(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 035 516 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
09.07.2008 Patentblatt 2008/28

(51) Int Cl.:
G07B 17/00 *(2006.01)* ***G07B 17/04*** *(2006.01)*

(21) Anmeldenummer: **00250055.1**

(22) Anmeldetag: **21.02.2000**

(54) **Anordnung für ein Sicherheitsmodul**

Arrangement for a security module

Système pour un module de sécurité

(84) Benannte Vertragsstaaten:
CH DE FR GB IT LI

(30) Priorität: **12.03.1999 DE 19912780**

(43) Veröffentlichungstag der Anmeldung:
13.09.2000 Patentblatt 2000/37

(73) Patentinhaber: **Francotyp-Postalia GmbH**
16547 Birkenwerder (DE)

(72) Erfinder:
- **Post, Peter**
  12357 Berlin (DE)
- **Rosenau, Dirk**
  13469 Berlin (DE)
- **Schlaaff, Torsten**
  16341 Zepernick (DE)

(56) Entgegenhaltungen:
WO-A-98/20461
GB-A- 2 303 173
US-A- 4 575 621
US-A- 5 097 253
US-A- 5 353 350
US-A- 5 515 540

- **USPS, UNITED STATES POSTAL SERVICE: INFORMATION BASED INDICIA PROGRAM, POSTAL SECURITY DEVICE SPECIFICATION, 13. Juni 1996 (1996-06-13), XP002137734**

EP 1 035 516 B1

Beschreibung

[0001] Die Erfindung betrifft eine Anordnung für ein Sicherheitsmodul, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art. Ein solcher postalischer Sicherheitsmodul ist insbesondere für den Einsatz in einer Frankiermaschine bzw. Postbearbeitungsmaschine oder Computer mit Postbearbeitungsfunktion geeignet.

[0002] Moderne Frankiermaschinen, wie die aus der US 4.746.234 bekannte Thermotransfer-Frankiermaschine, setzen eine vollelektronische digitale Druckvorrichtung ein. Damit ist es prinzipiell möglich, beliebige Texte und Sonderzeichen im Frankierstempeldruckbereich und ein beliebiges oder ein einer Kostenstelle zugeordnetes Werbeklischee zu drucken. So hat zum Beispiel die Frankiermaschine T1000 der Anmelderin einen Mikroprozessor, welcher von einem gesicherten Gehäuse umgeben ist, das eine Öffnung für die Zuführung eines Briefes aufweist. Bei einer Briefzuführung übermittelt ein mechanischer Briefsensor (Mikroschalter) ein Druckanforderungssignal an den Mikroprozessor. Der Frankierabdruck beinhaltet eine zuvor eingegebene und gespeicherte postalische Information zur Beförderung des Briefes. Die Steuereinheit der Frankiermaschine nimmt eine Abrechnung softwaremäßig vor, übt eine Überwachungsfunktion ggf. bezüglich der Bedingungen für eine Datenaktualisierung aus und steuert das Nachladen eines Portwertguthabens.

[0003] Für die oben genannte Thermotransfer-Frankiermaschine wurde bereits in US 5,606,508 (DE 42 13 278 B1) und in US 5,490,077 eine Dateneingabemöglichkeit mittels Chipkarten vorgeschlagen. Eine der Chipkarten lädt neue Daten in die Frankiermaschine und ein Satz an weiteren Chipkarten gestattet durch das Stecken einer Chipkarte eine Einstellung entsprechend eingespeicherter Daten vorzunehmen. Das Datenladen und die Einstellung der Frankiermaschine kann damit bequemer und schneller als per Tastatureingabe erfolgen. Eine Frankiermaschine zum Frankieren von Postgut, ist mit einem Drucker zum Drucken des Postwertstempels auf das Postgut, mit einer Steuerung zum Steuern des Drukkens und der peripheren Komponenten der Frankiermaschine, mit einer Abrecheneinheit zum Abrechnen von Postgebühren, mit mindestens einem nichtflüchtigen Speicher zum Speichern von Postgebührendaten, mit mindestens einem nichtflüchtigen Speicher zum Speichern von sicherheitsrelevanten Daten und mit einer Kalender/Uhr ausgestattet. Der nichtflüchtige Speicher der sicherheitsrelevanten Daten und/oder die Kalender/Uhr wird gewöhnlich von einer Batterie gespeist. Bei bekannten Frankiermaschinen werden sicherheitsrelevante Daten (kryptografische Schlüssel u.ä.) in nichtflüchtigen Speichern gesichert. Diese Speicher sind EEPROM, FRAM oder batteriegesicherte SRAM. Bekannte Frankiermaschinen verfügen oft auch über eine interne Echtzeituhr (Real Time Clock) RTC, die von einer Batterie gespeist wird. Bekannt sind z.B. vergossene Module, die integrierte Schaltkreise und eine Lithium-Batterie enthalten. Diese Module müssen nach Ablauf der Lebensdauer der Batterie im Ganzen ausgetauscht und entsorgt werden. Aus wirtschaftlichen und ökologischen Gesichtspunkten ist es günstiger, wenn nur die Batterie ausgetauscht werden muß. Dazu muß jedoch das Sicherheitsgehäuse geöffnet und anschließend wieder verschlossen und gesiegelt werden, denn die Sicherheit gegenüber Betrugsversuchen beruht im Wesentlichen auf dem gesicherten Gehäuse, welches die gesamte Maschine umschließt.

[0004] Seitens der Anmelderin wurde in EP 660 269 A2 (US 5,671,146) bereits ein geeignetes Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen vorgeschlagen, in welchem zwischen einem authorisierten und unauthorisierten Öffnen des Sicherheitsgehäuses unterschieden wird.

[0005] Eine eventuell erforderliche Reparatur einer Frankiermaschine ist dann vor Ort nur schwer möglich, wenn der Zugang zu den Bauteilen erschwert oder eingeschränkt ist. Bei größeren Postverarbeitungsmaschinen oder sogenannten PC-Frankierern wird zukünftig das gesicherte Gehäuse auf das sogenannte postalische Sicherheitsmodul reduziert werden, was die Zugänglichkeit zu den übrigen Bauteile verbessern kann. Zum wirtschaftlichen Austauschen der Batterie des Sicherheitsmoduls wäre es außerdem wünschenswert, daß sich diese auf relativ einfachem Wege auswechseln läßt. Dann würde sich die Batterie aber außerhalb des Sicherheitsbereichs der Frankiermaschine befinden. Wenn die Batterieklemmen aber von außen zugänglich gemacht werden, ist ein möglicher Angreifer in der Lage, die Batteriespannung zu manipulieren. Bekannte batteriegespeiste SRAM's und RTC's haben bzgl. ihrer geforderten Betriebsspannung unterschiedliche Anforderungen. Die notwendige Spannung zum Halten von Daten von SRAM's liegt unterhalb der geforderten Spannung zum Betrieb von RTC's. Daß bedeutet, daß ein Verringern der Spannung unter einen bestimmten Grenzwert zu einem unerwünschten Verhalten der Komponenten führt: Die RTC bleibt stehen, die Uhrzeit - gespeichert in SRAM-Zellen - und die Speicherinhalte des SRAM bleiben erhalten. Wenigstens eine der Sicherheitsmaßnahmen, beispielsweise Long Time Watchdogs, wären dann auf der Frankiermaschinenseite unwirksam. Unter Long Time Watchdogs wird folgendes verstanden: Die entfernte Datenzentrale gibt einen Zeitkredit bzw. eine Zeitdauer, insbesondere eine Anzahl von Tagen, oder einen bestimmten Tag vor, bis zu welchem sich die Frankiereinrichtung per Kommunikationsverbindung melden soll. Nach Erschöpfung des Zeitkredits oder Fristablauf wird das Frankieren verhindert. Unter dem Titel: Verfahren und Anordnung zur Erzeugung und Überprüfung eines Sicherheitsabdruckes wurde bereits in der EP 660 270 A2 (US 5,680,463) ein Verfahren vorgeschlagen, die voraussichtliche Zeitdauer bis zur nächsten Guthabennachladung zu ermitteln, wobei seitens einer Datenzentrale diejenige Frankiermaschine als suspekt gilt, welche sich nicht fristgemäß meldet. Suspekte Frankiermaschinen

werden der Postbehörde mitgeteilt, welche den Poststrom nach von suspekten Frankiermaschinen frankierten Briefen überwacht. Ein Ablauf des Zeitkredits oder der Frist wird bereits auch von der Frankiereinrichtung ermittelt und der Benutzer wird aufgefordert die überfällige Kommunikation durchzuführen.

[0006] Sicherheitsmodule sind von elektronischen Datenverarbeitungsanlagen her bereits bekannt. Zum Schutz vor Einbruch in eine elektronische Anlage wird in EP 417 447 B1 bereits eine Sperre vorgeschlagen, welche Stromversorgungsmittel- und Signalerfassungsmittel sowie Abschirmmittel im Gehäuse umfaßt. Das Abschirmmittel besteht aus Einkapselungsmaterial und Leitungsmitteln, an welchen die Stromversorgungs- und Signalerfassungsmittel angeschlossen sind. Letzteres reagiert auf eine Veränderung des Leitungswiderstandes des Leitungsmittels. Außerdem enthält das Sicherheitsmodul eine interne Batterie, einen Spannungsumschalter von Systemspannung auf Batteriespannung und weitere Funktionseinheiten (wie Power Gate, Kurzschlußtransistor, Speicher und Sensoren). Wenn die Spannung eine bestimmte Grenze unterschreitet, reagiert das Power Gate. Wenn der Leitungswiderstand, die Temperatur oder die Strahlung verändert ist, reagiert die Logik. Mittels des Power Gate oder mittels der Logik wird der Ausgang des Kurzschlußtransistor auf L-Pegel umgeschaltet, wodurch ein im Speicher gespeicherter kryptographischer Schlüssel gelöscht wird. Jedoch ist die Lebensdauer der nicht auswechselbaren Batterie und damit des Sicherheitsmoduls für den Einsatz in Frankiereinrichtungen bzw. Postverarbeitungsmaschinen zu klein.

[0007] Eine größere Postverarbeitungsmaschine ist beispielsweise die JetMail®. Ein Frankierdruck wird hier mittels einem stationär angeordneten Tintenstrahldruckkopf bei einem nichtwaagerechten annähernd vertikalen Brieftransport erzeugt. Eine geeignete Ausführung für eine Druckvorrichtung wurde bereits in der DE 196 05 015 C1 vorgeschlagen. Die Postverarbeitungsmaschine hat ein Meter und eine Base. Soll das Meter mit einem Gehäuse ausgestattet werden, so daß Bauteile leichter zugänglich sind, dann muß es durch ein postalisches Sicherheitsmodul vor Betrugsversuchen geschützt werden, welches mindestens das Abrechnen der Postgebühren durchführt. Um Einflüsse auf den Programmverlauf auszuschließen, wurde bereits in der EP 789 333 A2 vorgeschlagen, ein Sicherheitsmodul mit einer Anwenderschaltung (ASIC) auszustatten, die eine Hardware-Abrecheneinheit aufweist. Die Anwenderschaltung (ASIC) steuert außerdem die Druckdatenübertragung zum Druckkopf.

[0008] Letzteres wäre nur dann nicht erforderlich, wenn für jedes Poststück einzigartige Abdrucke erzeugt werden. Ein Verfahren und Anordnung zur schnellen Erzeugung eines Sicherheitsabdruckes ist beispielsweise in den US 5,680,463, US 5,712,916 und US 5,734,723 vorgeschlagen worden. Dabei wird eine spezielle Sicherheitsmarkierung elektronisch generiert und in das Druckbild eingebettet.

[0009] Weitere Maßnahmen zum Schutz eines Sicherheitsmodul vor einem Angriff auf die in ihm gespeicherten Daten wurden auch in den nicht vorveröffentlichten deutschen Anmeldungen 198 16 572.2 und 198 16 571.4 vorgeschlagen. Bei einer Vielzahl von Sensoren steigt der Stromverbrauch und ein nicht ständig von einer Systemspannung versorgter Sicherheitsmodul zieht dann den für die Sensoren benötigten Strom aus seiner internen Batterie, was letztere ebenfalls frühzeitig erschöpft. Die Kapazität der Batterie und der Stromverbrauch beschränken somit die Lebensdauer eines Sicherheitsmoduls. Würden aber die Batterieanschlußklemmen von außen zugänglich gemacht werden, um die Lebensdauer der Batterie zu erhöhen, bestünde eine Angriffsmöglichskeit auf die Sicherheit der postalischen Daten durch einen Betrüger.

[0010] Das nicht durch eine Systemspannung versorgte Sicherheitsmodul könnte dann über die von außen zugänglichen Batteriekontakte manipuliert werden, indem die Spannung unter die für den Prozessor spezifizierte Grenzspannung verringert wird. Wenn der Prozessor mit einem internen Uhren-RAM (RTC) ausgestattet ist, bleibt die Uhr zuerst stehen. Bei Erhöhung der Spannung würde die interne Uhr (RTC) wieder weiterlaufen. Beim Anlegen einer Impulsspannung mit Impulsweiten-modulation muß sichergestellt sein, daß die Batteriespannung nicht unter die spezifizierte Grenze sinken kann, oberhalb derer die Speicherinhalte erhalten bleiben sollen. Bei einer unter die Grenze herunter gehenden Spannungsverringerung muß dieser Zustand nachweisbar solange aufrechterhalten werden bis ein anderer zulässiger Zustand gültig ist. Grundsätzlich ist eine Abschätzung des Angreiferpotentials bzw. der Angreiferklassen erforderlich, um mit geeigneten, vom Aufwand her angemessenen, Maßnahmen den erwünschten Sicherheitslevel zu erreichen. Dabei gilt das Motto: "So viel wie nötig, so wenig wie möglich". Mit einer geeigneten Schaltung muß also die Manipilationsmöglichkeit mindestens eingeschränkt werden.

[0011] Die DE 44 10 338 A zeigt ein Datenübertragungssystem mit einer Sendeeinheit, welche zwei Betriebsmodi aufweist: Im Normalbetrieb erfolgt eine Versorgung der Sendeeinheit mit der Hauptenergiequelle, während im Notbetrieb eine interne bzw. externe Energiequelle zugeschaltet wird.

[0012] Der Erfindung liegt die Aufgabe zugrunde, die Sicherheit vor einer unbefugten Manipulation eines Sicherheitsmoduls zu gewährleisten, wenn die Batterie austauschbar angeordnet ist.

[0013] Die Aufgabe wird mit den Merkmalen des Anspruchs 1 gelöst.

[0014] Ein postalisches Gerät, insbesondere eine Frankiermaschine, wird mit einem steckbaren Sicherheitsmodul ausgestattet, welches mit dem Systembus des Meters bzw. einer anderen geeigneten Steuereinrichtung verbunden ist. Bei einem gestecktem Sicherheitsmodul, welches zum Servicezeitpunkt von einer Sy-

stemspannung versorgt wird, kann die Batterie des Sicherheitsmoduls von einem Servicetechniker ausgewechselt werden. Das Sicherheitsmodul ist mit einer harten Masse vergossen. Für einen Batteriewechsel bzw. Entsorgung ist die Batterie jedoch außerhalb der Vergußmasse angeordnet.

[0015] Erfindungsgemäß weist das Sicherheitsmodul eine Spannungsüberwachungseinheit mit rücksetzbarer Selbsthaltung auf, die vom Prozessor abgefragt und zurückgesetzt werden kann. Die Überwachung der Spannung einer Batterie, die für die batteriegestützten RAM-Speicher und zur Funktion einer internen Uhr erforderlich ist, hat das Ziel, beim Unterschreiten eines bestimmten Spannungspegels Aktionen auszulösen, die zum Löschen von sicherheitsrelevanten Daten und der aktuellen Uhrzeit führen. Die Selbsthaltung gestattet den Zustand der Spannungsunterschreitung solange zu konservieren, bis ein sicherer Nachweis möglich ist. Letzteres ist erst nachträglich der Fall, wenn das Modul wieder mit Systemspannung versorgt wird. Ein Inspektor oder eine andere authorisierte Person, die geeignete Eingaben an der Tastatur der Frankiereinrichtung ausführt, kann den ursprünglichen Zustand wiederherstellen.

[0016] Die Vorteile neben der Verlängerung der Lebensdauer des Sicherheitsmoduls durch die Möglichkeit des Batteriewechsels, liegen in einem geringen Stromverbrauch der Schaltung trotz einer schnellen Reaktion auf Spannungsänderungen und einer Verhinderung einer Mittelwert-bildung bei einer Manipulation mit Rechteckimpulsen an den Batterieanschlüssen.

[0017] Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, Blockbild und Interface des Sicherheitsmoduls,

Figur 2, Blockschaltbild der Frankiermaschine,

Figur 3, Perspektivische Ansicht der Frankiermaschine von hinten,

Figur 4, Blockschaltbild des Sicherheitsmoduls (zweite Variante),

Figur 5, Schaltbild der Spannungsüberwachungseinheit,

Figur 6, Seitenansicht des Sicherheitsmoduls,

Figur 7, Draufsicht auf das Sicherheitsmodul,

Figur 8a, Ansicht des Sicherheitsmoduls von rechts,

Figur 8b, Ansicht des Sicherheitsmoduls von links.

[0018] In der Figur 1 ist ein Blockbild des Sicherheitsmoduls 100 mit den Kontaktgruppen 101, 102 zum Anschluß an ein Interface 8 sowie mit den Batteriekontaktklemmen 103 und 104 eines Batterieinterfaces für eine Batterie 134 dargestellt. Obwohl das Sicherheitsmodul 100 mit einer harten Vergußmasse vergossen ist, ist die Batterie 134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse auf einer Leiterplatte auswechselbar angeordnet. Die Leiterplatte trägt die Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134. Mittels der Kontaktgruppen 101, 102 wird das Sicherheitsmodul 100 an ein entsprechendes Interface 8 der Hauptplatine (Motherboard) 9 gesteckt. Die erste Kontaktgruppe 101 steht mit dem Systembus einer Steuereinrichtung in Kommunikationsverbindung und die zweite Kontaktgruppe 102 dient der Versorgung des Sicherheitsmoduls 100 mit der Systemspannung. Über die Pins P3,P5-P19 der Kontaktgruppe 101 laufen Adreß- und Datenleitungen 117, 118 sowie Steuerleitungen 115. Die erste und/oder zweite Kontaktgruppe 101 und/oder 102 sind/ist zur statischen und dynamischen Überwachung des Angestecktseins des Sicherheitsmoduls 100 ausgebildet. Über die Pins P23 und P25 der Kontaktgruppe 102 wird die Versorgung des Sicherheitsmodul 100 mit der Systemspannung der Hauptplatine 9 realisiert und über die Pins P1, P2 bzw. P4 wird eine dynamische und statische Ungestecktsein-Detektion durch das Sicherheitsmodul 100 realisiert.

[0019] Das Sicherheitsmodul 100 weist in an sich bekannter Weise einen Mikroprozessor 120 auf, der einen - nicht gezeigten - integrierten Festwertspeicher (internal ROM) mit dem speziellen Anwendungsprogramm enthält, was für die Frankiermaschine von der Postbehörde bzw. vom jeweiligen Postbeförderer zugelassen ist. Alternativ kann an den modulinternen Datenbus 126 ein üblicher Festwertspeicher ROM oder FLASH-Speicher angeschlossen werden.

Das Sicherheitsmodul 100 weist in an sich bekannter Weise eine Reset-Schaltungseinheit 130, einen Anwenderschaltkreis ASIC 150 und eine Logik PAL 160 auf, die für den ASIC als Steuersignalgenerator dient. Die Reset-Schaltungseinheit 130 bzw. der Anwenderschaltkreis ASIC 150 und die Logik PAL 160 sowie eventuell weitere - nicht gezeigte - Speicher werden über die Leitungen 191 bzw. 129 mit Systemspannung Us+ versorgt, welche bei eingeschalteter Frankiereinrichtung von der Hauptplatine 9 geliefert wird.

In der EP 789 33 A2 wurden bereits die wesentlichen Teile eines postalischen Sicherheitsmoduls PSM dargestelllt, welche die Funktionen Abrechnen und Absichern der Postgebührendaten realisieren.

[0020] Die Systemspannung Us+ liegt außerdem über eine Diode 181 und die Leitung 136 am Eingang der Spannungsüberwachungseinheit 12 an. Am Ausgang der Spannungsüberwachungseinheit 12 wird eine zweite Betriebsspannung U_{b+} geliefert, welche über die Leitung 138 zur Verfügung steht. Bei ausgeschalteter Frankiereinrichtung steht nicht die Systemspannung Us+, son-

dern nur die Batteriespannung Ub+ zur Verfügung. Die am negativen Pol liegende Batteriekontaktklemme 104 ist mit Masse verbunden. Von der am positiven Pol liegenden Batteriekontaktklemme 103 wird Batteriespannung über eine Leitung 193, über eine zweite Diode 182 und die Leitung 136 an den Eingang der Spannungsüberwachungseinheit geliefert. Alternativ zu den beiden Dioden 181, 182 kann ein handelsüblicher Schaltkreis als Spannungsumschalter 180 eingesetzt werden.

[0021] Der Ausgang der Spannungsüberwachungseinheit 12 ist über eine Leitung 138 mit einem Eingang für diese zweite Betriebsspannung U_{b+} des Prozessors 120 verbunden, welcher mindestens auf einen RAM-Speicherbereich 122, 124 führt und dort eine nichtflüchtige Speicherung solange garantiert, wie die zweite Betriebsspannung U_{b+} in der erforderlichen Höhe anliegt. Der Prozessor 120 enthält vorzugsweise einen internen RAM 124 und eine Echtzeituhr (RTC) 122.

[0022] Die Spannungsüberwachungseinheit 12 im Sicherheitsmodul 100 weist eine rücksetzbare Selbsthaltung auf, die vom Prozessor 120 über eine Leitung 164 abgefragt und über eine Leitung 135 zurückgesetzt werden kann. Für eine Rücksetzung der Selbsthaltung weist die Spannungsüberwachungseinheit 12 Schaltungsmittel auf, wobei die Rücksetzung erst auslösbar ist, wenn die Batteriespannung über die vorbestimmte Schwelle angestiegen ist. Die rücksetzbare Selbsthaltung wird später anhand der Figur 5 näher erläutert.

[0023] Die Leitungen 135 and 164 sind je mit einem Anschluß (Pin1 und 2) des Prozessors 120 verbunden. Die Leitung 164 liefert ein Statussignal an den Prozessor 120 und die Leitung 135 liefert ein Steuersignal an die Spannungsüberwachungseinheit 12.

[0024] Die Leitung 136 am Eingang der Spannungsüberwchungseinheit 12 versorgt zugleich eine Detektions-Einheit 13 mit Betriebs- oder Batteriespannung. Vom Prozessor 120 wird der Zustand der Detektions-Einheit 13 über die Leitung 139 abgefragt oder die Detektions-Einheit 13 wird vom Prozessor 120 über die Leitung 137 ausgelöst bzw. gesetzt. Nach dem Setzen wird eine statische Prüfung auf Anschluß durchgeführt. Dazu wird über eine Leitung 192 Massepotential abgefragt, welches am Anschluß P4 des Interfaces 8 des postalischen Sicherheitsmoduls PSM 100 anliegt und nur abfragbar ist, wenn der Sicherheitsmodul 100 ordnungsgemäß gesteckt ist. Bei gesteckten Sicherheitsmodul 100 wird Massepotential des negativen Pols 104 der Batterie 134 des postalischen Sicherheitsmoduls PSM 100 auf den Anschluß P23 des Interfaces 8 gelegt und ist somit am Anschluß P4 des Interfaces 8 über die Leitung 192 von der Detektions-Einheit 13 abfragbar.

[0025] An den Pins 6 und 7 des Prozessors 120 liegt eine Leitungsschleife, welche über die Pins P1 und P2 der Kontaktgruppe 102 des Interfaces 8 zum Prozessor 120 zurückgeschleift wird. Zur dynamischen Prüfung des Angeschlossenseins des postalischen Sicherheitsmoduls PSM 100 am Motherbord 9 werden vom Prozessor 120 wechselnde Signalpegel in ganz unregelmäßigen Zeitabständen an die Pin's 6, 7 angelegt und über die Schleife zurückgeschleift.

[0026] Die Figur 2 zeigt ein Blockschaltbild einer Frankiermaschine, die mit einer Chipkarten-Schreib/Leseeinheit 70 zum Nachladen von Änderungsdaten per Chipkarte und mit einer Druckeinrichtung 2, welche von einer Steuereinrichtung 1 gesteuert wird, ausgestattet ist. Die Steuereinrichtung 1 weist ein mit einem Mikroprozessor 91 mit zugehörigen Speichern 92, 93, 94, 95 ausgestattetes Motherboard 9 auf.

[0027] Der Programmspeicher 92 enthält ein Betriebsprogramm mindestens zum Drucken und wenigstens sicherheitsrelevante Bestandteile des Programms für eine vorbestimmte Format-Änderung eines Teils der Nutzdaten.

Der Arbeitsspeicher RAM 93 dient zur flüchtigen Zwischenspeicherung von Zwischenergebnissen. Der nichtflüchtige Speicher NVM 94 dient zur nichtflüchtigen Zwischenspeicherung von Daten, beispielsweise von statistischen Daten, die nach Kostenstellen geordnet sind. Der Kalender/Uhrenbaustein 95 enthält ebenfalls adressierbare aber nichtflüchtige Speicherbereiche zur nichtflüchtigen Zwischenspeicherung von Zwischenergebnissen oder auch bekannten Programmteilen (beispielsweise für den DES-Algorithmus). Es ist vorgesehen, daß die Steuereinrichtung 1 mit der Chipkarten-Schreib/Leseeinheit 70 verbunden ist, wobei der Mikroprozessor 91 der Steuereinrichtung 1 beispielsweise dazu programmiert ist, die Nutzdaten N aus dem Speicherbereich einer Chipkarte 49 zu deren Anwendung in entsprechende Speicherbereiche der Frankiermaschine zu laden. Eine in einen Einsteckschlitz 72 der Chipkarten-Schreib/Leseeinheit 70 eingesteckte erste Chipkarte 49 gestattet ein Nachladen eines Datensatzes in die Frankiermaschine für mindestens eine Anwendung. Die Chipkarte 49 enthält beispielsweise die Portogebühren für alle üblichen Postbefördererleistungen entsprechend des Tarifs der Postbehörde und ein Postbefördererkennzeichen, um mit der Frankiermaschine ein Stempelbild zugenerieren und entsprechend des Tarifs der Postbehörde die Poststücke freizustempeln.

[0028] Die Steuereinrichtung 1 bildet das eigentliche Meter mit den Mitteln 91 bis 95 der vorgenannten Hauptplatine 9 und umfaßt auch eine Tastatur 88, eine Anzeigeeinheit 89 sowie einen anwendungsspezifischen Schaltkreis ASIC 90 und das Interface 8 für das postalische Sicherheitsmodul PSM 100. Das Sicherheitsmodul PSM 100 ist über einen Steuerbus mit dem vorgenannten ASIC 90 und dem Mikroprozessor 91 sowie über den parallelen µC-Bus mindestens mit den Mitteln 91 bis 95 der Hauptplatine 9 und der mit Anzeigeeinheit 89 verbunden. Der Steuerbus führt Leitungen für die Signale CE, RD und WR zwischen dem Sicherheits-modul PSM 100 und dem vorgenannten ASIC 90. Der Mikroprozessor 91 weist vorzugsweise einen Pin für ein vom Sicherheitsmodul PSM 100 abgegebenes Interruptsignal i, weitere Anschlüsse für die Tastatur 88, eine serielle Schnittstelle Sl-1 für den Anschluß der Chipkarten-Schreib/Le-

se-Einheit 70 und eine serielle Schnittstelle Sl-2 für den optionalen Anschluß eines MODEMs auf. Mittels des MODEMs kann beispielsweise das im nichtflüchtigen Speicher des postalischen Sicherheitsmittels PSM 100 gespeicherte Guthaben erhöht werden.

[0029] Das postalische Sicherheitsmittel PSM 100 wird von einem gesicherten Gehäuse umschlossen. Vor jedem Frankierabdruck wird im postalischen Sicherheitsmodul PSM 100 eine hardwaremäßige Abrechnung durchgeführt. Die Abrechnung erfolgt unabhängig von Kostenstellen. Das postalische Sicherheitsmittel PSM 100 kann intern so ausgeführt sein, wie in der europäischen Anmeldung EP 789 333 A3 näher beschrieben wurde.

[0030] Es ist vorgesehen, daß der ASIC 90 eine serielle Schnittstellenschaltung 98 zu einem im Poststrom vorschalteten Gerät, eine serielle Schnittstellenschaltung 96 zu den Sensoren und Aktoren der Druckeinrichtung 2, eine serielle Schnittstellenschaltung 97 zur Drucksteuerelektronik 16 für den Druckkopf 4 und eine serielle Schnittstellenschaltung 99 zu einem der Druckeinrichtung 20 im Poststrom nachgeschalteten Gerät aufweist. Der DE 197 11 997 ist eine Ausführungsvariante für die Peripherieschnittstelle entnehmbar, welche für mehrere Peripheriegeräte (Stationen) geeignet ist. Sie trägt den Titel: Anordnung zur Kommunikation zwischen einer Basisstation und weiteren Stationen einer Postbearbeitungsmaschine und zu deren Notabschaltung.

[0031] Die Schnittstellenschaltung 96 gekoppelt mit der in der Maschinenbasis befindlichen Schnittstellenschaltung 14 stellt mindestens eine Verbindung zu den Sensoren 6, 7, 17 und zu den Aktoren, beispielsweise zum Antriebsmotor 15 für die Walze 11 und zu einer Reinigungs- und Dichtstation RDS 40 für den Tintenstrahldruckkopf 4, sowie zum Labelgeber 50 in der Maschinenbasis her. Die prinzipielle Anordnung und das Zusammenspiel zwischen Tintenstrahldruckkopf 4 und der RDS 40 sind der DE 197 26 642 C2 entnehmbar, mit dem Titel: Anordnung zur Positionierung eines Tintenstrahldruckkopfes und einer Reinigungs- und Dichtvorrichtung.

[0032] Einer der in der Führungsplatte 20 angeordneten Sensoren 7, 17 ist der Sensor 17 und dient zur Vorbereitung der Druckauslösung beim Brieftransport. Der Sensor 7 dient zur Briefanfangserkennung zwecks Druckauslösung beim Brieftransport. Die Transporteinrichtung besteht aus einem Transportband 10 und zwei Walzen 11,11'. Eine der Walzen ist die mit einem Motor 15 ausgestattete Antriebswalze 11, eine andere ist die mitlaufende Spannwalze 11'. Vorzugsweise ist die Antriebswalze 11 als Zahnwalze ausgeführt, entsprechend ist auch das Transportband 10 als Zahnriemen ausgeführt, was die eindeutige Kraftübertragung sichert. Ein Encoder 5, 6 ist mit einer der Walzen 11, 11' gekoppelt. Vorzugsweise sitzt die Antriebswalze 11 mit einem Inkrementalgeber 5 fest auf einer Achse. Der Inkrementalgeber 5 ist beispielsweise als Schlitzscheibe ausgeführt, die mit einer Lichtschranke 6 zusammen wirkt, und gibt über die Leitung 19 ein Encodersignal an das Motherboard 9 ab.

[0033] Es ist vorgesehen, daß die einzelnen Druckelemente des Druckkopfes innerhalb seines Gehäuses mit einer Druckkopfelektronik verbunden sind und daß der Druckkopf für einen rein elektronischen Druck ansteuerbar ist. Die Drucksteuerung erfolgt auf Basis der Wegsteuerung, wobei der gewählte Stempelversatz berücksichtigt wird, welcher per Tastatur 88 oder bei Bedarf per Chipkarte eingegeben und im Speicher NVM 94 nichtflüchtig gespeichert wird. Ein geplanter Abdruck ergibt sich somit aus Stempelversatz (ohne Drucken), dem Frankierdruckbild und gegebenfalls weiteren Druckbildern für Werbeklischee, Versandinformationen (Wahldrucke) und zusätzlichen editierbaren Mitteilungen. Der nichtflüchtige Speicher NVM 94 weist eine Vielzahl an Speicherbereichen auf. Darunter sind solche, welche die geladenen Portogebührentabellen nichtflüchtig speichern.

[0034] Die Chipkarten-Schreib/Leseeinheit 70 besteht aus einem zugehörigen mechanischen Träger für die Mikroprozessorkarte und Kontaktiereinheit 74. Letztere gestattet eine sichere mechanische Halterung der Chipkarte in Lese-Position und eindeutige Signalisierung des Erreichens der Leseposition der Chipkarte in der Kontaktierungseinheit. Die Mikroprozessorkarte mit dem Mikroprozessor 75 besitzt eine einprogrammierte Lesefähigkeit für alle Arten von Speicherkarten bzw. Chipkarten. Das Interface zur Frankiermaschine ist eine serielle Schnittstelle gemäß RS232-Standard. Die Datenübertragungsrate beträgt min. 1,2 K Baud. Das Einschalten der Stromversorgung erfolgt mittels einem an der Hauptplatine angeschlossenen Schalter 71. Nach Einschalten der Stromversorgung erfolgt eine Selbsttestfunktion mit Bereitschaftsmeldung.

[0035] In der Figur 3 ist eine perspektivische Ansicht der Frankiermaschine von hinten dargestellt. Die Frankiermaschine besteht aus einem Meter 1 und einer Base 2. Letztere ist mit einer Chipkarten-Schreib/ Leseeinheit 70 ausgestattet, die hinter der Führungsplatte 20 angeordnet und von der Gehäuseoberkante 22 zugänglich ist. Nach dem Einschalten der Frankiermaschine mittels dem Schalter 71 wird eine Chipkarte 49 von oben nach unten in den Einsteckschlitz 72 eingesteckt. Ein zugeführter auf der Kante stehender Brief 3, der mit seiner zu bedruckenden Oberfläche an der Führungsplatte anliegt, wird dann entsprechend der Eingabedaten mit einem Frankierstempel 31 bedruckt. Die Briefzuführöffnung wird durch eine Klarsichtplatte 21 und die Führungsplatte 20 seitlich begrenzt. Die Statusanzeige des auf die Hauptplatine 9 des Meters 1 gesteckten Sicherheitsmoduls 100 ist von außen durch eine Öffnung 109 sichtbar.

[0036] Die Figur 4 zeigt ein Blockschaltbild des postalischen Sicherheitsmoduls PSM 100 in einer bevorzugten Variante. Der negative Pol der Batterie 134 ist auf Masse und einen Pin P23 der Kontaktgruppe 102 gelegt. Der positive Pol der Batterie 134 ist über die Leitung 193

mit dem einen Eingang des Spannungsumschalters 180 und die Systemspannung führende Leitung 191 ist mit dem anderen Eingang des Spannungsumschalters 180 verbunden. Als Batterie 134 eignet sich der Typ SL-389/P für eine Lebensdauer bis zu 3,5 Jahren oder der Typ SL-386/P für eine Lebensdauer bis zu 6 Jahren bei einem maximalen Stromverbrauch durch das PSM 100. Als Spannungsumschalter 180 kann ein handelsüblicher Schaltkreis vom Typ ADM 8693ARN eingesetzt werden. Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 an der Batterieüberwachungseinheit 12 und der Detektionseinheit 13 an. Die Batterieüberwachungseinheit 12 und die Detektionseinheit 13 stehen mit den Pins1, 2, 4 und 5 des Prozessors 120 über die Leitungen 135, 164 und 137, 139 in Kommunikationsverbindung. Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 außerdem am Versorgungseingang eines ersten Speichers SRAM an, der durch die vorhandene Batterie 134 zum nichtflüchtigen Speicher NVRAM einer ersten Technologie wird.

Das Sicherheitsmodul steht mit der Frankiermaschine über den Systembus 115, 117, 118 in Verbindung. Der Prozessor 120 kann über den Systembus und ein Modem 83 in Kommunikationsverbindung mit einer entfernten Datenzentrale eintreten. Die Abrechnung wird vom ASIC 150 vollzogen. Die postalischen Abrechnungsdaten werden in nichtflüchtigen Speichern unterschiedlicher Technologie gespeichert.

Am Versorgungseingang eines zweiten Speichers NVRAM 114 liegt Systemspannung an. Hierbei handelt es sich um einen nichtflüchtigen Speicher NVRAM einer zweiten Technologie, (SHADOW-RAM). Diese zweiten Technologie umfaßt vorzugsweise ein RAM und ein EEPROM, wobei letzteres die Dateninhalte bei Systemspannungsausfall automatisch übernimmt. Der NVRAM 114 der zweiten Technologie ist mit den entsprechenden Adress- und Dateneingängen des ASIC's 150 über einen internen Adreß- und Datenbus 112, 113 verbunden.

[0037] Der ASIC 150 enthält mindestens eine Hardware-Abrecheneinheit für die Berechnung der zu speichernden postalischen Daten. In der Programmable Array Logic (PAL) 160 ist eine Zugriffslogik auf den ASIC 150 untergebracht. Der ASIC 150 wird durch die Logik PAL 160 gesteuert. Ein Adreß- und Steuerbus 117, 115 von der Hauptplatine 9 ist an entsprechenden Pins der Logik PAL 160 angeschlossen und die PAL 160 erzeugt mindestens ein Steuersignal für das ASIC 150 und ein Steuersignal 119 für den Programmspeicher FLASH 128. Der Prozessor 120 arbeitet ein Programm ab, das im FLASH 128 gespeichert ist. Der Prozessor 120, FLASH 28, ASIC 150 und PAL 160 sind über einen modulinternen Systembus miteinander verbunden, der Leitungen 110,111,126,119 für Daten-, Adreß- und Steuersignale enthält.

[0038] Die RESET-Einheit 130 ist über die Leitung 131 mit dem Pin 3 des Prozessors 120 und mit einem Pin des ASIC's 150 verbunden. Der Prozessor 120 und das ASIC 150 werden bei Absinken der Versorgungsspannung durch eine Resetgenerierung in der RESET-Einheit 130 zurückgesetzt.

[0039] An den Pins 6 und 7 des Prozessors 120 sind Leitungen angeschlossen, welche nur bei einem an die Hauptplatine 9 gesteckten PSM 100 eine Leiterschleife 18 bilden.

[0040] Die Echtzeituhr RTC 122 und der Speicher RAM 124 werden von einer Betriebsspannung über die Leitung 138 versorgt. Diese Spannung wird von der Spannungsüberwachungseinheit (Battery Observer) 12 erzeugt. Letzterer liefert außerdem ein Statussignal 164 und reagiert auf ein Steuersignal 135. Der Spannungsumschalter 180 gibt als Ausgangsspannung auf der Leitung 136 für die Spannungsüberwachungseinheit 12 und Speicher 116 diejenige seiner Eingangsspannungen weiter, die größer als die andere ist.

[0041] Der Prozessor 120 weist intern eine Verarbeitungseinheit CPU 121, eine Echtzeituhr RTC 122 eine RAM-Einheit 124 und eine Ein/Ausgabe-Einheit 125 auf. An den Pins 8 und 9 liegen I/O-Ports der Ein/Ausgabe-Einheit 125, an welchen modulinterne Signalmittel angeschlossen sind, beispielsweise farbige Lichtemitterdioden LED's 107, 108, welche den Zustand des Sicherheitsmoduls 100 signalisieren. Die Sicherheitsmodule können in ihrem Lebenszyklus verschiedene Zustände einnehmen. So muß z.B. detektiert werden, ob das Modul gültige kryptografische Schlüssel enthält. Weiterhin ist es auch wichtig zu unterscheiden, ob das Modul funktioniert oder defekt ist. Die genaue Art und Anzahl der Modulzustände ist von den realisierten Funktionen im Modul und von der Implementierung abhängig.

[0042] Der Prozessor 120 des Sicherheitsmoduls 100 ist über einen modulinternen Datenbus 126 mit einem FLASH 128 und mit dem ASIC 150 verbunden. Der FLASH 128 dient als Programmspeicher und wird mit Systemspannung Us+ versorgt. Er ist beispielsweise ein 128 Kbyte-FLASH-Speicher vom Typ AM29F010-45EC. Der ASIC 150 des postalischen Sicherheitsmoduls 100 liefert über einen modulinternen Adreßbus 110 die Adressen 0 bis 7 an die entsprechenden Adreßeingänge des FLASH 128. Der Prozessor 120 des Sicherheitsmoduls 100 liefert über einen internen Adreßbus 111 die Adressen 8 bis 15 an die entsprechenden Adresseingänge des FLASH 128. Der ASIC 150 des Sicherheitsmoduls 100 steht über die Kontaktgruppe 101 des Interfaces 8 mit dem Datenbus 118, mit dem Adreßbus 117 und dem Steuerbus 115 der Hauptplatine 9 in Kommunikationsverbindung.

[0043] Durch die Möglichkeit, die beschriebene Schaltung in Abhängigkeit von der Höhe der Spannungen Us+ und Ub+ automatisch mit der größeren von beiden zu speisen, kann während des Normalbetriebs die Batterie 134 ohne Datenverlust gewechselt werden.

[0044] Die Batterie der Frankiermaschine speist in den Ruhezeiten außerhalb des Normalbetriebes in vorerwähnter Weise die Echtzeituhr 122 mit Datums und/oder Uhrzeitregistern und/oder den statischen RAM (SRAM) 124, der sicherheitsrelevante Daten hält. Sinkt die Span-

nung der Batterie während des Batteriebetriebs unter eine bestimmte Grenze, so wird von der im Ausführungsbeispiel beschriebenen Schaltung der Speisepunkt für RTC und SRAM mit Masse verbunden. D.h. die Spannung an der RTC und am SRAM liegt dann bei 0V. Das führt dazu, daß der SRAM 124, der z.B. wichtige kryptografische Schlüssel enthält, sehr schnell gelöscht wird. Gleichzeitig werden auch die Register der RTC 122 gelöscht und die aktuelle Uhrzeit und das aktuelle Datum gehen verloren. Durch diese Aktion wird verhindert, daß ein möglicher Angreifer durch Manipulation der Batteriespannung die frankiermaschineninterne Uhr 122 anhält, ohne daß sicherheitsrelevante Daten verloren gehen. Somit wird verhindert, daß er Sicherheitsmaßnahmen, wie beispielsweise Long Time Watchdogs umgeht.

[0045] Gleichzeitig mit der Indikation der Unterspannung der Batterie wechselt die beschriebene Schaltung in einen Selbsthaltezustand, in dem sie auch bei nachträglicher Erhöhung der Spannung bleibt. Beim nächsten Einschalten des Moduls kann der Prozessor den Zustand der Schaltung abfragen (Statussignal) und damit und/oder über die Auswertung der Inhalte des gelöschten Speichers darauf schließen, daß die Batteriespannung zwischenzeitlich einen bestimmten Wert unterschritten hat. Der Prozessor kann die Überwachungsschaltung zurücksetzen, d.h. "scharf" machen.

[0046] Anhand der Figur 5 wird das Schaltbild der Spannungsüberwachungseinheit (Batterieobserver) 12 erläutert. Die Schaltung wird durch die Batteriespannung auf der Leitung 136 versorgt. Im Normalzustand ist ein Transistor 1252 gesperrt und über den Widerstand 1254 wird die Batteriespannung auf der Leitung 138 als Betriebsspannung für die Echtzeituhr RTC 122 bzw. Speicher RAM 124 zur Verfügung gestellt. Die Leitung 138 ist die Speiseleitung für die RTC 122 und den RAM 124.

[0047] Es ist vorgesehen, daß die Spannungsüberwachungseinheit 12 einen Spannungsteiler 1242, 1244 zwischen der Leitung 136 und Masse enthält, der einen Abgriff 1246 aufweist, daß am Abgriff der invertierende Eingang eines Komparators 1250, eines der Schaltungsmittel 1258 für die Selbsthaltung und eines der Schaltungsmittel 1260 für eine Rücksetzung der Selbsthaltung angeschlossen ist. Der Ausgang des Komparators 1250 ist über einen Negator 1252, 1254 einerseits mit der Leitung 138 und andererseits mit dem anderen Schaltungsmittel 1256 für die Selbsthaltung verbunden. Letzteres ist eine Diode, welche L-Pegel auf den Abgriff zurückkoppelt. Der Spannungsteiler besteht aus zwei Widerständen 1242 und 1244 und einem Kondensator 1272, der zwischen Abgriff und Masse geschaltet ist. Der Abzweig 1246 am Verknüpfungspunkt der zwei Widerstände 1242 und 1244 ist auf den invertierenden Eingang eines Komparators 1250 geschaltet. Der nichtinvertierende Eingang des Komparators 1250 ist an eine Referenzspannungquelle 1248 geschaltet. Der Ausgang des Komparators 1250 ist auf den Steuereingang eines Transistors 1252 geführt, welcher mit Masse verbunden und mit einem an der Leitung 136 liegenden Widerstand 1254 verbunden ist, d.h. als Negator geschaltet ist. Der Ausgang des Negators 1252, 1254 ist mit der Leitung 138 und dem n-Gebiet der Diode 1256 verbunden, deren p-Gebiet über einen Widerstand 1258 mit dem Abzweig 1246 verbunden ist. Zwischen der Leitung 136 und dem Abzeig 1246 ist parallel zum Widerstand 1242 ein zweiter Transistor 1260 geschaltet, dessen Steuereingang mit der Leitung 135 verbunden ist.

Die Batteriespannung auf der Leitung 136 wird von einem Spannungsteiler, der aus zwei Widerständen 1242 und 1244 und einem Kondensator 1272 besteht, verringert und von einem Komparator 1250 mit der Referenzspannung der Referenzspannungsquelle 1248 verglichen. Ist die zu vergleichende Spannung auf dem Abzweig 1246 kleiner als die Referenzspannung, so erhält der Transistor 1252 an seinem Steuereingang H-Pegel und wird durchgeschaltet. Dadurch wird die Leitung 138 mit Massepotential verbunden und die RTC 122 und der RAM 124 werden nicht mehr mit der Batteriespannung versorgt. Das führt dazu, daß die Register der RTC 122 und die Daten im RAM 124 gelöscht werden und die RTC 122 stehen bleibt.

[0048] Da die Leitung 138 jetzt mit Masse verbunden ist, wird gleichzeitig über die Diode 1256 und den Widerstand 1258 die zu vergleichende Spannung am Abgriff 1246 auf einen Wert nahe 0 V gezogen. Dadurch wechselt die Überwachungsschaltung 12 in einen Selbsthaltezustand, in dem sie auch bei Erhöhung der Spannung auf der Leitung 136 bleibt und die Leitung 138 auf Massepotential läßt. Durch diesen Zustand der Schaltung 12 wird über eine Entkopplungsdiode 1262 ein L-Signal auf die Leitung 164 gelegt, welches vom Prozessor 120 abgefragt werden kann. Die Entkopplungsdiode 1262 dient der Verringerung des Stromverbrauchs im Batteriebetrieb. Der Prozessor 120 kann die Überwachungsschaltung 12 zurücksetzen. Dazu wird über die Leitung 135 ein H-Rücksetzsignal auf den Transistor 1260 gegeben, welcher durchgeschaltet wird, Somit wird die Spannung am Abzweig 1246 über die Referenzspannung angehoben, der Komparator 1250 schaltet zurück und der Transistor 1252 wird gesperrt. Als Komparator 1250 eignet sich der Typ ICL7665SAIBA. Eine Diode 1268 entkoppelt die Versorgungsspannung für den Komparator 1250 von der Batteriespannung. Ein Elektrolytkondensator 1270 sorgt dafür, daß der Komparator 1250 über einen relativ langen Zeitraum (> 2 s) mit der Versorgungsspannung versorgt wird, bei der dessen Funktion gewährleistet ist, obwohl die Batteriespannung auf der Leitung 136 abgeschaltet wurde. Die Schaltung 12 ist so dimensioniert, daß jegliches Absinken der Batteriespannung auf der Leitung 136 unter die spezifizierte Schwelle von 2,6 V zum Ansprechen der Schaltung 12 führt.

[0049] Die Figur 6 zeigt zeigt den mechanischen Aufbau des Sicherheitsmoduls in Seitenansicht. Das Sicherheitsmodul ist als Multi-Chip-Modul ausgebildet, d.h. mehrere Funktionseinheiten sind auf einer Leiterplatte 106 verschaltet. Das Sicherheitsmodul 100 ist mit einer harten Vergußmasse 105 vergossen, wobei die Batterie

134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse 105 auf einer Leiterplatte 106 auswechselbar angeordnet ist. Beispielsweise ist es so mit einem Vergußmaterial 105 vergossen, daß Signalmittel 107, 108 aus dem Vergußmaterial an einer ersten Stelle herausragen und daß die Leiterplatte 106 mit der gesteckten Batterie 134 seitlich einer zweiten Stelle herausragt. Die Leiterplatte 106 hat außerdem Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134, vorzugsweise auf der Bestückungsseite oberhalb der Leiterplatte 106. Es ist vorgesehen, daß zum Anstecken des postalischen Sicherheitsmoduls PSM 100 auf die Hauptplatine des Meters 1 die Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 (Leiterbahnseite) des Sicherheitsmoduls 100 angeordnet sind. Der Anwenderschaltkreis ASIC 150 steht über die erste Kontaktgruppe 101 - in nicht gezeigter Weise - mit dem Systembus einer Steuereinrichtung 1 in Kommunikationsverbindung und die zweite Kontaktgruppe 102 dient der Versorgung des Sicherheitsmoduls 100 mit der Systemspannung. Wird das Sicherheitsmodul auf die Hauptplatine gesteckt, dann ist es vorzugsweise innerhalb des Metergehäuses dergestalt angeordnet, so daß das Signalmittel 107, 108 nahe einer Öffnung 109 ist oder in diese hineinragt. Das Metergehäuse ist damit vorteilhaft so konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls trotzdem von außen sehen kann. Die beiden Leuchtdioden 107 und 108 des Signalmittels werden über zwei Ausgangssignale der I/O-Ports an den Pin 8, 9 des Prozessors 120 gesteuert. Beide Leuchtdioden sind in einem gemeinsamen Bauelementegehäuse untergebracht (Bicolorleuchtdiode), weshalb die Abmaße bzw. der Durchmesser der Öffnung relativ klein bleiben kann und in der Größenordnung des Signalmittels liegt. Prinzipiell sind drei unterschiedliche Farben darstellbar (rot, grün, orange), von denen aber nur zwei benutzt werden (rot und grün). Zur Zustandsunterscheidung werden die LED's auch blinkend benutzt, so daß verschiedene Zustandsgruppen unterschieden werden können, die beispielsweise durch folgende LED-Zustände charakterisiert werden: LED aus, LED rot blinkend, LED rot, LED grün blinkend, LED grün. In der Figur 7 ist eine Draufsicht auf das postalische Sicherheitsmodul dargestellt. Die Figuren 8a bzw. 8b zeigen eine Ansicht des Sicherheitsmoduls jeweils von rechts bzw. von links. Die Lage der Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 wird aus den Figuren 8a und 8b in Verbindung mit Figur 6 deutlich.

[0050] Erfindungsgemäß ist das postalische Gerät, insbesondere eine Frankiermaschine, jedoch kann das Sicherheitsmodul auch eine andere Bauform aufweisen, die es ermöglicht, daß es beispielsweise auf das Motherbord eines Personalcomputers gesteckt werden kann, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

[0051] Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die - vom gleichen Grundgedanken der Erfindung ausgehend - von den anliegenden Ansprüchen umfaßt werden.

Patentansprüche

1. Anordnung für einen Sicherheitsmodul, mit mindestens einer Funktionseinheit (120), mit einer Batterie (134) und Mitteln zur Versorgung mit einer Systemspannung und mit einem Spannungsumschalter (180) der über eine Leitung (136) mit einer Spannungsüberwachungseinheit (12) verbunden ist, welche über eine Leitung (138) eine Betriebsspannung an einen Speicher (122, 124) abgibt, wobei die Batterie (134) auswechselbar auf dem Sicherheitsmodul (100) angeordnet ist und die Spannungsüberwachungseinheit (12) Schaltungsmittel (1256, 1258, 1260) für eine rücksetzbare Selbsthaltung aufweist, wobei die Selbsthaltung ausgelöst wird, wenn die Batteriespannung unter eine vorbestimmte Schwelle sinkt.

2. Anordnung, nach Anspruch 1, **gekennzeichnet dadurch, daß** die Spannungsüberwachungseinheit (12) als Schaltungsmittel eine Leitung (135) und ein Schaltmittel (1260) für eine Rücksetzung der Selbsthaltung aufweist, wobei die Rücksetzung erst auslösbar ist, wenn die Batteriespannung über die vorbestimmte Schwelle gestiegen ist.

3. Anordnung, nach den Ansprüchen 1 bis 2, **gekennzeichnet dadurch, daß** die Spannungsüberwachungseinheit (12) einen Spannungsteiler (1242, 1244) zwischen der Leitung (136) und Masse enthält, der einen Abgriff (1246) aufweist, daß am Abgriff der invertierende Eingang eines Komparators (1250), eines der Schaltungsmittel (1258) für die Selbsthaltung und das Schaltmittel (1260) für eine Rücksetzung der Selbsthaltung angeschlossen ist und daß der Ausgang des Komparators (1250) über einen Negator (1252,1254) einerseits mit der Leitung (138) und andererseits mit dem anderen Schaltungsmittel (1256) für die Selbsthaltung verbunden ist.

4. Anordnung, nach Anspruch 3, **gekennzeichnet dadurch, daß** das andere Schaltungsmittel (1256) der Selbsthaltung eine Diode ist.

5. Anordnung, nach Anspruch 3, **gekennzeichnet dadurch, daß** der nichtinvertierende Eingang des Komparators (1250) mit einer Referenzspannungsquelle (1248) verbunden ist.

6. Anordnung, nach Anspruch 3, **gekennzeichnet dadurch, daß** der Zustand der Selbsthaltung über eine Leitung (164) von einem Prozessor (120) des Sicher-

heitsmoduls (100) abfragbar ist.

7. Anordnung, nach den Ansprüchen 1 bis 6, **gekennzeichnet dadurch, daß** der Prozessor (120) Speicher (122, 124) aufweist, an welche über die Leitung (138) eine Betriebsspannung von der Spannungsüberwachungseinheit (12) geführt wird, daß der Prozessor (120) mit Systemspannung versorgt wird und einen ersten Pin1 aufweist, um den Zustand der Selbsthaltung über eine Leitung (135) zurückzusetzen und einen zweiten Pin2 aufweist, an welchem die Leitung (164) angeschlossen ist, um den Zustand der Spannungsüberwachungseinheit (12) abzufragen, ob sie auf Betriebspannungsabgabe oder auf Selbsthaltung geschaltet ist.

8. Anordnung, nach Anspruch 7, **gekennzeichnet dadurch, daß** das Sicherheitsmodul (100) einen Anwenderschaltkreis ASIC (150) aufweist und daß der Prozessor (120) über einen modulinternen Datenbus (126) mit dem Anwenderschaltkreis ASIC (150) verbunden ist, wobei letzterer über eine erste Kontaktgruppe (101) mit dem Systembus einer Steuereinrichtung (1) in Kommunikationsverbindung steht.

9. Anordnung, nach Anspruch 1, **gekennzeichnet dadurch, daß** das Sicherheitsmodul (100) mit einer harten Vergußmasse (105) vergossen ist, daß die Batterie (134) des Sicherheitsmoduls (100) außerhalb der Vergußmasse (105) auf einer Leiterplatte (106) auswechselbar angeordnet ist, daß die Leiterplatte (106) die Batteriekontaktklemmen (103 und 104) für den Anschluß der Pole der Batterie (134) und eine zweite Kontaktgruppe (102) zur Versorgung des Sicherheitsmoduls (100) mit der Systemspannung aufweist.

Claims

1. An arrangement for a security module with at least one functional unit (120), with a battery (134) and means for supply with a system voltage and with a voltage changeover switch (180) that is connected via a line (138) to a voltage monitoring unit (12) that delivers an operating voltage to a memory (122, 124) via a line (138), wherein the battery (134) is exchangeably arranged on the security module (100) and the voltage monitoring unit (12) includes circuit means (1256, 1258, 1260) for a resettable self-holding, said self-holding being triggered when the battery voltage falls below a predefined threshold.

2. An arrangement according to claim 1, **characterized in that** the voltage monitoring unit (12) includes as circuit means a line (135) and a switching means (1260) for resetting the self-holding, wherein such resetting can only be triggered when the battery voltage has risen above the predefined threshold.

3. An arrangement according to claims 1 to 2, **characterized in that** the voltage monitoring unit (12) includes a voltage divider (1242, 1244) between the line (136) and ground that has a tapping (1246); that the inverting input of a comparator (1250), one of the circuit means (1258) for the self-holding and the switching means (1260) for resetting the self-holding are connected to said tapping; and that the output of the comparator (1250) is connected via a negator (1252, 1254) to the line (138) on the one hand and, on the other hand, to the other circuit means (1256) for the self-holding.

4. An arrangement according to claim 3, **characterized in that** the other circuit means (1256) of the self-holding is a diode.

5. An arrangement according to claim 3, **characterized in that** the non-inverting input of the comparator (1250) is connected to a reference voltage source (1248).

6. An arrangement according to claim 3, **characterized in that** the status of the self-holding can be interrogated via a line (164) by a processor (120) of the security module (100).

7. An arrangement according to claims 1 to 6, **characterized in that** the processor (120) has memory means (122, 124) to which an operating voltage is led via the line (138) by the voltage monitoring unit (12) and that the processor (120) is supplied with system voltage and has a first Pin1 for resetting the status of self-holding via a line (135) and has a second Pin2 to which the line (164) is connected for interrogating the status of the voltage monitoring unit (12), i.e. whether it is set to operating voltage supply or to self-holding.

8. An arrangement according to claim 7, **characterized in that** the security module (100) has a user circuit ASIC (150) and that the processor (120) is connected via an internal data bus (126) of the module to the user circuit ASIC (150), the latter being in a communication connection with the system bus of a control device (1) via a first contact set (101).

9. An arrangement according to claim 1, **characterized in that** the security module (100) is encapsulated with a hard sealing compound (105); that the battery (134) of the security module (100) is exchangeably arranged outside the sealing compound (105) on a circuit board (106); and that the circuit board (106) contains the battery contact clamps (103 and 104) for connecting the poles of the battery (134) and a second contact set (102) for the supply of the

security module (100) with system voltage.

Revendications

1. Disposition pour un module de sécurité équipé d'au moins une unité fonctionnelle (120), une batterie (134) et de dispositifs d'alimentation en tension de système et avec un commutateur de tension (180) qui est raccordé par une ligne (136) à une unité de contrôle de tension (12), laquelle fournit une tension de service à une mémoire (122, 124) via une ligne (138). La batterie (134) est disposée amovible sur le module de sécurité (100) et l'unité de contrôle de tension (12) présente des moyens de commutation (1256, 1258, 1260) pour un auto-maintien réinitialisable. Ledit auto-maintien est déclenché lorsque la tension de la batterie baisse en-dessous d'un seuil prédéterminé.

2. Disposition selon la revendication 1, **caractérisée en ce que** l'unité de contrôle de tension (12) en tant que moyen de commutation présente une ligne (135) et un dispositif de commutation (1260) pour une réinitialisation de l'auto-maintien. Ladite réinitialisation est déclenchée uniquement lorsque la tension de la batterie a dépassé le seuil prédéterminé.

3. Disposition selon l'une quelconque des revendications 1 à 2, **caractérisée en ce que** l'unité de contrôle de tension (12) comporte un diviseur de tension (1242, 1244) entre la ligne (136) et la masse, présentant un branchement (1246). L'entrée d'inversion d'un comparateur (1250) du moyen de commutation (1258) pour l'auto-maintien et le dispositif de commutation (1260) pour une réinitialisation de l'auto-maintien est branché à la prise. La sortie du comparateur (1250) est raccordée via un inverseur (1252, 1254) à la ligne (138) d'un côté et à l'autre moyen de commutation (1256) pour l'auto-maintien de l'autre.

4. Disposition selon la revendication 3, **caractérisée en ce que** l'autre moyen de commutation de l'auto-maintien est une diode.

5. Disposition selon la revendication 3, **caractérisée en ce que** l'entrée non inverseuse du comparateur (1250) est reliée à une source de tension de référence (1248).

6. Disposition selon la revendication 3, **caractérisée en ce que** l'état de l'auto-maintien peut être appelé via une ligne (164) par un processeur (120) du module de sécurité (100).

7. Disposition selon l'une quelconque des revendications 1 à 6, **caractérisée en ce que** le processeur (120) présente une mémoire (122, 124), à laquelle est amenée une tension de service par l'unité de contrôle de tension (12) via la ligne (138). Ledit processeur (120) est alimenté en tension de système et présente un premier Pin1, afin de réinitialiser l'état de l'auto-maintien par une ligne (135). Il présente également un second Pin2, auquel est raccordé la ligne (164), afin d'interroger l'état de l'unité de contrôle de tension (12), si elle est branchée sur décharge de tension de service ou sur auto-maintien.

8. Disposition selon la revendication 7, **caractérisée en ce que** le module de sécurité (100) présente un circuit de commutation utilisateur ASIC (150). Le processeur (120) est relié via un bus de données à l'intérieur du module (126) au circuit de commutation utilisateur ASIC (150), ce dernier restant en liaison de communication avec le bus de systèmes d'un dispositif de commande (1) via un premier groupe de contact (101).

9. Disposition selon la revendication 1, **caractérisée en ce que** le module de sécurité (100) est scellé avec une masse de coulage (105) dure. La batterie (134) du module de sécurité (100) est disposée amovible en dehors de la masse de coulage (105) sur une plaquette (106). Ladite plaquette (106) présente des bornes de contact de batterie (103 et 104) pour le raccord du pôle de la batterie (134) et un second groupe de contact (102) pour l'alimentation en tension de système du module de sécurité (100).

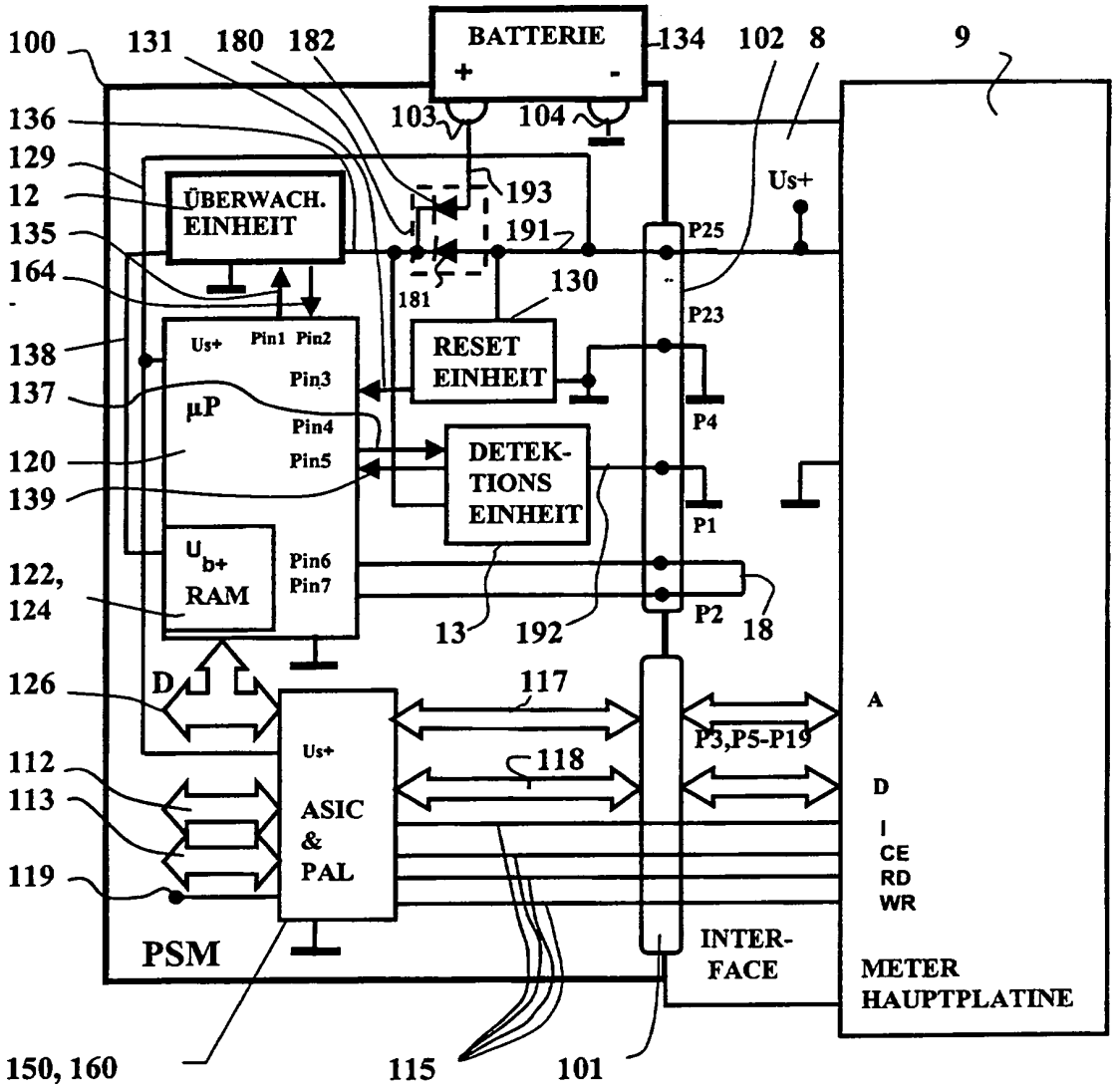
100
131
180
182
BATTERIE
+
-
134
102
8
9
136
103
104
129
12
135
164
ÜBERWACH.
EINHEIT
193
191
181
130
Us+
P25
P23
138
137
120
139
Us+
Pin1
Pin2
Pin3
Pin4
Pin5
µP
RESET
EINHEIT
DETEK-
TIONS
EINHEIT
P4
P1
122,
124
Ub+
RAM
Pin6
Pin7
13
192
P2
18
126
D
117
112
113
119
Us+
ASIC
&
PAL
118
P3,P5-P19
A
D
I
CE
RD
WR
PSM
INTER-
FACE
METER
HAUPTPLATINE
150, 160
115
101

Fig. 1

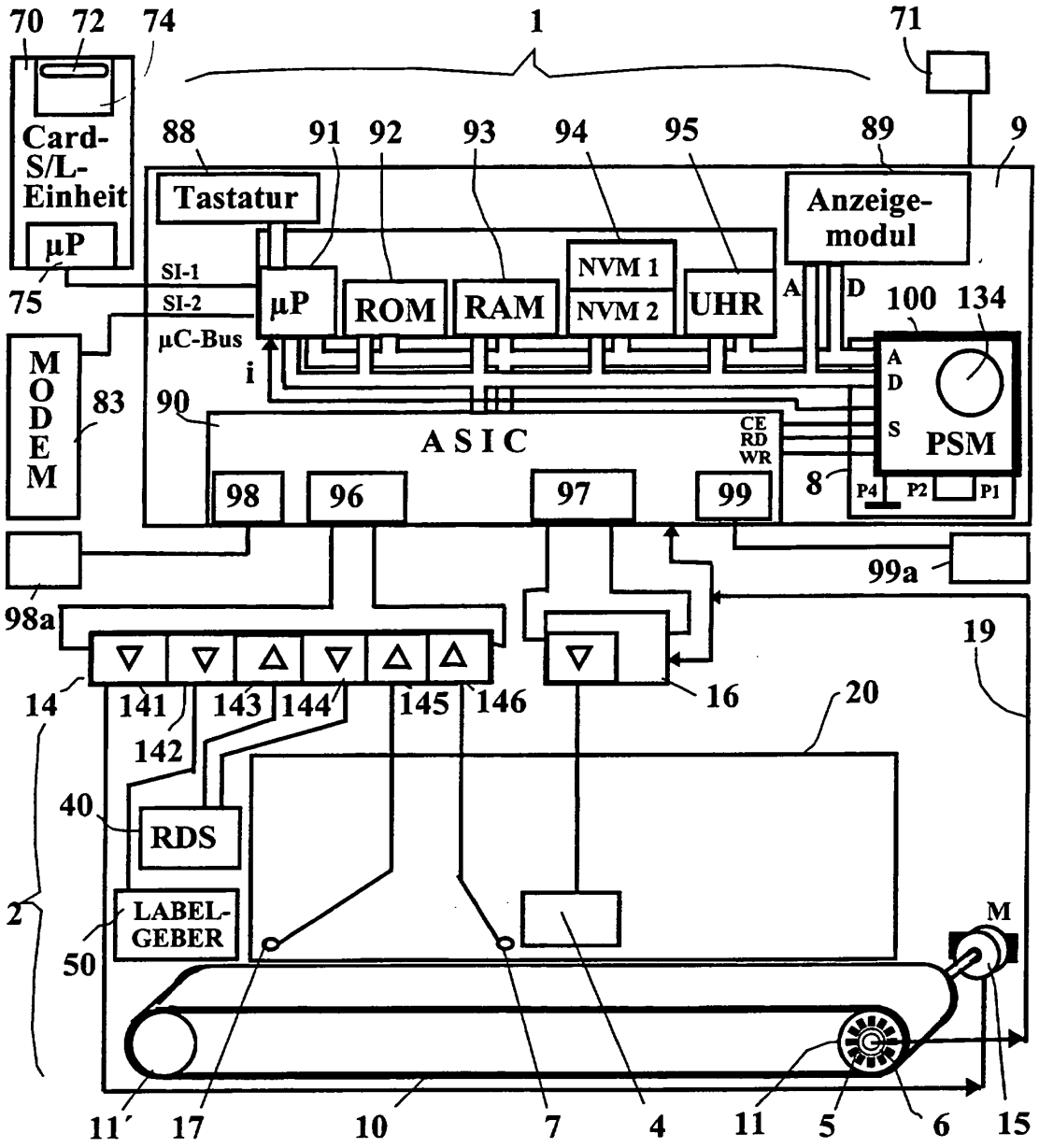
70
72
74
1
71
Card-
S/L-
Einheit
µP
75
88
91
92
93
94
95
89
9
Tastatur
Anzeige-
modul
SI-1
SI-2
µC-Bus
µP
ROM
RAM
NVM 1
NVM 2
UHR
A
D
100
134
i
MODEM
83
90
ASIC
CE
RD
WR
A
D
S
PSM
98
96
97
99
8
P4
P2
P1
98a
99a
19
14
141
142
143
144
145
146
16
20
40
RDS
LABEL-
GEBER
2
50
M
11´
17
10
7
4
11
5
6
15

Fig. 2

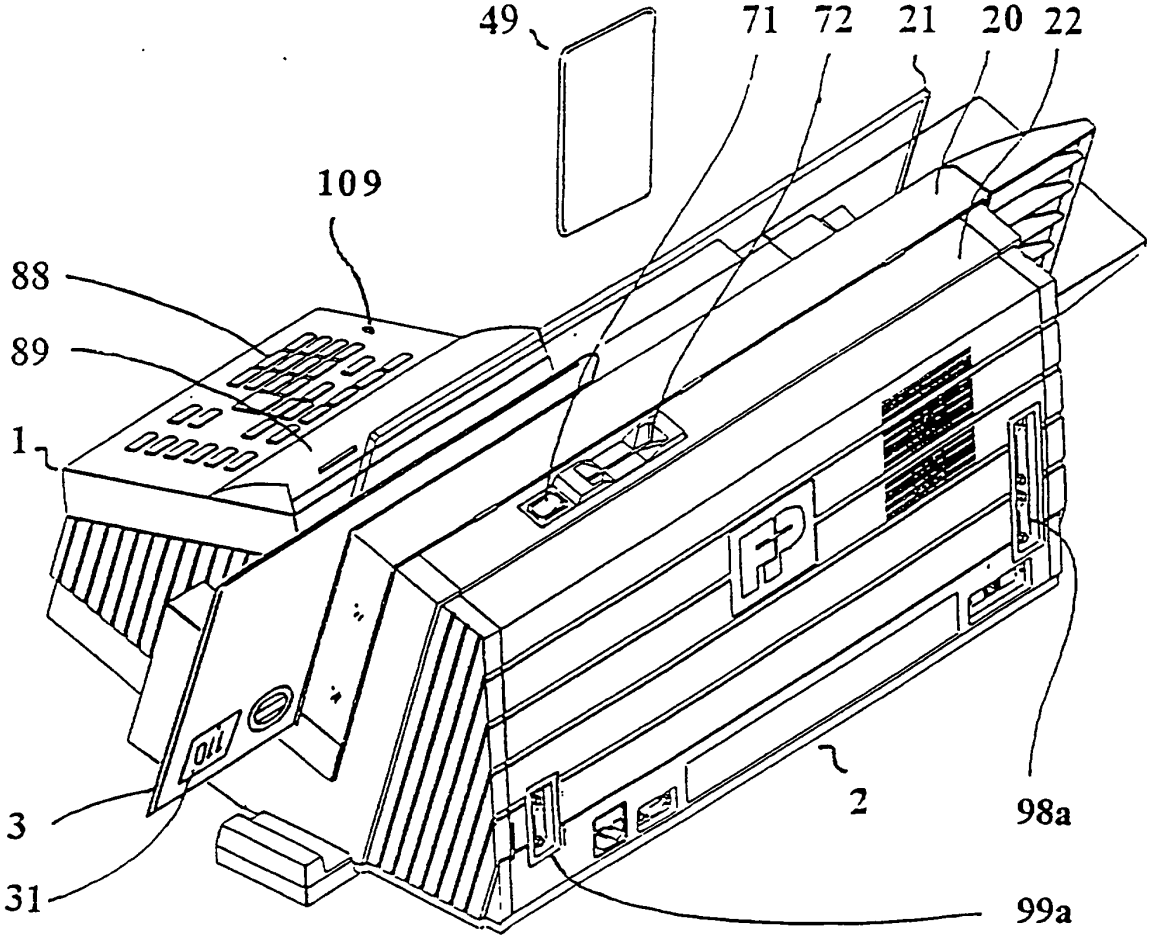

Fig. 3

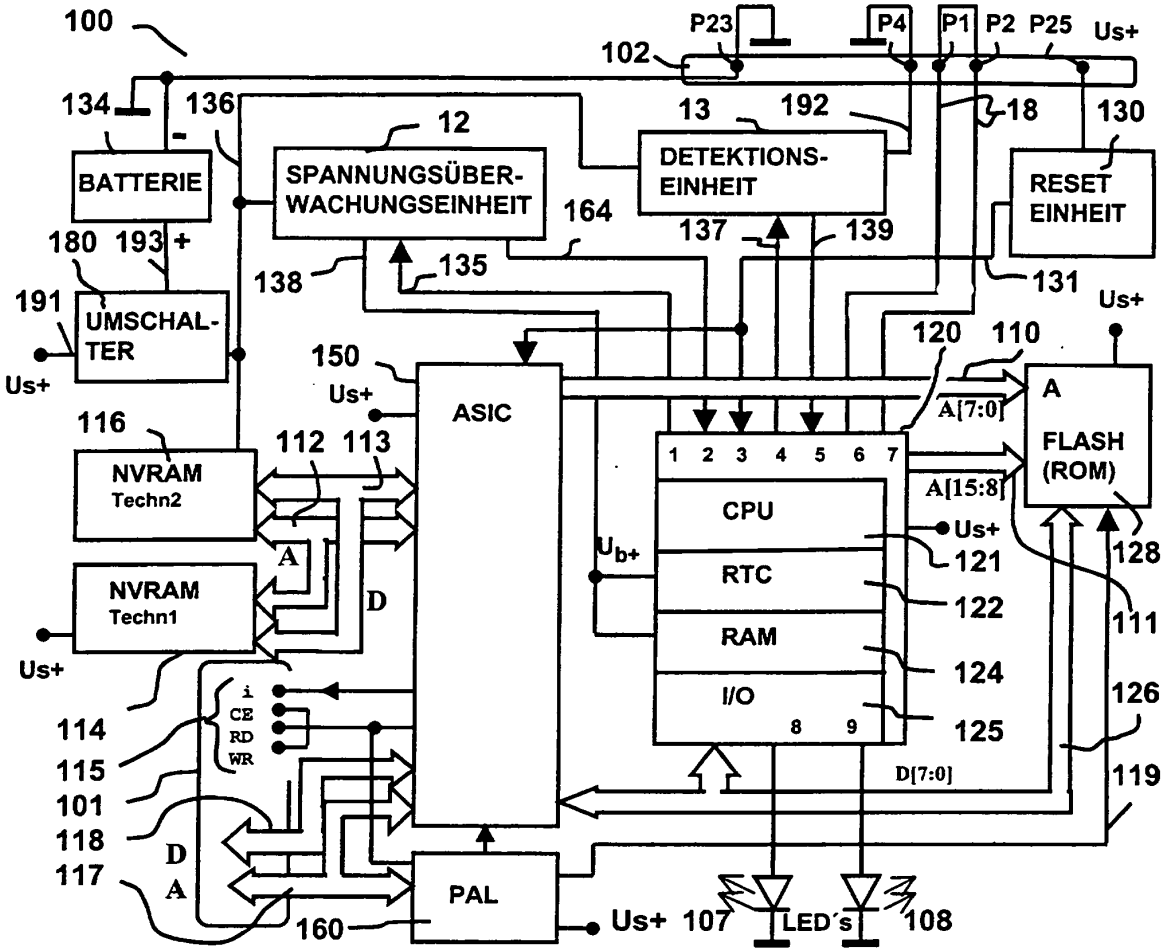
100
102
P23
P4
P1
P2
P25
Us+
134
136
12
13
192
18
130
BATTERIE
SPANNUNGSÜBER-
WACHUNGSEINHEIT
DETEKTIONS-
EINHEIT
RESET
EINHEIT
164
180
193
+
137
139
138
135
131
191
UMSCHAL-
TER
Us+
120
110
150
Us+
ASIC
A
A[7:0]
FLASH
(ROM)
116
112
113
1 2 3 4 5 6 7
A[15:8]
NVRAM
Techn2
CPU
Us+
128
A
U_{b+}
121
RTC
NVRAM
Techn1
D
122
111
RAM
124
Us+
i
CE
RD
WR
I/O
126
8 9
125
114
115
101
118
117
D[7:0]
119
D
A
PAL
160
Us+
107
LED's
108

Fig. 4

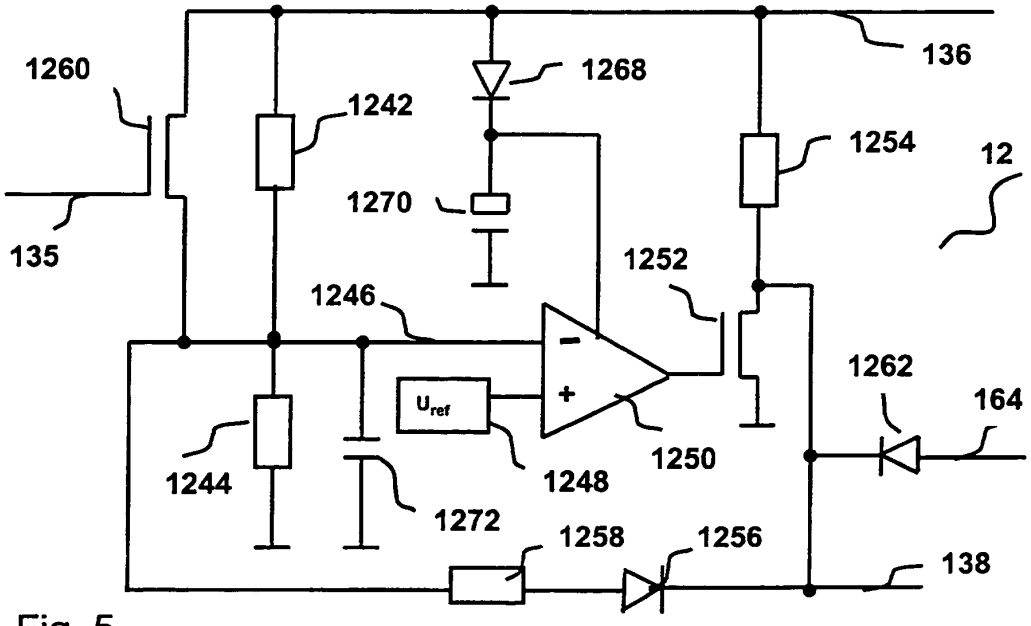
1260
136
1268
1242
1254
12
1270
135
1252
1246
1262
164
U_{ref}
1244
1248
1250
1272
1258
1256
138

Fig. 5

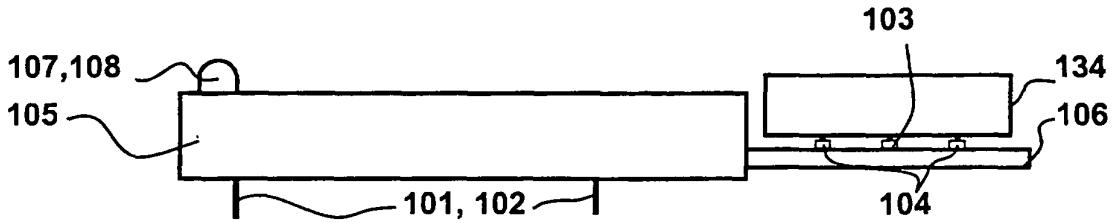

Fig. 6

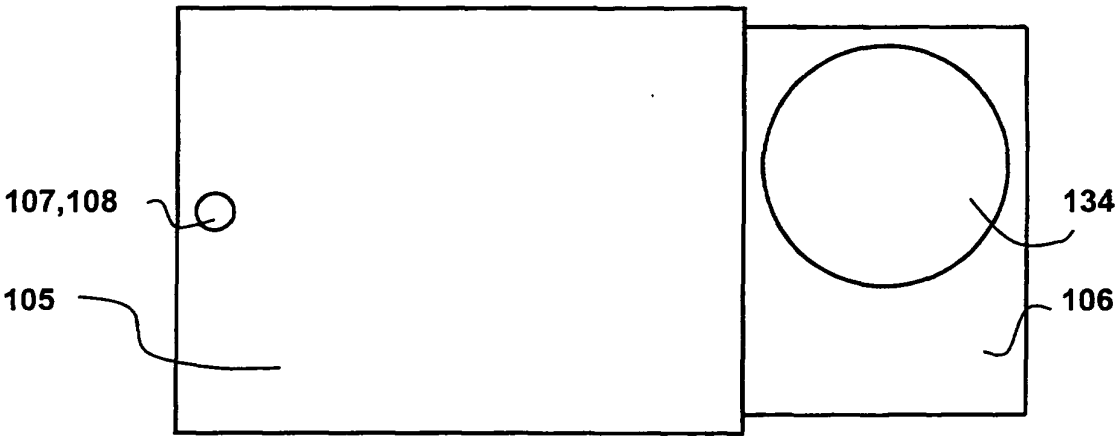

Fig. 7

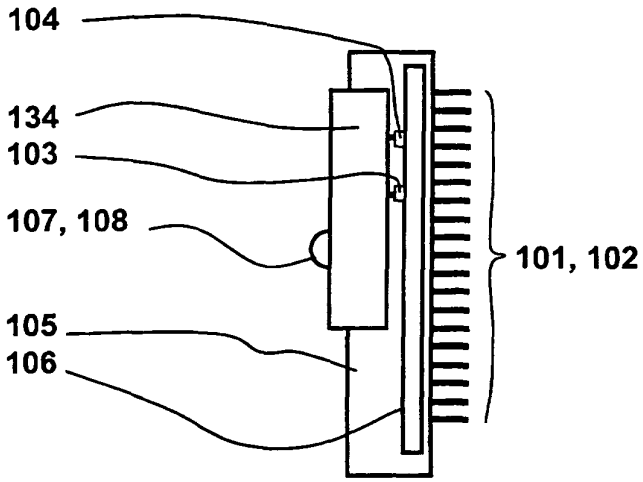

Fig. 8a

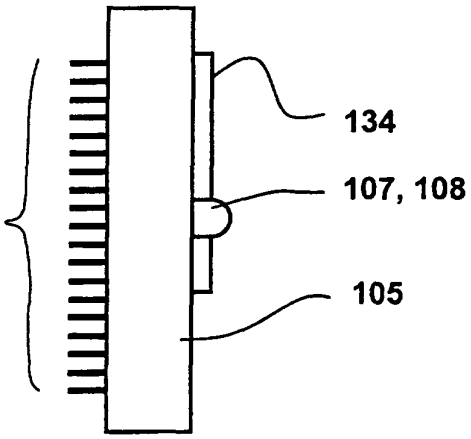

Fig. 8b

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- US 4746234 A **[0002]**
- US 5606508 A **[0003]**
- DE 4213278 B1 **[0003]**
- US 5490077 A **[0003]**
- EP 660269 A2 **[0004]**
- US 5671146 A **[0004]**
- EP 660270 A2 **[0005]**
- US 5680463 A **[0005] [0008]**
- EP 417447 B1 **[0006]**
- DE 19605015 C1 **[0007]**
- EP 789333 A2 **[0007]**
- US 5712916 A **[0008]**
- US 5734723 A **[0008]**
- DE 19816572 **[0009]**
- DE 19816571 **[0009]**
- DE 4410338 A **[0011]**
- EP 78933 A2 **[0019]**
- EP 789333 A3 **[0029]**
- DE 19711997 **[0030]**
- DE 19726642 C2 **[0031]**