(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 105892444 B
(45)授权公告日 2021.04.20

(21)申请号 201610083017.7
(22)申请日 2016.02.06
(65)同一申请的已公布的文献号
申请公布号 CN 105892444 A
(43)申请公布日 2016.08.24
(30)优先权数据
14/622,224 2015.02.13 US
(73)专利权人 费希尔-罗斯蒙特系统公司
地址 美国德克萨斯州
(72)发明人 R·A·米克瑟
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 曹雯
(51)Int.Cl.
G05B 23/02(2006.01)
审查员 张丹

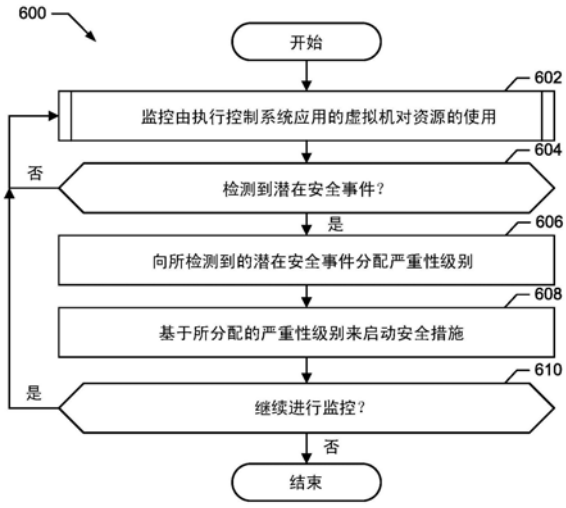
权利要求书2页 说明书10页 附图6页

(54)发明名称

通过虚拟机自省进行安全事件检测

(57)摘要

公开了用于通过虚拟机自省进行安全事件检测的方法和装置。示例性方法包括由监控代理监控在计算设备上执行的第一虚拟机对多个资源的使用,在计算设备上执行的监控代理与第一虚拟机分离。示例性方法进一步包括通过将多个资源的使用与资源使用模式相比较来检测潜在安全事件。示例性方法进一步包括为检测到的潜在安全事件分配严重性级别,以及启动为分配的严重性级别定义的安全措施。



CN 105892444 B

1.一种在过程控制系统的计算设备中的安全事件检测的方法,所述方法包括:

由监控代理监控在所述计算设备上执行的第一虚拟机对多个资源的使用,在所述计算设备上执行的所述监控代理与所述第一虚拟机分离;

通过将对所述多个资源的所述使用与资源使用模式相比较来检测潜在安全事件;

向所检测到的潜在安全事件分配严重性级别;

基于所检测到的潜在安全事件的所述严重性级别来减少向所述第一虚拟机分配的完整性级别,其中,所述完整性级别表示所述第一虚拟机已经受到所检测到的潜在安全事件的危害的可能性;

当所述完整性级别高于阈值时,基于所分配的严重性级别来启动第一安全措施;以及

当所述第一虚拟机的所述完整性级别低于所述阈值时,基于所述第一虚拟机的所述完整性级别来启动第二安全措施。

2.根据权利要求1所述的方法,其中,所述监控代理与对所述第一虚拟机进行管理的监管器通信,以监控所述第一虚拟机对所述多个资源的所述使用。

3.根据权利要求1所述的方法,其中,所述监控代理在所述计算设备上的第二虚拟机中执行。

4.根据权利要求1所述的方法,其中,所述监控代理是对所述第一虚拟机进行管理的监管器的部分。

5.根据权利要求1所述的方法,其中,所述监控代理监控所述第一虚拟机的存储器使用、储存盘使用、网络使用和硬件使用中的至少一者。

6.根据权利要求1所述的方法,其中,响应于将最高严重性级别分配给所检测到的潜在安全事件,启动所述第一安全措施包括:

基于在检测到潜在安全事件前创建的所述第一虚拟机的快照,使得第二虚拟机在所述计算设备上实例化;

将所述第一虚拟机的功能迁移到所述第二虚拟机;以及

终止所述第一虚拟机。

7.一种在过程控制系统中的计算设备中的安全事件检测的装置,所述装置包括:

资源监控器,其用于经由处理器来进行以下操作:

监控在计算设备上执行的第一虚拟机对多个资源的使用,所述资源监控器与所述第一虚拟机分离,以及

通过将对所述多个资源的所述使用与资源使用模式相比较来检测潜在安全事件;以及

安全事件处理机,其用于进行以下操作:

向所检测到的潜在安全事件分配严重性级别,

基于所检测到的潜在安全事件的所述严重性级别来减少向所述第一虚拟机分配的完整性级别,其中,所述完整性级别表示所述第一虚拟机已经受到所检测到的潜在安全事件的危害的可能性,

当所述完整性级别高于阈值时,基于所分配的严重性级别来启动第一安全措施;以及

当所述第一虚拟机的所述完整性级别低于所述阈值时,基于所述第一虚拟机的所述完整性级别来启动第二安全措施。

8.根据权利要求7所述的装置,其中,所述资源监控器与对所述第一虚拟机进行管理的

监管器通信，以监控所述第一虚拟机对所述多个资源的所述使用。

9.根据权利要求7所述的装置，其中，所述资源监控器是对所述第一虚拟机进行管理的监管器的部分。

10.根据权利要求7所述的装置，其中，所述资源监控器用于监控所述第一虚拟机的存储器使用、储存盘使用、网络使用和硬件使用中的至少一者。

11.根据权利要求7所述的装置，其中，响应于将最高严重性级别分配给所检测到的潜在安全事件，所述安全事件处理机用于进行以下操作：

基于在检测到所述潜在安全事件前创建的所述第一虚拟机的快照，使得第二虚拟机在所述计算设备上实例化；

将所述第一虚拟机的功能迁移到所述第二虚拟机；以及

终止所述第一虚拟机。

12.一种有形的计算机可读储存介质，包括指令，所述指令在被执行时，使得监控代理至少进行以下操作：

监控在计算设备上执行的第一虚拟机对多个资源的使用，在所述计算设备上执行的所述监控代理与所述第一虚拟机分离；

通过将对所述多个资源的所述使用与资源使用模式相比较来检测潜在安全事件；

向所检测到的潜在安全事件分配严重性级别；

基于所检测到的潜在安全事件的所述严重性级别来减少向所述第一虚拟机分配的完整性级别，其中，所述完整性级别表示所述第一虚拟机已经受到所检测到的潜在安全事件的危害的可能性；

当所述完整性级别高于阈值时，基于所分配的严重性级别来启动第一安全措施；以及

当所述第一虚拟机的所述完整性级别低于所述阈值时，基于所述第一虚拟机的所述完整性级别来启动第二安全措施。

13.根据权利要求12所述的有形的计算机可读储存介质，其中，所述指令在被执行时，使得监控代理还与对所述第一虚拟机进行管理的监管器通信，以监控所述第一虚拟机对所述多个资源的所述使用。

14.根据权利要求12所述的有形的计算机可读储存介质，其中，所述监控代理用于在所述计算设备上的第二虚拟机中执行。

15.根据权利要求12所述的有形的计算机可读储存介质，其中，所述监控代理是对所述第一虚拟机进行管理的监管器的部分。

16.根据权利要求12所述的有形的计算机可读储存介质，其中，所述指令在被执行时，使得监控代理监控所述第一虚拟机的存储器使用、储存盘使用、网络使用和硬件使用中的至少一者。

17.根据权利要求12所述的有形的计算机可读储存介质，其中，响应于将最高严重性级别分配给所检测到的潜在安全事件，所述指令在被执行时，使得监控代理进行以下操作：

基于在检测到所述潜在安全事件前创建的所述第一虚拟机的快照，使得第二虚拟机在所述计算设备上实例化；

将所述第一虚拟机的功能迁移到所述第二虚拟机；以及

终止所述第一虚拟机。

通过虚拟机自省进行安全事件检测

技术领域

[0001] 本公开内容总体上涉及过程控制系统，具体而言，涉及用于通过虚拟机自省进行安全事件检测的方法和装置。

背景技术

[0002] 如在化工、石油或其它过程中使用的过程控制系统通常包括一个或多个过程控制器，该一个或多个过程控制器经由模拟、数字或组合的模拟/数字总线来通信地耦合到至少一个主机或操作者工作站以及一个或多个现场设备。现场设备(其例如可以是设备控制器、阀、阀定位器、开关和传送器(例如温度、压力和流速传感器))在过程控制系统中执行功能，例如打开或关闭阀以及测量过程参数。过程控制器接收指示由现场设备进行的过程测量和/或关于现场设备的其它信息的信号，使用该信息来实现控制例程，随后生成控制信号，控制信号通过总线或其它通信线路被发送到现场设备以控制过程控制系统的操作。

发明内容

[0003] 在过程控制系统的计算设备中的安全事件检测的示例性公开的方法包括：由监控代理监控在计算设备上执行的第一虚拟机对多个资源的使用，在所述计算设备上执行的所述监控代理与所述第一虚拟机分离。示例性公开的方法还包括：通过将对所述多个资源的所述使用与资源使用模式相比较来检测潜在安全事件。示例性公开的方法还包括：向所检测到的潜在安全事件分配严重性级别，以及基于所分配的严重性级别来启动安全措施。

[0004] 示例性公开的装置包括：资源监控器，其用于经由处理器来进行以下操作：监控在计算设备上执行的第一虚拟机对多个资源的使用，所述资源监控器与所述第一虚拟机分离；以及通过将对所述多个资源的所述使用与资源使用模式相比较来检测潜在安全事件。示例性公开的装置还包括：安全事件处理机，其用于进行以下操作：向所检测到的潜在安全事件分配严重性级别，以及启动针对所分配的严重性级别而定义的安全措施。

[0005] 示例性公开的有形的计算机可读储存介质包括指令，所述指令在被执行时，使得监控代理监控在计算设备上执行的第一虚拟机对多个资源的使用，在所述计算设备上执行的所述监控代理与所述第一虚拟机分离。示例性公开的有形的计算机可读储存介质还包括指令，所述指令在被执行时，使得机器通过将对所述多个资源的所述使用与资源使用模式相比较来检测潜在安全事件。示例性公开的有形的计算机可读储存介质还包括指令，所述指令在被执行时，使得机器进行以下操作：向所检测到的潜在安全事件分配严重性级别，以及启动针对所分配的严重性级别而定义的安全措施。

附图说明

[0006] 图1示出了示例性过程控制系统。

[0007] 图2示出了用以在执行过程控制应用的虚拟机上检测安全事件的示例性系统。

[0008] 图3示出了用以检测安全事件的、图2的示例性监控代理的示例性实现方式。

[0009] 图4示出了示例性界面，其用于定义由用以检测安全事件的、图2和图3的示例性监控代理所使用的安全事件模式。

[0010] 图5示出了示例性界面，其用于定义图2和图3的示例性监控代理对安全事件的检测做出响应的措施。

[0011] 图6是表示可以被执行以实现用以检测安全事件的、图2和图3的监控代理的示例性方法的流程图。

[0012] 图7是表示可以被执行以实现用以检测安全事件的、图2和图3的监控代理的示例性方法的流程图。

[0013] 图8是示例性处理器系统的框图，其被构造为执行机器可读指令以执行由图6和/或图7所表示的方法来实现图2和图3的示例性监控代理。

具体实施方式

[0014] 本公开内容总体上涉及过程控制系统，具体而言，涉及用于通过虚拟机自省进行安全事件检测的方法和装置。过程控制系统包括工作站和/或服务器，工作站和/或服务器执行与用于执行例程、控制策略和/或算法的控制器(其管理位于控制系统中的现场设备)交互的过程控制应用。现场设备例如可以是阀、阀定位器、开关和传送器，并且可以执行过程控制功能，例如打开或关闭阀以及测量过程控制参数。除了管理现场设备以外，控制器还可以基于从现场设备接收的信息来生成过程数据(例如过程控制信息)。过程数据可以包括过程统计、告警、监控信息、过程趋势信息、诊断信息、现场设备状态信息和/或来自现场设备的消息。

[0015] 过程控制系统常常依赖于安全实用工具，例如反病毒软件、应用白名单、软件防火墙和/或操作系统安全机制，用以保护在过程控制系统中所涉及的工作站和/或服务器免于恶意攻击。但是，可以绕过这种安全实用工具。现代恶意软件能够禁用或躲避反病毒实用工具，并将自身插入到活跃运行的过程中。例如，恶意软件可以安装root kit(例如影响操作系统内核的恶意软件)和boot kit(例如影响计算机的引导过程的恶意软件)。通常，root kit和boot kit在安全实用工具前有效地隐藏其活动和加载。这允许恶意软件建立自身并保留在受危害的计算机上，而不被检测到。在一些示例中，恶意软件可以建立到受危害系统的后门，允许攻击者绕过普通安全实用工具和认证证书(例如用户名和密码、认证码等)。在一些示例中，恶意软件可以处于潜伏和未被检测到，直到攻击者准备使用恶意软件来完成更大的目的。

[0016] 如下所公开的，在虚拟化环境(例如虚拟机、容器等)中执行过程控制应用。在虚拟化环境中，管理器(例如监管器、容器守护进程(daemon)等)管理虚拟化环境(例如部署、终止、监控等)，并且允许多个虚拟化环境实例在相同的物理硬件上执行。另外，管理器将虚拟化环境与物理硬件隔离。管理器创建虚拟硬件(例如虚拟处理器、虚拟存储器、虚拟储存设备等)，并调节对这些虚拟资源的访问。管理器允许虚拟化环境的活动的可见性。例如，管理器可以有权使用虚拟化环境中的存储器、储存盘、网络和外设硬件(例如通用串行总线(USB)驱动器、CD/DVD驱动器等)等。虚拟化环境执行客户操作系统(OS)，该客户OS使用虚拟资源。客户OS如同它本来就安装好地执行(例如可以直接访问物理硬件)。安装在客户OS中的恶意软件可以禁用在相同虚拟化环境中执行的安全实用工具。但在这种配置中，恶意软

件不能影响在不同虚拟化环境中执行的管理器和过程控制应用。

[0017] 为了检测被编程以掩盖其活动的恶意软件，由管理器部署了监控代理。如下所公开的，监控代理与监控代理所监控的虚拟化环境分离。例如，监控代理在与被监控的虚拟机或容器不同的虚拟机、容器和物理机中执行。监控代理监控一个或多个虚拟化环境的活动。以此方式，在虚拟化环境中的恶意软件不能影响监控代理。在一些示例中，监控代理被并入到管理器中。

[0018] 在下述的一些示例中，监控代理使用自省来监控虚拟化环境。通常，由于虚拟化环境与在主机上执行的其它过程隔离，与虚拟资源的使用有关的信息不可用于其它过程。自省是一种过程，其中，准予在虚拟化环境外部的应用(例如监控代理)有权检查管理器对虚拟资源的使用。自省允许监控代理分析客户OS和/或由客户OS所执行的过程控制应用的状态(例如存储器值、处理器寄存器等)。通过自省，监控代理监控对虚拟化环境的资源使用。例如，监控代理可以监控存储器使用、储存盘使用、网络使用和外设硬件使用等。

[0019] 监控代理将资源使用与安全事件模式相比较。安全事件模式定义了由客户OS对资源的使用，该资源的使用指示恶意软件安装在虚拟化环境中的可能性。例如，安全事件模式可以被定义为检测网络使用，该网络使用指示已中毒的地址解析协议(ARP)表。在这种场景下，ARP表是计算机在网络上的地址的短期存储器。通过使ARP表中毒，恶意软件例如可以将假地址设置在计算机的ARP表上以便于在网络上的中间人攻击。用以检测中毒的ARP表的示例性安全事件模式可以包括：检测以与先前值不同的介质访问控制(MAC)地址到互联网协议(IP)地址映射发送的以太网帧。

[0020] 如下所述，安全事件模式与不同严重性级别相关联。严重性级别可以是名称或数值，其指示恶意软件已安装在虚拟化环境中的可能性和/或所检测到的恶意软件的危害。例如，安全事件模式可以与高、中等和/或低严重性相关联。例如，由于未授权USB设备可以是恶意软件的来源，检测到USB设备的插入的安全事件模式可以与低严重性级别相关联。举另一个示例，检测到通过网络连接到虚拟化环境的大量尝试的安全事件模式可以与中等严重性级别相关联。举另一个示例，检测到特定存储器值与虚拟化环境的初始实例化不同的安全事件模式可以与高严重性级别相关联。

[0021] 如下所述，监控代理可以基于检测到的安全事件模式的严重性来启动一个或多个措施。例如，对于低严重性安全事件模式，监控代理可以使得在工作站显示告警和/或将告警消息发送到管理员。举另一个示例，对于中等严重性安全事件模式，监控代理可以使得虚拟化环境进入只读模式(例如过程控制应用仅能够读取现场设备的状态，但不能向现场设备发出命令)。举另一个示例，对于高严重性安全事件模式，监控代理可以使得部署替换的虚拟化环境并使得受影响的虚拟化环境终止。

[0022] 如下所述，在一些示例中，监控代理向虚拟化环境分配完整性级别(例如信任级别)。完整性级别表示虚拟化环境已经受危害的可能性。当监控代理检测到安全事件模式时，监控代理根据与安全事件模式相关联的严重性来调整完整性级别。例如，在初始部署虚拟化环境时，监控代理可以向虚拟化环境分配100的完整性级别。在这个示例中，在检测到低级别安全事件模式时，监控代理可以将完整性级别减小设定量(例如1、5、10等)。在一些示例中，检测到的安全事件模式的影响随时间衰减。例如，监控代理可以在检测到低严重性安全事件模式后的24小时后，去除对低严重性安全事件模式的完整性级别的影响。在一些

示例中，管理员设定一个或多个完整性级别阈值，并定义用于监控代理响应于满足完整性级别阈值的完整性级别而执行的安全措施。例如，在100中的完整性级别阈值75，监控代理可以向管理员发送告警。举另一个示例，在100中的完整性级别阈值50，监控代理可以设置虚拟化环境以使得在虚拟化环境中执行的应用仅能够读取现场设备的状况，但不能向现场设备或外部计算机发送命令。举另一个示例，在100中的完整性级别阈值25，监控代理可以使得部署替换的虚拟化环境并使得受影响的虚拟化环境终止。

[0023] 如下所述，管理员基于例如存储器使用、储存盘使用、网络使用和硬件使用来定义安全事件模式。示例性存储器使用包括从易失性和非易失性存储器读取和/或向其写入、存储在存储器中的值、和/或与到存储器的访问有关的功能的使用(例如存储器分配、存储器清零等)。示例性储存盘使用包括对储存盘读和写、存储在储存盘上的值(例如主引导记录、注册表文件等)、以及与到存储器的访问有关的功能的使用(例如目录管理、卷管理等)。示例性网络使用包括通过网络连接发送和接收的消息、连接尝试等。示例性硬件使用包括处理器使用、硬件中断、外设硬件的检测、键盘输入等。在一些示例中，管理员定义用于监控代理响应于检测到安全事件模式而执行的措施。另外，在一些示例中，管理员定义检测到安全事件模式对虚拟化环境的完整性级别的影响。

[0024] 图1示出了结合本文所述的安全事件检测系统使用的示例性过程控制系统100。示例性系统100使用工厂过程控制架构，该架构集成了一个或多个智能化工厂能力，包括现场总线102(例如HART®和/或FOUNDATION™现场总线)、高速分立总线、嵌入式高级控制和高级单元和批量管理。现场总线网络现场设备104位于过程控制系统100内，并为各种应用(包括设备管理、配置、监控和诊断等)提供基础结构。

[0025] 示例性过程控制系统100包括示例性现场设备104、示例性控制器106、示例性I/O设备108、示例性工作站110和示例性服务器112。示例性现场设备104控制和/或监控过程，并且可以例如包括阀、传感器、接近开关、电机起动器、驱动器等。在所示出的示例中，现场设备104经由现场总线102通信地耦合到I/O设备108。示例性I/O设备108有助于与示例性现场设备104的通信。示例性I/O设备108支持各种模块与各种现场设备104通信(例如经由数字和/或模拟通信)。例如，I/O设备108可以具有与三线式温度传感器连接的模拟模块和与数字阀控制器连接的数字模块。示例性I/O设备108从现场设备104接收数据，并且将该数据转换为能够由示例性控制器106处理的通信。另外，示例性I/O设备108将来自示例性控制器106的数据和/或通信转换为能够由现场设备104处理的格式。在一些示例中，I/O设备108和控制器106被组合到一个单元中。

[0026] 示例性控制器106经由有线或无线网络(例如LAN、WAN、互联网等)耦合到工作站110和/或服务器112。示例性控制器106控制例程以基于来自现场设备104的输出来计算过程数据，以用于过程控制应用，例如包括监控应用、告警管理应用、过程趋势和/或历史应用、诊断应用、批量处理和/或商业活动管理应用、统计应用、流媒体视频应用、高级控制应用、安全仪表应用、事件应用等。控制器106以周期性间隔和/或在处理或生成过程数据后将过程数据转发到工作站110和/或服务器112。由控制器106发送的过程数据可以包括过程控制值、数据值、告警信息、文本、块模式元件状态信息、诊断信息、错误消息、参数、事件和/或设备标识符。

[0027] 在图1所示出的示例中，工作站110和/或服务器112执行过程控制应用。过程控制

应用与示例性控制器106通信以监控、控制和/或诊断现场设备104。例如，过程控制应用可以包括控制自动化、过程控制系统100的图形表示、改变管理、过程控制编辑、数据收集、数据分析等。在一些示例中，工作站110经由用户界面显示过程控制应用，以便以图形格式呈现过程数据，使得工作站110的用户能够图形化查看(经由应用)由现场设备104生成的过程数据。在一些示例中，当在服务器112上执行过程控制应用时，操作者可以建立从工作站(例如工作站110)到服务器112的远程连接来访问过程控制应用。

[0028] 在一些示例中，为了改进安全性和可扩展性，过程控制应用可以由工作站110和/或服务器112上的虚拟化环境(例如虚拟机、容器等)中的客户操作系统(OS)执行。如以下进一步详细公开的，虚拟化环境将由客户OS执行的过程控制应用与工作站110和/或服务器112的物理硬件隔离。在虚拟化环境中执行过程控制应用还允许过程控制应用彼此隔离。例如，如果一个过程控制应用受到危害(例如具有安全事件)，在不同虚拟化环境中的相同工作站110和/或服务器112上执行的其它过程控制应用保持不受影响。

[0029] 图2示出了用以在具有过程控制应用204的虚拟机202上检测安全事件的示例性系统200。在所示出的示例中，系统200在主机206(例如图1的工作站110、服务器112、控制器108、I/O设备108等)上执行。主机206包括物理硬件208(例如处理器、存储器、储存设备、外围设备、网络访问等)和监管器210。示例性监管器210管理物理硬件208，并创建虚拟硬件(例如虚拟处理器、虚拟存储器、虚拟储存设备等)，该虚拟硬件允许多个虚拟机202在主机206上执行。示例性监管器210将示例性虚拟机202隔离并控制对示例性物理硬件208的访问。以此方式，如果检测到危害在虚拟机202上执行的客户OS 212(例如Windows®、Linux、UNIX等)的安全事件，则可以保护其它虚拟机和/或物理资源208。

[0030] 在所示出的示例中，监控代理214在系统200中运行。示例性监控代理214被构造为检测安全事件模式。安全事件模式是存储器使用216、储存盘使用218、网络使用220和/或硬件使用222的模式，其指示恶意软件存在于客户OS 212上的可能性。示例性监控代理214与示例性虚拟机202分离，以使得存在于示例性客户OS 212上的恶意软件不能影响监控代理214。例如，监控代理214可以在与过程控制应用204不同的虚拟机或不同的容器中执行。在一些示例中，监控代理214集成到监管器210中。

[0031] 示例性监控代理214包括自省功能，该自省功能有助于实现对虚拟机202的存储器使用216、储存盘使用218、网络使用220和/或硬件使用222的实时访问。自省功能允许监控代理214从监管器210请求与虚拟机202有关的信息。由于监管器210创建和/或维护虚拟资源，自省功能允许监控代理214将虚拟资源与物理资源208相关联，以使得监控代理214可以检查由虚拟机202使用的物理资源的内容和使用。例如，监管器210可以维护虚拟存储器页表，其将虚拟存储器映射到物理存储器。在这个示例中，当监控代理214监控由虚拟机202使用的虚拟存储器时，自省功能允许监控代理214访问虚拟存储器页表以获知物理存储器中由虚拟机202使用的位置。

[0032] 在图2所示出的示例中，监控代理214实时(例如在资源使用216－222发生的几秒内对其监控)监控存储器使用216、储存盘使用218、网络使用220和/或硬件使用222，以检测安全事件模式(其导致对恶意软件已安装在虚拟机202上的推断)。例如，资源监控器214可以在对储存盘上的主引导记录的改变发生不久之后检测该改变。在一些示例中，监控代理214检测离散事件。例如，监控代理214可以检测何时特定存储器值改变。在一些示例中，监

控代理214检测连续事件。例如，监控代理214可以监控以太网帧，以检测ARP表的中毒(例如检测具有与先前值不同的介质访问控制(MAC)地址到网际协议(IP)地址映射的以太网帧)。

[0033] 在一些示例中，监控代理214与管理员通信，以警告管理员注意何时检测到安全事件模式和/或传送特定虚拟机202的完整性级别。在一些示例中，监控代理214与监管器210通信，以启动对检测到的安全事件模式的响应。例如，响应于特定的安全事件模式，监控代理214可以命令监管器210仅允许到受影响虚拟机202的输入网络流量，以使得在虚拟机202上执行的过程控制应用204可以从现场设备104接收状态更新，但过程控制应用204不能向现场设备104发出命令或与其它工作站和/或服务器通信。

[0034] 在一些示例中，监控代理214时常(例如周期性、非周期性等)地使得对虚拟机202获取快照。快照是虚拟机202在特定时间的状态(例如盘数据、存储器值、配置等)的副本。快照可以用于在将来的时间使虚拟机202返回到所捕获的状态。在一些示例中，可以(例如由管理员)对快照进行时间安排。在一些此类示例中，如果已检测到特定严重性(例如中等严重性、高严重性等)的安全事件模式和/或如果虚拟机202的完整性级别低于特定阈值，则监控代理214就可以取消或延迟快照。在一些示例中，如果完整性级别高于阈值，则监控代理214可以使得获取快照。

[0035] 在一些示例中，响应于检测到严重安全事件模式和/或如果虚拟机202的完整性级别低于阈值，监控代理214可以使得由监管器210部署新的虚拟机202。在一些示例中，新的虚拟机202基于客户OS 204的干净安装。在一些示例中，新的虚拟机202基于虚拟机202在检测到安全事件前的快照。在一些此类示例中，将功能(例如与现场设备104通信、通信显示设备等)迁移到新的虚拟机202。在一些示例中，在新的虚拟机202与现场设备104相通信后，监控代理214使得终止受危害的虚拟机202。

[0036] 图3示出了用以检测安全事件的、图2的示例性监控代理214的示例性实现方式。在所示出的示例中，监控代理214包括资源监控器300、安全事件处理机302、安全事件模式管理器304、和安全事件模式数据库306。示例性资源监控器300监控虚拟机202的存储器使用216、储存盘使用218、网络使用220和/或硬件使用222。在所示出的示例中，资源监控器300随着虚拟机202使用资源216－222而监控资源使用。示例性资源监控器300从安全事件模式数据库306取回安全事件模式，以确定监控资源使用216－222的哪些方面。例如，如果安全事件模式被定义为监控ARP表，则资源监控器300监控网络使用220，以便检测以与先前值不同的介质访问控制(MAC)地址到网际协议(IP)地址映射发送的以太网帧(例如指示ARP表已中毒)。如果资源使用216－222满足安全事件模式，则示例性资源监控器300向示例性安全事件处理机302告知所检测到的安全事件。

[0037] 在所示出的示例中，安全事件处理机302被构造为响应于资源监控器300检测到安全事件模式而执行安全措施。安全措施是用于监控代理214执行如在安全事件模式中所定义的和/或如由所检测到的安全事件模式的严重性级别所定义的措施。在一些示例中，安全措施由管理员308在定义安全事件模式和/或严重性级别时定义。在所示出的示例中，安全事件处理机302与管理员308相通信。在一些示例中，安全事件处理机302向管理员308发送通知。在一些示例中，通知包括与所检测到的安全事件模式和时间戳有关的信息。在一些示例中，安全事件处理机302经由通信系统(例如电子邮件、文本消息、语音消息等)向管理员308通知已检测到安全事件模式。

[0038] 在图3所示出的示例中，安全事件处理机302与监管器210相通信。在一些示例中，安全事件处理机302向监管器210发出请求，以限制虚拟机202对物理资源208的访问(图2)。例如，安全事件处理机302可以发出请求以阻止对外围设备(例如USB驱动器、盘驱动器等)的访问或者阻止网络设备上的输出流量。在一些示例中，安全事件处理机302可以请求部署虚拟机202的新副本、将与现场设备104、控制器106和/或I/O设备108的通信迁移到新的虚拟机202，并终止旧的虚拟机202。

[0039] 在一些示例中，安全事件处理机302可以管理(例如监控、调整等)虚拟机202的完整性级别。完整性级别表示虚拟机202已经受到恶意软件的损害的可能性。在一些示例中，当安全事件处理机302处理由资源监控器300检测到的安全事件模式时，安全事件处理机302调整虚拟机202的完整性级别。在一些示例中，对完整性级别的影响取决于与安全事件模式相关联的严重性。例如，虚拟机202的完整性级别可以初始地设定为100。在这个示例中，如果资源监控器300检测到与低严重性相关联的安全事件模式，则安全事件处理机302可以将虚拟机202的完整性级别减小到95。管理员308可以定义完整性级别阈值和相应的安全措施。例如，管理员308可以设定完整性级别阈值，以使得在虚拟机202的完整性级别下降到75以下时，安全事件处理机302发出告警(例如显示告警消息、发送消息(例如电子邮件、寻呼、短消息服务消息(SMS)等))。在一些示例中，安全事件处理机302基于所检测到的安全事件的严重性，在一段时间后取消特定的检测到的安全事件的影响(例如升高虚拟机202的完整性级别)。例如，在24小时后可以消除低严重性安全事件对虚拟机202的完整性的影响。

[0040] 在图3所示出的示例中，安全事件管理器304管理(例如创建、删除、修改等)安全事件模式数据库306中的安全事件模式。如下结合图4和图5更详细论述的，示例性安全事件管理器304提供界面，该界面允许管理员308定义安全事件模式和/或安全措施、修改现有安全事件模式和/或安全措施、和/或删除现有安全事件模式和/或安全措施。

[0041] 尽管图3中示出了实现图2的监控代理214的示例性方式，但图3中所示的一个或多个元件、过程和/或设备可以组合、分割、重新布置、省略、去除和/或以任何其它方式来实现。此外，示例性资源监控器300、示例性安全事件处理机302、示例性安全事件模式管理器304和/或更普遍地，图2的示例性监控代理214可以由硬件、软件、固件和/或硬件、软件和/或固件的任意组合来实现。因此，例如，示例性资源监控器300、示例性安全事件处理机302、示例性安全事件模式管理器304和/或更普遍地，图2的示例性监控代理214中的任意一个可以由一个或多个模拟或数字电路、逻辑电路、可编程处理器、专用集成电路(ASIC)、可编程逻辑器件(PLD)和/或现场可编程逻辑器件(FPLD)来实现。在阅读覆盖纯软件和/或固件实现方式的本发明的任意一个装置或系统权利要求时，示例性资源监控器300、示例性安全事件处理机302和/或示例性安全事件模式管理器304中的至少一个由此被明确地定义为包括有形的计算机可读储存设备或储存盘，例如存储软件和/或固件的存储器、数字多功能盘(DVD)、光盘(CD)、蓝光盘等。再进一步地，除了图3中所示的那些以外和/或代替那些，图2的示例性监控代理214可以包括一个或多个元件、过程和/或设备，和/或可以包括多于一个的任意或全部所示的元件、过程和设备。

[0042] 图4示出了示例性界面400，其可以用于定义由用以检测安全事件的、图2和图3的示例性监控代理214所使用的安全事件模式。在一些示例中，界面400由示例性安全事件管理器304(图3)提供。示例性界面400用于管理(例如创建、删除、修改等)在示例性安全事件

模式数据库306(图3)中所存储的安全事件模式。在所示出的示例中,界面400包括示例性名称字段402、示例性严重性字段404、示例性类别字段405、和示例性条件字段406。提供示例性名称字段402以便于示例性管理员308(图3)向安全事件模式分配唯一的标识符。提供示例性严重性字段404以便于示例性管理员308分配严重性级别(例如高、中等、低、危急的、紧急的、严重的、最小的等),该严重性级别指示恶意软件安装在虚拟机202(图2)上的可能性。

[0043] 在所示出的示例中,提供类别字段405以指示与安全事件模式相关的资源的类型。例如,类别字段405可以指示特定的安全事件模式与存储器使用216(图2)相关。提供示例性条件字段406以便于示例性管理员308创建一个或多个条件语句,其定义与存储器使用216、储存盘使用218、网络使用220和/或硬件使用222(图2)相关的哪些条件在被满足时构成安全事件模式。在一些示例中,条件语句是布尔语句和/或阈值,与监控代理通过监控存储器使用216、储存盘使用218、网络使用220和/或硬件使用222而访问的性质有关。

[0044] 图5示出了示例性界面500,其用于定义图2和图3的示例性监控代理对安全事件模式的检测做出响应所使用的措施。在一些示例中,界面500由示例性安全事件管理器304(图3)提供。示例性界面500用于便于管理员(例如图3的管理员308)定义要由示例性安全事件处理机302(图3)响应于资源监控器300(图3)检测到安全事件模式而执行的措施。在所示出的示例中,基于严重性来定义要由安全事件处理机302执行的措施。例如,响应于检测到中等严重性安全事件模式,安全处理机302可以限制过程控制应用204(图2)向现场设备104发出命令的能力。在一些示例中,由安全处理机302执行的措施可以基于特定的安全事件模式。

[0045] 图6和/或图7中示出了表示用于实现图2和图3的示例性监控代理214的示例性方法的流程图。在该示例中,可以使用机器可读指令来实现方法,所述指令包括用于由处理器(例如在以下结合图8论述的示例性处理器平台800中所示的处理器812)执行的程序。程序可以体现在软件中,软件存储在有形的计算机可读储存介质上,例如CD-ROM、软盘、硬盘驱动器、数字多功能盘(DVD)、蓝光盘或与处理器812相关联的存储器,但整个程序和/或其部分可以替代地由除了处理器812以外的设备来执行,和/或体现在固件或专用硬件中。此外,尽管参考图6和/或图7中所示的流程图说明了示例性程序,但可以替代地使用许多实现示例性监控代理214的其它方法。例如,可以改变框执行的顺序,和/或可以改变、去除或组合所描述的一些框。

[0046] 如上所述,图6和/或图7的示例性方法可以使用编码指令(例如计算机和/或机器可读指令)来实现,编码指令存储在有形的计算机可读储存介质上,例如硬盘驱动器、闪存、只读存储器(ROM)、压缩盘(CD)、数字多功能盘(DVD)、高速缓存器、随机存取存储器(RAM)和/或任何其它储存设备或储存盘上,在其中以任意持续时间(例如在延长的时间段上、永久地、短暂情况、临时缓冲、和/或信息的缓存)存储了信息。如本文所使用,术语有形的计算机可读储存介质被明确地定义为包括任何类型的计算机可读储存设备和/或储存盘,排除传播信号并排除传输介质。如本文所使用的,“有形的计算机可读储存介质”和“有形的机器可读储存介质”可互换地使用。另外或替代地,图6和/或图7的示例性方法可以使用编码指令(例如计算机和/或机器可读指令)来实现,编码指令存储在非暂时性计算机和/或机器可读介质上,例如硬盘驱动器、闪存、只读存储器、压缩盘、数字多功能盘、高速缓存器、随机存取存储器和/或任何其它储存设备或储存盘上,在其中以任意持续时间(例如在延长的时间

段上、永久地、短暂情况、临时缓冲、和/或信息的缓存)存储了信息。如本文所使用的,术语非暂时性计算机可读介质被明确地定义为包括任何类型的计算机可读储存设备和/或储存盘,排除传播信号并排除传输介质。如本文所使用的,当在权利要求的前序中将短语“至少”用作过渡词时,它是开放式的,方式与词语“包括”是开放式的相同。

[0047] 图6是表示可以用于实现用以检测并响应安全事件的、图2和图3的监控代理的示例性方法的流程图。初始地,资源监控器300(图3)监控由执行过程控制应用204(图2)的虚拟机202(图2)对资源的使用(框602)。以下结合图7进一步论述在框602的监控对资源的使用。资源监控器300继续监控资源使用,直到已检测到潜在安全事件(框604)。资源监控器300向所检测到的潜在安全事件分配严重性级别(框606)。在一些示例中,基于在安全事件模式数据库306中所存储的安全事件模式来分配严重性级别。安全事件处理机302(图3)基于所分配的严重性级别来启动安全措施(框608)。在一些示例中,要执行的安全措施由管理员(图3)预定义。在一些示例中,安全事件处理机302基于所检测到的潜在安全事件的严重性来调整虚拟机202的完整性级别。资源监控器300确定是否要继续监控虚拟机202(框610)。如果要继续监控虚拟机202,则资源监控器300监控虚拟机202所使用的资源的使用,以检测潜在安全事件(框602)。否则,如果不继续监控虚拟机202,则方法600结束。

[0048] 图7是表示可以被执行以实现在图6的框602的安全事件检测的示例性方法的流程图。初始地,资源监控器300(图3)监控虚拟机202(图2)的存储器使用216(图2),并将该使用与安全模式相比较(框700)。资源监控器300确定存储器使用216是否匹配(例如满足条件、满足阈值等)安全事件模式数据库306(图3)中的安全事件模式(框702)。在一些示例中,将存储器使用216与安全事件模式数据库306中与如由图4的类别字段405所指示的存储器使用有关的安全事件模式相比较。如果资源监控器300确定存储器使用216匹配安全事件模式,则资源监控器300(例如向安全事件处理机302)指示已发生了潜在的与存储器有关的安全事件(框703)。

[0049] 资源监控器300监控虚拟机202的储存盘使用218(图2)(框706)。资源监控器300确定储存盘使用218是否匹配(例如满足条件、满足阈值等)安全事件模式数据库306中的安全事件模式(框708)。在一些示例中,将储存盘使用218与安全事件模式数据库306中与如由类别字段405所指示的储存盘使用有关的安全事件模式相比较。如果资源监控器300确定储存盘使用218匹配安全事件模式,则资源监控器300(例如向安全事件处理机302)指示已发生了潜在的储存盘安全事件(框709)。

[0050] 资源监控器300监控虚拟机202的网络使用220(图2)(框710)。资源监控器300确定网络使用220是否匹配(例如满足条件、满足阈值等)安全事件模式数据库306中的安全事件模式(框712)。在一些示例中,将网络使用220与安全事件模式数据库306中与如由类别字段405所指示的网络使用有关的安全事件模式相比较。如果资源监控器300确定网络使用220匹配安全事件模式,则资源监控器300(例如向安全事件处理机302)指示已发生了潜在的与网络有关的安全事件(框713)。

[0051] 资源监控器300监控虚拟机202的硬件使用222(图2)(框710)。资源监控器300确定硬件使用222是否匹配(例如满足条件、满足阈值等)安全事件模式数据库306中的安全事件模式(框716)。在一些示例中,将硬件使用222与安全事件模式数据库306中与如由类别字段405所指示的硬件使用有关的安全事件模式相比较。如果资源监控器300确定硬件使用222

匹配安全事件模式，则资源监控器300(例如向安全事件处理机302)指示已发生了潜在的与硬件有关的安全事件(框717)。方法700随后结束。

[0052] 图8是示例性处理器平台800的框图，其被构造为执行指令以实现图6和/或图7的方法以及图2和图3的监控代理214。例如，处理器平台800可以是服务器、个人计算机、工作站或任何其它类型的计算设备。

[0053] 所示示例的处理器平台800包括处理器812。所示示例的处理器812是硬件。在所示出的示例中，处理器812包括示例性资源监控器300、示例性安全事件处理机302和示例性安全事件模式管理器306。例如，处理器812可以由来自任何期望的系列或制造商的一个或多个集成电路、逻辑电路、微处理器或控制器来实现。

[0054] 所示示例的处理器812包括本地存储器813(例如高速缓存器)。所示示例的处理器812经由总线818与包括易失性存储器814和非易失性存储器816的主存储器相通信。易失性存储器814可以由同步动态随机存取存储器(SDRAM)、动态随机存取存储器(DRAM)、RAMBUS动态随机存取存储器(RDRAM)和/或任何其它类型的随机存取存储器设备来实现。非易失性存储器816可以由闪存和/或任何其它期望类型的存储器设备来实现。对主存储器814、816的访问可以由存储器控制器来控制。

[0055] 所示示例的处理器平台800还包括接口电路820。接口电路820可以由任何类型的接口标准来实现，例如以太网接口、通用串行总线(USB)和/或PCI高速接口。

[0056] 在所示出的示例中，一个或多个输入设备822连接到接口电路820。输入设备822允许用户将数据和命令输入到处理器812中。例如输入设备可以由音频传感器、话筒、摄像机(静止或视频)、键盘、按钮、鼠标、触摸屏、触控板、跟踪球、等电点(isopoint)和/或语音识别系统来实现。

[0057] 一个或多个输出设备824也连接到所示示例的接口电路820。输出设备824例如可以由显示设备(例如发光二极管(LED)、有机发光二极管(OLED)、液晶显示器、阴极射线管显示器(CRT)、触摸屏、触觉输出设备、打印机和/或扬声器)来实现。所示示例的接口电路820因而典型地包括图形驱动卡、图形驱动芯片或图形驱动处理器。

[0058] 所示示例的接口电路820还包括通信设备，例如发射器、接收器、收发器、调制解调器和/或网络接口卡，以便于经由网络826(例如以太网连接、数字用户线路(DSL)、电话线、同轴电缆、蜂窝电话系统等)与外部机器(例如任何种类的计算设备)交换数据。

[0059] 所示示例的处理器平台800还包括用于存储软件和/或数据的一个或多个大容量储存设备828。这种大容量储存设备828的示例包括软盘驱动器、硬盘驱动器、压缩盘驱动器、蓝光盘驱动器、RAID系统和数字多功能盘(DVD)驱动器。

[0060] 用以实现图6和/或图7的方法的编码指令832可以存储在大容量储存设备828、易失性存储器814、非易失性存储器816中和/或存储在可移动、有形的计算机可读储存介质(例如CD或DVD)上。

[0061] 尽管本文公开了某些示例性方法、装置和制品，但本发明的覆盖范围不限于此。相反，本发明覆盖所有正当地落入本发明的权利要求书的范围内的方法、装置和制品。

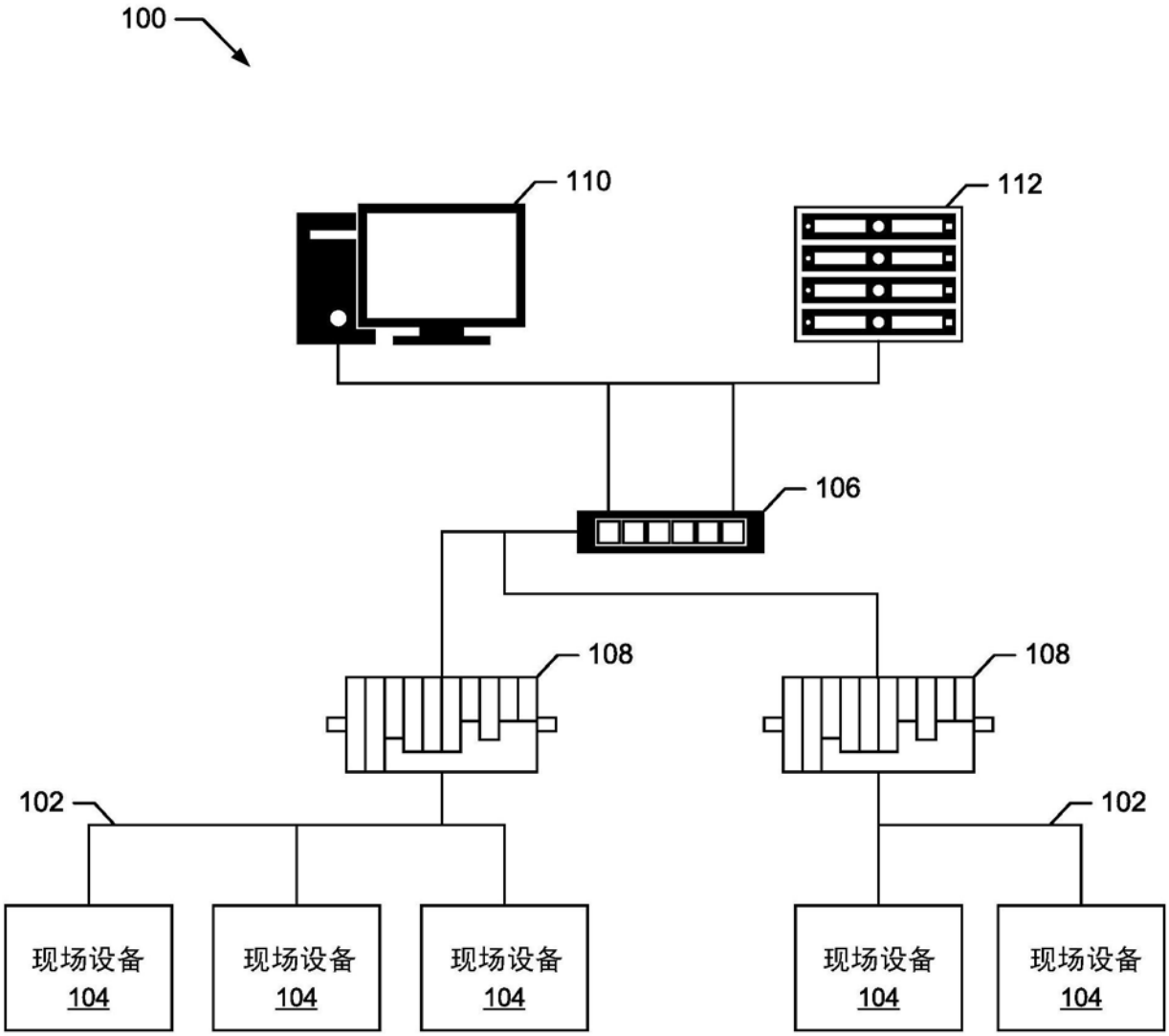

100
110
112
106
108
108
102
102
现场设备
104
现场设备
104
现场设备
104
现场设备
104
现场设备
104

图1

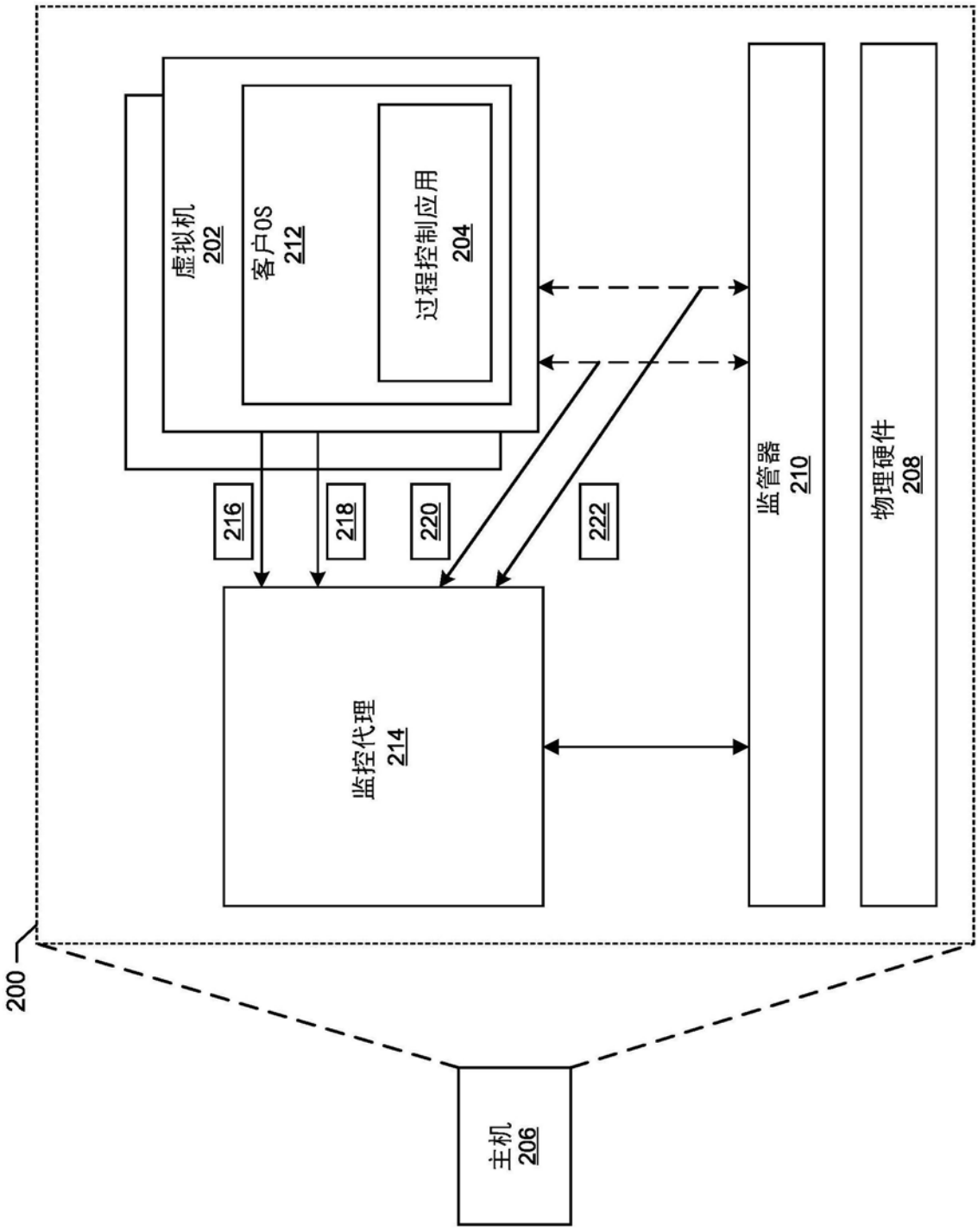

虚拟机
202
客户OS
212
过程控制应用
204
监管器
210
物理硬件
208
216
218
220
222
监控代理
214
200
主机
206

图2

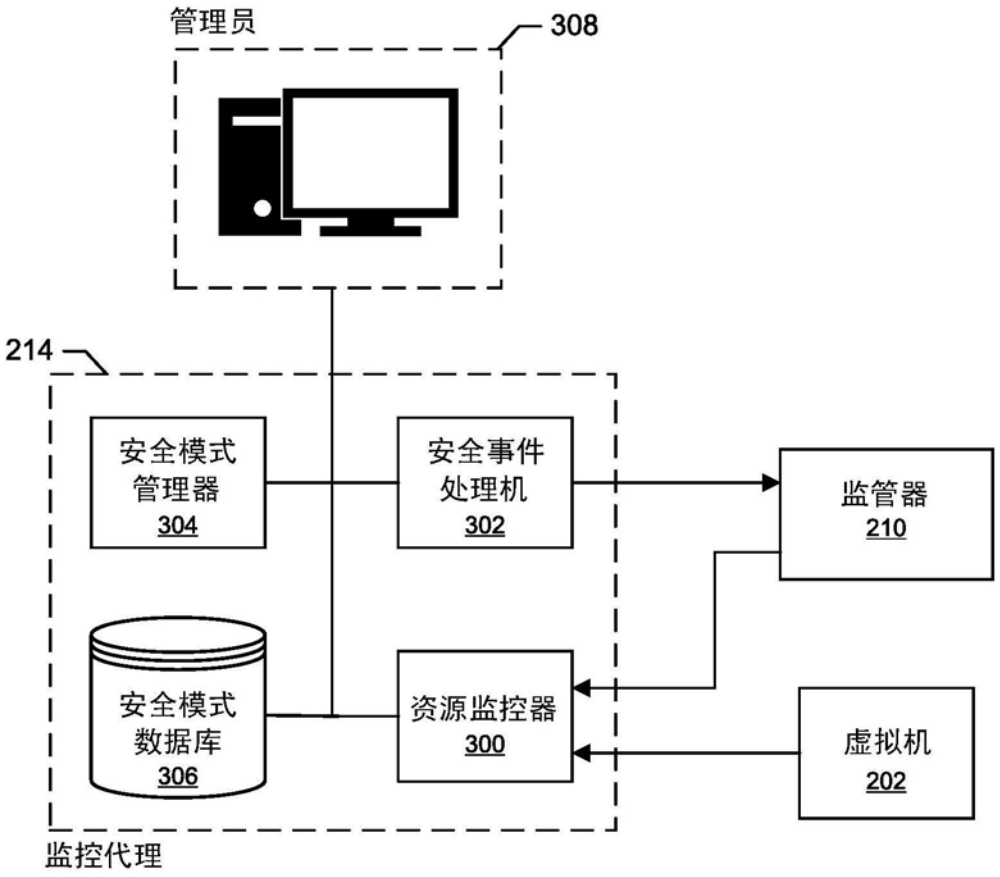

管理员
308
214
安全模式
管理器
304
安全事件
处理机
302
监管器
210
安全模式
数据库
306
资源监控器
300
虚拟机
202
监控代理

图3

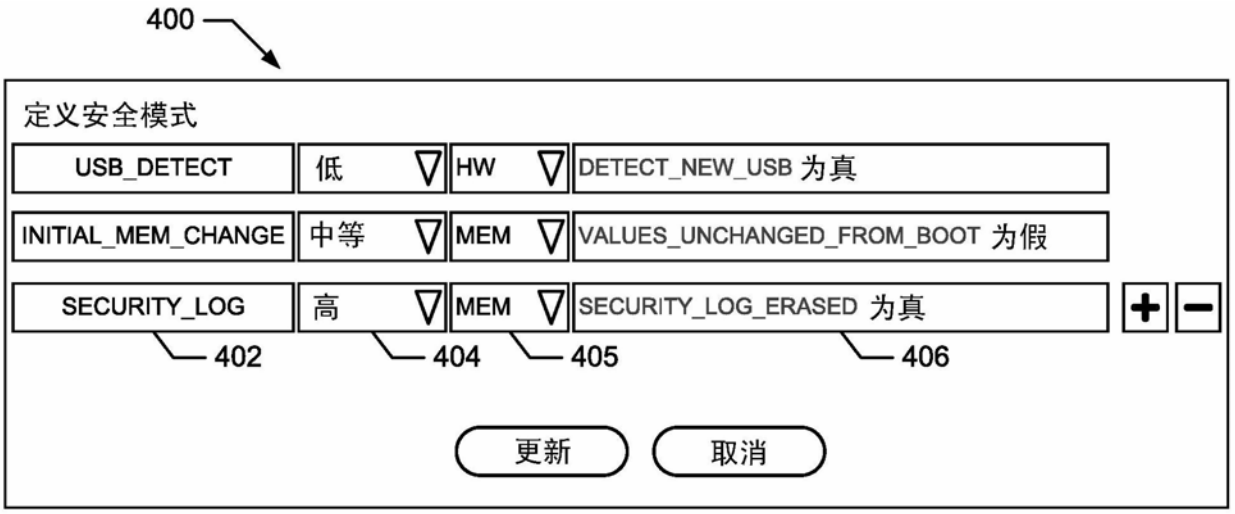

400
定义安全模式
USB_DETECT
低
HW
DETECT_NEW_USB 为真
INITIAL_MEM_CHANGE
中等
MEM
VALUES_UNCHANGED_FROM_BOOT 为假
SECURITY_LOG
高
MEM
SECURITY_LOG_ERASED 为真
402
404
405
406
更新
取消

图4

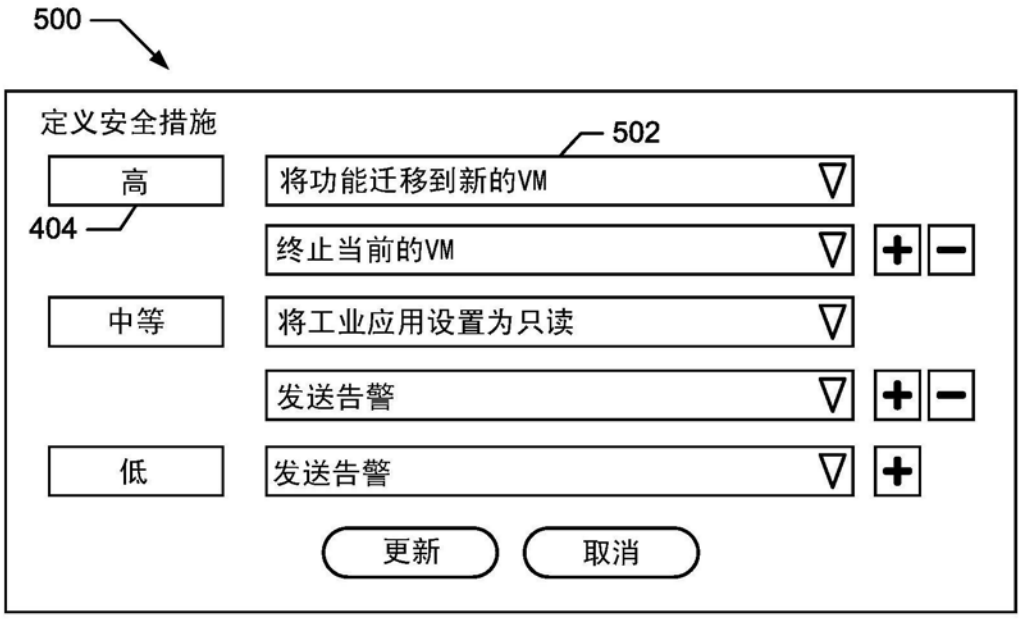

500
定义安全措施
502
高
404
将功能迁移到新的VM
终止当前的VM
中等
将工业应用设置为只读
发送告警
低
发送告警
更新
取消

图5

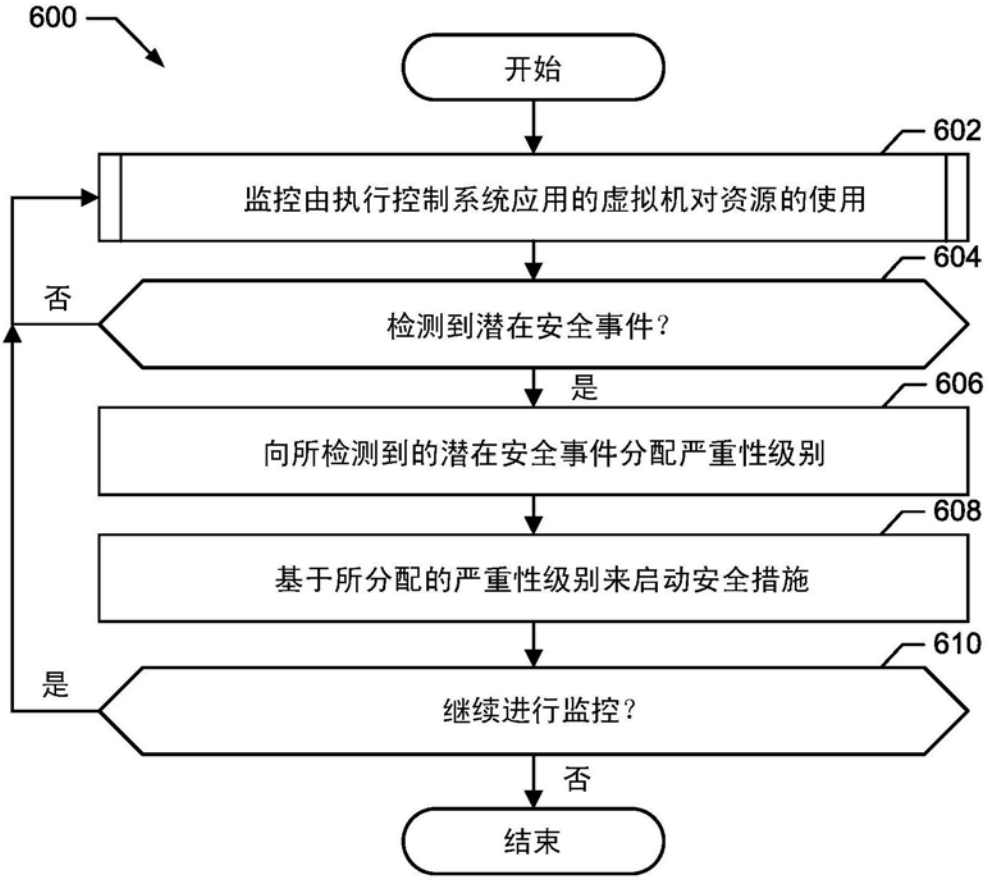

600
开始
602
监控由执行控制系统应用的虚拟机对资源的使用
604
否
检测到潜在安全事件?
是
606
向所检测到的潜在安全事件分配严重性级别
608
基于所分配的严重性级别来启动安全措施
610
是
继续进行监控?
否
结束

图6

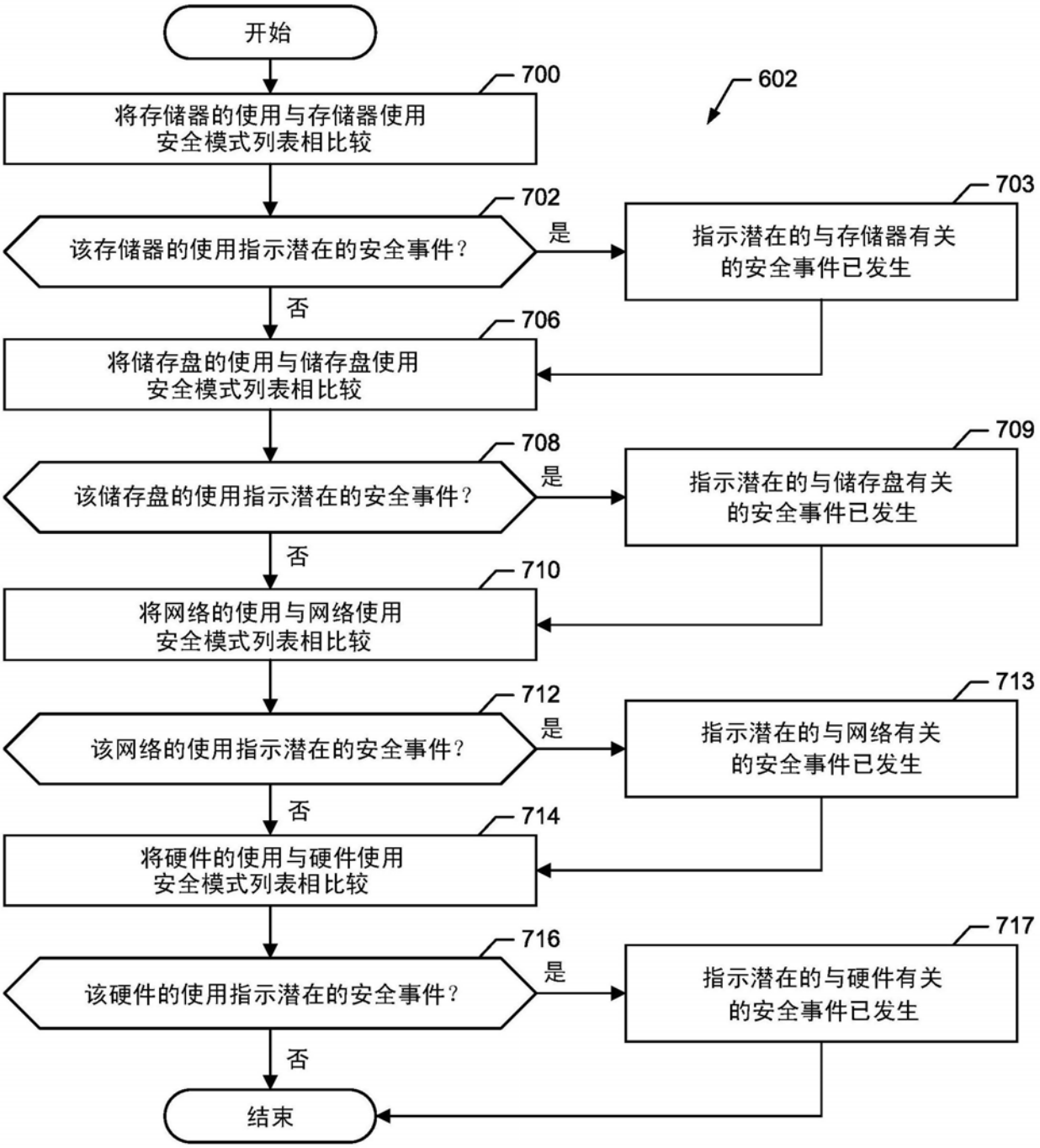

开始
700
将存储器的使用与存储器使用安全模式列表相比较
602
702
该存储器的使用指示潜在的安全事件？
是
703
指示潜在的与存储器有关的安全事件已发生
否
706
将储存盘的使用与储存盘使用安全模式列表相比较
708
该储存盘的使用指示潜在的安全事件？
是
709
指示潜在的与储存盘有关的安全事件已发生
否
710
将网络的使用与网络使用安全模式列表相比较
712
该网络的使用指示潜在的安全事件？
是
713
指示潜在的与网络有关的安全事件已发生
否
714
将硬件的使用与硬件使用安全模式列表相比较
716
该硬件的使用指示潜在的安全事件？
是
717
指示潜在的与硬件有关的安全事件已发生
否
结束

图7

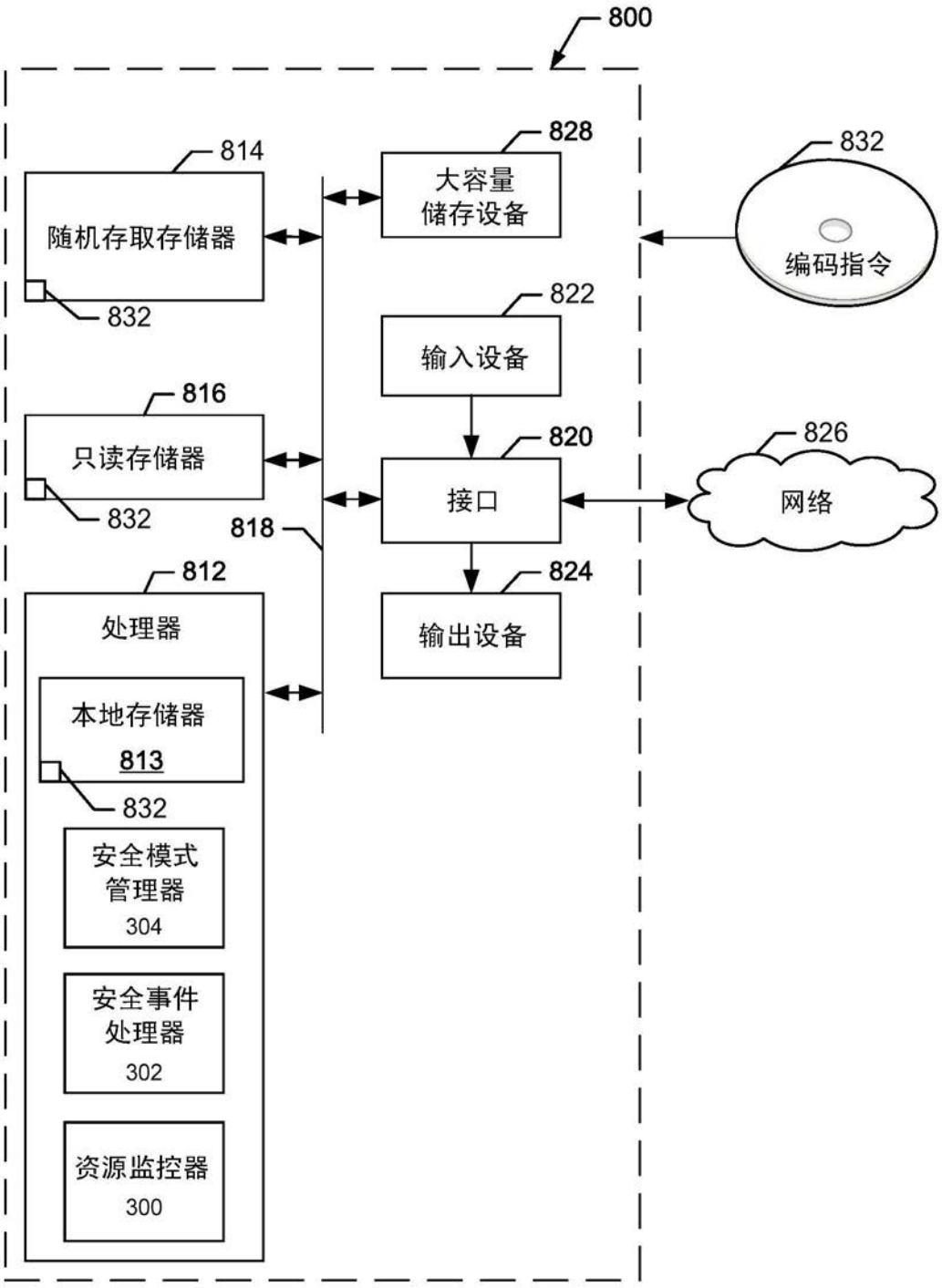

800
814
随机存取存储器
832
828
大容量
储存设备
832
编码指令
822
输入设备
816
只读存储器
832
820
接口
826
网络
818
812
处理器
824
输出设备
本地存储器
813
832
安全模式
管理器
304
安全事件
处理器
302
资源监控器
300

图8