



(12) **Patentschrift**

(21) Aktenzeichen: **101 10 808.7**  
(22) Anmeldetag: **06.03.2001**  
(43) Offenlegungstag: **13.09.2001**  
(45) Veröffentlichungstag  
der Patenterteilung: **17.03.2011**

(51) Int Cl.<sup>8</sup>: **G06F 12/14** (2006.01)

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:  
**0005535.0**                      **09.03.2000**    **GB**

(73) Patentinhaber:  
**GE Aviation UK, Manchester, GB**

(74) Vertreter:  
**PATENTANWÄLTE CHARRIER RAPP & LIEBAU,**  
**86152 Augsburg**

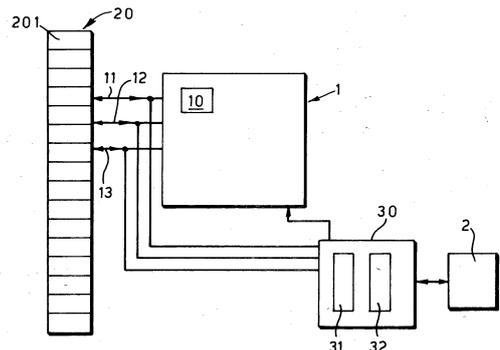
(72) Erfinder:  
**Davies, John Alun, Highnam, Gloucestershire,**  
**GB; Moore, James Frederick, Frampton Cotterell,**  
**Bristol, GB; Stevens, Peter John, Clearwell,**  
**Gloucestershire, GB; Weale, Denis Vaughan,**  
**Little Stoke, Bristol, GB**

(56) Für die Beurteilung der Patentfähigkeit in Betracht  
gezogene Druckschriften:

**US**            **55 13 337**    **A**  
**EP**            **04 15 515**    **A2**

(54) Bezeichnung: **Verarbeitungssystem**

(57) Hauptanspruch: Verarbeitungssystem mit einem Prozessor (1), einem Speicher (20) und einer Überwachungsvorrichtung (30), wobei der Prozessor mit dem Speicher verbunden ist und eine Speicherplaneinheit (10) enthält, die Speicherstellen innerhalb des Speichers (20) identifiziert, an denen festgelegte Daten gespeichert werden, der Prozessor (1) in zwei verschiedenen Betriebsarten betriebsfähig ist, in denen er auf jeweilige verschiedene Speicherstellen Zugriff hat, die Speicherplaneinheit (10) derart gestaltet ist, daß zu einer Anwendung gehörende Daten jedesmal, wenn eine Anwendung abgearbeitet wird, an derselben Speicherstelle gespeichert werden, der Prozessor (1) zum Abarbeiten jeder Anwendung während festgelegter Verarbeitungszeitschlitze eingerichtet ist, die Überwachungsvorrichtung (30) in einem Speicher (31) Informationen hinsichtlich der Speicherstelle, wo zu jeder Anwendung gehörende Daten gespeichert sind, und Informationen hinsichtlich der Zeitschlitze, während denen der Prozessor (1) jede Anwendung abarbeiten sollte, enthält, die Überwachungsvorrichtung (30) derart angeschlossen ist, daß sie Signale empfängt, die die adressierten Speicherstellen und die abgearbeitete Anwendung angeben, und die Überwachungsvorrichtung (30) zum...



## Beschreibung

**[0001]** Diese Erfindung betrifft ein Verarbeitungssystem mit einem Prozessor, einem Speicher und einer Überwachungsrichtung, wobei der Prozessor mit dem Speicher verbunden ist und wobei der Prozessor eine Speicherplaneinheit enthält, die Speicherstellen innerhalb des Speichers identifiziert, an denen festgelegte Daten gespeichert sind.

**[0002]** Verarbeitungssysteme, die in Luftfahrt- und Militär-Anwendungen verwendet werden, werden gewöhnlich speziell konstruiert und geprüft, um sicherzustellen, daß sie voraussehbar arbeiten. Es besteht jedoch ein zunehmender Druck auf Hersteller, die Kosten einer Anlage unter Verwendung von kommerziellen serienmäßigen (COTS, commercial off-the-shelf) Komponenten zu verringern. Kommerziell erhältliche Prozessoren sind jedoch aus verschiedenen Gründen zur Verwendung in Anwendungen mit hoher Integrität nicht geeignet. Obwohl das Betriebssystem des Mikroprozessors beispielsweise einen Speicherplan enthält, der die Speicherstelle innerhalb des Speichers angibt, an der verschiedene Programm- und Dateneinheiten gespeichert sind, befinden sich dieselben Dateneinheiten im allgemeinen nicht jedesmal, wenn der Prozessor eingeschaltet wird, an derselben Speicherstelle. Da sich die Daten nicht jedesmal in derselben Speicherpartition befinden, kann beispielsweise keine Garantie bestehen, daß die Daten immer in Speicherpartitionen enthalten sind, die genügend Kapazität aufweisen oder die im erforderlichen Standard für eine spezielle Anwendung geprüft wurden. Wenn außerdem mehrere verschiedene Softwareanwendungen auf einem Prozessor simultan abgearbeitet werden, arbeitet das Betriebssystem gewöhnlich die verschiedenen Anwendungen in Zeitschlitzen ab, die üblicherweise willkürlich zugeordnet werden. Dies kann dazu führen, daß einigen Anwendungen ungenügend Zeit zugeordnet wird, um jederzeit zuverlässig zu laufen, wohingegen weniger wichtigen Anwendungen mehr Zeit zugeordnet werden könnte, als strenggenommen erforderlich ist.

**[0003]** Beim Betrieb arbeiten Mikroprozessoren in einer von zwei verschiedenen Betriebsarten, nämlich einer Anwenderbetriebsart und einer Überwachungsbetriebsart. Anwendungsprogramme laufen vollständig in der Anwenderbetriebsart, wohingegen die Überwachungsbetriebsart leistungsfähiger ist und zur Bereitstellung von Betriebssystemdiensten für die Anwenderbetriebsart und zum Laufenlassen des Betriebssystems des Prozessors verwendet wird. Herkömmliche Prozessoren schalten entweder am Ende eines Zeitraums, der für eine spezielle Anwendung zugeordnet ist, oder wenn die Anwendung Dienste von der Anwenderbetriebsart anfordert, von der Anwenderbetriebsart in die Überwachungsbetriebsart um. Es ist im allgemeinen keine Anzeige vorhanden, ob der Prozessor in der Anwenderbetriebsart

oder in der Überwachungsbetriebsart arbeitet. Dies trägt zur Unsicherheit über den Betrieb des Prozessorsystems bei, was in Systemen mit hoher Integrität nicht annehmbar ist.

**[0004]** Es stehen Systeme zur Verfügung, die diese Probleme vermeiden, aber diese erfordern eine spezielle Herstellung, die zur Verwendung bei kommerziell erhältlichen Prozessoren im allgemeinen nicht geeignet ist.

**[0005]** Derartige Systeme gehen aus EP 0 415 515 A2 und US 5 513 337 A hervor.

**[0006]** Es ist eine Aufgabe der vorliegenden Erfindung, ein verbessertes Verarbeitungssystem bereitzustellen.

**[0007]** Diese Aufgabe löst die Erfindung durch ein Verarbeitungssystem mit den Merkmalen des Patentanspruchs 1.

**[0008]** Der Speicher umfaßt vorzugsweise einen Flash-Speicher, der eine Software hinsichtlich der Anwendungen enthält, die auf dem System abgearbeitet werden sollen und zu anderen Speicherstellen im Speicher herunterladbar sind.

**[0009]** Ein Verarbeitungssystem und sein Betriebsverfahren gemäß der vorliegenden Erfindung werden nun anhand eines Beispiels mit Bezug auf die zugehörige Zeichnung beschrieben, welche das System schematisch darstellt.

**[0010]** Das System umfaßt einen Prozessor **1** und einen Speicher **20**. Der Prozessor **1** kann von einer herkömmlichen Art sein und enthält eine Speicherplaneinheit **10**, die Speicherstellen im Speicher festlegt, an denen verschiedene Daten gespeichert werden sollen. Der Prozessor **1** wird verwendet, um verschiedene Softwareprogrammanwendungen abzuarbeiten.

**[0011]** Der Speicher **20** weist zahlreiche verschiedene Speicherstellen innerhalb desselben auf, die individuell adressiert werden können, um einen unterteilten Datenspeicher bereitzustellen. Es ist zu erkennen, daß dieser Speicher **20** keine einzelne Einheit sein muß, sondern aus einer beliebigen Anzahl von separaten Einheiten bestehen könnte. Der Speicher **20** kann einen Flash-Speicher **201** umfassen, in dem die gesamte Software hinsichtlich der auf dem System abzuarbeitenden Anwendungen gespeichert ist und aus dem die Software zu anderen Speicherstellen innerhalb des Speichers heruntergeladen werden kann. Der Speicher **20** ist über drei Datenkanäle **11**, **12** und **13** mit dem Prozessor **1** verbunden. Ein Datenkanal **11** überträgt Informationen hinsichtlich Adressenstellen innerhalb des Speichers **20**; der zweite Kanal **12** überträgt Daten, die zu oder von dem

Speicher an der im ersten Kanal festgelegten Adresse geliefert werden sollen; und der dritte Kanal **13** legt fest, ob Daten in den Speicher geschrieben oder aus diesem ausgelesen werden sollen. Diese drei Kanäle **11** bis **13** können durch einen einzelnen Datenbus bereitgestellt werden.

**[0012]** Das System umfaßt eine zusätzliche Komponente in Form einer Überwachungsvorrichtung **30**, die zum Prüfen des Betriebs des Systems wirkt. Die Überwachungsvorrichtung **30** ist mit einer Vorrichtung **2** in Form eines EPROMs oder Prozessors verbunden, so daß Informationen von der Vorrichtung zur Überwachungsvorrichtung geliefert werden. Die Vorrichtung **2** enthält Parameter, die während der Konstruktion des Systems festgelegt werden, welche zulässige Speicherzugriffsrechte und Laufzeitdauern definieren. Die Vorrichtung **2** kann auch Verletzungen verwalten, indem sie entweder den Prozessor **1** zum Stoppen zwingt oder eine Warnung oder einen Alarm erzeugt. Die Überwachungsvorrichtung **30** ist auch mit den drei Kanälen **11** bis **13** verbunden, so daß die Überwachungsvorrichtung Informationen von diesen drei Kanälen empfängt. Die Überwachungs- vorrichtung **30** enthält einen Speicher **31** für Informationen hinsichtlich der Speicherstellen oder Partitionen innerhalb des Speichers **20**, in denen verschiedene Dateneinheiten gespeichert werden sollen, und Informationen hinsichtlich der Zeitschlitze, während denen festgelegte Anwendungen abgearbeitet werden sollen. Die Überwachungs- vorrichtung **30** enthält auch Register **32**, die Kennworte für einen Vergleich mit Kennworten, die zur Überwachungs- vorrichtung geliefert werden, enthalten.

**[0013]** Der Prozessor **1** schaltet zwischen der Anwenderbetriebsart UM und der Überwachungs- betriebsart SM demgemäß um, ob er eine Anwendung abarbeitet oder ob er irgendeine andere Funktion ausführt. Der Prozessor **1** schaltet zwischen diesen zwei Betriebsarten durch eine Anwendungs- programmchnittstelle API um, die eine Softwareebene mit hoher Sicherheit darstellt. Bei der vorliegenden Erfindung ist die API zum Senden eines Kennworts zur Überwachungs- vorrichtung **30**, sobald sie aufgefordert wird, von der UM zur SM zu wechseln, gestaltet und sendet ein anderes Kennwort, sobald sie zur UM zurückkehrt. Wenn das von der API übertragene Kennwort dem im Register **32** in der Überwachungs- vorrichtung **30** gespeicherten entspricht, ermöglicht die Überwachungs- vorrichtung einen Zugriff vom Prozessor **1** auf diejenigen Partitionen des Speichers **20**, die ausschließlich zur Verwendung in der Überwachungs- betriebsart reserviert sind. Wenn das Kennwort nicht entspricht, liefert die Überwachungs- vorrichtung ein Signal zum Prozessor **1**, um eine Funktions- störung anzuzeigen. Aus den Daten von den Kanälen **11** bis **13** und vom E/A-Prozessor **2** weiß die Überwachungs- vorrichtung **30**, welche Anwendung abgearbeitet wird und welcher Speicherparti-

onzzugriff angefordert wurde. Wenn die angeforderte Speicherpartition für die abgearbeitete Anwendung unpassend ist, verweigert die Überwachungs- vorrichtung **30** den Zugriff, selbst wenn das korrekte Kennwort gesandt wird.

**[0014]** Die Überwachungs- vorrichtung **30** überwacht auch, wann eine Anwendung im Prozessor beginnt und endet, und die Speicherpartitionen, auf die zu irgendeiner Zeit zugegriffen wird. Speicher **31** in der Überwachungs- vorrichtung **30** definieren Zeitsequenzen und Speicheradressenpläne, die wiederholt zyklisch umlaufen. Wenn auf die geeignete Speicher- partition nicht im geeigneten Zeitschlitz zugegriffen wird, zeigt die Überwachungs- vorrichtung **30** dem Prozessor **1** eine Funktions- störung an.

**[0015]** Das System der vorliegenden Erfindung kann ohne übermäßige Modifikation leicht auf herkömmliche COTS-Prozessoren angewendet werden. Es kann auch bei einer breiten Vielfalt von verschiedenen Prozessoren verwendet werden und ist gegenüber Änderungen der Konstruktion von Prozessoren relativ unempfindlich.

### Patentansprüche

1. Verarbeitungssystem mit einem Prozessor (**1**), einem Speicher (**20**) und einer Überwachungs- vorrichtung (**30**), wobei der Prozessor mit dem Speicher verbunden ist und eine Speicherplaneinheit (**10**) enthält, die Speicherstellen innerhalb des Speichers (**20**) identifiziert, an denen festgelegte Daten gespeichert werden, der Prozessor (**1**) in zwei verschiedenen Betriebsarten betriebsfähig ist, in denen er auf jeweilige verschiedene Speicherstellen Zugriff hat, die Speicherplaneinheit (**10**) derart gestaltet ist, daß zu einer Anwendung gehörende Daten jedesmal, wenn eine Anwendung abgearbeitet wird, an derselben Speicherstelle gespeichert werden, der Prozessor (**1**) zum Abarbeiten jeder Anwendung während festgelegter Verarbeitungszeitschlitze eingerichtet ist, die Überwachungs- vorrichtung (**30**) in einem Speicher (**31**) Informationen hinsichtlich der Speicherstelle, wo zu jeder Anwendung gehörende Daten gespeichert sind, und Informationen hinsichtlich der Zeitschlitze, während denen der Prozessor (**1**) jede Anwendung abarbeiten sollte, enthält, die Überwachungs- vorrichtung (**30**) derart angeschlossen ist, daß sie Signale empfängt, die die adressierten Speicherstellen und die abgearbeitete Anwendung angeben, und die Überwachungs- vorrichtung (**30**) zum Prüfen, ob die korrekten Speicherstellen adressiert werden und ob die korrekte Anwendung in einem gegebenen Zeitschlitz abgearbeitet wird, gestaltet ist, wobei die Überwachungs- vorrichtung (**30**) einen Speicher (**32**) für mindestens ein Kennwort enthält, daß der Prozessor (**1**) zum Liefern eines Kennworts zur Überwachungs- vorrichtung (**30**), wenn er zwischen den zwei verschiedenen Betriebsarten umschaltet, eingerichtet ist, daß

die Überwachungsvorrichtung (30) zum Vergleichen des vom Prozessor (1) gelieferten Kennworts mit dem in der Überwachungsvorrichtung gespeicherten Kennwort betriebsfähig ist, und daß die Überwachungsvorrichtung (30) zum Verweigern des Zugriffs vom Prozessor (1) auf Speicherstellen im Speicher (20), die zu einer Betriebsart gehören, wenn das vom Prozessor gelieferte Kennwort nicht mit dem Kennwort in der Überwachungsvorrichtung übereinstimmt, gestaltet ist.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß der Speicher (20) einen Flash-Speicher (201) umfaßt, der eine Software hinsichtlich der Anwendungen enthält, die auf dem System abgearbeitet werden sollen und zu anderen Speicherstellen in dem Speicher herunterladbar sind.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

