(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
3. April 2003 (03.04.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/027815 A2

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/DE02/03202

(22) Internationales Anmeldedatum:
30. August 2002 (30.08.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 46 516.5 21. September 2001 (21.09.2001) 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)*: **ROHM, Peter** [DE/DE]; Bistumerweg 8, 85276 Pfaffenhofen (DE).

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

(81) Bestimmungsstaat *(national)*: US.

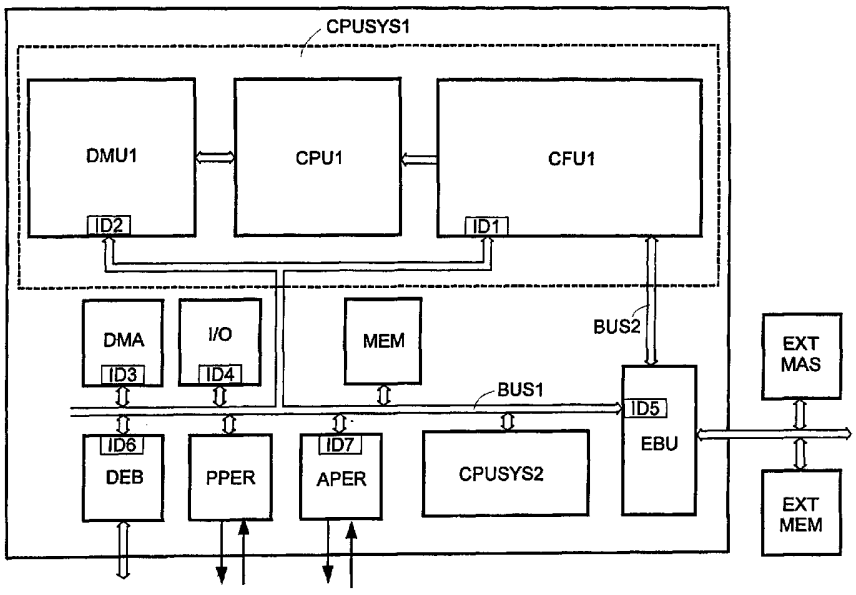
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

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

[Fortsetzung auf der nächsten Seite]

(54) Title: PROGRAMME-CONTROLLED UNIT

(54) Bezeichnung: PROGRAMMGESTEUERTE EINHEIT



(57) Abstract: The invention relates to a programme-controlled unit comprising a memory device, to which various other components of the programme-controlled unit can gain read or write access. Said programme-controlled unit is characterised in that when the memory device is accessed, a check is made as to whether the respective access has been initiated or could have been initiated by an unauthorised person and that the memory device only issues the requested data and/or only saves data that has been supplied, if the check shows that it can be assumed that the relevant access has not been initiated or could not have been initiated by unauthorised person.

[Fortsetzung auf der nächsten Seite]

WO 03/027815 A2

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.

(57) Zusammenfassung: Es wird eine programmgesteuerte Einheit beschrieben, mit einer Speichereinrichtung, auf welche von verschiedenen anderen Komponenten der programmgesteuerten Einheit lesend oder schreibend zugegriffen werden kann. Die beschriebene programmgesteuerte Einheit zeichnet sich dadurch aus, dass bei Zugriffen auf die Speichereinrichtung überprüft wird, ob der jeweilige Zugriff durch eine dazu nicht autorisierte Person veranlasst wurde oder veranlasst worden sein könnte, und dass die Speichereinrichtung angeforderte Daten nur ausgibt, und/oder ihr zugeführte Daten nur speichert, wenn die Überprüfung ergeben hat, dass davon ausgegangen werden kann, dass der betreffende Zugriff nicht durch eine dazu nicht autorisierte Person veranlasst wurde oder veranlasst worden sein könnte.

Beschreibung

Programmgesteuerte Einheit

Die vorliegende Erfindung betrifft eine Vorrichtung gemäß dem Oberbegriff des Patentanspruchs 1, d.h. eine programmgesteuerte Einheit mit einer Speichereinrichtung, auf welche von verschiedenen anderen Komponenten der programmgesteuerten Einheit lesend oder schreibend zugegriffen werden kann.

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

Mitunter besteht ein Bedarf, die in einer programmgesteuerten Einheit, genauer gesagt die in einer Speichereinrichtung derselben gespeicherten Daten vor unbefugten Zugriffen zu schützen, d.h. insbesondere dafür zu sorgen, daß die in der Speichereinrichtung gespeicherten Daten nicht durch unbefugte Personen ausgelesen und/oder verändert werden können. Hierfür gibt es zwei Gründe. Der erste Grund besteht darin, daß die gespeicherten Daten häufig einen wesentlichen Teil der Entwicklung des die programmgesteuerte Einheiten enthaltenden Systems darstellen und daher nach Möglichkeit nicht in die Hände von Mitbewerbern gelangen sollten. Dies ist beispielsweise bei Mikrocontrollern der Fall, die in Kraftfahrzeug-Steuergeräten eingesetzt werden. In solchen Mikrocontrollern sind wesentliche Motorkenndaten gespeichert, durch welche festgelegt wird, wie der Motor in welchen Situation anzusteuern ist. Wenn Mitbewerber von diesen Daten Kenntnis erlangen, können sie daraus für ihre eigenen Produkte neue Erkenntnisse gewinnen, wodurch ein gegebenenfalls vorhandener Entwicklungsvorsprung verloren geht. Der zweite Grund für den Schutz der Speichereinrichtung besteht darin, daß verhindert werden sollte, daß unbefugte Personen durch eine Manipulation der Daten die Motorsteuerung verändern, um dadurch die Leistung, die Höchstgeschwindigkeit etc. zu steigern. Eine sol-

che Manipulation der Motorsteuerung kann dazu führen, daß die Lebenserwartung des Motors sinkt, oder daß sonstige Schäden auftreten, die normalerweise nicht oder erst später auftreten. Dies verschlechtert das Ansehen des Kraftfahrzeugherstellers, und kann ferner dazu führen, daß dieser Garantieleistungen für Schäden zu erbringen hat, für die er nicht verantwortlich ist.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, die programmgesteuerte Einheit gemäß dem Oberbegriff des Patentanspruchs 1 derart weiterzubilden, daß unbefugte Personen keine Möglichkeit haben, in der Speichereinrichtung gespeicherte Daten auszulesen und/oder zu verändern.

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

Die erfindungsgemäße programmgesteuerte Einheit zeichnet sich dadurch aus, daß bei Zugriffen auf die Speichereinrichtung überprüft wird, ob der jeweilige Zugriff durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte, und daß die Speichereinrichtung angeforderte Daten nur ausgibt, und/oder ihr zugeführte Daten nur speichert, wenn die Überprüfung ergeben hat, daß davon ausgegangen werden kann, daß der betreffende Zugriff nicht durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte.

Dadurch kann zuverlässig ausgeschlossen werden, daß der Inhalt der Speichereinrichtung durch dazu nicht autorisierte Personen ausgelesen und/oder verändert werden kann.

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 Figur näher erläutert.

Die Figur zeigt das Blockschaltbild eines Mikrocontroller, bei welchem des nachfolgend beschriebene Speicherschutzsystem realisiert ist.

Obgleich das beschriebene Speicherschutzsystem vorliegend anhand eines Mikrocontrollers beschrieben wird, kann es auch in anderen programmgesteuerten Einheiten wie beispielsweise Mikroprozessoren und Signalprozessoren zum Einsatz kommen.

Der in der Figur gezeigte Mikrocontroller enthält

- ein erstes CPU-Subsystem CPUSYS1,
- ein zweites CPU-Subsystem CPUSYS2,
- einen DMA-Controller DMA,
- einen I/O-Controller I/O,
- eine Schnittstelle EBU zu einem außerhalb des Mikrocontrollers vorgesehenen externen Bus EXTBUS,
- beispielsweise durch ein OCDS-Modul (On-Chip-Debug-Support-Modul) gebildete Debug-Ressourcen DEB,
- ein oder mehrere sonstige aktive, d.h. Bus-Master werden könnende Peripherieeinheiten APER und/oder passive, d.h. nicht Bus-Master werden könnende Peripherieeinheiten PPER,
- eine gemeinsame Speichereinrichtung MEM,
- einen die genannten Komponenten miteinander verbindenden ersten Bus BUS1, und
- einen das erste CPU-Subsystem CPUSYS1 und die Schnittstelle EBU miteinander verbindenden zweiten Bus BUS2.

Das erste CPU-Subsystem CPUSYS1 enthält eine CPU CPU1, eine Befehlsholeinheit CFU1, und eine Datenspeicherzugriffseinheit DMU1.

Das zweite CPU-Subsystem CPUSYS2 kann, muß aber nicht den selben Aufbau aufweisen.

An den externen Bus EXTBUS sind eine externe Mastereinheit EXTMAS und eine externe Speichereinrichtung EXTMEM angeschlossen.

Der Vollständigkeit halber sei darauf hingewiesen, daß der Mikrocontroller auch eine größere Anzahl von Komponenten, oder eine kleinere Anzahl von Komponenten und/oder andere Komponenten enthalten kann. Ebenso können an den externen Bus EXTBUS auch eine größere Anzahl von Komponenten, oder eine kleinere Anzahl von Komponenten und/oder andere Komponenten angeschlossen sein.

Vorliegend interessieren insbesondere die gemeinsame interne Speichereinrichtung MEM und die Art und Weise, wie diese auf sie erfolgende Zugriffe handhabt. Diese gemeinsame Speichereinrichtung MEM ist im betrachteten Beispiel der durch das beschriebene Speicherschutzsystem zu schützende Speicher, d.h. ein Speicher, dessen Inhalt nicht durch dazu nicht autorisierte Personen auslesbar und/oder veränderbar sein soll.

Die Speichereinrichtung MEM ist an den Bus BUS1 angeschlossen, wodurch auf die Speichereinrichtung MEM von allen anderen Komponenten, die ebenfalls am Bus BUS1 angeschlossen sind, und am Bus BUS1 Bus-Master werden können, Zugriffe erfolgen können.

Die Komponenten, die Bus-Master werden können, sind im betrachteten Beispiel das erste CPU-Subsystem CPUSYS1, genauer gesagt die Befehlsholeinheit CFU1 und die Datenspeicherzugriffseinheit DMU1 desselben, die entsprechenden Komponenten des zweiten CPU-Subsystems CPUSYS2, der DMA-Controller DMA, der I/O-Controller I/O, die Schnittstelle EBU, die Debug-Ressourcen DEB, und die aktive(n) Peripherieeinheit(en).

Die gemeinsame Speichereinrichtung MEM ist im betrachteten Beispiel ein Flash-Speicher. Es könnte es sich aber auch um einen beliebigen anderen nichtflüchtigen oder flüchtigen Speicher handeln.

Die gemeinsame Speichereinrichtung MEM enthält einen Programmspeicher und einen Datenspeicher, wobei im Programmspeicher Befehle repräsentierende Daten gespeichert sind, und wobei im Datenspeicher sonstige Daten, beispielsweise Operanden gespeichert sind. Der Programmspeicher und der Datenspeicher sind jeweils über eigene Adreß-, Daten- und Steuerleitungen mit den anderen Komponenten des Mikrocontrollers verbunden. Die Adreß-, Daten- und Steuerleitungen sind Bestandteil des Busses BUS1.

Der betrachtete Mikrocontroller weist demnach die sogenannte Harvard-Architektur auf, arbeitet im übrigen aber nach dem Von-Neumann-Prinzip, führt die von ihm auszuführenden Befehle also sequentiell aus.

Es sei bereits an dieser Stelle darauf hingewiesen, daß das beschriebene Speicherschutzsystem auch bei programmgesteuerten Einheiten einsetzbar ist, welche nicht über getrennte Programmspeicher und Datenspeicher verfügen.

Bei den folgenden Ausführungen wird von den CPU-Subsystemen CPUSYS1 und CPUSYS2 nur das erste CPU-Subsystem CPUSYS1 betrachtet. Die hierzu gemachten Erläuterungen gelten jedoch für das zweite CPU-Subsystem CPUSYS2 entsprechend, wobei das erste CPU-Subsystem CPUSYS1 und das zweite CPU-Subsystem CPUSYS2 parallel arbeiten oder zumindest parallel arbeiten können.

Im Betrieb des Mikrocontrollers holt das erste CPU-Subsystem CPUSYS1 Befehle repräsentierende Daten und die dazugehörenden Operanden aus dem gemeinsamen Speicher MEM oder einem anderen Speicher und führt sie aus. Genauer gesagt

- holt die Befehlsholeinheit CFU1 des CPU-Subsystems CPUSYS1 Befehle repräsentierende Daten aus dem Programmspeicher-Teil der gemeinsamen Speichereinrichtung MEM,
- holt die Datenspeicherzugriffseinheit DMU1 des CPU-Subsystems CPUSYS1 bei Bedarf Operanden repräsentierende Daten aus dem Datenspeicher-Teil der gemeinsamen Speichereinrichtung MEM, und
- führt die CPU CPU1 des CPU-Subsystems CPUSYS1 die Befehle aus, wobei dann, wenn die Ausführung eines Befehls das Transferieren von Daten von und/oder zu einer innerhalb oder außerhalb des Mikrocontrollers vorgesehenen Systemkomponente umfaßt, diese Datentransfers ebenfalls durch die Datenspeicherzugriffseinheit DMU1 erfolgen.

Im betrachteten Beispiel ist es so, daß im normalen Betrieb keine Datentransfers zur gemeinsamen Speichereinrichtung MEM erfolgen. Zu speichernde Ergebnisse etc. werden in einen anderen Speicher geschrieben, beispielsweise in ein (in der Figur nicht gezeigtes) internes RAM des Mikrocontrollers, oder in den externen Speicher EXTMEM.

Sofern auf die gemeinsame Speichereinrichtung MEM überhaupt schreibend zugegriffen werden kann, erfolgt dies nur in bestimmten Betriebsarten des Mikrocontrollers und unter Sicherheitsvorkehrungen, durch welche gewährleistet werden kann, daß das Beschreiben der gemeinsamen Speichereinrichtung MEM nicht durch dazu nicht autorisierte Personen veranlaßt werden kann. Hierzu kann beispielsweise vorgesehen werden, daß eine Veränderung des Inhalts der gemeinsamen Speichereinrichtung MEM nur über die Ausführung eines in der gemeinsamen Speichereinrichtung MEM gespeicherten Bootstrap Loaders erfolgen kann, wobei dieser Bootstrap Loader ausschließlich durch eine nur bestimmten Personen bekannte Vorgehensweise zur Ausführung bringbar ist, und/oder wobei der Bootstrap Loader die gemeinsame Speichereinrichtung MEM nur umprogrammiert, nach-

dem ein nur bestimmten Personen bekannter Code in den Mikrocontroller eingegeben wurde.

Die gemeinsame Speichereinrichtung MEM weist darüber hinaus die Besonderheit auf, daß er bei Zugriffen auf sie überprüft, ob der jeweilige Zugriff durch eine dazu nicht autorisierte Person veranlaßt worden sein könnte, und daß die gemeinsame Speichereinrichtung MEM angeforderte Daten nur ausgibt, wenn die Überprüfung ergeben hat, daß der betreffende Zugriff nicht durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte.

Obgleich dies im betrachteten Beispiel nicht praktiziert wird, könnte bei Anwendung dieses Schutzmechanismus auf Schreibzugriffe auch zugelassen werden, daß die gemeinsame Speichereinrichtung MEM im normalen Betrieb des Mikrocontrollers beschrieben werden kann. Das Beschreiben der gemeinsamen Speichereinrichtung MEM könnte zugelassen werden, wenn dafür gesorgt wird, daß die gemeinsame Speichereinrichtung MEM ihr zugeführte Daten nur speichert, wenn davon ausgegangen werden kann, daß der betreffende Zugriff nicht durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte.

Die Überprüfung, ob ein jeweiliger Zugriff auf die gemeinsame Speichereinrichtung MEM durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte, erfolgt im betrachteten Beispiel durch eine Steuereinrichtung, welche Bestandteil der gemeinsamen Speichereinrichtung MEM ist. Die Steuereinrichtung könnte aber auch eine der Speichereinrichtung vorgeschaltete Einrichtung sein, welche auf die Speichereinrichtung MEM erfolgende Zugriffe nur dann an die gemeinsame Speichereinrichtung weiterleitet, wenn davon ausgegangen werden kann, daß der betreffende Zugriff nicht durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte.

Im betrachteten Beispiel wird davon ausgegangen, daß ein Zugriff auf die gemeinsame Speichereinrichtung MEM nicht durch eine dazu nicht autorisierte Person veranlaßt wurde, wenn der Zugriff

- durch die Befehlsholeinheit CFU1 erfolgt, oder

- durch die Datenspeicherzugriffseinheit DMU1 erfolgt, und der betreffende Zugriff mit der Ausführung eines Befehls in Zusammenhang steht, der aus einem innerhalb des Mikrocontrollers vorgesehenen Speicher stammt, dessen Inhalt nicht oder nur durch eine Person verändert werden kann, die zum Auslesen und/oder Verändern des Inhalts der gemeinsamen Speichereinrichtung MEM autorisiert ist.

Im betrachteten Beispiel enthält der Mikrocontroller "nur" einen einzigen Speicher, dessen Inhalt nicht oder allenfalls durch dazu autorisierte Personen verändert werden kann, und dies ist die gemeinsame Speichereinrichtung MEM. Wie später noch besser verstanden werden wird, bereitet es jedoch keinerlei Schwierigkeiten, die gemeinsame Speichereinrichtung MEM so auszubilden, daß sie angeforderte Daten nur ausgibt, und/oder ihr zugeführte Daten nur speichert, wenn davon ausgegangen werden kann, daß die betreffende Zugriff auf die gemeinsame Speichereinrichtung MEM mit der Ausführung eines Befehls in Zusammenhang steht, der aus der gemeinsamen Speichereinrichtung MEM selbst oder aus einem anderen Speicher stammt, dessen Inhalt nicht oder allenfalls durch besonders autorisierte Personen verändert werden kann.

Wenn die gemeinsame Speichereinrichtung MEM wie im betrachteten Beispiel in Programmspeicher und Datenspeicher unterteilt ist, wird vorzugsweise überprüft, ob Zugriffe auf den Programmspeicher durch die Befehlsholeinheit CFU1, und Zugriffe auf den Datenspeicher durch die Datenspeicherzugriffseinheit DMU1 erfolgen.

Die Überprüfung, von welcher Komponente des Mikrocontrollers ein jeweiliger Zugriff auf die gemeinsame Speichereinrichtung erfolgt, wird im betrachteten Beispiel anhand von Daten durchgeführt, die über einen vom ersten Bus BUS1 umfaßten ID-Bus übertragen werden. Über den ID-Bus werden sogenannte Identifier übertragen, aus welchen ermittelbar ist, welche der am ersten Bus BUS1 angeschlossenen Einheiten den jeweils aktuellen Buszyklus eingeleitet hat. Genauer gesagt ist jeder der am ersten Bus BUS1 angeschlossenen Einheiten, die Bus-Master werden können, ein bestimmter Identifier zugeordnet, den sie bei der Ausgabe von Daten, Datenanforderungen oder sonstigen Informationen oder Steuersignalen auf den ID-Bus ausgeben. Im betrachteten Beispiel ist es so, daß

- die Befehlsholeinheit CFU1 den Identifier-Wert 1 auf den ID-Bus gibt,
- die Datenspeicherzugriffseinheit DMU1 den Identifier-Wert 2 auf den ID-Bus gibt,
- der DMA-Controller DMA den Identifier-Wert 3 auf den ID-Bus gibt,
- der I/O-Controller I/O den Identifier-Wert 4 auf den ID-Bus gibt,
- die Schnittstelle EBU den Identifier-Wert 5 auf den ID-Bus gibt, und
- die Debug-Ressourcen DEB den Identifier-Wert 6 auf den ID-Bus geben, und
- die aktive Peripherieeinheit APER den Identifier-Wert 7 auf den ID-Bus gibt.

Die Befehlsholeinheit CFU1, die Datenspeicherzugriffseinheit DMU1, der DMA-Controller DMA, der I/O-Controller I/O, die Schnittstelle EBU, die Debug-Ressourcen DEB und die aktive Peripherieeinheit APER enthalten zu diesem Zweck Identifier-Erzeugungseinrichtungen ID1 bis ID7, welche die genannten Identifier auf den ID-Bus geben.

Die von den jeweiligen Einheiten auf den ID-Bus ausgegebenen Identifier sind entweder fest eingestellt oder, sofern sie veränderbar sind, nur durch dazu autorisierte Personen veränderbar.

Durch die Auswertung der Daten, die über den ID-Bus übertragen werden, ist die Steuereinrichtung in der Lage, festzustellen, von welcher Einheit ein Zugriff auf die gemeinsame Speichereinrichtung MEM stammt. Sie muß hierzu nur überprüfen, welcher Wert zusammen mit der Lese- oder Schreibanforderung auf dem ID-Bus übertragen wird.

Wenn zusammen mit einer Lese- oder Schreibanforderung an die gemeinsame Speichereinrichtung auf dem ID-Bus der Wert 1 übertragen wird, erkennt die Steuereinrichtung daran, daß der betreffende Zugriff von der Befehlsholeinheit CFU1 stammt. In diesem Fall besteht keine Gefahr, daß eine nicht dazu autorisierte Person in der gemeinsamen Speichereinrichtung MEM gespeicherte Daten aus der programmgesteuerten Einheit ausgeben läßt oder verändert, so daß dieser Zugriff gestattet werden kann. Noch sicherer wäre es, wenn der Zugriff nur gestattet wird, wenn es sich bei dem Zugriff um einen von der Befehlsholeinheit CFU1 stammenden Lesezugriff auf den Programmspeicher handelt.

Wenn zusammen mit einer Lese- oder Schreibanforderung an die gemeinsame Speichereinrichtung MEM auf dem ID-Bus der Wert 2 übertragen wird, erkennt die Steuereinrichtung daran, daß der betreffende Zugriff von der Datenspeicherzugriffseinheit DMU1 stammt. In diesem Fall muß die Steuereinrichtung zusätzlich überprüfen, ob der betreffende Zugriff mit der Ausführung eines Befehls in Zusammenhang steht oder stehen könnte, der aus einem Speicher stammt, dessen Inhalt nur durch eine Person verändert werden kann, die zum Auslesen des Inhalts der gemeinsamen Speichereinrichtung MEM autorisiert ist. Wenn diese zusätzliche Bedingung erfüllt ist, besteht keine Gefahr, daß eine dazu nicht autorisierte Person in der gemein-

samen Speichereinrichtung MEM gespeicherte Daten aus der programmgesteuerten Einheit ausgeben läßt oder verändert, so daß dieser Zugriff gestattet werden kann. Anderenfalls muß der Zugriff auf die gemeinsame Speichereinrichtung MEM verweigert werden. Wie die Überprüfung der zusätzlichen Bedingung durchgeführt wird, wird später noch genauer beschrieben.

Wenn zusammen mit einer Lese- oder Schreibanforderung an die gemeinsame Speichereinrichtung auf dem ID-Bus der Wert 3, 4, 5, 6 oder 7 übertragen wird, erkennt die Steuereinrichtung daran, daß der betreffende Zugriff vom DMA-Controller DMA, vom I/O-Controller I/O, von der Schnittstelle EBU, von den Debug-Ressourcen DEB, oder von der aktiven Peripherieeinheit APER stammt. In diesem Fall besteht die Gefahr, daß eine dazu nicht autorisierte Person in der gemeinsamen Speichereinrichtung gespeicherte Daten aus der programmgesteuerten Einheit ausgeben läßt oder verändert, so daß dieser Zugriff nicht gestattet wird. In bestimmten Fällen, genauer gesagt, wenn für eine nicht dazu autorisierte Person keine Möglichkeit besteht oder bestand, die den Zugriff anfordernde Einheit zu diesem Zugriff zu veranlassen, könnte dieser Zugriff auch zugelassen werden. Ein solcher Fall kann beispielsweise vorliegen, wenn die vom Mikrocontroller ausgeführten Befehle ausschließlich in der gemeinsamen Speichereinrichtung gespeicherte Befehle sind, und der DMA-Controller DMA, der I/O-Controller I/O, die Schnittstelle EBU, die Debug-Ressourcen DEB, und die aktive Peripherieeinheit APER nur durch vom Mikrocontroller ausgeführte Befehle oder durch besonders autorisierte Personen konfiguriert oder zu bestimmten Aktionen veranlaßt werden können.

Die Überprüfung, von welcher Komponente des Mikrocontrollers ein Zugriff auf die gemeinsame Speichereinrichtung MEM stammt, kann auch auf andere Art und Weise erfolgen.

Eine der möglichen Alternativen besteht darin, daß zumindest die Befehlsholeinheit CFU1 und die Datenspeicherzugriffsein-

heit DMU1, gegebenenfalls aber auch zusätzlich eine, mehrere, oder alle anderen Komponenten, die auf die gemeinsame Speichereinrichtung zugreifen dürfen, über in der Figur nicht gezeigte separate Leitungen mit der gemeinsamen Speichereinrichtung MEM oder der Steuereinrichtung verbunden sind, und daß die genannten Komponenten über die besagten Leitungen signalisieren, ob sie gerade über den Bus BUS1 auf die gemeinsame Speichereinrichtung MEM zugreifen. Auch in diesem Fall kann die gemeinsame Speichereinrichtung MEM oder die Steuereinrichtung zweifelsfrei feststellen, von welcher Komponente ein jeweiliger Zugriff auf die gemeinsame Speichereinrichtung MEM stammt.

Eine weitere Alternative besteht darin, daß Komponente, die einen Zugriff auf die gemeinsame Speichereinrichtung MEM fordert, sich durch die Übertragung entsprechender Daten über den Daten- und/oder den Adreßbus gegenüber der gemeinsamen Speichereinrichtung oder der Steuereinrichtung als Absender des Lese- oder Schreibanforderung identifiziert. Hierbei müßte jedoch sichergestellt werden, daß die von den jeweiligen Komponenten ausgegebenen Identifizierungsdaten nicht oder nur durch bestimmte Personen einstellbar oder veränderbar sind.

Bevor nun im folgenden die Durchführung der vorstehend bereits erwähnten zusätzlichen Überprüfung beschrieben wird, durch welche ermittelt wird, ob ein Zugriff auf die gemeinsame Speichereinrichtung MEM im Zusammenhang mit der Ausführung eines Befehls steht, der aus einem Speicher stammt, dessen Inhalt nicht oder allenfalls durch eine dazu autorisierte Person verändert werden kann, werden zunächst die hierbei mehrfach verwendeten Begriffe "geschützter Speicher" und "ungeschützter Speicher" definiert.

Als "geschützter Speicher" wird ein innerhalb des Mikrocontrollers vorgesehener Speicher bezeichnet, dessen Inhalt nicht oder zumindest nicht durch eine Person veränderbar ist,

die nicht zum Auslesen und/oder Verändern des Inhaltes des gemeinsamen Speichers MEM befugt ist.

Als "ungeschützter Speicher" wird ein Speicher bezeichnet, dessen Inhalt durch eine Person veränderbar ist, die nicht zum Auslesen und/oder Verändern des gemeinsamen Speichers MEM befugt ist. Ein solcher Speicher ist beispielsweise der externe Speicher EXTMEM oder ein nicht geschützter Speicher innerhalb des Mikrocontrollers.

Die vorstehend erwähnte zusätzliche Überprüfung, ob ein Zugriff auf die gemeinsame Speichereinrichtung MEM im Zusammenhang mit der Ausführung eines Befehls steht, der aus einem ungeschützten Speicher stammt, erfolgt im betrachteten Beispiel dadurch, daß die gemeinsame Speichereinrichtung MEM oder die Steuereinrichtung durch Verfolgung der über den Bus BUS1 übertragenen Adressen, Daten und/oder Steuersignale überwacht, ob die Befehlsholeinheit CFU1 zuvor Befehle aus einem ungeschützten Speicher geladen hat.

Wenn dies nicht der Fall ist, d.h., wenn seit der Inbetriebnahme des Mikrocontrollers durch die Befehlsholeinheit CFU1 kein Befehl aus einem ungeschützten Speicher geholt wurde, ist die Angelegenheit eindeutig: der Zugriff auf die gemeinsame Speichereinrichtung MEM kann nicht im Zusammenhang mit der Ausführung eines Befehls stehen, der aus einem ungeschützten Speicher stammt, so daß keine Gefahr besteht, daß die in der gemeinsamen Speichereinrichtung MEM gespeicherten Daten durch eine dazu nicht befugte Person aus dem Mikrocontroller ausgelesen werden oder verändert werden. Der Zugriff auf die gemeinsame Speichereinrichtung kann folglich gestattet werden.

Anderenfalls, genauer gesagt, wenn durch die Befehlsholeinheit CFU1 mehr oder weniger lange vor dem Zugriff auf die gemeinsame Speichereinrichtung MEM ein oder mehrere Befehle aus einem ungeschützten Speicher geholt wurden, besteht die Ge-

fahr, daß die in der gemeinsamen Speichereinrichtung MEM gespeicherten Daten durch eine dazu nicht autorisierte Person aus dem Mikrocontroller ausgelesen werden oder verändert werden. Ob dies tatsächlich der Fall ist, hängt vom Einzelfall ab, und zwar unter anderem davon,

- ob eine Befehlsabarbeitungs-Pipeline vorhanden ist,
- wie viele Stufen die Pipeline aufweist,
- ob eine instruction queue vorhanden ist,
- wie lange eine gegebenenfalls vorhandene instruction queue ist,
- ob die Befehlsholeinheit CFU1 über einen instruction cache verfügt, und
- wie lange es her ist, daß der letzte Befehl aus dem ungeschützten Speicher geholt wurde.

Wenn sicher ist, daß sich weder in der Pipeline, noch in der instruction queue, noch im instruction cache, noch in einer sonstigen Speichereinrichtung des CPU-Subsystems CPUSYS1 zuvor aus einem ungeschützten Speicher geholte Befehle befinden, kann der Zugriff auf die gemeinsame Speichereinrichtung MEM gestattet werden.

Wenn nicht mit Sicherheit feststellbar ist, daß sich weder in der Pipeline, noch in der instruction queue, noch im instruction cache, noch in einer sonstigen Speichereinrichtung der CPU-Subsystems CPUSYS1 zuvor aus einem ungeschützten Speicher geholte Befehle befinden, darf der Zugriff auf die gemeinsame Speichereinrichtung MEM nicht gestattet werden.

Die Überprüfung, ob ein Zugriff auf die gemeinsame Speichereinrichtung MEM im Zusammenhang mit der Ausführung eines Befehls steht, der aus einem ungeschützten Speicher stammt, kann auch auf andere Art und Weise erfolgen.

Eine mögliche Alternative besteht darin, daß die Befehlsholeinheit CFU1 mit der gemeinsamen Speichereinrichtung MEM

über eine in der Figur nicht gezeigte separate Leitung verbunden ist, und die Befehlsholeinheit CFU1 der gemeinsamen Speichereinrichtung MEM über diese separate Leitung signalisiert, ob zuvor aus einem ungeschützten Speicher geholte Befehle noch in der Pipeline, oder in der instruction queue, oder im instruction cache, oder in einer sonstigen Speichereinrichtung des CPU-Subsystems CPUSYS1 gespeichert sind oder gespeichert sein können.

Es könnte auch vorgesehen werden, daß der Programmierer des vom Mikrocontroller auszuführenden Programms durch eine entsprechende Programmerstellung dafür sorgen muß, daß kein Zweifel darüber besteht, ob ein Zugriff auf den gemeinsamen Speicher MEM im Zusammenhang mit der Ausführung eines aus einem ungeschützten Speicher stammenden Befehls steht. Dies kann beispielsweise dadurch erfolgen,

- daß dann, wenn nach der Ausführung von aus einem ungeschützten Speicher stammenden Befehlen wieder aus der gemeinsamen Speichereinrichtung MEM oder einem anderen geschützten Speicher stammende Befehle ausgeführt werden sollen, zunächst eine gewisse Anzahl von neutralen Befehlen wie beispielsweise NOP-Befehlen zur Ausführung gebracht werden, wobei die Anzahl dieser Befehle so groß bemessen ist, daß nach der Ausführung derselben mit Sicherheit davon ausgegangen werden kann, daß in der Pipeline, oder in der instruction queue, oder im instruction cache, oder in einer sonstigen Speichereinrichtung des CPU-Subsystems CPUSYS1 keine aus einem ungeschützten Speicher stammende Befehle mehr gespeichert sind oder gespeichert sein können, die einen Zugriff auf die gemeinsame Speichereinrichtung MEM erfordern, und

- daß dann, wenn nach der Ausführung von aus der gemeinsamen Speichereinrichtung MEM oder einem anderen geschützten Speicher stammenden Befehlen aus einem ungeschützten Speicher stammende Befehle ausgeführt werden sollen, zunächst

eine gewisse Anzahl von neutralen Befehlen wie beispielsweise NOP-Befehlen zur Ausführung gebracht werden, wobei die Anzahl dieser Befehle so groß bemessen ist, daß nach der Ausführung derselben mit Sicherheit davon ausgegangen werden kann, daß in der Pipeline, oder in der instruction queue, oder im instruction cache, oder in einer sonstigen Speichereinrichtung des CPU-Subsystems CPUSYS1 keine aus einem geschützten Speicher stammende Befehle mehr gespeichert sind oder gespeichert sein können, die einen Zugriff auf die gemeinsame Speichereinrichtung MEM erfordern.

Auf diese Art und Weise kann der Programmierer verhindern, daß sich in der Pipeline, oder in der instruction queue, oder im instruction cache, oder in einer sonstigen Speichereinrichtung des CPU-Subsystems CPUSYS1 sowohl aus einem geschützten Speicher als auch aus einem ungeschützten Speicher stammende Befehle befinden, die einen Zugriff auf die gemeinsame Speichereinrichtung MEM erfordern. Dadurch ist einfach und sicher feststellbar, ob ein Zugriff der Datenspeicherzugriffseinheit DMU1 auf die gemeinsame Speichereinrichtung MEM im Zusammenhang mit der Ausführung eines aus einem geschützten Speicher stammenden Befehls oder im Zusammenhang mit der Ausführung eines aus einem ungeschützten Speicher stammenden Befehls steht.

Der Vollständigkeit halber sei angemerkt, daß die Debug-Ressourcen DEB vorzugsweise in der Lage sind, den vorstehend beschriebenen Mechanismus zum Schutz der gemeinsamen Speichereinrichtung MEM zu deaktivieren, wobei eine Deaktivierung jedoch ausschließlich dann möglich sein sollte, wenn die die Deaktivierung veranlassende Person beispielsweise durch Eingabe eines geheimen Codewortes ihre Berechtigung hierzu nachgewiesen hat.

Durch die beschriebene programmgesteuerte Einheit kann unabhängig von den Einzelheiten der praktischen Realisierung unter allen Umständen ausgeschlossen werden, daß der Inhalt

einer zu schützenden Speichereinrichtung durch dazu nicht autorisierte Personen ausgelesen und/oder verändert wird.

Bezugszeichenliste

APER	aktive, d.h. Bus-Master werden könnende Peripherieeinheiten
BUS1	die Komponenten des Mikrocontrollers miteinander verbindender Bus
BUS2	CPUSYS1 und EBU verbindender Bus
CFU1	Befehlsholeinheit von CPUSYS1
CPU1	CPU von CPUSYS1
CPUSYS1	erstes CPU-Subsystem
CPUSYS2	zweites CPU-Subsystem
DEB	Debug-Ressourcen
DMA	DMA-Controller
DMU1	Datenspeicherzugriffseinheit von CPUSYS1
EBU	Interface zu externem Bus
EXTBUS	Externer Bus
EXTMAS	an EXTBUS angeschlossene, Master werden könnende Einheit
EXTMEM	an EXTBUS angeschlossene externe Speichereinrichtung
I/O	I/O-Controller
MEM	gemeinsame Speichereinrichtung
PPER	passive, d.h. nicht Bus-Master werden könnende Peripherieeinheiten

Patentansprüche

1. Programmgesteuerte Einheit mit einer Speichereinrichtung (MEM), auf welche von verschiedenen anderen Komponenten (CFU1, DMU1, CPUSYS2, DMA, I/O, EBU, DEB, APER) der programmgesteuerten Einheit lesend oder schreibend zugegriffen werden kann,
d a d u r c h g e k e n n z e i c h n e t,
daß bei Zugriffen auf die Speichereinrichtung (MEM) überprüft wird, ob der jeweilige Zugriff durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte, und daß die Speichereinrichtung (MEM) angeforderte Daten nur ausgibt, und/oder ihr zugeführte Daten nur speichert, wenn die Überprüfung ergeben hat, daß davon ausgegangen werden kann, daß der betreffende Zugriff nicht durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte.

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 die Speichereinrichtung (MEM) angeforderte Daten ausgibt, wenn die Anforderung von einer Befehlsholeinheit (CFU1) stammt, welche die von der programmgesteuerten Einheit auszuführenden Befehle holt und einer die Befehle ausführenden CPU (CPU1) der programmgesteuerten Einheit zuführt.

3. Programmgesteuerte Einheit nach Anspruch 1 oder 2,
d a d u r c h g e k e n n z e i c h n e t,
daß Zugriffe auf die Speichereinrichtung (MEM), die nicht von der Befehlsholeinheit (CFU1) stammen, welche die von der programmgesteuerten Einheit auszuführenden Befehle holt und einer die Befehle ausführenden CPU (CPU1) der programmgesteuerten Einheit zuführt, nicht oder nur unter bestimmten Umständen bedient werden.

4. Programmgesteuerte Einheit nach einem der vorhergehenden Ansprüche,

d a d u r c h g e k e n n z e i c h n e t,
daß die Speichereinrichtung (MEM) angeforderte Daten nicht ausgibt und/oder ihr zugeführte Daten nicht speichert, wenn der betreffende Zugriff mit der Ausführung eines Befehls in Zusammenhang steht oder stehen könnte, der aus einem Speicher (EXTMEM) stammt, dessen Inhalt durch eine Person verändert werden kann, die zum Auslesen und/oder Verändern des Inhalts der Speichereinrichtung (MEM) nicht autorisiert ist.

5. Programmgesteuerte Einheit nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
daß ein Zugriff auf die Speichereinrichtung (MEM), der von einer Datenspeicherzugriffseinheit (DMU1) stammt, durch welche Daten geholt oder ausgegeben werden, die zur Befehlsausführung benötigt werden oder deren Transfer eine der zur Befehlsausführung gehörenden Operationen ist, nur bedient wird, wenn der betreffende Zugriff nicht mit der Ausführung eines Befehls in Zusammenhang steht oder stehen könnte, der aus einem Speicher (EXTMEM) stammt, dessen Inhalt durch eine Person verändert werden kann, die zum Auslesen und/oder Verändern des Inhalts der Speichereinrichtung (MEM) nicht autorisiert ist.

6. Programmgesteuerte Einheit nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
daß die Überprüfung, ob ein Zugriff auf die Speichereinrichtung (MEM) durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte, die Überprüfung umfaßt, von welcher Komponente (CFU1, DMU1, CPUSYS2, DMA, I/O, EBU, DEB, APER) der programmgesteuerten Einheit der Zugriff auf die Speichereinrichtung (MEM) stammt.

7. Programmgesteuerte Einheit nach Anspruch 6,
d a d u r c h g e k e n n z e i c h n e t,

daß die Überprüfung, von welcher Komponente (CFU1, DMU1, CPUSYS2, DMA, I/O, EBU, DEB, APER) der programmgesteuerten Einheit der Zugriff auf die Speichereinrichtung (MEM) stammt, durch Auswertung eines Identifiers erfolgt, welchen die Komponente, von welcher der Zugriff stammt, über einen Teil des die Komponenten der programmgesteuerten Einheit miteinander verbindenden Bus (BUS1) überträgt.

8. Programmgesteuerte Einheit nach Anspruch 6,
d a d u r c h g e k e n n z e i c h n e t,
daß die Überprüfung, von welcher Komponente (CFU1, DMU1, CPUSYS2, DMA, I/O, EBU, DEB, APER) der programmgesteuerten Einheit der Zugriff auf die Speichereinrichtung (MEM) stammt, durch Auswertung von Signalen erfolgt, welche zumindest von einem Teil der Komponenten, von welchen ein Zugriff auf die Speichereinrichtung erfolgen kann, über dafür reservierte Leitungen zur Speichereinrichtung (MEM) übertragen werden, und durch welche die betreffenden Komponenten signalisieren, ob durch sie gerade ein Zugriff auf die Speichereinrichtung erfolgt oder nicht.

9. Programmgesteuerte Einheit nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
daß die Überprüfung, ob ein Zugriff auf die Speichereinrichtung (MEM) durch eine dazu nicht autorisierte Person veranlaßt wurde oder veranlaßt worden sein könnte, die Überprüfung umfaßt, ob der betreffende Zugriff mit der Ausführung eines Befehls in Zusammenhang steht oder stehen könnte, der aus einem Speicher (EXTMEM) stammt, dessen Inhalt durch eine Person verändert werden kann, die zum Auslesen und/oder Verändern des Inhalts der Speichereinrichtung (MEM) nicht autorisiert ist.

10. Programmgesteuerte Einheit nach Anspruch 9,
d a d u r c h g e k e n n z e i c h n e t,

daß die Überprüfung, ob ein Zugriff auf die Speichereinrichtung (MEM) mit der Ausführung eines Befehls in Zusammenhang steht oder stehen könnte, der aus einem Speicher (EXTMEM) stammt, dessen Inhalt durch eine Person verändert werden kann, die zum Auslesen und/oder Verändern des Inhalts der Speichereinrichtung nicht autorisiert ist, die Verfolgung der Adressen, Daten und/oder Steuersignale umfaßt, welche über einen Bus (BUS1, BUS2) übertragen werden, über welchen die Befehlsholeinheit (CFU1) des Mikrocontrollers die auszuführenden Befehle holt.

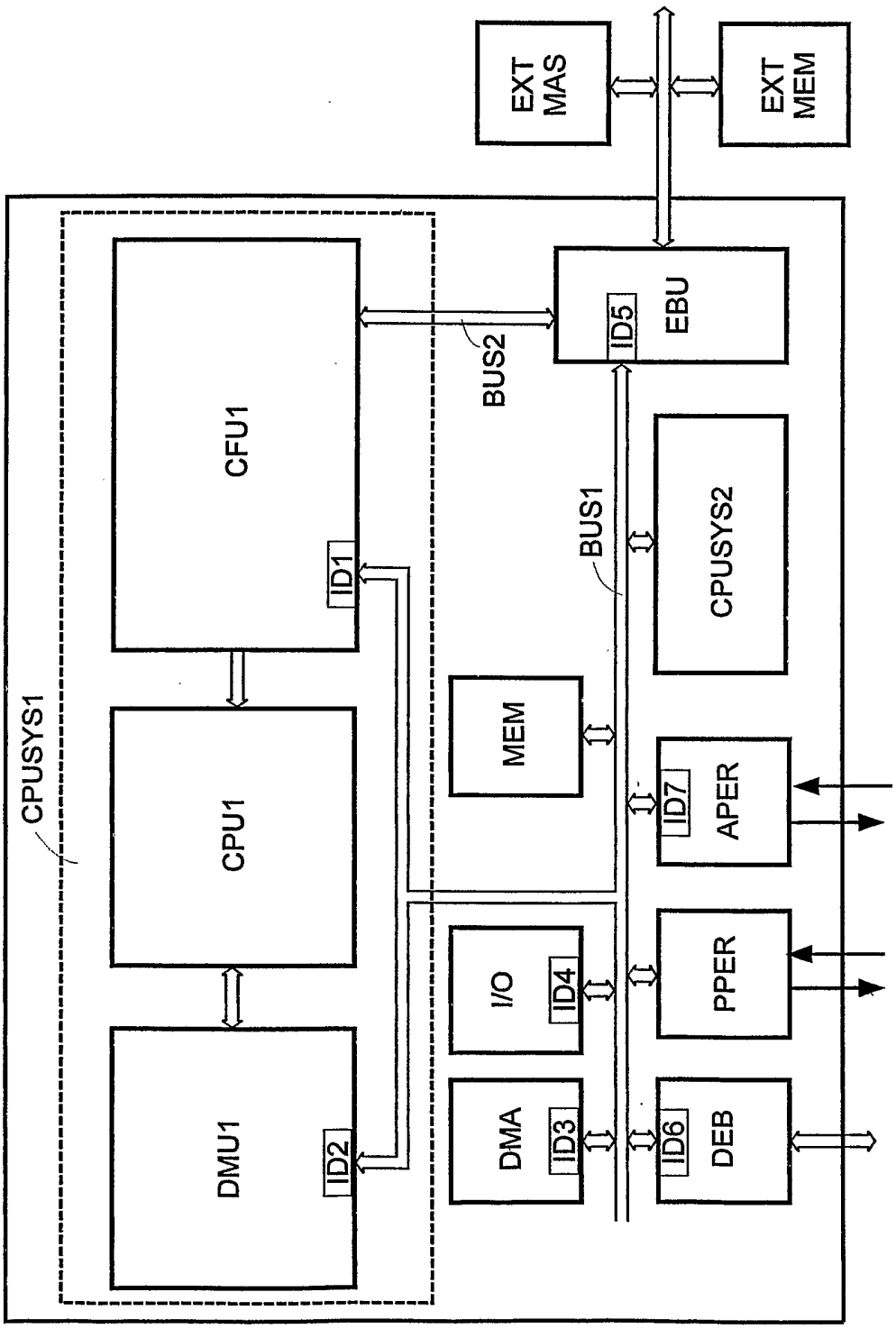
11. Programmgesteuerte Einheit nach Anspruch 9,
d a d u r c h g e k e n n z e i c h n e t,
daß die Überprüfung, ob ein Zugriff auf die Speichereinrichtung (MEM) mit der Ausführung eines Befehls in Zusammenhang steht oder stehen könnte, der aus einem Speicher (EXTMEM) stammt, dessen Inhalt durch eine Person verändert werden kann, die zum Auslesen und/oder Verändern des Inhalts der Speichereinrichtung (MEM) nicht autorisiert ist, durch die Auswertung eines Signals erfolgt, welches die Befehlsholeinheit (CFU1) über eine hierfür reservierte Leitung zur Speichereinrichtung (MEM) überträgt, und durch welches die Befehlsholeinheit (CFU1) signalisiert, ob sich in einer instruction queue, oder in einer Befehlsabarbeitungs-Pipeline, oder in einem instruction cache, oder in einem sonstigen Zwischenspeicher ein zuvor geholter Befehl befindet oder befinden kann, der aus einem Speicher (EXTMEM) stammt, dessen Inhalt durch eine Person verändert werden kann, die zum Auslesen und/oder Verändern des Inhalts der Speichereinrichtung (MEM) nicht autorisiert ist.

12. Programmgesteuerte Einheit nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
daß die Überprüfung, ob ein Zugriff auf die Speichereinrichtung (MEM) durch eine dazu nicht autorisierte Person veran-

laßt wurde oder veranlaßt worden sein könnte, durch eine Steuereinrichtung erfolgt.

13. Programmgesteuerte Einheit nach Anspruch 12,
d a d u r c h g e k e n n z e i c h n e t,
daß die Steuereinrichtung Bestandteil der Speichereinrichtung (MEM) ist.

14. Programmgesteuerte Einheit nach Anspruch 12,
d a d u r c h g e k e n n z e i c h n e t,
daß die Steuereinrichtung eine der Speichereinrichtung (MEM) vorgeschaltete Einrichtung ist.


EXT MAS
EXT MEM
EBU
ID5
BUS2
CFU1
ID1
BUS1
CPUSYS2
CPUSYS1
MEM
CPU1
ID7
APER
I/O
ID4
PPER
DMA
ID3
ID6
DEB
DMU1
ID2