



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 199 28 057 B4 2005.11.10**

(12)

Patentschrift

(21) Aktenzeichen: **199 28 057.6**
 (22) Anmeldetag: **15.06.1999**
 (43) Offenlegungstag: **28.12.2000**
 (45) Veröffentlichungstag
 der Patenterteilung: **10.11.2005**

(51) Int Cl.7: **G07B 17/04**
G06F 12/14

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 2 Patentkostengesetz).

(73) Patentinhaber:
Francotyp-Postalia AG & Co. KG, 16547
Birkenwerder, DE

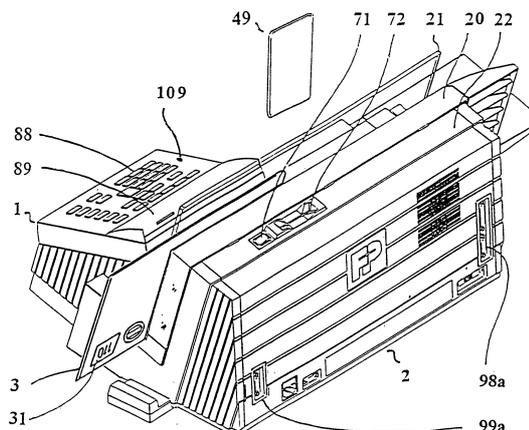
(56) Für die Beurteilung der Patentfähigkeit in Betracht
 gezogene Druckschriften:
DE 42 17 830 A1
US 58 05 711
EP 07 89 333 A2

(72) Erfinder:
Rosenau, Dirk, 13469 Berlin, DE

(54) Bezeichnung: **Sicherheitsmodul und Verfahren zur Sicherung der Postregister vor Manipulation**

(57) Hauptanspruch: Sicherheitsmodul zur Sicherung der Postregister vor Manipulation, mit einem Programmspeicher (128), einer ersten (120) und zweiten Datenverarbeitungseinheit (150), mit einem nichtflüchtigen Speicher (114, 116), welche operativ miteinander verbunden sind, um die erste Datenverarbeitungseinheit (120) zu veranlassen, ein Postwertguthaben in nichtflüchtige Speicher (114, 116) nachzuladen und um die zweite Datenverarbeitungseinheit (150) zu veranlassen, die Abrechnung durchzuführen sowie um im nichtflüchtigen Speicher (114, 116) die Postregisterdaten zu speichern, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit (120) einen internen nichtflüchtigen Speicher (124) aufweist, in welchem mindestens ein Schlüssel für die Berechnung eines Autorisierungscode (MAC) vor einem Zugriff geschützt gespeichert ist, und wobei die erste Datenverarbeitungseinheit (120) durch ein Programm im Programmspeicher (128) programmiert ist:

- die Gültigkeit der bei der vorherigen Abrechnung im nichtflüchtigen Speicher (114, 116) gespeicherten Postregisterdaten zu überprüfen und
- bei Gültigkeit der bei der vorherigen Abrechnung gespeicherten Postregisterdaten die neuen Postregisterdaten vorzuberechnen,
- einen zugehörigen Autorisierungscode (MAC)...



Beschreibung

[0001] Die Erfindung betrifft ein Sicherheitsmodul mit Sicherung der Postregister vor Manipulation, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art und für ein Verfahren zur Sicherung der Postregister vor Manipulation gemäß der im Oberbegriff des Anspruchs 5 angegebenen Art. Ein solcher postalischer Sicherheitsmodul ist insbesondere für den Einsatz in einer Frankiermaschine bzw. Postbearbeitungsmaschine oder Computer mit Postbearbeitungsfunktion geeignet.

Stand der Technik

[0002] Es sind vielfältige Sicherungsmaßnahmen zum Schutz gegen Ausfälle bzw. Störungen von intelligenten elektronischen Systemen bekannt. Bei einem Verfahren zum Betreiben einer Datenverarbeitungsanlage nach DE 42 17 830 C2 werden bei einer auf Spannungsausfall folgenden Spannungswiederkehr die vor dem Spannungsausfall im Speicher vorhandenen Informationen wieder bereitgestellt.

[0003] Es ist bereits aus EP 417 447 B1 bekannt, in elektronischen Datenverarbeitungsanlagen besondere Module einzusetzen und mit Mitteln zum Schutz vor einem Einbruch in ihre Elektronik auszustatten. Solche Module werden nachfolgend Sicherheitsmodule genannt.

[0004] 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. Ein Sicherheitsmodul (EP 789 333 A2) kann eine Hardware-Abrecheneinheit und/oder die Einheit zum Absichern des Druckens der Postgebührendaten aufweisen. Beispielsweise kann ersterer als Anwenderschaltkreis ASIC und letzterer als OTP-Prozessor (One Time Programmable) realisiert werden. Der interne OTP-ROM speichert auslesesicher sensible Daten (kryptografische Schlüssel), die beispielsweise zum Nachladen eines Guthabens erforderlich sind. Eine Kapselung durch ein Sicherheitsgehäuse bietet einen weiteren Schutz.

[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 8 mit dem Titel: Anordnung für ein Sicherheitsmodul und 198 16 571.4 mit dem Titel: Anordnung für den Zugriffsschutz für Sicherheitsmodule, sowie 199 12 780.8 mit dem Titel: Anordnung für ein Sicherheits-

modul, 199 12 781.6 mit dem Titel: Verfahren zum Schutz eines Sicherheitsmoduls und Anordnung zur Durchführung des Verfahrens und die deutsche Gebrauchsmusteranmeldung 299 05 219.2 mit dem Titel: Sicherheitsmodul mit Statussignalisierung vorgeschlagen. Ein steckbares Sicherheitsmodul kann in seinem Lebenszyklus verschiedene Zustände einnehmen. Es kann nun unterschieden werden, ob das Sicherheitsmodul funktioniert oder defekt ist. Dabei wird auf die Nichtmanipulierbarkeit der hardwaremäßigen Abrechnung vertraut, ohne dies noch einmal zu kontrollieren. Jede andere softwaregesteuerte Arbeitsweise gilt nur mit den Originalprogrammen als fehlerfrei, welche deshalb vor einer Manipulation geschützt werden müssen.

[0006] Bekanntlich wird in Frankiermaschinen, beispielsweise vom Typ T1000, ein MAC (MESSAGE AUTHENTICATION CODE) zur Absicherung der Postregisterdaten eingesetzt (EP 762 338 A2, US 5,805,711). Auf diese Weise kann auch der Mikroprozessor des Sicherheitsmoduls vor einer Abrechnung die Gültigkeit (Manipulationsfreiheit) der Postregister überprüfen. Der Mikroprozessor berechnet einen MAC über die Daten in den Postregistern und vergleicht diesen MAC mit einem Vergleichs-MAC der für diese Postregister bereits früher gespeichert worden ist. Anschließend erfolgt eine Abrechnung. Danach muß der Mikroprozessor erneut den Vergleichs-MAC für die vom Anwenderschaltkreis ASIC modifizierten Postregister berechnen, um ihn zu aktualisieren. In dieser Zeit, vom Start der Abrechnung bis zum Schreiben des neuen Vergleichs-MAC, sind jedoch für einen Betrüger mit Speicherzugriff die Postregister manipulierbar, ohne daß dies durch den Mikroprozessor erkannt werden kann.

Aufgabenstellung

[0007] Der Erfindung liegt die Aufgabe zugrunde, für ein Sicherheitsmodul die Sicherheit bei der Abrechnung zu erhöhen.

[0008] Es soll ein Verfahren gefunden werden, welches mit minimalen Aufwänden eine maximale Sicherheit vor einer Manipulation der gespeicherten Daten ermöglicht. Das Verfahren soll beispielsweise in Frankiermaschinen Anwendung finden, für die besondere Sicherheitsforderungen bezüglich der Postregisterdaten gelten, da insbesondere die geldwerten Abrechnungsdaten unmanipulierbar sein müssen.

[0009] Die Aufgabe wird mit den Merkmalen des Anspruchs 1 für eine Anordnung und mit den Merkmalen des Anspruchs 5 für ein Verfahren gelöst.

[0010] Eine Lösung des Problems wurde in der Durchführung von zwei zeitlich versetzten Abrechnungen durch unterschiedliche Rechner gefunden. Voraussetzung für eine Vorausberechnung eines

Postregistersatzes ist ein schon zu Beginn vorliegender Authorisierungscode (MAC_{alt}), der die Gültigkeit eines vorherigen Postregistersatzes und damit der vorherigen Abrechnungsdaten in an sich bekannter Weise zu überprüfen gestattet. Bei deren Gültigkeit wird von dem ersten Rechner eine Vorausberechnung eines zugehörigen Authorisierungscode (MAC_{neu}) über den vorausberechneten Postregistersatz vorgenommen. Vorzugsweise wird hierzu ein Mikroprozessor eines Sicherheitsmoduls eingesetzt, welcher nachfolgend als Modulprozessor bezeichnet wird. Wenn der Modulprozessor, beispielsweise vor Beginn der Vorausabrechnung, den alten Postregistersatz durch Berechnung eines MAC's und durch den Vergleich dieses MAC's mit dem gespeicherten MAC_{alt} überprüft hat, berechnet er im sicheren Speicherbereich den für die nächste Abrechnung zugehörigen neuen Authorisierungscode MAC_{neu} im Voraus, bevor die Hauptabrechnung angestoßen wird, die ein zweiten Rechner durchführt. Vorzugsweise wird hierzu eine anwenderspezifische Verarbeitungseinheit ASIC des Sicherheitsmoduls eingesetzt, welches eine Hardwareabrechnungsbaugruppe aufweist und die Abrechnungsdaten in die Postregister einschreibt. Zum Abschluß der Hauptabrechnung speichert der Modulprozessor nun noch den vorab berechneten MAC_{neu} als aktuellen gültigen MAC zu dem Postregistersatz mit den aktuellen Abrechnungsdaten. Der Unterschied liegt also:

1. im Zeitpunkt der MAC-Berechnung vor der Hauptabrechnung,
2. in der Quelle der MAC-Berechnung, weil dazu vom Modulprozessor zuerst die Postregisterabrechnungsdaten für den MAC_{neu} vorausberechnet werden müssen.

[0011] Wenn die nächste Abrechnung erfolgt, wird das o.g. Verfahren wiederholt. Mit dem erfindungsgemäßen Verfahren kann durch das Prüfen der MAC's nun auch eine während der Abrechnung vorgenommene Manipulation festgestellt werden. Da die Quellen für die MAC-Berechnung der beiden Vergleichswerte unterschiedlich sind, müssen die zu vergleichenden MAC's identisch sind. Unter der Annahme, daß bei der Abrechnung durch das ASIC kein Fehler auftritt, kann es sich nur um eine Manipulation handeln, wenn die MAC's nicht übereinstimmen.

[0012] Ein weiterer Vorteil dieser Methode ist der, dass beim Einschalten (PowerOn) zwei MAC's existieren.

1. einer, der für die Postregister gilt, falls die Abrechnung nicht vollständig beendet wurde
2. einer, der für die Postregister gilt, falls die Abrechnung beendet wurde, der neue MAC aber noch nicht geschrieben werden konnte.

[0013] Somit muß mindestens ein Postregistersatz existieren, dessen MAC mit einem dieser beiden übereinstimmt. Letzterer ist der gültige nicht manipu-

lierte Registersatz und kann als Referenz gelten. Andernfalls wurde manipuliert.

[0014] Diese Methode sichert zu jedem Zeitpunkt t die Postregisterdaten mit einem MAC. Ein Angriff durch eine Manipulation der Registerdaten zu einem beliebigen Zeitpunkt kann nicht mehr unbemerkt bleiben.

[0015] Ein Sicherheitsmodul für beispielsweise eine Frankiermaschine, nimmt deren Funktion einer Abrechnung war, insbesondere von Postgebühren und/oder deren kryptografische Absicherung. Es ist erfindungsgemäß durch eigene Signalmittel gekennzeichnet, die bei direkter Ansteuerung vom Prozessor des Sicherheitsmoduls eine Aussage über den aktuellen Zustand des Sicherheitsmoduls gestatten. Die Signalisierung des Modulzustandes wird nur bei Versorgung des Sicherheitsmoduls mit Systemspannung aktiviert, um eine Batterie zu schonen. Der Prozessor überwacht die hardwaremäßige Abrecheneinheit. Dabei steht nicht die Verfügbarkeit des Systems im Vordergrund, sondern die sichere Erkennung von Fehlfunktionen oder Ausfällen sowie eine geeignete Reaktion darauf, wie es bei besonders sicherheits sensitiven, eher zeitunkritischen Vorgängen der Fall ist.

Ausführungsbeispiel

[0016] 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:

[0017] [Fig. 1](#), Perspektivische Ansicht der Frankiermaschine von hinten,

[0018] [Fig. 2](#), Blockschaltbild des Sicherheitsmoduls,

[0019] [Fig. 3](#), Seitenansicht des Sicherheitsmoduls,

[0020] [Fig. 4](#), Draufsicht auf das Sicherheitsmodul,

[0021] [Fig. 5](#), Tabelle für Statussignalisierung,

[0022] [Fig. 6](#), Darstellung der Prüfungen im System für statische und dynamisch änderbare Zustände,

[0023] [Fig. 7](#), Darstellung von Abläufen bei der Abrechnung anhand eines Zeitstrahles,

[0024] [Fig. 8](#), Flußdiagramm für die Prüfungen des Systems vor dem Frankieren.

[0025] In der [Fig. 1](#) ist eine perspektivische Ansicht der Frankiermaschine von hinten dargestellt. Die Frankiermaschine besteht aus einem Meter **1** und ei-

ner Base **2**. Letztere ist mit einer Chipkarten-Schreib/Leseinheit **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.

[0026] 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.

[0027] 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 U_{s+} an den Prozessor des Sicherheitsmoduls ausreicht, die Anzeige zu aktivieren, um den Modulzustand ablesen zu können.

[0028] Die [Fig. 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 Modulprozessors **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.

[0029] Das Sicherheitsmodul steht mit der Frankiermaschine über den Systembus **115, 117, 118** in Verbindung. Der Modulprozessor **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.

[0030] 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.

[0031] 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 Modulprozessor **120** arbeitet ein Programm ab, das im FLASH **128** gespeichert ist. Der Modulprozessor **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.

[0032] Die RESET-Einheit **130** ist über die Leitung **131** mit dem Pin 3 des Modulprozessors **120** und mit einem Pin des ASIC's **150** verbunden. Der Modulprozessor **120** und das ASIC **150** werden bei Absinken der Versorgungsspannung durch eine Resetgenerierung in der RESET-Einheit **130** zurückgesetzt.

[0033] Der Modulprozessor **120** weist intern eine Verarbeitungseinheit CPU **121**, eine Echtzeituhr RTC **122** eine RAM-Einheit **124** und eine Ein/Ausgabe-Einheit **125** auf. Der Modulprozessor **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** Adressen 0 bis 7 an die entsprechenden Adreßein-

gänge des FLASH **128**. Der Modulprozessor **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**, dem Adreßbus **117** und dem Steuerbus **115** der Hauptplatine des Meters **1** in Kommunikationsverbindung.

[0034] 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 Normalbetriebs 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.

[0035] 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. Das heißt, 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 Sleeping Mode (EP 660 268 A2) oder Long Time Watchdog (wird anhand der [Fig. 5](#) noch erläutert) umgeht.

[0036] Die Schaltung der Spannungsüberwachungseinheit **12** ist beispielsweise so dimensioniert, daß jegliches Absinken der Batteriespannung auf der Leitung **136** unter die spezifizizierte 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 Selbsthaltezustand, 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 ab-

fragen (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**.

[0037] Die Leitung **136** am Eingang des Batterieobservers **12** versorgt zugleich eine Detektions-Einheit **13** mit Betriebs- oder Batteriespannung. Vom Modulprozessor **120** wird der Zustand der Detektions-Einheit **13** über die Leitung **139** abgefragt oder die Detektions-Einheit **13** wird vom Modulprozessor **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 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 über die Leitung **192** von der Detektions-Einheit **13** abfragbar.

[0038] An den Pins 6 und 7 des Modulprozessors **120** sind Leitungen angeschlossen, welche nur bei einem, beispielsweise an die Hauptplatine des Meters **1**, gesteckten Sicherheitsmodul **100** eine Leitererschleife **18** bilden. Zur dynamischen Prüfung des Angeschlossenseins des postalischen Sicherheitsmoduls PSM **100** an der Hauptplatine des Meters **1** werden vom Modulprozessor **120** wechselnde Signale in ganz unregelmäßigen Zeitabständen an die Pin's 6, 7 angelegt und über die Schleife zurückgeschleift.

[0039] Der Modulprozessor **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.

[0040] Die [Fig. 3](#) 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 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. 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 Modulprozessors **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), je nachdem die LED's einzeln oder gleichzeitig angesteuert werden. Zur Zustandsunterscheidung werden die LED's auch einzeln oder zusammen blinkend ggf. abwechseln blinkend gesteuert, so daß neun verschiedene Zustände unterschieden werden können, in welchem mindestens eine der LED's aktiviert wird.

[0041] In der [Fig. 4](#) ist eine Draufsicht auf das postalische Sicherheitsmodul 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.

[0042] Gemäß einer in der [Fig. 5](#) gezeigten – sich selbst erläuternden – Tabelle für Statussignalisierung geht eine Vielzahl möglicher Zustandsanzeigen hervor. Eine grün leuchtende LED **107** signalisiert einen OK-Zustand **220**, aber eine leuchtende LED **108** signalisiert einen Fehler-Zustand **230** im Ergebnis eines mindestens statischen Selbsttestes. Das Ergebnis eines solchen an sich bekannten Selbsttestes kann wegen der direkten Signalisierung über die LED's **107**, **108** nicht verfälscht werden.

[0043] Beispielsweise für den Fall, daß zwischenzeitlich die im Sicherheitsmodul gespeicherten Schlüssel verlohren gingen, würde die laufende Überprüfung im dynamischen Betrieb den Fehler feststellen und als den Zustand **240** mit orange leuchtenden LED's signalisieren. Nach einem Aus/Einschalten ist ein Booten erforderlich, da anderenfalls keine andere Operation mehr ausgeführt werden kann. Der Fall, daß bei der Herstellung die Installation eines Schlüssels vergessen wurde, wird als Zustand **260** beispielsweise mit einer grün blinkenden LED **107** signalisiert. Auch der Fall, daß ein long time watchdog-Timer abgelaufen ist, wird als Zustand **250** durch eine rot blinkende LED signalisiert. Der long time watchdog-Timer ist abgelaufen, wenn lange Zeit die Datenzentrale nicht mehr kontaktiert wurde, beispielsweise um ein Guthaben nachzuladen. Der Zustand **250** wird ebenfalls erreicht, wenn das Sicherheitsmodul vom Meter getrennt wurde. Weitere Zustandsanzeigen für die Zustände **270**, **280**, **290** sind optional für verschiedene weitere Prüfungen vorgesehen.

[0044] Die [Fig. 6](#) zeigt eine Darstellung der Prüfungen im System für statisch und dynamisch änderbare Zustände. Ein ausgeschaltetes System im Zustand **200** geht nach dem Einschalten über die Transition Start **201** in den Zustand **210** über, in welchem vom Sicherheitsmodule ein statischer Selbsttest durchgeführt wird sobald die Betriebsspannung anliegt. Bei der Transition **202**, bei der der Selbsttest ein OK bei ordnungsgemäßem Ergebnis ergibt, wird der Zustand **220** LED grün leuchtend erreicht. Ausgehend von letzterem Zustand ist bei Bedarf ein wiederholter statischer Selbsttest und ein dynamischer Selbsttest durchführbar. Eine solche Transition **203** oder **206** führt entweder zurück auf den Zustand **220** LED grün bei OK oder auf den Zustand **240** LED orange bei einem Fehler. Letzterer ist durch einen Recover-Versuch evtl. durch Ausschalten (Transition **211**) und Wiedereinschalten des Gerätes (Transition **201**) behebbar. Statische Fehler sind aber nicht behebbar. Von Zustand **210**, in welchem das eingeschaltete Gerät einen statischen Selbsttest ausführt, existiert bei einem Fehler eine Transition **204** zum Zustand **230** LED rot. Zu jeder Zeit, wenn sich das Gerät im Zustand **220** LED grün befindet, kann ein on demand ausgeführter statischer Selbsttest bei einem Fehler über eine Transition **205** zum Zustand **230** LED rot

führen. Ausgehend vom Zustand **220** LED grün können nicht gezeigte weitere Transitionen **207**, **208**, **209** zu den weiteren Zuständen **270** (mit orange blinkenden LED's signalisiert), **280** (mit rot leuchtend/orange blinkenden LED's signalisiert) und **290** (mit grün leuchtend/orange blinkenden LED's signalisiert) führen.

[0045] Der – in der [Fig. 2](#) gezeigte – Sicherheitsmodul **100** ist mit einem Programmspeicher **128**, der ein Programm zur Sicherung der Postregister vor Manipulation aufweist, einer ersten und zweiten Datenverarbeitungseinheit **120**, **150**, mit nichtflüchtigen Speichern **114**, **116**, mit weiteren miteinander verschalteten Funktionseinheiten **12**, **13**, **130**, **160** und **180** verbunden, wobei sämtliche vorgenannte Funktionseinheiten mit einer Vergußmasse **105** bedeckt sind, außer die Batterie **134** ([Fig. 3](#) und [Fig. 4](#)). Im Sicherheitsmodul **100** ist die erste Datenverarbeitungseinheit **120** der Modulprozessor. Letzterer ist für die Durchführung von mindestens einer Autorisierungsroutine für die Postregisterdaten programmiert, wobei deren Autorisierung in Verbindung mit dem zugehörigen Autorisierungscode MAC im nichtflüchtigen Speichern **114**, **116** einen Modulzustand signalisiert, welcher eine weitere Abrechnung durchzuführen gestattet, und wobei zur Signalisierung des Modulzustandes ein optisches oder akustisches Signalmittel **107**, **108** am Modulprozessor angeschlossen ist. Die erste Datenverarbeitungseinheit **120** kann für die Durchführung zusätzlicher Sicherungsroutinen in Verbindung mit weiteren miteinander verschalteten Funktionseinheiten **12**, **13** programmiert sein. Das Signalmittel **107**, **108** wird zur Zustandsunterscheidung entsprechend angesteuert. Ein separates Sicherheitsgehäuse, daß nahe an der Vergußmasse **105** und ringsherum angeordnet ist, kann eingespart werden, wenn das Meter bereits ein Sicherheitsgehäuse aufweist, d.h. daß das umgebende Sicherheitsgehäuse Bestandteil eines Meters **1** ist. Das Signalmittel **107**, **108** ragt in demjenigen Bereich des Sicherheitsmoduls **100** durch das Vergußmaterial **105** hindurch, wo das umgebende Metergehäuse zur Signalisierung des Modulzustandes eine Öffnung **109** aufweist, welche sich zur Bedienoberfläche **88**, **89** des Meters **1** erstreckt. Die Abmaße bzw. der Durchmesser der Öffnung liegen in der Größenordnung des Signalmittels, welches zum Beispiel als Anzeigeeinheit realisiert ist. Eine solche Anzeigeeinheit kann eine oder mehrere oder mehrfarbige Leuchtdioden (LED's) einschließen. Letztere können zur Zustandsunterscheidung auch blinkend gesteuert werden. Wenn die Leuchtdioden LED's **107**, **108** zur Zustandsunterscheidung gleichzeitig angesteuert werden, hat deren emittiertes sichtbares Licht eine kombinierte Farbe (beispielsweise Orange), die im Ergebnis der Autorisierungsroutine beim dynamischen Selbsttest einen Fehler signalisiert.

[0046] Die in der [Fig. 2](#) gezeigten Speicher **114** und

SRAM **116** werden nachfolgend zur Vereinfachung mit NVRAM_A bezeichnet. Im NVRAM_A sind zum Zeitpunkt t_i beispielsweise Ascending-, Descending-, Stückzahl- und weitere Daten gegeben, die für zukünftige Abrechnungen genutzt werden sollen. Vereinfachend wird die Zusammenfassung der vorgenannten Daten auch als P'_{t_i} = Postregistersatz bezeichnet. Dabei bedeutet das Zeichen „'“ hinter dem Buchstaben P, daß dieser Postregistersatz vom ASIC **150** berechnet wurde. Jeder Postregistersatz wird außerdem mit einem MAC abgesichert, welcher vom Modulprozessor **120** berechnet wurde und ebenfalls im NVRAM_A gespeichert vorliegt.

[0047] Der in der [Fig. 2](#) gezeigte batteriegestützte statische RAM **124** des OTP-Prozessorbausteins **120** wird nachfolgend mit NVRAM_P bezeichnet, weil OTP-intern nichtflüchtig gespeicherten Daten nicht von außen lesbar sind. Eine von der Batterie **134** über den Umschalter **180** und über die Spannungsüberwachungseinheit **12** gelieferte Spannung U_{b+} ist auf der Leitung **138** ständig verfügbar und versorgt den OTP-internen Speicher RAM **124**, der dadurch Daten nichtflüchtig speichern kann. Ein bereits früher eingegebener Portwert bleibt somit nichtflüchtig gespeichert, bis er überschrieben wird. Gegeben sei deshalb zum Zeitpunkt t_i im NVRAM_A oder NVRAM_P ein Portwert p_{t_i} , der für zukünftige Abrechnungen genutzt werden kann. Eine Abrechnung $P_{t_{(i+1)}} = F(P'_{t_{(i-1)}}, p_{t_i}) = P_{neu}$ bedeutet, daß zum Zeitpunkt t_{i-1} bereits ein Postregistersatz vorlag, der berücksichtigt wird, wenn Zeitpunkt t_i ein Portwert p_{t_i} eingegeben wird und daß die Abrechnung nach der Funktion F zum Zeitpunkt t_{i+1} vom Modulprozessor **120** vorgenommen wurde. Anderenfalls bedeutet eine Abrechnung $P'_{t_{(i+1)}} = F'(P'_{t_{(i-1)}}, p_{t_i})$, daß die Abrechnung nach der Funktion F' zum Zeitpunkt t_{i+1} von der Hardwareabrecheneinheit des ASIC's **150** vorgenommen wurde.

[0048] Zur Autorisierungsprüfung an einem beliebigen Zeitpunkt t_i können die Daten des Postregistersatz aus einem NVRAM_A verwendet werden, um einen MAC vom Postregistersatz zu bilden. Wenn der Ausdruck $MAC(P_{t_i})$ aber kein Zeichen „'“ hinter dem Buchstaben P hat, dann bedeutet dies, daß dieser Postregistersatz und MAC vom Modulprozessor **120** zum Zeitpunkt t_i berechnet wurde. Der Mikroprozessor kann im NVRAM_P erforderlichenfalls sofort berechnen:

$P_{t_{(i+1)}}$ = Postregistersatz zum Zeitpunkt t_{i+1}
 $MAC(P_{t_{(i+1)}})$ = MAC vom Postregistersatz zum Zeitpunkt t_{i+1}

[0049] Die [Fig. 7](#) zeigt eine Darstellung von Abläufen bei der Abrechnung anhand eines Zeitstrahles. Die Eingabe eines neuen Portwertes oder eine Briefanlage bildet den Ausgangspunkt t_0 für eine Anzahl an Abläufen. Bei Briefanlage kann auch von der Weiterverwendung eines bereits eingegebenen Por-

Portwertes als neuen Portwert ausgegangen werden. Zunächst wird vom Modulprozessor **120** aus dem NVRAM_A ein MAC_{alt} geholt und definiert durch den Zeitpunkt t_0 als $MAC(P_{t_0})$ im NVRAM_P gespeichert. Zugleich werden die P'_{ti} -Registerdaten zu einem MAC verarbeitet, wobei das Ergebnis spätestens zum Zeitpunkt t_1 vorliegt und ebenfalls im NVRAM_P zwischengespeichert wird. Dann wird der zum Zeitpunkt t_1 vorliegende $MAC(P'_{t_0})$ mit dem $MAC(P_{t_0})$ verglichen. Bei Übereinstimmung liegt kein Fehler vor und es wird vom Modulprozessor **120** das Ende der Eingabe zum Zeitpunkt t_2 abgewartet. Der Modulprozessor **120** stößt zum Zeitpunkt t_2 eine Vorausberechnung eines neuen Postregistersatzes P_{12} und eine weitere Bildung eines neuen MAC an, wobei der Wert des MAC_{neu} gespeichert wird. Der Vorgang ist zum Zeitpunkt t_3 abgeschlossen und nun wird eine an sich bekannte Abrechnung und Bildung eines neuen Postregistersatzes vom ASIC **150** vorgenommen. Während der Postregistersatz P'_{13} gebildet wird, liegen zwei MAC's gespeichert vor, nämlich $MAC_{alt} = MAC(P_{t_0})$ und der vorausberechnete $MAC_{neu} = MAC(P_{12})$. Davor gilt noch der alte MAC_{alt} und bei Spannungsausfall kann auf die vorherigen Daten zurückgegriffen werden, welche im NVRAM_A gespeichert vorliegen. Die Abrechnung wird dann vollständig wiederholt. Somit ergibt sich für einen eventuellen Manipulator zu keinem Zeitpunkt eine Fälschungsmöglichkeit. Ist der Postregistersatz P'_{13} zum Zeitpunkt t_4 vom ASIC berechnet worden, dann erfolgt ein Löschen bzw. Überschreiben des alten $MAC(P_{t_0})$ mit dem neuen $MAC(P_{12})$ und ein Speichern des neuen Registersatzes P'_{13} im NVRAM_A. Letzterer Vorgang ist zum Zeitpunkt t_5 abgeschlossen.

[0050] Anhand des – in der [Fig. 8](#) dargestellten – Flußdiagramms werden nun die Prüfungen näher erläutert, welche im System vor dem Frankieren ablaufen. Der Mikroprozessor CPU **121** ist durch ein entsprechendes im Flash **128** gespeichertes Programm programmiert, solche vorgenannten Selbsttests auszuführen, wobei nach dem Start **299**, in einem ersten Schritt **300** ein Power on-Selbsttest durchgeführt und dann im Schritt **301** gefragt wird, ob der Power on-Selbsttest ein OK ergeben hat. Ist das der Fall, so wird im Schritt **302** die grüne LED **107** vom Mikroprozessor CPU **121** über ein I/O-Port **125** leuchtend gesteuert. Anderenfalls wird im Schritt **303** die rote LED **108** vom Mikroprozessor CPU **121** über ein I/O-Port **125** leuchtend gesteuert.

[0051] Vom Schritt **302** wird auf die Abfrage **304** verzweigt, in welcher geprüft wird, ob eine weitere statische Prüfung verlangt wird. Ist das der Fall, so wird zum Schritt **300** zurückverzweigt. Anderenfalls wird auf die Abfrage **305** verzweigt, in welcher geprüft wird, ob durch einen Briefsensor eine Briefanlage festgestellt bzw. vom Modulprozessor **120** eine Eingabe einen neuen Portwertes erkannt wird. Ist dies beides nicht der Fall, dann wird auf den Schritt **302**

zurückverzweigt und somit eine Warteschleife solange durchlaufen, bis eine Briefanlage/Neueingabe festgestellt worden ist. Im letzteren Fall wird auf den Schritt **306** verzweigt, um das Eingeben der Daten zu beenden. Gleichzeitig oder kurz nach dem Zeitpunkt t_0 beginnend, wird ein Schritt **307** zur MAC-Berechnung auf der Grundlage der zum Zeitpunkt t_0 verfügbaren Postregisterdaten P'_{t_0} gestartet. Ein vom OTP bereits früher gebildeter $MAC(P_{t_0})$ ist zum Zeitpunkt t_0 gültig. Die MAC-Berechnung ist zum Zeitpunkt t_1 abgeschlossen. Der berechnete $MAC(P'_{t_0})$ wird mit dem alten zum Zeitpunkt t_0 gültigen (vom OTP bereits früher gebildeten) $MAC(P_{t_0})$ zum Zeitpunkt t_1 im Schritt **308** verglichen. Bei Nichtübereinstimmung wird zum Schritt **315** verzweigt, um die LED's **107**, **108** orange leuchtend zu steuern. Anderenfalls wird zu den Schritten **309**, **310** verzweigt. Dort erfolgt zum Zeitpunkt t_2 im OTP **120** eine Vorausberechnung des neuen Postregistersatzes P_{12} und anschließend eine MAC-Bildung, ggf. mit Speicherung des $MAC(P_{12})$ im NVRAM_P.

[0052] Zum Zeitpunkt t_3 , wenn im Schritt **311** die Speicherung des $MAC(P_{12})$ im NVRAM_P von der einen Datenverarbeitungseinheit **120** abgeschlossen worden ist, wird vom anderen Datenverarbeitungseinheit, nämlich von einer – nicht gezeigten – Hardware-Abrecheneinheit im ASIC **150** eine Berechnung des neuen Postregistersatzes im Schritt **312** durchgeführt.

[0053] In einem abschließenden Schritt **313** erfolgt wieder eine Abspeicherung der Ergebnisse P'_{13} und $MAC(P_{12})$ im NVRAM_A. In Vorbereitung eines Frankierens können dann noch eine Anzahl von weiteren Schritten durchlaufen werden, mindestens jedoch ein Schritt **314** Druckdatenbereitstellung zum Frankieren des Briefes. Anschließend wird zum Schritt **302** zurückverzweigt.

[0054] Der Schritt **314** mit Druckdatenbereitstellung zum Frankieren kann optional einen – nicht gezeigten – Subschritt zum Übermitteln eines generierten Sicherheitscodes einschließen. Zum Generieren des Sicherheitscode wird zwar ebenfalls eine prinzipiell vergleichbare Bildungsprozedure genutzt, wie bei der MAC-Bildung, der Daten-Authorisierungs-Code DAC setzt sich aber aus anderen Daten zusammen und das Generieren erfolgt zu einem anderem Zeitpunkt t_{i+1} ab Dateneingabeende zu einem Wert $DAC(P_{t(i+1)})$, sonstige Daten).

[0055] Der Modulprozessor **120** arbeitet mit einem – nicht gezeigten – Steuerungsprozessor des Meters zusammen, wobei letzterer den Sicherheitscode empfängt, die Druckdaten zusammenstellt und zum Druckkopf übermittelt.

[0056] Dadurch, dass nach dem Abspeichern der Ergebnisse zum Schritt **302** zurückgezweigt wird, er-

gibt sich on demand eine zweistufige Prüfung. Im Fehlerfall im Ergebnis der dynamischen Prüfung werden im Schritt **309** beide, die grüne LED **107** und die rote LED **108**, vom Mikroprozessor CPU **121** über ein I/O-Port **125** leuchtend gesteuert. Somit ergibt sich der Gesamteindruck, daß die LED's orange leuchten.

[0057] Die in der [Fig. 8](#) auf der rechten Hälfte des Flußplanes vermerkten Zeitpunkte t_0 bis t_5 sollen helfen, einen Bezug zur [Fig. 7](#) herzustellen. Damit sollen alternative Abläufe jedoch nicht ausgeschlossen werden. Die Vorausberechnung muß nicht nach einer Autorisierungsüberprüfung erfolgen. Ebensogut kann zuerst ein neuer Postregistersatz P_{t_i} vom Modulprozessor **120** vorausberechnet werden, wobei ein bereits eingegebener gespeicherter Portowert p_t berücksichtigt wird. Erst danach wird vom Modulprozessor **120** eine Autorisierungsüberprüfung bezüglich des alten im Speicher NVRAM_A gespeicherten Postregistersatzes $P'_{t_{i-1}}$ vorgenommen, wobei ein Autorisierungscode $MAC(P'_{t_{i-1}})$ vom Modulprozessor gebildet und mit einem zugehörigen im Speicher NVRAM_A gespeicherten bisherigen Autorisierungscode $MAC_{alt} = MAC(P'_{t_{i-1}})$ verglichen wird. Nach der Autorisierungsüberprüfung berechnet der Modulprozessor **120** einen neuen Autorisierungscode $MAC_{neu} = MAC(P_{t_i})$ über den neuen Postregistersatz P_{t_i} . Der neue Postregistersatz P_{t_i} bleibt bis zur MAC-Berechnung im OTP-internen NVRAM_P gespeichert. Das ist wichtig, um eine Manipulation während der Berechnung zu verhindern, insbesondere wenn die Vorausberechnung des neuen Postregistersatz P_{t_i} und des neuen MAC's zeitlich auseinander liegen.

[0058] Im NVRAM_A können zu einem Zeitpunkt t_i also folgende Daten gespeichert sein:

$P'_{t_{i-1}}$ – bisheriger Postregistersatz, der vom ASIC berechnet wurde,
 $MAC(P'_{t_{i-1}})$ – zugehöriger MAC_{alt} über einen gleichen Postregistersatz, der beim vorherigem Abrechnen vom Modulprozessor vorausberechnet wurde.

[0059] Im Speicher NVRAM_P speichert die erste Datenverarbeitungseinheit, vorzugsweise der Modulprozessor **120**, zu dem ersten Zeitpunkt t_i gegebenenfalls folgende Daten:

$$MAC(P_{t_i}) = MAC_{neu}$$

[0060] Von der zweiten Datenverarbeitungseinheit, vorzugsweise vom ASIC **150**, wird zu einem späteren zweiten Zeitpunkt t_{i+1} die Abrechnung mit einem Portowert p_{t_i} nach der Abrechnungsfunktion F' durchgeführt. Es erfolgt:

1. Bilden des Postregistersatzes $P'_{t_{i+1}} = F'(P'_{t_{i-1}}, p_{t_i})$ mit anschließender Speicherung im Speicher NVRAM_A.
2. Außerdem überschreibt der Modulprozessor **120** den im NVRAM_A gespeicherten $MAC(P'_{t_{i-1}})_{alt}$

mit dem vorausberechneten im NVRAM_P gespeicherten $MAC(P_{t_i})_{neu}$.

3. Optional übermittelt der Modulprozessor **120** einen zusätzlich generierten Sicherheitscode $DAC(P_{t_{i+1}})$, sonstige Daten) zur extern vom Sicherheitsmodul im Meter angeordneten dritten Datenverarbeitungseinheit (nicht gezeigt) zur Druckbilderzeugung.

[0061] Vor dem nächsten Frankieren wiederholt sich der Vorgang. Bis zum Zeitpunkt t_{i+2} wird ein neuer Portowert $p_{t_{i+2}}$ eingegeben. Zum Zeitpunkt t_{i+2} oder später kann wieder die Manipulationsfreiheit von $P'_{t_{i+1}}$ geprüft werden, indem $MAC(P'_{t_{i+1}})$ berechnet und mit dem im NVRAM_A gespeicherten Wert $MAC(P_{t_i})_{alt}$ verglichen wird. Es kann aber auch schon optional eine Generierung eines zusätzlichen Sicherheitscodes $MAC(P_{t_{i+1}})$, sonstige Daten) begonnen werden. Vor der eigentlichen Abrechnung durch den ASIC **150** erfolgt wieder eine MAC-Vorausberechnung durch den Modulprozessor. Zum Beispiel errechnet der Modulprozessor im Zeitpunkt t_{i+3} einen neuen Autorisierungscode:

$$MAC_{neu} = MAC(P_{t_{i+3}}) = MAC[F(P'_{t_{i+1}}, p_{t_{i+2}})].$$

[0062] Erfindungsgemäß ist in einer Subvariante vorgesehen, daß der aufgrund des vorausberechneten neuen Postregistersatzes gebildete zugehörigen Autorisierungscode MAC_{neu} nach seiner Erzeugung in einem Bereich des nichtflüchtigen Speichers **114**, **116** (NVRAM_A für die Postregisterdaten) gespeichert wird. Alternativ oder zusätzlich kann der aufgrund des vorausberechneten neuen Postregistersatzes gebildete zugehörigen Autorisierungscode MAC_{neu} nach seiner Erzeugung in einem Bereich des internen nichtflüchtigen Speichers **124** (NVRAM_P) der ersten Datenverarbeitungseinheit **120** (Modulprozessor) gespeichert werden.

[0063] Es ist in einer Subvariante vorgesehen, daß in Verbindung mit der Speicherung des von der zweiten Datenverarbeitungseinheit **150** (ASIC) ermittelten neuen Postregistersatzes $P'_{t_{i+1}}$ und des vorausberechneten neuen Autorisierungscode $MAC(P_{t_i})_{neu}$ in den nichtflüchtigen Speichern **114**, **116** (NVRAM_A) letzterer Autorisierungscode in einem weiteren Bereich des internen nichtflüchtigen Speichers **124** (NVRAM_P) der ersten Datenverarbeitungseinheit **120** (Modulprozessor) gespeichert wird, so daß der zu dem neuen Postregistersatz zugehörige Autorisierungscode bis zur nächsten Abrechnung redundant gespeichert ist.

[0064] Erfindungsgemäß ist das Sicherheitsmodul zum Einsatz in postalischen Geräten bestimmt, insbesondere zum Einsatz in einer Frankiermaschine. Jedoch kann das Sicherheitsmodul auch eine andere Bauform aufweisen, die es ermöglicht, daß es beispielsweise auf die Hauptplatine eines Personalcom-

puters gesteckt werden kann, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

Patentansprüche

1. Sicherheitsmodul zur Sicherung der Postregister vor Manipulation, mit einem Programmspeicher (128), einer ersten (120) und zweiten Datenverarbeitungseinheit (150), mit einem nichtflüchtigen Speicher (114, 116), welche operativ miteinander verbunden sind, um die erste Datenverarbeitungseinheit (120) zu veranlassen, ein Postwertguthaben in nichtflüchtige Speicher (114, 116) nachzuladen und um die zweite Datenverarbeitungseinheit (150) zu veranlassen, die Abrechnung durchzuführen sowie um im nichtflüchtigen Speicher (114, 116) die Postregisterdaten zu speichern, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit (120) einen internen nichtflüchtigen Speicher (124) aufweist, in welchem mindestens ein Schlüssel für die Berechnung eines Autorisierungscode (MAC) vor einem Zugriff geschützt gespeichert ist, und wobei die erste Datenverarbeitungseinheit (120) durch ein Programm im Programmspeicher (128) programmiert ist:

- die Gültigkeit der bei der vorherigen Abrechnung im nichtflüchtigen Speicher (114, 116) gespeicherten Postregisterdaten zu überprüfen und
- bei Gültigkeit der bei der vorherigen Abrechnung gespeicherten Postregisterdaten die neuen Postregisterdaten vorzuberechnen,
- einen zugehörigen Autorisierungscode (MAC) über die vorausgerechneten Postregisterdaten zu bilden und nach der Abrechnung den vorausgerechneten Autorisierungscode (MAC) zusammen mit den im Ergebnis der Abrechnung durch die zweite Datenverarbeitungseinheit (150) gebildeten Postregisterdaten im nichtflüchtigen Speicher (114, 116) zu speichern.

2. Sicherheitsmodul, nach Anspruch 1, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit (120) ein Modulprozessor (120) ist, welcher zur Gültigkeitsprüfung programmiert ist, einen zugehörigen Autorisierungscode (MAC) über die bei der vorherigen Abrechnung gespeicherten Postregisterdaten zu bilden und mit einem im nichtflüchtigen Speicher (114, 116) gespeicherten Autorisierungscode zu vergleichen, wobei bei Übereinstimmung die Gültigkeit der vorherigen Abrechnung signalisiert und die zweite Datenverarbeitungseinheit (150) berechtigt wird, eine weitere Abrechnung durchzuführen und wobei eine Nichtübereinstimmung signalisiert wird.

3. Sicherheitsmodul, nach den Ansprüchen 1 und 2, gekennzeichnet dadurch, dass die zweite Datenverarbeitungseinheit (150) eine anwenderspezifische Schaltung (ASIC) mit einer Hardwareabrecheneinheit einschließt, dass der Modulprozessor (120) des Sicherheitsmoduls (100) programmiert ist, eine Überwachung und Signalisierung des Modulzustandes

des Sicherheitsmoduls (100) vorzunehmen und bei Gültigkeit der vorherigen Abrechnung die zweite Datenverarbeitungseinheit (150) zu berechtigen, eine weitere Abrechnung durchzuführen.

4. Sicherheitsmodul, nach den Ansprüchen 1 bis 3, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit (120) als Modulprozessor für die Durchführung zusätzlicher Sicherungsroutinen für einen statischen oder dynamischen Selbsttest programmiert ist, wobei zur Signalisierung des Modulzustandes ein optisches oder akustisches Signalmittel (107, 108) am Modulprozessor angeschlossen ist und von dem das Signalmittel (107, 108) zur Zustandsunterscheidung entsprechend unterschiedlich angesteuert wird.

5. Verfahren zur Sicherung der Postregister vor Manipulation, mit einer Authorisierungscode-Berechnung und Abrechnung durch eine erste und eine zweite Datenverarbeitungseinheit eines Sicherheitsmoduls, gekennzeichnet durch die Schritte:

- Vorausberechnung des neuen Postregistersatzes (P_{ti}) mittels der ersten Datenverarbeitungseinheit (120), zu einem ersten Zeitpunkt (t_i) mindestens nach Briefanlage, wobei sich der neue Postregistersatz unter Verwendung des eingestellten Portowertes (p_{ti-1}) bei der Abrechnung ergibt, und Bilden eines neuen Autorisierungscode (MAC($P_{ti,neu}$)) nach einer Authorisierungsüberprüfung des bisher gültigen Postregistersatzes aus einer vorhergehenden Abrechnung mittels eines bisher zugeordneten Autorisierungscode (MAC_{alt}),
- Abrechnung mit Berechnung des neuen Postregistersatzes ($P'_{t(i+1)}$) zu einem zweiten Zeitpunkt (t_{i+1}), mittels der zweiten Datenverarbeitungseinheit (150), wobei sich der neue Postregistersatz unter Berücksichtigung des eingestellten Portowertes (p_{ti-1}) ergibt, und
- Speicherung des vorausgerechneten neuen Autorisierungscode (MAC($P_{ti,neu}$)) und des von der zweiten Datenverarbeitungseinheit (150) ermittelten neuen Postregistersatzes ($P'_{t(i+1)}$) in den nichtflüchtigen Speichern (114, 116).

6. Verfahren, nach Anspruch 5, gekennzeichnet dadurch, dass der aufgrund des vorausgerechneten neuen Postregistersatzes (P_{ti}) gebildete zugehörigen Autorisierungscode (MAC($P_{ti,neu}$)) nach seiner Erzeugung in einem Bereich des nichtflüchtigen Speichers (114, 116) für die Postregisterdaten gespeichert wird.

7. Verfahren, nach Anspruch 5, gekennzeichnet dadurch, dass der aufgrund des vorausgerechneten neuen Postregistersatzes (P_{ti}) gebildete zugehörigen Autorisierungscode (MAC($P_{ti,neu}$)) nach seiner Erzeugung in einem Bereich des internen nichtflüchtigen Speichers (124) der ersten Datenverarbeitungseinheit (120) gespeichert wird.

8. Verfahren, nach Anspruch 5, gekennzeichnet dadurch, dass in Verbindung mit der Speicherung des von der zweiten Datenverarbeitungseinheit (**150**) ermittelten neuen Postregistersatzes ($P'_{t(i+1)}$) und des vorausberechneten neuen Authorisierungscode ($MAC(P_{ti})_{neu}$) in den nichtflüchtigen Speichern (**114**, **116**) letzterer Authorisierungscode in einem weiteren Bereich des internen nichtflüchtigen Speichers (**124**) der ersten Datenverarbeitungseinheit (**120**) gespeichert wird, so dass der zu dem neuen Postregistersatz zugehörige Authorisierungscode bis zur nächsten Abrechnung redundant gespeichert ist.

9. Verfahren, nach einem der Ansprüche 5 bis 8, gekennzeichnet dadurch, dass die erste Datenverarbeitungseinheit (**120**) ein Modulprozessor ist.

10. Verfahren, nach einem der Ansprüche 5 bis 9, gekennzeichnet dadurch, dass der Modulprozessor (**120**) den in den nichtflüchtigen Speichern (**114**, **116**, NVRAM_A) gespeicherten alten Authorisierungscode (MAC_{alt}) mit dem im internen Speicher (**124**, NVRAM_P) gespeicherten vorausberechneten neuen Authorisierungscode ($MAC(P_{ti})_{neu}$) überschreibt.

11. Verfahren, nach den Ansprüchen 5 bis 10, gekennzeichnet dadurch, dass der Modulprozessor (**120**) einen zusätzlichen Sicherheitscode $MAC(P_{t(i+1)})$, sonstige Daten) generiert und zur extern vom Sicherheitsmodul erfolgenden Druckbilderzeugung übermittelt.

Es folgen 5 Blatt Zeichnungen

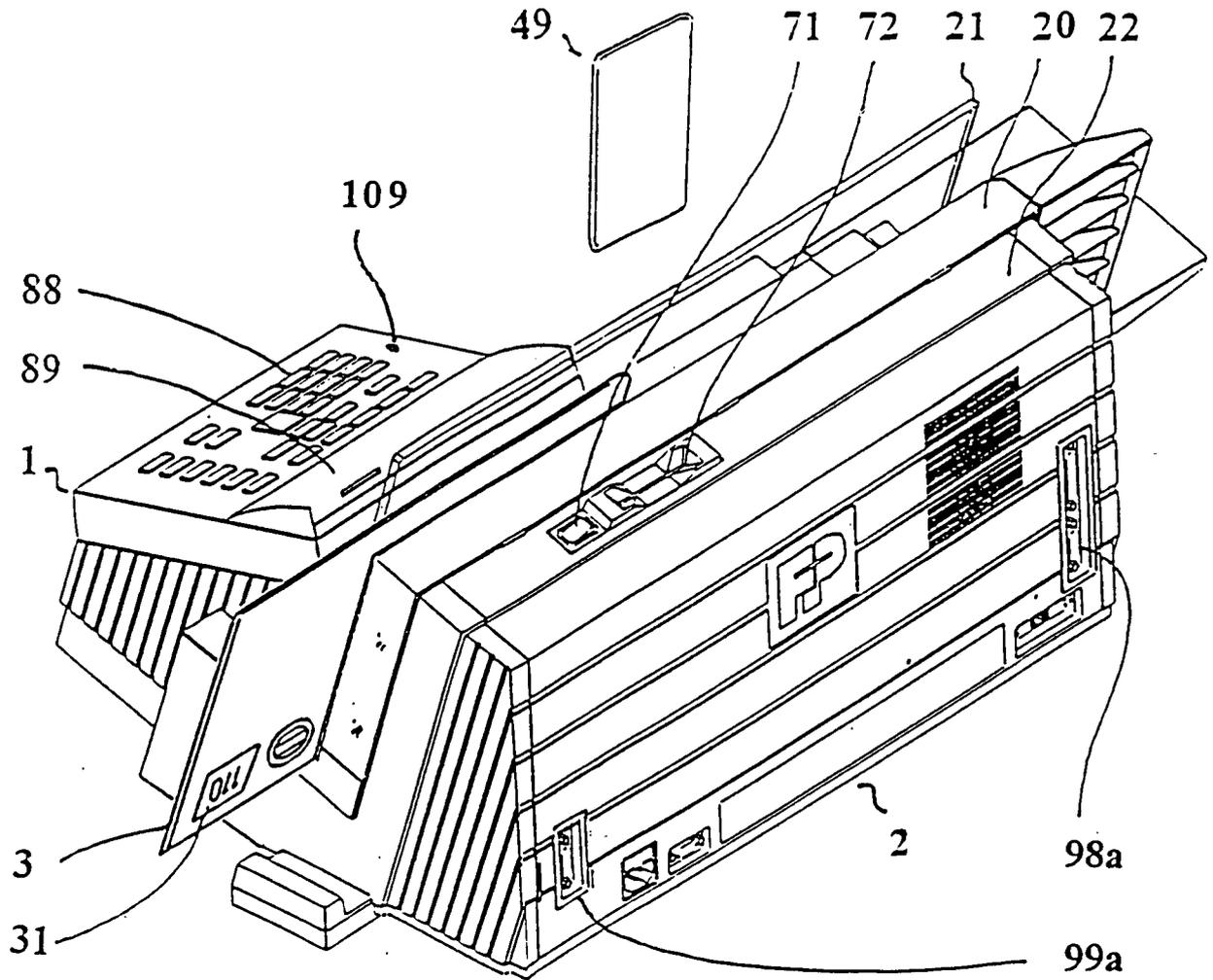


Fig. 1

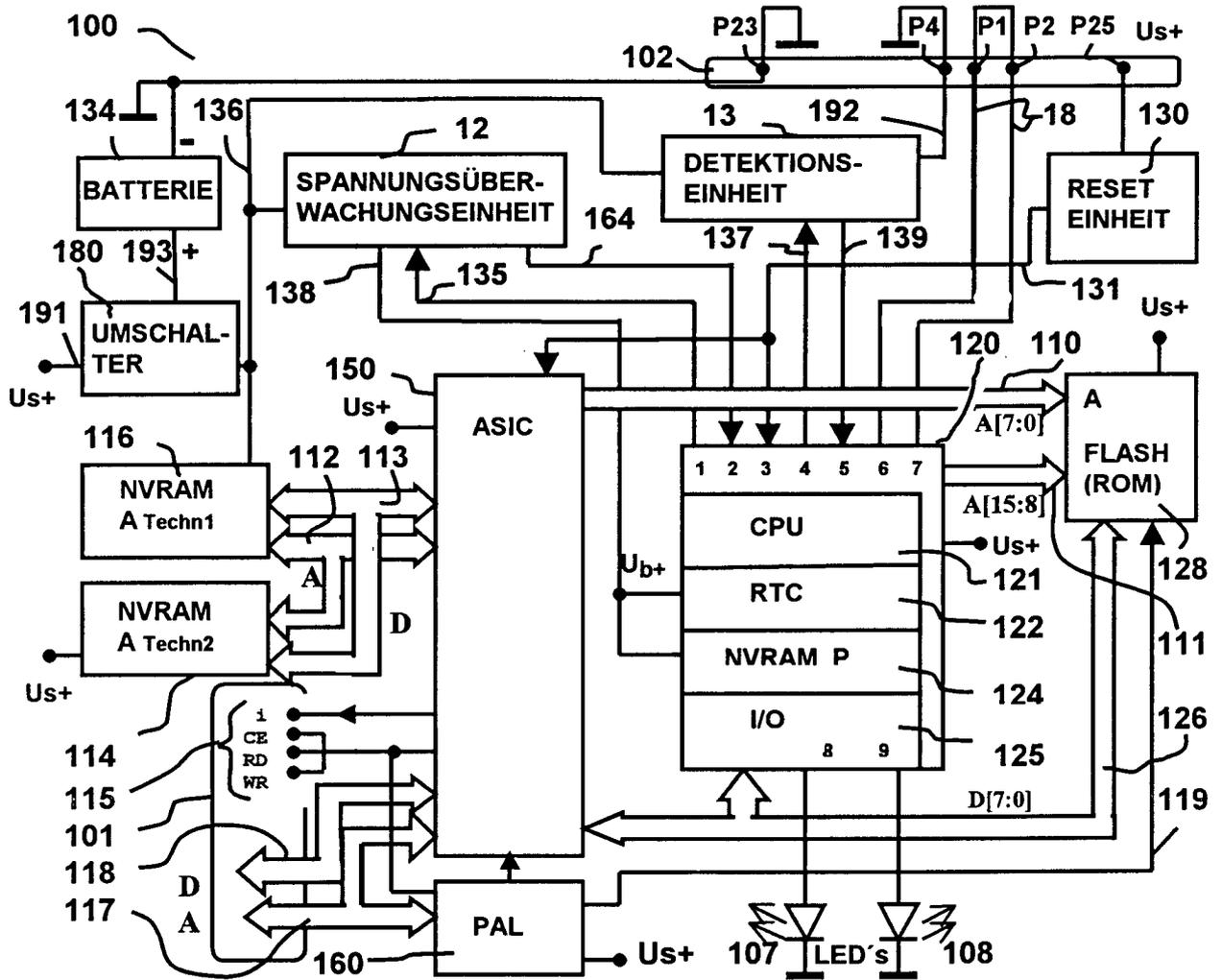


Fig. 2

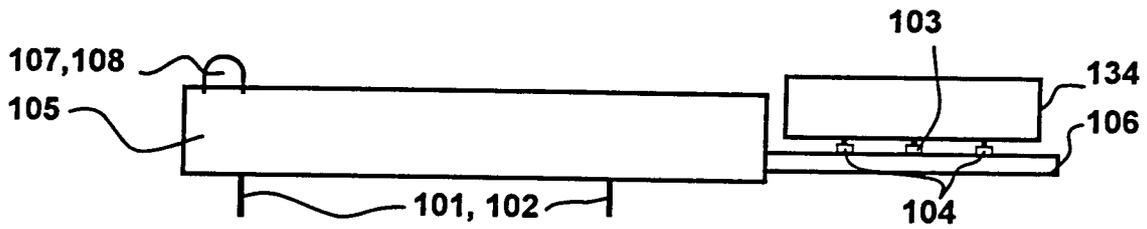


Fig. 3

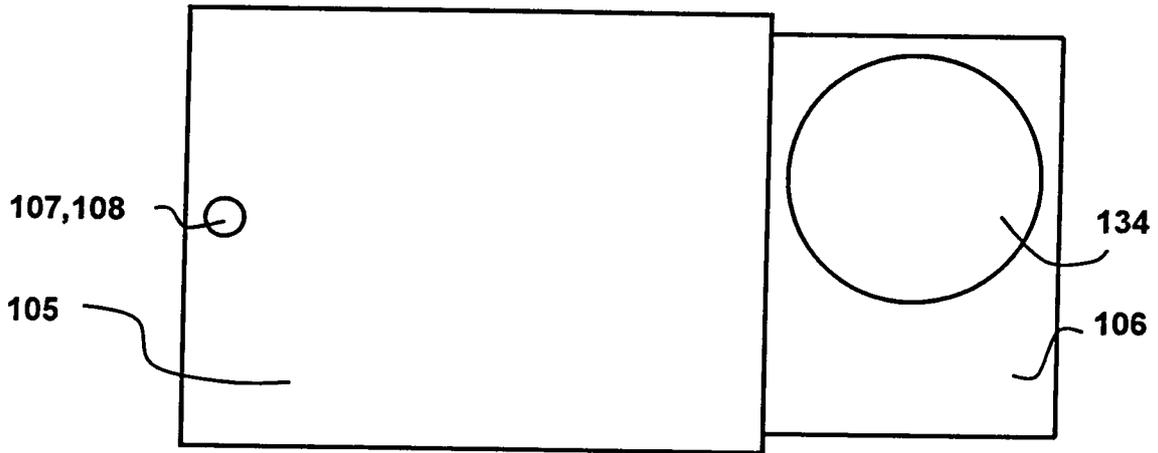


Fig. 4

Zustand Nr.	LEDs	leuchtet	blinkt	aus	Anzeige	Bedeutung
220	R			X	Grün - leuchtend	OK
	G	X				
230	R	X			Rot - leuchtend	Fehler
	G			X		
240	R	X			Orange - leuchtend	Dyn. Fehler
	G	X				
250	R		X		Rot - blinkend	lange Zeit kein Kontakt zur DZ
	G			X		
260	R			X	Grün - blinkend	Schlüssel ist nicht installiert
	G		X			
270	R		X		Orange - blinkend	
	G		X			
280	R	X			Rot leuchtend	
	G		X		Orange blinkend	
290	R		X		Grün leuchtend	
	G	X			Orange blinkend	

Fig. 5

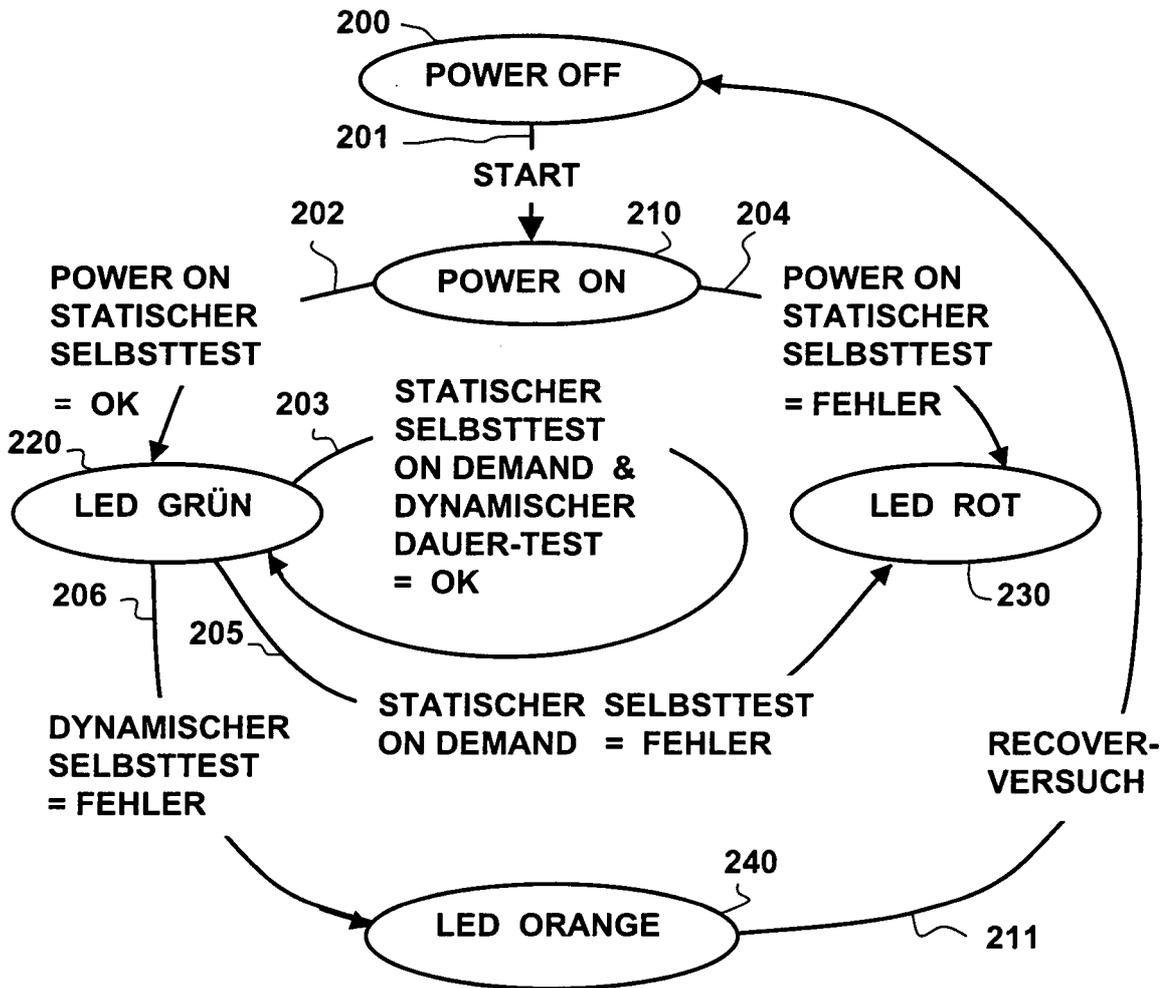


Fig. 6

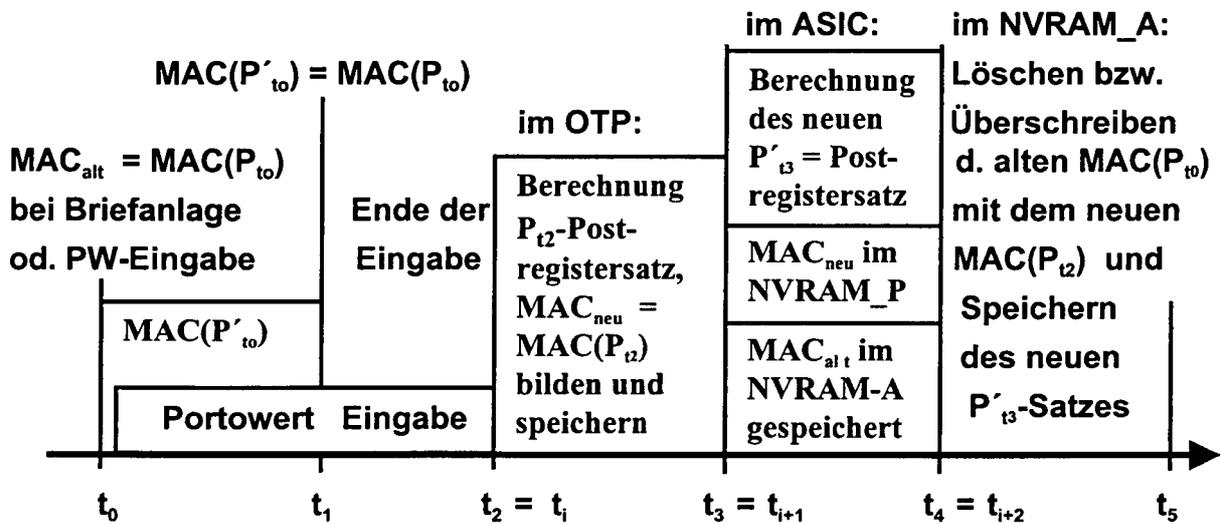


Fig. 7 *

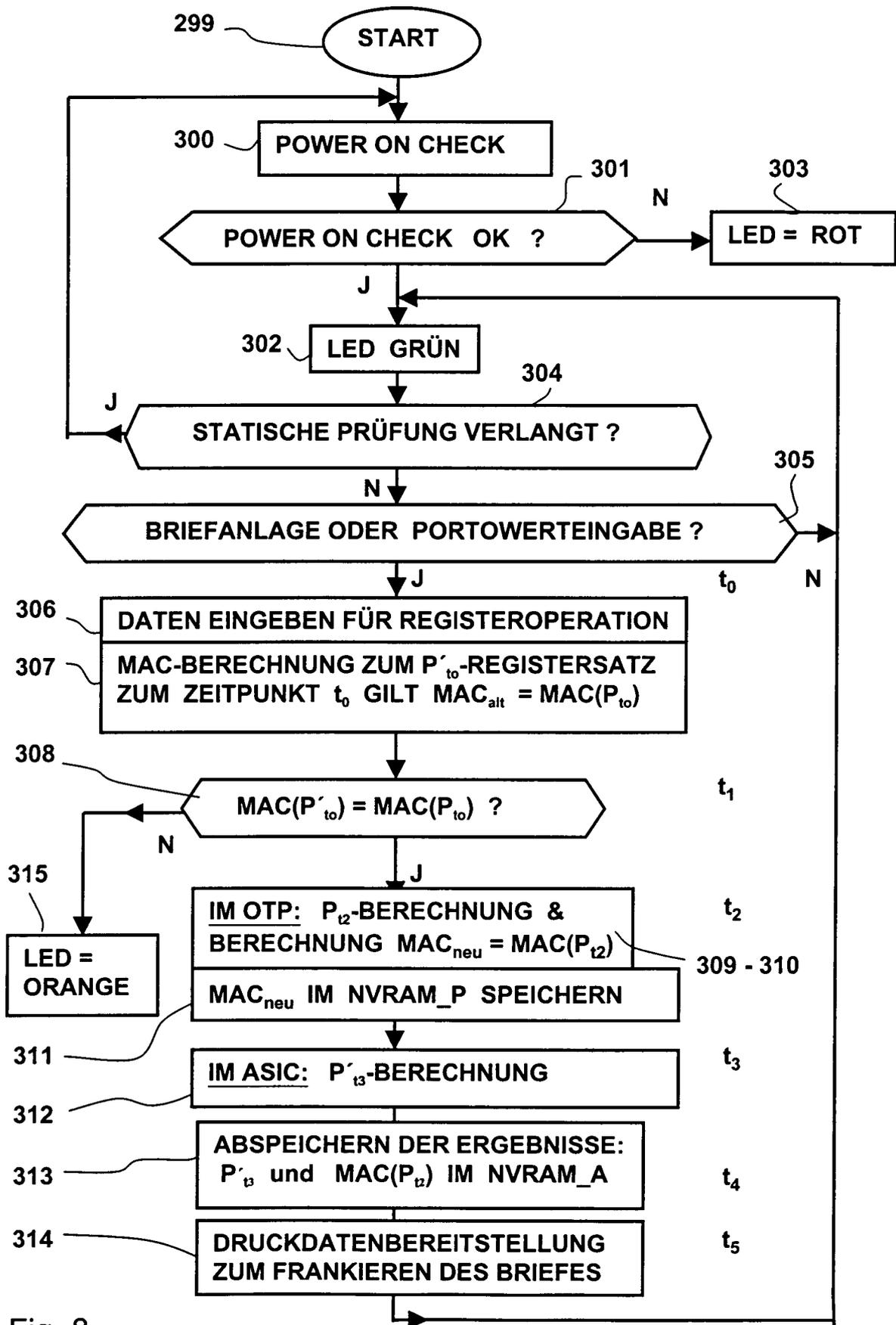


Fig. 8