

# 原创性声明

本小组声明所提交的电子设计作品文章是该小组所有成员在导师指导下进行的创新设计工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表和撰写过的研究成果。

电子设计题目：车载 COTS 信息处理平台的设计与实现

电子设计小组成员签名：黄影 李毅 刘东 李瑞 日期：二〇〇六年三月十九日

作者简介：

黄影，男（1983-），国防科技大学计算机学院，硕士研究生

李毅，女（1981-），国防科技大学计算机学院，硕士研究生

刘东，男（1980-），国防科技大学计算机学院，博士研究生

李瑞，男（1977-），国防科技大学计算机学院，博士研究生

指导老师：

张春元，男（1964-），国防科技大学计算机学院教授，博士生导师

通讯地址：湖南省长沙市国防科技大学六院五队，邮编 410073

联系电话：黄影 13723858300 李毅 13574842498

E-mail: [yinghuangying@nudt.edu.cn](mailto:yinghuangying@nudt.edu.cn) [necklacemary@163.com](mailto:necklacemary@163.com)

## Design and Implementation of The On-Board Information

### Processing Platform Based on COTS

HUANG Ying , LI Yi, LIU Dong, LI Rui and ZHANG Chun-yuan

Department of Computer

National University of Defense Technology

Changsha Hunan 410073

P . R . China

**Abstract:** Fault-tolerant technique is a key way to improve reliability of computer system, which is more and more widely applied in design and development of computers under on-board environment. An embedded resolver of the on-board information processing system based on COTS was presented and implemented. In allusion to abominable environment, a multi-level fault-tolerant mechanism based-on FPGA, which has greatly improved system's reliability and stability, were implemented, by using Altera's EP1C6Q240C8 and EP1C4F400C8. In addition, an abnormal-current-resisting protection circuit was designed with both chip-level and board-level's detections. With reliability greatly enhanced to fit the need, the system was high-performance, low-cost and small-volume.

**Key words:** COTS; Dual Fault-Tolerant; FPGA

# 车载 COTS 信息处理平台的设计与实现

黄影，李毅，刘东，李瑞，张春元

(国防科技大学计算机学院，长沙，410073)

**摘要：**容错技术是提高计算机系统可靠性的重要手段，广泛应用于各种抗恶劣环境计算机的设计中。本文提出并实现了一种基于 COTS 技术的车载信息处理系统的嵌入式解决方案。针对可能的恶劣工作环境，使用 Altera 的 EP1C6Q240C8 和 EP1C4F400C8 芯片设计实现了基于 FPGA 的多级容错技术，并采用芯片和板级两级监测大电流保护电路，有效地提高了系统的可靠性和稳定性，满足了该信息处理系统性能高、成本低和体积小的要求。

**关键词：**COTS；双机容错；FPGA

**中图分类号：**TP302.8

**文献标志码：**A

## 1 引言

嵌入式系统是泛计算领域的重要组成部分，是嵌入式对象宿主体系中完成某种特定功能的专用计算机系统。嵌入式系统有体积小、功耗低、集成度高和子系统能通信融合的优点。随着汽车技术的发展以及微处理器技术的不断进步，在汽车电子技术中得到了广泛应用。目前，从车身控制、底盘控制、发动机管理、主被动安全系统到车载娱乐、信息系统都离不开嵌入式技术的支持<sup>[1]</sup>。

车载信息处理平台作为汽车商业应用领域和计算机领域结合的产物，设计的目标之一就是成本低、质量小以及研制周期短，使用 COTS (Cost-Off-The-Shelf, 商用现货) 的元器件和开发工具可以更好的支持这一思想。通过多级容错技术的应用，本文设计并实现了一个能够恶劣辐射环境的嵌入式系统，能够应用在车载电子信息处理系统中。

COTS 技术的引入是当前嵌入式系统设计开发的一个趋势，在军用和商用领域都有着广阔的应用前景。采用商用微处理器具有运算速度快、软件编程平台完善、应用软件多、系统组成灵活等特点，但如何保证其在恶劣环境中的高可靠性、高稳定性和高性能，是一个具有挑战性的课题。

## 2 车载信息处理平台的设计与实现

### 2.1 系统结构及功能设计

#### 2.1.1 硬件平台结构及其功能

车载信息处理平台作为汽车控制系统的核心，是一个典型的实时嵌入式系统，负责汽车的电子控制和数据通讯等。该平台系统的硬件平台结构如图 1 所示，主要包括嵌入式处理器和外围设备。

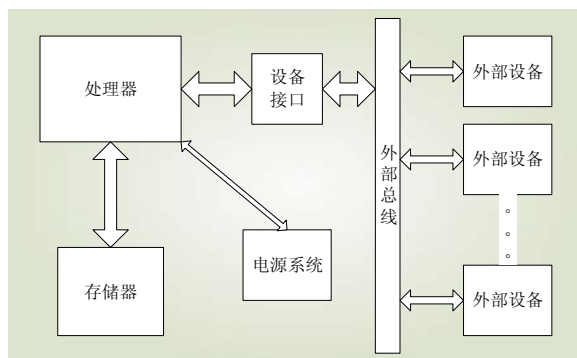


图 1 车载信息处理平台总体结构图

从图 1 中可以看出，嵌入式车载信息处理平台实现了模块化结构。外部存储器有两种，一是 Flash 存储器，用于存放系统程序和用户程序，因为这些程序有可能需要在线更新，因此采用可擦写的 Flash 存储器；二是 SRAM 控制器，用于存放临时的数据，因为系统运行时频率很高，必须采用高速 SRAM，提高数据读写的速度，以免其成为系统的瓶颈。

由于外设数量众多，数据量大，接口类型各异，本设计采用 USB 2.0 接口作为硬件平台对外部设备的统一接口，将各种外设的数据转换成统一的信号，经同一设备接口发往嵌入式硬件平台，如此可简化接口的设计，并方便其采集数据。

如图 2 所示，为嵌入式硬件平台的体系结构图。该平台共分为四个模块：

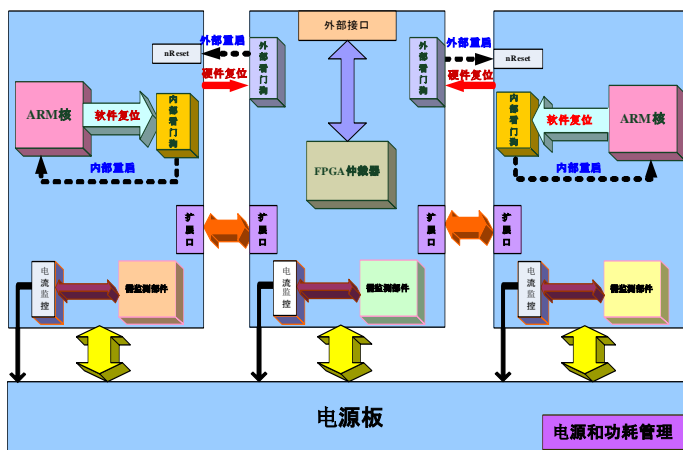


图 2 硬件平台体系结构图

#### ➤ 处理器（CPU）模块

CPU 模块是信息处理平台任务处理的核心，负责车载电子设备控制和数据通信等信息

的处理，此外系统软件也在 CPU 板中运行。为了提高整个系统的可靠性，对 CPU 拟采用系统级的双机容错设计方案，故设计中有两个相同的 CPU 模块。有关双机容错机制的方案可参见本文 2.2 节。系统所需的有线网口和用于外接 USB 无线网卡的 USB 接口设计在两块 CPU 板中。

➤ 接口模块（仲裁器模块）

主要完成两个功能：一是负责监控双机工作情况，并完成双机容错的仲裁器功能；二是负责向系统外部提供各种所需的设备接口，其中包括两个串口和一个 USB 接口。

➤ 电源模块

电源系统是一个相对独立的系统，负责供电和功耗管理，并对系统的其他部分进行实时检测。当其他系统发生异常时，嵌入式硬件平台可以检测到并对其进行重启，但当嵌入式硬件平台本身发生异常时，只能由电源系统对其进行重启。

### 2.1.2 软件平台结构及其功能

软件平台则包括应用软件和操作系统，软件通过数据结构、算法和通讯协议实现汽车电子控制策略，硬件则为软件提供了运行平台，执行具体控制。

如图 3 所示，嵌入式系统软件是整个嵌入式硬件系统上电启动后在操作系统上启动的系统程序，该系统程序与嵌入式硬件平台集成后，使整个系统成为完整意义上的信息处理平台，在此之上完成用户程序的启动和停止，使具有双机容错功能的平台能够完成全部工作（详见 2.2.2 节）。

嵌入式软件也是操作系统中用户程序与底层硬件之间的接口，它负责操作 CPU、FPGA 等硬件，并根据硬件的状态采取相应的措施，从而为系统中的用户程序提供底层的服务支持。

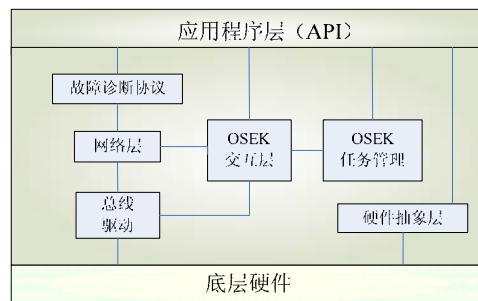


图 3 软件平台结构

## 2.2 可靠性设计

作为基于 COTS 的信息处理平台而言，可靠性和稳定性是影响整个嵌入式系统性能的关键因素。因此，针对恶劣的工作环境，容错技术是应用 COTS 器件的关键所在。本文对系统 COTS 器件的特点进行了可靠性加固设计

### 2.2.1 基于 FPGA 的多级容错机制

为适应工作环境提高系统的可靠性和稳定性，本文提出并实现了基于 FPGA 的多级容错机制：系统级基于 FPGA 的双机容错系统；模块级基于 FPGA 的 RAM 和 FLASH 的抗 SEU 容错；芯片级针对 FPGA 的抗 SEU 容错设计。通过该体系结构的多级容错机制提高整个系统的抗 SEU 能力。

➤ 系统级—基于 FPGA 的双机容错系统方案

本文提出的基于 FPGA 的双机容错机制（温备）<sup>[2]</sup>硬件设计结构如图 4 所示。看门狗监

控电路（WDT0 和 WDT1）和仲裁器（ARBITER）都是双机容错系统中的关键部分，分别负责对双机工作情况进行监控和通信控制等双机信号的仲裁。两个 CPU 通过中间的接口板（仲裁器）来实现基于温备的双机容错系统，以此实现系统级的冗余容错功能。同时，FPGA 系统（即接口板）还负责提供系统与外界通信的接口（即由 FPGA 仲裁后的接口）。

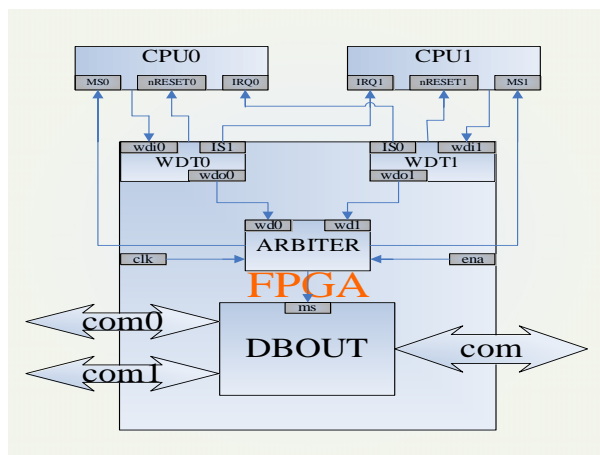


图 4 基于 FPGA 的双机容错设计结构图

在系统上电时，启动操作系统。随后在操作系统上加载嵌入式系统软件<sup>[3][4]</sup>，即 AT91RM9200（ARM 处理器）驱动程序和守护程序。如图 5 所示，守护程序启动后，根据仲裁器判断系统的主机标志（MS，Master Symbol），从而决定是否启动用户控制运行的用户程序。如果守护程序获得本机为主机的标志，则启动用户程序；反之，如果守护程序获得当前本机为备机的标志，则不启动用户程序。

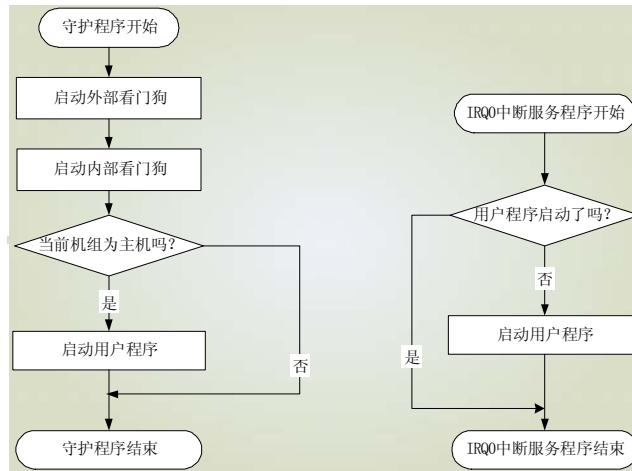


图 5 守护程序工作流程图

当机组正常工作时，守护程序通过 AT91RM9200 驱动程序向仲裁器模块上的外部 Watchdog 监控模块发送心跳信号，即信号 WDI。仲裁器模块上的外部 Watchdog 监控模块通过两台机组发送的心跳信号判断当前双机容错系统的工作状态。如果经过特定的时间后，仲裁器模块上的 Watchdog 模块没有收到机组发送的心跳信号，则将会向另一台机组发送中断请求信号 IS。如果另一台机组为备机，则备机上的守护程序随即启动用户程序，使故障机重启后进入备机状态。如果另一台机组为主机，则主机继续正常工作，故障机将会通过重启尝试故障的修复。

➤ 模块级—基于 FPGA 的 SDRAM 和 FLASH 的 TMR 容错技术

由于 RAM 和 FLASH 都是存储器，在恶劣环境中工作，存储单元易发生单位翻转效应，因此采取三模冗余（Triple Module Redundancy, TMR）技术来提高 RAM 和 FLASH 等存储器的可靠性。如图 6 所示，Flash 的 TMR 原理图（RAM 与此相同）。

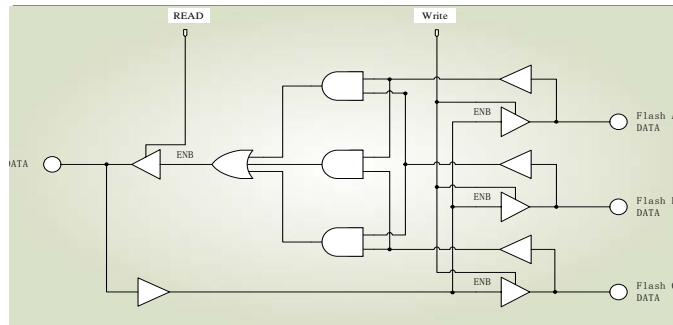


图 6 FLASH 的 TMR 原理图

➤ 芯片级—FPGA 的重配置容错设计

作为系统可靠性的瓶颈，FPGA 的容错设计是关键。设计原理如下：FPGA 内部对输入输出的 I/O 信号均使用在 FPGA 逻辑单元内部的三模冗余，以保证数据信号和控制信号在通过 FPGA 内部逻辑处理时，不受电子干扰等因素的影响（嵌入式系统的集成度高，易发生干扰）。如图 7 所示，为 FPGA 的容错设计原理图：

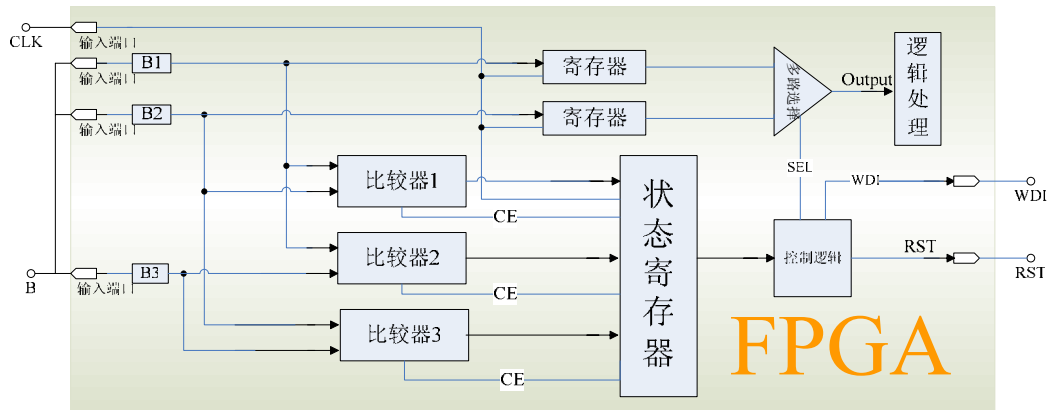


图 7 FPGA 的容错设计结构示意图

输入信号 B 经 FPGA 内部处理前先转存至 B1、B2、B3 三个 FPGA 的内部存储单元中；在信号 B1、B2、B3 经过 FPGA 逻辑处理之前都分别经过了比较器进行比较。如果发现比较结果不一致,那么某个信号所在的逻辑单元可能发生错误。状态寄存器保存比较器比较后的结果并由控制逻辑判断出错的存储单元,并由控制逻辑自动（通过图中的 CE 使能信号）屏蔽出错的存储单元发出来的数据。此时整个系统由一个三模冗余转化成一个双机比较,只有该对信号比较结果一致时可通过多路选择器输出至逻辑处理单元进行对数据的处理;否则假如其中又有一个存储单元受到影响而发生了错误,那么控制逻辑判断出错误,向外界发送一个 RST 中断信号,使配置芯片向 FPGA 进行全局重新配置,回到原来的三模冗余状态。如果三个比较器自身发生错误,那么比较后的输出有误,可以由控制逻辑判断纠正。如果控制逻辑发生了错误,那么只能发送 RST 信号,等待外部电路对之进行重新配置。其中状态寄存器中存放比较器的比较结果,从而可以由控制逻辑判断。为了保证控制逻辑的可靠性,可以通过设置看门狗的方法,对其进行检测。如果该控制逻辑遇到故障出错则看门狗计数器超时,发送超时信号给配置电路使其对 FPGA 重新配置。

2.2.2系统的过流监测保护电路设计

通常消除大电流的办法是当大电流发生时重启电源，即：监测大电流的过流监视器装置；自动断电和恢复的开关电路（即重启电源）。

如图 8 所示，本文设计的消除大电流电路工作原理如下：

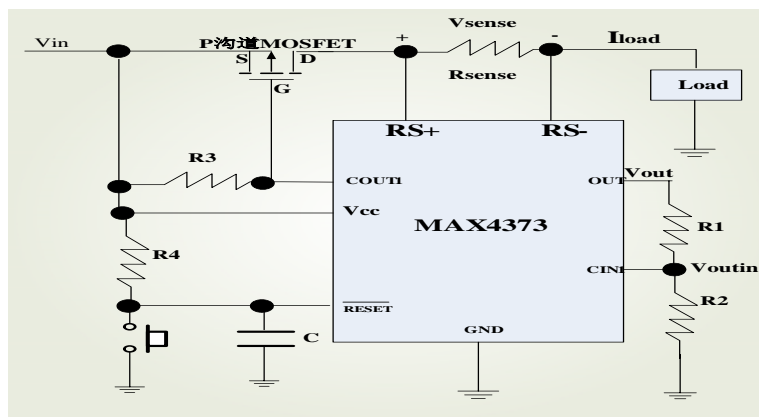


图 8 过流监测与保护电路原理图

若流入负载电路的电流未超过设定的阈值电压，则电流检测放大器输出的电压经分压后的  $V_{outin}$  小于极限值，内部电压比较器输出低电平（从  $COUT1$ ），于是 P 沟道 MOSFET 管导通，即负载的供电电路连通，正常工作；若流入负载电路的电流超过了设定的阈值电流，则由  $R_{sense}$  检测的电压经电流检测放大器放大后，使输出电压  $V_{out}$  经分压  $V_{outin}$  后大于极限值，内部电压比较器翻转， $COUT1$  输出高电平，使 P 沟道 MOSFET 管截止，于是负载的供电电路切断。内部电压比较器为输出锁存型，一旦翻转，则输出高电平锁存，电路保持断开状态，即负载断电；大电流消失后，内部电压比较器复位， $COUT1$  输出低电平，P 沟道 MOSFET 管导通，负载加电重新工作。

从图 2 中可以看到，本设计对每个模块中的关键芯片都有过流监控器，一旦监测到大电流的发生，由监控器发送出错信号至电源模块。电源模块立即对出现大电流的芯片进行断电重启的保护。

## 2.3 实现

如图 9 所示，为实现后的车载信息处理平台及其子板的实物图。该平台由 CPU 板（两块）、电源板和接口板四部分组成，并通过 PC104 总线接口连接在一起。

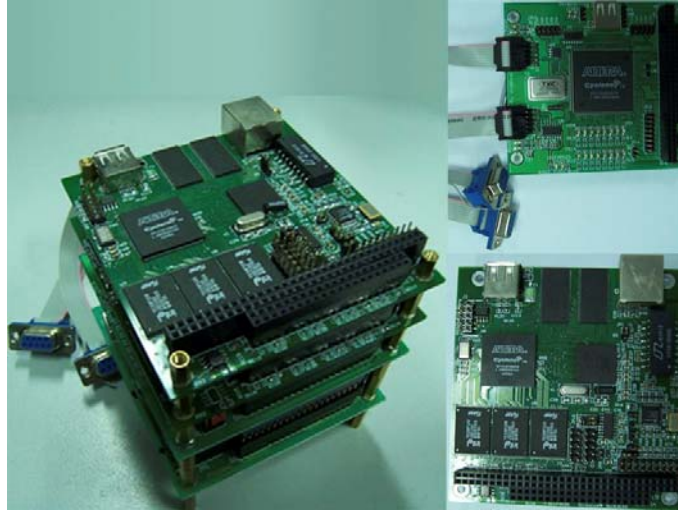


图 9 车载 COTS 信息处理平台原型实物图

➤ CPU 板

如图 9 右下角所示，CPU 板包括处理器 AT91RM9200、FPGA 芯片 EP1C4F400C8、存储器、总线等处理器资源，具有有线以太网口、USB 接口等外设接口；为了便于调试，还配备了调试串口。CPU 板在功能上，保留必须的外设接口。除此之外，为了提高 CPU 板的可靠性，对板上关键芯片设计大电流过流检测和保护电路，存储器的 TMR 冗余技术，CPU 的可靠性则是采取设计中的板级双机容错技术加以实现。

➤ 接口板

如图 9 右上角所示，接口板主要包括 Altera EP1C6Q240C8 的 FPGA 芯片、两个 RS232 串口和一个 USB2.0 接口为信息处理平台提供与外部设备连接的各种接口。为了与双机容错方案兼容，接口板需要对两块 CPU 板串口信号和 USB 信号的仲裁，因此，接口板中设计有 FPGA 芯片用于完成该功能。接口板为信息处理平台提供系统功能监控电路，Watchdog 监控模块在接口板中实现，与此配合的双机容错仲裁器功能在 FPGA 中实现。接口板是系统级容错功能的核心，是接口模块的实现，其硬件结构处于整个系统的咽喉部位，除了对接口板所需的电源提供过流检测和防护外，接口板还实现了 FPGA 的重配置容错功能，以防止接口板中 FPAG 芯片受到干扰而引起的错误。在串口信号的仲裁等实现上，TTL 电平的串口信号、USB 信号从两块 CPU 板直接输出，经过 PC104 接口引脚的电气连接，传送到接口板。

➤ 电源板

电源板为接口板和 CPU 板提供可靠稳定的电源，通过 PC104 总线接口分别向接口板和 CPU 板分别供电；电源板为整个硬件系统提供大电流检测和防护的功能，以减小或消除恶劣环境对嵌入式硬件系统产生的大电流效应；此外，各个子板中关键电路或芯片（如 FPGA）也设计有过流检测电路，这些检测电路与电源板上的检测电路一起成为该嵌入式平台的电源管理模块。结合工作特点，系统的电源管理和功耗管理在电源板中实现：通过控制各个子板的电源供应，可以根据实际使用情况分配功率。

➤ PC104 总线接口

PC104 总线接口仿照 ISA 接口定义，是应用于嵌入式领域的 ISA 总线标准，其独特的机械结构增强了嵌入式硬件的机械强度，为系统提供一个可靠稳定的工作平台<sup>[5]</sup>。接口板和 CPU 板的过流信号经过 PC104 接口传送到电源板。电源板对接口板和两块 CPU 板分别供电，各个子板所需的电源在 PC104 接口中的引脚各不相同，为电源管理和功耗管理提供了便利。

### 3 结果分析与讨论

本文最终实现了基于 COTS 的车载信息处理平台。如图 10 所示，利用 CPU 板的调试串口和终端显示，通过加载裁减后的 linux 操作系统、运行应用软件等测试证明该平台都工作正常符合设计要求。

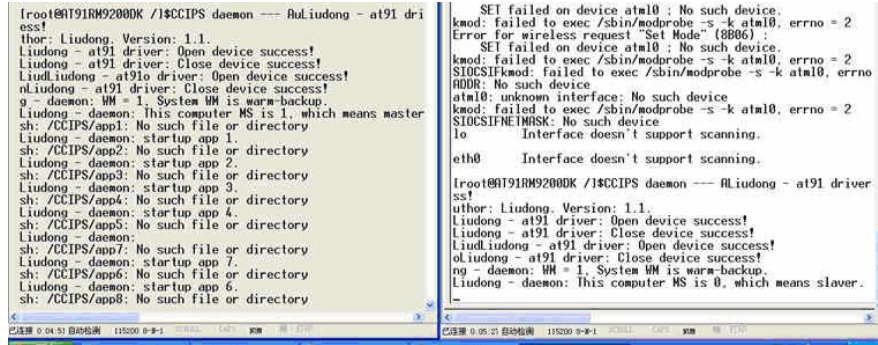


图 10 CPU 板（主备机）调试终端显示的工作状态

实验结果表明，系统采用 32 位的 AT91RM9200 处理器芯片，当主频为 180MHz 时，处理器能力达到 200MIPS；能够提供 32M SDRAM 和 16M FLASH 的存储空间；系统可外接两路 RS232 串口，并且能够外接多达 127 个设备的 USB 接口（通过 USB HUB），为系统提供了足够的设备扩展能力；除去接口电缆等外围插件，整个系统约重 450 克，体积约 1cm<sup>3</sup>；整个系统在正常工作时的功耗约为 3W 以内。因此，该系统具有显著的低功耗、低成本和体积小的优势。

由于车载信息处理平台的工作环境，本文通过对系统进行从芯片至板级的一系列旨在提高可靠性的加固设计来提高系统的可靠性。但由于实验条件限制，该平台未能在真实的车载环境中测试其抗辐射能力。因此，还需要通过故障注入技术模拟环境对系统可靠性指标检验后，才能应用在车载环境中。尽管如此，该车载信息处理平台已能够为车载电子设备的应用以及软件的设计和开发提供有效的调试和验证环境。

### 4 结语

综合成本、性能和体积等诸多因素的限制，基于 COTS 器件的车载信息处理平台在商业领域的应用将越来越广泛。由于 COTS 器件构建的系统运行在恶劣环境中，会影响系统的可靠性和稳定性。COTS 器件本身可靠性不高，只能通过可靠性加固技术增强其稳定性，消除影响，或尽快从影响中恢复。本文对可能引发的各种系统可靠性问题进行了分析和有效地处理：针对大电流，采用芯片和板级的两极过流监控和防护技术对系统进行保护和恢复；采用基于 FPGA 的多级容错机制提高整个系统的稳定性和可靠性。最后在此基础上实现了车载信息处理平台的设计方案。

由于试验环境和条件所限，该信息处理平台未能在真正的车载环境下进行测试，但各子系统都经过模拟验证测试，且双机系统温备份工作良好。在以后的工作中，将对整个系统进行可靠性量化分析并逐步完善，并对各种可靠性加固方法进行进一步的容错性能研究，使该平台最终能在实际的车载环境中正常工作。

## 参考文献

- [1] 何玮等. 汽车嵌入式 SoC 系统的应用与发展. 电子技术应用, 2005 (4)
- [2] 黄影等. 基于 FPGA 的双级容错系统设计与实现. 深圳大学学报, 2006 (2)
- [3] 金西等. 嵌入式 linux 技术及其应用. 计算机应用, 2007 (7)
- [4] 师明珠. 嵌入式应用系统软件设计技术研究. 计算机工程与应用, 2002 (7)
- [5] 易碧金. PC/104/嵌入式计算机在仪器中的应用前景分析. 石油仪器, 1999 (2)