(19) Deutsches Patent- und Markenamt

(10) **DE 10 2005 056 940 B4** 2016.06.30

(12) # Patentschrift

(21) Aktenzeichen: **10 2005 056 940.4**
(22) Anmeldetag: **29.11.2005**
(43) Offenlegungstag: **06.06.2007**
(45) Veröffentlichungstag der Patenterteilung: **30.06.2016**

(51) Int Cl.: ***G06K 19/073*** (2006.01)
G06F 12/16 (2006.01)

Innerhalb von neun 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. 1 Patentkostengesetz).

(73) Patentinhaber:
Infineon Technologies AG, 81669 München, DE

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler, Zinkler, Schenk & Partner mbB Patentanwälte, 81373 München, DE

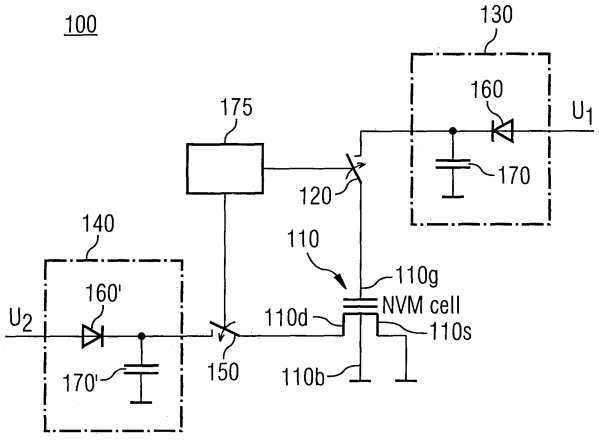
(72) Erfinder:
Otterstedt, Jan, Dr.-Ing., 82008 Unterhaching, DE; Peters, Christian, Dr., 85591 Vaterstetten, DE; Rabe, Dirk, Dr.-Ing., 81825 München, DE; Sedlak, Holger, Dipl.-Inform., 82054 Sauerlach, DE

(56) Ermittelter Stand der Technik:

DE	**103 27 285**	**A1**
DE	**196 10 070**	**A1**
DE	**199 42 437**	**A1**
DE	**199 47 574**	**A1**
AT	**4 08 925**	**B**

(54) Bezeichnung: **Vorrichtung und Verfahren zum nicht-flüchtigen Speichern eines Statuswertes**

(57) Zusammenfassung: Es wird eine Vorrichtung (100) zum nicht-flüchtigen Speichern eines Statuswerts, das anzeigt, dass eine Bedingung vorgelegen hat, beschrieben, die eine nicht-flüchtige Speichereinrichtung (110), eine Energiespeichereinrichtung (130, 140) zum Speichern von Energie bei Anliegen einer Versorgungsspannung und eine Schalteinrichtung (120, 150) umfasst, die ausgelegt ist, um die Energiespeichereinrichtung (130, 140) mit der nicht-flüchtigen Speichereinrichtung (110) zu koppeln, um den Statuswert in dieselbe zu schreiben, wenn die Bedingung vorliegt.



Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf eine Vorrichtung, ein System und ein Verfahren zum nicht-flüchtigen Speichern eines Statuswertes, insbesondere im Bereich sicherheitsrelevanter Systeme, wie z. B. Chipkarten oder auch Smartcards.

[0002] Integrierte Sicherheitsschaltungen, wie sie beispielsweise in Chipkarten oder Smartcards verwendet werden, zielen gerade im Bereich sicherheitsrelevanter Anwendungen, beispielsweise im Bereich der Zugangssicherung zu nicht-öffentlichen Bereichen, zu Computersystemen oder geheimen Informationen, darauf ab, in betrügerischer Absicht durchgeführte Angriffe abzuwehren. Ziel solcher Angriffe ist häufig das Erlangen von Informationen, die in den integrierten Sicherheitsschaltungen der Chipkarten abgespeichert sind, um in unberechtigter Art und Weise besondere Privilegien zu erlangen.

[0003] Mehrere Patentschriften und Patentanmeldungen beschreiben Vorrichtungen und Verfahren zum Zählen von Vorfällen und führen Zeitverzögerungen beispielsweise für die Eingabe einer PIN (persönliche Identifikationsnummer) ein. Die französische Patentschrift FR 2493564 B1 bzw. die deutsche Patentschrift DE 3041109 C2 bzw. die US-Patentschrift US 4484067 A beschreiben ein Identifikationselement in der Form einer integrierten Schaltung, beispielsweise für Identifikationskarten und ähnliche Datentransportmedien. Das Identifikationselement weist hierbei einen geheimen Code auf, der nur dem rechtmäßigen Besitzer der Karte bekannt ist und der im Inneren der integrierten Schaltung mit einem eingegebenen Code verglichen wird. Um eine unautorisierte Benutzung der Karte zu verhindern, weist das Element eine unabhängige Schaltung auf, die von dem Rest der Schaltung isoliert ist, und dazu dient, eine unkorrekte Codeeingabe zu detektieren und die Karte für eine vorbestimmte Zeitspanne funktionsunfähig zu machen. Die Abschaltungsdauer kann als Funktion der möglichen Codepermutationen so gewählt werden, dass es für einen Angreifer praktisch unmöglich wird, den korrekten Code innerhalb der normalen Dauer der Gültigkeit der Karte herauszufinden. Die Schaltung kann auch verwendet werden, um die Funktionstüchtigkeit der Karte für eine vorbestimmte Zeitdauer zu erhalten, wenn der korrekte Code eingegeben wurde, ohne dass weitere Eingaben notwendig sind. Hierdurch ist der rechtmäßige Besitzer in der Lage, den Code ungestört von anderen Personen vor dem eigentlichen Benutzen der Karte einzugeben.

[0004] Die französische Patentschrift FR 2311360 B1 bzw. die deutsche Patentschrift DE 2621271 C2 bzw. die US-Patentschrift US 4092524 A beschreiben ein tragbares unabhängiges elektronisches Objekt, das ausgelegt ist, um vertrauliche Informationen, die an eine Datentransfereinrichtung übergeben werden sollen, zu speichern und zu transferieren. Das tragbare Objekt weist in einer leicht transportablen Form wenigstens ein Speichermodul zum Abspeichern von Daten auf, das Aktivierungsdaten enthält, eine von außerhalb des tragbaren Objekts zugreifbare Kopplungseinrichtung, die das tragbare Objekt in die Lage versetzt, vorübergehend mit der erwähnten Transfereinheit gekoppelt zu werden, und Schaltungen für die Steuerung des Speichers, die zwischen die Kopplungseinrichtung und den Speicher geschaltet sind. Der Speicher und die Steuerschaltungen sind in der Form logischer Mikrostrukturen hergestellt. Das tragbare Objekt weist darüber hinaus einen Identifikationskomparator auf, der mit dem Speicher und der Kopplungseinrichtung verbunden ist und dem Vergleich der Aktivierungsdaten, die in dem Speicher abgelegt sind, mit einem vertraulichen Code, der von dem rechtmäßigen Besitzer des transportablen Objekts zur Verfügung gestellt und in das transportable Objekt über die erwähnte Transfereinheit eingebracht wird, dient. Das transportable Objekt ist dadurch gekennzeichnet, dass es zusätzlich eine Schaltung zum Speichern von Fehlern in dem vertraulichen Code, die dem Identifikationskomparator zugeordnet ist, aufweist und dazu dient, dauerhaft Fehler in dem vertraulichen Code zu verfolgen. Die Speicherschaltung weist hierbei wenigstens ein Speicherelement mit einem permanenten Speicher auf.

[0005] Das US-Patent US 5594227 A beschreibt ein Smartcardschutzsystem zum Schutz gegen unautorisierten Zugriff auf den Dateninhalt einer Smartcard durch menschliche oder elektronischmaschinelle Manipulation. Das Smartcardschutzsystem schließt eine Smartcard mit einem auf ihr abgespeicherten autorisierten Passwort für zugeordnete Daten und einen Smartcardanschluss ein, um ein eingegebenes Passwort zum Zugreifen auf die auf der Smartcard abgespeicherten Daten zu übergeben. Die Smartcard schließt darüber hinaus einen Komparator zum Vergleichen des eingegebenen Passworts und des abgespeicherten Passworts und zwei Zähler, einen Fehlerzähler und einen Verzögerungszähler, ein. Der Fehlerzähler speichert einen Fehlerzählerwert, der die Zahl der Fälle anzeigt, in denen das eingegebene Passwort und das abgespeicherte Passwort nicht übereinstimmen. Der Fehlerzähler wird inkrementiert, wenn das eingegebene Passwort nicht mit dem abgespeicherten Passwort übereinstimmt, und dekrementiert, wenn das eingegebene Passwort erfolgreich mit dem abgespeicherten Passwort übereinstimmt. Der Verzögerungszähler speichert einen Verzögerungszählwert, der jedes Mal inkrementiert wird, wenn der Komparator unabhängig von einer Übereinstimmung das eingegebene Passwort und das abgespeicherte Passwort vergleicht. In dem Fall, dass der Fehlerzählerwert nicht mit dem ursprünglichen Wert Null übereinstimmt, verweigert die Smartcard den Zugriff auf den Dateninhalt. Der Zugriff auf die Daten wird auch dann verweigert, wenn nach anfänglichen Nichtüber-

einstimmungen eine Übereinstimmung eintritt, da in diesem Fall der Fehlerzähler nicht Null ist. Darüber hinaus wird dem System eine Verzögerungsperiode auferlegt, wenn der Zugriff verweigert wird, bevor das nächste von dem Smartcardanschluss empfangene, eingegebene Passwort verglichen wird. Die Verzögerungszeit wird jedes Mal als Funktion des Verzögerungszählwertes erhöht.

[0006] Die Patentschrift WO 88/10479 A1 beschreibt eine hochzuverlässige IC-Karte (IC = integrated circuit = integrierter Schaltkreis), die keine Daten verlieren kann oder unerwartet unauslesbar wird, sowie eine zuverlässige und effiziente Vorrichtung zur Überwachung der Lebensdauer von IC-Karten, die eine technisch einfache Struktur haben. Die IC-Karte weist eine Speichereinrichtung zum Speichern des Datums der ersten Benutzung ihrer Batterie, eine Speichereinrichtung zum Abspeichern der Zahl der Benutzungen der betroffenen IC-Karte, eine Speichereinrichtung zum Abspeichern der Lebenszeit einer Energiequelle für die besagten Speichermedien oder die besagte IC-Karte, je nachdem, welche der beiden kürzer ist, und eine Speichereinrichtung zum Abspeichern der Zahl der erlaubten Benutzungen der speziellen IC-Karte. In der Vorrichtung zur Überwachung der Lebensdauer der IC-Karte wird der Inhalt des Speichers für die Zahl der Benutzungen der IC-Karte jedes Mal, wenn die IC-Karte benutzt wird, aktualisiert und die aktualisierte Zahl der Benutzungen und die Dauer von der ersten Benutzung an mit der Zahl der erlaubten Benutzungen und der Lebenszeit der speziellen IC-Karte verglichen. Jedes Mal, wenn einer der erstgenannten Werte den zugehörigen zweitgenannten Wert übersteigt, gibt die Vorrichtung diese Information preis.

[0007] Die Patentschrift WO 99/56253 A1 bzw. EP 1075681 B1 beschreibt ein Verfahren zur Verhinderung der missbräuchlichen Verwendung der auf einem Chipkarten-Interface vorhandenen Authentifizierungsprozeduren, wobei die Anzahl der ausgeführten Authentifizierungsprozeduren erfasst werden und bei Erreichen eines Grenzwertes weitere Prozeduren angestoßen werden, die als Endziel die Verhinderung der weiteren Verwendung der Chipkarte beinhalten.

[0008] Die Patentschriften EP 1249003 B1 bzw. US 2003005315 A1 der Anmelderin beschreiben eine integrierte Sicherheitsschaltung, beispielsweise einen Mikrocontroller für Smartcards, die eine Funktionseinheit zum Ausführen einer Sicherheitsfunktion aufweist. Ein Kontrollsystem bestimmt die Zahl der Ausführungen der Sicherheitsfunktion pro Zeiteinheit. Eine kontinuierliche Ausführung der Sicherheitsfunktion wird verhindert, wenn ein Schwellenwert überschritten wird. Um dies zu erreichen, wird eine analoge Zeitmesseinrichtung mit einem Ladungsspeicher vorzugsweise verwendet, der die vergangene Zeit auch dann misst, wenn das Versorgungspotential nicht angeschlossen ist. Ein Benutzungszähler wird aktualisiert, wenn die Sicherheitsfunktion aufgerufen wird. Die Sicherheitsschaltung bietet so einen höheren Schutz gegen statistische Angriffe. Die Komplexität bezogen auf die Implementierung ist rechtfertigbar gering. Die Sicherheitsschaltung ist kompatibel mit existierenden Systemen.

[0009] Die DE 19947574 A1 bezieht sich auf ein Verfahren zur Sicherung eines Datenspeichers beziehungsweise eines Sicherheitsdatenspeichers, bei dem eine äußere Einwirkung auf ein Bauteil, welches den Sicherheitsdatenspeicher enthält, von Sensoren detektiert wird. Durch Überschreiten eines Schwellenwerts an einem der Sensoren wird ein Angriff signalisiert, aufgrund dessen der Inhalt des Sicherheitsdatenspeichers zumindest teilweise gelöscht wird. Der Zustand der Sensoren wird permanent überwacht und die Zustandsdaten der Sensoren werden aufgezeichnet.

[0010] Die AT 408925 B bezieht sich auf eine Anordnung zum Schutz von elektronischen Recheneinheiten, insbesondere von Chipkarten, gegen unverwünschten Zugriff, wobei die einem Angriff ausgesetzte Fläche der Einheit zumindest teilweise mit einer Ummantelung abgedeckt wird. Hierbei werden von der Einheit Messwert an zumindest einer festgelegten Messstelle an und/oder in der Ummantelung ermittelt, nachdem an zumindest einer festgelegten Signalaufgabestelle an und/oder in der beziehungsweise die Ummantelung von der Einheit definierte Signalen eingeleitet wurden. Ferner kann mit den Messwerten und ggf. den Signalwerten eine für eine unversehrte Ummantelung charakteristische Signatur gebildet werden. Dazu umfasst die Einheit zumindest eine Aufgabeeinrichtung und eine Empfangseinrichtung zur Ermittlung zumindest einer Messgröße. Zumindest ein Teil der der Einheit bei ihrer Initialisierung aufgegeben Daten und/oder Programme wird unter Einbindung der bei der Initialisierung ermittelten Signatur verschlüsselt.

[0011] Die DE 19610070 A1 bezieht sich auf eine Chipkarte mit einem Kartenkörper und innerhalb des Kartenkörpers untergebrachten Halbleiterchip, auf welchem eine Steuerschaltung und eine mit der Steuerschaltung elektrisch gekoppelte Halbleiterspeichereinrichtung integriert ausgebildet ist, welche Steuerschaltung mit einer Spannungsversorgungsschaltung erzeugten Versorgungsspannung und einem von einer separat von der Steuerschaltung angeordneten Taktversorgungsschaltung erzeugten Takt versorgt ist. Der Steuerschaltung des innerhalb des Kartenkörpers untergebrachten Halbleiterchips ist eine Sensorschaltung zugeordnet, welche eine Abweichung des erlaubten Betriebszustandes der Steuerschaltung erfasst und bei Vorliegen eines unerlaubten Betriebszustands der Steuerschaltung ein Auslösesignal erzeugt, welches einer der Sensorschaltung

nachgeschalteten und der Halbleiterspeichereinrichtung zugeordneten Auslöseschaltung zugeführt, die als Reaktion auf das Auslösesignal eine wenigstens bereichsweise Löschung des Dateninhalts von Speicherzellen der Halbleiterspeichereinrichtung steuert.

[0012] Die DE 19942437 A1 bezieht sich auf eine selbstlöschende Speicherzelle beziehungsweise eine Vorrichtung zum sicheren Löschen einer flüchtigen Speicherzelle. Eine RAM-Zelle besteht im Wesentlichen aus zwei n- oder p-Kanal-Transistoren, wobei der Gate-Anschluss eines Transistors an dem Ausgang des zweiten Transistors und der Gateanschluss des zweiten Transistors an den Ausgang des ersten Transistors rückgekoppelt ist. Die Source-Anschlüsse der Transistoren sind mit Masse verbunden. Die Drain-Anschlüsse sind über Widerstände mit der Versorgungsspannung verbunden. Hierbei ist mindestens ein Schaltelement vorgesehen, welches bei Trennen der RAM-Zelle von der Versorgungsspannung in den leitenden Zustand geschaltet wird und die Ausgänge der Transistoren der RAM-Zelle kurz schließt. Durch die leitende Verbindung der komplementären Transistorausgänge, welche vorzugsweise auf Masse gelegt sind, wird ein Potentialausgleich erzeugt, so dass alle noch verbleibenden Ladungsträger abschließen können und der vorherige Speicherinhalt nicht mehr ermittelbar ist.

[0013] Die DE 10327285 A1 bezieht sich auf eine Schaltungsanordnung mit einem Spannungsregler zur Erzeugung einer geregelten Betriebsspannung und einer Spannungsüberwachungseinheit, die die geregelte Betriebsspannung auf Abweichungen gegenüber Sollwerten überwacht, wobei erste Erkennungsmittel der Sensorüberwachungseinheit ein Alarmsignal erzeugen, wenn die Betriebsspannung außerhalb eines ersten Spannungsintervalls liegt. Darüber hinaus enthält die Spannungsüberwachungseinheit ein zweites Erkennungsmittel zur Erkennung, ob die geregelte Betriebsspannung außerhalb eines zweiten Spannungsintervalls liegt, das innerhalb eines ersten Spannungsintervalls liegt. Ferner sind Mittel zur Einleitung von spannungsbeeinflussenden Gegenmaßnahmen vorgesehen, wenn die Betriebsspannung außerhalb des zweien Spannungsintervalls liegt.

[0014] Ausgehend von diesem Stand der Technik besteht die Aufgabe der vorliegenden Erfindung darin, eine Vorrichtung, ein System ein Verfahren sowie ein Software-Programmprodukt zu schaffen, die eine erhöhte Sicherheit gegen Angriffe ermöglichen.

[0015] Diese Aufgabe wird durch eine Vorrichtung gemäß Anspruch 1, ein System gemäß Anspruch 12, ein Verfahren gemäß Anspruch 14 oder ein Software-Programm-Produkt gemäß Anspruch 18 gelöst.

[0016] Die vorliegende Erfindung schafft eine Vorrichtung zum nicht-flüchtigen Speichern eines Statuswertes, der anzeigt, dass eine Alarmbedingung vorgelegen hat, und die weist eine nicht-flüchtige Speichereinrichtung, eine Energiespeichereinrichtung zum Speichern von Energie bei Anliegen einer Versorgungsspannung und eine Schalteinrichtung aufweist, die ausgelegt ist, um die Energiespeichereinrichtung mit der nicht-flüchtigen Speichereinrichtung zu koppeln, um den Statuswert in dieselbe zu schreiben, wenn die Bedingung vorliegt.

[0017] Die vorliegende Erfindung schafft ein Verfahren zum nicht-flüchtigen Speichern eines Statuswerts, der anzeigt, dass eine Bedingung vorgelegen hat, und einen Schritt des Speicherns von Energie in einer Energiespeichereinrichtung, wenn eine Versorgungsspannung anliegt und einen Schritt des Koppelns der Energiespeichereinrichtung mit einer nicht-flüchtigen Speichereinrichtung zum Schreiben des Statuswerts in die nicht-flüchtige Speichereinrichtung umfasst, wenn die Bedingung auftritt.

[0018] Der vorliegenden Erfindung liegt die Erkenntnis zu Grunde, dass eine erhöhte Sicherheit gegen Angriffe erreicht werden kann, wenn bei Auftreten einer Bedingung, bei der es sich bei bevorzugten Ausführungsbeispielen der Erfindung um eine Unterbrechung von einer Versorgungsspannung handelt, ein Statuswert nicht-flüchtig abgelegt wird. Bei bevorzugten Ausführungsbeispiele der Erfindung kann dies dadurch erreicht werden, dass eine beschränkte Menge Energie in einem Energiespeicher gespeichert wird, die für eine bestimmte Zeitspanne beispielsweise nach einer unerwarteten Unterbrechung von der Versorgungsspannung verfügbar bleibt, um den Zustand einer nicht-flüchtigen Speicherzelle (NVM = non-volatile memory = nicht-flüchtiger Speicher) zu ändern. Durch ein Vorhalten einer begrenzten oder unbegrenzten Energie bzw. Restenergie kann so eine flüchtige Information in einer nicht-flüchtigen Art und Weise gespeichert werden, so dass diese nach einem späteren Neustart zur Verfügung steht. Besonders vorteilhaft hieran ist, dass Informationen selbst dann nicht-flüchtig gespeichert werden können, wenn die Energiezufuhr simultan bzw. zeitnah zu dem Schreibprozess unterbrochen wird.

[0019] In einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung ist die Schalteinrichtung zur automatischen Kopplung der Energiespeichereinrichtung an die nicht-flüchtige Speichereinrichtung durch einen Schalter implementiert, der mit einem Steuereingang an eine von der Versorgungsspannung abgeleiteten Spannung gekoppelt ist. Hierbei wird im Rahmen der vorliegenden Anmeldung unter einer von der Versorgungsspannung abgeleiteten Spannung eine elektrische Spannung verstanden, die mit einem Unterbrechen der Versorgungsspan-

nung ebenfalls nicht mehr zur Verfügung steht. Hierbei kann die abgeleitete Spannung bezogen auf die Versorgungsspannung auch ein betragsmäßig größeren oder kleineren Wert oder auch ein zur Versorgungsspannung umgekehrtes Vorzeichen aufweisen.

[0020] In einem weiteren bevorzugten Ausführungsbeispiel der vorliegenden Erfindung ist die Schalteinrichtung mit einem Steuereingang mit einer Einrichtung zum Erzeugen eines Steuersignals gekoppelt, die es ermöglicht, die Kopplung der Energiespeichereinrichtung mit der nicht-flüchtigen Speichereinrichtung beispielsweise im Fall eines erwartungsgemäßen Ausschaltens zu unterbinden.

[0021] Ein Vorteil der erfindungsgemäßen Vorrichtung zum nicht-flüchtigen Speichern eines Statuswerts besteht darin, dass neue Anwendungsmöglichkeiten eröffnet werden. So kann beispielsweise eine Sicherheits-Validierung, die auch im Englischen als „Security Certification" bezeichnet wird, dadurch vereinfacht werden, dass als Statuswert eine Alarminformation abgespeichert wird. Der Statuswert bzw. in diesem Fall die Alarminformation kann beispielsweise dazu verwendet werden, einen anschließenden Neustart des Systems zu verzögern oder auch mit Hilfe eines Zählers und einer entsprechenden Auswertung der Alarminformation eine Prozessoreinrichtung, mit der die erfindungsgemäße Vorrichtung zum nicht-flüchtigen Speichern gekoppelt ist, nach einer vorbestimmten Zahl von Alarmzuständen zu blockieren bzw. zu sperren oder gebrauchsunfähig zu machen.

[0022] Somit kann als weiterer Vorteil die Zahl der möglichen Angriffsversuche in einer vorbestimmten Zeitspanne beschränkt werden, die beispielsweise bezogen auf eine benötigte Zeitspanne sehr hoch sein kann. Als zusätzlicher Vorteil ist es so durch die vorliegende Erfindung möglich, die Zahl der Angriffe auf ein bestimmtes Bauelement zu limitieren.

[0023] Eine häufig durchgeführte Angriffsvariante auf Mikrocontroller von Chipkarten besteht darin, die betreffende Chipkarte sehr häufig zu aktivieren und jedes Mal festzustellen, ob der Mikrocontroller den Zugriff zu der Chipkarte als berechtigt akzeptiert oder als unberechtigt abgelehnt hat. Diese Angriffe gehen darüber hinaus häufig mit einer gezielten Unterbrechung der Versorgungsspannung bzw. der Energieversorgung der Chipkarte einher. Hierdurch gehen flüchtig gespeicherte Informationen durch das Abschalten der Energieversorgung verloren, so dass eine angemessene Informationsverarbeitung im Rahmen eines nächsten Systemstarts der Prozessoreinrichtung, die mit der erfindungsgemäßen Vorrichtung gekoppelt ist und bei der es sich beispielsweise um eine CPU (CPU = central processing unit = Zentralprozessor), einen Chip, einen Kryptoprozessor, einen Prozessor oder eine andere integrierte Schaltung handeln kann, mehr möglich ist.

[0024] Ein weiterer Vorteil der erfindungsgemäßen Vorrichtung zum nicht-flüchtigen Speichern besteht darin, dass nur eine Programmieroperation bzw. ein Speichervorgang im „energielosen Zustand", also unmittelbar nach der Unterbrechung der externen Energieversorgung, durchgeführt werden können muss, was einerseits die Menge an zwischengespeicherter Energie und andererseits den schaltungstechnischen Aufwand gering hält. Da der Schreibvorgang häufig durch das Auftreten eines auslösenden Ereignisses initiiert wird, wird ein solcher Schreibvorgang auch als „Powerless Event Storage", also als energielose Ereignisspeicherung bezeichnet. Im normalen Betriebsmodus, wenn also eine externe Versorgungsspannung wieder zur Verfügung steht, so dass eine Energiespeicherung in diesem Fall nicht notwendig ist, kann über eine Ausleseoperation bzw. über eine Löschoperation der Ereignisspeicher ausgelesen bzw. gelöscht werden.

[0025] Beispielsweise ist für die Problematik der oben beschriebenen Angriffsvariante, die mit einer Unterbrechung der Versorgungsspannung einhergeht, keine Lösung bekannt. Die vorliegende Erfindung schafft so erstmals eine Lösung für bei bisherigen Systemen bestehenden Nachteilen.

[0026] Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend unter Bezugnahme auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

[0027] Fig. 1 ein Teilschaltbild eines ersten Ausführungsbeispiels einer erfindungsgemäßen Vorrichtung zum nicht-flüchtigen Speichern eines Statuswerts;

[0028] Fig. 2 ein Teilschaltbild eines zweiten Ausführungsbeispiels einer erfindungsgemäßen Vorrichtung zum nicht-flüchtigen Speichern eines Statuswerts;

[0029] Fig. 3 ein schematisches Teilschaltbild eines Ausführungsbeispiels einer Schaltung zum Auslesen einer erfindungsgemäßen Vorrichtung zum nicht-flüchtigen Speichern eines Statuswerts; und

[0030] Fig. 4 ein schematisches Teilschaltbild eines Ausführungsbeispiels einer Schaltung zum Löschen einer erfindungsgemäßen Vorrichtung zum nicht-flüchtigen Speichern eines Statuswerts.

[0031] Bezug nehmend auf die **Fig.** 1–**Fig.** 4 wird nun ein erstes Ausführungsbeispiel einer Vorrichtung zum nicht-flüchtigen Speichern eines Statuswerts beschrieben.

[0032] Fig. 1 zeigt ein Teilschaltbild eines ersten Ausführungsbeispiels einer erfindungsgemäßen Vor-

richtung **100** zum nicht-flüchtigen Speichern eines Statuswerts. Die Vorrichtung **100** weist als nicht-flüchtige Speichereinrichtung eine Standard-Floating-Gate-NVM-Zelle **110** (NVM = non-volatile memory = nicht-flüchtiger Speicher) auf, die in **Fig.** 1 auch als NVM Cell bezeichnet ist und beispielsweise bei EEPROM-Speichern (EEPROM = electrically erasable read-only memory = elektrisch löschbarer Nur-Lese-Speicher) zum Einsatz kommt. Aus diesem Grund wird die NVM-Zelle **110** auch als EEPROM-Zelle bezeichnet. Die NVM-Zelle **110** weist einen Sourceanschluss **110s** und einen Substratanschluss bzw. Bulkanschluss **110b**, die mit einem Bezugspotential (z. B. Masse) verbunden sind, auf. Ein Gateanschluss **110g**, der genauer gesagt mit dem Steuergate der NVM-Zelle **110** verbunden ist, ist mit einem ersten Anschluss einer ersten Schalteinrichtung **120** gekoppelt. Ein zweiter Anschluss der ersten Schalteinrichtung **120** ist mit einem Ausgang einer ersten Energiespeichereinrichtung **130** verbunden. Ein Eingang der ersten Energiespeichereinrichtung **130** ist mit einer Spannung U_1 gekoppelt, die bei dem in **Fig.** 1 gezeigten Ausführungsbeispiel der Energiespeichereinrichtung **130** einen Spannungswert von 10 V zur Verfügung stellt. Die Spannung U_1 liegt immer dann an, wenn eine Versorgungsspannung anliegt. Unter Versorgungsspannung ist dabei im Sinne der Erfindung die Versorgungsspannung einer Prozessoreinrichtung, beispielsweise eines Chips, einer CPU oder eines anderen integrierten Schaltkreises, mit dem die erfindungsgemäße Vorrichtung gekoppelt ist, zu verstehen. Die erfindungsgemäße Vorrichtung kann dabei als Teil der elektrischen bzw. elektronischen Vorrichtung ausgebildet sein.

[0033] Die Vorrichtung **100** zum nicht-flüchtigen Speichern eines Statuswerts weist neben der ersten Energiespeichereinrichtung **130** auch eine zweite Energiespeichereinrichtung **140** auf, die einen Eingang aufweist, der mit einer Spannung U_2, die einen Wert von 4 V aufweist, gekoppelt ist. Die Spannung U_2 liegt immer dann an, wenn die Versorgungsspannung anliegt. Die beiden aus der Versorgungsspannung abgeleiteten Spannungen U_1 und U_2 können sich hierbei sowohl in bezug auf die betragsmäßigen Spannungswerte, wie auch in bezug auf ihr Vorzeichen von der Versorgungsspannung unterscheiden. So kann eine solche abgeleitete Spannung betragsmäßig größer oder kleiner als die Versorgungsspannung sein und bezogen auf ihr Vorzeichen auch ein umgekehrtes Vorzeichen aufweisen. Betragsmäßig kleinere Spannungswerte können so beispielsweise mit Hilfe eines Spannungsteilers, betragsmäßig höhere Spannungswerte beispielsweise mit Hilfe von Ladungspumpen erzeugt werden. Die beiden abgeleiteten Spannungen U_1 und U_2 liegen hierbei nicht an, wenn die Versorgungsspannung nicht anliegt. In diesem Zusammenhang sollte erwähnt werden, dass die hier genannten Spannungswerte nur exemplarisch zu verstehen sind und keine Einschränkung in Bezug auf die vorliegende Erfindung darstellen, was ebenfalls für die in dem weiteren Verlauf der vorliegenden Anmeldung exemplarischen Spannungswerte gilt.

[0034] Ein Ausgang der zweiten Energiespeichereinrichtung **140** ist mit einem ersten Anschluss einer zweiten Schalteinrichtung **150** gekoppelt. Die zweite Schalteinrichtung **150** ist mit einem zweiten Anschluss an einen Drainanschluss **110d** der NVM-Zelle **110** angeschlossen. Die beiden Energiespeichereinrichtungen **130**, **140** weisen jeweils eine Diode **160** und **160'** auf, die jeweils mit einem Anodenanschluss an den Eingang der beiden Energiespeichereinrichtungen **130**, **140** gekoppelt sind. Die beiden Dioden **160**, **160'** sind jeweils mit einem Kathodenanschluss an den Ausgang der beiden Energiespeichereinrichtungen **130**, **140** gekoppelt. Darüber hinaus weisen die beiden Energiespeichereinrichtungen **130**, **140** jeweils eine Kapazität **170**, **170'** auf, die jeweils mit einem Anschluss an den Ausgang der Energiespeichereinrichtungen **130**, **140** und die Kathodenanschlüsse der Dioden **160**, **160'** und mit einem zweiten Anschluss an das Bezugspotential gekoppelt sind.

[0035] Der erste und der zweite Schalter **120**, **150** weisen jeweils einen Steuereingang auf, die an eine Steuereinrichtung **175** gekoppelt sind. Die Steuereinrichtung **175** stellt den beiden Schaltern **120**, **150** jeweils ein Steuersignal zur Verfügung, so dass die beiden Schalter **120**, **150** auf das Steuersignal hin geschlossen werden.

[0036] Im normalen Betriebszustand trennen die beiden Schalteinrichtungen **120**, **150** die beiden Energiespeicher **130**, **140** von der NVM-Zelle **110**. In diesem Fall, wenn also die beiden aus der Versorgungsspannung abgeleiteten Spannungen U_1 und U_2 an den Eingängen der beiden Energiespeichereinrichtungen **130** bzw. **140** anliegen, werden die beiden Kapazitäten **170**, **170'** über die beiden Dioden **160**, **160'**, die beide in Durchlassrichtung betrieben werden, geladen. Das Laden der beiden Kondensatoren **170**, **170'** geschieht hierbei mit einer charakteristischen Zeitkonstante, bei der es sich um eine RC-Zeitkonsante handelt, die sich einerseits aus dem Wert der Kapazität der beiden Kapazitäten **170**, **170'** und dem elektrischen Widerstand der beiden in Durchlassrichtung betriebenen Dioden **160**, **160'** ergibt. Da der elektrische Widerstand einer in Durchlassrichtung betriebenen Diode im Allgemeinen sehr gering ist, weisen die beiden Kondensatoren **170**, **170'** sehr schnell eine Ladung auf, die unter Berücksichtigung ihrer jeweiligen Kapazitätswerte der anliegenden Versorgungsspannung im Wesentlichen entsprechen. Auf Grund der sich ergebenden kurzen RC-Zeitkonstanten der beiden Energiespeichereinrichtungen **130**, **140** kann die erfindungsgemäße Vorrichtung **100** bereits nach einer sehr kurzen Zeitspan-

ne, die etwa im Bereich einiger weniger RC-Zeitkonstanten liegt, auf ein Alarmsignal hinden Statuswert nicht-flüchtig speichern. Hierdurch ist die erfindungsgemäße Vorrichtung **100** bereits nach dieser sehr kurzen Zeitspanne einsatzbereit.

[0037] Tritt nun eine Bedingung ein, bei der es sich beispielsweise um eine Alarmbedingung in dem Sinne eines Sicherheitsalarms oder aber einer beliebeigen anderen Alarmbedingung handeln kann, werden die Schalter **120** und **150** geschlossen. Die Bedinung kann hierbei prinzipiell von einer Vielzahl von Ereignissen ausgelöst werden, wie beispielsweise dem Zusammenbrechen der Versorgungsspannung, also einem Sinken der Versorgungsspannung unter einen vorbestimmten Wert. Bei Auftreten der Bedingung kann dabei durch die Steuereinrichtung **175** das Steuersignal erzeugt werden, durch das die Schalter **120**, **150**, die durch Transistoren gebildet sein können, geschlossen werden. Durch das Schließen der beiden Schalter werden die beiden Energiespeichereinrichtungen **130**, **140** so mit der NVM-Zelle **110** verbunden, dass es zu einer Programmierung der NVM-Zelle **110** durch eine sogenannte Channel-Hot-Electron-Programmierung kommt. Um ein erwartungsgemäßen Ausschalten der Prozessoreinrichtung, die mit der erfindungsgemäßen Vorrichtung **100** gekoppelt ist, zu ermöglichen, kann die Steuereinrichtung **175** so ausgelegt sein, dass sie kein Steuersignal bereitstellt, wenn ihr ein Signal, oder auch ein Flag, zur Verfügung gestellt wird, das ein solches erwartungsgemäßen Ausschalten anzeigt. Ein mögliches Beispiel stellt das Beenden eines Programms, das die Prozessoreinrichtung ausgeführt hat, dar. In diesem Fall ist eine Speicherung eines eine Alarmbedingung bzw. Bedingung anzeigenden Statuswerts nicht notwendig, so dass die Schalter **120**, **150** nicht geschlossen werden müssen.

[0038] Die zu der Programmierung der NVM-Zelle **110** notwendige elektrische Energie bzw. Spannung wird hierbei durch die beiden Kapazitäten **170**, **170'** der beiden Energiespeichereinrichtungen **130**, **140** gepuffert bzw. bereitgestellt. Die Energiespeicherung funktioniert auch dann, wenn die äußeren Versorgungsspannungen bereits zusammengebrochen sind, also unter einen vorbestimmten Spannungswert gefallen sind, da die beiden Kapazitäten **170**, **170'** aufgrund der nun in Sperrrichtung betriebenen Dioden **160**, **160'** sich nicht bzw. nur sehr langsam über die an die Eingänge der beiden Energiespeichereinrichtungen **130**, **140** angeschlossenen, nicht in **Fig.** 1 gezeigten Komponenten entladen können. Der Grund hierfür liegt in dem sehr hohen elektrischen Widerstand einer in Sperrrichtung betriebenen Diode, der auch zu einer bezogen auf eine zur Programmierung der NVM-Zelle **110** notwendigen Zeitspanne sehr großen RC-Zeitkonstante führt.

[0039] Die in den beiden Energiespeichereinrichtungen **130**, **140** gespeicherte begrenzte Energie bleibt so aufgrund der beiden Dioden **160**, **160'** für eine bestimmte Zeitspanne nach einem unerwarteten Versorgungsspannungsausfall verfügbar, und kann so zur Änderung des Zustands der NVM-Zelle **110** verwendet werden. Die erfindungsgemäße Vorrichtung **100** zum nicht-flüchtigen Speichern eines Statuswerts ermöglicht es so, selbst nachdem die Versorgungsspannung zu dem elektrischen System insgesamt unterbrochen wurde bzw. diese entfernt wurde, eine Speicherung der Alarminformation unmittelbar nachdem diese auf einem Chip, der die erfindungsgemäße Vorrichtung **100** zum nicht-flüchtigen Speichern eines Statuswerts umfasst, aufgetreten ist. Das in **Fig.** 1 gezeigte Ausführungsbeispiel der erfindungsgemäßen Vorrichtung **100** stellt somit eine exemplarische Implementation einer „energielosen Ereignisspeicherung" (Powerless Event Storage) dar, die beispielsweise auf Chipkarten, Smartcards und anderen integrierten Schaltkreisen mit einer integrierten Sicherheitsfunktionalität (Security-IC; IC = integrated circuit = integrierter Schaltkreis) eingesetzt werden kann. Das den Alarmzustand repräsentierende und in der NVM-Zelle **110** gespeicherte Bit kann nach einem Auslesevorgang, der weiter unten beschrieben wird, beispielsweise als mögliche Anwendung dazu verwendet werden, den folgenden Neustart des Systems zu verzögern oder zusammen mit einer Steuereinheit und einem Zähler dazu verwendet werden, den Chip nach einer vorbestimmten Anzahl von Alarmzuständen zu blockieren oder betriebsunfähig zu machen.

[0040] **Fig.** 2 zeigt ein Teilschaltbild eines zweiten Ausführungsbeispiels einer Vorrichtung **100** zum nicht-flüchtigen Speichern eines Statuswerts. Das in **Fig.** 2 gezeigte Ausführungsbeispiel unterscheidet sich von dem in **Fig.** 1 gezeigten Ausführungsbeispiel einer erfindungsgemäßen Vorrichtung **100** nur dadurch, dass die beiden in **Fig.** 1 gezeigten Schalteinrichtungen **120**, **150** gegen zwei selbstsperrende PMOS-Transistoren **180**, **190** ausgetauscht wurden. Das in **Fig.** 2 gezeigte Ausführungsbeispiel zeigt somit ein Ausführungsbeispiel, bei dem die Schalteinrichtungen als Transistoren realisiert worden sind. Die Verschaltung der beiden Transistoren erfolgt hierbei so, dass jeweils ein Sourceanschluss und ein Substratsanschluss bzw. Bulkanschluss der beiden selbstsperrenden PMOS Transistoren **180**, **190** mit dem Ausgang einer der beiden Energiespeichereinrichtungen **130**, **140** verbunden ist. Der selbstsperrende PMOS-Transistor **180** ist mit einem Drainanschluss an den Gateanschluss **110g** der NVM-Zelle **110**, die in **Fig.** 2 wiederum als NVM Cell bezeichnet ist, verbunden. Der selbstsperrende PMOS-Transistor **190** ist mit einem Drainanschluss mit dem Drainanschluss **110d** der NVM-Zelle **110** verbunden.

[0041] Die beiden selbstsperrenden PMOS-Transistoren **180**, **190** sind darüber hinaus jeweils mit einem Gateanschluss mit dem Eingang der beiden Energiespeichereinrichtungen **130**, **140** gekoppelt, so dass der Gateanschluss des PMOS-Transistors **180** im normalen Betriebsmodus mit einer aus der Versorgungsspannung abgeleiteten Spannung U_1 von beispielsweise 10 V und der Gateanschluss des PMOS-Transistors **190** mit einer von der Versorgungsspannung abgeleiteten Spannung U_2 von beispielsweise 4 V versorgt werden. Die Steuereinrichtung **175** aus **Fig.** 1 ist also bei dem in **Fig.** 2 gezeigten Ausführungsbeispiel als jeweils eine Verbindung der beiden Gateanschlüsse der beiden selbstsperrenden PMOS-Transistoren **180**, **190** mit den beiden abgeleiteten Spannungen U_1 und U_2 implementiert. In dem in **Fig.** 2 gezeigten Ausführungsbeispiel liegen die beiden abgeleiteten Spannungen U_1 und U_2 jeweils genau dann an, wenn auch die Versorgungsspannung anliegt.

[0042] Die Funktionsweise der in **Fig.** 2 gezeigten Vorrichtung **100** zum nicht-flüchtigen Speichern eines Statuswerts unterscheidet sich von der Funktionsweise des in **Fig.** 1 gezeigten Ausführungsbeispiels nur geringfügig. Auch bei dem hier gezeigten Ausführungsbeispiel weisen die beiden elektrischen Kapazitäten **170**, **170'** aufgrund des geringen elektrischen Widerstands der in Durchlassrichtung geschalteten Dioden **160**, **160'** kurze Zeit nach dem Anlegen der beiden aus der Versorgungsspannung abgeleiteten Spannungen U_1 und U_2 Ladungen auf, die unter Berücksichtigung der beiden Kapazitätswerte der beiden Kapazitäten **170**, **170'** im Wesentlichen den beiden aus der Versorgungsspannung abgeleiteten Spannungen U_1 und U_2 entsprechen. Im Normalbetriebszustand sperren somit die beiden selbstsperrenden PMOS-Transistoren **180**, **190** aufgrund der Verschaltung der beiden Gateelektroden mit der jeweiligen Versorgungsspannung so, dass an dem Gateanschluss **110g** und dem Drainanschluss **110d** der NVM-Zelle **110** keine Spannungswerte anliegen, die zu einer Änderung des Zustands der NVM-Zelle **110** führen. Bei diesem Ausführungsbeispiel ist die Bedingung bzw. Alarmbedingung erfüllt, wenn die Versorgungsspannung zusammenbricht bzw. unter einen vorbestimmten Wert fällt.

[0043] In diesem Fall, nachdem die beiden Kapazitäten **170**, **170'** geladen sind, werden die beiden selbstsperrenden PMOS-Transistoren **180**, **190** aufgrund des an dem Gateanschluss anliegenden gesunkenen Potenzials leitend geschaltet, so dass an der NVM-Zelle **110**, eine geeignete Auslegung der beiden PMOS-Transistoren **180**, **190** und der beiden Kapazitäten **170**, **170'** vorausgesetzt, Spannungen anliegen, die zu einer Änderung des Zustands der NVM-Zelle **110** führen.

[0044] Das in **Fig.** 2 gezeigte Ausführungsbeispiel einer erfindungsgemäßen Vorrichtung **100** zum nicht-flüchtigen Speichern eines Statuswerts speichert somit auf ein Zusammenbrechen der äußeren Versorgungsspannung hin ein Alarmsignal bzw. Statussignal, das aufgrund seiner flüchtigen Natur sonst verloren wäre und nicht weiter berücksichtigt werden könnte.

[0045] Um ein erwartungsgemäßes Ausschalten bzw. Abschalten der Versorgungsspannung zu ermöglichen, weisen die in **Fig.** 2 gezeigten Energiespeichereinrichtungen **130**, **140** als optionale Komponenten, die in **Fig.** 2 gestrichelt eingezeichnet sind, jeweils einen standardmäßig geschlossenen Schalter **194**, **194'** auf, die jeweils zwischen die Kathodenanschlüsse der Dioden **160**, **160'** und die Kapazitäten **170**, **170'** geschaltet sind. Als weitere optionale Komponenten weisen die beiden Energiespeichereinrichtungen **130**, **140** jeweils einen standardmäßig geöffneten Schalter **196**, **196'** auf, die parallel zu den Kapazitäten **170**, **170'** geschaltet und mit dem Bezugspotenzial, also Masse, verbunden sind. Über die in Reihe zu den Kapazitäten **170**, **170'** geschalteten Schalter **194**, **194'** können die Kapazitäten gezielt vor einem erwartungsgemäßen Abschalten der Versorgungsspannung von dem Rest der Schaltung abgetrennt werden, wie dies auch die Pfeile in **Fig.** 2 andeuten. Über die beiden standardmäßig geöffneten Schalter **196**, **196'** können die beiden Kapazitäten in diesem Fall dann entladen werden, so dass in den beiden Energiespeichereinrichtungen **130**, **140** keine Energiemenge gespeichert ist, die zu einer Änderung des Zustands der NVM-Zelle **110** führt.

[0046] Neben der in den **Fig.** 1 und **Fig.** 2 gezeigten Ausführungsbeispiele der beiden Energiespeichereinrichtungen **130**, **140**, die als energiespeichernde Komponenten die beiden Kapazitäten **170**, **170'** umfassen, können die beiden Energiespeichereinrichtungen **130**, **140** auch als energiespeichernde Komponenten Induktivitäten, also beispielsweise Spulen oder einzelne Windungen von Spulen, aufweisen.

[0047] Grundsätzlich ist es bei den in **Fig.** 1 und **Fig.** 2 gezeigten Ausführungsbeispielen einer erfindungsgemäßen Vorrichtung **100** zum nicht-flüchtigen Speichern eines Statuswerts möglich, anstelle zweier Energiespeichereinrichtungen **130**, **140** nur eine modifizierte Energiespeichereinrichtung zu verwenden. Abgesehen von einer entsprechenden Auslegung der die Energie bzw. die Spannung zur Verfügung stellenden Kapazität bzw. Mehrzahl von Kapazitäten, kann es notwendig sein, um mehr als einen Spannungswert der als nicht-flüchtigen Speichereinrichtung dienenden NVM-Zelle **110** zur Verfügung zu stellen, einen Spannungsteiler einzusetzen. Darüber hinaus kann im Unterschied zu dem in **Fig.** 1 und **Fig.** 2 gezeigten Ausführungsbeispiel gegebe-

nenfalls auch auf eine zweite Schalteinrichtung verzichtet werden.

[0048] Neben der in den beiden Ausführungsbeispielen in den **Fig.** 1 und **Fig.** 2 gezeigten Möglichkeit einer nicht-flüchtigen Speicherung eines Statussignals, das beispielsweise einen Angriff anzeigen kann, über eine Channel-Hot-Electron-Programmierung einer EEPROM-Zelle als NVM-Zelle, kann bei entsprechender Verschaltung auch eine Channel-Hot-Hole oder eine den Fowler-Nordheim-Tunneleffekt nutzende Programmierung der EEPROM-Zelle Verwendung finden. Weiterhin kann die nicht-flüchtige Speichereinrichtung beispielsweise auch einen schnellen nicht-flüchtigen Speicher nutzen, bei dem mit einer geringen Energieaufnahme ein direktes Schreiben erfolgen kann.

[0049] Neben dem eigentlichen Speichern eines Statuswertes bzw. einer Alarminformation im Rahmen eines Powerless Event Storage-Vorgangs muss das System, das die erfindungsgemäße Vorrichtung **100** zum nicht-flüchtigen Speichern eines Statuswerts umfasst, beispielsweise nach einem Neustart in der Lage sein, die nicht-flüchtige Speichereinrichtung, also die NVM-Zelle **110**, auszulesen und gegebenenfalls zu löschen, also in den ursprünglichen Zustand zurückzuversetzen. Zu diesem Zweck weist das System im Allgemeinen weitere Schaltungskomponenten auf, die einerseits eine Ausleseoperation und andererseits eine Löschoperation der NVM-Zelle **110** ermöglichen. Die **Fig.** 3 und **Fig.** 4 zeigen schematisch jeweils ein Ausführungsbeispiel in Form eines Teilschaltbildes der zum Auslesen bzw. Löschen der NVM-Zelle **110** heranziehbaren Schaltungen. Der Aufbau und die Funktionsweise der beiden in **Fig.** 3 und **Fig.** 4 dargestellten Ausführungsbeispiele wird im Folgenden erläutert.

[0050] **Fig.** 3 zeigt ein schematisches Teilschaltbild eines Ausführungsbeispiels einer Ausleseschaltung zum Auslesen der bereits in den **Fig.** 1 und **Fig.** 2 gezeigten NVM-Zelle **110**, die auch hier wiederum als NVM Cell bezeichnet ist. Der Drainanschluss **110d** der NVM-Zelle **110** ist über einen ersten Ausleseschalter **200** mit einer ersten Auslesespannung U_{r1}, die beispielsweise eine Spannung von 1,5 V aufweist. Der Gateanschluss **110g** der NVM-Zelle **110** ist mit einer zweiten Auslesespannung U_{r2}, beispielsweise mit einem Potential von ebenfalls 1,5 V, verbunden. Der Substratanschluss bzw. Bulkanschluss **110b** der NVM-Zelle **110** ist wiederum mit dem Bezugspotential verbunden. Der Sourceanschluss **110s** der NVM-Zelle **110** ist über einen zweiten Ausleseschalter **210** mit dem Bezugspotential verbunden. Darüber hinaus ist der Sourceanschluss **110s** auch mit eine Auslesekapazität **220** und einem Ausleseanschluss **230**, der in **Fig.** 3 auch als „out" bezeichnet ist, verbunden. Neben der Verbindung mit dem Sourceanschluss **110s** ist die Auslesekapazität **220** mit dem Bezugspotential verbunden.

[0051] Um nun die NVM-Zelle **110** auszulesen, werden, wie in **Fig.** 3 durch die Pfeile angedeutet sind, der erste Ausleseschalter **200** geschlossen und der zweite Ausleseschalter **210** geöffnet. Durch das Öffnen des zweiten Ausleseschalters **210** wird die Verbindung beider Anschlüsse der Auslesekapazität **220** zu dem Bezugspotential unterbrochen, so dass gegebenenfalls, wenn also durch Anlegen der Auslesespannung an den Gateanschluss **110g** und den Drainanschluss **110d** der NVM-Zelle **110** die Strecke zwischen dem Sourceanschluss **110s** und dem Drainanschluss **110d** leitend geschaltet wird, die Auslesekapazität **220** auf Grund des durch die NVM-Zelle **110** fließenden Stroms geladen werden kann. Nach einer Zeit, die einerseits durch den Kapazitätswert der Auslesekapazität **220** und andererseits im Wesentlichen durch den elektrischen Widerstand der NVM-Zelle **110** bestimmt ist, liegt an dem Ausleseanschluss **230** in dem Fall, dass die NVM-Zelle **110** leitend geschaltet ist, im Wesentlichen die Auslesespannung an. Ist hingegen die NVM-Zelle **110** durch Anlegen der Auslesespannungen an den Gateanschluss **110g** und den Drainanschluss **110d** in einem nichtdurchgeschalteten Zustand, sperrt also die NVM-Zelle **110**, so ist das an dem Ausleseanschluss **230** anliegende Potential im Wesentlichen mit dem Bezugspotential identisch. Abweichungen hiervon können im Wesentlichen durch Leckströme beispielsweise durch die NVM-Zelle **110** entstehen. Hierdurch kann je nach Zustand der NVM-Zelle **110** diese den Ausleseanschluss **230** bzw. den zugehörigen Ladungsknoten laden oder nicht laden.

[0052] Da im Allgemeinen das Auslesen der nicht-flüchtigen Speichereinrichtung **110**, also der NVM-Zelle **110**, nur im normalen Betriebsmodus durchgeführt werden muss, ist eine Energie- oder Spannungspufferung mit Hilfe einer Energiespeichereinrichtung nicht notwendig.

[0053] Ist der Auslesevorgang beendet, werden der erste und der zweite Ausleseschalter **200**, **210** in ihren ursprünglichen Zustand zurückversetzt, so dass also der erste Ausleseschalter **200** geöffnet und der zweite Ausleseschalter **210** geschlossen ist. Die auf der Auslesekapazität **220** angesammelte Ladung wird so über das Bezugspotential abgeleitet, so dass an dem Ausleseanschluss **230** unabhängig von dem Zustand der NVM-Zelle **110** das Bezugspotential zur Verfügung steht.

[0054] Um gegebenenfalls die NVM-Zelle **110** wieder löschen zu können, also in ihren ursprünglichen Zustand zurückzuversetzen, ist es notwendig, eine Schaltung vorzusehen, mit deren Hilfe die NVM-Zelle **110** gelöscht werden kann. **Fig.** 4 zeigt ein schematisches Teilschaltbild eines Ausführungsbeispiel einer

entsprechenden Schaltung zum Löschen der NVM-Zelle **110**. Die NVM-Zelle **110** ist mit ihrem Drainanschluss **110d** an einen ersten Löschschalter **240** gekoppelt. Darüber hinaus ist die NVM-Zelle **110** mit ihrem Substratanschluss bzw. Bulkanschluss **110b** an eine erste Löschspannung U_{e1}, die beispielsweise eine Spannung von 4 V aufweist, mit ihrem Sourceanschluss **110s** an eine zweite Löschspannung U_{e2}, die beispielsweise auch eine Spannung von 4 V aufweist, und mit ihrem Gateanschluss **110g** über einen zweiten Löschschalter **250** an eine dritte Löschspannung U_{e3}, die beispielsweise eine Spannung von –11 V aufweist, gekoppelt. Darüber hinaus ist auch hier, wie im Fall der Ausleseoperation, im Allgemeinen keine Energie- oder Spannungspufferung notwendig, da die Löschoperation im Allgemeinen nur während der normalen Betriebsbedingungen durchgeführt werden muss.

[0055] Um die NVM-Zelle **110** zu löschen, also ihren ursprünglichen Zustand wiederherzustellen, wird, wie in **Fig.** 4 durch die Pfeile angedeutet ist, der erste Löschschalter **240** geöffnet, wodurch der Drainanschluss **110d** der NVM-Zelle **110** von der weiteren, nicht in **Fig.** 4 gezeigten Schaltung getrennt. Des weiteren wird, wie ebenfalls in **Fig.** 4 durch den Pfeil angedeutet ist, der zweite Löschschalter **250** geschlossen, so dass an den Gateanschluss **110g** der NVM-Zelle **110** die zweite Löschspannung angelegt wird. Hierdurch kommt es im vorliegenden Ausführungsbeispiel zu einem Löschen der NVM-Zelle **110** durch den als Fowler-Nordheim-Tunneln bezeichneten Vorgang bzw. Prozess.

[0056] Abhängig von den Gegebenheiten kann das erfindungsgemäße Verfahren zum nicht flüchtigen Speichern eines Statuswerts in Hardware oder in Software implementiert werden. Die Implementierung kann auf einem digitalen Speichermedium, insbesondere einer Diskette, CD oder DVD mit elektronisch auslesbaren Steuersignalen erfolgen, die so mit einem programmierbaren Computersystem zusammenwirken können, dass das erfindungsgemäße Verfahren zum nicht-flüchtigen Speichern eines Statuswerts ausgeführt wird. Allgemein besteht die Erfindung somit auch in einem Software-Programm-Produkt bzw. einem Computer-Programm-Produkt bzw. einem Programm-Produkt mit einem auf einem maschinenlesbaren Träger gespeicherten Programmcode zur Durchführung des erfindungsgemäßen Verfahrens, wenn das Software-Programm-Produkt auf einem Rechner oder einem Prozessor abläuft. In anderen Worten ausgedrückt kann die Erfindung somit als ein Computer-Programm bzw. Software-Programm bzw. Programm mit einem Programmcode zur Durchführung des Verfahrens realisiert werden, wenn das Programm auf einem Prozessor abläuft. Der Prozessor kann hierbei von einem Computer, einer Chipkarte (Smartcard) oder einem anderen integrierten Schaltkreis gebildet sein.

Bezugszeichenliste

100	Vorrichtung zum nicht-flüchtigen Speichern eines Statuswerts
110	NVM-Zelle
120	erste Schalteinrichtung
130	erste Energiespeichereinrichtung
140	zweite Energiespeichereinrichtung
150	zweite Schalteinrichtung
160	Diode
160'	Diode
170	Kapazität
170'	Kapazität
175	Steuereinrichtung
180	selbstsperrender PMOS-Transistor
190	selbstsperrender PMOS-Transistor
194	Schalter
194'	Schalter
196	Schalter
196'	Schalter
200	erster Ausleseschalter
210	zweiter Ausleseschalter
220	Auslesekapazität
230	Ausleseanschluss
240	erster Löschschalter
250	zweiter Löschschalter

Patentansprüche

1. Vorrichtung (**100**) zum nicht-flüchtigen Speichern eines Statuswerts, der anzeigt, dass eine Bedingung vorgelegen hat, mit folgenden Merkmalen:
einer nicht-flüchtigen Speichereinrichtung (**110**);
einer Energiespeichereinrichtung (**130**, **140**) zum Speichern von Energie bei Anliegen einer Versorgungsspannung; und
einer Schalteinrichtung (**120**, **150**), die ausgelegt ist, um die Energiespeichereinrichtung (**130**, **140**) mit der nicht-flüchtigen Speichereinrichtung (**110**) zu koppeln, um den Statuswert in dieselbe zu schreiben, wenn die Bedingung auftritt,
wobei die Vorrichtung eine integrierte Schaltung ist.

2. Vorrichtung (**100**) nach Anspruch 1, bei der die Bedingung vorliegt, wenn die Versorgungsspannung unter einen vorbestimmten Wert fällt.

3. Vorrichtung (**100**) nach Anspruch 1, bei der die Bedingung vorliegt, wenn die Versorgungsspannung unter einen vorbestimmten Wert fällt und kein Signal vorliegt, dass ein erwartungsgemäßes Ausschalten anzeigt.

4. Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche, bei der die Schalteinrichtung (**130**, **140**) einen Steueranschluss aufweist, an dem eine von der Versorgungsspannung abgeleitete Spannung anliegt.

5. Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche, die eine Einrichtung (**175**) zum Erzeugen eines Steuersignals, für die Schalteinrichtung (**120**, **150**) aufweist, wenn die Bedingung vorliegt, wobei das Steuersignal die Schalteinrichtung (**110**, **150**) steuert, um die nicht-flüchtige Speichereinrichtung (**110**) mit der Energiespeichereinrichtung (**130**, **140**) zu koppeln.

6. Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche, bei der die Energiespeichereinrichtung (**130**, **140**) eine Kapazität (**170**, **170'**), die zwischen einen Anschluss der Schalteinrichtung (**120**, **150**) und ein Bezugspotenzial geschaltet ist, und eine Diode (**160**, **160'**), die zwischen einen Spannungsanschluss der Energiespeichereinrichtung (**130**, **140**) zum Laden der Kapazität und die Kapazität (**170**, **170'**) geschaltet ist.

7. Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche, bei der die Schalteinrichtung (**120**, **150**) einen Transistor (**180**, **190**) umfasst.

8. Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche, bei der die Schalteinrichtung (**120**, **150**) einen selbstsperrenden PMOS-Transistor (**180**, **190**) umfasst.

9. Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche, bei der die Energiespeichereinrichtung (**130**, **140**) in eine erste Energiespeichereinrichtung (**130**) und eine zweite Energiespeichereinrichtung (**140**) untergliedert ist.

10. Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche, bei der die nicht-flüchtige Speichereinrichtung (**110**) eine EEPROM-Zelle (**110**) umfasst, die ausgelegt ist, um mittels heißer Ladungsträger oder dem Fowler-Nordheim-Tunneleffekt programmierbar zu sein, oder eine schnelle nicht-flüchtige Speicherzelle umfasst, die ausgelegt ist, um mit niedriger Energie programmierbar zu sein.

11. Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche, bei der die Vorrichtung (**100**) an eine Verzögerungseinrichtung gekoppelt ist, wobei die Verzögerungseinrichtung ausgelegt ist, um einen Neustart einer Prozessoreinrichtung, mit der die Vorrichtung (**100**) gekoppelt ist, zu verzögern.

12. System, mit folgenden Merkmalen:
einer Vorrichtung (**100**) nach einem der vorhergehenden Ansprüche;
einem Zähler; und
einer Zählersteuereinrichtung;
wobei die Vorrichtung (**100**) an den Zähler und die Zählersteuereinrichtung gekoppelt ist, wobei die Zählersteuereinrichtung ausgelegt ist, um in Abhängigkeit von dem Statuswert den Zähler zu inkrementieren oder zu dekrementieren.

13. System nach Anspruch 12, bei der die Zählersteuereinrichtung ausgelegt ist, um eine Prozessoreinrichtung, die die Vorrichtung (**100**), den Zähler und die Zählersteuereinrichtung umfasst, zu sperren, wenn ein Zählwert des Zählers eine vorbestimmte Bedingung erfüllt.

14. Verfahren zum nicht-flüchtigen Speichern eines Statuswerts, der anzeigt, dass eine Bedingung vorgelegen hat, in einer Vorrichtung (**100**) zum nicht-flüchtigen Speichern eines Statuswerts, die eine nicht-flüchtige Speichereinrichtung (**110**) und eine Energiespeichereinrichtung (**130**, **140**) zum Speichern von Energie bei Anliegen einer Versorgungsspannung umfasst und die eine integrierte Schaltung ist, mit folgenden Schritten:
Speichern von Energie in der Energiespeichereinrichtung (**130**, **140**), wenn die Versorgungsspannung anliegt;
Koppeln der Energiespeichereinrichtung (**130**, **140**) mit der nicht-flüchtigen Speichereinrichtung (**110**) zum Schreiben des Statuswerts in die nicht-flüchtige Speichereinrichtung (**110**), wenn die Bedingung auftritt.

15. Verfahren nach Anspruch 14, bei der die Bedingung vorliegt, wenn eine Versorgungsspannung unter einen vorbestimmten Wert fällt.

16. Verfahren nach Anspruch 14, bei der die Bedingung vorliegt, wenn eine Versorgungsspannung unter einen vorbestimmten Wert fällt und kein Signal vorliegt, dass ein erwartungsgemäßes Ausschalten anzeigt.

17. Verfahren nach einem der Ansprüche 14 bis 16, bei der die nicht-flüchtige Speichereinrichtung (**110**) eine EEPROM-Zelle (**110**) umfasst, die ausgelegt ist, um mittels heißer Ladungsträger oder dem Fowler-Nordheim-Tunneleffekt programmierbar zu sein, oder eine schnelle nicht-flüchtige Speicherzelle umfasst, die ausgelegt ist, um mit niedriger Energie programmierbar zu sein.

18. Programm mit einem Programmcode zum Durchführen des Verfahrens zum nicht-flüchtigen Speichern eines Statuswerts nach Anspruch 14, wenn das Programm auf einem Prozessor abläuft.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

FIG 1

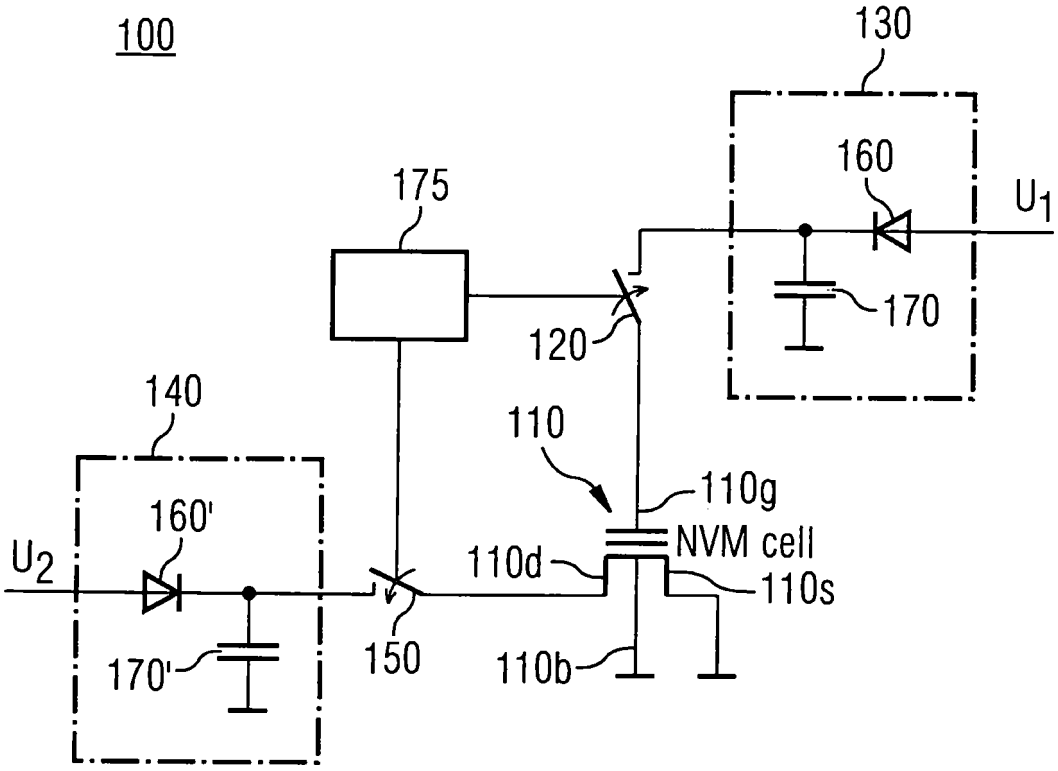


FIG 2

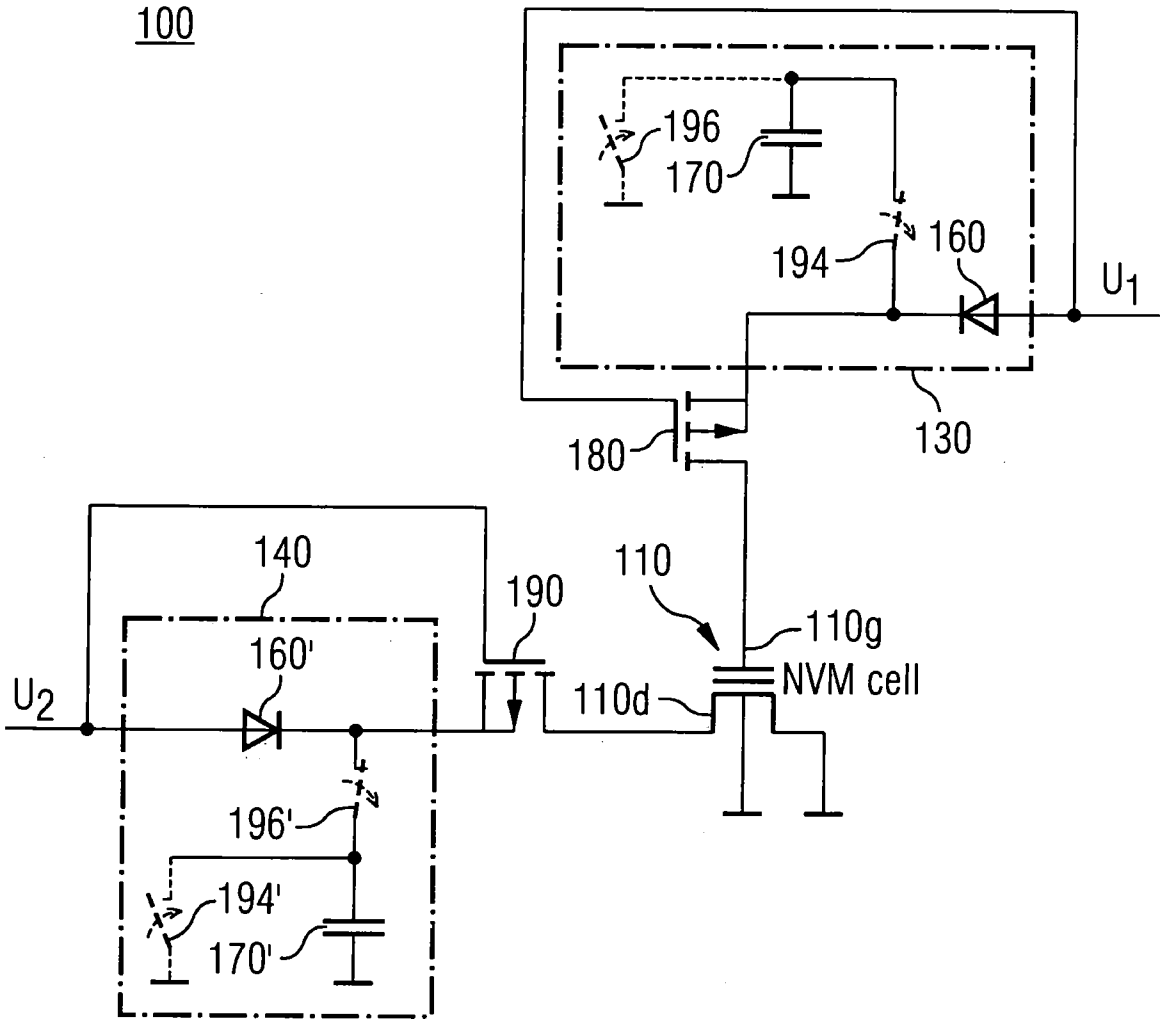

100
196
170
194
160
U1
130
180
140
190
110
160'
110g
NVM cell
U2
110d
196'
194'
170'

FIG 3

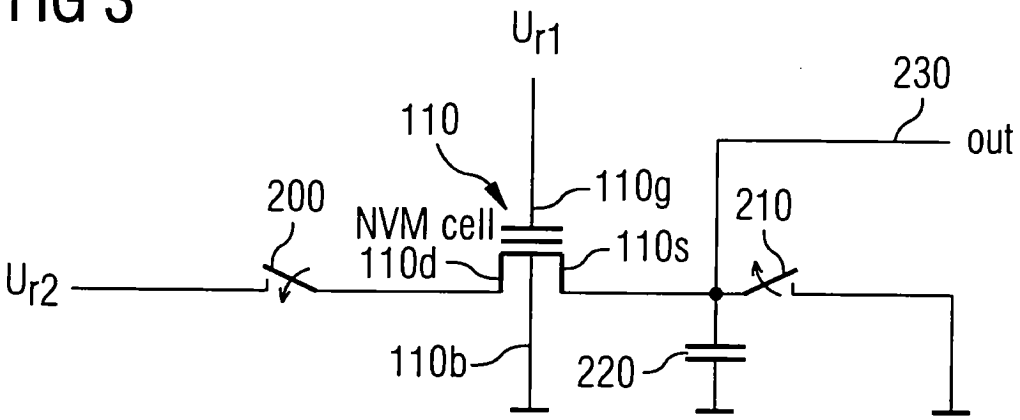
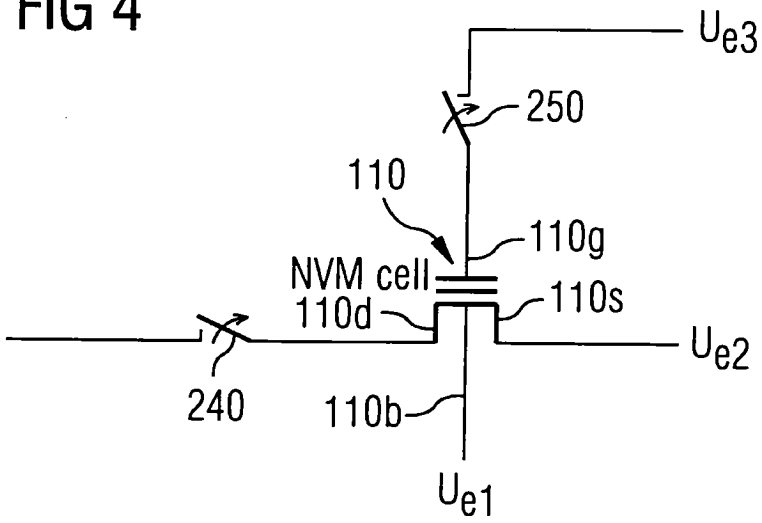

U_{r1}
230
out
110
110g
200
NVM cell
210
110d
110s
U_{r2}
110b
220

FIG 4


U_{e3}
250
110
110g
NVM cell
110d
110s
U_{e2}
240
110b
U_{e1}