(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105684049 B
(45)授权公告日 2019.11.08

(21)申请号 201480057139.8

(22)申请日 2014.08.27

(65)同一申请的已公布的文献号
申请公布号 CN 105684049 A

(43)申请公布日 2016.06.15

(30)优先权数据
102013111429.6 2013.10.16 DE

(85)PCT国际申请进入国家阶段日
2016.04.18

(86)PCT国际申请的申请数据
PCT/EP2014/068184 2014.08.27

(87)PCT国际申请的公布数据
WO2015/055344 DE 2015.04.23

(73)专利权人 锁定你的世界有限及两合公司
地址 德国巴特奥尔布

(72)发明人 马努埃拉·恩格尔-达汉
拉尔夫·科诺布林 蒂洛·迈泽尔

(74)专利代理机构 北京博华智恒知识产权代理事务所(普通合伙) 11431
代理人 樊卫民 黄向阳

(51)Int.Cl.
G07C 9/00(2006.01)

(56)对比文件
US 2013043973 A1,2013.02.21,
US 2008150684 A1,2008.06.26,
CN 102800142 A,2012.11.28,
CN 1161726 A,1997.10.08,
CN 1169173 A,1997.12.31,
WO 9914504 A2,1999.03.25,
CN 102436686 A,2012.05.02,

审查员 皮婉素

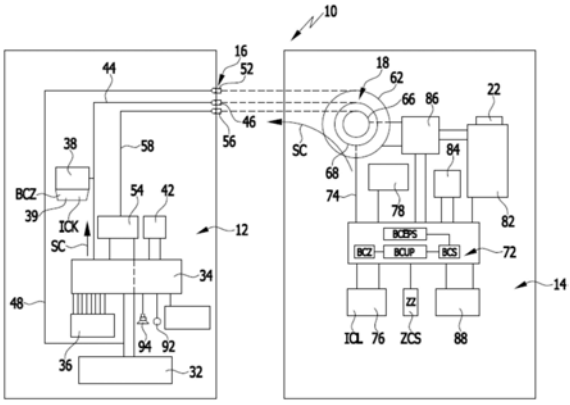
权利要求书3页 说明书16页 附图13页

(54)发明名称

用于运行锁闭系统的方法以及锁闭系统

(57)摘要

本发明涉及一种用于运行锁闭系统的方法，所述锁闭系统包括电子钥匙和电子锁以及在锁闭运行中与电子钥匙和电子锁局部分离地使用的中央单元，其中，在所述方法中由中央单元借助于授权码确定程序产生外部授权码，该外部授权码被传输给电子钥匙，该外部授权码由电子钥匙存放在存储器中，其中，在电子钥匙与电子锁配合作用时，外部授权码被电子锁由存储器读出并且由电子锁的处理器通过如下方式检查，即，处理器本身利用自身的授权码确定程序确定自身的授权码并且与由电子钥匙获得的外部授权码进行比较；并且其中，在所确定的自身的授权码与经传输的外部授权码相同时，处理器能实现打开过程。



CN 105684049 B

1.用于运行锁闭系统(10)的方法,所述锁闭系统包括电子钥匙(12)和电子锁(14)以及在锁闭运行中与所述电子钥匙(12)和电子锁(14)局部分离地使用的中央单元(102),所述电子钥匙和电子锁能通过触点组(16)和对应触点组(18)彼此相互作用;其中,在所述方法中由所述中央单元(102)借助于授权码确定程序(BCEPZ)产生外部授权码(BCZ),所述外部授权码(BCZ)被传输给电子钥匙(12),所述外部授权码(BCZ)由电子钥匙(12)存放在存储器(39)中;其中,所述电子锁(14)能通过所述电子钥匙(12)的电气的电压源运行;其中,所述电子钥匙(12)具有处理器(34),该处理器触发用于显示所述电子锁(14)的由电子锁传输的状态的信号元件(92、94),将所述电子锁(14)的状态信号传输给所述电子钥匙(12)以便进行显示;其中,在所述电子钥匙(12)与所述电子锁(14)配合作用时,外部授权码(BCZ)被所述电子锁(14)从所述存储器(39)读出并且由所述电子锁(14)的处理器(72)通过如下方式检查,即,处理器(72)本身利用自身的授权码确定程序(BCEPS)确定自身的授权码(BCS)并且与由所述电子钥匙(12)获得的外部授权码(BCZ)进行比较;并且其中,在所确定的自身的授权码(BCS)与经传输的外部授权码(BCZ)相同时,所述处理器(72)能实现打开过程。

2.根据权利要求1所述的方法,其特征在于,所述中央单元(102)的授权码确定程序(BCEPZ)如此确定所述外部授权码(BCZ),从而利用该授权码允许仅一次性的打开。

3.根据权利要求2所述的方法,其特征在于,所述中央单元(102)的授权码确定程序(BCEPZ)此外通过考虑循环计数器(ZCZ)来确定授权码(BCZ)。

4.根据权利要求3所述的方法,其特征在于,所述电子锁(14)的授权码确定程序(BCEPS)同样在考虑到循环计数器(ZCS)的情况下确定自身的授权码(BCS)。

5.根据权利要求1所述的方法,其特征在于,所述中央单元(102)和所述电子锁(14)的授权码确定程序(BCEPZ、BCEPS)在考虑所述电子钥匙(12)的识别码(ICK)和所述电子锁(14)的识别码(ICL)的情况下确定相应的授权码(BCZ、BCS)。

6.根据权利要求1所述的方法,其特征在于,所述授权码(BCZ、BCS)通过授权码确定程序(BCEPZ、BCEPS)借助于哈希算法来确定。

7.根据权利要求1所述的方法,其特征在于,在将所述电子锁(14)装配在为其预设的地点处之前通过所述中央单元(102)激活所述电子锁(14),其中,所述中央单元(102)在此利用在所述中央单元(102)中保存的识别码(ICL)和循环计数器(ZZ)的存储的状态校准所述电子锁(14)的识别码(ICL)和所述电子锁(14)的循环计数器(ZZ)的状态。

8.根据权利要求1所述的方法,其特征在于,所述电子锁(14)的识别码(ICL)存储在安全的存储器(76)中。

9.根据权利要求1所述的方法,其特征在于,所述中央单元(102)在激活所述电子锁(14)时在所述电子锁(14)和所述中央单元(102)之间校准有待存储的密码。

10.根据权利要求1所述的方法,其特征在于,在激活所述电子锁(14)时校准配置密码。

11.根据权利要求1所述的方法,其特征在于,所述中央单元(102)在激活所述电子钥匙(12)时利用所述电子钥匙(12)的在所述中央单元(102)中存储的识别码(ICK)校准所述电子钥匙(12)的识别码(ICK)。

12.根据权利要求10所述的方法,其特征在于,在激活所述电子钥匙(12)时将配置密码存放在存储器(39)中。

13.根据权利要求1所述的方法,其特征在于,所述电子钥匙(12)的识别码(ICK)存储在

所述电子钥匙(12)的存储器(39)中。

14.根据权利要求1所述的方法,其特征在于,所述电子钥匙(12)的存储器(39)仅能在使用安全哈希码(SC)时写入和读出。

15.根据权利要求14所述的方法,其特征在于,由在所述电子钥匙(12)中的处理器(34)确定安全哈希码(SC)以便存储外部授权码(BCZ)。

16.根据权利要求14或15所述的方法,其特征在于,为了从所述电子钥匙(12)的安全的存储器(39)读出外部授权码(BCZ),在所述电子锁(14)中的处理器(72)产生安全哈希码(SC)以便访问安全的存储器(39)。

17.根据权利要求1所述的方法,其特征在于,安全处理器(38)的存储器用作在所述电子钥匙(12)中的存储器(39)。

18.电子锁闭系统(10),所述电子锁闭系统包括电子钥匙(12)和电子锁(14),所述电子钥匙和电子锁能通过触点组(16)和对应触点组(18)彼此相互作用,所述电子锁(14)能通过所述电子钥匙(12)的电气的电压源运行;其中,所述电子钥匙(12)具有处理器(34),该处理器触发用于显示所述电子锁(14)的由电子锁传输的状态的信号元件(92、94),将所述电子锁(14)的状态信号传输给所述电子钥匙(12)以便进行显示,其中,所述处理器(34)与输入单元(36)配合作用,通过所述输入单元能将外部产生的授权码(BCZ)传输给处理器(34),其中,所述处理器(34)与存储器(39)配合作用并且将外部产生的授权码(BCZ)写入到存储器(39)中;并且其中,所述电子锁(14)具有处理器(72),该处理器在所述电子钥匙(12)与所述电子锁(14)相互作用时通过触点组(16)和对应触点组(18)与在所述电子钥匙(12)中的存储器(39)相互作用,以便读出外部产生的授权码(BCZ)。

19.根据权利要求18所述的电子锁闭系统,其特征在于,所述存储器(39)是安全的存储器并且所述电子钥匙(12)的处理器(34)产生安全码(SC),以便在所述安全的存储器(39)中存放产生的外部授权码(BCZ)。

20.根据权利要求19所述的电子锁闭系统,其特征在于,所述电子锁(14)的处理器(72)产生安全码(SC),以便读出在所述安全的存储器(39)中存放的授权码(BCZ)。

21.根据权利要求18所述的电子锁闭系统,其特征在于,所述电子钥匙(12)具有显示元件(92、94),以便显示所述电子锁(14)的由电子锁(14)传输给电子钥匙(12)的状态。

22.根据权利要求21所述的电子锁闭系统,其特征在于,所述电子锁(14)的处理器(72)将关于所述电子锁(14)的状态的状态信号传输给所述电子钥匙(12)的处理器(34),并且所述电子钥匙(12)的处理器(34)根据经传输的状态触发所述电子钥匙(12)的显示元件(92、94)。

23.根据权利要求19所述的电子锁闭系统,其特征在于,所述安全的存储器(39)是安全处理器(38)的存储器。

24.根据权利要求18所述的电子锁闭系统,其特征在于,所述电子锁(14)包括用于操纵锁闭止动器(22)的锁闭驱动器(82)。

25.根据权利要求24所述的电子锁闭系统,其特征在于,所述电子锁(14)的锁闭驱动器(82)能通过电子钥匙(12)的电气的电压源(32)运行。

26.根据权利要求25所述的电子锁闭系统,其特征在于,所述电子锁(14)具有变压器(86),以便运行所述锁闭驱动器(82)。

27.根据权利要求18所述的电子锁闭系统，其特征在于，所述电子锁(14')具有切换单元(362)，以便激活或者锁止外部的锁闭系统(268)。

28.根据权利要求18所述的电子锁闭系统，其特征在于，所述电子钥匙(12)具有用于借助于中央单元(102)激活所述电子钥匙(12)的接口(42)。

29.根据权利要求18所述的电子锁闭系统，其特征在于，所述电子锁(14)具有用于通过中央单元(12)激活电子锁(14)的接口(84)。

30.根据权利要求28或29所述的电子锁闭系统，其特征在于，所述电子钥匙(12)或者所述电子锁(14)的激活通过所述中央单元(102)导线连接地进行。

用于运行锁闭系统的方法以及锁闭系统

[0001] 技术区域

[0002] 本发明涉及一种用于运行锁闭系统的方法以及一种锁闭系统。

背景技术

[0003] 在锁闭系统中普遍存在如下要求，即，在尽可能简单的操作中确保尽可能高的安全性。

发明内容

[0004] 该任务能够通过一种用于运行锁闭系统的方法通过如下方式来解决，所述锁闭系统包括电子钥匙和电子锁以及在锁闭运行中与电子钥匙和电子锁局部分离地使用的中央单元，即，在所述方法中，由中央单元借助于授权码确定程序产生外部授权码，所述外部授权码被传输给电子钥匙，该外部授权码由电子钥匙存放在存储器中，其中，在电子钥匙与电子锁配合作用时外部授权码被电子锁由存储器读出并且由电子锁的处理器通过如下方式检查，即，所述处理器本身利用自身的授权码确定程序来确定自身的授权码并且将自身的授权码与由电子钥匙获得的外部授权码进行比较，并且其中，所述处理器能在所确定的自身的授权码与经传输的外部授权码相同时实现打开过程。

[0005] 按照本发明的方法的优点在于，利用多个电子钥匙和多个电子锁，通过输出外部授权码，仅一个确定的电子钥匙能够在输入外部授权码时打开一个确定的电子锁。

[0006] 按照本发明的方法的另一个优点在于，通过确定外部授权码并且将该外部授权码传输到电子钥匙上而存在如下可能性，即，已经在传输外部授权码之前检查是否存在如下情况，在该情况下由操作人员合理地要求这样的授权码并且因此已经能够明白打开电子锁的前提条件是局部远离电子钥匙和电子锁。

[0007] 此外，在按照本发明的方法中，通过借助于中央单元确定外部授权码不可以由拥有电子钥匙的用户滥用或者不完全合理地打开。

[0008] 对于按照本发明的方法的安全性特别有利的是，所述中央单元的授权码确定程序这样确定外部授权码，使得利用该授权码允许仅一次性的打开。

[0009] 因此，特别是防止操作人员存储所述授权码并且尝试再次使用。

[0010] 如果所述授权码此外通过考虑在中央单元中的循环计数器来确定，则能够以特别简单的方式利用所述中央单元的授权码确定程序确定作为一次有效的授权码的授权码，其中，所述循环计数器确定并且记录用于打开等待处理的电子锁的打开过程。

[0011] 为了同样给电子锁的授权码确定程序提供确定正确的自身的授权码的可能性而规定，电子锁的授权码确定程序同样在考虑循环计数器的情况下确定自身的授权码。

[0012] 此外，优选地规定，中央单元和电子锁的授权码确定程序在考虑有待使用的电子钥匙的识别码和有待打开的电子锁的识别码的情况下确定相应的授权码。

[0013] 为了生成尽可能高的安全水平，优选地规定，授权码确定程序借助于哈希算法确定授权码。

[0014] 为了确保中央单元的授权码确定程序和电子锁的授权码确定程序可以由相同的参数和状态出发相互独立地确定授权码，优选地规定，在将电子锁装配在为其预设的地点处之前，通过中央单元激活电子锁，其中，中央单元在此利用保存在中央单元中的电子锁的识别码和循环计数器的存储在中央单元中的状态来校准电子锁的识别码和电子锁的循环计数器的状态。

[0015] 在此，“校准”的概念可理解为，相应的数据、亦即例如识别码和/或循环计数器的状态，在电子锁和中央单元之间交换或者由其中一个读出并且存放在另一个中。

[0016] 在此，优选地规定，电子锁的识别码存储在安全的存储器中。

[0017] 此外，优选地规定，中央单元在激活电子锁时校准要在电子锁和中央单元之间存储的密码、特别是用于电子钥匙和电子锁的配置密码，例如校准成一个或者多个访问组的配置密码。

[0018] 对于安全性特别有利的是，在激活电子锁时校准配置密码。

[0019] 在此，所述配置密码应该将电子锁的配置固定成确定的锁组和/或确定的钥匙组。

[0020] 此外，一种有利的技术方案规定，中央单元在激活电子钥匙时利用电子钥匙的存储在中央单元中的识别码校准电子钥匙的识别码。

[0021] 在这种情况下“校准”的概念也要这样理解，从而使得电子钥匙在两个单元之间交换或者在其中一个单元中读出并且保存在另一个单元中或者同时保存在两个单元中。

[0022] 对于使用电子钥匙特别安全的是，在激活电子钥匙时将配置密码保存在存储器中。

[0023] 此外，优选地规定，电子钥匙的识别码存储在电子钥匙的存储器中。

[0024] 优选地，电子钥匙的存储器仅能在使用安全哈希码时写入和读出。

[0025] 在此优选地规定，由在电子钥匙中的处理器为了存储外部授权码而确定安全哈希码。

[0026] 此外，同样优选地规定，为了由电子钥匙的安全的存储器读出外部授权码，在电子锁中的处理器产生安全的哈希码以便访问安全的存储器。

[0027] 关于安全的存储器的类型，至今未作出更详细地说明。

[0028] 因此，一种优选的技术方案规定，安全处理器的存储器用作在电子钥匙中的存储器，其中，安全处理器特别是要求生成安全的哈希码，以便可以将数据、例如授权码和/或识别码和/或密码保存在安全处理器的存储器中。

[0029] 此外，为了防止对电子锁本身进行破坏并且在此电子锁至少显示是否可以通过利用还未授权的电子钥匙的破坏达到某种重要的状态，优选地规定，电子锁的状态信号传输给电子钥匙以用于显示并且因此特别是电子锁本身不具有显示其状态的可能性。

[0030] 在此，特别是规定，电子钥匙具有处理器，该处理器触发用于显示电子锁的由电子锁传输的状态的信号元件。

[0031] 一种用于安全获得访问授权或者用于借助于电子锁和至少一个由用户携带的电子钥匙将钥匙安全交付给至少一个用户的、特别是按照以下描述的特征的方法的实施方式包括下列方法步骤：

[0032] 借助于通信装置将至少一个用于电子锁和/或用户的特征信息发送给远离电子锁布置的中央信息处理位置或者中央单元；

[0033] 通过中央信息处理位置检查经发送的信息；

[0034] 借助于通信装置在积极检查信息的情况下将授权码发送给用户；

[0035] 由用户借助于输入单元将授权码输入到所携带的电子钥匙中；

[0036] 通过与电子钥匙配合作用来解锁电子锁。

[0037] 为此例如规定，用于锁的特征信息由数字组合或者由条形码(Barcode)形成。

[0038] 备选地或者对此补充地，特别是规定，对于用户来说独特的信息由字母组合/数字组合和/或由密码形成。

[0039] 特别有利的是，信息处理位置或者中央单元在将授权码发送给用户之前除了用于锁和/或用户的特征信息之外还检查与两个信息结合的、用于使用地点和/或使用时间的时间参量。

[0040] 一种有利的技术方案规定，电子锁布置在保险管的锁盖上，在解锁电子锁之后取出物理钥匙以用于走进至少一个另外的房间。

[0041] 此外有利地规定，电子锁和/或该电子锁解锁的装置在激活和/或解除时将信息发送到中央信息处理位置或者中央单元处。

[0042] 一种有利的技术方案规定，为了发送所述至少一个用于电子锁和/或用户的特征信息和/或为了接收授权码而将移动电话用作通信装置。

[0043] 特别有利的是，通信装置含有应用程序，借助于该应用程序能检测所述至少一个用于电子锁和/或用户的特征信息和/或能借助于该应用程序接收授权码和/或能借助于该应用程序将授权码传递给电子钥匙。

[0044] 一种特别有利的变形方案这样设计，从而使得通信装置和电子钥匙形成一个单元。

[0045] 通过检查用于电子锁的特征信息、例如布置在锁的区域中能借助于通信装置机械地或者由用户手动地读出的编码和用于用户的特征信息、例如密码或者输入到通信装置中的字母/数字组合提供高度的安全性，所述字母/数字组合借助于通信装置发送到远离锁布置的中央信息处理位置处并且在那里被检查。访问授权不是就地在有待打开的电子锁的区域中而是远离于此地在具有中央单元的信息处理位置中被检查并且颁发。

[0046] 在颁发并且发送授权码之后，该授权码传输给由用户携带的电子钥匙，接着借助于该电子钥匙进行电子锁的解锁。将授权码传输给电子钥匙是另一个有利的安全屏障。对于借助于输入装置手动地将经传输的授权码输入到电子钥匙中备选地，也可以自动地、例如通过借助于蓝牙技术、红外线发射器或者其它的近距离传输方法由通信装置到电子钥匙上的传输来进行授权码的传输。

[0047] 在此，电子锁本身已经可以实现对受保护的区域或者受保护的装置的访问授权。然而，在一种备选的实施方式中，所述受保护的区域由相对小的、布置在建筑物外面或者布置在建筑物附近的防盗窃的容器、例如保险管形成。在该保险管中电子锁在通过电子钥匙打开之后解锁用于物理钥匙的入口，接着可以借助于该入口走进所述建筑物。在此，所述物理钥匙特别有利地与保险管的包含电子锁的锁盖的内侧连接，从而该物理钥匙在离开建筑物之后回转到保险管上并且保险管借助于锁盖强制地进行重新闭锁。

[0048] 按照另一种有利的应用方案，电子锁在进行授权码的检查之后接收由电子钥匙的电气的电压源传递的(可选地通过变压器改变的)电压并且将该电压进一步导向到电马达

锁或者电致动器上(可选地在控制仪中间换挡的情况下)以用于激活所述电马达锁或者电致动器。

[0049] 在一种特别简单的形式中,通信装置由移动电话形成,用户(例如安全服务人员)借助于该移动电话呼唤信息处理位置(例如安全服务的服务中心)并且传输他的名字、锁专用的信息和密码,紧接着信息处理位置检查这些信息,必要时附加地利用在那里备份的使用计划来校准并且在积极地评价所有信息时将授权码传输给用户或者通信装置。授权码可以电话告知用户亦或可以通过由计算机在信息处理位置处生成的短信息告知。

[0050] 用户进一步将授权码通过输入单元提供给由他携带的电子钥匙并且接着可以利用该电子钥匙通过接触或者通过无接触的信号传输、例如通过无线电来操纵电子锁。

[0051] 由这种特别简单的形式出发可以自动化地进行一个或者多个所述步骤。因此例如可以借助于存储在通信装置中的软件("APP")和相应的传感器(例如用作通信装置的智能手机的照相机)自动地读出电子锁的编码。这例如可以借助于存储在智能手机中的条形码阅读程序或者二维码阅读程序来进行,为此,在这些情况中,在电子锁的区域中布置有相应的图形码。然而,在通信装置中其它布置在电子锁的区域中的电子信号传感器和相应地对准该电子锁的传感器同样也是可能的,例如看不见的、磁性编码的信号。

[0052] 授权码也可以作为条形码、QR编码或者以类似的形式传输到用户的智能手机上。所传输的编码接着在该编码以可机读的形式被传输的情况下由通信装置(智能手机)传输到在电子钥匙上的电子输入装置上。

[0053] 对于用户来说独特的信息也可以例如在读入对于电子锁专用的信息之后通过存储在通信装置中的软件自动化地询问并且由用户例如作为字母/数字组合输入并且传输到信息处理位置处。

[0054] 作为其它有利的方法步骤规定,在给用户发送授权码之前信息处理位置除了用于电子锁和/或用户的特征信息之外还检查通过使用计划与两个信息结合的、用于使用位置和/或使用时间的信息。由此,提供了附加的安全性,因为也完全排除了访问编码在安全人员的通常预定的路线之外传输。

[0055] 本发明的另一种有利的设计方案规定,电子锁和/或由该电子锁保护的装置在解锁和在锁闭电子锁时将信息发送到信息处理位置处。

[0056] 该系统的一种有利的改进方案规定,此外,在中央信息处理位置中的检查包括对至少一个时间参量的评价,该时间参量为了锁的预定的打开借助于备份的时间计划(特别是看守人员的路线计划)验证对于锁和/或用户来说独特的信息。

[0057] 在一种特别的设计方案中可以规定,通信装置和电子钥匙形成一个单元。该单元将用于检测并且对中央信息处理位置发送用于锁和/或用户的特征信息并且用于接收授权码的发送器和接收器的所有功能与电子钥匙的功能统一。借助于详细探讨的授权码,电子钥匙、例如磁性的变频器被这样编程,使得该电子钥匙能用于打开电子锁。

[0058] 本发明例如能与保险管(Rohrtresor)结合使用,正如其例如在文献WO 2012/045474 A1中所公开的那样。在此,作为电子钥匙的变频器在安放到电子锁上之后直接用作取出锁盖用的把手。

[0059] 此外,开始时提到的任务通过包括电子钥匙和电子锁的电子锁闭系统来解决,该电子钥匙和电子锁能通过触点组和对应触点组彼此相互作用,其中,电子钥匙具有处理器,

该处理器与输入单元配合作用，通过该输入单元能将外部产生的授权码传输给处理器，其中，所述处理器与存储器配合作用并且将外部产生的授权码写入到存储器中，并且其中，电子锁具有处理器，该处理器在电子钥匙与电子锁相互作用时通过触点组和对应触点组与在电子钥匙中的存储器相互作用，以便读出外部产生的授权码。

[0060] 按照本发明的技术方案的优点已经与按照本发明的方法相联系地进行了阐述，从而在此可以参照相关内容得出。

[0061] 另一个优点在于，因此能够以尽可能最大的安全性使用电子钥匙和电子锁，而只要不存在外部产生的授权码，就不存在单独利用电子钥匙和电子锁打开的可能性。

[0062] 为了提高电子钥匙的安全性，优选地规定，在电子钥匙中的存储器是安全的存储器并且电子钥匙的处理器产生安全码，以用于将外部产生的授权码保存在安全的存储器中。

[0063] 此外，也为了在由安全的存储器读出授权码时确保高的安全水平，优选地规定，电子钥匙的处理器产生安全码，以用于读出保存在安全的存储器中的授权码。

[0064] 此外优选地规定，电子钥匙具有显示元件，以便显示由电子锁传递给电子钥匙的电子锁的状态。

[0065] 在这种情况下，有利地规定，电子锁的处理器对电子钥匙的处理器传输关于电子锁的当前状态的状态信号并且电子锁的处理器按照所传输的状态触发电子钥匙的显示元件。

[0066] 在实现安全的存储器方面，至今还未更详细地说明。

[0067] 因此，一种有利的技术方案规定，安全的存储器是安全处理器的存储器。

[0068] 这样的安全处理器优选是一种仅在传输安全码时才允许访问安全的存储器的处理器。

[0069] 在此，有利地通过哈希算法来确定安全码。

[0070] 原则上，电子锁能够始终利用自身的电压供应来运行。

[0071] 然而，自身的电压供应有如下缺点，即在这种情况下、特别是在电子锁长时间不使用的情况下电压源不再提供充分的电压。

[0072] 基于这种原因，有利地规定，电子锁能通过电子钥匙的电压源来运行。

[0073] 在此，电子锁还可以附加地具有自身的电压源并且仅在自身的电压源不起作用时才通过电子钥匙的电压源来运行。

[0074] 然而特别有利的是，电子锁能始终运行电子钥匙的电压源，因为施加电压也可以用于电子锁的功能的启动。

[0075] 此外，按照本发明的技术方案规定，电子锁包括用于操纵锁闭止动器的锁闭驱动器。

[0076] 因此，在这种情况下，电子锁本身直接能够通过操纵锁闭驱动器触发打开过程或者通过不操纵锁闭驱动器允许闭锁。

[0077] 对于电子锁具有锁闭驱动器的情况，同样优选地规定，电子锁的锁闭驱动器能通过电子钥匙的电压源来运行。

[0078] 在这种情况下，有利地规定，电子锁具有变压器，以用于运行锁闭驱动器，因为，这样的锁闭驱动器通常需要比用于运行在电子钥匙中和在电子锁中的处理器需要的电压更

高的电压。

[0079] 对于在电子锁中布置电气的锁闭驱动器备选地，另一种有利的技术方案规定，电子锁具有切换单元，以便激活或者锁止外部的锁闭系统。

[0080] 在这种情况下，电子锁本身不用于直接触发或者导入锁闭过程或者打开过程，而是电子锁可以用于激活或者锁止外部锁闭系统。

[0081] 因此，存在例如通过使用电子钥匙和电子锁来使用现有的锁闭系统的可能性，然而这些现有的锁闭系统具有不充分的安全级。

[0082] 由此，当电子锁激活或者锁止现有的锁闭系统时，所述现有的锁闭系统可以达到更高的安全级、亦即电子钥匙或者电子锁的安全级。

[0083] 另一种有利的技术方案规定，电子钥匙具有用于借助于中央单元激活电子钥匙的接口。

[0084] 中央单元用于产生外部授权码，从而需要中央单元激活电子钥匙并且因此了解电子钥匙的对于产生授权码所需的数据。

[0085] 此外规定，电子锁具有用于通过中央单元激活电子锁的接口。

[0086] 在这种情况下，在电子锁中也需要激活，以便将电子锁也置于如下的状态中，该状态使电子锁允许该电子锁产生外部授权码。

[0087] 特别优选地规定，电子钥匙或者电子锁的激活通过中央单元导线连接地进行，以便在激活时获得尽可能高的安全性以防数据由第三方接收。

[0088] 带有至少两个用于对电子锁传输数据和/或能量的触点的电子钥匙的一种有利的技术方案设有至少一个在电子钥匙的壳体上布置的、用于输入授权码的输入装置。

[0089] 在此有利的是，输入装置和触点布置在壳体的不同的侧面上。

[0090] 特别有利的是，输入装置布置在正面上而触点布置在壳体的对置的背面上。

[0091] 有利地，电子钥匙配设有至少一个电压。

[0092] 特别是电子钥匙配设有至少一个用于与相应的对应磁铁配合作用地在电子锁上定心的磁铁。

[0093] 此外，电子钥匙的触点弹簧弹性地支承在壳体中。

[0094] 此外，电子锁闭系统包括至少一个电子锁，该电子锁配设有至少两个同心地布置的对应触点和一个磁性的中心孔。

[0095] 在此，特别是对应触点构成为同心的圆，这些对应触点与电子钥匙的触点在电子钥匙的任意相对的角度位置中接触。

[0096] 有利地，电子锁布置在保险管的锁盖上，其中，与电子锁接触的电子钥匙用作操纵锁盖用的把手。

[0097] 例如电子锁连接在有待锁定的装置的马达锁的上游并且激活该马达锁的通电。

[0098] 但是也可设想，在电子锁和马达锁之间布置有控制仪，该控制仪的通电通过在与电子锁接触中的电子钥匙和借助于输入单元输入的授权码所进行的确认来激活。

[0099] 此外，优选地规定，电子锁闭系统的实施方式按照开始时描述的、用于运行锁闭系统的方法工作。

[0100] 本发明特别是允许提供一种电子钥匙，该电子钥匙为了打开最为不同的锁能短时间地并且交替地被激活。

[0101] 在此，特别是按照本发明的电子钥匙有利地与至少一个电子锁配合作用。

[0102] 按照本发明的电子钥匙通过布置在电子钥匙的壳体上的、用于输入授权码的输入单元而突出。

[0103] 在此，所述输入单元能够设计成数字的或者文字数字的键盘的形式，其中在这种情况下，用于期望的解锁的授权码由用户手动地输入。

[0104] 按照本发明的另一种观点，电子钥匙能借助于能通过输入单元输入的、用于打开不同的电子锁的授权码来编程。

[0105] 备选地或者补充地，输入单元也可以由电子检测装置构成。该电子检测装置例如可以由阅读器或者接收器形成，该阅读器或者接收器通过无线电、蓝牙、无线射频识别或者近距离无线通信或者通过光学传输、例如条形码、QR编码或者类似物由用户或者由该用户操作的通信装置(例如智能手机)检测所传输的授权码。

[0106] 授权码优选暂存在电子钥匙的存储器中并且在通过至少一个触点与电子锁接触之后传输给该电子锁。

[0107] 借助于输入单元无需在空间上接近有待打开的电子锁就能单独地输入到电子钥匙中的授权码显著地提高了在鉴定访问授权时的安全性，因为相应的访问数据几乎不可能被未经认可的第三方拦截并且电子钥匙仅利用已完成输入的授权码接近于电子锁。

[0108] 可能被偷窃的或者丢失的电子钥匙对于小偷或者拾得者来说是无用的，因为该电子钥匙不能通过授权码识别有关的钥匙是为哪个电子锁准备的。

[0109] 输入单元和触点优选布置在壳体的不同的侧面上。特别优选地，输入装置布置在壳体的正面上并且触点布置在壳体的背面上。由此，输入装置也能够相当简单地在如下位置中操纵，在该位置中，触点与相应的对应触点在电子锁上作用。

[0110] 特别优选地，电子钥匙配设有至少一个电压源(优选配设有可充电的蓄电池)，该电压源不仅用于电子钥匙的电子组件的自身供应，而且此外至少在打开过程或者初始化或激活过程期间也可以用于电子锁的供电，而在此期间电子锁可以不接通自身的电压供应。

[0111] 优点在于，配设有电子锁的装置不必被永久地供应运行电压，因为仅在需要时由电子钥匙提供用于打开的必需的电流。因此，例如所指定的、在其中寄存有物理钥匙的保险管可以远离电网地、完全没有固定的电流供应但是也没有要交换的电池地运行。由此减低了该系统的维护费用和损耗。

[0112] 银行保险箱(Schließfächer)、贵重物品抽屉(Wertsachenfächer)或者保险柜(Tresore)同样可以无需永久的电压供应地运行，因为用于访问的初始化的电流由电子钥匙提供。在此，电子锁可选地在批准访问授权的鉴定之后首先操纵控制仪，接着借助于该控制仪激活外界的运行电压源以用于操纵马达锁或者其它的致动器。

[0113] 电子钥匙优选配设有至少一个用于与相应的对应磁铁配合作用地在电子锁上定心的磁铁(特别是环形磁铁)。电子钥匙通过有吸引力的磁力在接近于电子锁时自动地达到接触位置中。

[0114] 为了支持可靠的触点形成，在电子钥匙上的触点优选弹簧弹性地支承在该电子钥匙的壳体中。

[0115] 除了电子钥匙之外，电子锁闭系统至少还包括电子锁，该电子锁配设有至少两个同心地布置的对应触点和一个磁性的中心孔。

[0116] 按照电子锁闭系统的一种有利的应用方案，电子锁布置在保险管的锁盖上，其中，电子钥匙在其与电子锁接触的接触位置中同时优选用作操纵锁盖的把手。

[0117] 按照电子锁闭系统的一种备选的应用方案，电子锁连接在马达锁或者有待锁定的装置的致动器的上游并且激活该马达锁或者致动器的通电。由此，如已经提到那样，银行保险箱、贵重物品抽屉或者保险柜可以无需永久的电压供应地运行，因为用于访问的初始化的电流由电子钥匙提供。

[0118] 在此，电子锁可选地在批准访问授权的鉴定之后首先操纵控制器，接着借助于该控制器激活外界的运行电压源以用于操纵马达锁或者其它的致动器。

[0119] 在电子锁上的对应触点面优选构成为同心的圆，这些对应触点与电子钥匙的触点在电子钥匙的任意相对的角度位置中接触。因为需要电子钥匙关于电子锁的完全无旋转的定向，所以电子钥匙在电子锁上的对接即使在能见度条件差时也由用户极其简单地实施。

[0120] 此外，本发明还涉及一种包括管主体和管主体盖的保险管，电子锁布置在该保险管中，以便在管主体盖的嵌入到管主体中的锁闭位置中闭锁或者解锁管主体盖。

[0121] 在此，在管主体中优选保管有钥匙，因为该管主体通常用作钥匙保险箱。

[0122] 为了在此可以以简单的方式获得对钥匙的访问并且另一方面可以以简单的方式将钥匙寄存在管主体中，而无需在将钥匙转移到锁闭位置中时特别地进行利用管主体盖夹紧，根据按照本发明的保险管的一种实施方式规定，在管主体盖上保持有钥匙容纳器，该钥匙容纳器能利用管主体盖导入到管主体中或者由该管主体取出。

[0123] 在此优选地，这样构造钥匙容纳器，从而使得该钥匙容纳器具有容纳钥匙用的容纳室，从而钥匙可以以简单的方式寄存在钥匙容纳器中或者能由该钥匙容纳器取出。

[0124] 此外优选地规定，将钥匙固定在钥匙容纳器上以防其完全远离钥匙容纳器，这确保钥匙在使用该钥匙时不丢失或者不远离钥匙容纳器。

[0125] 另一种有利的技术方案规定，钥匙容纳器的容纳室能通过开口进入，通过该开口能取出钥匙或者能将钥匙插入到该容纳室中。

[0126] 为了确定操作人员将钥匙容纳器寄存在管主体中，亦即在闭锁管主体时这样寄存钥匙容纳器，从而使得管主体的闭锁通过管主体盖进行，优选地规定，能通过传感器来检测钥匙容纳器在管主体中的位置。

[0127] 所述传感器能通过每种类型的传感器形成。

[0128] 特别简单并且可靠的是，传感器是磁场传感器，该磁场传感器识别保持在钥匙容纳器上的磁铁。

[0129] 为了能够以简单的方式评价传感器信号，优选地规定，传感器与传输单元配合作用，该传输单元传输安全中心、例如上面提到的中央单元的管主体盖的锁闭位置。

[0130] 为了完全确保管主体准确地通过管主体盖闭锁，另一种有利的技术方案规定，在管主体上布置有传感器，该传感器检测管主体盖在管主体中的锁闭位置。

[0131] 在这种情况下也优选地规定，管主体盖配设有磁铁，传感器检测该磁铁的位置。

[0132] 所述传感器优选也与上面已经阐述的传输单元配合作用，以便将保险管的闭锁传输给安全中心或者开始时提到的中央单元。

附图说明

[0133] 本发明的其他特征和优点是以下描述以及若干实施例的所绘制的示图的主题。

[0134] 在附图中示出：

[0135] 图1是按照本发明的锁闭系统的第一实施例的电子钥匙和电子锁的示意图；

[0136] 图2是利用电子锁闭系统的中央单元激活电子钥匙和电子锁的示意图；

[0137] 图3是产生和传输外部授权码的可能性的示意图；

[0138] 图4是在没有安放电子钥匙的情况下保险管的第一实施例的透视的正视图；

[0139] 图5是在有安放的电子钥匙的情况下保险管沿着图4中的线5-5的剖面图；

[0140] 图6是按照图4所示的保险管在该保险管打开时的透视图；

[0141] 图7是按照本发明的锁闭系统的第二实施例的类似于图1的示意图；

[0142] 图8是带有集成到锁盖中的电子锁和对于电子锁来说独特的编码的保险管的另一实施例；

[0143] 图9是一流程图，该流程图说明了编码在用户和中央信息处理位置之间的传输；

[0144] 图10是在将授权码输入到电子钥匙中时用户的手；

[0145] 图11是在打开电子锁时电子钥匙作为把手的使用；

[0146] 图12是物理钥匙在保险管的锁盖的内侧上的布置；

[0147] 图13是一流程图，该流程图说明了在用户、客户计算机、服务器、管理员和电子锁之间的通信；

[0148] 图14是一简图，该简图说了在用户、客户计算机、服务器和管理员方面的功能；

[0149] 图15是用于电子锁与控制仪和马达锁配合作用地使用的示意的接线图；

[0150] 图16是电子钥匙的示意性的正视图；以及

[0151] 图17是电子钥匙的后侧的示意图。

具体实施方式

[0152] 在图1中示出的按照本发明的、整体上以附图标记10标识的电子锁闭系统10的第一实施例包括电子钥匙12以及电子锁14。

[0153] 电子钥匙12在此具有特别的弹簧触点组成的触点组16，该触点组与具有特别是同心的触环的对应触点组18能通过由将触点组16接入到对应触点组18上形成的电流连接而有效连接。

[0154] 于是，基于在电子钥匙12和电子锁14之间的电气的相互作用能够借助于电子钥匙12操纵锁闭止动器22，这意味着，锁闭止动器例如由锁闭位置运动到打开位置中或者必要时也相反地运动。

[0155] 电子钥匙12为此包括电压源32、例如电池形式的电压源，该电压源对处理器34供应电流和电压。

[0156] 处理器34能够与输入单元36和安全处理器38相互作用，该安全处理器配设有安全的存储器39。

[0157] 在安全的存储器39中不仅存储识别码ICK和钥匙12的配置密码，而且在该安全的存储器中也可以由处理器34保存外部产生的授权码BCZ。

[0158] 处理器34还配设有接口42，该接口用于激活和/或配置处理器34。

[0159] 此外，数据线44由处理器34导向至存储器39并且进一步导向至触点组16的数据触点46。

[0160] 接地线48由电压源32一方面直接导向至处理器34并且另一方面直接导线至触点组16的接地触点52。

[0161] 处理器34能够通过切换单元54激活由电压源32导向至触点组16的供应触点56的供应导线58。

[0162] 在电子钥匙12的触点组16与电子锁14的对应触点组18相互作用时，接地触点52触碰特别是构造为触环的接地对应触点62并且供应触点56触碰特别是构造为触环的供应对应触点66。因此，布置在电子锁14中的处理器72能通过电子钥匙12激活并且能利用电子钥匙12的电压源32运行，而电子锁14为此不需要单独的电压源。

[0163] 此外，在这种情况下，触点组16的数据触点46也触碰对应触点组18的特别是构成为触环的对应数据触点68，该对应数据触点本身通过数据线74与处理器72连接。

[0164] 此外，电子锁14的识别码ICL以及接收配置密码的EEPROM形式的存储器76、时钟78和锁闭驱动器82还与处理器72耦合。

[0165] 此外，处理器72的激活和/或配置可以通过与处理器耦合的接口84进行。

[0166] 处理器72本身利用电压源32的电压运行，在锁闭驱动器82同样要通过电压源32运行的情况下，优选在电子锁14中布置有变压器86，该变压器将由电压源32提供的电压转换成例如用于运行锁闭驱动器的更高的电压。

[0167] 附加地，处理器72还配设有记录存储器88，在该记录存储器中记录并且保存电子锁14的处理器72的激活。

[0168] 按照本发明的锁闭系统10现在如下地工作：

[0169] 通过输入单元36将外部生成的授权码BCZ传输给电子钥匙12，处理器34将该授权码存放在安全处理器38的安全的存储器39中。

[0170] 为此，由处理器34计算哈希码形式的安全码SC并且传输给具有授权码BCZ的安全码38。

[0171] 此外，处理器34通过切换单元54激活供应触点56，从而该供应触点处于电压源32的供应电压上。

[0172] 如果在电子钥匙12的触点组16和电子锁14的对应触点组18之间建立连接，则仅由于在供应对应触点66上存在供应电压并且在接地对应触点62上存在接地线，电子锁14的处理器72通过复位来提高功率并且这时开始通过数据线74与数据线44的连接而与安全处理器38通信。

[0173] 然而，在读出安全处理器38的安全的存储器39的内容之前进行检查，检查安全处理器38本身是否被授权与处理器72交换数据，例如通过如下方式，即，检查在存储器76中包含的编目是否记录安全处理器38。

[0174] 此后，通过处理器72进行哈希码形式的安全码SC的计算并且在使用安全码SC的情况下进行安全的存储器39的读出，该安全的存储器包括授权码BCZ。

[0175] 在此，特别是在没有激活电子钥匙12的处理器34的情况下进行存储器39的读出。

[0176] 在读出授权码BCZ之后，处理器72基于利用自身的授权码确定程序BCEPS确定的自身的授权码BCS和将授权码BCZ与授权码BCS鉴于其相同性来比较的授权码检查程序BCUP检

查授权码BCZ,并且在授权码BCZ和BCS之一的情况下规定电子锁14的打开。

[0177] 在授权码BCZ和BCS相同时,在第一实施例中的处理器72激活锁闭驱动器82并且该处理器使锁闭止动器22例如由该锁闭止动器的锁闭位置运动到锁闭止动器的打开位置中,从而电子锁14接着解锁例如对安全单元的访问。

[0178] 处理器72同时通过读出钟表78来建立记录,该记录保留了对锁14的访问、由存储器38读出通道数据组ZD和记录驱动器82的激活,其中,所述记录接着存放在记录存储器88中。

[0179] 电子锁14的、应由处理器72确定并且对用户显示的所有状态优选不是由电子锁14显示,而是通过数据线74和数据线44传递给电子钥匙12的处理器34,该处理器然后本身激活一个或者多个光学的显示单元92、94、例如LED灯或者显示器或者例如蜂鸣器的声学信号传感器,或者该处理器生成通过扬声器传输的曲调。

[0180] 为了获得电子钥匙12和电子锁14的规定的功能,电子钥匙12和电子锁14通过中央单元102导线连接地激活,该中央单元本身可以通过接口104访问电子钥匙12的接口42并且同时亦或依次或者相应地单独访问电子锁14的接口84,以便激活电子钥匙12或电子锁14,其中,特别是在中央单元102和电子钥匙12以及电子锁14之间校准或者交换、亦即要么传递要么读出配置密码和/或相应的识别码ICK以及相应的识别码ICL以及循环计数器ZCZ和ZCS的循环状态ZZ。

[0181] 在这样激活电子钥匙12和电子锁14之后,可以分离在接口42和104以及84和106之间的相应的连接,并且中央单元102能够借助于存在于中央单元102中的授权码确定程序BCEPZ借助于哈希算法确定相应的一次性的外部授权码BCZ,该外部授权码然后可以通过输入单元36例如由用户输入到电子钥匙12上,对此,电子钥匙12的处理器34接着能够将授权码BCZ存放在安全的存储器39中。

[0182] 此外,电子锁14于是能够如描述的那样在与电子钥匙12相互作用之后读出外部授权码并且同样通过授权码确定程序BCEPS在考虑识别码ICS的识别码ICK、自身的循环计数器ZCS的循环状态ZZ的情况下借助于该授权码确定程序的哈希算法如在中央单元102中那样确定自身的授权码BCS并且检查该授权码是否与外部授权码BCZ相同并且是否允许打开锁闭止动器22。

[0183] 如在图3中示出的那样,按照本发明的锁闭装置10例如如下地在区域中使用,即,操作人员可以在区域中静止地布置的锁14中利用电子钥匙12中通过下列方式开始打开锁14。

[0184] 想要打开在区域中静止地布置的锁14的操作人员要求由中央单元102例如通过移动的通信单元112、特别是可携带的手机或者另一种通信仪器传输外部授权码BCZ。

[0185] 对此,从中央单元102方面来说可以进行大量参数的检查或者大量参数的调查,这些检查或者调查必须在获得授权码BCZ之前完成。

[0186] 这样的数据例如是锁14的局部编码LC,和/或操作人员的个人编码PC和/或在操作人员的地点处的时间参数ZA和/或操作元件的地点参数OA。

[0187] 所有这些信息可以由中央单元102检查。在积极地取消检查所有的信息和参数的情况下,中央单元102生成外部授权码BCZ,因为中央单元102可以由局部编码LC和/或个人编码PC和/或时间参数和/或地点参数OA推断出识别码ICK和ICL并且因此在使用要用于打

开的电子钥匙12的已知的识别码ICK和要打开的电子锁14的识别码ICL以及循环计数器ZCZ的循环状态ZZ的情况下借助于识别码确定程序BCEPZ借助于哈希算法传输外部授权码BCZ确定外部授权码BCZ，该外部授权码例如声学地或者作为情报或者作为数据组例如通过移动的通信单元112传输给操作人员。

[0188] 于是，进行授权码BCZ由操作人员或者由移动的通信单元112通过输入单元36向电子钥匙12的传输。

[0189] 授权码BCZ尤其仅仅是对一次性打开电子锁14授权的授权码BCZ。

[0190] 于是，电子钥匙12将该授权码BCZ借助于处理器34存放在存储器39中。

[0191] 如果现在触点组16与对应触点组18连接，则如已经描述的那样激活电子锁14的处理器72，并且如已经描述的那样由电子钥匙12读出授权码BCZ。

[0192] 通过授权码BCS借助于授权码的授权码确定程序BCEPS在使用由安全的存储器39读出的电子钥匙12的识别码ICK、在存储器76中存放的电子锁14的识别码ICK和电子锁14的循环计数器ZCS的循环状态ZZ的自身的授权并且通过借助于授权码的授权码检查程序BCUP检查授权码BCZ与授权码BCS的相同性，处理器72在此能够确定外部授权码BCZ是否对锁闭止动器22的随后的打开授权，并且当这是在授权码相同时的情况时，锁闭驱动器82被激活以用于操纵锁闭止动器22。

[0193] 不过，在一次性打开电子锁14之后，用于一次性打开电子锁14的授权码BCZ被消耗并且不可以再用于相同的电子锁的打开。

[0194] 因此，即使接近数据组ZD保持保存在电子钥匙12中，也得出电子锁14的处理器72的再次激活和授权码BCZ的检查，该授权码对再次打开电子锁14授权。

[0195] 在中央单元102中可以由人员进行通过移动的通信单元传输的、关于局部编码和/或个人编码和/或时间参数和/或地点参数的信息的检查，该检查例如检测操作人员在区域中的激活并且能够判断这些信息是否恒定。

[0196] 但是也可能的是，通过中央单元102程序控制地实施检查。

[0197] 然而，在中央单元102中的授权码BCZ的确定通过一个所述授权码确定程序BCEPZ进行，该授权码确定程序考虑所有的或者仅一部分所述信息以用于确定授权码BCZ。

[0198] 在此，可看出按照本发明的锁闭系统的优点在于，电子锁14本身不需要电压源，而是可以任意长时间地不使用，因为用于激活电子锁的处理器72和用于运行电子锁的处理器72的所有电流供应通过电子钥匙的电压源32进行，该电压源由操作人员携带并且因此可以始终由操作人员再充电或者更新。

[0199] 此外，由于电子钥匙12和从属于其的电子锁14通过中央单元102的激活而存在在电子钥匙12和电子锁14以及中央单元102之间的明确的关联并且因此存在在对于确定的电子锁14布置用于打开该电子锁的电子钥匙12和同样相应地关联的中央单元102之间的明确的关联，该关联基于电子钥匙12、电子锁14和中央单元102在授权授权码BCZ时的关联。

[0200] 因此，在激活一个或者多个电子钥匙12和一个或者多个对于所述电子钥匙12布置的电子锁14时，能够通过交换密码、交换或者检查识别码ICK和ICS以及校准循环计数器来提供原始条件，利用这些原始条件，授权码确定程序BCEPS和BCEPK相互独立地确定相同的授权码BCZ和BCS。

[0201] 这样的电子锁闭装置例如能够在整体上以附图标记202标识的保险管中使用，该

保险管具有局部固定地安装的管主体204，包括电子锁14的管主体盖206能嵌入到该管主体中并且能利用管主体204闭锁。

[0202] 在此，管主体盖206在其处于外部的正面208上支承电子锁14的具有触环62、66、68的对应触点单元18。

[0203] 此外，管主体204配设有局部编码LC，该局部编码允许在相应的确定的地点处识别确定的保险管202。

[0204] 正如在图5中示出的那样，管主体盖用作容纳电子锁14用的壳体，其中，在管主体盖206中也布置有锁闭驱动器82和锁闭止动器22，从而锁闭止动器22例如可以嵌入到在管主体204的内侧214上的锁闭止动器容纳部212中，以便将管主体盖206固定在管主体盖的在图5中示出的锁闭位置中。

[0205] 因为这样的保险管202经常用于可靠地保留入口钥匙，所以钥匙容纳器222还在管主体盖206上保持、例如固定地装配或者可拆卸地保持，该钥匙容纳器具有用于钥匙226的容纳室224，其中，钥匙226例如也还通过保持带228固定在容纳室224中，从而钥匙226虽然可以由容纳室224取出，然而不可以与钥匙容纳器222分离。

[0206] 这样的钥匙容纳器222具有很大的优点，即，所述钥匙容纳器提供如下可能性，即，将钥匙226这样布置在管主体盖206上，使得钥匙与管主体盖206可以在钥匙不可以在管主体204中夹紧或者在管主体204和管主体盖206之间夹紧的情况下以简单的方式导入到管主体204中并且可以通过闭锁管主体盖206可靠地固定。

[0207] 此外，钥匙容纳器222也还提供如下可能性，即，例如在将管主体206安装在潮湿的环境中时在管主体204中烘干和/或无污染地存放钥匙226，从而例如可以在保存钥匙期间将进入到管主体204中的污染物与钥匙226远离。

[0208] 如在图5和图6中示出的那样，按照本发明的电子钥匙12布置在壳体232中，该壳体具有能安放到管主体盖206的正面208上的背面234，该背面具有用于在管主体盖206的正面208上接触对应触点组18的触点组16，并且另一方面在其与背面234对置的正面236上支承输入单元36'，该输入单元在所述情况中构造为键盘或者触摸屏并且用于输入授权码BCZ。

[0209] 为了将电子钥匙12的壳体232可拆卸地固定在管主体盖2046上布置有磁铁连接部238，该磁铁连接部要么包括两个磁铁M1、M2要么包括磁铁M1和能由该磁铁磁化的元件。

[0210] 在此，磁铁连接部不仅用于将电子钥匙12可拆卸地固定在电子锁上，而且也用于将触点组16相对于对应触点组18定心地定向。

[0211] 在壳体232和管主体盖206之间的磁性耦合能够在电子锁14与电子钥匙12的壳体232解锁时将管主体盖206由管主体206通过由管主体204拉出管主体盖206来取出，该管主体盖是用于电子锁14的壳体。

[0212] 此外，为了能够对于局部的显示来说实现，管主体盖206可靠地位于管主体204中，而存在如下可能性，即，例如在钥匙容纳器222上布置有磁铁242，该磁铁在管主体内部的位置通过布置在管主体上的、关于其位置的磁场传感器244在管主体204中探测并且由此确定钥匙容纳器222和管主体盖206是否在此优选地也接着以如下位置布置在管主体204中，在该位置中，管主体盖206通过例如由弹性的蓄能器24加载的锁闭止动器22闭锁。

[0213] 如果管主体盖206的位置在此方面同样被检测，则也存在如下可能性，即，在管主体盖206中布置由磁铁246并且该磁铁的位置通过同样布置在管主体204上的磁场传感器

248来检测，从而存在如下可能性，即，不仅检测钥匙容纳器222的正确的位置而且检测管主体盖206在其锁闭位置中的正确的位置并且例如传输单元252要么无线地要么有线连接地传输给安全中心亦或中心单元102。

[0214] 在按照本发明的锁闭装置10的、在图7中示出的第二实施例中，所有与第一实施例的部件相同的部件配设有相同的附图标记，从而在这些部件的说明方面可以内容完整地参照第一实施例。

[0215] 不过，与第一实施例相反，电子钥匙14'并非配设有锁闭驱动器82，而是配设有切换单元262，该切换单元能够建立或者中断在电子锁14'的外部的端口264和266之间的连接，从而通过外部的端口264和266存在如下可能性，即，激活或者锁止存在的锁闭系统268。

[0216] 外部的端口266和264例如可以用于中断向已经存在的锁闭系统268的电流输送并且因此时锁闭系统无效或者建立向该锁闭系统的电流输送并且因此激活已经存在的锁闭系统268。

[0217] 在此，存在的锁闭系统268可以是任意构建的锁闭系统，该锁闭系统例如已经存在于壳体中并且是完全安装的，从而按照本发明的锁闭系统10'仅用于使锁闭系统268完全无效或者激活该锁闭系统。

[0218] 因此，已经存在的锁闭系统268可以利用按照本发明的锁闭系统10'固定，而不是必须完全卸载存在的锁闭系统268并且安装新的锁闭系统，该已经存在的锁闭系统具有较小的安全水平，该按照本发明的锁闭系统具有相当高的安全水平。

[0219] 在图8中示出的闭锁设备310由保险管312形成，该保险管以防盗和防破坏的方式布置在建筑物的墙壁中或布置在建筑物附近的稳固的支承件上。保险管312借助于锁盖314在其正面上闭锁。在锁盖314中集成有电子锁316，该电子锁例如详细地在WO 2012/045474 A1中示出并且描述，其公开内容在此用于本申请的主题。

[0220] 在锁盖314的内侧上(如在图12中示出的那样)布置有物理钥匙318，借助于所述物理钥匙可以打开至未示出的建筑物的至少一个入口和可选的在所述建筑物中的其他门。

[0221] 在借助于例如符合第一实施例的电子锁的电子锁316封锁的锁闭设备10上布置有电子锁316的特征编码320。特征编码在示出的实施例中以条形码320的形式构造，然而也可以由二维码或不可见的磁性码形成。编码320在最简单的情况下由用户320人工读出。按照一种有利的设计方案，由用户322携带的通信装置324具有传感器或读取装置以用于自动检测编码320。通信装置324例如可以由智能电话形成，所述智能电话的照相机与存储的应用程序(“App”)相结合地用于读入条形码或备选地读入二维码，所述条形码或二维码在该实施例中用作电子锁316用的特征编码320。如已经提及的那样，不可见的磁性的或通过无线电信号传输的编码320也可以由电子锁316或在其附近布置的装置发出并且由通信装置324接收或读出。

[0222] 只要将匹配于电子锁316的授权码336输入到电子钥匙332中，所述电子锁316能够借助于电子钥匙332打开。在图10中示出，授权码336如何由用户322通过布置在电子钥匙332上的键盘输入。接着，能够如在图11中示出的那样将电子钥匙332安放到电子锁316上并且直接作为把手以用于打开锁盖314。

[0223] 然而，按照本发明，在该过程之前发生在图9、图13和图14中示出的过程步骤，其中，用户322将电子锁316的特征信息(编码320)和其个人的特征信息以编码326的形式(例

如以个人密码或字母/数字组合的形式)借助于通信装置324传输给中央数据处理位置330，例如安全服务中心。电子锁316的特征信息320和用户322的个人特征信息326共同形成询问数据组334，所述询问数据组在最简单的情况下人工地通过电话传输给中央数据处理位置330。

[0224] 按照本发明的一种有利的设计方案，询问数据组334的传输自动地进行，例如作为由通信装置324发送的短消息(SMS)中的字符串。

[0225] 在信息处理位置330中，优选在附加地利用时间参量328(例如用户322的服务计划或路线计划)校准的条件下检验询问数据组334连同包含在其中的编码320和326。只要所述检验得出积极的结果，那么信息处理位置330将授权码336发送给通信装置324。这在最简单的情况下又能够通过电话进行。

[0226] 按照一种有利的改进方案，自动地进行将授权码336传输给通信装置324，例如以嵌入到短消息(SMS)中的字符串的形式。

[0227] 授权码336由用户如已经结合图10提及的那样要么通过输入装置、尤其是键盘手动地传输到电子钥匙332上，要么将授权码336自动地从通信装置324传输到电子钥匙332上。所述传输能够通过如下方式进行：通信装置324具有发送器并且电子钥匙332具有与所述发送器通信的接收器。传输例如能够通过红外信号、通过蓝牙或其他适当的近距离传输协议来进行。

[0228] 按照本发明的一种改进方案，通信装置324和电子钥匙332也能够形成结构单元，所述结构单元具有用于检测编码320的传感器、用于编码326的输入装置、用于将询问数据组334传递到中央信息处理位置330上的发送装置、用于接收授权编码336的接收器和用于将授权编码336存储在电子钥匙232中的存储器。结构单元也包含用于检测编码320和326、用于自动传输询问数据组334、用于自动接收并且用于存储授权码336的软件。

[0229] 中央信息处理位置330有利地具有至少一个客户计算机310和至少一个服务器3320。客户计算机3310用于接收询问数据组34并且用于将所述询问数据组传输给服务器3320。客户计算机3310和服务器3320之间的数据交换在图中用3315表示。

[0230] 在服务器3320中附加地存储时间参量328，所述时间参量例如以打开相关的电子锁316的特征性的时间优选以相应的时间缓冲(最早的打开时间，最晚的打开时间，最晚的锁闭时间)绘制用户322的路线计划。服务器3320中的所有数据由管理者3330管理。服务器3320和管理者3330之间的数据交流在图中用3325表示。

[0231] 优选也将下述信号传输给服务器3320，所述信号在打开和锁闭电子锁316时由安装在电子锁316上的发送器自动发送。

[0232] 按照本发明的方法和按照本发明的系统也能够与图9、图13和图14中的示图相反地在一种改进的实施方式中全自动地在没有人相互作用的情况下作用。通过客户计算机3310接收询问数据组334、将询问数据组334传输给服务器3320、检验包含在询问数据组334中的特征信息(编码320和326)、用至少一个时间参量328校准、生成授权码336和必要时又在客户计算机3310中间换挡的情况下将授权码336传输给通信装置324优选能够借助于软件可控地全自动地进行。

[0233] 已经结合通信装置324的和电子钥匙332的可能的实施方式描述了，按照本发明的用于安全地解除访问授权和/或用于安全地交付钥匙的方法和系统也能够在用户322侧全

自动地进行。

[0234] 电子钥匙332按照本发明配设有输入装置333，借助于所述输入装置，用户322能够将由中央信息处理位置330传输给通信装置324的授权码336输入到电子钥匙中。这种配设有输入装置333的电子钥匙332通常也能够用在当今已经广泛发展的固定的输入装置的位置上，在所述输入装置中，由授权用户输入编码能够由未经授权的观察者相对容易地看到并且由此表现出大的安全风险。相反地，将编码输入到随后为了打开电子锁才使用的移动电子钥匙332中，能够完全未被观察地已经在一定地远离电子锁316时进行。

[0235] 作为电子钥匙332，如在示出的实施例中那样能够使用安放到电子锁316上的、优选通过磁力暂时与电子锁316连接的钥匙332。磁力通过电子钥匙332的中央区域中的磁铁3329并且通过电子锁316的中央区域中的配合磁铁3161提供，所述磁铁和配合磁铁优选构成为永久环形磁铁并且负责电子钥匙332与电子锁316的自动定心以及接触部3324、3325和3326与在电子锁316上同心布置的配合接触面3164、3165、3166的与相互间相对角度无关的对准。

[0236] 然而，同样能够使用无接触地通过一定间距与电子锁316配合作用的电子钥匙332，例如以变频器的形式的电子钥匙。

[0237] 电子钥匙332具有壳体3321，在所述壳体的正面上根据图10和16布置有输入装置333。在示出的实施例中，这是数字键盘，所述数字键盘具有十个数字键3331、删除键3332(“C”)和输入键3333(“OK”)。在壳体3321的背侧上露出三个弹簧弹性地安装在壳体中的接触部3324、3325和3326，其中布置在中央的接触部3325例如引导正电压，位于最远的接触部3324为接地连接并且接触部3326用于串行的数据传输。

[0238] 在根据图17的电子钥匙332的后视图中，也示出电池盒3327的盖，在所述盖之后布置有蓄电池3322。所述蓄电池例如构造为具有输出电压的锂离子蓄电池。

[0239] 电子钥匙332此外设有至少一个接口328，所述接口在当前情况下例如由微型USB接口形成并且用于对电子钥匙332编程并且可选地也用于对蓄电池3322充电。

[0240] 电子钥匙332或者与在图8至图13中示出的例如在保险管312上或在受保护的空间上的电子锁316或者与其他的、要求访问授权的装置配合作用。术语“装置”在此视为非常宽。通过电子锁316能够保护机器、车辆等，但是也能够保护银行保险箱、保险柜、保险箱或至安全区域的门。

[0241] 根据图15的实施例示出，由电子锁316保护的装置也能够不仅直接地、而且也间接地解锁。在该情况下，电子锁316用作为220V保护模块以用于没有示出的受保护的装置，所述装置最终才通过操作马达锁340来解锁。

[0242] 在电子锁316和马达锁340之间，在该情况下还布置有控制仪50，所述控制仪能够借助于自身的电压供应来供应，所述电压供应然而仅通过操作电子锁316激活。在将有效的授权码336从在图15中没有示出的电子锁332通过负责用于数据传输的配合接触部3166传输之后，激活控制设备350上的外部电压源并且操纵马达锁350。对控制设备350的详细描述在说明书结尾时进行。

[0243] 间接操作的优点在于，在没有使用受保护装置时，不必也在所述装置上施加运行电压。所述装置能够通过电子钥匙332通过电子锁316在需要时在任何时刻初始化。

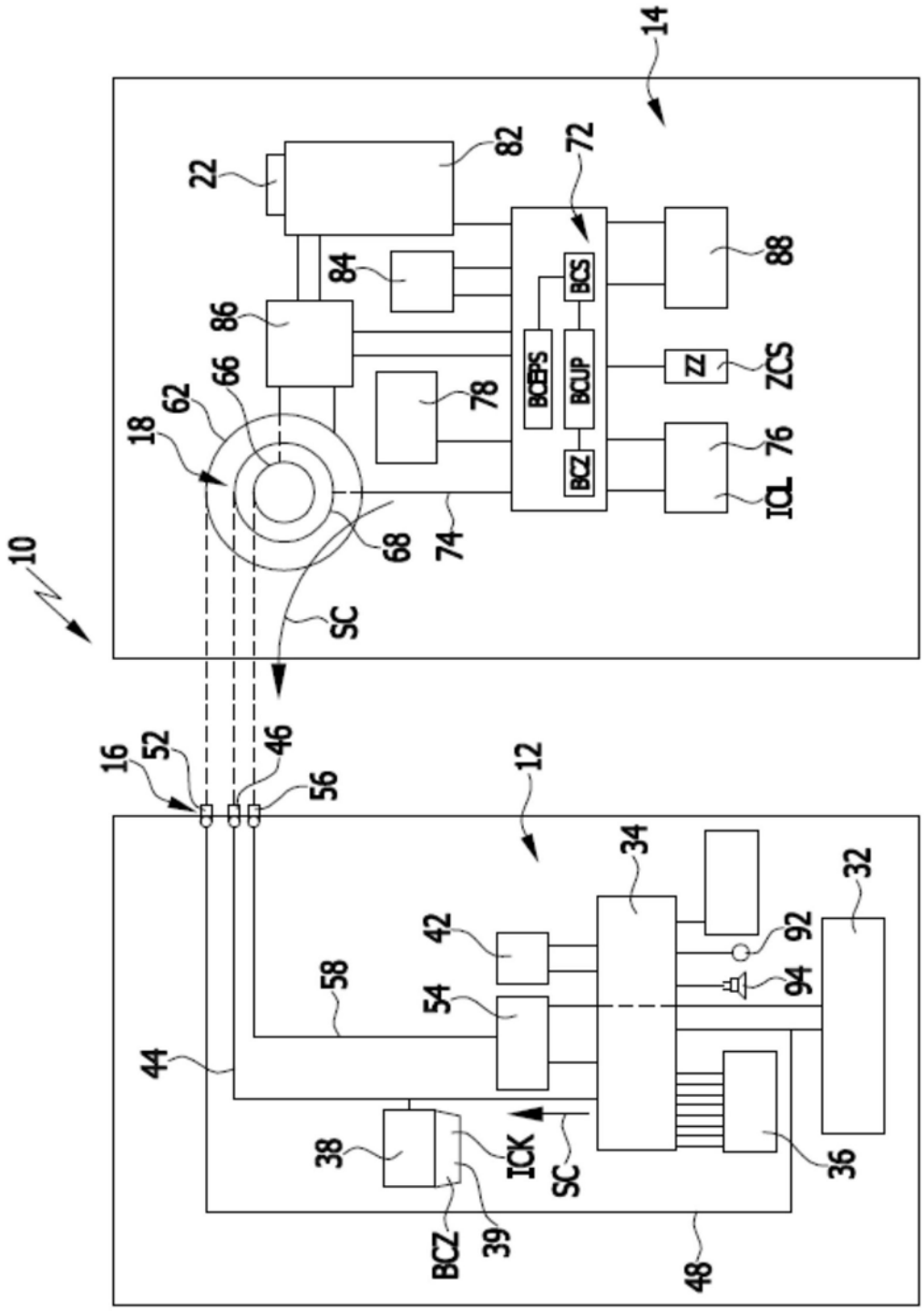

14
22
82
72
84
88
86
BCS
BCBPS
BCUP
ZZ
ZCS
66
62
78
18
BCZ
76
IQL
68
74
10
SC
16
52
46
56
12
34
32
42
92
94
58
54
44
38
ICK
SC
36
BCZ
39
48

图1

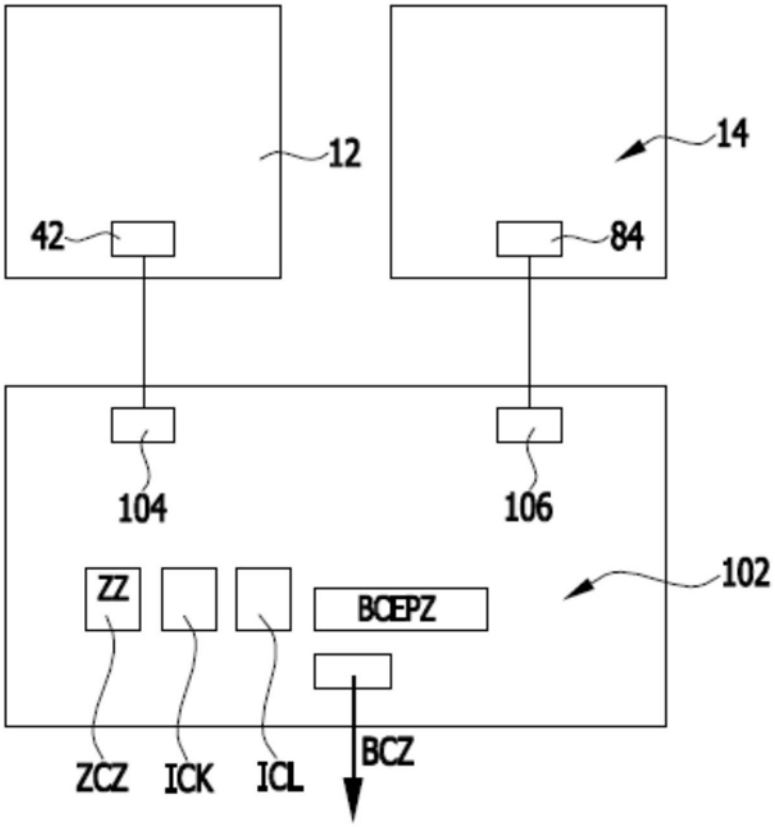


图2

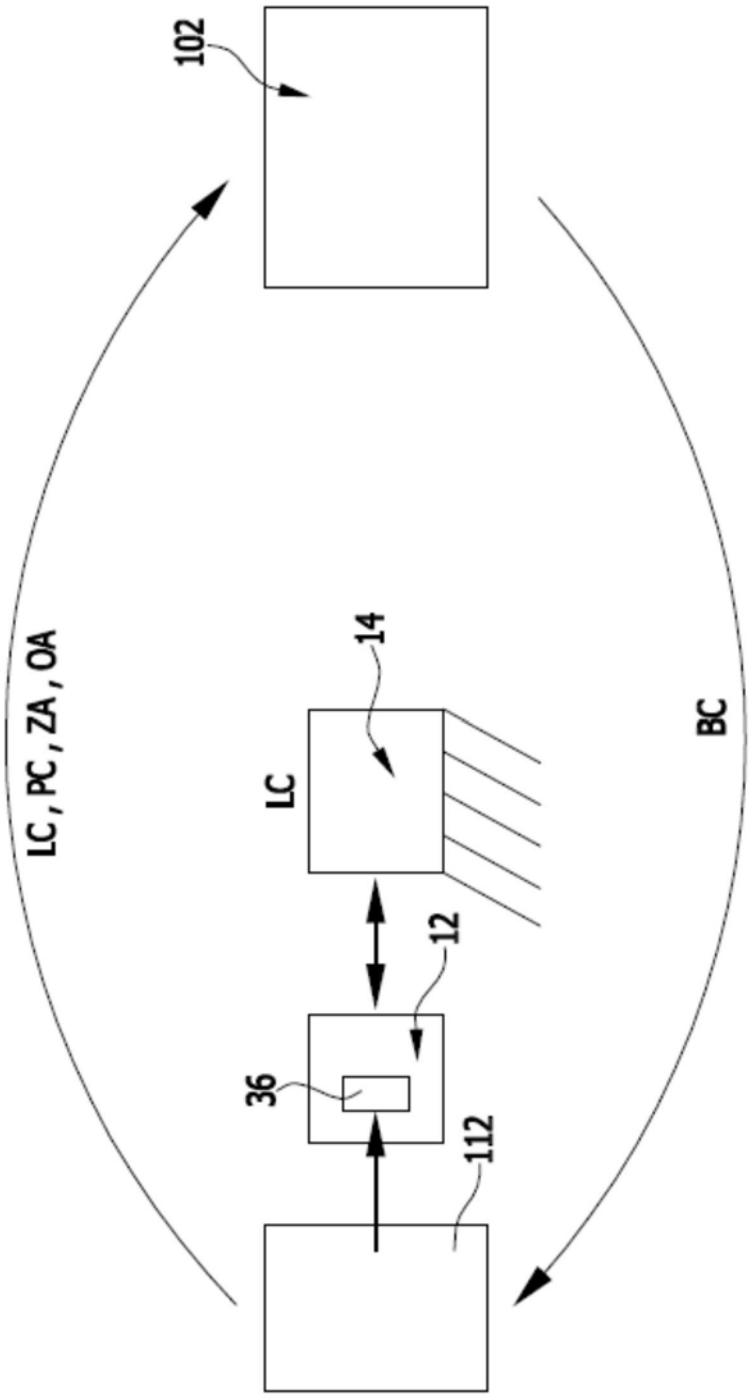


图3

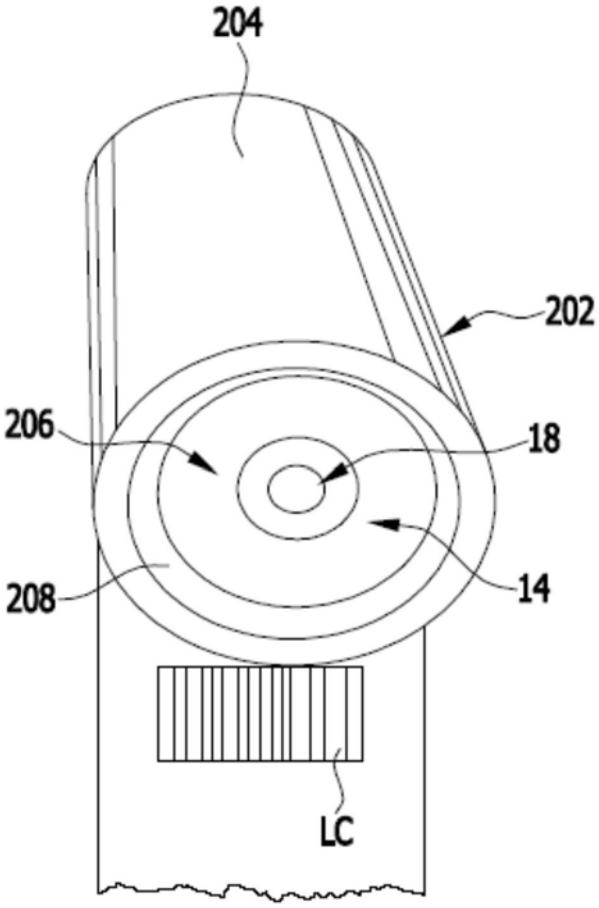


图4

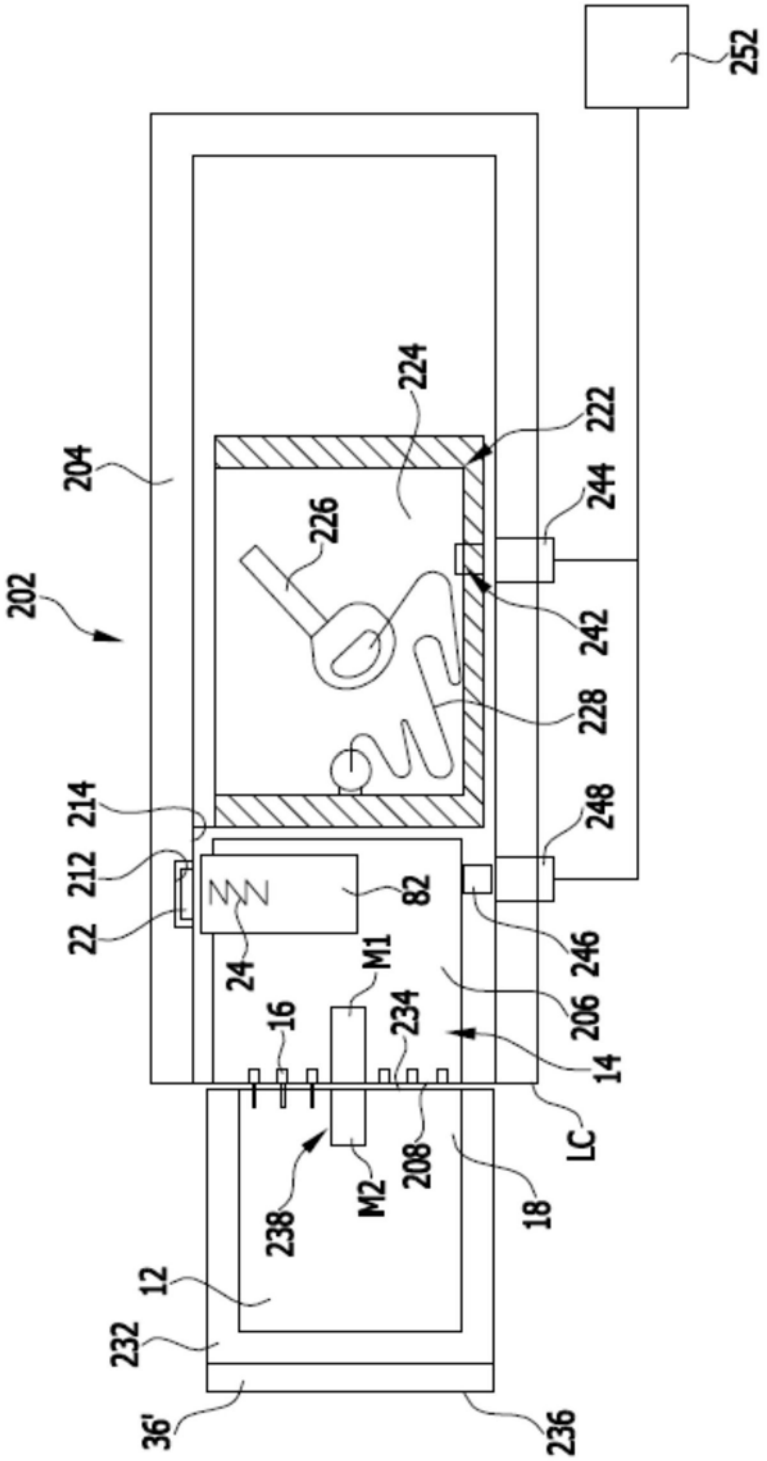

252
224
222
204
244
226
202
242
228
214
248
212
82
22
246
24
M1
206
16
234
14
LC
208
M2
18
238
12
232
36'
236

图5

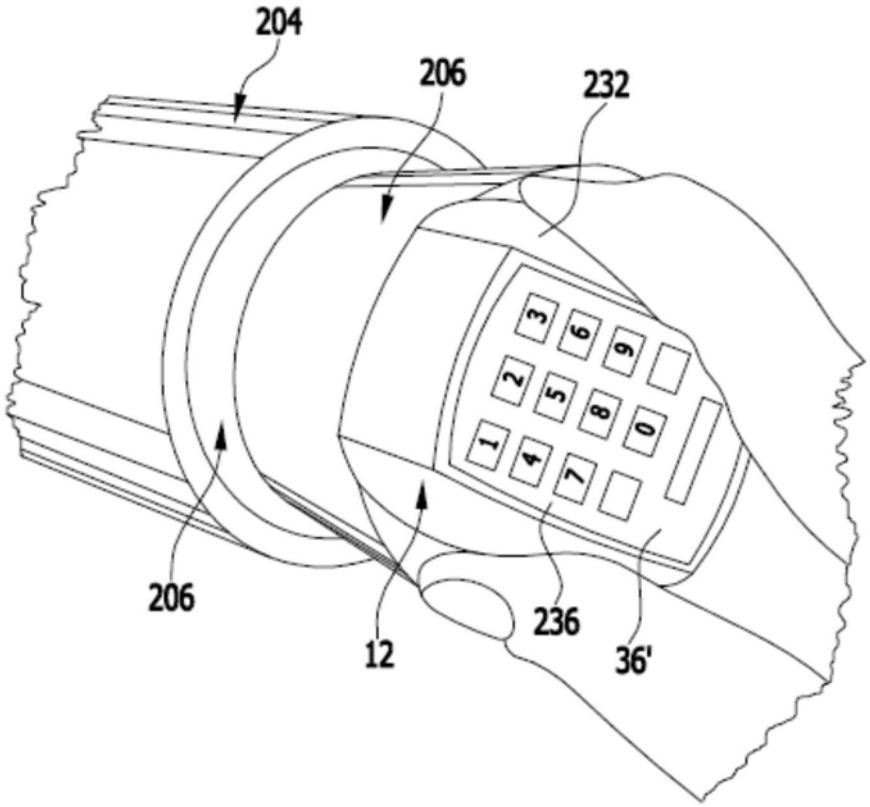


图6

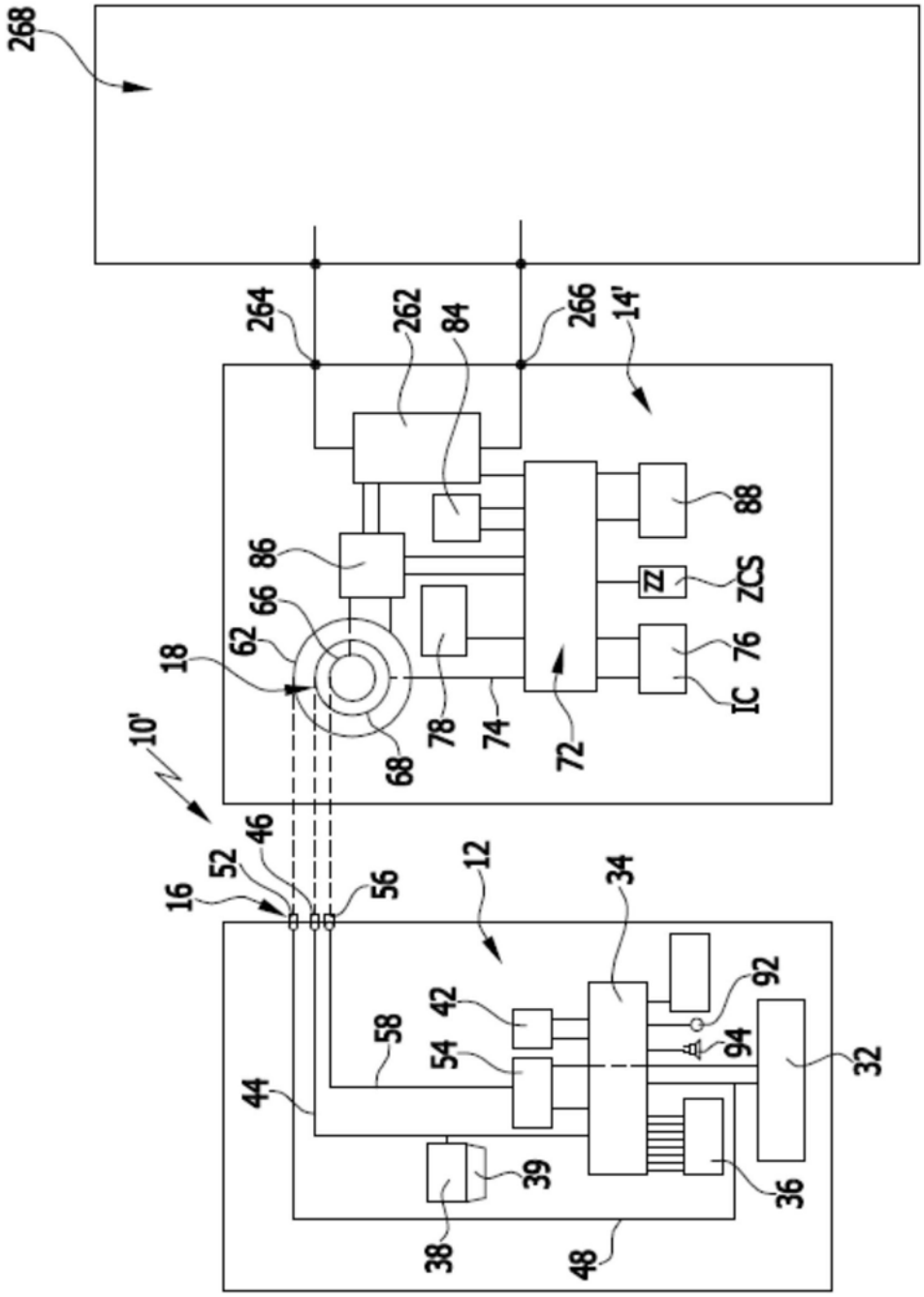

268
264
262
84
266
14'
88
86
ZZ
ZCS
66
62
76
18
IC
10'
78
74
72
68
46
52
16
56
12
34
92
42
58
54
94
32
44
39
36
38
48

图7

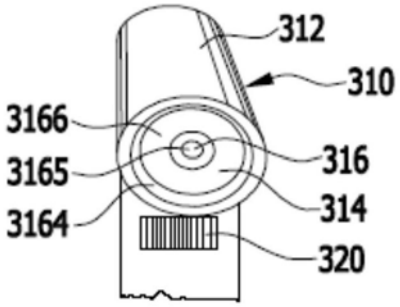

312
310
3166
316
3165
314
3164
320

图8

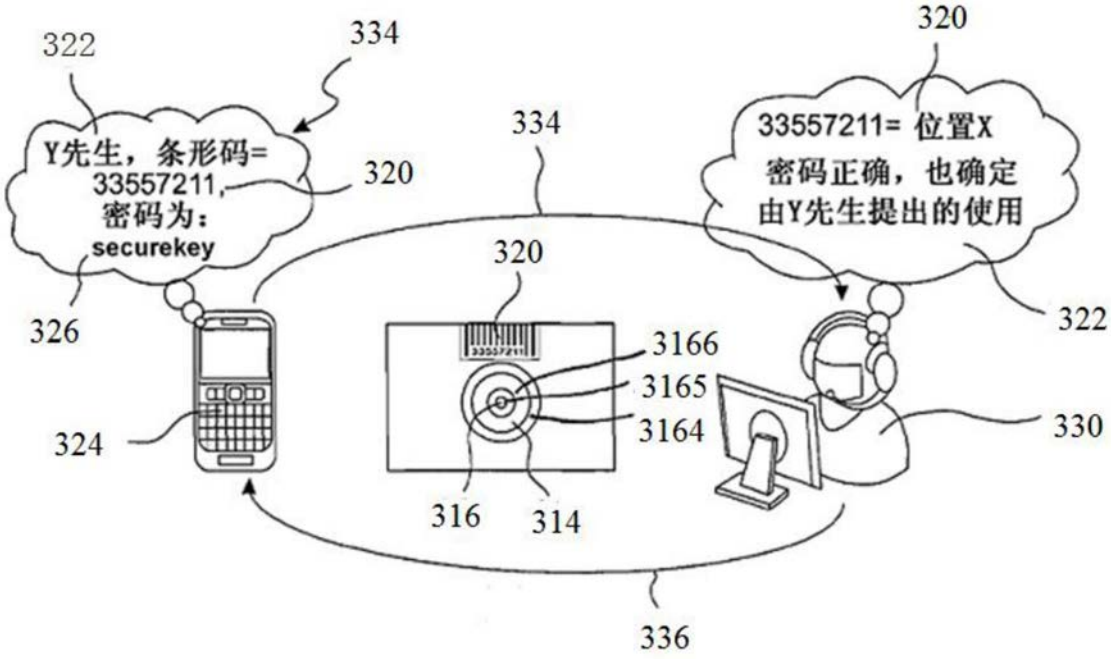

322
334
Y先生，条形码=
33557211，
密码为：
securekey
320
334
320
33557211= 位置X
密码正确，也确定
由Y先生提出的使用
322
326
320
3166
3165
3164
330
324
316
314
336

图9

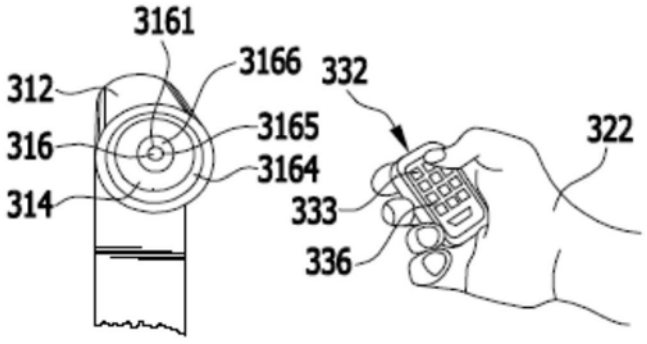

3161
3166
332
312
3165
322
316
3164
314
333
336

图10

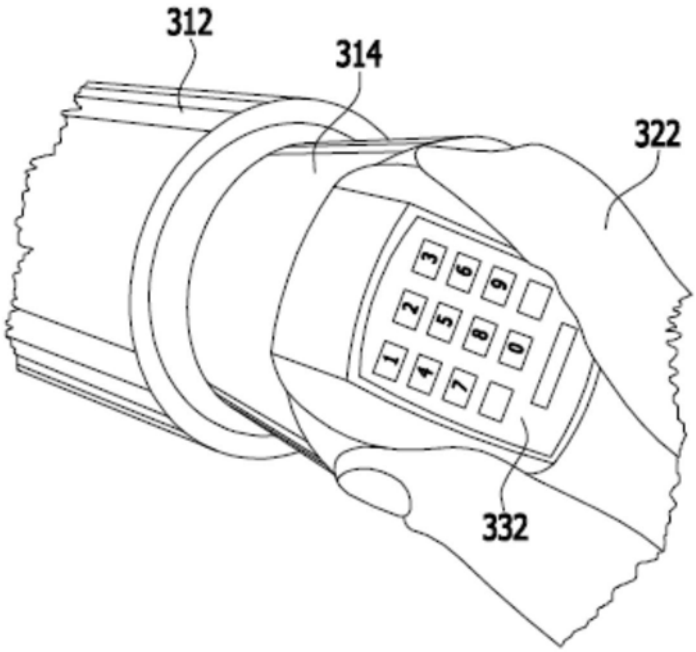


图11

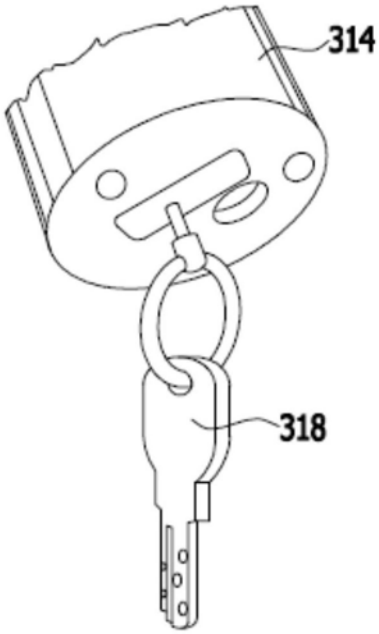


图12

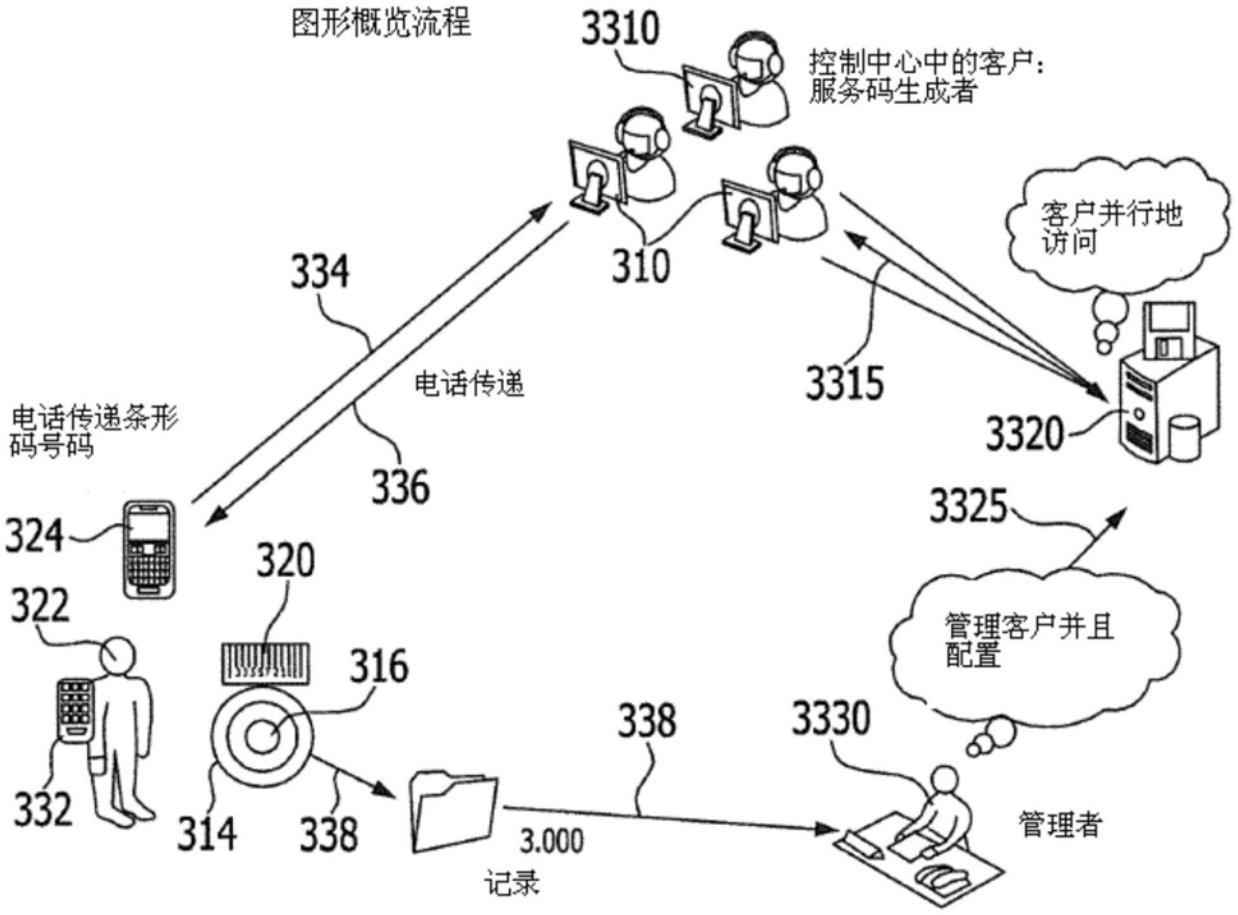

图形概览流程
3310
控制中心中的客户:
服务码生成者
客户并行地
访问
334
310
电话传递
3315
电话传递条形
码号码
3320
336
3325
324
320
322
管理客户并且
配置
316
338
3330
332
314
338
3.000
记录
管理者

图13

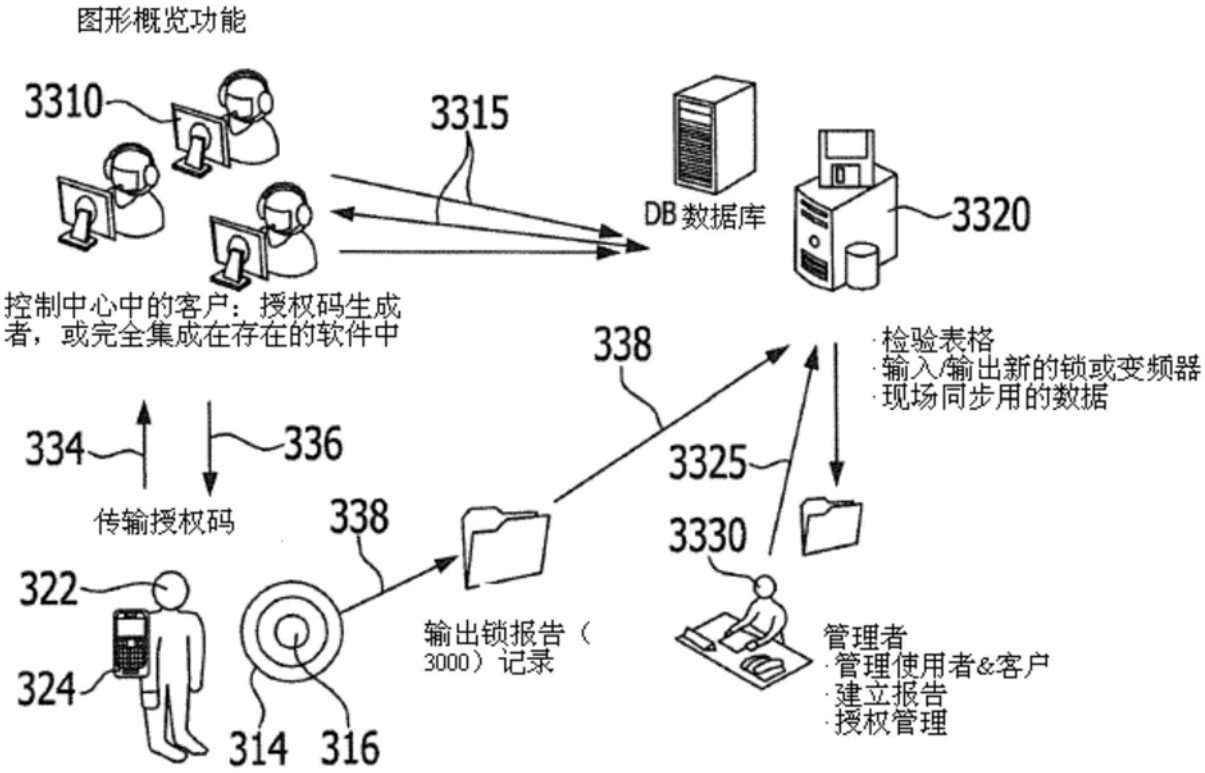

图形概览功能
3310
3315
DB 数据库
3320
控制中心中的客户：授权码生成者，或完全集成在存在的软件中
338
·检验表格
·输入/输出新的锁或变频器
·现场同步用的数据
334
336
传输授权码
3325
338
3330
322
输出锁报告（3000）记录
管理者
·管理使用者&客户
·建立报告
·授权管理
324
314
316

图14

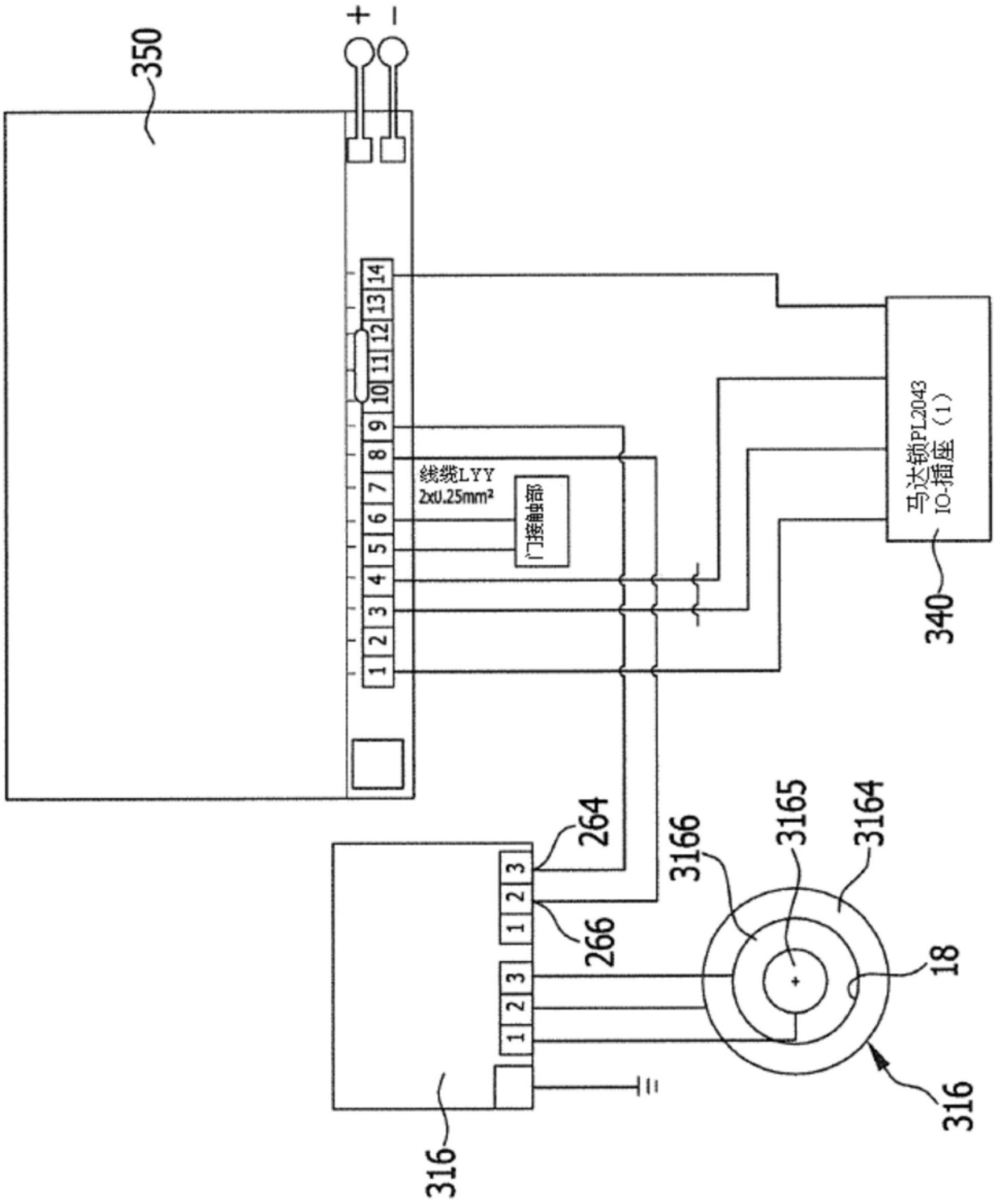

350
+
-
1
2
3
4
5
6
7
8
9
10
11
12
13
14
线缆LYY
2x0.25mm²
门接触部
马达锁PL2043
IO-插座（1）
340
264
266
3166
3165
3164
18
316
316

图15

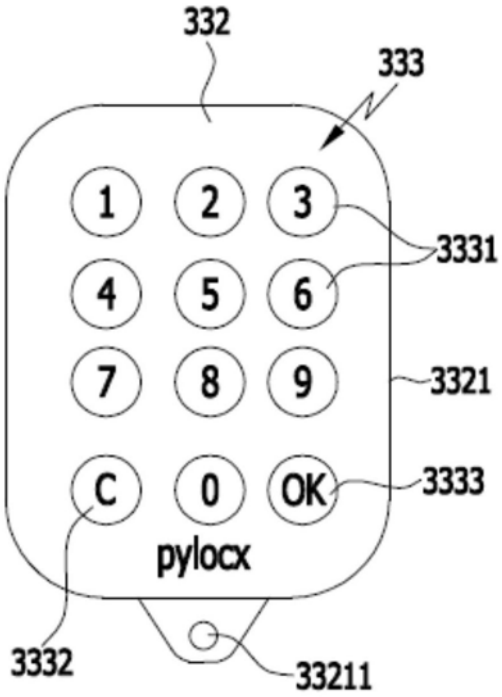

332
333
1
2
3
3331
4
5
6
7
8
9
3321
C
0
OK
3333
pylocx
3332
33211

图16

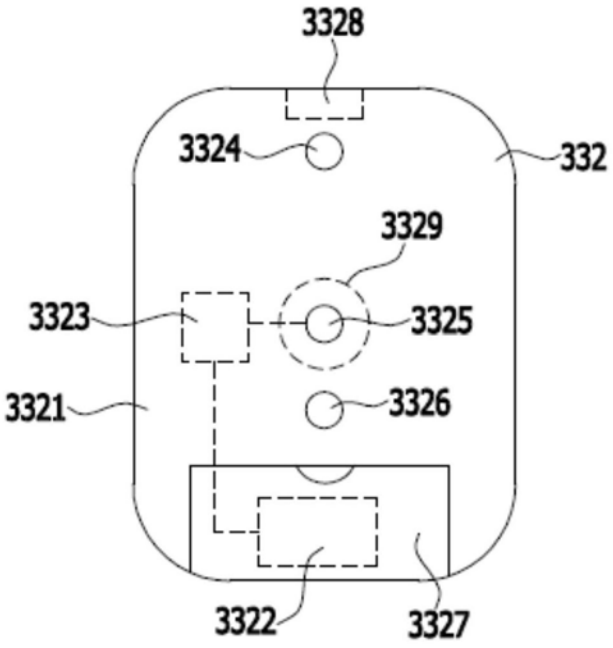

3328
3324
332
3329
3323
3325
3321
3326
3322
3327

图17