[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/20 (2006.01)
G06F 13/40 (2006.01)
H04L 29/12 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810014221.9

[43] 公开日 2008 年 11 月 5 日

[11] 公开号 CN 101299228A

[22] 申请日 2008.1.26
[21] 申请号 200810014221.9
[71] 申请人 青岛大学
地址 266071 山东省青岛市宁夏路 308 号
[72] 发明人 邵峰晶 于忠清 王双宝 张 乐 刁克刚

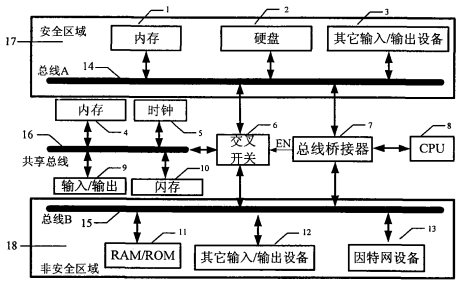
[74] 专利代理机构 青岛高晓专利事务所
代理人 于正河
权利要求书 2 页 说明书 7 页 附图 1 页

[54] 发明名称

一种基于单 CPU 双总线的安全网络终端

[57] 摘要

本发明涉及一种新型的基于单 CPU 双总线的安全网络终端，通过物理隔离和访问控制对已知或未知的网络入侵提供抵御功能，采用单一的 CPU 和两条物理上隔离的安全区域和非安全区域系统总线，由总线桥接器控制 CPU 和系统总线的动态连接，实现两条系统总线的物理隔离；涉及的因特网通讯设备仅连接到一条总线，涉及的安全数据存储设备连接到另一条系统总线上；使用一条共享总线用于共享键盘、鼠标等输入/输出设备与内外系统总线通信；本发明能有效防止网络入侵，保障信息安全，具有成本低廉，扩展功能强，安全可靠等优点。



1. 一种基于单 CPU 双总线的安全网络终端，其特征在于采用单一的 CPU 和两条物理上隔离的安全区域和非安全区域系统总线，由总线桥接器控制 CPU 和系统总线的动态连接，实现两条系统总线的物理隔离；因特网通讯设备连接到一条总线，安全数据存储设备连接到另一条系统总线上；一条共享总线用于共享键盘、鼠标或其他输入/输出设备与内外系统总线通信；两条独立系统总线分别服务于本地与网络访问操作，因特网设备用一条分离的系统总线与网络终端中的其它部分分离，在网络终端中，除了因特网之外的组件属于同一条非安全区域总线，因特网接口属于另一分离的安全区域总线；两条系统总线间的数据交换通过总线桥接器控制的共享总线完成,由计算机操作者或者操作系统发出控制命令；存储设备中的数据仅能被计算机用户存取，使用户数据与外部网络分离，入侵者通过外部网络非法进入，用户数据也不能被获取。

2. 根据权利要求 1 所述的基于单 CPU 双总线的安全网络终端，其特征在于由总线桥接器控制 CPU 在同一时刻仅能连接到一条总线，形成两条总线的物理隔离，保护连接到非安全区域总线的用户数据；非安全区域总线和安全区域总线之间的通信或者共享设备通过共享总线实现，由总线桥接器控制共享总线在同一时刻仅和一条系统总线相连；连接于共享总线的设备包括键盘、鼠标、显示器、内存和闪存。

3. 根据权利要求 1 所述的基于单 CPU 双总线的安全网络终端，其特征在于以安全区域总线为主体的安全区域由内存、硬盘和输入/输出设备电连通组合构成；以非安全区域总线为主体的非安全区域由内存、因特网设备和输入/输出设备电连通组合构成；以共享总线为主体构成的中间电信连接体系由内存、时钟、交叉开关、总线桥接器、

CPU、闪存和输入/输出设备电连通组合而成。

4. 根据权利要求 1 所述的基于单 CPU 双总线的安全网络终端，其特征在于总线桥接器位于 CPU8 和两条总线之间，根据切换总线命令切换 CPU 与总线的连接；产生 EN 信号给交叉开关，使共享设备连接到相应的系统总线；保证两条总线物理上完全隔离；保证访问程序在安全区域执行，使敏感数据存储在安全区域存储设备上。

一种基于单 CPU 双总线的安全网络终端

技术领域：

本发明涉及一种新型的基于单 CPU 双总线的安全网络终端，特别是一种通过物理隔离和访问控制可对已知或者未知的网络入侵提供抵御功能，提高因特网可靠性、稳定性和安全性的网络终端装置。

背景技术：

现有的计算机网络尤其是因特网具有开放性、互联性、连接方式的多样性及网络终端分布的不均匀性,网络通讯协议、操作系统本身的安全漏洞，再加上人为的疏忽，致使网络易受计算机病毒、黑客或恶意软件的侵害。存储在计算机中的敏感信息（例如密钥、信用卡、银行账户、网络账户、以及个人隐私信息等）容易在用户不知情的情况下被黑客或者恶意软件窃取。

传统的网络终端都是基于冯·诺伊曼体系结构或哈佛体系结构的，CPU、内存、输入/输出、外存和网络接口都被连接到一个单一的系统总线（包括控制总线，数据线和地址线，以下简称单总线）上。一旦来自任何网点的入侵者强行进入系统，它们可以获取对整个网络终端的控制权，对于这种模型，CPU 是一个集中的控制和运算单元。尽管现在多处理器计算机非常普遍，但是这些处理器只是通过软件组合，来完成一个或者一系列任务。换句话说，它们共用同一条系统总线，一旦入侵者从任何网点入侵系统，它们就可以接管整个系统。受限于该体系结构模型，网络终端经由网络尤其是因特网特别容易受到入侵。因此，存储在网络终端内的信息非常容易遭受到计算机黑客的攻击。近年来，网络安全问题已经成为研究热点，例如病毒扫描技术和防火墙技术、各类入侵检测技术、软硬件加密技术、网络终端设备中植入可信平台模块（Trusted Platform Module）安全芯片等。这些技术在一定程度上解决了信息窃取问题，但是当前的研究都是基于单总线的，其解决方案不能从根本上解决信息安全问题。

发明内容：

本发明的目的在于克服现有的单总线体系结构的终端技术存在的缺点，设计一种新型的基于单 CPU 双总线的安全网络终端，通过其物理隔离和访问控制功能，实现防入侵、保护信息安全的特性。

为实现上述目的，本发明采用单一的 CPU 和两条物理上隔离的安全区域和非安全区域系统总线，由总线桥接器控制 CPU 和系统总线的动态连接，实现两条系统总线的物理隔离；涉及的因特网通讯设备仅连接到一条总线，涉及的安全数据存储设备连接到另一条系统总线上；使用一条共享总线用于共享键盘、鼠标等输入/输出设备与内外系统总线通信；所述的基于单 CPU 双总线的安全网络终端体系结构的两条独立系统总线，分别服务于本地与网络访问操作；因特网设备用一条分离的系统总线与网络终端中的其它部分分离，在网络终端中，除了因特网之外的所有组件属于同一条系统总线（非安全区域总线）；因特网接口属于另一分离的系统总线（安全区域总线）；两条系统总线间的数据交换通过总线桥接器(BUS Bridge)控制的共享总线完成,由计算机操作者或者操作系统发出控制命令；存储设备中的数据仅能被计算机操作者（用户）存取，使用户数据与外部网络分离，入侵者通过外部网络非法进入，用户数据也不能被获取；由总线桥接器控制的 CPU 在同一时刻仅能连接到一条总线，形成两条总线的物理隔离，保护连接到非安全区域总线的用户数据；非安全区域总线和安全区域总线之间的通信或者共享设备通过共享总线实现，由总线桥接器控制共享总线在同一时刻仅和一条系统总线相连；连接于共享总线的设备包括键盘、鼠标、显示器、内存（RAM/ROM）和闪存（FLASH）等。

本发明的系统结构分为安全区域、非安全区域和中间电信连接体系三个部分，以安全区域总线 A 为主体的安全区域，由内存、硬盘和其他输入/输出设备电连通组合构成；以非安全区域总线 B 为主体的非安全区域由内存、因特网设备和其他输入/输出设备电连通组合构成；以共享总线为主体构成中间电信连接体系由内存、时钟、交叉

开关、总线桥接器、CPU、闪存和输入/输出设备电连通组合而成。

本发明与现有的网络终端相比，能够有效地防止网络入侵，保障信息安全，具有成本低廉，扩展功能强，安全可靠等优点，并可对已知或者未知的网络入侵提供强大的抵御能力，从根本上解决网络终端的信息安全问题。

附图说明：

图 1 本发明涉及的体系结构原理示意框图。

图 2 为本发明实施例之硬件组成结构原理示意框图。

具体实施方式：

下面通过实施例并结合附图做进一步描述。

实施例：

本实施例涉及一种新型的基于单 CPU 双总线安全网络终端的实现体系结构，是一个具有免入侵(intrusion-free)、信息和数据安全的安全网络终端。该体系结构包括：带有独立系统总线 A 和 B 的安全区域和非安全区域；因特网接口仅连接到非安全区域总线 15 上；总线桥接器 7（BUS Bridge）通过约定机制控制 CPU8 和两条总线 A 与 B 的连接；主要的（受保护的）存储器仅连接到安全区域的总线(总线 A)上；共享设备通过双端口电路和总线 A 或总线 B 连接，用于基本输入输出设备的共享以及内外通信等。

实现本实施例体系结构的单元部件包括内存 1、硬盘 2、其他输入/输出设备 3 和 12、时钟 5、交叉开关 6、总线桥接器 7、CPU8、输入/输出 9、闪存 10、RAM/ROM11、因特网设备 13、安全区域 17、安全区域总线 14（或总线 A）、共享总线 16、非安全区域 18、非安全区域总线 15（或总线 B）、CommonFlash19、外围设备 20、DMA 控制器 21 和 22、SDRAM 控制器 23 和 25、IDE 控制器 24、以太网接口 26、可扩展外围设备接口 27 和 28、串行配置设备 29 和扩展 Flash30。

本实施例的网络接口作为输入/输出设备加到系统总线上，并与其它硬件接口分离，既把网络和其它部分分隔开，又保证数据通过网

络传送；通常网络终端处于安全区域的状态中，在此执行所有的计算工作；根据网络的访问需求（如当需要数据传送时），通过总线桥接器 7 动态进行区域间的切换。在非安全区域中，所有通信数据通过总线桥接器 7 存储在共享总线 16 上的片内内存 1 上；总线桥接器 7 由网络终端操作者或 OS 管理。

本实施例涉及的网络终端系统包含 CPU、外存、网络接口（以太网或无线的）以及共享总线上的内存、闪存、显示器、键盘和鼠标等。因为非安全区域仅仅处理网络通讯，网络入侵者所能接触到的只是共享总线上相应设备中的数据，而不可能访问到主存储器（受保护的）上的数据。

本实施例涉及的总线桥接器 7 位于 CPU8 和两条总线 A 和 B 之间，其主要功能包括：一是切换 CPU 与总线(总线 A 或总线 B)的连接，由计算机操作者或者操作系统发出切换总线命令，切换时保证时序一致；二是产生 EN 信号给交叉开关，使共享设备连接到相应的系统总线(总线 A 或总线 B)；三是保证两条总线物理上完全隔离（切换前、后，非安全区域总线无法看到安全区域的设备）；四是保证访问 INTERNET 的程序在安全区域执行，使敏感数据存储在安全区域存储设备上。

本实施例涉及的交叉开关 6，由 EN 使能信号控制同一时刻仅能有和一条总线(总线 A 或总线 B)和共享设备连接，通过交叉开关即可在两条总线(总线 A 和总线 B)之间共享设备，又可以保证两条总线在物理上的隔离。总线桥接器根据当前网络终端所处的工作区域，向交叉开关提供 EN 使能信号。

本实施例采用单板实现方案，其中 CPU、部分内存、总线互连模块、外围设备控制器或者接口集成在单一芯片现场可编程逻辑阵列（FPGA）上,外设通过现场可编程逻辑阵列引脚连接到片上系统。其中核心部分就是实现包含一个处理器软核、内存、DMA 控制器及外围设备接口的片上系统。各个功能模块均以知识产权（IP）核的形式进行设计，最后进行系统集成。

本实施例的网络终端的硬件系统各部分描述如下：

（1）、 NiosII 处理器及 Avalon 总线。采用 Altera 公司提供的 NiosII 处理器软内核，NiosII 处理器软核几乎可以用在 Altera 所有的 FPGA 内部，和 Altera 提供的外设相同均用 HDL 语言编写，在 FPGA 内部利用通用的逻辑资源实现。将 NiosII 与 PLD 特有的灵活性和可定制性相结合，使得嵌入式系统的开发具有极大的灵活性。此外，NiosII 常被用于一些集成度较高，对成本敏感，以及功耗要求低的场合，特别适合本课题拟开发的网络终端需求。Avalon 总线模块由各类控制、数据和地址信号、地址译码以及数据通道多路复用和仲裁逻辑等组成，主要用于连接片内处理器和外设，以构成可编程片上系统（SOPC）。它描述了主从设备间的端口连接关系，以及设备间通信的时序关系。Altera 公司提供大量符合 Avalon 总线规范的 IP 核，可以和 NiosII 处理器通过 Avalon 总线模块无缝互联。另外，Altera 公司开发的 SOPC Builder 工具对 Avalon 总线模块开发提供强大的支持，系统用户不需要关心总线与外设的具体连接，大大简化了设计,降低系统开发成本。

（2）、顶层共享用 Avalon 总线模块。

该模块主要用于挂接 NiosII 处理器软核、片内指令内存、片内数据内存、总线桥接器、Common Flash 接口以及其它外围设备控制器。片内指令内存用于存储内外区域切换程序段，经调研发现基于现有的处理器结构以及操作系统设计，这种设计是必需的，如果内外区域分别存储区域切换程序，其实际执行流程将与我们期望的执行流程不同，从而无法实现区域切换功能；片内数据内存用于内外区域通信缓冲区；片内指令内存和片内数据内存可以利用 FPGA 芯片中内嵌的内存模块。Altera 的 CycloneII 芯片中内嵌如若干 M4K RAM（4 Kbit RAM）块，可以实现真正双端口、简单双端口和单端口的 RAM，并且支持移位寄存器和 ROM 方式，配置灵活。

本实施例的总线桥接器 7 作为一个从设备连接到共享用总线模块上，其主要功能如下：主设备（NiosII 处理器）通过总线桥接器从

端口写区域切换命令字，控制命令字分初始化（请求、完成）、通信（请求、完成）、切换工作区域三种模式；主设备（NiosII 处理器）通过总线桥接器从端口读状态字，状态字包括当前工作区域、区域切换模式。总线桥接器 7 作为一个桥接从设备连接到该总线模块上，主要是接收共享区域主设备发给安全区域 Avalon 总线模块或者非安全区域 Avalon 总线模块的地址、控制信号；发送安全区域 Avalon 总线模块或者非安全区域 Avalon 总线模块的数据信号、响应信号给共享区域主设备。

本实施例的总线桥接器 7 作为主设备分别连接到安全区域 Avalon 总线模块和非安全区域 Avalon 总线模块。任何时刻，总线桥接器 7 保证该模块的主设备仅能控制一个区域的从设备，即总线桥接器 7 的两个主端口任何时刻仅有一个输出控制命令、地址信号、数据信号以及接收数据信号、响应信号。闪存（Common Flash）接口 10 用于连接片外 Common Flash19，存放系统引导程序。其它外围设备控制器用于连接内外区域共享用外围设备，主要包括基本 I/O 设备、USB 设备、USB 主机等，在设计的各个阶段可以根据需要随时增删。

（3）、安全区域 Avalon 总线模块。

本实施例的安全区域总线模块主要用于挂接总线桥接器主端口、DMA 控制器、IDE 控制器、SDRAM 控制器以及扩展外围设备控制器。总线桥接器 7 主端口仅当用户切换到该区域时才将顶层共享用 Avalon 总线模块主设备信号输出到该总线模块以及接收该总线模块的数据信号和响应信号。IDE 控制器 24 用于连接片外硬盘 IDE 接口，连接的 IDE 硬盘用于存储用户本地数据，包括系统和应用程序数据、用户数据等。SDRAM 控制器 23 和 25 用于连接片外内存，作为安全区域工作时程序、数据存储空间。扩展外围设备接口 27 和 28 用于连接安全区域工作时需要的外围设备，可以根据需要随时增删，并预留接口和扩展插槽，供制版完成后扩展用。

（4）、非安全区域 Avalon 总线模块。

本实施例的非安全区域总线模块主要用于挂接总线桥接器主端

口、DMA 控制器、以太网接口、SDRAM 控制器以及扩展外围设备接口。总线桥接器主端口仅当用户切换到非安全区域时才将顶层共享用 Avalon 总线模块主设备信号输出到该总线模块以及接收该总线模块的数据信号和响应信号。以太网接口 26 连接片外以太网卡，用户在该区域可以通过太网卡与 Internet 连接。SDRAM 控制器 23 和 25 用于连接片外内存，作为非安全区域工作时程序、数据存储空间。扩展外围设备接口用于连接非安全区域工作时需要的外围设备，可以根据需要随时增删，并预留接口和扩展插槽，供制版完成后扩展用。

本实施例的实现时各元器部件均选用常规市售产品，经过计算机电信息连通原理组合构成完整的结构体系，实现本发明的目的，其实施例运行结果可以完全达到理想效果，有效实现完全功能。

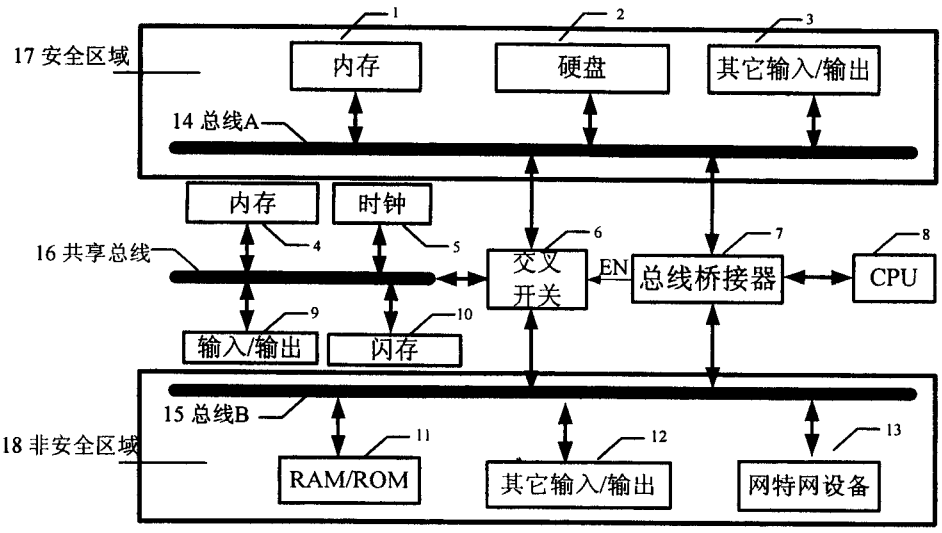

17 安全区域
内存
硬盘
其它输入/输出
14 总线A
内存
时钟
16 共享总线
交叉开关
EN
总线桥接器
CPU
输入/输出
闪存
15 总线B
18 非安全区域
RAM/ROM
其它输入/输出
网特网设备

图1

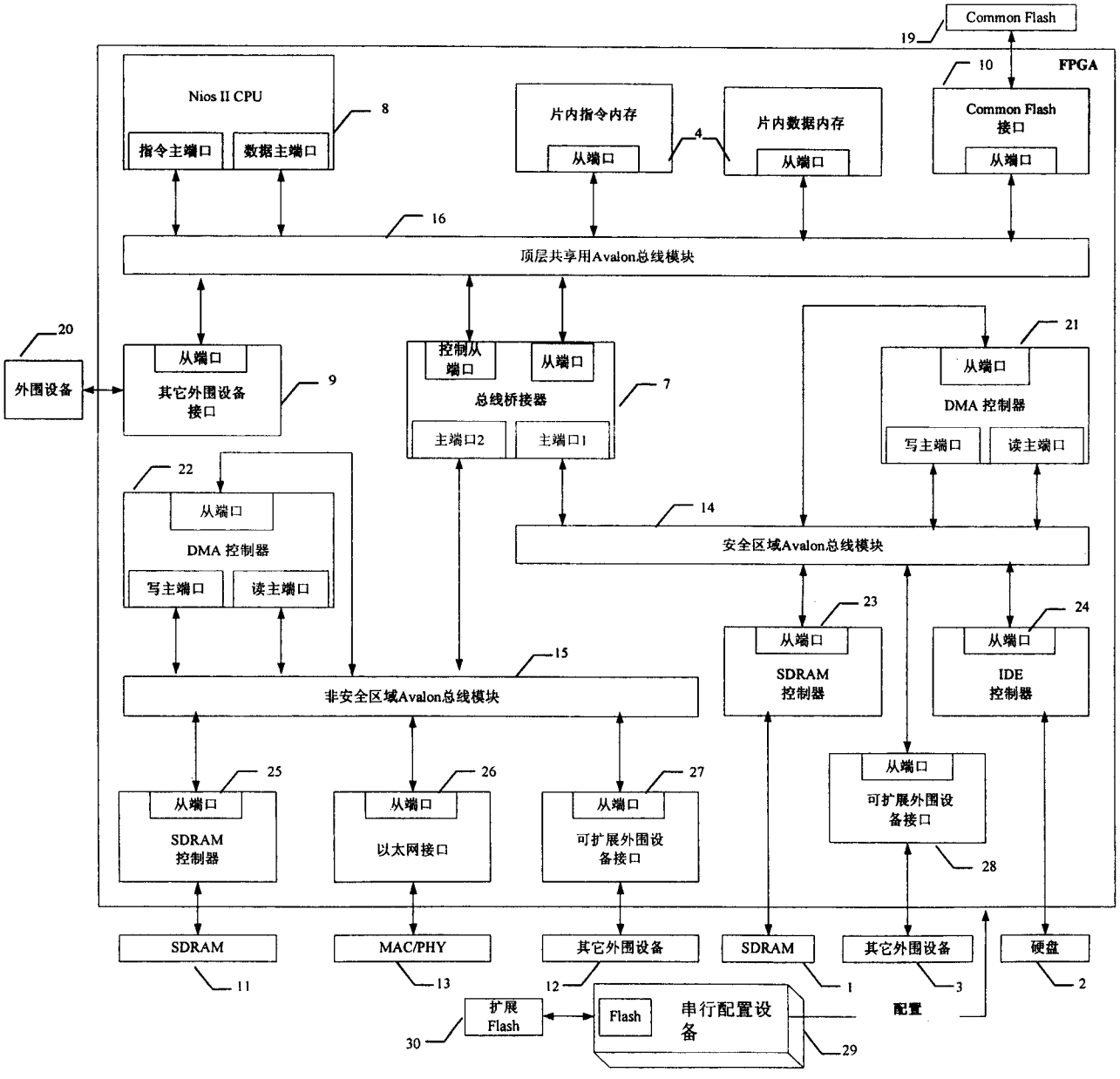

Common Flash
FPGA
Nios II CPU
指令主端口
数据主端口
片内指令内存
片内数据内存
Common Flash 接口
从端口
顶层共享用Avalon总线模块
外围设备
其它外围设备接口
控制从端口
总线桥接器
主端口2
主端口1
DMA 控制器
写主端口
读主端口
安全区域Avalon总线模块
非安全区域Avalon总线模块
SDRAM 控制器
IDE 控制器
以太网接口
可扩展外围设备接口
SDRAM
MAC/PHY
其它外围设备
硬盘
扩展 Flash
Flash
串行配置设备
配置

图2