

机载嵌入式设备中故障管理机制的研究与实现

陈 宁, 李向东, 赵根学

(中国航空计算技术研究所, 陕西 西安 710065)

摘 要: 介绍了一种新的机载嵌入式设备故障检测和故障记录的管理机制. 以符合 ARINC653 标准的国产实时操作系统天脉 2 和 PowerPC 系列处理器为软硬件平台, 对故障码动态注册、故障检测、故障记录和故障回放的运行机制进行详细阐述, 并设计了以中断功能和看门狗功能部件为例的工程实例. 实例结果表明, 该机制高效灵活, 且移植性良好, 对提高机载系统的安全性有较大的意义.

关键词: 机载系统; 故障管理; 故障记录; 故障码注册

中图分类号: TP319

文献标识码: A

文章编号: 1000-7180(2018)01-0110-05

Fault Management Mechanism in Airborne Embedded Devices

CHEN Ning, LI Xiang-dong, ZHAO Gen-xue

(China Aeronautics Computing Technique Research Institute, Xi'an 710065, China)

Abstract: A technique of fault management mechanism was proposed in this paper. Based on the platform of PowerPC series processor and the embedded real-time operating system AcoreOS653 which follows ARINC653 standard, this scheme includes four parts: dynamical fault codes registration, fault detection, fault recording and records check. An algorithm of the scheme was designed based on Interrupt functions unit and watchdog circuit. The results prove that the technique is effective and has good flexibility and portability. It is of great significance to improve the safety of airborne system.

Key words: airborne system; fault management; fault recording; fault codes registration

1 引言

新一代航电系统的高速发展大大增加了航电系统的复杂性, 这与其高安全、高可靠的发展方向之间的矛盾日益突出. 因此, 研究一套高效、灵活、移植性强的机载嵌入式设备故障管理系统十分必要.

目前航电系统中故障测试软件种类繁多, 功能独立, 结构分散, 开发人员难以做到对多类型故障的统一定义、管理及保存, 且综合航空电子系统故障诊断与健康管理技术(PHM)^[1] 目前在国内尚处于理论研究和部分功能开发研究的阶段. 当航电系统在飞机空中运行模式中发生故障时, 位于地面的排故人员难以排查和定位故障, 这为故障追踪与处理带来了极大的不便. 本文基于 PowerPC 处理器^[2] 及国

产操作系统天脉 2 等平台, 提出了一种针对多类型驱动的可注册的故障管理方法. 同时, 各处理器节点间具备故障数据交互能力, 可对各类型故障进行统一管理, 且基于本方法所开发的软件具备良好的灵活性、兼容性、扩展性和可移植性.

2 机载系统软硬件平台和系统运行模式

本文以机载嵌入式领域应用广泛的 PowerPC 系列处理器 P2010^[3] 为硬件平台, 该处理器属于 QorIQ P2 系列, 具有优秀的处理性能和通讯能力. P2010 采用 e500V2 核心, 集成一套非常丰富的接口, 包括 SerDes、千兆以太网、PCI-Express、RapidIO、USB 等等.

操作系统采用符合 ARINC653 标准的国产实

时操作系统天脉 2(ACoreOS653),该操作系统是一款面向多应用多任务的分区实时操作系统,满足当前综合模块化的航空电子系统的应用要求。通过分区技术,实现了运行于同一硬件平台上的多个应用之间的时间和空间隔离。ACoreOS653 操作系统结构如图 1 所示。

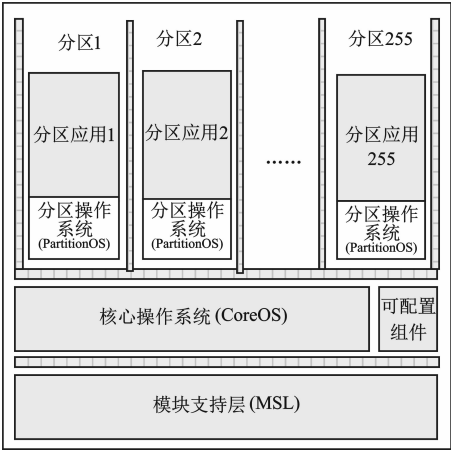


图 1 ACoreOS653 操作系统结构

系统存在两种运行模式:空中运行模式和地面试验模式,也称为空中态和地面态,两者由硬件离散量区别,BOOT 软件根据硬件离散量开关所处位置,进入不同分支。空中运行模式指飞机运行于正常任务时的模式。空中运行模式下,系统层面的软件部件启动流程如图 2 所示。其中,BOOT 是引导程序,完成系统硬件初始化和引导操作系统内核,并自行引导后续软件部件启动。图 2 中 PUBIT(Power Up Build-in-Test)是上电自检测程序^[4],对系统硬件状态进行检测,属于本文中故障管理机制的故障检测的一部分。地面试验模式指供开发人员和排故人员使用的地面调试工作态。

上电后,BOOT 首先被执行,当 BOOT 对硬件环境完成初始化后,即进入人机交互模式,开发人员可对后续执行程序进行选择,可选项一般有:PU-BIT、MSL、操作系统、在线编程项、参数设置等,故障回放、导出功能也在此模式下执行。

3 故障管理机制概述

本文提出的故障管理机制按功能主要分为四部分:故障码注册、故障检测和故障记录及故障回放,如表 1 所示。执行流程为系统上电后,在可能出现故障的功能部件的驱动接口初始化过程中完成故障码注册,获取一一对应的系统返回注册码。系统运行过程中通过多种故障检测手段实时监控系统状态。当

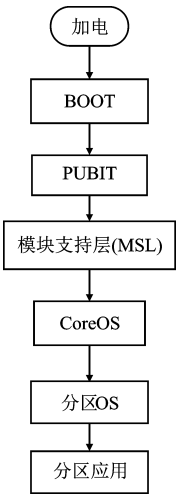


图 2 空中运行模式程序执行流

故障发生时,调用故障记录接口对故障码和故障现场进行记录,再进行故障处理程序注入。

表 1 故障管理机制说明

步骤 编号	步骤 名称	运行 状态	调用时期	获得的结果
1	故障码 注册	空中态	各类驱动初始化 过程	动态获得的故障码
2	故障 检测	空中态	各类驱动接口调 用结束后	是否有故障标识
3	故障 记录	空中态	当 2 检测到故障 发生时	1 中所获得的故障码及 当前执行的故障现场
4	故障 回放	地面态	地面态人机交互 过程	3 所记录的所有信息

4 故障码注册

系统上电后,BOOT 软件完成所有系统软硬件资源的初始化。使用 NVRAM 的空间 (FAULT_ NVM_ SPACE, FNS) 对发生的故障进行记录,BOOT 在初始化的过程中,需对 FNS 区域进行初始化操作,使其处于已管理状态。机载嵌入式系统中可能出现故障的功能部件有 CPU、浮点、中断、RAM、FLASH、定时器、看门狗定时器、FC、串口等,驱动开发人员在对这些功能部件的驱动接口初始化过程中对可能出现的错误进行故障码注册,获取系统返回注册码。应注意的是每一种故障应生成与之唯一对应的系统注册码。

故障码注册机制需要使用两个数据结构:故障码池 (Fault codes pool) 和已注册故障码信息表^[5]。首先设置一个故障码池,为了节省系统的存储资源和保证注册机制的动态可变性,选择单向动态链表来创建故障码池,通过指针来分配故障码。以 CPU 功能部件为例,CPU 驱动进行故障码注册的接口

如下:

UINT32 errCodeReg(UINT32 * SYS_ERR_CMN),SYS_ERR_CMN 作为系统错误码移动指针,始终指向当前数值最小的未被占用的故障码,该接口获取一个返回值,等于 SYS_ERR_CMN 指向的故障码。此接口完成故障码池中未注册使用的故障码与实际故障之间的绑定。同时将该绑定关系存入已注册故障码信息表。

已注册故障码信息表数据结构为结构体:

```
typedef struct errNode
{
    UINT32 errCode; //此次注册返回的故障码
    UINT32 const char * str = "DRV_INF_Name"; //该
    处驱动接口名称
}ERR_NODE;
```

该结构体表示注册过的故障码信息对应情况,便于排查人员定位故障。

除了初始化过程中注册的故障码之外,在系统运行过程中产生的未知故障也注册相应的故障码,只需使用该机制获得未使用的故障码,并将该故障码关联到具体故障,同时在已注册故障码信息表添加注册信息,即可快速动态地为新出现故障分配故障码。该种机制较好地体现了动态性。

5 故障检测

故障检测指运用一系列的测试程序来验证系统的正确性和可用性。这对于保障系统安全具有很大的意义。在目前的航电系统中,通常具有两种类型的故障检测方法:主动检测^[6]和被动检测^[7]。主动检测是指自检检测程序(Built-In-Test,BIT),本文中定义了三种自检检测程序:上电 BIT(Power up BIT,PU-BIT),周期 BIT(Periodic BIT,PBIT)和维护 BIT(Maintenance BIT,MBIT)。被动检测指在系统程序(如 Module Support Layer(MSL)程序、OS 程序以及应用程序等)运行过程中出现程序报错,进行故障记录和故障隔离的过程。PUBIT 运行在 BOOT 之后 MSL 层之前,对系统硬件状态进行检测。它以二进制文件 bin 形式固化在 ROM 空间中。PUBIT 不受操作系统的限制,独自占有系统资源,故测试范围较广且高度依赖硬件,测试项目一般包括 CPU 运算及浮点精度测试、RAM 存储测试、FLASH、看门狗逻辑、NvRam、串口、中断功能、定时器、光纤网络(FC)等;PBIT 是以规定时间间隔周期地启动测试的 BIT,用于系统工作时以固定周期连续不断地监

测系统性能与状态。PBIT 存在于 CoreOS 的静态库中,分区应用通过系统调用方式调用 PBIT 接口。PBIT 运行于系统空闲状态,所以其测试内容不宜过多,通常是对决定系统关键性能的部件进行连续监控;MBIT 在地面试验和维护模式下运行,存在于 CoreOS 的静态库中,对分区应用提供调用接口,包含全局功能检测和各局部功能检测的多个 MBIT 模式,测试人员可根据系统的状态选择相应的测试模式。在 MBIT 运行时,无其他功能性任务对其进行干扰,由此,可在排故联试后,对航电系统进行完整性确认。

6 故障记录

系统运行过程中故障检测程序实时监控可能出现的故障。当故障发生时,调用故障记录接口将故障码和故障现场进行记录。例如在 CPU 驱动的故障处理程序中,调用故障记录接口,接口形式如下:

```
UINT32 faultRec(UINT32 cpuErrorCode,
UINT32 errScene),其中 cpuErrorCode 为该驱动初
始化时调用 errCodeReg()注册得到的故障码,
errScene 为故障现场,保存了故障现场和故障发生
时间。在地面状态时,通过地面维护工具将故障记录
进行回放、导出,从而便于用户定位错误和解决
故障。
```

6.1 空中态故障记录设计

目标机在空中态正确运行起操作系统后,在各故障检测和故障处理程序中调用故障记录接口,在故障发生时将故障码和故障现场存储于 NVRAM 中的故障记录区 FAULT_SPACE。存储故障时采取阈值存储法,根据功能部件的重要程度和开发人员的工程经验,为每一种故障设置阈值,当故障发生次数小于阈值时,将此次故障信息存储于瞬态区域 TEMP_FAULT_SPACE;当此种故障发生次数达到阈值时,将此次故障信息存储于永态区域 FOREVER_FAULT_SPACE,并将此种故障处于瞬态区的数据搬移至永态区域。执行流程如图 3 所示。

6.2 地面态 PC 机端回放

当设备处于地面状态时,系统以地面态方式启动,此时可通过地面态人机交互界面对系统空中态运行时出现的故障进行回放和定位。地面态提供永态区故障回放显示功能、瞬态区故障显示功能、永态区记录数据清除功能、瞬态区记录数据清除功能、故障数据批量导出功能等。

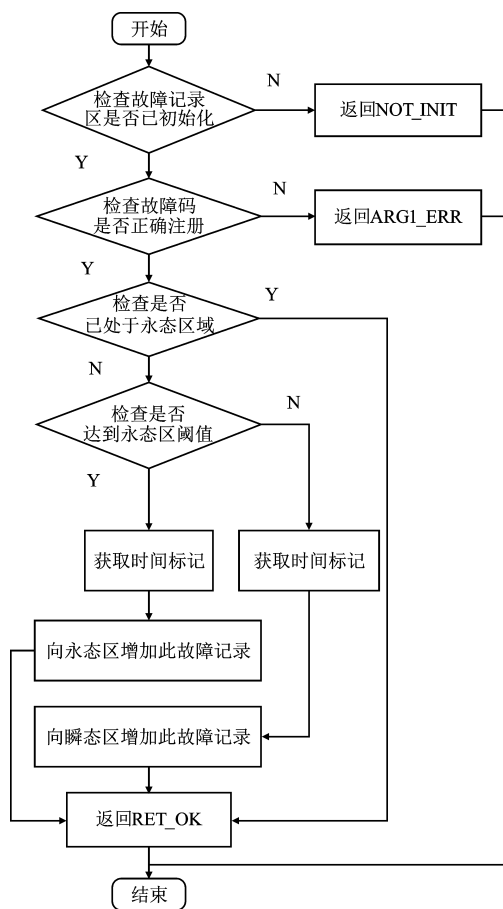


图 3 空中态故障记录执行流程

7 工程实例

本文以系统中断功能为例,执行中断自检测以及对中断故障进行处理的过程,检测本文提出的故障管理机制.中断功能对于要求强实时的嵌入式航电系统至关重要,关系到系统的安全性和实时性.P2010 处理器内部集成可编程中断控制器^[8](Programmable Interrupt Controler, PIC),PIC 是处理器与外设之间的中断处理桥梁,处理外设发出的中断请求并通知内核执行异常服务程序.

中断功能的测试项一般包含“中断响应测试”“中断屏蔽测试”“中断优先级判断测试”等.“中断响应测试”指设置特定功能部件达到中断产生条件,并屏蔽其他中断时,检测 PIC 能否正确响应中断;“中断屏蔽测试”检测当屏蔽某特定功能部件产生的中断时,PIC 是否正确屏蔽该中断;“中断优先级测试”检测当不同优先级的中断同时发生时,PIC 是否能够优先处理优先级较高的中断.中断功能的测试必须依托功能部件触发中断,如看门狗、定时器、FC 总线 2 等.本文的工程实例选择用看门狗来触发中断.

看门狗本质是一个定时计数器,是防止程序跑飞的安全保障措施.本文中由以下 4 个函数进行维护:

enableWatchdog()使能看门狗定时器;

disableWatchdog()屏蔽看门狗定时器;

feedWatchdog()喂狗,即复位看门狗定时器,重新给看门狗一个计数值;

WatchdogIntHandler()看门狗中断服务程序.

本文将结合看门狗定时器的 4 个函数对“中断响应测试”、“中断屏蔽测试”进行设计,由此显示嵌入式故障管理的运行机制.

7.1 中断故障码注册

```

{
    /* 在中断驱动函数(IntrDRV)中进行故障码注册 */
    UINT32 IntrErrorCode;
    IntrErrorCode = errCodeReg(UINT32 * SYS_ERR_CMN);
}
  
```

7.2 故障检测程序设计及故障记录

(1) 中断响应测试算法

```

{
    中断向量表和 PIC 初始化;
    DisableWatchDog(vector);
    feedWatchdog();
    disableWatchdog();
    /* 设置 Watchdog 定时器计数值 */
    SetWatchdogCountNumber();
    /* WatchdogIntHandler 中应设置 FLAG 标志位,此标志位用来判断处理器是否响应了中断 */
    中断向量与 WatchdogIntHandler(*FLAG)挂接;
    EnableWatchdog(vector);
    /* 使能看门狗定时器,使程序运行至此看门狗就开始计数 */
    EnableWatchdog();
    /* 延时一段时间,此时间应大于上面设置的看门狗计数值.等待看门狗计时器溢出产生中断 */
    Delay();
    /* 判断处理器是否响应中断 */
    If(FLAG == FALSE) /* 表示处理器未正常响应看门狗定时器中断 */
    {
        FeedWatchdog();
        DisableWatchDog(vector);
        disableWatchdog();

        Report error;
        /* 调用故障记录接口存储故障信息,故障码 IntrEr-
  
```

```
rorCode 为中断驱动初始化时动态注册得到的 * /
    faultRec( IntrErrorCode, errScene)
}
Return result;
}
```

(2)中断屏蔽测试算法

中断屏蔽算法设计与中断响应测试算法类似,区别在于通过 PIC 屏蔽看门狗中断后,设置看门狗定时器的中断产生条件,延时等待看门狗定时器产生中断.最后通过 WatchdogIntHandler 中设置的标志位是否发生改变判断处理器是否响应了中断.如果响应了中断,则说明通过 PIC 屏蔽中断失败,应上报与此错误相关的动态故障码.

8 结束语

故障管理技术是机载系统中不可缺少的部分.有效的记录和定位故障方法可以带给开发人员和排故人员极大便利,对提高机载系统安全性,降低开发成本有很大的意义.

本文结合当前主流的机载系统架构,提出了一套完整的故障管理机制,并以工程实例为依据验证了该机制.该实例显示此机制高效灵活,移植性良好.

参考文献:

[1] 卢海涛,王自力.综合航空电子系统故障诊断与健康管理技术发展[J].电光与控制,2015,22(8):60-65.

[3] Zhang J, Zhou G, Huang C, et al. TMMAC: An energy efficient multi-channel MAC protocol for Ad Hoc networks[C] // IEEE International Conference on Communications. IEEE, 2007;3554-3561.

[4] Būgra Gedik, Liu L, Yu P S. ASAP: An adaptive sampling approach to data collection in sensor networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2007, 18(12):1766-1783.

[5] Surhone L M, Timpledon M T, Marseken S F, et al. OPNET[M]. Betascript Publishing, 2010.

[6] Young D. USAP: A unifying dynamic multichannel TDMA slot assignment protocol[J]. IEEE, 1996, 1(1):235-239.

[7] Bahl P, Chandra R, Dunagan J. SSCH: slotted seeded

[2] Semiconductor F. Programming Environments Manual for 32-Bit Implementations of the PowerPCTM Architecture[Z]. Freescale Semiconductor, 2005.

[3] Semiconductor F. P2020 QorIQ Integrated Processor Reference Manual[Z]. Freescale Semiconductor, 2012.

[4] 李向东,张晓红,戴小氏,等.机载嵌入式系统中多种机内自测试的软件设计[J].计算机测量与控制,2014,22(4):107-112.

[5] 李向东,赵根学,杜杏虎. MPC8641 处理器内中断控制器的自检测技术[J]. 计算机工程与设计,2014,35(5):1630-1633.

[6] 任国鹏,柴小丽,蒋祺明. 基于 ASAAC 标准的 BIT 设计[J]. 计算机工程,2012,38(12):228-231.

[7] 杨芳,齐璇,董丽,等. 嵌入式软件中断系统资源冲突检测技术研究[J]. 计算机工程与设计,2010,31(23):5036-5038.

[8] 徐凯,张天宏. 航空发动机电子控制器可测试性技术应用研究[J]. 航空发动机,2008,34(2):51-55.

作者简介:

陈 宁 女,(1993-),硕士研究生.研究方向为机载嵌入式软件. E-mail:1025822449@qq. com.

李向东 男,(1986-),工程师.研究方向为嵌入式实时操作系统、嵌入式软件.

赵根学 男,(1975-),高级工程师.研究方向为嵌入式操作系统内核.

(上接第 109 页)

[3] Zhang J, Zhou G, Huang C, et al. TMMAC: An energy efficient multi-channel MAC protocol for Ad Hoc networks[C] // IEEE International Conference on Communications. IEEE, 2007;3554-3561.

[4] Būgra Gedik, Liu L, Yu P S. ASAP: An adaptive sampling approach to data collection in sensor networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2007, 18(12):1766-1783.

[5] Surhone L M, Timpledon M T, Marseken S F, et al. OPNET[M]. Betascript Publishing, 2010.

[6] Young D. USAP: A unifying dynamic multichannel TDMA slot assignment protocol[J]. IEEE, 1996, 1(1):235-239.

[7] Bahl P, Chandra R, Dunagan J. SSCH: slotted seeded

channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks[C] // International Conference on Mobile Computing and NETWORKING. ACM, 2004;216-230.

[8] 叶林睿. 基于 TDMA 的 Ad Hoc 网络 MAC 协议研究[D]. 成都:电子科技大学,2011.

作者简介:

朱全继 男,(1992-),硕士研究生.研究方向为自组网 MAC 层算法. E-mail:zhuquanji@ciotc. org.

慕福奇 男,(1957-),博士研究生,博士生导师.研究方向为无线通信系统与技术、物联网传输与应用.

冷永清 男,(1981-),博士研究生,助理研究员.研究方向为微波固态功率技术、高效功率放大器、微波发射机和接收机.