

引用格式:杨金颖,高文炜,罗雪,等. 基于 VPX 平台的国产 BMC 设计与实现[J]. 微电子学与计算机, 2021, 38(8): 80-86.
[YANG J Y, GAO W W, LUO X, et al. Design and implementation of domestic BMC based on VPX platform[J].
Microelectronics&Computer, 2021, 38(8): 80-86.]

基于 VPX 平台的国产 BMC 设计与实现

杨金颖,高文炜,罗雪,王波
(西安微电子技术研究所,陕西 西安 710000)

摘 要: 针对航天领域 VPX 架构服务器对高可靠性和自主可控的特殊需求,设计并实现了一种基于国产嵌入式 ARM 控制芯片的 BMC 控制器. 该设计满足 VITA46. 11 标准和 IPMI 协议,采用主备冗余机制提高可靠性保证系统正常提供服务;与功能板卡上的 IPMC 通过双冗余 IPMB 总线通信;与远程主机的 IPMI LAN 通信采用 RMCP+ 协议结合 HMAC-SHA1 算法和 AES-CBC-128 加密算法进行身份认证、密钥交换、加密传输实现数据完整性,保证通信安全性,以实现对硬件健康信息的采集与监控及上下电控制等功能. 经测试验证,该设计方案有效可行,在满足功能需求的基础上能够保证可靠性和安全性.

关键词: IPMI 协议;基板管理控制器 BMC;VPX 架构;国产化自主可控;RMCP+

中图分类号: TP315 **文献标识码:** A **文章编号:** 1000-7180(2021)08-0080-07

Design and implementation of domestic BMC based on VPX platform

YANG Jinying, GAO Wenwei, LUO Xue, WANG Bo

(Xi'an Microelectronics Technology Institute, Xi'an 710000, Shaanxi, China)

Abstract: Aiming at the special requirements of high reliability and independent control of servers based on VPX architecture in aerospace , a BMC controller design solution based on domestic embedded ARM control chip is designed and implemented. The design meets VITA46. 11 standard and IPMI protocol. It adopts the redundancy mechanism of main and standby to improve the reliability and ensure the normal service of the system. It can communicate with the IPMC on the function board through the dual redundant IPMB bus. The IPMI LAN communication with the remote host adopts RMCP+ protocol, combining HMAC-SHA1 algorithm and AES-CBC-128 encryption algorithm for identity authentication, key exchange and encrypted transmission, to realize data integrity and ensure communication security, so as to realize the acquisition and monitoring of hardware health information as well as power on and off control. The test results show that the design scheme is effective and feasible, and can ensure the reliability and safety on the basis of meeting the functional requirements.

Key words: IPMI protocol; baseboard management controller BMC; VPX architecture; localization and independent control; RMCP+

1 引言

航天领域计算机系统应用环境复杂、特殊,且随

需求发展软、硬件复杂程度越来越高,故障隐患也随之增加,当出现故障若未能及时诊断和针对性维修,将影响服务器正常运行,甚至导致宕机等严重后果,

这对于航天领域特殊应用结果是不堪设想的. 传统服务器管理主要依赖人工和安装在服务器系统上的远程监控软件如 Telnet、SSH 等. 人工管理需定期巡视、现场排查故障,存在浪费时间又耗费人力,成本高,效率低下,故障信息无法追查等缺点,对于航天领域特殊复杂环境存在较多局限性;远程监控软件运行于服务器操作系统,占用系统资源,影响系统性能,可靠性和安全性无法保障. 为保证军用设备的高可靠性和稳定性,提出一种集中、高效、统一维护和管理解决方案尤为重要. IPMI 协议应用于服务器系统管理的解决方案为航天领域计算机系统提供了一种远程带外监控和管理的方式,其核心 BMC 独立于服务器的 CPU、BIOS 和操作系统进行工作,保证监控管理的可靠性.

针对上述问题及需求,本文在 VPX 平台上基于 IPMI^[1]协议选用国产嵌入式 ARM 芯片设计了一种 BMC 控制器. 采用主备冗余机制设计硬件,基于 RMCP+^[2]协议、HMAC-SHA1 和 AES-CBC-128 算法进行 IPMI LAN 上身份认证和加密传输,以提高 BMC 可靠性和安全性,实现对服务器电压、电流、温度、电源工作状态等的集中、远程、高效监控和管理,为航天领域 BMC 控制器设计提供国产化、自主可控的解决方案.

2 相关协议及算法

为保证 BMC 控制器的可靠性和安全性,本文对于 IPMI 远程网络通信采用 RMCP+协议实现, HMAC-SHA1 算法用于 RAKP(RMCP+ Authenticated Key-Exchange Protocol)^[1]身份认证、密钥交换和数据完整性检验, AES-CBC-128 算法用于对 IPMI 负载加密传输.

2.1 HMAC-SHA1 算法

HMAC^[2]是一种使用加密哈希函数基于密钥提供完整性检查进行消息认证的机制,加密强度取决于底层哈希函数的属性,本文与秘密共享密钥、安全哈希算法 SHA-1^[3]结合使用(用 HMAC-SHA1 表示). 密钥用 K 表示,哈希数据块长度 B 为 64,哈希输出字节长度 L 为 20, K 长度不小于 L ; K 长度大于 B 时,先用 SHA-1 对密钥进行哈希处理,再将所得的 L 字节字符串用作 HMAC 的实际密钥. 定义内部和外部填充字符串 $ipad(0x36$ 重复 B 次)和 $opad(0x5C$ 重复 B 次),对于受保护数据 $data$ 的 HMAC,用式(1)进行计算.

$$SHA1(K \oplus opad, SHA1(K \oplus ipad, data))$$

(1)

2.2 AES-CBC-128 算法

AES-CBC-128 采用高级加密标准 AES^[4]和密文分组链接模式 CBC^[5]对 IPMI 负载进行加密和解密,加/解密时使用一个 16 字节的初始化向量 IV,它是一个由算法生成的高质量随机数,不可预测. 加密和解密的过程如图 1 所示.

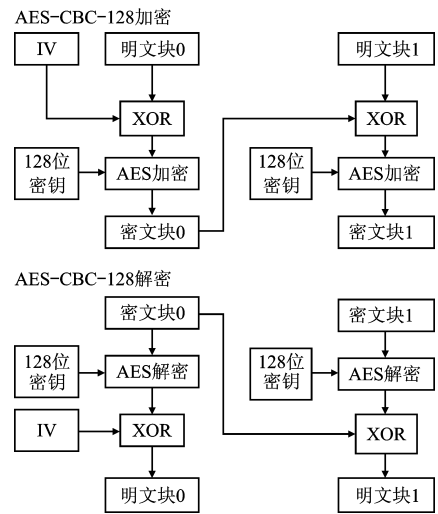


图 1 AES-CBC-128 加密和解密

加密时,有效负载数据被填充为整数个块,每个块 16 字节,第一个块与 IV 异或,再使用 128 位 AES 密钥加密得到加密数据,之后每个块在加密之前与前一个块的加密数据进行异或.

解密时,将密文的第一个块进行 AES 解密,然后将结果与 IV 异或得到明文,之后的每个密文块先 AES 解密,再将结果与前一个密文块异或.

3 VPX 机箱远程管理系统架构

整体架构如图 2 所示,包括运行于 FRU 的 IPMC 控制器上的板卡管理子系统,运行于机箱内主控板的 BMC 控制器上的机箱管理子系统,提供远程管理功能的远程管理子系统^[6]. 板卡管理子系统中,IPMC 监测本板温度、电压、电流等传感器信息,通过两路 IPMB 总线与 BMC 通信,向机箱管理子系统上报系统事件. 机箱管理子系统内的 BMC 采用主备冗余机制,与 IPMC 通信获取传感器信息,接收上报的事件存入 SEL 并处理,对各单板进行上下电控制,通过网络为远程管理子系统提供服务. 远程管理子系统与 BMC 进行 IPMI LAN 通信,远程控制各单板上电及实时监控传感器信息.

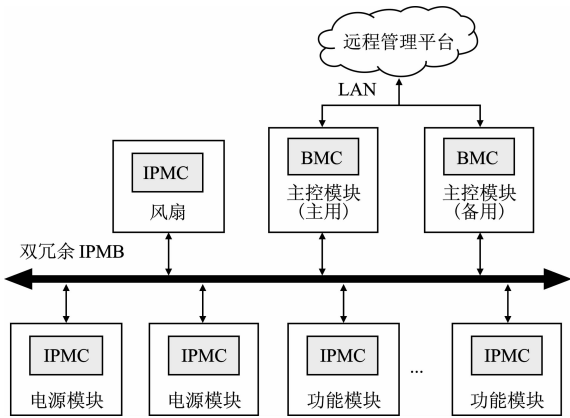


图2 VPX 机箱远程管理系统整体架构

4 BMC 控制器设计

4.1 BMC 控制器功能设计

BMC 为机箱远程管理提供访问 FRU 的远程管理接口,主要实现以下功能:

- (1)BMC 遵循 IPMI 2.0 协议,提供 IPMB 访问接口,支持与 IPMC 通信获取单板温度、电压、电流等信息,接收 IPMC 上传的系统事件存入 SEL(System Event Log)中,并进行相应处理。
- (2)BMC 提供 SDR(Sensor Data Record),可通过 SDR 获取传感器编号,传感器数值计算参数等信息。
- (3)可通过 BMC 控制器串口进行数据访问。
- (4)BMC 提供网络接口,远程管理子系统可通过网络与 BMC 建立 RMCP+安全通信访问 SDR 和 SEL,BMC 再与 IPMC 进行 IPMB 总线通信,从而实现远程访问传感器信息,实时监控机箱内各功能板卡的硬件健康信息。
- (5)可对单板进行远程上下电控制。

4.2 BMC 控制器硬件设计

BMC 是整个系统的核心部件,硬件选型非常关键。结合芯片性能筛选综合比较,最终选用兆易创新的 GD32F450ZKT6 芯片进行硬件设计,该 32 位通用控制器基于 ARMv7 架构,MCU 时钟主频最大可达 200 MHz,Flash 可达 3072 KB 且前 512 KB 零等待,有 256 KB 到 512 KB 的片上 SRAM。

为提高系统可靠性,BMC 采用主备冗余机制,两 BMC 模块先上电的为主用,同时上电采用默认,主备定期相互发送心跳信息进行检测,向工作异常的对端发送硬复位信号,切换主备状态,保证系统能正常提供服务。BMC 硬件还需外设接口支持,双冗余 IPMB 总线 IPMB-A 和 IPMB-B 采用两路 I2C 总线来实现;网络通信通过以太网接口来实现,为提高

安全性将 IPMI 接口访问限制在一个专用的物理隔离的网络上;看门狗电路监测由软件故障导致的系统故障以提高软件可靠性;根据功能需求还需串口 UART、定时器、ADC 等硬件接口和设备的支持^[7]。BMC 硬件模块结构如图 3 所示。

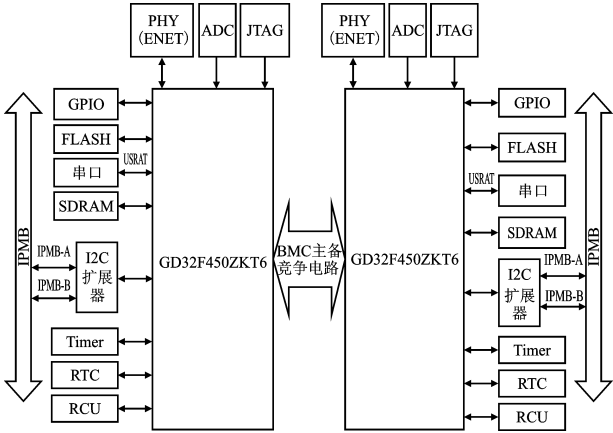


图3 主备冗余 BMC 硬件模块结构图

4.3 BMC 控制器软件设计

BMC 控制器软件总体设计流程图如图 4 所示。根据功能需求和硬件设计,基于 IPMI 2.0 协议进行 BMC 的软件设计。航天军工特殊应用对 BMC 的稳定性和可靠性提出更高要求,本设计向 BMC 移植 FreeRTOS 嵌入式实时操作系统以提高 BMC 的运行效率,该操作系统基于多任务调度管理,体积小,适用于 BMC 硬件;在安全性和可靠性方面,BMC 远程通信基于 RAKP 消息机制通过 HMAC-SHA1 算法实现 IPMI 增强认证 RMCP+,通过 AES-CBC-128 算法加密有效负载数据。

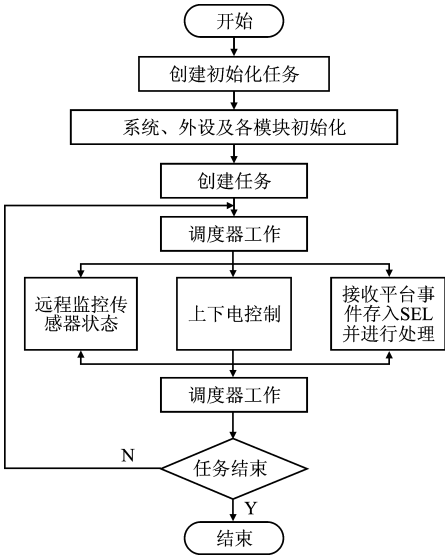


图4 BMC 软件总体设计流程图

4.3.1 远程监控传感器状态和 SDR

远程管理软件(RMS)实现对 FRU 的实时监控和管理,先与 BMC 建立基于 RMCP+ 的 IPMI LAN 通信;再通过 BMC 消息桥接机制在 LAN 通道和 IPMB 通道之间发送消息,实现远程访问 IPMC 进行管理,流程图如图 5 所示.

4.3.1.1 基于 RMCP+建立 IPMI LAN 通信

SID_{BMC} 表示 BMC 会话 ID, SID_{RMS} 表示 RMS 会话 ID, R_{RMS} 表示 RMS 随机数, R_{BMC} 表示 BMC 随机数, $GUID_{BMC}$ 表示 BMC 全局唯一 ID, $Role_{RMS}$ 表请求的角色权限等级, $ULength_{RMS}$ 表示用户名长度, $UName_{RMS}$ 表用户名.

RMS 向 BMC 发送 Get Channel Authentication Capabilities 请求命令开启建立一个 RMCP+ 会话的过程,BMC 返回包含 RMCP+ 认证类型和匿名、一键、两键登录信息的响应;再发送 RMCP+ Open Session Request 命令请求一个受保护的会话,主要包括 SID_{RMS} 和身份认证、完整性、加密负载建议,BMC 返回响应包含 SID_{RMS} 、 SID_{BMC} 和从 RMS 建议列表中选择负载,接下来通过 RAKP 消息机制开始会话身份认证密钥交换过程,该过程通过两个密钥完成,用户密钥 $K[UID]$ (UID 表示用户特定配置命令中的用户 ID)与 $Role_{RMS}$ 和 $UName_{RMS}$ 关联,在 BMC 和 RMS 之间共享;还有一个单独的 160 位 BMC 密钥 KG ,一键登录时用 $K[UID]$ 代替 KG .

(1)RAKP Message 1:RMS→BMC

开始会话身份认证过程,向 BMC 发送 RMCP+ Open Session Response 中指定的 SID_{BMC} , R_{RMS} , $Role_{RMS}$ 和 $\langle UName_{RMS} \rangle$ (可选).

(2)RAKP Message 2:BMC→ RMS

收到 RAKP Message 1 后,BMC 验证 SID_{BMC} 是否处于活动状态,能否使用 $Role_{RMS}$ 、 $ULength_{RMS}$ 、 $UName_{RMS}$ 根据 RAKP-HMAC-SHA1 算法创建会话,若请求有效,发送 SID_{RMS} , R_{BMC} , $GUID_{BMC}$ 以及将 $K[UID]$ 和 $(SID_{RMS}, SID_{BMC}, R_{RMS}, R_{BMC}, GUID_{BMC}, Role_{RMS}, ULength_{RMS}, \langle UName_{RMS} \rangle)$ 代入 2.1 节中式(1)生成的 20 字节 HMAC.

(3)RAKP Message 3:RMS→ BMC

收到 RAKP Message 2 后,RMS 验证 SID_{RMS} 是否处于活动状态, $GUID_{BMC}$ 是否与希望通信的 BMC 匹配,然后验证消息中的密钥交换身份认证码,若有效,RMS 用 KG 根据式(2)创建会话完整性密钥 SIK ,再发送 SID_{BMC} 以及将 $K[UID]$ 和 $(SID_{RMS}, R_{BMC}, Role_{RMS}, ULength_{RMS}, \langle UName_{RMS} \rangle)$ 代入

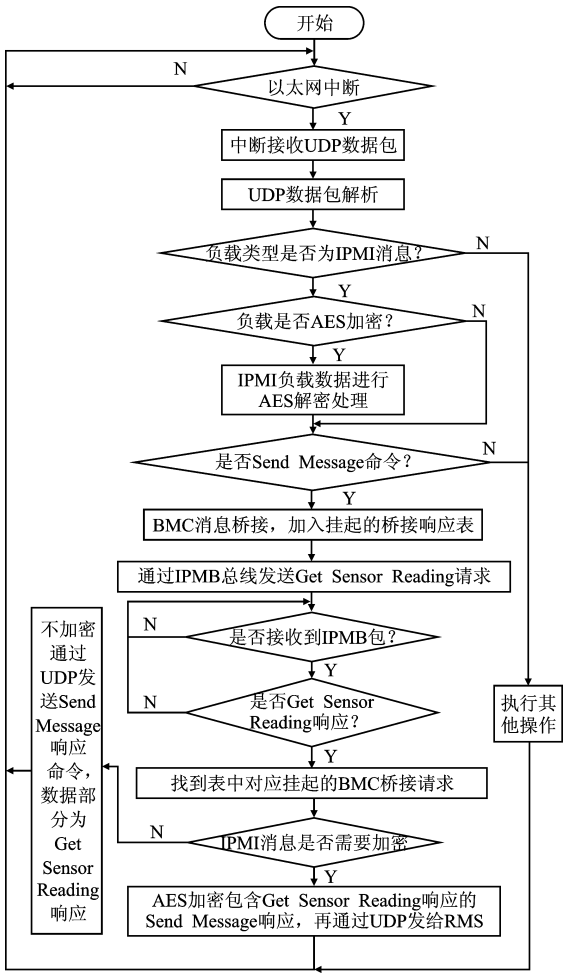


图 5 远程监控传感器状态流程图

2.1 节中式(1)生成的 20 字节 HMAC.

$SIK =$

$$HMAC_{KG} \left[\begin{array}{l} R_{RMS} \parallel R_{BMC} \parallel Role_{RMS} \\ \parallel ULength_{RMS} \parallel \langle UName_{RMS} \rangle \end{array} \right] \quad (2)$$

(4)RAKP Message 4:BMC→ RMS

收到 RAKP Message 3 后,BMC 验证 SID_{BMC} 是否处于活动状态,再验证 HMAC,若有效则 BMC 按式(2)创建会话完整性密钥 SIK ,发送 SID_{RMS} 以及用 SIK 和 $(R_{RMS}, SID_{BMC}, GUID_{BMC})$ 根据 HMAC-SHA1-96^[8] 算法生成的 12 字节完整性检查值.

RMS 收到 RAKP Message 4 后验证 SID_{RMS} 活动状态和完整性检查值,若有效则验证与 BMC 的相互身份认证是否成功以及在连接的两端是否成功生成相同的成对唯一 SIK ,然后转换到消息传输会话状态,此时可传输经过身份验证/加密的有效负载.

对 IPMI 负载采用 2.2 节中的 AES-CBC-128 算法进行加/解密,AES 的 128 位密钥是密钥 $K2$ 的

前 128 位, K2 由会话激活期间创建的 SIK 根据 HMAC-SHA1 算法处理预定义常数生成. 加密的 IPMI 负载包含头部、数据、尾部, 头部存储初始化向量 IV, 尾部存储加密填充数据和长度.

4. 3. 1. 2 传感器数据记录 SDR 的设计

SDR 可供 RMS 访问来获取传感器信息, 如传感器编号 (Get Sensor Reading 请求的参数字段)、传感器真实值计算参数等. SDR 由记录头部、记录关键字段、记录体三个主要部分组成, 其中记录关键字段可确定传感器位置 (由传感器 ID 和传感器 LUN 确定) 和传感器编号; 记录体主要包括实体 ID、传感器类型 (温度、电压、电流等)、传感器单位类型 (degrees C、Volts、Amps 等)、传感器真实值计算公式参数、传感器门限、传感器名称等信息. 考虑到本设计使用基于门限的传感器, SDR 设计使每条记录唯一标识一个传感器并存储其信息, 可存储 64 字节信息, RMS 在访问 BMC 的 SDR 时由记录 ID 唯一确定每条记录, 打印信息时对于同类型传感器可由 SDR 中 Sensor ID String 字段区分.

4. 3. 1. 3 BMC 消息桥接通过 IPMB 获取传感器信息

BMC 消息桥接提供在连接到 BMC 的不同介质通道发送 IPMI 消息的机制, 要将 IPMI 请求从 LAN 发送到 IPMB, 再将响应从 IPMB 发送到 LAN, 可通过 Send Message 命令机制实现. 为获取单板传感器读数, RMS 向 BMC 发送 Send Message 请求命令, 数据部分包含通道号 (0 为 IPMB) 和 Get Sensor Reading 请求命令信息; 设计使 BMC 能处理桥接请求将 Get Sensor Reading 数据部分参数、LAN 会话信息存入挂起桥接响应表中, BMC 的序列号分配器产生一个唯一的序列号来标识该桥接, 此序列号即为 BMC 将 Get Sensor Reading 请求重新格式化后发送到 IPMB 通道的请求序列号; 当接收到来自 IPMB 的响应后, 根据序列号在挂起桥接响应表中找到对应桥接信息, 生成 LAN 通道的 Send Message 响应信息返回给 RMS 即可获取到传感器的读数.

4. 3. 2 上下电控制

通过嵌入式 Web 服务器实现上下电控制主要基于公共网关接口 (Common Gateway Interface, CGI) 设计, 提供与客户端 HTML 页面进行交互的接口. 设计将 BMC 作为嵌入式 Web 服务器, 与远程 PC 能进行以太网通信, 在 PC 端浏览器中输入 BMC 的 IP 地址进行访问, 在上下电控制页面, 点击

上电或下电、提交表单, BMC 接收浏览器发送的 URL 进行分析并提取. cgi 名和变量的值 (操作码和板卡编号), 调用上下电控制处理程序 powerCtl. cgi, 通过 IPMB 接口向对应板卡 IPMC 发送 Set FRU Activation 命令 (该命令为 VSO 扩展的 IPMI 命令) 来进行上下电控制, 流程图如图 6 所示.

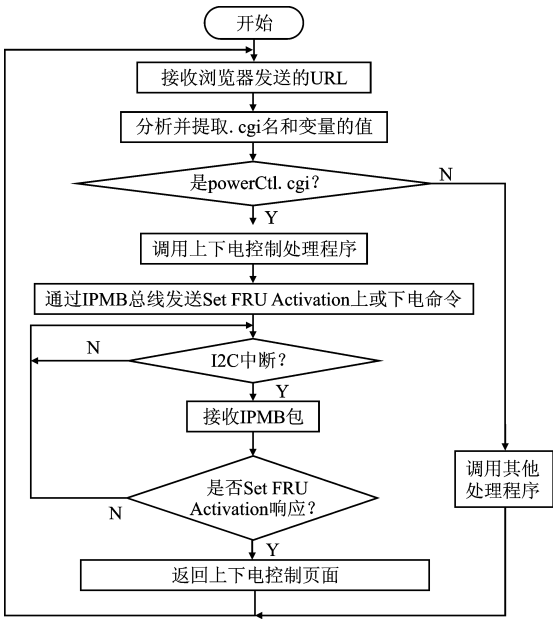


图 6 嵌入式 Web 服务器实现网页控制上下电流程图

4. 3. 3 平台事件处理和 SEL

该模块流程图如图 7 所示.

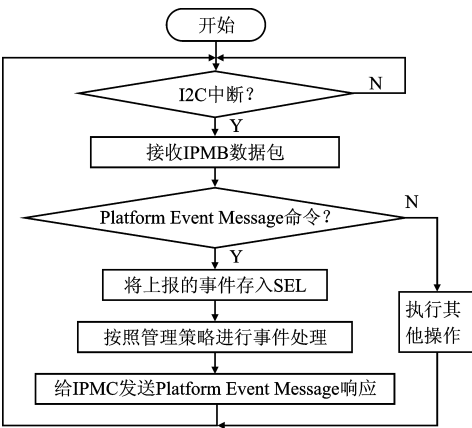


图 7 接收平台事件存入 SEL 并处理的流程图

4. 3. 3. 1 接收平台事件并处理

IPMC 通过双冗余 IPMB 总线发送 Platform Event Message 命令向 BMC 上报平台事件, 包括三种类型事件消息, 一是板卡的工作状态变化事件, 二是板卡传感器告警事件, 三是板卡 Payload 电源周期性自检结果事件. 板卡在系统上、下电, 电源错误等情况影响下工作状态会在七种状态间切换, 工作

状态切换时 IPMC 需向 BMC 上报工作状态变化事件. IPMC 周期性检测传感器数值并与传感器对应上下门限进行比较,超出门限时需向 BMC 上报传感器告警事件. IPMC 周期性检测 Payload 电源状态并将自检结果生成事件上报给 BMC. BMC 在接收到这三种事件消息时,给予 IPMC 响应并执行相应处理策略,将事件存入 SEL 中,例如接收到温度过高的事件时,根据管理策略提高风机转速.

4.3.3.2 系统事件日志 SEL 的设计

SEL 事件记录具体格式如表 1 所示.

表 1 SEL 事件记录格式

字节	数据字段
1,2	记录 ID
3	记录类型
4,5,6,7	时间戳
8,9	生成事件的设备 ID(请求地址,请求逻辑单元)
10	事件消息格式版本
11	传感器类型
12	传感器编号
13	事件类型
14	事件数据 1
15	事件数据 2
16	事件数据 3

SEL 的设计是在事件消息数据的前边加上 SEL 记录 ID、记录类型、时间戳字段和 Generator ID. 记录 ID 唯一标识每条 SEL 记录,记录类型 02h 表示系统事件记录,时间戳记录的是事件被存入 SEL 的时间.

5 测试与实现

为验证本设计可行性,对于远程监控传感器信息,采用 Ipmitool 工具作为 RMS 通过网络连接到 BMC 进行测试. Ipmitool 在 Linux 和 Windows 平台上均可使用,在 Windows 平台上使用时需在类 Unix 环境 Cygwin 中编译源码得到工具软件和相关库包. PC 与 BMC 进行网络连接,保证互相能够 ping 通,在命令行窗口输入 Ipmitool 命令,后台会自动发送封装在 UDP 包中且符合 IPMI 协议的 RMCP+数据包,与 BMC 建立会话连接,开始 IPMI LAN 通信. 以获取传感器信息为例,输入 ipmitool-lanplus-H 192. 168. 51. 100-U USERID-P PASSWORD sensor list 命令,表示使用 lanplus 接口向目标 IP 地址所指向的主机发送命令获取传感器信

息,-U 和 -P 后参数分别为登录 BMC 的用户名和密码. 用 Wireshark 软件抓包可看到 BMC 与 Ipmitool 之间 IPMI 通信的过程,可根据数据包信息确定发送的是哪条命令以及具体数据信息. Ipmitool 将从 BMC 收到的数据按照传感器名称、传感器值、单位、状态以及上下六种门限的字段格式打印出来,测试结果如图 8 所示,在 Ipmitool 中打印出了各传感器的详细信息,可以证明 IPMC 监测结果、IPMC 和 BMC 间通信、BMC 和远程管理软件之间通信的准确性和有效性. 对于系统事件日志、远程控制上下电、传感器信息等功能,BMC 作为 Web 服务器提供可视化管理服务如图 9 所示,PC 端浏览器输入 BMC 的 IP 地址访问,经测试可实现上述功能证明本设计是可行的.

Exhaust Temp	25.000	degrees C	ok	-121.000	127.000	na
DSP1 Temp	na	degrees C	na	-121.000	127.000	na
DSP2 Temp	na	degrees C	na	-121.000	127.000	na
CPU1 Temp	35.000	degrees C	ok	na	na	na
CPU1 UOLTI	87.000	Volts	ok	na	1.282	na
DSP2 UOLTI	na	Volts	na	0.083	3.034	na
DSP3 UOLTI	na	Volts	na	0.083	3.034	na

图 8 Ipmitool 获取传感器信息打印结果



图 9 BMC 提供可视化管理界面

本设计提供可视化管理硬件健康信息的服务,与其它实现方式相比,通过 BMC 实现带外管理不占用系统资源,可提高系统运行效率;远程集中高效管理可降低管理成本;采用国产芯片以及自主可控的设计方案可提高系统安全性和可靠性.

6 结束语

本文针对航天领域 VPX 平台硬件健康信息监控,设计并实现了一种基于国产嵌入式 ARM 控制芯片的 BMC 控制器设计解决方案来提高可靠性. 本设计基于 IPMI 协议,硬件采用主备冗余机制保证正常提供服务,IPMI LAN 通信采用 RMCP+协

议结合 HMAC-SHA1 算法和 AES-CBC-128 加密算法保证数据完整性和通信安全性,将 IPMI LAN 通信和 IPMB 通信桥接起来,从而实现对硬件信息如温度、电压、电流等的远程监控以及上下电控制等功能,经测试验证本设计有效可行,可监控系统硬件健康信息,保证可靠性和安全性,为国产化自主可控 BMC 控制器研究提供了参考。

参考文献:

- [1] Intel Hewlett-Packard NEC Dell. Intelligent platform management interface specification v2.0 rev. 1.1[S]. 2013.
- [2] KRAWCZYK H, BELLARE M, CANETTI R. RFC 2104-HMAC Keyed-hashing for message authentication[S]. 1997.
- [3] NIST. FIPS PUB 180-1 Secure hash standard [S]. 1995.
- [4] DAEMEN J, RIJMEN V. The design of rijndael; AES - the advanced encryption standard[M]. Berlin Heidelberg: Springer, 2002. DOI: 10.1007/978-3-662-04722-4.
- [5] VAIDEHI M, RABI B J. Design and analysis of AES-CBC mode for high security applications[C]//Proceedings of the 2nd International Conference on Current Trends in Engineering and Technology. Coimbatore, India; IEEE, 2014: 499-502. DOI: 10.1109/IC-CTET.2014.6966347.
- [6] 张睿, 黄泳铭, 吴悠, 等. 基于国产平台 VPX 架构的 IPMC 控制器设计[J]. 计算机测量与控制, 2018, 26(6): 99-103. DOI: 10.16526/j.cnki.11-4762/tp.2018.06.025.
- ZHANG R, HUANG Y M, WU Y, et al. Design of the VPX architecture IPMC controller based on domestic platform[J]. Computer Measurement & Control, 2018, 26(6): 99-103. DOI: 10.16526/j.cnki.11-4762/tp.2018.06.025.
- [7] 吴之光, 耿士华. 浅谈 BMC 管理系统在国产平台服务器中的应用[J]. 信息技术与信息化, 2016(1-2): 51-53. DOI: 10.3969/j.issn.1672-9528.2016.01-02.010.
- WU Z G, GENG S H. Application of BMC management system on the server of domestic platform[J]. Information Technology & Informatization, 2016(1-2): 51-53. DOI: 10.3969/j.issn.1672-9528.2016.01-02.010.
- [8] MADSON C, GLENN R. RFC2404 The use of HMAC-SHA-1-96 within ESP and AH[S]. 1998.

作者简介:

杨金颖 女, (1996-), 硕士研究生. 研究方向为嵌入式计算机应用技术. E-mail: yjy_0729@163.com

高文炜 男, (1975-), 硕士, 研究员, 硕士生导师. 研究方向为嵌入式系统.

罗雪 女, (1989-), 硕士, 工程师. 研究方向为嵌入式 DSP、ARM 等软件设计.

王波 男, (1993-), 硕士研究生. 研究方向为嵌入式计算机应用技术.