

机载嵌入式计算机通用操作系统故障管理软件设计

许 斌, 杨 漫

(中国航空无线电电子研究所, 上海 200233)

[摘 要] 提出了一种对机载嵌入式计算机中常见操作系统故障的监控和记录方法, 结合记录操作系统和处理器的状态信息, 同时考虑到在多种操作系统、处理器上的适应性, 设计一套具有操作系统故障监控和状态信息记录功能的通用操作系统故障管理软件, 提高机载嵌入式计算机的可维护性。

[关键词] 通用化; 故障管理; 日志记录

[中图分类号] TP316

[文献标识码] A

[文章编号] 1006-141X(2020)04-0038-04

The Design Technology of Universal Fault Management Software for Airborne Embedded Computer

XU Bin, YANG Man

(China National Aeronautical Radio Electronics Research Institute, Shanghai 200233, China)

Abstract: A general method of monitoring and recording the operating system fault is presented, which can be applied to airborne embedded computer. Combined with recording the state information of the operating system and the processor, and taking into account the adaptability of various operating systems and processors, a set of general fault management software with fault monitoring and information recording functions for the operating system is designed, which can improve the maintainability of the airborne embedded computing.

Key words: generalization; fault management; log recording

机载嵌入式计算机普遍存在故障监控能力不足的问题, 导致无法检测故障的发生, 或是故障发生后无章可循, 使得排故周期变长。

本文通过对常见操作系统故障的监控以及相关状态信息的记录, 提高系统的故障定位能力, 并设计了一套能够在多种操作系统、处理器以及硬件平台上适配的, 具有故障监控和信息记录功能的通用操作系统故障管理软件。

1 设计实现方法

通用操作系统故障管理软件的主要设计功能包括:

(1) 中断管理

系统中断运行监控、监控信息获取和存储;

(2) 异常管理

系统异常运行监控、监控信息获取和存储;

收稿日期: 2020-03-10

引用格式: 许斌, 杨漫. 机载嵌入式计算机通用操作系统故障管理软件设计 [J]. 航空电子技术, 2020, 51(4): 38-41.

(3) 重启管理

重启运行监控、监控信息获取和存储;

(4) 解析管理

对个监控信息进行在线或离线解析;

(5) 配置管理

对监控运行方式和监控存储方式进行静态和动态配置;

(6) 通用化适配

适配机载嵌入式计算机主流操作系统有 VxWorks6.x、Vxworks5.x、VxWorks653 2.x、天脉操作系统; 适配机载嵌入式计算机主流处理器有 PowerPC 系列、ARM 系列、MIPS 系列。

1.1 中断管理

中断问题会引起应用软件运行卡滞、看门狗复位等故障, 主要原因有:

(1) 中断服务程序处于“死循环”或“长时间阻塞”;

(2) 中断由于非正常原因被频繁触发, 导致 CPU 频繁处理中断。

中断管理功能主要完成上述故障情况下的监控、信息获取、记录功能。监控和记录的内容包括:

(1) 故障发生时间;

(2) 发生“死循环”的中断类型;

(3) 中断发生次数。

1.2 异常管理

异常是处理器自带的一种错误检测形式, 操作系统本身通常具有异常检测机制和异常处理机制^[1]。

在异常发生时, 异常管理实现了获取和存储异常向量信息、异常任务的任务控制块(TCB: Task Control Block)信息、相关硬件模块状态信息, 供排故时通过反汇编等手段进行故障定位。监控和记录的内容包括:

(1) 异常发生的时间;

(2) 异常向量类型;

(3) 异常任务 TCB 信息;

(4) 异常发生时的中央处理器(CPU: Central Processing Unit)寄存器信息;

(5) 异常发生时的函数调用关系;

(6) 异常发生时周边硬件模块的状态信息。

1.3 重启管理

当系统发生不可恢复的故障时, 系统会被复位。

重启管理可获取和记录复位方式和复位前故障信息, 以备故障定位和故障分析。

系统复位方式包括硬复位和软复位^[2], 硬复位需要区分上电复位、看门狗复位还是手动复位。软复位需要记录复位前故障任务号、故障任务 TCB 信息。

重启管理监控和记录的内容包括:

(1) 复位方式;

(2) 复位发生的时间;

(3) 造成系统复位的任务信息;

(4) 复位发生时周边硬件模块的状态信息。

1.4 解析管理

监控信息解析管理对各功能记录的监控信息进行在线或离线解析, 并在解析完成后输出。

在线解析是指通过串口、网口等向目标机发送解析指令, 目标机解析自己的监控信息并输出可视化的字符串信息。

离线解析指的是将目标机内保存的监控信息保存并上传到其他环境中(如非易失存储卡), 通过离线解析程序解析保存的监控信息并输出可视化的字符串信息。

1.5 配置管理

考虑到产品和监控需求的多样化, 监控配置管理实现了通用操作系统故障管理软件的功能可裁剪性和可配置性^[3], 可配置的内容包括:

(1) 各功能是否开启;

(2) 各功能监控信息的存储位置、存储地址;

(3) 各功能监控信息的存储数目;

(4) 其他可配置项。

1.6 通用化适配

通用操作系统故障管理软件支持在多种平台上运行。目前支持机载嵌入式计算机主流操作系统有: VxWorks653 2.x、VxWorks6.x、Vxworks5.x、天脉操作系统; 支持处理器有: PowerPC 系列、ARM 系列、MIPS 系列等。

2 关键技术

2.1 通用化架构设计

本文设计了接口层、功能层、适配层的通用化架构设计方案。适配层完成不同操作系统及 CPU 的通用化适配, 实现不同硬件、操作系统的解耦; 功能

层实现各个监控功能的算法实现；接口层实现对应用调用接口的通用化设计，由应用层完成功能的调用。

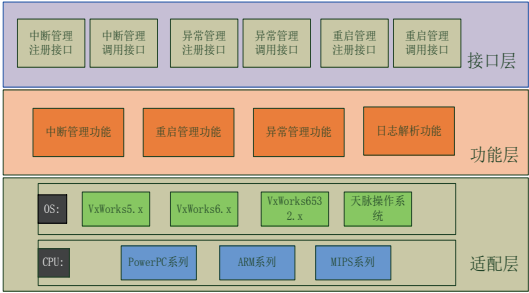


图 1 通用化架构设计图

2.2 捕获方法及通用化实现

异常管理功能中，针对 vxWorks5.x、vxWorks6.x、vxWorks653 的 coreOS 态及分区态；天脉操作系统的 coreOS 态及分区态下堆栈及其他 TCB 信息的捕获进行了通用化实现，实现了堆栈信息到函数调用关系的解析。

2.3 中断管理方法设计

中断管理功能中，将中断可能导致的系统问题分类为：中断服务程序处于“死循环”或“长时间阻塞”^[4]；中断由于非正常原因被频繁触发，导致 CPU 频繁处理中断。中断管理功能通过在中断服务程序总入口挂接处理函数的方法实现上述故障情况下的监控、信息获取、记录功能。

3 测试方案及结果

3.1 测试环境

通用操作系统故障管理软件测试示意图如图 2 所示，被测设备单板由电源 12/28 V 直流输出供电，调试工控机通过标准 RS232 串行接口与单板连接，进行数据通信，完成命令的发送与返回值收集。

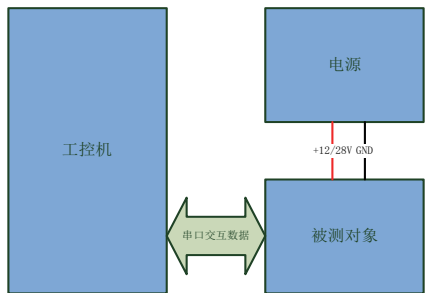


图 2 软件测试示意图

3.2 测试策略

(1) 功能测试

表 1 功能性测试策略

测试范围	验证业务功能、数据类型、数据精确度等方面的相关正确性。
测试目标	核实所有功能均已正确实现，即是否与技术方
采用方法	主要采用黑盒测试、边界测试、等价类划分等测试方法。
工具与方法	实现测试函数和部分手工测试。
开始标准	开发阶段对应的功能完成并且测试用例设计完成。
完成标准	测试用例通过，且最高级缺陷全部解决。
特殊项	该产品将部署于各类航电系统中，要做到通用性，需适配内容较多。

(2) 兼容性测试^[5]

表 2 兼容性测试策略

测试范围	软件须适配各版本操作系统。
测试目标	核实系统在不同软件和硬件配置中的适配情况，是否能正常稳定运行。
采用方法	黑盒测试。
工具与方法	实现测试函数和部分手工测试。
开始标准	开发阶段对应的功能完成并且测试用例设计完成。
完成标准	在各版本操作系统下软件均能正常的实现其功能。
特殊项	根据实际情况而定。

(3) 性能测试

表 3 性能测试策略

测试范围	验证业务性能、软件运行速度等方面的性能指标。
测试目标	核实所有性能均已达到技术方案的要求。
采用方法	代码包或专用测量工具。
工具与方法	实现测试函数和部分手工测试。
开始标准	功能测试完成。
完成标准	测试用例通过并且性能指标符合预期。
特殊项	该产品将部署于各类航空电子系统中，要做到通用性，需适配内容较多。

(4) 可靠性测试

表 4 可靠性测试策略

测试范围	验证软件的可靠性指标。
测试目标	核实软件是否稳定运行并且不会影响到原系统其他功能的正常运行。
采用方法	黑盒测试
工具与方法	实现测试函数和部分手工测试。
开始标准	功能测试完成。
完成标准	软件稳定运行并且不会影响原系统其他功能的正常运行。
特殊项	根据实际情况而定。

(5) 回归测试

表 5 回归性测试策略

测试范围	所有功能、性能、兼容性等测试类型。
测试目标	核实所有功能、性能等均已正确实现并达到用户需求所要求的指标。
采用方法	黑盒测试
工具与方法	实现测试函数和部分手工测试。
开始标准	每当被测软件或运行环境改变时，在适合的测试阶段上进行回归测试。
完成标准	回归测试用例通过，缺陷解决并未引入新的缺陷。
特殊项	软件和硬件设备问题

3.3 自动化测试

自动化测试是将自动化工具和技术应用于软件测试，旨在减少测试工作，更快，更经济地验证软件质量。本文基于 TestStand 和 LabVIEW 进行了自动化测试。通过 TestStand 强大的测试序列功能以及 LabVIEW 中的串口、电源、文本等接口，实现了设备串口调试、用例输入与参数配置、预期结果比对等功能，具体文件及脚本用途如表 6 所示。

表 6 自动化测试

序号	名称	用途
1	Testcasestart.seq	自动化运行序列
2	ReadTestCaseName.vi	用例管理，读取需要运行的用例名称
3	ParseTestCase.vi	用例内容解析
4	TestCaseInput.vi	用例串口输入
5	TestCaseInputUser.vi	用例中各环境串口的登录操作
6	InputConfig.vi	读取输入参数的配置
7	TestCaseName.txt	需要运行的用例名称配置文件
8	ComPortSet.txt	串口参数配置文件
9	cml_XXX_XXX_XXX.txt	测试用例（输入命令行、预期结果、特殊命令）

性能测试结果如表 8 所示。

表 8 性能测试结果

序号	功能模块	测试参数	耗时
1	中断管理功能	100 次	2 毫秒
2		1000 次	12 毫秒
3		10000 次	52 毫秒
4	异常管理功能	第 1 次	3 毫秒
5		第 N 次 (N>1)	2 毫秒
6	重启管理功能	1 次	1 毫秒

本软件完成了所有测试项，测试结果满足了设计需求，通过功能测试、性能测试等确保了软件开发质量。并且，通过对自动化测试工具的引入，更快、更高效的完成了软件测试，实现了软件开发和测试

的快速迭代。

3.4 测试结果

功能测试结果如表 7 所示。

表 7 功能测试结果

序号	处理器类型	操作系统类型	功能测试结果
1	ARM 系列	vxWorks5.x	通过
2		vxWorks6.x	通过
3		vxWorks653	通过
4		天脉操作系统	通过
5	PowerPc 系列	vxWorks5.x	通过
6		vxWorks6.x	通过
7		vxWorks653	通过
8		天脉操作系统	通过
9	MIPS 系列	vxWorks5.x	通过
10		vxWorks6.x	通过
11		vxWorks653	通过
12		天脉操作系统	通过

4 结论

针对机载嵌入式计算机普遍存在操作系统故障监控能力不足的问题，本文提出了一种通用化的操作系统故障管理设计方法，该方法适用于目前机载嵌入式计算机中主流的操作系统和处理器，在很大程度上提高了操作系统故障定位能力和效率，提高了机载嵌入式计算机的可维护性。同时，本文还提出了对本软件设计方案的测试方案和策略，保证了软件的功能完整性和软件质量。

参 考 文 献

[1] Wang Gang,Qiu Jing,Liu Guanjun,Lyu Kehong .Test results judgment method based on BIT faults [J]. Chinese Journal of Aeronautics,2015, 28(6): 1650–1657.

[2] 刘鸽,叶宏,李运喜,等. 基于多分区操作系统的多核确定性调度方法设计 [J]. 航空计算技术 ,2016,46(1):99–102.

[3] 田心宇,张小林,吴海涛,姚英. 机载计算机 BIT 虚警及解决策略研究 [J]. 西北工业大学学报 ,2011, 29(3):400–404.

[4] 何翔,任晓瑞,刘帅. 嵌入式多核操作系统确定性研究 [J]. 航空计算技术 ,2014,44(3):96–100.

[5] 吕向阳,陈明义. 嵌入式系统创新实验室建设 [J]. 实验室研究与探索 ,2005,24(5):32-33.