

(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
15. Februar 2007 (15.02.2007)

PCT

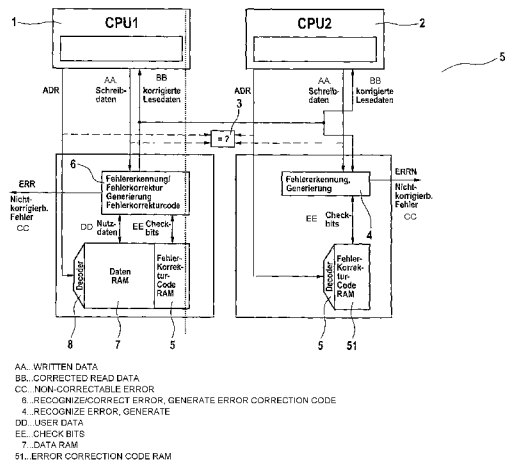
(10) Internationale Veröffentlichungsnummer
WO 2007/017444 A1

- (51) Internationale Patentklassifikation:
G06F 11/10 (2006.01) G06F 11/16 (2006.01)
- (21) Internationales Aktenzeichen: PCT/EP2006/064976
- (22) Internationales Anmeldedatum:
2. August 2006 (02.08.2006)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
10 2005 038 306.8 11. August 2005 (11.08.2005) DE
10 2006 036 384.1 2. August 2006 (02.08.2006) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): CONTINENTAL TEVES AG & CO. OHG [DE/DE]; Guerickestrasse 7, 60488 Frankfurt (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (nur für US): FEY, Wolfgang [DE/DE]; Nesselweg 17, 65527 Niedernhausen (DE). KIRSCHBAUM, Andreas [DE/DE]; Parsevalstrasse 1, 64347 Griesheim (DE). TRASKOV, Adrian [DE/DE]; Hardtbergstrasse 8, 61449 Steinbach (DE).
- (74) Gemeinsamer Vertreter: CONTINENTAL TEVES AG & CO. OHG; Guerickestrasse 7, 60488 Frankfurt (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, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA,

[Fortsetzung auf der nächsten Seite]

(54) Title: MICROPROCESSOR SYSTEM FOR CONTROLLING OR REGULATING AT LEAST PARTIALLY SAFETY-CRITICAL PROCESSES

(54) Bezeichnung: MIKROPROZESSORSYSTEM ZUR STEUERUNG BZW. REGELUNG VON ZUMINDEST ZUM TEIL SICHERHEITSKRITISCHEN PROZESSEN



(57) Abstract: Disclosed is a microprocessor system (50) for controlling or regulating at least partially safety-critical processes. Said microprocessor system (50) comprises two central arithmetic units (1, 2) that are integrated into a chip housing, a first and a second bus system, at least one complete memory (7) on the first bus system, at least one test data memory (51) on the second bus system, which has a reduced storage capacity compared to the complete memory on the first bus system and in which test data is stored that correlate with data of the memory (7) on the first bus system. The bus systems are provided with comparative components and/or driver components that allow data to be exchanged and/or compared between the two bus systems. A hardware test data generator (4) is disposed at least on the second bus system. At least some of the complete memory on the first bus is additionally secured by means of another test data memory (5) and test data on the second bus. The invention further relates to the use of said microprocessor system in control devices of motor vehicles.

(57) Zusammenfassung: Mikroprozessorsystem (50) zur Steuerung bzw. Regelung von zumindest zum Teil sicherheitskritischen Prozessen umfassend zwei in einem Chipgehäuse integrierte Zentralrechenheiten (1,2), ein erstes und ein zweites Bussystem, zumindest einen vollständiger Speicher (7) am ersten Bussystem, mindestens einen Prüf datenspeicher (51) am zweiten Bussystem, welcher gegenüber dem vollständige Speicher am ersten Bussystem

[Fortsetzung auf der nächsten Seite]

WO 2007/017444 A1



NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC,
SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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).

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, 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, IS, IT, LT, LU, LV, MC,

Veröffentlicht:

— mit internationalem Recherchenbericht

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.

einen reduzierten Speicherumfang hat und in dem Prüfdaten gespeichert sind, die mit Daten des Speichers (7) am ersten Bussystem zusammenhängen, wobei die Bussysteme Vergleichs- und/oder Treiberkomponenten umfassen, welche den Datenaustausch und/oder Vergleich von Daten zwischen den beiden Bussystemen ermöglichen und wobei zumindest am zweiten Bussystem ein Hardware-Prüfdatengenerator (4) angeordnet ist, wobei zumindest ein Teil des vollständigen Speichers am ersten Bus mittels eines weiteren Prüfdatenspeichers (5) und Prüfdaten am ersten Bus zusätzlich abgesichert ist. Die Erfindung betrifft außerdem die Verwendung des obigen Mikroprozessorsystems in Kraftfahrzeugsteuergeräten.

Mikroprozessorsystem zur Steuerung bzw. Regelung von zumindest zum Teil sicherheitskritischen Prozessen

Die Erfindung betrifft ein Mikroprozessorsystem gemäß Anspruch 1 und dessen Verwendung in Kraftfahrzeugsteuergeräten.

Aus der DE 195 29 434 A1 (P 7959) geht ein Mikroprozessorsystem für sicherheitskritische Anwendungen gemäß dem Oberbegriff von Anspruch 1 hervor. In diesem Mikroprozessorsystem sind aus Gründen der Redundanz zwei gleichartige Mikroprozessorkerne (Kernredundanz) vorgesehen, welche taktsynchron und parallel das gleiche Programm abarbeiten. Die den Mikroprozessorsystemen zugeordneten Bussysteme sind ebenfalls zweifach vorhanden, jedoch ist der Speicher aus Kostengründen nicht vollsymmetrisch aufgebaut. Es hat sich gezeigt, dass eine hohe Fehlererkennungsrate erreicht werden kann, wenn an einem der beiden Bussysteme lediglich Prüfdaten in einem Prüfdatenspeicher mit geringerem Speicherumfang gespeichert werden, welche den vollständigen Daten im vollständigen Speicher eindeutig zugeordnet sind. Damit beiden Kernen jeweils alle Daten redundant zur Verfügung stehen, wird ständig ein Vergleich der vollständigen Daten mit den Prüfdaten unter Verwendung von Hardware-Generatoren durchgeführt. Die Hardware-Generatoren können entweder Prüfdaten erzeugen oder die Prüfdaten zum Vergleich mit Hilfe der vollständigen Daten vervollständigen (Datenfehlerkorrektur).

Die vorliegende Erfindung setzt sich zum Ziel, eine alternatives zweikerniges Mikroprozessorsystem anzugeben, welches ebenfalls einen vollständigen Speicher und einen Prüfdatenspeicher mit geringerer Größe zur Speicherung von Redundanzinformationen umfasst, welche den im vollständigen Speicher gespeicherten Originaldaten zugeordnet sind, und wobei das Mikroprozessorsystem gegenüber entsprechenden zweikernigen Mikroprozessorsystem eine erhöhte Fehlererkennungsrate auf-

weist.

Diese Aufgabe wird erfindungsgemäß gelöst durch das Mikroprozessorsystem gemäß Anspruch 1.

Das Mikroprozessorsystem gemäß der Erfindung umfasst zwei in einem Chipgehäuse integrierte Zentralrecheneinheiten.

Jeder Recheneinheit ist ein eigenes Bussystem (erster und zweiter Bus) zugeordnet, so dass dieses ebenfalls redundant ausgeführt ist.

An dem ersten Bus ist zumindest ein vollständiger Speicher angeordnet. Am zweiten Bussystem befindet sich mindestens ein Prüfdatenspeicher, welcher gegenüber dem vollständigen Speicher am ersten Bussystem einen reduzierten Speicherumfang hat.

Im Prüfdatenspeicher am zweiten Bus werden Prüfdaten gespeichert, die mit Daten des Speichers am ersten Bussystem zusammenhängen. Das Speichern der Prüfdaten dient zur Erkennung von typischen Datenspeicherfehlern, welche bei Schreib- oder Leseoperationen in seltenen Fällen vorkommen können. Die Erkennung solcher Fehler kann auch dadurch erfolgen, dass der vollständige Speicher doppelt vorhanden ist und die Daten zweimal in identischer Form gespeichert werden. Dies ist jedoch kostenintensiv, da der Speicher einen beträchtlichen Teil der Herstellungskosten eines Chips einnimmt. Es hat sich gezeigt, dass entsprechend dem Mikroprozessorsystem nach der vorliegenden Erfindung eine ausreichende Fehlererkennung auch mit einem im Speicherplatzbedarf reduzierten Redundanzspeicher, dem Prüfdatenspeicher vorgenommen werden kann. Hierzu wird beispielsweise zu einem Datenwort (Datum) im vollständigen Speicher eine Prüfinformation oder ein

Prüfwert (z.B. Paritätsinformation, Hamming-Code oder dergleichen) im Prüfdatenspeicher gespeichert. Im einfachsten Fall kann das ein Paritätsbit der Breite 1 Bit sein. Komplexere Codierungsverfahren, z.B. Hamming-Codes können auch eine Fehlerkorrektur ermöglichen sowie mehrfache Fehler erkennen. Die Paritätsinformation kann wortweise und/oder aus mehreren Datenworten des vollständigen Speichers zusammengefasst (blockweise Prüfdatenkodierung) gebildet sein.

Bevorzugt ist nur ein Teil des vollständigen Speichers durch einen Prüfdatenspeicher am zweiten Bus abgesichert. In diesem Fall gibt es folglich Speicherbereiche im vollständigen Speicher, die nicht gegen Fehler abgesichert sind. Diese Speicherbereiche können mit weniger wichtigen Programmfunktionen gefüllt werden, welche nicht sicherheitskritisch sind. Es ist aber auch möglich, dass der gesamte vollständige Speicher durch den Prüfdatenspeicher am zweiten Bus abgesichert ist.

Die Bussysteme umfassen außerdem Vergleichs- und/oder Treiberkomponenten, welche den Datenaustausch und/oder Vergleich von Daten zwischen den beiden Bussystemen ermöglichen.

Zumindest am zweiten Bussystem ist ein an sich bekannter Hardware-Prüfdatengenerator angeordnet, welcher beispielsweise durch logische Gatter realisiert ist. Die für die Erkennung von Speicherfehlern notwendigen Prüfinformationen werden demzufolge nicht von einer Zentralrecheneinheit (CPU) erzeugt, sondern durch einen sogenannten, physikalisch von der CPU getrennt angeordneten Hardware-Prüfdatengenerator. Ein Hardware-Prüfdatengenerator ist vorzugsweise eine im wesentlichen festverdrahtete Halbleiterstruktur, welche nach einer vorgegebenen Logik bestimmte Arbeitsschritte zur Datenverarbeitung und/oder Signalverarbeitung selbstständig

- 4 -

ohne Hilfe einer Zentralrecheneinheit durchführt. Die vom Hardware-Generator durchgeführten Operationen könnten zwar im Prinzip auch von der Zentralrecheneinheit durchgeführt werden, jedoch ist dies - neben einer möglichen erhöhten Fehlerrate - in der Regel mit einem höheren Taktzyklenverbrauch verbunden, wodurch die Laufzeit stark erhöht werden würde.

Bei dem vollständigen Speicher handelt es sich bevorzugt um einen Schreib-/Lesespeicher. Es ist aber auch möglich, dass ein Nur-Lesespeicher (z.B. ROM, Otp-ROM, EPROM, EEPROM oder Flash-ROM) nach dem erfindungsgemäßen Prinzip abgesichert wird.

Das aus der DE 195 29 434 A1 bekannte Verfahren der Absicherung mit einem Prüfdatenspeicher erfüllt zwar die für heutige Anwendungen erforderlichen Anforderungen an Verfügbarkeit, jedoch existieren außer den erwähnten Speicherfehlern auch zusätzliche Fehlerarten, welche sich durch die bekannte Architektur nicht absichern lassen. So lassen sich zum Beispiel Fehler auf dem Adress-Bus und Fehler des Adress-Dekoders nicht erkennen. Zwar würde eine blockweise Prüfdatenkodierung zur Erzeugung von Prüfinformationen die Erkennung dieser zusätzlichen Fehlerarten zulassen, jedoch wäre dieses Verfahren auf die Anwendung eines Festwertspeichers beschränkt. Daher wird gemäß der Erfindung zumindest ein Teil des vollwertigen Speichers am ersten Bus mittels eines ebenfalls am ersten Bus angeordneten zusätzlichen weiteren Prüfdatenspeichers und entsprechenden Prüfdaten abgesichert. Hierdurch wird eine Erkennung der vorstehend erwähnten zusätzlichen Fehlerarten erreicht.

Vorzugsweise ist im Mikroprozessorsystem nach der Erfindung eine Einrichtung zur Adressfehlererkennung implementiert.

Diese ist insbesondere so ausgestaltet, dass Mittel vorgesehen sind, welche die Adresse der abzusichernden Daten bei der Berechnung der Prüfdaten einbeziehen. Ganz besonders bevorzugt werden beim Schreiben insbesondere die Prüfdaten, welche z.B. Prüfbits sind, nicht nur an Hand der Datenbits berechnet, sondern an Hand der abzusichernden Daten und der zugehörigen Adresse. Auf diese Weise können Adressierungsfehler beim Lesen der Daten erkannt werden. Die Adressfehlererkennung ist vorzugsweise an jedem der beiden Bussysteme vorhanden.

Ein alternativ bevorzugtes Mittel zur Adressfehlererkennung besteht in einer zusätzlich im Mikroprozessorsystem implementierten Einrichtung, die im Hintergrund einen oder mehrere Tests zur Adressfehlererkennung durchführt. Diese Art der Fehlererkennung wird zweckmäßigerweise nicht parallel während Schreib-/Lesezugriffen durchgeführt. Diese Fehlererkennungsmaßnahme wird vielmehr insbesondere nur im Rahmen einer periodischen gesonderten Prüfung durchgeführt, bei der bevorzugt keine weiteren wesentlichen CPU-Aktivitäten vorliegen. Die hier beschriebene alternative Adressfehlererkennung kann als Software oder als Hardware-Maßnahme ausgeführt sein. Die hier beschriebenen Mittel können insbesondere innerhalb der CPU oder innerhalb der Hardware State Maschine als nach Art eines eingebauten Selbsttests ausgeführt werden.

Gemäß dem Selbsttest wird bevorzugt der Speicher mit einem vordefinierten Muster (Pattern) beschrieben und anschließend ausgelesen. Das Muster kann besonders bevorzugt so ausgelegt sein, dass mögliche Decodierungsfehler oder Ansteuerungsfehler absichtlich zu einer Verfälschung der Daten führen. Beim Auslesen wird dieser absichtlich herbeigeführte Fehler dann erkannt.

Zusätzlich oder alternativ zu den beiden vorstehend erwähnten Fehlererkennungseinrichtung ist bevorzugt ein Adressierungsfehlererkennungsmittel implementiert, bei dem in eine Speicherzelle die Adresse der Speicherzelle geschrieben und danach überprüft wird.

Ein Beispiel für die zuvor beschriebene Methode ist der sogenannte „Address-to-Data“ Test. Gemäß diesem Test wird jede Speicherstelle mit dem Zahlenwert der Adresse der Speicherstelle beschrieben:

Adresse	Datum
0x00	0x00
0x01	0x01
...	
0xff	0xff

Bei einem Fehler wird dann eine Zahl nicht zurückgelesen, eine andere dafür doppelt.

Der Prüfdatenspeicher, der gemäß der Erfindung eingesetzt wird, ist im Prinzip ein herkömmlicher Schreib-/Lesespeicher, jedoch mit einem gegenüber dem vollständigen Speicher reduzierten Speicherumfang.

Die Mikroprozessorsysteme sind in einem gemeinsamen Chipgehäuse integriert und werden bevorzugt taktsynchron betrieben. Bevorzugt sind beide Systeme auf einem gemeinsamen Halbleitermaterial angeordnet.

Das Mikroprozessorsystem umfasst zwei Bussysteme, welche bevorzugt jeweils aus einem Datenbus, Adressbus und Kontrollbus bestehen.

Neben dem oder den Schreib-/Lesespeichern ist zum Betrieb des Mikroprozessorsystems natürlich auch zumindest ein Festwertspeicher vorhanden. Unter dem Begriff Festwertspeicher wird gemäß der Erfindung ein zumindest für eine gewisse Zeit nicht flüchtiger Speicher, wie insbesondere vom Typ ROM, Flash-ROM oder OTP-ROM verstanden. Entsprechend dem Prinzip der Kernredundanz ist es dabei nicht unbedingt nötig, dass an beiden Bussystemen vollständige bzw. inhaltlich identische Festwertspeicher vorhanden sind. Wenn das Redundanzkonzept, was bevorzugt ist, auch auf den Festwertspeicher übertragen wird, dann ist vorgesehen, dass durch entsprechende Prüfinformationen sichergestellt ist, dass die Daten des Festwertspeichers abgesichert sind. Dies kann insbesondere durch einen kleineren Festwertspeicher am zweiten Bus erreicht werden, welcher an Stelle der Daten geeignete Prüfinformation enthält.

Bevorzugt werden in dem Mikroprozessorsystem nach der Erfindung Prüfdaten zusätzlich am ersten Bus im physikalischen Speicher oder zumindest in unmittelbarer Nähe des vollwertigen Schreib-/Lesespeichers gespeichert. In unmittelbarer Nähe bedeutet, dass die entsprechenden Chipstrukturen aneinander angrenzen, so dass die notwendige geringe Laufzeit der Daten eingehalten werden kann.

Das Mikroprozessorsystem ist bevorzugt so aufgebaut, dass bei einem Lesezyklus die Daten des vollständigen Speichers mit diesen Daten zugeordneten Prüfdaten durch eine oder mehrere Hardware-Prüfeinheiten verglichen werden, welche insbesondere im oder in der Nähe des Daten-Speicherbereichs positioniert ist/sind. Die Hardware-Korrekturereinheit(en) korrigieren die Daten im Falle eines Fehlers mit Hilfe der Prüfdaten. Durch diese Korrektur lassen sich beispielsweise Ein-

fachfehler, wie z.B. ein falsches Bit, ohne weiteres korrigieren, so dass das Mikroprozessorsystem nicht abgeschaltet werden muss. Je nach Komplexität des Prüfwortes können so auch kompliziertere Fehler abgefangen werden. Ist eine Korrektur nicht erfolgreich, das heißt, war der Fehler in den Daten so komplex, dass durch Verknüpfung mit den Prüfinformationen die korrigierten Daten immer noch fehlerhaft sind, so werden diese durch eine bevorzugt vorhandene weitere Vergleichseinheit, die die auf den parallelen Bussystemen anstehenden Daten vergleicht, entdeckt. Als Folge davon wird zweckmäßigerweise ein Fehlersignal auf einer geeigneten Fehlerleitung ausgegeben, welche insbesondere das Mikroprozessorsystem stilllegt oder von der weiteren Elektronik abkoppelt. Hierdurch wird beispielsweise in einem elektronischen Bremssystem wirksam verhindert, dass irrtümlich die Ventiltreiber angesteuert werden.

Im Gegensatz zu bekannten fehlerkorrigierenden/fehlererkennenden Mikroprozessoren, die das Prinzip der Kernredundanz nutzen, und in denen lediglich Mechanismen zur Erkennung/Korrektur von Fehlern in einer Speicherzelle vorhanden waren, ist es gemäß der Erfindung nun möglich, den gesamten Speicher abzusichern. Dies ermöglicht die Ausweitung des verwendeten Redundanzkonzepts vom Nur-Lesespeicher auch auf den Datenspeicher. Hierdurch lassen sich die Herstellungskosten unter Beibehaltung der vorhandenen Sicherheitsanforderungen weiter absenken.

Weitere bevorzugte Ausführungsformen ergeben sich aus den Unteransprüchen und der nachfolgenden Beschreibung eines Ausführungsbeispiels an Hand einer Figur.

Es zeigt

Fig. 1 einen zweikernigen integrierten Mikrocontroller mit einem Datenspeicher und zusätzlichem Prüfspeicher.

Der Mikrocontroller in Fig. 1 umfasst zwei Zentralrecheneinheiten (CPU) 1, 2, die taktsynchron arbeiten. Beide Mikrocomputer arbeiten das gleiche Programm ab. Jede Einheit ist jeweils getrennt einem Adress- und Datenbus zugeordnet. An CPU 1 ist ein vollständiger Datenspeicher 7 angeschlossen, welcher zum Teil durch einen Prüfdatenspeicher 51 am zweiten Bus abgesichert ist. Das Mikroprozessorsystem umfasst weiterhin einen als Hardware-Element ausgeführten Vergleicher 3, mit dem die anstehenden Adressen und Daten der beiden Bussysteme ständig miteinander verglichen werden. Bei Nichtübereinstimmung wird ein Fehlersignal erzeugt. Zur vereinfachten Darstellung sind in den Figuren die bei Mikroprozessorsystemen üblicherweise vorhandenen Komponenten, wie Eingabe-/Ausgabeeinheiten, Nur-Lesespeicher, etc. nicht näher dargestellt. Diese nicht dargestellten Komponenten entsprechen im wesentlichen dem in der W099/35543 beschriebenen kernreduzanten Mikrocontroller.

Prüfdatenspeicher 51 am zweiten Bus besitzt gegenüber Speicher 7 einen um den Faktor 8 reduzierten Speicherumfang. In Speicher 51 werden Prüfdaten gespeichert, welche praktisch gleichzeitig bei jedem Schreibvorgang von Daten durch CPU 1 in Speicher 7 durch Hardware-Generator 6 erzeugt werden. Durch die Erzeugung der Prüfdaten ohne programmtechnische Mittel kann der Schreibvorgang im Prinzip ohne erhöhten Taktzyklenverbrauch durchgeführt werden. Zusätzlich werden im physikalischen Speichermodul des Speichers 7 in andere Speicheradressen 5 dieses Speichers die bereits für Speicher 51 erzeugten Prüfdaten noch ein weiteres Mal abgelegt. Die dabei verwendeten Codes für die Fehlerkorrektur und für die

- 10 -

Fehlererkennung können identisch oder unterschiedlich ausgeführt sein, so dass die Prüfdaten entweder identisch oder unterschiedlich sind.

Beim Lesen wird Speicher 7 von CPU 1 über Adressdeko-der 8 adressiert. Während des Lesevorgangs ist Hardware-Einheit 6 aktiv. In Hardware-Einheit 6 werden die Daten entsprechend dem Prüfdatenerzeugungsverfahren (z.B. Hamming-Code) überprüft und ggf. sofort korrigiert. Über die in Block 3 enthaltenen Bustreiber werden die anstehenden Daten gleichzeitig CPU 1 und CPU 2 zur Verfügung gestellt. Während des Lesevorgangs durch CPU 1 wird außerdem parallel zum Datenlesen von CPU 2 über Adressdeko-der 9 Speicher 51 adressiert. Speicher 51 enthält ebenfalls Prüfdaten zur Fehlererkennung, welche insbesondere Prüfsummen der Daten in Speicher 7 sind. Falls Daten und Prüfdaten nicht zueinander passen, wird ebenfalls ein Fehler erkannt. Am zweiten Bus findet zwar auch eine Fehlererkennung statt, jedoch bezieht sich diese auf ggf. im Bereich des ersten Bus korrigierte Daten. Diese Prüfung wird in Hardware-Vergleicher 4 vorgenommen, welcher ebenfalls ein Fehlersignal erzeugen kann. Der Prüfdatenspeicher 5 ist in räumlicher Nähe des Datenspeichers 7 angeordnet, damit eine Korrektur der Daten innerhalb kurzer Zeit erfolgen kann und damit noch im Rahmen des vorgegebenen Timings möglich ist.

Patentansprüche

1. Mikroprozessorsystem (50) zur Steuerung bzw. Regelung von zumindest zum Teil sicherheitskritischen Prozessen umfassend zwei in einem Chipgehäuse integrierte Zentralrecheneinheiten (1, 2), ein erstes und ein zweites Bussystem, zumindest einen vollständiger Speicher (7) am ersten Bussystem, mindestens einen Prüfdatenspeicher (51) am zweiten Bussystem, welcher gegenüber dem vollständige Speicher am ersten Bussystem einen reduzierten Speicherumfang hat und in dem Prüfdaten gespeichert sind, die mit Daten des Speichers (7) am ersten Bussystem zusammenhängen, wobei die Bussysteme Vergleichs- und/oder Treiberkomponenten umfassen, welche den Datenaustausch und/oder Vergleich von Daten zwischen den beiden Bussystemen ermöglichen und wobei zumindest am zweiten Bussystem ein Hardware-Prüfdatengenerator (4) angeordnet ist, dadurch **gekennzeichnet**, dass zumindest ein Teil des vollständigen Speichers am ersten Bus mittels eines weiteren Prüfdatenspeichers (5) und Prüfdaten am ersten Bus zusätzlich abgesichert ist.
2. Mikroprozessorsystem nach Anspruch 1, dadurch **gekennzeichnet**, dass die weiteren Prüfdaten am ersten Bus durch einen zusätzlichen Prüfdatengenerator (6) am ersten Bus abgesichert sind.
3. Mikroprozessorsystem nach Anspruch 2, dadurch **gekennzeichnet**, dass der vollständige Speicher und/oder der Prüfdatenspeicher am ersten Bus und der Prüfdatenspeicher am zweiten Bus jeweils einen eigenen Adressdekoder (8,9) aufweisen.

4. Mikroprozessorsystem nach mindestens einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, dass die Prüfdaten, die am ersten Bus anstehen, im physikalischen Speicher oder zumindest in unmittelbarer Nähe des vollwertigen vollständigen Speichers gespeichert werden.
5. Mikroprozessorsystem nach mindestens einem der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, dass eine oder mehrere Vergleichsstrukturen in Hardware (3) implementiert ist/sind, welche während eines jeden Schreib- und/oder Lesevorgangs die anstehenden Adressen der Adressbusse und/oder die an den Datenbussen anstehenden Daten miteinander vergleicht, und bei abweichenden Adressen und/oder Daten ein Fehlersignal erzeugt.
6. Mikroprozessorsystem nach mindestens einem der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, dass bei einem Lesezyklus die Daten des vollständige Speichers vor dem Vergleich in Vergleichsstruktur (3) zunächst auf Fehler mittels dem dem vollständigen Speicher direkt an diesem Bus zugeordneten Prüfdatenspeicherbereich geprüft werden und im Falle eines Fehler die Daten korrigiert werden oder ein Fehlersignal erzeugt wird.
7. Mikroprozessorsystem nach mindestens einem der Ansprüche 1 bis 6, dadurch **gekennzeichnet**, dass bei einem Lesezyklus die Daten des Speichers mit diesen Daten zugeordneten Prüfdaten durch eine Hardware-Prüfeinheit (6) verglichen werden, welche insbesondere im oder in der Nähe des Daten-Speicherbereichs positioniert sind, und eine Hardware-Korrekturereinheit (6) die Daten im Falle eines Fehlers mit Hilfe der Prüfdaten korrigiert.

8. Mikroprozessorsystem nach mindestens einem der Ansprüche 1 bis 7, dadurch **gekennzeichnet**, dass am ersten Bussystem ein Hardware-Prüfdatengenerator (6) angeordnet ist, welcher die Prüfdaten für Prüfdatenspeicher (5) erzeugt.
9. Verwendung der Mikroprozessorsysteme gemäß den obigen Ansprüchen in Kraftfahrzeugsteuergeräten, insbesondere in Kraftfahrzeugbremsensteuergeräten, Steuergeräten für Fahrwerksregelung, Steuergeräten für Sicherheitssysteme oder für entsprechende Kombinationssteuergeräte.

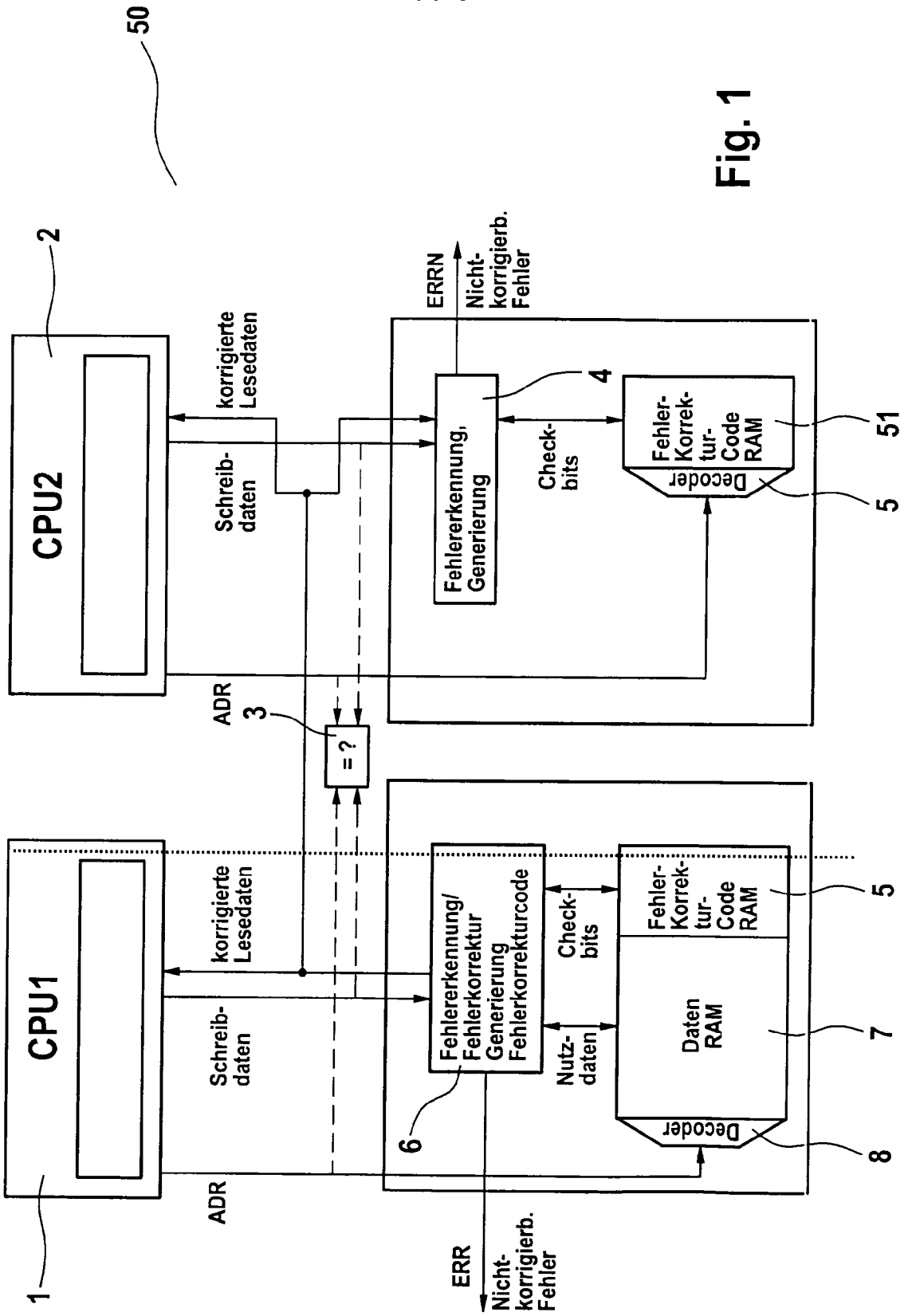


Fig. 1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/064976

A. CLASSIFICATION OF SUBJECT MATTER INV. G06F11/10 G06F11/16		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 909 541 A (SAMPSON NEIL L [US] ET AL) 1 June 1999 (1999-06-01) column 4, line 40 - line 64 column 5, line 53 - column 7, line 5 figures 1a,1b,2a,2b,3a claim 6 -----	1-9
X	EP 0 306 348 A2 (DIGITAL EQUIPMENT CORP [US]) 8 March 1989 (1989-03-08) page 5, line 23 - page 6, line 66 figures 1,3,5-8 -----	1-9
A	DE 195 29 434 A1 (TEVES GMBH ALFRED [DE]) 13 February 1997 (1997-02-13) cited in the application the whole document -----	1-9
<input type="checkbox"/> Further documents are listed in the continuation of Box C.		
<input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents :		
A document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the International filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family	
Date of the actual completion of the international search <p align="center">13 November 2006</p>	Date of mailing of the international search report <p align="center">20/11/2006</p>	
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer <p align="center">Bauer, Regine</p>	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No PCT/EP2006/064976

Patent document cited in search report	Publication date	Publication date	Patent family member(s)	Publication date
US 5909541	A	01-06-1999	NONE	
EP 0306348	A2	08-03-1989	CA 1320276 C	13-07-1993
DE 19529434	A1	13-02-1997	WO 9706487 A1	20-02-1997
			EP 0843853 A1	27-05-1998
			JP 11510925 T	21-09-1999
			US 6201997 B1	13-03-2001

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2006/064976

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. G06F11/10 G06F11/16

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
 EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 909 541 A (SAMPSON NEIL L [US] ET AL) 1. Juni 1999 (1999-06-01) Spalte 4, Zeile 40 - Zeile 64 Spalte 5, Zeile 53 - Spalte 7, Zeile 5 Abbildungen 1a, 1b, 2a, 2b, 3a Anspruch 6	1-9
X	EP 0 306 348 A2 (DIGITAL EQUIPMENT CORP [US]) 8. März 1989 (1989-03-08) Seite 5, Zeile 23 - Seite 6, Zeile 66 Abbildungen 1, 3, 5-8	1-9
A	DE 195 29 434 A1 (TEVES GMBH ALFRED [DE]) 13. Februar 1997 (1997-02-13) in der Anmeldung erwähnt das ganze Dokument	1-9

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen Siehe Anhang Patentfamilie

- | | |
|---|--|
| <p>* Besondere Kategorien von angegebenen Veröffentlichungen :</p> <ul style="list-style-type: none"> *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist | <ul style="list-style-type: none"> *T* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist *X* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden *Y* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist *Z* Veröffentlichung, die Mitglied derselben Patentfamilie ist |
|---|--|

Datum des Abschlusses der internationalen Recherche 13. November 2006	Absenddatum des internationalen Recherchenberichts 20/11/2006
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bevollmächtigter Bediensteter Bauer, Regine

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2006/064976

Im Recherchenbericht angeführtes Patentedokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5909541	A	01-06-1999	KEINE	
EP 0306348	A2	08-03-1989	CA 1320276 C	13-07-1993
DE 19529434	A1	13-02-1997	WO 9706487 A1	20-02-1997
			EP 0843853 A1	27-05-1998
			JP 11510925 T	21-09-1999
			US 6201997 B1	13-03-2001