(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103370717 A
(43)申请公布日 2013.10.23

(21)申请号 201180068132.2

(22)申请日 2011.12.22

(85)PCT申请进入国家阶段日
2013.08.21

(86)PCT申请的申请数据
PCT/US2011/067066 2011.12.22

(87)PCT申请的公布数据
WO2013/095596 EN 2013.06.27

(71)申请人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 M. 伯格

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张金金 汤春龙

(51)Int.Cl.
G06F 21/57(2013.01)

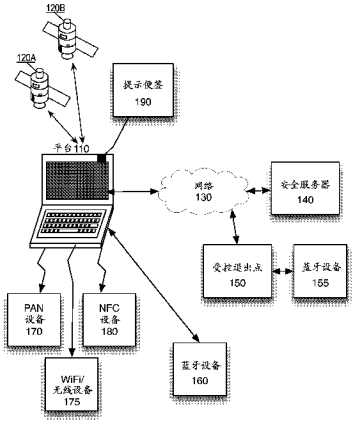
权利要求书2页 说明书21页 附图33页

(54)发明名称

始终可用的嵌入式盗窃反应子系统

(57)摘要

描述包括始终可用的盗窃保护系统的平台。在一个实施例中,平台包括:存储,其包括全盘加密;风险行为逻辑,用于在平台被布防时检测潜在问题;和核逻辑部件,提供用于在潜在问题指示盗窃怀疑时分析潜在问题并且触发安全动作逻辑来进行安全动作的逻辑。在一个实施例中,系统进一步包括:安全动作逻辑,用于将关于盗窃怀疑的告警发送到另一个设备,并且触发存储来对数据加密;以及加密逻辑,用于在平台处于关闭或低功率状态时对数据加密。



CN 103370717 A

1. 一种平台，包括始终可用的盗窃保护系统，所述平台包括：

存储，其包括全盘加密；

风险行为逻辑，用于在所述平台被布防时检测潜在问题；

核逻辑部件，提供用于在所述潜在问题指示盗窃怀疑时分析所述潜在问题并且触发安全动作逻辑来进行所述安全动作的逻辑；

所述安全动作逻辑用于将关于所述盗窃怀疑的告警发送到另一个设备，并且触发所述存储来对数据加密；以及

加密逻辑，用于在所述平台处于关闭或低功率状态时对所述数据加密。

2. 如权利要求 1 所述的平台，其进一步包括：

告警便签，其对任何未授权用户指示所述平台受到保护并且在怀疑盗窃时在没有移除电力源的情况下发送警报，所述便签设计成促使所述未授权用户将所述电力源断连，所述电力源的断连促使所述存储被加密，由此保护所述存储上的数据以免被未授权用户得到。

3. 如权利要求 2 所述的平台，其进一步包括：

模式指示器用户界面特征，用于在视觉上表示即将到来的告警的警示。

4. 如权利要求 1 所述的平台，其进一步包括：

撤防逻辑，用于对所述平台撤防，所述撤防逻辑触发所述加密逻辑来对数据解密。

5. 如权利要求 3 所述的平台，其中所述模式指示器包括发光二极管（LED）和音频输出中的一个或多个。

6. 如权利要求 1 所述的平台，其中所述低功率状态包括休眠状态。

7. 一种平台，包括始终可用的盗窃保护系统，所述平台包括：

存储，其包括全盘加密；

布防逻辑，用于对所述平台布防；

风险行为逻辑，用于在所述平台被布防时检测潜在问题；

安全动作逻辑，用于触发功率转变逻辑，来使所述平台转变到低功率状态，所述低功率状态通过对数据加密并且需要验证来访问所述平台而保护所述平台。

8. 如权利要求 7 所述的平台，其进一步包括：

对潜在盗窃者的通知，用于触发所述潜在盗窃者使所述平台掉电，以便保护所述平台。

9. 权利要求 8 所述的平台，其中所述通知包括以下中的一个或多个：告警便签、用于在视觉上表示即将到来的通知的警示的模式指示器、用于发出警示的音频输出。

10. 权利要求 7 所述的平台，其进一步包括：

撤防逻辑，用于对所述平台撤防，所述撤防逻辑触发所述加密逻辑来对数据解密。

11. 如权利要求 7 所述的平台，其中所述低功率状态包括休眠状态。

12. 如权利要求 7 所述的平台，其进一步包括：

撤防逻辑，用于使用户能够在所述安全动作逻辑触发所述功率转变逻辑之前对所述平台撤防。

13. 一种使用始终可用的安全系统来保护平台的方法，其包括：

响应于布防命令对平台布防；

监视所述平台来检测潜在问题；

响应于检测所述潜在问题，显示警示，其指示将发出警报，所述警示设计成提示盗窃者

使平台掉电；

响应于使所述平台掉电，通过对数据加密并且需要验证来访问所述平台而保护所述平台。

14. 如权利要求 13 所述的方法，其中所述警示包括以下中的一个或多个：警示便签、用于在视觉上表示即将到来的通知的警示的模式指示器、用于发出警示的音频输出。

15. 如权利要求 13 所述的方法，其进一步包括：

响应于撤防命令对所述平台撤防，所述撤防逻辑触发数据的解密。

16. 如权利要求 13 所述的方法，其中所述低功率状态包括休眠状态。

17. 如权利要求 13 所述的方法，其进一步包括：

使用户能够在响应于所述潜在问题而对数据加密之前对所述平台撤防。

始终可用的嵌入式盗窃反应子系统

技术领域

[0001] 本发明涉及安全性，并且更特定地涉及始终可用的嵌入式盗窃反应系统。

背景技术

[0002] 全盘加密(FDE)技术设计成万一平台被偷则保护数据。这样的技术可以是基于软件或基于硬件的。这些技术依靠终端用户在从某些状态启动时提供密码以便解锁对存储在设备上的数据的访问。然而，FDE 仅在计算机尚未被解密时(例如，在它启动时)保护计算机的静态数据。

[0003] 另一个盗窃保护系统是基于软件的告警机构。基于软件的告警机构提供即刻告警能力以便防止盗窃。问题是这些机制易受盗窃者基于软件的攻击(例如，关掉 WIFI 无线电)、盗窃者简单的基于硬件的攻击(例如，按压平台的电力源按钮持续 4 秒)。

[0004] 另一个盗窃保护系统依靠分立硬件部件，其包含基于触发的告警机构。对此的示例是类似基于密钥的盘的部件，其插入 PC。然而，这需要额外的插入设备，并且仅在计算机系统已经启用时起作用。另外，盗窃者可以容易地破坏这样的部件同时保持平台未被动过，例如将它浸入一杯水中或用锤子敲打它。

附图说明

[0005] 本发明通过示例而非限制的方式在附图的图中图示，并且在图中类似的数字指代相似的元件并且其中：

图 1 是环境中的平台的一个实施例的图。

[0006] 图 2A 是实现本发明的安全特征的平台的一个实施例的框图。

[0007] 图 2B 是可与平台关联的额外系统的一个实施例的框图。

[0008] 图 3 是示出在平台内被单独供电的子系统的一个实施例的图。

[0009] 图 4 是平台的一个实施例的图。

[0010] 图 5 是平台的另一个实施例的图。

[0011] 图 6A 是电池移除保护系统的一个实施例的图。

[0012] 图 6B 是电池移除保护系统的另一个实施例的图。

[0013] 图 7 是平台的状态的一个实施例的状态图。

[0014] 图 8 是示出状态的另一个实施例的第二状态图。

[0015] 图 9 是示出的每个状态时的动作表的一个实施例。

[0016] 图 10 是功率状态图，其示出系统的功率状态的一个实施例。

[0017] 图 11A 是始终打开始终可用的环境中使用保护系统的一个实施例的综览流程图。

[0018] 图 11B 是系统可遇到的各种情形以及在平台、服务器和用户携带设备处的反应的一个实施例的表。

[0019] 图 12 是对系统布防的一个实施例的流程图。

[0020] 图 13 列出示范性手动或自动布防机制。

[0021] 图 14 是对保护系统撤防的一个实施例的流程图。

[0022] 图 15 列出示范性手动或自动撤防机制。

[0023] 图 16 是使用用户携带设备用于基于网络的自动布防和撤防的一个实施例的流程图。

[0024] 图 17 是使用启用双向蓝牙的设备用于布防 / 撤防和通知服务的一个实施例的流程图。

[0025] 图 18 是在接近性进一步与运动数据耦合时基于接近性的布防和撤防的一个实施例的流程图。

[0026] 图 19 是使用近场通信用于对系统布防和撤防的一个实施例的流程图。

[0027] 图 20 是用于保护系统的静态数据的功率操作的一个实施例的流程图。

[0028] 图 21 是对于用户的透明启动 / 恢复(其面对盗窃者或未授权用户是安全的)的一个实施例的流程图。

[0029] 图 22 是多 kill pill 系统的一个实施例的图。

[0030] 图 23 是防盗机构部件的电力管理的一个实施例的流程图。

[0031] 图 24 示出要确认的布防模式和关联的输入类型的示范性列表。

[0032] 图 25 是保护性超驰(override)机制的一个实施例的流程图。

[0033] 图 26 将防盗机构的超驰机制与其他可能的超驰机制比较。

[0034] 图 27A 和 27B 是平台的联合预备和它与用户配置共存的一个实施例的流程图。

[0035] 图 28 是在受监视环境中平台安全性的一个实施例的流程图。

[0036] 图 29 是可用作平台的计算机系统和 / 或配对设备的一个实施例的框图。

[0037] 特定实施方式

公开了这样的技术,其采用嵌入的、安全且始终可用方式对盗窃企图提供反应。在一个实施例中,该技术在所有平台功率状态中操作,只要存在连接到平台的足够大的电力源即可。在一个实施例中,该技术不允许有基于软件的盗窃者攻击或恶意软件。该技术还防止基于硬件的攻击。

[0038] 本发明的实施例的下列详细描述参考附图,其中类似的数字指示相似的元件,其通过图示的方式示出实践本发明的特定实施例。这些实施例的描述足够详细地使本领域内技术人员能够实践本发明。本领域内技术人员理解,可利用其他实施例并且可做出逻辑的、机械的、电气的、功能的和其他改变而不偏离本发明的范围。因此,下列详细说明不是从限制性意义来对待,并且本发明的范围仅由附上的权利要求限定。

[0039] 图 1 是环境中的平台的一个实施例的图。在一个实施例中,平台 110 可以是膝上型计算机。平台 110 可以是另一个类型的计算设备,例如网络、平板计算机、移动设备或另一个类型的计算设备。在一个实施例中,平台 110 包括使平台能够连接到网络 130 的网络连接。

[0040] 在一个实施例中,平台 110 可与安全服务器 140 或经由网络 130 与另一个设备通信。在一个实施例中,通过例如 WiFi 网络、有线网络或另一个类型的网络等网络接口访问网络 130。

[0041] 在一个实施例中,平台 110 直接耦合于个人区域网(PAN)设备 170。该个人区域网可以是蓝牙网络。从而,蓝牙设备 160 可以连接到平台 110。

[0042] 在一个实施例中，平台 110 与近场通信（NFC）设备 180 配对。该 NFC 设备可以是徽章、RFID、移动电话中的芯片或便签或由授权用户所携带的其他系统（其包括 NFC 芯片）。相似地，无线 /WiFi 设备可直接或通过网络 130 而耦合于平台 110。

[0043] 在一个实施例中，如在本领域内已知的，平台 110 可能够通过 GPS 120A、120B 接收位点数据。在一个实施例中，平台 110 可从网络连接（使用无线集线器数据）、从蜂窝网络三角网、从加速器数据（未示出）或从这些和 / 或其他位点数据指示器的组合获得它的数据。

[0044] 在一个实施例中，在使用平台 110 的环境中可存在受控退出点 150。受控退出点 150 在安全服务器 140 能够在怀疑平台盗窃时将告警发送给受控退出点 150 的环境中存在。受控退出点 150 可以是具有可以被告警的守卫、可以被锁住的闸或门的退出点，或具有不同类型的退出控制机制的退出点。在一个实施例中，受控退出点可包括蓝牙设备 155，其可以检测平台到退出点 150 的接近性（通过检测平台的蓝牙设备 160）。

[0045] 在一个实施例中，平台 110 可包括提示便签 190。该提示便签 190 试图保护平台上的数据，即使平台被偷也如此。大部分盗窃者是为了平台本身来偷取平台，而不是为了它上面的数据。因此，在包括平台上的全盘加密的系统中，经由便签 190 来使盗窃者察觉平台将发送告警，除非所有的电力源立即被移除。例如，便签 190 可显示“该平台包含防盗响应嵌入式子系统。在盗窃时，闪光 LED 将指示向平台的拥有方将告警该盗窃。为了停止告警，移除 AC 连接和电池。”

这将提示理性的盗贼取出所有可见电源－ AC 和主电池－从而抑制告警。取出电源的动作将使平台处于 G3 状态（机械关闭）。因为 HDD/SSD 失去电力，它的数据现在受到保护。在平台的下一次启动时，全盘加密将启用，并且数据将仅通过在密码提示处成功输入密码而可访问。注意在假肯定的情况下，当平台怀疑有盗窃者但它实际上是授权用户时，不发生功率转变，并且因此没有扰乱过程或丢失数据这样的问题。该技术方案可能尤其与市场段相关，在这些市场段中，平台上数据泄漏的成本可能达到平台资产更换成本的许多倍。

[0046] 系统对平台 110 提供始终打开始终可用的安全系统，其向系统 110 提供保护。在一个实施例中，平台 110 还可与 PAN 设备 170 配对，由此对平台 110 和 PAN 设备 170 两者提供保护。

[0047] 图 2A 是实现本发明的安全特征的平台的一个实施例的框图，而图 2B 是相关设备的一个实施例的框图。在一个实施例中，安全系统 210 包括模式逻辑 212。状态逻辑 212 管理机构的模式。在一个实施例中，机构的模式包括未布防（无保护）、布防（受保护）、布防进行中（未布防与布防之间的过渡阶段）以及怀疑（布防，并且怀疑有盗窃）。在一个实施例中，模式指示器 UI 特征 215 在视觉上指示平台的当前模式。在一个实施例中，模式指示器 UI 特征 215 是 LED，其通过闪烁方式来指示模式。在一个实施例中，模式指示器 UI 特征 215 是多颜色 LED，其通过颜色来指示模式。可使用在视觉上指示当前模式的备选方法。

[0048] 电力源 214 可包括 AC（交流电）以及电池电力。在一个实施例中，安全系统 210 可包括电池访问控制器 244，用于控制对电池盒的访问，如将在下文更详细描述的。

[0049] 在一个实施例中，安全系统 210 包括电力管理逻辑 216。该电力管理逻辑 216 控制到各种元件（可与安全系统 210 关联）的电力。在一个实施例中，为了将功耗减少至较低功率状态（例如，睡眠和休眠）中，系统可选择性地对安全系统 210 的元件的子集供电。这将在下文更详细地描述。在一个实施例中，功率转变逻辑 246 通过多个功率状态来控制平台。

在一个实施例中，功率状态包括 S0（打开）至 S5（关闭）。功率转变逻辑 246 使系统在功率状态（唤醒）以及一个或多个睡眠状态（休眠和关闭）之间移动。

[0050] 核逻辑部件 218 是与安全系统 210 关联的处理器。在一个实施例中，核逻辑 218 从接口 220 接收数据。接口 220 可包括以下中的一个或多个：蓝牙传感器 / 通信器 222、NFC 读取器 224、运动传感器 226、GPS 接收器 227、RSSI 传感器 228、手动控制 229 和手动布防机构 218。在一个实施例中，这些接口 220 用于检测用户输入、盗窃风险和可影响安全系统 210 的其他事件。

[0051] 在一个实施例中，配对逻辑 240 用于在安全系统 210 与另一个设备之间设置配对。该另一设备可以是移动设备，其包括蓝牙连接、NFC 设备或可用于对安全系统 210 布防 / 撤防、通知安全系统 210 或用别的方式与它交互的另一个设备。在一个实施例中，配对使用配对设备的唯一标识来确保授权 NFC 设备、蓝牙设备或其他设备类型被使用。

[0052] 在一个实施例中，系统包括布防逻辑和撤防逻辑 230。该布防 & 撤防逻辑 230 使平台从未布防模式转变到布防模式，并且反之亦然。在一个实施例中，该布防 & 撤防逻辑 230 还对布防进行中模式负责。在一个实施例中，布防 & 撤防逻辑 230 将模式信息传送到模式逻辑 212 和核逻辑部件 218。在一个实施例中，当安全系统 210 怀疑有盗窃时，存储 / 加密逻辑 242 对平台上的数据加密来阻止访问平台。

[0053] 当平台处于布防或布防进行中模式时，风险行为逻辑 232 使用来自接口 220 的数据来检测风险行为。在一个实施例中，风险行为逻辑 232 向核逻辑部件 218 传达检测的风险因素。

[0054] 当核逻辑部件 218 基于来自风险行为逻辑 232 的信息而确定设备处于风险情形中时，安全动作逻辑 250 采取安全动作。在一个实施例中，安全动作逻辑 250 可利用通信逻辑 252 来将消息发送到用户携带设备 270、安全服务器 280 或另一个设备。在一个实施例中，到用户携带设备 270 或安全服务器 280 的网络通信采取报告存在或接近性的形式。在一个实施例中，该报告的缺乏构成怀疑盗窃。安全动作逻辑 250 还可包括音频输出 254，用于发出音频警报。在一个实施例中，安全动作逻辑 250 还可包括 kill pill 256。kill pill 256 致使平台不能操作。在一个实施例中，它还破坏平台上的数据。在一个实施例中，kill pill 256 是在平台内自动实现的自 kill pill。在一个实施例中，kill pill 256 由用户授权，如将在下文描述的。在一个实施例中，kill pill 256 通过服务来授权。在一个实施例中，存储 / 加密 242 在 kill pill 256 被调用时删除数据。在一个实施例中，安全动作逻辑 250 可触发功率转变逻辑 246 来使系统转变到不同的功率状态。

[0055] 配置逻辑 238 配置安全系统 210 的设定。在一个实施例中，配置逻辑 238 具有用户可修改和管理员可修改的部分。

[0056] 网络连接 236 用于将数据发送到安全服务器 280 和 / 或用户携带设备 270。

[0057] 图 2B 是可与平台关联的额外系统的一个实施例的框图。在一个实施例中，用户携带设备 270 与安全系统 210 配对。配对逻辑 272 处理对用户手持设备 270 的配对。告警逻辑 274 使平台能够经由 SMS、MMS、蓝牙、个人区域网（PAN）或另一个告警机构将告警发送给用户。在一个实施例中，告警逻辑 274 将基于缺少来自平台的通信而向终端用户提供告警。在一个实施例中，接近性逻辑 276 在双向监视情形中监视平台的接近性。

[0058] 安全服务器 280 是安全系统 210 可向其发送数据的服务器。在一个实施例中，安

全服务器 280 包括监视器 282，用于接收来自平台的数据。在一个实施例中，监视器 282 接收来自平台的告警。服务器 280 包括 ping 接收器 / 计时器 286，一旦接收到指示该平台正被怀疑有盗窃的初始消息，该 ping 接收器 / 计时器 286 监视来自平台的后续消息。这确保了如果盗窃者成功地停用平台并且阻止它发出后续消息，则响应被执行。在一个实施例中，安全服务器 280 包含或具有到无线 AP 数据库 292 的访问，该无线 AP 数据库 292 可以有助于将接收的关于无线接入点（例如，BSSID 和 RSSI）的原始信息转化成位点信息。在一个实施例中，安全服务器 280 包含或具有到平台 ID 数据库 294 的访问，该平台 ID 数据库 294 将平台的平台 ID（其报告它的机制模式）映射到用户特定信息。平台 ID 数据库可以用于采取用户特定策略决定或告警特定用户。在一个实施例中，安全服务器 280 包含告警日志 296，其可以有助于 IT 基于先前与平台的通信而确定平台上被偷的数据是否受到保护。该信息可用于触发远程 kill pill。

[0059] 在一个实施例中，平台 210 将移动信息从运动传感器 226 和 / 或 BSSID 和 RSSI 传感器 228 或 GPS 接收器 227 发送到安全服务器 280。由移动评估器 284 评估该移动信息来确定平台是否被偷。如果是这样的话，安全服务器 280 可经由告警逻辑 290 发送告警。在一个实施例中，安全服务器 280 还具有对于退出控制系统 288 的消息传递。退出控制系统 288 在怀疑平台盗窃时将消息发送到受控退出点。受控退出点可以是具有可以被告警的守卫、可以被锁住的闸或门的退出点，或具有不同类型的退出控制机制的退出点。当从安全服务器 280 接收消息时，出口被锁住并且 / 或守卫被告警，以他们能够搜查。

[0060] 图 3 是示出在平台内被单独供电的子系统的一个实施例的图。在一个实施例中，安全系统在 OEM（原始设备制造商）板 310 上实现。在一个实施例中，该 OEM 板 310 内置到平台内。在一个实施例中，OEM 板 310 是电路板（未另外示出）的一部分。通过使安全系统在 OEM 板 310 中实现，系统通过在原始硬件内建立防御而确保标准硬件和软件攻击无法起作用。

[0061] 在一个实施例中，板 310 包括防盗机构处理器 & 核子系统 330。该防盗机构处理器 & 核子系统 330 实现上文描述的逻辑。

[0062] 防盗机构处理器 & 核子系统 330 耦合于布防 / 撤防开关 320 和 WiFi/ 蓝牙 340。子系统 330 还从加速计 380 和 NFC 读取器 390 接收数据。

[0063] 硬件 RF kill 开关 360（其在许多设备中存在）具有 RF kill 超驰 335。这使防盗机构处理器 & 核子系统 330 能够超驰开关 360。布防 / 撤防开关 320 经由 GPIO 而直接耦合于核 330。加速计 380 直接耦合于核 330。NFC 390 耦合于核 330。OEM 嵌入式控制器 350 耦合于电力源 355 和 LED 370。

[0064] 在一个实施例中，OEM 板 310 提供从核子系统 330 到用于撤防或安全动作的每个外设（例如 WiFi/ 蓝牙 340、加速计 380、NFC 390 和其他）的安全路径。在一个实施例中，从核逻辑 330 到外设 340、380、390 的路径使用专用总线。这意味着另一个实体干扰业务、监视机密或导致拒绝服务是不可能的。在一个实施例中，控制器本身是安全的，使得没有人可以侵入它们。这确保没有人可以在这些控制器上对未授权或列入黑名单的图像进行固件更新、没有人可以使这些控制器挂起，等。

[0065] 在另一个实施例中，在核子系统 330 与外设之间可存在验证（非专用）连接，来代替专用连接。

[0066] 在另一个实施例中，在核子系统330与外设之间可存在加密(非专用)连接，来代替专用连接。这确保消息的目标知道消息不能被任何人读取。

[0067] 在另一个实施例中，在核子系统330与外设之间可存在验证和加密的连接，来代替专用连接。

[0068] 在一个实施例中，每个外设与核系统之间的连接类型可取决于该外设与核子系统之间的处理和数据交换的类型。例如，在一个实施例中，NFC读取器390读取标签，并且核子系统330进行比较来确保NFC设备被授权。在这样的情况下，核系统330与NFC读取器390之间的连接在不是专用时应该被验证和加密。另一方面，如果NFC读取器390在它的侧上进行处理并且仅将OK/Not OK消息发送到核子系统330，连接应该被验证，但不必加密，因为没有传递机密数据。加速计380例如处于拒绝服务攻击的风险中。如果盗窃者设法导致拒绝服务(或干扰消息)，则系统无法成功地检测平台已经被盗窃者移动。因此，核系统330与加速计380之间的连接应该是专用的。

[0069] 图4是平台的一个实施例的图。在图4中示出的示范性实施例中，各种元件耦合于OEM嵌入式控制器450，而不是核430与那些元件之间直接连接。在一个实施例中，核430直接耦合于WiFi/蓝牙440和NFC读取器490。其他元件通过嵌入式控制器450而耦合。在一个实施例中，嵌入式控制器450超驰硬件RF kill开关。

[0070] 图5是平台的另一个实施例的图。该实施例使用高效电力设计。OEM嵌入式控制器550控制通向FET 585、595、545的电力轨。

[0071] 在一个实施例中，布防/撤防机构520是机械开关，并且从而不需要驻留在由OEM嵌入式控制器550控制的电力轨上。

[0072] 在一个实施例中，WiFi和蓝牙设备540用作布防/撤防的触发器。因此，当可接收布防或撤防信号时，应该对WiFi和/或蓝牙接收器供电。WiFi设备还可采用怀疑模式提供告警，从而在怀疑模式中，OEM控制器550对WiFi和/或蓝牙供电。

[0073] NFC 590是开始撤防过程的备选方法，从而，在可发生撤防时将电力供应给NFC 590。

[0074] 下文的表图示在什么时间对哪些元件供电的一个实施例。在一个实施例中，OEM嵌入式控制器550选择性地向WiFi、蓝牙、加速计和NFC提供电力。X标记示出元件中的每个被供电所针对的动作。

	触发完成布防	触发检测盗窃事件	用于资产保护的设备	触发开始撤防
WiFi	X		X	X
蓝牙	X			X
加速计		X		
NFC				X

[0075] 图6A是电池移除保护系统的一个实施例的图。通过阻止电池移除，系统消除了盗窃者移除对平台的所有主要电力源的机会，使得平台可以完成它的保护性活动。

[0076] 在一个实施例中，防盗核逻辑子系统610将它的数据传递到模式解码逻辑620。电池640受到螺线管630的保护。当设备模式处于布防或怀疑模式中时，螺线管630使电池盒保持关闭，从而迫使电池640仍然附连。即使在移除外部电力时，螺线管630仍然关闭。这样，当盗窃者试图移除电池640时，它被锁住并且无法被移除。然而，授权用户或管理员(其可以对平台撤防)可以毫不费力地移除电池640。

[0077] 在一个实施例中，为了将螺线管功耗降至最小值，也可以存在电池机械闩锁 645，使得如果机械闩锁 645 闭合或螺线管 630 被激活，电池 640 无法被移除，并且只要机械闩锁闭合，螺线管 630 就不被激活。

[0078] 图 6B 是电池移除保护系统的另一个实施例的图。核子系统 650 向 OEM 控制器 670 提供模式消息。当设备处于布防或怀疑模式时，OEM 控制器 670 向螺线管 680 提供信号以锁定盒来保护电池 690。在一个实施例中，为了使螺线管功耗降至最小值，也可以存在电池机械闩锁 695，使得如果机械闩锁 695 闭合或螺线管 680 被激活，电池 690 无法被移除，并且只要机械闩锁 695 闭合，螺线管 630 就不被激活。

[0079] 图 7 是平台的模式的一个实施例的模式图。在一个实施例中，该模式包括未布防 710、布防进行中 730、布防 750 和怀疑 770 模式。

[0080] 在未布防模式 710 中，平台不受保护或未被锁住，并且数据被加密。当授权用户利用平台时，即是该模式。在一个实施例中，当用户将开关设置到布防位置或用别的方式起动平台的布防时，平台从未布防模式 710 转变到布防进行中模式 730。在一个实施例中，开关可以是手动开关。在一个实施例中，开关可以是软开关、键盘上的键的组合或另一个类型的手动激活。

[0081] 在系统完成布防的同时，布防进行中 730 模式是中间阶段。在一个实施例中，平台仍然处于布防进行中模式 730 直到完成布防。一般，布防由于不能完成保护策略所指定的一个或多个步骤(例如，当保护策略请求对服务器的告警时不能连接到告警服务器)而无法完成。在任一情况下，系统可告警授权用户 / 管理员布防无法完成。在一个实施例中，用户可在平台处于布防进行中模式 730 时在没有验证的情况下对平台撤防，来返回未布防模式 710。一旦完成布防，平台处于布防模式 750。

[0082] 在一个实施例中，在布防模式 750 中，平台受保护。这可包括万一平台相继移到怀疑模式则对平台上的数据加密的要求。它包括对平台撤防以便在没有发出告警的情况下访问数据或取数据的要求。它还意指安全系统正监视平台来检测可触发某些响应的任何可疑活动。当接收撤防指令时，系统从布防模式 750 转到未布防模式 710。在一个实施例中，撤防需要授权用户存在的指示。

[0083] 当处于布防模式 750 中时，如果系统接收盗窃的指示，例如可疑交互，系统移到怀疑模式 770。在怀疑模式 770 中，系统通过进行安全动作而作出响应。在一个实施例中，系统将告警发送给用户和 / 或服务器。在一个实施例中，系统保护系统的静态数据。在一个实施例中，如果释放引起怀疑的某些触发，系统可以从怀疑模式 770 返回布防模式 750。例如，平台可返回允许的区域。在一个实施例中，如果持续一定时段地未检测到额外的可疑活动，可释放触发。在一个实施例中，不允许触发释放，并且用户必须明确地对设备撤防来使它从怀疑模式移走。

[0084] 当设备处于怀疑模式 770 中时，用户还可对设备撤防，从而使它移到未布防模式 710。在一个实施例中，通过备选机构，授权用户或管理员还可使用超驰来从怀疑 770 模式移到未布防模式 710，或从布防模式 750 通过怀疑模式 770 到未布防模式 710。这实现了如果用户的密码或链接设备丢失或如果链接设备出故障或失去电力的话则系统恢复。

[0085] 图 8 是第二模式图，其示出模式的另一个实施例。如可以看到的，存在相同的四个模式。然而，在该示例中，来自链接个人区域网(PAN)设备的接近性信息用于激活系统。在

一个实施例中，PAN 设备是移动电话，其包括蓝牙配对能力。

[0086] 如示出的，当平台是静止的并且授权用户接近平台时，它不怀疑盗窃，并且仍然处于未布防模式 810。在一个实施例中，用户起动“布防进行中”模式，其开始监视授权用户到平台的接近性。

[0087] 如果失去设备接近性，系统从布防进行中模式 830 移到布防模式 850。一旦处于布防模式 850，当平台是静止的并且终端用户远离平台时，它不怀疑盗窃。然而，当平台是静止时，终端用户远离平台，并且它被移动，平台怀疑盗窃。这促使模式移到怀疑 870。

[0088] 在一个实施例中，当平台在靠近配对设备（例如，与授权用户）的同时移动（运送中）时，它不怀疑盗窃，不管终端用户是否使它移动。在一个实施例中，模式然后仍然处于布防进行中模式 830。

[0089] 然而，当平台与用户一起移动（运送中）并且有人将它带离用户而超过蓝牙接近极限时，系统认识到已经失去蓝牙接近性，并且移到布防模式 850。由于移动（这促使它怀疑盗窃），它自动移到怀疑模式 870。

[0090] 在一个实施例中，当平台与终端用户一起移动（运送中）并且终端用户将它放下并且远离它而移动时，平台将不怀疑盗窃。然而，系统将转变到布防模式 850。那时，如果有除终端用户以外的人将它拾起，平台怀疑盗窃，并且转变到怀疑模式 870。这在发生移动而之前没有重新获取用户的设备接近性时出现。在一个实施例中，如果用户配置蓝牙设备以在平台失去蓝牙接近性时告警用户，蓝牙设备将在失去接近性时将告警用户。

[0091] 如在上文关于图 7 指出的，系统可提供超驰，以及撤防能力和触发释放。

[0092] 在一个实施例中，当配对的蓝牙设备接近时，系统处于布防模式 830，而不是布防进行中模式 850。从布防模式 850 移到怀疑模式 870 的触发是平台远离静止配对设备的移动（经由接近性失去的检测），或配对设备从静止平台的移动。

[0093] 图 9 是在示出的每个模式时的动作表的一个实施例。在一个实施例中，存在 LED（发光二极管）或相似的视觉模式指示器。在一个实施例中，LED 示出模式（例如，未布防、正布防、布防、怀疑）。LED 可具有不同的颜色，或对于各种模式的闪光 / 发光样式或强度。

[0094] 系统在它进入各种模式时发送各种包。在一个实施例中，当它进入未布防模式时，它将撤防包发送到服务器，可已经告警该服务器该平台被布防。在一个实施例中，当系统处于布防进行中模式时，将初始连接发送到服务器。在一个实施例中，在布防模式中，将布防 ping 发送到服务器。如果系统进入怀疑模式，发送关于怀疑的信息。在一个实施例中，信息可包括平台的状态和环境指标，例如附近无线接入点的 RSSI、加速计数据、蓝牙接近性数据、数据保护策略，等。

[0095] 系统的配置实现对系统设定的改变。在未对系统布防时将配置解塞，并且在对系统布防或系统正怀疑时将配置阻塞。当在布防进行中时，系统处于配置阻塞中。在一个实施例中，任何时候模式不是未布防，都使配置阻塞。

[0096] 转变计时器用于监视功率状态之间的转变。在系统未处于怀疑模式时取消该转变计时器，因为系统直到接收怀疑触发时才转变出该模式。当系统未处于怀疑模式时，取消转变到休眠功率状态。在怀疑模式中，转变计时器用于使系统转变到休眠状态。在休眠状态中，利用全盘加密在系统上对数据加密，并且需要全盘加密密码来访问数据。因此，使平台转变到休眠功率状态提高对平台的保护。然而，到休眠状态的转变取决于来自 OS 软件或

BIOS 的帮助。转变计时器用于在 BIOS 或 OS 软件无法完成转变到休眠时实现保护。如果到休眠的转变失败，防盗机构可以迫使机构掉电，这不取决于 OS 软件或 BIOS 帮助。该操作还将使系统处于其中它的静态数据被加密的模式。

[0097] 图 10 是功率状态图，其示出系统的功率状态的一个实施例。该平台具有三个状态 :活动的，其中数据不受保护（状态 1，1010）；平台随时备用或连接备用，其中数据不受保护（状态 2，1030）以及数据受保护（状态 3，1050）（其中平台既不处于备用、连接备用也不是活动的）。连接备用指这样的状态，其中平台维持网络连接性和 / 或更新其数据而无需用户觉察平台打开。

[0098] 初始状态不受保护，其中平台活动。如果接收布防动作（后跟怀疑触发），平台移到数据保护状态 1050。在该状态中，对数据加密，并且平台受保护。如果用户走开，则可自动触发初始布防动作。这可基于例如移动电话等配对网络设备、手动键或其他指示器的使用、对于用户失去视觉识别或其他布防动作而确定。怀疑触发可包括由加速剂检测移动、移除 AC 电力、脱离停靠点或潜在盗窃的另一个指标。

[0099] 在一个实施例中，如果平台不活动，在闲置某一时期后，它移到备用状态或连接备用状态，但仍然不受保护（状态 1030）。在一个实施例中，转变到备用状态或连接备用状态可由于用户的明确请求而发生。如果在备用状态 1030 中，接收需要被处理的事件，系统转回平台活动状态 1010。

[0100] 如果在设备处于备用或连接备用状态 1030 时，用户远离平台移动，并且怀疑盗窃企图，则系统移入数据保护状态 1050。一旦发生此情况，需要访问证书来回到平台活动、数据不受保护的状态 1010。在一个实施例中，在已经经过预设闲置期后，甚至在没有用户离开或可发生盗窃这样的指示的情况下，系统可自动进入休眠或相似的较低功率状态，并且起动数据保护。

[0101] 尽管未示出，当观察到另外的闲置时间时，系统可以从备用状态移到休眠或关闭。在一个实施例中，当平台移到休眠状态时，它自动保护平台数据。在一个实施例中，这简单地是允许 OS 启动的默认密码要求。在一个实施例中，这包括在进入休眠之前对平台上的数据加密。在一个实施例中，这包括自加密驱动器，其在驱动器的任何上电时需要解密，这是在离开休眠或关闭状态时发生的事件。这些可以是全盘加密的方面，其可用安全系统实现。

[0102] 图 11A 是在始终打开、始终可用的环境中使用保护系统的一个实施例的综览流程图。过程在框 1110 开始。在一个实施例中，每当对系统布防时，该过程活动。如何对系统布防和撤防在下文更详细地论述。

[0103] 在框 1120，对具有电力源的平台布防。在一个实施例中，该布防可以是手动、半自动（手动起动和自动完成）或自动的。当平台被布防时，它监视攻击（无论是软件、硬件还是盗窃）的指标。

[0104] 在框 1130，过程确定是否存在基于软件攻击的可能性。这通过监视例如企图重设设定为默认值等某些动作而进行。如果检测到基于软件的攻击，在框 1135 解决该攻击。攻击可通过禁止动作（例如，在平台被布防时，平台的更改）而解决。平台还可进入其中数据被加密的模式。平台还可在一个或多个预定位点处向用户发送告警。例如，用户可具有电子邮件地址、SMS 目的地、启用蓝牙的带消息传递能力的电话等。系统还可通知安全服务器。该安全服务器然后可依次通知用户、管理员或另一方。

[0105] 过程然后继续框 1160，来确定是否已经对平台撤防。授权用户可在任何时间对平台撤防。例如，可发生授权用户意外触发平台对基于软件的企图的怀疑。用户可对平台撤防来结束攻击的解决。这可通过证明授权用户以各种方式控制着平台而进行。如果平台被撤防，在框 1170，过程确定解决攻击的动作是否在进行中。如果是这样的话，在框 1175，终止动作，并且通知用户 / 服务器(如需要的话)。因为平台被撤防，过程在框 1180 结束。过程在用户下一次对平台布防时重新开始。如果还未对平台撤防(如在框 1160 确定的)，过程继续框 1130 来继续监视攻击。

[0106] 如果不存在基于软件的攻击(如在框 1130 确定的)，过程在框 1140 确定是否存在基于硬件的攻击。基于硬件的攻击可以是移除电池的企图、关闭 WiFi 的企图、使设备脱离停靠点等。如果检测到基于硬件的攻击，过程继续框 1145。

[0107] 在框 1145，解决基于硬件的攻击。一般，基于硬件的攻击无法在物理上被阻止(例如，平台无法阻挡 AC 线被拉扯)。然而，每当可能之前完成基于硬件的攻击时，将发送通知。

[0108] 在一个实施例中，某些硬件攻击可被系统阻止。例如，在一个实施例中，如上文描述的，电池机械闩锁或基于螺线管的保护系统阻止移除电池。在一个实施例中，WiFi 的硬件 kill 开关由嵌入式控制器超驰，从而使平台能够发出通知消息。过程然后继续框 1160 来确定是否已经对平台撤防。

[0109] 如果未检测到基于硬件的攻击，在框 1150，过程确定是否存在盗窃企图。可在平台移动时检测盗窃企图，同时它被布防。如果存在盗窃企图，在框 1155，解决盗窃企图。在一个实施例中，通过向用户和 / 或安全服务器发送通知来解决盗窃企图。在一个实施例中，该通知可包括当前位点和 / 或移动数据。在一个实施例中，系统设置 ping，来定期向用户 / 服务器发送位点 / 运动信息。在一个实施例中，系统通过移入休眠功率状态而保护它的数据。过程然后继续框 1160，来确定是否平台被撤防。

[0110] 这样，系统在被布防时解决多个形式的潜在攻击。注意，不管平台的功率状态如何，只要提供足够大的电力源，这些防御是可用的。注意尽管图 11A 和其他图示出为流程图，流程图的组织简单地将相关动作组合在一起。这些动作的排序不必按示出的顺序。此外，过程可单独监视在流程图中论述的设定中的每个。例如，在上文的流程图中，可存在监视攻击的多个传感器。如果任何传感器指示攻击，进行与该攻击关联的过程。相似地，对于下文的流程图，不应理解为需要每个步骤，也不应理解为需要按呈现的顺序执行这些步骤。

[0111] 图 11B 是系统可遇到的各种情形以及在平台、服务器和用户携带设备处的反应的一个实施例的表。如可以看到的，如果用户与平台在一起，大体上未对平台布防，或平台处于布防进行中模式。如果存在用户并且未对设备布防，没有采取服务器动作或用户携带设备动作。

[0112] 如果用户可远离平台，并且平台被布防，但未检测到有威胁，不采取服务器动作，但可以可选地告警用户他或她超出平台的范围。

[0113] 如果用户离开，并且检测到威胁，平台模式移到怀疑模式，来保护数据并且发送告警。服务器能够跟踪平台的 ping。如果存在明显的移动，或平台停止发送 ping，则服务器能够告警用户或受控退出点或另一个授权目标该平台受到威胁。根据策略，用户携带的设备可告警或不告警。

[0114] 图 12 是对系统布防的一个实施例的流程图。过程在框 1210 开始。在一个实施例

中，在对系统供电时，它始终监视布防指示。在一个实施例中，因此每当对系统供电并且尚未对其布防时，过程开始。

[0115] 在框 1220，过程确定是否已经满足自动布防策略。自动布防设置促使对设备布防的某些策略。图 13 示出可能的自动布防策略中的一些。它们可包括失去蓝牙接近性、经由拍摄装置失去用户、关闭盖子、设备移动、设备闲置、位点、一天中的时间或用于布防的其他预设自动触发。在一个实施例中，系统可没有适当的自动布防策略。在该实例中，无法满足自动布防策略。

[0116] 回到图 12，如果系统确定已经满足自动布防策略，在框 1225，对平台布防。过程然后继续框 1270。在框 1270，过程确认是否平台被布防。如果是这样的话，在框 1280 结束监视布防。在一个实施例中，这包括关闭传感器或被供电的其他设备以便实现布防动作的检测。一旦平台被布防，仅撤防和检测怀疑触发所需要的那些元件仍然被供电。

[0117] 如果缺少自动布防规则，或其未被满足，过程继续框 1230。在框 1230，过程确定是否已经起动半自动布防。半自动布防使用第一手动起动，并且然后使用自动布防规则。例如，如果用户起动与蓝牙设备配对、设置开关或用别的方式使布防系统初始化，则可出现半自动布防。一旦发生初始化，在出现某一条件时可自动对平台布防。这些条件可以是图 13 中列出的那些。初始手动开关可以是在手动布防下在图 13 中列出的那些中的一个，或另一个。如果在框 1230 起动半自动布防，过程继续框 1235。

[0118] 在框 1235，过程确定是否满足自动布防规则。如果是这样的话，在框 1240 对平台布防。过程然后继续框 1270，其中系统确认平台被布防，并且退出布防循环。如果在框 1235 不满足自动布防规则，过程继续框 1250。在另一个实施例中，一旦起动半自动布防，过程仅检查是否满足与半自动布防关联的自动布防规则（例如，过程围绕框 1235 循环直到满足规则或对半自动布防撤防）。

[0119] 如果在系统中未起动或未启用半自动布防，过程继续框 1250。在框 1250，过程确定是否接收手动布防。手动布防命令可以是在图 13 中列出的形式中的一个，或用户要起动布防的另一个动作。如果接收手动布防动作，在框 1265，对平台布防。过程然后继续框 1270，来确定是否平台被布防，并且退出布防循环（如果它是的话）。如果未接收手动布防动作，在框 1270，过程确定是否平台被布防。如果平台被布防，过程在框 1280 结束。如果未对平台布防，过程回到框 1220，来继续监视布防。

[0120] 在一个实施例中，特定布防规则可由用户设置。在一个实施例中，可存在对系统的默认设定。例如，默认设定可以是，当用户携带配对设备离开时、当平台从网络连接断连时等，在 5 分钟闲置后自动对平台布防。在对平台撤防时，用户可修改这些设定。在一个实施例中，管理员也可修改这些设定。在一个实施例中，对于企业拥有的平台，管理员可设置默认布防设定，其无法被用户改变。在一个实施例中，对于个人计算机，用户可停用管理员对设定的访问。

[0121] 图 14 是对保护系统撤防的一个实施例的流程图。过程在框 1410 开始。在一个实施例中，每当平台被布防时，该过程活动。在一个实施例中，这在多个功率状态中活动，例如当平台处于打开或睡眠状态中时。在一个实施例中，这包括对一个或多个传感器、检测器或可接收撤防命令的设备供电。

[0122] 在框 1420，过程确定是否已经接收自动撤防信号。自动撤防信号的一些示例在图

15 中列出。在一个实施例中，用户可停用自动撤防。如果自动撤防被停用，将不存在将自动对平台撤防的条件。在一个实施例中，系统对与自动撤防命令关联的那些元件供电。例如，如果存在配对蓝牙设备，并且启用蓝牙自动撤防，系统将在平台被布防时对蓝牙配对供电，甚至在减少功率状态中也如此。

[0123] 如果已经接收自动撤防信号，在框 1425 对平台撤防。对平台撤防可导致启用键盘输入、对数据解密或用别的方式使平台准备与用户交互。

[0124] 过程然后继续框 1440，其中过程证实平台被撤防。如果是这样的话，过程在框 1450 结束。这时，系统切换成启用与对平台布防关联的传感器，如在上文关于图 12 论述的。

[0125] 如果未接收自动撤防，在框 1430，过程确定是否接收手动撤防命令。手动撤防指标的一些示例在图 15 中示出。一般，撤防需要证明授权用户控制着平台。因此，可使用通过近场通信设备（例如，用户徽章或电话）的分接（tapping）或例如用户图像、指纹、语音等生物计量，以及密码 / 移动，其将仅被授权用户知晓。

[0126] 如果接收手动撤防命令，在框 1435 对平台撤防。

[0127] 在任何情况下，过程在框 1440 确定平台被撤防。如果它被撤防，过程在框 1450 结束。如果平台未被撤防，过程回到框 1420 来继续监视自动和手动撤防命令。

[0128] 图 16 是对于基于网络的布防和撤防使设备配对的一个实施例的流程图。过程在框 1610 开始。在框 1615，用户获取平台，其包括蓝牙或其他局域网连接能力。在一个实施例中，网络连接格式是蓝牙配对。

[0129] 在框 1620，用户设置另一个启用网络的设备作为与平台配对的设备。在一个实施例中，可使用能够与启用蓝牙的平台配对的任何设备。在一个实施例中，这样的设备可包括移动电话、有蓝牙能力的无线耳机、包括蓝牙能力的徽章，或任何其他设备。

[0130] 在框 1625，用配对的用户设备来设置自动或半自动布防 / 撤防。在一个实施例中，用户可在该设置期间设置配对的细节。细节可包括计时和其他限制。例如，在极其安全的环境中，用户可设置平台应该在失去与配对设备的连接时立即对平台布防。在不太安全的环境中，用户可喜欢在对平台布防之前设置短的时期，以移除对平台布防和撤防的潜在时间延迟（针对短暂失去连接性）。

[0131] 如果配对是活动的，过程在框 1635 确定平台是否接近设备。如果平台接近设备，在框 1640，过程确定是否平台被布防。如果平台被布防，在框 1645，对平台撤防。因为设备接近平台，用户视为存在。因此，对平台撤防。过程然后回到框 1635，来检查平台是否仍与用户携带设备接近。

[0132] 如果平台未接近配对设备（在框 1635），过程继续框 1650。在框 1650，过程确定是否平台被布防。如果平台未布防，在框 1655，对平台布防。因为设备不存在，平台假设用户也不存在。因此，对平台布防。过程然后继续框 1635，来检查平台是否仍不接近用户携带设备。如果平台被布防，过程直接继续框 1635。

[0133] 这样，系统在配对设备接近平台或不接近平台时简单地对平台布防以及不对平台布防。在一个实施例中，在发生蓝牙配对时，平台将设备视为接近。在一个实施例中，平台中的蓝牙系统设置成具有半径限制。尽管蓝牙网络范围可以达到 10 米远，可以设置系统来将配对可用的距离限制在可接受距离。此外，在一个实施例中，系统使用需要加密的蓝牙协议的较新版本，并且阻止 XOR 攻击来获得配对密钥。

[0134] 图 17 是使用启用双向蓝牙的设备用于布防 / 撤防和通知服务的一个实施例的流程图。除在上文关于图 16 描述的单向通知外，还可设置双向通信。过程在框 1710 开始。该过程在存在活动的双向蓝牙系统设置时以配对设备开始。

[0135] 在框 1720，平台和设备感测接近性并且设置配对网络。这打开了平台与设备之间的通信信道。下文的过程在平台和设备两者上发生。在一个实施例中，这需要在配对设备上的单独应用。

[0136] 在框 1730，过程确定发送计时器是否显示该是向设备发送 ping 的时间。如果是这样的话，在框 1740，平台向设备发送 ping。过程然后继续框 1750，其中 ping 发送计时器被重设。过程然后回到框 1730，来确定是否该是发送另一个 ping 的时间。

[0137] 如果尚未到向平台发送 ping 的时间，过程在框 1760 确定平台是否本应从设备接收 ping。如果尚未到时间（在框 1730），过程往回循环来继续测试是否到时间发送，或接收 ping。

[0138] 如果到时间接收 ping，在框 1770，过程确定是否已经从设备接收指示连续接近的 ping。如果已经接收接近性信号，过程继续框 1750，来重设接收计时器。

[0139] 如果未接收到接近性信号，在框 1780，发出和 / 或发送告警。在一个实施例中，该告警发送到配对设备，来告警用户设备现在超出接近性范围。在一个实施例中，告警经由无线连接而不是经由蓝牙配对连接来发送。在一个实施例中，如果平台处于布防进行中模式，平台可另外移到布防模式。这保护平台上的数据，并且开始监视潜在盗窃的其他指标。

[0140] 上文的过程的镜像在设备中发生。该配对的双向蓝牙连接使用户能够跟踪蓝牙设备和平台，并且具有双向保护。在一个实施例中，该过程与上文描述的布防 / 撤防过程并行运行。

[0141] 图 18 是当接近性与运动数据进一步耦合时基于接近性的布防和撤防的一个实施例的流程图。在一个实施例中，系统在平台移动和平台不移动时的反应不同。过程在框 1810 开始。

[0142] 在框 1815，未布防防盗技术。在框 1820，过程确定用户是否已经对平台布防，或是否基于自动或半自动设定而已经对平台布防。如果否的话，过程继续监视，从而回到框 1815。

[0143] 如果平台被布防，过程继续框 1825。在框 1825，过程确定平台是否在用户设备超出范围外的同时正在移动。如果平台在用户设备超出它的范围外的同时正在移动，过程继续框 1830。在框 1830，在一个实施例中，依照策略，平台保护数据并且向与平台关联的拥有方、用户和 / 或服务器发送告警。在一个实施例中，数据可已经受到保护，在该情况下仅发送告警。过程然后继续框 1845。

[0144] 如果在用户设备超出范围的同时平台不在移动（在框 1825），过程继续框 1845。在框 1845，过程确定用户或平台是否正移动使得平台正超出用户范围。如果是这样的话，过程继续框 1835，来确定用户携带的设备是否具有策略使得它应该经由警报来告警用户他或她正移动到平台范围外。

[0145] 在一个实施例中，可在受限境况下发出警报。例如，用户可发出仅在平台初始与配对设备一起移动并且然后两个分开移动时发送的警报。在一个实施例中，如果平台在平台和设备分开移动之前持续至少短时期地成为静止，用户可不希望告警。这可能例如在工作

中出现，其中用户将定期携带他们的移动电话(配对设备)远离他们的便携式电脑(平台)。相比之下，用户将带着平台一起走开并且突然离开它，这相对不可能。

[0146] 如果设定是为了经由警报来告警用户(在框 1835)，在框 1840，由于失去蓝牙接近性，设备向用户发出警报。

[0147] 如果用户未移出范围，如在框 1845 确定的，过程在框 1850 确定用户是否已经对平台撤防。如果用户还未对平台撤防，过程继续框 1825 来继续监视平台的移动以及用户设备是否在范围内。如果用户已经对平台撤防，过程回到框 1815，从而使得未布防防盗技术。

[0148] 图 19 是使用近场通信用于对系统布防和撤防的一个实施例的流程图。过程在框 1910 开始。在一个实施例中，过程以包括近场通信读取器的平台开始。

[0149] 在框 1915，系统初始设置成建立包含 NFC 芯片的设备用于布防 / 撤防。在一个实施例中，NFC 芯片可以处于用户徽章中、用户移动电话中，可以是可附连到密钥链的标签，可处于可附连到用户习惯携带的某种事物(例如徽章或电话)的便签上。

[0150] 在框 1920，过程确定是否平台被布防。如果未对平台布防，在框 1925，过程确定是否激活 NFC 布防。在一个实施例中，当布防过程是半自动时，用户需要对基于 NFC 的布防过程初始化。如果 NFC 布防未被激活，在框 1930，平台仍然未布防。过程然后回到框 1920，来继续循环通过该过程。

[0151] 如果 NFC 布防被激活，过程继续框 1935。在框 1935，过程确定是否已经接收并且验证具有启用 NFC 的设备的激活分接(tap)。在一个实施例中，系统使用分接样式(例如，在特定步调中的分接 - 分接 - 分接)。在另一个实施例中，多个定时接近性(例如，分接或挥动启用 NFC 芯片的对象)可以是激活分接。在另一个实施例中，使启用 NFC 芯片的对象保持接近是足够的。验证包括检查 NFC 设备所递交的证书。这些证书必须是在初始设置期间注册的证书，来实现使用 NFC 设备用于布防和撤防。如果未接收或未成功验证激活分接，过程继续框 1930，并且平台仍然不受保护。

[0152] 如果接收并且验证激活分接，在框 1940，对平台布防，并且万一有盗窃怀疑则保证数据受到保护。一旦平台被布防，它由对平台撤防的授权用户或管理员撤防。

[0153] 过程然后回到框 1920，以证实是否平台被布防。

[0154] 如果在框 1920 过程发现平台被布防，它继续框 1945。在框 1945，过程确定是否接收并且验证撤防分接。如果接收并且验证撤防分接，在框 1955 对平台撤防。如果未接收撤防分接，或验证失败，在框 1950，平台仍然被布防。过程然后回到框 1920。为了撤防，可存在预设分接样式。在一个实施例中，NFC 读取器将分接“识别”为在预设时期内多个接近性检测。例如，样式可以是在一秒时期内的接近 - 不接近 - 接近。这样，只采取启用 NFC 芯片的设备是不够的。

[0155] 注意尽管该过程仅描述基于 NFC 的布防和撤防，本领域内技术人员将理解手动方法和布防的各种自动和半自动方法可共存。

[0156] 图 20 是包括系统的触发数据保护的电力管理的一个实施例的流程图。示例在这里描述四个功率状态：打开、备用 / 连接备用、休眠和关闭。本领域内技术人员将理解仅仅是四个示范性功耗水平，而不管它们的命名方案如何。打开是全供电(尽管不是它的所有方面需要被供电以便用于平台要打开)，备用或连接备用是较低功率状态，并且休眠也是较低功率状态，但在关闭之上。在一个实施例中，尽管描述四个单独状态，可在平台上实现较少

的状态。过程在框 2010 开始。

[0157] 在框 2015，平台在没有盘加密的情况下处于功率状态，例如备用或连接备用。在一个实施例中，平台还可以处于打开状态。

[0158] 在框 2020，过程确定用户是否已经对系统布防。在一个实施例中，用户可手动对系统布防。如果用户还未对系统布防，过程在 2025 确定是否满足自动布防的标准。如果不满足该标准，过程在 2030 结束。

[0159] 如果满足自动布防标准，过程继续框 2035。如果在框 2020 用户对系统布防，过程还继续框 2035。

[0160] 在框 2035，平台被布防，但数据可不受保护。

[0161] 在框 2040，过程确定是否检测到怀疑事件。如果未检测到怀疑事件，过程继续框 2065。在框 2065，过程确定系统是否转变到数据保护状态。这可因为用户动作而出现。如果系统处于数据保护状态，过程行进到框 2055，其中数据是受保护状态。在一个实施例中，过程循环回到框 2040 来继续监视怀疑事件，以便万一怀疑平台盗窃则进行额外的安全动作。

[0162] 如果在框 2040 检测到怀疑事件，过程继续框 2042。在框 2042，过程确定平台是否已经处于休眠或关闭状态。如果是这样的话，因为平台受保护，则过程在 2030 结束。如果过程不处于休眠或关闭状态，过程继续框 2045，其中平台试图移到休眠状态。在一个实施例中，当系统处于休眠状态时，需要验证来访问平台，以完成使平台从休眠移到打开状态，并且访问数据。在一个实施例中，这意指数据被加密。这使得在平台被打开后对平台的访问减慢，并且从而这对于备用不是最佳的。它还阻止平台的自动唤醒以便下载例如电子邮件等信息，并且因此它打断了连接备用。在一个实施例中，尽管系统被布防（在框 2035），不需要手动撤防或解密。

[0163] 在框 2050，过程确定到休眠的转移是否成功。如果是这样的话，在框 2055，平台在休眠中并且因此数据受到保护。一旦数据受到保护，过程在框 2030 结束。在一个实施例中，在框 2040，过程继续监视可疑盗窃事件以便进行其他安全动作。在一个实施例中，如果系统正在休眠状态中监视可疑事件，系统可在检测到可疑盗窃事件时发出告警或进行另一个动作。

[0164] 如果到休眠的转移不成功（如在框 2050 确定），在框 2060 过程迫使平台关闭。设计该被迫关闭使得没有软件能够中断该过程。一旦平台关闭，在框 2055，数据仅利用密码而可访问并且从而平台被布防并且数据受到保护。过程然后在框 2030 结束。在一个实施例中，在框 2040，过程继续监视可疑盗窃事件以便进行其他安全动作。这样，系统允许受保护的备用状态，而无需施加如果未检测到可疑事件则需要密码来访问数据的额外开销，并且不打断连接备用使用。这实现对于用户是透明的保护层（除非检测到可疑事件）。

[0165] 图 21 是透明启动 / 恢复的一个实施例的流程图。一般，当移动系统从备用或连接备用恢复时，计算机系统不需要输入密码。在一个实施例中，该过程允许系统迫使未授权用户在恢复时输入密码，即使从未对用户本身提示该密码（假设在未授权用户试图访问时用户离开）也如此。在一个实施例中，该过程还允许系统从通常需要手动输入密码的状态启动，而不对授权用户提示密码。过程在框 2110 开始。在一个实施例中，该过程在用户打开计算机或起动启动过程时开始。为了简单起见，术语“启动”在这里指从减少功率状态移到

打开状态，而不管是否需要 BIOS 启动。

[0166] 在框 2120，系统开始启动过程。在一个实施例中，如果平台是计算机系统，CPU（中央处理单元，或处理器）对它自身初始化。因为防盗系统在所有功率模式中是运行的，能够得出关于甚至在系统启动开始之前的用户接近性的结论。

[0167] 在框 2130，证实用户存在。在一个实施例中，该确定可基于在系统启动之前出现的用户存在监视。用户存在可基于配对蓝牙或其他网络设备的接近性而证实、可以是基于拍摄装置输入（例如，识别平台处的用户）的视觉标识，或另一个存在标识。

[0168] 如果用户存在被证实，在框 2180，过程直接转到可用屏幕。这意指系统跳过输入密码的必要性。这使可用性增加并且对于授权用户避免对平台可用性的不利影响。过程然后在框 2170 结束。

[0169] 如果用户存在未被证实，过程继续框 2140。在框 2140，过程完成对密码屏幕的启动。在一个实施例中，可修改密码要求来实现 NFC、生物计量或其他验证机制的使用。

[0170] 在框 2150，在接收标识 / 密码之后，系统证实它是否准确。如果是这样的话，因为授权用户的存在已经被证实，过程继续框 2180 来提供可用屏幕。

[0171] 如果密码不正确，或未反映授权用户的存在，过程继续框 2160。在一个实施例中，这仅在提供多个输入正确的密码 /ID 的机会之后出现。

[0172] 在框 2160，在一个实施例中，向用户发送告警，并且采取另一个安全动作。在另一个实施例中，不采取动作，但要阻止平台启动。安全动作可告警用户、向安全服务器发送告警、关闭计算机，或在一个实施例中，授权 kill pill（例如，使计算机不可用）。过程然后在框 2170 结束。

[0173] 图 22 是多 kill pill 系统的一个实施例的图。该图示出三个可能的 kill pill 实现。kill pill 是使计算机系统平台不可用或它的数据不可访问或被清除的方法。它设计成在平台被偷或丢失时应用，并且平台上的数据的价值高于平台自身的价值。

[0174] 第一示例具有客户端平台 2210，和自 kill pill 2215。在存在盗窃怀疑并且没有及时出现用户动作时调用该自 kill pill。一般，在调用自 kill pill 之前的时间可以是几小时到几天。这意指盗窃者可有机会在调用 kill pill 之前使用或卖掉平台。

[0175] 第二示例具有客户端平台 2220 和服务 kill pill 2225。该服务 kill pill 2225 使拥有方 2230 能够通知服务 2235、发送服务 kill pill 2225。然而，因为这需要通知，拥有方 2230 必须察觉盗窃，然后通知服务 2235 并且等待 kill pill 2225 的服务起动。因此，该方法也可为窃取提供足够的时间以在激活 kill pill 之前使用或卖掉平台。

[0176] 第三示例是多 kill pill 2255。客户端平台 2250 受到 kill pill 2255 的保护，可以以许多方法调用该 kill pill 2255。在一个实施例中，三个选项可用 ：自 kill 选项、告警 kill pill 服务用于远程调用 kill pill 和通知拥有方，该拥有方然后可以占用服务 2265 来调用 kill pill 2255。因为该多管齐下的方法实现快速响应，盗窃者无法足够快地卖掉平台，这意指与没有即刻反应元件的 kill-pill 技术方案相比，该技术方案使对盗窃的威慑增加。

[0177] 在一个实施例中，当客户端平台 2250 识别盗窃怀疑时，向拥有方 2260 和服务 2265 发出告警。如果拥有方 2260 作出响应（其指示没有盗窃），过程结束。但如果告警不成功（未正确地被拥有方接收，或未接收响应），系统起动自 kill pill。备选地，服务 2265 可响应于

用户 2260 验证而发送 kill pill 通知。

[0178] 在一个实施例中，因为即刻防盗反应技术也在低功率状态操作，它不会帮助盗窃者使平台处于低功率状态以便延迟 kill-pill 的调用。

[0179] 图 23 是防盗机构部件的电力管理的一个实施例的流程图。过程在框 2310 开始。在框 2320，系统进入减少的功耗状态。在一个实施例中，这在每当平台从 AC 电力断连时出现。在一个实施例中，这在平台处于减少的功率状态（例如，备用、连接备用、休眠或关闭模式）时出现。在一个实施例中，所有平台状态可视为能适用于减少的功耗模式（例如，甚至打开和连接到 AC 电力）。

[0180] 在框 2330，系统确定平台的保护模式。如在上文指出的，这些模式是：未布防、布防、布防进行中和怀疑。

[0181] 在框 2340，过程识别可与平台一起使用的授权接口。这些接口可包括以下中的一个或多个：NFC 读取器、蓝牙配对、视频拍摄装置、生物计量读取器、麦克风和其他。这些接口中的每个可位于 OEM 板上或实现为外设。

[0182] 在框 2350，过程确定任何接口是否与当前模式相关。当前模式示出可经由接口接收哪些动作（如有的话）。图 24 示出将确认的模式和关联输入类型的示范性列表。一个或多个接口类型可与这些输入类型中的每个关联。

[0183] 如果没有接口相关，过程在框 2360 将电力从所有接口移除。如果一些接口相关，在框 2370，仅对那些选择的接口供电。这使平台的总功耗减少。因为甚至在低功耗状态中对这些接口供电，减少功耗是有用的。

[0184] 过程然后继续框 2380。

[0185] 在框 2380，过程确定降低的功耗要求是否结束。在一个实施例中，降低的功耗要求可在系统处于打开状态和 / 或平台插入 AC 插座或停靠时结束，从而移除对节省电力的需要。在一个实施例中，降低的功耗要求可视为能适用于所有平台功率状态。如果降低的功耗需要结束，过程在框 2385 结束。当系统将再一次需要减少它的功耗时，在框 2310，该过程将再次重新开始。

[0186] 如果降低的功耗需要未结束，过程在框 2390 确定机构的模式是否改变。机构的模式可由于用户输入、闲置时间或其他设定而改变。如果模式未改变，过程回到框 2380，来继续监视降低的功耗需要是否结束。如果在该模式中存在改变，过程继续框 2330 来确定模式并且根据需要调整设定。

[0187] 这样，系统实现了在减少功耗（在可能时）的同时使用接口，而不管模式如何。

[0188] 图 25 是保护性超驰机构的一个实施例的流程图。由于各种原因，可对防盗机构调用超驰。原因可包括：终端用户将他的撤防设备（例如，电话或徽章）留在别处，撤防设备出故障或失去电力，平台从终端用户回到 IT 并且被改用途成用于另一个终端用户，平台从终端用户召回到 OEM，和其他原因。过程在框 2510 开始。

[0189] 在框 2520，平台处于布防模式。在布防模式中，需要撤防来访问平台上的数据。在一个实施例中，平台可已经自动或由于用户动作而进入布防模式。

[0190] 在框 2530，过程确定是否请求撤防。如果未请求撤防，过程继续框 2520 来使平台维持在布防模式。

[0191] 如果请求撤防，过程继续框 2540。在框 2540，过程确定撤防请求是否成功。如果

是这样的话，在框 2550 对平台撤防。过程然后在框 2560 结束。在该模式中的后续超驰请求将立即被准许。

[0192] 如果撤防请求不成功，过程继续框 2570。在一个实施例中，这仅在设置数量的失败尝试之后出现。

[0193] 在框 2570，过程确定是否已经请求超驰。如果未请求超驰，过程回到框 2520，并且平台仍然处于布防模式。

[0194] 如果请求超驰，过程在框 2580 使平台移到怀疑模式。在怀疑模式中，在框 2590 进行对怀疑模式的软响应。软响应可限定为不难逆转以便重获平台功能性的反应。软反应的示例包括告警的传输、到不同功率状态的转变以便保护数据（在终端用户知晓数据保护密码这一假设下）。

[0195] 在已经进行所有软响应后（在怀疑模式中），过程继续框 2550，并且转变到未布防模式。在一个实施例中，在未布防模式中，平台不能用。然而，系统未对平台上的数据解密。从而，当平台不是“不能用”时，数据仍然受保护。过程然后结束。

[0196] 图 26 在超驰情景的各种选项之间比较。上文描述的选项是最后一个，其中盗窃者无法偷数据和资产，但当请求超驰时，拥有方将不以不能用系统来结束。这样，数据仍然受保护并且发送盗窃怀疑告警以便万一盗窃者试图调用超驰时则防止可能的盗窃。然而，万一是终端用户调用超驰，则平台仍然不可访问。

[0197] 图 27A 和 27B 是平台的企业预备的一个实施例的流程图。过程在框 2710 开始。在框 2715，接收配置更改请求。该配置更改可改变告警机构、使设备与平台配对、使设备从配对移除、改变告警的定时、添加或移除 kill pill 或进行对系统的其他更改。

[0198] 在框 2720，过程确定请求是否是直接用户请求。如果是这样的话，在框 2725，过程确定用户是否已经识别为远离平台。如上文指出的，可基于配对设备或设备的布防模式来监视用户到平台的接近性。

[0199] 如果用户识别为离开，过程在框 2730 拒绝请求（假设它是恶意请求）。在一个实施例中，如果请求识别为恶意请求，系统可进一步发送告警。过程然后在框 2733 结束。

[0200] 如果在框 2725 用户还未识别为离开，过程继续框 2735。在框 2735，过程证实用户的物理存在，来证实配置由操作配置软件的物理用户进行，这与恶意软件所进行的不同。在一个实施例中，这可通过聚集用户对策略改变的请求并且然后在屏幕（其对于软件不可读（例如，“精灵”屏幕），但用户可以看见）的一部分上显示它们而证实。在一个实施例中，这通过对图形控制器提供防盗机构直接边带访问而实现。屏幕的该部分还将包含确认的一些部件。例如，它可显示仅用户可看见的确认代码，或请求来自用户的动作。用户然后输入代码、进行请求的动作或用别的方式证明配置请求由实际用户做出。如果物理用户存在的证明未被正确地接收，过程继续框 2730 来拒绝作为恶意请求的请求。否则，过程继续框 2737。

[0201] 在框 2737，接受并且记录请求。

[0202] 在框 2740，过程确定先前对于该配置元素的验证设定是“空”（例如，空白）。如果是这样的话，由用户输入的最新值作为机构的活动策略应用（在框 2745）。在任何情况下，由用户输入的值记录为用户期望的策略。过程然后在框 2733 结束。如果在用户输入之前配置元素不是空，则在框 2750，最新记录和验证的值作为机构的活动策略而应用。过程然后在框 2733 结束。

[0203] 如果在框 2720，过程发现请求不是直接用户请求(例如，通过不要求或不允许证明物理用户配置的接口而到达)，过程继续框 2755。在框 2755，过程确定是否允许非用户配置。在一个实施例中，用户可使管理员配置能力停用。在一个实施例中，对于企业拥有的平台，用户可不具有对管理员配置撤防的能力。

[0204] 如果不允许非用户配置，在框 2730，系统假设它是恶意请求，并且过程结束。

[0205] 如果曾允许非用户配置，过程继续框 2765。在框 2765，过程确定在最后一次用户通过策略允许非用户配置之后用户是否已经重设设定为默认使得不允许非用户配置的策略也逆转到默认。如果是这样的话，过程继续框 2730(假设这是恶意请求并且丢弃它)。在一个实施例中，用户可证实非用户配置请求。在一个实施例中，可告知用户关于非用户配置请求。在一个实施例中，系统未丢弃这样的恶意请求，相反保存它们，并且使用户能够证实它们，或将它们告知用户。这使管理器能够做出改变，即使先前的改变被用户超驰也如此。

[0206] 如果系统的模式使得用户允许非用户配置请求并且后来未将该策略逆转到默认，过程继续框 2770。

[0207] 在框 2770，过程确定是否已经预备非用户。预备非用户向特定非用户提供授权来做出改变。如果还没有预备非用户，在框 2730，系统假设请求是恶意请求并且丢弃它。如果已经预备用户，过程在框 2780 确定命令是否可以被验证。在一个实施例中，验证包括证实管理员为预备非用户。如果命令无法被验证，在框 2730，过程假设请求是恶意的并且丢弃它。

[0208] 如果可以验证命令，在框 2785，过程假设请求有效、接受并且记录它。过程然后继续框 2740，来确定是应用该非用户设定(万一它不是空的)，还是应用最新记录的用户设定(万一现在记录的非用户设备是空的)。本文描述的过程是针对其中用户对平台的配置具有主要控制的系统。在所有情形中情况可能不是这样。

[0209] 图 28 是在监视的环境中平台安全性的一个实施例的流程图。监视的环境是其中存在受控退出点的环境。受控退出点可以是可远程锁定的退出点、具有一个或多个守卫的退出点或可以用别的方式变得不可访问的退出点。过程在框 2810 开始。在一个实施例中，过程在平台在监视的环境中使用时开始。流程图是从安全服务器(其接收来自平台的信息并且向受控接入点发送信息)的角度来看。在一个实施例中，系统可配置成使平台能够直接向受控退出点发送控制信号。

[0210] 在框 2815，安全服务器接收对平台布防的通知。服务器假设平台未被偷。

[0211] 在框 2820，过程确定是否已经从平台接收“怀疑”状态更新。如果未接收这样的模式，过程回到框 2815，来进行监视被布防的平台。在一个实施例中，当平台被撤防时，安全服务器的监视被关闭。在一个实施例中，平台发送已经撤防的通知，其结束监视。

[0212] 如果从平台接收“怀疑”状态更新(在框 2820)，过程继续框 2825。在框 2825，因为在布防或怀疑模式中超驰撤防的试图，过程确定是否进入了怀疑模式。如果是这样的话，在框 2830，系统告警受控退出点。这可包括在退出点或整个建筑中告警守卫、锁定闸、发出音频警报，或其他动作。在一个实施例中，这些动作中的一些可具有时间延迟地发生。例如，在告警守卫之前，系统可对用户提供足够的时间来对他的平台撤防，以防这是假肯定。在一个实施例中，为了进一步减少假肯定，平台可在本地向用户提供指示器，使得他意识到平台处于怀疑模式并且与它一起的进一步明显的移动将使守卫被告警。该指示器可以是视觉指

示器、音频指示器或另一个类型的指示器。

[0213] 在框 2835，过程确定用户是否已经对平台撤防，指示授权用户已经指示他或她具有平台并且没有进行中的盗窃。如果终端用户已经成功地对平台撤防，在框 2840，取消告警。过程然后回到框 2815，其中平台被布防并且指示为未被偷。在一个实施例中，平台可进入撤防模式并且终止该监视循环。

[0214] 如果未接收授权用户撤防（在框 2835），服务器继续跟踪平台位点并且保持告警。在一个实施例中，平台可能够接收运动数据，这基于无线接入点数据、加速计数据、GPS 数据或其他基于运动或位点的信息中的一个或多个。服务器可使用该信息来跟踪平台。

[0215] 在框 2850，过程确定是否已经发现平台。如果是这样的话，过程在框 2852 结束。否则，过程回到框 2835，来继续监视用户撤防或使平台被发现。这样，系统跟踪平台并且确保盗窃者无法从监视的环境取得平台。

[0216] 在平台被布防时检测到明显移动（框 2855）或在平台未能在怀疑模式中发送状态更新（2870）时，系统可进入告警模式来代替状态超驰。在这些情形以及未示出的其他情形（其中安全服务器可将平台视为被偷）中的每个中，过程继续框 2830，并且由安全服务器告警受控退出点，来试图阻挠盗窃者。如果不需要这样的告警，过程回到框 2825 来继续监视。当监视框 2825、2855 和 2870 中告警模式进入时，在框 2860，系统可以由用户撤防。如果对系统撤防，在框 2865，系统从怀疑模式移到未布防模式，并且过程在框 2852 结束。

[0217] 图 29 是根据本发明的实施例的示范性系统 2900 的框图。该系统 2900 可耦合于 OEM 板（上文描述），其实现本文描述的始终可用的防盗系统。如在图 29 中示出的，多处理器系统 2900 是点到点互连系统，并且包括经由点到点互连 2950 而耦合的第一处理器 2970 和第二处理器 2980。

[0218] 分别示出处理器 2970 和 2980，其包括集成存储器控制器（IMC）单元 2972 和 2982。处理器 2970 还包括点到点（P-P）接口 2976 和 2978 作为它的总线控制器单元的部分；相似地，第二处理器 2980 包括 P-P 接口 2986 和 2988。处理器 2970、2980 可经由点到点（P-P）接口 2950 使用 P-P 接口电路 2978、2988 来交换信息。如在图 29 中示出的，IMC 2972 和 2982 使处理器耦合于相应的存储器，即，存储器 2932 和存储器 2934，其可以是在本地附连到相应处理器的主存储器的部分。

[0219] 处理器 2970、2980 可每个经由个体 P-P 接口 2952、2954 使用点到点接口电路 2976、2994、2986、2998 来与芯片集 2990 交换信息。芯片集 2990 可以可选地经由高性能接口 2939 与协处理器 2938 交换信息。在一个实施例中，协处理器 2938 是专用处理器，例如高吞吐量 MIC 处理器、网络或通信处理器、压缩引擎、图形处理器、GPGPU、嵌入式处理器或类似物。在一个实施例中，芯片集 2990 可实现 OEM 板，其提供始终可用的安全系统。在一个实施例中，芯片集 2990 可被单独供电，如上文描述的。

[0220] 共享高速缓存（未示出）可包括在处理器中或在两个处理器外部（但经由 P-P 互连而与处理器连接），使得如果处理器被置于低功率状态，则任一或两个处理器的本地高速缓存信息可存储在共享高速缓存中。

[0221] 芯片集 2990 可经由接口 2996 而耦合于第一总线 2916。在一个实施例中，第一总线 2916 可以是外设部件互连（PCI）总线，或例如 PCI Express 总线或另一第三代 I/O 互连总线等总线，但本发明的范围不这样受到限制。

[0222] 如在图 29 中示出的，各种 I/O 设备 2914 可连同总线桥 2918 一起耦合于第一总线 2916，该总线桥 2918 使第一总线 2916 耦合于第二总线 2920。在一个实施例中，例如协处理器、高吞吐量 MIC 处理器、GPGPU 的处理器、加速计（例如，图形加速计或数字信号处理（DSP）单元）、现场可编程门阵列或任何其他处理器等一个或多个额外的处理器 2915 耦合于第一总线 2916。在一个实施例中，第二总线 2920 可以是低引脚数（LPC）总线。在一个实施例中，各种设备可耦合于第二总线 2920，其包括例如键盘和 / 或鼠标 2922、通信设备 2927 和例如盘驱动器或其他大容量存储设备（其可包括指令 / 代码和数据 2930）等存储单元 2928。此外，音频 I/O 2924 可耦合于第二总线 2920。注意其他架构是可能的。例如，系统可实现多点总线或其他这样的架构，来代替图 29 的点到点架构。在一个实施例中，实现始终可用防盗系统（未示出）的 OEM 板可耦合于总线 2916 或第二总线 2920。

[0223] 现在参考图 30，其示出根据本发明的实施例的第二更特定的示范性系统 3000。与图 29 和 30 中的元件一样具有类似的标号，并且图 29 的某些方面已经从图 30 省略以便避免混淆图 30 的其他方面。

[0224] 图 30 图示处理器 2970、2980，其可分别包括集成存储器和 I/O 控制逻辑（“LC”）2972 和 2982。从而，CL 2972、2982 包括集成存储器控制器单元并且包括 I/O 控制逻辑。图 30 图示不仅存储器 2932、2934 耦合于 LC 2972、2982，而且 I/O 设备 3014 也耦合于控制逻辑 2972、2982。遗留 I/O 设备 3015 耦合于芯片集 2990。

[0225] 至少一个实施例的一个或多个方面可由存储在机器可读介质上的代表性指令来实现，该机器可读介质代表处理器内的各种逻辑，指令在被机器读取时促使机器制造逻辑来进行本文描述的技术。这样的表示（称为“IP 核”）可存储在有形的机器可读介质上并且供应给各种客户或制造设施来装入制造机器，其实际上构成逻辑或处理器。

[0226] 这样的机器可读存储介质可非限制性地包括由机器或设备制造或形成的物品的非暂时性有形设置，包括存储介质，例如硬盘、任何其他类型的盘（包括软盘、光盘、压缩盘只读存储器（CD-ROM）、压缩盘可重写（CD-RW）和磁光盘）、半导体设备，例如只读存储器（ROM）、例如动态随机存取存储器（DRAM）、静态随机存取存储器（SRAM）等随机存取存储器（RAM）、可擦除可编程只读存储器（EPROM）、闪速存储器、电可擦除可编程只读存储器（EEPROM）、相变存储器（PCM）、磁或光卡，或适合于存储电子指令的任何类型的介质。

[0227] 因此，本发明的实施例还包括非暂时性有形机器可读介质，其包含指令或包含设计数据，例如硬件描述语言（HDL），其限定本文描述的结构、电路、装置、处理器和 / 或系统特征。这样的实施例还可称作程序产品。

[0228] 在前面的说明书中，本发明已经参照其具体示范性实施例描述。然而，可对其做出各种修改和改变而不偏离如在附上的权利要求中阐述的本发明的更宽的精神和范围，这将是明显的。因此，说明书和附图在说明性而非限制性意义上来看待。

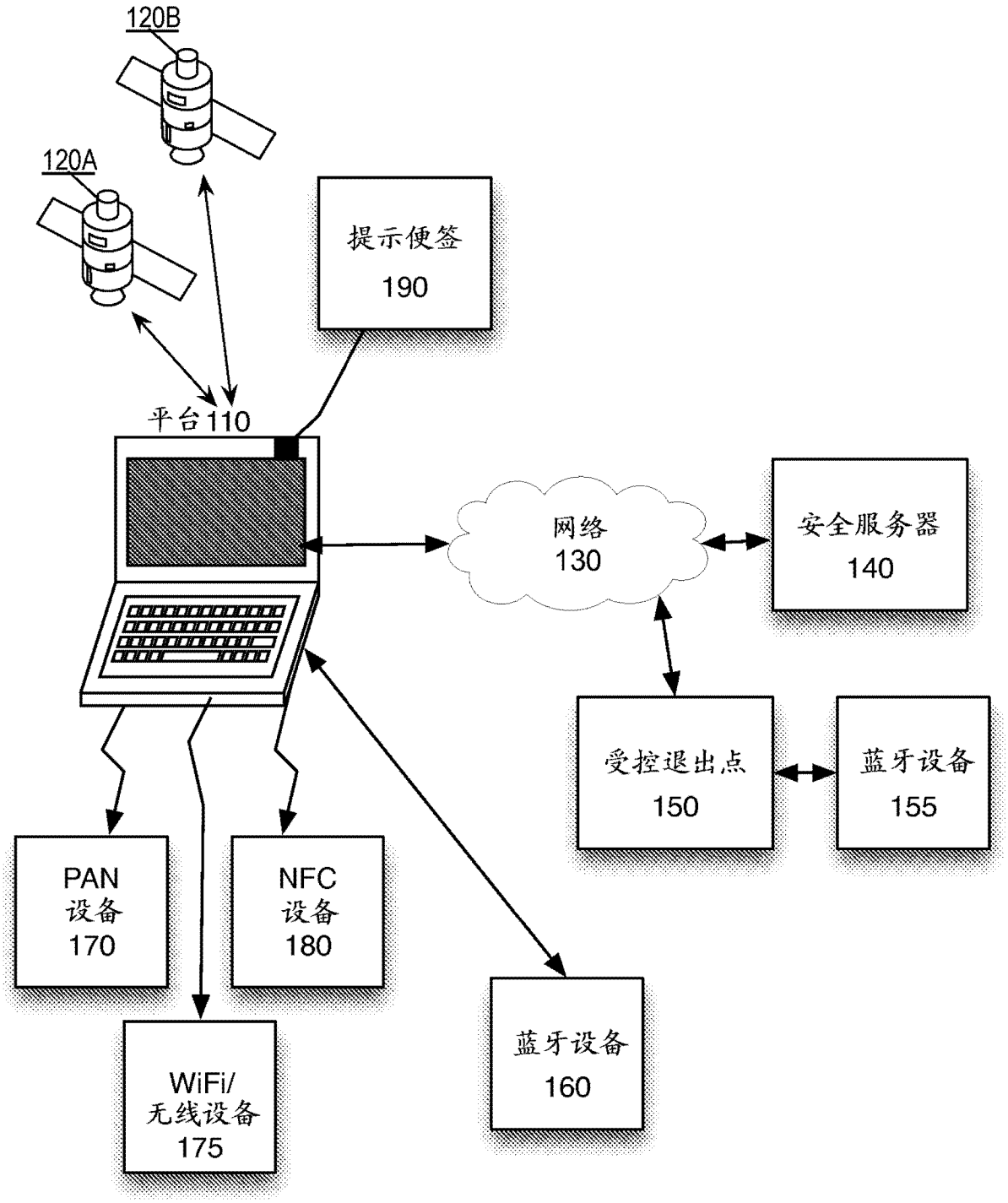

120B
120A
提示便签
190
平台110
网络
130
安全服务器
140
受控退出点
150
蓝牙设备
155
PAN
设备
170
NFC
设备
180
WiFi/
无线设备
175
蓝牙设备
160

图 1

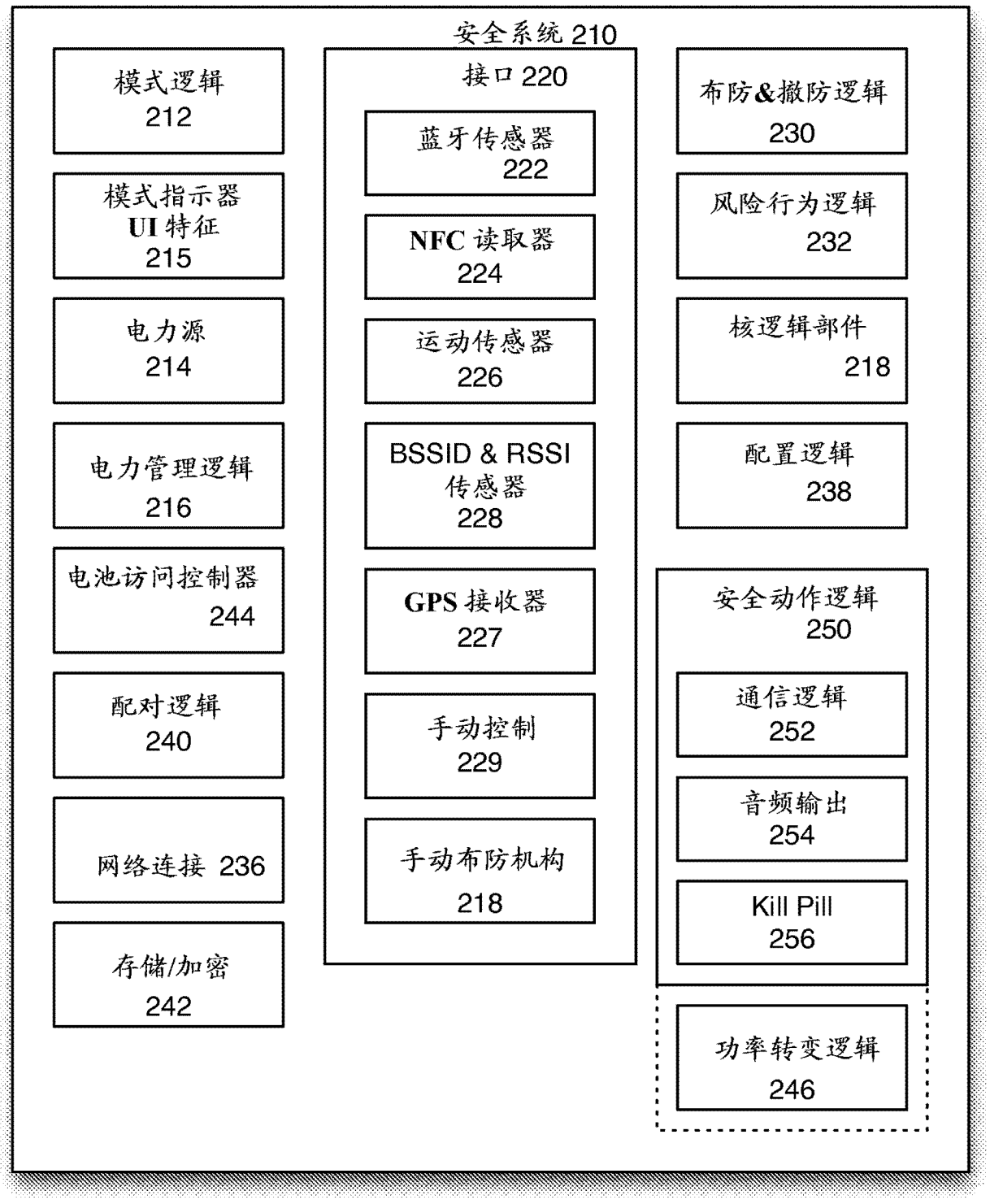

安全系统 210
模式逻辑 212
模式指示器 UI 特征 215
电力源 214
电力管理逻辑 216
电池访问控制器 244
配对逻辑 240
网络连接 236
存储/加密 242
接口 220
蓝牙传感器 222
NFC 读取器 224
运动传感器 226
BSSID & RSSI 传感器 228
GPS 接收器 227
手动控制 229
手动布防机构 218
布防&撤防逻辑 230
风险行为逻辑 232
核逻辑部件 218
配置逻辑 238
安全动作逻辑 250
通信逻辑 252
音频输出 254
Kill Pill 256
功率转变逻辑 246

图 2A

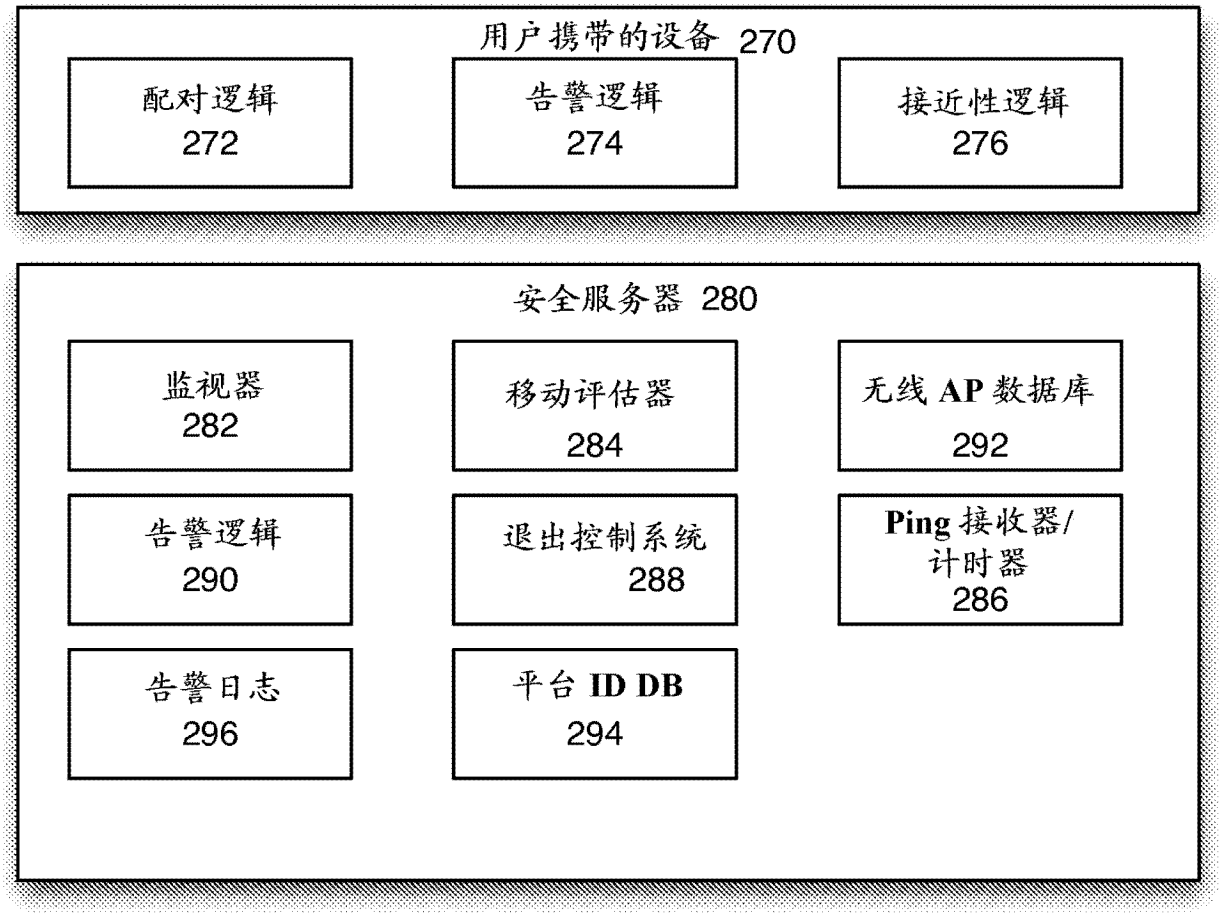

用户携带的设备 270
配对逻辑 272
告警逻辑 274
接近性逻辑 276
安全服务器 280
监视器 282
移动评估器 284
无线 AP 数据库 292
告警逻辑 290
退出控制系统 288
Ping 接收器/计时器 286
告警日志 296
平台 ID DB 294

图 2B

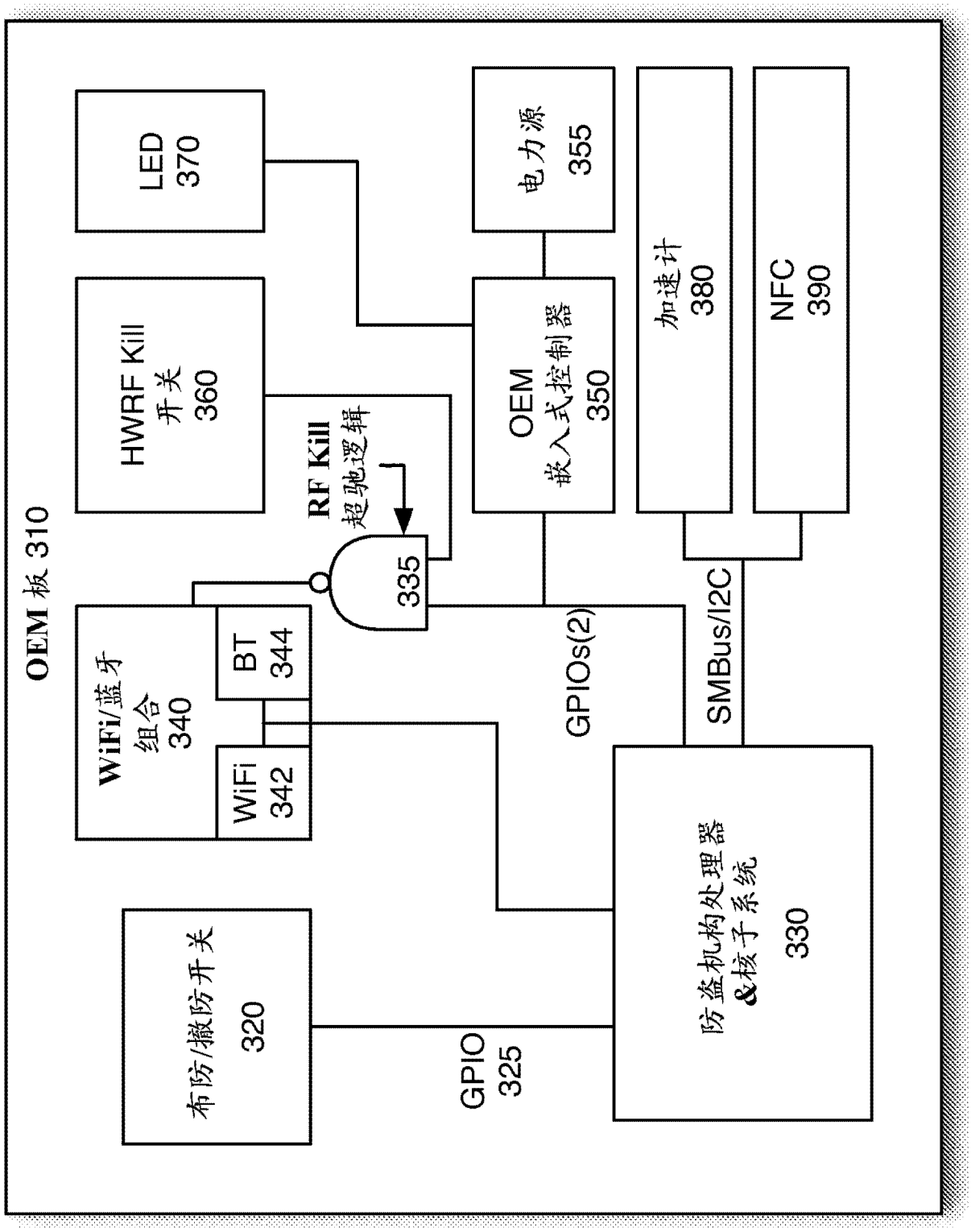

OEM 板 310
LED 370
HWRF Kill 开关 360
RF Kill 超驰逻辑
335
电力源 355
OEM 嵌入式控制器 350
加速计 380
NFC 390
WiFi/蓝牙 组合 340
BT 344
WiFi 342
GPIOs(2)
SMBus/I2C
布防/撤防开关 320
GPIO 325
防盗机构处理器 &板子系统 330

图 3

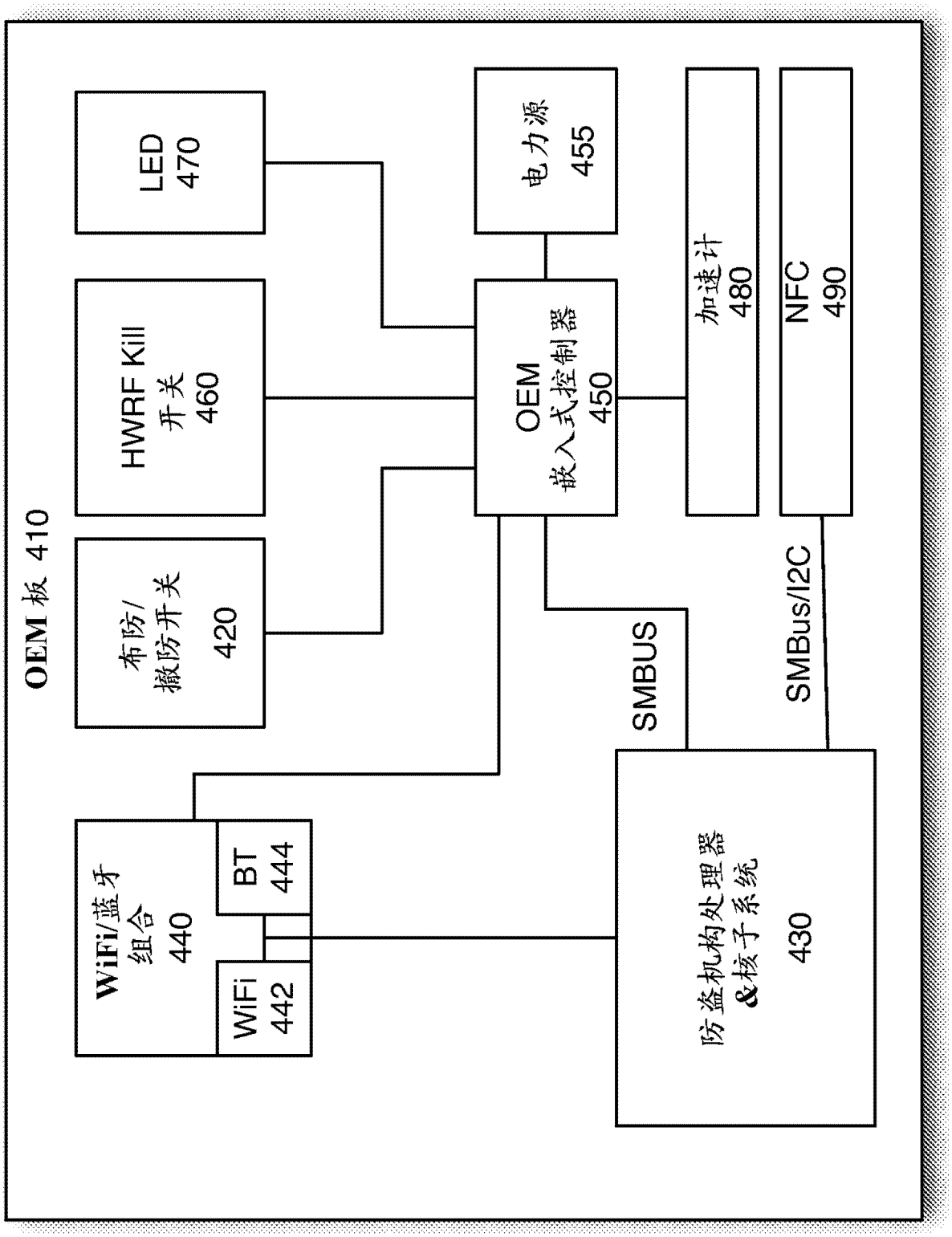

OEM 板 410
LED 470
HWRF Kill 开关 460
布防/撤防开关 420
WiFi/蓝牙组合 440
BT 444
WiFi 442
OEM 嵌入式控制器 450
电力源 455
加速计 480
NFC 490
SMBUS
SMBus/I2C
防盗机构处理器 &核子系统 430

图 4

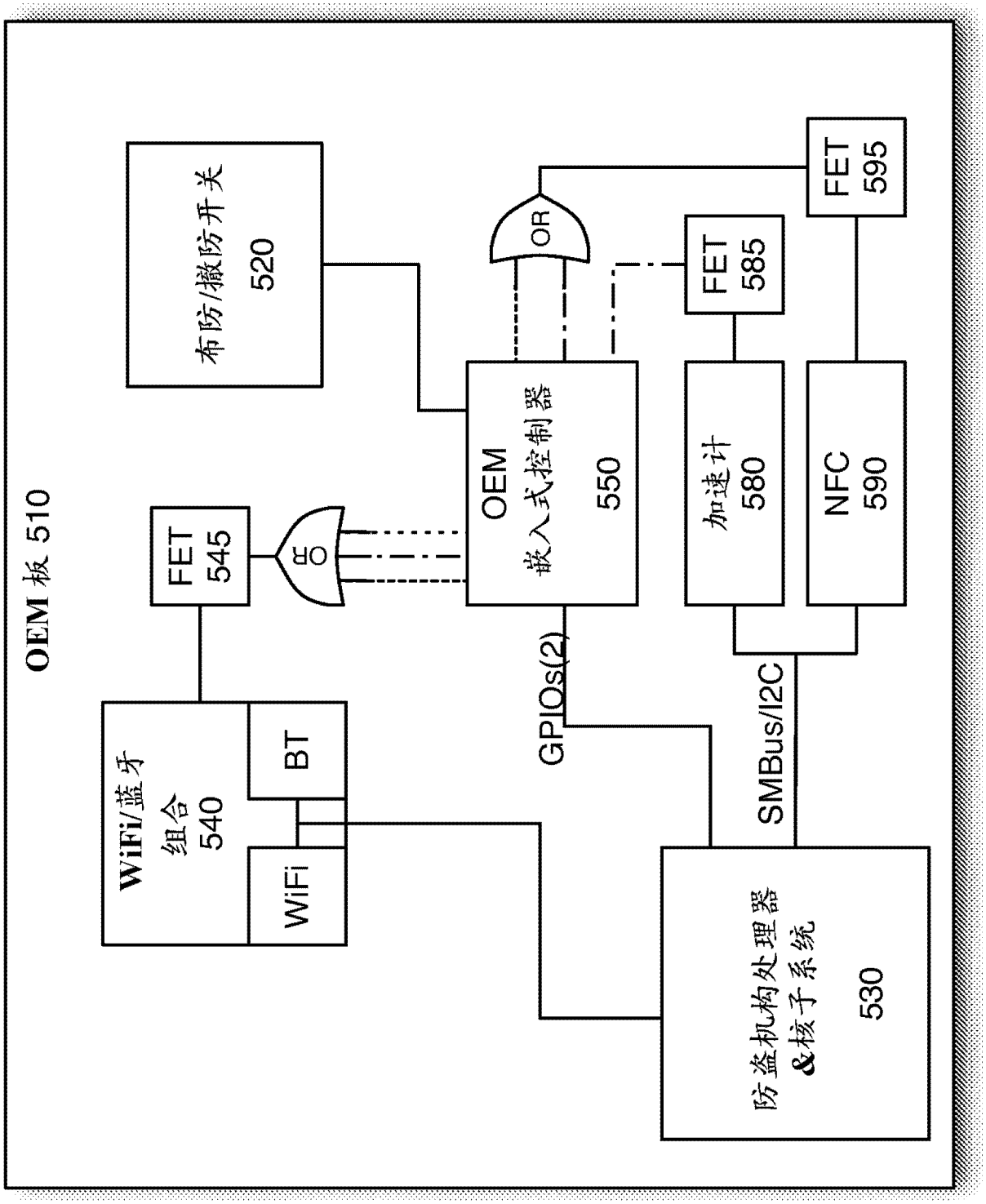

OEM 板 510
布防/撤防开关 520
FET 595
OR
FET 585
OEM 嵌入式控制器 550
加速计 580
NFC 590
FET 545
GPIOs(2)
SMBus/I2C
WiFi/蓝牙 组合 540
BT
WiFi
防盗机构处理器 &核子系统 530

图 5

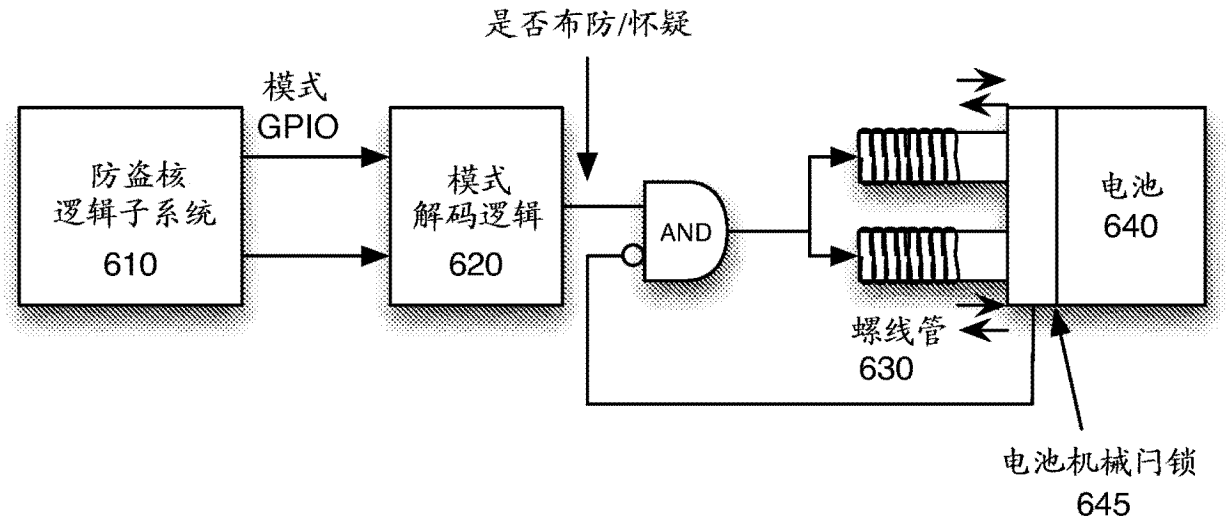

是否布防/怀疑
模式
GPIO
防盗核
逻辑子系统
610
模式
解码逻辑
620
AND
电池
640
螺线管
630
电池机械闩锁
645

图 6A

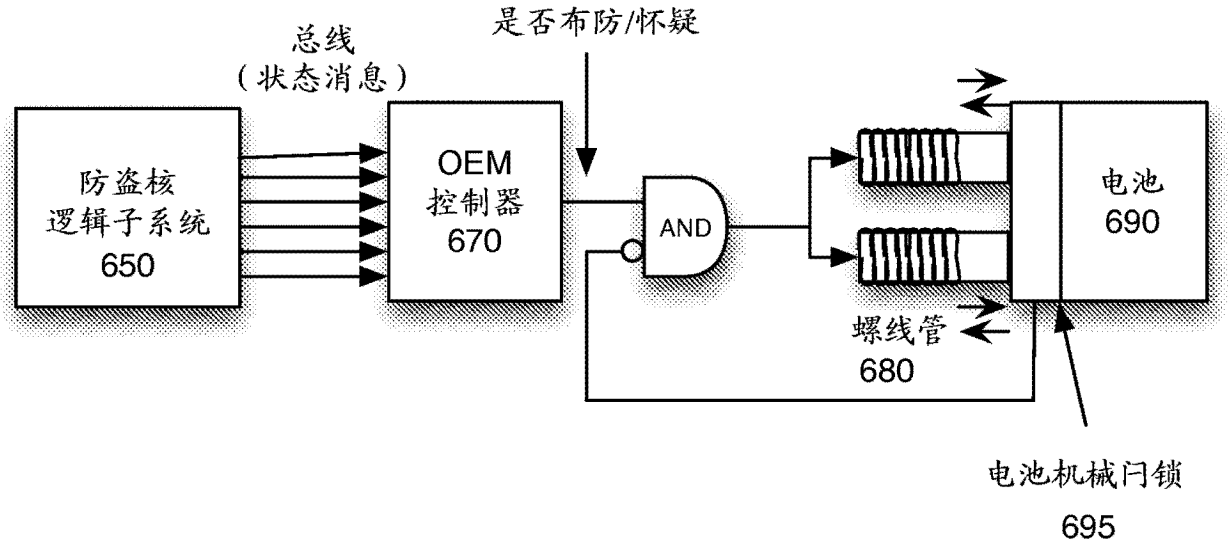

总线
(状态消息)
是否布防/怀疑
防盗核
逻辑子系统
650
OEM
控制器
670
AND
电池
690
螺线管
680
电池机械闩锁
695

图 6B

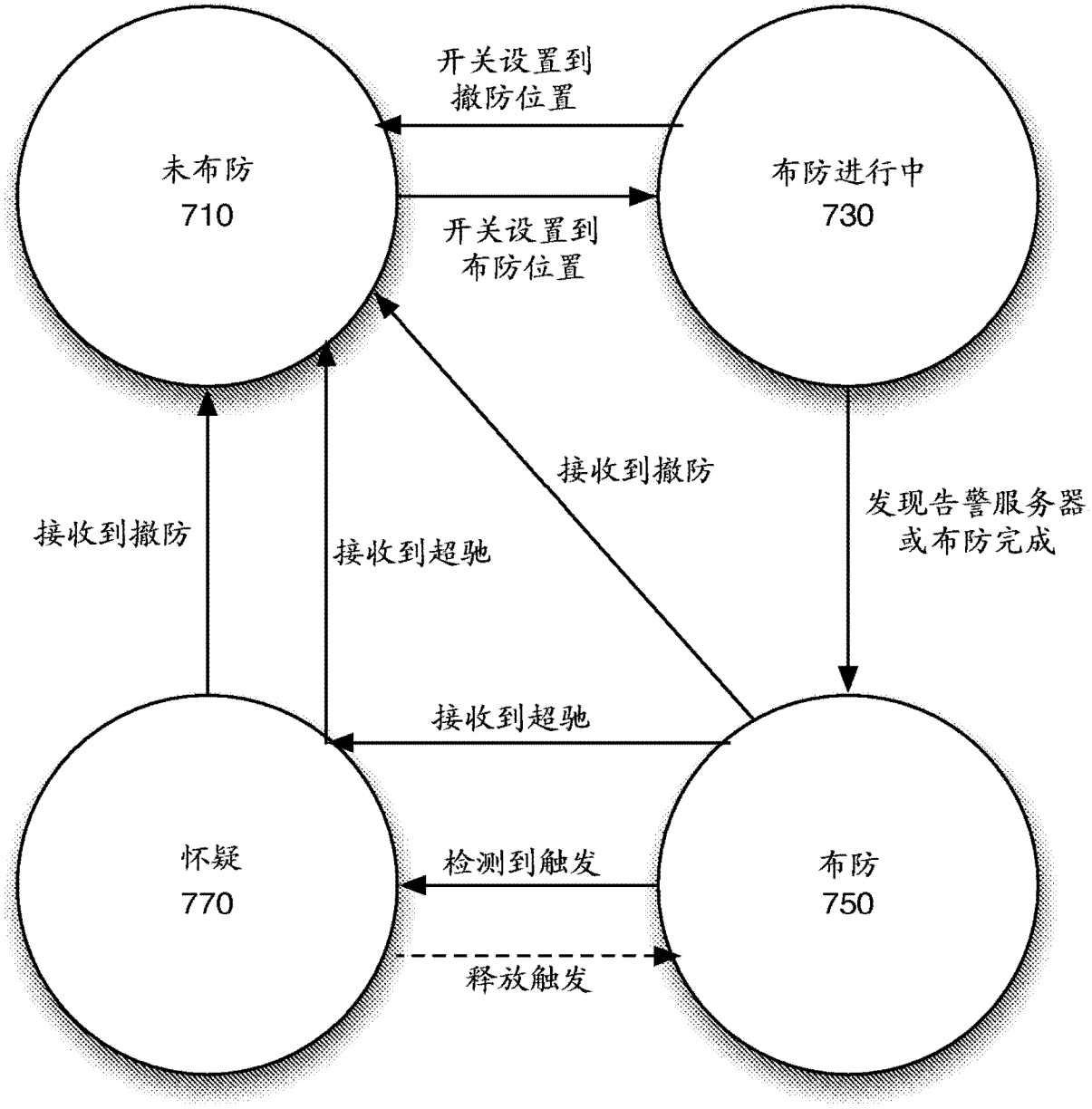

未布防
710
布防进行中
730
怀疑
770
布防
750
开关设置到
撤防位置
开关设置到
布防位置
接收到撤防
接收到超驰
接收到撤防
发现告警服务器
或布防完成
接收到超驰
检测到触发
释放触发

图 7

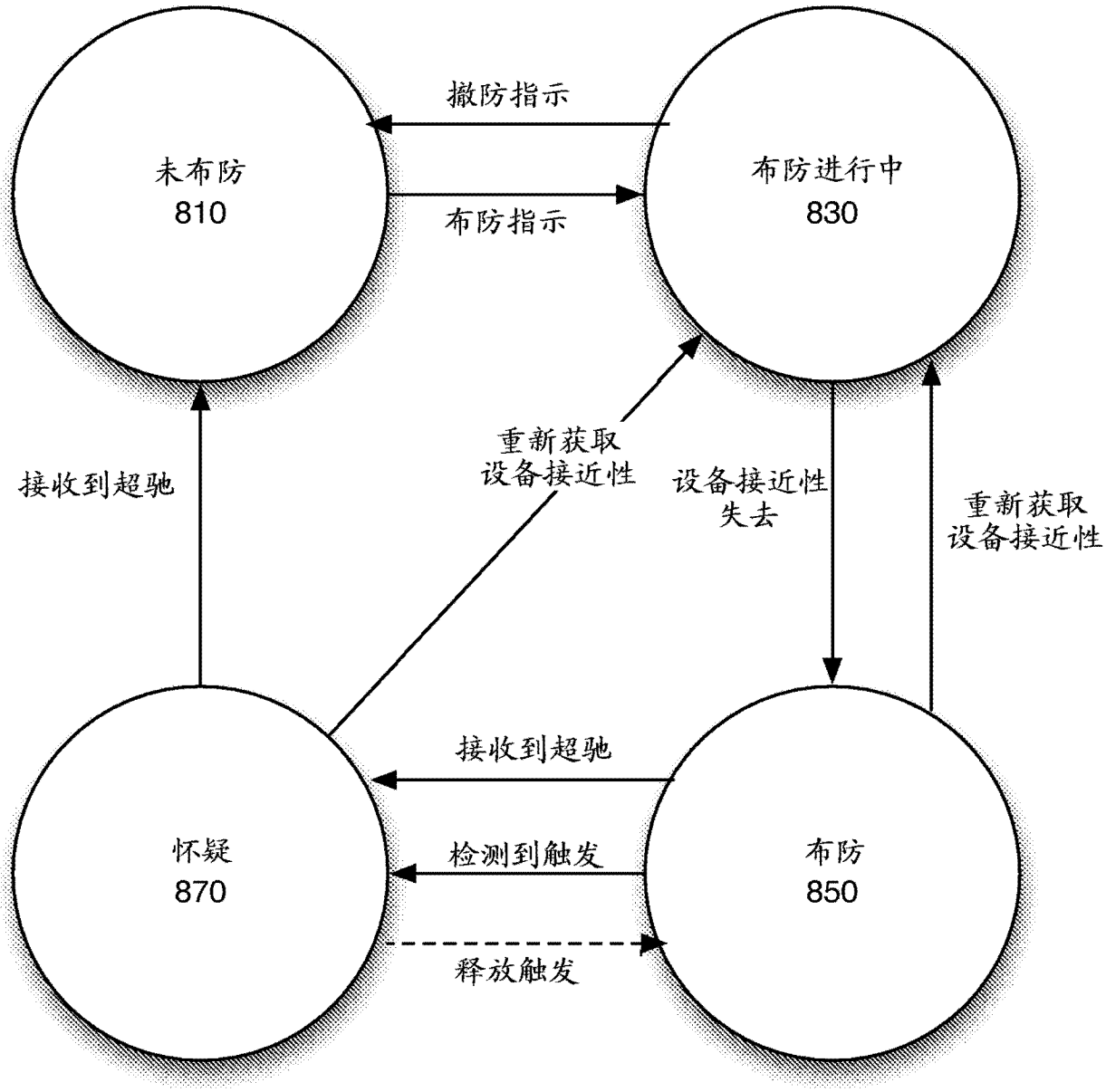

未布防
810
撤防指示
布防指示
布防进行中
830
接收到超驰
重新获取
设备接近性
设备接近性
失去
重新获取
设备接近性
接收到超驰
检测到触发
释放触发
怀疑
870
布防
850

图 8

	模式			
	未布防	布防进行中	布防	怀疑
LED	关闭	布防中（闪光）	布防（照亮）	怀疑（闪烁）
包发送	撤防（如布防的话）	初始连接	布防	通知再怀疑
配置	解塞	-	阻塞	阻塞
转变计时器	取消	取消	取消	用来转变

图 9

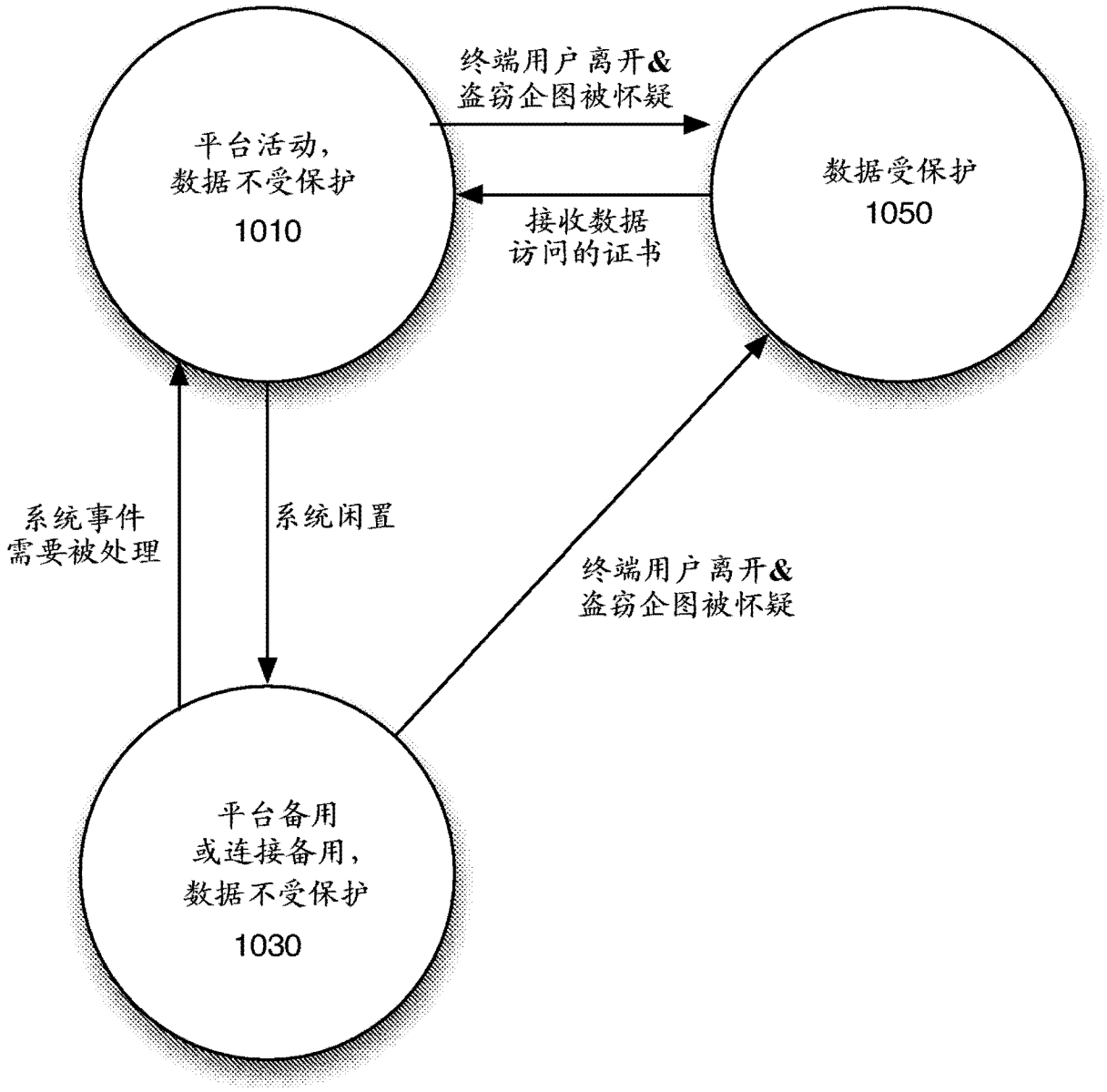

平台活动，
数据不受保护
1010
终端用户离开&
盗窃企图被怀疑
接收数据
访问的证书
数据受保护
1050
系统事件
需要被处理
系统闲置
终端用户离开&
盗窃企图被怀疑
平台备用
或连接备用，
数据不受保护
1030

图 10

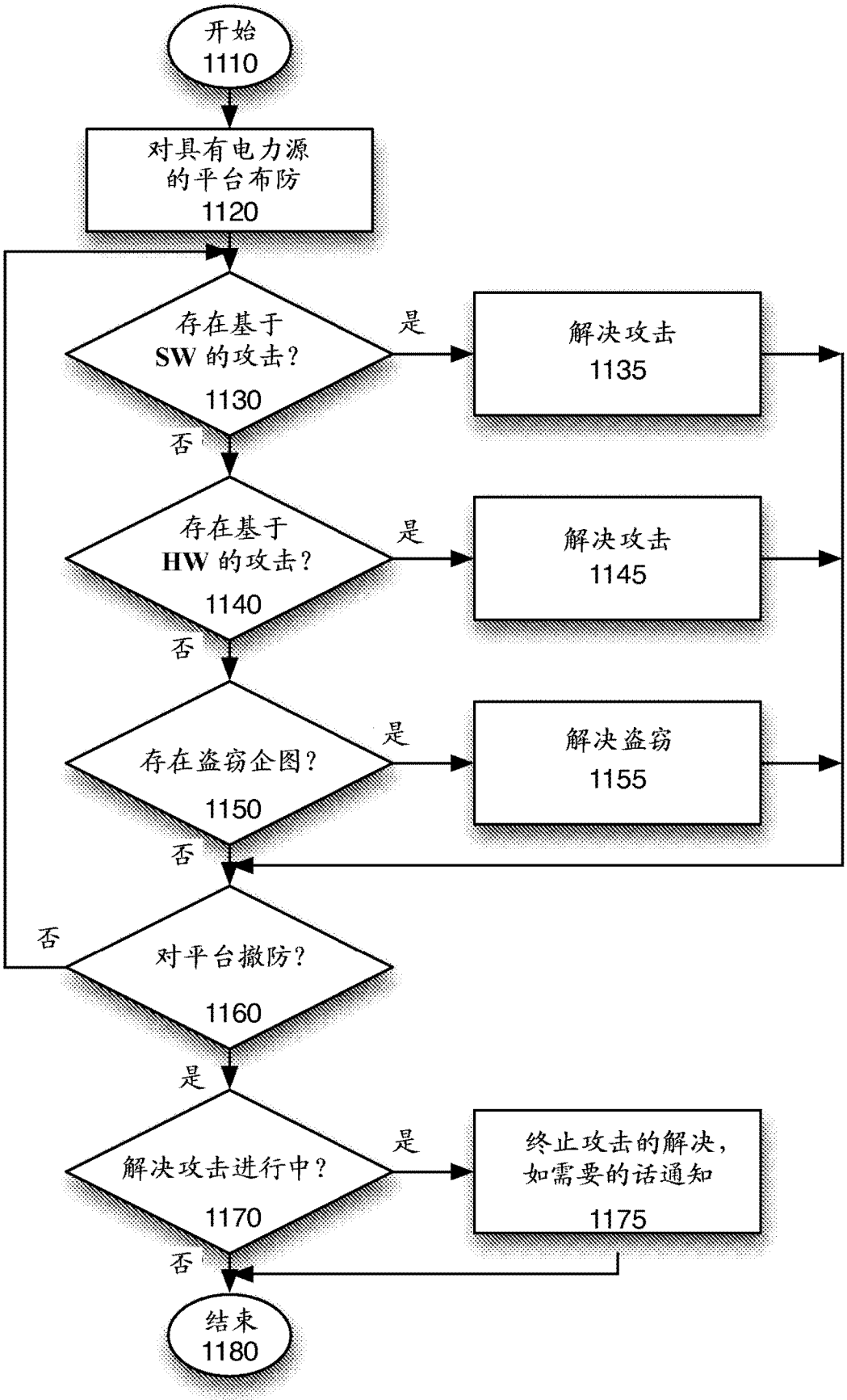

开始
1110
对具有电力源的平台布防
1120
存在基于SW的攻击？
1130
是
解决攻击
1135
否
存在基于HW的攻击？
1140
是
解决攻击
1145
否
存在盗窃企图？
1150
是
解决盗窃
1155
否
对平台撤防？
1160
否
是
解决攻击进行中？
1170
是
终止攻击的解决，如需要的话通知
1175
否
结束
1180

图 11A

用户可能离开平台？	可能有人拿走平台？	平台模式&动作	服务器动作	用户携带的设备动作
否	否	未布防/布防进行中	没有	没有
否	是	未布防/布防进行中	没有	没有
是	否	布防	没有	没有（用户配置的策略是在接近性失去时电话不告警）
是	否	布防	没有	告警（用户配置的策略是在接近性失去时电话告警）
是	是	怀疑-保护数据和/或发送告警	跟踪-告警保持到达但示出没有明显的移动	没有（用户配置的策略是在接近性失去时电话不告警）
是	是	怀疑-保护数据和/或发送告警	跟踪-告警保持到达但示出没有明显的移动	告警（用户配置的策略是在接近性失去时电话告警）
是	是	怀疑-保护数据和/或发送告警	告警（例如，拥有方、用户、守卫）-告警示出明显的移动或突然停止到达	没有（用户配置的策略是在接近性失去时电话不告警）
是	是	怀疑-保护数据和/或发送告警	告警（例如，拥有方、用户、守卫）-告警示出明显的移动或突然停止到达	告警（用户配置的策略是在接近性失去时电话告警）

图 11B

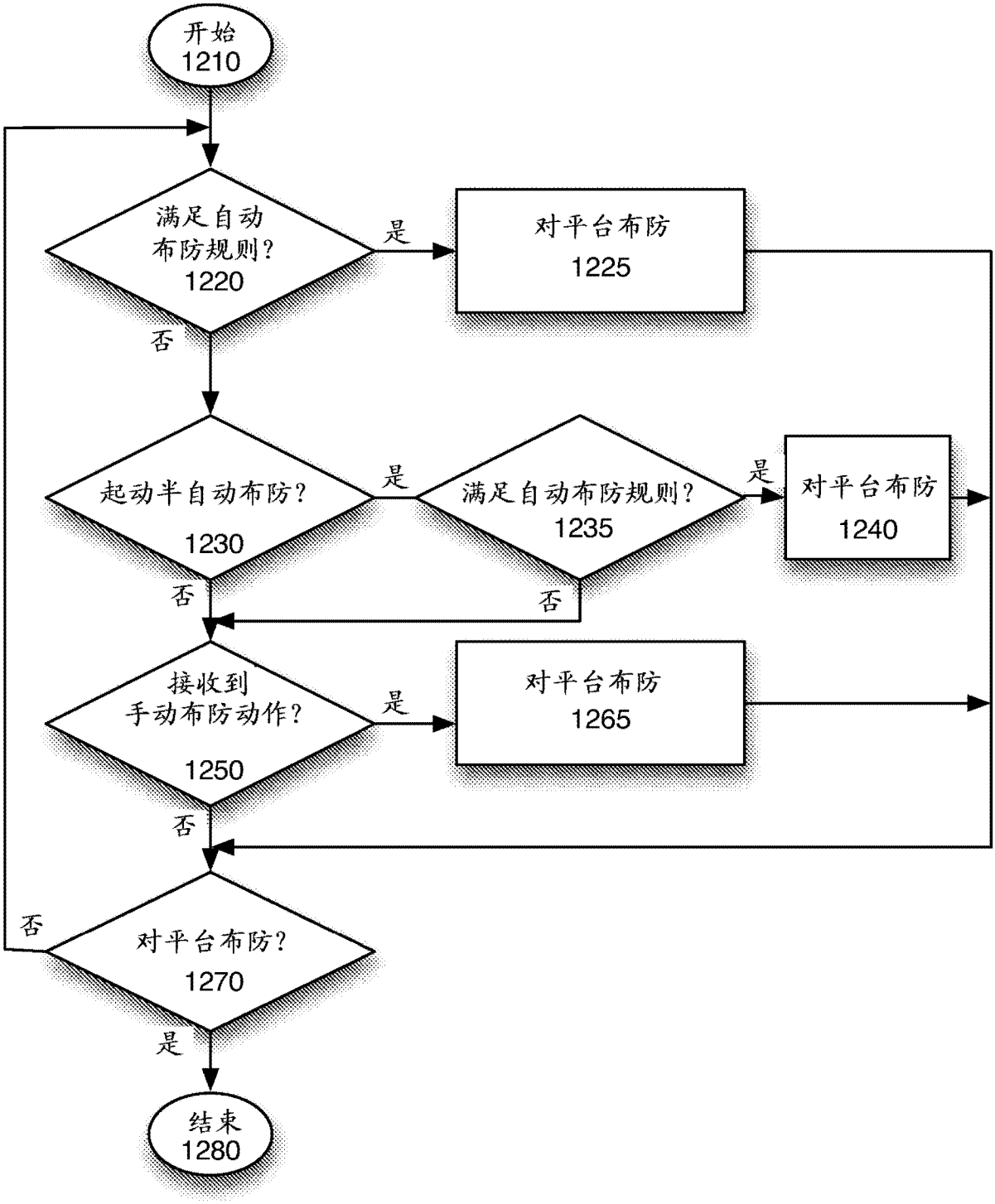

开始
1210
满足自动布防规则？
1220
是
对平台布防
1225
否
起动半自动布防？
1230
是
满足自动布防规则？
1235
是
对平台布防
1240
否
否
接收到手动布防动作？
1250
是
对平台布防
1265
否
否
对平台布防？
1270
是
结束
1280

图 12

手动布防	自动布防
键盘功能/键	位点/一天中的时间
NFC 分接	从网络断连
物理开关/按钮	蓝牙接近性失去
语音命令	拍摄装置中失去用户的面部
生物计量/指纹	关闭盖子/设备移动
移动序列	设备闲置
软件开关/按钮	个人区域网配置失去
图标选择	计时器

图 13

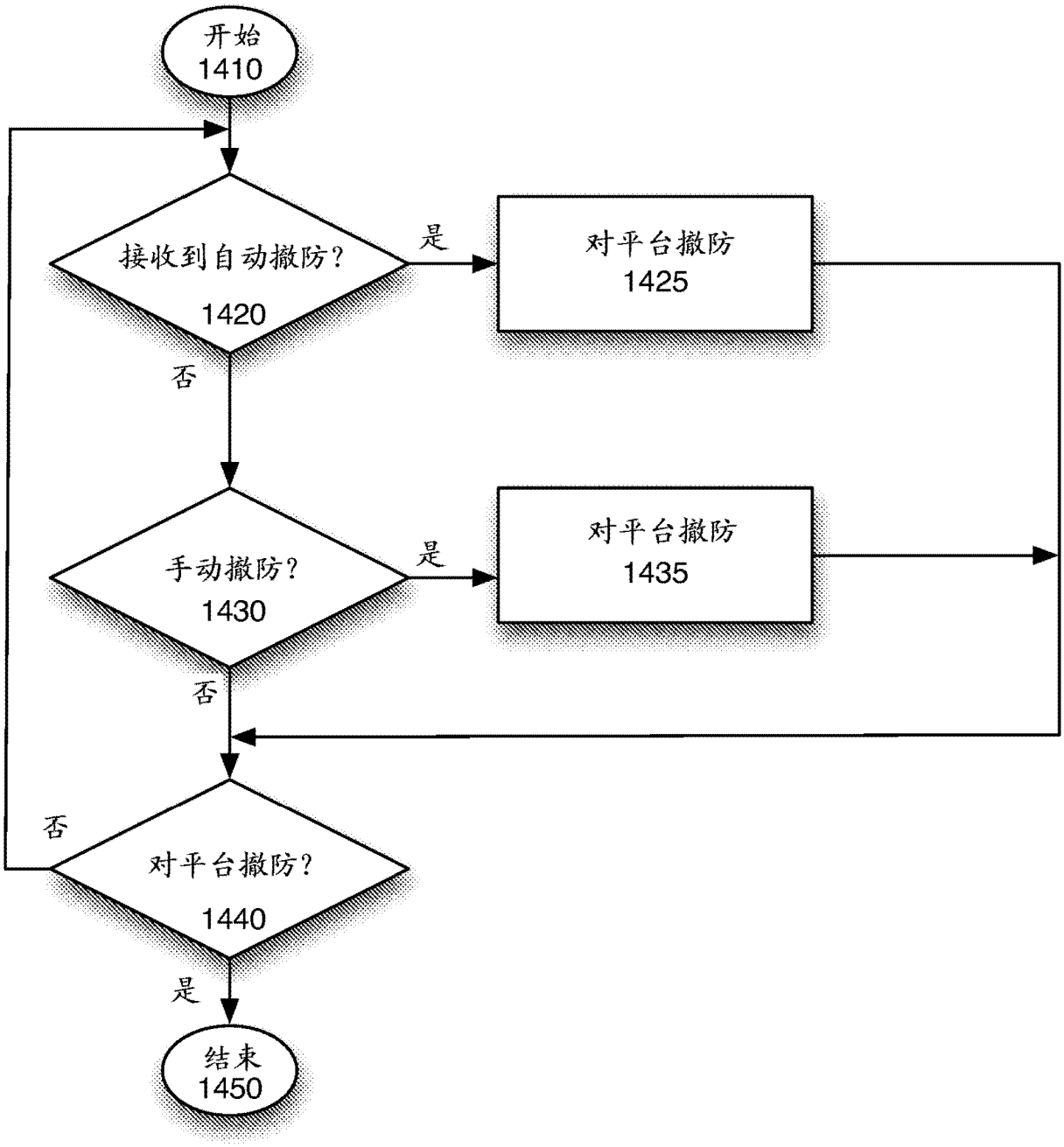

开始
1410
接收到自动撤防？
1420
是
对平台撤防
1425
否
手动撤防？
1430
是
对平台撤防
1435
否
否
对平台撤防？
1440
是
结束
1450

图 14

手动撤防	自动撤防
近场通信	检测到蓝牙接近性
密码输入	经由拍摄装置的用户 ID
语音命令	已知网络连接性的存在
生物计量/指纹	检测到个人区域网配置
移动序列	图形位点识别

图 15

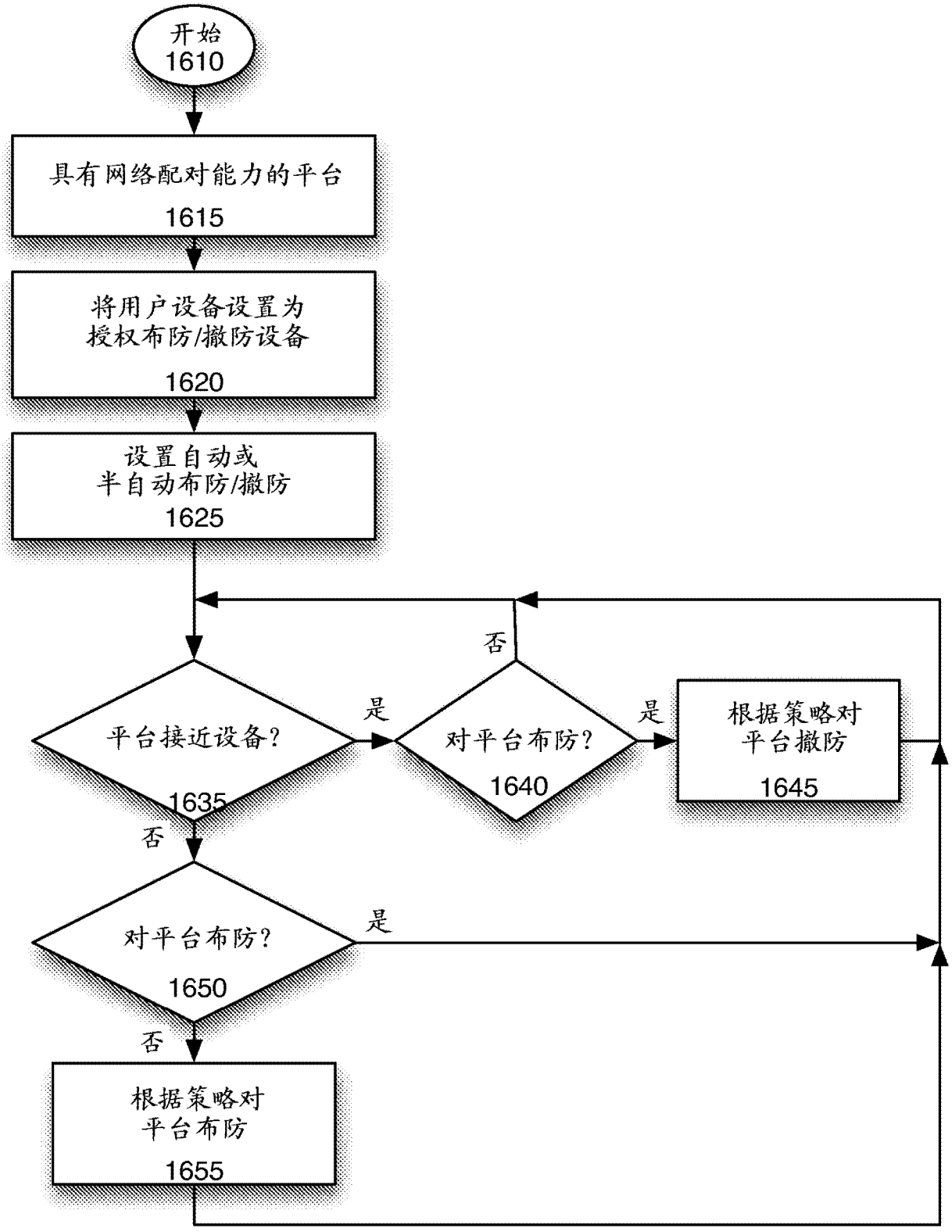

开始
1610
具有网络配对能力的平台
1615
将用户设备设置为
授权布防/撤防设备
1620
设置自动或
半自动布防/撤防
1625
平台接近设备?
1635
是
对平台布防?
1640
否
是
根据策略对
平台撤防
1645
否
对平台布防?
1650
是
否
根据策略对
平台布防
1655

图 16

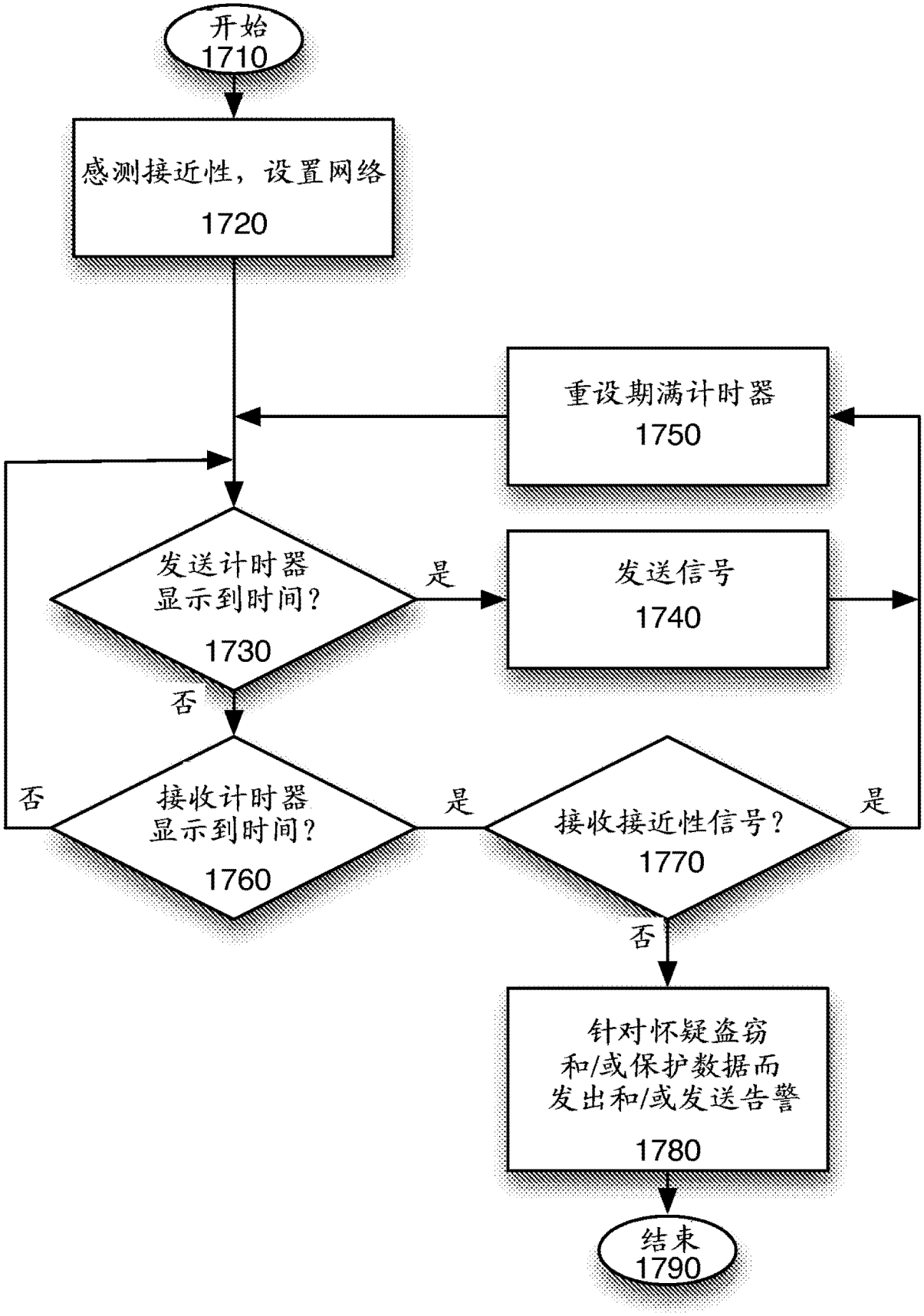

开始
1710
感测接近性，设置网络
1720
重设期满计时器
1750
发送计时器
显示到时间？
1730
是
发送信号
1740
否
否
接收计时器
显示到时间？
1760
是
接收接近性信号？
1770
是
否
针对怀疑盗窃
和/或保护数据而
发出和/或发送告警
1780
结束
1790

图 17

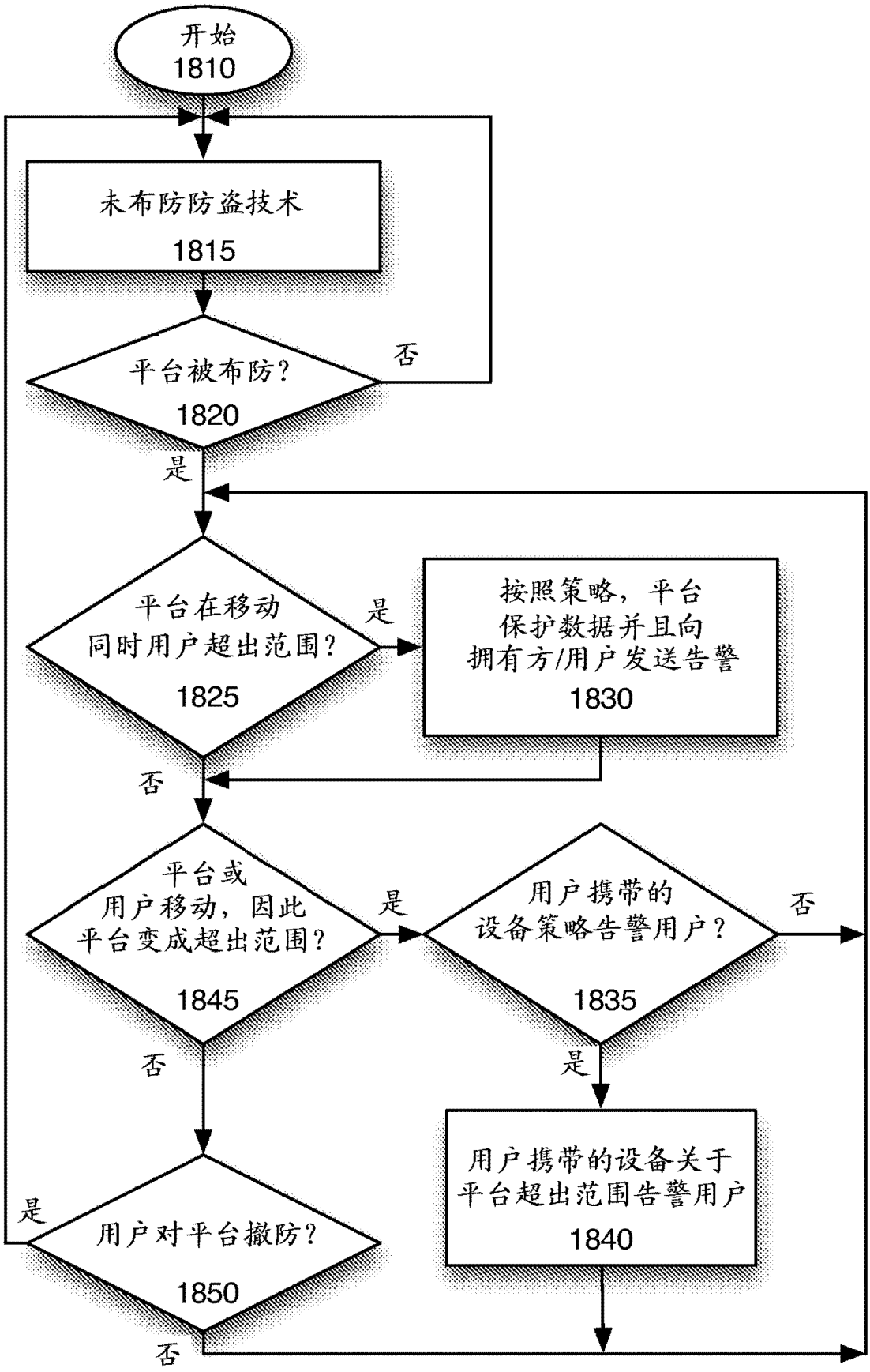

开始
1810
未布防防盗技术
1815
平台被布防？
1820
否
是
平台在移动
同时用户超出范围？
1825
是
按照策略，平台
保护数据并且向
拥有方/用户发送告警
1830
否
平台或
用户移动，因此
平台变成超出范围？
1845
是
用户携带的
设备策略告警用户？
1835
否
否
是
用户携带的设备关于
平台超出范围告警用户
1840
是
用户对平台撤防？
1850
否

图 18

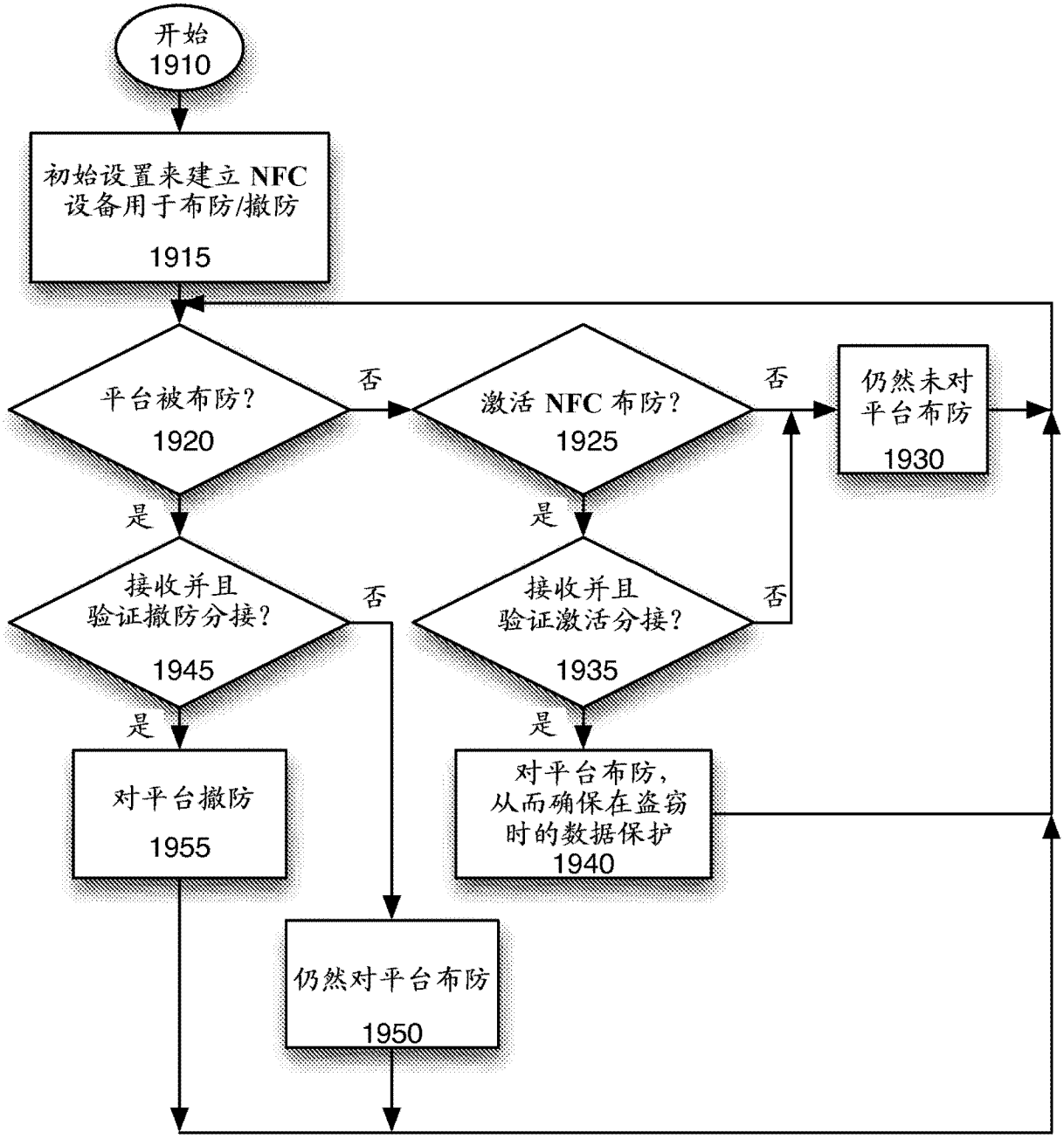

开始
1910
初始设置来建立 NFC 设备用于布防/撤防
1915
平台被布防?
1920
否
激活 NFC 布防?
1925
否
仍然未对平台布防
1930
是
是
接收并且验证撤防分接?
1945
否
接收并且验证激活分接?
1935
否
是
是
对平台撤防
1955
对平台布防，从而确保在盗窃时的数据保护
1940
仍然对平台布防
1950

图 19

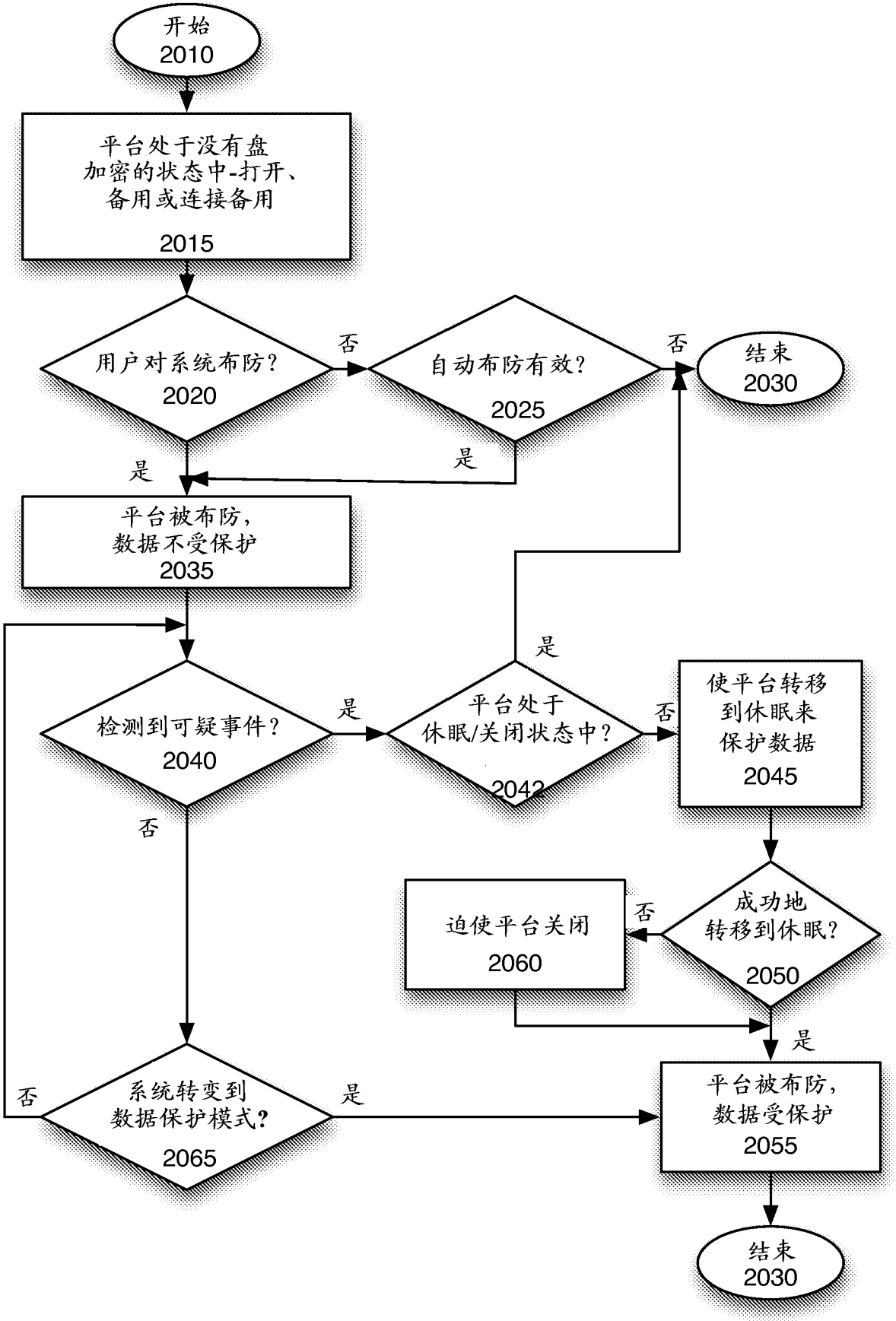

开始
2010
平台处于没有盘加密的状态中-打开、备用或连接备用
2015
用户对系统布防?
2020
否
自动布防有效?
2025
否
结束
2030
是
是
平台被布防，数据不受保护
2035
检测到可疑事件?
2040
是
平台处于休眠/关闭状态中?
2042
是
否
使平台转移到休眠来保护数据
2045
否
成功地转移到休眠?
2050
否
迫使平台关闭
2060
是
系统转变到数据保护模式?
2065
否
是
平台被布防，数据受保护
2055
结束
2030

图 20

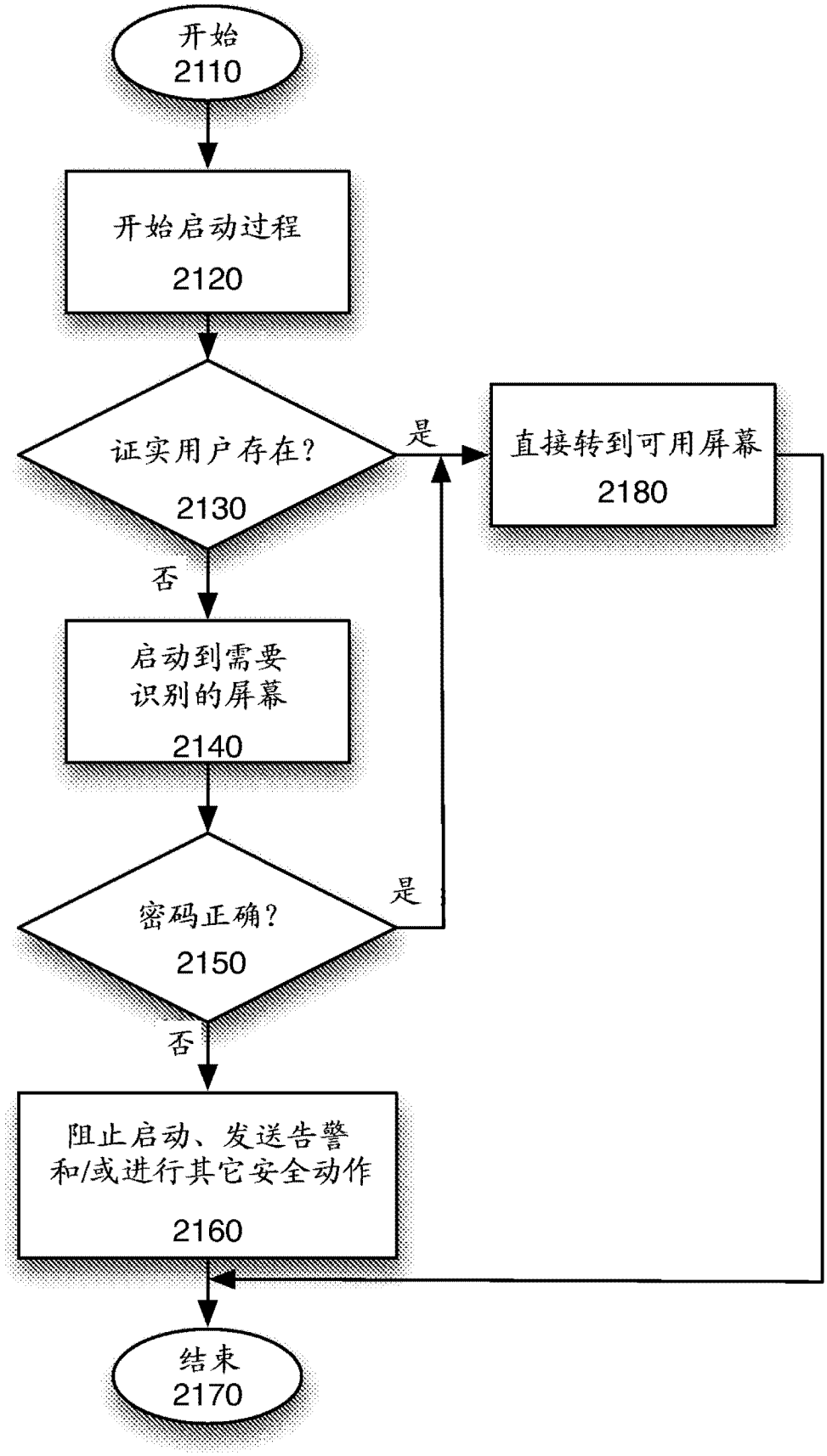

开始
2110
开始启动过程
2120
证实用户存在?
2130
是
直接转到可用屏幕
2180
否
启动到需要
识别的屏幕
2140
密码正确?
2150
是
否
阻止启动、发送告警
和/或进行其它安全动作
2160
结束
2170

图 21

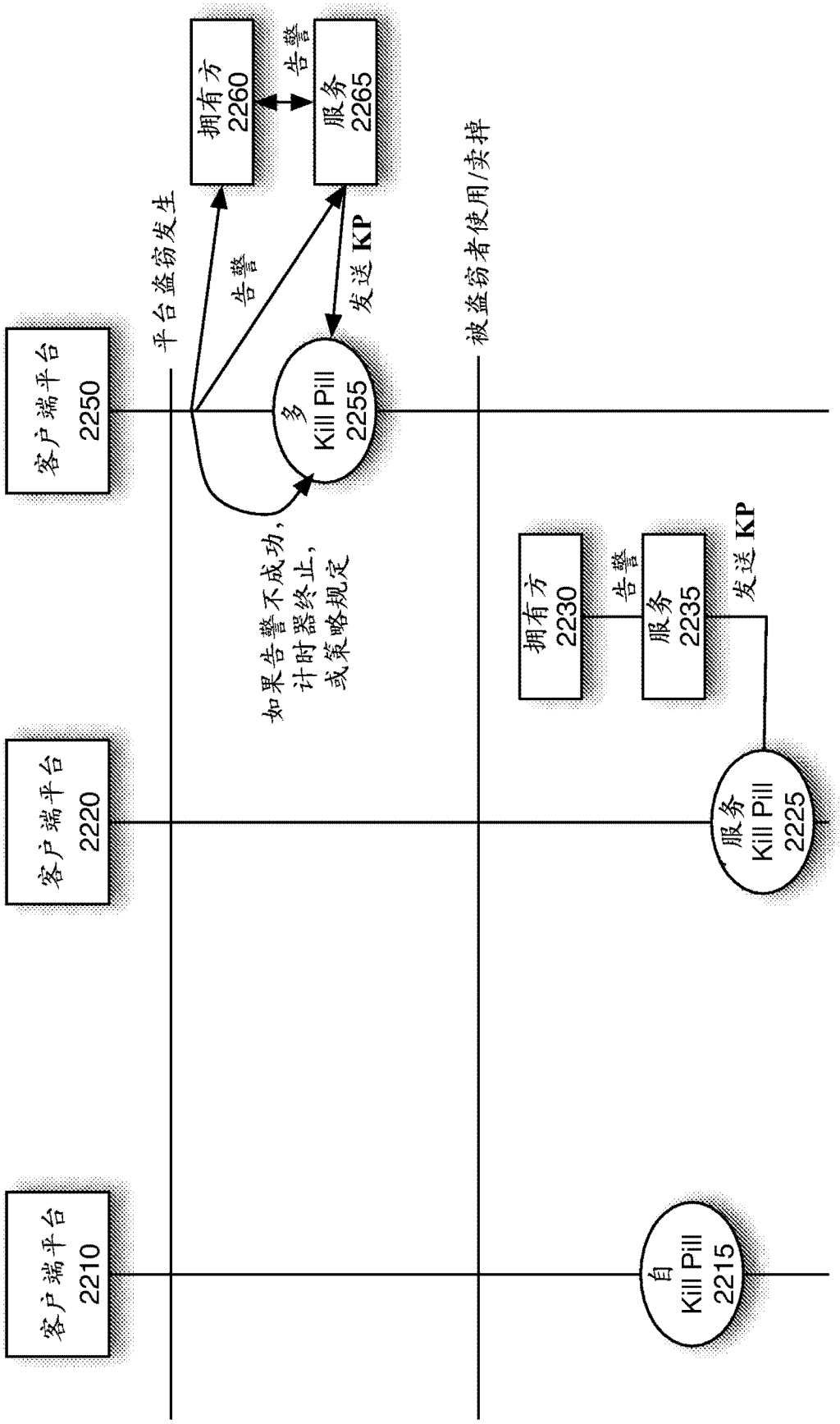

客户端平台
2210
客户端平台
2220
客户端平台
2250
自
Kill Pill
2215
服务
Kill Pill
2225
多
Kill Pill
2255
拥有方
2230
服务
2235
拥有方
2260
服务
2265
告警
告警
发送 KP
发送 KP
平台盗窃发生
被盗窃者使用/卖掉
如果告警不成功，
计时器终止，
或策略规定

图 22

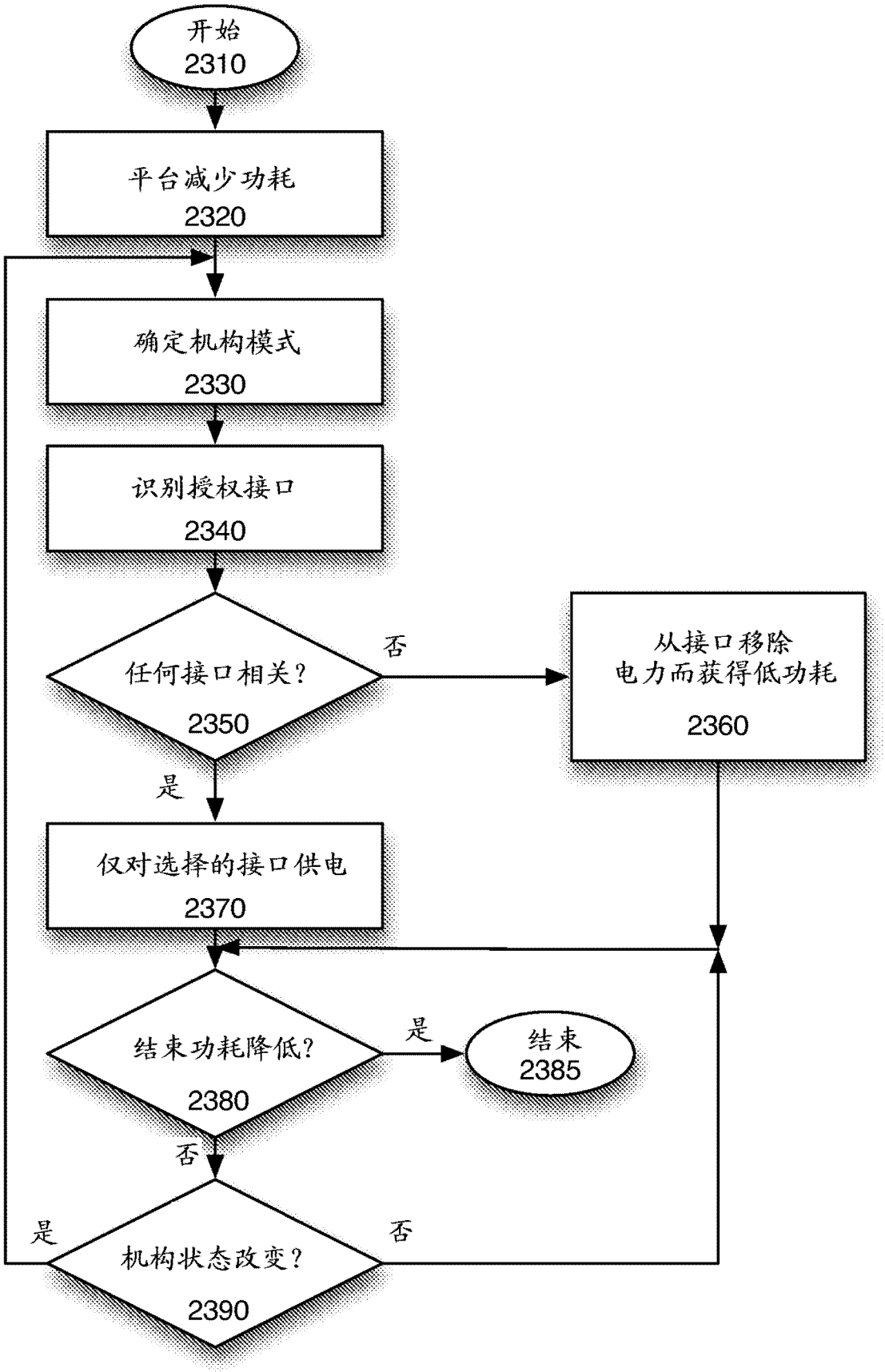

开始
2310
平台减少功耗
2320
确定机构模式
2330
识别授权接口
2340
任何接口相关?
2350
否
从接口移除
电力而获得低功耗
2360
是
仅对选择的接口供电
2370
结束功耗降低?
2380
是
结束
2385
否
是
机构状态改变?
2390
否

图 23

	未布防	布防进行中	布防	怀疑
触发开始布防过程（如果不是机械的）	是-NFC、按钮、键盘或其他	否	否	否
触发完成布防过程	否	是：接近性传感器或相似的传感器	否	否
触发检测可能的盗窃事件	否	否	是：移动传感器	否
触发起动防盗响应	否	否	否	是：对通信系统供电
触发开始撤防过程	否	否	是：接近性传感器，或其他用户存在传感器	是：接近性传感器或其他用户存在传感器
触发完成撤防过程	否	是：键盘	否	否

图 24

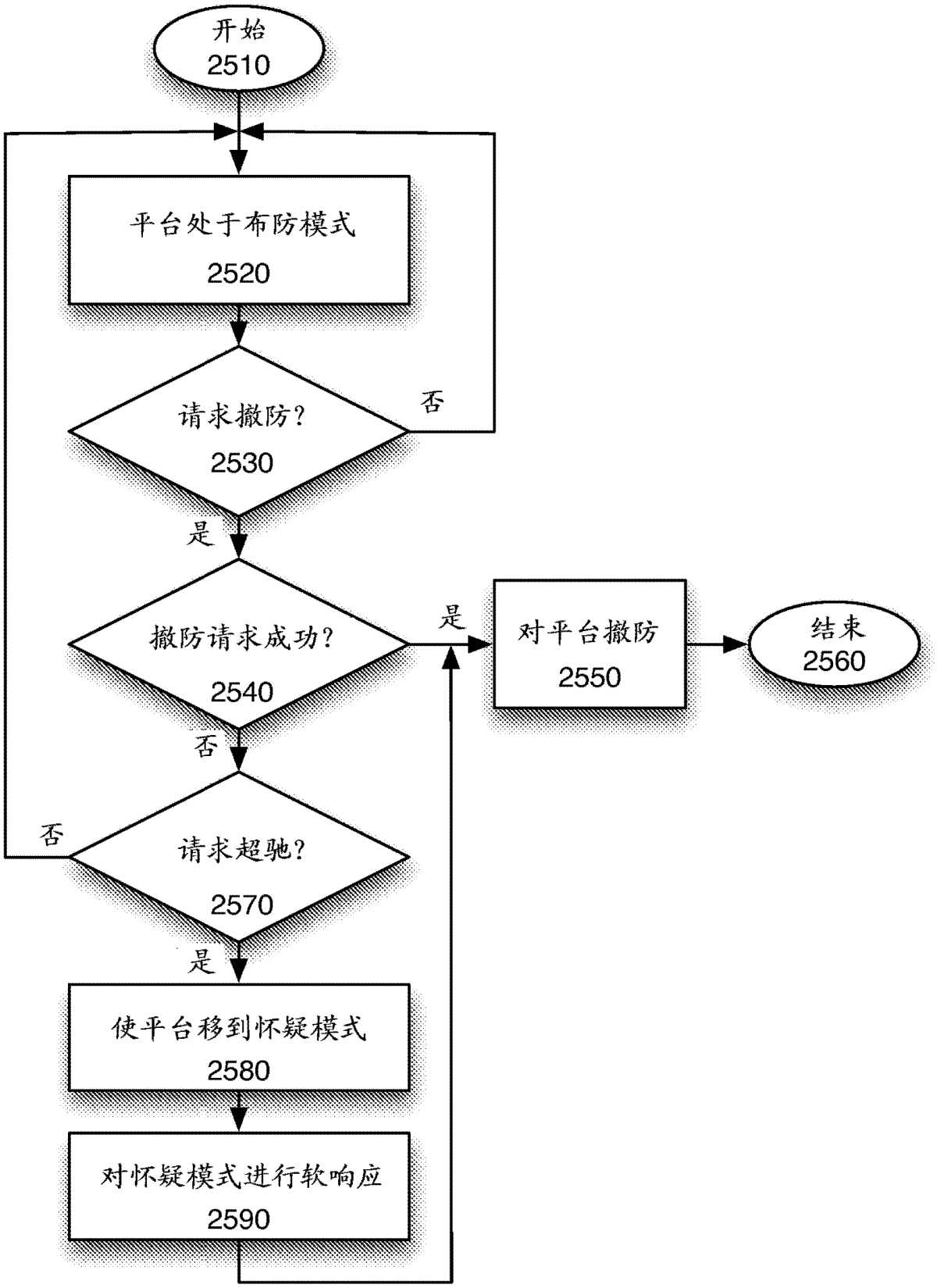

开始
2510
平台处于布防模式
2520
请求撤防?
2530
否
是
撤防请求成功?
2540
是
对平台撤防
2550
结束
2560
否
否
请求超驰?
2570
是
使平台移到怀疑模式
2580
对怀疑模式进行软响应
2590

图 25

	盗窃者可能偷数据和资产	拥有方可能因不能使用的系统而终止
没有超驰	否	是
具有特殊密码超驰	否	是
具有无状态改变的不安全超驰	是	否
不安全超驰，具有怀疑状态，以及硬防盗动作	否	是
不安全超驰，具有怀疑状态，和软防盗动作	否	否

图 26

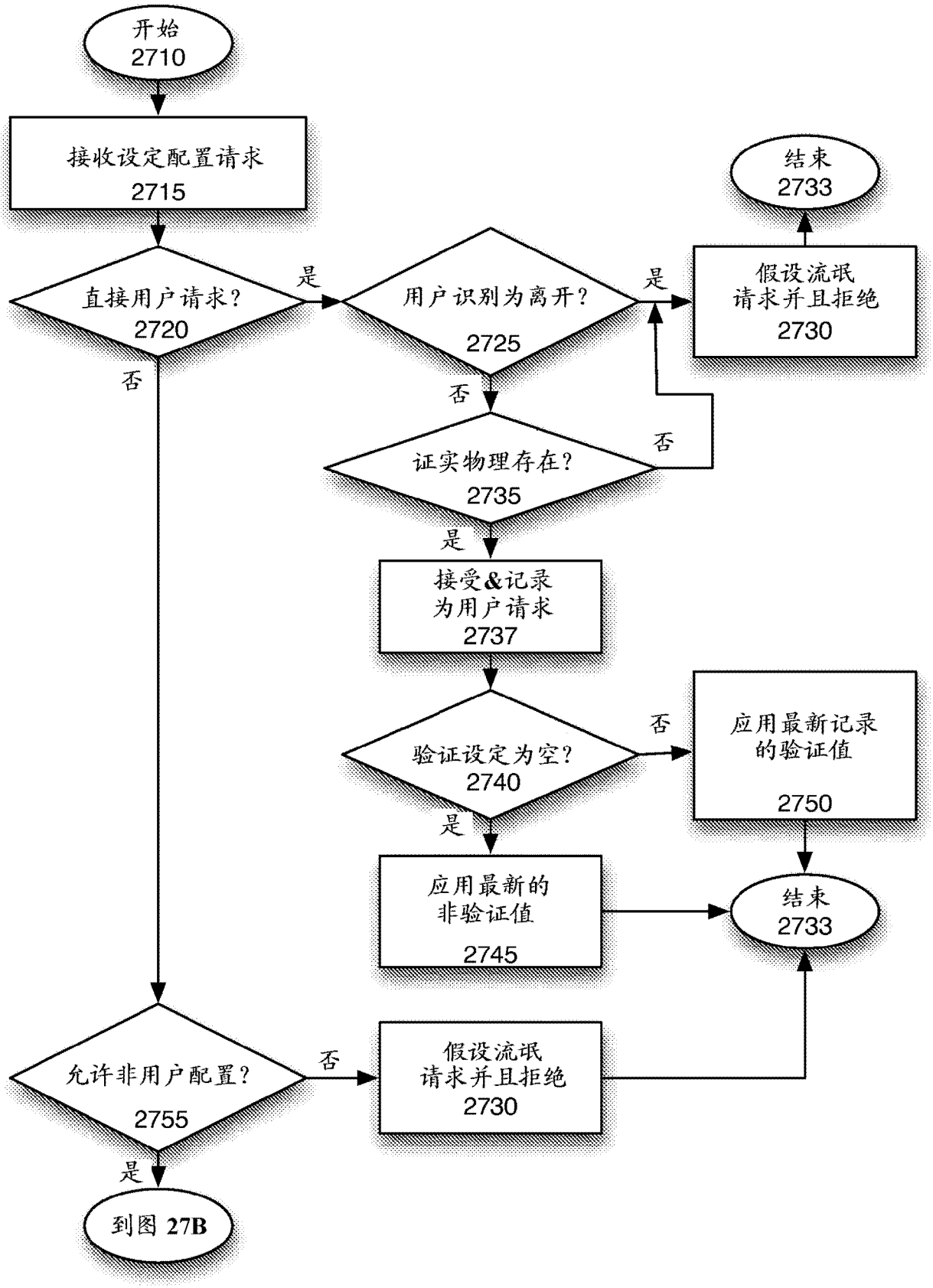

开始
2710
接收设定配置请求
2715
直接用户请求？
2720
是
否
用户识别为离开？
2725
是
否
假设流氓
请求并且拒绝
2730
结束
2733
证实物理存在？
2735
否
是
接受&记录
为用户请求
2737
验证设定为空？
2740
否
是
应用最新记录
的验证值
2750
应用最新的
非验证值
2745
结束
2733
允许非用户配置？
2755
否
是
假设流氓
请求并且拒绝
2730
到图 27B

图 27A

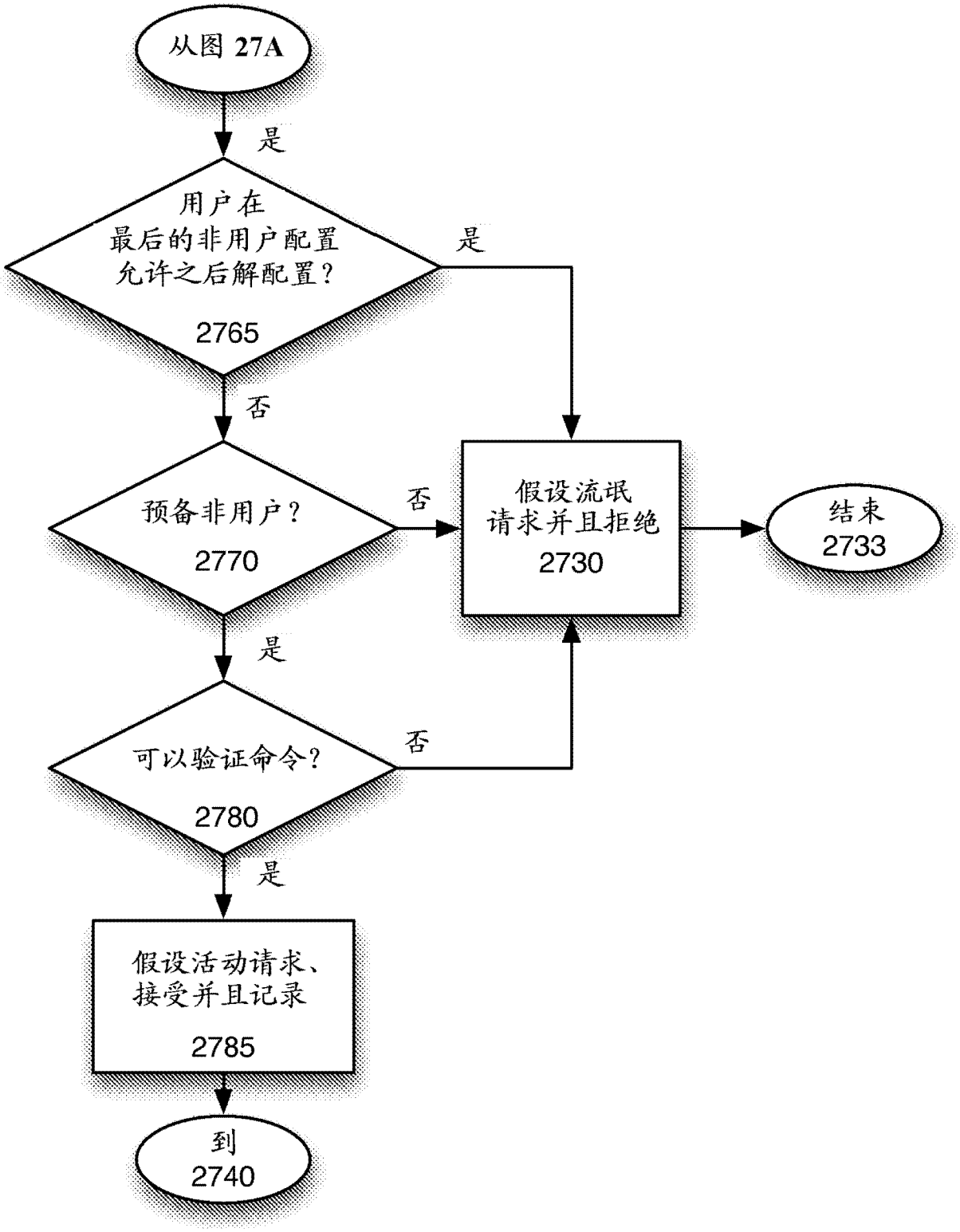

从图 27A
是
用户在
最后的非用户配置
允许之后解配置？
2765
是
否
预备非用户？
2770
否
假设流氓
请求并且拒绝
2730
结束
2733
是
可以验证命令？
2780
否
是
假设活动请求、
接受并且记录
2785
到
2740

图 27B

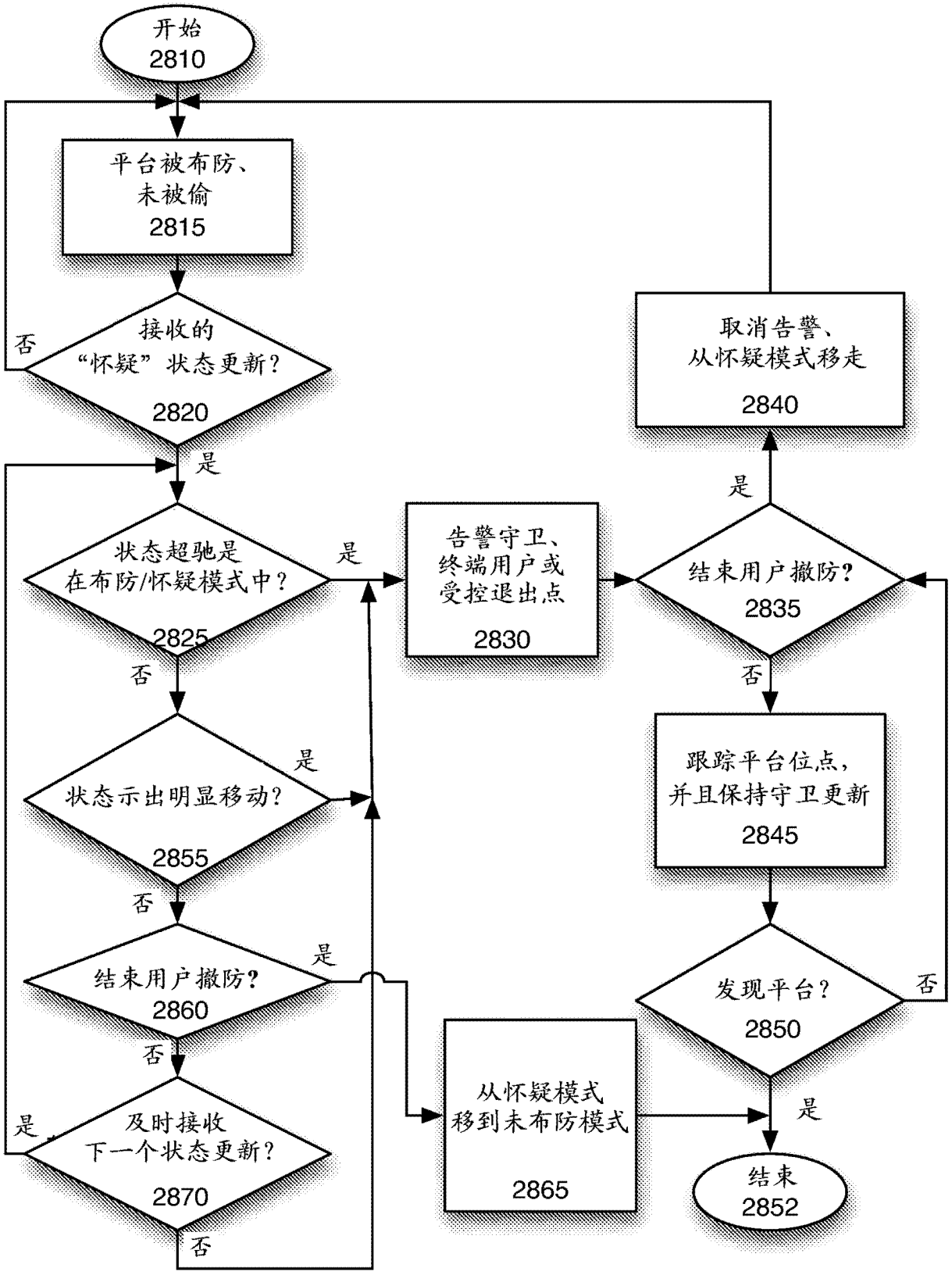

开始
2810
平台被布防、
未被偷
2815
接收的
“怀疑”状态更新？
2820
否
是
状态超驰是
在布防/怀疑模式中？
2825
是
否
告警守卫、
终端用户或
受控退出点
2830
结束用户撤防？
2835
是
否
取消告警、
从怀疑模式移走
2840
跟踪平台位点，
并且保持守卫更新
2845
发现平台？
2850
否
是
状态示出明显移动？
2855
是
否
结束用户撤防？
2860
是
否
及时接收
下一个状态更新？
2870
是
否
从怀疑模式
移到未布防模式
2865
结束
2852

图 28

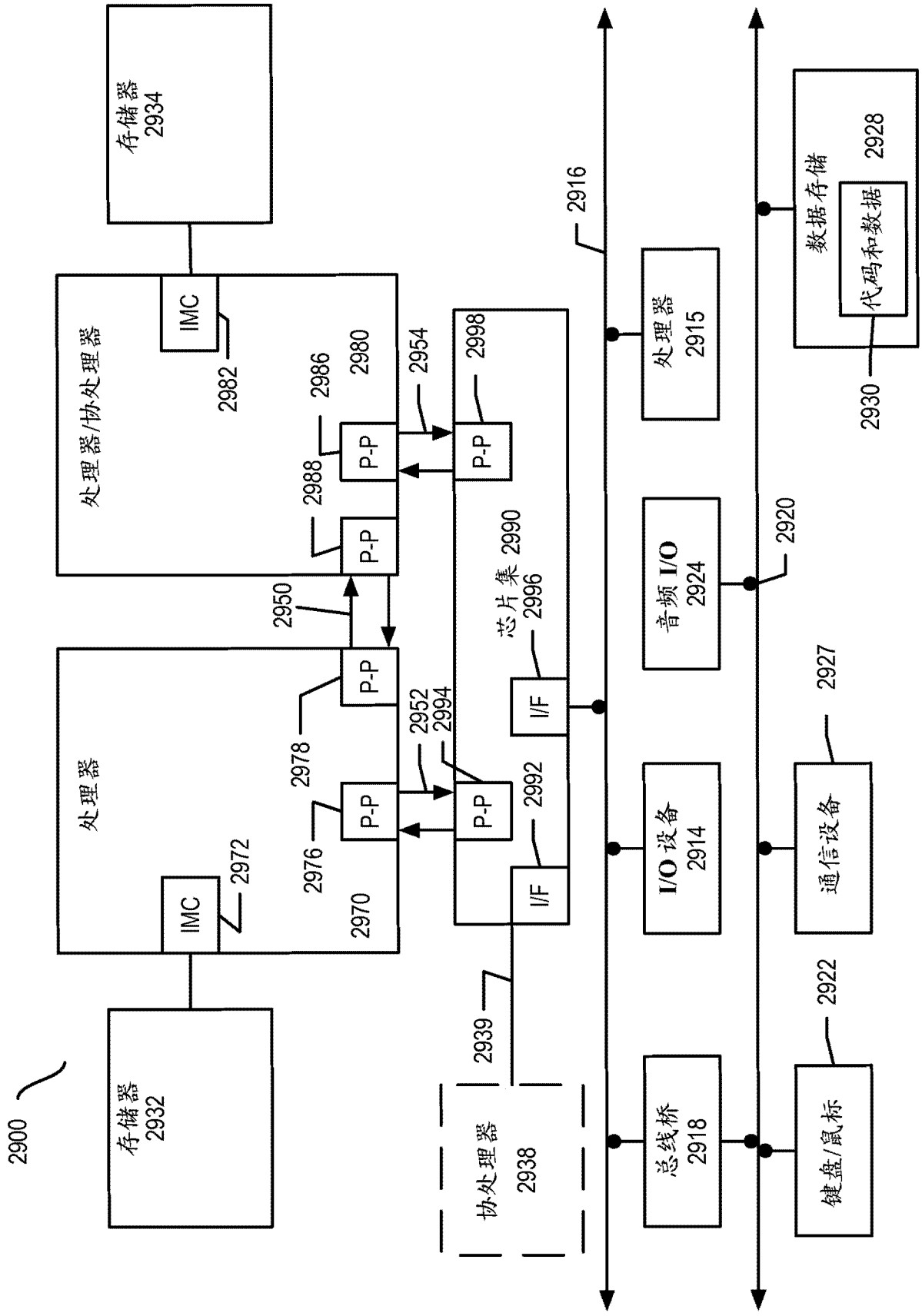

2900
存储器
2932
存储器
2934
处理器
处理器/协处理器
IMC
2972
2982
2970
2980
2976
2978
2986
2988
2950
2952
2954
2994
P-P
2998
芯片集 2990
2996
I/F
2992
2939
协处理器
2938
2916
处理器
2915
音频 I/O
2924
2920
I/O 设备
2914
2927
通信设备
总线桥
2918
2922
键盘/鼠标
数据存储
2928
代码和数据
2930

图 29

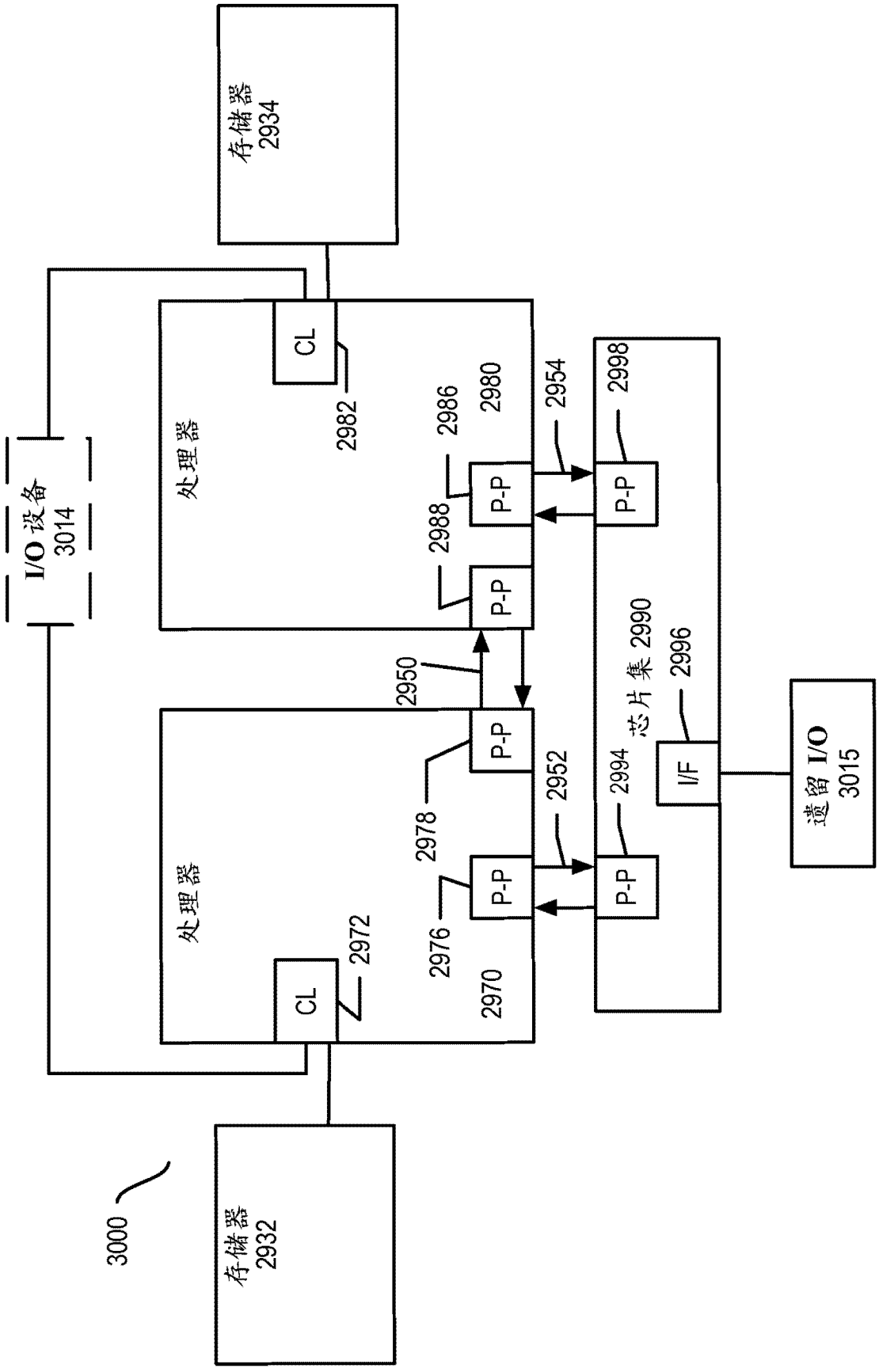

存储器
2934
CL
2982
处理器
2980
2986
2988
P-P
P-P
2954
2998
P-P
I/O 设备
3014
2950
芯片集 2990
2996
I/F
遗留 I/O
3015
2978
P-P
2952
2994
P-P
2976
2970
处理器
2972
CL
3000
存储器
2932

图 30