



(12)发明专利

(10)授权公告号 CN 106485849 B

(45)授权公告日 2020.04.07

(21)申请号 201610649806.2

(22)申请日 2016.08.10

(65)同一申请的已公布的文献号
申请公布号 CN 106485849 A

(43)申请公布日 2017.03.08

(30)优先权数据
14/838,469 2015.08.28 US

(73)专利权人 NCR公司
地址 美国佐治亚州

(72)发明人 拉梅什·瓦达迪
克里希纳·库玛瑞·鲁德拉拉祖

(74)专利代理机构 上海脱颖律师事务所 31259
代理人 脱颖

(51)Int.Cl.
G07F 19/00(2006.01)

(56)对比文件
US 2015186861 A1,2015.07.02,
US 2015081829 A1,2015.03.19,
审查员 张小波

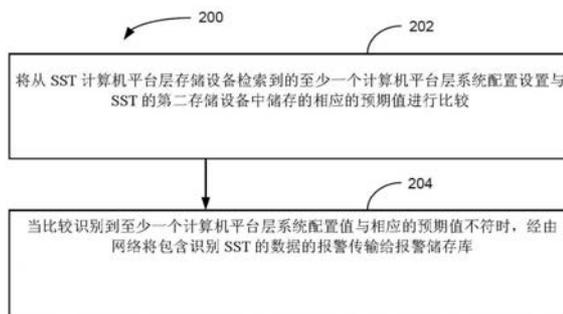
权利要求书1页 说明书5页 附图3页

(54)发明名称

用于自助服务终端技术状况监控和报警的方法和系统

(57)摘要

在本发明的各个实施例中,每个实施例包括 SST技术状况监控和报警的系统(100)、方法(200和300)和软件中的至少一种。SST(102)(例如,ATM或自助结帐POS终端)计算机上执行的方法形式的一个此类实施例包括将从SST(102)的计算机平台层存储设备检索到的至少一个计算机平台层系统配置设置与储存在SST(102)第二存储设备上的相应的预期值进行比较。然后,当所述比较识别到至少一个计算机平台层系统配置值与相应的预期值不符时,所述方法经由网络将包含识别SST的数据的报警传输给报警储存库。



1. 一种用于自助服务终端技术状况监控和报警的方法,包括:

将从自助服务终端的计算机平台层存储设备检索的至少一个计算机平台层系统配置设置与储存在所述自助服务终端的第二存储设备上的相应的预期值进行比较;及

当所述比较识别到至少一个计算机平台层系统配置值与相应的预期值不符时,经由安全网络将包含识别所述自助服务终端的数据的报警传输给报警储存库;

使所述自助服务终端离线以防止欺诈活动;以及

其中所述方法在硬件设备上执行,所述硬件设备嵌在执行计算机平台层系统的计算机主板内或与主板连接,其中所述硬件设备包括带外控制器,从而当所述自助服务终端的计算机关闭时,能够将所述至少一个计算机平台层系统配置值与相应的预期值进行比较,并且当所述比较识别到所述至少一个计算机平台层系统配置值与相应的预期值不符时将所述报警传输给所述报警储存库。

2. 根据权利要求1所述的方法,其中计算机平台层系统包括基本输入/输出系统(BIOS)或统一可扩展固件接口。

3. 根据前述任一项权利要求所述的方法,其中所述报警经由所述安全网络传输至自助服务终端管理系统的报警储存库。

4. 根据权利要求1所述的方法,其中所述至少一个计算机平台层系统配置设置包括至少一个启动设备顺序配置设置。

5. 根据权利要求1所述的方法,其中所述第二存储设备是非易失性安全存储设备。

6. 一种用于自助服务终端技术状况监控和报警的系统,其中

所述系统包括:与自助服务终端一起使用的监控和报警模块,所述模块经操作:

从所述自助服务终端内的计算机平台层检索系统配置设置;

检索预期配置设置;

将检索的所述系统配置设置与所述预期配置设置进行比较;及

当检索的所述系统配置设置与所述预期配置设置不符时,传输包含识别所述自助服务终端的数据的报警;以及

使所述自助服务终端离线以防止欺诈活动;

所述系统进一步包括:

具有配备处理器和安装在其上的存储设备的母板,所述存储设备储存平台层系统,所述平台层系统包括配置设置,所述平台层系统可由所述处理器按照配置设置来执行,从而为系统执行平台层服务,包括执行系统启动过程,其中所述平台层系统监控和报警模块包括嵌在母板内或与主板连接并作为带外控制器操作的硬件设备,并且其中当所述自助服务终端的计算机关闭时,所述系统能够将检索的所述系统配置设置与所述预期配置设置进行比较,并且当检索的所述系统配置设置与所述预期配置设置不符时,传输包含识别所述自助服务终端的数据的报警。

7. 根据权利要求6所述的系统,进一步包括:网络接口设备,所述监控和报警模块经由所述网络接口设备传输所述报警,其中所述计算机平台层系统包括统一可扩展固件接口或基本输入/输出系统(BIOS)。

用于自助服务终端技术状况监控和报警的方法和系统

技术领域

[0001] 本发明涉及自助服务终端技术状况监控和报警。

背景技术

[0002] 自助服务终端 (SST) (例如,自动柜员机 (ATM) 和自助服务销售点 (POS) 终端) 包括重要的安全措施,用于保护存在它们里面的钞票和在它们上面执行的交易服务。

[0003] 其中一种安全措施是采用密码保护控制SST的计算机的基本输入/输出系统 (BIOS), 例如, 保护启动设备顺序。原因在于, 如果SST从可移动媒体 (如光盘或记忆棒) 启动, 则可以执行储存在其上面的软件, 导致SST出钞、载入恶意代码, 或为了恶意目的而改变SST的操作。因此, 需要确保启动设备顺序和其它BIOS设置的安全。然而, BIOS设置可能仍然被破坏 (即被更改), 但是, 在技术人员在检测到欺诈行为后对SST进行实地检查之前, 通常不会发现它们已经被破坏这一事实。这种欺诈活动可包括未经授权出钞。

发明内容

[0004] 在本发明的各个实施例中, 每个实施例包括SST技术状况监控和报警的系统、方法和软件中的至少一种。SST (例如, ATM或POS终端) 计算机上执行的方法形式的一个此类实施例包括将从SST的计算机平台层存储设备检索的至少一个计算机平台层系统配置设置与储存在SST的第二存储设备上的相应的预期值进行比较。然后, 当所述比较识别到至少一个计算机平台层系统配置值与相应的预期值不符时, 所述方法经由网络将包含识别SST的数据的报警传输给报警储存库。

[0005] 另一个方法实施例包括检索SST计算机平台层系统的至少一个计算机平台层系统配置设置和从SST的第二存储设备检索预期的配置设置。所述方法接下来将每个所述至少一个配置设置与从第二存储设备检索的各预期配置设置进行比较。然后, 当所述比较识别到至少一个计算机平台层系统配置值与相应的预期值不符时, 所述方法可经由SST的网络接口设备将包含识别SST的数据的报警传输给报警储存库。

[0006] 另一个系统形式的实施例, 例如, SST的计算机控制操作, 包括配备至少一个处理器和至少一个存储设备的母板。所述至少一个存储设备储存平台层系统及其配置设置。所述平台层系统可由所述至少一个处理器按照配置设置来执行, 从而为该系统执行平台层服务, 包括执行系统启动过程。系统还包括网络接口设备和平台层系统监控和报警模块。平台层系统监控和报警模块经操作可执行数据处理活动。在一些实施例中, 数据处理活动包括从至少一个存储设备检索至少一个计算机平台层系统配置设置和从至少一个存储设备检索预期配置设置。在这些实施例中, 然后, 数据处理活动将至少一个配置设置的每个设置与各预期配置设置进行比较。当这种比较识别到至少一个计算机平台层系统配置值与预期值不符时, 数据处理活动包括经由网络接口设备将包含识别SST的数据的报警传输至报警储存库。

[0007] 根据本发明的第一个方面, 提供一种方法, 包括: 将从自助服务终端 (SST) 的计

机平台层存储设备检索的至少一个计算机平台层系统配置设置与储存在SST的第二存储设备上的相应的预期值进行比较;当这种比较识别到至少一个计算机平台层系统配置值与预期值不符时,经由网络将包含识别SST的数据的报警传输给报警储存库。

[0008] 计算机平台层系统任选是基本输入/输出系统 (BIOS)、统一可扩展固件接口 (UEFI) 等。

[0009] 所述方法任选在嵌在执行计算机平台层系统的计算机母板内或与该母板连接的硬件设备上执行。

[0010] 硬件设备任选是带外控制器。

[0011] 报警任选经由网络传输给SST管理系统的报警储存库。

[0012] 至少一个计算机平台层系统配置设置任选是至少一个启动设备顺序配置设置。

[0013] 第二存储设备任选是非易失性安全存储设备。

[0014] 根据本发明的第二个方面,提供一种系统,包括:配备至少一个处理器和其上有至少一个存储设备的母板,至少一个储存平台层系统的存储设备及其配置设置,所述平台层系统可由所述至少一个处理器按照配置设置来执行,从而为该系统执行平台层服务,包括执行系统启动过程;网络接口设备;及平台层系统监控和报警模块,其经操作可执行数据处理活动,包括:从至少一个存储设备检索至少一个计算机平台层系统配置设置;从至少一个存储设备检索预期配置设置;将至少一个配置设置的每个设置与各预期配置设置进行比较;当这种比较识别到至少一个计算机平台层系统配置值与预期值不符时,经由网络接口设备将包含识别SST的数据的报警传输给报警储存库。

[0015] 计算机平台层系统任选是统一可扩展固件接口 (UEFI)。

[0016] 平台层系统监控模块任选是嵌在母板内或与母板连接的硬件设备。

[0017] 平台层系统监控模块硬件设备任选是母板的带外控制器,包括在其上面执行的平台层系统监控模块指令。

[0018] 至少一个计算机平台层系统配置设置任选是至少一个启动设备顺序配置设置。

[0019] 系统任选是自动柜员机 (ATM)。

[0020] 根据本发明的第三个方面,提供一种方法,包括:检索自助服务终端 (SST) 计算机平台层系统的至少一个计算机平台层系统配置设置;从SST的第二存储设备检索预期配置设置;将至少一个配置设置的每个设置与从第二存储设备检索的各预期配置设置进行比较;当这种比较识别到至少一个计算机平台层系统配置值与预期值不符时,经由SST的网络接口设备将包含识别SST的数据的报警传输至报警储存库。

[0021] 至少一个计算机平台层系统配置设置任选经由计算机平台层系统的接口进行检索。

[0022] 计算机平台层系统任选是基本输入/输出系统 (BIOS)、统一可扩展固件接口 (UEFI) 等。

[0023] 任选带外控制器执行以下步骤:检索至少一个配置设置和预期配置设置,进行比较,并传输。

[0024] SST任选是自助服务结帐终端。

[0025] 根据本发明的第四个方面,提供一种与自助服务终端一起使用的监控和报警模块,该模块经操作:从自助服务终端的计算机平台层检索系统配置设置;检索预期配置设

置;将检索的配置设置与预期配置设置进行比较;当检索的配置设置与预期配置设置不符时,传输包含识别自助服务终端数据的报警。

附图说明

[0026] 以下通过举例并参照附图,对本发明的上述内容和其他方面加以具体说明:

[0027] 根据一个示例实施例,图1是系统的逻辑方框图;

[0028] 根据一个示例实施例,图2是方法的流程方框图;

[0029] 根据一个示例实施例,图3是方法的流程方框图;及

[0030] 根据一个示例实施例,图4是计算设备的方框图。

具体实施方式

[0031] 在本发明的各个实施例中,每个实施例包括SST技术状况监控和报警的系统、方法和软件中的至少一种。SST,例如,ATM和自助结帐POS终端,包括控制SST及与其连接的各种外围设备的操作的计算机。外围设备可包括钞箱、出钞器、显示器、一个或多个输入设备等。当计算机控制SST的操作时,如果计算机被破坏,储存在SST上面或通过SST的钞票和其它数据可能被破坏、盗用或用于欺诈活动。可能破坏SST的一种方法是从存储设备(如记忆棒或光盘)载入恶意代码、程序或过程。来自此类设备的代码通常只能在控制计算机启动时被载到SST上。因此,启动设备顺序通过计算机平台层系统得以确保。但是,启动设备顺序仍然可能被破坏。但是,仍然可以通过操作其它计算机平台层系统来破坏SST。此处的各实施例添加作为计算机平台层系统的一部分的硬件或软件元件,或添加作为嵌在控制SST的计算机主板内的或与该主板连接的固件设备的硬件或软件元件,或为了监控计算机平台层系统的配置设置(例如启动设备顺序)而添加硬件或软件元件。在其它实施例中,可以使用现有硬件元件,例如,带外(out-of-band)控制器,从而,即使计算机关闭时,此处的各实施例也可以监控计算机平台层系统的配置设置。计算机平台层系统的监控是对比储存在易失性或非易失性存储设备上的预期配置设置而执行的。当检测到配置设置与预期配置设置不同时,产生和提供报警。该报警可被发送到操作SST的实体的企业管理系统、SST维护提供商、电子邮箱或SMS帐户、其它实施例中配置的其它地方等。

[0032] 计算机平台层系统是计算设备(例如个人计算机)初始化时首先执行的软件系统。计算机平台层系统的实例包括BIOS和统一可扩展固件接口(UEFI)。当与SST一起部署时,所述计算机平台层系统通常得到保护,以防止篡改;这种篡改通常用于更改或控制SST的操作,以达到盗窃、欺诈和其它非法行为的目的。

[0033] 本文参照图形对该等及其他实施例加以描述。

[0034] 在下文的详细描述中,引用了构成本文组成部分的附图,并在所述附图中以图示方式显示了其中可以实施发明主旨事项的特定实施例。该等实施例乃以足够的细节予以描述,以确保本领域的技术人员能够实施它们,并且需要了解的是,可以利用其他实施例,且可以在不偏离发明主旨事项范围的情况下做出结构、逻辑及电气改变。该等发明主旨事项的实施例在本文中可以单独及/或共同地被称为“发明”,其仅仅是为了方便而无意将本申请的范围主动限制为任何单个发明或发明概念(如果实际披露的多于一个的话)。

[0035] 因此,下文的描述不应被视为具有限制意义,并且发明主旨事项的范围由所附权

利要求予以界定。

[0036] 在一个实施例中,本文描述的功能或算法可以以硬件、软件或软件和硬件的组合来实现。软件包括存储在诸如存储器或其他类型的存储设备等计算机可读媒体上的计算机可执行指令。此外,所描述的功能可对应于模块,其可以是软件、硬件、固件或其任何组合。多个功能以所期望的一个或多个模块来执行,并且所描述的实施例仅仅是示例。软件在数字信号处理器、ASIC、微处理器或在系统(例如个人计算机、服务器、路由器或能够处理数据的其他设备,包括网络互连设备)上操作的其他类型的处理器上执行。

[0037] 某些实施例实现其中相关控制及数据信号在模块之间及通过模块传送的两个或多个具体互连的硬件模块或设备中的功能,或作为应用程序专用集成电路的一部分。因此,示范流程可适用于软件、固件及硬件实现。

[0038] 根据一个示例实施例,图1是系统100的逻辑方框图。系统100包括经由安全网络104与银行业务系统106和企业管理系统108连接的SST,例如ATM 102。

[0039] 安全网络104通常是至少部分与SST(例如ATM网络)进行通信的网络。安全网络104可依赖允许安全数据在其他网络(例如因特网)上传输的安全联网协议。但是,在一些实施例中,安全网络104至少部分是物理安全网络。银行业务系统106通常是参与处理经由SST(例如,ATM 102)执行的交易的至少金融部分业务的系统。企业管理系统108是监控SST(例如,ATM102)性能的系统。

[0040] 在操作中,平台层系统监控和报警模块位于ATM 102上面,或其他类型的SST上面,并监控控制ATM 102操作的计算机的平台层系统的配置设置。平台层系统监控和报警模块将计算机平台层系统的实际配置设置与储存的预期配置设置者进行比较。比较的主题可能是其中一些或全部配置设置。主题配置设置通常至少包括启动设备顺序,可以包括其他或另外一些配置设置。当检测到不符时,一些实施例包括经由安全网络104传输报警到企业管理系统108。然后,企业管理系统108可进一步采取行动,例如通知安全人员或其他人员,说明发出报警的SST(例如ATM 102)可能已经被破坏。在一些实施例中,平台层系统监控和报警模块可进一步启动程序,使ATM 102离线,防止任何进一步的欺诈活动。

[0041] 在一些实施例中,平台层监控和报警模块在计算机启动时对配置设置进行比较。平台层系统监控和报警模块还可以在其他时间、定期或按照安排或随机执行或替代执行配置设置比较。

[0042] 根据一个示例实施例,图2是方法200的流程方框图。方法200是可由计算机平台层系统、平台层系统监控和报警模块,或控制SST或其他计算机的操作的计算机的平台层上的其他元件执行的方法实例。

[0043] 方法200包括将从SST的计算机平台层存储设备或其他计算机检索到的至少一个计算机平台层系统配置设置与储存在SST的第二存储设备或其他计算机内的相应的预期值进行比较(步骤202)。方法200进一步包括当所述比较识别到至少一个计算机平台层系统配置值与相应的预期值不符时,经由网络将包含识别SST或其它计算机的数据的报警传输给报警储存库(步骤204)。在一些实施例中,计算机平台层系统是BIOS、UEFI或其他平台层系统。

[0044] 根据一个示例实施例,图3是方法300的流程方框图。方法300是可由计算机平台层系统、平台层系统监控和报警模块或控制SST或其他计算机的操作的计算机的平台层上的

其他元件来执行的方法的另一个实例。

[0045] 方法300包括检索SST计算机平台层系统的至少一个计算机平台层系统配置设置(步骤302)和从SST的第二存储设备检索预期的配置设置(步骤304)。然后,方法300将所述至少一个配置设置的每个配置设置与从第二存储设备检索的各预期配置设置进行比较(步骤306)。当这种比较(步骤306)识别到至少一个计算机平台层系统配置值与预期值不符时,方法300包括经由SST的网络接口设备传输包含识别SST的数据的报警至报警储存库(步骤308)。

[0046] 在一些实施例中,至少一个计算机平台层系统配置设置经由计算机平台层系统的接口进行检索。在其他实施例中,至少一个计算机平台层系统配置设置从储存至少一个配置设置的存储位置进行检索。

[0047] 根据一个示例实施例,图4是计算设备的方框图。在一个实施例中,在分布式网络中采用多个计算机系统来在交易环境中(例如图1ATM 102、企业管理系统108和银行业务系统106)执行多个组成部分。一个面向对象、面向服务或面向其他的架构可能被用以实现该等功能,并在多个系统及组件之间进行通信。以计算机410形式存在的一个示例计算设备可能包括处理单元402、存储器404、可移动存储设备412,以及非可移动存储设备414。存储器404可能包括易失性存储器406和非易失性存储器408。计算机410可能包括一或者能够存取包括各种计算机可读媒体的计算环境,例如易失性存储器406和非易失性存储器408、可移动存储设备412和非可移动存储设备414。计算机存储包括随机存取存储器(RAM)、只读存储器(ROM)、可擦可编程只读存储器(EPROM)及电可擦可编程只读存储器(EEPROM)、闪存或其他存储器技术、光盘只读存储器(CD ROM)、数码多功能光碟(DVD)或其他光盘存储器、盒式磁带、磁带、磁盘存储器或其他磁存储设备,或者能够存储计算机可读指令的任何其他媒体。计算机410可包括或能够存取包含输入416、输出418以及通信连接420的计算环境。计算机可使用通信连接与一个或多个远程计算机连接,例如数据库服务器,从而在网络环境中操作。远程计算机可包括个人计算机(PC)、服务器、路由器、网络个人计算机、对等设备或其他共用网络节点等等。通信连接可包括局域网(LAN)、广域网(WAN)或其它网络。

[0048] 存储在电脑可读媒体上的计算机可读指令可由计算机410的处理单元402执行。硬盘(磁盘或固态盘)、CD-ROM和RAM是包括永久性计算机可读媒体的物品的一些实例。例如,各种计算机程序425或应用程序(如实现本文图示及描述的一个或多个方法的一个或多个实用程序及模块,或者可在移动设备上执行的应用程序或通过网络浏览器可予存取的应用程序)可被存储在永久性计算机可读媒体中。

[0049] 本领域的技术人员将容易理解,可以在不偏离如所附权利要求中表达的本发明主旨事项的原理和范围的情况下,在已经描述或图示的细节、材料及部件的布置和方法阶段方面作出各种其他改变,以便解释发明主旨事项的本质。

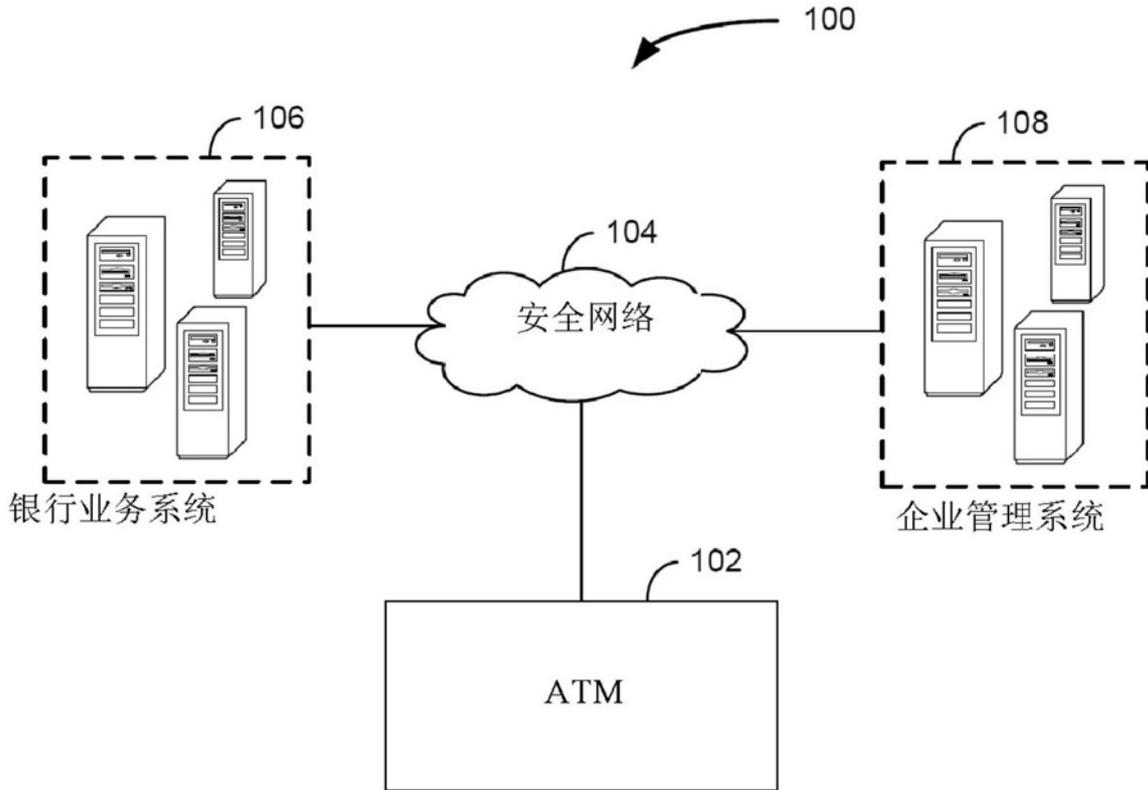


图1

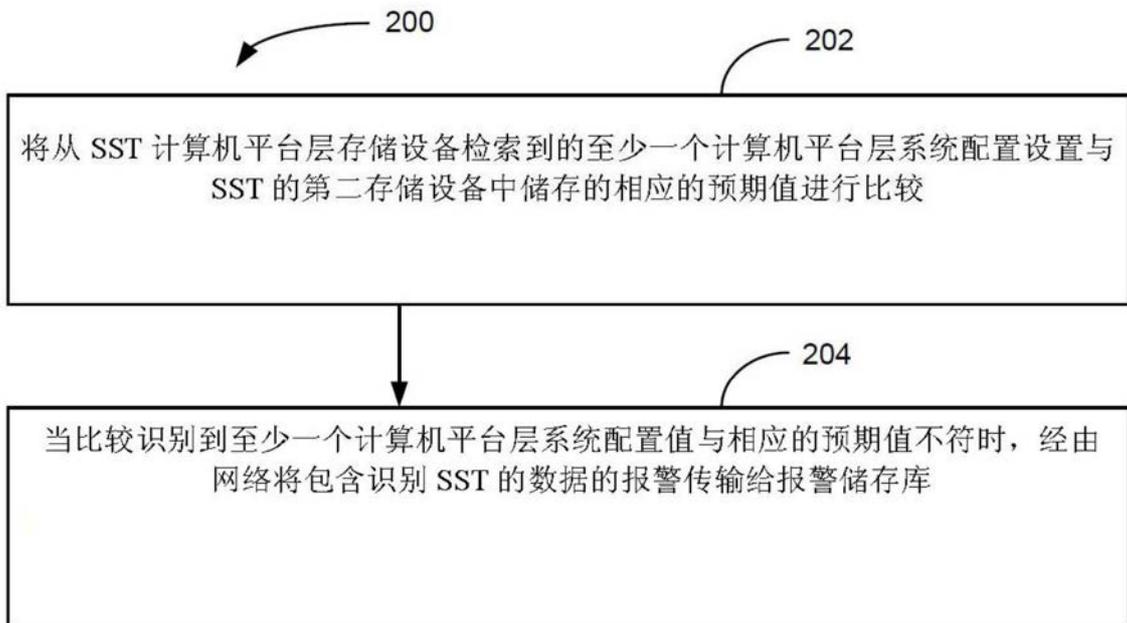


图2

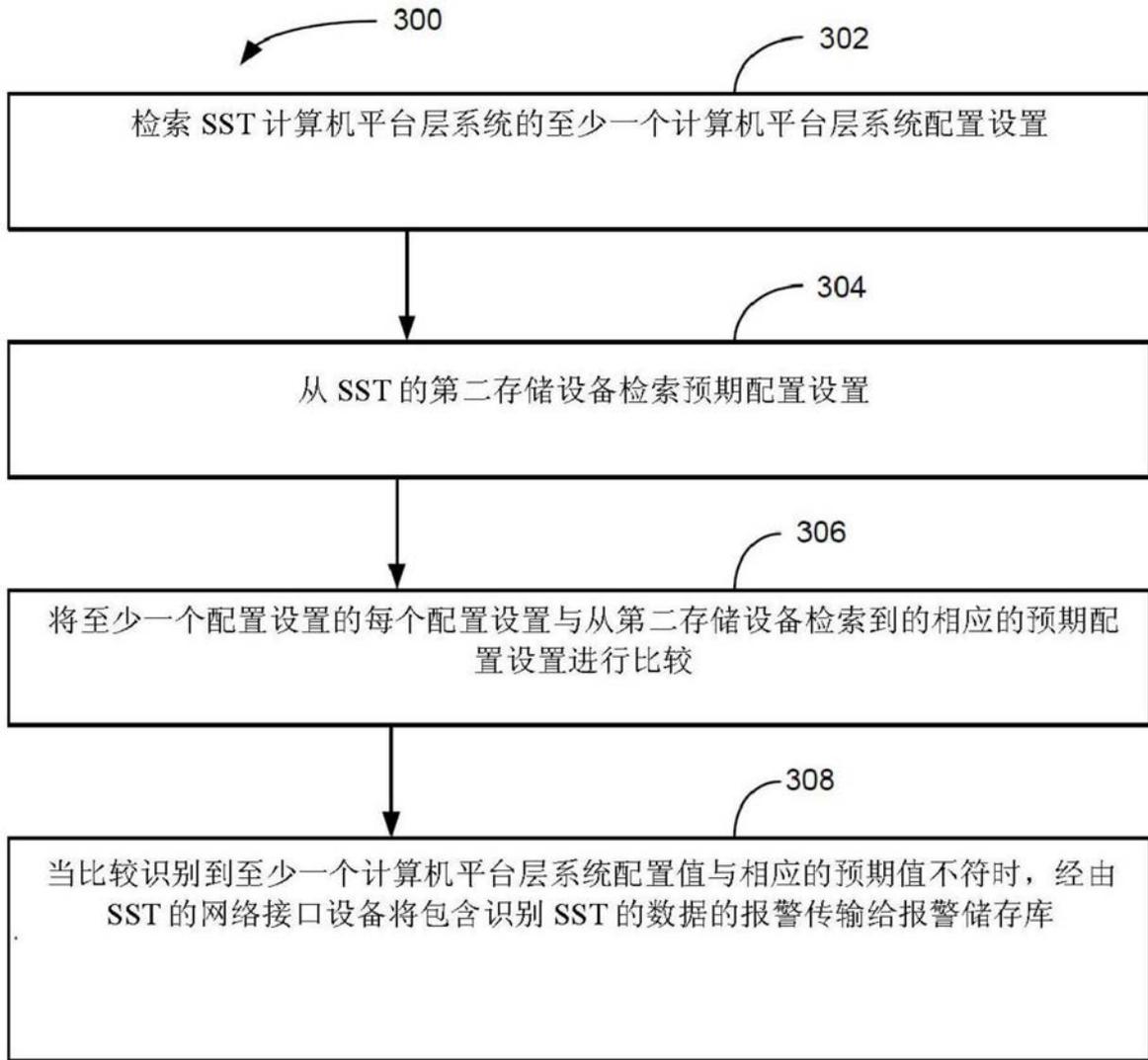


图3

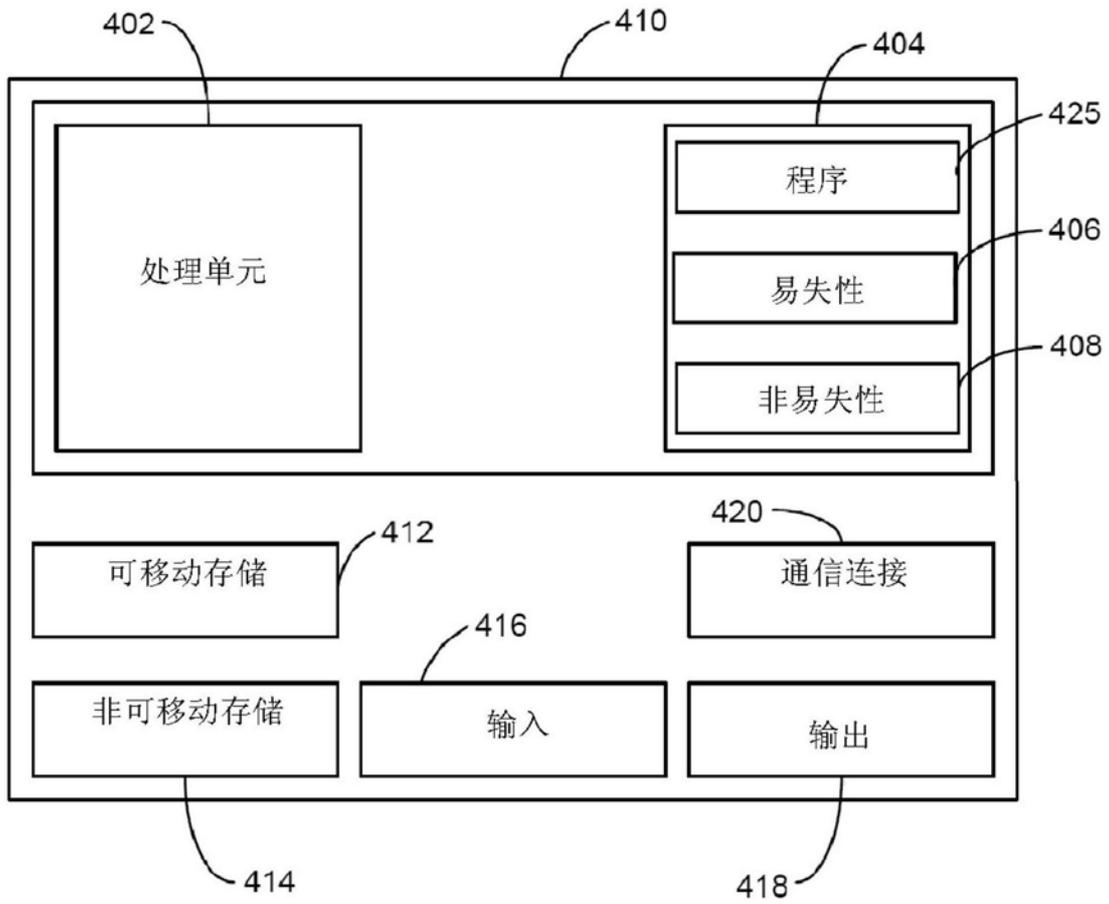


图4