

(19)



(11)

EP 1 035 513 B1

(12)

EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
02.07.2008 Patentblatt 2008/27

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

(21) Anmeldenummer: **00250057.7**

(22) Anmeldetag: **21.02.2000**

(54) Sicherheitsmodul mit Statussignalisierung

Security module with status signalization

Module de sécurité avec signalisation de l'état

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

(30) Priorität: **12.03.1999 DE 29905219 U**

(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)
- **Wagner, Andreas**
13503 Berlin (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 1 035 513 B1

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

Beschreibung

[0001] Die Erfindung betrifft ein Sicherheitsmodul mit Statussignalisierung, gemäß der im Oberbegriff des Patentanspruchs 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, oder andere Einrichtungen zum Frankieren von Postgut, sind mit einem Drucker zum Drucken des Postwertstempels auf das Postgut, mit einer Steuerung zum Steuern des Druckens und der peripheren Komponenten der Frankiermaschine, mit einer Abrecheneinheit zum Abrechnen von Postgebühren, die in nichtflüchtigen Speichern gehalten werden, und einer Einheit zum kryptografischen Absichern der Postgebührendaten ausgestattet. Die Abrecheneinheit und/oder die Einheit zum Absichern des Druckens der Postgebührendaten kann von einem sogenannten Sicherheitsmodul realisiert werden (EP 789 333 A2).

[0003] Der Prozessor des Sicherheitsmoduls ist beispielsweise ein OTP (One Time Programmable), welcher sensible Daten, wie kryptografische Schlüssel, auslesesicher speichert. Die Kapselung durch ein Sicherheitsgehäuse bietet einen weiteren Schutz.

[0004] Sicherheitsmodule sind auch von anderen elektronischen Datenverarbeitungsanlagen bereits bekannt und mit Mitteln zum Schutz vor einem Einbruch in ihre Elektronik ausgestattet (EP 417 447 B1).

[0005] Weitere Maßnahmen zum Schutz eines Sicherheitsmoduls 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.

[0006] Sicherheitsmodule für Frankiermaschinen können als Multi-Chip-Module oder als Ein-Chip-Systeme (z.B. Chipkarten) realisiert werden. Sie sind konstruktiv entweder fest mit der Frankiermaschine verbunden oder steckbar. Gerade ein steckbares Sicherheitsmodul kann in seinem Lebenszyklus verschiedene Zustände einnehmen. Dabei muß detektiert werden, ob das Sicherheitsmodul gültige kryptografische Schlüssel enthält. Weiterhin ist es auch wichtig zu unterscheiden, ob das Sicherheitsmodul funktioniert oder defekt ist. Nachteilig ist, dass dafür ein geeignetes "Zustandslesegerät", beispielsweise eine Frankiermaschine oder ein anderes Gerät vorhanden sein muß. Letzteres kann unter Umständen zu einer manipulierten falschen Zustandssignalisierung veranlaßt werden. Existierende Sicherheitsmodule für Frankiermaschinen besitzen keine eigenen optischen

oder akustischen Signalmittel. Sie können ihren Zustand nur indirekt, beispielsweise über Beeper oder die Anzeigeelemente einer Frankiermaschine, ausgeben. Die Zustandsanzeige kann hierbei automatisch beim Starten des Systems oder interaktiv durch den Benutzer der Frankiermaschine aufgerufen werden, wenn die Sicherheit bei der Signalisierung eines Zustandes garantiert werden kann.

[0007] Die EP 0 649 080 zeigt ein Verfahren zur Sicherung sicherheitsrelevanter Informationen in einem mit einer zentralen Datenverarbeitungsanlage gekoppelten Sicherheitsmodul eines Terminals.

[0008] Der Erfindung liegt die Aufgabe zugrunde, für ein steckbares Sicherheitsmodul eine hohe Lebensdauer zu erzielen und es zur sicheren Signalisierung des Modulzustandes auszubilden.

[0009] Die Aufgabe wird mit den Merkmalen des Patentanspruchs 1 gelöst.

[0010] Die Schaltung mit dem Prozessor des Sicherheitsmoduls, der auslesesicher sensible Daten enthält, und weiteren Funktionseinheiten werden lediglich durch eine Vergußmasse geschützt. Deshalb wird die Hauptplatine eines Meters bzw. einer vergleichbaren Steuereinrichtung mit einem Sicherheitsgehäuse umgeben, welches ggf. zusätzlich versiegelt ist. Das Sicherheitsmodul ist mit einer harten Masse vergossen. Für einen Batteriewechsel bzw. Entsorgung ist die Batterie jedoch außerhalb der Vergußmasse angeordnet. In vorteilhafter Weise kann bei einem gestecktem Sicherheitsmodul, welches zum Servicezeitpunkt von einer Systemspannung versorgt wird, die Batterie von einem Servicetechniker leicht ausgewechselt werden.

[0011] Es ist beim erfindungsgemäßen Sicherheitsmodul vorteilhaft, wenn letzteres selbstständig - bei Anlegen der Betriebsspannung - optisch (oder akustisch) seinen Zustand signalisiert. Es ist hierbei möglich und auch ausreichend, wenn das Modul nur eine grobe Unterscheidung des aktuellen Zustands durch eigene Signalmittel zuläßt. Die genaue Art und Anzahl der Modulzustände ist von den realisierten Funktionen im Modul und von der Implementierung abhängig.

[0012] Das Sicherheitsmodul für eine Frankiermaschine nimmt deren Funktion einer Abrechnung der Postgebühren und/oder die kryptografische Absicherung der Postgebührendaten war. Es ist erfindungsgemäß durch eigene Signalmittel oder eine Anzeigeeinheit gekennzeichnet, die bei direkter Ansteuerung vom Sicherheitsmodul eine Aussage über den aktuellen Zustand des Sicherheitsmoduls gestatten, wobei der Modulzustand geändert wird, wenn das Sicherheitsmodul in den ungesteckten Zustand überführt wird und/oder wenn die Batteriespannung unter eine vorbestimmte Schwelle sinkt, die jedoch bei Versorgung des Sicherheitsmoduls mit Systemspannung unterbrochen ist. Die Signalisierung des Modulzustandes wird nur bei Versorgung des Sicherheitsmoduls mit Systemspannung aktiviert. Es ist vorgesehen, dass das Signalmittel in demjenigen Bereich einer Leiterplatte des Sicherheitsmoduls montiert ist, wo das

umgebende Sicherheitsgehäuse zur Signalisierung des Modulzustandes ein Sichtfenster bzw. eine Öffnung aufweist. Das Signalmittel ist vorteilhaft als Anzeigeeinheit realisiert und kann im einfachsten Fall eine Leuchtdiode LED sein. Sie kann durch das Vergußmaterial hindurchragen. Alternativ oder zusätzlich sind mehrere oder mehrfarbige LED's oder eine Flüssigkristallanzeige LCD o.a. Signalmittel möglich, die am von Vergußmaterial freien Teil der Leiterplatte angeordnet sind.

[0013] 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, Perspektivische Ansicht der Frankiermaschine von hinten,

Figur 2, Blockschaltbild des Sicherheitsmoduls,

Figur 3, Seitenansicht einer ersten Variante des Sicherheitsmoduls,

Figur 4, Draufsicht auf das Sicherheitsmodul in der ersten Variante,

Figur 5a, Ansicht des Sicherheitsmoduls (1. Variante) von rechts,

Figur 5b, Ansicht des Sicherheitsmoduls (1. Variante) von links,

Figur 6, Seitenansicht einer zweiten Variante des Sicherheitsmoduls,

Figur 7, Draufsicht auf das Sicherheitsmodul in der zweiten Variante,

Figur 8a, Ansicht des Sicherheitsmoduls (2. Variante) von rechts,

Figur 8b, Ansicht des Sicherheitsmoduls (2. Variante) von links.

[0014] In der Figur 1 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.

[0015] Das Modul wird auf die Hauptplatine des Meters der Frankiermaschine oder eines anderen geeigneten Gerätes gesteckt. Es ist vorzugsweise innerhalb des Metergehäuses untergebracht, welches als Sicherheitsgehäuse ausgebildet ist. Das Metergehäuse ist dabei vorteilhaft so konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls trotzdem von außen durch eine Öffnung 109 sehen kann, wobei sich die Öffnung 109 zur Bedienoberfläche 88, 89 des Meters 1 erstreckt.

[0016] Die Anzeige wird direkt vom modulinternen Prozessor gesteuert und ist so von außen nicht ohne weiteres manipulierbar. Die Anzeige ist im Betriebszustand ständig aktiv, so daß das Anlegen der Systemspannung Us+ an den Prozessor des Sicherheitsmoduls ausreicht, die Anzeige zu aktivieren, um den Modulzustand ablesen zu können.

[0017] Die Figur 2 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 einer Spannungsüberwachungseinheit 12 und einer Detektionseinheit 13 an. Die Spannungsüberwachungseinheit 12 und die Detektionseinheit 13 stehen mit den Pins 1, 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 116 einer ersten Technologie wird.

[0018] 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 NV-RAM 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.

[0019] 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 für den ASIC 150 untergebracht. Der ASIC 150 wird durch die Logik PAL 160 gesteuert. Ein Adreß- und Steuerbus 117, 115 von der Hauptplatine des Meters 1 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 12 und PAL 160 sind über einen modulinternen Systembus miteinander verbunden, der Leitungen 110, 111, 126, 119 für Daten-, Adreß- und Steuersignale enthält.

[0020] 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.

[0021] Der Prozessor 120 weist intern eine Verarbeitungseinheit CPU 121, eine Echtzeituhr RTC 122 eine RAM-Einheit 124 und eine Ein/Ausgabe-Einheit 125 auf. Der Prozessor 120 des Sicherheitsmoduls 100 ist über einen modul-internen Datenbus 126 mit einem FLASH 128 und mit dem ASIC 150 verbunden. Der FLASH 128 dient als Programmspeicher und wird mit Systemspannung U_{s+} 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 mit dem Datenbus 118, mit dem Adreßbus 117 und dem Steuerbus 115 der Hauptplatine des Meters 1 in Kommunikationsverbindung.

[0022] 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. Durch die Möglichkeit, die beschriebene Schaltung in Abhängigkeit von der Höhe der Spannungen U_{s+} und U_{b+} automatisch mit der größeren von beiden zu speisen, kann während des Normalbetriebes die Batterie 134 ohne Datenverlust gewechselt werden. Die Echtzeituhr RTC 122 und der Speicher RAM 124 werden von einer Betriebsspannung über die Leitung 138 versorgt. Diese Spannung wird von der Spannungsüberwachungseinheit 12 erzeugt.

[0023] 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 Spannung der Batterie während des Batteriebetriebs unter eine bestimmte Grenze, so wird von der Schaltung 12 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.

[0024] Die Schaltung der Spannungsüberwachungseinheit 12 ist beispielsweise 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. Gleichzeitig mit der Indikation der Unterspannung der Batterie wechselt die Schaltung 12 in einen Selbsthaltungszustand, in dem sie auch bei nachträglicher Erhöhung der Spannung bleibt. Sie liefert außerdem ein Statussignal 164. 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 12 zurücksetzen, d.h. "scharf" machen. Letztere reagiert auf ein Steuersignal auf der Leitung 135.

[0025] Die Leitung 136 am Eingang des Batterieobservers 12 versorgt zugleich eine Detektions-Einheit 13 mit Betriebs- oder Batteriespannung. Die Detektions-Einheit 13 kann ein Ungestecktsein-Sensor oder irgend einen anderen Sensor überwachen und hat eine Selbsthaltung, welche vom Prozessor rücksetzbar ist. Der Zustand (ist Selbsthaltung oder nicht ausgelöst) der Detektions-Einheit 13 wird vom Prozessor 120 über die Leitung 139 abgefragt oder die Detektions-Einheit 13 wird vom Prozessor 120 über die Leitung 137 ausgelöst bzw. rückgesetzt. Nach dem Rücksetzen wird eine statische Prüfung auf Anschluß durchgeführt. Dazu wird über eine Leitung 192 Massepotential abgefragt, welches am Anschluß P4 des Interfaces 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 mit der Kontaktgruppe 102 gelegt und ist somit am Anschluß P4 des Interfaces über die Leitung 192 von der

Detektions-Einheit 13 abfragbar.

[0026] An den Pins 6 und 7 des Prozessors 120 sind Leitungen angeschlossen, welche nur bei einem, beispielsweise an die Hauptplatine des Meters 1, gesteckten Sicherheitsmodul 100 eine Leiterschleife 18 bilden. Zur dynamischen Prüfung des Angeschlossenseins des postalischen Sicherheitsmoduls PSM 100 an der Hauptplatine des Meters 1 werden vom Prozessor 120 wechselnde Signalpegel in ganz unregelmäßigen Zeitabständen an die Pin's 6, 7 angelegt und über die Schleife zurückgeschleift.

[0027] Der Prozessor 120 ist mit der Ein/Ausgabe-Einheit 125 ausgestattet, deren Anschlüsse Pin's 8, 9 zur Ausgabe mindestens eines Signals zur Signalisierung des Zustandes des Sicherheitsmoduls 100 dienen. An den Pin's 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. Diese signalisieren den Modulzustand bei einem auf die Hauptplatine des Meters 1 gesteckten Sicherheitsmoduls 100 durch eine Öffnung 109 im Metergehäuse. 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.

[0028] Die Figur 3 zeigt den mechanischen Aufbau des Sicherheitsmoduls nach einer ersten Variante 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 das Signalmittel 107, 108 aus dem Vergußmaterial an einer ersten Stelle herausragt 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. Beispielsweise dient eine Kontaktgruppe 101 zur Kommunikation des Sicherheitsmoduls 100 mit dem Meter 1 und eine zweite Kontaktgruppe 102 dient zur Versorgung des Sicherheitsmoduls 100 mit der Systemspannung, wobei mindestens eine der Kontaktgruppen 101, 102 einseitig durch das Vergußmaterial 105 umgeben ist. 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 Bauelementgehäuse 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 gesteuert, so daß fünf verschiedene Zustandsgruppen unterschieden werden können, die durch folgende LED-Zustände charakterisiert werden: LED aus, LED rot blinkend, LED rot, LED grün blinkend, LED grün.

[0029] In der Figur 4 ist eine Draufsicht auf das postalische Sicherheitsmodul der ersten Variante dargestellt. Die Vergußmasse 105 umgibt quaderförmig einen ersten Teil der Leiterplatte 106, während ein zweiter Teil der Leiterplatte 106 für die auswechselbar angeordnete Batterie 134 von Vergußmasse frei bleibt. Die Batteriekontaktklemmen 103 und 104 werden hier von der Batterie verdeckt, sind aber wieder in der Seitenansicht nach Fig. 5a sichtbar.

[0030] Die Figuren 5a bzw. 5b zeigen eine Ansicht des Sicherheitsmoduls der ersten Variante jeweils von rechts bzw. von links. Die Lage der Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 wird aus den Figuren 5a und 5b in Verbindung mit Figur 3 deutlicher sichtbar. Das Signalmittel 107, 108 ist vorzugsweise im ersten Teil der Leiterplatte 106 angeschlossen, welches durch das Vergußmaterial 105 umgeben ist (Figuren 3, 4 und 5b). Aus Energiespargründen erfolgt nur bei Versorgung des Sicherheitsmoduls mit Systemspannung die Signalisierung des Modulzustandes.

[0031] Die Figur 6 zeigt den mechanischen Aufbau des Sicherheitsmoduls nach einer zweiten Variante in Seitenansicht. Das Sicherheitsmodul ist wieder als Multi-Chip-Modul ausgebildet und mit einer harten Vergußmasse 105 vergossen, wobei die Batterie 134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse 105 auf einer Leiterplatte 106 auswechselbar angeordnet ist. Aus Kostengründen erfolgt der Verguß an einer ersten Stelle so mit einem Vergußmaterial 105, dass das Signalmittel 107, 108 und die gesteckte Batterie 134 extern vom Vergußmaterial an einer zweiten Stelle auf der Oberseite der Leiterplatte 106 montiert sind. Die Leiter-

platte 106 hat wieder Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134, vorzugsweise auf der Bestückungsseite oberhalb der Leiterplatte 106. Die beiden Leuchtdioden 107 und 108 des Signalmittels sind bei dieser Variante separate Bauelemente. 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. Zur Zustandsunterscheidung können die LED's wiederum auch blinkend gesteuert werden, so dass mindestens fünf verschiedene Zustandsgruppen unterschieden werden können, die beispielsweise durch folgende LED-Zustände charakterisiert werden: LED 107, 108 beide aus, LED 107 rot blinkend, LED 107 rot leuchtend, LED 108 grün blinkend, LED 108 grün leuchtend. Das Metergehäuse ist ebenfalls wieder so konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls von außen, beispielsweise durch ein Sichtfenster oder eine Öffnung 109 sehen kann.

[0032] Es ist ebenfalls vorgesehen, dass zum Anstecken des postalischen Sicherheitsmoduls PSM 100 auf die Hauptplatine des Meters 1 die Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 des Sicherheitsmoduls 100 angeordnet sind. Vorteilhaft enthält ein Verbinder 127 die Kontaktgruppen 101 und 102, wobei der Verbinder 127 auf der Leiterbahnseite der Leiterplatte 106 angeordnet ist.

[0033] In der Figur 7 ist eine Draufsicht auf das postalische Sicherheitsmodul der zweiten Variante dargestellt. Die Vergußmasse 105 umgibt quaderförmig den ersten Teil der Leiterplatte 106, während der zweite Teil der Leiterplatte 106 für die beiden Leuchtdioden 107 und 108, die auswechselbar angeordnete Batterie 134 und für den Verbinder 127 (hier nicht sichtbar) frei von Vergußmasse bleibt. Die Batteriekontaktklemmen 103 und 104 werden in der Figur 7 von der Batterie verdeckt, sind aber ebenso wie der Verbinder 127 in der Seitenansicht nach Fig.8a sichtbar.

[0034] Der Verguß des ersten Teils der Leiterplatte 106 zeigt weder Öffnungen noch Erhebungen und bietet somit weniger Angriffspunkte für ein Manipulation in krimineller Absicht. Das Vergußmaterial 105 ist vorzugsweise ein Zweikomponenten-Epoxyharz oder Polymer bzw. Kunststoff. Geeignet ist eine Vergußmasse aus STYCAST ®2651-40 FR von der Firma EMERSON & CUMING mit vorzugsweise CATALYST 9 als zweite Komponente. Bei der Herstellung des Vergusses werden beide Komponenten gemischt und auf beide Seiten der Leiterplatte 106 in deren ersten Teil aufgebracht. Letzteres kann beispielsweise durch Eintauchen in die frische Mischung erfolgen. Nun kann eine - nach einem abschließend äusserem Verguß von aussen nicht sichtbare - Schutz- und/oder Sensorschicht angebracht werden, welche während des Aushärtens des Vergußmaterials 105 mit letzterem eine feste Verbindung eingeht. Nach dem abschließenden äusseren Verguß härtet die Vergußmasse zu dem festen undurchsichtigen Vergußmaterial 105 aus.

[0035] Die Figuren 8a bzw. 8b zeigen eine Ansicht des Sicherheitsmoduls der zweiten Variante jeweils von rechts bzw. von links. Die Lage des Verbinders 127 mit den Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 wird aus den Figuren 8a und 8b in Verbindung mit Figur 6 deutlicher sichtbar.

[0036] Alternativ kann beispielsweise ein Verbinder 127 - in nicht gezeigter Weise - auf der Oberseite des zweiten Teils der Leiterplatte 106 angebracht werden.

[0037] Erfindungsgemäß ist das postalische Gerät, insbesondere eine Frankiermaschine, jedoch kann das Sicherheitsmodul auch eine andere Bauform aufweisen, die es ermöglicht, daß es beispielsweise auf die Hauptplatine eines Personalcomputers gesteckt werden kann, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

[0038] 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 Schutzansprüchen umfaßt werden.

25 Patentansprüche

1. Sicherheitsmodul (100) mit Statussignalisierung, mit Funktionseinheiten, welche miteinander verschaltet und von einer Vergußmasse bedeckt sind, **gekennzeichnet dadurch,** daß die Vergußmasse (105) mindestens einen Teil der Leiterplatte (106) mit den verschalteten Funktionseinheiten umgibt, daß zur Signalisierung des Modulzustandes ein optisches oder akustisches Signalmittel (107, 108) an einer Funktionseinheit der Leiterplatte (106) angeschlossen ist, wobei die Signalisierung des Modulzustandes erfolgt, wenn am Sicherheitsmodul (100) eine Betriebsspannung anliegt.
2. Sicherheitsmodul (100), nach Anspruch 1, **gekennzeichnet dadurch, daß** Signalmittel (107, 108) im ersten Teil der Leiterplatte (106) in demjenigen Bereich durch das Vergußmaterial (105) hindurchragt, wo das umgebende Sicherheitsgehäuse eines Gerätes zur Signalisierung des Modulzustandes ein Sichtfenster oder eine Öffnung (109) aufweist.
3. Sicherheitsmodul (100), nach Anspruch 1, **gekennzeichnet dadurch, dass** ein zweiter Teil der Leiterplatte (106) von Vergußmasse frei bleibt, daß Signalmittel (107, 108) im zweiten Teil der Leiterplatte (106) in demjenigen Bereich montiert ist, wo das umgebende Sicherheitsgehäuse eines Gerätes zur Signalisierung des Modulzustandes ein Sichtfenster oder eine Öffnung (109) aufweist.
4. Sicherheitsmodul (100), nach den Ansprüchen 2

oder 3, **gekennzeichnet dadurch, daß** das Gerät ein Meter (1) ist und dass sich das Sichtfenster oder die Öffnung (109) zur Bedienoberfläche (88, 89) des Meters (1) erstreckt und daß die Abmaße bzw. der Durchmesser der Öffnung in der Größenordnung des Signalmittels liegen.

5. Sicherheitsmodul (100), nach einem der Ansprüche 1 bis 4, **gekennzeichnet dadurch, daß** das Signalmittel als Anzeigeeinheit realisiert ist.
6. Sicherheitsmodul (100), nach Anspruch 5, **gekennzeichnet dadurch, daß** die Anzeigeeinheit eine oder mehrere oder mehrfarbige Leuchtdioden (LED's) einschließt.
7. Sicherheitsmodul (100), nach Anspruch 6, **gekennzeichnet dadurch, daß** die Leuchtdioden LED's zur Zustandsunterscheidung blinkend gesteuert werden.
8. Sicherheitsmodul (100), nach Anspruch 5, **gekennzeichnet dadurch, daß** die Anzeigeeinheit eine Flüssigkristallanzeige (LCD) ist.
9. Sicherheitsmodul (100), nach Anspruch 1, **gekennzeichnet dadurch, daß** ein zweiter Teil der Leiterplatte (106) für eine auswechselbar angeordnete Batterie (134) ausgebildet ist und von Vergußmasse frei bleibt, Batteriekontaktklemmen (103 und 104) für den Anschluß der Pole der Batterie (134) aufweist, daß die Leiterplatte (106) eine erste Kontaktgruppe (101 zur Kommunikation des Sicherheitsmoduls (100) mit dem Meter (1) und daß die Leiterplatte (106) eine zweite Kontaktgruppe (102) zur Versorgung des Sicherheitsmoduls (100) mit der Systemspannung aufweist, wobei der Modulzustand geändert wird, wenn die Batteriespannung unter eine vorbestimmte Schwelle sinkt, wobei jedoch die Signalisierung des Modulzustandes nur bei Versorgung des Sicherheitsmoduls (100) mit Systemspannung aktiviert wird.
10. Sicherheitsmodul, nach Anspruch 9, **gekennzeichnet dadurch, dass** mindestens eine der Kontaktgruppen (101, 102) einseitig durch das Vergußmaterial (105) umgeben ist.
11. Sicherheitsmodul (100), nach Anspruch 9, **gekennzeichnet dadurch, daß** ein Verbinder (127) mit den Kontaktgruppen (101, 102) auf der Unterseite oder auf der Oberseite der Leiterplatte (106) angeordnet ist.
12. Sicherheitsmodul (100), nach Anspruch 11, **gekennzeichnet dadurch, daß** ein Verbinder (127) mit den Kontaktgruppen (101, 102) auf der Unterseite oder auf der Oberseite der Leiterplatte (106) im

zweiten Teil angeordnet ist, der frei von Vergußmaterial (105) ist.

5 Claims

1. A security module (100) with status signalling, with functional units that are interconnected and are covered by a sealing compound, **characterized in that** the sealing compound (105) encloses at least a part of the printed circuit board (106) with the interconnected functional units and that, for signalling the module status, an optical or acoustic signal means (107, 108) is connected to a functional unit of the printed circuit board (106), wherein the module status is signalled when an operating voltage is applied to the security module (100).
2. A security module (100) according to claim 1, **characterized in that** the signal means (107, 108) sticks out in the first part of the printed circuit board (106), in the area of the sealing compound (105) where the enclosing security housing of a device for signalling the module status has a view window or an opening (109).
3. A security module (100) according to claim 1, **characterized in that** a second part of the printed circuit board (106) remains free from sealing compound and that the signal means (107, 108) is mounted in the second part of the printed circuit board (106), in the area where the enclosing security housing of a device for signalling the module status has a view window or an opening (109).
4. A security module (100) according to claims 2 or 3, **characterized in that** the device is a meter (1) and that the view window or the opening (109) extends to the operating surface (88, 89) of the meter (1) and that the dimensions or the diameter of the opening corresponds to the size of the signal means.
5. A security module (100) according to one of the claims 1 to 4, **characterized in that** the signal means is designed as a display unit.
6. A security module (100) according to claim 5, **characterized in that** the display unit includes one or several or multicolour light-emitting diode/s (LED).
7. A security module (100) according to claim 6, **characterized in that** the light-emitting diode/s (LED) are controlled in a flashing manner for distinguishing between statuses.
8. A security module (100) according to claim 5, **characterized in that** the signal means is a liquid crystal display (LCD).

9. A security module (100) according to claim 1, **characterized in that** a second part of the printed circuit board (106) is designed for a replaceable battery (134) and remains free from the sealing compound and is provided with battery clamps (103 and 104) for connecting the poles of the battery (134); that the printed circuit board (106) has a first contact set (101) for the communication of the security module (100) with the meter (1) and that the printed circuit board (106) has a second contact set (102) for supplying the security module (100) with system voltage, wherein the module status is changed when the battery voltage falls below a predefined threshold level, wherein, however, the signalling of the module status is only activated when the security module (100) is supplied with system voltage.
10. A security module (100) according to claim 9, **characterized in that** at least one of the contact sets (101, 102) is enclosed by the sealing compound (105) on one side.
11. A security module (100) according to claim 9, **characterized in that** a connector (127) with the contact sets (101, 102) is arranged on the bottom side or on the top side of the printed circuit board (106).
12. A security module (100) according to claim 11, **characterized in that** a connector (127) with the contact sets (101, 102) is arranged on the bottom side or on the top side of the printed circuit board (106) in the second part that is free from sealing compound (105).

Revendications

1. L'invention concerne un module de sécurité (100) équipé d'un dispositif de signalisation d'état et d'unités fonctionnelles, lesquelles sont imbriquées entre elles et recouvertes d'une masse de coulage **caractérisée en ce que**, ladite masse de coulage (105) entoure au moins une partie de la plaquette (106) avec les unités fonctionnelles imbriquées. Un moyen de signalement (107, 108) visuel ou acoustique pour la signalisation de l'état du module est raccordé à une unité fonctionnelle de la plaquette (106). Ladite signalisation de l'état du module se déclenche lorsqu'une tension de régime est appliquée au module de sécurité (100).
2. Module de sécurité (100) selon la revendication 1, **caractérisé en ce que** le moyen de signalement (107, 108) fait saillie dans la première partie de la plaquette (106) via le matériau de coulage (105) dans la zone, où le coffret de sécurité entourant un appareil pour la signalisation de l'état du module présente une fenêtre d'inspection ou une ouverture

(109).

3. Module de sécurité (100) selon la revendication 1, **caractérisé en ce qu'**une deuxième partie de la plaquette (106) n'est pas prise par la masse de coulage. Le moyen de signalement (107, 108) est monté dans la deuxième partie de la plaquette (106) dans la zone, où le coffret de sécurité entourant un appareil pour la signalisation de l'état du module présente une fenêtre d'inspection ou une ouverture (109)
4. Module de sécurité (100) selon l'une des revendications 2 ou 3, **caractérisé en ce que** l'appareil est un mètre (1). La fenêtre d'inspection ou l'ouverture (109) s'étend vers la surface utilisateur (88, 89) du mètre (1) et les dimensions ou plutôt le diamètre de l'ouverture sont dans la dimension du moyen de signalement.
5. Module de sécurité (100) selon l'une quelconque des revendications 1 à 4, **caractérisé en ce que** le moyen de signalement est réalisé comme une unité d'affichage.
6. Module de sécurité (100) selon la revendication 5, **caractérisé en ce que** l'unité d'affichage comprend une ou plusieurs diodes électroluminescentes (DEL) pouvant être aussi de plusieurs couleurs.
7. Module de sécurité (100) selon la revendication 6, **caractérisé en ce que** les diodes électroluminescentes DEL sont commandées clignotant pour différencier les états.
8. Module de sécurité (100) selon la revendication 5, **caractérisé en ce que** l'unité d'affichage est un affichage à cristaux liquides (LCD).
9. Module de sécurité (100) selon la revendication 1, **caractérisé en ce qu'**une deuxième partie de la plaquette (106) est formée pour une pile (134) disposée de manière amovible et n'est pas prise par la masse de coulage. Ledit module de sécurité présente des bornes de contact de pile (103 et 104) pour le raccord du pôle de la pile (134). La plaquette (106) présente un premier groupe de contact (101) pour la communication du module de sécurité (100) avec le mètre (1) et cette même plaquette (106) présente également un second groupe de contact (102) pour l'alimentation du module de sécurité (100) en tension de système en changeant l'état du module lorsque la tension de la pile passe en-dessous d'un seuil prédéterminé. Toutefois, la signalisation de l'état du module est activé uniquement lorsque le module de sécurité (100) est alimenté en tension de système.
10. Module de sécurité (100) selon la revendication 9, **caractérisé en ce qu'**au moins un des groupes de

contact (101, 102) est entouré d'un côté par le matériau de coulage (105).

11. Module de sécurité (100) selon la revendication 9, **caractérisé en ce qu'un** connecteur (127) est disposé avec les groupes de contact (101, 102) sur le côté inférieur ou sur le côté supérieur de la plaquette (106). 5
12. Module de sécurité (100) selon la revendication 11, **caractérisé en ce qu'un** connecteur (127) est disposé avec les groupes de contact (101, 102) sur le côté inférieur ou sur le côté supérieur dans la seconde partie de la plaquette (106) qui ne présente aucun matériau de coulage (105). 10 15

20

25

30

35

40

45

50

55

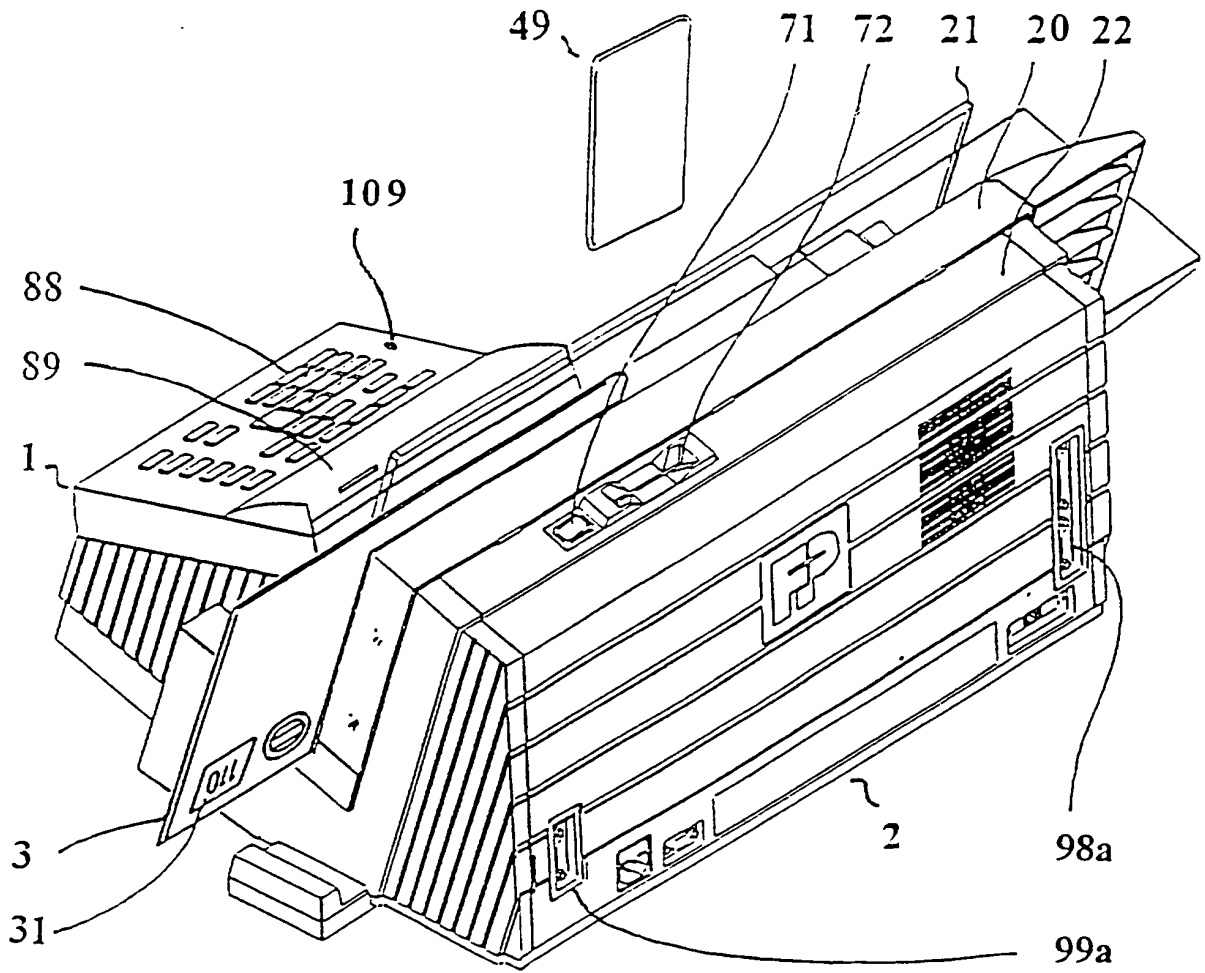


Fig. 1

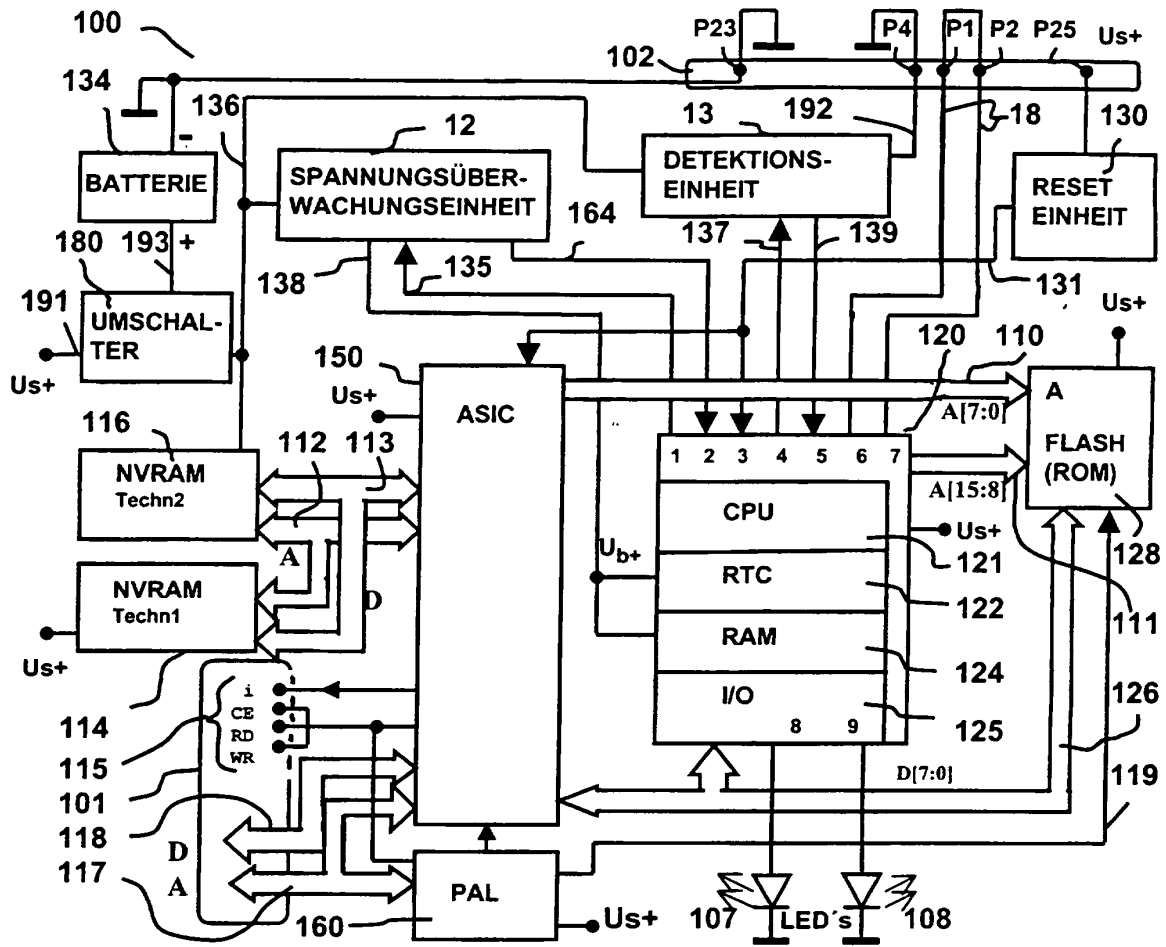


Fig. 2

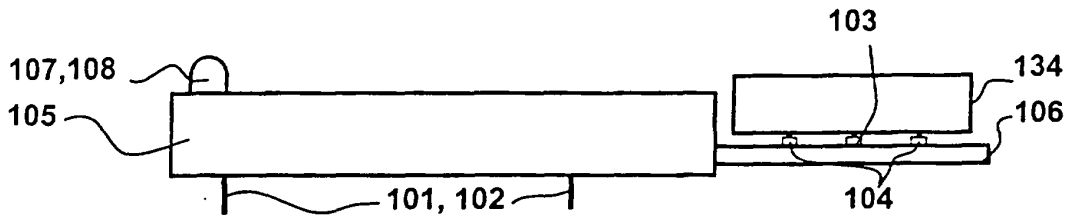


Fig. 3

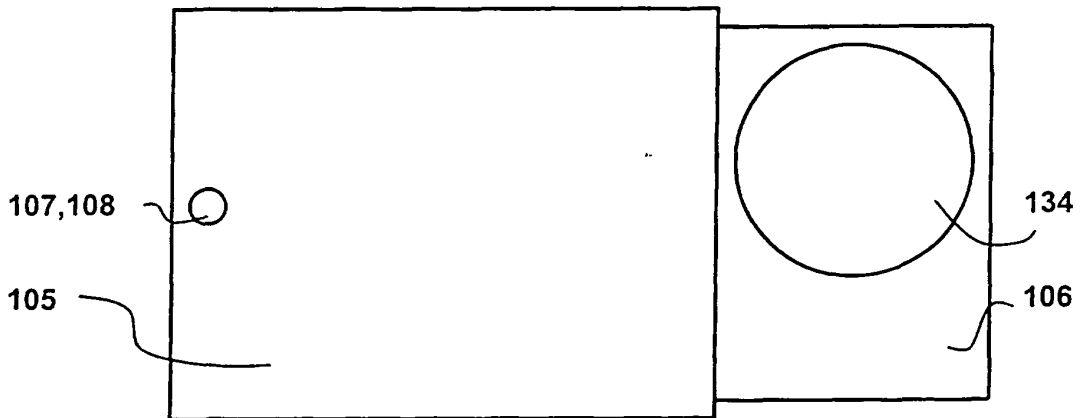


Fig. 4

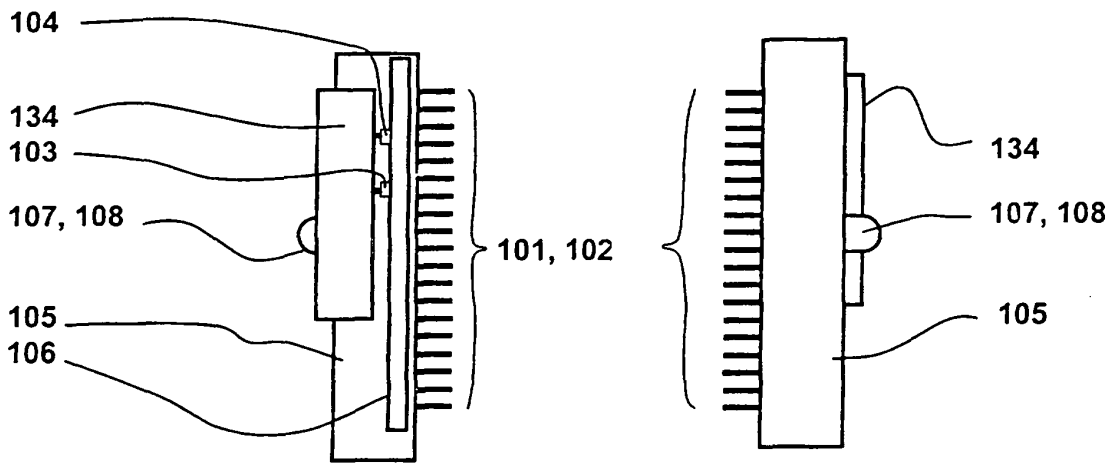


Fig. 5a

Fig. 5b

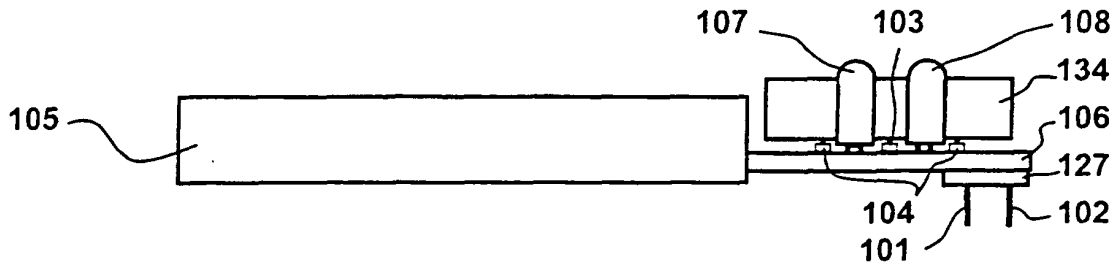


Fig. 6

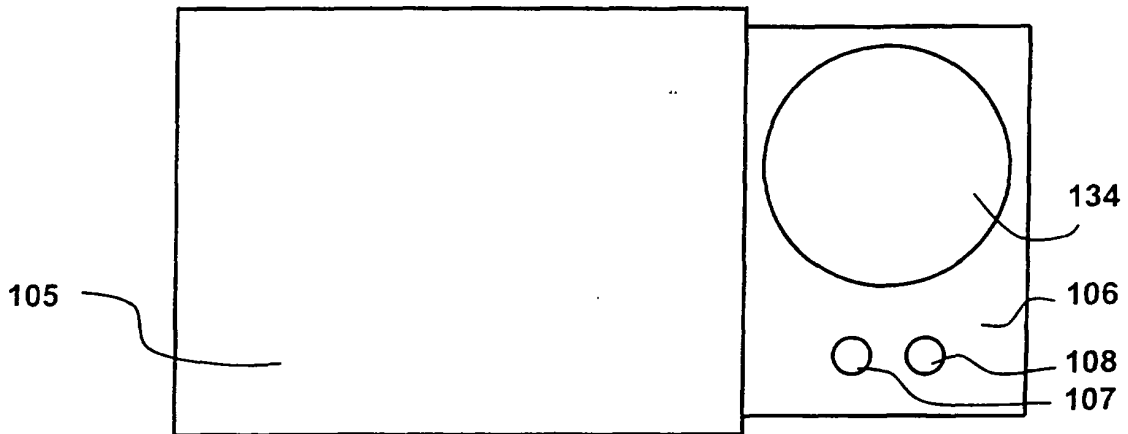


Fig. 7

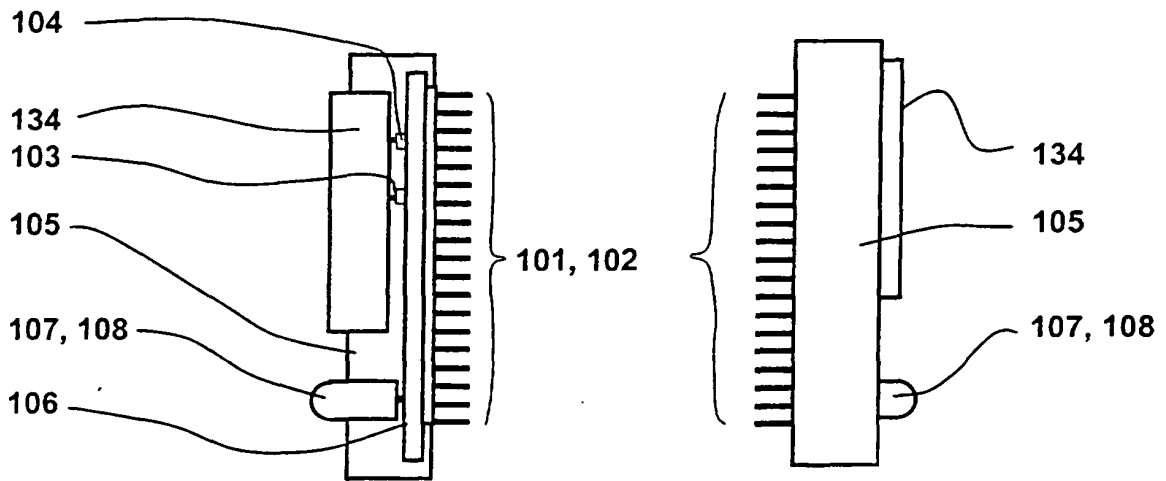


Fig. 8a

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

- EP 789333 A2 [0002]
- EP 417447 B1 [0004]
- DE 19816572 [0005]
- DE 19816571 [0005]
- EP 0649080 A [0007]