(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
11. November 2004 (11.11.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/097646 A2

(51) Internationale Patentklassifikation[7]: G06F 12/00

(21) Internationales Aktenzeichen: PCT/DE2004/000794

(22) Internationales Anmeldedatum:
14. April 2004 (14.04.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 18 730.8 25. April 2003 (25.04.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **CONTI TEMIC MICROELECTRONIC GMBH** [DE/DE]; Sieboldstrasse 19, 90411 Nürnberg (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **DÜRR, Daniel** [DE/DE]; Chorherrenweg 10, 88339 Bad Waldsee (DE). **PETER, Wolfgang** [DE/DE]; Unterer Sonnenberg 15, 88368 Bergatreute (DE).

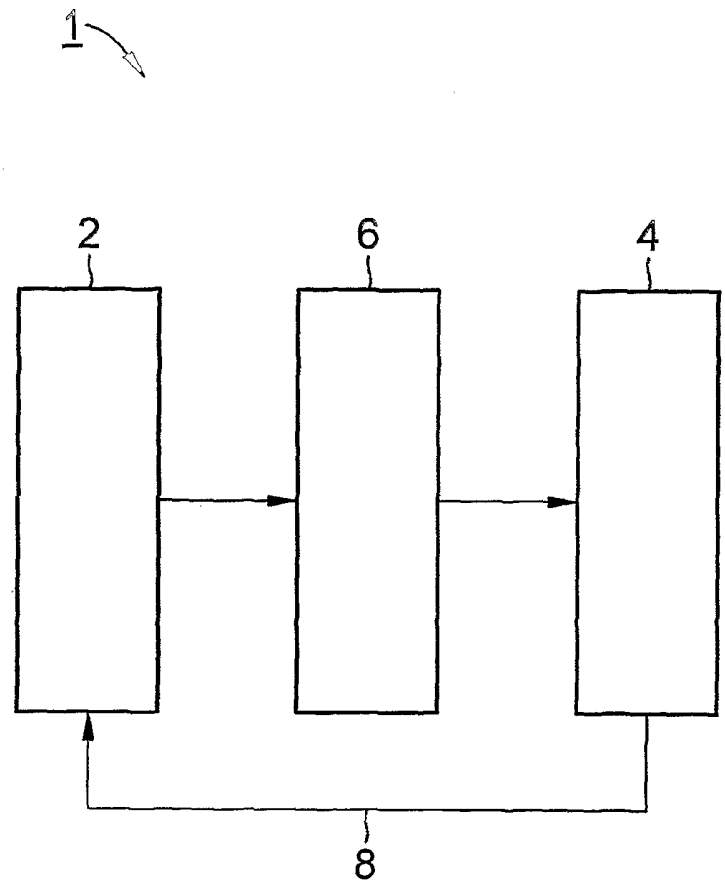
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,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

[Fortsetzung auf der nächsten Seite]

WO 2004/097646 A2

(54) **Title:** METHOD FOR THE OPERATION OF A DATA PROCESSING UNIT AND DATA PROCESSING SYSTEM FOR CARRYING OUT THE METHOD

(54) **Bezeichnung:** VERFAHREN ZUM BETREIBEN EINER DATENVERARBEITUNGSEINHEIT SOWIE DATENVERARBEITUNGSSYSTEM ZUR DURCHFÜHRUNG DES VERFAHRENS



(57) **Abstract:** The invention relates to a method for the operation of a data processing unit (2), which reads data on demand from a provided storage unit (4), by recourse to specifically deposited target addresses, whereby the target addresses given by the data processing unit (2) are converted into an actual address by means of a deposited encoding algorithm, before an access to the storage unit (4) occurs.

(57) **Zusammenfassung:** Die Erfindung betrifft ein Verfahren zum Betreiben einer Datenverarbeitungseinheit (2), die bedarfsweise unter Rückgriff auf spezifisch hinterlegte Zieladressen Daten aus einer zugeordneten Speichereinheit (4) einliest, wobei vor einem Zugriff auf die Speichereinheit (4) die von der Datenverarbeitungseinheit (2) jeweils ausgegebene Zieladresse über einen hinterlegten Verschlüsselungsalgorithmus in eine tatsächliche Zieladresse umgesetzt wird.

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

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

Veröffentlicht:

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

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

Beschreibung

Verfahren zum Betreiben einer Datenverarbeitungseinheit sowie Datenverarbeitungssystem zur Durchführung des Verfahrens

Die Erfindung betrifft ein Verfahren zum Betreiben einer Datenverarbeitungseinheit, die bedarfsweise unter Rückgriff auf spezifisch hinterlegte Zieladressen Daten aus einer zugeordneten Speichereinheit einliest. Sie bezieht sich weiter auf ein Datenverarbeitungssystem, insbesondere zur Durchführung eines derartigen Verfahrens mit einer derartigen Datenverarbeitungseinheit.

In Datenverarbeitungssystemen kommen üblicherweise Datenverarbeitungseinheiten wie beispielsweise μ-Controller, μ-Prozessoren oder allgemein Prozessoren, zum Einsatz, in denen eingespeicherte Funktionsabläufe nach einem vorgegebenen Ablaufplan abgearbeitet werden. Dazu greift die jeweilige Datenverarbeitungseinheit üblicherweise auf in einer zugeordneten Speichereinheit hinterlegte Informationen zu, wobei beispielsweise einzelne Programmfunktionen oder auch Datensätze zur weiteren Be- oder Verarbeitung eingelesen werden. Beim bedarfsweisen Zugriff der Datenverarbeitungseinheit auf die jeweilige Speichereinheit wird dabei üblicherweise in der Art eines Indexpunkts oder Startpunkts für die folgende, einzulesende Information eine geeignete Zieladresse von der Datenverarbeitungseinheit an die Speichereinheit übermittelt, wobei anhand der solchermaßen vorgegebenen Zieladresse der Startpunkt für die einzulesenden Informationen vorgegeben wird.

Bei einem derartigen System können jedoch im Allgemeinen die jeweiligen Speicherinhalte direkt lesbar sein, so dass ein eingelesenes Informationselement unmittelbar auch einem auszuführenden Informationselement entspricht. Dadurch ist es bei unauthorisiertem Zugriff auf ein Speicherabbild, beispielsweise durch unauthorisiertes Auslesen des Programmspei-

chers, Röntgenmethoden oder Abschleifen des Gehäuses, grundsätzlich möglich, dass das in der Datenverarbeitungseinheit oder dem übergeordneten Datenverarbeitungssystem hinterlegte Programm oder Arbeitsprogramm anhand der Speicheradressen und -inhalte in der Art einer Rekompilierung wiederherzustellen oder zu rekonstruieren. Insbesondere kann somit das komplette Programm nebst zugehöriger Konstantwerte und möglicher Applikationsdaten wiederhergestellt werden, so dass auch bei eigentlich geheim zu haltenden Programmen oder Funktionen eine Entschlüsselung denkbar wäre.

Gerade bei geheimhaltungsbedürftigen Programmabläufen oder Informationsinhalten ist somit eine Absicherung gegen unberechtigten Zugriff nur bedingt möglich.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zum Betreiben einer Datenverarbeitungseinheit der oben genannten Art anzugeben, mit dem in der Art einer zuverlässigen Geheimhaltung eine besonders günstige Absicherung gegen unauthorisiertes Entschlüsseln von auf der Datenverarbeitungseinheit hinterlegten Programmen möglich ist. Zudem soll ein für die Durchführung des Verfahrens besonders geeignetes Datenverarbeitungssystem mit einer derartigen Datenverarbeitungseinheit angegeben werden.

Bezüglich des Verfahrens wird diese Aufgabe erfindungsgemäß gelöst, indem vor einem Zugriff der Datenverarbeitungseinheit auf die Speichereinheit die von der Datenverarbeitungseinheit jeweils ausgegebene Zieladresse über einen hinterlegten Verschlüsselungsalgorithmus in eine tatsächliche Zieladresse umgesetzt wird.

Die Erfindung geht dabei von der Überlegung aus, dass für die Datenverarbeitungseinheit eine besonders wirkungsvolle Absicherung gegen die Rekonstruktion hinterlegter Programme erreichbar ist, indem die für eine Rekompilierung erforderliche systematische Zusammenfügung einzelner Programmbausteine und

Dateninhalte systematisch erschwert wird. Dazu sollte eine geeignete Verschleierung von Querverknüpfungen zwischen einzelnen Bestandteilen oder Elementen der hinterlegten Programme oder Dateninhalte vorgesehen sein. Als ein besonders geeigneter Ansatzpunkt hierfür ist eine gezielte Verschleierung der Zieladressen vorgesehen, über die die Datenverarbeitungseinheit selektiv auf die Speichereinheit zugreift. Mit einer derartigen Verschlüsselung der Zieladressen ist somit ein konsistentes Zusammenfügen einzelner Programmelemente ohne Kenntnis des für die Verschleierung verwendeten Verschlüsselungsalgorithmus weitgehend ausgeschlossen. Mit der Verschlüsselung wird insbesondere die sogenannte Einsprungstabelle oder Interrupt-Vektor-Tabelle geeignet modifiziert, in der insbesondere die Zieladressen für die Initialisierung von Unterfunktionen oder Unterprogrammen auf der Speichereinheit hinterlegt sind.

Zur Verschlüsselung kann ein geeigneter Verschlüsselungsalgorithmus wie beispielsweise DES, Triple DES o.ä. eingesetzt sein. Eine besonders wirksame Verschleierung der verwendeten Zieladressen ist dabei auf einfache Weise erreichbar, indem vorteilhafterweise zur Umsetzung der Zieladresse in die tatsächliche Zieladresse ein Verschlüsselungsalgorithmus auf Basis eines CRC ("Cyclic Redundancy Check")-Polynoms verwendet wird.

Für eine besonders hohe Absicherung gegen unauthorisierte Entschlüsselung hinterlegter Programme ist zudem vorgesehen, dass eine Übertragung von bei der Analyse einer Datenverarbeitungseinheit gewonnenen Erkenntnissen auf eine baugleiche, andere Datenverarbeitungseinheit grundsätzlich unmöglich ist. Dazu wird vorteilhafterweise selbst für den Fall, dass eine Herstellung der jeweiligen Datenverarbeitungseinheit in vergleichsweise großen Stückzahlen vorgesehen ist, für jede individuelle Datenverarbeitungseinheit spezifisch ein eigener, nicht auf eine baugleiche andere Datenverarbeitungseinheit übertragbarer Verschlüsselungsalgorithmus verwendet. Damit

ist selbst für den Fall, dass in der Art eines unautorisierten Zugriffs durch Demontage der Datenverarbeitungseinheit von deren sämtlichen Komponenten inklusive den für die Speicherung des Verschlüsselungsalgorithmus vorgesehenen Elementen ein komplettes Speicherabbild beschafft wird, die Nutzung von daraus gewonnenen Erkenntnissen für die unautorisierte Entschlüsselung baugleicher, anderer Datenverarbeitungseinheiten ausgeschlossen.

Bezüglich des Datenverarbeitungssystems wird die genannte Aufgabe gelöst mit einem datenseitig zwischen die Datenverarbeitungseinheit und die Speichereinheit geschalteten Codiermodul, das bei einem Zugriff auf die Speichereinheit die von der Datenverarbeitungseinheit jeweils ausgegebene Zieladresse in eine tatsächliche Zieladresse umsetzt.

Vorteilhafterweise greift das Codiermodul dabei zur Umsetzung der Zieladressen auf ein CRC-Polynom zurück. In weiterer vorteilhafter Ausgestaltung ist das CRC-Polynom dabei individuell für die jeweilige Datenverarbeitungseinheit erzeugt, so dass eine spezifisch auf die jeweilige Datenverarbeitungseinheit zugeschnittene, nicht übertragbare Codierung erreichbar ist.

Eine weitere Absicherung insbesondere im Hinblick auf unautorisierte analytische Zugriffe auf die jeweilige Datenverarbeitungseinheit ist erreichbar, indem das Datenverarbeitungssystem vorteilhafterweise ein Controllermodul umfasst, das die Zugriffe auf die Speichereinheit steuert, wobei die das Codiermodul bildenden Elemente, insbesondere die für die Verschlüsselung der Zieladressen verwendeten funktionalen Bestandteile, dezentral hinterlegt sind. Durch eine derartige dezentrale Hinterlegung ist nämlich eine geschlossene, konsistente Entschlüsselung des insgesamt verwendeten Verschlüsselungsverfahrens nicht ohne weiteres möglich.

Um dabei auch eine besonders gute Absicherung gegen eine Informationsbeschaffung durch destruktive und/oder invasive Maßnahmen in die Hardwarekomponenten zu erreichen, sind die das Codiermodul bildenden Elemente in weiterer vorteilhafter Ausgestaltung in einem räumlich schwer zugänglichen Bereich des Controllermoduls hinterlegt. Als räumlich schwer zugänglicher Bereich kommt dabei insbesondere ein in der Hardwarearchitektur des Controllermoduls vergleichsweise tief- oder innenliegender Bereich in Betracht, der destruktiv oder invasiv lediglich nach Abtrag anderer wesentlicher Bestandteile des Controllermoduls zugänglich ist.

Die mit der Erfindung erzielten Vorteile bestehen insbesondere darin, dass gerade durch die Verschlüsselung der Zieladressen beim bedarfsweisen Zugriff der Datenverarbeitungseinheit auf die Speichereinheit bei einem unauthorisierten Zugriff auf die Speicherinhalte eine konsistente Rekonstruktion der hinterlegten Programme oder Funktionseinheiten weitgehend ausgeschlossen ist. Die Programm- und Dateninhalte sind somit nicht ohne weiteres auslesbar, wobei insbesondere möglicherweise unauthorisiert gewonnenes Datenmaterial ohne Kenntnis des bei der Verschlüsselung verwendeten Verfahrens und seiner Parameter nicht verwertet werden kann. Gerade das solchermaßen mögliche "Verstecken" oder "Verbergen" der Einsprung- oder Interrupt-Vektor-Tabelle auf der Speichereinheit unterbindet vergleichsweise wirkungsvoll ein Redesign von programmierter Software. Durch eine zusätzliche generische Abwandlung des Codes bei der individuellen Programmierung des Controllers oder der Datenverarbeitungseinheit lasen sich auch bei der Übertragung von Erkenntnissen zwischen Datenverarbeitungseinheiten gleichen Typs keine Rückschlüsse mehr auf die Struktur von dort hinterlegten Programmen ziehen.

Ein Ausführungsbeispiel der Erfindung wird anhand einer Zeichnung näher erläutert. Darin zeigt die Figur schematisch ein Datenverarbeitungssystem.

Das Datenverarbeitungssystem 1 gemäß der Figur umfasst eine Datenverarbeitungseinheit 2, die bestimmungs- und funktionsabhängig nach vorgegebenen Ablaufplänen Berechnungs- oder Steuerungsaufgaben abwickelt. Dazu werden bei der Programmierung der Datenverarbeitungseinheit 2 geeignete Programme oder Module hinterlegt, die für sich genommen oder in ihrem Zusammenspiel die vorgegebenen Funktionsabläufe erfüllen.

Beispielsweise zur Initialisierung weiterer Unterfunktionen oder auch zur Beschaffung notwendiger Zwischen- oder Zusatzdaten greift die Datenverarbeitungseinheit 2 bedarfsweise auf eine zugeordnete Speichereinheit 4 zu. Dabei löst das in der Datenverarbeitungseinheit jeweils gerade ablaufende Programm oder Modul zur bedarfsweisen Beschaffung weiterer Informationen oder zum bedarfsweisen Aufruf weiterer Funktionen den Zugriff auf die Speichereinheit 4 aus, wobei zum Auffinden der korrekten jeweils benötigten Daten auf der Speichereinheit 4 auf eine zugeordnete, den jeweils genutzten Speicherbereich charakterisierende Zieladresse zurückgegriffen wird. Diese Zieladresse wird von der Datenverarbeitungseinheit 2 mit an die Speichereinheit 4 ausgegeben, so dass der Aufruf der korrekten jeweils benötigten Daten sichergestellt ist.

Allerdings könnte bei einem unauthorisierten Zugriff auf die Speicherinhalte in der Datenverarbeitungseinheit 2 und der Speichereinheit 4 bei Kenntnis der die einzelnen Segmente miteinander verknüpfenden Zieladressen eine Entschlüsselung der in ihrer Gesamtheit im Datenverarbeitungssystem 2 ablaufenden Programme durch geeignete Rekonstruktion der einzelnen Bestandteile möglich sein. Das Datenverarbeitungssystem 1 ist jedoch dafür ausgelegt, einen derartigen unauthorisierten Eingriff zur Entschlüsselung möglicherweise geheimnisrelevanter Informationen sicher zu unterbinden.

Dazu ist datenseitig zwischen die Datenverarbeitungseinheit 2 und die Speichereinheit 4 ein Codiermodul 6 geschaltet. Das Codiermodul 6 setzt dabei unter Rückgriff auf ein CRC-Polynom

in der Art einer Verschlüsselung die bei einem Zugriff der Datenverarbeitungseinheit 2 auf die Speichereinheit 4 eintreffenden, zur Charakterisierung des Speicherorts für die jeweiligen Daten mitgelieferten Zieladressen in tatsächliche Zieladressen um. Dabei wird beispielsweise die sogenannte Einsprungs- oder Interrupt-Vektor-Tabelle durch Verschlüsselung auf der Grundlage des CRC-Polynoms geeignet modifiziert. Anschließend gibt das Codiermodul 6 die solchermaßen umgesetzten tatsächlich genutzten Zieladressen gemeinsam mit möglicherweise zusätzlich benötigten Daten an die Speichereinheit 4 weiter, so dass das Auslesen der angeforderten Daten anhand der im Codiermodul generierten, tatsächlichen Zieladressen erfolgt. Die solchermaßen ausgelesenen Daten werden unter Umgehung des Codiermoduls 6 über eine Datenleitung 8 an die Datenverarbeitungseinheit 2 zurückgegeben.

Hardewareseitig umfasst das Datenverarbeitungssystem 1 ein im schematischen Aufbau nach der Figur nicht mehr dargestelltes Controllermodul, das physikalisch die einzelnen Zugriffe der Datenverarbeitungseinheit 2 auf die Speichereinheit 4 steuert. In diesem Controllermodul sind die in ihrer Gesamtheit das Codiermodul 6 bildenden Elemente dezentral und zudem an einer räumlich schwer zugänglichen Stelle hinterlegt, so dass auch bei destruktiven oder invasiven Eingriffen in das Controllermodul eine Rekonstruktion der verwendeten Verschlüsselungsverfahren nicht möglich ist.

Bezugszeichenliste

1	Datenverarbeitungssystem
2	Datenverarbeitungseinheit
4	Speichereinheit
6	Codiermodul
8	Datenleitung

Patentansprüche

1. Verfahren zum Betreiben einer Datenverarbeitungseinheit (2), die bedarfsweise unter Rückgriff auf spezifisch hinterlegte Zieladressen Daten aus einer zugeordneten Speichereinheit (4) einliest, wobei vor einem Zugriff auf die Speichereinheit (4) die von der Datenverarbeitungseinheit (2) jeweils ausgegebene Zieladresse über einen hinterlegten Verschlüsselungsalgorithmus in eine tatsächliche Zieladresse umgesetzt wird.

2. Verfahren nach Anspruch 1, bei dem zur Umsetzung der Zieladresse ein Verschlüsselungsalgorithmus auf Basis eines CRC-Polynoms verwendet wird.

3. Verfahren nach Anspruch 1 oder 2, bei dem zur Umsetzung der Zieladresse ein spezifisch für die Datenverarbeitungseinheit (2) erzeugter Verschlüsselungsalgorithmus verwendet wird.

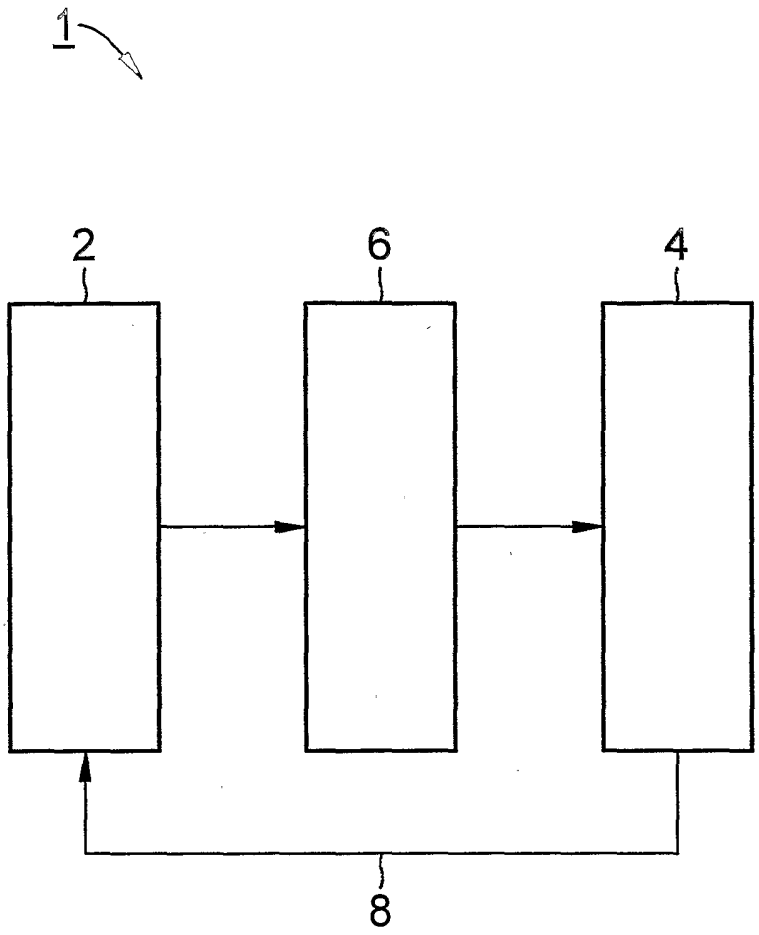
4. Datenverarbeitungssystem (1), insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 3, mit einer Datenverarbeitungseinheit (2), die bedarfsweise unter Rückgriff auf spezifisch hinterlegte Zieladressen Daten aus einer zugeordneten Speichereinheit (4) einliest, und mit einem datenseitig zwischen die Datenverarbeitungseinheit (2) und die Speichereinheit (4) geschalteten Codiermodul (6), das bei einem Zugriff auf die Speichereinheit (4) die von der Datenverarbeitungseinheit (2) jeweils ausgegebene Zieladresse in einen tatsächliche Zieladresse umsetzt.

5. Datenverarbeitungseinheit (2) nach Anspruch 4, dessen Codiermodul (6) zur Umsetzung der Zieladressen auf ein CRC-Polynom zurückgreift.

6. Datenverarbeitungssystem (1) nach Anspruch 5, bei dem das CRC-Polynom individuell für die Datenverarbeitungseinheit (2) erzeugt ist.

7. Datenverarbeitungssystem (1) nach einem der Ansprüche 4 bis 6 mit einem Controllermodul, das die Zugriffe auf die Speichereinheit (4) steuert, und in dem die das Codiermodul (6) bildenden Elemente dezentral hinterlegt sind.

8. Datenverarbeitungssystem (1) nach Anspruch 7, bei dem das Codiermodul (6) bildende Elemente in einem räumlich schwer zugänglichen Bereich des Controllermoduls hinterlegt sind.


1
2
6
4
8