(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 11 2005 002 314 T5** 2007.09.06

(12) **Veröffentlichung**

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2006/047762**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2005 002 314.1**
(86) PCT-Aktenzeichen: **PCT/US2005/039048**
(86) PCT-Anmeldetag: **27.10.2005**
(87) PCT-Veröffentlichungstag: **04.05.2006**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **06.09.2007**

(51) Int Cl.[8]: ***G06F 21/00*** (2006.01)
G06F 9/46 (2006.01)

(30) Unionspriorität:
10/974,217 **27.10.2004** **US**

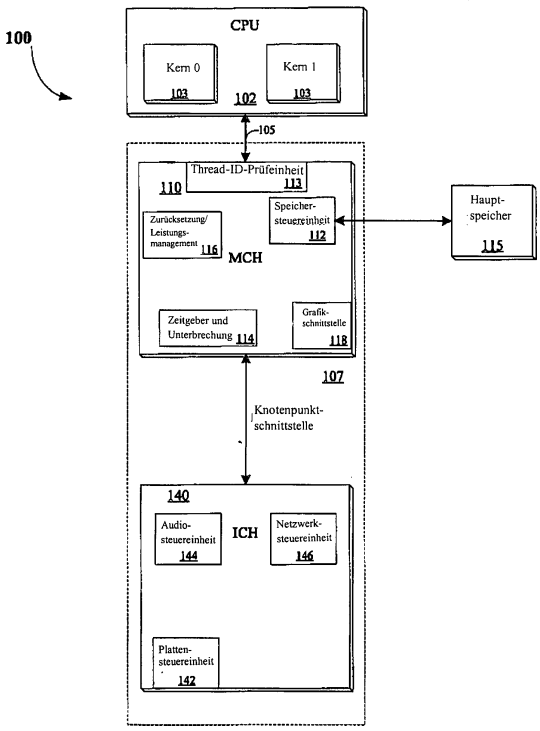
(74) Vertreter:
BOEHMERT & BOEHMERT, 28209 Bremen

(71) Anmelder:
Intel Corporation, Santa Clara, Calif., US

(72) Erfinder:
Poisner, David, Folsom, Calif., US

(54) Bezeichnung: **Mechanismus zum Erzeugen eingeschränkter und uneingeschränkter Ausführungsumgebungen**

(57) Hauptanspruch: Computersystem, umfassend:
eine zentrale Verarbeitungseinheit (CPU) mit:
einem ersten Thread mit einer ersten zugehörigen Thread-Kennung (ID); und
einem zweiten Thread mit einer zweiten zugehörigen Thread-ID; und
einen Chipsatz, der so verbunden ist, daß er Zugriffsanforderungen von der CPU empfängt und eine der Zugriffsanforderung beigeschlossene Thread-ID prüft, um zu bestimmen, welcher Thread Zugriff fordert.



Beschreibung

[0001] Hierin ist urheberrechtlich geschütztes Material enthalten. Der Inhaber des Urheberrechts hat keine Einwände gegen die Vervielfältigung durch Kopieren der Patentoffenbarung durch eine beliebige Person, so wie sie in den Patentakten oder -dateien des Patent- und Markenamtes aussieht, behält sich jedoch ansonsten alle durch das Urheberrecht gewährten Rechte vor.

GEBIET DER ERFINDUNG

[0002] Die vorliegende Erfindung betrifft Computersysteme; insbesondere betrifft die vorliegende Erfindung Computersysteme, die in einer vertrauenswürdigen oder geschützten Umgebung operieren können.

[0003] Es gibt eine Vielzahl von Anwendungen, für die eine „isolierte Ausführung" und eine „isolierte Speicherung" von Vorteil wären. Isolierte Ausführung ist die Fähigkeit eines Ausführungscodes, der durch andere Software nicht unterbrochen oder beobachtet werden kann. Isolierte Ausführung ist wichtig für Sicherheitssoftware sowie für den Schutz vor nicht bösartiger, aber schlecht geschriebener Software. Zum Beispiel kann ein schlecht geschriebener Gerätetreiber potentiell den ordnungsgemäßen Betrieb eines Betriebssystems (OS) stören, was einen Absturz zur Folge hat, der den Betrieb zeitkritischer Anwendungen (wie eines digitalen Videorecorders) verhindert.

[0004] Isolierte Speicherung bezieht sich auf eine Fähigkeit, Daten in einem nicht flüchtigen Speicher zu speichern, auf den nur ein autorisierter Besitzer zugreifen kann. Somit kann keine andere Software die Daten modifizieren oder löschen. Das Löschungskonzept ist wichtig, weil ein Fehler in einem OS oder seinem Gerätetreiber dazu führen könnte, daß auf Daten oder eine Platte nicht mehr zugegriffen werden kann.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0005] Die Erfindung ist beispielhaft und nicht einschränkend in den Figuren der beigefügten Zeichnungen illustriert, in denen gleiche Bezugszeichen ähnliche Elemente bezeichnen und in denen:

[0006] Fig. 1 ein Blockdiagramm einer Ausführungsform eines Computersystems ist;

[0007] Fig. 2 ein Blockdiagramm ist, das eine Ausführungsform einer mit einer Platte verbundenen Plattensteuereinheit illustriert; und

[0008] Fig. 3 ein Ablaufschema einer Ausführungsform für den Betrieb eines Computersystems ist.

DETAILLIERTE BESCHREIBUNG

[0009] Es wird ein Mechanismus für eingeschränkte und uneingeschränkte Ausführungsumgebungen bei einem Computersystem beschrieben. In der folgenden detaillierten Beschreibung der vorliegenden Erfindung werden zahlreiche spezifische Details dargelegt, um ein umfassendes Verständnis der vorliegenden Erfindung zu gewährleisten. Es ist jedoch für den Fachmann auf dem Gebiet offensichtlich, daß die vorliegende Erfindung ohne diese spezifischen Details praktiziert werden kann. Andererseits werden hinlänglich bekannte Strukturen und Vorrichtungen in Form von Blockdiagrammen statt im Detail gezeigt, um die vorliegende Erfindung nicht undurchschaubar zu machen.

[0010] Die Bezugnahme auf „eine Ausführungsform" in der Beschreibung bedeutet, daß ein(e) bestimmte(s) Merkmal, Struktur oder Eigenschaft, die im Zusammenhang mit der Ausführungsform beschrieben wird, in mindestens einer Ausführungsform der Erfindung eingeschlossen ist. Die Vorkommen der Formulierung „in einer Ausführungsform" an verschiedenen Stellen der Beschreibung beziehen sich nicht unbedingt alle auf dieselbe Ausführungsform.

[0011] Einige Abschnitte der folgenden detaillierten Beschreibungen werden in Form von Algorithmen und symbolischen Darstellungen von Operationen auf Datenbits in einem Computerspeicher präsentiert. Diese algorithmischen Beschreibungen und Darstellungen sind die Mittel, die von Datenverarbeitungsfachleuten verwendet werden, um anderen Fachleuten den Inhalt ihrer Arbeit am effektivsten zu vermitteln.

[0012] Ein Algorithmus wird hier, und im allgemeinen, verstanden als eine in sich widerspruchsfreie Abfolge von Schritten, die zu einem gewünschten Ergebnis führt. Die Schritte sind solche, die eine physikalische Verarbeitung physikalischer Größen erfordern. Üblicherweise, jedoch nicht unbedingt, haben diese Größen die Form elektrischer oder magnetischer Signale, die gespeichert, übertragen, kombiniert, verglichen und anderweitig verarbeitet werden können. Es hat sich zuweilen als praktisch erwiesen, hauptsächlich aus Gründen der allgemeinen Üblichkeit, auf diese Signale als Bits, Werte, Elemente, Symbole, Zeichen, Ausdrücke, Zahlen oder dergleichen Bezug zu nehmen.

[0013] Es sollte jedoch bedacht werden, daß all diese und ähnliche Begriffe den eigentlichen physikalischen Größen zuzuordnen sind und lediglich praktische Etiketten sind, mit denen diesen Größen versehen wurden. Sofern nicht im Einzelfall anders angegeben, wie aus der folgenden Erörterung zu entnehmen, betreffen in der gesamten Beschreibung Erörterungen unter Verwendung von Begriffen wie „verar-

beiten" oder "berechnen" oder „rechnen" oder "bestimmen" oder „anzeigen" oder dergleichen den Betrieb und die Prozesse eines Computersystems oder einer ähnlichen elektronischen Recheneinrichtung, die in den Registern und Speichern des Computersystems als physikalische (elektronische) Größen dargestellte Daten zu/in andere(n) Daten verarbeitet und umformt, die in ähnlicher Weise als physikalische Größen in den Speichern oder Registern oder anderen solchen Informationsspeicher-, Übertragungs- oder Anzeigeeinrichtungen des Computersystems dargestellt werden.

[0014] Die vorliegende Erfindung betrifft auch eine Vorrichtung zum Ausführen der hierin dargelegten Operationen. Diese Vorrichtung kann speziell für die erforderlichen Zwecke konstruiert sein, oder sie kann einen allgemein einsetzbaren Computer umfassen, der durch ein in dem Computer gespeichertes Computerprogramm selektiv aktiviert oder neu konfiguriert wird. Ein solches Computerprogramm kann auf einem computerlesbaren Speichermedium gespeichert sein, wie, jedoch nicht beschränkt auf, jede Art von Platte einschließlich Floppy-Disks, optische Platten, CD-ROMs und magnetooptische Platten, Nur-Lese-Speicher (ROMs), Speicher mit wahlfreiem Zugriff (RAMs), EPROMs, EEPROMs, magnetische oder optische Karten oder jede Art von Medien, die für das Speichern elektronischer Befehle geeignet und jeweils mit einem Bus des Computersystems verbunden sind.

[0015] Die hierin präsentierten Algorithmen und Anzeigen sind nicht an eine(n) bestimmten Computer oder andere Vorrichtung gebunden. Verschiedene allgemein einsetzbare Systeme können mit Programmen gemäß den hierin dargelegten Lehren verwendet werden, oder es kann sich als praktisch erweisen, eine speziellere Vorrichtung zu konstruieren, um die erforderlichen Verfahrensschritte auszuführen. Die erforderliche Struktur für eine Vielzahl dieser Systeme ist der nachstehenden Beschreibung zu entnehmen. Darüber hinaus ist die vorliegende Erfindung nicht unter Bezugnahme auf eine bestimmte Programmiersprache beschrieben. Es kann eine Vielzahl von Programmiersprachen verwendet werden, um die Lehren der Erfindung, wie hierin beschrieben, umzusetzen.

[0016] Die Befehle der Programmiersprache(n) können durch eine oder mehrere Verarbeitungsvorrichtungen (z. B. Prozessoren, Steuereinheiten, zentrale Verarbeitungseinheiten (CPUs), Ausführungskerne etc.) ausgeführt werden.

[0017] Fig. 1 ist ein Blockdiagramm einer Ausführungsform eines Computersystems **100**. Das Computersystem **100** schließt eine zentrale Verarbeitungseinheit (CPU) **102** ein, die mit einem Bus **105** verbunden ist. Gemäß einer Ausführungsform schließt die CPU **102** mehrere Kerne **103** ein. Zum Beispiel schließt die CPU **102** Kern 0 und Kern 1 ein. Bei einer Ausführungsform betreibt das Computersystem **100** mehrere Betriebssysteme gleichzeitig. Bei einer solchen Ausführungsform operiert auf jedem Kern **103** ein separates OS. So operiert ein erstes OS auf dem Kern 0, während ein zweites OS auf dem Kern 1 operiert. Bei einer weiteren Ausführungsform kann jeder einzelne Kern mehr als einen Thread ausführen. In der nachstehenden Beschreibung wird der Begriff Thread jedoch verwendet, um eine Prozessorfunktion anzuzeigen, die ein OS umsetzt.

[0018] Bei einer Ausführungsform ist die CPU **102** ein Prozessor der Pentium®-Prozessorfamilie einschließlich der Pentium® II-Prozessorfamilie, Pentium® III-Prozessoren und Pentium® IV-Prozessoren, erhältlich von Intel Corporation, Santa Clara, Kalifornien. Alternativ können andere CPUs verwendet werden.

[0019] Ein Chipsatz **107** ist ebenfalls mit dem Bus **105** verbunden. Der Chipsatz **107** schließt einen Speichersteuerknotenpunkt (MCH) **110** ein. Der MCH **110** kann eine Speichersteuereinheit **112** einschließen, die mit einem Hauptsystemspeicher **115** verbunden ist. Der Hauptsystemspeicher **115** speichert Daten und Befehlsfolgen, die durch die CPU **102** oder eine andere in das System **100** eingeschlossene Vorrichtung ausgeführt werden. Bei einer Ausführungsform schließt der Hauptsystemspeicher **115** einen dynamischen Speicher mit wahlfreiem Zugriff (DRAM) ein; der Hauptsystemspeicher **115** kann jedoch unter Verwendung anderer Speicherarten umgesetzt werden.

[0020] Gemäß einer Ausführungsform schließt der MCH **110** eine Thread-ID-Prüfeinheit **112** ein. Die ID-Prüfeinheit **116** empfängt von der CPU über den Bus **105** eine Thread-ID, die anzeigt, welcher Thread einen Speicher- oder I/O-Zugriff ausführt. Bei einer Ausführungsform weist die Thread-ID-Prüfeinheit **112** einem bestimmten Thread bestimmte Speicherbereiche zu.

[0021] Bei einer weiteren Ausführungsform wird einem uneingeschränkten Thread Zugriff auf alle Speicherseiten gewährt, während einem oder mehreren anderen eingeschränkten Thread(s) lediglich Zugriff auf bestimmte Seiten gewährt wird. Weiterhin ermöglichen es die CPU **102** und der Chipsatz **110**, daß eingeschränkte Komponenten der Computersystem-**100** Plattform modifiziert werden, während die uneingeschränkten Komponenten der Plattform nicht zurückgesetzt werden. Bei noch einer weiteren Ausführungsform kann der uneingeschränkte Thread Überwachungszugriff über eingeschränkte Threads haben. Ein solcher Überwachungszugriff ermöglicht, daß der uneingeschränkte Thread die Zugriffsniveaus der eingeschränkten Threads prüft.

[0022] Der MCH schließt auch Zeitgeber und Unterbrechungsressourcen **114** und Zurücksetzungs- und Leistungsmanagementregister **116** ein. Die Zeitgeber- und Unterbrechungsressourcen sind den uneingeschränkten Threads beigegeben, damit der uneingeschränkte Thread über Zeitgeber- und Unterbrechungsleistungen verfügen kann, die durch den/die uneingeschränkten Thread(s) nicht (absichtlich oder versehentlich) modifiziert werden können.

[0023] Die Zurücksetzungs- und Leistungsmanagementregister **116** sind ebenfalls für die uneingeschränkten Threads umgesetzt. Die Zurücksetzungs- und Leistungsmanagementregister **116** verursachen Ereignisse, die durch die eingeschränkten Threads gemanagt werden. Dadurch können die eingeschränkten Threads die Zurücksetzungs- und Leistungsmanagementpolitiken innehaben. Gemäß einer Ausführungsform ermöglicht der MCH **110**, daß kritische Ereignisse, die normalerweise eine Systemmanagementunterbrechung (SMI) verursachen würden, statt dessen eine Unterbrechung des uneingeschränkten Thread verursachen. Dadurch können OS-unabhängige Threads auf dem uneingeschränkten Thread ausgeführt werden, ohne den Ausführungsfluß des auf dem eingeschränkten Thread laufenden OS zu stören.

[0024] Der MCH **110** kann auch eine Grafikschnittstelle **113** einschließen, die mit einem Grafikbeschleuniger **130** verbunden ist. Gemäß einer Ausführungsform ermöglicht die Grafikschnittstelle **113**, daß ein uneingeschränkter Thread ein Fenster auf einem Anzeigemonitor (nicht gezeigt) so anzeigt, daß ein einem eingeschränkten Thread zugehöriges Fenster nicht über dem dem uneingeschränkten Thread zugehörigen Fenster angeordnet werden kann.

[0025] Der MCH **110** ist über eine Knotenpunktschnittstelle mit einem Eingangs/Ausgangs-Steuerknotenpunkt (ICH) **140** verbunden. Der ICH **140** stellt eine Schnittstelle für Eingangs/Ausgangs-(I/O-)Einrichtungen in dem Computersystem **100** bereit. Der ICH **140** schließt eine Plattensteuereinheit **142**, eine Audiosteuereinheit **144** und eine Netzwerksteuereinheit **146** ein. Die Plattensteuereinheit **142** ist über eine Schnittstelle mit einem oder mehreren Plattenlaufwerk(en) (nicht gezeigt) verbunden, um die Datenübertragung zwischen dem Chipsatz **107** und den Laufwerken zu steuern.

[0026] Gemäß einer Ausführungsform wird dem uneingeschränkten Thread über die Plattensteuereinheit **142** vollständiger Zugriff auf Daten auf der Festplatte **260** gewährt. Bei einer solchen Ausführungsform wird jedoch eingeschränkten Threads nicht gestattet, auf bestimmte Abschnitte der Festplatte **260** zuzugreifen. Fig. 2 ist ein Blockschaltbild, das eine Ausführungsform einer mit einer Platte verbundenen Plattensteuereinheit **142** illustriert. Die Plattensteuereinheit **142** schließt Schnittstellen **230** und DMA-Maschinen **250** ein. Die Schnittstellen **230** schließen die Schnittstellen 0 und 1 ein.

[0027] Die Schnittstelle 0 und die Schnittstelle 1 stellen unabhängige Schnittstellen für Software bereit, die auf Daten auf der Festplatte **260** zugreift. Zum Beispiel kann ein Konfigurationsraum durch den uneingeschränkten Thread eingesehen werden, während der andere durch einen oder mehrere uneingeschränkte(n) Thread(s) eingesehen werden kann. Die DMA-Maschinen **250** ermöglichen direkte Speicherzugriffe zwischen der Festplatte **260**.

[0028] Wiederum unter Bezugnahme auf Fig. 1 operiert die Audiosteuereinheit **144**, um die Aufnahme und Wiedergabe von Klängen zu koordinieren. Gemäß einer Ausführungsform ermöglicht die Audiosteuereinheit **144**, daß ein Ausgangs-Audiostrom unabhängig für die uneingeschränkten und eingeschränkten Threads operiert. Dies verhindert, daß der eingeschränkte Thread den uneingeschränkten Thread "stummschaltet". Bei einer weiteren Ausführungsform schließt die Audiosteuereinheit **144** einen Modus ein, um zu ermöglichen, daß ein Eingangsstrom zuerst zu dem uneingeschränkten Thread übertragen wird, der entscheiden kann, ob die Audiodaten an den eingeschränkten Thread weitergeleitet werden sollten.

[0029] Die Netzwerksteuereinheit **146** verbindet das Computersystem **100** mit einem Computernetzwerk (in Fig. 1 nicht gezeigt) und unterstützt die Kommunikation zwischen den Maschinen. Gemäß einer Ausführungsform wird dem uneingeschränkten Thread vollständiger Zugriff auf die Netzwerksteuereinheit **146** gewährt, während die eingeschränkten Threads keinen vollständigen Zugriff haben. Bei einer Ausführungsform werden durch die eingeschränkten Threads "übertragene" Pakete zuerst für eine Inspektion oder Modifikation durch den uneingeschränkten Thread zugänglich gemacht. Weiterhin können vom Netzwerk empfangene Pakete zuerst durch den uneingeschränkten Thread inspiziert werden, bevor sie dem eingeschränkten Thread zugänglich gemacht werden.

[0030] Fig. 3 ist ein Ablaufschema einer Ausführungsform für die Speicher- oder I/O-Zugriffsanforderung bei dem Computersystem **100**. Beim Verarbeitungsblock **310** empfängt der Chipsatz **107** von der CPU **102** eine Anforderung, auf eine Vorrichtung zuzugreifen. Zum Beispiel kann der MCH **110** eine solche Anforderung, auf den Speicher **115** zuzugreifen, empfangen. In ähnlicher Weise kann die Plattensteuereinheit **142** die Anforderung empfangen, auf die Festplatte **260** zuzugreifen.

[0031] Beim Verarbeitungsblock **320** prüft die Thread-ID-Prüfeinheit **116** die der Anforderung bei-

geschlossene Thread-ID, um den anfordernden Thread zu bestimmen. Beim Entscheidungsblock **330** wird bestimmt, ob der anfordernde Thread ein eingeschränkter Thread oder ein uneingeschränkter Thread ist. Wenn es ein uneingeschränkter Thread ist, wird dem uneingeschränkten Thread vollständiger Zugriff auf Daten von der Vorrichtung, auf das die Anforderung zielt, gewährt, Verarbeitungsblock **340**.

[0032] Wenn es jedoch ein eingeschränkter Thread ist, findet eine Prüfung statt, um zu bestimmen, ob der eingeschränkte Thread Zugriff auf die angeforderten Ressourcen hat, Verarbeitungsblock **350**. Beim Entscheidungsblock **360** wird bestimmt, ob der eingeschränkte Thread auf die angeforderten Daten zugreifen kann. Wenn Zugriff ausgewiesen wird, wird dem Thread Zugriff auf die angeforderten Daten von dem Gerät, auf das die Anforderung zielt, gewährt, Verarbeitungsblock **370**. Wird jedoch bestimmt, daß der Thread keinen Zugriff auf die angeforderten Daten hat, wird der Zugriff verweigert, Verarbeitungsblock **380**.

[0033] Obgleich viele Veränderungen und Modifikationen der vorliegenden Erfindung für einen Fachmann nach dem Lesen der vorstehenden Beschreibung zweifellos offensichtlich sind, versteht es sich, daß jede besondere Ausführungsform, die illustrationshalber gezeigt und beschrieben ist, in keiner Weise als einschränkend angesehen werden soll. Daher sollen Bezugnahmen auf Details verschiedener Ausführungsformen den Umfang der Ansprüche nicht einschränken, die als solche nur diejenigen Merkmale wiedergeben, die als wesentlich für die Erfindung angesehen werden.

Zusammenfassung

[0034] Gemäß einer Ausführungsform wird ein Computersystem offenbart. Das Computersystem schließt eine zentrale Verarbeitungseinheit (CPU) mit einem ersten Thread mit einer ersten zugehörigen Thread-Kennung (ID) und einem zweiten Thread mit einer zweiten zugehörigen Thread-ID ein. Das Computersystem schließt ebenfalls einen Chipsatz ein, der so verbunden ist, daß er Zugriffsanforderungen von der CPU empfängt und eine der Zugriffsanforderung beigeschlossene Thread-ID prüft, um zu bestimmen, welcher Thread Zugriff fordert.

Patentansprüche

1. Computersystem, umfassend:
eine zentrale Verarbeitungseinheit (CPU) mit:
einem ersten Thread mit einer ersten zugehörigen Thread-Kennung (ID); und
einem zweiten Thread mit einer zweiten zugehörigen Thread-ID; und
einen Chipsatz, der so verbunden ist, daß er Zugriffsanforderungen von der CPU empfängt und eine der Zugriffsanforderung beigeschlossene Thread-ID prüft, um zu bestimmen, welcher Thread Zugriff fordert.

2. Computersystem nach Anspruch 1, dadurch gekennzeichnet, daß der erste Thread ein uneingeschränkter Thread ist, dem vollständiger Zugriff auf Daten gewährt wird, und der zweite Thread ein eingeschränkter Thread ist, dem beschränkter Zugriff auf Daten gewährt wird.

3. Computersystem nach Anspruch 2, das weiterhin eine mit dem Chipsatz verbundene Speichereinrichtung umfaßt, wobei dem uneingeschränkten Thread Zugriff auf alle Seiten der Speichereinrichtung gewährt wird und dem eingeschränkten Thread Zugriff auf zugewiesene Bereiche der Speichereinrichtung gewährt wird.

4. Computersystem nach Anspruch 2, dadurch gekennzeichnet, daß die CPU und der Chipsatz ermöglichen, daß eingeschränkte Komponenten des Computersystems modifiziert werden, während die uneingeschränkten Komponenten unmodifiziert bleiben.

5. Computersystem nach Anspruch 4, dadurch gekennzeichnet, daß der uneingeschränkte Thread Überwachungszugriff über den eingeschränkten Thread hat, damit der uneingeschränkte Thread die Zugriffsniveaus des eingeschränkten Threads prüfen kann.

6. Computersystem nach Anspruch 2, dadurch gekennzeichnet, daß der Chipsatz Zeitgeber- und Unterbrechungsressourcen umfaßt, die durch den eingeschränkten Thread nicht modifiziert werden können.

7. Computersystem nach Anspruch 2, dadurch gekennzeichnet, daß der Chipsatz weiterhin Register umfaßt, um es dem uneingeschränkten Thread zu ermöglichen, Ereignisse zu verursachen, die durch die eingeschränkten Threads gemanagt werden.

8. Computersystem nach Anspruch 2, dadurch gekennzeichnet, daß der Chipsatz eine Grafikschnittstelle umfaßt, um dem uneingeschränkten Thread zu ermöglichen, ein Fenster auf einem Monitor so anzuzeigen, daß ein dem eingeschränkten Thread zugehöriges Fenster nicht über dem dem uneingeschränkten Thread zugehörigen Fenster angeordnet werden kann.

9. Computersystem nach Anspruch 2, dadurch gekennzeichnet, daß der Chipsatz eine Plattensteuereinheit umfaßt, um dem uneingeschränkten Thread vollständigen Zugriff auf Daten auf einer mit der Plattensteuereinheit **142** verbundenen Festplatte zu gewähren und den eingeschränkten Threads Zugriff auf

bestimmte Abschnitte der Festplatte zu gewähren.

10. Computersystem nach Anspruch 9, dadurch gekennzeichnet, daß die Plattensteuereinheit umfaßt:
eine erste, dem uneingeschränktem Thread zugehörige Schnittstelle;
eine zweite, dem eingeschränktem Thread zugehörige Schnittstelle; und
eine DMA-Maschine.

11. Computersystem nach Anspruch 2, dadurch gekennzeichnet, daß der Chipsatz eine Audiosteuereinheit umfaßt, um einem Ausgangs-Audiostrom zu ermöglichen, unabhängig für die uneingeschränkten und eingeschränkten Threads zu operieren, um zu verhindern, daß der eingeschränkte Thread den uneingeschränkten Thread stummschaltet.

12. Computersystem nach Anspruch 11, dadurch gekennzeichnet, daß die Audiosteuereinheit einen Modus einschließt, um zu ermöglichen, daß ein Eingangsstrom zuerst zu dem uneingeschränkten Thread übertragen wird, um zu bestimmen, ob die Audiodaten an den eingeschränkten Thread weitergeleitet werden sollten.

13. Computersystem nach Anspruch 2, dadurch gekennzeichnet, daß der Chipsatz eine Netzwerksteuereinheit umfaßt, um dem uneingeschränkten Thread vollständigen Zugriff und dem eingeschränkten Thread eingeschränkten Zugriff zu gewähren.

14. Computersystem nach Anspruch 13, dadurch gekennzeichnet, daß durch die eingeschränkten Threads übertragene Pakete für eine Inspektion oder Modifikation durch den uneingeschränkten Thread zugänglich gemacht werden und vom Netzwerk empfangene Pakete zuerst durch den uneingeschränkten Thread inspiziert werden, bevor sie dem eingeschränkten Thread zugänglich gemacht werden.

15. Verfahren, umfassend:
Empfangen einer Anforderung, auf Datenressourcen einer Einrichtung zuzugreifen;
Prüfen einer der Anforderung zugehörigen Thread-Kennung (ID); und
Gewähren eines vollständigen Zugriffs auf die Datenressourcen, wenn die Thread-ID eine Anforderung von einem uneingeschränkten Thread anzeigt.

16. Verfahren nach Anspruch 15, das weiterhin das Gewähren von Zugriff auf festgelegte Komponenten der Datenressourcen umfaßt, wenn die Thread-ID eine Anforderung von einem eingeschränkten Thread anzeigt.

17. System, umfassend:
ein Festplattenlaufwerk; und
eine mit dem Festplattenlaufwerk verbundene Plattensteuereinheit, einschließend:
eine erste, einem uneingeschränktem Thread zugehörige Schnittstelle, um dem uneingeschränkten Thread vollständigen Zugriff auf Daten auf dem Festplattenlaufwerk zu gewähren; und
eine zweite, einem eingeschränktem Thread zugehörige Schnittstelle, um dem eingeschränkten Thread Zugriff auf bestimmte Abschnitte der Festplatte zu gewähren.

18. System nach Anspruch 9, dadurch gekennzeichnet, daß die Plattensteuereinheit weiterhin eine DMA-Maschine umfaßt.

19. Fertigungsartikel, das ein oder mehrere computerlesbare(s) Medium/Medien einschließt, das/die ein Befehlsprogramm verkörpert/n, dadurch gekennzeichnet, daß das Befehlsprogramm, wenn es durch eine Verarbeitungseinheit ausgeführt wird, die Verarbeitungseinheit zu folgendem veranlaßt:
Empfangen einer Anforderung, auf Datenressourcen einer Vorrichtung zuzugreifen;
Prüfen einer der Anforderung zugehörigen Thread-Kennung (ID); und
Gewähren eines vollständigen Zugriffs auf die Datenressourcen, wenn die Thread-ID eine Anforderung von einem uneingeschränkten Thread anzeigt.

20. Fertigungsartikel nach Anspruch 19, dadurch gekennzeichnet, daß das Befehlsprogramm, wenn es durch eine Verarbeitungseinheit ausgeführt wird, die Verarbeitungseinheit weiterhin dazu veranlaßt, Zugriff auf festgelegte Komponenten der Datenressourcen zu gewähren, wenn die Thread-ID eine Anforderung von einem eingeschränkten Thread anzeigt.

21. Chipsatz, der eine Thread-Kennungs-(ID-)Prüfeinheit umfaßt, um Thread-IDs, die einer von einer zentralen Verarbeitungseinheit (CPU) empfangenen Zugriffsanforderung beigeschlossen sind, zu prüfen, um zu bestimmen, ob die Zugriffsanforderung von einem ersten Thread mit einer ersten zugehörigen Thread-Kennung (ID) oder einem zweiten Thread mit einer zweiten zugehörigen Thread-ID stammt.

22. Chipsatz nach Anspruch 21, dadurch gekennzeichnet, daß der erste Thread ein uneingeschränkter Thread ist, dem vollständiger Zugriff auf Daten gewährt wird, und der zweite Thread ein eingeschränkter Thread ist, dem beschränkter Zugriff auf Daten gewährt wird.

23. Chipsatz nach Anspruch 4, dadurch gekennzeichnet, daß der uneingeschränkte Thread Überwachungszugriff über den eingeschränkten Thread hat, damit der uneingeschränkte Thread die Zugriffsniveaus des eingeschränkten Threads prüfen kann.

24. Chipsatz nach Anspruch 22, dadurch gekennzeichnet, daß der Chipsatz Zeitgeber- und Unterbrechungsressourcen umfaßt, die durch den eingeschränkten Thread nicht modifiziert werden können.

25. Chipsatz nach Anspruch 24, dadurch gekennzeichnet, daß der Chipsatz weiterhin Register umfaßt, um dem uneingeschränkten Thread zu ermöglichen, Ereignisse zu verursachen, die durch die eingeschränkten Threads gemanagt werden.

26. Chipsatz nach Anspruch 22, dadurch gekennzeichnet, daß der Chipsatz eine Grafikschnittstelle umfaßt, um es dem uneingeschränkten Thread zu ermöglichen, ein Fenster auf einem Monitor so anzuzeigen, daß ein dem eingeschränkten Thread zugehöriges Fenster nicht über dem dem uneingeschränkten Thread zugehörigen Fenster angeordnet werden kann.

27. Chipsatz nach Anspruch 22, dadurch gekennzeichnet, daß der Chipsatz eine Plattensteuereinheit umfaßt, um dem uneingeschränkten Thread vollständigen Zugriff auf Daten auf einer mit der Plattensteuereinheit **142** verbundenen Festplatte zu gewähren und den eingeschränkten Threads Zugriff auf bestimmte Abschnitte der Festplatte zu gewähren.

28. Chipsatz nach Anspruch 22, dadurch gekennzeichnet, daß der Chipsatz eine Audiosteuereinheit umfaßt, um einem Ausgangs-Audiostrom zu ermöglichen, unabhängig für die uneingeschränkten und eingeschränkten Threads zu operieren, um zu verhindern, daß der eingeschränkte Thread den uneingeschränkten Thread stummschaltet.

29. Chipsatz nach Anspruch 22, dadurch gekennzeichnet, daß der Chipsatz eine Netzwerksteuereinheit umfaßt, um dem uneingeschränkten Thread vollständigen Zugriff und dem eingeschränkten Thread eingeschränkten Zugriff zu gewähren.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

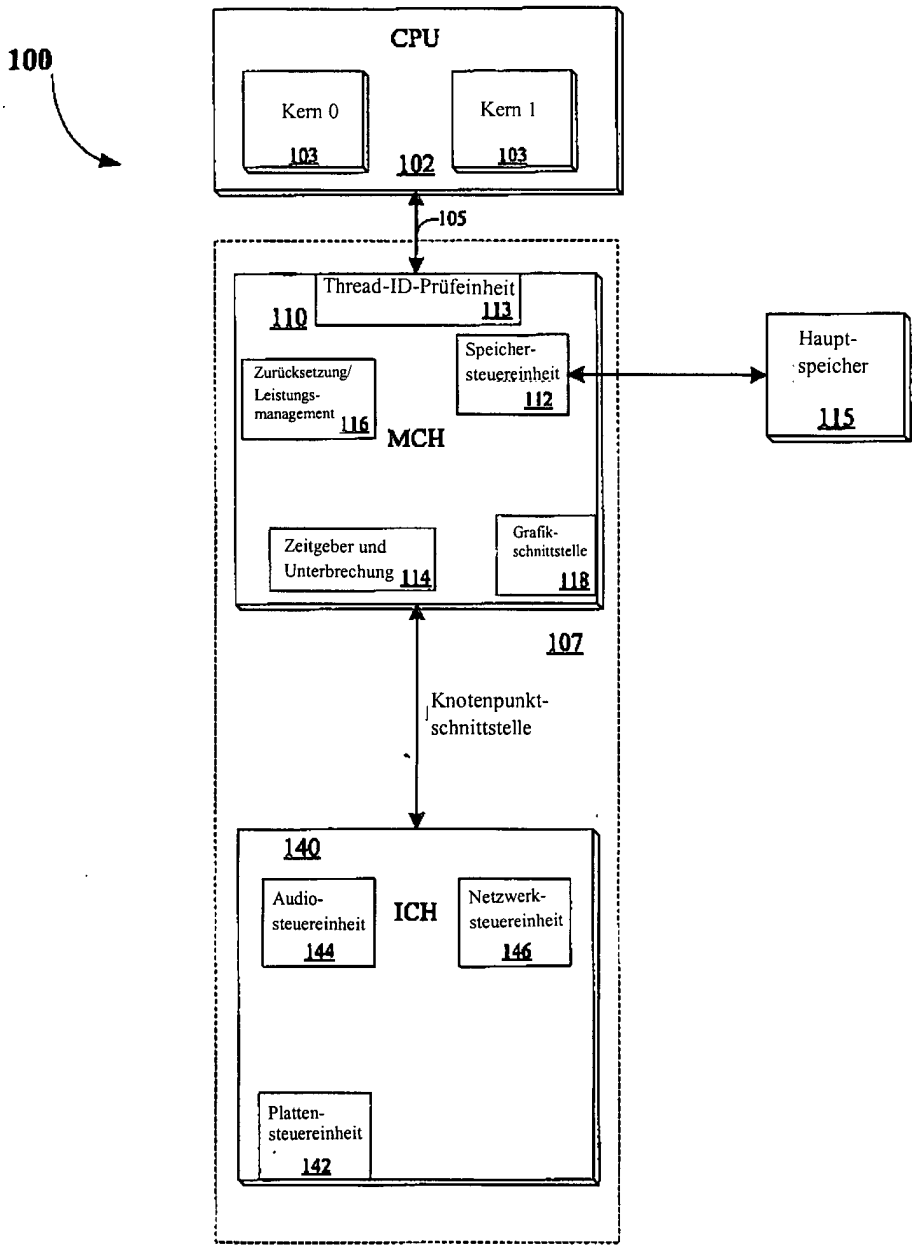


FIG. 1

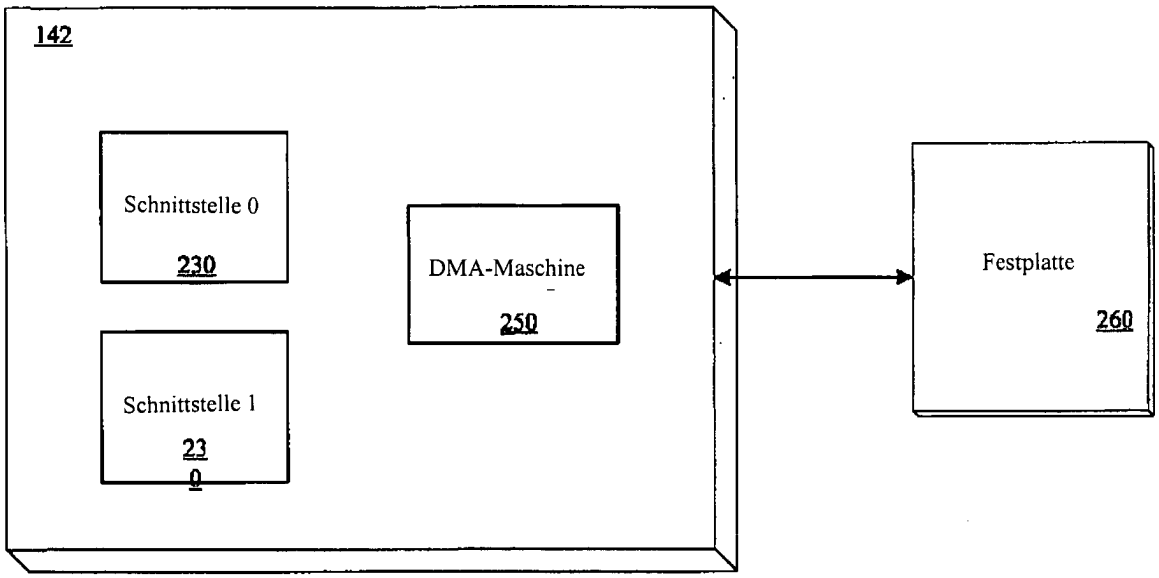

142
Schnittstelle 0
230
Schnittstelle 1
23
0
DMA-Maschine
250
Festplatte
260

FIG. 2

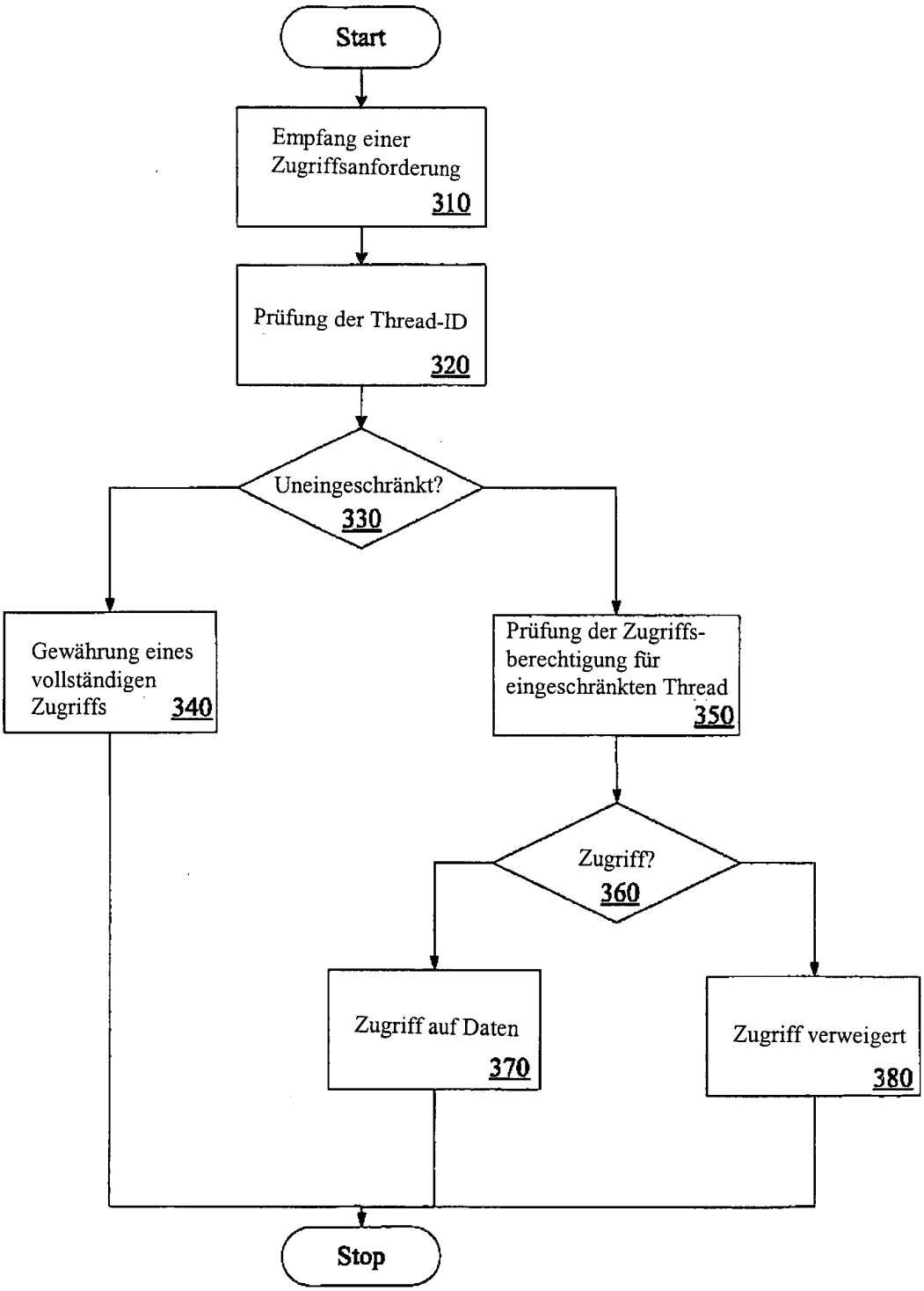

Start
Empfang einer Zugriffsanforderung
310
Prüfung der Thread-ID
320
Uneingeschränkt?
330
Gewährung eines vollständigen Zugriffs
340
Prüfung der Zugriffs-berechtigung für eingeschränkten Thread
350
Zugriff?
360
Zugriff auf Daten
370
Zugriff verweigert
380
Stop

FIG. 3