(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103353931 B
(45)授权公告日 2017.10.24

(21)申请号 201310121238.5

(22)申请日 2013.02.08

(65)同一申请的已公布的文献号
申请公布号 CN 103353931 A

(43)申请公布日 2013.10.16

(30)优先权数据
13/396,582 2012.02.14 US

(73)专利权人 杰纳斯技术股份有限公司
地址 美国加利福尼亚

(72)发明人 王震华 S·帕斯金
L·罗则恩鲍伊姆

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 叶勇

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/80(2013.01)

审查员 唐剑

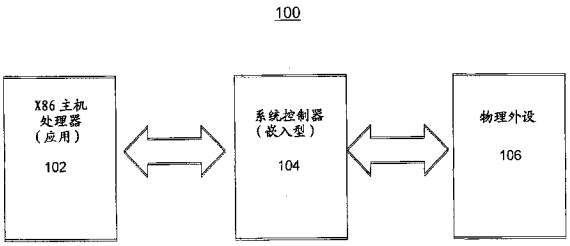
权利要求书2页 说明书12页 附图6页

(54)发明名称

安全增强型计算机系统和方法

(57)摘要

一种安全增强型计算机系统和方法。本发明总体提供被设计用来增强数据安全性的计算机体系结构。在实施例中，该体系结构包括两个子系统，其中每个都有自己的处理单元和存储器，以及规定的一组互连两个子系统和外界的接口。一个子系统被设计来提供用于运行计算机应用的惯用环境。另一个子系统被设计成提供在第一子系统和的用户之间的经由输入和输出装置的安全桥。



CN 103353931 B

1.一种计算机系统,包括:

第一硬件子系统,包括被配置用于运行应用的第一硬件处理器;

第二硬件子系统,包括被配置用于运行安全固件的第二独立硬件处理器;以及

连接到第二硬件子系统的外设,其中应用对连接的外设的访问由运行在第二硬件处理器上的安全固件选择性地阻止,该安全固件仿真第一硬件子系统上的对应外设连接,

其中外设包括视频显示器,该计算机系统进一步包括:

视频多路复用器,具有连接到第一硬件子系统的第一输入、连接到第二硬件子系统的第二输入以及连接到该视频显示器的输出,对来自第一输入和第二输入的内容进行选择以用于驱动输出,该选择由运行在第二硬件处理器上的安全固件控制。

2.根据权利要求1所述的计算机系统,其中外设进一步包括键盘,具有启动序列的安全固件,其中键盘和用于视频显示器的输出由第二硬件处理器专门控制,其中第一硬件处理器被阻止访问键盘和视频显示器。

3.根据权利要求1所述的计算机系统,其中外设包括磁盘驱动器,磁盘驱动器包含用于第一硬件子系统的操作系统和应用软件,该系统进一步包括:

由安全固件维护的仿真磁盘驱动器,其中第一硬件处理器对磁盘驱动器上的操作系统和应用软件的访问由该仿真磁盘驱动器控制。

4.根据权利要求3所述的计算机系统,其中安全固件保持该仿真磁盘驱动器的一个或多个特定时间的映像。

5.根据权利要求3所述的计算机系统,其中该磁盘驱动器包括固态磁盘驱动器。

6.根据权利要求3所述的计算机系统,其中安全固件加密磁盘驱动器上的全部数据,并且其中用于加密的密钥由安全固件专门保存。

7.根据权利要求1所述的计算机系统,其中外设包括网络连接,其中安全固件控制第一硬件子系统对外部网络的访问。

8.根据权利要求7所述的计算机系统,进一步包括由安全固件维护的VPN通道,VPN通道用于第一硬件子系统和外部网络之间的所有通信。

9.一种保护计算机系统安全的方法,包括:

配置计算机系统的第一硬件子系统,第一硬件子系统包括第一硬件处理器来运行应用;

配置计算机系统的第二硬件子系统,第二硬件子系统包括第二独立硬件处理器用于运行安全固件;

将外设连接到第二硬件子系统;和

利用运行在第二硬件处理器上的安全固件选择性地阻止应用对连接的外设的访问,该安全固件仿真第一硬件子系统的对应外设连接,

其中外设包括视频显示器,该方法进一步包括:

在计算机系统中提供视频多路复用器;

将视频多路复用器的第一输入连接到第一硬件子系统;

将视频多路复用器已连接的第二输入连接到第二硬件子系统;

将视频多路复用器的输出连接到视频显示器;以及

使用运行在第二硬件处理器上的安全固件控制对来自第一输入和第二输入的内容进

行的选择，以用于驱动输出。

10.根据权利要求9所述的方法，其中外设进一步包括键盘，该方法进一步包括：

由安全固件执行的启动序列，其中键盘和用于视频显示器的输出由第二硬件处理器专门控制，其中第一硬件处理器被阻止访问键盘和视频显示器。

11.根据权利要求9所述的方法，其中外设包括磁盘驱动器，磁盘驱动器包含用于第一硬件子系统的操作系统和应用软件，该方法进一步包括：

使用安全固件维护仿真磁盘驱动器，其中通过仿真磁盘驱动器控制第一硬件处理器对磁盘驱动器上的操作系统和应用软件的访问。

12.根据权利要求11所述的方法，进一步包括：

使用安全固件维护仿真磁盘驱动器的一个或多个特定时间的映像。

13.根据权利要求11所述的方法，其中磁盘驱动器包括固态磁盘驱动器。

14.根据权利要求11所述的方法，进一步包括：

使用安全固件加密磁盘驱动器上所有的数据；并且

通过安全固件专门地保存用于加密的密钥。

15.根据权利要求9所述的方法，其中外设包括网络连接，该方法进一步包括：

使用安全固件控制第一硬件子系统对外部网络的所有访问。

16.根据权利要求15所述的方法，进一步包括：

使用安全固件维护VPN通道，VPN通道用于第一硬件子系统和外部网络之间的所有通信。

安全增强型计算机系统和方法

技术领域

[0001] 本发明一般涉及到计算机、并特别涉及到在信息安全性非常重要的公司和政府组织使用的计算机。

背景技术

[0002] 传统上，个人的和公司的数据安全功能通过在实质上与依据消费者支付能力设计的消费级个人计算机一致的硬件体系结构上采用附加的软件模块的形式实现。有时也实现专用于安全的附加硬件模块，例如用于更安全地验证用户(例如智能卡、生物特征识别)。但即使在这些情况下，传统上大部分的安全功能还是通过附加软件组件实现，这些软件组件有时集成到操作系统中，但是通常都存在于内存中并就像任何其他软件应用一样执行。

[0003] 传统方法的一个重要问题在于当在软件中执行安全功能时，可能被多种不同方式损害。在操纵计算机的正常过程中，用户偶而添加或改变一些软件组件——添加和替换一些软件组件的能力给通用型计算机体系结构带来了在广泛而多样的任务和分配中的灵活性和可用性。改变或添加软件模块的同样会为攻击者损害计算机系统的安全带来机会。

[0004] 当引入新的软件组件时，存在这样的风险：它包括会招致攻击的功能，或者它包括可能被外部利用而易于攻击的程序设计错误。并且，因为安全软件与应用软件一样地分布和安装，因此它也具有同样易受攻击的风险。

[0005] 在传统的通用计算机中，整个随机访问存储器(RAM)组成单个大的统一存储体，可由处理器物理访问，或如果该系统包含多个处理器的话，则可由全部的处理器访问。存储器访问的统一为计算机关键性资源之一的RAM的使用提供了最大的灵活性，并且使得操作系统和应用软件对RAM的利用达到最优。尽管经济效益显著，但是统一的RAM体系结构也意味着并发运行的程序可以访问彼此的存储器区域或者由操作系统或其组件占用的存储器。因此，统一的RAM体系结构的这个特征已经成为最常利用来损害计算机安全的途径。

[0006] 现代计算机系统还使用一种叫做“虚拟存储”的机制，其中嵌入到处理器中、被称作存储器管理单元(“MMU”)的硬件细件执行存储地址转换的功能。增加虚拟存储允许RAM分割成段，每个段分配给某一软件组件或一组软件组件。并且虚拟存储还阻止了对属于不同的软件组件或操作系统的存储器的偶然访问。虚拟存储机制已经被证明对阻止错误的软件行为影响系统总体上的稳定性来说非常有效，但是它不能用于阻止恶意的破坏，并且在每个操作系统中存在文件机制来绕过由用于诊断目的的MMU提供的保护。这些机制经常被利用来损害计算机的安全及其包含的数据。

[0007] 在一种实现提升安全水平的常规方法中，安全机制的一些部分由独立的和专用的硬件模块实现，硬件模块设计有附加的抗干扰部件，从而为可能的入侵者增加了难度。或许硬件增强型计算机安全部件的最早一个非机密范例为IBM的HSM(硬件安全模块)，其是小型单机计算机，带有它自己的存储器和存储子系统，存储子系统被嵌入到坚固的外壳中，这种外壳设计成类似于办公室保险箱。银行卡的个人识别号保存在HSM中，使得即使银行雇员也不能访问这些明码形式的代码。当自动柜员机需要验证持卡者的身份时，密码的询问-应答

序列启动，使得PIN决不会在通信链路上被逐字传输，并且HSM安全地执行验证程序。

[0008] 全球标准移动电话系统(基于GSM)的智能卡方式用户验证机制有一类似的机制，不同在于该硬件安全模块小型化到指甲的大小，并且各用户都配备有这样的器件。SIM卡结构让其难以在不毁坏嵌入的存储芯片的情况下被拆解。

[0009] 另一个常规方法是可信平台模块，其嵌入到一些目前制造的个人计算机。TPM有点类似于SIM卡，这是由于它为具有受限访问性的小型存储芯片，并且包含一些安全相关的识别信息和一些加密密钥。TPM的关键性概念在于阻止攻击者改变该识别信息来错误地识别计算机或它的用户、从而绕过安全机制而到达该系统中的其他地方。然而它的缺点是包含在TPM中的密钥和号码仅为该保护的一部分，而其余的部分按照传统在操作系统和应用软件组件中实现。因此该TPM提供了附加的保护层，使得非验证用户不可能改变一些密钥相关的信息令牌。然而，TPM在系统软件的其他部分及其通信中存在显著的弱点，而这会被利用来进行成功的攻击。

[0010] 因此，存在改进用于计算机系统安全的方法的需要。

发明内容

[0011] 本发明涉及一种被设计用于增强数据安全性的计算机体系结构。在实施例中，该体系结构包括两个子系统，其中每个都有自己的处理器和存储器，一组被明确定义的互连两个子系统和外界的接口。

[0012] 根据某些方面，两个子系统中的一个根据流行的处理器体系结构构建，比如今天大多数个人计算机采用的x86，并且被指定为应用处理器子系统。选择这个处理器体系结构是因为它可适用种类繁多的应用软件和操作系统，这样的目的在于使用户在安装他们选择的应用软件方面具有最大灵活性。不同于也是按照x86体系结构设计的传统个人计算机，该应用处理器所有的外设连接都通向另一个子系统而不是实际的外置或内置外设。因此，虽然软件可以在该x86上几乎无限制地运行，但是从外部访问该软件及其数据被专用系统处理器子系统严格控制，其强制执行维护这些应用和它们的数据安全所必需的保护。

[0013] 根据某些附加的方面，被指定为系统处理器的另一个子系统实质上是一种嵌入式系统。它运行随处理器提供的嵌入式软件系统，并且在任何情况下都不能被计算机的终端用户所改变，并且嵌入式软件系统可以被所谓的固件取代。作为嵌入式系统，系统处理器模块的具体处理器体系结构不关紧要，但是最终用户和任何第三方开发者都不能被允许写入或改变它的任何软件组件。系统处理器实质上充当运行在它自己的硬件子系统上的固有不安全的应用软件环境和外界之间的“桥”。在实施例中，系统处理器对于每种外设连接具有两个端口，一个连接到实际的外设并且另一个连接到应用处理器子系统。固件连同系统处理器硬件一起为应用处理器子系统仿真每种外设，同时强制执行一组适用于每种可支持类型外设的规则和机制，并且必须一直对应用软件及其数据保持最高的防护标准。所有内置和外置外设都连接到系统处理器并通过外设仿真固件功能使用。

[0014] 根据这些及其他方面，一种根据本发明实施例的计算机系统包括第一子系统，第一子系统包括用来运行应用的第一处理器；第二子系统，包括被配置用于运行安全固件的第二独立处理器；以及连接到第二子系统的外设，其中应用对外设的访问由运行在第二处理器上的安全固件控制，安全固件仿真第一子系统上的对应外设连接。

[0015] 进一步根据这些及其他方面，一种根据本发明实施例的保护计算机系统安全的方法包括配置计算机系统的第一子系统，第一子系统包括第一处理器来运行应用；配置计算机系统的第二子系统，第二子系统包括第二独立处理器来运行安全固件；连接外设到第二子系统；利用运行在第二处理器上的安全固件控制应用对外设的访问，安全固件仿真第一子系统上的对应外设连接。

[0016] 作为这些及其他方面的进一步补充，一种根据本发明实施例的系统包括单机计算机系统，所述计算机系统包括：第一子系统，包括被配置用于运行应用的第一处理器，以及第二子系统，包括被配置用于运行安全固件的第二独立处理器；以及由机构托管的安全内部网，该机构控制该单机计算机系统，其中应用对安全内部网的访问由运行在第二处理器上的安全固件控制，安全固件仿真第一子系统的相应物理网络连接。

附图说明

[0017] 通过阅读下面对本发明具体实施例的描述并结合附图，本发明的这些及其他的方面和特征对于本领域技术人员来说将变得明显，其中：

[0018] 图1是顶层示意图，示出了一种根据本发明实施例的安全计算机体系结构；

[0019] 图2是根据本发明原则的计算机系统的功能方框图；

[0020] 图3是一示意图，示出根据本发明实施例的保护计算机系统的显示和启动功能安全的范例方面；

[0021] 图4是一示意图，示出根据本发明的实施例的保护计算机系统的网络连接功能安全的范例方面；

[0022] 图5是一示意图，示出根据本发明实施例的保护计算机系统的应用访问外设安全的范例方面；以及

[0023] 图6是一流程图，示出根据本发明实施例的保护计算机系统安全的范例流程。

具体实施方式

[0024] 本发明现在将参考附图进行详细描述，附图作为本发明的说明性范例提供，以使本领域技术人员能实现本发明。值得注意的是，附图和下面的范例并不意味着将本发明的范围限制到单个实施例，反而通过对一些或所有描述的元素进行互换也可能获得其他实施例。此外，在本发明的可以部分或完全利用现有组件实现的某些要素中，将仅描述对于理解本发明来说所必需的那部分现有组件，并且将省略对其他部分现有组件的详细说明以免使本发明过于晦涩。被描述为以软件形式实现的实施例并不局限于此，而可以包括以硬件形式实现的实施例，或者软件和硬件组合来实现，并且反之亦然，这对本领域技术人员来说是显而易见的，除非在文中另作说明。在本说明书中，示出为单个组件的实施例不应被视为限制；相反，本发明意图包含其他包括多个相同组件的实施例，并且反之亦然，除非在文中明确地陈述。此外，申请人并不意图在说明书和权利要求中将任何术语赋予生僻的或特殊的意义，除非对此有明确的阐述。更进一步的，本发明包含在这里作为例示参考的现有组件的现在和将来的等效组件。

[0025] 通常，本发明提供用来增强数据安全性的计算机体系结构。在实施例中，该体系结构包括两个子系统，其中每个都有自己的处理单元和存储器，以及规定的一组互连两个子

系统和外界的接口。一个子系统被设计来提供用于运行计算机应用的惯用环境。另一个子系统被设计成通过输入输出装置提供在第一子系统和用户之间的安全桥。

[0026] 图1是一方框图，示出根据本发明一些方面的范例系统体系结构100。

[0027] 如图1所示，两个子系统中的一个优选为根据流行的微处理器体系结构构建，比如今天大多数个人计算机采用的x86，并且其被指定为应用处理器子系统102。选择这个体系结构是因为它可适用种类繁多的应用软件和操作系统，这样的目的在于使用户在安装他们选择的应用软件方面具有最大灵活性。不同于传统的按照x86体系结构设计的个人计算机，该应用处理器所有的外设连接都通向另一个子系统而不是实际的外置或内置外设。所以虽然软件可以在该x86上几乎无限制地运行，但是从外部访问这个软件或其数据被专用系统处理器子系统严格控制，其强制执行维护这些应用和它们的数据安全所必需的保护。

[0028] 该另一个子系统，系统处理器104，优选为嵌入式系统。因而，它运行随该处理器一起提供的指定软件系统，嵌入式软件系统在任何情况下都不会被计算机的最终用户所改变，并且实际上应当被称为固件。作为嵌入式系统，系统处理器模块的具体处理器体系结构并不重要，但是最终用户和任何第三方开发者都不能被允许写入或改变它的任何软件组件。系统处理器104实质上充当运行在它自己的硬件子系统102上的固有不安全的应用软件环境和外界之间的“桥”。

[0029] 外设106典型地包括任一类型的、提供系统100的功能和计算机用户之间的接口的设备。这样的设备可以包括输出装置，比如显示器、扬声器、打印机等，以及输入装置，比如键盘、鼠标、触控板、触摸屏等。外设106的数量和种类可以取决于包容应用处理器102和104的设备的特定形式因素。例如，在本发明的实施例中，其形式因素为传统的台式计算机，外设106可以包括显示器、键盘和鼠标，这些为外置配属。当形式因素为传统的笔记本计算机时，外设106可以包括集成显示器、键盘及触控板。当形式因素为平板计算机或智能电话时，外设106可以包括集成显示器/触摸屏。应当注意到在形式因素类型不同的系统100之间，外设106并不必然互不相容，也并非永远不变。例如，许多传统的触控板计算机系统可能被可选的独立键盘和鼠标操纵(例如通过USB或蓝牙连接)。同样地，许多传统的台式计算机系统可能通过可选的触摸屏或语音控制装置操纵。

[0030] 在一些实施例中，系统100被设计成看起来像普通计算机系统那样，同时其中嵌入有系统处理器102的附加安全组件，而这不容易被外行的观察者看到。例如，系统100可以看起来像普通的膝上型计算机，其带有传统的折叠显示器和嵌入式键盘、扬声器以及指点设备。在其他可能的实施例中，系统处理器102和应用处理器104被分开容纳或者容纳在一起，或者更进一步的与某些外设106分开。然而，应当注意到基于附加的安全方面的考虑，处理器子系统102和104优选地尽可能集成，位于同一个壳体内并且甚至位于同一个电路板上，或许甚至两个独立处理器核芯位于同一个ASIC、SOC或FPGA上。例如，本发明的发明人认识到位于这些子系统之间的任一类型的暴露互连都可能被攻击者利用。因此，优选地将这样的互连做成尽可能难以接近(例如位于同一个集成电路和/或电路板内部)。至于连接到系统处理器104的外设106，它们可以根据系统100的特定形式因素，或为集成或为独立。

[0031] 应当注意到，不是任一给定系统100中的所有外设都必须由系统处理器104控制其访问。然而，典型地，至少系统100最常用的或最重要的外设100都被控制，例如全部的输入设备比如键盘和鼠标，以及最常用的输出设备比如显示器。在这点上，本发明的发明人认识

到这样的外设典型地包括那些输入/输出装置，应用处理器102的特定执行通过它们能与人类操作员或其他的计算机接口（例如经由网络或其他的通信链路）来控制或访问它的运行和/或数据。因而，所有实质上将应用处理器102的数据和运行暴露到外界的外设106优选通过系统处理器104路由。因此，术语“外设”应该看作是既包括实际的外围设备又包括将处理器连接到外围设备的连接（例如端口）。系统处理器104因此优选在这些通信中最安全的物理点截取外设106和处理器102之间的通信。换句话说，应用处理器102不会有任何重要的外设直接连接到或者通过暴露的或外部可访问的连接而连接到它或者它的运行环境；相反，这些连接通过系统处理器104路由或被系统处理器104控制。

[0032] 此外应该注意到，或许取决于类型，外设106可以位于通常容纳应用处理器102和系统处理器104的装置之内或之外。在下面将更详细描述系统100的一个最优实施例为形式因素是台式计算机或笔记本计算机的设备，但是这不应当被认为是限制性的。在这样的实施例中，外设106包括附加的显示器、键盘和指示设备（例如触控板和/或摇杆鼠标），以及内置的扬声器和无线调制解调器（例如802.11a/b/g/n）。在这样的实施例中，外设106可以更进一步包括任一经由系统100上对应的插孔连接的输入/输出外部设备，包括传统的插孔或接口，例如USB，RJ-45，Firewire，eSATA，VGA，HDMI，DVI，DisplayPort和MiniDisplayPort。在经过本发明范例的教导之后，本领域技术人员将认识到如何以较少的或附加类型的接口和/或外设106实现本发明。

[0033] 系统处理器104典型地对于每种外设连接具有两个连接，一个连接到实际的外设106并且另一个连接到应用处理器子系统102。如下面将要更详细地描述到的，随系统处理器104的硬件提供的固件对每种用于应用处理器子系统102而事实上连接到系统处理器104的外设106进行仿真。固件进一步优选执行一组规则和机制，它们适合于每一种支持的外设，并且必须一直为应用软件及其数据维持最高级别的防护。在实施例中，所有内置和外置外设106连接到系统处理器104并通过外设仿真固件功能而使用。

[0034] 虽然没有在图1中详细示出，但是应当注意到应用处理器102和系统控制器104可以进一步包括存储器、内存和I/O寻址空间、操作系统软件、应用软件、图形处理器、声音处理器和处理器总线。例如，在系统100的形式因素为台式计算机或笔记本计算机时，系统100可以包括传统的个人计算机组件、比如PCI总线、RAM和ROM存储器，ROM存储器存储有例如为Windows7的操作系统以及关联的BIOS软件和例如Windows Office的应用软件。系统100可以进一步包括这样的传统个人计算机组件，比如XGA图形处理器（例如英特尔的x86、AMD的集成显卡或例如由nVidia提供的那些外部处理器），a5.1音频处理器、USB输入和输出、以太网接口、串联/并行接口等。在某种程度上，通过系统处理器104控制这些组件和这些组件与应用处理器102的互操作是本发明的一方面，在下面将提供这些细节。然而，为了使本发明清楚起见，将省略应用处理器102进一步的附加实施细节。此外，在经过这些范例的教导之后，本领域技术人员将领会处理器102用于其他类型形式因素、例如平板计算机和智能电话的多种可替换实施例。

[0035] 现在将从它仿真和支持的外设类型以及各种用于支持系统级运行逻辑和安全的辅助功能方面的范例来描述系统处理器子系统104的范例实施例。

[0036] 在比如结合图2示出的范例实施例中，系统100、系统处理器204耦合到应用处理器202，同时耦合到键盘206、视频多路复用器208和固件214。应用处理器202可以相当于如上

所述的应用处理器102。系统处理器204可以由任何传统的、专有的或将来的处理器实现，比如x86处理器、定制的ASIC或SOC、ARM处理器等。固件214优选在ROM(例如闪存)中实现，ROM属于系统处理器204，并包括控制系统处理器204和实现其如这里和下面描述的功能所需的所有操作系统和应用软件。本领域技术人员将认识到包括固件214的软件的语言和构架可以取决于用来实现处理器204的处理器类型和/或使用的操作系统。经过以上描述的教导，本领域技术人员将更进一步懂得如何实现执行处理器204功能的软件和固件，它们或许与传统的操作系统和应用一起实现。应该进一步注意到系统处理器204可以包括没有示出的附加功能和/或组件，比如处理器总线、RAM/应用存储器、图形处理器功能、输入/输出端口等。

[0037] 如所示，视频多路复用器208包括至少两个输入216、218以及一个输出220。视频多路复用器的输出220连接到计算机显示器210。视频多路复用器208的一个输入218连接到内置于系统处理器子系统204的视频图形模块，其用来传递与操作和安全有关的信息并与最终用户互动，且用于嵌入在系统处理器204固件中的任何应用。视频多路复用器208的另一个输入216连接到应用处理器子系统202的视频图形模块的的输出，使得应用产生的图形传送到多路复用器208，并且在系统处理器204和控制信号222的控制下，通过多路复用器有条件地传递到显示监视器210。在实施例中，多路复用器208测量视频输入的分辨率并调节其帧频，使得它们合乎显示监视器210期望的显示模式、实际分辨率和帧频。取决于由系统处理器204确定的系统的运行和安全模式，应用图形输出216可能被完全阻止显示出来、作为小窗口显示，或者直接达到显示监视器210的实际大小。系统处理器204的图形218本身还可以有条件地以各种依赖于操作系统运行和安全模式的方法通到监控器210。

[0038] 在实施例中，在初始的系统启动和验证期间，处于系统处理器204以信号222控制下的视频多路复用器208，使得整个显示器210被用于系统处理器204的图形。系统处理器204更进一步控制键盘206(以及或许有的其他输入装置，比如触控板等)，并且该互动需要正确地验证该用户，并通过显示器210将这个过程的改进和结果通知他。在实施例中，即使操作系统和应用软件也许之前已经在应用处理器202上被激活，应用处理器202的视频输出也不允许被看到直到该验证已经成功。一旦验证已经成功地完成且系统处理器204声明了正常的运行模式，那么它将通过信号222使视频多路复用器208允许来自输入216的应用图形占据整个屏幕。

[0039] 在实施例中，在成功验证之后，系统处理器204的图形将不会经常可见，除了当需要传送系统级信息、或者需要与系统处理器204相互作用而特定的密钥组合已经被按下时。在这样的时刻，视频多路复用器208可以使得系统处理器204的图形覆盖在应用图形的上方而显示。在特殊条件下，例如当用户已经被验证但是应用处理器202被激活或重新启动时，或者当嵌入系统处理器204固件中的应用运行时，视频多路复用器208可以使得应用图形视频216在屏幕210上以小视窗显示，因此用户可以监控它的进程并同时与系统处理器204互动。

[0040] 多路复用器208被来自系统处理器204的信号222控制。它可以使用任何传统的、专有的或将来的技术以混合来自多个信源的视频和图形，比如色度键、覆盖、视窗等。因而，208的实现细节取决于使用的特定多路复用技术，并且为了使本发明清楚起见，在这里将省略它进一步的细节。在实施例中，当应用处理器202包括标准的XGA图形控制器时，标准XGA

接口用来实现接口216。应该更进一步注意到多路复用器208可以使用共同待决美国申请13/241073描述的附加视频安全功能，其内容通过引用的方式整体结合到本申请。

[0041] 验证可以包括任何传统的、专有的或将来的技术，并且本领域技术人员将认识到许多可能的替换。在一个非限制性范例中，系统处理器204可以提示用户输入/提供凭证，比如用户名、口令、安全密钥、生物识别特征(例如指纹)。这些凭证可以与存储的凭证相比较，或者系统处理器204可以将它们发送到远距离的验证服务器来比较。更进一步，本地存储的凭证可以有时间限制并在需要时从一外部信源刷新或撤消。

[0042] 类似于通过多路复用器208将应用处理器的图形提供216给显示器210，系统处理器204阻止处理器202访问键盘206及其他外设，直到验证成功。如下面将更详细阐述的那样，在成功验证以后，处理器204允许通过处理器202经总线224仿真访问键盘206及其他外设，这由固件214提供的仿真功能控制。

[0043] 现在将描述根据本发明的方面的保护计算机系统100的数据网络功能安全的范例方法。在实施例中，系统100为一公司购买的、由特定雇员使用的单机计算机。如图3所示，在这些及其他的实施例中，该公司优选更进一步拥有/保持有与公众访问数据网络322(例如因特网)互连的专用通信网320(例如为内部网)。优选地，专用通信网320为了安全和为避免受到所有相关威胁而进行充分保护，该保护可以通过如防火墙这样的传统设备，侵入检测及其他法律和体系结构层面的保护机制。因此本发明这样的实施例的一方面就是利用了现有的保护措施并且受益于对它们的集中定制和管理。

[0044] 在比如图3示出的实施例中，系统处理器子系统204上存在至少两个物理网络接口。这些网络接口中的一个，典型地为十亿比特以太网端口304，以“背靠背”结构连接到应用处理器子系统202上的类似端口302，并且这是访问应用处理器202的仅有的物理网络连接。所以，来自处理器202上应用的全部通信量将被系统处理器204截取，并且任何发送给该应用的数据包必须首先通过该系统处理器204。

[0045] 位于系统处理器204上的一个或多个物理网络接口306中的另一个典型地为另一个十亿比特以太网。其他类型可以包括无线网络接口模块，比如Wi-Fi。这些接口中的一个或两个可以连接到可利用的物理网络，网络可以被自动地检测。系统处理器的网络管理功能330(优选由固件214实现)然后确定被检测的网络是否可以被识别和验证。例如，网络管理功能330可以验证被检测的网络是否为购买该计算机的指定公司的内部网320。例如，网络管理功能330可以存储公司内使用的地址范围并可以将被检测网络的地址与该范围进行比较。网络管理功能330可以更进一步尝试连接到列出的已知服务器中的一个，从该服务器取回密码证书并依靠本地存储的证书数据库验证该证书。如果验证通过，则直接连接的网络被认为是安全的，然后系统处理器204在第一网络接口302/304和激活的外部接口306之间转发所有的数据包。

[0046] 如果验证进程没有成功，或者在某些情况下当期望提高保护水平使得该进程被完全绕过时，该可用网络被认为是不安全的，并且将在位于系统处理器204上的VPN客户端332(优选由固件214实现)和位于公司内网320上的指定VPN网关310上的VPN服务器334建立虚拟专用网络(“VPN”)连接，(a.k.a.VPN通道308)。一旦VPN通道308建立，则连接到应用服务器202的第一接口304往来的所有通信量将独占地通过VPN通道308，使得应用和它的操作系统在计算机连接到任何其他公司或专用网络308，同时被使用它的雇员经常移动时，仍然表

现得像计算机本地连接到公司安全网络320(例如内部网)一样。优选实施例使用基于IP协议312/314的以太网(其中EoIP312优选在固件214中实现)来在VPN通道308上通过VPN客户端332压缩来往应用处理器202的原始以太网通信量。在服务器334端,VPN网关310,在解码和验证这些数据包后,将它们发送到公司内网320,。本领域技术人员应该理解VPN通道308提供用于将传输的数据包加密并利用加密签名来验证这些数据包的可靠性。因此当包含保密信息的数据包在运行于计算机内的应用处理器202上的应用软件和公司数据服务器之间交换时,这样的数据被保护来免于在公共访问网络322的链路上传输时遭到窃听和在途数据篡改。

[0047] 在实施例中,嵌入到系统处理器204的固件214中的应用访问同一个VPN通道308,也能直接访问本地可用网络322。所以如果嵌入型应用需要传输任何敏感信息时,它应该通过VPN隧道308进行其业务。然而,在某些范例嵌入型应用中,例如视频会议代理,控制器204可以允许用户选择通过VPN通道308安全连接到公司网络,并且从那儿经由另一个VPN通道尽可能的前进,而且在指示器上显示该连接是安全的。附加地或可替换地,当(例如,由于性能的原因)该安全连接不符合期望时,控制器204可以允许该用户通过直接访问本地的可用网络322来建立视频会议连接,并且告知用户该连接不安全,因此用户应该避免讨论任何敏感信息。

[0048] 系统处理器204的其他嵌入固件214的应用可以包括用于备份和同步虚拟硬盘映像(在下面更详细地描述),并且将其经由如上所述的同一个VPN通道308传递给公司的存储服务器。

[0049] 用于当今计算机的一种重要外设为磁盘驱动器,因此现在将结合图4描述根据本发明对访问该外设进行控制的范例方法。如图4所示,趋势是基于闪存的固态驱动器410将取代基于磁介质的旋转磁盘。如已知的,该驱动器典型地在其上保存传统计算机的所有软件和重要的那部分数据。当一计算机上电时,小型低电平固件从只读或闪速存储器处运行,其用于“基本输入/输出系统”、通常被称作“BIOS”,“BIOS”将初始化内存和磁盘驱动器并且将从磁盘驱动器加载操作系统软件到内存,该进程被称作“开机”或“引导”。一旦该操作系统已经开始执行,那么它将连续地访问该磁盘驱动器来读取应用和软件程序库、设备驱动程序和配置文件。

[0050] 当操作系统执行任一安全相关机制时,被用于这些保护元件的密钥和口令也存储在同一个磁盘上。任一需要运行在单机环境的软件应用,当网络不可用时,需要将它的所有数据以及可执行的程序代码和配置数据存储到磁盘驱动器上。因为这些及其他的理由,磁盘驱动器需要对付各种可能性威胁的保护,其中最值得注意的威胁是磁盘驱动器本身或其随着整个计算机有失窃的可能,以及随后它所包含的数据被提取的可能。对于当今的计算机来说,将它磁盘驱动器上存储的数据加密日益普遍,其中磁盘的整个内容以单个密钥加密。这使得如果这单个密钥汇露,则数据易受攻击,并且同时它产生了新的潜在问题:如果计算机用户忘记或丢失加密密钥,则公司和使用该计算机的雇员将都不能再取回该硬盘上的任何数据。

[0051] 这里披露的计算机体系结构的一个方面在于磁盘驱动器的实现方式。在实施例中,例如结合图4所示出的,运行应用软件和操作系统的应用处理器202不需要实施任何安全保护措施,并且不能直接访问计算机实际的磁盘驱动器410。反而,应用处理器202的大容

量存储外设连接，典型地为串联ATA(或“SATA”)的主机控制器404，连接到系统处理器204上的兼容式接口，即串联ATA目标接口406。该接口406响应由应用处理器202发出的标准ATA指令，并且与系统级固件214一起为应用处理器202提供仿真磁盘驱动器414。由固件214实现仿真磁盘驱动器的进程可以类似于虚拟化环境中采用的技术-仿真磁盘驱动器414实际上为以特定格式存储在真实的磁盘驱动器410上的文件集合。从而系统处理器204将具有第二大容量存储器接口408，其将它连接到一真实磁盘驱动器(例如一磁介质或其他介质的HDD)、或更优选为固态磁盘驱动器(“SSD”)410。这样的SSD(例如由闪速存储器或其他的非易失性存储器技术，比如铁电RAM和相变RAM，实现)提供了比磁性驱动器更好的性能，并且将实质上掩蔽任何性能退化，而这可以被如下所述的仿真进程和加密所利用。

[0052] 在图示的范例体系结构中，系统处理器204的固件214以文件集合和主要索引文件的方式保存一个或多个仿真磁盘驱动器414的映像，它们按顺序以特定格式存储在真实磁盘驱动器410的文件系统中。仿真磁盘驱动器414会分布到多个文件，这存在几个原因。第一，磁盘驱动器很少会被整体使用，由此不必在真实磁盘驱动器上为不用的存储空间分配任何存储空间。因此，将仿真驱动器414提供的空间分散到文件集合上能允许对它的地址空间进行稀疏提供，并且省略了用于没有使用的区域的实际存储。第二，在某些时候，需要保持仿真驱动器的一致映像416，其对应于它在某个时间点的内容，这被称为检测点，然后将所有随后修改的数据写入位于真实驱动器上的新的和独立的文件，使得即使当仿真磁盘414被连续使用时，在检测点的那个时间，它的内容仍然可用。为什么需要检测点存在各种原因，其中一个原因是能够备份或同步位于中心公司数据储存库中的磁盘的内容，并且防止在计算机丢失或被损事件中损失数据。该检测点和备份功能由系统处理器204的固件214实现，因此这些功能独立于处理器202的操作系统或应用软件之外。此外，由于系统处理器204消耗的功率显著地小于应用处理器202，如果计算机没有活跃地使用而是需要执行周期性备份进程，则不需要施加功率到应用处理器202，此时计算机能完全地与公司备份服务器通信并安全地、独立地将仿真磁盘414的最新区传输到服务器。

[0053] 当存储在真实磁盘驱动器上时，优选加密仿真磁盘414的数据。为了避免混乱，应用处理器202和系统处理器204之间的数据块交换不加密，并且传输用明码正文。该数据然后在写入真实固态磁盘驱动器410之前被进程412(例如利用AES256)加密。被用于加密仿真磁盘数据的加密密钥优选为无论任何时刻都不存在于应用处理器202的存储空间中，并且因此任何借助于嵌入到计算机上的恶意软件执行的针对该加密密钥的攻击都将无效。甚至在系统处理器204内，仿真磁盘414的加密密钥将决不保存在主存储器中，反而为加密密钥配备单独的存储空间来在正常运行期间存储这些密钥。该特别的密钥保护存储器也优选由非易失性存储器技术制成，使得这些密钥从不需要存储在真实的固态磁盘驱动器410上，反而保存在构成系统处理器204的一个芯片内。

[0054] 为了进一步改善仿真磁盘的防护水平，由于仿真磁盘414的数据保存在多个文件中，因此理想的是为这些文件中的每个指定专门的加密密钥，使得如果真实驱动器失窃，则使整个磁盘泄密需要的时间量将加倍。在正常运行期间，优选由任何存在于仿真磁盘中的文件使用的所有加密密钥都存在系统处理器204分配的安全模块存储器中。

[0055] 在备份进程期间，固件214将解密仿真磁盘数据414，使用VPN通道加密协议和如上所述的密钥来压缩它且重新加密它来用于传输。这样，决不需要在网络上传输仿真磁盘的

加密密钥或将它们存储在公司服务器上，因此使得在这些服务器中的一个出现泄密的事件中，泄露公司所有的计算机数据的风险最小。然而如果一计算机丢失或毁坏，存储在它的仿真磁盘414上的数据安全地保持在一个公司服务器中，并且可以很快地提供新的计算机给同一个用户并通过拷贝仿真磁盘映象416到新的计算机而恢复所有运行。

[0056] 为了使磁盘仿真对应用处理器202和它的软件的性能影响最小，系统处理器204应当能并发地执行若干大容量存储指令。这可以使用串行ATA指令集的原生命令排序特征实现。从而能有若干存储相关的动作同时发生：存储器指令由SATA目标硬件406接收到存储器中；存储器上的许多数据块被模块412加密或解密；并且在连接到真实驱动器的SATA主机接口408上执行另一个存储指令，这些全部同时进行，因此可能同时有至少三个存储操作由系统处理器204处理。只要应用处理器202及其运行的操作系统能够在接收第一个指令的响应之前发出另外的存储指令，由于在仿真磁盘驱动器414的同时处理这些指令增加了复杂性而导致的不可避免的延迟将有效地被掩蔽。

[0057] 不属于上述组的外设以及可选的一些属于上述组的外设，通常使用通用串行总线(USB)接口。现在将结合附图5描述根据本发明的一些方面提供的安全访问这些外设的范例方法。这样的外设可以包括键盘、鼠标、打印机、无线调制解调器、读卡器、外部磁盘驱动器和各种专用于应用的I/O器件。如已知的，可以经由USB连接的各个外设属于多种类型，就计算机系统的安全而言每种类型都可能具有独特的含义。一些USB外设可以被认为相当地安全，同时另外一些在近年来经常被盗窃数据和被电子破坏。因此优选在于将USB外设连接作为总体来受一附加层的保护，附加层稍微有点像网络保护防火墙，其将利用一组策略512来选择哪些外设被允许、哪些外设被禁止、以及哪些外设可被用于受限的或受控的方式。例如，一些公司可以禁止利用外部USB大容量存储器(比如闪存驱动器)。其他公司可以选择只要这些器件来自本公司就允许它们的使用，或者将读取和写入闪存驱动器的每个文件都发送给公司安全团队来检查可能的嵌入恶意软件或用于审核。

[0058] 按照上述考虑，图5示出的本发明实施例中的系统处理器204优选包括两个USB端口，一个作为扩充目标504，并且另一个作为正常USB主机502。主机端口502用来连接到真实的USB外设506，其中一些可能内置于计算机；例如，视频会议摄像机、音频扬声器和麦克风、键盘和触控板，以及若干用于连接外部外设的标准化USB端口。

[0059] USB目标端口504“背靠背”直接连接存在于应用处理器子系统202上的标准USB端口508，并且包含与专门设计的固件214互补的适当硬件资源来仿真多个USB外设。常规的USB目标控制器包括足够资源来实现唯一的单个目标器件，但其不足以应付多个USB外设的情况。为了实现本申请公开的计算机体系结构，USB目标端口504优选实现更多的硬件资源和逻辑，并且能够仿真514多个(例如至少8个)独立的USB外设，其中每个都有它自己的设备地址。这些由应用处理器202操作系统的USB软件堆栈计数，就像实际上有若干独立的USB设备经USB Hub连接到应用处理器202一样。因为一些真实的、将依赖于仿真USB器件514提供功能的器件可能速变比应用处理器202上的USB接口508的最大速度低，所以USB目标端口504如果实现USB Hub所需逻辑的话将受益于总体系统性能。换句话说，扩充USB目标端口504所需的资源相当于USBHub510和若干独立的USB目标器件506的资源。

[0060] 系统处理器204的固件214与硬件功能互补，并且将每个被仿真的USB外设514映射到连接到它的USB主机端口502的真实USB器件506，但是这样做的方式要和一组安全策略

512一致。这些策略512由固件214本地存储并且可以有时自动地从公司的服务器上找回，这无需用户干涉。这些策略512可以允许映射和对被认为实质上无恶意的某一类器件的透明桥接。然而，即使最无恶意的USB器件(例如外部鼠标)，也必须检查它们的USB数据结构的合法性，使得可能存在于应用操作系统USB堆栈中的任一可被恶意嵌入的USB数据包利用的弱点被引擎512保护。

[0061] 其他的USB器件可能被引擎512根据他们类型和子类禁止。一些USB器件可能根据制造和类型编号乃至更具体地说根据它们的串行号码来允许，使得例如USB闪存驱动器可以被普遍地禁止，同时很多专门的具有嵌入安全屏蔽的、由公司提供的闪速驱动器将被允许。

[0062] 有时被允许的器件将以某些特定动作仿真514。例如，计算机键盘是USB器件，并且应该被普遍允许，除去某些应该被系统处理器204截取并且不送达到应用处理器202的、用来请求调用某些需要的系统级功能的特定组合键之外。另一个范例是当允许的USB闪速驱动器被策略512请求时保持审核跟踪。在这种情况下，用来在USB闪速驱动器读写数据的指令将被系统处理器的两个USB端口502、504转发，但是这些指令与附带数据一起将被记录在本地驱动器上的专用文件中，随后通过VPN通道提交给公司服务器用于存储和随后的审核。

[0063] 在USB目标端口504随着USB hub510上的逻辑扩展时，即支持分割事务，桥接可以成为透明。分割事务支持允许系统处理器204来处理任何来自应用处理器202的USB堆栈的指令，这通过转发同一个请求(如果被允许)到实际的真实USB器件506，然后当它就绪时返回响应来执行。如果不使用分割事务支持，则固件必须准备提前响应任何可预料到的USB指令，并且将它存储到适当的USB目标设备终端缓存器，这将始终允许在真实的和仿真的USB器件之件的桥接有足够的透明度。

[0064] 除上述之外，在两个子系统202和204之间将往往需要多个连接，包括那些纯粹为运行目的所需的而且对应用和操作系统的运行没有任何影响的连接。一个这样的连接将使系统处理器子系统204能控制应用处理器子系统202的电源，并且仿真标准的计算机电源。另一个连接可以控制和监控在应用处理器202上的“BIOS”低层操作软件，其优选经由低速串行端口实现。这将允许可操作的监控功能嵌入系统处理器204的固件214中，并且允许通过远距离的结构，将操作系统的引导进程报告到公司的服务器群。

[0065] 将结合图6描述根据本发明的实施例的提供到计算机系统100的安全访问的范例进程。

[0066] 如图6所示，进程开始于初始系统启动S602期间，例如当系统上电/重置按钮被按下时。起初，如步骤S604所示，运行在系统处理器204上的固件214承担系统100的所有控制和并阻止应用处理器202到全部系统外设的访问。例如，系统处理器204阻止到键盘206和比如鼠标的类似输入装置的访问。换句话说，即使这样的外设附接到系统100，来自它们的信号也仅提供给系统处理器204，并且这些信号不转发到应用处理器202。同样，系统处理器204使得视频多路复用器208阻止任何来自应用处理器202的视频输出在显示器210上显示。同时，系统处理器204可以使视频多路复用器208显示由系统处理器204输出的启动屏幕。

[0067] 如步骤S606所示，系统处理器204可以允许应用处理器202启动。在其他实施例中，这些步骤不会发生，直到用户已经被验证。无论如何，在启动应用处理器202期间，系统处理器204可以控制应用处理器202到磁盘驱动器410的访问(例如允许处理器202加载一操作系

统，比如Windows7)，并且为应用处理器202提供用于BIOS/操作系统的仿真键盘和显示器连接，即使这样的输入和输出实际上被系统处理器204阻止。

[0068] 在下一步骤S608中，系统处理器204专门地控制键盘206(以及或许其他的输入装置，比如触控板等)、以及正确地验证该用户所需的互动，并通过显示器210将这个流程的进程和结果通知他。如上所阐述的，验证可以包括传统的、专有的或将来的技术，并且本领域技术人员将认识到许多可能的替换。在一个非限制性范例中，系统处理器204可以提示用户输入/提供凭证，比如用户名、口令、安全密钥、生物识别特征(例如指纹)。这些凭证可以与本地存储的凭证相比较，或者系统处理器204可以将它们转送到远距离的验证服务器来比较。

[0069] 如果在步骤S610中验证被确认不成功，则在步骤S612显示出错屏幕，并且来自用户的、在配属的外设上的进一步输入将不被理会。

[0070] 或者，如果确定在步骤S610中验证成功，那么系统处理器204在步骤S614中声明了正常运行模式，并且使得视频多路复用器208允许应用处理器202的图形占据整个屏幕。同样，在成功验证之后，处理器204允许通过处理器202经总线224仿真访问到键盘206及其他外设，这由固件214中编程提供的仿真功能控制。应当注意到“验证”状态不必是永久的。例如，在系统不活动或部分关闭的情况下，该系统可以锁定且恢复到未经验证的状态。在这种情况下，应用处理器202虽然或许仍然运行，但是处理器204阻止来自任何外设的访问，除了或许系统维持工作状态所需的某些存储器和网络之外。此时，系统处理器204可以显示登录屏幕且与用户互动来进行再验证。

[0071] 作为另一个范例，甚至在该系统处于“验证状态”时，系统处理器204可以周期地在显示器210上通过以“覆盖”模式显示信息或图形以请求操作员注意，并且通过在键盘上输入预先定义的组合键来启动操作员和系统处理器204之间的互动，这将会在系统处理器204的固件的控制下使得一菜单弹出。这样的互动可用于校准网络设定，执行保持功能或请求任何其他的系统处理器204固件内建的功能，比如保密语音或视频通信。

[0072] 虽然本发明已经通过参考它的最优实施例进行具体描述，但是对于本领域技术人员来说显而易见的是，在形式和细节上的进行变动和修改并没有脱离本发明的精神和范围。附带的权利更求意图包含这样的变动和修改。

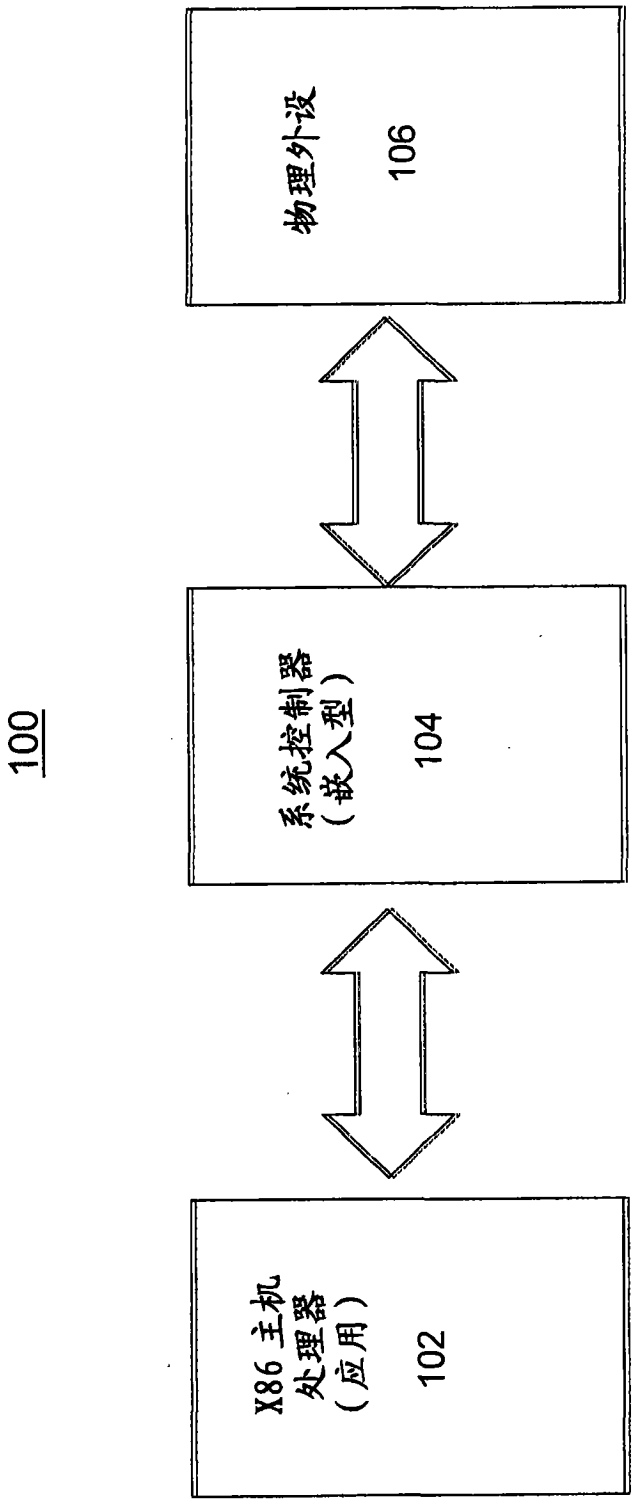


图1

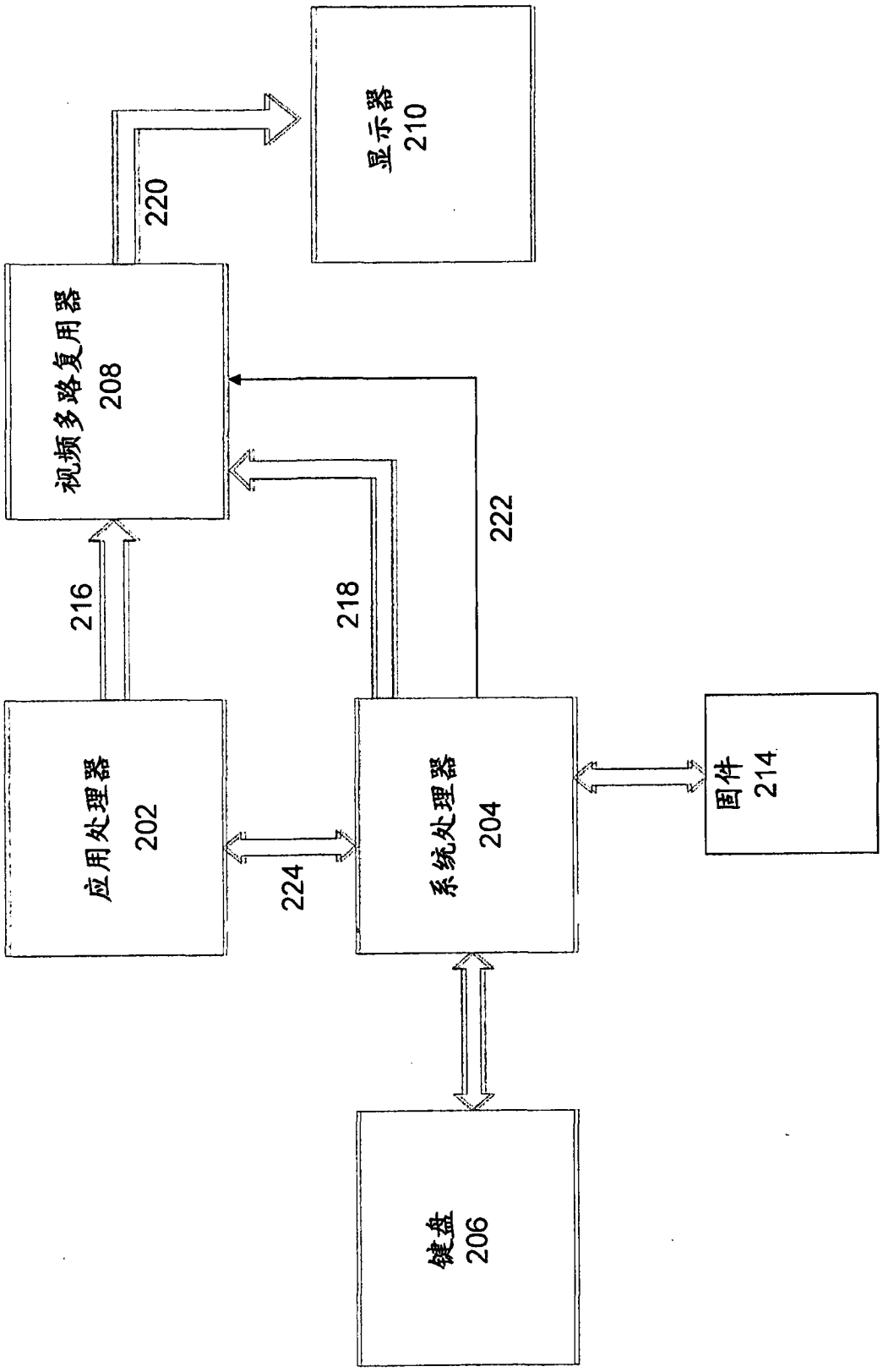

显示器
210
220
视频多路复用器
208
216
218
222
应用处理器
202
224
系统处理器
204
固件
214
键盘
206

图2

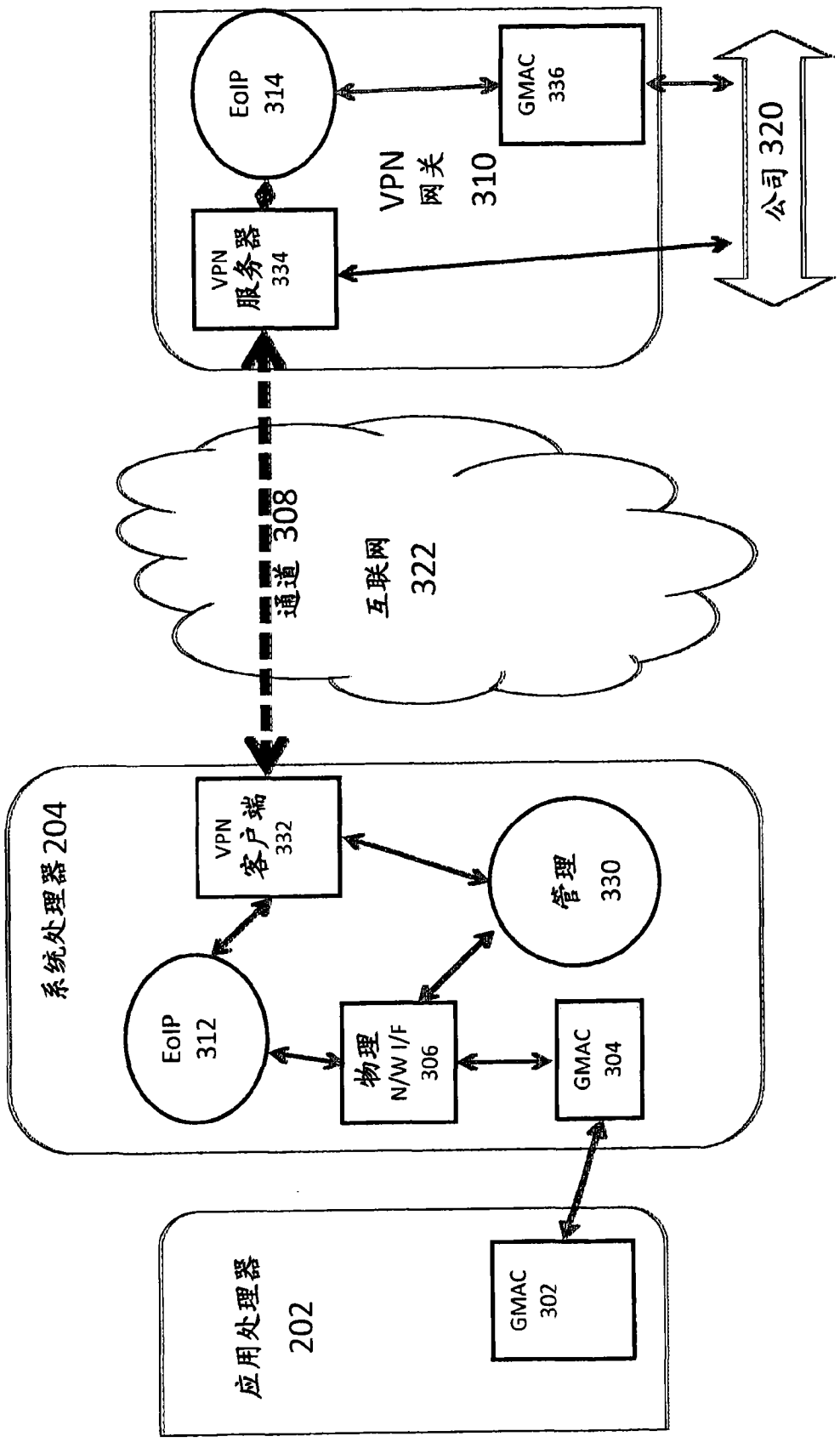

应用处理器
202
GMAC
302
系统处理器 204
EoIP
312
物理
N/W I/F
306
GMAC
304
VPN
客户端
332
管理
330
通道 308
互联网
322
VPN
网关
310
EoIP
314
GMAC
336
VPN
服务器
334
公司 320

图3

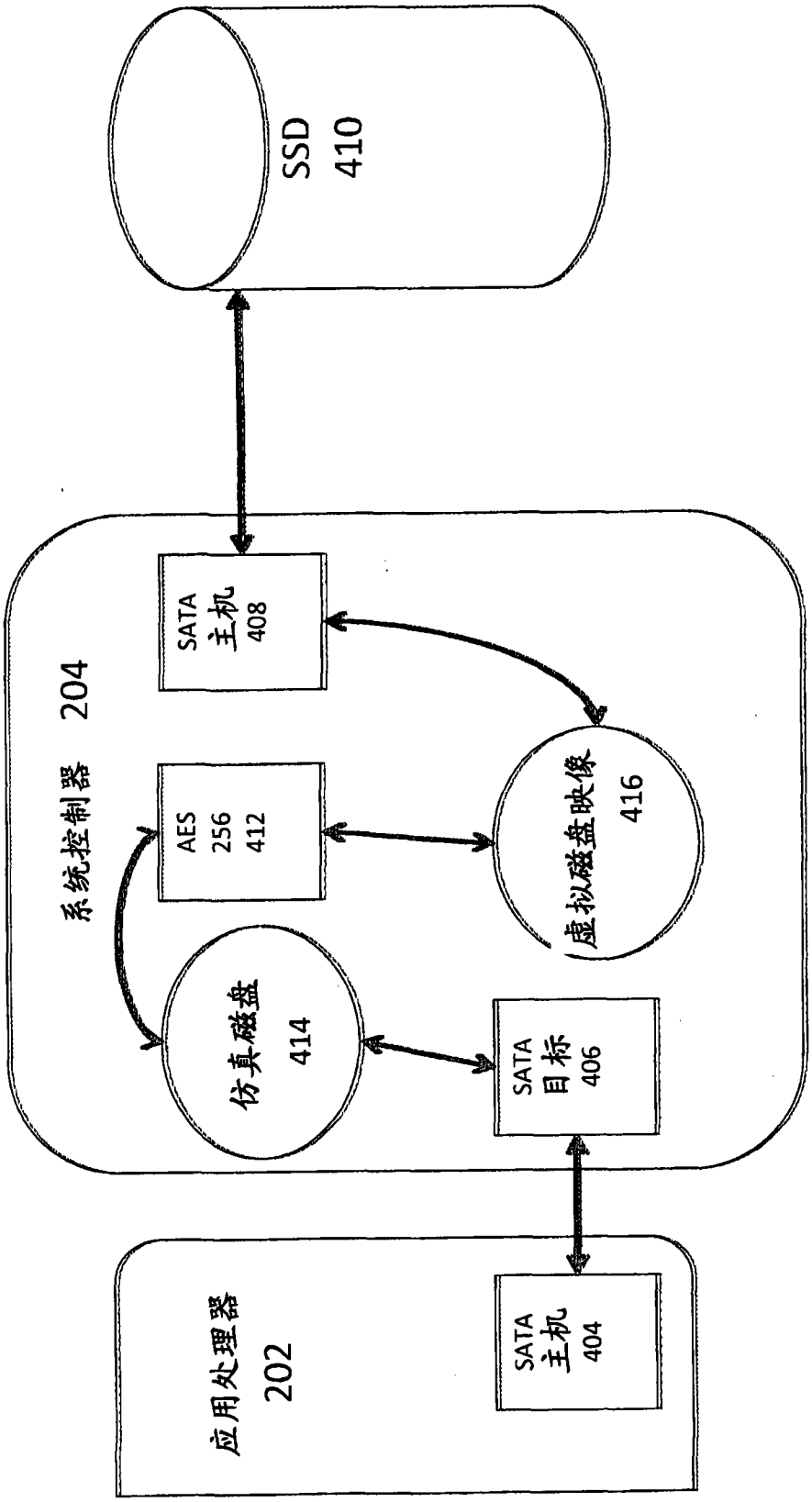

SSD
410
系统控制器 204
SATA
主机
408
AES
256
412
虚拟磁盘映像
416
仿真磁盘
414
SATA
目标
406
应用处理器
202
SATA
主机
404

图4

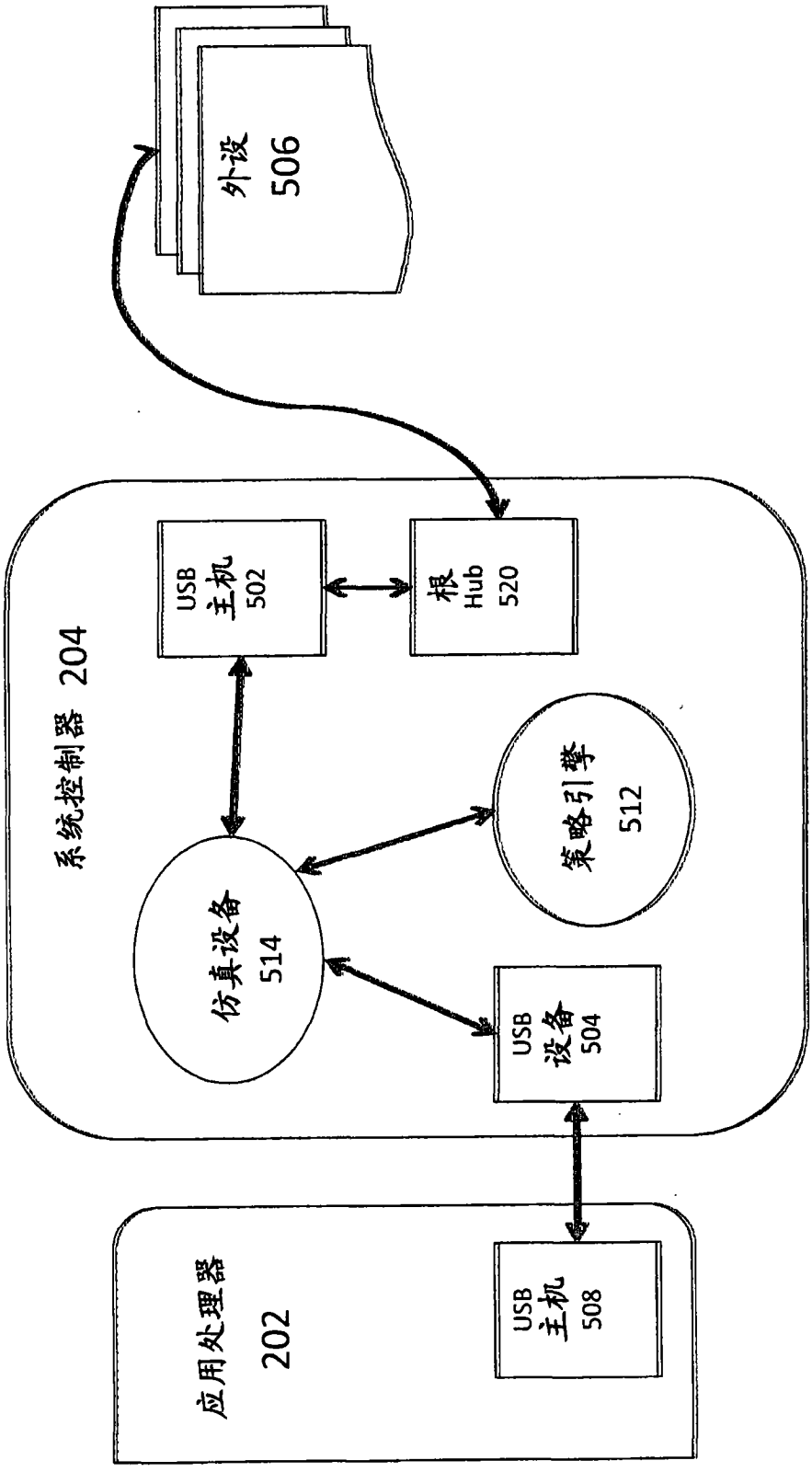

外设
506
系统控制器 204
USB
主机
502
根
Hub
520
仿真设备
514
策略引擎
512
USB
设备
504
应用处理器
202
USB
主机
508

图5

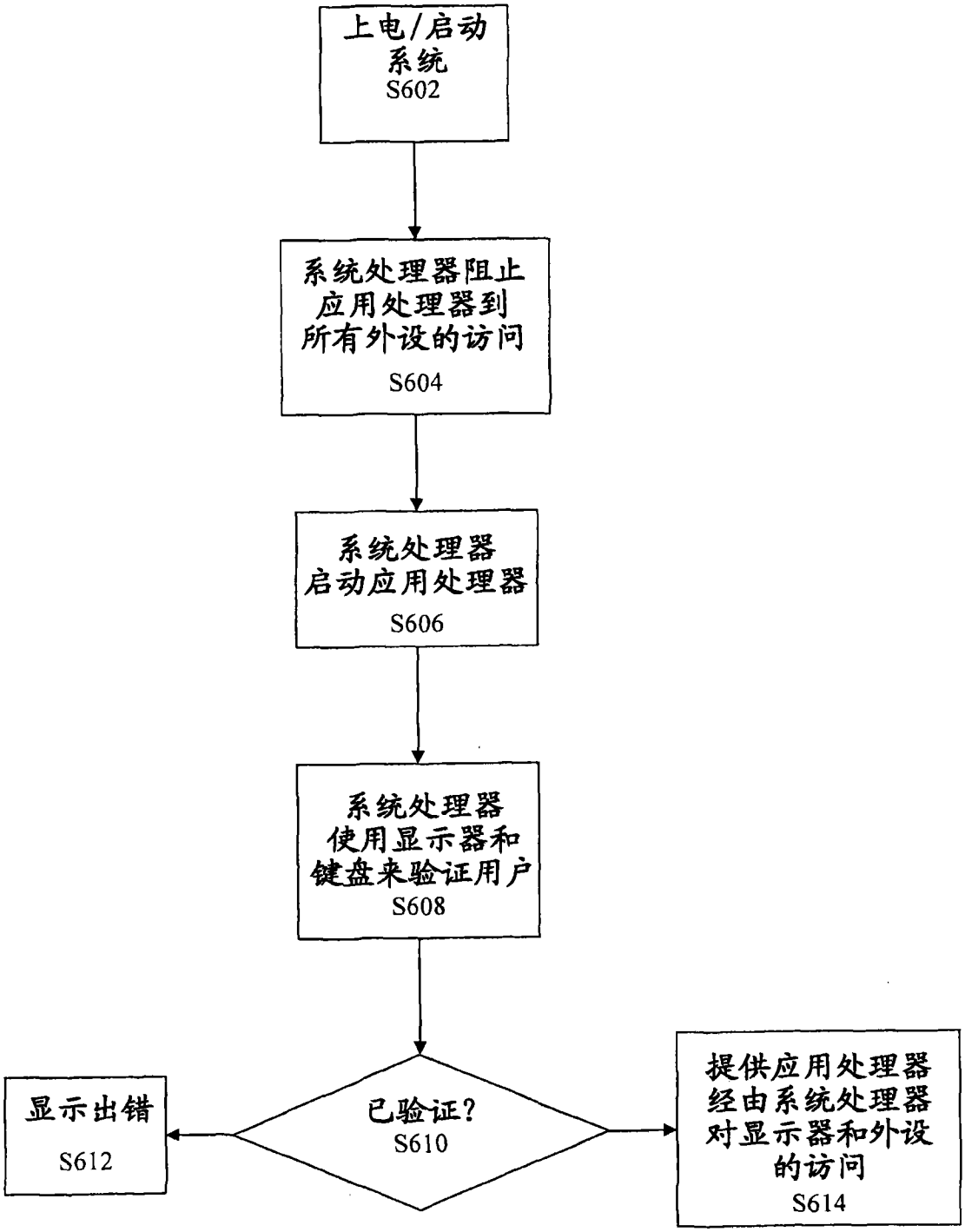

上电/启动系统
S602
系统处理器阻止应用处理器到所有外设的访问
S604
系统处理器启动应用处理器
S606
系统处理器使用显示器和键盘来验证用户
S608
已验证?
S610
显示出错
S612
提供应用处理器经由系统处理器对显示器和外设的访问
S614

图6