



(12) 发明专利申请

(10) 申请公布号 CN 102867346 A

(43) 申请公布日 2013. 01. 09

(21) 申请号 201210233279. 9

(22) 申请日 2012. 07. 05

(30) 优先权数据

102011051586. 0 2011. 07. 05 DE

(71) 申请人 霍弗·霍斯贝克及弗斯特两合公司

地址 德国费尔伯特

(72) 发明人 亚历山大·戈尔德马赫

(74) 专利代理机构 北京康信知识产权代理有限

责任公司 11240

代理人 余刚 李慧

(51) Int. Cl.

G07C 9/00(2006. 01)

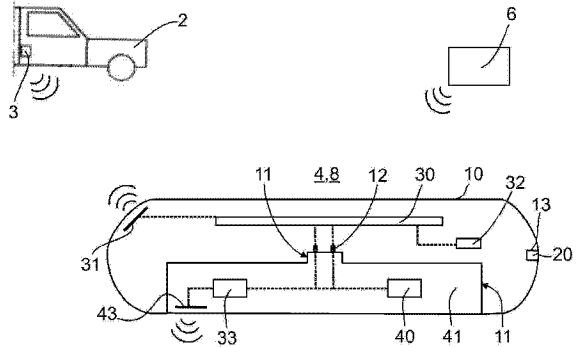
权利要求书 2 页 说明书 6 页 附图 2 页

(54) 发明名称

可被设置为正常状态和安全状态的移动身份发射机

(57) 摘要

本发明涉及一种移动身份发射机(1),用于激活机动车安全系统,特别是门禁和/或点火控制系统,具有壳体(10),壳体中装有电子设备(30)和通信装置(43),其中通信装置(43)可被带入与位于机动车上的安全系统的通信装置(43)通信。支付元件(40)可被移除地固定在壳体(10)的插座(11)中。根据本发明,盖体(20)被单独设置在壳体(10)上,身份发射机(1)可被设置在正常状态(4)和安全状态(5),在正常状态(4)和安全状态(5),可进行与安全系统的通信,在安全状态(5),从插座(11)移除支付元件(40),且盖体(20)封闭并保护插座(11)。



1. 移动身份发射机(1),用于激活机动车(2)的安全系统,具有:  
壳体(10),在所述壳体中设置有电子(30)和通信装置(31),其中所述通信装置(31)可被带入与位于机动车上的安全系统的通信装置(3)的通信中,  
其特征在于:  
所述支付元件(40)被可移除地固定在壳体(10)的插座(11)中,所述盖体(20)被单独设置在所述壳体(10)上,  
所述身份发射机(1)可被设置在正常状态(4)和安全状态(5),在所述正常状态(4)和所述安全状态(5),可进行与所述安全系统的通信,以及  
在所述安全状态(5),从所述插座(11)移除所述支付元件(40),且所述盖体(20)封闭并保护所述插座(11)。
2. 根据权利要求1所述的移动身份发射机(1),  
其特征在于:  
在所述正常状态(4),所述支付元件(40)可被带入与所述支付系统(6)的数据通信中。
3. 根据权利要求1所述的移动身份发射机(1),  
所述支付元件(40)具有信用卡功能和/或借记卡功能。
4. 根据权利要求1所述的移动身份发射机(1),  
其特征在于:  
所述插座(11)具有接触元件(12),所述支付元件(40)在所述正常状态(4)与所述接触元件(12)接触并连接,其中在所述安全状态(5)下,所述盖体(20)保护所述接触元件(12)以防外部环境侵扰。
5. 根据权利要求1所述的移动身份发射机(1),  
其特征在于:  
包括载体(41),以及所述支付元件(40)被集成在所述载体中,其中所述载体(41)可移除地固定在所述插座(11)中。
6. 根据权利要求1所述的移动身份发射机(1),  
其特征在于:  
所述盖体(20)可被可移动地安装在所述壳体(10)上,且可在主动位置(7)和被动位置(8)之间移动,其中在处于所述安全状态(5)中,所述身份发射机处于所述主动位置(7)。
7. 根据权利要求1所述的移动身份发射机(1),  
其特征在于:  
包括储能设备(32),所述储能设备向电子设备(30)供电。
8. 根据权利要求1所述的移动身份发射机(1),  
其特征在于:  
包括储能设备(32),所述储能设备向支付元件(40)供电。
9. 根据权利要求1所述的移动身份发射机(1),  
其特征在于:  
包括第二储能设备(33)。
10. 根据权利要求5和9所述的移动身份发射机(1),  
所述第二储能设备(33)集成在所述载体(41)中。

11. 根据权利要求 1 所述的移动身份发射机(1),  
其特征在于:  
所述盖体(20)可被设计为假插头。
12. 根据权利要求 11 所述的移动身份发射机(1),  
所述假插头被固定在所述壳体(10)的线缆(14)上。
13. 根据权利要求 2 和 5 所述的移动身份发射机(1),  
其特征在于:  
所述载体(41)和 / 或所述支付元件(40)具有用于与所述支付系统(6)通信的其自身的通信装置(43)。
14. 根据权利要求 2 所述的移动身份发射机(1),  
其特征在于:  
所述身份发射机(1)的通信装置(31)同时服务于与所述支付系统(6)通信的目标。
15. 根据权利要求 1 所述的移动身份发射机(1),  
其特征在于:  
包括阻断设备,所述阻断设备在所述身份发射机(1)的正常 状态(4)下锁定所述支付元件(40)在所述壳体(10)的所述插座(11)中的位置。
16. 根据权利要求 1 所述的移动身份发射机(1),  
其特征在于:  
包括锁定设备,所述锁定设备在所述身份发射机(1)的安全状态(5)下锁定所述盖体(20)在所述插座(11)中的位置。
17. 根据权利要求 1 所述的移动身份发射机(1),  
其特征在于:  
在所述盖体(20)上设置信息。

## 可被设置为正常状态和安全状态的移动身份发射机

### 技术领域

[0001] 本发明涉及一种移动身份发射机,以激活机动车安全系统为目的,特别是门禁和/或点火控制系统,具有壳体,壳体中设置有电子设备和通信装置,其中通信装置可被带入与位于机动车上的安全系统的通信装置的通信中。

### 背景技术

[0002] DE 10 2010 061 331.2 公开了机动车的一种无钥匙安全系统。在这种情况下,授权用户能主动操作一个移动身份发射机以向基站发送信号,例如机动车中包括的一个接收机单元,以解锁/锁定机动车。

[0003] 在数据单元中包含的身份数据也可在已知的门禁控制程序中重新生成。此外,用于机动车的电子锁系统目前正在市场中扩张,它们同时配备需要手动操作的上述两个功能,并且也配备不需要手动操作的一种功能,所谓“无钥匙启动”或“无钥匙进入”功能。对比传统的远程控制,无钥匙进入功能不需要操作身份发射机以解锁/锁定机动车门或机动车后备箱,或机动车的其他组成部分。相反,在操作汽车门上的门把手后,机动车和身份发射机之间的通信被启动,且在认证通过后,机动车的电动门打开、后备箱打开等被激活。这意味着携带一个有效身份发射机的用户可解锁和/或锁定其机动车,无须主动操作身份发射机。例如,已知一个门禁控制方法,其中根据门把手的操作来通过电感天线发送一个传输脉冲至身份发射机。随后,身份发射机因此被唤醒,并向机动车上的发射机/接收机单元发送一个无线信号,发射机/接收机单元从控制单元中继该信号用于门禁认证。如果在这一点识别出正确代码,那么电动门解锁被激活。如果门把手被触碰,可在门锁程序中进行同样的进程。

### 发明内容

[0004] 本发明解决的问题为,创建一个移动身份发射机,用于无钥匙激活机动车的安全系统,它具有更强大的功能,并有一个简单的设计,其中同时为用户提供一个舒适的移动身份发射机。

[0005] 具备权利要求 1 所有功能的移动身份发射机解决了该问题。优选实施例在附属权利要求中列出。

[0006] 根据本发明,为此一个支付元件被可移除地固定在壳体的插座中,一个盖体被单独安装在壳体上,身份发射机可被设置在正常状态和安全状态,在正常和安全状态,可能进行与安全系统的通信,在安全状态,移除插座中的支付元件,且盖体保护并封闭插座。

[0007] 必要时,支付元件可由用户从身份发射机壳体上移除。这是在这种情况下,例如,如果具有身份发射机的机动车被带入一个修理店,或第三人接收到移动身份发射机以,例如,停放机动车等等。通过这种可移除地固定在壳体的插座中的支付元件的方式,用户可进行各种支付行为,例如在一个加油站,购物中心,等等。在支付过程中,支付元件最好保留在壳体内。为了排除未经授权人使用移动身份发射机使用支付功能的风险,授权用户可在任

意时间从壳体上移除支付元件,其中移动身份发射机的所有附加功能,特别是无钥匙激活机动车安全系统继续保留。这意味着无论是在身份发射机正常状态还是安全状态,都可能进行与安全系统的通信。但是,如果移动身份发射机在安全状态下,一个支付行为被阻止,因为支付元件不再安装在壳体插座中。根据本发明,为了保证身份发射机功能,有必要,特别是在安全状态,应有效封闭通常安装支付元件的插座。特别是在水分、灰尘颗粒物等等从外部渗透插座的情况下,对于正常状态,这种情况已被证明可不利地干扰支付元件和壳体中集成的电子产品之间的电气连接,由此,于支付行为不利,它将不再可能通过支付元件进行。根据本发明的盖体有效保护支付元件和身份发射机中安装的电子产品之间的连接以防止任何中断,和/或防止支付元件和电子支付系统之间的通信发生任何中断。此外,封闭盖体防止水分、灰尘颗粒物等等当身份发射机处于安全状态时渗透进入壳体的内部,并防止负责与车载安全系统通信的电子设备因此受损。

[0008] 在改进本发明的进一步措施中,在正常状态,可将支付元件带入与支付系统的数据通信中,且支付元件特别具有信用卡功能和/或借记卡功能。

[0009] 支付元件可具有一个微处理器,其中支付元件可与支付系统通信,特别地,可进行远程金融交易,例如在支付元件上装载一定金额的钱或从支付元件借记限定金额的钱。例如,支付元件可仅提供小额款项,特别是作为支付小额日常花销的支付装置,因此以这种方式,提供了一种使用小额电子现金的插件(insert)。此外,支付元件可以这种方式配备,即金额可在与支付系统的通信中没有任何限制的转移。

[0010] 支付元件被有利地设计为具有一个存储设备,其中支付元件可在本发明的一个额外实施例中设计具有一个集成电路,该集成电路具有一个或多个微处理器。在这种情况下,微处理器和存储设备在本发明的一个关于安全的可能实施例中起到重要作用,因为存储设备可包含代码,例如,用于认证、控制、新的结余等等。在本发明的一个可能实施例中,可使得微处理器执行复杂计算算法或从输入微处理器的身份数据中估计一个秘密值。

[0011] 在将支付元件带入与电子支付系统的数据通信中之后,在本发明的一个实施例中,如果经计算的秘密代码与已存在于卡中的秘密代码不同,支付元件可保持为无功能。

[0012] 插座有利地具有接触元件,其中处于正常状态的支付元件与所谓接触元件接触并连接,其中在安全状态下,盖体保护接触元件以防外部环境的侵扰。在移动身份发射机的正常状态下,支付元件,特别是具有其自有接触元件时,直接与插座上的接触元件相接。此外,在配置中,类似支付元件同时具有一个可靠的封闭功能,这样在身份发射机的正常状态下,同样没有水分、灰尘颗粒物等可以渗透进入插座和/或壳体。在身份发射机的安全状态下,通过盖体来封闭并保护插座的接触元件,且在正常状态下,通过支付元件来封闭并保护插座的接触元件。

[0013] 类似地,可包含一个载体,其中支付元件被集成如所谓载体中,且该载体可移除地固定在插座中。在身份发射机的正常状态下,载体被插入壳体的插座中,其中对于用户载体可构成至少壳体组件的其中一部分。载体与壳体插座相应的几何形状有利地匹配,这样载体可被壳体插座牢牢保持。该载体可以形状配合和/或力配合方式,例如,在壳体上固定,特别是在壳体插座上固定。

[0014] 盖体可有利地被可移动地安装在壳体上,且可在主动位置和被动位置之间移动,其中当处于安全状态下,身份发射机在主动位置。在盖体的被动位置,支付元件位于壳体插

座中,这样支付行为可由用户发起。

[0015] 此外,可以设想一个配置,其中通过对身份发射机的一个相应的、有意的激活,特别是对激活元件的激活,支付元件和 / 或载体可由用户从壳体插座上移除。这意味着在身份发射机的正常状态下,支付元件位于壳体插座中,并保险在那个位置,以这样的方式,其中从插座上的任意移除都被阻止。这可以通过,例如,锁定元件来实现,它直接作用于支付元件和 / 或载体。只有一旦用户自觉发起对身份发射机的激活,对插座中支付元件和 / 或载体的阻止才会被取消,这样用户随后可将支付元件从插座上移除。

[0016] 可同样设想一个配置,其中包括一个储能设备,该设备向电子设备和 / 或支付元件提供电流。因此,可以在身份发射机中仅包含一个储能设备,它向壳体内的电子设备供电,且也通过可能的支付元件进行支付行为。同样,移动身份发射机可包括一个第二储能设备作为冗余。此外,在能量的放电和 / 或能量消耗已经发生的情况下,一个储能设备可同样对额外的储能设备进行重新充电。第一和 / 或第二储能设备可被设计为一个电池、蓄电池、磁储能设备,或一个电容。

[0017] 此外,盖体可被设计为一个假插头(dummy plug),尤其被固定在壳体缆索上。在这种情况下,缆索可以是柔性的和 / 或有弹性的,其中缆索作为安全元件起作用,这样盖体不会从身份发射机上松开从而丢失。将盖体设计为假插头的好处在于,通过插头的功能可以保证在插座中可靠地保持,其中插座具有相应固定装置,利用所述固定装置假插头可以啮合。

[0018] 可同样设想一个配置,其中载体和 / 或支付元件具有用于与支付系统通信的其自身的通信装置。这意味着一个独立的、第二通信装置在身份发射机上使用,用于无钥匙激活机动车的安全系统,且同样位于载体和 / 或支付元件上。

[0019] 类似地,身份发射机的通信装置可同时服务于与支付系统通信的目标。

[0020] 特别有利的是,一个无现金支付交易可在销售点终端(POS)处通过可移除支付元件的方式发生,其中可能进行一个电子借记,其中同样行为可作为例如一个在线过程或脱机过程发生。在在线过程的情况下,电子支付系统在有或没有电脑支持的情况下,连接至卡片运营商,例如,Maestro、VISA 等等。在这种情况下,利用数字和 PIN 检测支付元件是否被滥用,且随后客户账号的借记可由卡片运营商和客户银行之间一个相应的交易来实施。同时,可设想的是在脱机过程中进行电子借记过程,其中,只有账号数据在支付行为中使用。为了获取收费的许可,特别是对于借记程序,销售、代理等等通过从客户收到收据上的签名来获取收费许可,其中根据本发明,所谓客户在他或她身上携带身份发射机。

[0021] 为了提高支付元件和支付系统之间通信的安全性,支付元件的通信装置有利地具有一个小于 20cm 的范围,尤其是小于 10cm。支付元件和电子支付系统有利地彼此加密通信。同样的,支付元件的通信装置可在近似为 13.56MHz 的频率范围内工作,由此,特别是可能达到大于 400kBits 每秒的数据传输速率。支付元件和支付系统之间的通信可通过蓝牙或近距离无线通信技术来开展。

[0022] 本发明额外的优势、功能和详细信息在以下描述中可以找到,其中本发明的多个实施例参考示意图被详细描述。权利要求和描述中声明的功能,无论是单独或者其中任意组合对于本发明都至关重要。

## 附图说明

[0023] 图 1 示出了移动身份发射机的一个纯粹的示意图,该发射机具有一个位于身份发射机壳体插座中的支付元件,

[0024] 图 2 示出了图 1 中的身份发射机,其中支付元件从壳体插座上移除,

[0025] 图 3 示出了根据图 1 的移动身份发射机的一个进一步的变体,

[0026] 图 4 示出了图 1 中壳体插座在一个额外实施例变化中的放大图,以及

[0027] 图 5 示出了图 1 壳体插座的一个进一步的实施例。

## 具体实施方式

[0028] 在图 1 和图 2 中,展示了一个移动身份发射机 1,它用于激活机动车 2 的安全系统。此外,这个实施例公开了一种系统,其中一个安装在移动身份发射机 1 内的支付元件 40 可被带入与电子支付系统 6 的数据通信中。此外,移动身份发射机 1 具有电子设备 30,该电子设备可包括存储的身份数据。此外,机动车 2 具有通信装置 3,该通信装置可被设计为发射机和 / 或接收机单元。此外,移动身份发射机 1 具有一个通信装置 31,该通信装置可与机动车载的通信装置 3 通信。为了进行一个机动车门的解锁或锁定的过程,机动车 2 的安全系统只有在一旦根据通信装置 3、31 之间的通信确认认证通过时才被激活。这意味着,例如,具备有效身份发射机 1 的用户可打开他的机动车 2。

[0029] 移动身份发射机 1 的壳体 10 被设计为具有插座 11,支付元件 40 可插入该插座。在本实施例中,包括载体 41,且同样载体中集成了支付元件 40。将载体 41 与壳体 10 的插座 11 的几何形状进行相应地匹配。根据图 1,当载体 41 处于插入在插座 11 中的状态时,载体 41 承担一定的壳体功能。此外,可将插座 11 以各种方式进行几何设计,以在身份发射机 1 的壳体 10 中可靠地保持载有支付元件 40 的载体 41。但是,在所有实施例中,支付元件 40 与载体 41 一起被插入插座 11,以这种方式用户需要在需要时可从插座 11 移除支付元件 40。根据图 1,可设想的是,通信装置 31 同样用于与电子支付系统 6 的通信,其中所谓通信装置 31 也用于与机动车载的通信装置 3 的通信。作为替代,也可能是移动身份发射机 1 中包括第二通信装置 43,用于与电子支付系统 6 通信。在这种情况下,通信装置 43 可被安装在例如移动身份发射机 1 的壳体 10 上。类似地,可设想的是支付元件 40 本身被设计为具有该通信装置 43。同样地,可设想的是载体 41 具有通信装置 43。

[0030] 在一个没有明确说明的进一步实施例中,将支付元件 40 可移除地独立连接在壳体 10 的插座 11 中。根据图 1 或图 2,这意味着可不需支持地将支付元件 40 安装在壳体 10 中。例如,根据支付元件 40 的几何形状在壳体 10 上构建一个插座、窗口、开口等等,这样可靠地容纳了支付元件 40。如果用户将支付元件 40 从壳体 10 在这一点移除,为了可靠地再次关闭支付元件 40 的插座,在壳体上额外包括并单独安装一个相应的盖体。

[0031] 为了开展与支付系统 6 的支付行为,支付元件 40 可具有一个芯片,例如,包括一个微处理器、电路、存储设备等等。例如,图 1 和图 2 示意图所示。支付系统 6 可位于销售点终端(POS),例如,来保证购买方,或例如同样携带移动身份发射机 1 的客户,与卖方和 / 或信用卡机构之间的无现金支付交易。在这种情况下,支付元件 40 可具有例如一个信用卡功能和 / 或借记卡功能。在图 1 中,有载体 41 的支付元件 40 插在壳体 10 的插座 11 中,这样身份发射机 1 处于其正常状态,其中可能进行与机动车 2 安全系统的通信以及与支付系统

6 的通信。在图 2 中示出了安全状态 5, 其中一个盖体 20 被固定在插座 11 中, 这样保护了例如插座 11 的接触元件 12 的组件, 例如, 同样对中断敏感的组件, 由此可能防止功能中断。在这个安全状态 5 中, 可能进行身份发射机 1 和机动车安全系统之间的通信; 但是, 不可能通过支付元件 40 (从插座 11 上移除的同样元件) 进行支付行为。

[0032] 此外, 可以设想的是为了向必要电子组件供电, 在身份发射机 1 上包括一个储能设备 32。图 1 展示了可在壳体 11 中集成储能设备 32, 例如为了向电子设备 30, 包括通信装置 3、43、31 供电。同样地, 可能包括一个第二储能设备 33, 它直接在支付元件 40 中集成或直接在载体 41 中集成。该第二储能设备 33 作为第一储能设备 32 的冗余工作。

[0033] 如图 1 和图 2 所示, 盖体 20 被插入到壳体 10 的插座 13 中, 且根据本发明位于被动位置 8。盖体 20 的主动位置 7 在图 2 中展示, 其中盖体 20 被固定在插座 11 中。

[0034] 盖体 20 可被设计为一个假插头, 它被设计为具有相应的接触元件, 这些接触元件可被插入到壳体 10 的接触元件 12 中, 其中这个假插头 20 在插座 11 中可靠地保持, 并构成对插座 11 的可靠封闭。

[0035] 根据本发明的身份发射机 1 的进一步实施例, 如图 1 和图 2 所示, 其中盖体 20 通过缆索 14 固定在壳体 10 上。例如, 缆索 14 可被设计为一条柔软的缆索。身份发射机 1 的其他实施例, 如图 1 和图 2 所示, 参考图 3 中所示的身份发射机 1。

[0036] 在图 4 或图 5 中, 示出了插座 11, 其中在图 4 中, 盖体 20 为一个盖子, 它能以轴 21 为枢纽转动, 且当处于被动位置 8 时处于弹簧张力之下。在这一点, 如图 4 所示, 如果支付元件从插座 11 上移除, 盖体 20 同时绕轴 21 逆时针转动, 并到达其主动位置 7。这个动作由图 4 的虚线表示。因此可有效地密封位于插座 11 中的接触元件 12, 并保护其以防外部环境侵害。

[0037] 在图 5 中, 盖体 20 可在其主动位置 7 和被动位置 8 之间平移。在这一点, 如果支付元件 40 从壳体 10 的插座 11 上移除, 可手动将盖体 20 滑至主动位置 7 (由虚线表示) - 或盖体 20 的向其主动位置 7 的这个移动可自动进行。这个是实施例的特征尤其在于它的紧凑性; 且当盖体 20 在主动位置 7 时, 同时密封和保护插座 11 中的接触元件 12。

[0038] 根据所有的实施例, 为了有效密封接触元件 12、42 以及电子设备 30 及其附属电子组件, 盖体 20 和 / 或载体 41 上和 / 或插座 11 的壁上包括一个相应的密封垫。这同时应用于身份发射机 1 的正常状态 4 和安全状态 5。此外, 在所有实施例中, 盖体 20 可作为广告或信息板, 在其之上可应用并特别印刷信息、特别是标识、字母、数字组合、广告信息等等。

[0039] 参考数字列表

[0040] 1 移动身份发射机

[0041] 2 机动车

[0042] 3 机动车通信装置

[0043] 4 正常状态

[0044] 5 安全状态

[0045] 6 支付系统

[0046] 7 盖体主动位置

[0047] 8 盖体被动位置

[0048] 10 壳体



- 
- [0049] 11 插座
  - [0050] 12 接触元件
  - [0051] 13 凹槽
  - [0052] 14 缆索
  - [0053] 20 盖体
  - [0054] 21 轴
  - [0055] 30 电子设备
  - [0056] 31 通信装置
  - [0057] 32 储能设备, 电池
  - [0058] 33 第二储能设备
  - [0059] 40 支付元件
  - [0060] 41 载体
  - [0061] 42 借助元件
  - [0062] 43 通信装置

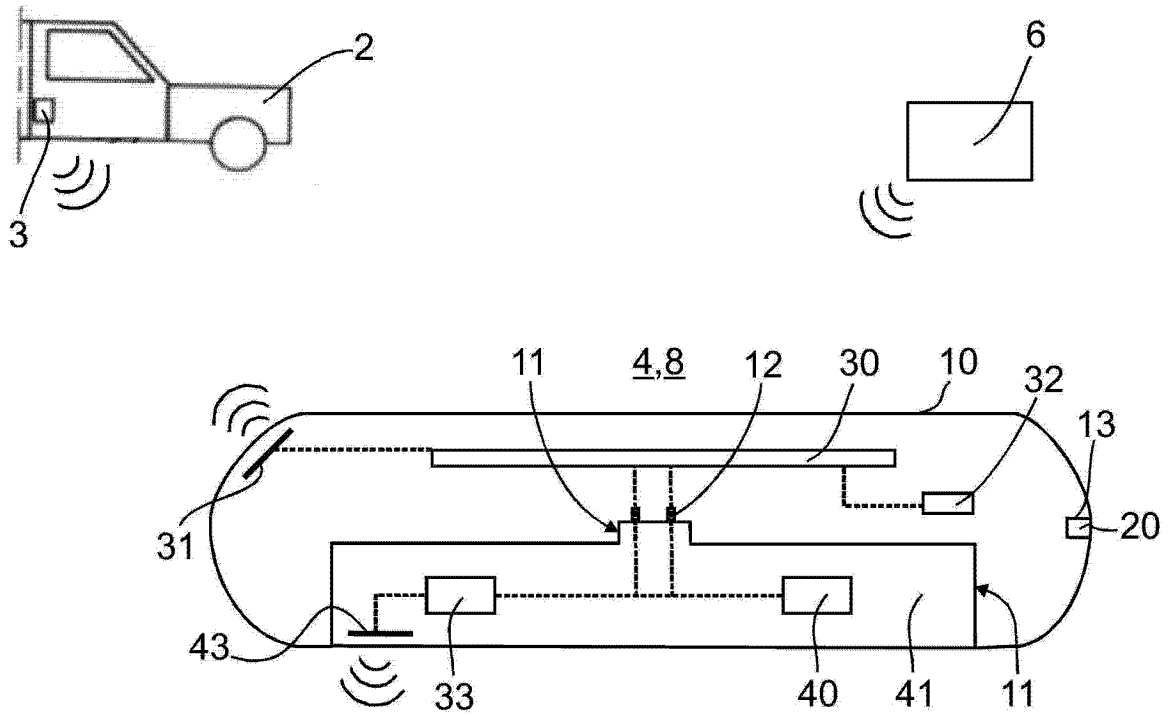


图 1

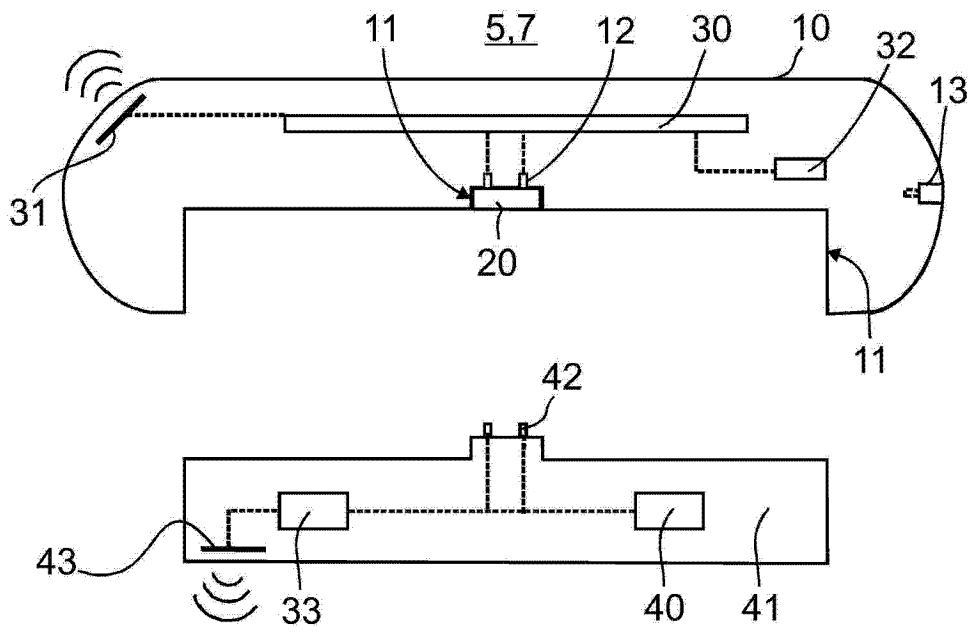


图 2

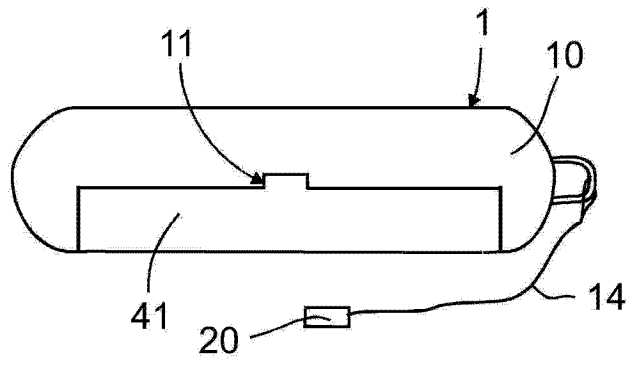


图 3

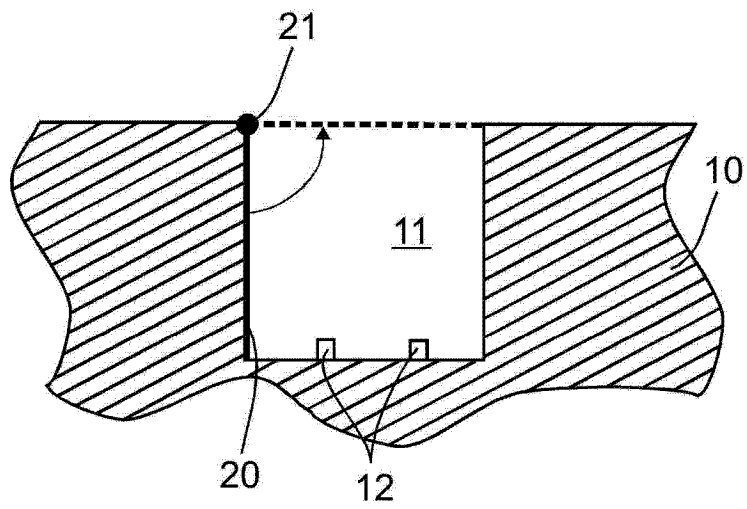


图 4

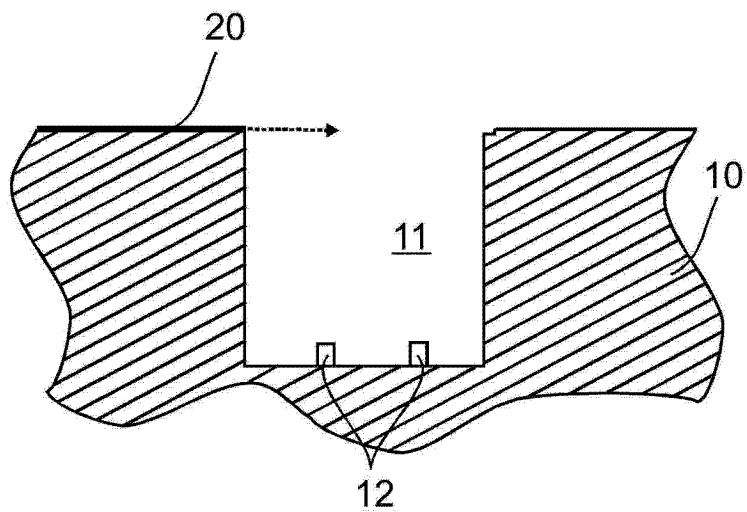


图 5