(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
21. Oktober 2004 (21.10.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/090730 A2

(51) Internationale Patentklassifikation[7]: G06F 12/14

(21) Internationales Aktenzeichen: PCT/DE2004/000704

(22) Internationales Anmeldedatum:
1. April 2004 (01.04.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 15 726.3 4. April 2003 (04.04.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BÖNING, Werner** [DE/DE]; Prinzenstr. 31, 80639 München (DE).

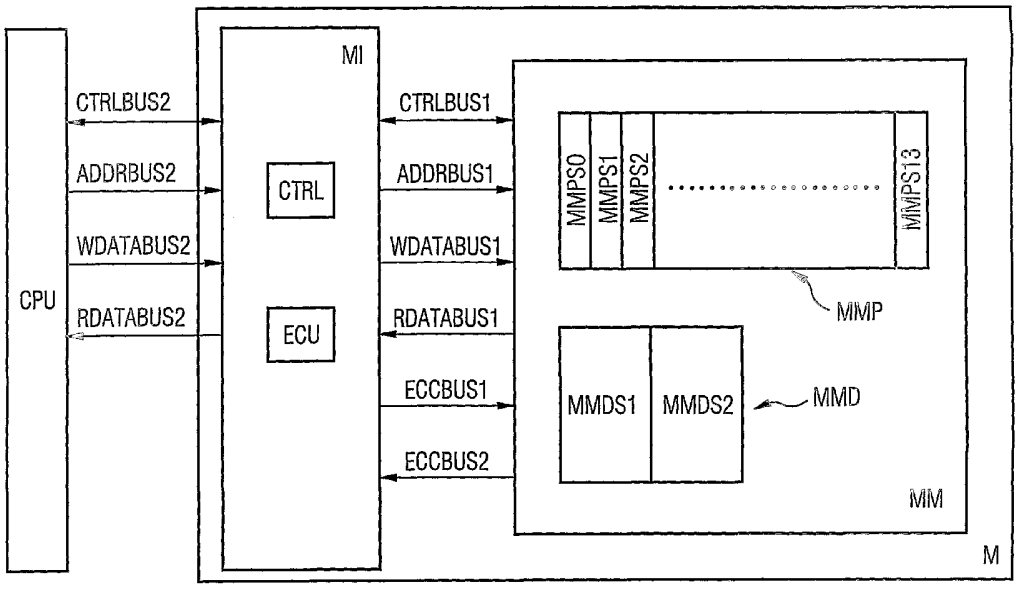
(74) Anwälte: **REPKOW, Ines** usw.; Patentanwälte Jannig & Repkow, Klausenberg 20, 86199 Augsburg (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,

[Fortsetzung auf der nächsten Seite]

(54) **Title:** PROGRAM-CONTROLLED UNIT

(54) **Bezeichnung:** PROGRAMMGESTEUERTE EINHEIT



(57) **Abstract:** The invention relates to a program-controlled unit comprising a memory for storing data and a memory protection device for protecting the memory from read-access operations initiated by non-authorized personnel. Said program-controlled unit is characterized in that it is configured in such a way that it automatically activates the read protection if required and that the read protection can be adapted to given conditions by authorized personnel.

(57) **Zusammenfassung:** Es wird eine programmgesteuerte Einheit mit einem Speicher zum Speichern von Daten, und mit einer Speicherschutzvorrichtung zum Schützen des Speichers vor Lesezugriffen durch hierzu nicht autorisierte Personen beschrieben. Die beschriebene programmgesteuerte Einheit zeichnet sich dadurch aus, daß sie so ausgebildet ist, dass der Leseschutz durch die programmgesteuerte Einheit bei Bedarf automatisch aktiviert wird, und durch eine hierzu autorisierte Person an die gegebenen Verhältnisse angepaßt werden kann.

WO 2004/090730 A2

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Programmgesteuerte Einheit

Die vorliegende Erfindung betrifft eine Vorrichtung gemäß dem Oberbegriff des Patentanspruchs 1, d.h. eine programmgesteuerte Einheit mit einem Speicher zum Speichern von Daten, und mit einer Speicherschutzvorrichtung zum Schützen des Speichers vor Lesezugriffen durch hierzu nicht autorisierte Personen.

Eine solche programmgesteuerte Einheit ist beispielsweise ein Mikrocontroller, ein Mikroprozessor, oder ein Signalprozessor.

Der prinzipielle Aufbau einer solchen programmgesteuerten Einheit ist in Figur 6 gezeigt.

Die in der Figur 6 gezeigte programmgesteuerte Einheit ist mit dem Bezugszeichen PG bezeichnet. Sie enthält eine CPU CPU, eine mit der CPU verbundene Speichereinrichtung M, und über einen Bus BUS mit der CPU verbundene Peripherieeinheiten P1 bis Pn.

Die CPU führt ein Programm aus, das in der Speichereinrichtung M oder in einer in der Figur 6 nicht gezeigten anderen Speichereinrichtung gespeichert ist, wobei diese andere Speichereinrichtung eine weitere interne Speichereinrichtung oder eine außerhalb der programmgesteuerten Einheit PG vorgesehene externe Speichereinrichtung sein kann.

Die Speichereinrichtung M dient zur Speicherung eines Programmes und/oder der zugehörigen Operanden und/oder sonstiger Daten.

Die Peripherieeinheiten P1 bis Pn umfassen beispielsweise einen DMA-Controller, einen A/D-Wandler, einen D/A-Wandler,

einen Timer, Schnittstellen und Controller zur Ein- und/oder Ausgabe von Daten, ein On-Chip-Debug-Support- bzw. OCDS-Modul, etc.

Nicht selten hat der Entwickler des von der programmgesteuerten Einheit ausgeführten Programmes ein Interesse daran, daß hierzu nicht autorisierte Personen nicht in der Lage sind, das Programm und/oder die Operanden aus dem diese speichernden Speicher auszulesen. Ein Auslesen des Programmes und/oder der Operanden durch hierzu nicht autorisierte Personen würde es nämlich Mitbewerbern des Programmentwicklers ermöglichen, das Programm, die Operanden oder bestimmte Teile davon zu kopieren und diese oder das darin enthaltene Knowhow in ihren eigenen Produkten zu verwenden.

Es sind bereits diverse Möglichkeiten bekannt, um das Auslesen von Programmen und/oder Operanden durch hierzu nicht autorisierte Personen zu verhindern. Beispielsweise kann vorgesehen werden, die zu schützenden Daten (Programme und/oder Operanden) in einem internen Speicher der programmgesteuerten Einheit wie beispielsweise der Speichereinrichtung M zu speichern, und die programmgesteuerte Einheit mit einer Speicherschutzvorrichtung auszustatten, die von dazu nicht autorisierten Personen veranlaßte Lesezugriffe auf den internen Speicher blockiert.

Die bekannten programmgesteuerten Einheiten, bei welchen von dazu nicht autorisierten Personen veranlaßte Lesezugriffe auf den internen Speicher blockiert werden, bieten entweder keinen perfekten Leseschutz, und/oder sind kompliziert in der Handhabung, und/oder weisen einen komplizierten Aufbau auf und/oder weisen nur eingeschränkte Verwendungsmöglichkeiten auf.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, die programmgesteuerte Einheit gemäß dem Oberbegriff des Patentanspruchs 1 derart weiterzubilden, daß diese einen zu-

verlässigen Leseschutz bietet, einen einfachen Aufbau aufweist, einfach handhabbar ist, und universell einsetzbar ist.

Diese Aufgabe wird erfindungsgemäß durch die in Patentanspruch 1 beanspruchte programmgesteuerte Einheit gelöst.

Die erfindungsgemäße programmgesteuerte Einheit zeichnet sich dadurch aus, daß sie so ausgebildet ist, daß der Leseschutz

- durch die programmgesteuerte Einheit bei Bedarf automatisch aktiviert wird, und

- durch eine hierzu autorisierte Person an die gegebenen Verhältnisse angepaßt werden kann.

Bei einer solchen programmgesteuerten Einheit kann der zu schützende Speicher auf einfache Weise zuverlässig vor Lesezugriffen durch hierzu nicht autorisierte Personen geschützt werden.

Vorteilhafte Weiterbildungen der Erfindung sind den Unteransprüchen, der folgenden Beschreibung, und den Figuren entnehmbar.

Die Erfindung wird nachfolgend anhand von Ausführungsbeispielen unter Bezugnahme auf die Figuren näher erläutert. Es zeigen

Figur 1 den Aufbau einer vor Zugriffen durch dazu nicht autorisierte Personen schützbaren Speichereinrichtung der im folgenden beschriebenen programmgesteuerten Einheit,

Figur 2 die Anordnung von protection configuration bits in einem ersten user configuration block der in der Figur 1 gezeigten Speichereinrichtung,

Figur 3 die Anordnung von protection configuration bits in einem zweiten user configuration block der in der Figur 1 gezeigten Speichereinrichtung,

Figur 4 die Anordnung von protection configuration bits in einem dritten user configuration block der in der Figur 1 gezeigten Speichereinrichtung,

Figur 5 den Aufbau eines Konfigurationsregisters der in der Figur 1 gezeigten Speichereinrichtung, und

Figur 6 den Aufbau einer programmgesteuerten Einheit.

Bei der im folgenden beschriebenen programmgesteuerten Einheit handelt es sich um einen Mikrocontroller. Es sei jedoch bereits an dieser Stelle darauf hingewiesen, daß es sich auch um eine beliebige andere programmgesteuerte Einheit wie beispielsweise um einen Mikroprozessor oder um einen Signalprozessor handeln könnte.

Der beschriebene Mikrocontroller hat den selben prinzipiellen Aufbau wie die in der Figur 6 gezeigte programmgesteuerte Einheit. Er enthält jedoch Schutzmechanismen, durch welche besonders einfach, flexibel und zuverlässig verhindert werden kann, daß in der Speichereinrichtung M gespeicherte Daten durch dazu nicht autorisierte Personen ausgelesen und/oder verändert werden können. Unter Daten sind sowohl Befehle repräsentierende Daten (Befehlscode) als auch keinen Befehlscode repräsentierende "normale" Daten wie Operanden, Parameter, Konstanten etc. zu verstehen.

Diese Schutzmechanismen sind im betrachteten Beispiel Bestandteil der Speichereinrichtung M.

Der Aufbau der Speichereinrichtung M des hier vorgestellten Mikrocontrollers ist in Figur 1 gezeigt.

Die Speichereinrichtung M enthält ein Speichermodul MM und eine Schnittstelle MI.

Das Speichermodul MM ist der Speicher, dessen Inhalt vor einem Auslesen und/oder Verändern durch eine hierzu nicht autorisierte Person geschützt werden soll.

Der Vollständigkeit halber sei bereits an dieser Stelle angemerkt, daß dann, wenn aus dem Speichermodul MM stammende Befehle und/oder Daten in einem Cache, einen Scratchpad-Speicher oder einem sonstigen Zwischenspeicher der programmgesteuerten Einheit zwischengespeichert werden, auch deren Inhalt vor einem Auslesen durch hierzu nicht autorisierte Personen geschützt werden muß.

Das Speichermodul MM enthält im betrachteten Beispiel einen als Programmspeicher verwendeten Teil MMP, einen als Datenspeicher verwendeten Teil MMD, und weitere, in der Figur 1 nicht gezeigte Komponenten, wie insbesondere Leseverstärker, Pufferspeicher, Steuereinrichtungen etc. Der Vollständigkeit halber sei bereits an dieser Stelle darauf hingewiesen, daß das Speichermodul MM auch ein ausschließlich als Programmspeicher verwendeter Speicher, oder ein ausschließlich als Datenspeicher verwendeter Speicher sein könnte. Außerdem können auch im Programmspeicher Daten (Operanden, Konstanten etc.) gespeichert sein, und können auch im Datenspeicher Programme gespeichert sein.

Das Speichermodul MM wird im betrachteten Beispiel durch einen Flash-Speicher gebildet. Das Speichermodul MM kann aber auch ein anderer umprogrammierbarer nichtflüchtiger Speicher, beispielsweise ein EEPROM, oder ein Festspeicher wie beispielsweise ein ROM, oder ein flüchtiger Speicher wie beispielsweise ein RAM sein.

Im betrachteten Beispiel ist der Programmspeicher MMP in 14 Sektoren MMPS0 bis MMPS13 unterteilt, wobei die Sektoren MMPS1 bis MMPS13 zum Speichern von Programmen vorgesehen sind, und wobei der Sektor MMPS0 zur Speicherung von Konfigurationsdaten vorgesehen ist.

Von den zur Speicherung von Programmen vorgesehenen Sektoren MMPS1 bis MMPS13 weisen die Sektoren MMPS1 bis MMPS8 jeweils eine Speicherkapazität von 16 kByte auf, der Sektor MMPS9 eine Speicherkapazität von 128 kByte, der Sektor MMPS10 eine Speicherkapazität von 256 kByte, und die Sektoren MMPS11 bis MMPS13 jeweils eine Speicherkapazität von 512 kByte.

Die im Sektor MMPS0 gespeicherten Konfigurationsdaten dienen zur Konfigurierung des Schreibschutzes und des Leseschutzes, durch welche das Auslesen und/oder Verändern der in den Sektoren MMPS1 bis MMPS13 und im Datenspeicher MMD gespeicherten Daten durch dazu nicht autorisierte Personen verhindert wird.

Der Datenspeicher MMD weist im betrachteten Beispiel eine Speicherkapazität von 128 kByte auf und ist in 2 Sektoren MMDS1 und MMDS2 unterteilt, welche jeweils 64 kByte umfassen.

Der Vollständigkeit halber sei darauf hingewiesen, daß sowohl beim Programmspeicher MMP als auch beim Datenspeicher MMD sowohl die Anzahl der Sektoren als auch die Größe der Sektoren beliebig viel größer oder kleiner sein kann.

Das Speichermodul MM wird über die Schnittstelle MI angesprochen. D.h., sämtliche Zugriffe auf das Speichermodul MM erfolgen über die Schnittstelle MI.

Die Schnittstelle MI enthält eine Steuereinrichtung CTRL, eine Fehlerkorrektureinrichtung ECU, sowie in der Figur 1 nicht gezeigte weitere Komponenten wie Buffer, Latches, Register etc..

Die Schnittstelle MI und das Speichermodul MM sind über einen Steuerbus CTRLBUS1, einen Adreßbus ADDRBUS1, einen Schreibdatenbus WDATABUS1, einen Lesedatenbus RDATABUS1, und Fehlerkorrekturdatenbusse ECCBUS1 und ECCBUS2 miteinander verbunden.

Die Schnittstelle MI ist mit der CPU und weiteren Komponenten des Mikrocontrollers, die auf die Speichereinrichtung M zugreifen können, über einen Steuerbus CTRLBUS2, einen Adreßbus ADDRBUS2, einen Schreibdatenbus WDATABUS2, und einen Lesedatenbus RDATABUS2 verbunden.

Zu den weiteren Komponenten, die neben der CPU auf die Speichereinrichtung M zugreifen können, gehören im betrachteten Beispiel ein DMA-Controller, ein OCDS-Modul, und ein Peripheral Control Prozessor (PCP)). Es wäre jedoch auch denkbar, daß weitere und/oder andere Mikrocontroller-Komponenten auf die Speichereinrichtung M zugreifen können.

Wenn eine der Einrichtungen, die auf die Speichereinrichtung M zugreifen können, Daten aus der Speichereinrichtung, genauer gesagt aus dem Programmspeicher MMP oder aus dem Datenspeicher MMD auslesen möchte, übermittelt sie über den Steuerbus CTRLBUS2 ein Lesesignal, und über den Adreßbus ADDRBUS2 die Adresse, unter welcher die benötigten Daten gespeichert sind. Die Steuereinrichtung CTRL der Schnittstelle MI überprüft zunächst, ob es sich um einen zulässigen Zugriff handelt. Ein unzulässiger Zugriff liegt insbesondere vor, wenn ein Leseschutz wirksam ist, durch welchen das Auslesen der durch den Lesezugriff angeforderten Daten aus der Speichereinrichtung M verhindert werden soll. Wenn die Steuereinrichtung CTRL feststellt, daß es sich um einen unzulässigen Zugriff auf die Speichereinrichtung M handelt, führt sie diesen Zugriff nicht aus und signalisiert zudem der CPU und/oder sonstigen Mikrocontroller-Komponenten, daß ein unzulässiger Zugriff auf die Speichereinrichtung M erfolgt ist. Anderenfalls, d.h. wenn es sich um einen zulässigen Zugriff handelt,

veranlaßt die Steuereinrichtung CTRL durch Übermittlung entsprechender Steuersignale und Adressen an das Speichermodul MM, daß die durch den Lesezugriff aus der Speichereinrichtung M angeforderten Daten aus dem Speichermodul MM ausgelesen und an die Schnittstelle MI ausgegeben werden. Die von der Steuereinrichtung CTRL an das Speichermodul MM übermittelten Steuersignale und Adressen werden über den Steuerbus CTRLBUS1 und den Adreßbus ADDRBUS1 übertragen; die vom Speichermodul MM ausgegebenen Daten werden über den Lesedatenbus RDATABUS1 übertragen.

Neben den über den Lesedatenbus RDATABUS1 übertragenen Daten gibt das Speichermodul MM auch noch diesen Daten zugeordnete Fehlerkorrektur- bzw. ECC-Daten aus. Diese Daten werden über den ECCBUS2 übertragen.

Anschließend wird durch die Fehlerkorrektureinrichtung ECU unter Auswertung der über die Busse RDATABUS1 und ECCBUS2 erhaltenen Daten überprüft, ob die über den Lesedatenbus RDATABUS1 übertragenen Daten fehlerfrei sind. Wenn die Daten nicht fehlerfrei sind und es sich um einen korrigierbaren Fehler handelt, korrigiert sie diesen. Wie Fehler unter Verwendung eines ECC (error correction code) erkannt und korrigiert werden, ist bekannt und bedarf keiner näheren Erläuterung.

Danach gibt die Schnittstelle MI die vom Speichermodul MM ausgegebenen und gegebenenfalls korrigierten Daten über den Lesedatenbus RDATABUS2 an die Einrichtung aus, von welcher der Lesezugriff stammte.

Alle anderen Zugriffe auf die Speichereinrichtung M, insbesondere auch die Zugriffe, durch welche das Löschen von in der Speichereinrichtung M gespeicherten Daten veranlaßt wird, und die Zugriffe, durch welche das Einschreiben von Daten in die Speichereinrichtung M veranlaßt wird, werden durch die Übertragung von beispielsweise auf dem JEDEC-Standard basie-

renden Kommandosequenzen an die Speichereinrichtung M veranlaßt oder eingeleitet. Die Übertragung einer Kommandosequenz an die Speichereinrichtung M ist letztlich nichts anderes als ein Schreibzugriff auf die Speichereinrichtung M. D.h., der Speichereinrichtung M werden über den Steuerbus CTRLBUS2 ein Schreibsignal, über den Adreßbus ADDRBUS2 eine Adresse, und über den Schreibdatenbus WDATABUS2 Daten zugeführt. Eine Kommandosequenz kann einen oder mehrere aufeinanderfolgende Schreibzugriffe auf die Speichereinrichtung M umfassen.

Die Schnittstelle MI interpretiert Schreibzugriffe auf die Speichereinrichtung M nicht als Zugriff, durch welchen die über den Schreibdatenbus WDATABUS2 übertragenen Daten in das Speichermodul MM zu schreiben sind. Statt dessen interpretiert sie Schreibzugriffe als Kommandos. Genauer gesagt bestimmt sie anhand der über den Adreßbus ADDRBUS2 übertragenen Adressen und der über den Schreibdatenbus WDATABUS2 übertragenen Daten, welche Aktion daraufhin auszuführen ist.

Um im Speichermodul MM Daten zu löschen, wird an die Speichereinrichtung M eine Kommandosequenz übertragen, die ein Kommando "Erase Sector" repräsentiert. Diese Kommandosequenz besteht im betrachteten Beispiel 6 Schreibzyklen, von welchen 5 Zyklen reine fail-safe-Zyklen, d.h. Zyklen mit festen Adressen und Daten sind, und nur in einem Zylus (im betrachteten Beispiel der sechste Zyklus) eine variierbare Adresse und/oder variierbare Daten übertragen werden. Eine solche Kommandosequenz kann beispielsweise darin bestehen, daß

- in einem ersten Zyklus bzw. in einem ersten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten AA,
- in einem zweiten Zyklus bzw. in einem zweiten Schreibzugriff auf die Speichereinrichtung die Adresse AAA8 und die Daten 55,
- in einem dritten Zyklus bzw. in einem dritten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten 80,

- in einem vierten Zyklus bzw. in einem vierten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten AA,
- in einem fünften Zyklus bzw. in einem fünften Schreibzugriff auf die Speichereinrichtung die Adresse AAA8 und die Daten 55, und
- in einem sechsten Zyklus bzw. in einem sechsten Schreibzugriff auf die Speichereinrichtung als Adresse die Adresse des zu löschenden Sektors und die Daten 30,

an die Speichereinrichtung M übertragen werden.

Der Vollständigkeit halber sei angemerkt, daß die Adressen und Daten vorstehend im Hexadezimal-Format angegeben sind, und daß das Löschen von im Speichermodul MM gespeicherten Daten in Einheiten von Sektoren erfolgt, also daß nur immer ein ganzer Sektor gelöscht werden kann. Insbesondere wenn es sich beim Speichermodul MM nicht um einen Flash-Speicher handelt, sondern beispielsweise um ein RAM, ein ROM, ein EEPROM etc., kann das Löschen auch in anderen Einheiten erfolgen, beispielsweise pageweise, wortweise, etc.

Die Steuereinrichtung CTRL decodiert die der Speichereinrichtung M durch Schreibzugriffe zugeführte Kommandosequenz. Genauer gesagt ermittelt sie aus den ihr durch die Schreibzugriffe zugeführten Adressen und Daten die von ihr auszuführende Aktion.

Wenn der Speichereinrichtung M eine des Kommando "Erase Sector" repräsentierende Kommandosequenz zugeführt wird, erkennt sie, daß ein bestimmter Sektor im Speichermodul MM gelöscht werden soll. Sodann überprüft die Steuereinrichtung CTRL, ob es sich hierbei um einen zulässigen Zugriff auf die Speichereinrichtung M handelt. Ein unzulässiger Zugriff liegt insbesondere vor, wenn für den zu löschenden Sektor ein Schreibschutz wirksam ist. Wenn die Steuereinrichtung CTRL feststellt, daß es sich um einen unzulässigen Zugriff auf die Speichereinrichtung M handelt, führt sie diesen Zugriff nicht

aus und signalisiert zudem der CPU und/oder sonstigen Mikrocontroller-Komponenten, daß ein unzulässiger Zugriff auf die Speichereinrichtung M erfolgt ist. Anderenfalls, d.h. wenn es sich um einen zulässigen Zugriff handelt, veranlaßt die Steuereinrichtung CTRL durch Übermittlung entsprechender Steuersignale und Adressen an das Speichermodul MM, daß der im "Erase Sector"-Kommando spezifizierte Sektor im Speichermodul MM gelöscht wird.

Um in das Speichermodul MM Daten zu schreiben, wird im betrachteten Beispiel an die Speichereinrichtung M zunächst eine Kommandosequenz übertragen, die ein Kommando "Enter Page Mode" repräsentiert. Diese Kommandosequenz kann beispielsweise darin bestehen, daß in einem Schreibzugriff auf die Speichereinrichtung M die Adresse 5554 und die Daten 50 an die Speichereinrichtung M übertragen werden.

Wenn der Speichereinrichtung M eine das Kommando "Enter Page Mode" repräsentierende Kommandosequenz zugeführt wird, erkennt sie, daß sie in den Page Mode wechseln muß. Im Page Mode findet ein pageweiser Zugriff auf das Speichermodul MM statt. Eine Page umfaßt im betrachteten Beispiel bei Zugriffen auf den Programmspeicher MMP 256 Bytes, und bei Zugriffen auf den Datenspeicher MMD 128 Bytes.

Der Vollständigkeit halber sei angemerkt, daß die Größen der Pages unabhängig voneinander beliebig groß sein können. Ferner sei angemerkt, daß das "Enter-Page-Mode"-Kommando und auch die im folgenden noch genauer beschriebenen weiteren Page-Kommandos nur vorgesehen werden müssen, wenn das Speichermodul MM pageweise beschrieben wird. Insbesondere wenn das Speichermodul nicht durch einen Flash-Speicher gebildet wird, kann das Beschreiben des Speichermoduls auch in größeren oder kleineren Einheiten, beispielsweise wortweise erfolgen.

Der Wechsel in den Page Mode hat noch kein Einschreiben von Daten in das Speichermodul MM zur Folge. Dies geschieht erst durch ein später noch genauer beschriebenes "Write Page"-Kommando.

Vor der Ausführung dieses Kommandos müssen jedoch erst die in das Speichermodul MM zu schreibenden Daten an die Speichereinrichtung M übertragen werden. Dies geschieht durch ein oder mehrere "Load Page"-Kommandos.

Eine ein "Load Page"-Kommando repräsentierende Kommandosequenz kann beispielsweise darin bestehen, daß in einem Schreibzugriff auf die Speichereinrichtung M die Adresse 5550 und als Daten 32 oder 64 Bits der Daten, die in das Speichermodul MM geschrieben werden sollen, an die Speichereinrichtung M übertragen werden.

Wenn der Speichereinrichtung M eine des Kommando "Load Page" repräsentierende Kommandosequenz zugeführt wird, schreibt die Steuereinrichtung CTRL die in der Kommandosequenz enthaltenen Daten in einen beispielsweise durch ein Register gebildeten Zwischenspeicher der Schnittstelle MI. Darüber hinaus erzeugt die Steuereinrichtung CTRL, genauer gesagt die Fehlerkorrektureinrichtung ECU derselben für diese Daten Fehlerkorrektur- bzw. ECC-Daten, unter Verwendung welcher sich bei einem späteren Auslesen dieser Daten aus dem Speichermodul MM in den ausgelesenen Daten enthaltene Fehler erkennen und/oder beheben lassen, und speichert diese Daten ebenfalls in einem beispielsweise durch ein Register gebildeten Zwischenspeicher.

Der Speichereinrichtung M werden nacheinander so viele "Load Page" repräsentierende Kommandosequenzen zugeführt, bis im Zwischenspeicher so viele Daten gespeichert ist, wie von einer Page umfaßt werden.

Danach wird der Speichereinrichtung M eine ein "Write Page"-Kommando repräsentierende Kommandosequenz zugeführt. Diese Kommandosequenz kann beispielsweise darin bestehen, daß

- in einem ersten Zyklus bzw. in einem ersten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten AA,
- in einem zweiten Zyklus bzw. in einem zweiten Schreibzugriff auf die Speichereinrichtung die Adresse AAA8 und die Daten 55,
- in einem dritten Zyklus bzw. in einem dritten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten A0, und
- in einem vierten Zyklus bzw. in einem vierten Schreibzugriff auf die Speichereinrichtung als Adresse die Adresse der zu beschreibenden Page innerhalb des Speichermoduls, und die Daten AA,

an die Speichereinrichtung übertragen werden.

Zumindest jetzt, d.h. nach dem Empfang eines "Write Page"-Kommandos, eventuell aber auch schon nach dem Empfang eines "Enter Page Mode"-Kommandos und/oder nach dem Empfang eines "Load Page"-Kommandos überprüft die Steuereinrichtung CTRL, ob es sich bei dem betreffenden Zugriff um einen zulässigen Zugriff auf die Speichereinrichtung M handelt. Ein unzulässiger Zugriff liegt insbesondere vor, wenn ein Schreibschutz wirksam ist, durch welchen Veränderungen des Inhalts des zu beschreibenden Speicherbereiches verhindert werden sollen. Wenn die Steuereinrichtung CTRL feststellt, daß es sich um einen unzulässigen Zugriff auf die Speichereinrichtung M handelt, führt sie diesen Zugriff nicht aus und signalisiert zudem der CPU und/oder sonstigen Mikrocontroller-Komponenten, daß ein unzulässiger Zugriff auf die Speichereinrichtung M erfolgt ist. Anderenfalls, d.h. wenn es sich um einen zulässigen Zugriff handelt, veranlaßt die Steuereinrichtung CTRL durch Übermittlung der entsprechenden Steuersignale, Adressen und Daten an das Speichermodul MM, daß die im Zwischenspeicher gespeicherten Daten an die im "Write Page"-

Kommando spezifizierte Stelle innerhalb des Speichermoduls geschrieben werden.

Darüber hinaus werden die zuvor erzeugten Fehlerkorrektur- bzw. ECC-Daten von der Steuereinrichtung CTRL über den Fehlerkorrekturdatenbus ECCBUS1 zum Speichermodul MM übertragen und ebenfalls im Speichermodul MM gespeichert.

Durch die vorstehend beschriebenen Kommandos können nur die Sektoren MMPS1 bis MMPS13 des Programmspeichers MMP und die Sektoren MMDS1 und MMDS2 des Datenspeichers gelöscht und beschrieben werden. Zum Löschen und Beschreiben des Sektors MMPS0 werden zumindest teilweise andere Kommandos benötigt. Diese Kommandos werden später noch genauer beschrieben.

Durch den vorstehend bereits mehrfach erwähnten Leseschutz und Schreibschutz soll und kann verhindert werden, daß in der Speichereinrichtung M gespeicherte Daten durch dazu nicht autorisierte Personen ausgelesen und/oder verändert werden.

Ob und gegebenenfalls in welchem Umfang ein Leseschutz und/oder ein Schreibschutz wirksam ist, hängt unter anderem von durch den Benutzer des Mikrocontrollers vorgenommenen Einstellungen ab. Es sei jedoch bereits an dieser Stelle darauf hingewiesen, daß es auch noch von anderen Faktoren abhängt, ob und in welchem Umfang ein Leseschutz und/oder ein Schreibschutz wirksam ist. Hierauf wird später noch genauer eingegangen.

Die durch den Benutzer vornehmbaren Einstellungen erfolgen

- durch ein entsprechendes Beschreiben von im folgenden als UCBs bezeichneten user configuration blocks,

- durch ein temporäres Aufheben und Wiederinkraftsetzen der in den UCBs enthaltenen Einstellungen, und

- durch ein Setzen und Zurücksetzen bestimmter Bits in Steuerregistern der Speichereinrichtung M.

Die erwähnten UCBs sind Bestandteil des Sektors MMPS0 des Programmspeichers MMP, und können durch den Benutzer der programmgesteuerten Einheit nur beschrieben, aber nicht ausgelesen werden. Der Sektor MMPS0 des Programmspeichers MMP enthält in betrachteten Beispiel drei UCBs, welche im folgenden als UCB0, UCB1, und UCB2 bezeichnet werden. Jeder UCB besteht aus vier Pages (Page 0 bis Page 3), von welchen jede 256 Bytes umfaßt.

Es sei bereits an dieser Stelle darauf hingewiesen, daß auch mehr oder weniger UCBs vorgesehen sein können, und daß die Anzahl und die Größe der Pages, die die UCBs umfassen, unabhängig voneinander beliebig groß sein können.

Der UCB0 kann durch einen ersten Benutzer der programmgesteuerten Einheit beschrieben und gelöscht werden und enthält im betrachteten Beispiel

- Leseschutzeinstellungen, durch welche der erste Benutzer vorgeben kann, ob ein Leseschutz wirksam sein soll,
- Schreibschutzeinstellungen, durch welche der erste Benutzer vorgegeben kann, für welche Teile des Speichermoduls MM ein Schreibschutz wirksam sein soll,
- ein vom ersten Benutzer wählbares Kennwort, unter Verwendung dessen der erste Benutzer den durch seine Leseschutzeinstellungen definierten Leseschutz und/oder den durch seine Schreibschutzeinstellungen definierten Schreibschutz temporär aufheben kann, und
- einen vorgegebenen Confirmation Code, durch dessen Einschreiben in den UCB0 der erste Benutzer die Gültigkeit der im UCB0 gespeicherten Daten bestätigt.

Die Leseschutzeinstellungen und die Schreibschutzeinstellungen umfassen im betrachteten Beispiel zwei Bytes. Diese Bytes

werden im folgenden als Schutzeinstellungs-Bytes bezeichnet und sind in Figur 2 dargestellt.

Die Bits 0 bis 12 der Schutzeinstellungs-Bytes sind Schreibschutzeinstellungs-Bits, durch welche spezifiziert wird, für welche der Sektoren MMPS1 bis MMPS13 des Programmspeichers ein Schreibschutz wirksam sein soll; die Schreibschutzeinstellungs-Bits sind in der Figur 2 mit den Bezugszeichen S0L bis S12L bezeichnet. Von den Bits S0L bis S12L ist jeweils ein Bit einem der Sektoren MMPS1 bis MMPS13 zugeordnet. Genauer gesagt ist das Bit S0L dem Sektor MMPS1 zugeordnet, das Bit S1L dem Sektor MMPS2 zugeordnet, das Bit S2L dem Sektor MMPS3 zugeordnet,..., und das Bit S12L dem Sektor MMPS13 zugeordnet. Durch den Wert der einzelnen Bits S0L bis S12L wird festgelegt, ob für den zugeordneten Sektor ein Schreibschutz wirksam sein soll oder nicht. Wenn beispielsweise das Bit S5L den Wert 1 aufweist, bedeutet dies, daß für den zugeordneten Sektor MMPS6 ein Schreibschutz wirksam sein soll; wenn dieses Bit den Wert 0 aufweist, bedeutet dies, daß für den zugeordneten Sektor MMPS6 kein Schreibschutz wirksam sein soll.

Das Bit 15 der Schutzeinstellungs-Bytes ist ein Leseschutzeinstellungs-Bit, durch welches spezifiziert wird, ob für das Speichermodul MM ein Leseschutz wirksam sein soll; das Leseschutzeinstellungs-Bit ist in der Figur 2 mit dem Bezugszeichen RPRO bezeichnet. Wenn das Bit RPRO den Wert 1 aufweist, bedeutet dies, daß ein Leseschutz wirksam sein soll; wenn das Bit RPRO den Wert 0 aufweist, bedeutet dies, daß kein Leseschutz wirksam sein soll.

Das Kennwort umfaßt im betrachteten Beispiel 64 Bits, kann aber auch beliebig länger oder kürzer sein.

Im betrachteten Beispiel ist es so, daß die Schutzeinstellungs-Bytes und das Kennwort Bestandteil der ersten Page (Page 0) von UCB0 sind, der Confirmation Code Bestandteil der

dritten Page (Page 2) von UCB0 ist, und die restlichen Pages (Pages 1 und 3) von UCB0 für zukünftige Verwendungen reserviert sind.

Der UCB1 kann durch einen zweiten Benutzer der programmgesteuerten Einheit beschrieben und gelöscht werden und enthält im betrachteten Beispiel

- Schreibschutzeinstellungen, durch welche der zweite Benutzer vorgeben kann, für welche Bereiche des Speichermoduls MM ein Schreibschutz wirksam sein soll,
- ein vom zweiten Benutzer wählbares Kennwort, unter Verwendung dessen der zweite Benutzer den durch seine Schreibschutzeinstellungen definierten Schreibschutz temporär aufheben kann, und
- einen vorgegebenen Confirmation Code, durch dessen Einschreiben der zweite Benutzer die Gültigkeit der im UCB1 gespeicherten Daten bestätigt.

Die Schreibschutzeinstellungen sind wie beim UCB0 in zwei Schutzeinstellungs-Bytes enthalten. Diese Schutzeinstellungs-Bytes sind in Figur 3 veranschaulicht.

Die Schutzeinstellungs-Bytes des UCB1 entsprechen weitestgehend den Schutzeinstellungs-Bytes des UCB0. Einziger Unterschied ist, daß in den Schutzeinstellungs-Bytes des UCB1 kein Leseschutzeinstellungs-Bit RPRO vorgesehen ist. Dies hat den Effekt, daß der zweite Benutzer nicht bestimmen kann, ob ein Leseschutz wirksam sein soll oder nicht; dies kann nur der erste Benutzer tun.

Die Schutzeinstellungs-Bytes des UCB1 enthalten aber wie die Schutzeinstellungs-Bytes des UCB0 Schreibschutzeinstellungs-Bits S0L bis S12L, über welche der zweite Benutzer einstellen kann, für welche der Sektoren MMPS1 bis MMPS13 ein Schreibschutz wirksam sein soll.

Das Kennwort umfaßt im betrachteten Beispiel 64 Bits, kann aber auch beliebig länger oder kürzer sein.

Im betrachteten Beispiel ist es so, daß die Schutzeinstellungs-Bytes und das Kennwort Bestandteil der ersten Page (Page 0) von UCB1 sind, der Confirmation Code Bestandteil der dritten Page (Page 2) von UCB1 ist, und die restlichen Pages (Pages 1 und 3) von UCB1 für zukünftige Verwendungen reserviert sind.

Der UCB2 weist gegenüber dem UCB0 und dem UCB1 einige Besonderheiten auf und wird später genauer beschrieben.

Durch Einschreiben entsprechender Daten in die Schutzeinstellungs-Bytes des UCB0 und des UCB1 kann durch den bzw. die Benutzer des Mikrocontrollers eingestellt werden, ob bzw. im welchem Umfang ein Leseschutz und/oder ein Schreibschutz wirksam sein soll.

Wenn ein Leseschutz wirksam sein soll, muß der erste Benutzer des Mikrocontrollers das Leseschutzeinstellungs-Bit RPRO der Schutzeinstellungs-Bytes des UCB0 setzen.

Im betrachteten Beispiel wird durch Setzen des Leseschutzeinstellungs-Bits RPRO des UCB0 eingestellt, daß aus dem gesamten Speichermodul MM keine Daten ausgelesen werden können sollen. Der Vollständigkeit halber sei angemerkt, daß es ohne Probleme möglich wäre, Einstellmöglichkeiten in UCB0 vorzusehen, durch welche eingestellt werden kann, daß nur für bestimmte Bereiche des Speichermoduls MM ein Leseschutz wirksam sein soll. Dies ließe sich beispielsweise dadurch bewerkstelligen, daß in den Schutzeinstellungs-Bytes von UCB0 zusätzliche Leseschutzeinstellungs-Bits vorgesehen werden und die dann vorhandenen Leseschutzeinstellungs-Bits ähnlich wie die Schreibschutzeinstellungs-Bits bestimmten Bereichen des Speichermoduls MM zugeordnet werden. Dann wäre durch die Leseschutzeinstellungs-Bits einstellbar, für welche Bereiche

des Speichermoduls MM ein Leseschutz wirksam sein soll. Darüber hinaus wäre es selbstverständlich auch möglich, daß sowohl der UCB0 als auch der UCB1 ein oder mehrere Leseschutzeinstellungs-Bits enthalten. Dann könnten sowohl der erste Benutzer als auch der zweite Benutzer einstellen, ob und gegebenenfalls für welche Bereiche des Speichermoduls MM ein Leseschutz wirksam sein soll. Natürlich wäre es auch möglich, daß nur der zweite Benutzer durch entsprechende Einstellungen in UCB1 vorgeben kann, ob und gegebenenfalls in welchem Umfang ein Leseschutz wirksam sein soll.

Wenn ein Schreibschutz wirksam sein soll, müssen der erste Benutzer des Mikrocontrollers und/oder der zweite Benutzer des Mikrocontrollers eines oder mehrere der Schreibschutzeinstellungs-Bits S0L bis S12L der Schutzeinstellungs-Bytes des UCB0 bzw. des UCB1 setzen.

Im betrachteten Beispiel wird durch die Schreibschutzeinstellungs-Bits S0L bis S12L von UCB0 und UCB1 eingestellt, für welche Bereiche des Speichermoduls MM, genauer gesagt für welche Sektoren des Speichermoduls ein Schreibschutz wirksam sein soll. Ein Schreibschutz ist jeweils nur für diejenigen Sektoren wirksam, welchen die gesetzten Bits unter den Schreibschutzeinstellungs-Bits S0L bis S12L zugeordnet sind. Wenn von den Schreibschutzeinstellungs-Bits S0L bis S12L des UCB0 und des UCB1 beispielsweise nur das Schreibschutzeinstellungs-Bit S3L des UCB0 und das Schreibschutzeinstellungs-Bit S5L des UCB1 gesetzt sind, bedeutet dies, daß nur für die Sektoren MMPS4 und MMPS6 ein Schreibschutz wirksam sein soll.

Der vorstehend bereits erwähnte UCB2 kann durch einen dritten Benutzer der programmgesteuerten Einheit beschrieben werden und enthält im betrachteten Beispiel

- Schreibschutzeinstellungen, durch welche der dritte Benutzer vorgeben kann, welche Bereiche des Speichermoduls MM sich wie ein ROM verhalten sollen, und

- einen vorgegebenen Confirmation Code, durch dessen Einschreiben der dritte Benutzer die Gültigkeit der im UCB2 gespeicherten Daten bestätigt.

Die Schreibschutzeinstellungen sind wie beim UCB0 und beim UCB1 in zwei Schutzeinstellungs-Bytes enthalten. Diese Schutzeinstellungs-Bytes sind in Figur 4 veranschaulicht.

Die Bits 0 bis 12 der Schutzeinstellungs-Bytes sind Schreibschutzeinstellungs-Bits, durch welche spezifiziert wird, für welche der Sektoren MMPS1 bis MMPS13 des Programmspeichers ein Schreibschutz wirksam sein soll; die Schreibschutzeinstellungs-Bits sind in der Figur 4 mit den Bezugszeichen S0ROM bis S12ROM bezeichnet. Von den Bits S0ROM bis S12ROM ist jeweils ein Bit einem der Sektoren MMPS1 bis MMPS13 zugeordnet. Genauer gesagt ist das Bit S0ROM dem Sektor MMPS1 zugeordnet, das Bit S1ROM dem Sektor MMPS2 zugeordnet, das Bit S2ROM dem Sektor MMPS3 zugeordnet,..., und das Bit S12ROM dem Sektor MMPS13 zugeordnet. Durch den Wert der einzelnen Bits S0ROM bis S12ROM wird festgelegt, ob für den zugeordneten Sektor ein Schreibschutz wirksam sein soll oder nicht. Wenn beispielsweise das Bit S5ROM den Wert 1 aufweist, bedeutet dies, daß für den zugeordneten Sektor MMPS6 ein Schreibschutz wirksam sein soll; wenn dieses Bit den Wert 0 aufweist, bedeutet dies, daß für den zugeordneten Sektor MMPS6 kein Schreibschutz wirksam sein soll.

Insoweit entsprechen die Schutzeinstellungs-Bytes des UCB2 im wesentlichen den Schutzeinstellungs-Bytes des UCB1. Im Gegensatz zu UCB0 und UCB1 ist der UCB2 nach dem Einschreiben des Confirmation Codes jedoch nicht mehr löschbar und nicht mehr wiederbeschreibbar. Ferner kann - ebenfalls im Gegensatz zu UCB0 und UCB1 - der durch UCB2 definierte Schreibschutz nicht temporär deaktiviert werden. Dies hat den Effekt, daß durch die Schreibschutzeinstellungs-Bits des UCB2 vorgegeben wird, ob und gegebenenfalls welche Bereiche des Speichermoduls MM sich wie ein nie mehr umprogrammierbarer Speicher, also wie

ein ROM verhalten. Der UCB2 verhält sich nach dem Einschreiben des Confirmation Code in diesen wie ein zumindest durch den Benutzer nicht lesbares ROM.

Im betrachteten Beispiel ist es so, daß die Schutzeinstellungs-Bytes Bestandteil der ersten Page (Page 0) von UCB2 sind, der Confirmation Code Bestandteil der dritten Page (Page 2) von UCB2 ist, und die restlichen Pages (Pages 1 und 3) von UCB2 für zukünftige Verwendungen reserviert sind.

Die UCBs können durch den ersten bzw. den zweiten bzw. den dritten Benutzer durch die Übermittlung spezieller Kommandosequenzen an die Speichereinrichtung M beschrieben werden.

Die UCBs können - ebenfalls durch die Übermittlung spezieller Kommandosequenzen - auch wieder gelöscht und erneut beschrieben werden. Sie können jedoch durch den Benutzer der programmgesteuerten Einheit nicht ausgelesen werden.

Der UCB2 kann allerdings nach dem Einschreiben des Confirmation Code in den UCB2 nicht mehr gelöscht und nicht mehr beschrieben werden.

Um einen UCB zu löschen, muß zunächst durch das vorstehend bereits erwähnte und später noch genauer beschriebene Kommando "Disable Write Protection" der Schreibschutz für den zu löschenden UCB aufgehoben werden, denn obgleich dem die UCBs enthaltenden Sektor MMPS0 kein Schreibschutzeinstellungs-Bit in den UCBs zugeordnet ist, ist jeder ordnungsgemäß, d.h. einschließlich des richtigen Confirmation Codes beschriebene UCB automatisch lese- und schreibgeschützt. Nur wenn der zu löschende UCB noch nicht oder nicht ordnungsgemäß, d.h. ohne gültigen Confirmation Code beschrieben wurde, ist keine Aufhebung des Schreibschutzes erforderlich.

Zum eigentlichen Löschen eines UCB wird an die Speichereinrichtung M eine Kommandosequenz übertragen, die ein Kommando "Erase UCB" repräsentiert. Diese Kommandosequenz kann beispielsweise darin bestehen, daß

- in einem ersten Zyklus bzw. in einem ersten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten AA,
- in einem zweiten Zyklus bzw. in einem zweiten Schreibzugriff auf die Speichereinrichtung die Adresse AAA8 und die Daten 55,
- in einem dritten Zyklus bzw. in einem dritten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten 80,
- in einem vierten Zyklus bzw. in einem vierten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten AA,
- in einem fünften Zyklus bzw. in einem fünften Schreibzugriff auf die Speichereinrichtung die Adresse AAA8 und die Daten 55, und
- in einem sechsten Zyklus bzw. in einem sechsten Schreibzugriff auf die Speichereinrichtung als Adresse die Adresse des zu löschenden UCB und die Daten 40,

an die Speichereinrichtung übertragen werden.

Wenn der Speichereinrichtung M eine das Kommando "Erase UCB" repräsentierende Kommandosequenz zugeführt wird, erkennt sie, genauer gesagt die Steuereinrichtung CTRL derselben, daß der im sechsten Zyklus der Kommandosequenz spezifizierte UCB gelöscht werden soll. Die Steuereinrichtung CTRL überprüft sodann, ob es hierbei um einen zulässigen Zugriff handelt. Ein unzulässiger Zugriff liegt insbesondere vor, wenn der zu löschende UCB schreibgeschützt ist. Wenn die Steuereinrichtung feststellt, daß ein unzulässiger Zugriff vorliegt, führt sie das Kommando nicht aus und signalisiert zudem der CPU und/oder sonstigen Mikrocontroller-Komponenten, daß ein unzulässiger Zugriff auf die Speichereinrichtung erfolgt ist. Anderenfalls, d.h. wenn es sich um einen zulässigen Zugriff

handelt, veranlaßt die Steuereinrichtung CTRL durch Übermittlung entsprechender Steuersignale und Adressen an das Speichermodul MM, daß der im "Erase UCB"-Kommando spezifizierte UCB im Sektor MMPS0 des Speichermoduls MM gelöscht wird. Anders als beim eingangs beschriebenen Kommando "Erase Sector" wird durch das Kommando "Erase UCB" nicht das Löschen eines kompletten Sektors des Speichermoduls MM, sondern nur eines bestimmten UCB des Sektors MMPS0 veranlaßt.

Um in einen UCB Daten zu schreiben, wird an die Speichereinrichtung M zunächst ein "Enter Page Mode"-Kommando, dann ein oder mehrere "Load Page"-Kommandos, und schließlich ein "Write UC Page"-Kommando übertragen.

Das Beschreiben eines UCB ist nur zulässig, wenn dieser noch nie beschrieben wurde oder zuvor gelöscht wurde. Ob dies der Fall ist, wird von der Steuereinrichtung CTRL überprüft und kann beispielsweise daran erkannt werden, daß im zu beschreibenden UCB kein oder kein gültiger Confirmation Code steht.

Die das "Enter Page Mode"-Kommando und das "Load Page"-Kommando repräsentierenden Kommandosequenzen sowie die Reaktion der Steuereinrichtung CTRL auf diese Kommandos wurden bereits eingangs beschrieben.

Die das "Write UC Page"-Kommando repräsentierende Kommandosequenz kann beispielsweise darin bestehen, daß

- in einem ersten Zyklus bzw. in einem ersten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten AA,
- in einem zweiten Zyklus bzw. in einem zweiten Schreibzugriff auf die Speichereinrichtung die Adresse AAA8 und die Daten 55,
- in einem dritten Zyklus bzw. in einem dritten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten 00, und

- in einem vierten Zyklus bzw. in einem vierten Schreibzugriff auf die Speichereinrichtung als Adresse die Adresse der zu beschreibenden Page des zu beschreibenden UCB und die Daten 90,

an die Speichereinrichtung übertragen werden.

Wenn die Speichereinrichtung M ein "Write UC Page"-Kommando zugeführt bekommt, überprüft die Steuereinrichtung CTRL, ob es sich bei dem betreffenden Zugriff um einen zulässigen Zugriff auf die Speichereinrichtung M handelt. Ein unzulässiger Zugriff liegt insbesondere vor, wenn der zu beschreibende UCB bereits einen gültigen Confirmation Code enthält, also schreibgeschützt ist. Wenn die Steuereinrichtung CTRL feststellt, daß es sich um einen unzulässigen Zugriff auf die Speichereinrichtung M handelt, führt sie diesen Zugriff nicht aus und signalisiert zudem der CPU und/oder sonstigen Mikrocontroller-Komponenten, daß ein unzulässiger Zugriff auf die Speichereinrichtung M erfolgt ist. Anderenfalls, d.h. wenn es sich um einen zulässigen Zugriff handelt, veranlaßt die Steuereinrichtung CTRL durch Übermittlung der entsprechenden Steuersignale, Adressen und Daten an das Speichermodul MM, daß die der Speichereinrichtung M durch das "Load Page"-Kommando zugeführten und zwischengespeicherten Daten an die im "Write UC Page"-Kommando spezifizierte Page des zu beschreibenden UCB geschrieben werden.

Die Einträge in UCB0, UCB1, und UCB2 werden nur wirksam, wenn der jeweilige Confirmation Code in die UCBs geschrieben wurde. Durch ein Löschen oder Beschreiben der UCBs erfolgte Veränderungen des Inhalts der UCBs entfalten jedoch erst ab dem nächsten Rücksetzen des Mikrocontrollers Wirkung.

Der Confirmation Code sollte erst in den jeweiligen UCB geschrieben werden, wenn sicher ist, daß die darin gespeicherten Informationen richtig sind. Insbesondere sollte sicher sein, daß das im jeweiligen UCB gespeicherte Kennwort auch das Kennworte ist, das der Benutzer in den UCB schreiben

wollte. Dies kann beispielsweise durch das später noch genauer beschriebene Kommando "Disable Write Protection" ermittelt werden. Die Übermittlung eines "Disable Write Protection"-Kommandos an die Speichereinrichtung M hat eine Fehlermeldung zur Folge, wenn das im Kommando enthaltene Kennwort nicht mit dem im UCB gespeicherten Kennworte übereinstimmt. Übermittelt der den UCB beschreibende Benutzer an die Speichereinrichtung M ein "Disable Write Protection"-Kommando, welches das soeben in den UCB geschriebene Kennwort als Kennwort enthält, so kann am Auftreten oder Ausbleiben dieser Fehlermeldung erkannt werden, ob das im UCB gespeicherte Kennwort das vom Benutzer festgelegte Kennwort ist oder nicht.

Der UCB0 und der UCB1 können durch den ersten Benutzer bzw. den zweiten Benutzer des Mikrocontrollers beliebig oft beschrieben und gelöscht werden. Es könnte auch vorgesehen werden, das Löschen und Wiederbeschreiben von UCB0 und UCB1 nur eine bestimmte Anzahl von Malen zuzulassen. Beispielsweise könnte vorgesehen werden, daß der UCB0 und der UCB1 maximal fünf mal beschreibbar sind.

Der erste Benutzer und der zweite Benutzer des Mikrocontrollers haben die Möglichkeit, die in UCB0 bzw. in UCB1 enthaltenen Einstellungen durch Übertragung entsprechender Kommandos, genauer gesagt durch Übertragung von diese Kommandos repräsentierenden Kommandosequenzen an die Speichereinrichtung M vorübergehend außer Kraft zu setzen. Dadurch kann durch den ersten Benutzer der von ihm in UCB0 eingestellte Lese- und Schreibschutz bzw. durch den zweiten Benutzer der von ihm in UCB1 eingestellte Schreibschutz temporär aufgehoben werden.

Die erwähnten Kommandos umfassen im betrachteten Beispiel ein Kommando "Disable Write Protection", ein Kommando "Disable Read Protection", und ein Kommando "Resume Protection".

Eine ein "Disable Write Protection"-Kommando repräsentierende Kommandosequenz kann beispielsweise darin bestehen, daß

- in einem ersten Zyklus bzw. in einem ersten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten AA,
- in einem zweiten Zyklus bzw. in einem zweiten Schreibzugriff auf die Speichereinrichtung die Adresse AAA8 und die Daten 55,
- in einem dritten Zyklus bzw. in einem dritten Schreibzugriff auf die Speichereinrichtung die Adresse 1111 und als Daten eine Kennung, die dem das Kommando veranlassenden Benutzer zugeordnet ist,
- in einem vierten Zyklus bzw. in einem vierten Schreibzugriff auf die Speichereinrichtung die Adresse 1112 und als Daten eine erste Hälfte des Kennwortes, das in dem UCB gespeichert ist, der dem im dritten Zyklus spezifizierten Benutzer zugeordnet ist,
- in einem fünften Zyklus bzw. in einem fünften Schreibzugriff auf die Speichereinrichtung die Adresse 1112 und als Daten die zweite Hälfte des Kennwortes, das in dem UCB gespeichert ist, der dem im dritten Zyklus spezifizierten Benutzer zugeordnet ist, und
- in einem sechsten Zyklus bzw. in einem sechsten Schreibzugriff auf die Speichereinrichtung die Adresse 3333 und die Daten 01,

an die Speichereinrichtung übertragen werden.

Wenn der Speichereinrichtung M eine des Kommando "Disable Write Protection" repräsentierende Kommandosequenz zugeführt wird, überprüft sie, genauer gesagt die Steuereinrichtung CTRL derselben, zunächst, ob die im dritten Zyklus übertragene Kennung die dem ersten Benutzer oder die dem zweiten Benutzer zugeordnete Kennung ist, und ob das im vierten Zyklus und im fünften Zyklus übertragene Kennwort das Kennwort ist, das in dem dem betreffenden Benutzer zugeordneten UCB gespeichert ist. Das Kennwort muß mit den in UCB0 gespeicherten Kennwort übereinstimmen, wenn die im dritten Zyklus übertra-

gene Kennung die dem ersten Benutzer zugeordnete Kennung ist, bzw. muß mit dem in UCB1 gespeicherten Kennwort übereinstimmen, wenn die im dritten Zyklus übertragene Kennung die dem zweiten Benutzer zugeordnete Kennung ist. Wenn die Überprüfung ergibt, daß die genannten Bedingungen nicht erfüllt sind, geht die Steuereinrichtung CTRL davon aus, daß es sich bei dem ihr zugeführten Kommando um einen unzulässigen Zugriff (um einen Zugriff durch eine dazu nicht autorisierte Person) auf die Speichereinrichtung M handelt. In diesem Fall führt die Steuereinrichtung CTRL das Kommando nicht aus und signalisiert zudem der CPU und/oder sonstigen Mikrocontroller-Komponenten, daß ein unzulässiger Zugriff auf die Speichereinrichtung M erfolgt ist. Anderenfalls sorgt die Steuereinrichtung CTRL dafür, daß der Schreibschutz in dem Umfang, in welchen ihn der im dritten Zyklus der Kommandosequenz spezifizierte Benutzer in dem ihm zugeordneten UCB festgelegt hat, unwirksam wird.

In welchem Umfang der Schreibschutz unwirksam wird, hängt im betrachteten Beispiel zusätzlich davon ab, von welchem Benutzer das "Disable Write Protection"-Kommando stammt. Genauer gesagt ist es im betrachteten Beispiel so, daß die Einstellungen und Kommandos des ersten Benutzers Vorrang haben. D.h., durch ein vom zweiten Benutzer veranlaßtes "Disable Write Protection"-Kommando kann der Schreibschutz nur für diejenigen Sektoren aufgehoben werden, für die der erste Benutzer keinen Schreibschutz begehrt. D.h., wenn beispielsweise in UCB0 die Schreibschutzeinstellungs-Bits S0L und S1L gesetzt sind, und in UCB1 die Schreibschutzeinstellungs-Bits S0L und S2L, so wird durch ein vom zweiten Benutzer veranlaßtes "Disable Write Protection"-Kommando nur der Schreibschutz für den Sektor MMPS3 aufgehoben, nicht aber auch der Schreibschutz für den Sektor MMPS1, denn für diesen Sektor hat auch der erste Benutzer einen Schreibschutz eingestellt. Umgekehrt kann aber der erste Benutzer den Schreibschutz auch für solche Sektoren aufheben, für die der zweite Benutzer einen Schreibschutz eingestellt hat. D.h. wenn beispielsweise

in UCB0 die Schreibschutzeinstellungs-Bits S0L und S1L gesetzt sind, und in UCB1 die Schreibschutzeinstellungs-Bits S0L und S2L, so wird durch ein vom ersten Benutzer veranlaßtes "Disable Write Protection"-Kommando der Schreibschutz für die Sektor MMPS1, MMPS2 und MMPS3 aufgehoben.

Es dürfte einleuchten, daß auch der umgekehrte Fall möglich ist, d.h. daß die Einstellungen und Kommandos des zweiten Benutzers Vorrang haben.

Ferner ist es auch möglich, daß der erste Benutzer und der zweite Benutzer gleichberechtigt sind, und kein Benutzer den Schreibschutz für Sektoren aufheben kann, für die der jeweils andere Benutzer einen Schreibschutz eingestellt hat.

Es wäre auch denkbar, eine Einstellmöglichkeit vorzusehen, durch welche einstellbar ist, welche Wirkung ein "Disable Write Protection"-Kommando der jeweiligen Benutzer hat. Beispielsweise könnte vorgesehen werden, daß die jeweiligen Benutzer einstellen können, ob und gegebenenfalls in welchem Umfang (für welche Sektoren) der jeweils andere Benutzer den Schreibschutz aufheben kann.

Unabhängig hiervon hat ein "Disable Write Protection"-Kommando auf keinen Fall zur Folge, daß der Schreibschutz für einen Sektor aufgehoben wird, der sich gemäß den Einstellungen in UCB2 wie ein ROM verhalten soll.

Eine ein "Disable Read Protection"-Kommando repräsentierende Kommandosequenz kann beispielsweise darin bestehen, daß

- in einem ersten Zyklus bzw. in einem ersten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten AA,
- in einem zweiten Zyklus bzw. in einem zweiten Schreibzugriff auf die Speichereinrichtung die Adresse AAA8 und die Daten 55,

- in einem dritten Zyklus bzw. in einem dritten Schreibzugriff auf die Speichereinrichtung die Adresse 1111 und die Daten 00,
- in einem vierten Zyklus bzw. in einem vierten Schreibzugriff auf die Speichereinrichtung die Adresse 1112 als Daten die erste Hälfte des Kennwortes, das in UCB0 gespeichert ist,
- in einem fünften Zyklus bzw. in einem fünften Schreibzugriff auf die Speichereinrichtung die Adresse 1112 als Daten die zweite Hälfte des Kennwortes, das in UCB0 gespeichert ist, und
- in einem sechsten Zyklus bzw. in einem sechsten Schreibzugriff auf die Speichereinrichtung die Adresse 3333 und die Daten 02,

an die Speichereinrichtung übertragen werden.

Wenn der Speichereinrichtung M eine das Kommando "Disable Read Protection" repräsentierende Kommandosequenz zugeführt wird, überprüft sie, genauer gesagt die Steuereinrichtung CTRL derselben zunächst, ob das im vierten und im fünften Zyklus übertragene Kennwort mit dem in UCB0 gespeicherten Kennwort übereinstimmt. Wenn die Überprüfung ergibt, daß diese Bedingungen nicht erfüllt ist, geht die Steuereinrichtung CTRL davon aus, daß es sich bei dem ihr zugeführten Kommando um einen unzulässigen Zugriff (um einen Zugriff durch eine dazu nicht autorisierte Person) auf die Speichereinrichtung M handelt. In diesem Fall führt die Steuereinrichtung CTRL das Kommando nicht aus und signalisiert zudem der CPU und/oder sonstigen Mikrocontroller-Komponenten, daß ein unzulässiger Zugriff auf die Speichereinrichtung M erfolgt ist. Anderenfalls sorgt die Steuereinrichtung CTRL dafür, daß kein Leseschutz mehr wirksam ist.

Eine ein "Resume Protection"-Kommando repräsentierende Kommandosequenz kann beispielsweise darin bestehen, daß in einem einzigen Zyklus bzw. in einem einzigen Schreibzugriff

auf die Speichereinrichtung die Adresse 5554 und die Daten BB an die Speichereinrichtung M übertragen werden.

Wenn der Speichereinrichtung M eine des Kommando "Resume Protection" repräsentierende Kommandosequenz zugeführt wird, werden der Leseschutz und der Schreibschutz in dem Umfang, in welchem er durch die Lese- und Schreibschutzeinstellungs-Bits des UCB0 und des UCB1 festgelegt ist, wieder wirksam.

Die Kommandos "Disable Read Protection", "Disable Write Protection", und "Resume Protection" entfalten jeweils sofort, also nicht etwa erst nach dem nächsten Rücksetzen des Mikrocontrollers oder einem sonstigen späteren Zeitpunkt Wirkung.

Ob und gegebenenfalls in welchem Umfang ein Leseschutz und/oder ein Schreibschutz wirksam ist, hängt auch noch vom Inhalt eines Speicher-Konfigurationsregisters ab. Dieses Speicher-Konfigurationsregister ist im betrachteten Beispiel Bestandteil der Steuereinrichtung CTRL der Speichereinrichtung M. Der Aufbau des Speicher-Konfigurationsregisters ist in Figur 5 veranschaulicht.

Wie aus der Figur 5 ersichtlich ist, handelt es sich beim Speicher-Konfigurationsregister um ein 32-Bit-Register, von welchem vorliegend jedoch nur die Bits 0 bis 5 interessieren.

Bit 0 ist mit dem Bezugszeichen RPA bezeichnet, Bit 1 mit dem Bezugszeichen DCF, Bit 2 mit dem Bezugszeichen DDF, Bit 3 mit dem Bezugszeichen DDFDBG, Bit 4 mit dem Bezugszeichen DDFDMA, und Bit 5 mit dem Bezugszeichen DDFPCP.

Durch das Bit RPA wird angegeben, ob ein Leseschutz wirksam sein soll. Ein Leseschutz ist wirksam und das Bit RPA ist gesetzt, wenn das Bit RPRO in UCB0 gesetzt ist, und der Leseschutz nicht durch durch das Kommando "Disable Read Protection" temporär aufgehoben ist.

Durch die Bits DCF und DDF wird festgelegt, welche Art von Lesezugriffen auf das Speichermodul MM zulässig sein sollen, und durch die Bits DDFDBG, DDFDMA, und DDFPCP und/oder weitere oder andere Steuerbits wird festgelegt, welche Mikrocontroller-Komponenten, die auf die Speichereinrichtung M zugreifen können, zulässige Lesezugriffe auf die Speichereinrichtung M ausführen können. Die Bits DCF und DDF werden allerdings nur ausgewertet, wenn Bit RPA gesetzt ist. Genauer gesagt ist es so,

- daß es von den Werten der Bits RPA (Read Protection Active) und DCF (Disable Code Fetch) abhängt, ob Code Fetches, also Lesezugriffe der CPU des Mikrocontrollers auf von der CPU als Befehlscode verwendete Daten zulässig sind; wenn das Bit RPA gesetzt ist und das Bit DCF den Wert 0 hat, sind Code Fetches zulässig, anderenfalls nicht.

- daß es von den Werten der Bits RPA (Read Protection Active) und DDF (Disable Data Fetch) abhängt, ob Data Fetches, also Lesezugriffe der CPU des Mikrocontrollers auf nicht als Befehlscode verwendete Daten zulässig sind; wenn das Bit RPA gesetzt ist und das Bit DDF den Wert 0 hat, sind Data Fetches zulässig, anderenfalls nicht.

- daß es vom Wert des Bits DDFDBG (Disable Data Fetch from Debug Controller) abhängt, ob ein im Mikrocontroller enthaltener Debug Controller, also beispielsweise das eingangs bereits erwähnte OCDS-Modul, Lesezugriffe auf das Speichermodul MM (den Programmspeicher MMP und den Datenspeicher MMD) ausführen darf; wenn das Bit DDFDBG den Wert 0 hat, sind Lesezugriffe durch den Debug Controller auf das Speichermodul MM zulässig, anderenfalls nicht.

- daß es vom Wert des Bits DDFDMA (Disable Data Fetch from DMA Controller) abhängt, ob ein im Mikrocontroller enthaltener DMA-Controller Lesezugriffe auf das Speichermodul MM (den Programmspeicher MMP und den Datenspeicher MMD) aus-

führen darf; wenn das Bit DDFDBG den Wert 0 hat, sind Lesezugriffe durch den DMA-Controller auf das Speichermodul MM zulässig, anderenfalls nicht.

- daß es vom Wert des Bit DDFPCP (Disable Data Fetch from PCP) abhängt, ob ein im Mikrocontroller enthaltener PCP (Peripheral Control Processor) Lesezugriffe auf das Speichermodul MM (den Programmspeicher MMP und den Datenspeicher MMD) ausführen darf; wenn das Bit DDFDBG den Wert 0 hat, sind Lesezugriffe durch den DMA-Controller auf das Speichermodul MM zulässig, anderenfalls nicht.

Es können selbstverständlich auch noch weitere Konfigurations-Bits vorgesehen sein, von deren Wert es jeweils abhängt, ob eine bestimmte weitere Komponente des Mikrocontrollers oder des den Mikrocontroller enthaltenden Systems Lesezugriffe auf das Speichermodul MM (den Programmspeicher MMP und den Datenspeicher MMD) ausführen darf. Beispielsweise können weitere Konfigurations-Bits vorgesehen sein, von deren Wert es abhängt, ob weitere Prozessoren des Mikrocontrollers, oder außerhalb des Mikrocontrollers vorgesehene Prozessoren Lesezugriffe auf das Speichermodul MM durchführen dürfen.

Welche Mikrocontroller-Komponente auf das Speichermodul MM zugreift, und ob es sich bei dem Zugriff um einen Code Fetch oder um einen Data Fetch handelt, kann anhand eines Identifiers ermittelt werden, den die auf das Speichermodul MM zugreifende Mikrocontroller-Komponente bei einem Zugriff auf das Speichermodul MM zusammen mit der Leseanforderung bzw. der Schreibanforderung an das Speichermodul MM oder die Speichereinrichtung M übermittelt.

Das Speicher-Konfigurationsregister kann sowohl durch die Hardware, insbesondere durch die Steuereinrichtung CTRL oder eine sonstige Mikrocontroller-Komponente, als auch durch den Benutzer des Mikrocontrollers ausgelesen und beschrieben werden.

Das Beschreiben des Speicher-Konfigurationsregisters durch den Benutzer des Mikrocontrollers erfolgt im betrachteten Beispiel durch die Übermittlung eines Kommandos "Write Register" an die Speichereinrichtung M, genauer gesagt durch die Zuführung einer dieses Kommando repräsentierenden Kommandosequenzen. Es sei jedoch bereits an dieser Stelle darauf hingewiesen, daß das Beschreiben des Speicher-Konfigurationsregisters auch auf andere Art und Weise, beispielsweise durch einen einfachen Registerzugriff erfolgen könnte.

Durch das Kommando "Write Register" kann der Benutzer jedoch nur bestimmte Bits des Speicher-Konfigurationsregisters verändern, wobei selbst dies teilweise auch noch an bestimmte Bedingungen geknüpft ist. Insbesondere ist es nicht möglich, daß der Benutzer durch das Kommando "Write Register" das Bit RPA verändert. Das Beschreiben dieses Bits kann nur durch die Steuereinrichtung CTRL erfolgen. Ferner ist es nicht möglich, durch das Kommando "Write Register" die Fetch Control Bits DCF und DDF zu verändern, wenn das Bit RPA gesetzt ist; vor einer Veränderung der Bits DCF und DDF muß gegebenenfalls erst durch das Kommando "Disable Read Protection" der Leseschutz aufgehoben werden. Es könnte sich jedoch unter Umständen als vorteilhaft erweisen, wenn nur vor dem Rücksetzen der Bits DCF, DDF eine Aufhebung des Leseschutzes erfolgen muß, und ein Setzen dieser Bits ohne eine Aufhebung des Leseschutzes durchgeführt werden kann. Im folgenden wird jedoch davon ausgegangen, daß sowohl beim Setzen als auch beim Zurücksetzen der genannten Bits kein Leseschutz wirksam sein darf.

Eine ein "Write Register"-Kommando repräsentierende Kommandosequenz kann beispielsweise darin bestehen, daß

- in einem ersten Zyklus bzw. in einem ersten Schreibzugriff auf die Speichereinrichtung die Adresse 5554 und die Daten CC, und

- in einem zweiten Zyklus bzw. in einem zweiten Schreibzugriff auf die Speichereinrichtung als Adresse die Adresse des zu beschreibenden Registers, und als Daten die in dieses Register zu schreibenden Daten

an die Speichereinrichtung übertragen werden.

Wenn der Speichereinrichtung M eine des Kommando "Write Register" repräsentierende Kommandosequenz zugeführt wird, überprüft sie, genauer gesagt die Steuereinrichtung CTRL derselben zunächst, ob es sich hierbei um einen zulässigen Zugriff auf die Speichereinrichtung M handelt. Ein unzulässiger Zugriff liegt beispielsweise vor, wenn ein Leseschutz wirksam ist und das Bit DCF und/oder das Bit DDF verändert werden soll. Wenn die Steuereinrichtung CTRL feststellt, daß es sich um einen unzulässigen Zugriff auf die Speichereinrichtung M handelt, führt sie diesen Zugriff nicht aus und signalisiert zudem der CPU und/oder sonstigen Mikrocontroller-Komponenten, daß ein unzulässiger Zugriff auf die Speichereinrichtung M erfolgt ist. Anderenfalls, d.h. wenn es sich um einen zulässigen Zugriff handelt, veranlaßt die Steuereinrichtung CTRL, daß die im zweiten Zyklus der Kommandosequenz übertragenen Daten in das im zweiten Zyklus der Kommandosequenz spezifizierte Register geschrieben werden.

Der Vollständigkeit halber sei angemerkt, daß die Speichereinrichtung M neben dem Speicher-Konfigurationsregister auch noch ein Flash Status Register enthält, in welchem der aktuelle Status des Speichermoduls MM sowie und eventuelle unzulässige Zugriffe auf die Speichereinrichtung M angezeigt werden. Dieses Register kann durch den Benutzer nicht überschrieben werden. Die darin enthaltenen Status- und Fehleranzeigen lassen sich jedoch mit dem Kommando "Clear Status" zurücksetzen

Eine ein "Clear Status"-Kommando repräsentierende Kommandosequenz kann beispielsweise darin bestehen, daß in einem Schreibzugriff auf die Speichereinrichtung die Adresse 5554

und die Daten DD an die Speichereinrichtung übertragen werden.

Der Vollständigkeit halber sei angemerkt, daß auch noch ein Kommando "Read Register" existiert, durch welches die Inhalte bestimmter Register der Speichereinrichtung M ausgelesen werden können. Zu den durch das Kommando "Read Register" auslesbaren Registern gehören auch das Speicher-Konfigurationsregister und das Flash Status Register.

Veränderungen der Bits DCF, DDF, DDFDBG, DDFDMA, und DDFPCP entfalten jeweils sofort, also nicht etwa erst nach dem nächsten Rücksetzen des Mikrocontrollers oder einem sonstigen späteren Zeitpunkt Wirkung.

Wie vorstehend beschrieben wurde, hat der Benutzer des Mikrocontrollers eine ganze Reihe von Möglichkeiten, den Leseschutz und den Schreibschutz entsprechend seinen Wünschen zu konfigurieren. Wann und in welchem Umfang der Leseschutz und der Schreibschutz wirksam sind, wird aber auch durch die Speichereinrichtung M, genauer gesagt durch die Steuereinrichtung CTRL derselben mitbestimmt. Dies wird im folgenden näher erläutert.

Unmittelbar nach dem Einschalten oder Zurücksetzen des Mikrocontrollers überprüft die Steuereinrichtung CTRL oder eine sonstige Mikrocontroller-Komponente, ob ein Leseschutz wirksam sein soll. Dies ist der Fall, wenn das Leseschutzeinstellungs-Bit RPRO des UCB0 gesetzt ist und in den UCB0 ein gültiger Confirmation Code geschrieben wurde.

Wenn ein Leseschutz wirksam sein soll, überprüft die Steuereinrichtung CTRL oder eine sonstige Mikrocontroller-Komponente, wie sich der Mikrocontroller nach dem Einschalten oder Zurücksetzen verhalten soll. Beim betrachteten Mikrocontroller existieren hierfür drei Möglichkeiten, nämlich

1) daß der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen ein außerhalb der Speichereinrichtung M, also ein in einem ungeschützten internen oder externen Speicher gespeichertes Programm ausführen soll,

2) daß der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen einen dem Mikrocontroller von außen zugeführten Bootstrap-Loader ausführen soll, und

3) daß der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen ein innerhalb der Speichereinrichtung M gespeichertes Programm ausführen soll.

Wie sich der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen verhalten soll, wird ihm im betrachteten Beispiel durch Signale vorgegeben, die während des Einschaltens oder des Zurücksetzens des Mikrocontrollers an bestimmte Ein- und/oder Ausgabeanschlüsse des Mikrocontrollers angelegt werden. Unter Auswertung dieser Signale stellt der Mikrocontroller fest, wie er sich nach dem Einschalten bzw. nach dem Zurücksetzen zu verhalten hat.

Wenn sich hierbei ergibt, daß der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen ein außerhalb der Speichereinrichtung M gespeichertes Programm ausführen soll, sorgt die Steuereinrichtung CTRL oder eine andere Mikrocontroller-Komponente dafür, daß die Bits DCF und DDF des Speicher-Konfigurationsregisters gesetzt werden, wodurch, wenn gleichzeitig ein Leseschutz gewünscht wird, also das Bit RPA gesetzt ist, weder Lesezugriffe auf den Programmspeicher MMP noch Lesezugriffe auf den Datenspeicher MMD zugelassen werden. Falls der Entwickler des außerhalb der Speichereinrichtung M gespeicherten Programmes nicht eine zum Auslesen der Speichereinrichtung M autorisierte Person ist, kann diese den Leseschutz nicht aufheben, denn hierzu müßte sie das in UCB0 gespeicherte Kennwort kennen, was aber im allgemeinen nicht der Fall sein dürfte.

Wenn der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen einen dem Mikrocontroller von außen (z.B. über ein serielles Interface des Mikrocontrollers) zugeführten Bootstrap-Loader ausführen soll, sorgt die Steuereinrichtung CTRL oder eine andere Mikrocontroller-Komponente dafür, daß die Bits DCF und DDF gesetzt werden und somit ein Leseschutz wirksam ist, während das zugeführte Programm ausgeführt wird.

Wenn der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen ein innerhalb der Speichereinrichtung M gespeichertes Programm ausführen soll, wird dies zugelassen und darüber hinaus durch die Steuereinrichtung CTRL oder eine andere Mikrocontroller-Komponente dafür gesorgt, daß die Bits DCF und DDF des Speicher-Konfigurationsregisters zurückgesetzt werden, wodurch sowohl Lesezugriffe auf den Programmspeicher MMP als auch Lesezugriffe auf den Datenspeicher MMD zugelassen werden.

Wie aus den vorstehenden Erläuterungen ersichtlich ist, wird nur im Fall, daß der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen ein außerhalb der Speichereinrichtung M gespeichertes Programm ausführt, durch Setzen der Bits DCF und DDF dafür gesorgt, daß ein Leseschutz wirksam ist. Wenn der Mikrocontroller nach der Inbetriebnahme bzw. dem Rücksetzen ein innerhalb der Speichereinrichtung M gespeichertes Programm ausführt, ist dies nicht erforderlich, denn in diesem Fall kann der Entwickler des in der Speichereinrichtung M gespeicherten Programmes selbst dafür sorgen, daß keine Lesezugriffe durch hierzu nicht autorisierte Personen auf die Speichereinrichtung M erfolgen: er kann das in der Speichereinrichtung M gespeicherte Programm so schreiben, daß keine Sprünge in ungeschützte Speicher oder Speicherbereiche erfolgen bzw. daß dann, wenn ein Sprung in einen ungeschützten Speicher oder Speicherbereich erfolgt, kein Zugriff mehr oder nur noch bestimmte Zugriffe auf die Speichereinrichtung M erfolgen können. Letzteres kann dadurch geschehen, daß das in

der Speichereinrichtung M gespeicherte Programm Befehle enthält, die dafür sorgen, daß vor der Ausführung eines Sprunges in einen ungeschützten Speicher oder Speicherbereich die Bits DCF und/oder DDF des Speicher-Konfigurationsregisters gesetzt werden. Der Vollständigkeit halber sei angemerkt, daß bei nicht gesetztem Bit DCF wieder ein Rücksprung in die Speichereinrichtung M möglich ist, wohingegen bei gesetztem Bit DCF nicht einmal dies mehr möglich ist. Damit ein Rücksprung in die Speichereinrichtung M erfolgen kann, müßte zunächst durch das Kommando "Disable Read Protection" der Leseschutz aufgehoben werden.

Dadurch kann - teils automatisch durch den Mikrocontroller, und teils durch ein entsprechend geschriebenes Programm - zuverlässig verhindert werden, daß der Inhalt der Speichereinrichtung M durch nicht in der Speichereinrichtung M gespeicherte Befehle ausgelesen wird. Da bei entsprechender Konfiguration des Lese-/Schreibschutzes aber nur bestimmte Personen in der Lage sind, die Speichereinrichtung M zu beschreiben, haben nicht autorisierte Personen keine Chance, den Inhalt der Speichereinrichtung M auszulesen oder zu verändern.

Wenn das Leseschutzeinstellungs-Bit RPRO des UCB0 gesetzt ist und in den UCB0 ein gültiger Confirmation Code geschrieben wurde, wird durch die Steuereinrichtung CTRL oder eine sonstige Mikrocontroller-Komponente vorzugsweise auch sofort das Bit DDFDBG des Speicher-Konfigurationsregisters, und gegebenenfalls auch die Bits DDFDMA und/oder DDFPCP des Speicher-Konfigurationsregisters gesetzt. Die genannten Bits können aber auch durch entsprechende Befehle im ausgeführten Programm gesetzt und zurückgesetzt werden. Durch diese Maßnahme können nicht autorisierte Personen auch nicht über den Debug-Controller und/oder den DMA-Controller und/oder den Peripheral Control Prozessor auf die Speichereinrichtung M zugreifen.

Vorzugsweise ist bei wirksamem Leseschutz automatisch auch ein Schreibschutz wirksam, und zwar für die gesamte Speichereinrichtung M. Dadurch kann verhindert werden, daß durch eine hierzu nicht autorisierte Person eine Leseroutine (beispielsweise ein Trojanisches Pferd) in die Speichereinrichtung M geschrieben wird, welche dann den gesamten Speicherinhalt auslesen und aus dem Mikrocontroller ausgeben könnte.

Der Mikrocontroller sorgt darüber hinaus dafür, daß nach der Inbetriebnahme oder dem Rücksetzen des Mikrocontrollers in dem Umfang, wie er in den UCBs festgelegt ist, ein selektiver, d.h. vom Leseschutz unabhängiger Schreibschutz wirksam ist.

Dieser selektive Schreibschutz kann durch den Benutzer mittels der Kommandos "Disable Write Protection" und "Resume Protection", genauer gesagt durch Programmbefehle, durch welche die Übermittlung dieser Kommandos an die Speichereinrichtung M veranlaßt wird, temporär ganz oder teilweise aufgehoben werden.

Der mit dem Leseschutz gekoppelte Schreibschutz kann durch das Kommando "Disable Read Protection"temporär aufgehoben werden.

Wie vorstehend bereits mehrfach erwähnt wurde, signalisiert die Steuereinrichtung CTRL der CPU und/oder einer sonstigen Mikrocontroller-Komponente eine Speicherschutzverletzung, wenn ein unzulässiger Zugriff auf die Speichereinrichtung M erfolgt. Dies kann beispielsweise durch einen entsprechenden Eintrag in ein Statusregister, beispielsweise in das vorstehend bereits erwähnte Flash Status Register, und/oder durch einen Interrupt Request erfolgen. Wie die CPU hierauf reagiert, hängt vorzugsweise vom Einsatz des Mikrocontrollers ab. Die Reaktionen können beispielsweise, aber verständlicherweise nicht ausschließlich darin bestehen,

- daß dafür gesorgt wird, daß die Programmausführung beendet wird und bis zur nächsten Inbetriebnahme oder bis zum nächsten Zurücksetzen des Mikrocontrollers keine weiteren Befehle mehr ausgeführt, oder

- daß dafür gesorgt wird, daß der unzulässige Zugriff mit korrekten Parametern wiederholt werden kann, oder

- daß dafür gesorgt wird, daß bis zur nächsten Inbetriebnahme oder oder bis zum nächsten Zurücksetzen des Mikrocontrollers nur noch bestimmte Zugriffe auf die Speichereinrichtung M zugelassen werden, beispielsweise nur solche Zugriffe, welche keinen Einfluß auf den Umfang des Leseschutzes und/oder des Schreibschutzes haben oder die Voraussetzung für solche Zugriffe sind (also kein "Disable Read Protection"-Kommando, und/oder kein "Disable Write Protection"-Kommando, und/oder kein "Erase UCB"-Kommando, und/oder kein "Write UC Page"-Kommando mehr ausgeführt wird).

Vorzugsweise ist es so, daß nach einem Versuch, den Leseschutz oder den Schreibschutz betreffende Einstellungen oder Konfigurationen unter Verwendung eines falschen Kennwortes zu verändern, ein weiterer Versuch zur Veränderung der Einstellungen oder Konfigurationen erst nach dem Zurücksetzen oder einer erneuten Inbetriebnahme der programmgesteuerten Einheit möglich ist. Zumindest nach einem Versuch, den Leseschutz oder den Schreibschutz unter Verwendung eines falschen Kennwortes temporär aufzuheben, sollte ein weiterer Versuch zur temporären Aufhebung des Leseschutzes oder des Schreibschutzes erst nach dem Zurücksetzen oder einer erneuten Inbetriebnahme der programmgesteuerten Einheit möglich sein.

Selbstverständlich kann der Mikrocontroller auf einen unzulässigen Zugriff auf die Speichereinrichtung M auch beliebig anders reagieren. Die Reaktion des Mikrocontrollers kann auch

von der Art des unzulässigen Zugriffes abhängig gemacht werden. Beispielsweise kann vorgesehen werden, daß der gescheiterte Versuch, den Leseschutz temporär aufzuheben (Disable Read Protection), durch härtere bzw. umfangreichere Maßnahmen sanktioniert wird als ein unzulässiger Lesezugriff auf den Datenspeicher MMD.

Wie vorstehend erläutert wurde, kann der UCB0 durch einen ersten Benutzer des Mikrocontrollers beschrieben und gelöscht werden, der UCB1 durch einen zweiten Benutzer des Mikrocontrollers beschrieben und gelöscht werden, und der UCB2 durch einen dritten Benutzer beschrieben werden. Dies erweist sich als vorteilhaft, weil dadurch im betrachteten Beispiel bis zu drei Benutzer ihre Daten weitestgehend unabhängig voneinander vor Zugriffen durch dazu nicht autorisierte Personen schützen können.

Wenn der beschriebene Mikrocontroller Bestandteil eines Kraftfahrzeugsteuergerätes ist, und durch den Mikrocontroller ein Programm ausgeführt wird, dessen Befehle und/oder Operanden teilweise vom Hersteller des Kraftfahrzeugsteuergerätes stammen, und teilweise vom Hersteller des Kraftfahrzeuges, so können sowohl der Hersteller des Kraftfahrzeugsteuergerätes als auch der Hersteller des Kraftfahrzeuges ihre Programmteile und/oder Operanden vor einem Auslesen und/oder vor Veränderungen durch dazu nicht autorisierte Personen schützen: der Hersteller des Kraftfahrzeugsteuergerätes kann der erste Benutzer des Mikrocontrollers sein und den Schutz seiner Programmteile und/oder Operanden durch entsprechendes Beschreiben des UCB0 konfigurieren, und der Hersteller des Kraftfahrzeuges kann der zweite Benutzer des Mikrocontrollers sein und den Schutz seiner Programmteile und/oder Operanden durch entsprechendes Beschreiben des UCB1 konfigurieren; darüber hinaus kann entweder der Hersteller des Kraftfahrzeugsteuergerätes oder der Hersteller des Kraftfahrzeuges der dritte Benutzer sein und den Schutz seiner Programmteile und/oder Operanden zusätzlich durch entsprechendes Beschreiben des UCB2

konfigurieren. Selbstverständlich kann der dritte Benutzer auch eine dritte Person oder ein drittes Unternehmen sein, das an der Entwicklung des in der Speichereinrichtung M gespeicherten Programmes beteiligt ist. Ebenso ist es natürlich auch möglich, daß eine einzige Person oder ein einziges Unternehmen sowohl der erste Benutzer als auch der zweite Benutzer ist.

Durch Vorsehen weiterer UCBs können auch noch weitere Benutzer des Mikrocontrollers ihre Daten vor Zugriffen durch hierzu nicht autorisierte Personen schützen.

Der Vollständigkeit halber sei angemerkt, daß die Übertragung der vorstehend beschriebenen Kommandosequenzen zur Speichereinrichtung M, auch die Übertragung der Kommandosequenzen zur Konfigurierung des Leseschutzes und/oder des Schreibschutzes durch entsprechende Befehle in dem von der CPU ausgeführten Programm veranlaßt wird.

Die Speichereinrichtung M kann nach alledem auf sehr einfache Art und Weise zuverlässig vor Zugriffen durch hierzu nicht autorisierte Personen geschützt werden. Darüber hinaus können der Umfang des Leseschutzes und der Umfang des Schreibschutzes unabhängig voneinander optimal an die jeweiligen Verhältnisse angepaßt werden.

Bezugszeichenliste

ADDRBUSx	Adreßbus
BUS	Bus
CPU	CPU
CTRL	Steuereinrichtung
CTRLBUSx	Steuerbus
DCF	Konfigurations-Bit
DDF	Konfigurations-Bit
DDFDBG	Konfigurations-Bit
DDFDMA	Konfigurations-Bit
DDFPCP	Konfigurations-Bit
ECCBUSx	Fehlerkorrekturdatenbus
ECU	Fehlerkorrektureinrichtung
M	Speichereinrichtung
MI	Schnittstelle
MM	Speichermodul
MMD	Datenspeicher
MMDSx	Datenspeicher-Sektor
MMP	Programmspeicher
MMPSx	Programmspeicher-Sektor
Px	Peripherieeinheit
PG	Programmgesteuerte Einheit
RDATABUSx	Lesedatenbus
RPA	Konfigurations-Bit
RPRO	Leseschutzeinstellungs-Bit
SxL	Schreibschutzeinstellung-Bit
SxROM	Schreibschutzeinstellung-Bit
WDATABUSx	Schreibdatenbus

Patentansprüche

1. Programmgesteuerte Einheit mit einem Speicher zum Speichern von Daten, und mit einer Speicherschutzvorrichtung zum Schützen des Speichers vor Lesezugriffen durch hierzu nicht autorisierte Personen,
d a d u r c h g e k e n n z e i c h n e t ,
daß die programmgesteuerte Einheit so ausgebildet ist, daß der Leseschutz

- durch die programmgesteuerte Einheit bei Bedarf automatisch aktiviert wird, und

- durch eine hierzu autorisierte Person an die gegebenen Verhältnisse angepaßt werden kann.

2. Programmgesteuerte Einheit nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t ,
daß der Benutzer der programmgesteuerten Einheit einstellen kann, ob und gegebenenfalls welche Bereiche des Speichers vor Lesezugriffen durch hierzu nicht autorisierte Personen geschützt sein sollen.

3. Programmgesteuerte Einheit nach Anspruch 2,
d a d u r c h g e k e n n z e i c h n e t ,
daß die Einstellungen des Benutzers in einem nichtflüchtigen Speicher der programmgesteuerten Einheit gespeichert werden.

4. Programmgesteuerte Einheit nach Anspruch 3,
d a d u r c h g e k e n n z e i c h n e t ,
daß der die Einstellungen des Benutzers speichernde Speicher ein wiederholt umprogrammierbarer Speicher ist.

5. Programmgesteuerte Einheit nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t ,
daß die programmgesteuerte Einheit auf eigene Veranlassung dafür sorgt, daß bei Bedarf nach der Inbetriebnahme oder dem

Rücksetzen der programmgesteuerten Einheit ein Leseschutz aktiv ist, durch welchen Lesezugriffe auf den Speicher blockiert werden.

6. Programmgesteuerte Einheit nach Anspruch 5, dadurch gekennzeichnet, daß die programmgesteuerte Einheit selbst festlegt, ob und in welchem Umfang nach der Inbetriebnahme oder dem Rücksetzen der programmgesteuerten Einheit ein Leseschutz aktiv sein soll.

7. Programmgesteuerte Einheit nach Anspruch 5, dadurch gekennzeichnet, daß es von den Einstellungen des Benutzers der programmgesteuerten Einheit abhängt, ob und in welchem Umfang die programmgesteuerte Einheit den Leseschutz aktiviert.

8. Programmgesteuerte Einheit nach Anspruch 5, dadurch gekennzeichnet, daß es von dem vom Benutzer der programmgesteuerten Einheit gewünschten Verhalten der programmgesteuerte Einheit nach der Inbetriebnahme oder dem Rücksetzen derselben abhängt, ob und in welchem Umfang die programmgesteuerte Einheit den Leseschutz aktiviert.

9. Programmgesteuerte Einheit nach Anspruch 8, dadurch gekennzeichnet, daß das vom Benutzer gewünschte Verhalten der programmgesteuerte Einheit nach der Inbetriebnahme oder dem Rücksetzen derselben unter Auswertung der Signale ermittelt wird, die während der Inbetriebnahme oder des Rücksetzens der programmgesteuerten Einheit von außerhalb der programmgesteuerten Einheit an bestimmte Ein- und/oder Ausgabeanschlüsse derselben angelegt werden.

10. Programmgesteuerte Einheit nach Anspruch 8, dadurch gekennzeichnet,

daß die programmgesteuerte Einheit dafür sorgt, daß nach der Inbetriebnahme oder dem Rücksetzen derselben kein Leseschutz aktiv ist, durch welchen von der CPU der programmgesteuerten Einheit stammende Lesezugriffe auf den zu schützenden Speicher oder Speicherbereich blockiert werden,

- wenn die Einstellungen des Benutzers der programmgesteuerten Einheit besagen, daß der Speicher oder Teile desselben vor Lesezugriffen durch hierzu nicht autorisierte Personen geschützt sein soll, und

- wenn der erste Befehl, der nach der Inbetriebnahme oder dem Rücksetzen der programmgesteuerten Einheit auszuführen ist, in dem zu schützenden Speicher oder Speicherbreich gespeichert ist.

11. Programmgesteuerte Einheit nach Anspruch 8,
d a d u r c h g e k e n n z e i c h n e t ,
daß die programmgesteuerte Einheit

- dafür sorgt, daß nach der Inbetriebnahme oder dem Rücksetzen derselben kein Leseschutz aktiv ist, durch welchen von der CPU der programmgesteuerten Einheit stammende Lesezugriffe auf den zu schützenden Speicher oder Speicherbereich blockiert werden,

- wenn die Einstellungen des Benutzers der programmgesteuerten Einheit besagen, daß der Speicher vor Lesezugriffen durch hierzu nicht autorisierte Personen geschützt sein soll, und

- wenn die programmgesteuerten Einheit nach der Inbetriebnahme oder dem Zurücksetzen derselben einen ihr von außerhalb der programmgesteuerten Einheit zugeführten Bootstrap-Loader ausführen soll.

12. Programmgesteuerte Einheit nach Anspruch 8,

d a d u r c h g e k e n n z e i c h n e t ,
daß die programmgesteuerte Einheit dafür sorgt, daß nach der Inbetriebnahme oder dem Rücksetzen derselben ein Leseschutz aktiv ist, durch welchen sämtliche Lesezugriffe auf den zu schützenden Speicher oder Speicherbereich blockiert werden,

- wenn die Einstellungen des Benutzers der programmgesteuerten Einheit besagen, daß der Speicher oder Teile desselben vor Lesezugriffen durch hierzu nicht autorisierte Personen geschützt sein soll, und

- wenn der erste Befehl, der nach der Inbetriebnahme oder dem Rücksetzen der programmgesteuerten Einheit auszuführen ist, nicht in dem zu schützenden Speicher gespeichert ist.

13. Programmgesteuerte Einheit nach Anspruch 5,
d a d u r c h g e k e n n z e i c h n e t ,
daß die programmgesteuerte Einheit dafür sorgt, daß nach der Inbetriebnahme oder dem Rücksetzen derselben ein Leseschutz aktiv ist, durch welchen Lesezugriffe auf den zu schützenden Speicher oder Speicherbereich, die nicht von der CPU der programmgesteuerten Einheit stammen, blockiert werden.

14. Programmgesteuerte Einheit nach Anspruch 13,
d a d u r c h g e k e n n z e i c h n e t ,
daß die programmgesteuerte Einheit dafür sorgt, daß nach der Inbetriebnahme oder dem Rücksetzen derselben ein Leseschutz aktiv ist, durch welchen von einem Debug-Controller der programmgesteuerten Einheit stammende Lesezugriffe auf den zu schützenden Speicher oder Speicherbereich blockiert werden.

15. Programmgesteuerte Einheit nach Anspruch 13,
d a d u r c h g e k e n n z e i c h n e t ,
daß die programmgesteuerte Einheit dafür sorgt, daß nach der Inbetriebnahme oder dem Rücksetzen derselben ein Leseschutz aktiv ist, durch welchen von einem DMA-Controller der pro-

grammgesteuerten Einheit stammende Lesezugriffe auf den zu schützenden Speicher oder Speicherbereich blockiert werden.

16. Programmgesteuerte Einheit nach Anspruch 13, dadurch gekennzeichnet, daß die programmgesteuerte Einheit dafür sorgt, daß nach der Inbetriebnahme oder dem Rücksetzen derselben ein Leseschutz aktiv ist, durch welchen Lesezugriffe auf den zu schützenden Speicher oder Speicherbereich blockiert werden, die von einem nicht durch die CPU gebildeten weiteren Prozessor der programmgesteuerten Einheit oder einem außerhalb der programmgesteuerten Einheit vorgesehenen Prozessor stammen.

17. Programmgesteuerte Einheit nach Anspruch 1, dadurch gekennzeichnet, daß der Benutzer der programmgesteuerten Einheit den Leseschutz durch entsprechende Befehle in dem von der programmgesteuerten Einheit ausgeführten Programm aktivieren, deaktivieren, erweitern und reduzieren kann.

18. Programmgesteuerte Einheit nach Anspruch 17, dadurch gekennzeichnet, daß der Benutzer der programmgesteuerten Einheit durch entsprechende Befehle in dem von der programmgesteuerten Einheit ausgeführten Programm einen Leseschutz aktivieren und deaktivieren kann, durch welchen Code Fetches repräsentierende Lesezugriffe auf den zu schützenden Speicher blockiert werden.

19. Programmgesteuerte Einheit nach Anspruch 17, dadurch gekennzeichnet, daß der Benutzer der programmgesteuerten Einheit durch entsprechende Befehle in dem von der programmgesteuerten Einheit ausgeführten Programm einen Leseschutz aktivieren und deaktivieren kann, durch welchen Data Fetches repräsentierende Lesezugriffe auf den zu schützenden Speicher blockiert werden.

20. Programmgesteuerte Einheit nach Anspruch 17, dadurch gekennzeichnet, daß der Benutzer der programmgesteuerten Einheit durch entsprechende Befehle in dem von der programmgesteuerten Einheit ausgeführten Programm einen Leseschutz aktivieren und deaktivieren kann, durch welchen von einem Debug-Controller der programmgesteuerten Einheit stammende Lesezugriffe auf den Speicher blockiert werden.

21. Programmgesteuerte Einheit nach Anspruch 17, dadurch gekennzeichnet, daß der Benutzer der programmgesteuerten Einheit durch entsprechende Befehle in dem von der programmgesteuerten Einheit ausgeführten Programm einen Leseschutz aktivieren und deaktivieren kann, durch welchen von einem DMA-Controller der programmgesteuerten Einheit stammende Lesezugriffe auf den Speicher blockiert werden.

22. Programmgesteuerte Einheit nach Anspruch 17, dadurch gekennzeichnet, daß der Benutzer der programmgesteuerten Einheit durch entsprechende Befehle in dem von der programmgesteuerten Einheit ausgeführten Programm einen Leseschutz aktivieren und deaktivieren kann, durch welchen Lesezugriffe auf den zu Speicher blockiert werden, die von einem nicht durch die CPU gebildeten weiteren Prozessor der programmgesteuerten Einheit oder einem außerhalb der programmgesteuerten Einheit vorgesehenen Prozessor stammen.

23. Programmgesteuerte Einheit nach Anspruch 17, dadurch gekennzeichnet, daß die Befehle, durch welche der Benutzer der programmgesteuerten Einheit den Leseschutz aktivieren, deaktivieren, erweitern, und reduzieren kann, zumindest teilweise ein Kennwort enthalten müssen, das mit einem in der programmgesteuerten Einheit gespeicherten Kennwort übereinstimmt.

24. Programmgesteuerte Einheit nach Anspruch 23,
dadurch gekennzeichnet,
daß das in der programmgesteuerten Einheit gespeicherte Kennwort durch einen hierzu autorisierten Benutzer der programmgesteuerten Einheit in einen nichtflüchtigen und zumindest durch den Benutzer der programmgesteuerten Einheit nicht auslesbaren Speicher derselben geschrieben wurde.

25. Programmgesteuerte Einheit nach einem der Ansprüche 5 bis 22,
dadurch gekennzeichnet,
daß die Aktivierung, Deaktivierung, Erweiterung und Reduzierung des Leseschutzes durch Setzen und Rücksetzen bestimmter Bits in einem Konfigurationsregister der programmgesteuerten Einheit erfolgen.

26. Programmgesteuerte Einheit nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß diese dafür sorgt, daß bei wirksamem Leseschutz auch ein Leseschutz wirksam ist, durch welchen verhindert wird, daß aus dem zu schützenden Speicher ausgelesene und in einen anderen Speicher der programmgesteuerten Einheit geschriebene Daten durch hierzu nicht autorisierte Personen aus dem anderen Speicher ausgelesen und aus der programmgesteuerten Einheit ausgegeben werden können.

27. Programmgesteuerte Einheit nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß nach einem Versuch, den Leseschutz oder den Schreibschutz betreffende Einstellungen oder Konfigurationen unter Verwendung eines falschen Kennwortes zu verändern, ein weiterer Versuch zur Veränderung der Einstellungen oder Konfigurationen erst nach dem Zurücksetzen oder einer erneuten Inbetriebnahme der programmgesteuerten Einheit möglich ist.

28. Programmgesteuerte Einheit nach Anspruch 27,
d a d u r c h g e k e n n z e i c h n e t ,
daß nach einem Versuch, den Leseschutz oder den Schreibschutz unter Verwendung eines falschen Kennwortes temporär aufzuheben, ein weiterer Versuch zur temporären Aufhebung des Leseschutzes oder des Schreibschutzes erst nach dem Zurücksetzen oder einer erneuten Inbetriebnahme der programmgesteuerten Einheit möglich ist.

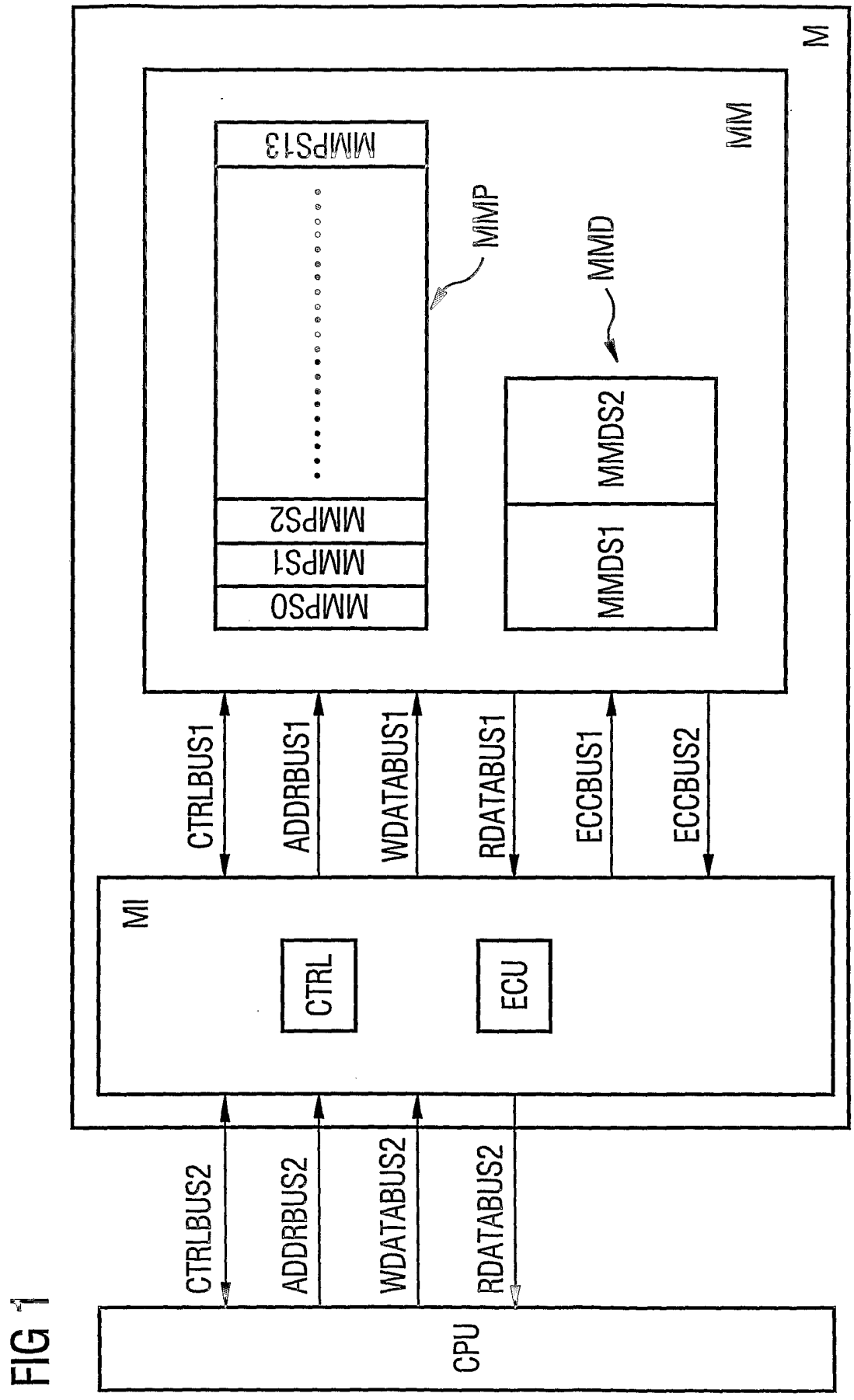

M
MIM
MIMPS13
MIMPS2
MIMPS1
MIMPS0
MIMP
MMD
MMDS2
MMDS1
CTRLBUS1
ADDRBUS1
WDATABUS1
RDATABUS1
ECCBUS1
ECCBUS2
MI
CTRL
ECU
CTRLBUS2
ADDRBUS2
WDATABUS2
RDATABUS2
CPU

FIG 1

FIG 2

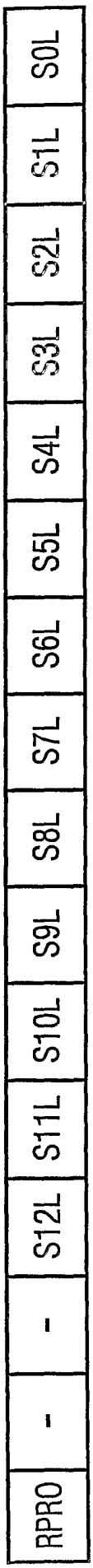


FIG 3

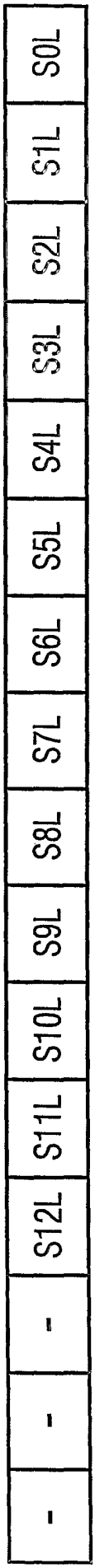


FIG 4

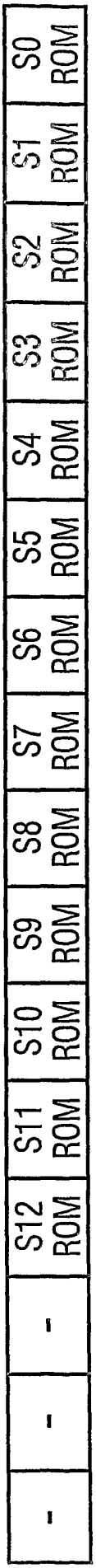


FIG 5

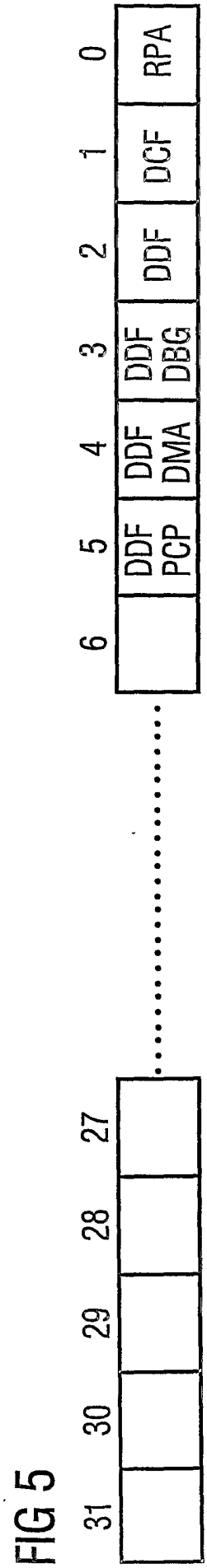


FIG 6