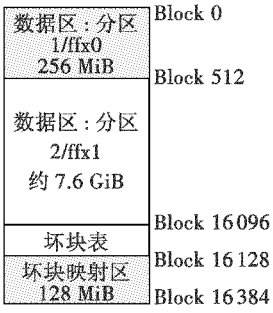

图2 物理空间分配图

Fig. 2 Physical space allocation

2.2.2　损耗均衡

Nand-Flash 芯片的块擦除次数可以达到 10^6 以上，但是如果不采取损耗均衡的策略，某些常用的块可能会被不断擦写以致逐渐失效成为使用坏块，而此时某些不常用块可能还从未被使用过[13-14]。本文采用的损耗均衡策略主要有两种：1）写空块，即当数据需要更新时，不是在数据原有的块内更新，而是将更新的数据写入空块中，将原有的块擦除；2）定期碎片整理，即每隔一定操作次数，将 Nand-Flash 芯片中所有数据集中到一起，尽量将数据块的空间写完，而不是将数据分散在不同的数据块上。

2.3　文件系统层设计

文件系统层向上层分区内应用提供标准的文件读写接口，使不同的分区内应用均能够直接访问，向下基于 Flash 管理层和驱动层，操作 Nand-Flash 芯片，完成数据存储任务。本文采用嵌入式事务型文件系统 Reliance，通过 ARINC653 标准定义的用户系统调用机制向分区提供标准的文件读写接口。

2.4　应急毁钥设计

为了应对复杂多变的战场环境，避免存储设备落入敌手后重要信息泄露而造成的巨大损失，当紧急情况出现后，机载高安全、高可靠存储模块应当具有应急毁钥的功能。

2.4.1　Flash 毁钥技术

常用的 Flash 销毁技术主要有如下 3 种[15-17]。

1）页写零技术。通过对指定的页进行写零覆盖，达到销毁有效数据的目的。该技术的优点是比较灵活，缺点是当销毁的内容较多时，会浪费大量系统时间。

2）块删除技术。通过整块擦除达到销毁有效数据的目的。该技术的优点是销毁速度快，缺点是不够灵活。

3）删除密钥技术。使用过程中对写入 Flash 的数据进行加密，在需要销毁时只销毁密钥。该技术的优点是删除迅速，而缺点是写入和读出的过程中需要加解密操作，消耗系统资源；而且销毁后密文仍然存在，一旦密钥被破解，会造成销毁操作失败。

2.4.2　毁钥方案设计

上述毁钥技术均在 Flash 的物理层考虑，通过 Flash 驱动进行写零或者擦除。但是实际使用中，由于 Nand-Flash 坏块管理和写入均衡，以及文件系统的存在，应用写入 Flash 中的数据位置对于应用来说是不可知的。在这种情况下，一旦需要毁钥，可行的方案只有将整个 Flash 芯片中所有的块页全部销毁，或者删除密钥。

具体到本文的模块设计，由于页写零技术耗时太长，不能采用，删除密钥技术在高安全领域存在密钥被破解的巨大风险，也不能采用，因此考虑块删除技术。机载系统要求在 1.5 s 以内完成毁钥操作，因此将 8 GiB 电子盘物理分区，将要销毁的关键数据放到较小的分区中，进行应急销毁，无关数据放到较大的分区中，不进行销毁。

2.4.3　毁钥流程设计

考虑到毁钥时间要求和坏块管理机制的存在，文件系统将 8 GiB 电子盘分为“/ffx0”和“/ffx1”两个分区，物理空间分配如图 2 所示。软件收到毁钥中断信号时，中断服务程序按照如下顺序执行：1）关中断；2）调用 Flash 驱动层扇区擦除接口擦除“/ffx0”分区共 256 MiB；3）调用 Flash 驱动层扇区擦除接口擦除分区公共替换区域共 128 MiB；4）开中断；5）此时如果毁钥中断信号还存在，则重复上述 1）~4）。

图 2 所示的“坏块映射区”由 Flash 管理层配置，当“/ffx0”分区或者“/ffx1”分区中产生坏块时，从电子盘的最后一个扇区开始，依次替换坏块。当配置的替换区空间用满时，如果再出现坏块，则系统认为电子盘故障，由于可能存在“/ffx0”分区的关键数据的替换，所以在毁钥操作时必须进行销毁。

3　测试和验证

由于相关行业标准中并无专门的高安全、高可靠方面的量化衡量方法，因此本文从数据读写性能、应急毁钥性能和高可靠性功能的角度对数据存储模块进行测试和验证。

3.1　读写性能

3.1.1　裸盘读写性能

在 Flash 管理层进行裸盘数据的读写性能测试，读写次数为 10，读写长度分别为 128 MiB 的 1 ~ 10 整数倍，测试数据如图 3 所示。

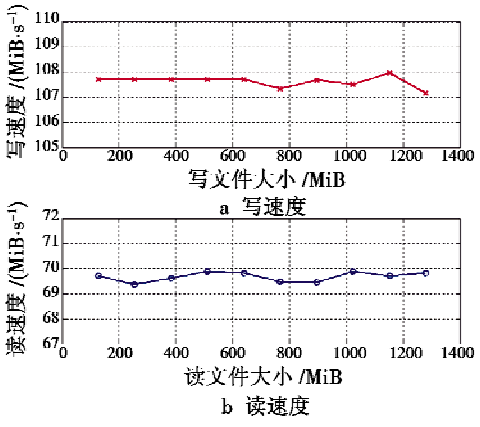

图 3　裸盘读写速度测试

Fig. 3　Disk read and write speed test

3.1.2　文件系统读写性能

分别使用 16 KiB，32 KiB，64 KiB 长度的数据进行

文件写入操作,写入文件大小为 128 MiB,写入次数为 100,测试数据如图 4 所示。

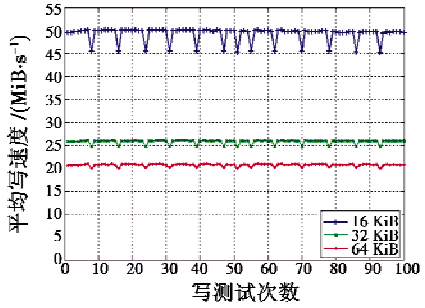

图 4 文件系统写入速度

Fig. 4 Write speed of the file system

分别使用 16 KiB,32 KiB,64 KiB 长度的数据进行文件读取操作,读取文件大小为 128 MiB,读取次数为 100,测试数据如图 5 所示。

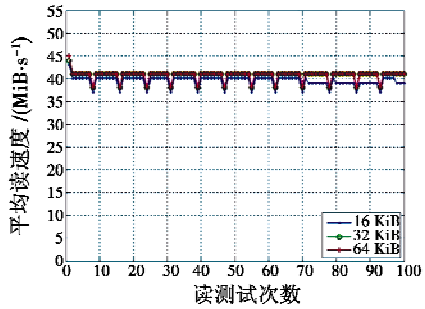

图 5 文件系统读取速度

Fig. 5 Read speed of the file system

3.2 应急毁钥性能

3.2.1 理论推算

根据 2.4 节应急毁钥设计,该方法每次毁钥时擦除的数据总长度均为 384 MiB,因此毁钥操作消耗时间是稳定的,与 Flash 芯片扇区擦除操作时间相关。

3.2.2 实验验证

在数据存储模块上进行 10 次毁钥测试,测得 2.4.3 节所述步骤 1)~4)消耗时间,如图 6 所示。

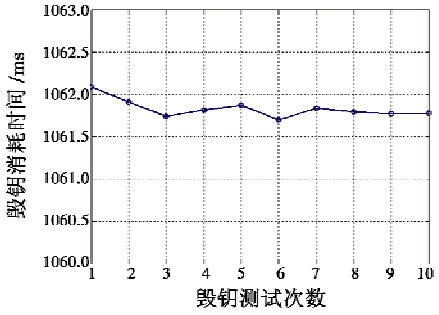

图 6 毁钥操作消耗时间

Fig. 6 Operating time of emergency key data destruction

3.3 可靠性测试

为了测试系统在突发情况下的可靠性,采用了一种成熟的模拟系统崩溃的情况进行测试,测试方法为:

1) 创建一个 4 KiB 的文件;

2) 将该文件的内容全部写为数据“0”;

3) 正常关闭后以可写入的方式再次打开该文件,写入一段时间数据“1”后系统崩溃;

4) 读取文件中的数据进行分析。

经过分析文件中数据的结果全部为“0”可知,在第二次写“1”中系统崩溃,系统回滚到先前一个一致的状态,表明系统可以提供高可靠性的服务。

4 结束语

本文根据 IMA 架构航电系统 LRM 模块的特点,讨论了一种机载高安全、高可靠的数据存储模块设计方法,具有 Flash 驱动层、Flash 管理层、文件系统层架构,应用于 ARINC653 标准的分区操作系统。通过坏块管理、损耗均衡、分区管理和应急销毁关键数据的设计方法,保障了数据存储模块的高安全性和高可靠性。对数据存储模块进行了不同层级不同文件大小的读写测试、应急毁钥测试和可靠性测试,结果满足设计要求,可以应用于需要高可靠性和高安全性的航空电子领域。

参 考 文 献

[1] 牛文生. 机载计算机技术[M]. 北京:航空工业出版社,2013:345-350.

[2] 褚文奎,张凤鸣,樊晓光. 综合模块化航空电子系统软件体系结构综述[J]. 航空学报,2009,30(10):1912-1917.

[3] 张凤鸣,褚文奎,樊晓光,等. 综合模块化航空电子体系结构研究[J]. 电光与控制,2009,16(9):47-51,59.

[4] Aeronautical Radio, Inc. ARINC specification 653-1 avionics application software standard interface[S]. Annapolis:Aeronautical Radio, Inc., 2003.

[5] WOLFIG R. A distributed platform for integrated modular avionics[M]. Berlin:Sudwestdeutscher Verlag Fur Hochschulschrifte AG, 2008:45-50.

[6] LIM S H, PARK K H. An efficient NAND Flash file system for Flash memory storage[J]. IEEE Transactions on Computers, 2006, 55(7):906-912.

[7] YANG S F, WU C H. A low-memory management for log-based file systems on Flash memory[C]//Proceedings of 15th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, Beijing, 2009:219-227.

[8] 高杨,管雪元. 基于 ARM 的大容量 NAND FLASH 应用[J]. 现代电子技术,2016,39(2):65-68.

[9] 秦晓康，徐惠民. 嵌入式设备 NAND Flash 存储系统的设计与实现[J]. 计算机工程与设计,2010,31(3):514-517.
[10] 翟正军,宋霄罡. 机载数据加卸载卡的设计与实现[J]. 测控技术,2010,29(9):96-98,102.
[11] 吴洪成,潘琪. 高可靠固态存储模块的实现与应用[J]. 计算机时代,2015(9):14-16.
[12] PARK C, TALAWAR P, WON D, et al. A high performance controller for NAND Flash-based solidstate disk (NSSD)[J]. Non-Volatile Semiconductor Memory Workshop, 2006(7):17-20.
[13] 晏敏,龙小奇,章兢,等. 开放式大容量 NAND Flash 数据存储系统设计与实现[J]. 微电子学与计算机,2009,26(11):13-16.
[14] 彭卓文,杨新民,王胜红. 基于 FPGA 控制的高速大容量 NAND FLASH 存储模块设计[J]. 电子设计工程,2017,25(7):111-114,118.
[15] BREEUWSMA M, DE JONGH M, KLAVER C, et al. Forensic data recovery from Flash memory[J]. Small Scale Digital Device Forensics Journal, 2007, 1(1):1-17.
[16] 郑光,苏锦海,孙万忠. 闪存数据应急销毁算法的研究与设计[J]. 计算机应用与软件, 2013,30(9):305-308.
[17] 王强,吴海容,陈晓晨. 基于故障物理的航空电子设备高可靠性评估[J]. 航天器环境工程,2016,33(2):216-219.

(上接第 96 页)

[5] 陈增强,李毅,孙明玮,等. 四旋翼无人飞行器 ADRC-GPC 控制[J]. 哈尔滨工业大学学报,2016,48(9):176-180,188.
[6] 何勇灵,陈彦民,周岷峰. 四旋翼飞行器在风场扰动下的建模与控制[J]. 中国惯性技术学报,2013,21(5):624-630.
[7] 张天毅,赵庆展,刘伟. 四旋翼飞行器悬停模式 ITAE 最优 PID 控制[J]. 电光与控制,2016,23(8):48-52.
[8] 甄红涛,齐晓慧,夏明旗,等. 四旋翼无人机块控反步姿态控制器设计[J]. 电光与控制,2013,20(10):87-91,101.
[9] ISLAM S, LIU P X, EL SADDIK A. Nonlinear adaptive control for quadrotor flying vehicle[J]. Nonlinear Dynamics, 2014, 78(1):117-133.
[10] 韩业壮,华容. 四旋翼飞行器的 RBF 网络自适应滑模控制[J]. 电光与控制,2017,24(11):22-27.
[11] 岳欣,姚建勇. 基于自适应的电液负载模拟器积分鲁棒控制[J]. 液压与气动,2016(12):25-30.
[12] WANG X H, SHIRINZADEH B. Nonlinear augmented observer design and application to quadrotor aircraft [J]. Nonlinear Dynamics, 2015, 80(3):1463-1481.
[13] XIAN B, DAWSON D, DE QUEIRO Z M, et al. A continuous asymptotic tracking control strategy for uncertain nonlinear systems [J]. IEEE Transactions on Automatic Control, 2004, 49(7):1206-1211.
[14] KRSTIC M, KANELLAKOPOULOS I, KOKOTOVIC P V. Nonlinear and adaptive control design [M]. New York: Wiley-Interscience, 1995.

(上接第 108 页)

[8] 刘清. 基于自抗扰控制器的永磁同步电机伺服系统控制策略的研究及实现[D]. 天津:天津大学,2011.
[9] 郑春艳,张红刚,冯兴伟,等. 机载光电稳定平台自抗扰控制研究[J]. 电光与控制,2017,24(2):51-54.
[10] 邝平,李军,雷阳,等. 高精度稳定平台伺服系统的自抗扰控制[J]. 工业仪表与自动化装置,2016(1):14-18.
[11] LI J, REN H P, ZHONG Y R. Robust speed control of induction motor drives using first-order auto-disturbance rejection controllers[J]. IEEE Transactions on Industry Applications, 2015, 51(1):712-720.
[12] ZHENG Q, DONG L L, LEE D H, et al. Active disturbance rejection control for MEMS gyroscopes [J]. IEEE Transactions on Control Systems Technology, 2009, 17(6): 1432-1438.
[13] WU D, CHEN K. Design and analysis of precision active disturbance rejection control for noncircular turning process [J]. IEEE Transactions on Industrial Electronics, 2009, 56(7):2746-2753.