(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117396107 A
(43)申请公布日 2024.01.12

(21)申请号 202280038151.9
(22)申请日 2022.05.26
(30)优先权数据
63/194,347 2021.05.28 US
(85)PCT国际申请进入国家阶段日
2023.11.27
(86)PCT国际申请的申请数据
PCT/US2022/031202 2022.05.26
(87)PCT国际申请的公布数据
WO2022/251544 EN 2022.12.01
(71)申请人 INVUE安全产品公司
地址 美国北卡罗来纳州
(72)发明人 W·J·布兰查德 C·R·赫尔曼
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 王冉
(51)Int.Cl.
A47F 3/00(2006.01)

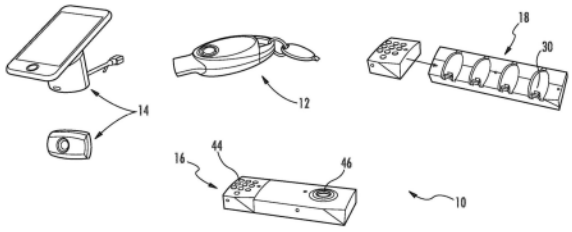
权利要求书3页 说明书20页 附图55页

(54)发明名称

商品展示安全系统和方法

(57)摘要

提供了安全系统和方法。在一个实例中,一种安全系统包含:至少一个锁,所述至少一个锁被配置成保护一个或多个物品免于从固定装置中盗窃;以及锁扣板,所述锁扣板被配置成安装到所述固定装置。所述锁包括柱塞销,所述柱塞销被配置成在与所述锁扣板接合时的锁定状态和与所述锁扣板脱离接合时的解锁状态之间移动,并且所述锁包括凸轮,所述凸轮被配置成使所述柱塞销在所述锁定状态与所述解锁状态之间移动。所述锁被配置成当所述锁处于所述解锁状态时在闩锁位置与未闩锁位置之间移动,所述固定装置被配置成在所述未闩锁位置被接近,并且所述锁扣板被配置成当所述锁从所述未闩锁位置移动到所述闩锁位置时相对于所述锁移动以使所述锁与所述锁扣板对准。



CN 117396107 A

1.一种安全系统,其包括:

至少一个锁,所述至少一个锁被配置成保护一个或多个物品免于从固定装置中盗窃,

锁扣板,所述锁扣板被配置成安装到所述固定装置,

其中所述锁包括柱塞销,所述柱塞销被配置成在与所述锁扣板接合时的锁定状态和与所述锁扣板脱离接合时的解锁状态之间移动,

其中所述锁包括凸轮,所述凸轮被配置成使所述柱塞销在所述锁定状态与所述解锁状态之间移动,

其中所述锁被配置成当所述锁处于所述解锁状态时在闩锁位置与未闩锁位置之间移动,所述固定装置被配置成在所述未闩锁位置被接近,

其中所述锁扣板被配置成当所述锁从所述未闩锁位置移动到所述闩锁位置时相对于所述锁移动以使所述锁与所述锁扣板对准。

2.根据权利要求1所述的安全系统,其进一步包括计算装置,所述计算装置被配置成与所述锁无线通信以使所述锁在所述锁定状态与所述解锁状态之间转变。

3.根据权利要求1所述的安全系统,其进一步包括电子钥匙,所述电子钥匙被配置成与所述锁无线通信以在所述锁定状态与所述解锁状态之间转变。

4.根据权利要求1所述的安全系统,其中所述柱塞销被配置成在所述锁定状态与所述解锁状态之间轴向移动。

5.根据权利要求1所述的安全系统,其中所述凸轮被配置成旋转以在所述锁定状态与所述解锁状态之间转变。

6.根据权利要求1所述的安全系统,其中当所述锁从所述未闩锁状态移动到所述闩锁状态时,所述锁扣板是铰接的以供移动。

7.根据权利要求1所述的安全系统,其中当所述锁从所述未闩锁状态移动到所述闩锁状态时,所述锁扣板是柔性的以供移动。

8.根据权利要求1所述的安全系统,其中所述锁包括用于使所述锁扣板移动的磁体。

9.根据权利要求1所述的安全系统,其中所述柱塞销被配置成当所述柱塞销从所述未闩锁位置移动到所述闩锁位置时在所述锁定状态下自动接合所述锁扣板。

10.根据权利要求1所述的安全系统,其中所述柱塞销包括被配置成围绕所述凸轮的开口。

11.根据权利要求1所述的安全系统,其中所述凸轮被配置成响应于接收到无线授权信号而移动以使所述锁在所述锁定状态与所述解锁状态之间转变。

12.根据权利要求11所述的安全系统,其进一步包括电机,所述电机可操作地与所述凸轮接合并且被配置成在激活时使所述柱塞销移动。

13.根据权利要求1所述的安全系统,其中所述锁被配置成在所述闩锁位置与所述未闩锁位置之间手动滑动。

14.根据权利要求1所述的安全系统,其中所述锁不具有内部电源。

15.根据权利要求1所述的安全系统,其中所述锁包含内部电源。

16.根据权利要求1所述的安全系统,其中所述固定装置是一对滑动门,并且其中所述锁被配置成安装到所述滑动门中的一个滑动门,并且所述锁扣板被配置成安装到另一个滑动门。

17.根据权利要求1所述的安全系统,其进一步包括开关,所述开关被配置成检测与所述锁扣板的接合,以指示所述锁处于所述锁定状态还是处于所述闩锁位置。

18.根据权利要求1所述的安全系统,其进一步包括权利要求1至17中任一项所述的特征的任何组合。

19.一种安全系统,其包括:

至少一个锁,所述至少一个锁被配置成保护一个或多个物品免于从固定装置中盗窃;以及

计算装置,

锁扣板,所述锁扣板被配置成安装到所述固定装置,

其中所述锁包括柱塞销,所述柱塞销被配置成在与所述锁扣板接合时的锁定状态和与所述锁扣板脱离接合时的解锁状态之间移动,

其中所述锁包括凸轮,所述凸轮被配置成使所述柱塞销在所述锁定状态与所述解锁状态之间移动,

其中所述锁被配置成当所述锁处于所述解锁状态时在闩锁位置与未闩锁位置之间移动,所述固定装置被配置成在所述未闩锁位置被接近,

其中所述锁扣板被配置成当所述锁从所述未闩锁位置移动到所述闩锁位置时相对于所述锁移动以使所述锁与所述锁扣板对准,并且

其中所述计算装置被配置成与所述锁无线通信以使所述锁在所述锁定状态与所述解锁状态之间转变。

20.根据权利要求19所述的安全系统,其进一步包括电子钥匙,所述电子钥匙被配置成与所述锁无线通信以在所述锁定状态与所述解锁状态之间转变。

21.根据权利要求19所述的安全系统,其中当所述锁从所述未闩锁状态移动到所述闩锁状态时,所述锁扣板是铰接的以供移动。

22.根据权利要求19所述的安全系统,其中当所述锁从所述未闩锁状态移动到所述闩锁状态时,所述锁扣板是柔性的以供移动。

23.根据权利要求19所述的安全系统,其中所述锁包括用于使所述锁扣板移动的磁体。

24.根据权利要求1所述的安全系统,其进一步包括权利要求19至23中任一项所述的特征的任何组合。

25.一种用于保护物品免于从固定装置中盗窃的方法,所述方法包括:

提供至少一个锁和锁扣板,所述至少一个锁被配置成保护一个或多个物品免于从固定装置中盗窃,所述锁扣板被配置成安装到所述固定装置;

使柱塞销在与所述锁扣板接合时的锁定状态和与所述锁扣板脱离接合时的解锁状态之间移动,其中所述锁包括凸轮,所述凸轮被配置成使所述柱塞销在所述锁定状态与所述解锁状态之间移动;

当所述锁处于所述解锁状态时将所述锁从闩锁位置移动到未闩锁位置,所述固定装置被配置成在所述未闩锁位置被接近,

当所述锁处于所述解锁状态时将所述锁从所述未闩锁位置移动到所述闩锁位置,其中所述锁扣板被配置成当所述锁从所述未闩锁位置移动到所述闩锁位置时相对于所述锁移动以使所述锁与所述锁扣板对准。

26.一种系统、方法和/或计算机程序介质,其包括本文所公开的特征的任何组合。

商品展示安全系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2021年5月28日提交的美国临时申请第63/194,347号的优先权的权益,所述美国临时申请的全部内容特此通过引用并入。

技术领域

[0003] 本发明的实施例总体上涉及安全系统、锁、装置、计算机程序产品以及用于保护物品免于盗窃和/或在无线网络中交换各种类型的信息的方法。

背景技术

[0004] 对于零售商来说,通常的做法是在通常被称为“保险箱”的安全包装内的安全装置(如展示钩或展示固定装置)上或者以其它方式在展示表面上展示相对较小、相对较贵的商品项。安全装置或保险箱展示商品项,使得潜在的购买者在决定是否购买所述物品时可以检查所述物品。然而,所述物品的小尺寸和相对昂贵的价格使其成为商店扒手的诱人目标。商店扒手可能试图将物品从安全装置上拆卸,或者可替代地可能试图将安全装置与商品一起从展示区移走。商品项也可以使用展示架来保护,以允许用户为潜在的购买对物品进行取样。在一些情况下,使用由钥匙操作的锁,例如机械锁,将安全装置固定到展示支架上。在其它情况下,使用由电子钥匙操作的锁将安全装置固定到展示支架,以布防和撤防安全装置。

发明内容

[0005] 本申请的实施例涉及用于保护物品免于盗窃的安全系统和方法。在一个实施例中,一种安全系统包含:至少一个锁,所述至少一个锁被配置成保护一个或多个物品免于从固定装置中盗窃;以及锁扣板,所述锁扣板被配置成安装到所述固定装置。所述锁包括柱塞销,所述柱塞销被配置成在与所述锁扣板接合时的锁定状态和与所述锁扣板脱离接合时的解锁状态之间移动,并且所述锁包括凸轮,所述凸轮被配置成使所述柱塞销在所述锁定状态与所述解锁状态之间移动。所述锁被配置成当处于所述解锁状态时在闩锁位置与未闩锁位置之间移动,所述固定装置被配置成在所述未闩锁位置被接近,并且所述锁扣板被配置成当所述锁从所述未闩锁位置移动到所述闩锁位置时相对于所述锁移动以使所述锁与所述锁扣板对准。

[0006] 在另一个实施例中,提供了一种方法并且所述方法包含:提供至少一个锁以及锁扣板,所述至少一个锁被配置成保护一个或多个物品免于从固定装置中盗窃,所述锁扣板被配置成安装到所述固定装置。所述方法进一步包含使柱塞销在与所述锁扣板接合时的锁定状态和与所述锁扣板脱离接合时的解锁状态之间移动,其中所述锁包括凸轮,所述凸轮被配置成使所述柱塞销在所述锁定状态与所述解锁状态之间移动。所述方法还包含当所述锁处于所述解锁状态时将所述锁从闩锁位置移动到未闩锁位置,其中所述固定装置被配置成在所述未闩锁位置被接近。另外,所述方法包含当所述锁处于所述解锁状态时将所述锁

从所述未闩锁位置移动到所述闩锁位置,其中所述锁扣板被配置成当所述锁从所述未闩锁位置移动到所述闩锁位置时相对于所述锁移动以使所述锁与所述锁扣板对准。

附图说明

[0007] 图1展示了根据本发明的一个实施例的商品安全系统。

[0008] 图2展示了根据本发明的另一个实施例的商品安全系统。

[0009] 图3展示了根据一个实施例的通过云与远程装置通信的钥匙。

[0010] 图4展示了根据一个实施例的具有不同授权级别的多个钥匙。

[0011] 图5是根据一个实施例的电子钥匙的平面视图。

[0012] 图6是图5所示的电子钥匙的透视图。

[0013] 图7是根据另一个实施例的电子钥匙的平面视图。

[0014] 图8是图7所示的电子钥匙的透视图。

[0015] 图9是根据另一个实施例的电子钥匙的平面视图。

[0016] 图10是图9所示的电子钥匙的透视图。

[0017] 图11是根据一个实施例的商品安全装置的透视图。

[0018] 图12是根据一个实施例的电子钥匙的透视图。

[0019] 图13是图12所示的电子钥匙的横截面视图。

[0020] 图14是根据一个实施例的处于锁定和解锁位置的商品安全装置的透视图。

[0021] 图15是根据另一个实施例的处于锁定和解锁位置的商品安全装置的透视图。

[0022] 图16是根据一个实施例的充电站的平面视图。

[0023] 图17是图16所示的充电站的透视图。

[0024] 图18展示了根据一个实施例的商品安全系统。

[0025] 图19展示了根据一个实施例的与计算装置通信的电子钥匙。

[0026] 图20展示了根据另一个实施例的电子钥匙的顶部和底部透视图。

[0027] 图21展示了图20所示的电子钥匙的平面视图和侧视图。

[0028] 图22是根据一个实施例的编程或授权站的平面视图。

[0029] 图23是图22所示的编程或授权站的透视图。

[0030] 图24是图22所示的编程或授权站的另一个透视图。

[0031] 图25是根据一个实施例的在无线网络中通信的多个传感器和警报节点的示意图。

[0032] 图26是根据本发明的一个实施例的无线网络内的基础设施和安全装置的示意图。

[0033] 图27是根据一个实施例的无线网络中的系统的透视图。

[0034] 图28是根据一个实施例的无线网络中的系统的透视图。

[0035] 图29是根据一个实施例的无线网络中的系统的透视图。

[0036] 图30是根据一个实施例的无线网络中的系统的透视图。

[0037] 图31是根据一个实施例的无线网络中的系统的透视图。

[0038] 图32示出了根据另外的实施例的被配置用于无线网络的各种安全装置。

[0039] 图33示出了根据一个实施例的被配置用于无线网络的安全装置。

[0040] 图34示出了根据一个实施例的被配置用于无线网络的安全装置。

[0041] 图35示出了根据一个实施例的被配置用于无线网络的安全装置。

[0042] 图36示出了根据一个实施例的被配置用于无线网络的安全装置。

[0043] 图37是根据一个实施例的无线网络中的系统的透视图。

[0044] 图38是根据一个实施例的无线网络中的系统的透视图。

[0045] 图39是根据一个实施例的无线网络中的系统的透视图。

[0046] 图40是根据一个实施例的无线网络中的系统的透视图。

[0047] 图41是根据一个实施例的无线网络中的系统的透视图。

[0048] 图42是根据一个实施例的无线网络中的系统的透视图。

[0049] 图43是根据一个实施例的商品展示安全系统的透视图。

[0050] 图44展示了根据一个实施例的商品展示安全系统的各个组件。

[0051] 图45A-C展示了根据一个实施例的锁的内部罐横截面视图。

[0052] 图46A-B是根据另外的实施例的不同锁的透视图。

[0053] 图47是根据另一个实施例的商品展示安全系统的透视图。

[0054] 图48是根据一个实施例的安装到固定装置的锁的透视图。

[0055] 图49是根据一个实施例的安装有锁的固定装置的透视图。

[0056] 图50A-B是根据另外的实施例的不同锁的透视图。

[0057] 图51是根据一个实施例的锁和电子钥匙的透视图。

[0058] 图52A-B是根据一个实施例的具有模块化组件的锁的透视图。

[0059] 图53A-C展示了根据另外的实施例的各种锁的操作。

[0060] 图54A-C展示了根据另外的实施例的各种锁的操作。

[0061] 图55是根据本发明的一个实施例的锁的透视图。

[0062] 图56是图55所示的锁的侧视图。

[0063] 图57是图55所示的锁的后视图。

[0064] 图58是图55所示的锁的侧面透视图。

[0065] 图59是图55所示的锁的内部侧视图。

[0066] 图60是图55所示的锁的内部透视图。

[0067] 图61是图55所示的锁的另一个内部侧视图。

[0068] 图62是图55所示的锁的内部正视图。

[0069] 图63是图55所示的锁的内部端视图。

[0070] 图64是根据一个实施例的图55所示的安装到固定装置的锁的侧视图。

具体实施方式

[0071] 以下公开包含系统、装置、方法和计算机程序产品的各个实施例。应当理解的是，已经预见了本文所公开的实施例的任何组合。因此，对一个特定实施例的讨论并不旨在排除任何其它实施例。

[0072] 现在参考相关附图，示出了展示安全系统的一个或多个实施例。在本文示出和描述的实施例中，所述系统包含电子钥匙和商品安全装置。适合与电子钥匙一起使用的商品安全装置的实例包含但不限于安全显示器(例如，报警支架或装置)、安全固定装置(例如，锁钩、架子、橱柜等)、橱柜锁、门锁、缆包、线缆锁或用于商品项的安全包装(例如，商品保管员)。然而，电子钥匙(本文也称为可编程钥匙或通常称为钥匙)可以与任何安全装置或锁定

装置一起使用,所述安全装置或锁定装置利用从钥匙传输的电力来操作机械和/或电子锁机构,和/或利用从钥匙传输的数据来授权锁机构的操作和/或布防或撤防警报电路。换言之,电子钥匙可与任何需要从钥匙向装置传输电力和/或从钥匙向装置传输数据的安全装置或锁定装置一起使用。安全装置和锁定装置的另外的实例包含但不限于门锁、抽屉锁或货架锁,以及防止未经授权人员从安全定位或位置接近、移除或拆卸物品的任何装置。虽然以下讨论涉及一种供零售店中使用的系统,但是应当理解,所述系统也适用于其它行业,如医院、餐馆等。在一些实施例中,商品安全系统、商品安全装置和电子钥匙类似于以下中公开的那些:题为"商品展示安全系统和方法"的PCT公开WO 2020/227513(以及相关的美国申请第17/261,757号),题为"用于商品安全装置的电子钥匙"的美国公开第2012/0047972号,题为"用于从展示的商品制品中获取数据的系统和方法"的美国专利第10,258,172号,题为"商品展示安全系统和方法"的美国专利第10,210,681号,题为"具有无线通信的系留安全系统"的美国公开第2018/0365948号以及题为"用于远程控制安全装置的系统和方法"的美国公开第2016/0335859号,所述文献的全部公开内容通过引用整体并入本文。

[0073] 图1展示系统10的一个实施例。在此实施例中,所述系统通常包含电子钥匙12、一个或多个商品安全装置14、编程或授权站16以及充电站18。图2示出了作为商品安全装置网络的一部分的系统10的实施例。根据一些实施例,网络使得多个电子钥匙与商品安全装置之间能够进行通信。所述网络可以是基于云的,并且包含用于从电子钥匙和/或商品安全装置接收数据和/或向电子钥匙和/或商品安全装置提供数据的云22。云22可以促进与一个或多个计算装置26(例如,移动装置、平板计算机或计算机)的通信。例如,云22可用于将数据传输到一个或多个远程定位或计算装置26,在所述一个或多个远程定位或计算装置处,数据可以被查看和分析。计算装置26可以位于任何期望的定位处,如在与安全装置14和/或电子钥匙12相同的零售店中。在一些情况下,计算装置26可以属于零售店员工(例如,移动装置)或者是由零售商或公司使用的后端计算机。所述网络可以是无线网络,包含被配置成彼此通信的多个节点20、一个或多个电子钥匙12和/或一个或多个商品安全装置14。所述网络可以是用于促进无线通信的任何合适的网络,例如网状、星形、多星形、中继器、IoT等网络。节点20和/或安全装置14可以位于一个或多个区域内。在一些情况下,节点和安全装置可以彼此集成,使得安全装置作为节点进行操作。可以采用网关24或集线器或"主机"来允许一个或多个节点20与云22之间的通信。在一些实施例中,网络内的所有通信都是无线的,如通过射频信号(例如,亚GHz ISM频带或2.4GHz)、蓝牙、LoRa和Wi-Fi,尽管其它类型的无线通信也是可能的。

[0074] 在一些实施例中,每个商品安全装置14和/或电子钥匙12被配置成存储各种类型的数据。例如,每个商品安全装置14和/或钥匙12可以存储一个或多个商品安全装置14的序列号、一个或多个商品项的序列号、钥匙激活的数据和时间、钥匙的用户、钥匙的序列号、安全装置的定位、商品项的定位、零售店内的部门号、钥匙激活的次数、激活类型(例如,"裸"激活、仅传输数据的激活、传输功率的激活、传输数据和功率的激活)和/或各种事件(例如,商品安全装置已经被锁定、解锁、布防或撤防)。例如,图3示出了电子钥匙12的用户的身份可以被传送到远程定位或装置26。此信息可以在每次激活钥匙12时或者在任何其它期望的时间段,如在与编程或授权站16通信时,被传输到远程定位或装置26。因此,在一些实施例中,来自电子钥匙12和/或安全装置14的数据传输可以实时或自动发生。在一些情况下,电

子钥匙12、安全装置14和/或编程站16可以被配置成存储数据并且将数据传输到远程定位或装置26。经授权人员可以使用此数据来使用计算装置26采取各种动作,如审计和监测员工活动、授权或取消授权特定钥匙12、确定钥匙12的电池寿命、审计商品安全装置14(例如,确保安全装置被锁定或布防)、布防或撤防安全装置、锁定或解锁安全装置、锁定或解锁连接到商品项的传感器25到可移除地支撑传感器的基座或支架35,等等(例如,参见图30)。此外,可以使用计算装置26按需如从电子钥匙12、安全装置14和/或编程站16请求和获得此类信息。

[0075] 在一些情况下,数据可以包含电子钥匙12的电池分析。例如,电池分析可以包含当电子钥匙12被放置在充电站18上时监测所述钥匙的电池电压以及达到完全充电所花费的时间。这些值可以用于确定放电深度。电池分析可以指示电池接近其寿命终点。零售商或其它经授权人员可以使用此信息采取各种行动,如更换钥匙或禁用钥匙,以防止电池膨胀和壳体故障。

[0076] 在一个实施例中,电子钥匙12被配置成从商品安全装置14(例如,安全固定装置)获得数据。例如,商品安全装置14可以存储关于与先前电子钥匙12的过去通信的各种数据(例如,钥匙标识、通信时间等),并且当后续的电子钥匙与同一商品安全装置通信时,数据被传输到电子钥匙。因此,商品安全装置14可以包含用于存储此类数据的存储器。在一些情况下,商品安全装置14包含用于接收和存储数据的电源,而在其它情况下,由电子钥匙12提供的电力用于允许商品安全装置存储数据。电子钥匙12然后可以传送数据用于收集和检查,如在远程定位或装置26处。在一些情况下,电子钥匙12与编程或授权站16之间的通信可以允许数据从电子钥匙中提取出来并且传送到如远程定位或装置26。在其它情况下,电子钥匙12可以被配置成从商品安全装置14(例如,安全显示器)获得数据,如商品安全装置的标识、展示的商品项的类型、商品项的标识和/或安全装置和/或商品项的系统健康。电子钥匙12可以存储数据,并且直接或在与编程或授权站16通信时将数据提供给远程定位或装置26。因此,电子钥匙12可以是在不需要有线连接或复杂的无线网络或系统的情况下用于从商品安全装置14获得各种类型数据的有用资源。

[0077] 在一个实施例中,安全装置14可以使用各种技术传送其标识符。例如,在一些情况下,安全装置14可以具有被配置成存储序列号的存储器,并且能够使用双向通信将所述序列号传送到电子钥匙12。在安全装置14可能不具有存储器、电源和/或双向通信能力(例如,缆包或锁钩)的情况下,安全装置可以具有存储安全装置的标识符(例如,序列号)的RFID标签、NFC标签等。此类安全装置可以类似于题为“与电子钥匙一起使用的商品安全装置”的美国专利第9,133,649号中公开的安全装置,所述美国专利的全部公开内容通过引用整体并入本文。在一些实例中,标签可以附着(例如,通过粘合剂)到现有的安全装置14,使得它容易适用于当前装置,或者标签可以集成在安全装置内。电子钥匙12可以被配置成向标签递送电力以读取标签的标识符,如对于无源标签,尽管标签可以是无源的或有源的。电子钥匙12可以将多个授权标识符存储在存储器中(例如,通过查找表),并且然后可以确定所读取的标识符是否在其存储器中。可替代地,电子钥匙12可以被配置成无线连接到具有查找表的网络装置26。电子钥匙12本身或网络装置26然后可以确定特定钥匙或所述钥匙的用户是否被授权用所读取的标识符解锁安全装置14。所述标识符对于安全装置14可以是唯一的,或者可以是更通用的标识符,例如“6面盒”或如“保健”等部门,或者上文所有的。一旦获得

授权,只有这样,电子钥匙才能够向安全装置14递送电力,以成功地操作锁并将其解锁。如果没有授权,电子钥匙12不继续此循环,并且锁从不解锁。因此,本发明的实施例可以被配置成与任何类型的安全装置14通信,用于基于安全装置的识别来执行各种审计、区域控制和货架图分析。

[0078] 在一个实施例中,电子钥匙12和安全装置14可以通过NFC彼此通信,以在钥匙和安全装置被定位成彼此靠近或彼此直接接触时传输数据。NFC标签可以包含各种组件,如天线或线圈以及定义电路的一个或多个芯片。天线可以用于实现与电子钥匙12的通信,所述电子钥匙可以通过磁场激活。例如,电子钥匙12可以生成磁场以与NFC标签通信。

[0079] 在一些实施例中,电子钥匙12被配置成感应传输电力,如下文进一步详细解释的,并且被配备成使用NFC或RFID进行通信,钥匙的感应线圈可以被配置成使用相同的线圈进行数据传输和电力传输两者。在一些情况下,电子钥匙12被配置成在能量传输模式与NFC或RFID接收器电路之间切换线圈。在其它实例中,多个安全装置14可以彼此“嵌套”,使得对嵌套的安全装置之一的授权导致所有安全装置被撤防或解锁。例如,多个锁可以彼此配对,使得任何一个锁与电子钥匙12之间的成功通信导致所有锁被解锁。

[0080] 在一些实施例中,商品安全装置14包含用于在网络内进行通信的无线功能。例如,商品安全装置可以彼此、与商品项、电子钥匙12、计算装置26和/或节点无线通信,包含但不限于传送本文所讨论的各种类型的数据。因此,在一些情况下,计算装置26可以直接与安全装置14和/或电子钥匙12通信。

[0081] 此类无线系统的一个实施例包含能够与本文所公开的实施例结合使用的各种类型的无线网络。在一些情况下,无线系统包含完全集成的硬件、软件和数据分析,这有效地消除了数据集成解决方案的额外硬件成本或使其可忽略不计——所有其它特征保持不变。在一些实施例中,无线系统被配置成适应不断变化的市场,其中越来越多的智能手机利用基于Qi的感应充电,并且暴露的数据端口不再存在。例如,在安全装置14包含传感器25和基座或支架35的实施例中(参见例如,图30),传感器可以利用Qi技术,如被配置成与商品项中的对应线圈通信的Qi线圈。另外,无线系统的实施例可以被配置成利用本文所讨论的各种无线网络为未来的联网产品提供公共无线接口和IP网关。根据无线系统实施例,可以实施各种操作模式。在一个实例中,可以采用非IP连接模式,由此选择不订购SaaS服务的客户能够独立于到IP使能网络的连接来利用无线系统的展示推销和安全特征。另一种模式可以包含IP连接模式,其可以提供信息,例如,关于安全布防和电源状态以及基于本地商店的警报警告活动。另外,此模式可以提供对如产品文档、产品视频、产品选择指南和支持联系信息等其它网络应用程序的访问。另外的模式也是包含SaaS订购服务的IP连接网络,所述服务允许访问无线系统的全部能力,如本文所描述的各种装置之间的数据通信。

[0082] 在一些实施例中,无线通信可以使用专有无线网络来进行,例如,每个安全装置14可以被配置成与星形网络配置中的中央集线器通信。每个安全装置14可以包含收发器(例如,亚GHz收发器),所述收发器被配置成向和从公共中央集线器或“主机”24传送数据,如本文所讨论的各种类型的信息和数据,以及关于电源状态和对主机的安全破坏的信息,而不需要到智能集线器或控制器的单独的数据连接。应当理解,可以采用任何数量的节点20来促进安全装置14与主机例如一个或多个本地节点之间的通信。在一个实施例中,每个安全装置14被配置成将其电力和安全状态、安全漏洞(警报通知)以及安全装置和/或商品项的

各种其它识别数据传送到主机24。在一些实施例中,整个零售店可以由单个主机24服务,而不需要中继器,并且实际上不受网络中的安全装置数量的限制。在一个实施例中,主机24可以被配置成生成安全信号,如听觉和/或视觉警报信号。在一些情况下,安全信号的音量是可调整的。当任何安全装置14检测到安全事件时,安全装置被配置成向主机24发送信号。零售商可以选择安全事件的通知级别,例如,响亮的声音警报、较低的音量、声音通知或没有声音警报通知。在其它特征中,所述系统可以包含对警报通知进行编程的能力。例如,零售商可以选择无声警报、视觉警报、可调音量和音调听觉警报或这些警报的组合。另外,主机24可以被配置成通过改变颜色(例如,从金色变为红色和/或通过间歇闪烁)来指示安全漏洞。听觉和视觉报警信号可以单独或一起使用。

[0083] 如本文所讨论的,电子钥匙12可以与各个系统实施例结合。电子钥匙12可以被配置成在安全事件之后禁用任何报警安全装置14。然而,主机24可以被配置成继续发射安全信号,如直到安全装置14被重新布防。此外,禁用主机24上的安全信号不会影响商店中其余安全装置14的戒备状态,即,除了生成安全信号之外,安全装置可以在各个方面一对一地进行操作。当然,如本文所公开的多种类型的电子钥匙12,包含利用智能手机、平板计算机或PC上可用的安全应用程序。

[0084] 在一些实施例中,可以采用先发制人的撤防,以便重新销售商品项或者在夜间从相关联的安全装置14中取出物品。例如,零售商26的计算装置26(例如,移动装置)可以被配置成在预定时间段自动撤防一个或多个安全装置14。在一些情况下,安全软件应用程序可以允许在可编程的时间段内暂时中止对安全装置14的特定位置的警报,以允许重新销售。一旦撤防,安全装置的收发器将停止通信,直到它被重新布防。对于那些在“非IP连接”模式下操作的客户来说,当重新销售时,可以选择使安全装置14的声音警报静音,使得不会发出声音警报,但是主机可以继续生成信号(例如,光信号),直到所有的安全装置都被重新布防。

[0085] 如本文所描述,本发明的实施例可以利用多种无线网络配置。在一些情况下,通用架构需要两种不同的网络拓扑结构。第一网络可以是专用于部署在商店中的安全装置14的专用无线网络。此网络与由零售商操作的任何专用或公共网络不同。第二网络可以是专用网络与互联网之间的IP网关。此第二网络可以是零售商的管理网络上的连接,或者可以通过蜂窝调制解调器。网关可以集成到主机中,或者是连接到主机的单独装置。

[0086] 在一些实施例中,专用网络可以被所有安全装置14共同用于内部数据传输,并且最小化零售商管理的网络的频率拥塞。此外,在一个实例中,专用网络实际上采取“星形网络”的形式,其中多个单独的节点20执行单独的功能并且收集和提供数据。此数据被无线发送到公共“主机”并且在其中聚合。主机允许通过专用网络无线提供数据的节点20独立于到基于云的应用程序的互联网连接向客户递送功能和价值,如报警和报告功能。在一个实施方案中,主机而不是安全装置14将被配置成通过音频、视觉和/或触觉响应来提供通知(例如,响应于安全事件)。

[0087] 关于专用网络,可以考虑各种因素。例如,在为专用网络选择适当的公共网络架构时,可以考虑数据包的尺寸和所需的数据速率、所需的无线范围、网络的潜在的干扰、功耗、尺寸和/或成本的注意事项。在一些应用程序中,可以使用不需要更高数据速率的小数据包的间歇传输,这可以受益于具有低功率需求和长数据范围的网络。专用网络的实例包含各

种RF网络,如Wi-Fi(2.4GHz)、蓝牙(2.4GHz)和亚GHz(小于1.0GHz)ISM频带网络。如Zigbee和LoRa等一些网络堆栈(控制软件)可以在亚GHz和2.4GHz网络上运行。

[0088] 无线网络系统的另一个示例实施例包含各种类型的安全装置14和电子钥匙12,所述安全装置和电子钥匙可以与无线网络中的一个或多个节点20、集线器24和/或计算装置26协作(参见例如,图26-42)。系统中可以采用各种类型的安全装置14,如本文所公开的那些安全装置。例如,包含被配置成连接到物品(例如,通过粘合剂和/或托架)的传感器的安全装置14。在一些实施方案中,传感器可以用系绳45连接到基座或支架35(参见例如,图30-32),或者在一些情况下可以不使用系绳(参见例如,图32-33)。传感器25可以采取许多不同的形式,例如,独立传感器(参见例如,图36)、“椅背”传感器(参见例如,图33)、为商品项提供电力和安全性的传感器(例如,通过USB-C、微型USB等连接器)(参见例如,图35)、和/或仅提供安全性的传感器(例如,包含柱塞开关的传感器)(参见例如,图34)。类似地,用于可移除地支撑传感器25的基座35也可以采取不同的形式(参见例如,图33,其中椅背传感器与用于在传感器与基座之间传输电力的电触点一起使用)。当然,安全装置14可以用于各种行业,如零售店,以及用于各种物品,如商品或商业项(例如,平板计算机)。

[0089] 如图27-29所示,各种数量和类型的安全装置14可以被配置成在网络中彼此通信,如上文所讨论的专用无线网络。主机或集线器24可以被配置成与网络中的多个安全装置14中的每个安全装置通信,并且提供各种安全信号,如本文所公开的。可以在集线器24上设置接口,用于促进与电子钥匙12的通信。图27示出了实例,其中多个安全装置14和集线器24被配置成在IP网络中通信,这可以允许向一个或多个计算装置26提供各种信息和警报(例如,系统健康、电源状态、警报状态和/或库存信息)。此外,图28展示了类似于图27的实例,但是其中所述系统包含通过对企业软件的SaaS订阅的另外的特征,例如展示货架图(“POG”)符合性信息、消费者活动、可编程KPI、库存再库存阈值和/或库存POG符合性。图30-31示出了传感器和基座的形式的多个安全装置14的各种描述,所述传感器和基座被配置成与集线器24和计算装置26通信,所述计算装置被配置成从集线器接收通知(例如,在安全装置处没有电力或者发生了破坏)。此外,图37-42展示了锁的形式的安全装置14的实施例,所述锁被配置成在无线网络中与集线器24通信。在这些实例中,客户可能能够请求帮助(例如,通过安全装置14上的呼叫按钮),所述帮助使得销售员工能够被通知,并且此后利用电子钥匙12或计算装置26来联系客户或控制安全装置14。零售员工可以使用电子钥匙12为顾客解锁安全装置14(参见例如,图38),或者使用计算装置26解锁安全装置。在一些情况下,顾客的移动电话可以执行本文所公开的一些功能(“可信顾客”),如响应于接收到无线授权信号来解锁安全装置14(参见例如,图39)。例如,可信顾客可以是已经购买了物品并且正在商店中提取所述物品的顾客,或者是在零售商处具有账户并且正在使用所述顾客的移动装置购买所述物品的顾客。另外,可以收集关于安全装置14的各种数据,例如从被锁保护的橱柜或抽屉中取出的产品的类型,并且允许向一个或多个计算装置26提供警报(参见例如,图40)。安全装置14可以被配置成在授权打开和获取商品项后自动重新锁定(参见例如,图41),并且可以采用各种技术来跟踪从橱柜或抽屉添加或移除的商品项,如RFID扫描仪,所述扫描仪被配置成在商品项被添加到橱柜或抽屉或从橱柜或抽屉移除时扫描产品(参见例如,图42)。

[0090] 在其它实施例中,可以获得关于如锁钩等安全装置14上的商品的库存信息,可以获得关于从安全装置(例如,橱柜)移除的商品项的信息,并且计算装置26可以用于获得各

种类型的信息并且提供用于控制安全装置和/或商品项的各种类型的命令。本文所公开的无线系统的实施例可以提供关于谁/什么/何时/何处/为什么/如何与安全装置14和商品项交互的实时报告,是响应性的/交互性的,在零售店内从安全焦点转移到全渠道体验实现,促进可信客户与安全资产的接触,允许容易地定制和扩展系统,实现如SaaS模型等替代性商业模型,将所连接资产的本地网络与用于本地计算的中央集线器连接,和/或将集线器连接到云平台,用于提供警报、报告、系统管理、日常操作。实施例还可以提供平台基础设施,所述平台基础设施具有每个零售店的中央集线器和几个适合目的的连接的终端安全装置资产,如均与集线器通信的支架、传感器、桌子管理器、锁、橱柜传感器、库存传感器、顾客住所传感器等。由于在一些实施例中无线系统的灵活性,由于平台基础设施是公共的,客户不需要预先选择购买哪个安全装置14。此外,零售商使用的计算装置26和移动装置可以允许零售商和商店员工动态地与安全装置14交互,以做出实时决策,如响应于安全事件、补充缺货库存或者响应于顾客对安全商品项的帮助请求。

[0091] 在一些情况下,每个电子钥匙12可以被授权用于特定的定位、部门或商品安全装置。例如,图4示出了经理可以具有对所有区域、定位、部门或商品安全装置(表示为数字1-6)的授权,而第一员工可能仅具有对两个区域、定位、部门或商品安全装置(表示为数字4和5)的授权,并且第二员工可能仅具有对一个区域、定位、部门或商品安全装置(表示为数字6)的授权。因此,零售店或其它机构可以限制同一零售店内不同员工的授权范围。为了适应不同的授权级别,每个钥匙12可以被配置成存储与每个区域、定位、部门或商品安全装置相关联的代码。例如,每个区域可以包含多个商品安全装置14,并且零售店可以具有多个区域(例如,电子产品区域、珠宝区域等)。

[0092] 可以使用各种技术对电子钥匙12进行初始编程。例如,电子钥匙12可以最初被呈现给每个经授权的商品安全装置14。在与安全装置14或云22通信时,电子钥匙12将与每个安全装置配对。编程站16可以向电子钥匙12提供代码,并且然后钥匙或云22可以将所述代码传送到其每个经授权的安全装置14。每个钥匙12可以进需要被编程一次。在一些实施例中,编程站16可以位于每个区域内,并且钥匙12可以从其被授权的每个编程站接收代码。此后,每个钥匙12可能需要在编程站16或充电站18处在预定的时间段之后或响应于被禁用而被“刷新”,如本文中的各个实例中所描述。在其它实施例中,电子钥匙12可以通过云22被直接编程。

[0093] 在另一个实施例中,每个电子钥匙12可以包含一个或多个商品安全装置14的安全代码和序列号。例如,在安全代码和序列号彼此匹配的情况下,钥匙12可能仅能够布防、撤防、锁定或解锁商品安全装置14。在一个实例中,每个序列号对于商品安全装置14是唯一的,并且可以在制造时或由零售商编程。此技术允许在对钥匙12进行编程和将钥匙分配到特定商品安全装置14和/或区域时具有更大的灵活性。在一个实施例中,设置电子钥匙12”可以用于初始映射特定商品安全装置14和序列号。在这方面,设置钥匙12”可以用于与每个钥匙12通信,并且获得每个商品安全装置14的序列号。设置钥匙12”也可以获得安全装置14的位置,或者设置钥匙的用户可以提供每个商品安全装置的描述(例如,SN#123＝商品安全装置#1)。设置钥匙12”可以与平板计算机或其它计算装置26通信,用于累积所有信息(参见例如,图3和19),这可以通过有线或无线通信来进行。因此,平板或计算装置26可以将每个序列号与商品安全装置14进行映射,并且在一些情况下,还可以包含序列号和对应的电子

钥匙12。单独的电子钥匙12然后可以被分配用于经授权商品安全装置14的特定序列号(例如,用户1包含序列号1、2、3;用户2包含序列号1、4、5)。可以使用编程站16用相同的安全代码对每个电子钥匙12进行编程。在一些实施例中,设置过程可以与商品安全装置14的货架图结合使用。货架图可以表示零售商店或其它机构内的商品安全装置14的布局。例如,当设置钥匙12"与每个商品安全装置通信时,所述设置钥匙可以用于将序列号映射到货架图上的特定商品安全装置14。设置钥匙12"可以与平板计算机或其它计算装置26通信,用于如通过有线连接(参见例如,图19)用序列号填充货架图。此货架图可以被上传到远程定位或装置,用于基于安全装置14与计算装置26之间交换的信息来管理货架图并且确保货架图符合性。与以前一样,特定的序列号可以被分配到经授权用户。

[0094] 为了布防、撤防、锁定或解锁商品安全装置14,电子钥匙12可以与特定的商品安全装置通信,并且确定安全代码和序列号是否匹配。如果代码匹配,则电子钥匙12布防、撤防、锁定或解锁商品安全装置14。在刷新电子钥匙12时和/或当用户通过编程或授权站16请求电子钥匙时,可以使用任何可用的电子钥匙,因为所述钥匙可以用所述用户的适当授权级别(例如,特定区域、部门和/或商品安全装置)实时编程。

[0095] 在一个实施例中,商品展示安全系统10包括电子钥匙12和商品安全装置14,所述商品安全装置被配置成由钥匙操作。所述系统可以进一步包括任选的编程站16,所述编程站可操作用于用安全代码对钥匙12进行编程,所述安全代码在本文也可以被称为安全撤防代码(SDC)。除了编程站16之外,所述系统可以进一步包括任选的充电站18,所述充电站可操作用于对安置在钥匙12内的电源进行初始充电和/或后续再充电。例如,钥匙12和商品安全装置14可以各自用相同的SDC编程到相应的永久存储器中。钥匙12可以配备有单次使用的(即,不可再充电的)电源,如常规的或延长寿命的电池,或者可替代地,钥匙可以配备有多次使用的(即,可再充电的)电源,如常规的电容器或可再充电电池。在任一种情况下,根据需要,电源可以是永久的、半永久的(即,可更换的)或可再充电的。在后一种情况下,充电站18被提供来对钥匙12内提供的电源进行初始充电和/或后续再充电。此外,钥匙12和/或商品安全装置14可以仅提供有暂时性存储器,使得SDC必须以预定的时间间隔被编程(或重新编程)。在此情况下,提供编程站16来初始编程和/或后续将SDC重新编程到钥匙12中。如将要描述的,钥匙12可操作来用SDC对商品安全装置14进行初始编程和/或后续重新编程。然后,钥匙12进一步可操作以通过将电力和/或数据传输到装置来操作商品安全装置14,如将描述的。

[0096] 在图1-2所展示的系统的示例性实施例中,电子钥匙12被配置成由编程站16用唯一的SDC编程。在一些实施例中,钥匙12被呈现给编程站16,并且例如通过按压或以其它方式致动设置在钥匙的外部上的控制按钮28来启动其间的通信。编程站16与钥匙12之间的通信可以直接实现,例如通过一个或多个电触点,或者间接实现,例如通过无线通信。能够在编程站16与钥匙12之间传输数据的任何形式的无线通信也是可能的,包含但不限于光传输、声传输或磁感应。在本文示出和描述的一些实施例中,编程站16与钥匙12之间的通信是通过无线光传输来实现的,并且更具体地,是通过在编程站和钥匙中提供的协作红外(IR)收发器来实现的。在一些实施例中,编程站16的功能可以类似于题为"用于保护商品的安全系统的编程站(PROGRAMMING STATION FOR A SECURITY SYSTEM FOR PROTECTING MERCHANDISE)"的美国专利第7,737,844号中公开的功能,所述专利的公开内容通过引用整

体并入本文。为了描述本发明的一些实施例,编程站至少包括用于生成或被提供有SDC的逻辑控制电路、用于存储SDC的存储器、以及适于以本文所描述的方式与电子钥匙12交互以用SDC对钥匙进行编程的通信系统就足够了。

[0097] 根据一个实施例的商品安全系统10的可用特征是电子钥匙12可以包含超时功能。更具体地,钥匙12向商品安全装置14传输数据和/或电力的能力可以在预定时间段之后被停用。通过实例的方式,电子钥匙12可以在从钥匙被编程或最后一次刷新的时间起约六至约二十四小时之后被停用。以此方式,经授权销售员工通常必须在每次轮班开始时对分配到他的钥匙12进行编程或刷新。此外,充电站18可以被配置成当电子钥匙12定位于充电端口30内或者以其它方式与所述充电端口接合时,停用所述钥匙(参见例如,图1)。以此方式,充电站18可以被经授权的销售员工使用。在一个实施例中,电子钥匙12可以在销售员工输入授权码时被授权,以释放钥匙供使用。例如,销售员工可以在与充电站18通信的键盘上输入代码。当输入正确的代码时,充电站18可以指示哪个钥匙12被销售员工授权以供使用(例如,通过听觉和/或视觉指示器)。在一些情况下,超时时段可以由用户预先确定或定制。例如,零售店的经理可以为一个或多个电子钥匙12输入特定的时间段。那些“活动的”电子钥匙12可以通过基于云的网络内的通信来监测。在其它实施例中,电子钥匙12可以响应于事件而超时或以其它方式被禁用。例如,电子钥匙12可以响应于钥匙被放错地方或被盗,或者钥匙被带入未被授权以供使用的零售店而被禁用。此类禁用可以可替代地通过来自装置26的通过云22发送到电子钥匙12的命令来发生。在其它情况下,电子钥匙12可以响应于与网络通信失败(例如,在特定时间或时间间隔)、失去与网络的连接和/或不能重新连接到网络而被禁用。在另一个实例中,电子钥匙12可以响应于其存储器已满(例如,具有审计数据)而被禁用。

[0098] 在一个实施例中,可以远程提供用于采取各种动作的命令。例如,在发生盗窃的情况下,可以从远程定位或装置26(例如,平板计算机或计算机)提供命令来锁定和/或布防商品安全装置14的全部或一部分。类似地,可以从远程定位或装置26提供命令来停用电子钥匙12和/或安全装置14的全部或一部分。因此,系统10提供了用于电子钥匙12、商品安全装置14和系统内其它组件的集中安全和控制的技术。如上文所讨论,电子钥匙12也可以被远程控制。此外,在一些实施例中,此类请求或命令可以由计算装置26针对单独安全装置14或多个安全装置做出(例如,响应于安全事件发送锁定所有安全装置的命令)。此外,安全装置14中的一个或多个安全装置可以被配置成响应于安全事件而锁定或报警(例如,自动将连接到商品项的传感器锁定到可移除地支撑传感器的基座)。

[0099] 图5-6展示了电子钥匙12的一个实施例。电子钥匙12可以包含用于激活钥匙的控制按钮28,如用于启动与商品安全装置的通信。此外,电子钥匙12还可以包含一个或多个视觉指示器。在这方面,钥匙12可以包含一个或多个状态指示器32,所述一个或多个状态指示器展示了钥匙与商品安全装置14的通信的状态。状态指示器32可以引导用户知道钥匙12与商品安全装置14之间的通信何时正在进行并且已经完成。状态指示器32可以根据通信是授权的(例如,解锁或撤防)、未授权的(例如,错误的区域或部门)还是不成功的而不同。状态指示器32还可以指示钥匙12上剩余的授权使用时间量,如钥匙包含如上文所讨论的超时特征。电子钥匙12还可以包含一个或多个其它指示器34,所述一个或多个其它指示器提供钥匙上剩余电力的视觉指示。这些其它指示器34也可以用于任何其它期望的目的,如指示钥

匙12的编程状态。例如,指示器34可以在电子钥匙12被初始编程时被激活。应当理解,所展示的状态指示器32、34仅用于说明,因为在替代性实施例中可以采用各种类型和配置的指示器。

[0100] 图7-10展示了电子钥匙12的另外实施例。在这些实例中,电子钥匙12包含可移除部分36。在图7-8中,可移除部分36允许接近输入电源端口38,如用于对电子钥匙12进行再充电。可移除部分36可以被配置成相对于电子钥匙12滑动,以暴露输入电源端口38。输入端口38可以被配置成接收并且电连接到对应的连接器,如与充电站18相关联的连接器。例如,电子钥匙12可以被配置成停靠在充电站18内用于对其进行充电(参见例如,图1)。如图9-10所示,可移除部分36也可以被配置成从电子钥匙12完全移除,并且可以是多用途的,因为它可以包含工具部分40。例如,工具部分40可以用于促进断开连接各种连接器,如螺丝刀等。电子钥匙12可以包含开口42,所述开口被限定为在非使用位置将可移除部分36收纳在其中。

[0101] 图20-21示出了电子钥匙12'的另外的实施例。在此实施例中,电子钥匙12'包含一个或多个对准特征15,用于促进与编程或授权站16'和/或充电站18'的对准,如下文进一步详细讨论的。另外,电子钥匙12'包含输入端口17(例如,微型USB端口),所述输入端口可以被配置成可释放地接合编程或授权站16'和/或充电站18'上的对应端口,用于数据和/或电力传输。值得注意的是,在图20所示的实例中,电子钥匙12'上的输入端口17位于侧表面上,而一对对准特征15设置在电子钥匙的相对表面上。在图21所示的实施例中,提供了单个对准特征15。输入端口17可以位于一个端部处的传输端口与相对端部处的钥匙链环开口之间的侧表面上。将输入端口17定位在电子钥匙12'的侧表面上可以提供对编程或授权站16'和/或充电站18'的更安全和稳定的连接。如上文所讨论,可以在电子钥匙12'的外部上提供一系列状态指示器32、34,例如发光二极管(LED),用于指示其操作状态。

[0102] 如图1所示,编程站16包括壳体,所述壳体被配置成包含生成SDC的逻辑控制电路、存储SDC的存储器、以及用于将SDC传送到钥匙的通信系统(例如,无线地)。在使用中,逻辑控制电路生成SDC,其可以是预定的(即,“工厂预置的”)安全码、手动输入的安全码或由逻辑控制电路随机生成的安全码。在后一种情况下,逻辑控制电路进一步包括用于产生唯一SDC的随机数生成器。一系列视觉指示器,例如发光二极管(LED)可以设置在壳体的外部,用于指示编程站16的操作状态。编程站16可以进一步设置有访问机构,用于防止未经授权的人使用编程站。例如,编程站可以包含键盘44。经授权用户可以在键盘44中输入代码,所述代码允许编程站16生成用于传送到钥匙12的SDC。

[0103] 在特定实施例中,编程站16的逻辑控制电路与钥匙的逻辑控制电路执行数据的电子交换,通常被称为“握手通信协议”。握手通信协议确定钥匙12是先前未被编程的授权钥匙(例如,“新”钥匙),还是在后续时间被呈现给编程站16以刷新SDC的授权钥匙。在握手通信协议失败的情况下,编程站16不会向试图获得SDC的未经授权的装置提供SDC。当握手通信协议成功时,编程站16允许SDC由钥匙12发射。对于本领域技术人员来说显而易见的是,根据需要,SDC可以通过任何合适的方式从编程站16发射到钥匙12,包含但不限于无线、电接触或机电、电磁或磁导体。此外,在其它情况下,编程站16可以仅向电子钥匙12提供SDC,而无需首先启动任何握手通信协议。

[0104] 在一些实施例中,商品安全装置14是“无源”装置。如本文所使用的,术语“无源”是

指安全装置14不具有足以锁定和/或解锁机械锁机构的内部电源。当商品安全装置14是无源的时,零售商获得了显著的成本节约,因为内部电源的费用局限于钥匙12,并且一把此类钥匙能够操作多个安全装置。如果期望的话,商品安全装置14还可以设置有临时性电源(例如,电容器或有限寿命电池),其具有足够的电力来响应于安全漏洞而激活警报器,例如压电听觉警报器,所述警报器由传感器致动,例如接触、接近或限位开关。临时性电源也可以足以从商品安全装置14向钥匙12传送数据,例如SDC,以认证安全装置,并且由此授权钥匙向安全装置提供电力。在其它情况下,安全装置可以是电子装置,例如连接到商品的传感器和可移除地支撑其上的传感器的基座。传感器可以用系绳连接到基座,或者可以是无线的(例如,使用如下文更详细描述的测距技术)。

[0105] 在一些实施例中,商品安全装置14进一步包括逻辑控制电路,类似于安置在钥匙12内的逻辑控制电路,所述逻辑控制电路被适配成以与编程站16与钥匙之间的方式基本上相同的方式与钥匙的逻辑控制电路执行握手通信协议。实质上,钥匙12的逻辑控制电路和商品安全装置14的逻辑控制电路彼此通信,以确定商品安全装置是不具有安全码的授权装置,还是具有匹配SDC的装置。在握手通信协议失败的情况下(例如,装置未被授权或者装置具有不匹配的SDC),钥匙12不会用SDC对装置进行编程,并且因此,商品安全装置不会进行操作。如果商品安全装置14先前用不同的SDC进行编程,所述装置将不再与钥匙12通信。在握手通信协议成功的情况下,钥匙12允许存储在钥匙中的SDC被发射到商品安全装置14,以用SDC对装置进行编程。对于本领域技术人员来说显而易见的是,根据需要,SDC可以通过任何合适的方式从钥匙12发射到商品安全装置14,包含但不限于通过射频、一个或多个电触点、机电、电磁或磁导体。此外,SDC可以通过从电子钥匙12到商品安全装置14的数据感应传输来发射。此外,在其它情况下,电子钥匙12可以仅向商品安全装置14提供SDC,而无需首先启动任何握手通信协议。

[0106] 在一个实施例中,当握手通信协议成功并且商品安全装置14是具有匹配SDC的授权装置时,商品安全装置可以被布防或撤防,如在安全装置包含警报电路的情况下。在其它实施例中,当SDC码匹配时,商品安全装置14可以被布防或撤防。在一些实施例中,当握手通信协议成功并且SDC码匹配时,钥匙12的逻辑控制电路使钥匙的内部电源向装置14传输电力,以操作机械锁机构。在其它实施例中,当SDC码匹配并且电力被传输到商品安全装置时,商品安全装置14可以被锁定或解锁。应当理解,可以交换各种信息和代码,以便执行期望的功能,如布防、撤防、锁定或解锁商品安全装置14。例如,交换的数据可以包含仅商品安全装置的序列号和/或SDC。

[0107] 图11更详细地示出了商品安全装置140的一个实施例。如先前所述,商品安全装置14可以是利用警报电路和/或将锁锁定和/或解锁的锁机构的任何类型的安全装置。在一些情况下,商品安全装置140可以是无源装置,因为它不具有足以操作锁机构的内部电源。因此,商品安全装置140可以被配置成从外部源,如本文所示和所描述的电子钥匙12,接收电力,或者可替代地电力和数据两者。图11所描绘的商品安全装置的实施例是橱柜锁,所述橱柜锁被配置成牢固地固定到常规橱柜锁托架105的锁臂104。如先前所描述,橱柜锁140可以包含逻辑控制电路,用于与钥匙12的逻辑控制电路执行握手通信协议,并且用于从钥匙接收SDC。在其它实施例中,橱柜锁140可以被配置成将SDC发射到钥匙12以认证安全装置,并且由此授权钥匙将电力传输到安全装置。

[0108] 图12更详细地示出了具有感应传输的电子钥匙120的实施例。如先前所述,钥匙120可以被配置成将数据和电力两者传输到商品安全装置140。因此,可编程电子钥匙120可以是有源装置,因为它具有足以操作商品安全装置140的机械锁机构的内部电源。因此,可编程电子钥匙120可以被配置成从内部源传输数据和电力两者,所述内部源如安置在钥匙内的逻辑控制电路(例如,数据)和电池(例如,电力)。本文所描绘的可编程电子钥匙120的实施例是具有感应传输能力的钥匙,所述钥匙被配置成被收纳在图11所示的橱柜锁140的传输端口142以及编程站的编程端口46和充电站的充电端口30内。因此,电子钥匙120可以被放置成靠近传输端口142或位于所述传输端口内,用于与其通信。在一些实施例中,如上文所讨论的标签(例如,RFID或NFC标签)可以定位于传输端口内,或者以其它方式位于安全装置140上,使得电子钥匙120被配置成从标签读取或者以其它方式获得识别数据。

[0109] 在一些实施例中,电子钥匙120包括具有内部空腔或隔室的壳体121,所述内部空腔或隔室包含钥匙的内部组件,包含但不限于逻辑控制电路、存储器、通信系统和电池,如将要描述的。如所示出的,壳体121由下部部分123和上部部分124形成,所述下部部分和所述上部部分在组装之后例如通过超声波焊接结合在一起。电子钥匙120进一步在一个端部限定了开口128,用于将钥匙联接到钥匙链环或挂绳等。电子钥匙120可以进一步包括位于壳体121的与开口128相对的端部处的传输探针125,用于将数据和/或电力传输到商品安全装置140。如先前所描述,传输探针125还可操作来从编程站16发射和接收握手通信协议和SDC,并且从充电站接收电力。

[0110] 如图13中最佳示出的,内部电池131和逻辑控制电路或印刷电路板(PCB)132安置在电子钥匙120的壳体121内。电池131可以是适于与充电站18一起使用的常规的延长寿命的可更换电池或可再充电电池。逻辑控制电路132可操作地耦接并且电连接到开关133,所述开关由通过壳体121设置在钥匙120的外部上的控制按钮122致动。控制按钮122结合开关133控制逻辑控制电路132的某些操作,并且具体地数据和/或电力的传输。在这方面,逻辑控制电路132进一步可操作地耦接并且电连接到通信系统134,用于传输数据和/或电力。在一个实施例中,通信系统134是无线红外(IR)收发器,用于电子钥匙120与编程站之间以及钥匙与商品安全装置140之间的数据的光传输。因此,钥匙120的传输探针125可以设置有光学透明或半透明的滤光器窗口135,用于根据需要发射和收集钥匙120与编程站16之间或者钥匙与商品安全装置140之间的光传输。传输探针125可以进一步包括感应芯127和感应芯绕组129,用于根据需要将电力传输到商品安全装置140和/或从充电站18接收电力以对内部电池131进行充电。可替代地,可以排除光收发器134,并且通过感应线圈126的磁感应在可编程电子钥匙120与商品安全装置140之间传输数据。

[0111] 在一些实施例中,电子钥匙120的重要方面,尤其是当与本文所描述的商品安全装置140结合使用时,在于钥匙不需要用户对钥匙施加物理力来操作商品安全装置的机械锁机构。通过延伸,钥匙120没有在机械锁机构上施加物理力。因此,钥匙120不会像常规的机械钥匙和锁机构经常发生的那样在锁中被意外折断。此外,钥匙120和机械锁机构都不会像常规机械钥匙和锁机构那样经常发生过度磨损。另外,在一些情况下,不需要电子钥匙120的传输探针125相对于编程站、充电站和/或商品安全装置140中的任何一个上的端口的定向。因此,传输探针125上的电触点以及端口的任何磨损可以被最小化。作为一些实施例中的另外的优点,经授权人员不需要将电子钥匙120的传输探针125定位在相对于商品安全装

置140的传输端口142的特定定向上,并且然后对钥匙施加压力和/或扭力来操作装置的机械锁机构。

[0112] 图22-24展示了编程或授权站16'的实施例。如所展示的,编程或授权站16'包含用于收纳如上文所讨论的电子钥匙12'的几何形状(参见例如,图21)。在这方面,编程或授权站16'可以包含一个或多个对准特征15',所述一个或多个对准特征被配置成与电子钥匙12'的对准特征15对准并接合。此外,编程或授权站16'可以进一步限定凹槽48,用于至少部分地收纳电子钥匙12'的侧表面。凹槽48可以是弯曲的或任何其它形状,以对应于电子钥匙12'的形状。在凹槽48内,编程或授权站16'可以包含端口30',用于可释放地接合电子钥匙12'的输入端口17。对准特征15、15'被配置成彼此对准,以确保输入端口17和端口30'彼此对准和接合。此类接合可以允许电子钥匙12'与编程或授权站16'之间的数据通信,所述数据通信在一些情况下可以在使用键盘44输入授权码时发生。另外,编程或授权站16'可以包含一个或多个输入端口50,用于接收电力和数据通信(例如,以太网端口)。

[0113] 图1更详细地示出了充电站18。如先前所述,充电站18对钥匙12的内部电池131进行再充电。在某些情况下,充电站18还停用钥匙12的数据传输和/或电力传输能力,直到编程站16用SDC对钥匙进行重新编程,或者用户向充电站提供授权码。无论如何,充电站18包括用于容纳充电站的内部组件的壳体。壳体的外部具有形成在其中的至少一个,并且优选地多个充电端口30,所述充电端口的尺寸和形状被设定为收纳电子钥匙12(参见例如,参见图1)。可以提供机械或磁性装置,用于将钥匙12正确定位并牢固地保持在充电端口18内,以确保正确的电力传输。

[0114] 图16-18示出了充电站18的实施例,其中提供了多个端口30用于与多个对应的电子钥匙12'接合。图21中所示的电子钥匙12'可以与图16-18中所示的充电站18兼容,由此电子钥匙12'在其侧面包含用于与端口30接合的输入端口17,类似于结合编程或授权站16'所描述的端口。同样,每个端口30可以位于相应的凹槽48内,用于收纳电子钥匙12'的至少一个侧表面。此布置可以允许更多数量的电子钥匙12'在任一时刻与充电站18接合。

[0115] 图14-15示出了商品安全装置150的另外的实施例。在此实施例中,商品安全装置150包括利用“能量收集”的锁机构。因此,商品安全装置150可以是如上文所描述的无源装置。然而,在此实施例中,商品安全装置150包含用于生成要存储的电力的装置。例如,商品安全装置150可以被配置成在锁定位置与解锁位置之间旋转,并且包含被配置成生成要存储的能量(例如,通过电容器)的生成器。在一些情况下,商品安全装置150可以包含边框,并且边框的每一圈可以生成要存储的电荷。在一个实施例中,电子钥匙12可以最初用于脱离接合机械锁,并且然后商品安全装置150可以旋转到解锁位置。商品安全装置150然后可以旋转回到锁定位置。由于商品安全装置150不具有电源,安全装置能够使用存储的电力执行各种安全功能。例如,商品安全装置150可以被配置成使用存储的电力来将数据推送到一个或多个节点20,或者生成听觉和/或视觉信号。在一个实例中,商品安全装置150可以包含内部无线电,用于使用存储的电力发射无线信号,如用于在安全装置被篡改时生成求救信号。在另一个实例中,商品安全装置150可以包含由存储的电力供电的发光装置(LED)。

[0116] 在另一个实施例中,多个节点被用于对等通信,以促进生成警报信号,如听觉和/或视觉信号。例如,图25示出了多个商品安全装置14(例如,传感器)和警报节点30,所述商品安全装置和所述警报节点被配置成通过网络将各种信息无线传送到网关24。例如,传感

器14和/或节点30可以被配置成向网关24发送关于它们的配置、警报状态(例如,报警、布防、撤防)和/或指令(例如,布防、报警或撤防)的信息和从所述网关接收所述信息。商品安全装置14和节点30也可以被配置成如下文所描述彼此直接通信,以及在与网关24的通信与彼此的通信之间切换。任何数量的节点30可以位于零售店内的不同位置处,例如,在展示台上或商店入口或出口。节点30可以使用各种无线通信协议与网络内的商品安全装置14和网关24进行无线通信,如上文所描述。使用无线通信在远离商品安全装置14的定位处启动警报的一个缺点是,警报信号通常必须传播到无线集线器,在所述线集线器,服务器然后解密数据并决定向适当的警报节点发出警报信号。这种系统可能在生成警报信号时产生等待时间,特别是如果服务器不在本地,并且如果无线通信链的任何组件被中断(例如,集线器断电),警报信号可能永远不会到达警报节点,并且因此不会发生警报。在一个实施例中,可以使用多种通信模式来减少或消除这些问题。例如,除了商品安全装置14与网关24和/或警报节点30与网关之间的第一无线通信协议(例如,WiFi、LoRa等)之外,可以使用第二无线通信协议,所述第二无线通信协议是商品安全装置与警报节点之间的不必也与任何集线器或网关通信的直接节点到节点通信方案。在一些实施例中,通信协议可以相同或不同。在一个实例中,第二无线通信协议可以使用与其它操作信号与集线器或网关24(例如,Wi-Fi、LoRa等)通信的相同的无线电天线来执行,从而不会给商品安全装置14和警报节点30增加另外的成本或尺寸来完成通信。然而,第二无线电也是一种选择。另外,警报信号可以在与其它信号不同的频率上广播,以便满足地区法规要求和/或如果检测到或知道某些频带变得拥塞。此通信可以是双向的,但是在大多数情况下单向通信就足够了。商品安全装置14可以响应于安全事件发出“帮助我”信号。警报节点30然后将仅需要“监听”所述信号,并且如果它接收到所述信号,警报节点可以通过它被编程的任何手段(例如,光、声音、振动等)生成警报。

[0117] 在一些情况下,可以使用多个警报节点30,并且特定的商品安全装置14可以被配置成激活特定的警报节点。例如,在零售店包含用于多个商品安全装置14的多个展示台的情况下,可能存在与每个台相关联的警报节点30,所述警报节点仅由来自与同一台相关联的任何一个商品安全装置的“帮助我”信号触发。在此情况下,标识符(例如,ID代码)可以被添加到“帮助我”信号,所述信号对应于存储在警报节点30中的代码。因此,警报节点30可能必须接收或识别其代码,以便生成警报信号。例如,如果需要将超过一个动作(例如,“警报”或“停止报警”)传送到警报节点,这可以简单到代码本身是“帮助我”信号,或者某个其它指令代码可以被添加到标识符或包含在标识符中。商品安全装置14可以被配置成在发生破坏时立即生成此“帮助我”信号,并且仅在将所述信号发送到警报节点30之后,商品安全装置才会通过无线通信向集线器和网关传送发生了破坏。因此,在此类破坏情况下,应当最小化延迟。

[0118] 如上文所讨论,电子钥匙12、120和计算装置26可以被配置成通信和/或控制各种安全装置14。图43展示了商品展示安全系统200的实施例,其包含用于锁定各种类型的固定装置(如橱柜和抽屉)的锁202。在图43和47所示的实例中,锁202可以用于固定滑动玻璃门和抽屉(也参见图48-49)。系统10可以包含用于锁202、计算装置26、集线器或网关、电子钥匙12、120和/或远程装置之间通信的各种无线功能。例如,图44展示了零售店可以包含无线路由器等形式的无线通信电路系统,集线器24可以促进Wi-Fi通信,但是也可以使用其它形

式的通信,如蜂窝通信。集线器24可以用于促进计算装置26与一个或多个远程装置之间的通信。在一些情况下,电子钥匙120可以被配置成也通过集线器24与一个或多个远程装置通信。计算装置26与一个或多个远程装置之间的通信可以用于向各种计算装置分配授权和/或传送各种数据类型,如上文所公开的数据类型。

[0119] 计算装置26可以包含被配置用于BLE、蓝牙和/或NFC通信的无线通信电路系统。计算装置26还可以或可替代地包含相机或扫描仪,用于扫描来自锁202的图像或信息,如下文进一步详细讨论的。类似地,锁202可以包含被配置用于BLE、蓝牙和/或NFC通信的各种无线通信电路系统。锁202也可以或可替代地包含条形码或其它标识符。在一些情况下,计算装置26可以被配置成与一个或多个锁202配对(例如,通过蓝牙通信)和/或包含用于操作锁的一个或多个另外的通信协议(例如,NFC、相机、条形码等)。

[0120] 在一个示例实施例中,计算装置26被配置成使用第一通信协议(例如,蓝牙)与一个或多个锁202通信。为了解锁特定的锁,计算装置26可以进一步被配置成使用第二通信协议(例如,NFC或图像扫描)与每个锁通信。第二通信协议可以用于识别计算装置26被授权解锁的特定锁202。例如,NFC标签可以具有对于锁202唯一的标识符(类似于序列号),并且如果计算装置26确认标识符匹配,则计算装置被授权对锁进行解锁。如果基于对锁202的识别的确认,计算装置26被授权,则计算装置可以使用第一通信协议向锁传送解锁命令。

[0121] 锁202可以采取许多不同的形式和配置。锁202可以包含用于不同应用的各种类型的锁组合件,如用于滑动橱柜门的柱塞锁或用于抽屉的凸轮锁。图45示出了锁202的一个实施例,其中锁包含锁组合件、驱动组合件、NFC标签、具有IR收发器的传输端口、感应线圈、具有蓝牙模块的PCBA 214以及内部电源(例如,电池)。此外,图46示出了锁202可以根据应用具有不同的形状。例如,一些锁202可以包含或可以不包含内部电源,有此影响锁的尺寸。在一些应用中,内部电源可以在锁202的外部,如对于抽屉,其中锁可以定位于抽屉的前面,并且内部电源可以定位于抽屉内部并且与锁电通信。在图50中进一步展示的一个实施例中,锁202可以包含NFC标签204和传输端口206,其中传输端口类似于上文描述的用于与电子钥匙12、120通信的端口。NFC标签204可以定位于遮盖或以其它方式隐藏NFC标签的盖208的后面。例如,盖可以是具有旋转金属效果的塑料。在另一实例中,锁202可以包含2D条形码210。锁202可以包含可移除盖208,所述可移除盖被配置成隐藏NFC标签204、条形码210或类似标识符,并且被移除以与计算装置26通信。

[0122] 如上所述,锁202可以被配置成与电子钥匙120通信,用于解锁所述锁。图51示出了通过传输端口206与锁202通信的钥匙120的实例。除了使用计算装置26来对锁进行解锁之外,或者作为其替代,还可以使用钥匙120。在锁202的电源不再能够将锁解锁的情况下(例如,电池耗尽),钥匙120可以被配置成将电力传输到锁以对锁进行操作,如上文所公共的。在另一个实施例中,图52示出了内部电源可以是模块化组件212,使得所述电源可以被另一个电源替代,如以具有包含一个或多个电池的壳体的可移除电池包的形式。在其它情况下,如果不再需要内部电源或者锁被用于不同的应用,则可移除电池包可以被移除并且用盖替代。因此,即使内部电源不能将锁解锁,本发明的实施例也能够操作锁202。

[0123] 在一些实施例中,电源(例如,电池包)的模块化可以依赖于或独立于锁202的操作。在这方面,如果电源被盗窃妨碍了锁202的操作,则其可能是有问题的。在一个实例中,用于将锁202解锁的锁定机构可以依赖于用于访问内部电源的机构。因此,用户将需要使用

计算装置26或电子钥匙120来访问内部电源。在可以访问内部电源之前,锁202可能需要处于解锁状态,有此在能够访问内部电源之前需要经授权用户在场。在其它实施例中,独立于锁202的锁定机构的第二锁机构可以用于访问内部电源。第二锁机构可以被配置成由计算装置26、电子钥匙120和/或其它类型的钥匙操作。例如,机械锁机构可以使用磁性钥匙或工具来操作,所述磁性钥匙或工具被配置成解锁所述锁机构以释放或访问内部电源。在一些情况下,可以使用不同的用户访问级别,使得仅特定的用户被授权解锁第二锁机构以访问内部电源(例如,经理可以被分配用于此类访问的访问权限,但是零售员工没有)。当如上文所公开分配访问权限时,可以使用此类访问级别。

[0124] 在操作中,图53示出了用户使用计算装置26来使用NFC通信来将锁解锁的实例,其中用户将计算装置放置成靠近在NFC标签204,这使得自动将锁解锁。图53还示出了用户可以使用计算装置26的相机或扫描仪来扫描条形码210以将锁解锁。消费者或商店员工可以使用计算装置26的相机来将锁202解锁,而仅商店员工可以被授权使用计算装置26的扫描仪。计算装置26可以包含软件应用程序,所述软件应用程序促进与任何上述实例中的锁的通信,如通过允许用户选择用于将锁202解锁的“解锁”命令,如果用户被授权这样做的话。授权可以以各种方式完成,如通过上文所描述的实施例(例如,特定锁或区域的分配)。在其它情况下,用户可以通过下载软件应用程序并且输入用于识别用户的各种信息而被授权。软件应用程序也可以是密码保护的,用于确保用户被授权操作锁202。另外,软件应用程序可以促进数据收集和与一个或多个远程装置的通信。

[0125] 在一些实施例中,在使用计算装置26或电子钥匙120将锁解锁之后,用户可能需要将锁202手动解除闩锁。在来自计算装置26的成功解锁命令之后,图54示出了用户可以具有有限或预定量的时间来将锁202解除闩锁。例如,锁202可以包含可视指示器(例如,LED),其根据锁202是否能够被解除闩锁而照射或闪烁不同颜色的频率。如果用户在成功的解锁命令之后选择将锁202解除闩锁,锁可以被配置成手动解除闩锁,如通过旋转或拉动锁的一部分。例如,如果锁202是凸轮式锁,用户可以旋转旋钮来将锁解除闩锁,而如果锁是柱塞式锁,用户可以拉动旋钮来将锁解除闩锁。锁202可以被配置成在预定时间段之后自动重新锁定自身。此外,用户可能需要将锁202手动重新闩锁。在一些情况下,可能需要用户在相反的方向上旋转或推动锁202的旋钮,以将用于将锁解除闩锁的旋钮重新闩锁。如果用户过早地将锁202重新闩锁,当固定装置处于其完全关闭位置时,用户可能需要首先将锁解锁以再次将锁重新闩锁。应当理解,锁202可以包含用于将锁解除闩锁的各种致动器,如可以用于将锁手动解除闩锁和重新闩锁的旋钮、把手等。在其它实施例中,可以省略单独的闩锁操作,如在用户能够打开门而不必将闩锁机构解除闩锁的情况下。

[0126] 图55-58展示了根据本发明的一个实施例的锁302。在此实施例中,锁302可以是滑动锁,所述滑动锁被配置成与如一个或多个滑动门等固定装置一起使用。例如,锁302的解锁允许柱塞销306与安装到固定装置的锁扣板304的接合解除闩锁,由此允许接近固定装置(例如,将门滑动开)。类似于上文所讨论的实施例,锁302可以被配置成与各种计算装置26、集线器或网关、电子钥匙12、120和/或远程装置通信。此外,锁302可以包含用于与计算装置26通信的NFC标签204、条形码210或类似标识符,和/或用于与电子钥匙12、120通信的传输端口206。在一些实施例中,旋钮或其它致动器可以被配置成由用户轴向推动和牵拉,用于使柱塞销306在锁定状态与解锁状态之间移动,尽管可以采用其它手动运动,如旋转。在其

它实施例中,柱塞销306可以被配置成在锁定状态与解锁状态之间自动移动,而无需手动致动,如下文所描述。当处于解锁状态时,用户能够将锁302滑动到未闩锁位置,以由此接近固定装置。当然,在其它实施例中,其它手动致动可以用于将锁移动到未闩锁位置(例如,旋转、推动/牵拉等)。在一些实施例中,柱塞销306的端部可以以这样的方式配置,使得锁302能够自由地朝向闩锁位置移动,但是阻止或禁止朝向未闩锁位置的移动(例如,通过如图61所示的倾斜或锥形端部)。

[0127] 锁302可以包含开口308,所述开口被配置成收纳穿过其中的锁扣板304。因此,当锁在闩锁位置与未闩锁位置之间移动时,锁扣板304可以被配置成滑动或以其它方式被引导穿过开口308。如图57所示,锁扣板304可以包含沿其长度限定的多个开口312,其中每个开口的尺寸被设定成并且被配置成收纳柱塞销306的端部。锁扣板304可以包含多个开口以容纳不同的固定装置和/或可以允许安装中更大的灵活性。在使用中,锁302可以被配置成安装到固定装置的第一组件330(例如,第一门),并且锁扣板304可以被配置成安装到固定装置的第二组件332(例如,第二门)。在一些情况下,锁302和固定装置的相关联的第一组件330可以被配置成当在闩锁位置与未闩锁位置之间移动时相对于锁扣板304和固定装置的相关联的第二组件332滑动。

[0128] 锁扣板304可以被配置成当锁从未闩锁位置移动到闩锁位置时相对于锁302移动以使锁相对于锁扣板对准。因此,锁302可以被配置成当锁扣板304接近或进入限定在锁中的开口308时,促进所述锁扣板的端部对准,这可以减轻由固定装置的第一组件330和第二组件332的间隙或其它不规则性引起的问题。在这方面,当锁从未闩锁位置移动到闩锁位置时,锁扣板304可以是柔性的、铰接的、弹簧加载的或以其它方式能够相对于锁壳体移动。在一个实例中,锁302可以包含磁体320,所述磁体被配置成当锁朝向或沿着锁扣板304移动时吸引所述锁扣板(参见例如,图64)。因此,在一些情况下,锁扣板304可以包括被配置成被磁体320吸引的磁性吸引材料。当然,在其它实施例中,磁体320可以安装在锁扣板304上或者与所述锁扣板集成在一起,并且锁302包含磁性吸引材料。在一个实例中,锁扣板304可以被配置成响应于磁体320与锁扣板304之间的磁引力而绕接头324铰接或弯曲。此外,经考虑,接头324可以是柔性的或向锁302偏压的,以促进锁与锁扣板304之间的对准。

[0129] 图59-63示出了锁302的内部视图的实施例,其中为了图示的目的移除了锁的后壳体。锁302包含凸轮314,所述凸轮可操作地与电机310接合,并且被配置成接合柱塞销306。因此,给电机310通电使凸轮314旋转,这进而使柱塞销306线性移动。例如,凸轮314的旋转(例如,逆时针)将使凸轮接触柱塞销306,以将柱塞销从锁扣板304的接合中缩回,从锁定状态到解锁状态,同时凸轮的进一步旋转将使(或允许)柱塞销重新接合锁扣板。在一个替代方案中,凸轮314被配置成在一个方向上旋转以缩回柱塞销306,并且在相反方向上旋转以使柱塞销重新接合锁扣板304。柱塞销306可以在期望的方向上被偏压,如通过弹簧318相对于锁扣板304被偏压向锁定状态。因此,在凸轮314已经充分旋转以缩回柱塞销306之后,柱塞销可以被配置成由于弹簧的偏压而自动返回到其延伸位置。凸轮314的旋转轴线可以与电机310的轴线同轴。在一些情况下,柱塞销306可以限定被配置成由凸轮314接合的内表面。例如,柱塞销306可以包含开口,所述开口被配置成收纳并围绕凸轮314。凸轮314可以是各种形状的,但是如图63所示,凸轮可以包含圆形表面(例如,泪珠形)。

[0130] 在一些情况下,计算装置26或电子钥匙12、120的经授权用户可以与锁302通信,用

于移动凸轮314,由此使柱塞销306与锁扣板304脱离接合。因此,如上文所讨论,凸轮314的旋转使柱塞销306移动。然后,用户能够相对于锁扣板304线性滑动锁302,以将锁与锁扣板解除闩锁,由此允许打开和接近固定装置。为了将柱塞销306重新闩锁,用户可以线性滑动锁302以使锁与锁扣板304重新接合,这使柱塞销306与锁扣板重新接合。因此,在一些情况下,柱塞销306可以被配置成当锁相对于锁扣板从未闩锁位置移动到闩锁位置时自动接合锁扣板304。

[0131] 在一些实施例中,锁302可以进一步包含一个或多个开关,所述一个或多个开关被配置成响应于柱塞销306和/或凸轮314的移动而被接合和脱离接合,用于向电机310发送信号以开启或关闭电机。以此方式,当经授权的计算装置26或电子钥匙12、120被呈现给锁302时,电机310可以开启,并且当柱塞销306已经移动了足以使柱塞销与锁扣板304脱离接合的预定距离时,或者当凸轮314已经旋转了预定旋转角度时,所述电机可以关闭。锁302可以进一步包含柱塞开关318,所述柱塞开关被配置成提供锁处于锁定状态和/或闩锁位置的信号。柱塞开关318可以被配置成检测与锁扣板304的接合,这指示锁处于锁定状态和/或闩锁位置。例如,当柱塞开关318接合或以其它方式感测锁扣板304时,柱塞销306可以被配置成接合锁扣板中的第一开口312或其它开口,以指示锁处于锁定状态和闩锁位置。此数据可以由锁302存储和/或报告给计算装置26、电子钥匙12、120和/或远程装置。柱塞开关318可以包含类似柱塞销306的倾斜或锥形端部(参见例如,图61)。类似于上文所讨论的实施例,锁302可以包含电源322,在一些情况下,所述电源可以容纳在模块化组件212内(参见例如,图65)。

[0132] 关于安装,如上文所讨论,锁302可以被配置成安装到固定装置的第一组件330(例如,第一门),并且锁扣板304可以被配置成安装到固定装置的第二组件332(例如,第二门)(参见例如,图64)。锁302和锁扣板304可以用粘合剂和/或紧固件连接。当处于解锁状态时,锁302和第一组件330可以滑动脱离与锁扣板304的接合,到达未闩锁位置,这允许接近固定装置。在与闩锁状态相反的方向滑动锁302使柱塞销306重新接合锁扣板304。如上所述,锁302可以包含磁体320,所述磁体被配置成将锁扣板304的端部吸引向锁,这可以使锁扣板被定位成与第一组件330齐平,以相对于锁的开口308对准锁扣板。一旦锁扣板304的端部通过开口308插入,柱塞销306的端部可以被配置成在尺寸和构造被设定成收纳柱塞销的开口312之一内接合和脱离接合锁扣板304。因此,当柱塞销306从锁扣板302缩回时,固定装置能够被打开。

[0133] 前面已经描述了各种安全系统的一个或多个示例性实施例。出于说明和使本领域普通技术人员能够制造、使用和实践本发明的目的,本文已经示出和描述了安全系统的实施例。然而,本领域的普通技术人员将容易理解和认识到,在不脱离本发明的精神和范围的情况下,可以对本发明进行许多变化和修改。因此,所有此类变化和修改均旨在被所附权利要求涵盖。

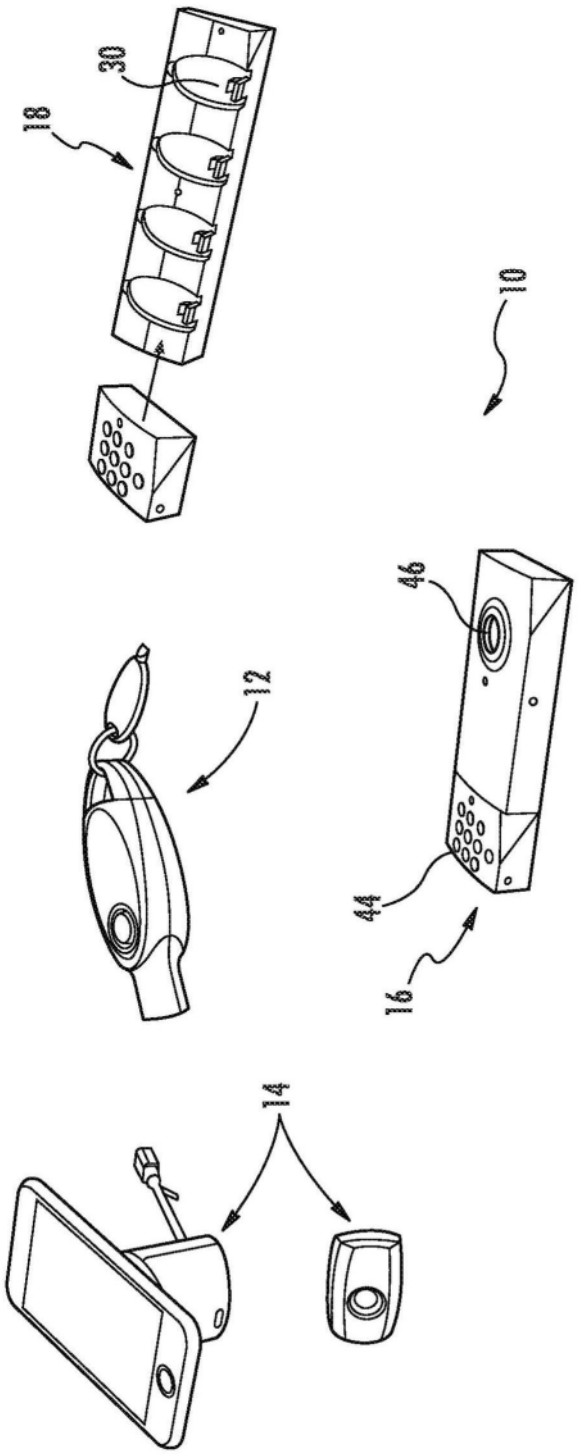


图1

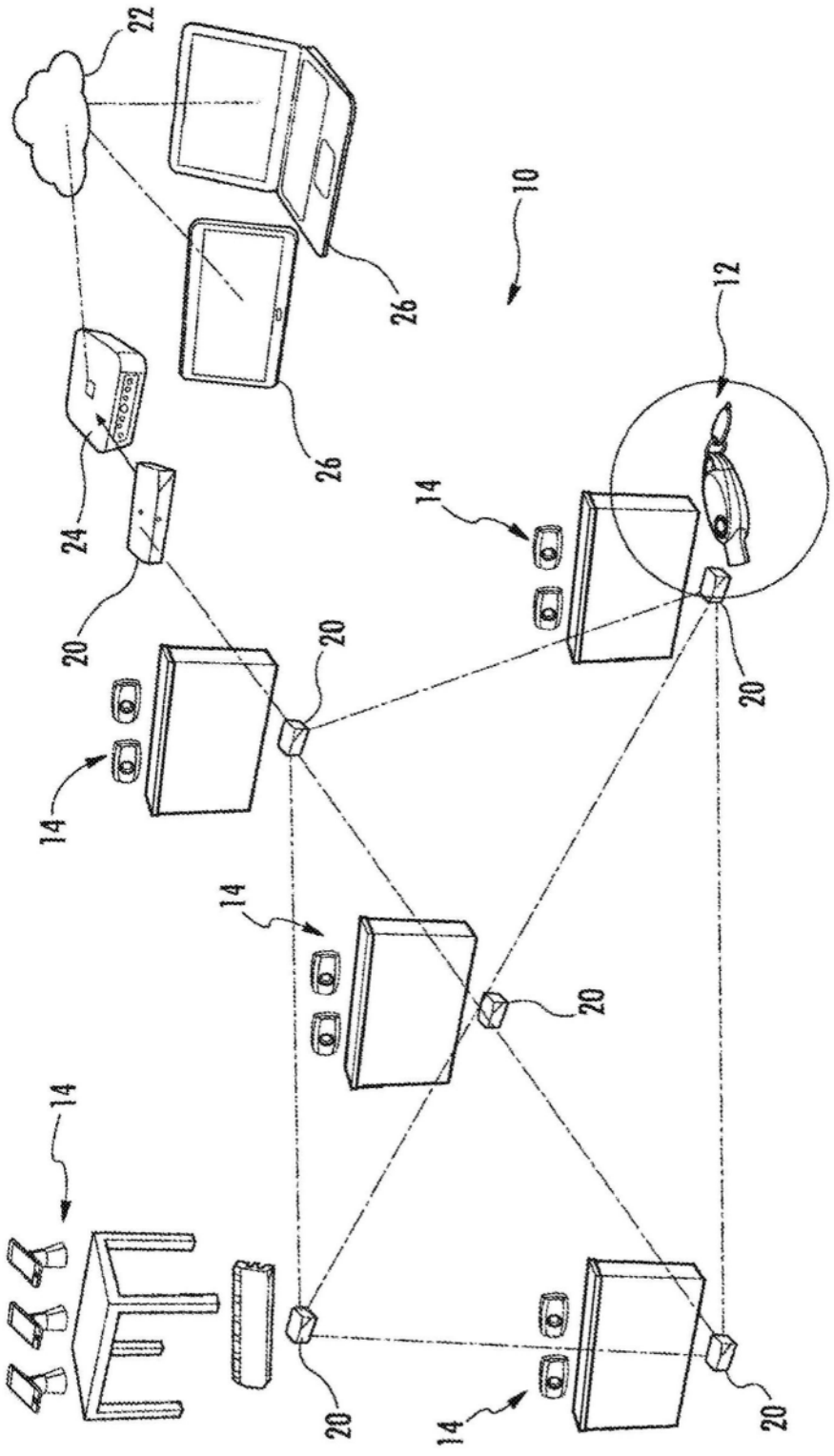


图2

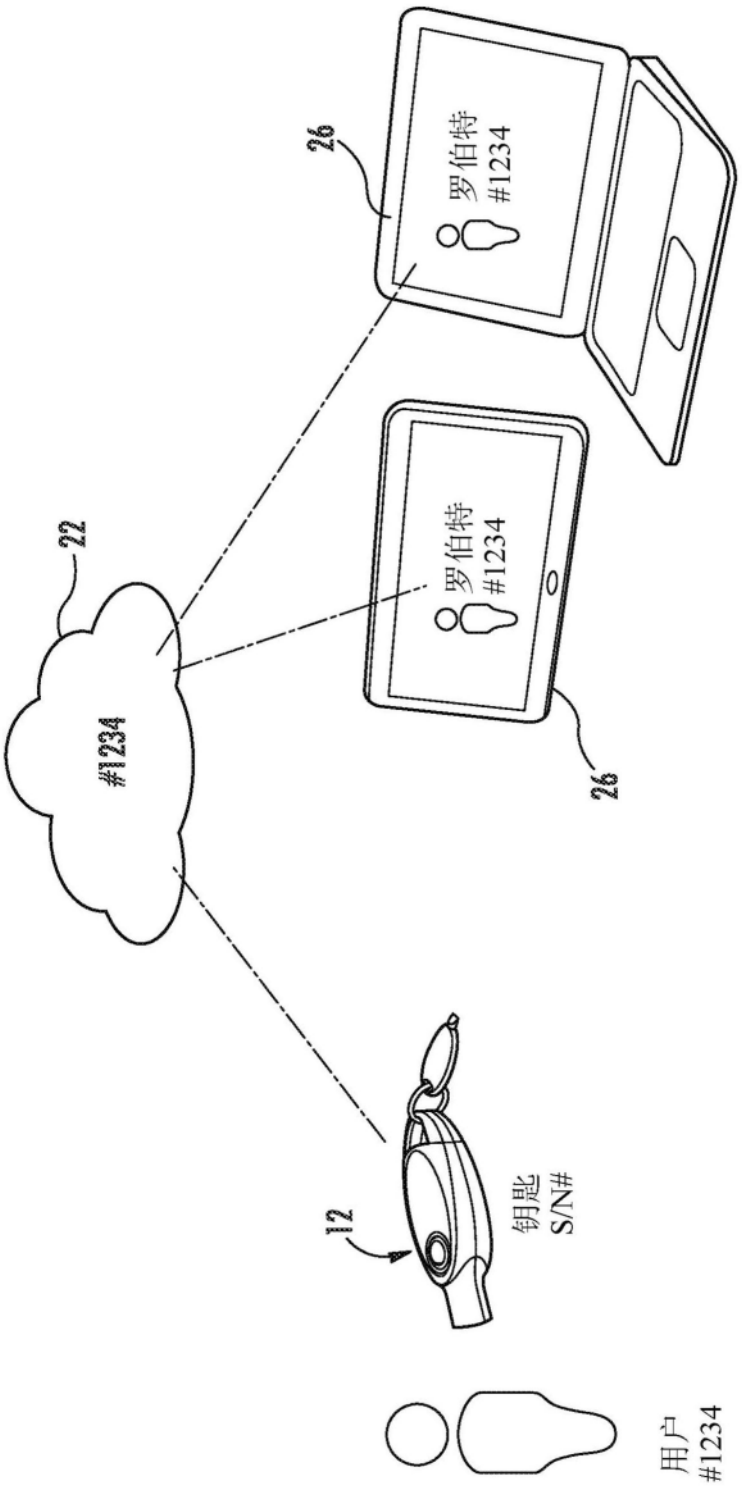


图3

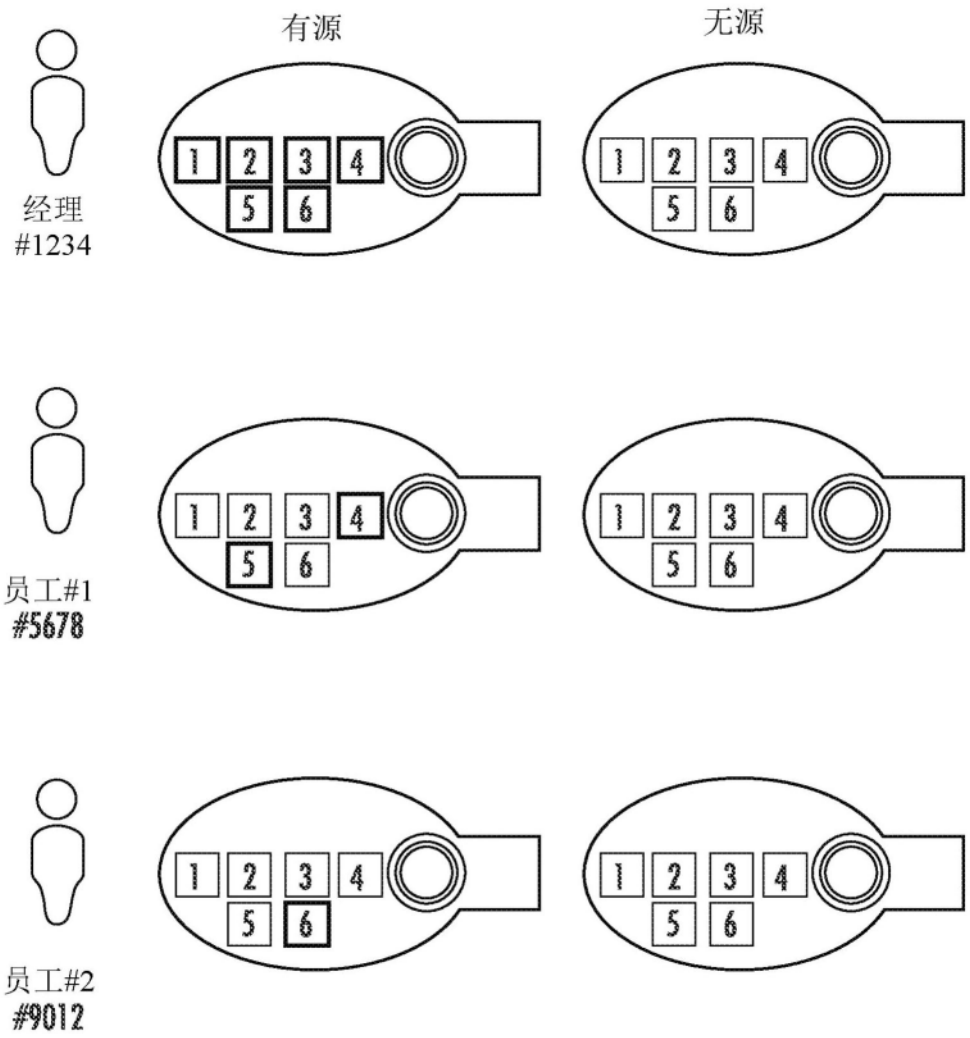


图4

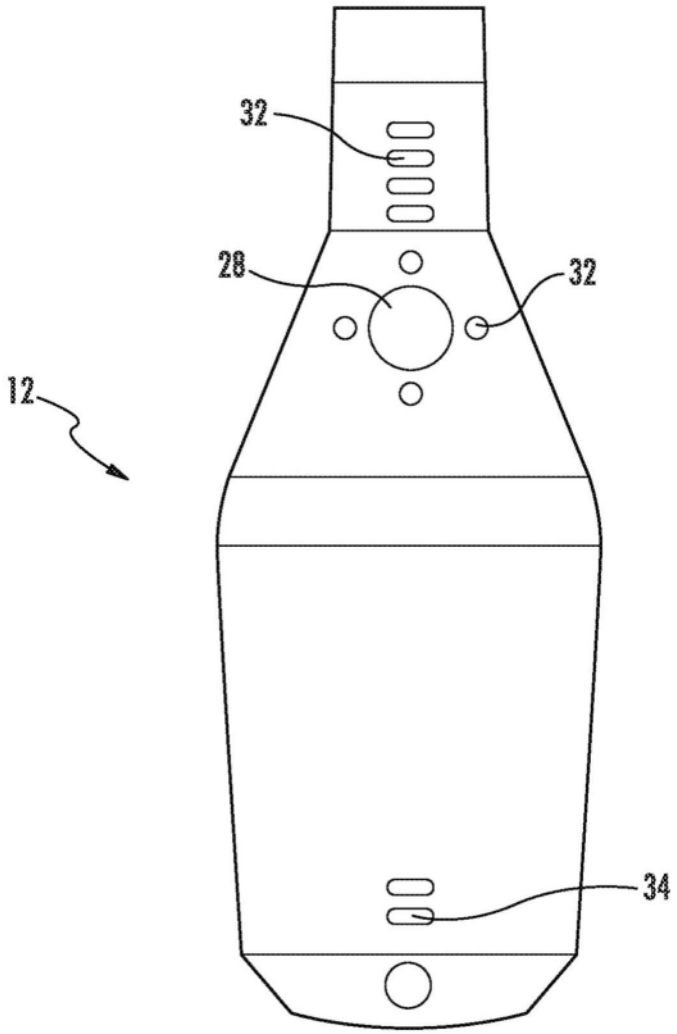


图5

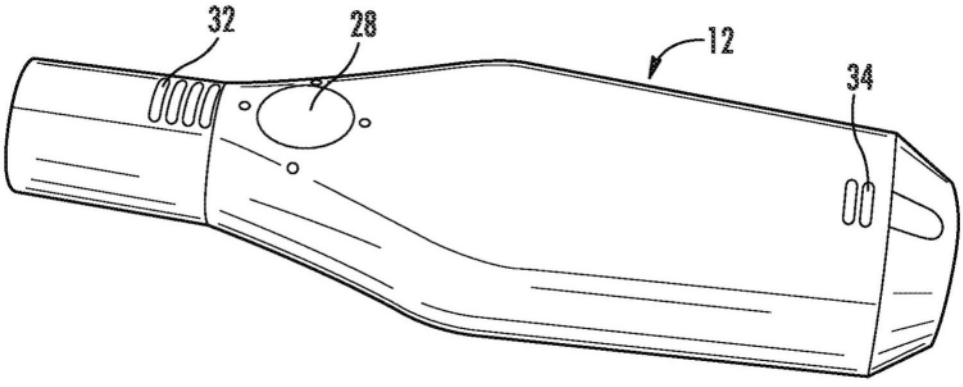


图6

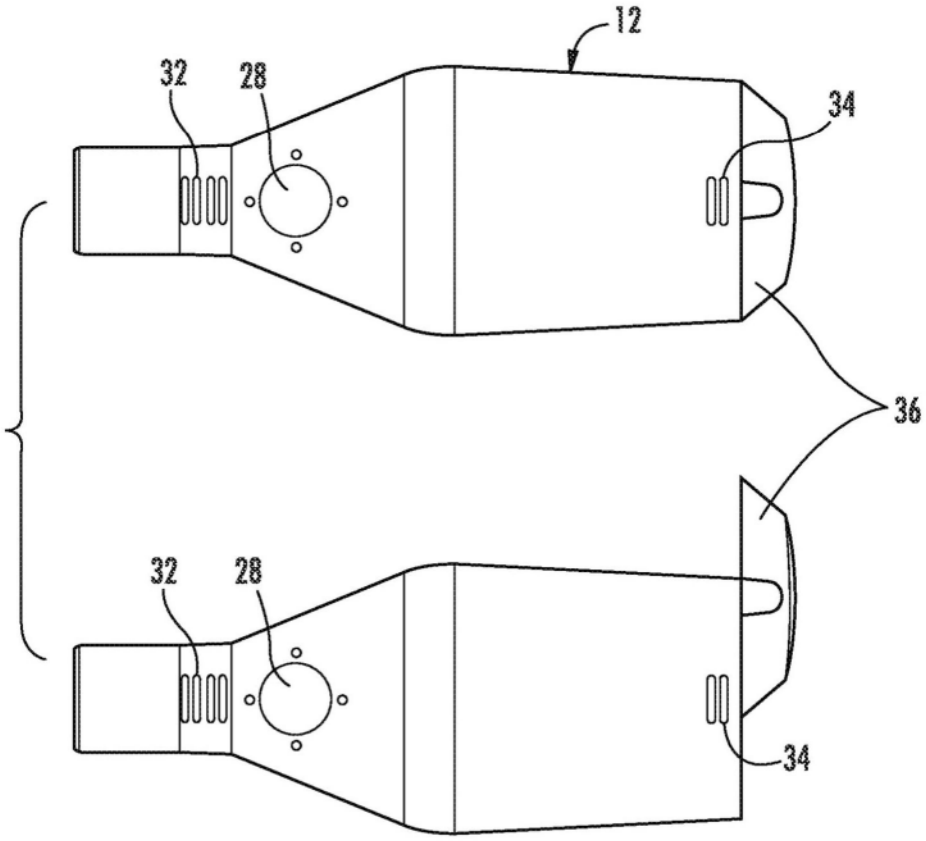


图7

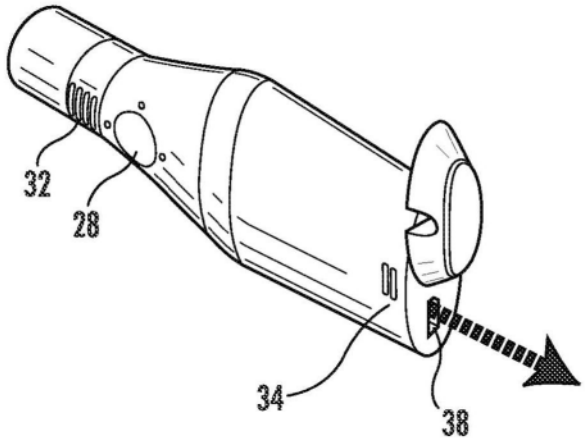


图8

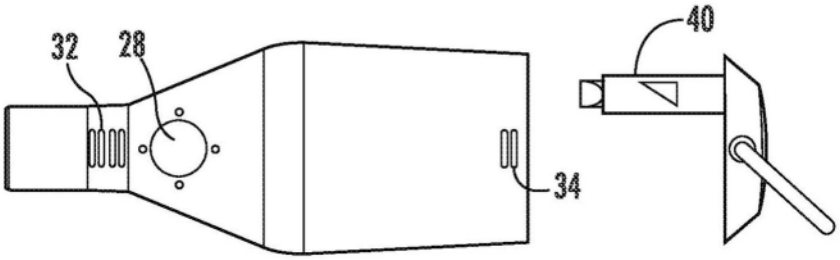


图9

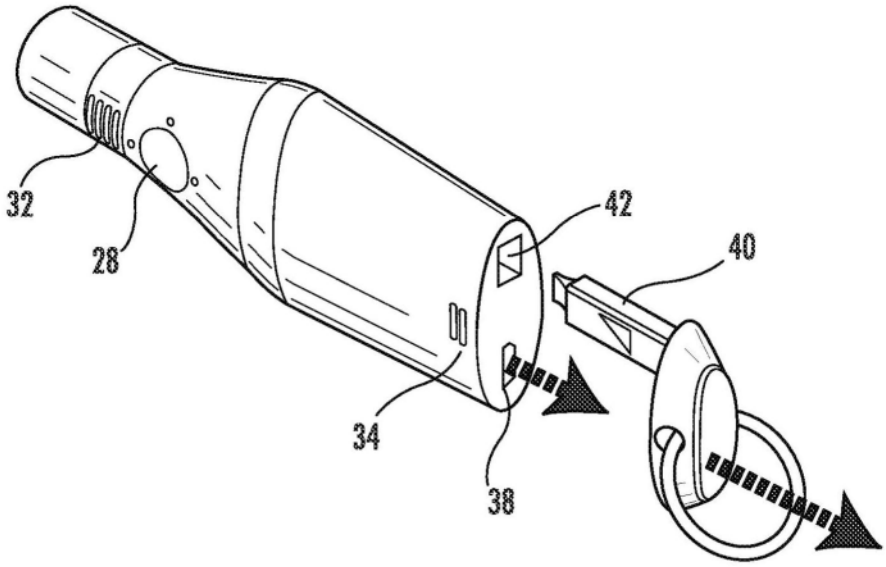


图10

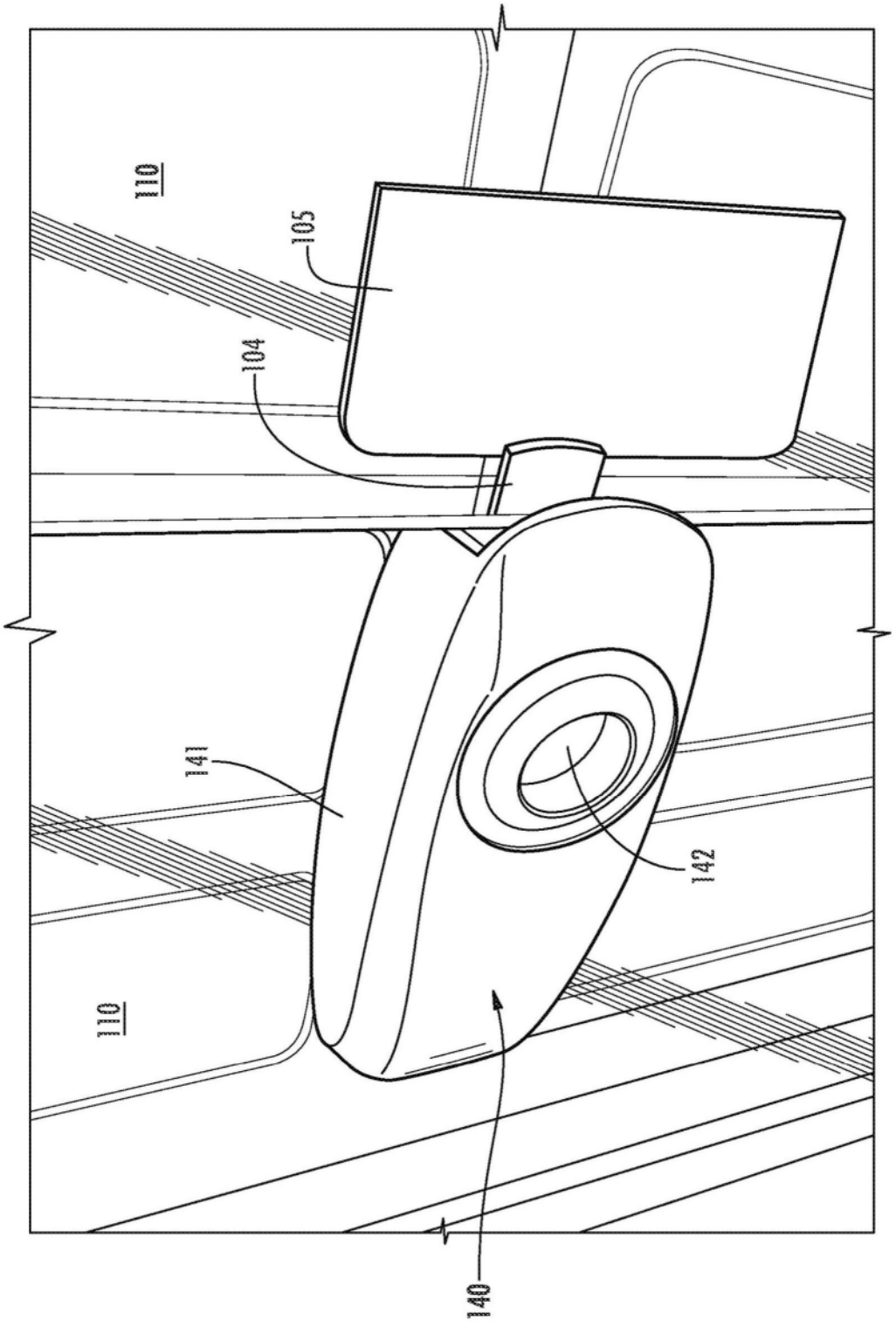


图11

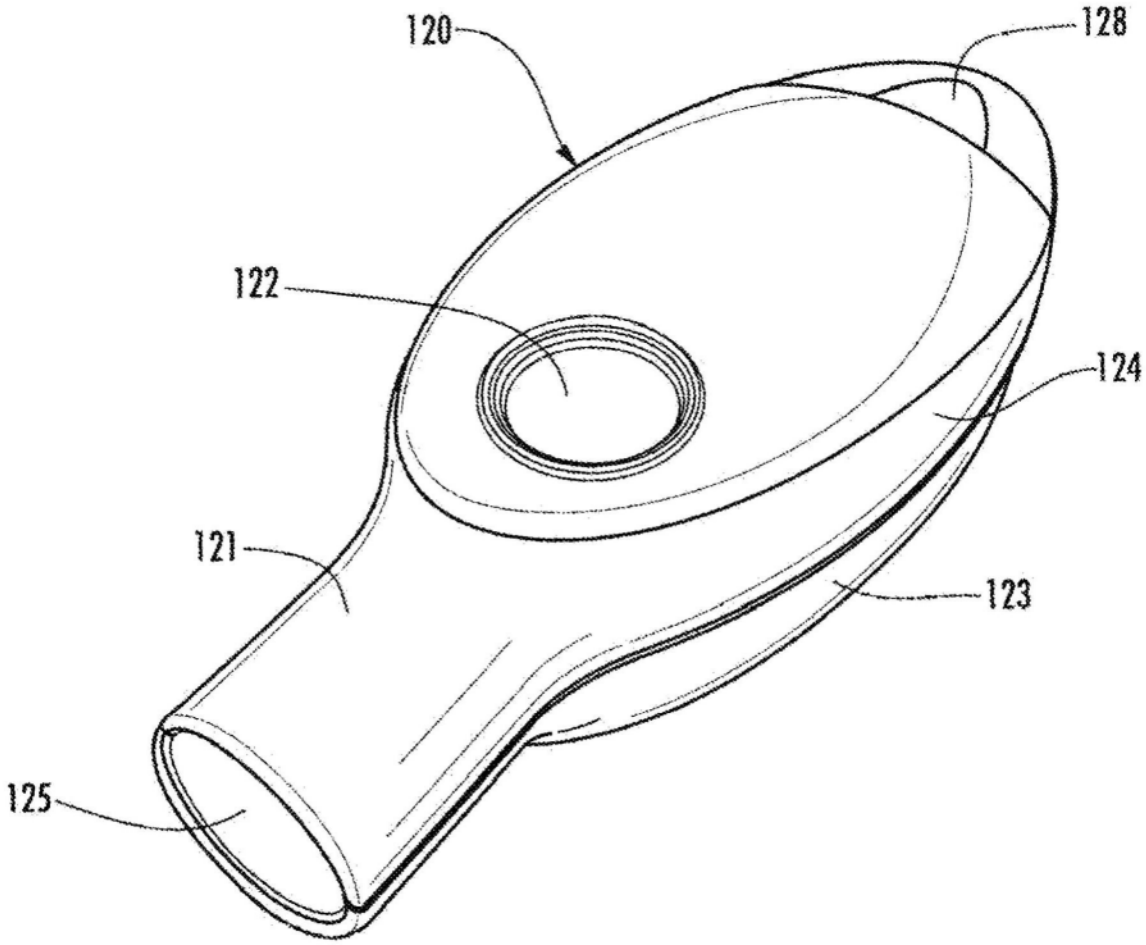


图12

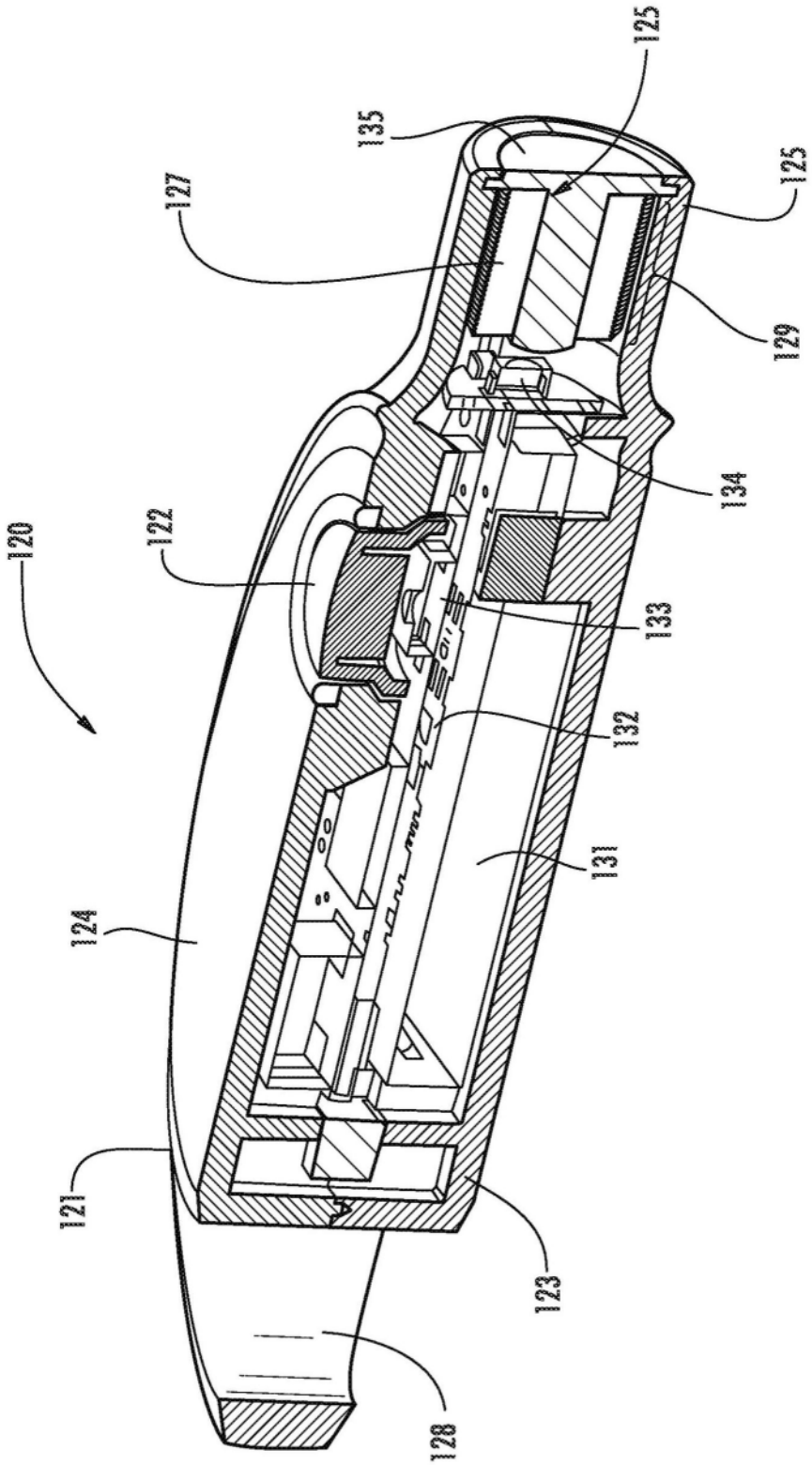


图13

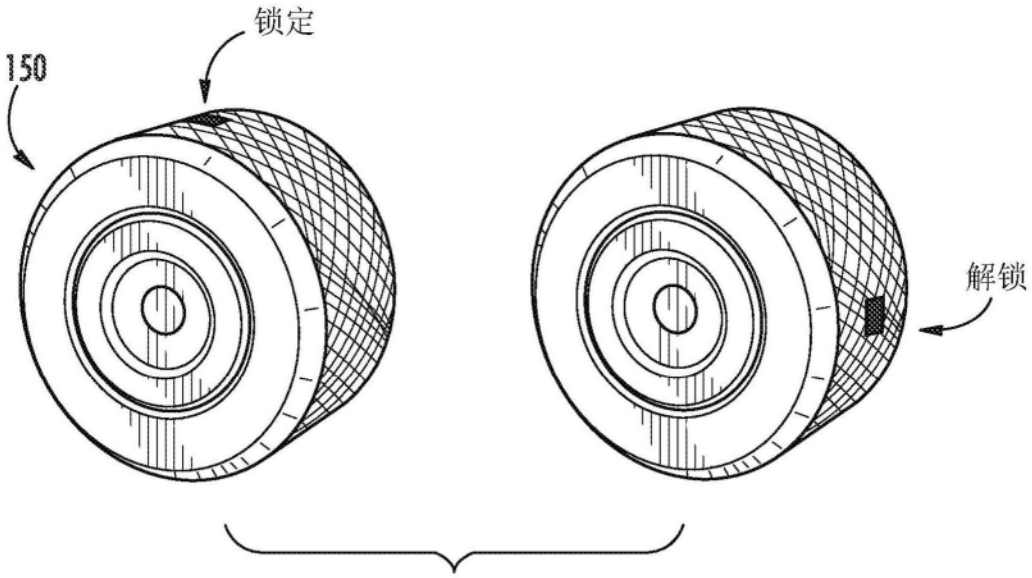


图14

图14

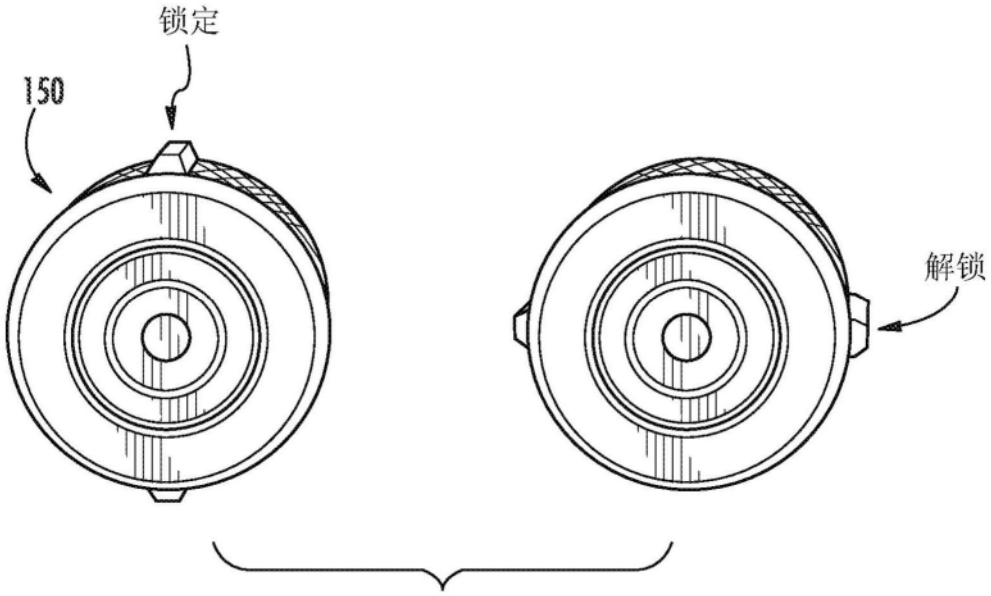


图15

图15

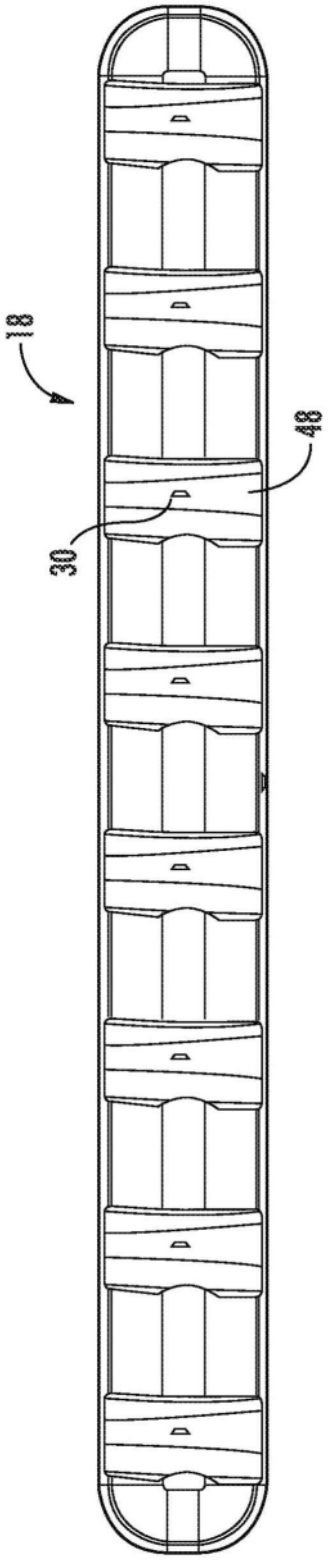


图16

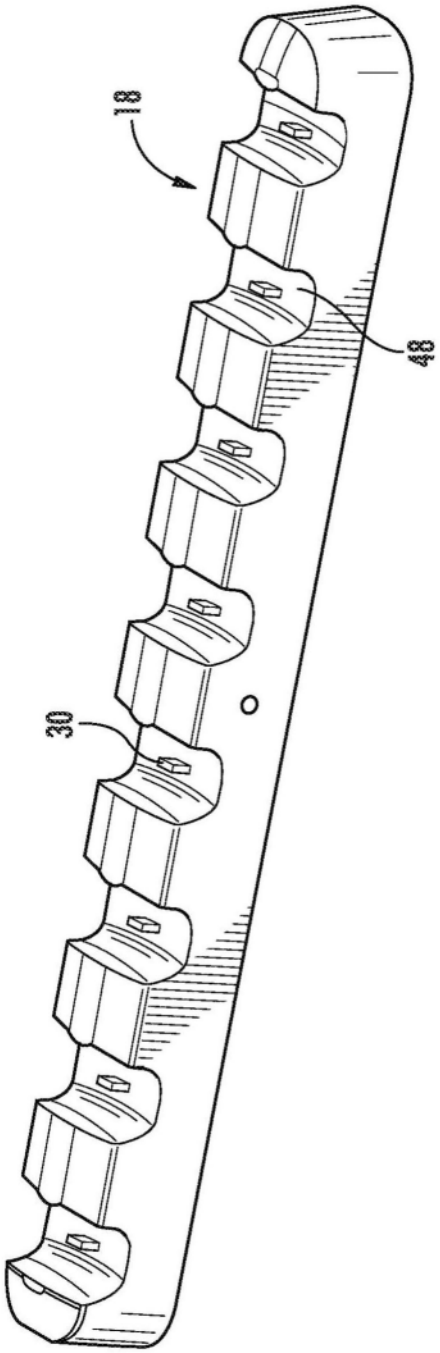


图17

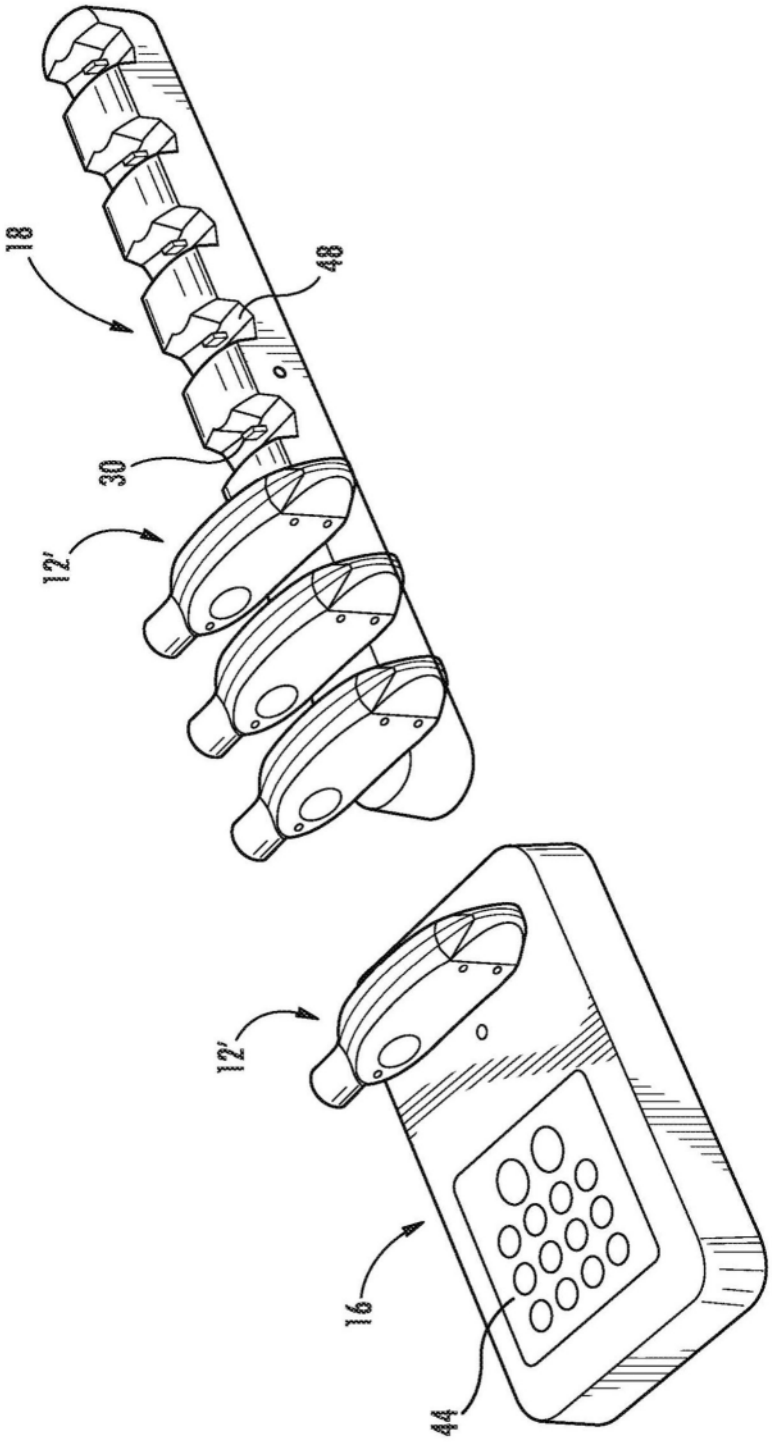


图18

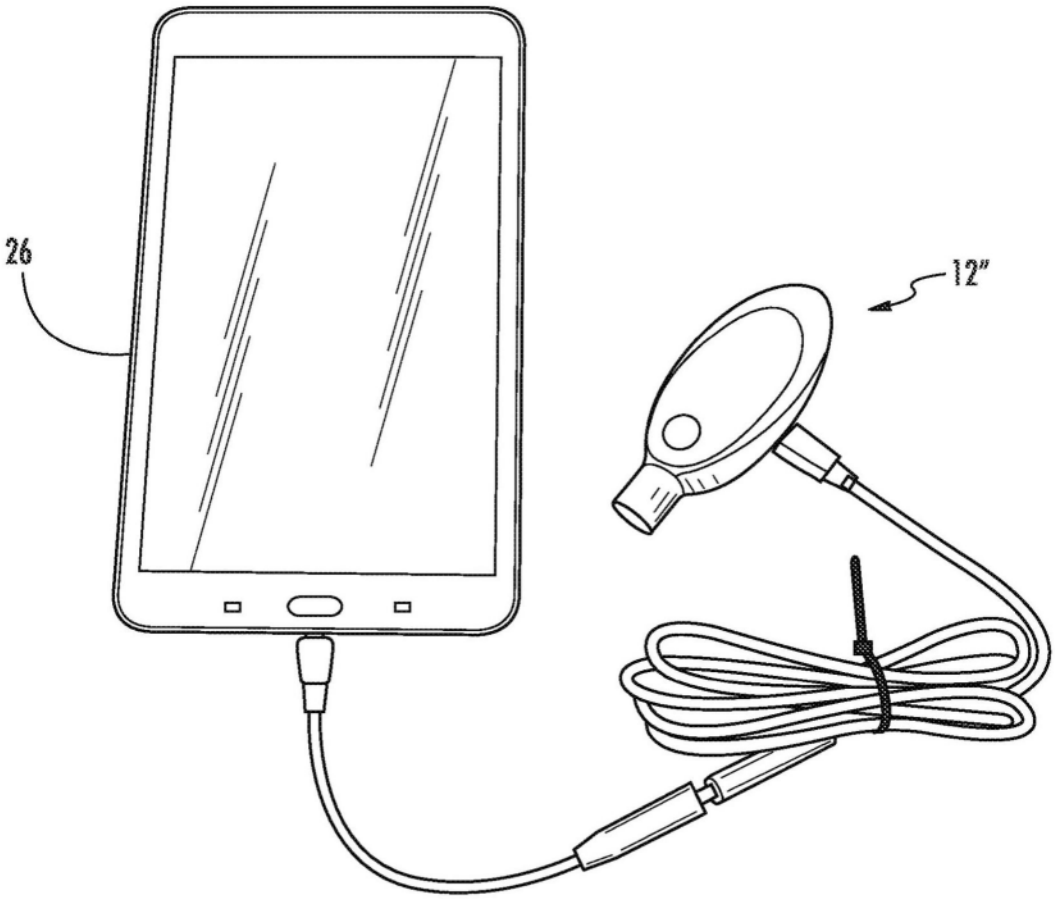


图19

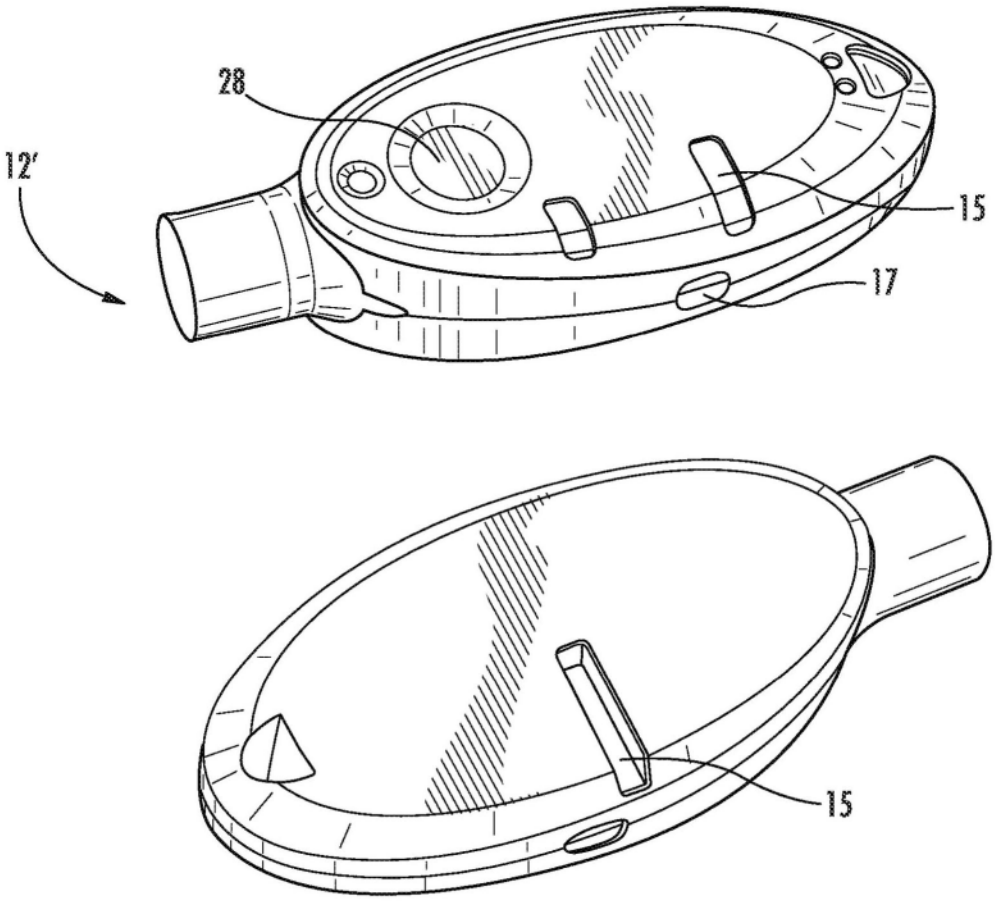


图20

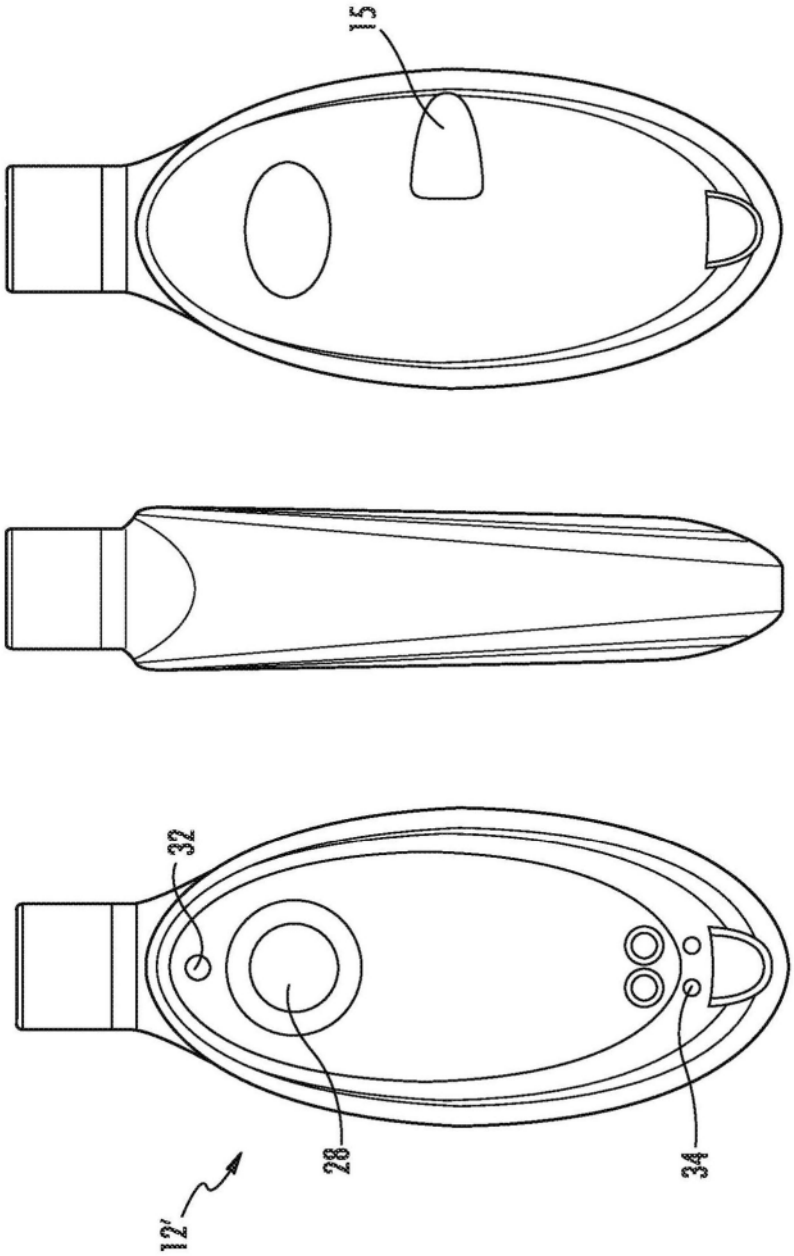


图21

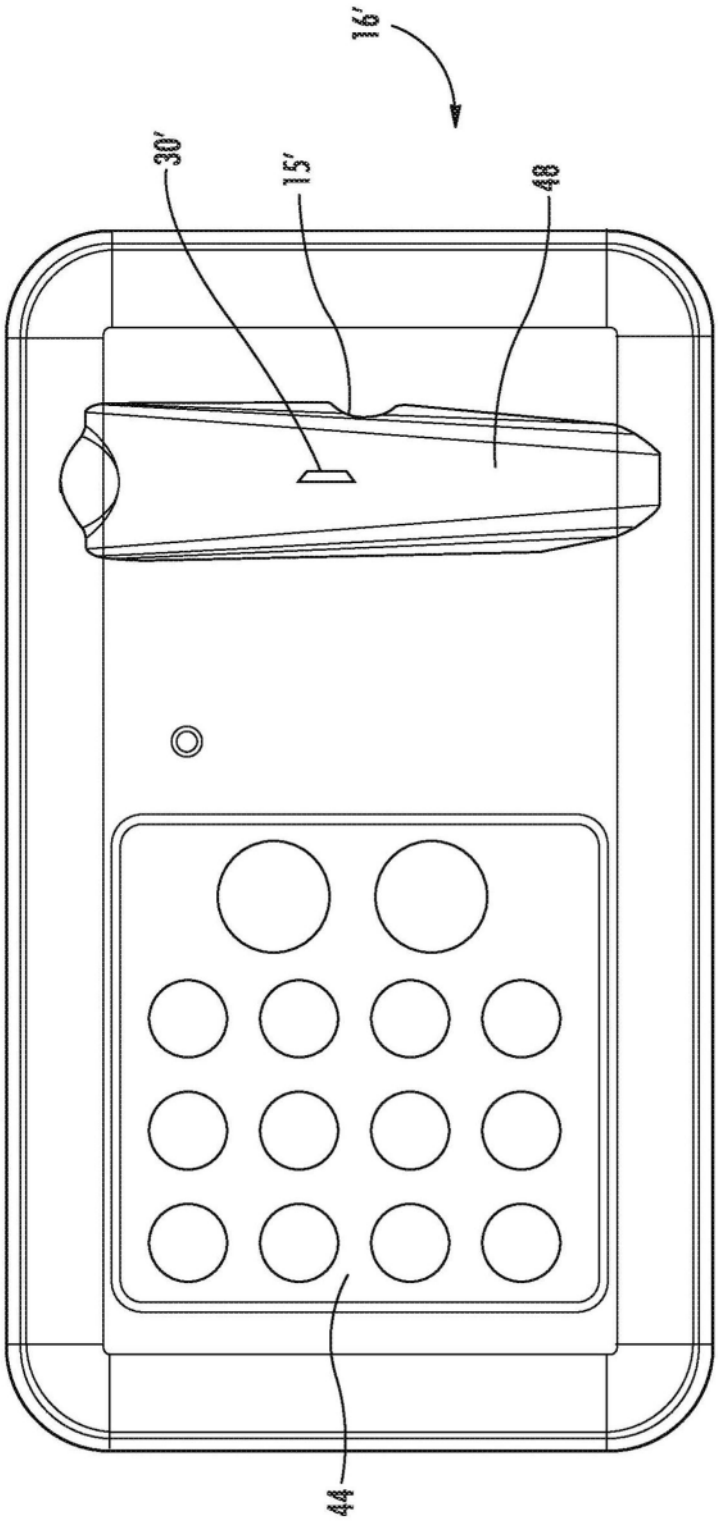


图22

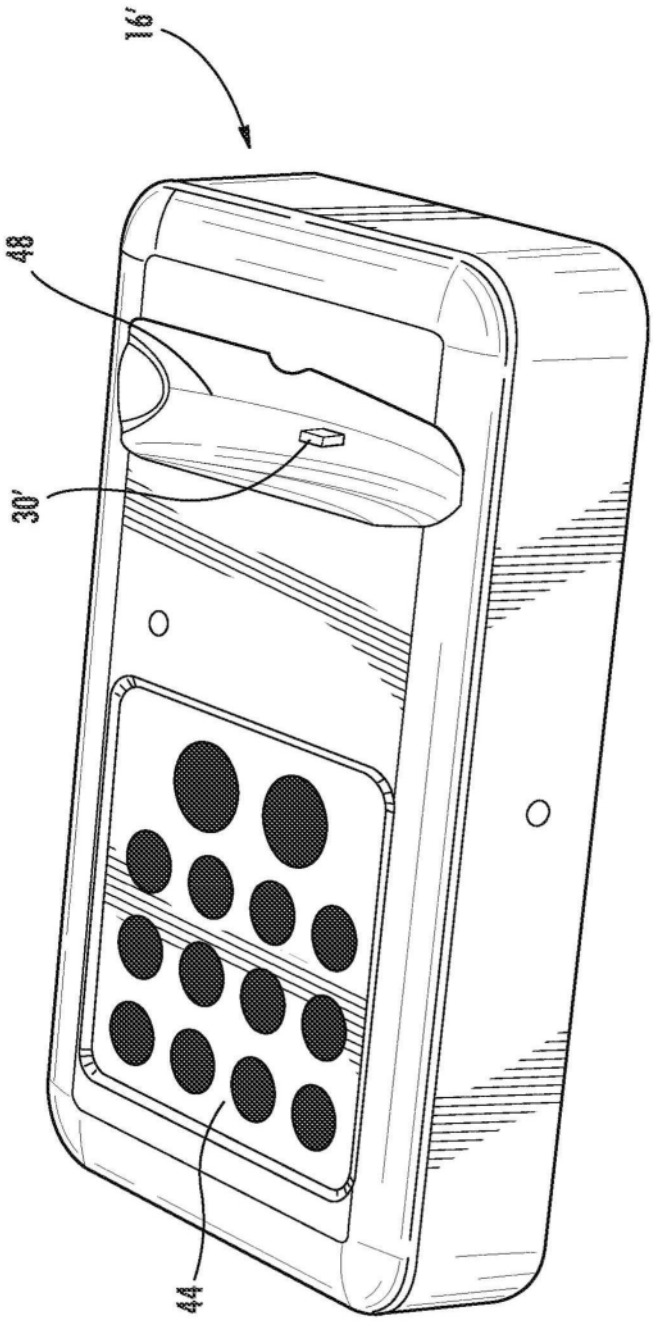


图23

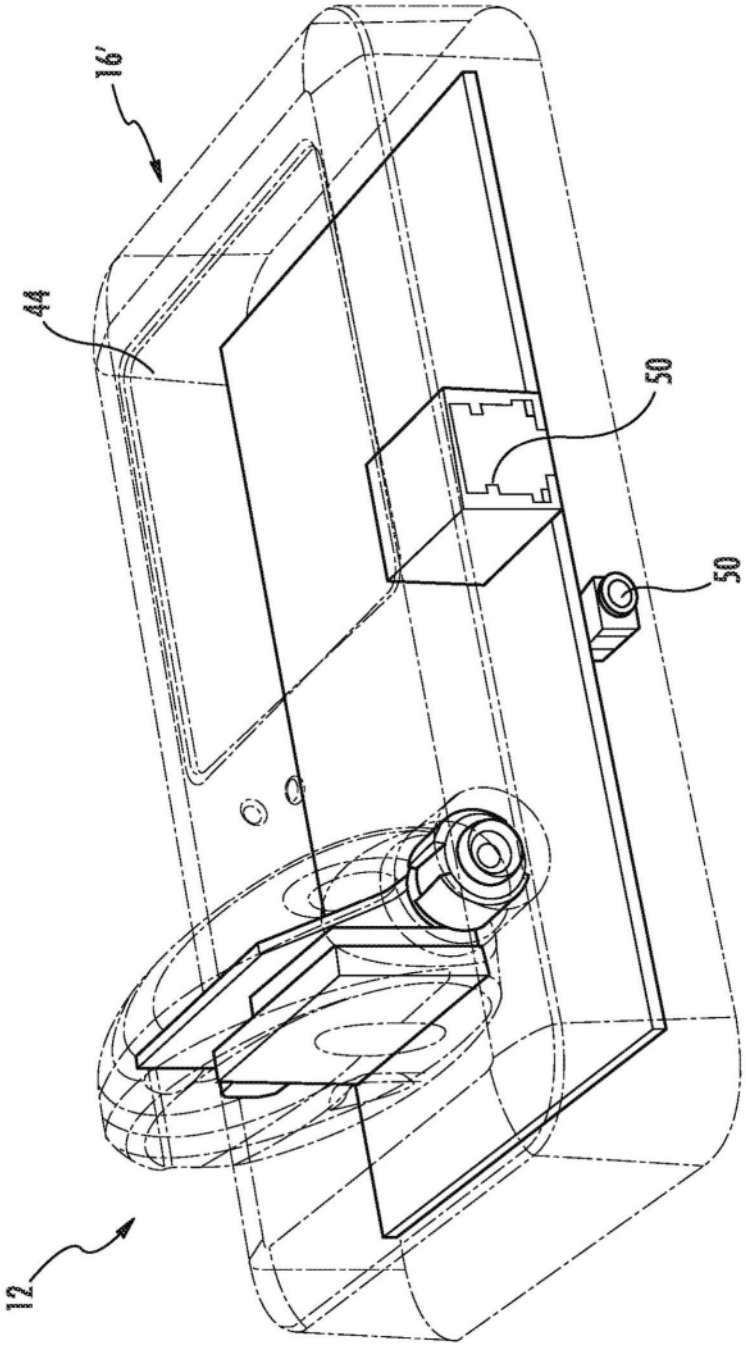


图24

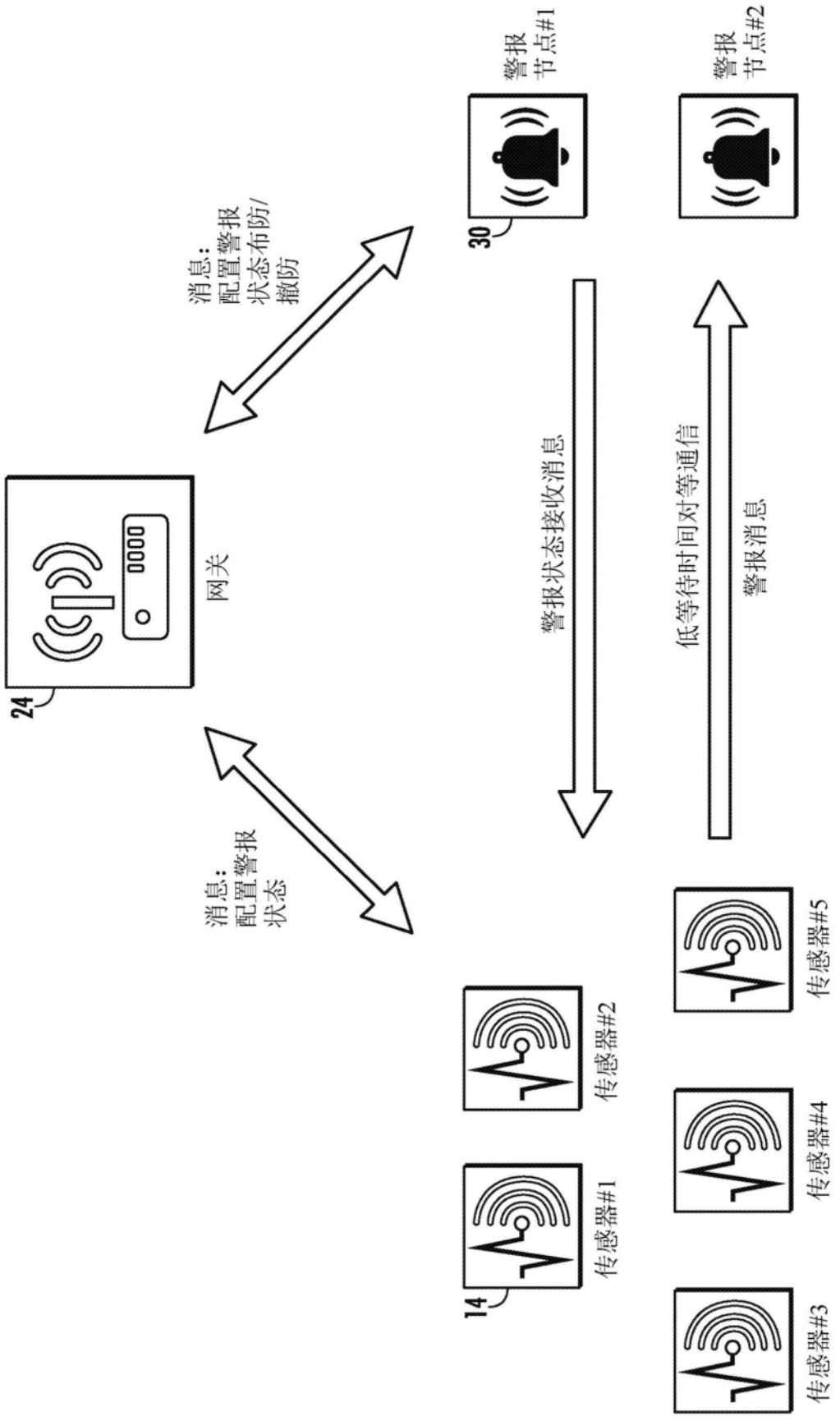

警报
节点#1
警报
节点#2
30
消息:
配置警报
状态布防/
撤防
网关
24
警报状态接收消息
低等待时间对等通信
警报消息
消息:
配置警报
状态
传感器#2
传感器#1
传感器#5
传感器#4
传感器#3
14

图25

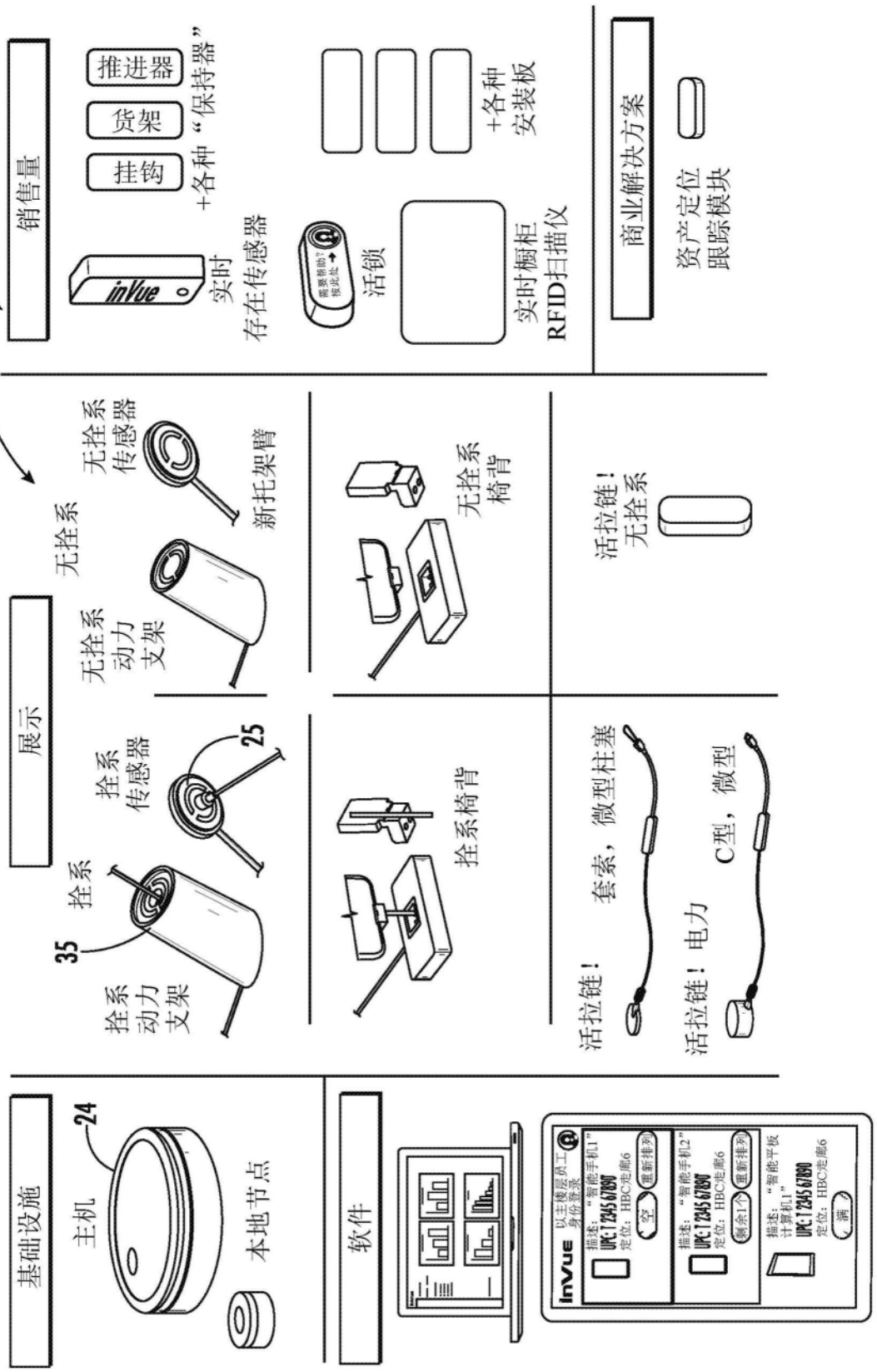

基础设施
主机
24
本地节点
软件
展示
拴系
35
拴系
动力
支架
拴系
传感器
25
拴系椅背
无拴系
无拴系
动力
支架
无拴系
传感器
新托架臂
无拴系
椅背
活拉链！
套索，微型柱塞
活拉链！电力
C型，微型
销售量
14
inVue
实时
存在传感器
挂钩
袋架
推进器
+各种“保持器”
活锁
实时橱柜
RFID扫描仪
+各种
安装板
商业解决方案
资产定位
跟踪模块

图26

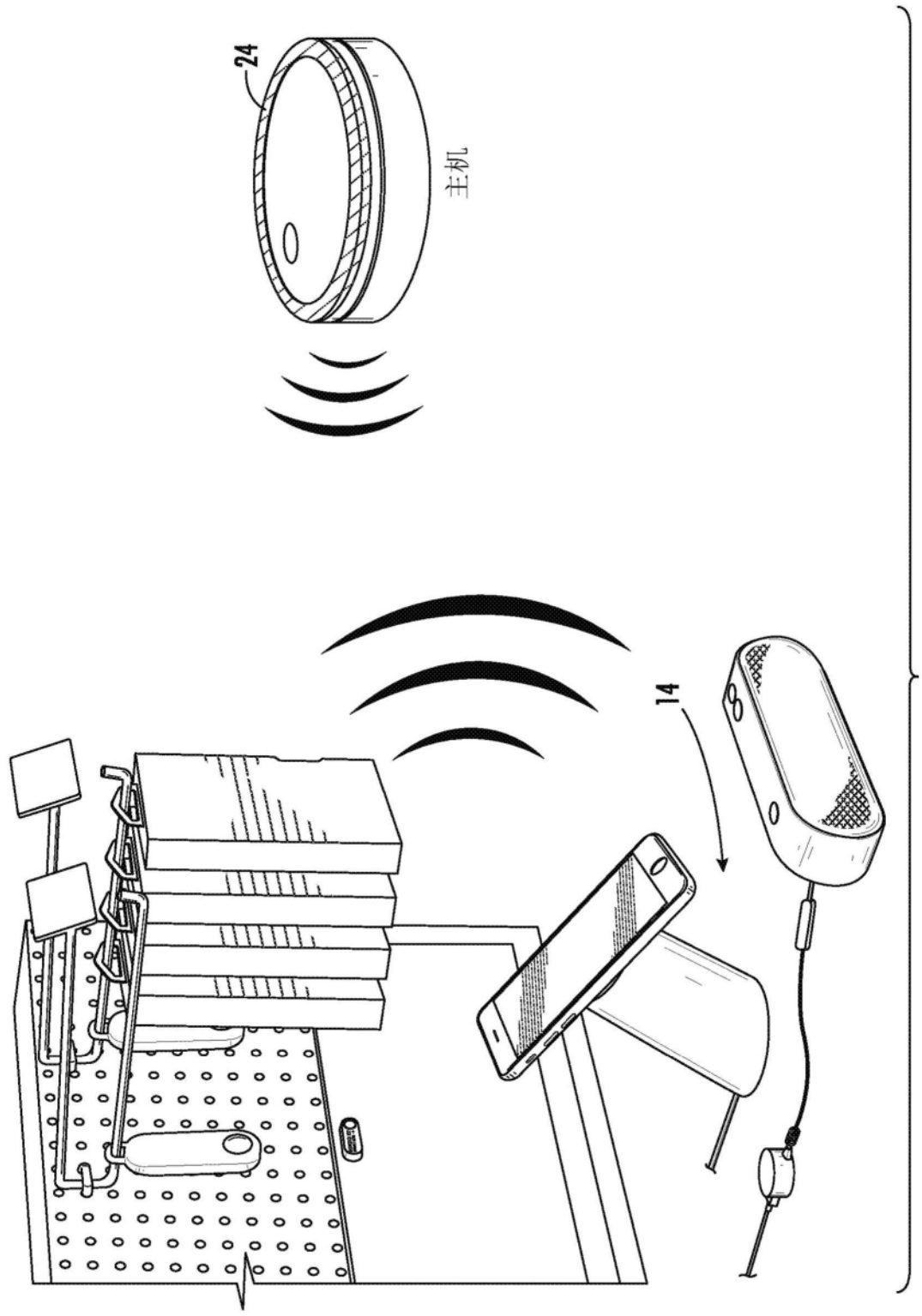


图27

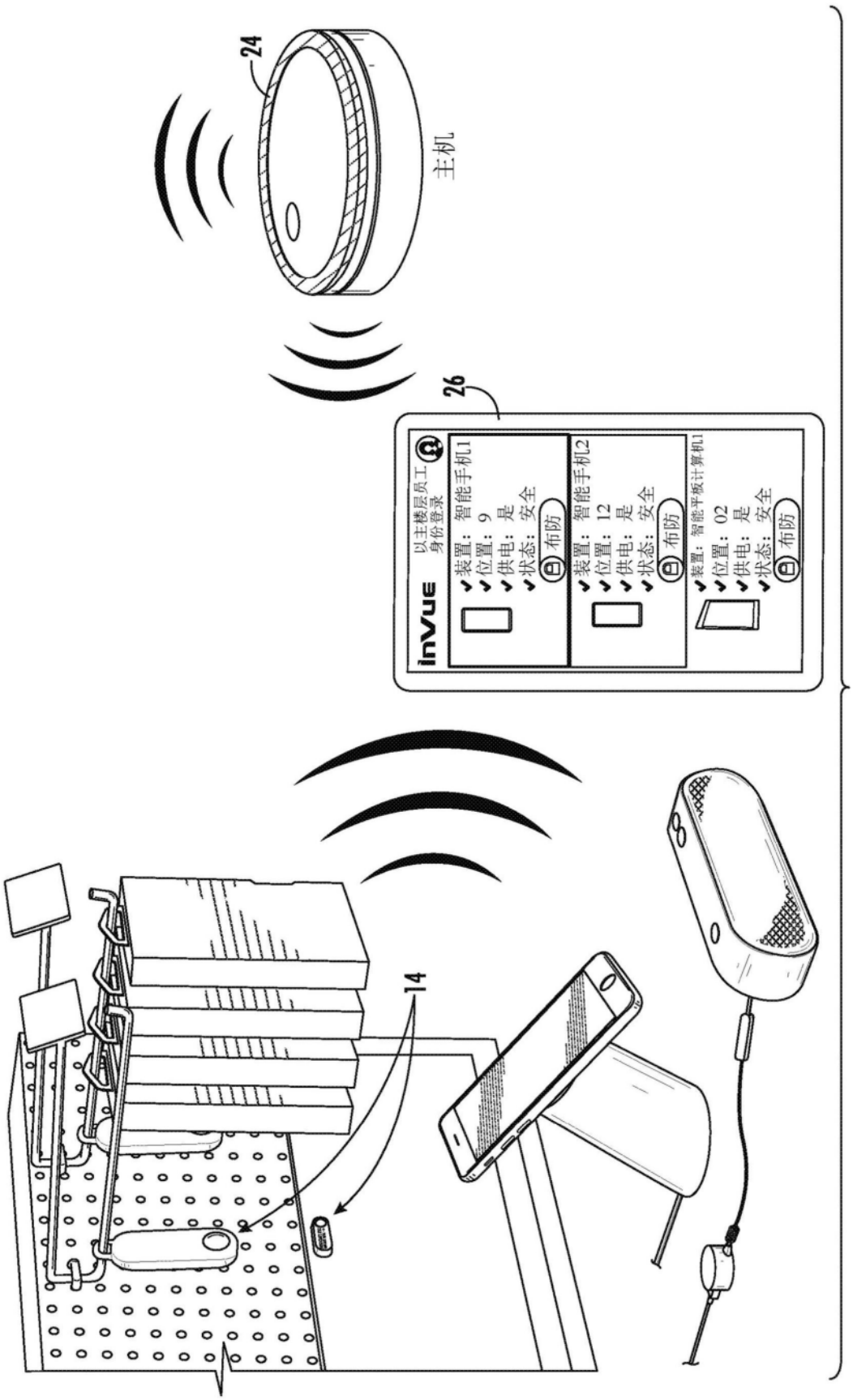

24
主机
26
inVue
以主楼层员工
身份登录
装置：智能手机1
位置：9
供电：是
状态：安全
布防
装置：智能手机2
位置：12
供电：是
状态：安全
布防
装置：智能平板计算机1
位置：02
供电：是
状态：安全
布防
14

图28

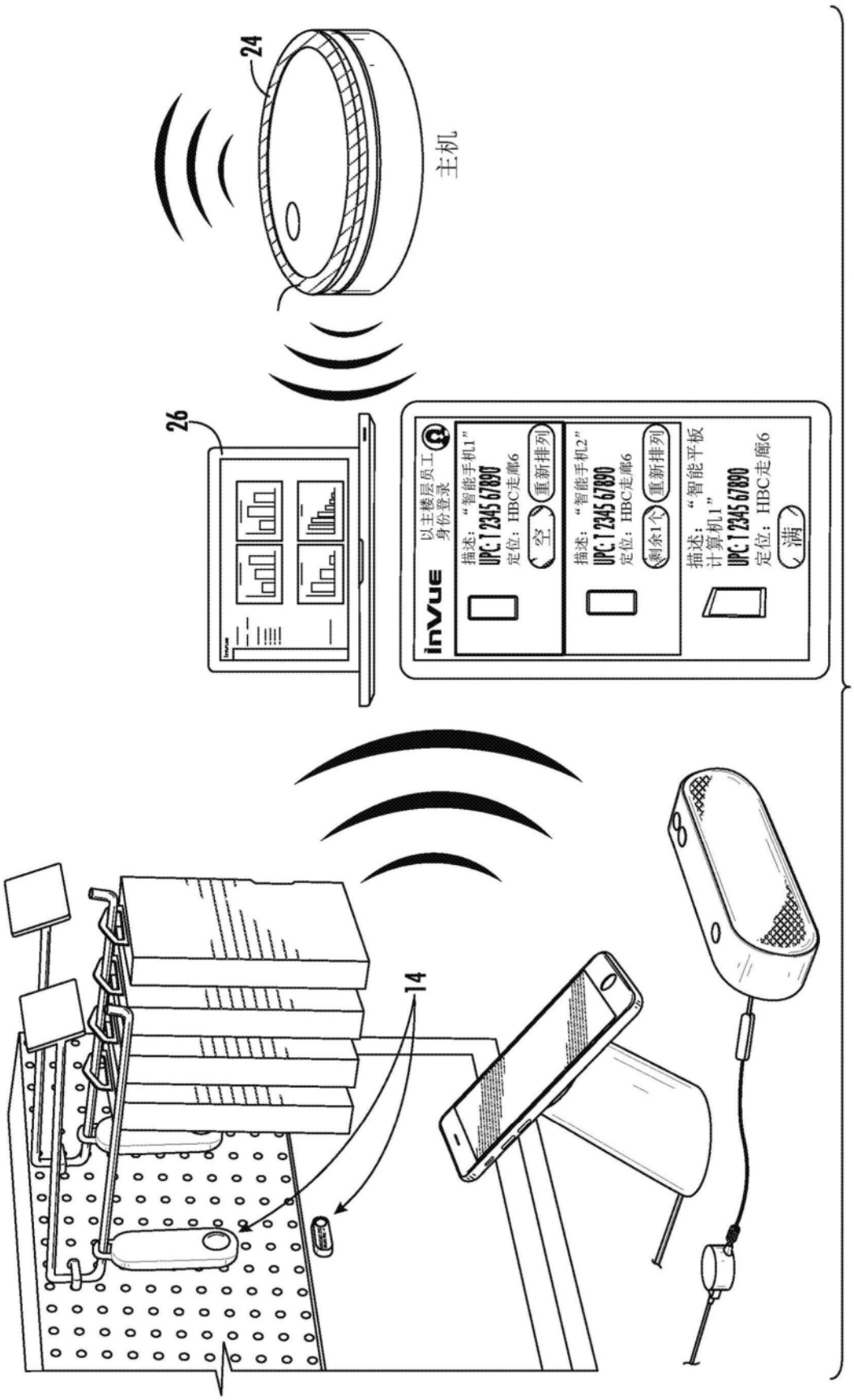

24
主机
26
inVue
以主楼层员工身份登录
描述：“智能手机1”
UPC:1 2345 67890
定位：HBC走廊6
空
重新排列
描述：“智能手机2”
UPC:1 2345 67890
定位：HBC走廊6
剩余1个
重新排列
描述：“智能平板计算机1”
UPC:1 2345 67890
定位：HBC走廊6
满
14

图29

图29

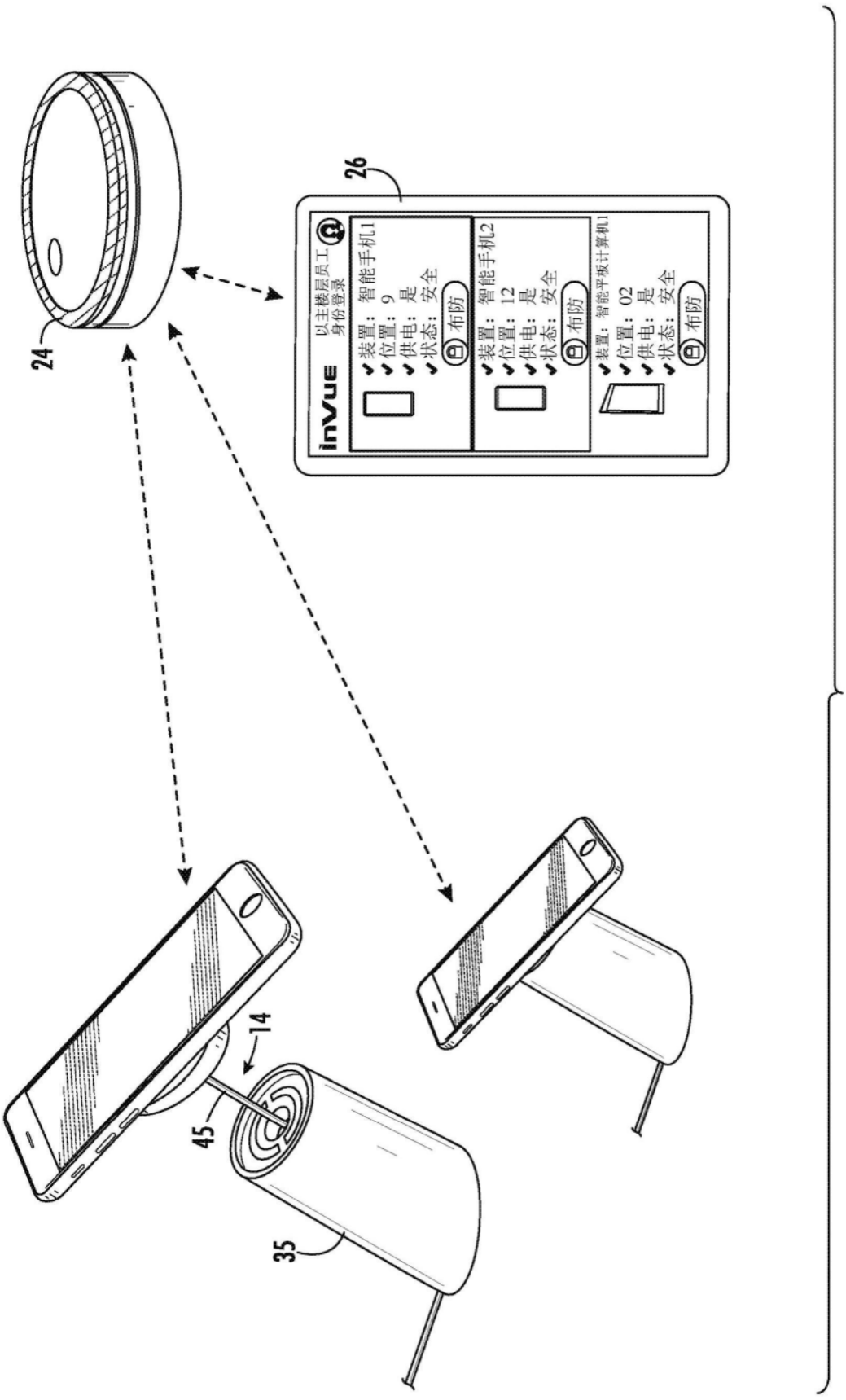

24
26
inVue
以主楼层员工身份登录
装置：智能手机1
位置：9
供电：是
状态：安全
布防
装置：智能手机2
位置：12
供电：是
状态：安全
布防
装置：智能平板计算机1
位置：02
供电：是
状态：安全
布防
14
45
35

图30

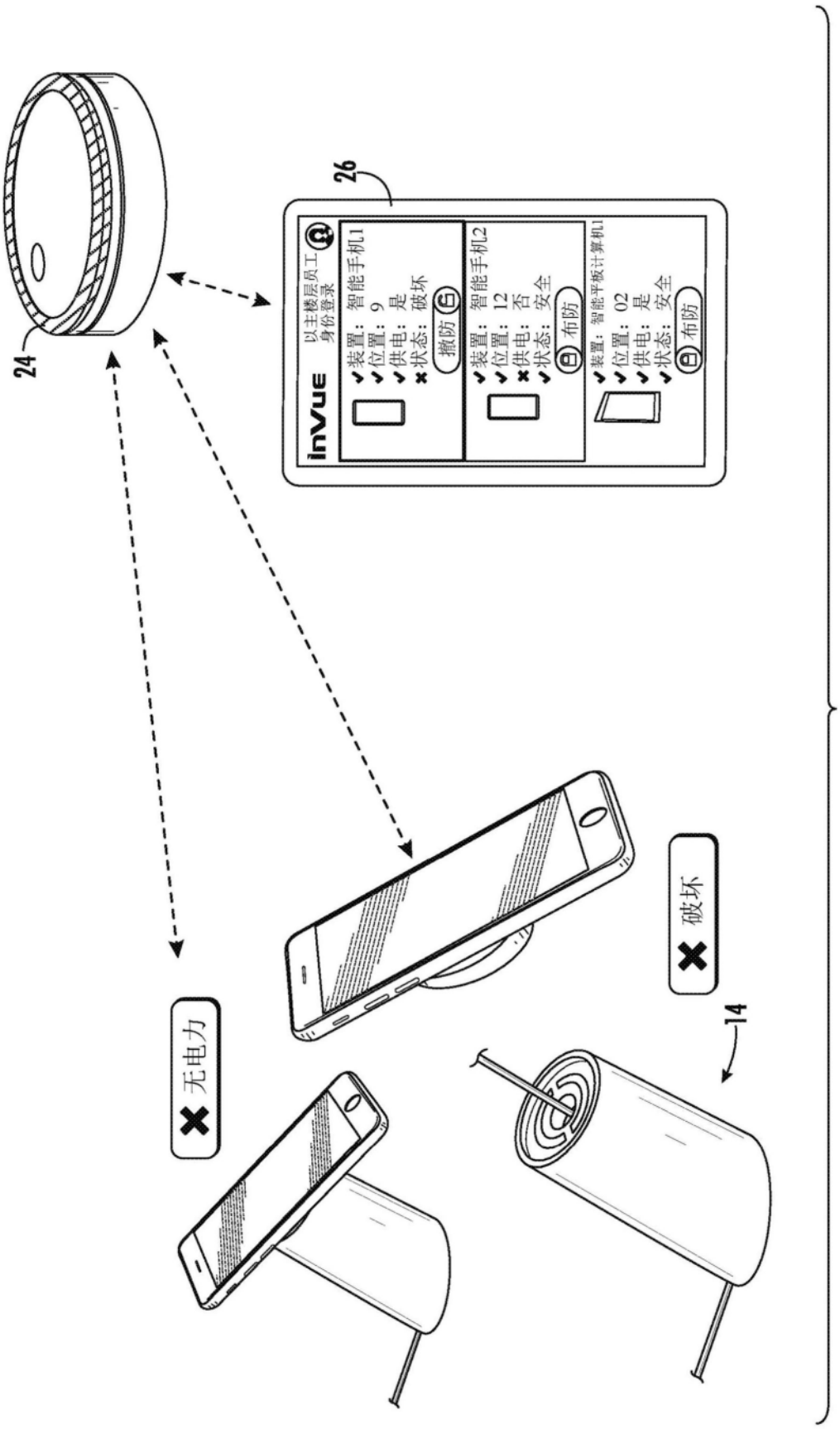

24
26
inVue
以主楼层员工
身份登录
装置：智能手机1
位置：9
供电：是
状态：破坏
撤防
装置：智能手机2
位置：12
供电：否
状态：安全
布防
装置：智能平板计算机1
位置：02
供电：是
状态：安全
布防
无电力
破坏
14

图31

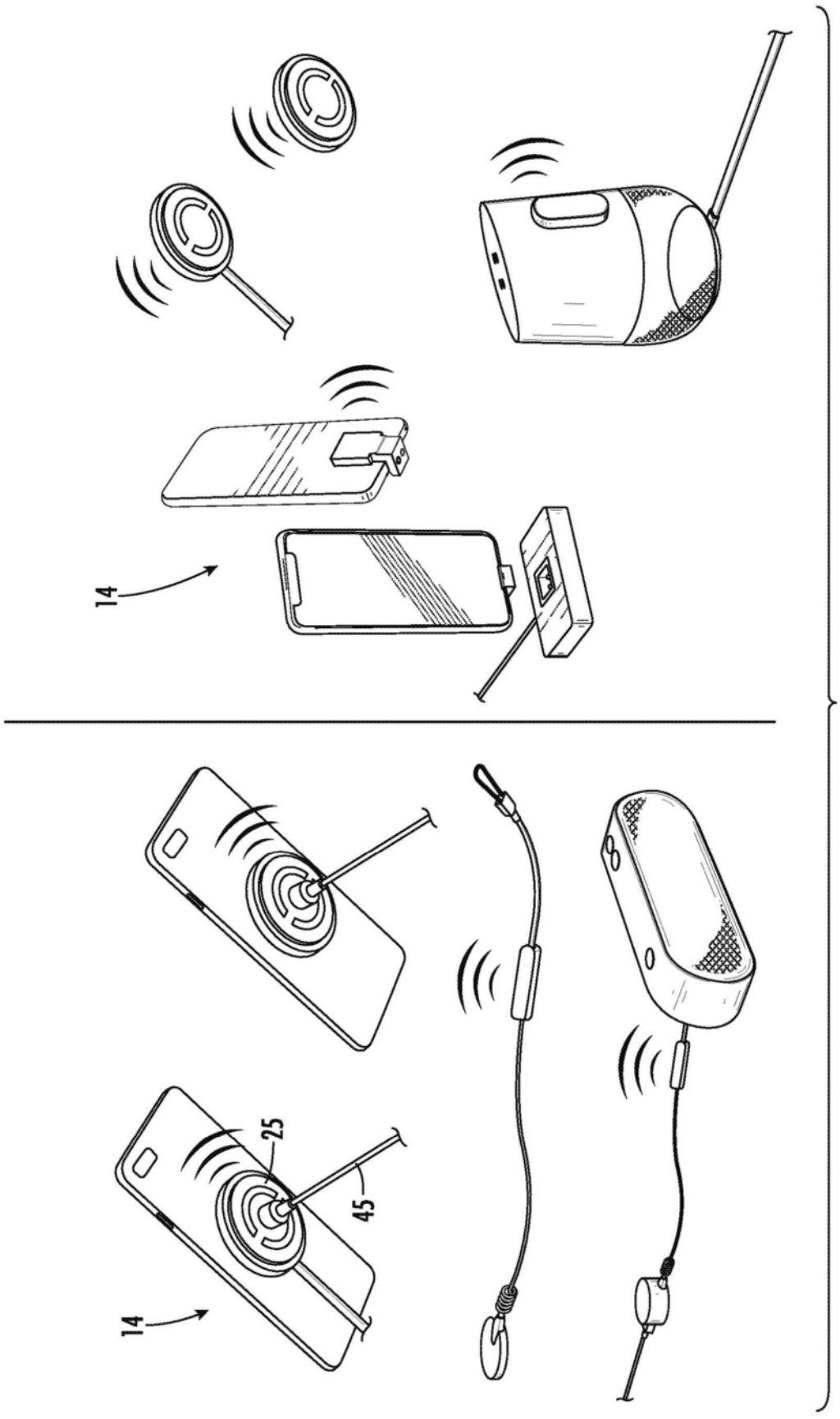


图32

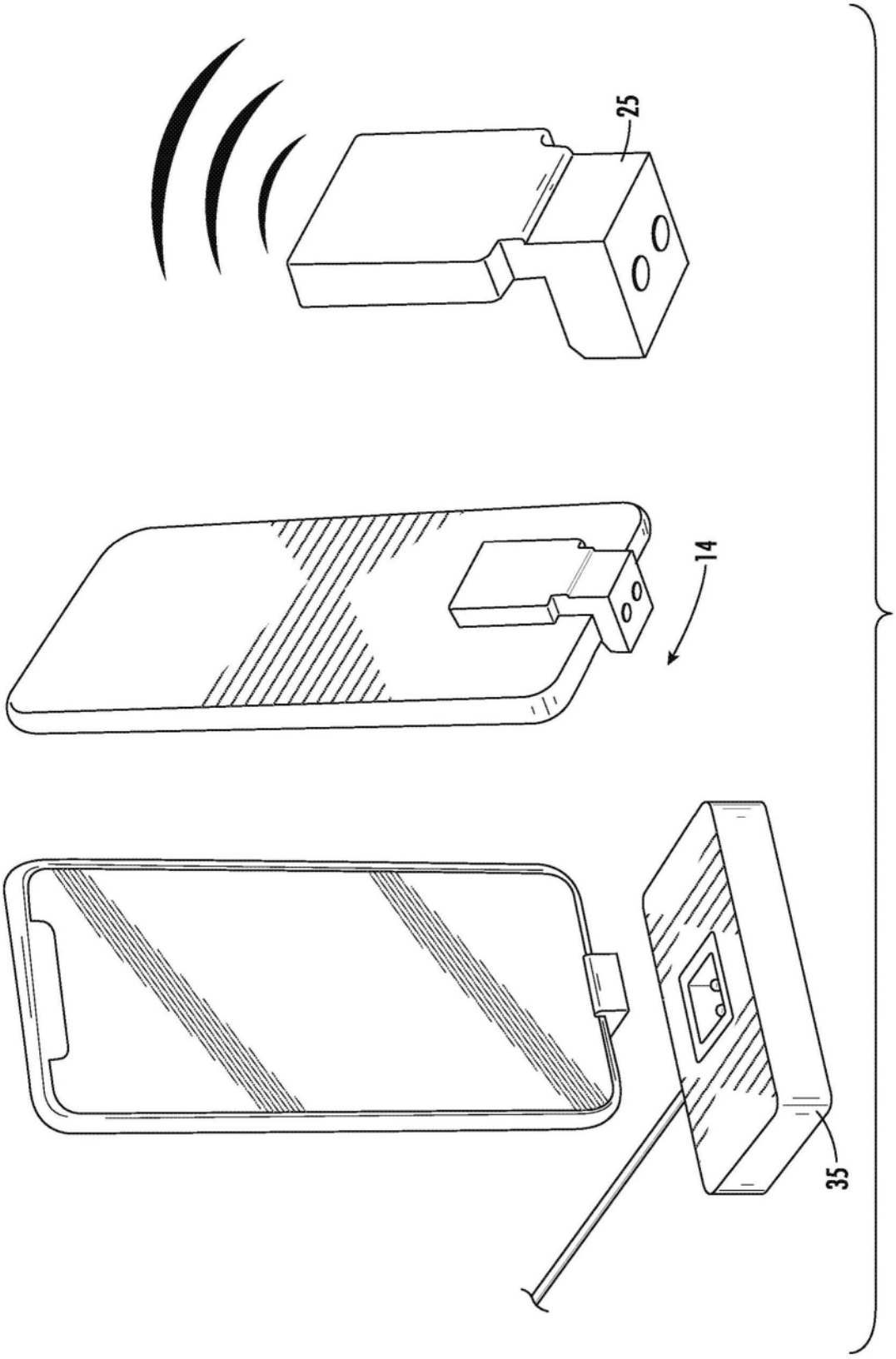


图33

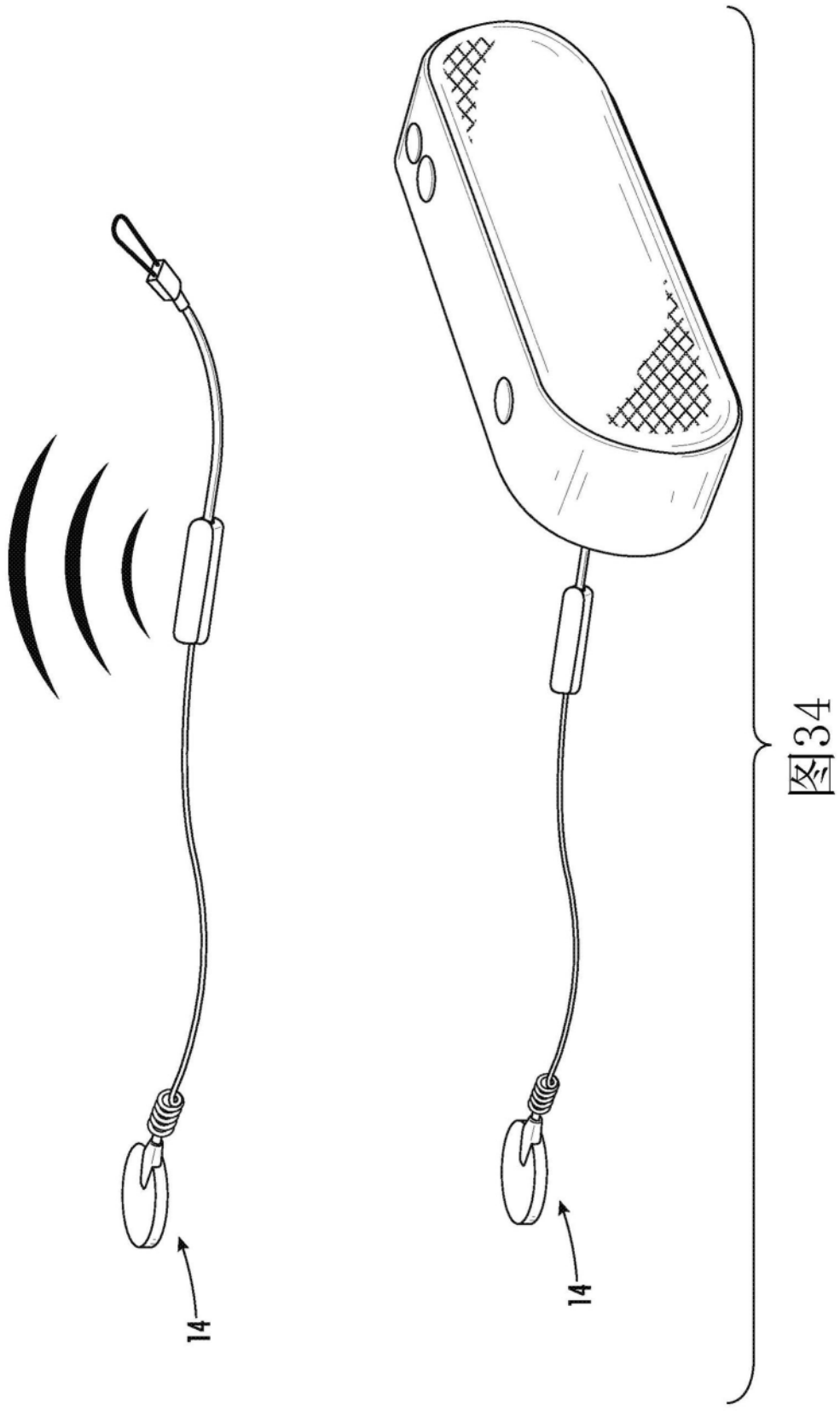


图34

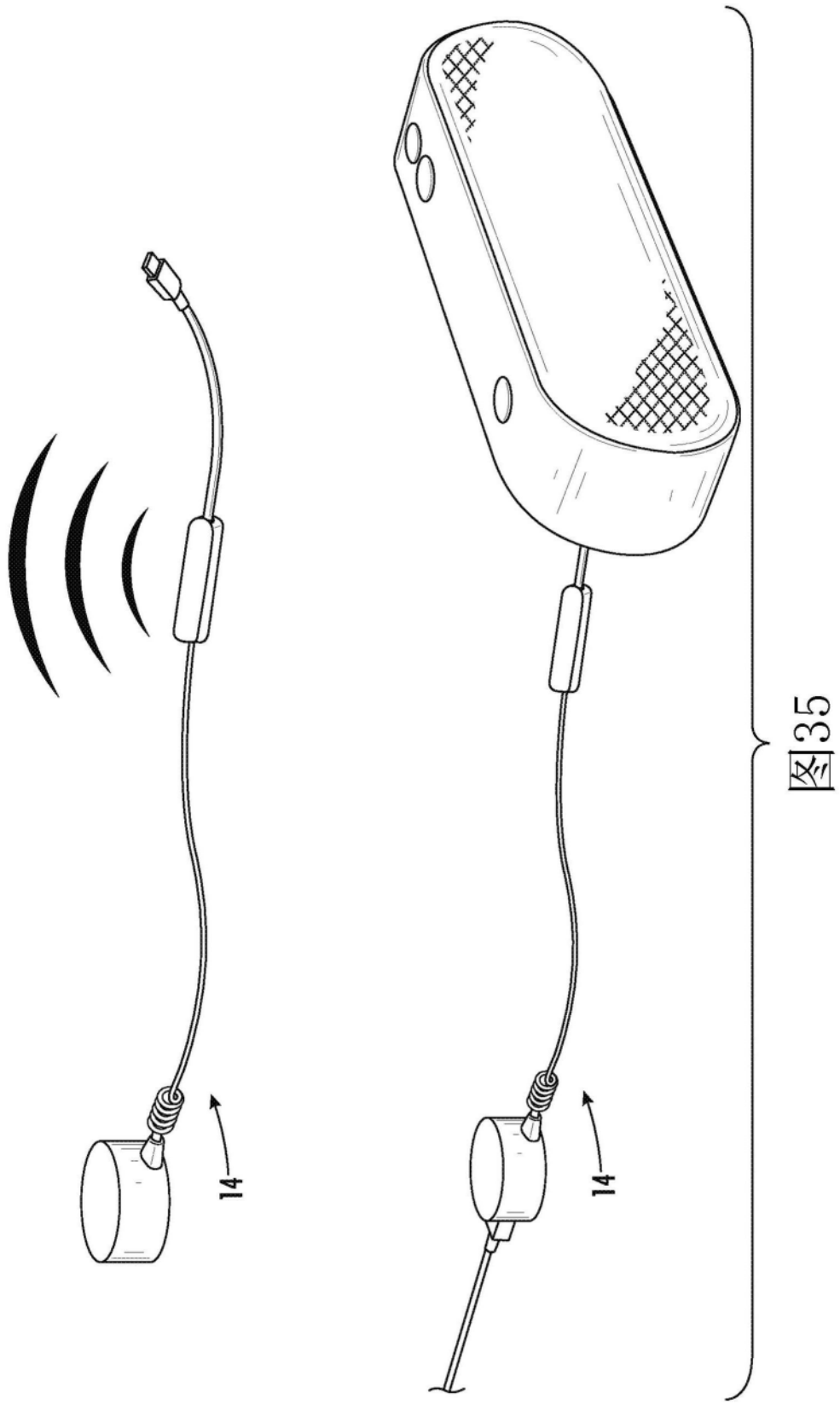


图35

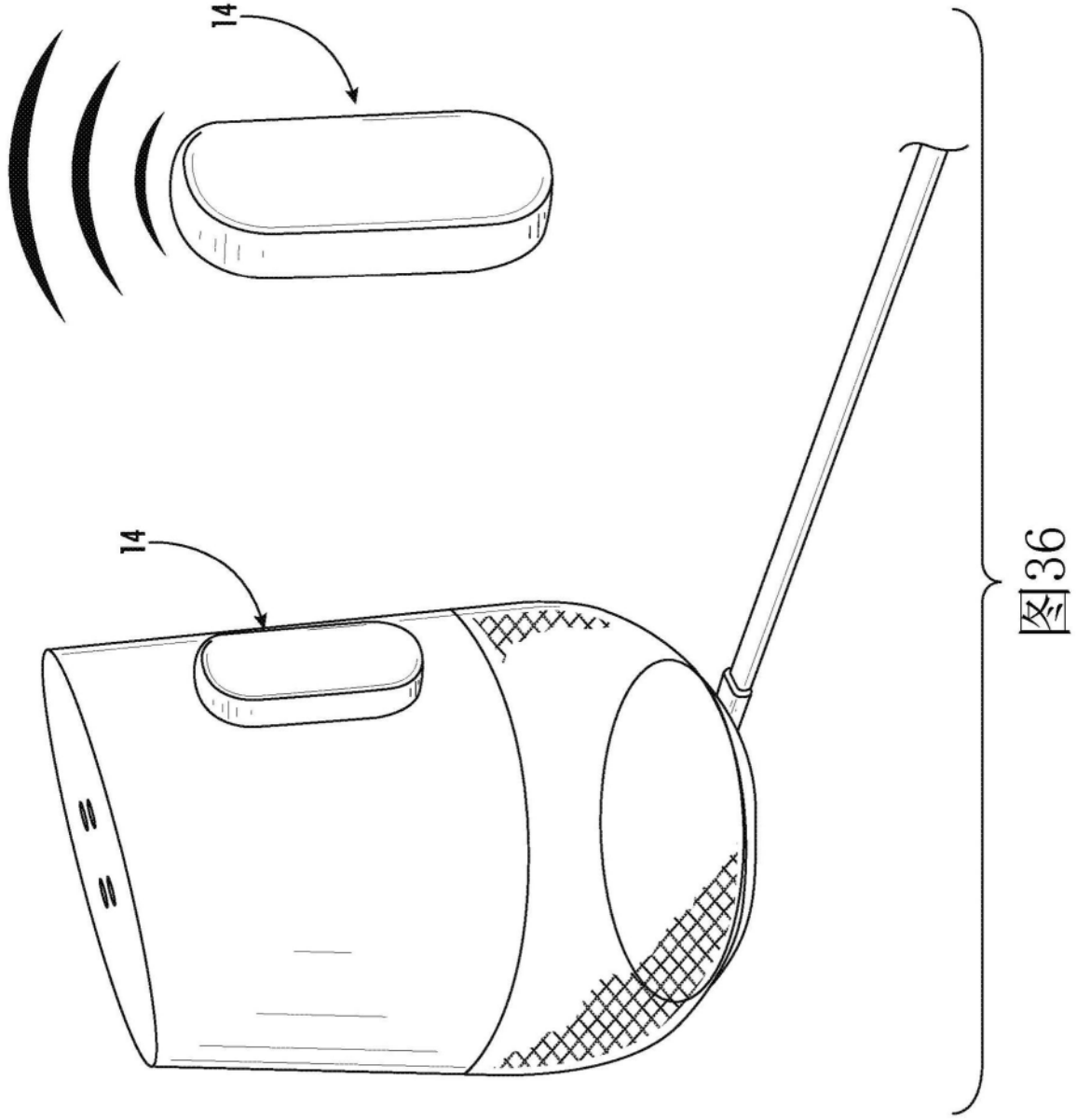


图36

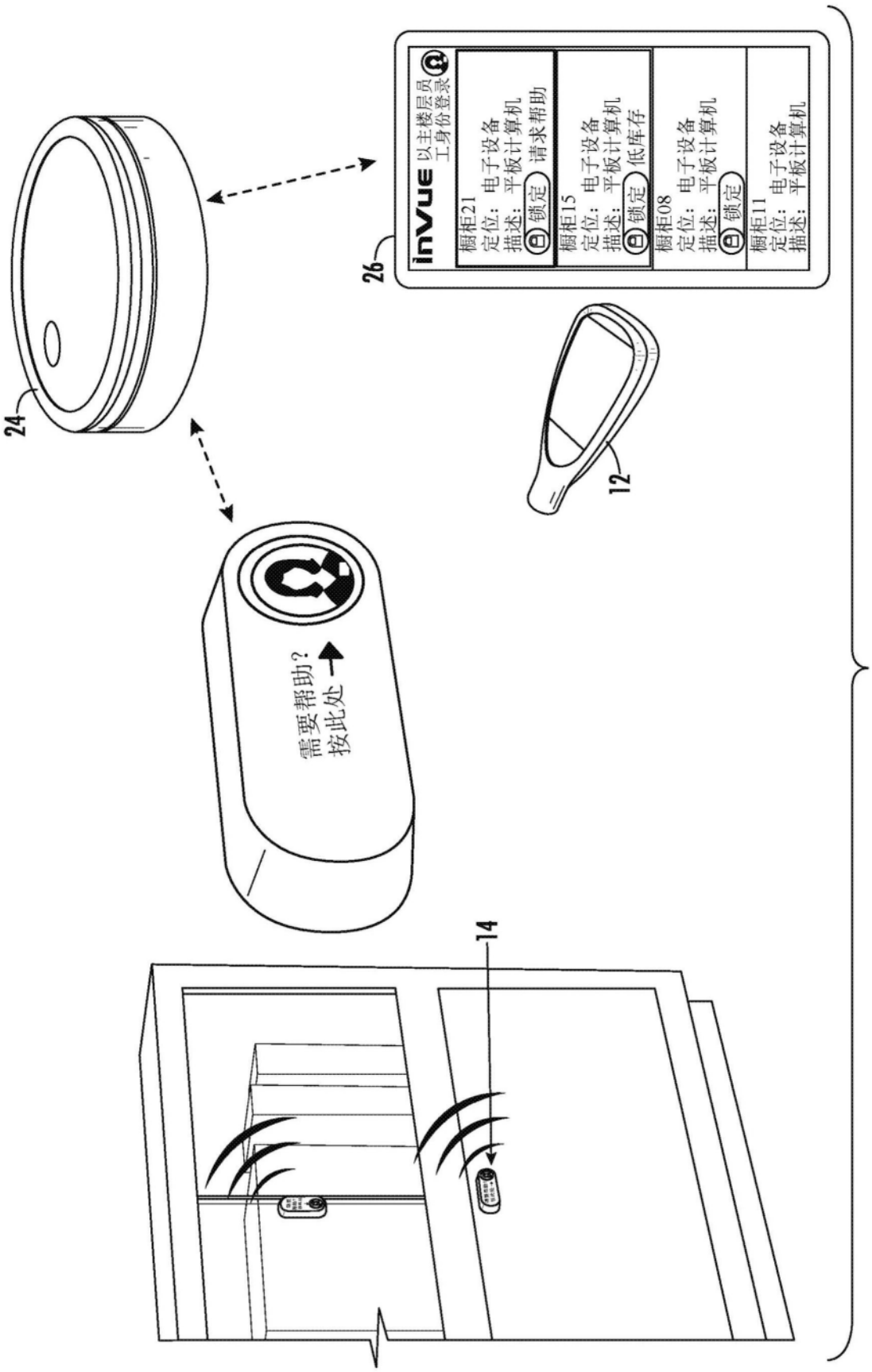

24
26
inVue 以主楼层员工身份登录
橱柜21
定位：电子设备
描述：平板计算机
锁定 请求帮助
橱柜15
定位：电子设备
描述：平板计算机
锁定 低库存
橱柜08
定位：电子设备
描述：平板计算机
锁定
橱柜11
定位：电子设备
描述：平板计算机
12
需要帮助？
按此处
14

图37

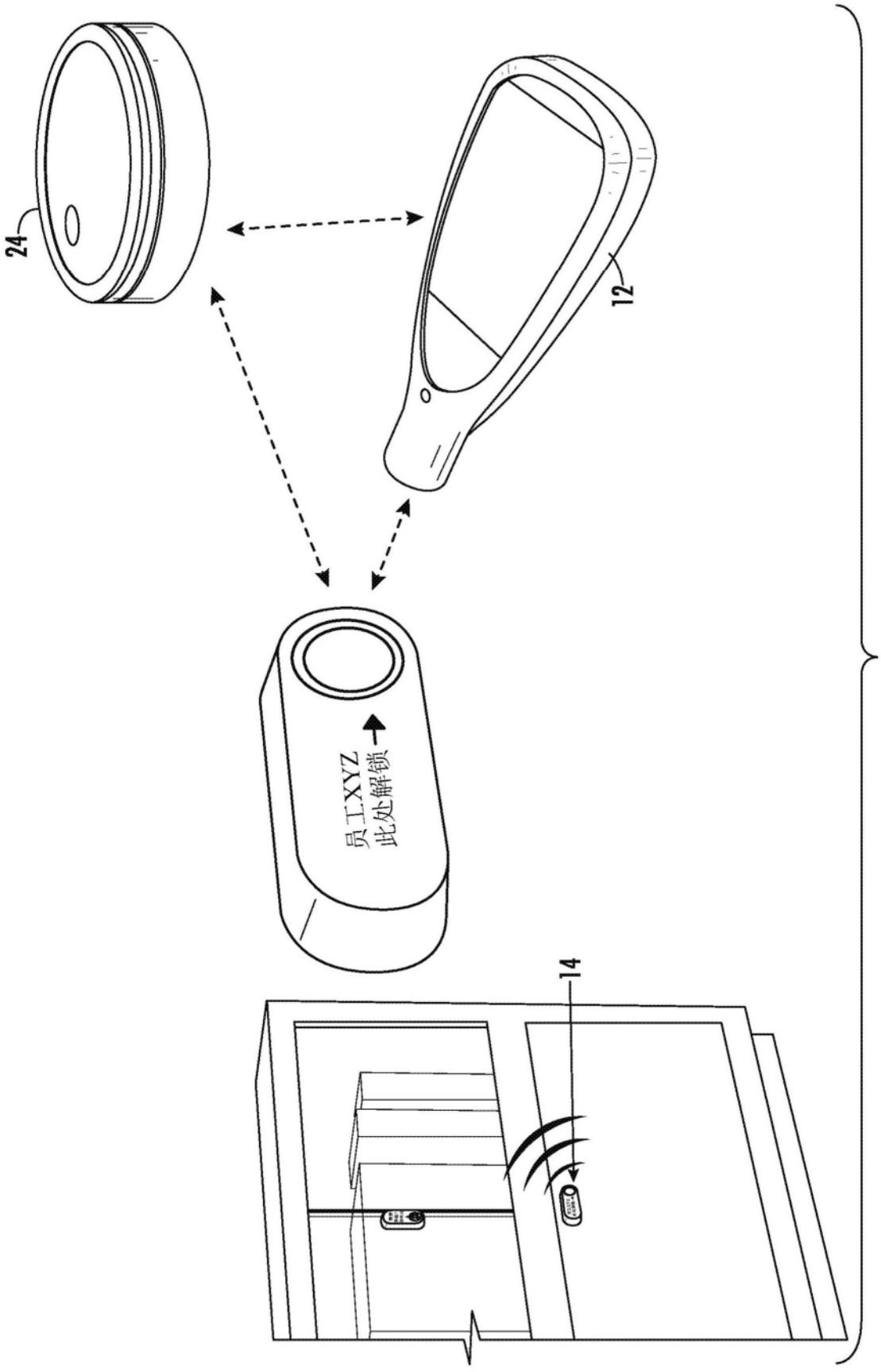


图38

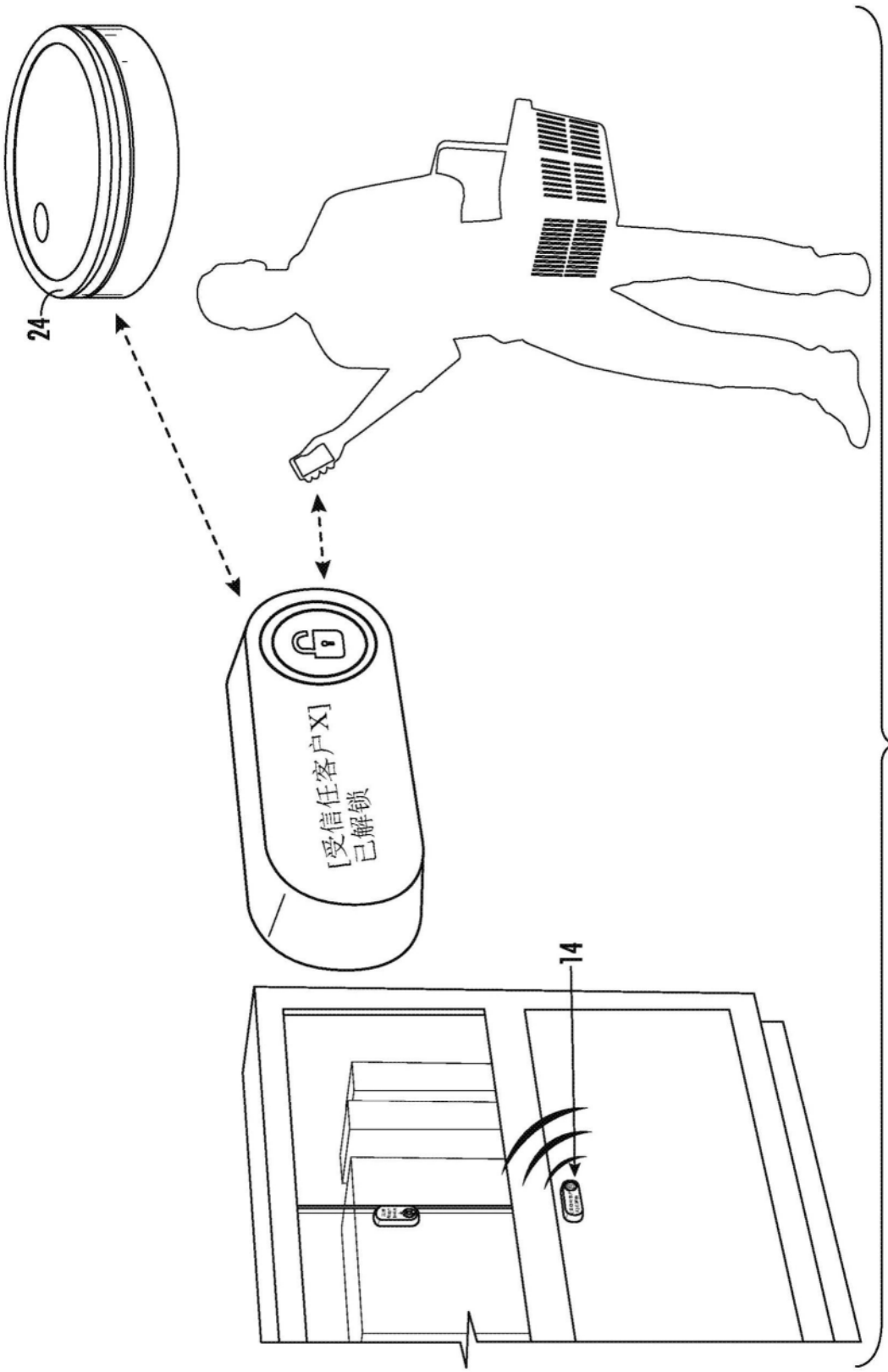


图39

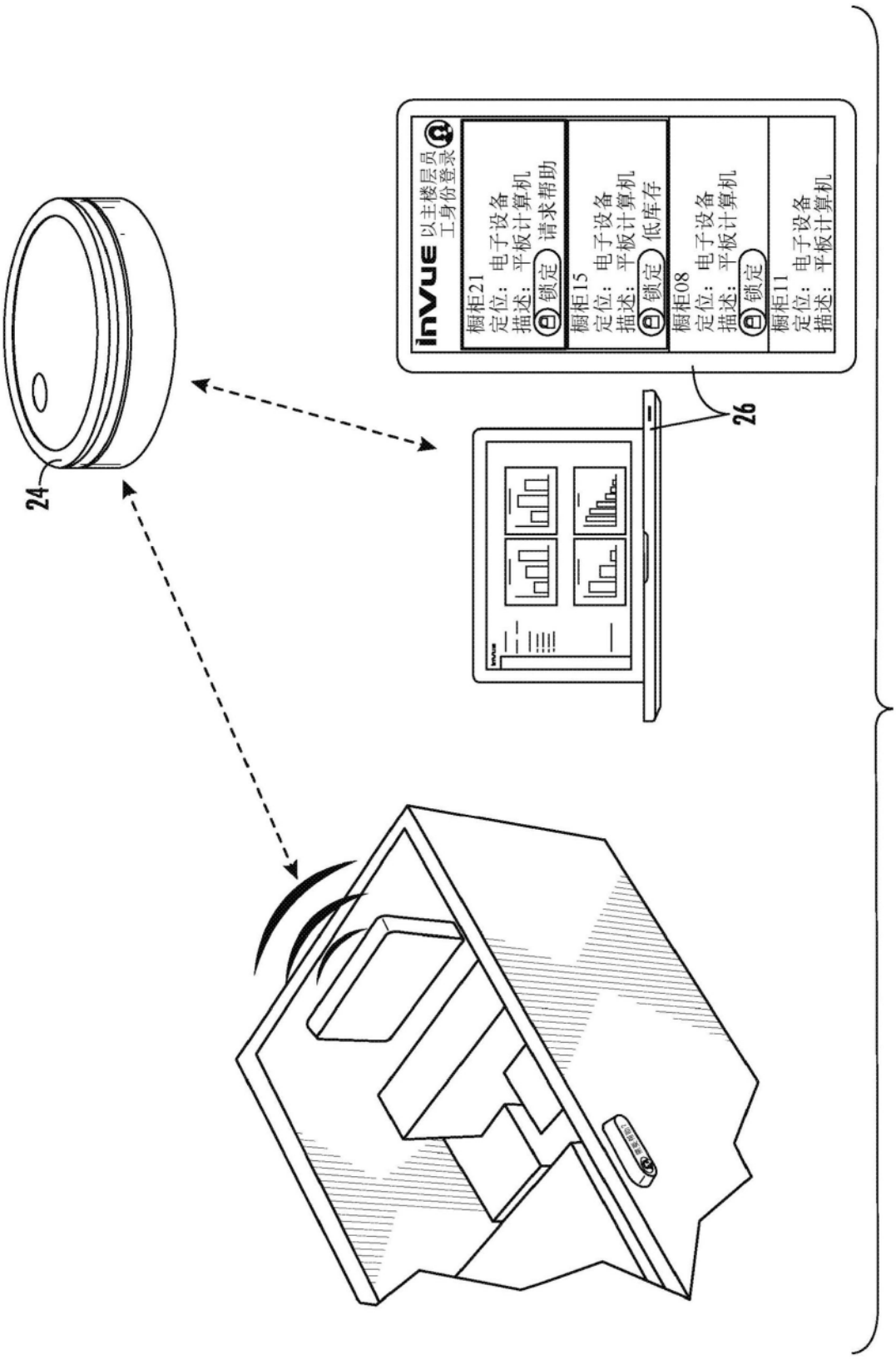

24
26
inVue 以主楼层员工身份登录
橱柜21
定位：电子设备
描述：平板计算机
锁定 请求帮助
橱柜15
定位：电子设备
描述：平板计算机
锁定 低库存
橱柜08
定位：电子设备
描述：平板计算机
锁定
橱柜11
定位：电子设备
描述：平板计算机

图40

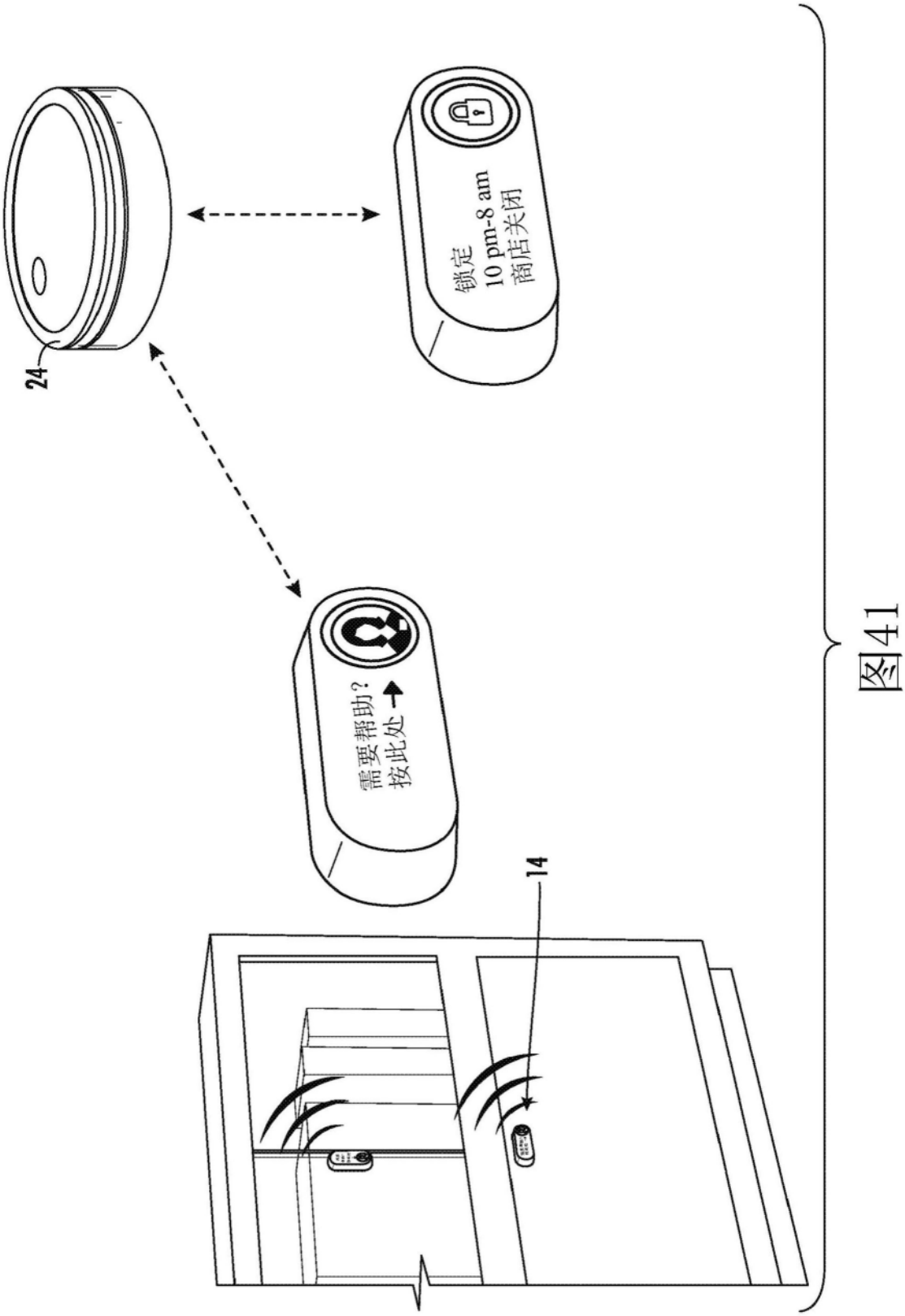


图41

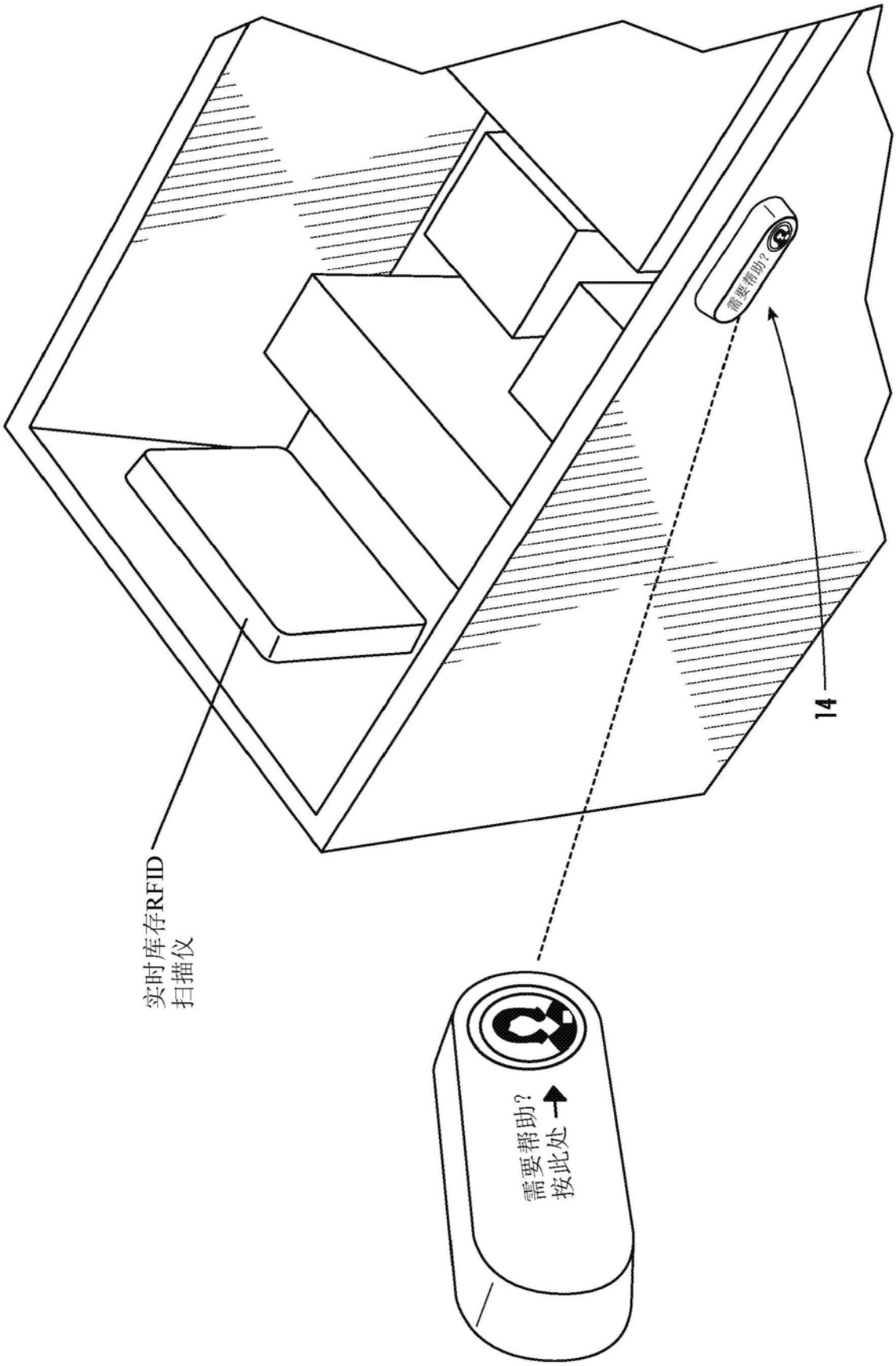


图42

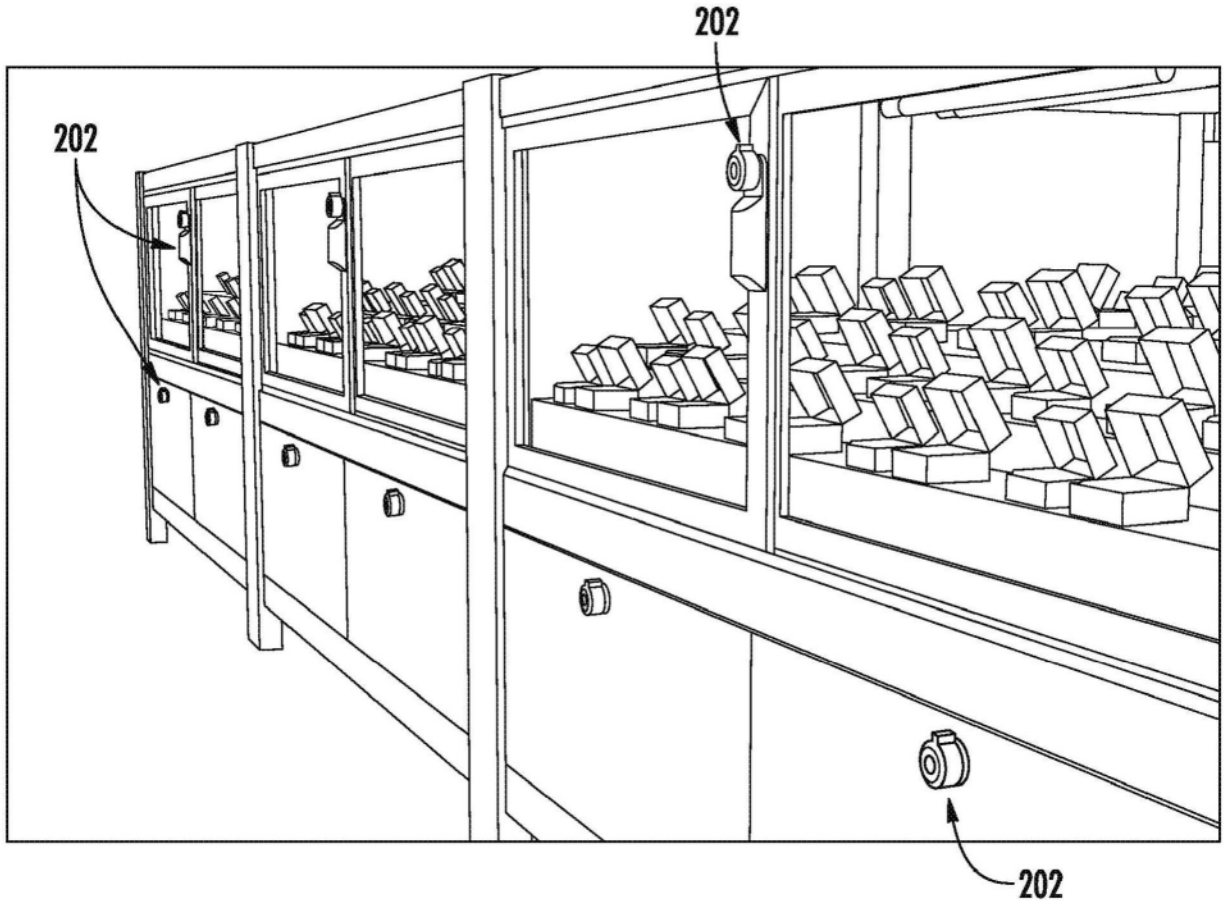


图43

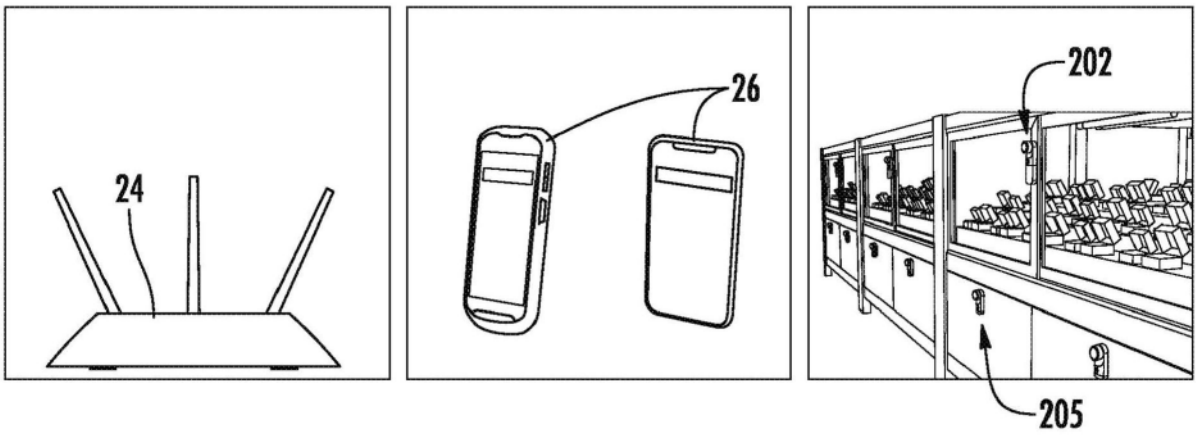


图44

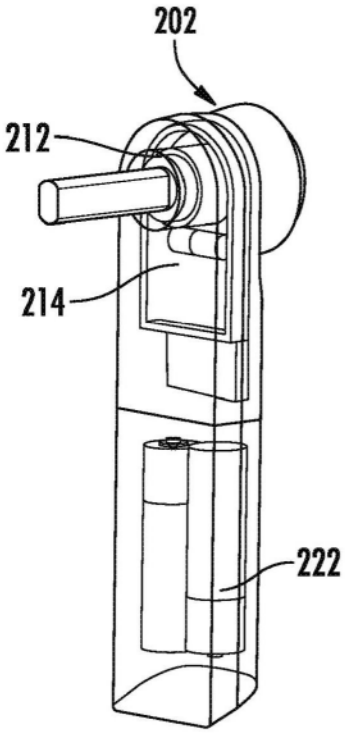


图45A

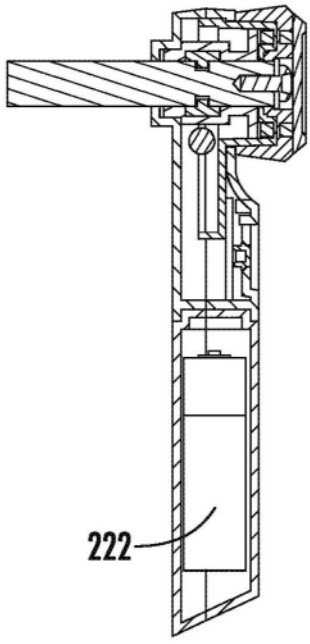


图45B

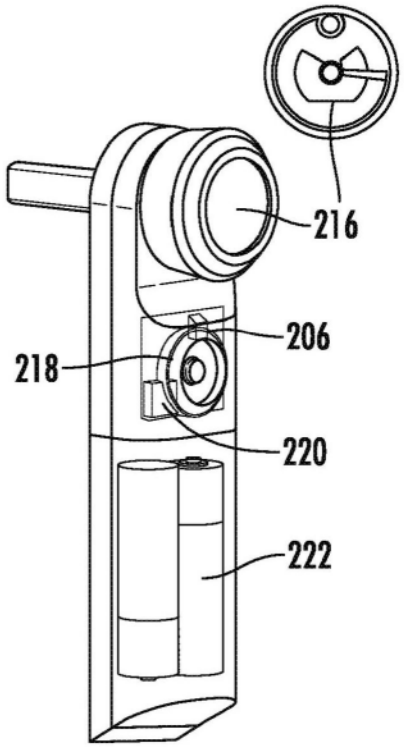


图45C

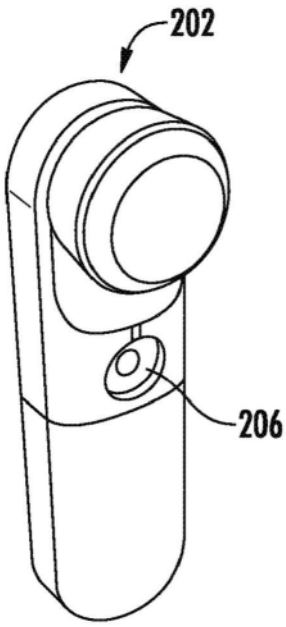


图46A

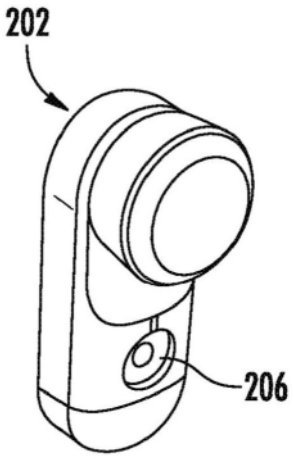


图46B

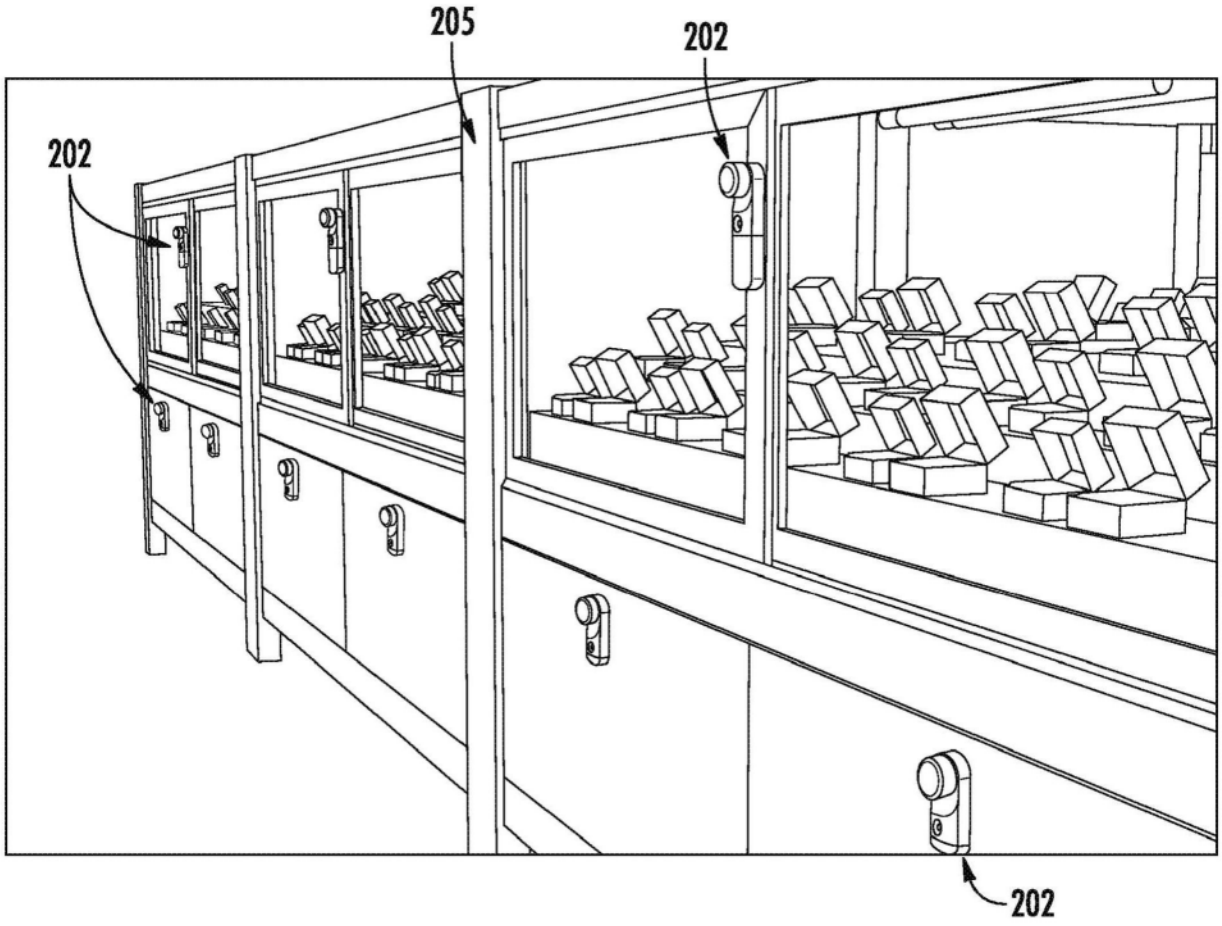


图47

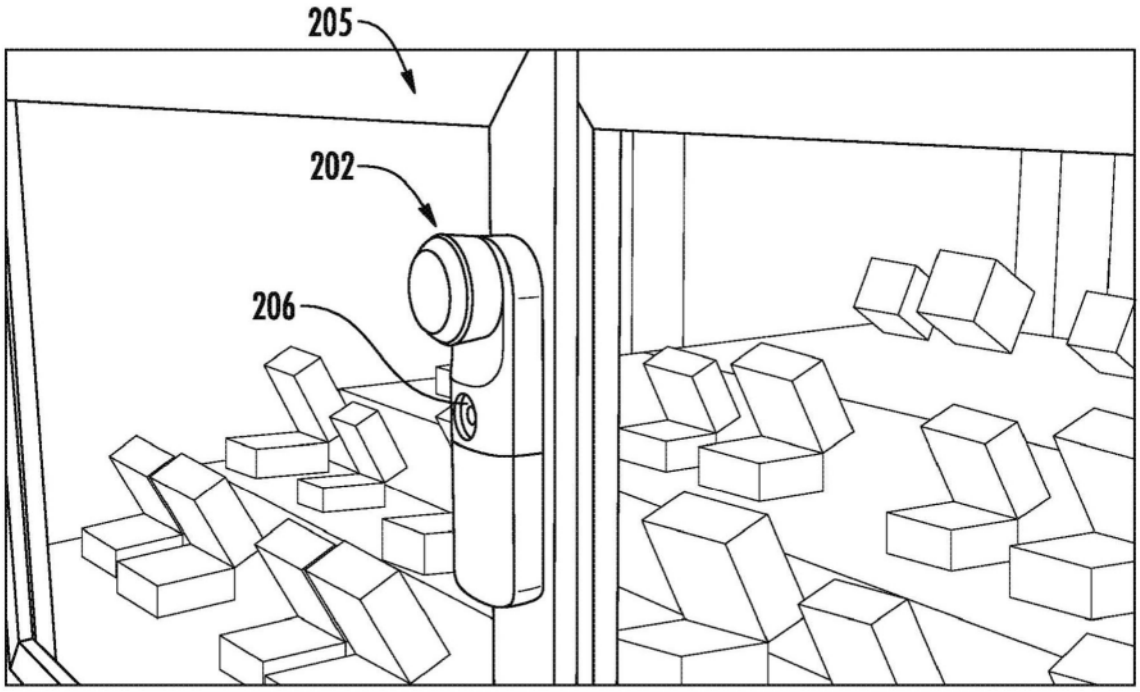


图48

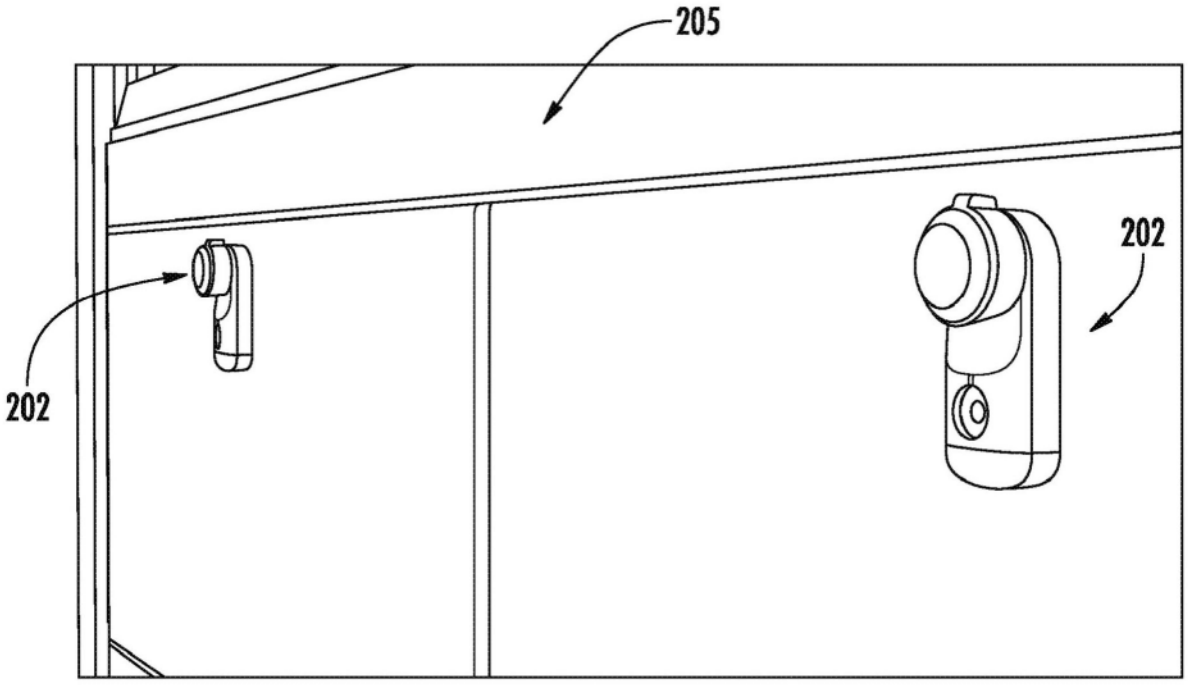


图49

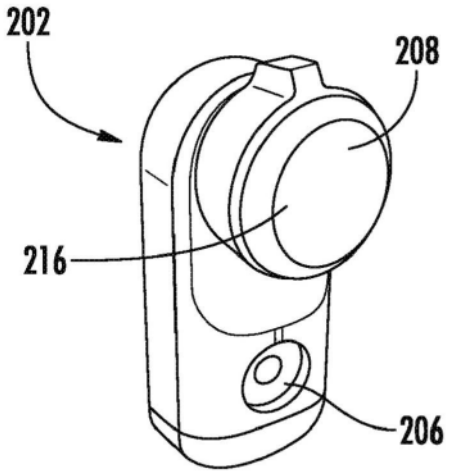


图50A

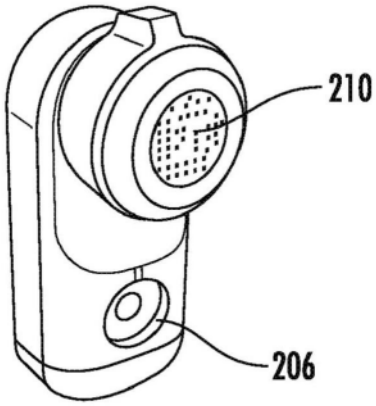


图50B

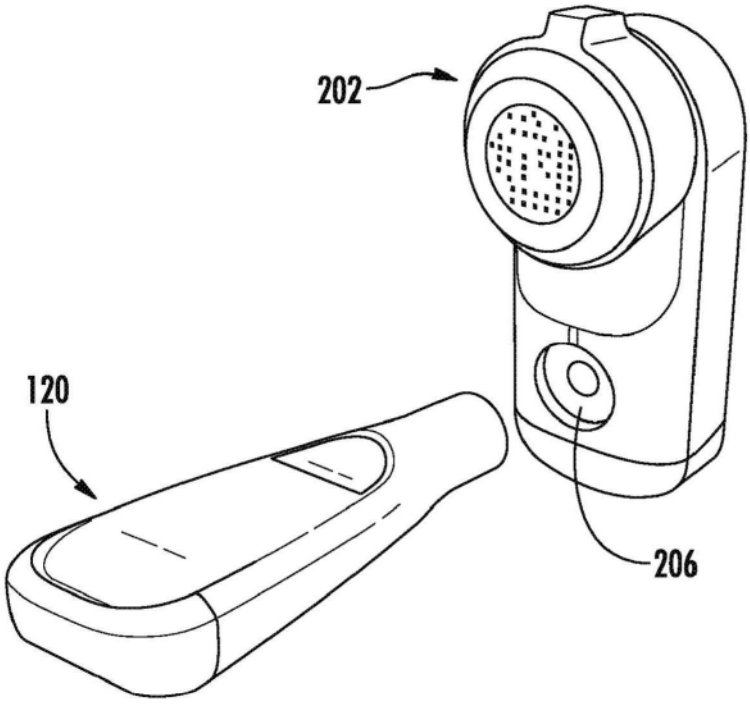


图51

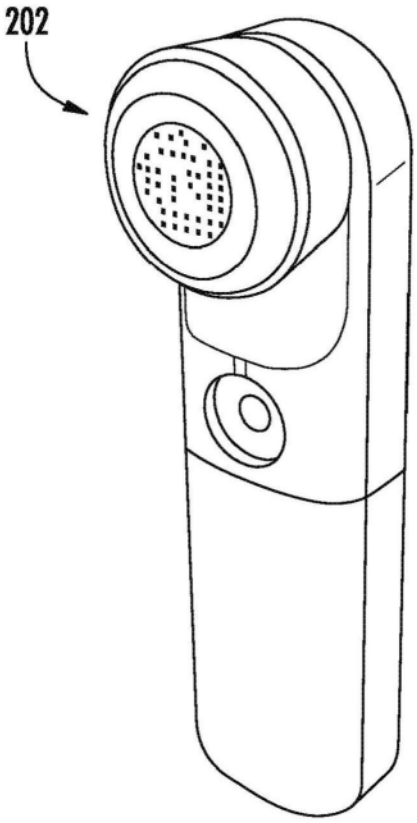


图52A

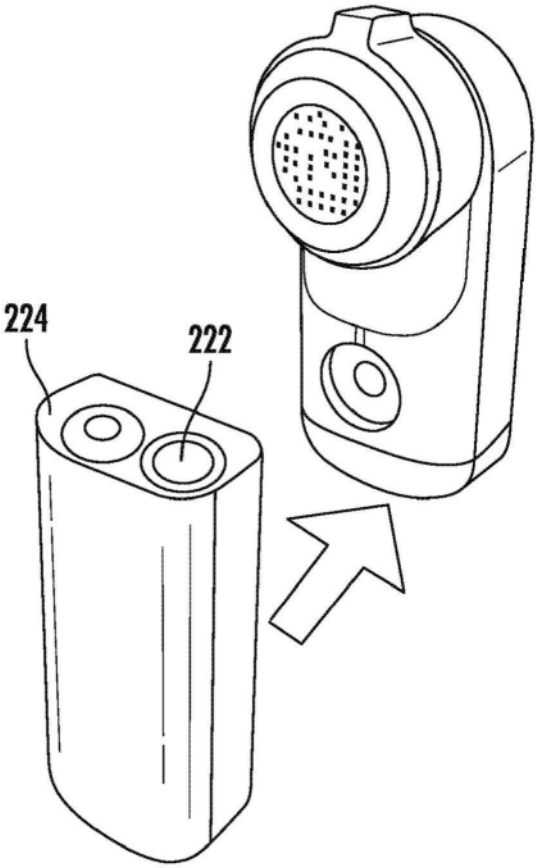


图52B

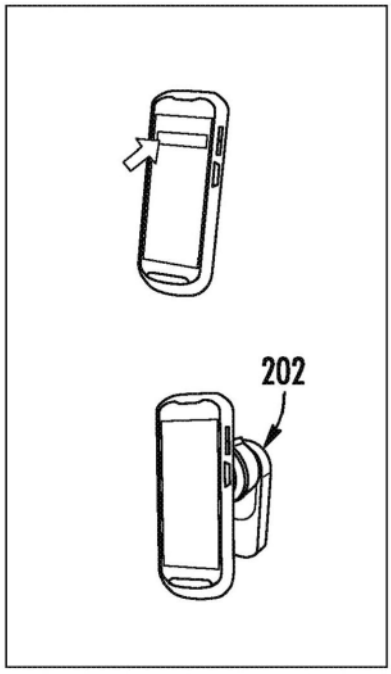


图53A

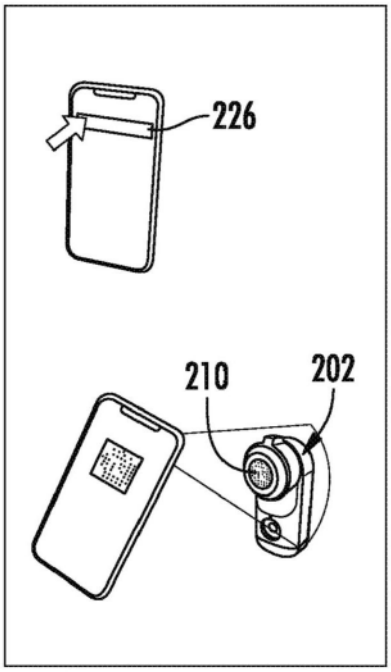


图53B

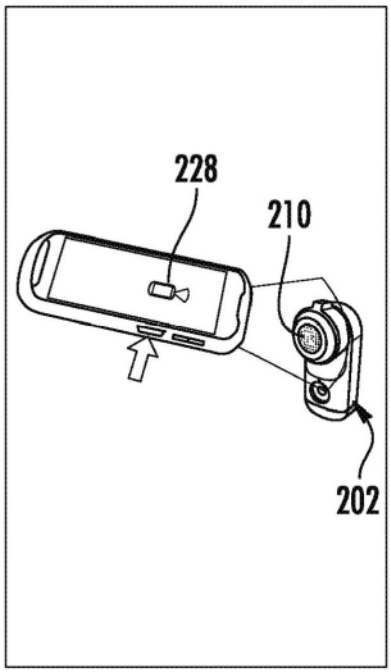


图53C

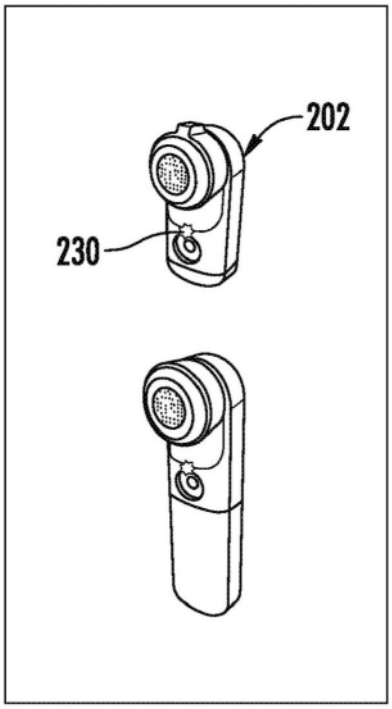


图54A

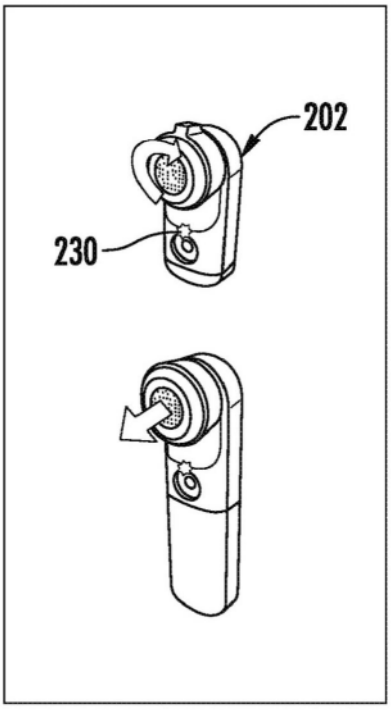


图54B

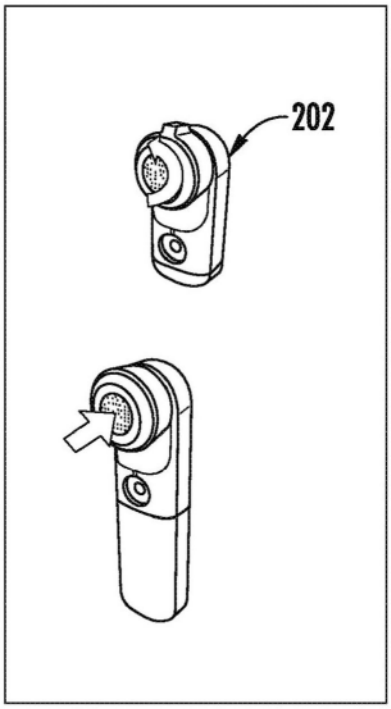


图54C

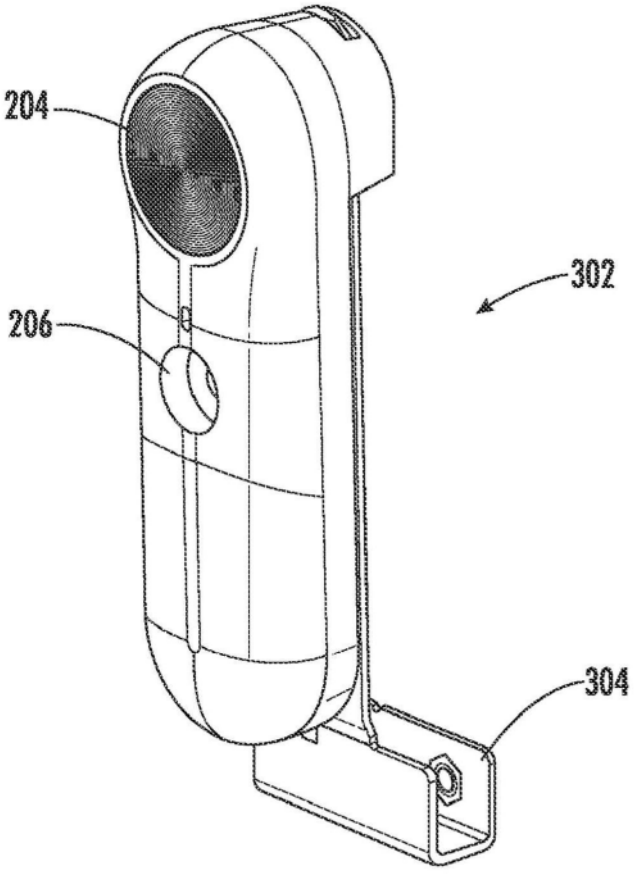


图55

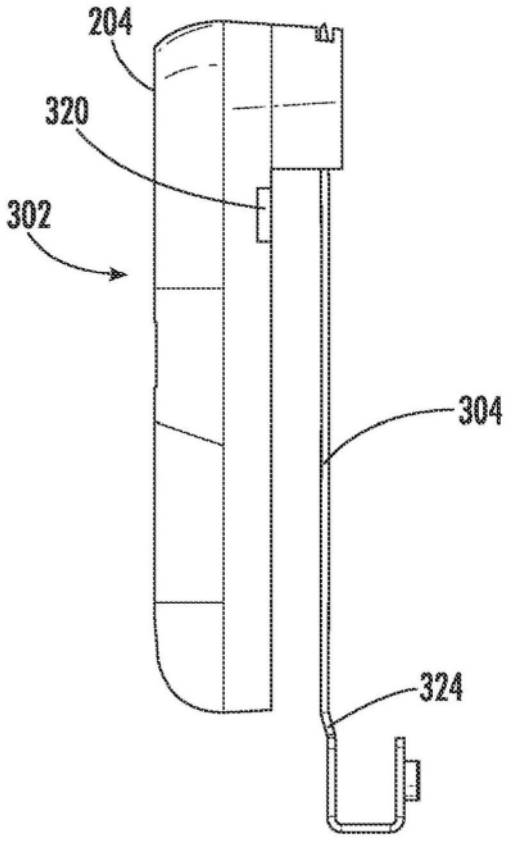


图56

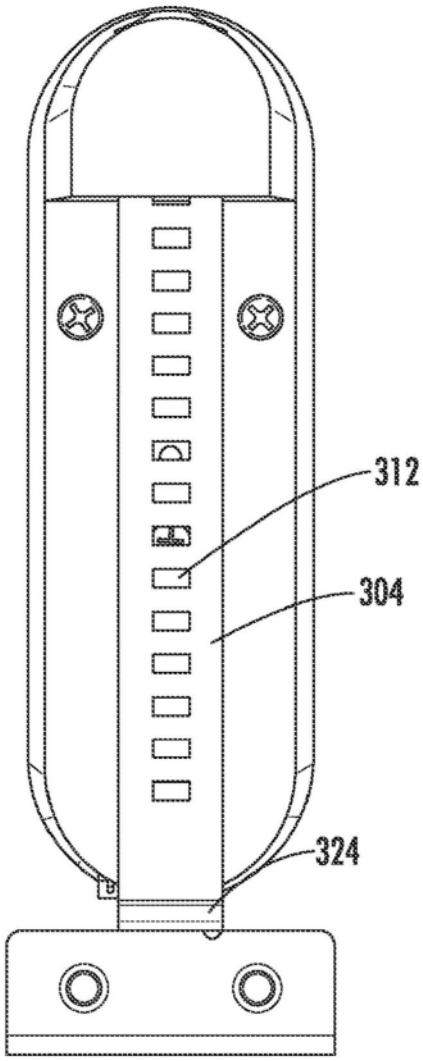


图57

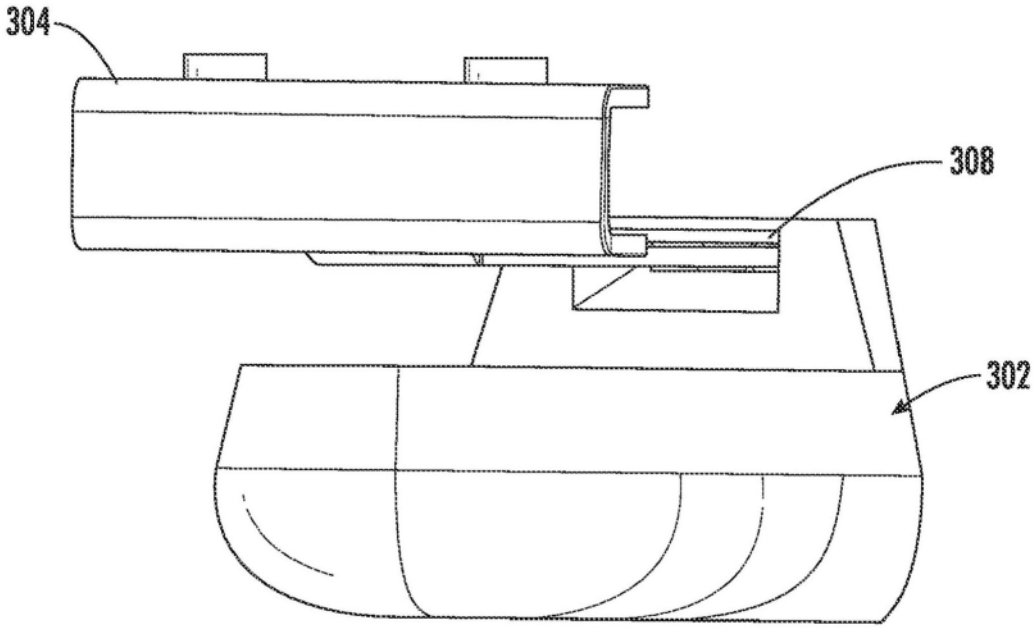


图58

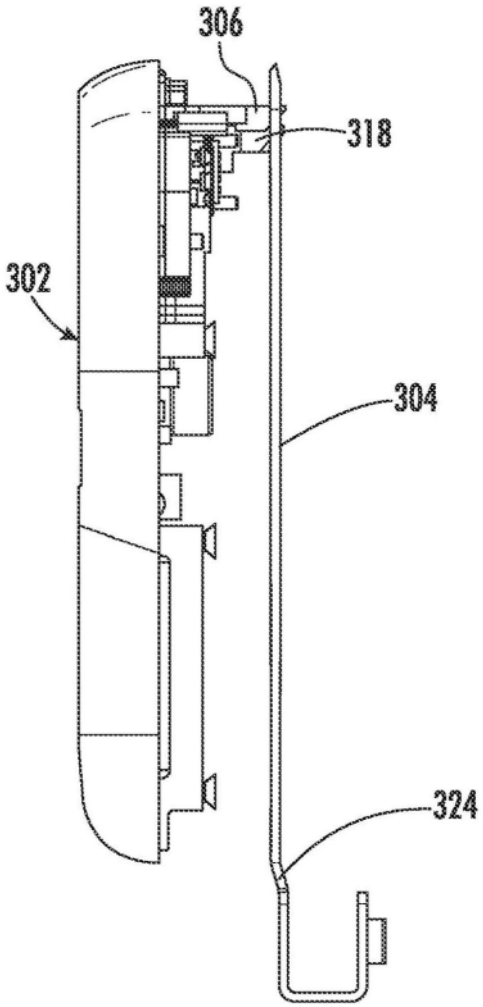


图59

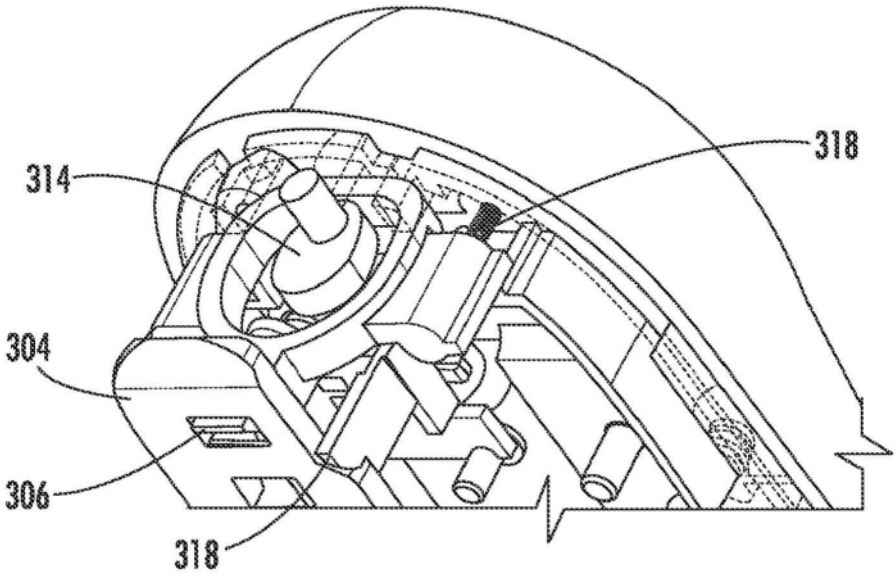


图60

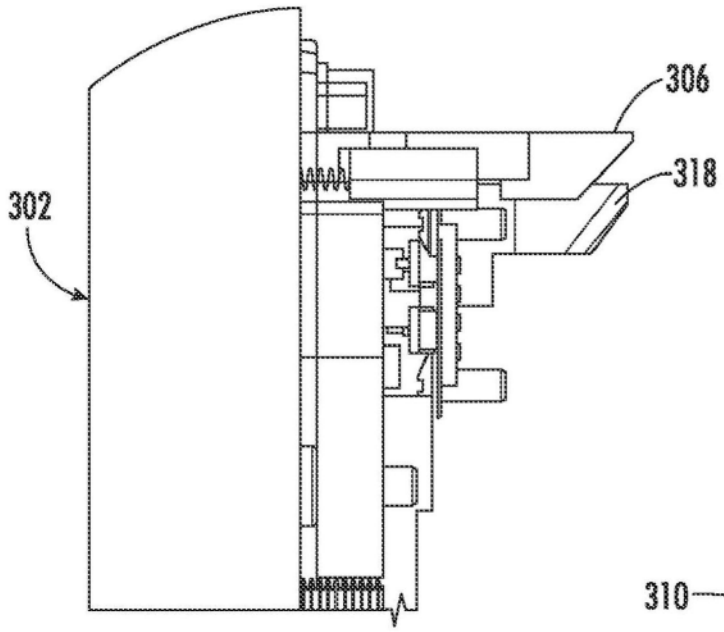


图61

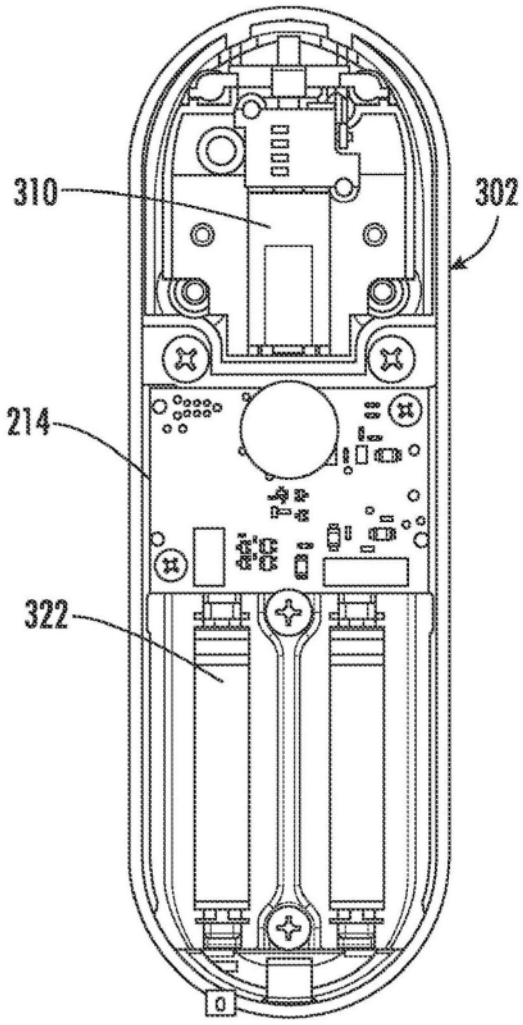


图62

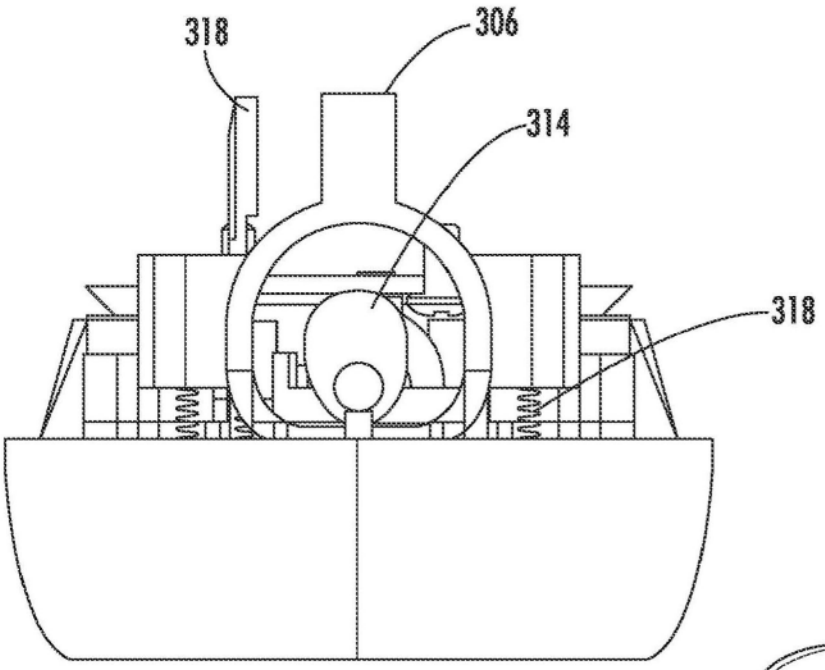


图63

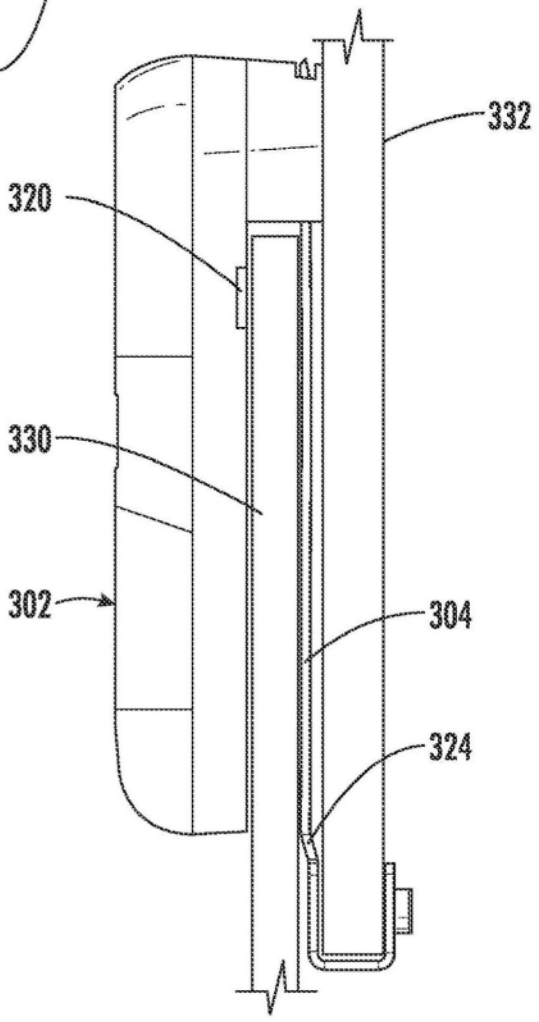


图64