[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07B 17/00

[12] 发明专利说明书

[21] ZL 专利号 00103871.0

[45] 授权公告日 2004 年 7 月 7 日

[11] 授权公告号 CN 1156800C

[22] 申请日 2000.3.10 [21] 申请号 00103871.0

[30] 优先权

[32] 1999. 3.12 [33] DE [31] 19912781.6

[32] 1999. 6.15 [33] DE [31] 19928057.6

[71] 专利权人 弗朗科泰普 - 波斯特利亚两合公司

地址 联邦德国比肯韦德

[72] 发明人 彼得·波斯特 德克·罗西瑙

托斯坦·施拉夫

审查员 沈乐平

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

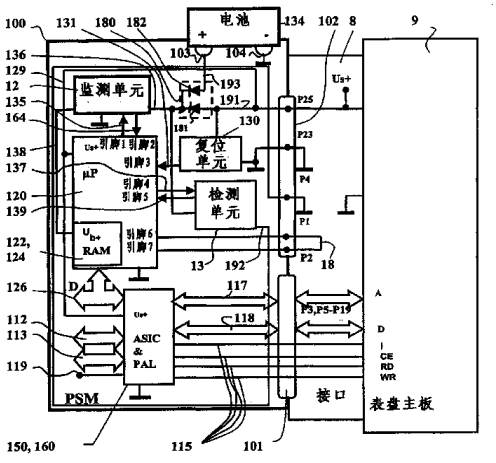
代理人 王以平

权利要求书 3 页 说明书 20 页 附图 7 页

[54] 发明名称 保护安全模块的方法及实现此方法的装置

[57] 摘要

本发明涉及一种保护安全模块的方法，它用第一个，第二个和第三个功能单元监测安全模块的状态，符合规定的使用或更换，用第一个功能单元控制至少一个状态的指示，以及在不符合规定的使用或更换时至少用第二个功能单元清除敏感数据。此外，在更换安全模块时用第三个功能单元闭锁功能，在符合规定的使用或更换安全模块之后重新初始化已被清除的敏感数据并且通过释放安全模块的功能单元而重新工作。



ISSN1008-4274

1. 保护安全模块的方法，其中所述安全模块具有第一、第二和第三个功能单元，第一个功能单元是一个处理器（120），第二个功能单元是一个电压监测单元(12)，第三个功能单元是一个检测单元(13)，包括步骤：

·当安全模块以系统电压来供电时利用第一个功能单元来监测安全模块的状态，利用第二个功能单元来监测安全模块是否被符合规定地使用，或者利用第三个功能单元来监测安全模块的更换，其中用第二个功能单元实现对电池（134）符合规定的插入或状态的监测，在更换安全模块或者在其受到袭击后处于损坏状态时用第三个功能单元使安全模块停止工作，

·在第一个功能单元控制下指示至少一个状态（220，230，240，250，260，270，280，290），以及

·在不符合规定的使用或更换时至少用第二个功能单元清除敏感数据。

2. 如权利要求 1 所述的方法，其特征在于，用第一个功能单元来检测时间进程，并且用以下步骤实现后继过程，以使安全模块恢复工作：

·在安全模块符合规定的使用或更换之后用第一个功能单元（120）重新初始化已被清除的敏感数据，并且

·通过释放安全模块（100）的第二个功能单元和第三个功能单元以使安全模块重新工作。

3. 如权利要求 1 所述的方法，其特征在于，用第三个功能单元检测机械的或化学的袭击之后的损坏状态。

4. 如权利要求 2 所述的方法，其特征在于，第一个功能单元不断地判定第一个借贷天数是否用尽，并且在其用尽时指示一个受怀疑状态。

5. 如权利要求 4 所述的方法，其特征在于，通过与数据中心的

接触来恢复正常工作状态而无需通过维护进行现场检查。

6. 如权利要求 2 所述的方法，其特征在于，借贷时间是可变的，并且对于不同的安全模块是不同的，并且在安装时装载到安全模块的一个存储器中。

7. 如权利要求 2 所述的方法，其特征在于，第一个功能单元不断地判定第二个借贷天数是否用尽，它比第一个借贷天数长，并且在其用尽时指示“丢失”状态。

8. 用于实现权利要求 1 所述的方法的装置，其中一个安全模块装配有一个逻辑电路，用系统电压或电池（134）的电压给安全模块供电的装置以及多个监测装置，其特征在于，所述安全模块具有第一个，第二个和第三个功能单元，用来装载至少由数据中心给出的借贷时间的装置以及与第一个功能单元相连接的指示装置（107，108），并且所述装载在安装和补充时在安全模块的存储器（124）中进行，第一个功能单元是一个处理器（120），它在时间进程中判定借贷天数是否用尽，指示装置（107，108）被控制来至少指示时间进程，并且第二个功能单元还具有在安全模块非符合规定的使用或更换时清除存储器（124）中的敏感数据的装置，第二个功能单元是一个电压监测单元（12），它通过导线和安全模块的供电装置与系统电压或电池电压相连接，并且第二个功能单元通过导线将工作电压给到存储器，第三个功能单元是一个具有用于可复原自保电路的电路元件（1310，1316，1322，1320）的检测单元（13），其中在测量电压线（192）上的电平偏离规定电位时自保电路起动，并且与电压监测单元（12）和检测单元（13）相连接的处理器（120）被编程，它判定并指示安全模块（100）的相应状态。

9. 如权利要求 8 所述的装置，其特征在于，处理器（120）具有存储器，电压监测单元（12）输出的工作电压 U_b^+ 经导线送给存储器，处理器（120）由系统电压 U_s^+ 供电并具有第 4 个引脚，用来经导线复原检测单元（13）中自保电路的状态，并且处理器具有第 5 个引脚，其上连接导线，用来查询检测单元（13）的状态。

10. 如权利要求 8 或 9 所述的装置，其特征在于，安全模块（100）用固化的灌注物质（105）灌注，安全模块（100）的电池（134）可更换地安装在电路板（106）上灌注物质（105）之外，电路板（106）具有用于连接电池（134）的电极的电池连接端子（103 和 104）和用于系统电压对安全模块（100）供电的第二个连接件（102），灌注物质中具有在安全模块（100）受到袭击时进行告警和必要时保护的装置，以及至少一个连接件（101，102）用来静态和动态监测安全模块（100）是否插入和是否受到袭击。

11. 如权利要求 8 所述的装置，其特征在于，安全模块的处理器（120）装配有用以输出至少一个指示安全模块（100）的状态的信号的引脚。

12. 如权利要求 11 所述的装置，其特征在于，指示装置（107，108）在模块内部连接到处理器（120）的输入/输出单元（125）的 I/O 口上。

保护安全模块的方法及实现此方法的装置

技术领域

本发明涉及保护安全模块的一种方法，以及实现此方法的一种装置。这种邮政安全模块尤其适用于盖邮戳机及邮政处理机或者具有邮政处理功能的计算机。

背景技术

诸如 US 4746234 所公开的热变换盖邮戳机这样的现代盖邮戳机使用一个全数字的打印装置。因而原则上可以打印任意的文字和特殊符号在邮戳打印区以及任意的或与付费处相关的广告内容。例如盖邮戳机 T1000 具有一个包装在保安外壳中的微处理器，外壳上有一个开槽用来送入信件。在信件被送入时一个机械的信件传感器（微动开关）给出一个打印请求信号到微处理器。邮戳打印内容包括用于信件传递的事先输入和存储的邮政信息。盖邮戳机的控制单元按照软件完成结算，必要时对数据的实时性进行监测，以及控制邮资收付差额的装载。

US 5606508（DE 4213278B1）和 US 5490077 已经建议了借助于芯片卡对上述热变换盖邮戳机实现数据输入的可能性。一张芯片卡装新数据到盖邮戳机中，一组另外的芯片卡可以通过插入一张芯片卡来更改已输入的相应数据。这样可以比用键盘输入更方便和迅速地实现数据装载和更改。用于邮件的盖邮戳的盖邮戳机装配有一个用于在邮件上打印邮资印记的打印机，一个控制打印机和盖邮戳机外设的控制装置，一个用于结算邮费的结算单元，至少一个用来存储邮费数据的非易失存储器，至少一个用于存储安全有关的数据的非易失存储器以及一个日历/时钟。存储安全有关的数据的存储器和/或日历/时钟通常由电池供电。在现有盖邮戳机中安全有关的数据（密钥等）存储在非易失存储器中。这些存储器是 EEPROM，FRAM 或电池保证的 SRAM。现有盖邮戳机常常也提供一个内部实时时钟（Real Time Clock）RTC，它由电池供电。例如

现在存在灌注的模块，它们包含有集成电路和锂电池。这种模块在电池寿命到期后必须整个地被更换和去掉供电。从科学和经济的观点看仅需更换电池才更有效。然而这就必须打开保安外壳，且然后再封闭它，因为抵抗袭击的安全性主要依赖于保安外壳，它包封了整个装置。EP 660269A2（US 5671146）已经提出一种合适的方法来提高盖邮戳机的安全性，其中保安外壳的授权和非授权开启是不同的。

盖邮戳机有时需要修理，如果接近元件是困难的或受到限制，修理是困难的。将来在大型邮政处理机或所谓的 PC 盖邮戳机中保安外壳将被压缩成所谓的邮政安全模块，这将改善其他元件的可接近性。为了经济地更换安全模块的电池也希望在相对简单的途径上更换电池。为此电池必须在盖邮戳机的保安范围之外。但是如果电池连接端子也从外部可接近，则可能的袭击会发生，即控制电池的电压。现在的电池供电的 SRAM 和 RTC 对其工作电压有不同的要求。保持 SRAM 的数据所需的电压低于 RTC 工作所需电压。这意味着电压降到某个门限值之下将导致不希望的行为：RTC 停止运动，存储在 SRAM 单元中的时间和 SRAM 所存储的内容仍然保持着。至少有的安全措施，例如长时间监视器，可能在盖邮戳机上是无效的。长时间监视器工作于以下情况：远地数据中心预先给定一个时间借贷量或者一个时间持续期，尤其是一个天数或一个规定日期，直到此日期盖邮戳装置可以通过通信连接报到。在时间借贷量或期限抵达之后不能盖邮戳。EP 660270A2（US 5680463）以“产生和检验安全打印的方法和配置”为题提出了一种方法，它求出直到下一次存入款项的假设时间持续期，并且每个没有按期报到的盖邮戳机被数据中心视为受怀疑的。受怀疑的盖邮戳机被通知给邮局，邮局对从受怀疑的盖邮戳机出来的盖过戳的信件进行检查。时间借贷量或期限的到期也由盖邮戳装置查明。使用者被要求完成关于到期的通信。然而此盖邮戳装置不具备独立的安全模块。

在有电子数据处理设备以来安全模块已为大家所熟悉。为了抵抗对电子设备的袭击，EP 417447B1 建议了一种封锁装置，它将供电装置和信号收集装置以及屏蔽装置包在外壳中。此屏蔽装置由填充物质和连接装置组成，在连接装置上连接供电装置和信号收集装置。后者对连接装

置的连接电阻的变化有反应。此外安全模块包含一个内部电池，一个由系统电压转换为电池电压的电压转换器，一个电源门和一个短路晶体管及其他传感器。当电压降到规定门限值以下时，电源门动作。当连接电阻，温度或光射线改变时逻辑电路给以响应。借助于电源门或借助于逻辑电路短路晶体管的输出端切换到低电平，这样存储在存储器中的密钥被清除掉。然而对于在盖邮戳机或邮政处理机中的使用而言，不能更换的电池的使用寿命太短，由此导致安全模块的使用寿命太短。

大型邮政处理机例如是 JetMail®。邮戳打印在其中是借助于静态安置的喷墨打印头实现的，而信件的传递是非水平的，接近于垂直的。DE 19605105C1 提出了打印装置的一种合适的实施方案。邮政处理机有一个表盘和一个基座。表盘应装配一个外壳，并使得元件容易被接近，它必须由一个邮政安全模块来使其能抵抗袭击，此模块至少完成邮费的结算。为了排除对程序运行的影响，EP 789333A2 以“盖邮戳机”为题建议安全模块装配一个专用电路（Application Specific Integrated Circuit）ASIC，它有一个硬件结算电路。此外专用电路控制给打印头的打印数据传输。仅当对于每个邮件产生唯一的打印内容时该数据传输才是不需要的。例如在 US 5680463，US 5712916 和 US 5734723 中建议了一种用于产生和检验一个安全性打印的合适的方法和配置。其中一个专用的安全标记用电子方法产生并被嵌入到打印图形中。

在未公开的德国专利申请 19816572.2 和 19816571.4 中也提出了安全模块在遭到袭击时保护其中存储的数据的其他措施。在有多个传感器时耗电量增加，并且一个不是持续地由系统电压供电的安全模块从其内部电池吸取传感器所需之电流，因此电池被提早耗尽。电池的容量和耗电量限制了安全模块的使用寿命。

与许多其他产品一样，盖邮戳机结构也实现了模块化。这种模块化使得出自各种原因的模块和元件的更换成为可能。例如故障模块可被取下并且通过检查，修理或被新的模块替换。因为在更换那些包含安全相关数据的组件时要求最高的操作水平，通常其更换需由业务技术人员进行并采取一些措施，这些措施在安全模块被不符合规定的使用或非授权的更换时中断安全模块的功能执行。但是采取这些措施费用很昂贵。

发明内容

本发明的目的在于，以小的费用实现在安全模块可更换地安装时保证能抵抗对其的未经许可的操纵。其更换应可由任何人以尽可能简单的方式进行。

本发明的出发点是：借助于功能单元来确认盖邮戳机，邮政处理装置或类似设备的安全模块的更换，操纵和使用，以提供给各种设备的使用者一个关于安全模块乃至整个设备正确地执行其功能的保证。安全模块的更换或损害至少被检测出来并且必要时，在安全模块重新被插上并用系统电压供电时事后作为状态信号发出。安全模块的状态变化借助于第一个功能单元和一个检测单元来收集，检测单元具有一个可复原的自保电路并由电池电压供电。第一个功能单元在其重又由系统电压供电时能判定各种状态。优点在于对安全模块的状态变化的快速反应以及检测单元有小的电池耗电量且不用系统电压供电。

必要时第二个功能单元可监测电池电压，判定电池的容量是否已耗尽。一个要求的电池更换被告知，当然必须保证由系统电压供电。这至少避免了在更换时对安全模块的不符合规定的使用，在更换时不仅没有系统电压，而且可更换地安装的电池也被取走。为使更换工作可由不熟悉的人员完成，并且在将来完全由使用者来完成，第二个功能单元完成对更换电池时的电压下降的监测，同时第一个功能单元在必要时首先清除掉敏感的数据并且限制或完全中断安全模块的继续使用。在由一个业务员现场检查安全模块之后原有的功能可被恢复且外壳原封未动。在以后的恢复运行过程中第一个功能单元强迫安全模块与一个远地数据中心接触以释放至少一个功能单元。

如果不是更换电池，而是整个安全模块被替换，首先由第二个功能单元清除敏感的数据，然而可以在恢复运行时重新初始化这些敏感数据。为了建立接触，可以利用采用数字或模拟传输线路的方法。同样安全模块的检查由一次维护引发。安全模块可指示各种状态。因此可以例如：离上次与数据中心的接触时间如此之长，已经产生怀疑，或者离上次与数据中心的接触时间太长，不再允许重新初始化。第一个功能单元不断判别第一个借贷天数是否用尽，当此借贷天数已用尽时指示受怀疑

状态。通过与数据中心的接触可以恢复正常的工作状态，而无需由一次维护作现场检查。借贷时间可以是可变的并且对不同的安全设备不同。借贷时间可由数据中心预先规定并且在安装时装载到安全装置的一个存储器中。第一个功能单元不断判定第二个借贷天数是否用尽。当它被用完时指示“丢失”状态。在此状态下，也通过一次维护对安全模块作现场检查。

保护安全模块的方法，其中所述安全模块具有第一、第二和第三个功能单元，第一个功能单元是一个处理器，第二个功能单元是一个电压监测单元，第三个功能单元是一个检测单元，包括步骤：

·当安全模块以系统电压来供电时利用第一个功能单元来监测安全模块的状态，利用第二个功能单元来监测安全模块是否被符合规定地使用，或者利用第三个功能单元来监测安全模块的更换，其中用第二个功能单元实现对电池符合规定的插入或状态的监测，在更换安全模块或者在其受到袭击后处于损坏状态时用第三个功能单元使安全模块停止工作，

· 在第一个功能单元控制下指示至少一个状态，以及

·在不符合规定的使用或更换时至少用第二个功能单元清除敏感数据。

由以下步骤完成此方法的其他过程：

·在符合规定地使用或更换安全模块之后借助于第一个功能单元对以前被清除的敏感数据重新初始化，

·通过释放安全模块的第二个和第三个功能单元使安全模块恢复工作。

必要时需要更换安全模块。借助于第三个功能单元也可检测机械或化学的袭击之后的损坏状态，步骤为：

·在更换安全模块或在一次袭击后处于损坏状态时借助于第三个功能单元使安全模块停止工作。

在成功完成动态的插入检测之后，借助于第一个功能单元与远地数据中心的通信连接重新初始化，在第一个功能单元检测时经过接口电路

回路交换信息，这些信息无错的传递证明了安全模块结构符合规定。安全模块的功能单元的释放通过其复原实现。第一个功能单元是一个与其他功能单元相连接的处理器，它被编程来确定各种状态。第二个功能单元是一个具有可复原自保电路的电压监测单元，第三个功能单元是一个具有可复原自保电路的检测电路，它能检测非插入状态和受到机械或化学的袭击后的损坏状态。装置用灌注物质灌注，以警戒和保护安全模块受到袭击。

实施该方法的装置，其特征在于，安全模块用固化的灌注物质灌注，安全模块的电池可更换地安装在电路板上灌注物质之外，电路板具有用于连接电池的电极的电池连接端子和用于系统电压对安全模块供电的第二个连接件，灌注物质中具有在安全模块受到袭击时进行告警和必要时保护的装置，以及至少一个连接件用来静态和动态监测安全模块是否插入和是否受到袭击。

附图说明

下面借助于附图详细说明本发明的优选实施方案。附图中

图 1 是安全模块的方框图和接口，

图 2 是盖邮戳机的方框电路图，

图 3 是盖邮戳机从后面看去的透视图，

图 4 是安全模块（第二种形式）的方框电路图，

图 5 是检测单元电路图，

图 6 是安全模块（第一种形式）的侧视图，

图 7 是安全模块（第一种形式）的顶视图，

图 8a 是安全模块（第一种形式）的右视图，

图 8b 是安全模块（第一种形式）的左视图，

图 9 是状态指示列表，

图 10 是系统中对静态和动态可变的状态的检验描述，

图 11 是安全模块（第二种形式）的侧视图，

图 12 是安全模块（第二种形式）的顶视图，

图 13a 是安全模块（第二种形式）的右视图，

图 13b 是安全模块（第二种形式）的左视图。

具体实施方式

图 1 示出安全模块 100 的方框图，安全模块具有用于连接接口 8 的连接件 101，102 和用于电池 134 的电池接口的电池连接端子 103 和 104。虽然安全模块被用固化的灌注物质灌注，安全模块 100 的电池 134 可更换地安装在电路板上灌注物质之外。电路板载有用于连接电池 134 的电极的电池连接端子 103 和 104。借助于连接件 101，102 安全模块 100 被插到主板（母板）9 的相应接口 8 上。第一个连接件 101 建立与控制装置的系统总线的通信连接，第二个连接件 102 用于系统电压对安全模块 100 的供电。经过连接件 101 的引脚 p3，p5－p19 的是地址和数据线 117，118 以及控制线 115。第一个连接件 101 和/或第二个连接件 102 被用于对安全模块 100 的插入与否进行静态和动态的监测。主板 9 的系统电压对安全模块 100 的供电通过连接件 102 的引脚 p23 和 p25 实现，并且通过引脚 p1，p2 和 p4 由安全单元 100 实现动态和动态的非插入检测。这需要一个检测单元，它通过导线回路 192，194 连接于连接件 102 的引脚 p4。导线回路可设计成安全模块 100 的特殊保安部分并且如此嵌入灌注物质中，使得在有机械或化学的袭击加到安全模块 100 的相应部分时与引脚 p4 的连接被切断。

安全模块 100 以大家所熟悉的方式具有一个微处理器 120，它具有一个图中未示出的装有专用程序的集成只读存储器（内部 ROM），该程序是邮局或邮局长官允许用于盖邮戳机的。也可以在内部数据总线 136 上连接一个常用的只读存储器 ROM 或 FLASH 存储器。

安全模块 100 以大家所熟悉的方式具有一个复位单元 130，一个专用电路 ASIC 150 和一个逻辑 PAL，它用作 ASIC 的控制信号发生器。复位单元 130，专用电路 150 和逻辑 PAL 以及可能还有其他图中未示出的存储器通过导线 191 及 129 由系统电压 U_s^+ 供电，在盖邮戳机开动时此电压由主板 9 给出。在 EP 789333A2 中已经说明了邮政安全模块 PSM 的主要部分，它实现邮费数据的结算和安全。

此外系统电压 U_s^+ 经二极管 181 和导线 136 加到电压监测单元 12

的输入端。在电压监测单元 12 的输出端给出第二个工作电压 U_b^+，它经过导线 138 供使用。在更换盖邮戳装置时不存在系统电压 U_s^+，而仅有电池电压 U_b^+供使用。连接电池负极的电池连接端子 104 接地。从连接电池正极的电池连接端子 103 给出电池电压，经导线 193，第二个二极管 182 和导线 136 加到电压监测单元的输入端。市售电压转换器 180 也可用以替代二个二极管 181，182。

电压监测单元 12 的输出通过导线 138 连接到处理器 120 第二个工作电压 U_b^+的输入端，此电压至少被连接于一个 RAM 存储区 122，124，并且只要第二个工作电压达到要求的大小，就保证上述存储区的非易失存储。最好处理器 120 含有一个内部 RAM 124 和一个实时时钟（RTC）122。

安全模块中的电压监测单元 12 具有一个可复原的自保电路，它可由处理器 120 经导线 164 查询并经导线 135 复原。电压监测单元 12 具有用于自保电路复原的电路元件。当电池电压超过规定门限值时复原才能被触发。导线 135 和 164 分别连接于处理器的一个引脚(引脚 1 和 2)。导线 164 给一个状态信号到处理器 120，导线 135 加一个控制信号到电压监测单元 12。

电压监测单元 12 输入端上的导线 136 同时用工作电压或电池电压给未插入检测单元 13 供电。未插入检测单元 13 给出状态信号在导线 139 上送到处理器 120 的引脚 5 上，此信号给出关于电路状态的指示。经过导线 139 未插入检测单元 13 的状态被处理器 120 查询。处理器可用一个从处理器 120 的引脚 4 经导线 137 给出的信号复原未插入检测单元 13。在此复原之后对连接作静态检查。为此经过导线 192 查询地电位，此地电位加在邮政安全模块 PSM 100 的接口 8 的连接端 p4 上并且仅当安全模块 100 被正常插入时才能被查询到。在插入安全模块 100 时邮政安全模块 PSM 100 的电池 134 的负极 104 的地电位加到接口 8 的连接端 p23 上，因此它可以被未插入检测单元 13 在接口 8 的连接端 p4 上通过导线 192 查询到。

在处理器 120 的引脚 6 和 7 上接一个导线回路，它经过接口 8 的连接件 102 的引脚 p1 和 p2 对于处理器 120 形成回路。为了动态检查邮政

安全模块 PSM 100 是否插入主板 9 上，处理器 120 以完全无规则的时间间隔给出变化的信号电平到引脚 6，7 上并经过导线回路返回。

邮政安全模块 PSM 100 装配有一个长寿命电池，在安全模块没有加上邮政处理装置的系统电压时它也可以监视使用情况。符合规定的使用，运行，安装或装入合适的环境是安全模块的功能单元所检查的特性。原始安装由邮政安全模块的生产者进行。在原始安装之后首先仅检查邮政安全模块是否从其使用场所（邮政处理装置）分离，这种分离通常出现在更换它的时候。

此状态的监测由未插入检测单元 13 进行。这时通过接到接口 8 的引脚 p4 上的地来监测一个电压大小。在更换功能单元时此与地的连接被断开，未插入检测单元 13 将其作为信息予以响应。因为在对安全模块 100 进行机械或化学的袭击以及每次安全模块 100 与接口 8 分离时，专用电池供电的电路结构保证了上述信息的存储，此信息的分析利用可随时进行，如果希望重新工作的话。按规律地判定检测单元 13 的导线 139 上的这个分离信号或未插入信号使处理器 120 可以清除敏感数据，而并不改变在 NVRAM 存储器中的结算和顾客数据。邮政安全模块的这种清除了敏感数据的暂时状态可理解为维护状态，通常在此状态下进行更换，修理或其他工作。因为功能单元的敏感数据被清除，由于对邮政安全模块的不符合规定的操作而产生的错误被避免了。此敏感数据例如是密钥。在维护状态下处理器 120 停止了邮政安全模块的核心功能，这些功能是例如结算和/或求取用于安全打印中安全标记的安全码。

为了恢复工作，邮政安全模块 PSM 首先被插入并与邮政处理装置的相应接口 8 建立电气连接。接着开动设备，从而邮政安全模块重又由系统电压 U_s^+ 供电。基于此特殊状态，邮政安全模块的装入是否符合规定必须由其功能单元重新检查。为此进行第二级检查（动态插入检测）。通过在第一个功能单元（处理器 120）和接口 8 的电流回路 18 之间建立的工作连接交换信息，它的无错传输证实了安装符合规定。这是成功地重新工作的先决条件。

为了进入工作状态现在只需重新初始化敏感数据。在邮政安全模块与第三个部门之间进行通信，以传递这些敏感数据。在传递完成之后未

插入检测单元 13 被复原并且邮政安全模块重新进入工作状态，重新工作过程结束。

图 2 示出盖邮戳机的方框电路图，它具有一个用于通过芯片卡装载变化数据的芯片卡读写单元 70 和一个由控制装置 1 控制的打印装置 2。控制装置 1 具有一个装配有微处理器 91 和相应存储器 92，93，94，95 的主板 9。

程序存储器 92 含有至少用于打印的工作程序，并至少含有与安全有关的程序，它用于部分有用数据的预先规定的格式转换。

工作存储器 RAM 93 用于中间结果的易失的中间存储。非易失存储器 NVM 94 用于数据的非易失中间存储，数据例如是按付费处排序的统计数据。日历/时钟 95 必要时含有可寻址的非易失存储区，用于中间结果或者公开的程序部分（例如 DES 算法）的非易失中间存储。控制装置 1 与芯片卡读写单元 70 连接，控制装置 1 的微处理器 91 被编程来装载从芯片卡 49 的存储区来的有效数据 N 到盖邮戳机的与其应用相应的存储区。插入芯片卡读写单元 70 的插槽 72 的第一张芯片卡 49 允许下载至少用于一种应用的数据组到盖邮戳机中。芯片卡 49 具有例如所有通常邮局业务按邮局价目表的邮费和一个邮局标记，以供盖邮戳机产生印记图形并给邮件盖上邮局价目。

控制装置 1 构成原来的表盘，它具有主板 9 的装置 91 至 95 并且还包含键盘 88，显示单元 89 及专用电路 ASIC 90 和用于邮政安全模块 PSM 100 的接口 8。安全模块 PSM 100 通过总线与 ASIC 100 和微处理器 91 连接，通过并行μc 总线至少与主板 9 的装置 91 至 95 和显示单元 89 连接。控制总线在安全模块 PSM 100 和 ASIC 90 之间连接信号 CE，RD 和 WR。微处理器 91 最好有一个引脚用于由安全模块 PSM 100 给出中断信号 i，其他连接端用于键盘 88，一个串行接口 S1－1 用于连接芯片卡读写单元 70，以及一个串行接口 S1－2 用于附加连接一个调制解调器。借助于调制解调器可以例如增加在邮政安全模块 PSM 100 的非易失存储器中存储的内容。

邮政安全模块 PSM 100 被包封在一个保安外壳中。每次盖邮戳之前在邮政安全模块 PSM 100 中完成硬件的结算。结算的完成与付费处无

关。邮政安全模块 PSM 100 内部可像欧洲报告 EP 789333A3 中详细说明的那样被实现。

ASIC 90 有一个对邮政业务流前接设备的串行接口电路 98，一个对打印装置 2 的传感器和执行器件的串行接口电路 96，一个对打印头 4 的打印控制电路 16 的串行接口电路，以及一个对邮政业务流后续设备中的打印装置 20 的串行接口电路。DE 19711997 是可选用的外设接口实施方案，它适用于多外设（站），其题目是：实现邮政处理机的基站和其他站之间通信及其紧急切断的配置。

与机器底座中的接口电路14连接的接口电路96提供至少与传感器 6，7，17，与执行器件，例如与辊子 11 的驱动电机 15，与喷墨打印头 4 的净化和稠度调节站 RDS 40，以及与机器底座中的标签发生器 50 的连接。主要配置和喷墨打印头 4 与 RDS 40 之间的配合关系可采用 DE 19726642C2 提出的方案，其题目是：实现喷墨打印头及净化和稠度调节装置的定位的配置。

安装在前板上的传感器 7，17 中的一个是用于信件传递中起动打印准备的传感器 17。传感器 7 用于信件传递中以起动打印为目的的信件起始识别。传送装置由一个传送带 10 和两个辊子 11，11′组成。其中一个辊子是装配有电机 15 的驱动辊子 11，另一个是从动张力辊子 11′。最好驱动辊子 11 设计成齿轮辊子，相应地传送带 10 也设计成齿轮传送带，它保证明确的力传递。编码器 5，6 与辊子 11，11′中的一个相耦合。最好驱动辊子 11 与一个增量发生器 5 一起固定安装在一根轴上。增量发生器 5 例如被设计成开槽圆盘，它与一个光栅 6 一起工作，并经导线 19 给出编码信号到主板 9。

打印头的各个打印元件在其外壳中与打印头电路相连接，并且精密电打印的打印头是可控的。打印控制基于路径控制实现，其中所选的印记配方被考虑到，此配方是通过键盘 88 或者在需要时通过芯片卡输入并非易失地存储在存储器 NVM 94 中的。计划的打印由印记配方（不打印），邮戳打印图形和必要时其他用于广告内容的打印图形，运送信息（选择打印）和附加可编辑的通知产生。非易失存储器 NVM 94 具有多个存储区。在那里非易失地存储下载的邮资表。

芯片卡读写单元 70 由相应的微处理器卡的机械载体和连接单元 74 组成。后者使得芯片卡机械上可靠地保持在读出位置上并且明确地指示芯片卡在连接单元中抵达读出位置。具有微处理器 75 的微处理器卡具有对所有类型的存储器卡及芯片卡的编程读出能力。与盖邮戳机的接口是符合 RS 232 标准的串行接口。数据传输率最低为 1.2K 波特。供电的接通借助于安装在主板上的开关 71 实现。在接通电源后进行自测并发出准备好通知。

图 3 示出盖邮戳机从后面看去的透视图，盖邮戳机由表盘 1 和基座 2 构成。后者装配有芯片卡读写单元 70，它安装在前板 20 的后面并且可从外壳上沿 22 接近它。在用开关 71 开动盖邮戳机之后芯片卡 49 从上向下插到插入槽 72 中。被送入的信件 3 立在边缘上，以其被打印的正向躺在前板上，然后它根据输入数据被打印上一个邮戳 31。信件输入开孔被透明板 21 和导向板 20 从侧面限制。插在表盘 1 主板 9 上的安全模块 100 的状态指示可通过开孔 109 从外面看到。

图 4 示出邮政安全模块 PSM 100 的一种优选形式的方框电路图。电池 134 的负极连接到地和连接件 102 的引脚 p23 上。电池 134 的正极通过导线 193 连接到电压转换器 180 的输入端，并且馈送系统电压的导线 191 与电压转换器 180 的另一输入端连接。在 PSM 100 最大用电量时寿命可达 3.5 年的 SL－380/p 型电池或寿命可达 6 年的 SL－386/p 型电池适于用作电池 134。市售 ADM 8693ARN 型电路可用作电压转换器 180。电压转换器 180 的输出端经导线 136 接到电池监测单元 12 和检测单元 13。电池监测单元 12 和检测单元 13 经过导线 135，164 和 137，139 与处理器 120 的引脚 1，2，4 和 5 建立通信连接。电压转换器 180 的输出还经过导线 136 连接到第一个存储器 SRAM 的供电输入端，该存储器在存在电池 134 时转化为第一种工艺的非易失存储器 NVRAM。

安全模块经过系统总线 115，117，118 与盖邮戳机建立连接。处理器 120 可经过系统总线和一个调制解调器 83 与远地数据中心建立通信连接。结算由 ASIC 150 完成并由处理器 120 检查。邮政结算数据被存储在不同工艺的非易失存储器中。

系统电压加到第二个存储器 NV－RAM 114 的供电输入端。它是第

二种工艺的非易失存储器 NVRAM，（SHADOW－RAM）。此第二种工艺最好包含一个 RAM 和一个 EEPROM，其中后者在系统电压中断时自动保存数据内容。第二种工艺的 NVRAM 114 经过内部地址总线和数据总线 112，113 与 ASIC 150 的相应地址输入端和数据输入端相连接。

ASIC 150 至少包含一个用于计算要存储的邮政数据的硬件结算单元。在可编程阵列逻辑（PAL）160 中安排了 ASIC 150 上的存取逻辑。ASIC 150 受逻辑 PAL 160 控制。主板 9 的地址总线和数据总线 117，115 连接到逻辑 PAL 160 的对应引脚上，并且 PAL 160 至少产生一个用于 ASIC 150 的控制信号和一个对程序存储器 FLASH 128 的控制信号 119。处理器 120 运行一个程序，它存储在 FLASH 128 中。处理器 120，FLASH 28，ASIC 150 和 PAL 160 通过模块内部的系统总线相互连接，总线包括用于数据信号，地址信号和控制信号的导线 110，111，126，119。

安全模块 100 的处理器 120 通过内部数据总线 126 与 FLASH 128 和 ASIC 150 连接。FLASH 128 由系统电压 U_s^+供电。例如它是一个 128K 字节的 AM29F01045EC 型 FLASH 存储器。邮政安全模块 100 的 ASIC 150 通过模块内部的地址总线 110 将地址 0 至 7 接到 FLASH 128 的对应地址输入端上。安全模块 100 的处理器 120 通过内部地址总线 111 将地址 8 至 15 接到 FLASH 128 的对应地址输入端上。安全模块 100 的 ASIC 150 通过接口 8 的连接件 101 与主板 9 的数据总线 118，地址总线 117 和控制总线 115 建立连接。

处理器 120 具有存储器 122，124，从电压监测单元 12 来的工作电压 U_b^+通过导线 138 给它们供电。尤其是一个实时时钟 RTC 122 和存储器 RAM 128 通过导线 138 由工作电压供电。电压监测单元（电池观测器）12 还给出一个状态信号 164 并响应控制信号 135。电压转换器 180 给出输出电压到导线 136 上对电池观测器 12 和存储器 116 供电，其输出电压是其二个输入电压中大的那一个。由于此电路根据电压 U_s^+和 U_b^+的大小自动用两个中较大的一个供电，因此在正常工作时电池 134 可被更换而不会发生数据丢失。

在上述方式下，在正常工作之外的停止运行时间内由安全模块 100

的电池 134 给实时时钟（RTC）122 和/或静态 RAM（SRAM）124 供电，该时钟具有日期和/或时期时间寄存器，SRAM 保存安全相关的数据。如果在电池工作时电池电压降到规定门限值以下，则由电压监测单元 12 将 RTC 和 SRAM 的馈电点接地，直到其复原，于是 RTC 和 SRAM 的供电电压为 0 伏。这导致包含例如重要的密钥的 SRAM 124 很快被清零。同时 RTC 122 的寄存器也被清除并且丢失实时时钟时间和实时日期。通过上述动作避免了在可能受到通过操纵电池电压进行的袭击时盖邮戳机时钟 122 的停止和安全相关不丢失。从而不再需要像例如长时间定时器或监视器这样的安全措施来对付袭击。所用的安全措施借助于图 9 和图 10 详细说明。

复位单元 130 通过导线 131 与处理器 120 的引脚 3 和 ASIC 150 的一个连接。处理器 120 和 ASIC 150 在供电电压下降时被复位单位 130 中产生的复位信号复位。

同时上述电路与电池低电压指示一起进入自保状态，即使后来电压升高了也仍保持在此状态。在下一次开通模块时处理器可查询电路的状态（状态信号）和/或通过读取被清除的存储器的内容来判定在前面时间中电池电压曾经降到规定值以下。处理器可复原监测电路，即恢复其功能。

未插入检测单元 13 为了测量输入电压，有一根导线 192 经过安全模块的插脚和接口 8，最好经盖邮戳机母板 9 上的一个插座与地连接。此测量用作是否插入的静态监测并构成第一级监测的基础。未插入检测单元 13 具有用于可复原自保电路的电路元件，并且当测量电压线 192 上的电压偏离规定电位时自保电路起动。同时被编程并与其他功能连接的处理器 120 根据应用逻辑保持或改变安全模块 100 的相应状态。自保电路的状态经过导线 139 被安全模块 100 的处理器 120 查询。当安全模块 100 正常插入时导线 192 上的测量电压电位对应地电位，导线 139 上为工作电压电位。当安全模块 100 没插入时地电压电位在导线 139 上。处理器 120 的第 5 引脚接导线 139，以查询未插入检测单元 13 的状态：是否该引脚由自保电路接到地电位上。为了经过导线 137 复原未插入检测单元 13 的自保电路，处理器 120 采用其第 4 引脚。

此外还存在一个电流回路 18，它通过安全模块的插脚和盖邮戳机主板 9 上的插座将处理器 120 的引脚 6 和 7 相互连接起来。处理器 120 的引脚 6 和 7 上的导线仅当 PSM 100 插入主板 9 上时才连接成电流回路 18。这个回路构成第二级上动态监测安全模块是否插入的基础。

处理器 120 内部有一个处理单元 CPU 121，一个实时时钟 RTC 122，一个 RAM 单元 124 和一个输入/输出单元 125。处理器 120 的引脚 8，9 输出至少一个信号用以指示安全模块 100 的状态。引脚 8 和 9 连接输入/输出单元 125 的 I/O 口，其上接有模块内部的指示装置，例如彩色发光二极管 LED 107，108，它们指示安全模块 100 的状态。安全模块在其寿命期内可处于不同的状态下。因而例如必须检测模块是否含有有效密钥。此外判定模块功能正常还是有故障也是重要的。模块状态的精确类型和数量与模块实现的功能和实现有关。

下面借助图 5 说明检测单元 13 的电路。未插入检测单元 13 具有一个分压器，它由电阻 1310，1312，1314 的串联电路构成，此分压器接在连接电容器 1371 的供电电压电位与导线 192 上的测量电位之间。电路通过导线 136 由系统电压或电池电压供电。导线 136 的供电电压通过二次管 1369 到达电路的电容器 1371 上。电路的输出侧有一个反相器 1320，1398。在正常状态下反相器的晶体管 1320 截止，供电电压经过电阻 1398 加到导线 139 上，所以在正常状态下输出逻辑 '1' 即高电平。最好导线 139 上的低电平作为未插入状态信号，因为这样在处理器 120 引脚 5 中没有电流流进，这将增加电池寿命。二极管 1369 最好与电解电容器 1371 一起供电，使得导线 136 上的电压被切断后，反相器前面的电路在一个相对长的时间期（大于 2s）内仍得到供电电压，保证其功能。

分压器 1310，1312，1314 有一个引出头 1304，其上连接电容器 1306 和比较器 1300 的同相输入端。比较器 1300 的反相输入端连接参考电压源 1302。比较器 1300 的输出一方面经反相器 1320，1398 连接导线 139，另一方面与自保电路元件 1322 的控制输入端连接。电路元件 1322 与分压器的电阻 1310 并联，电路元件 1316 用来复原自保电路，它接在引出头 1304 和地之间。分压器的引出头 1304 位于电阻 1312 和 1314 的连接

点。接在引出头 1304 和地之间的电容器 1306 阻止振荡。分压器的引出头 1304 上的电压在比较器 1300 中与源 1302 的参考电压比较。如果引出头 1304 上被比较的电压小于源 1302 的参考电压，比较器输出保持低电平，反相器的晶体管 1320 截止。这样导线 139 具有工作电压电位，状态信号为逻辑“1”。分压器被设计成使得在导线 192 为地电位时引出头 1304 上的电压可靠地低于比较器 1300 的切换门限。如果因为安全模块 100 从主板 9 的插座或盖邮戳机接口 8 脱离而使得连接被切断且导线 192 不再接地，则引出头 1304 上的电压超过参考电压源 1302 的电压，比较器 1300 反转。比较器输出切换为高电平，晶体管 1320 导通。这样导线 139 接地电位，状态信号为逻辑‘0’。

借助于与分压器的电阻 1310 并联的晶体管 1322 实现未插入检测单元 13 的自保电路。晶体管 1322 的控制输入端被比较器输出端接到高电平上。因而晶体管 1322 导通并且跨接在电阻 1310 上，从而电压分压器仅还由电阻 1312 和 1314 构成。这样切换门限被进一步提高，使得当因重新插入安全模块而使导线 192 重又接到地电位时比较器仍保持在反转状态。

电路的状态可通过导线 139 上的信号由处理器 120 查询。

未插入检测单元 13 具有用来复原自保电路的电路元件：导线 137 和电路元件 1316。复原由处理器 120 通过导线 137 上的信号触发。

处理器 120 可随时通过专用电路 ASIC 150，第一个连接件 101，控制装置 1 的系统总线，以及例如通过微处理器 91 经调制解调器与远地数据中心建立接触，此中心检查结算数据并必要时传送其他数据到处理器 120。安全模块 100 的专用电路 ASIC 150 经过模块内部的数据总线 126 与处理器 120 连接。

在借助于传送的数据成功地结束了重新初始化之后，处理器 120 可复原未插入检测单元为此通过加到导线 137 上的复原信号使晶体管 1316 导通，从而引出头 1304 上的电压被拉到源 1302 的参考电压以下并且晶体管 1320 和 1322 截止。在正常状态下晶体管 1322 截止，电阻 1310 和 1312 串联构成上述分压器的上面部分，从而切换门限重又降到原来状态。

图 6 示出安全模块机械结构的侧视图。此安全模块构造成多芯片模块，即多个功能单元装在一块电路板 106 上。安全模块 100 用固化的灌注物质 105 灌注，其中安全模块 100 的电池 134 可更换地安装在电路板 106 上灌注物质 105 之外。例如，如此用灌注物质 105 灌注，使得指示装置 107，108 在第一个位置处从灌注物质中伸出，并且电路板 106 带着被安放的电池 134 从侧面第二个位置处伸出。此外电路板 106 还具有用来连接电池 134 的电极的电池连接端子 103 和 104，它最好在电路板 106 上方元件安装面上。为了插邮政安全模块 PSM 100 在表盘 1 的主板上，连接件 101 和 102 被安装在安全模块 100 的电路板 106 的下面（线路面）。专用电路 ASIC 150 通过第一个连接件 101 以图中未示出的方式与控制装置 1 的系统总线建立通信连接，第二个连接件 102 用于系统电压对安全模块 100 的供电。若安全模块已插在主板上，然后最好这样将它装在表盘外壳中，使得指示装置 107，108 接近或者伸进开孔 109 中。表盘外壳最好如此构造，使得使用者能从外面看到安全模块的状态指示。指示装置的两个发光二极管 107 和 108 由处理器 120 引脚 8，9 上 I/O 口的两个输出信号控制。两个发光二极管被安置在一个共同的元件壳中（双彩色发光二极管），这样开孔的偏差及直径可保持相对小些并在指示装置的数量级之内。原则上可呈现三种不同的颜色（红、绿、橙）。为区别状态也可使 LED 闪烁，这样可以区分 8 种不同的状态组，它们用以下的 LED 状态来表示：LED 绿色亮，LED 红色亮，LED 橙色亮，LED 红色闪，LED 绿色闪，LED 橙色闪，LED 红色亮和橙色闪，以及 LED 绿色亮和橙色闪。

图 7 示出邮政安全模块的顶视图。

图 8a 和 8b 示出分别从右或从左看去的安全模块的视图。从图 8a 和 8b，结合图 6 可清楚看出电路板 106 下面连接件 101 和 102 的位置。

按照图 9 所示的状态指示表，得到多个可能的状态指示。绿色 LED 107 亮指示正常状态 220，而 LED 108 亮指示至少静态自测结果错误的错误状态 230。由于直接经 LED 107，108 指示，这种自测的结果不能被篡改。

例如对于以下情况：在前面时间内安全模块中存储的密钥已经丢

失，在动态工作中进行的检查确认错误，则橙色 LED 亮指示这种状态 240。在一次关断/开动之后要求一个起动过程，因为否则就不能完成其他工作。在生产时忘了安装密钥的情况作为状态 260 例如用绿色 LED 107 闪来指示。

第一个功能单元是处理器 120，它不断地判断第二个借贷天数是否已用尽。在其用尽时，一个长时间定时器运行期满。如果有太长的时间数据中心没有被接触，例如为了装载余额的接触，则长时间定时器运行期满。例如数据中心可规定 90 天作为借贷天数，并在安装或装载时装入安全设备的存储器 124 中。在运行了 90 天后一个“丢失”状态 250 用红色 LED 闪来指示。长时间定时器最好是一个回退计数器，它在处理器 120 中实现。因为当时间期满时计数器达到状态零，在“状态抵达后”，安全模块与表盘分开时保持状态 250。如果离前次与数据中心的接触已如此之久，以致已产生怀疑，则指示怀疑状态 270。最好一个也是实现在处理器 120 中的回退计数器不断地判断例如 30 天的第一个借贷天数是否已用尽。

对状态 280 和 290 的状态指示可选用于其他各种检查。为此可用其他功能单元于模块中，特别是一个温度敏感元件。例如若超过某一能引起安全模块损坏的温度，此状态 280 可用 LED 107，108 指示，它们红色亮，橙色闪，并且引起交替地红色/橙色闪的总体效果。第二个功能单元可在必要时监测电池电压，其容量是否已用尽。最好要求更换电池的状态 290 用 LED 107，108 指示：绿色亮，橙色闪，并且引起交替地绿色/橙色闪的总体效果。

图 10 示出系统中对静态和动态可变的状态的检查。处在状态 200 下的关机系统在开机后经转换线“起动”201 转到状态 210，此状态下在加上工作电压后立即由安全模块进行一次静态自测。转换线 202 发生在自测给出正常结果（OK）时，它转换到状态 220，用 LED 107 绿色亮指示。在此状态下根据需要可进行重复静态自测，动态寿命测试，至少一个周期性的借贷时间测试和其他测试。在测试结果正常时这些测试按图中转换线 203 引回到状态 220 LED 绿色亮。在动态自测确认故障时转换线 206 引导到状态 240，LED 橙色亮。此故障可通过复原尝试即通

过设备的关机（转换线 211）和再开机（转换线 201）来排除。然而静态故障是不能排除的。在状态 210 下已开机的设备进行一次静态自测，当有故障时由转换线 204 转到状态 230，LED 108 红色亮。在任何时间如果设备处于状态 220（LED 绿色），一次根据命令而进行的静态自测在有故障时经转换线 205 转到状态 230（LED 红色）。从状态 220（LED 绿色）出发的其他转换线 207，208，209 引导到状态 270，250，260。状态 270 用 LED 107，108 橙色闪指示，它表示应该建立与数据中心的连接，因为安全设备已被怀疑。装载产生的转换线 212 重又抵达状态 210。

在状态 250 下用 LED 108 红色闪指示“丢失”状态。在处理器 120 的自测说明有必要装载密钥时，转移线 209 抵达 LED 107 绿色闪的状态 260。

从状态 220（LED 107 绿色）出发能可选地不是转移到 LED 红色亮/橙色闪的状态 280，就是转移到 LED 绿色亮/橙色闪的状态 290。在第一个可选的转移中温度测量产生更换整个安全模块的需要。在后一个转换时电池的容量测量给出更换电池的要求。

图 11 示出按照第二种形式的安全模块机械结构侧视图。安全模块也构造成多芯片模块，并且用固化的灌注物质 105 灌注，其中安全模块 100 的电池 134 可更换地安装在电路板 106 上灌注物质 105 之外。由于费用的原因，用灌注物质 105 在第一个位置处如此灌注，使得指示装置 107，108 和插入的电池 134 在灌注物质之外电路板 106 的上面第二个位置处。电路板 106 也具有用来连接电池 134 的电极的电池连接端子 103 和 104，它最好在电路板 106 上方元件安装面上。在此形式中指示装置的两个发光二极管 107 和 108 是分开的元件。指示装置的两个发光二极管 107 和 108 由处理器 120 引脚 8，9 上 I/O 口的两个输出信号控制。为了区分状态，LED 也可以控制成闪烁，这样可区别各种状态组合。表盘外壳也构造成使得使用者能从外部看到安全模块的状态指示，例如通过一个视窗或一个开孔 109 看到状态指示。

为了插邮政安全模块 PSM 100 在表盘 1 的主板上，连接件 101 和 102 被安装在安全模块 100 的电路板 106 的下方。最好连接件 101 和 102

具有一个焊接头 127，并且焊接头 127 安装在电路板 106 的线路面上。

图 12 是第二种形式邮政安全模块的顶视图。灌注物质 105 以方形包住电路板 106 的第一部分，而电路板 106 的第二部分在灌注物质之外，这一部分用于安装两个发光二极管 107 和 108，可更换地安装的电池 134 和焊接头 127（此图中看不见）。电池连接端子 103 和 104 在图 12 中被电池遮挡住，但是在图 13a 的侧视图中与焊接头 127 同样是可见的。

电路板 106 的第一部分的灌注既不开孔也不增高，这样给犯罪企图中的操纵提供小的攻击点。灌注物质最好是双成份环氧树脂或聚合物及塑料。EMERSON & CUMING 公司的 STYCAST® 2651－40FR 适于用作灌注物质，最好用 CATALYST9 作为第二种成份。在生产中两种成份被混合后涂敷在电路板 106 的第一部分板的两个侧面上。这可例如通过浸入流动的混合物中实现。然后一层保护层和/或传感层被覆盖上，这一层在最外层灌注后从外部是看不见的，它在灌注物质 105 固化时与其牢固地结合在一起。在最外层灌注之后灌注物质固化为坚固且不透明的灌注物质 105。

图 13a 和 13b 示出第二种形式安全模块的右视图和左视图。由图 13a 和 13b，结合图 12 可清楚地看到电路板 106 下面具有连接件 101 和 102 的焊接头 127 的位置。

此外，焊接头 127 也可以例如用图中未示出的方式安装在电路板 106 第二部分的上表面上。

原则上当然也可以采用与邮政设备相连接的另一个指示装置。

按照本发明邮政设备主要是盖邮戳机。安全模块可以经相应邮局同意用作邮政安全设备 PSD（POSTAL SECURITY DEVICE）。

安全模块及 PSD 也具有其他结构形式，可以例如插在个人计算机的主板上，它作为 PC－盖邮戳机控制一台市售的打印机。

本发明不限于上述实施形式，公开的本发明的其他的配置和实施方案可以被开发和利用，它们从本发明的基本思路出发并被包含在本发明保护范围中。

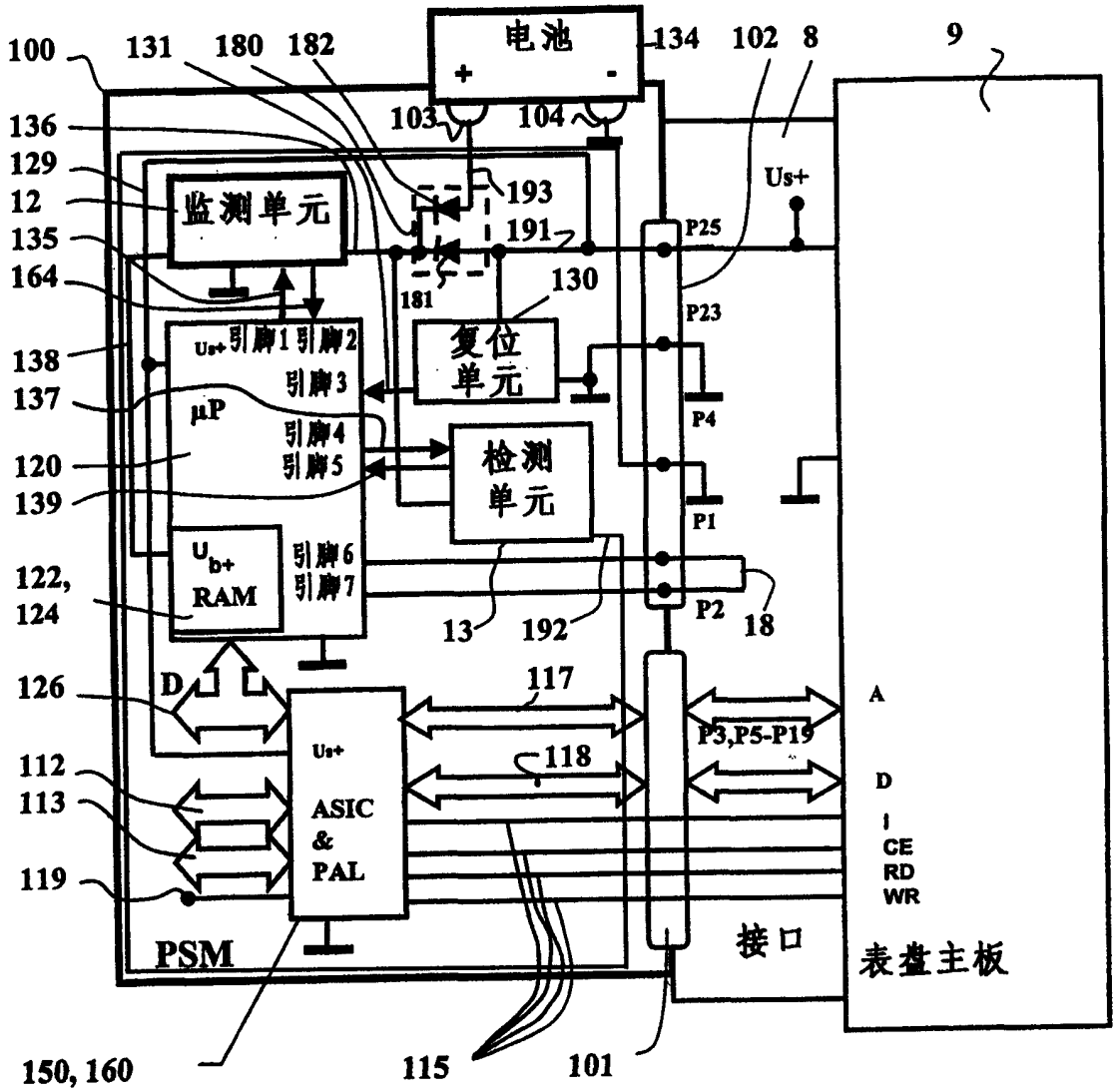

电池
+
-
100
131
180
182
134
102
8
9
136
103
104
129
193
Us+
12
监测单元
191
P25
135
181
130
164
P23
Us+
引脚1
引脚2
138
复位
单元
引脚3
P4
137
μP
引脚4
检测
单元
120
引脚5
139
P1
U_{b+}
RAM
引脚6
引脚7
122,
124
13
192
P2
18
126
D
117
A
P3,P5-P19
Us+
112
118
D
ASIC
&
PAL
I
113
CE
RD
WR
119
PSM
接口
表盘主板
150, 160
115
101

图1

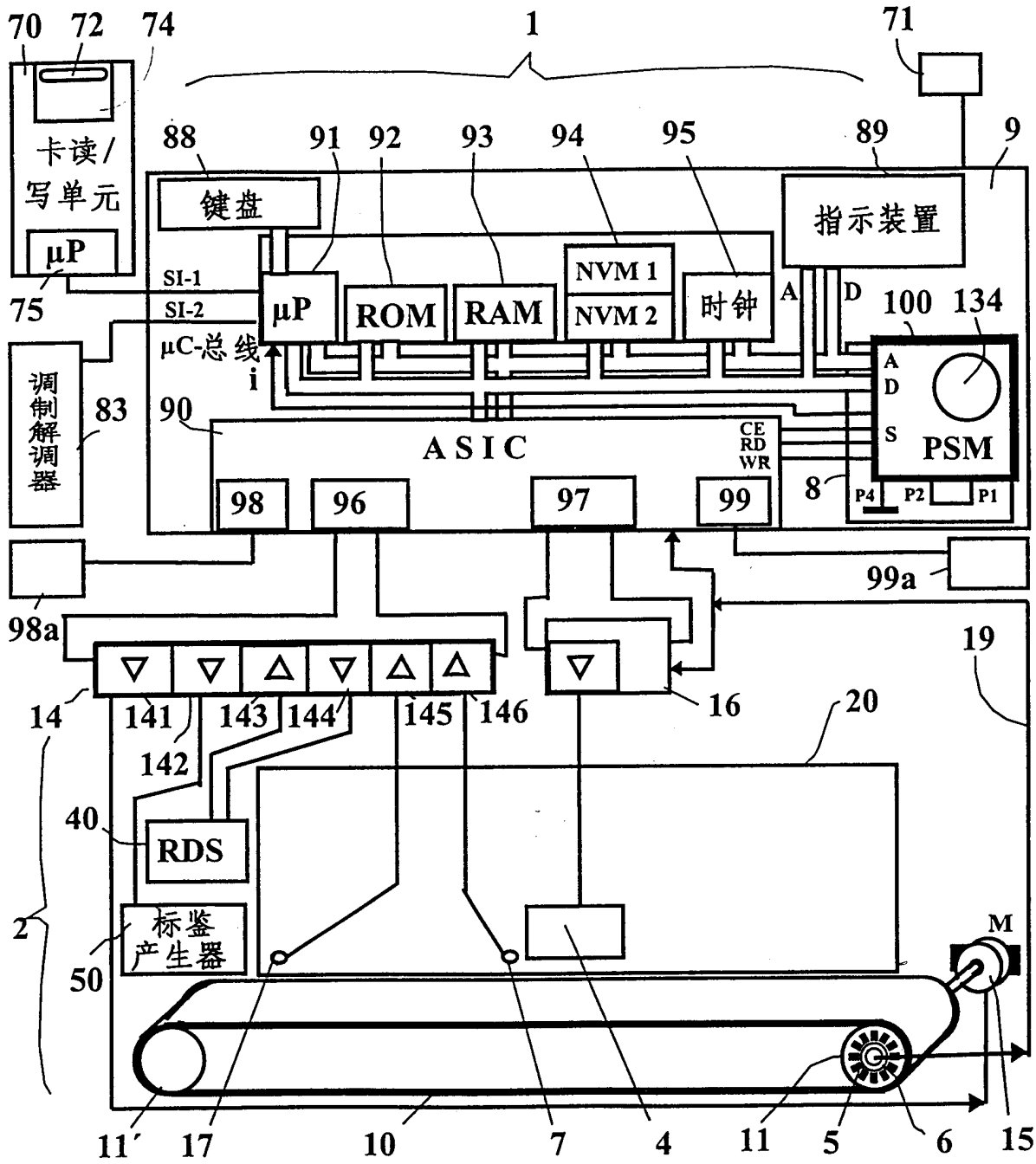
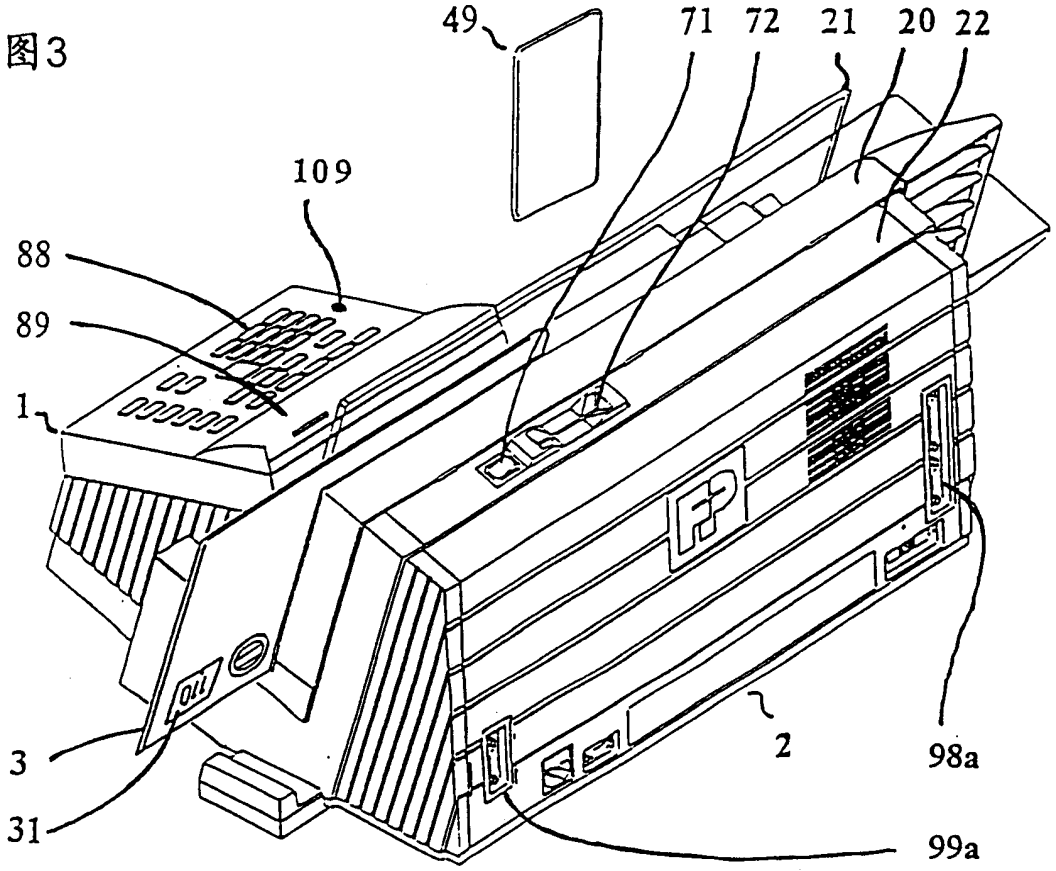

70
72
74
1
71
卡读/
写单元
μP
75
88
91
92
93
94
95
89
9
键盘
指示装置
SI-1
SI-2
μP
ROM
RAM
NVM 1
NVM 2
时钟
A
D
100
134
μC-总线
i
调制解调器
83
90
ASIC
CE
RD
WR
A
D
S
PSM
98
96
97
99
8
P4
P2
P1
99a
98a
19
14
141
143
144
145
146
16
20
142
40
RDS
2
标鉴
产生器
50
M
11′
17
10
7
4
11
5
6
15

图2

图3



状态号	发光二极管	亮	闪	灭	指示	说明
220	R			X	- 绿-亮	正常
	G	X				
230	R	X			-红-亮	静态检查错误
	G			X		
240	R	X			-橙-亮	动态检查错误
	G	X				
250	R		X		- 红-闪	与数据中心长时间无接触
	G			X		
260	R			X	-绿-闪	未装密钥
	G		X			
270	R		X		-橙-闪	怀疑
	G		X			
280	R	X			红-亮 橙-闪	温度过高
	G		X			
290	R		X		绿-亮 橙-闪	需更换电池
	G	X				

图9

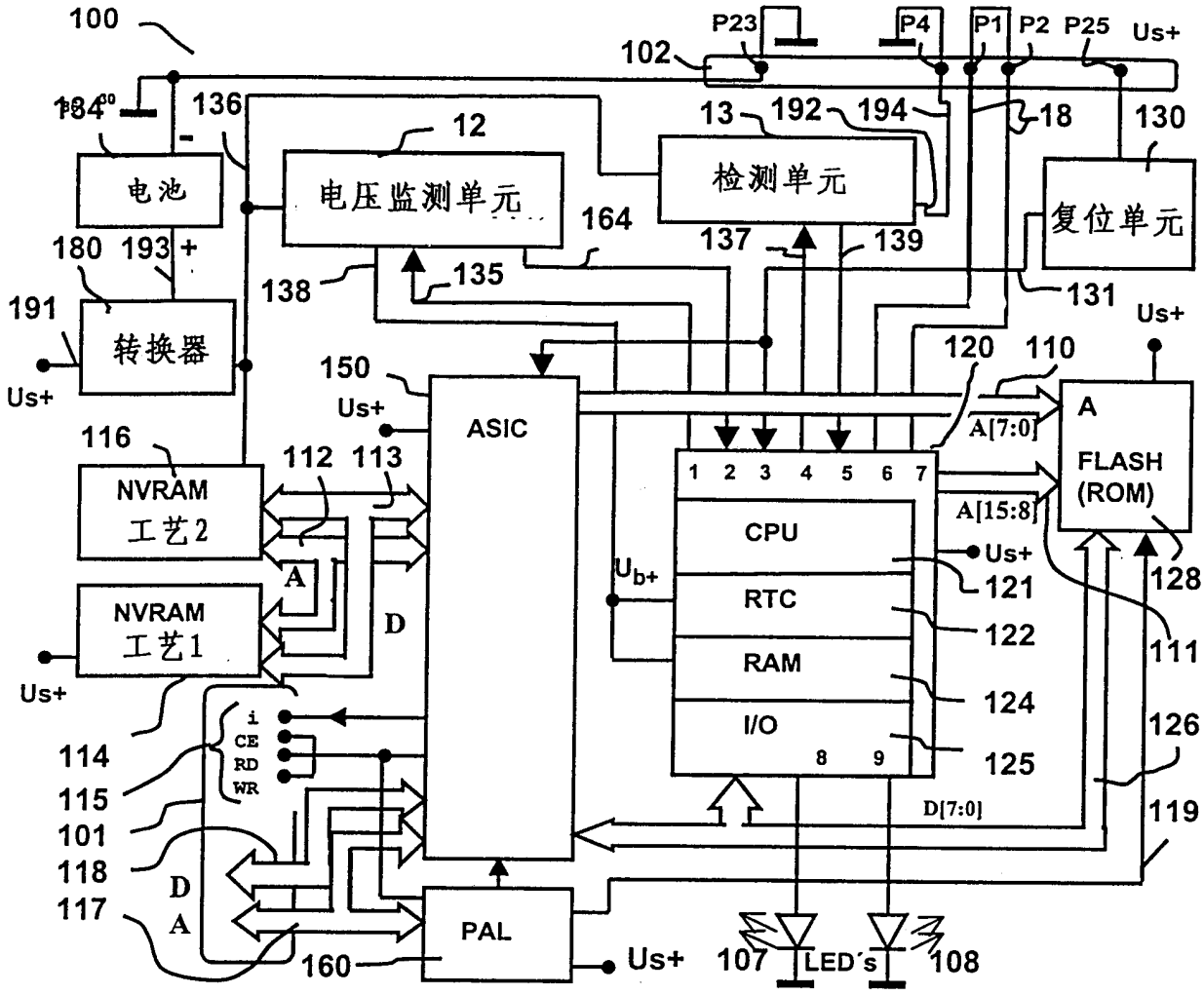

100
102
P23
P4
P1
P2
P25
Us+
184
136
12
电压监测单元
13
192
194
18
130
检测单元
复位单元
电池
180
193
164
137
139
138
135
131
191
转换器
Us+
150
120
110
ASIC
A
FLASH
(ROM)
A[7:0]
116
112
113
NVRAM
工艺2
1 2 3 4 5 6 7
A[15:8]
CPU
Us+
U_{b+}
121
128
NVRAM
工艺1
A
D
RTC
122
111
RAM
124
126
i
CE
RD
WR
I/O
8 9
125
114
115
101
118
117
D
A
D[7:0]
119
PAL
160
Us+
107
LED's
108

图4

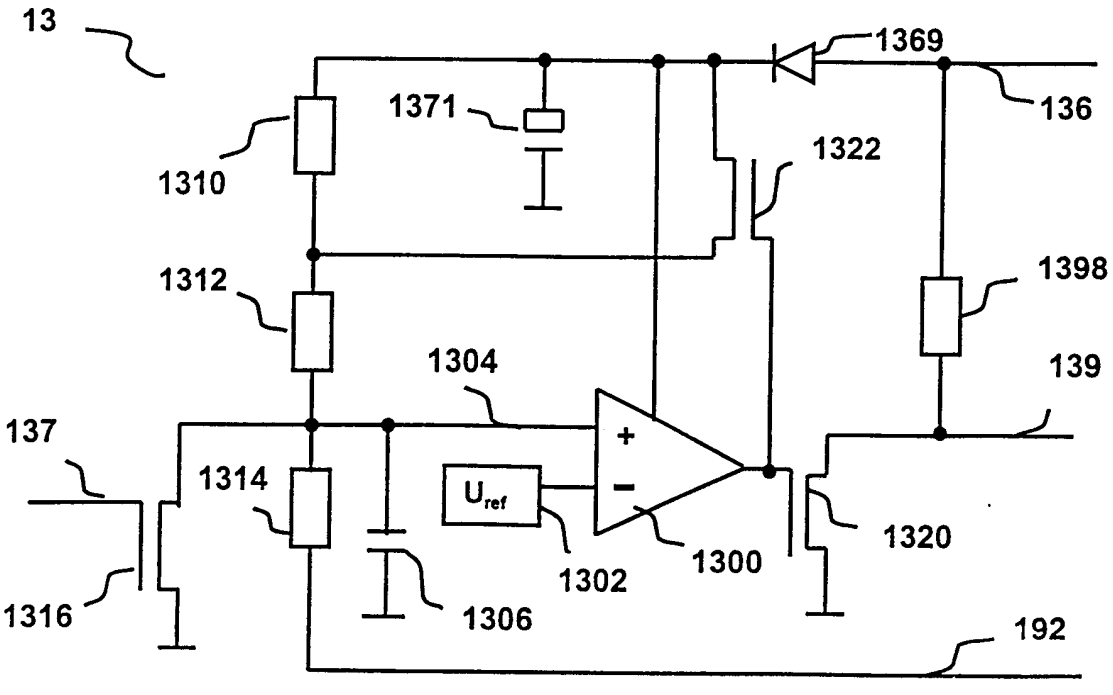

13
1369
1371
136
1310
1322
1312
1398
1304
139
137
1314
U_{ref}
1320
1316
1302
1300
1306
192

图5

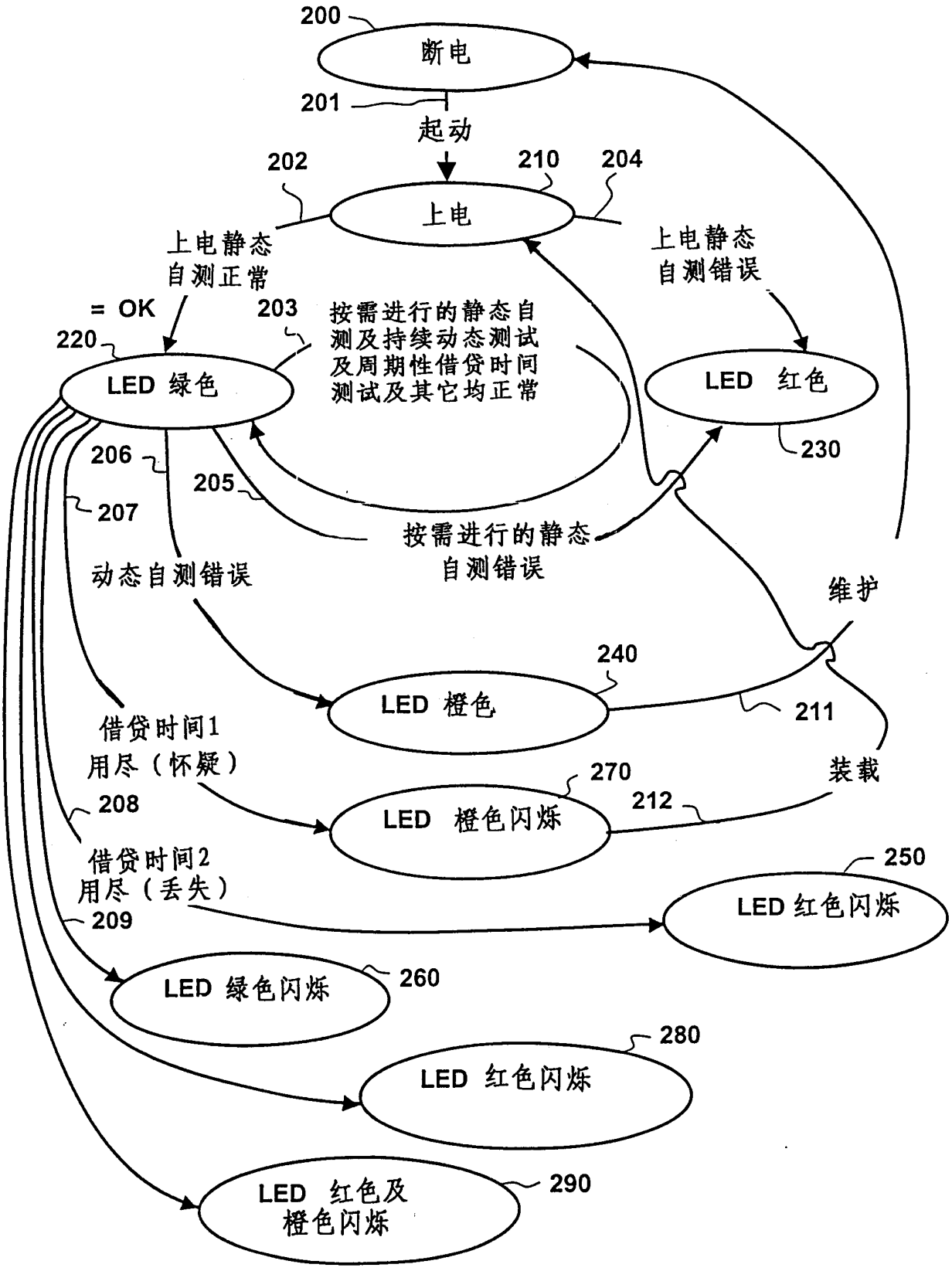

200
断电
201
起动
202
210
204
上电
上电静态
自测正常
= OK
上电静态
自测错误
203
按需进行的静态自
测及持续动态测试
及周期性借贷时间
测试及其它均正常
220
LED 绿色
LED 红色
230
206
205
207
按需进行的静态
自测错误
动态自测错误
维护
240
LED 橙色
211
借贷时间1
用尽（怀疑）
装载
270
208
LED 橙色闪烁
212
借贷时间2
用尽（丢失）
250
209
LED 红色闪烁
LED 绿色闪烁
260
280
LED 红色闪烁
LED 红色及
橙色闪烁
290

图10

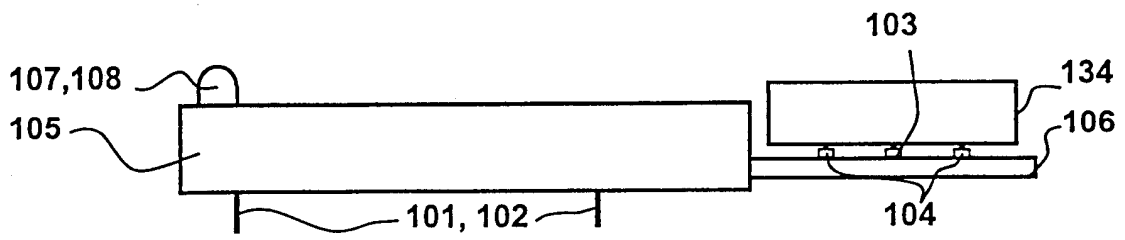

103
107,108
134
105
106
101, 102
104

图 6

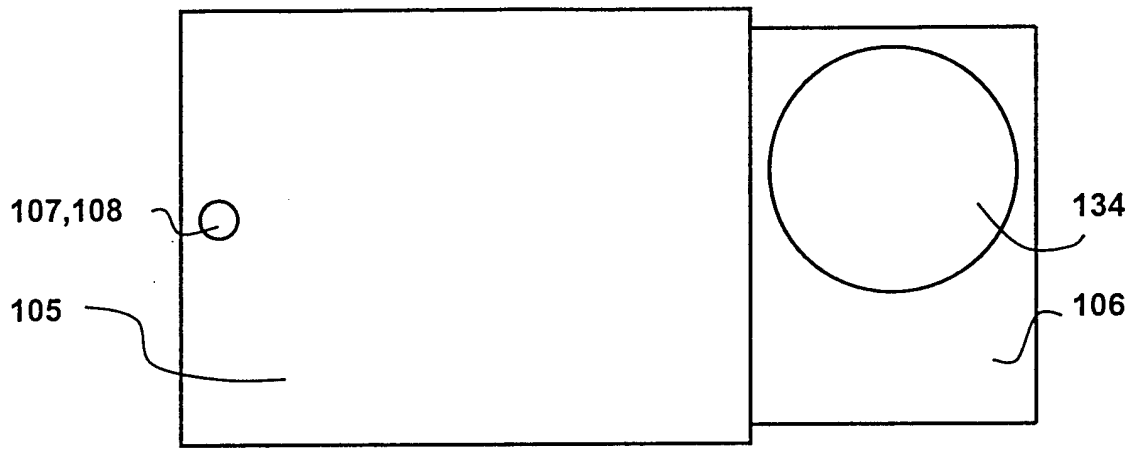

107,108
134
105
106

图7

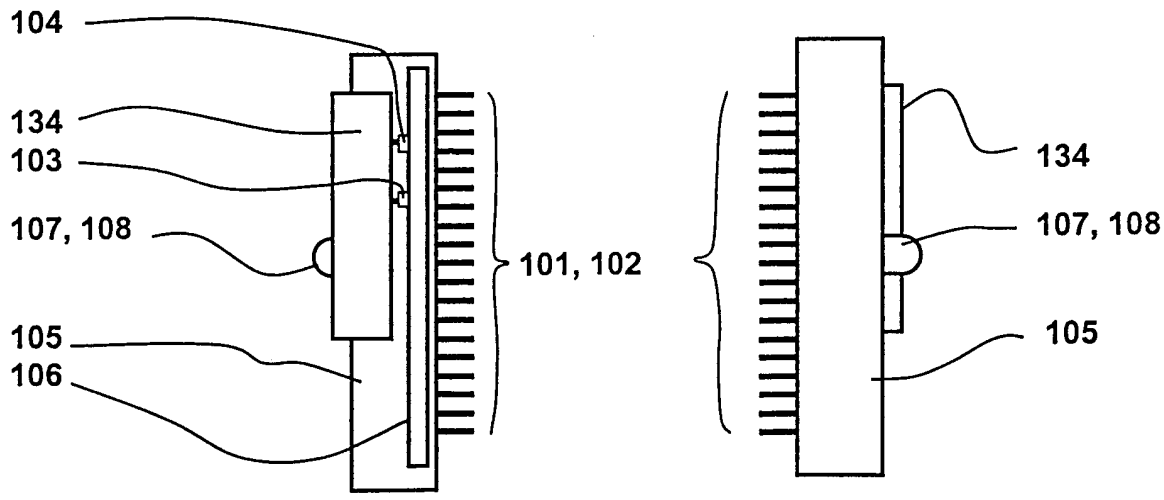

104
134
103
107, 108
101, 102
105
106
134
107, 108
105

图 8a 图8b

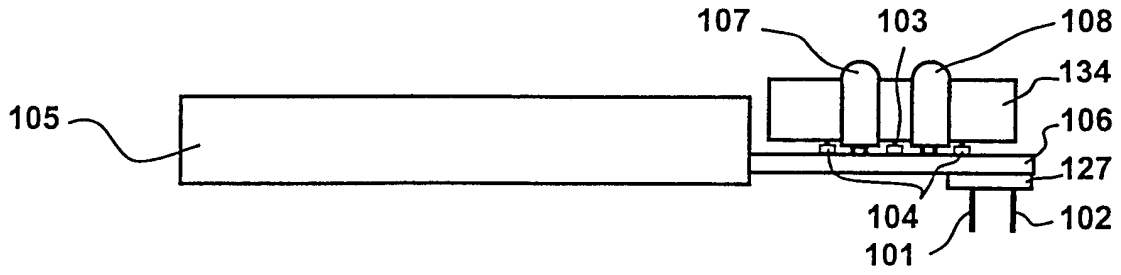


图11

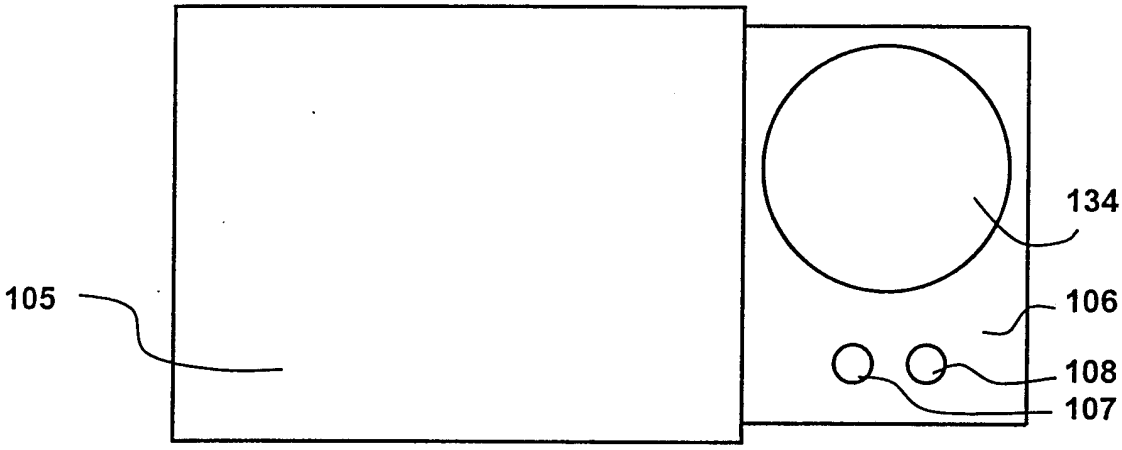


图12

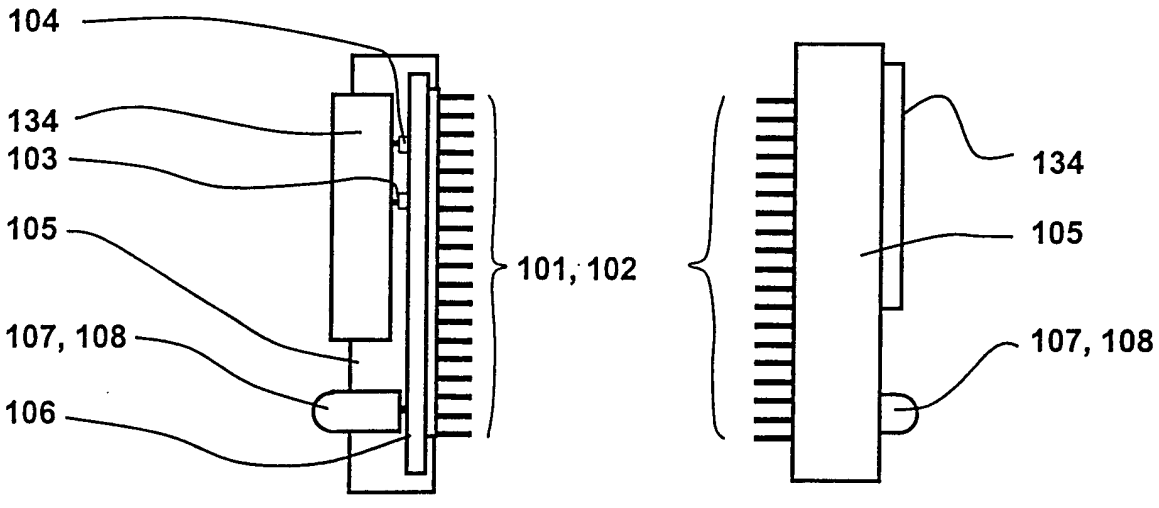


图13a 图13b